Micro Focus Security
ArcSight ESM CIP for PCI

Compliance Insight Package for the Payment Card Industry

Solutions Guide

Document Release Date: August 31, 2019
Software Release Date: August 31, 2019

Legal Notices

Copyright Notice

Trademark Notices

Support

Contact Information

Phone	A list of phone numbers is available on the Technical Support Page: https://softwaresupport.softwaregrp.com/support-contact-information
Support Web Site	https://softwaresupport.softwaregrp.com/
ArcSight Product Documentation	https://community.softwaregrp.com/t5/ArcSight-Product-Documentation/ct-p/productdocs

Contents

Chapter 1: Overview

This section contains the following topics:

The PCI DSS

The Payment Card Industry (PCI) Data Security Standard (DSS) PCI DSS 3.2.1 is a comprehensive standard defined by the Payment Card Industry Security Standards Council to help organizations protect customer account data and to advance the broad adoption of consistent data security measures across the globe. The standard includes twelve requirements, each with many sub-requirements, for security management, policies, procedures, network architecture, software design, and other key protective measures.

The following table lists the PCI DSS requirements.

Note: Excerpts from the PCI DSS and related control statements are provided courtesy of PCI Security Standards Council, LLC and/or its licensors. © 2014 PCI Security Standards Council, LLC. All Rights Reserved.

Objectives	PCI DSS Requirements
Build and Maintain a Secure Network	**1.** Install and maintain a firewall configuration to protect cardholder data **2.** Do not use vendor-supplied defaults for system passwords and other security parameters
Protect Cardholder Data	**3.** Protect stored cardholder data **4.** Encrypt transmission of cardholder data across open, public networks
Maintain a Vulnerability Management Program	**5.** Use and regularly update anti-virus software or programs **6.** Develop and maintain secure systems and applications

Objectives	PCI DSS Requirements
Implement Strong Access Control Measures	**7.** Restrict access to cardholder data by business need to know **8.** Identify and authenticate access to system components **9.** Restrict physical access to cardholder data
Regularly Monitor and Test Networks	**10.** Track and monitor all access to network resources and cardholder data **11.** Regularly test security systems and processes
Maintain an Information Security Policy	**12.** Maintain a policy that addresses information security for all personnel

Compliance Insight Package for Payment Card Industry (CIP for PCI) coupled with ArcSight ESM can assist you in complying with the requirements specified in the (DSS) PCI DSS 3.2.1, and includes support for logs generated by payment applications subject to the Payment Application Data Security Standard PCI DSS 3.2.1.

The CIP for PCI Compliance Framework

CIP for PCI provides the following benefits:

- CIP for PCI maintains a ***compliance score*** for each asset in your PCI environment, so dashboards and reports can demonstrate your organization's overall PCI compliance and individual asset compliance.
- 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 each asset's compliance score. You can also create custom scenario rules to address organizational, regional, and national regulations and policies.
- The CIP for PCI resources 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 CIP.
- There is an overall compliance status use case and a use case for each security domain group. The domain-based use cases can apply to multiple regulations.
- In this 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***.

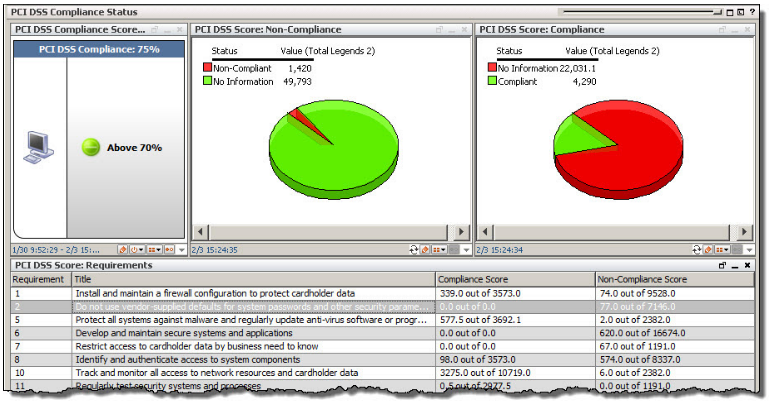
What CIP for PCI Can Do for You

The CIP for PCI helps demonstrate to stakeholders and auditors that the controls over the credit card data systems of your organization expose little or no risk.

CIP for PCI provides dashboards, reports, and real-time checks to monitor systems that:

- Contain cardholder data
- Manage vulnerability and access control
- Monitor networks
- Maintain security policies

CIP for PCI calculates compliance and non-compliance scores for assets in your PCI environment. In the following dashboard, those scores are aggregated to provide an overall picture of compliance in your organization.



PCI DSS Compliance Status

PCI DSS Compliance Score...

PCI DSS Compliance: 75%

Above 70%

1/30 9:52:29 - 2/3 15:...

PCI DSS Score: Non-Compliance

Status	Value (Total Legends 2)
🟥 Non-Compliant	1,420
🟩 No Information	49,793

2/3 15:24:35

PCI DSS Score: Compliance

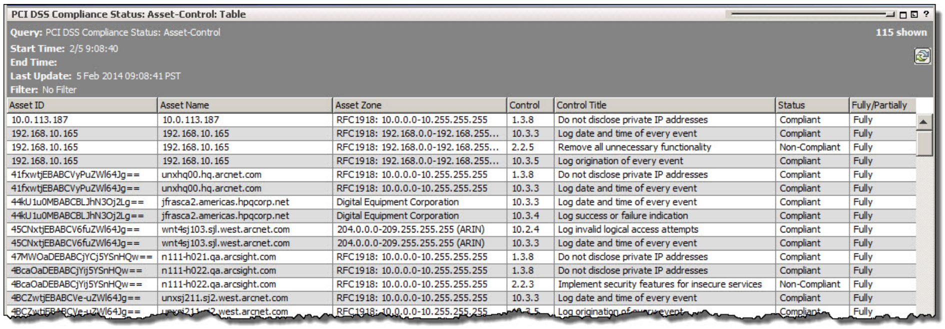
Status	Value (Total Legends 2)
🟥 No Information	22,031.1
🟩 Compliant	4,290

2/3 15:24:34

PCI DSS Score: Requirements

Requirement	Title	Compliance Score	Non-Compliance Score
1	Install and maintain a firewall configuration to protect cardholder data	339.0 out of 3573.0	74.0 out of 9528.0
2	Do not use vendor-supplied defaults for system passwords and other security parame...	0.0 out of 0.0	77.0 out of 7146.0
5	Protect all systems against malware and regularly update anti-virus software or progr...	577.5 out of 3692.1	2.0 out of 2382.0
6	Develop and maintain secure systems and applications	0.0 out of 0.0	620.0 out of 16674.0
7	Restrict access to cardholder data by business need to know	0.0 out of 0.0	67.0 out of 1191.0
8	Identify and authenticate access to system components	98.0 out of 3573.0	574.0 out of 8337.0
10	Track and monitor all access to network resources and cardholder data	3275.0 out of 10719.0	6.0 out of 2382.0
11	Regularly test security systems and processes	0.5 out of 2977.5	0.0 out of 1191.0

You can drill down from this dashboard to detailed information about individual asset compliance, as shown below:



PCI DSS Compliance Status: Asset-Control: Table

Query: PCI DSS Compliance Status: Asset-Control

Start Time: 2/5 9:08:40

End Time:

Last Update: 5 Feb 2014 09:08:41 PST

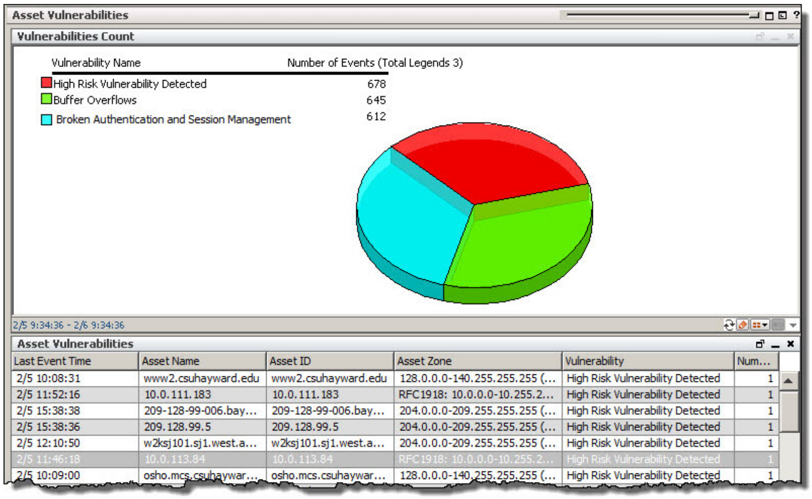
Filter: No Filter

115 shown

Asset ID	Asset Name	Asset Zone	Control	Control Title	Status	Fully/Partially
10.0.113.187	10.0.113.187	RFC1918: 10.0.0.0-10.255.255.255	1.3.8	Do not disclose private IP addresses	Compliant	Fully
192.168.10.165	192.168.10.165	RFC1918: 192.168.0.0-192.168.255...	10.3.3	Log date and time of every event	Compliant	Fully
192.168.10.165	192.168.10.165	RFC1918: 192.168.0.0-192.168.255...	2.2.5	Remove all unnecessary functionality	Non-Compliant	Fully
192.168.10.165	192.168.10.165	RFC1918: 192.168.0.0-192.168.255...	10.3.5	Log origination of every event	Compliant	Fully
41fxwtjEBABCVyPuZWl64Jg==	unxhq00.hq.arcnet.com	RFC1918: 10.0.0.0-10.255.255.255	1.3.8	Do not disclose private IP addresses	Compliant	Fully
41fxwtjEBABCVyPuZWl64Jg==	unxhq00.hq.arcnet.com	RFC1918: 10.0.0.0-10.255.255.255	10.3.3	Log date and time of every event	Compliant	Fully
44kU1u0MBABCBLJhN3Oj2Lg==	jfrasca2.americas.hpqcorp.net	Digital Equipment Corporation	10.3.3	Log date and time of every event	Compliant	Fully
44kU1u0MBABCBLJhN3Oj2Lg==	jfrasca2.americas.hpqcorp.net	Digital Equipment Corporation	10.3.4	Log success or failure indication	Compliant	Fully
45CNxtjEBABCV6fuZWl64Jg==	wnt4sj103.sjl.west.arcnet.com	204.0.0.0-209.255.255.255 (ARIN)	10.2.4	Log invalid logical access attempts	Compliant	Fully
45CNxtjEBABCV6fuZWl64Jg==	wnt4sj103.sjl.west.arcnet.com	204.0.0.0-209.255.255.255 (ARIN)	10.3.3	Log date and time of every event	Compliant	Fully
47MWOaDEBABCjYCj5YSnHQw==	n111-h021.qa.arcsight.com	RFC1918: 10.0.0.0-10.255.255.255	1.3.8	Do not disclose private IP addresses	Compliant	Fully
4BcaOaDEBABCjYij5YSnHQw==	n111-h022.qa.arcsight.com	RFC1918: 10.0.0.0-10.255.255.255	1.3.8	Do not disclose private IP addresses	Compliant	Fully
4BcaOaDEBABCjYij5YSnHQw==	n111-h022.qa.arcsight.com	RFC1918: 10.0.0.0-10.255.255.255	2.2.3	Implement security features for insecure services	Non-Compliant	Fully
4BCZwtjEBABCVe-uZWl64Jg==	unxsj211.sj2.west.arcnet.com	RFC1918: 10.0.0.0-10.255.255.255	10.3.3	Log date and time of every event	Compliant	Fully
4BCZwtjEBABCVe-uZWl64Jg==	unxsj211.sj2.west.arcnet.com	RFC1918: 10.0.0.0-10.255.255.255	10.3.5	Log origination of every event	Compliant	Fully

For more information about this dashboard, see "Using the PCI DSS Compliance Status Dashboard" on page 57.

Several other dashboards show domain-specific information, such as Asset Vulnerabilities:



Asset Vulnerabilities

Vulnerabilities Count

Vulnerability Name	Number of Events (Total Legends 3)
🟥 High Risk Vulnerability Detected	678
🟩 Buffer Overflows	645
🟦 Broken Authentication and Session Management	612

2/5 9:34:36 - 2/6 9:34:36

Asset Vulnerabilities

Last Event Time	Asset Name	Asset ID	Asset Zone	Vulnerability	Num...
2/5 10:08:31	www2.csuhayward.edu	www2.csuhayward.edu	128.0.0.0-140.255.255.255 (...	High Risk Vulnerability Detected	1
2/5 11:52:16	10.0.111.183	10.0.111.183	RFC1918: 10.0.0.0-10.255.2...	High Risk Vulnerability Detected	1
2/5 15:38:38	209-128-99-006.bay...	209-128-99-006.bay...	204.0.0.0-209.255.255.255 (...	High Risk Vulnerability Detected	1
2/5 15:38:36	209.128.99.5	209.128.99.5	204.0.0.0-209.255.255.255 (...	High Risk Vulnerability Detected	1
2/5 12:10:50	w2ksj101.sj1.west.a...	w2ksj101.sj1.west.a...	204.0.0.0-209.255.255.255 (...	High Risk Vulnerability Detected	1
2/5 11:46:18	10.0.113.84	10.0.113.84	RFC1918: 10.0.0.0-10.255.2...	High Risk Vulnerability Detected	1
2/5 10:09:00	osho.mcs.csuhaywar...	osho.mcs.csuhaywar...	128.0.0.0-140.255.255.255 (...	High Risk Vulnerability Detected	1

In addition to the dashboards, you can run detailed reports to demonstrate compliance to auditors and convey issues to stakeholders for remediation.

How CIP for PCI Works

CIP for PCI relies on ArcSight asset categorization to define your PCI environment. By evaluating events from that environment, CIP for PCI tracks asset compliance for PCI DSS sub-requirements and uses that information to provide an overall compliance picture.

CIP for PCI uses ***compliance scenario rules*** and ***compliance scores*** to determine compliance.

Compliance Scenario Rules

Compliance scenario rules detect events that affect compliance and non-compliance, for example, unauthorized access to cardholder data or insecure password transmission. The rule names are typically an abbreviation of the requirement description found in the PCI DSS. Each PCI DSS sub-requirement addressed by CIP for PCI is mapped to a single compliance scenario rule.

In addition to the out-of-the-box compliance scenario rules, you can create custom rules, as described in "Creating Custom Compliance Scenarios" on page 29.

For a list of the compliance scenario rules, see "Rules" on page 109. For a list of rules organized by requirement, see "Compliance Scenario Configuration" on page 33. For a list of rules mapped to PCI DSS requirements within the ArcSight Console, see the Scenario Controls active list.

Compliance Scores

The compliance score indicates whether an asset is compliant with a PCI DSS sub-requirement. In the CIP for PCI reports and dashboards, the score for an asset is either 1, indicating compliance, 0, indicating non-compliance, or between 0 and 1, indicating partial compliance. CIP for PCI aggregates the asset scores to provide compliance and non-compliance scores for your organization.

CIP for PCI determines the compliance score by using the ***impact type*** attribute of each scenario rule and a few key active lists. If you plan to create your own scenario rules or you are interested in how the impact type affects the score, see "Scenario Impact Type" on page 31.

CIP for PCI Resources

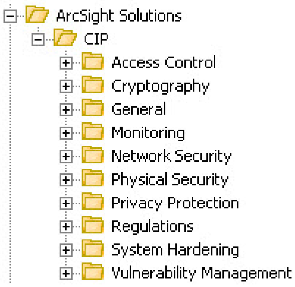
CIP for PCI contains the following ArcSight ESM resources:

- **Active channel**—CIP for PCI provides an active channel that shows all the events related to the compliance scenarios.
- **Active Lists**—CIP for PCI contains active lists that capture static and dynamic data about compliance-related assets and events to aid in compiling and correlating data for the various PCI requirements.
- **Asset Categories**—CIP for PCI uses asset categories to classify your compliance-relevant devices.
- **Dashboards** and **Data Monitors**—CIP for PCI provides graphical dashboards to help you demonstrate appropriate risk management and monitoring practices.
- **Global Variables**—CIP for PCI contains global variables that provide the ability to derive particular values from existing data fields. A global variable can be defined once, then re-used in multiple places wherever conditions can be expressed (active channels, rules, filters, data monitors, and queries), and wherever fields can be selected (CCE, field sets).
- **Filters**—CIP for PCI contains dozens of filters that focus package content on activity that involves compliance-relevant categorized assets.
- **Queries**—CIP for PCI contains queries that gather the compliance-related event data displayed by reports.
- **Query Viewers**—CIP for PCI contains query viewers that allow you to drill down and investigate anomalies or other interesting events without having to create low-level active channels. Query viewers use events and other resources, such as trends, active lists, session lists, assets, cases, and notifications, as data sources.
- **Reports**—CIP for PCI contains reports that focus on several aspects of regulation compliance.
- **Rules**—CIP for PCI includes real-time rules to immediately identify activity that presents a high risk to the integrity of your systems that store and process compliance-relevant data.
- **Trends**—CIP for PCI contains trends that define how and over what time period data is aggregated and evaluated for prevailing tendencies or currents. A trend executes a specified query on a defined schedule and time duration.

All CIP for PCI resources are described in "Compliance Insight Package for the Payment Card Industry Resources by Type" on page 66.

Resources Organized by Domains

Most of the CIP for PCI resources are organized by the following functional domain groups:

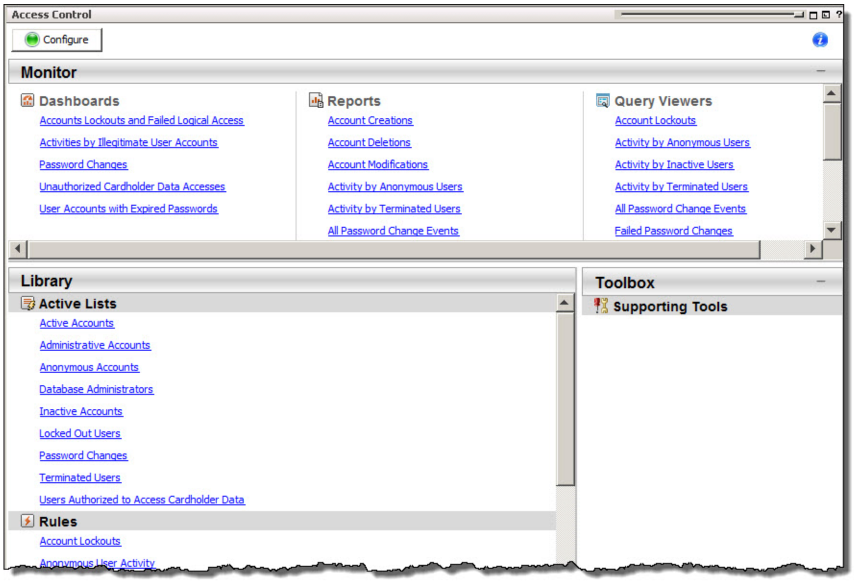


ArcSight Solutions
CIP
Access Control
Cryptography
General
Monitoring
Network Security
Physical Security
Privacy Protection
Regulations
System Hardening
Vulnerability Management

Each group contains domain-specific resources, as described below.

Access Control	Resources that pertain to access issues, such as the use of inactive or locked accounts, terminated users, unauthorized access, password changes and expirations, improper access control, and failed logical access.
Cryptography	Resources that pertain to encryption violations and the insecure transmission of sensitive data.
General	Resources that do not affect compliance directly, but can be referenced by other CIP for PCI resources.
Monitoring	Resources that pertain to object creation or deletion, cleared audit logs, file integrity tools, and events that include information such as origination, user accounts, and time inconsistencies.
Network Security	Resources that pertain to network perimeter protection mechanisms, such as a DMZ, IDS, or firewall, unauthorized access points, and disallowed ports.
Physical Security	Resources that pertain to physical access attempts.
Privacy Protection	Resources that pertain to the unacceptable disclosure of personal information, such as passwords and account numbers.
Regulations	Resources that are specific to a particular regulation, such as the PCI DSS.
System Hardening	Resources that pertain to system surface vulnerabilities, including the use of custom or default vendor accounts, insecure services, multi-function servers, and unnecessary functionality.
Vulnerability Management	Resources that pertain to infrastructure and application vulnerabilities, such as anti-virus issues, broken authentication, buffer overflows, cross-site scripting, injection flaws, missing security patches, misconfiguration, improper error handing, and malware.

There is a use case resource for each domain group. The use cases provide easy access to the resources for a particular domain. The Access Control use case is shown below.



Access Control

Configure

Monitor

Dashboards

- Accounts Lockouts and Failed Logical Access
- Activities by Illegitimate User Accounts
- Password Changes
- Unauthorized Cardholder Data Accesses
- User Accounts with Expired Passwords

Reports

- Account Creations
- Account Deletions
- Account Modifications
- Activity by Anonymous Users
- Activity by Terminated Users
- All Password Change Events

Query Viewers

- Account Lockouts
- Activity by Anonymous Users
- Activity by Inactive Users
- Activity by Terminated Users
- All Password Change Events
- Failed Password Changes

Library

Active Lists

- Active Accounts
- Administrative Accounts
- Anonymous Accounts
- Database Administrators
- Inactive Accounts
- Locked Out Users
- Password Changes
- Terminated Users
- Users Authorized to Access Cardholder Data

Rules

- Account Lockouts
- Anonymous User Activity

Toolbox

Supporting Tools

Supported Devices

CIP for PCI acts on events from systems that store and process credit card data, and the systems that interact with and protect those systems, including the following:

- Applications that process cardholder data
- Databases that store cardholder data
- Operating systems
- Host and network-based IDS
- Firewalls
- Anti-virus solutions
- Vulnerability scanners that monitor system state

What Next?

Before you begin using the CIP for PCI use cases, dashboards, and reports, you need to install the CIP for PCI solution package and perform some general configuration. Minimally, you need to:

- Categorize assets and zones to define your PCI environment
- Deploy and enable rules
- Enable trends
- Enable data monitors

For details, see "Installation and General Configuration" on page 16.

After you complete the general configuration, you can configure additional resources to address the individual PCI DSS requirements, as described in "Compliance Scenario Configuration" on page 33.

Chapter 2: Installation and General Configuration

This section explains how to install and configure the Compliance Insight Package for the Payment Card Industry (CIP for PCI):

Preparing for Installation

Before installing CIP for PCI, prepare your environment.

To prepare your environment:

1. Verify that your version of ESM CIP for PCI supports this version of CIP for PCI. Check the ***ArcSight Compliance Insight Package for PCI Release Notes***.
2. Verify that your system has an ArcSight Console connected to the ArcSight Manager and that your system meets the prerequisites for your operating system, as detailed in the ***ESM CIP for PCI Support Matrix***.
3. Install and configure the appropriate ***SmartConnector***s for the devices found in your environment.

   The devices that provide events for each PCI requirement are listed in "Supported Devices" on page 15.
4. Model your network to include devices that supply events that help satisfy the PCI requirements. Verify that zones and networks are defined for your environment, and that networks are assigned to the connectors reporting PCI-relevant events to your ArcSight Manager. For more information, see "Modeling Assets" on page 21.

   Learn more about the ArcSight network modeling process in the ***ESM CIP for PCI 101 Guide***. Find instructions on how to configure zones and networks in the ***ArcSight Console User's Guide***.

Micro Focus provides a digital public key to enable you to verify that the signed software you received is indeed from Micro Focus and has not been manipulated in any way by a third party.

Visit the following site for information and instructions:

https://h22253.www2.hpe.com/ecommerce/efulfillment/digitalSignIn.do

Upgrading from PCI 4.0 to 4.1

Before you begin:

Do you have active lists in PCI 4.0 that have data, and you want to continue using them? If so, the upgrade process starts with exporting the list data. This step is optional if you do not want list data from PCI 4.0.

To export active list data from PCI 4.0 into a CSV file:

This example uses the Administrative Accounts active list.

1. In the Navigator panel, select the **Resources** tab and select **Lists**.
2. Locate the CIP for PCI 4.0 active lists.
3. Right-click the active list whose data you want to export select **Show Entries**.

   The active list displays entries in the Viewer.
4. In the Viewer panel, select all the entries, right-click, and select **Export | CSV - All Columns**.
5. Enter an applicable filename, for example **AdministrativeAccounts**, and click **Save**.

   A CSV file is saved on the file system, such as `AdministrativeAccounts.csv`.
6. Repeat for each applicable 4.0 active list with entries you want to reuse after the upgrade.

To upgrade from PCI 4.0 to CIP for PCI 4.1:

1. Back up the CIP for PCI v4.0 resources currently on the ArcSight ESM Manager into one package bundle (.arb) file.

   For detailed instructions, see "Backing Up and Uninstalling a Package" on page 62.
2. Install CIP for PCI V4.1. Follow the instructions provided in the section "Installing CIP for PCI " on the next page.

To import values from a CSV file to a PCI 4.1 active list:

1. In the Navigator panel, select the **Resources** tab and select **Lists**.
2. Locate the active list that is getting the data. For example, if you exported data for Administrative Accounts, select that list.
3. Right-click the active list and select **Import CSV File**.
4. Browse for the corresponding CSV file containing the active list entries created in the previous procedure, for example, `AdministrativeAccounts.csv`, and click **Open**.
5. Click **OK** to add entries to the list.

For more information, refer to "Configuring Active Lists" on page 24.

Installing CIP for PCI

CIP for PCI is a self-contained solution that does not rely on any other ArcSight solution. You can install CIP for PCI alongside other solutions on the same ArcSight Manager. However, 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.

Before installing a new solution, back up any existing solutions installed on the ArcSight Manager. For detailed instructions, see "Backing Up and Uninstalling a Package" on page 62.

> **Caution:** There is no migration path from CIP for PCI 3.*X*. If you are running CIP for PCI 3.*X* and you need to keep your current data, do not uninstall; instead install CIP for PCI 4.1 on a different system.

Micro Focus provides a digital public key to enable you to verify that the signed software you received is indeed from Micro Focus and has not been manipulated in any way by a third party.Visit the following site for information and instructions:https://h22253.www2.hpe.com/ecommerce/efulfillment/digitalSignIn.do

To install the CIP for PCI:

1. Download the following CIP for PCI package bundle to the computer where you plan to run the ArcSight Console:

   `ArcSight-ComplianceInsightPackage-PCI.4.1.<nnnn>.0.arb`

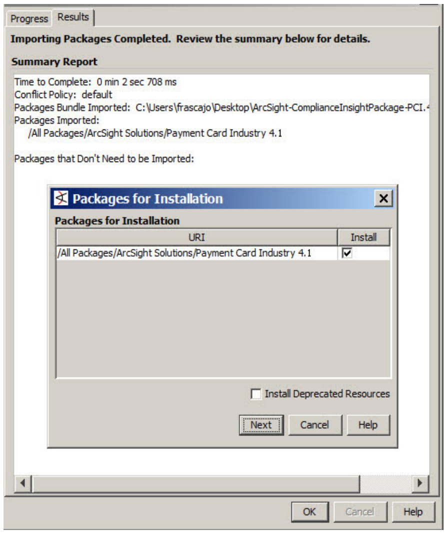
   Where `<nnnn>` is the 4 character build number specified in the ArcSight Compliance Insight Package for PCI Release Notes.

   > **Caution:** 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.

2. Log into the ArcSight Console with an account that has administrative privileges.
3. In the Navigator panel, click the **Packages** tab.
4. Click **Import** (⬇).
5. In the Open dialog, browse and select the package bundle file, and then select **Open**.

   The Progress tab of the Importing Packages dialog shows how the package bundle import is progressing.

   When the import is complete, the Results tab of the Importing Packages dialog is displayed together with the Packages for Installation dialog, as shown in the following figure.



Importing Packages Completed. Review the summary below for details.

Summary Report

```
Time to Complete:  0 min 2 sec 708 ms
Conflict Policy:  default
Packages Bundle Imported:  C:\Users\frascajo\Desktop\ArcSight-ComplianceInsightPackage-PCI.4
Packages Imported:
    /All Packages/ArcSight Solutions/Payment Card Industry 4.1

Packages that Don't Need to be Imported:
```

Packages for Installation

URI	Install
/All Packages/ArcSight Solutions/Payment Card Industry 4.1	☑

□ Install Deprecated Resources

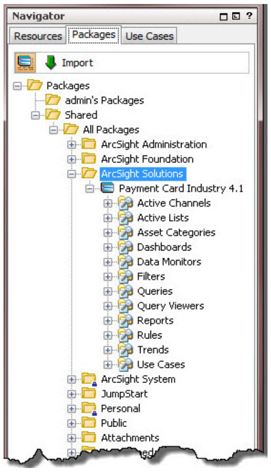
6. In the Packages for Installation dialog, leave the `Payment Card Industry 4.1` checkbox selected and click **Next**.

   The Installing Packages dialog opens. The Progress tab shows how the installation is progressing. When the installation is complete, the Results tab displays the Summary Report.

7. In the Installing Packages dialog, click **OK**.

8. In the Importing Packages dialog, click **OK**.

9. On the **Packages** tab of the Navigator panel, expand the `ArcSight Solutions/Payment Card Industry 4.1` group to verify that the installation is successful and that the content is accessible in the Navigator panel.



If the installation is not successful, contact ArcSight technical support. See "Support" on page 2.

To back up or uninstall the CIP for PCI at a later date, see "Backing Up and Uninstalling a Package" on page 62.

Configuring CIP for PCI

Several of the CIP for PCI resources need to be configured with values specific to your environment. Some features also require additional ArcSight SmartConnector configuration.

Depending on the features you want to implement and how your network is set up, some configuration is required and some is optional. The list below shows the configuration tasks for the CIP for PCI and where to find instructions for performing the configuration.

Assigning User Permissions

By default, users in the **`Default`** user group can view CIP for PCI content, and users in the **`ArcSight Administrators`** and **`Analyzer Administrators`** user groups have read and write access to the solution content. Depending on how you set up user access controls within your organization, you might need to adjust those controls to make sure the new content is accessible to the right users in your organization.

The following process assumes that you have user groups set up and users assigned to those groups.

In the following procedure, assign user permissions to all the following resource types:

- Active Channels
- Active Lists
- Asset Categories
- Cases
- Dashboards
- Data Monitors
- Fields (Global Variables)

- Filters
- Queries
- Query Viewers
- Reports
- Rules
- Trends
- Use Cases

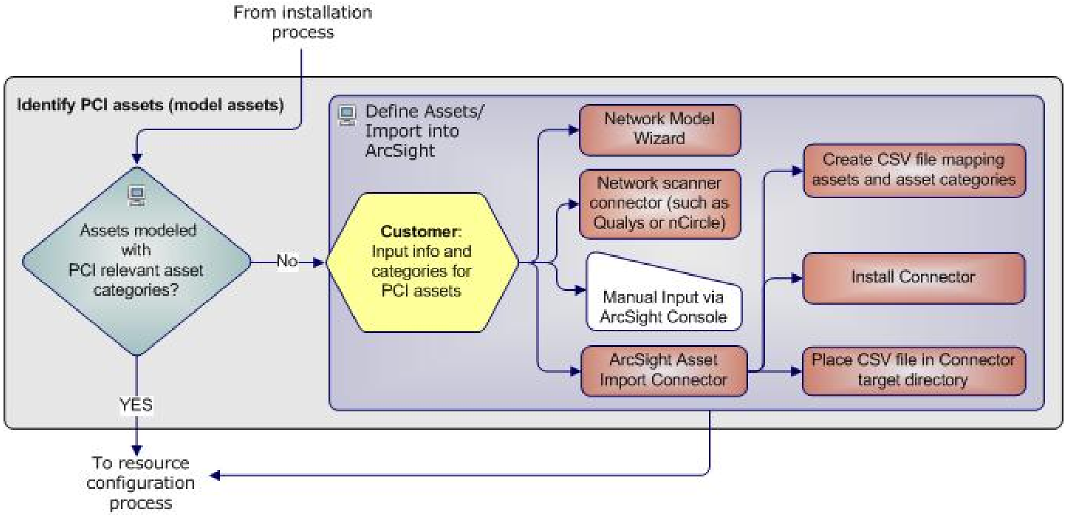
To assign user permissions:

1. Log into the ArcSight Console with an account that has administrative privileges.
2. For all the resource types listed above, change the user permissions:
   a. In the Navigator panel, go to the resource type and navigate to `ArcSight Solutions/CIP`.
   b. Right-click the `CIP` group and select **Edit Access Control** to open the ACL editor in the Inspect/Edit panel.
   c. In the ACL editor of the Inspect/Edit panel, select the user groups for which you want to grant permissions to the CIP for PCI resources and click **OK**.

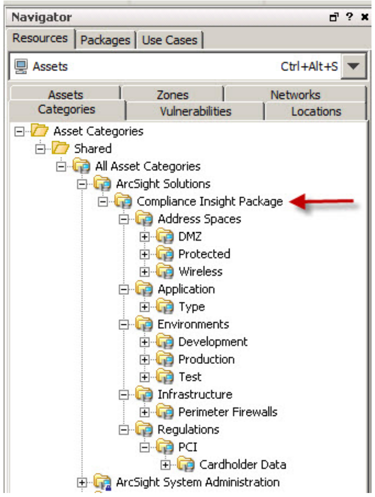
Modeling Assets

Asset modeling is required to activate CIP for PCI content. Classifying assets in one or more asset category is essential.

Some of the CIP for PCI content requires assets to be modeled to function correctly. In some cases, modeling assets adds valuable business context to the events being evaluated by the CIP for PCI


From installation process
Identify PCI assets (model assets)
Assets modeled with PCI relevant asset categories?
No
YES
To resource configuration process
Define Assets/ Import into ArcSight
Customer: Input info and categories for PCI assets
Network Model Wizard
Network scanner connector (such as Qualys or nCircle)
Manual Input via ArcSight Console
ArcSight Asset Import Connector
Create CSV file mapping assets and asset categories
Install Connector
Place CSV file in Connector target directory

CIP for PCI uses the asset categories under the`/ArcSight Solutions/Compliance Insight Package`/ group shown below.



Categorizing Assets and Zones

CIP for PCI relies on ArcSight asset categorization to define your PCI environment. Certain content does not display unless assets or zones are categorized.

For detailed information about which assets need to be categorized for each PCI DSS requirement, see "Compliance Scenario Configuration" on page 33.

You can assign the solution asset categories with the following methods.

- One-by-One from the ArcSight Console
- Using the Network Model Wizard
- If you have many assets that you want to track, you can configure them in a batch using the ArcSight Asset Import Connector. This connector can also create new assets as part of the batch function. For instructions about how to use this connector to configure your assets for CIP for PCI, see the ArcSight Asset Import *SmartConnector* Configuration Guide.

For information about how to assign asset categories using the ArcSight Console tools, refer to the ***ArcSight Console User's Guide***.

Deploying and Enabling Rules

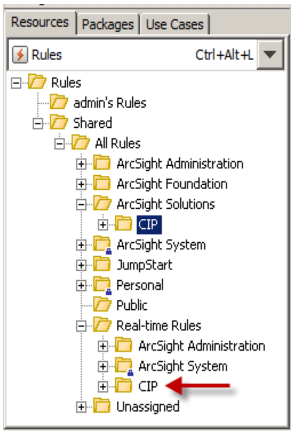
For CIP for PCI to process PCI-related events, the CIP for PCI rules must be deployed to the `Real-time Rules` group.

To deploy the CIP for PCI rules:

1. From the Resources tab in the Navigator panel, go to **Rules** and navigate to the `ArcSight Solutions/CIP` group.

2. Right-click the `CIP` group and select **Deploy Real-time Rule(s)**.

   A new `Real-time Rules/CIP` group is created as a link to the original `ArcSight Solutions/CIP` group, as shown in the following figure.



By default, the CIP for PCI rules are disabled. The rules do not trigger until they are deployed and enabled. After you have deployed the CIP for PCI rules to the `Real-time Rules` group, you can enable individual rules.

Rules can place an additional load on the ArcSight Manager. Enable only the rules for the compliance scenarios you want to implement.

Note: You must enable the PCI DSS rule in the `ArcSight Solutions/CIP/Regulation Rules` group. You can enable the rule before or after you enable the scenario rules. However, until the PCI DSS rule is enabled, the Compliance Score active list is not updated with the asset data captured by scenario rules.

To enable a rule:

1. In the Navigator panel, go to **Rules** and navigate to the `Real-time Rules/CIP` group.
2. Navigate to the rule you want to enable.
3. Right-click the rule and select **Enable Rule**.

   To select multiple rules, press the **Ctrl** key and click each rule.

   To select a range of rules, press the **Ctrl** and **Shift** keys and click the first and last rule in the range.

After you enable the rules, you can see the correlation events created by the rules in the Compliance Scenario Correlation Events active channel. Right-click the active channel in the Navigator panel and select **Show Active Channel**.

Configuring General Filters

Configure the following general filters stored in the `General` group to reflect your organization.

Filter	Description
Event Limit	Use this filter to limit the events processed and reported by CIP for PCI. For example, you can exclude events with a destination of a particular port. This filter is included in the conditions of all the CIP for PCI rules. Edit this filter to change the events processed and reported by this solution.
Internal Source	This filter identifies events originating from systems inside the network in your organization. Review the filter conditions and modify as necessary for your environment.
Internal Destination	This filter identifies events targeting systems inside the network in your organization. Review the filter conditions and modify as necessary for your environment.

Configuring Active Lists

CIP for PCI contains active lists that retain specific data that is cross-referenced dynamically during run-time by ArcSight resources that use conditions, such as filters, rules, and reports.

This section provides information about the active lists that affect the entire CIP for PCI solution. For information about the active lists that affect specific PCI DSS requirements, see "Compliance Scenario Configuration" on page 33.

Ignoring Assets and Network Zones

Use the PCI DSS Ignore List active list to identify assets or network zones that are irrelevant to the PCI DSS regulation and are ignored by CIP for PCI.

When adding entries to the active list:

- An asset is identified by either its IP address, host name, or ESM resource ID. You must use the ESM resource ID if the asset is known to the ArcSight Manager and has, therefore, been assigned an ESM resource ID.
- Host names must be entered in lowercase text.
- ESM resource IDs, IP addresses, and zone names must be entered as is, in their original case text.
- Both the Asset ID and Asset Zone fields must be specified.
- An asterisk (*) indicates all assets or all zones, as shown in the examples below.

Examples

To ignore an asset by IP address in a zone:

```
Asset ID = 10.0.0.0
Asset Zone = RFC1918: 10.0.0.0-10.255.255.255
```

To ignore all assets in a zone:

```
Asset ID = *
Asset Zone = RFC1918: 10.0.0.0-10.255.255.255
```

To ignore an asset by host name in all zones:

```
Asset ID = myhostname
Asset Zone = *
```

To ignore an asset by ESM resource ID in a zone:

```
Asset ID = 4K5yF+EMBABCU--70AvXMzg==
Asset Zone = RFC1918: 10.0.0.0-10.255.255.255
```

Populating the Active Lists

You can populate the CIP for PCI active lists using any of the following processes:

- Add entries to active lists, one-by-one, using the Active List editor in the ArcSight Console. For detailed instructions, see "Configuring Active Lists Using ArcSight Console" below. You can use this method to populate active lists with one, two, or more columns.
- Add entries in batch to active lists from a comma-separated value (CSV) file. For detailed instructions see "Configuring Active Lists by Importing a CSV File" on the next page. You can use this method to populate active lists with one, two, or more columns.

For a complete list (with descriptions) of all active lists provided with CIP for PCI, see "Active Lists" on page 67.

Configuring Active Lists Using ArcSight Console

You can add entries to active lists, one-by-one, using the Active List editor of the ArcSight Console.

1. In the Navigator panel, go to **Lists** and navigate to `ArcSight Solutions/CIP`.
2. Right-click the active list you want to populate and select **Show Entries**. The active list details are displayed in the Viewer panel.
3. For each entry you want to add to the active list, repeat the following steps:
   a. To add an entry to the list, click the add icon (✚) in the active list header.
   b. In the **Active List Entry** editor of the Inspect/Edit panel, enter values for each column in the list except for the dynamic columns listed in the following table and click **Add**.

Name	Value
Creation Time	This field is reserved for active lists that are populated dynamically by rule actions. Leave this field blank.
Last Seen Time	This field is reserved for active lists that are populated dynamically by rule actions. Leave this field blank.
Count	This field is reserved for active lists that are populated dynamically by rule actions. Leave this field unchanged.

Configuring Active Lists by Importing a CSV File

You can populate active lists in a single step by importing entries from an existing CSV file. The number of columns in the active list must match the number of comma-separated values in the CSV file. For example, if the active list has two columns of data, the imported CSV file must have two comma-separated fields.

1. In the Active Lists resource tree of the ArcSight Console, right-click an active list and choose **Import CSV File**.

   A file browser displays.

2. Browse to find the CSV file you want to import, select it, and click **Open**. The Import Preview dialog displays the data from the CSV file to be imported into the active list.
3. To add the entries from the selected file into the active list, click **OK** in the Import Preview dialog. The new entries from the file are appended to the existing entries in the active list.
4. To verify that your entries are imported as expected, right-click the active list you just populated with the CSV file and select **Show Entries**.

   This displays the newly-added data from the CSV file in the Viewer panel as active list details.

   Tip: By default, the active list displays 2000 entries at a time. To view entries outside this range, create an active list filter that specifies a different range (click **Filter** in the active list header).

Testing Filters

Most of the content in the CIP for PCI relies on event categorization fields to identify events of interest. Although this method applies to most of the events and devices, for certain scenarios, test key filters to verify that they actually capture the required events. This section describes how to test filters.

Caution: Perform the following procedure on a test system.

To ensure that a filter captures the relevant events:

1. Generate or identify the required events and verify that they are being processed by ArcSight ESM by viewing them in an active channel or query viewer.

   Note: To generate relevant events and send them to ArcSight ESM, you can either:

- Set up a connector to capture events from a target system and perform the actions that would generate the required events on that system.
- Import into ArcSight ESM an existing batch file that contains relevant events.

Alternatively, you can identify that these types of events have already been processed by ArcSight ESM and ensure that the start and end time of the active channel or query viewer (as shown in the next step) covers the event time of these events.

2. Navigate to the appropriate filter, right-click it, and then choose **Create Channel with Filter**. If you see the events of interest in the newly created channel, the filter is functioning properly.

   If you do not see the events of interest:

   a. Verify that the configuration of the active channel is suitable for the events in question. For example, ensure that the event time is within the start and end time of the channel.

   b. Modify the filter condition to capture the events of interest. After applying the change, repeat this step to verify that the modified filter captures the required events.

Enabling and Testing Trends

By default, the CIP for PCI solution trends are not enabled. Many reports, query viewers, and dashboards require enabled trends to show data.

The following trends must be enabled for basic CIP for PCI functionality:

`/All Trends/ArcSight Solutions/CIP/Regulations/PCI DSS/`

- `PCI DSS Number of Assets`
- `PCI DSS Maximal Asset Compliance Score`
- `PCI DSS Maximal Asset Compliance Score: Requirement`
- `PCI DSS Maximal Asset Non-Compliance Score`
- `PCI DSS Maximal Asset Non-Compliance Score: Requirement`
- `PCI DSS Compliance Score Sum`

`/All Trends/ArcSight Solutions/CIP/General/Compliance Scenario Correlation Events`

Additional trends must be enabled for PCI DSS requirements 1 and 8, as described in "Compliance Scenario Configuration" on page 33.

Note: By default, the trends listed above that begin with `PCI DSS` are scheduled to run in the order shown. If you run the trends manually in a different order, for example, during initial testing, the PCI DSS Compliance Status dashboard might display a negative number of assets. To resolve this issue, re-run the trends in the order shown above.

Until the trends above run, some dashboards and query viewers do not show the maximum scores and compliance percentages.

Before enabling a trend, verify that the trend captures data relevant for your environment as described in procedure below. In addition, before enabling a trend, you can also customize the following values:

- The `Schedule Range Start` date on the Schedule tab in the Inspect/Edit panel. By default, the CIP for PCI trends collect data based on the installation time of the CIP for PCI package on the ArcSight Manager. Before enabling the trend, ensure that the `Start` field of the trend on the Schedule tab reflects the date from which you want to start collecting events.
- The `Partition Retention Period (in days)` attribute on the Attributes tab in the Inspect/Edit panel. Specify the number of days you want to retain the partitions from this trend as active in the ArcSight database. You can increase the value of this attribute. This attribute is used in combination with the `Partition Size` attribute.

  Caution: Reducing the `Partition Retention Period` might prevent the resources from functioning properly.

For general information about trends, see the ***ArcSight Console User's Guide***.

To ensure that a trend captures the relevant events:

1. Generate or identify the required events and verify that they are being processed by ArcSight ESM.

   Note: To generate relevant events and send them to ArcSight ESM, you can do one of the following:

   - Set up a connector to capture events from a target system and perform the actions that would generate the required events on that system.
   - Import into ArcSight ESM an existing batch file that contains relevant events.

2. Navigate to the appropriate trend, right-click the trend, and then choose **Test**. If you see the events of interest in the test panel, the ArcSight ESM is processing events that can be captured by the trend. The test panel shows relevant events that can be captured by the trend in the last hour, up to 25 rows.

   If you do not see the events of interest, customize the queries invoked by the trend for your environment.

Enabling Data Monitors

All of the CIP for PCI data monitors must be enabled to display data in the dashboards that use them.

To enable the data monitors:

1. In the Navigator panel, go to **Dashboards** and click the **Data Monitors** tab.
2. Navigate to the `/All Data Monitors/ArcSight Solutions/CIP` group.
3. Right-click the `CIP` group and select **Enable Data Monitor** to enable all the data monitors in the group.

Configuring Notifications

You can add a rule action to a CIP for PCI rule that sends notifications when the rule is triggered. In addition, you can create notification destinations that receive the notifications when the rules trigger. For more information including configuration information, see the ***ArcSight Console User's Guide***. This configuration is optional.

Creating Custom Compliance Scenarios

If you are familiar with creating ArcSight rules, and your organization has a compliance issue that is not addressed by an existing scenario rule, you can create a custom scenario rule to handle the issue. Create the rule and then map it to a control, as described below.

> **Tip:** You can use an existing scenario rule as a model. Either examine the rule and use it as a guideline, or copy the rule by dragging it to a new location and modify it to meet your needs.

Before you begin:

Determine the ***impact type*** of your rule. The conditions and actions that you add to the rule depend on the impact type. For more information, see "Scenario Impact Type" on page 31.

To create a scenario rule:

1. Create a new standard rule in the following group:

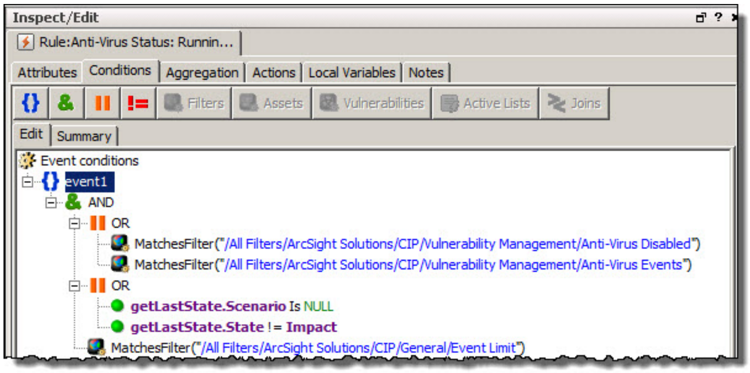
   `Rules/Shared/ArcSight Solutions/CIP/Compliance Scenarios`

   Put the rule in an appropriate domain group, such as `Network Security` or `System Hardening`, based on what the rule does. If an appropriate group does not exist, you can create a new group.
2. Give the rule a unique name that indicates what the rule detects.

   This rule name will appear as the scenario name in active lists, reports, and dashboards.
3. Add conditions for the rule to the **Conditions** tab, as required by your business logic.

   You can use existing filters or create a new filter. Optionally, you can include a `MatchesFilter` condition for the Event Limit filter.

If your rule has an impact type of Y/N, add a condition to check the latest scenario state in the Scenario State active list for each control-asset pair. The rule triggers only if the latest state (impact) is empty or different from the current state (current impact of the rule). The Anti-Virus Status: Running or Disabled rule shown below demonstrates one way to do this:



```
Event conditions
  event1
    AND
      OR
        MatchesFilter("/All Filters/ArcSight Solutions/CIP/Vulnerability Management/Anti-Virus Disabled")
        MatchesFilter("/All Filters/ArcSight Solutions/CIP/Vulnerability Management/Anti-Virus Events")
      OR
        getLastState.Scenario Is NULL
        getLastState.State != Impact
      MatchesFilter("/All Filters/ArcSight Solutions/CIP/General/Event Limit")
```

4. Create local variables for your rule on the **Local Variables** tab.

   All of the scenario rules in the Compliance Scenarios group provided by CIP for PCI use the `$AssetID`, `$AssetName`, `$AssetZone` local variables. The rules that have the Y/N impact type also use `$Impact`.

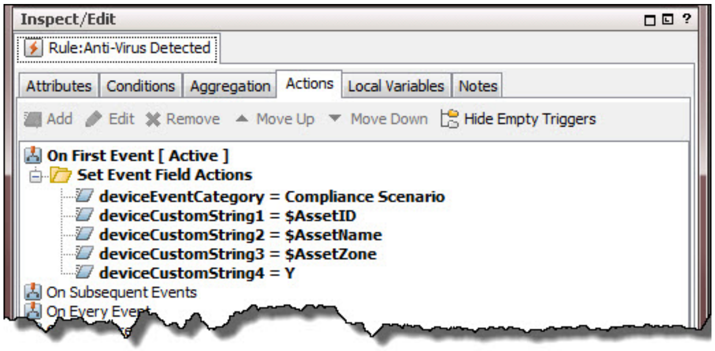
5. Add actions for the rule on the **Actions** tab.

   The rule must generate a correlation event that includes the following fields:

- The asset identifier, as either Source, Destination, Agent or Device, depending on your scenario logic. This field identifies where the issue occurred.

- The impact type, as either Y, N, or the `$Impact` local variable, which returns Y or N.

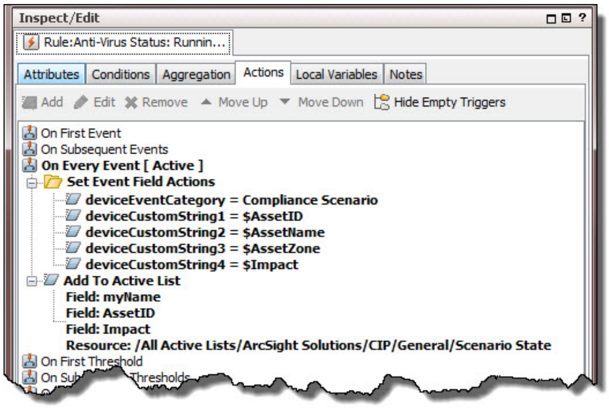
  If your rule has an impact type of Y or N, the action occurs **On First Event** and sets **deviceCustomString4** to Y or N, as shown below:



```
On First Event [ Active ]
  Set Event Field Actions
    deviceEventCategory = Compliance Scenario
    deviceCustomString1 = $AssetID
    deviceCustomString2 = $AssetName
    deviceCustomString3 = $AssetZone
    deviceCustomString4 = Y
On Subsequent Events
On Every Eve
```

  If your rule has an impact type of Y/N, the action occurs **On Every Event**, sets **deviceCustomString4** to the `$Impact` local variable, and updates the Scenario State active list. The

Anti-Virus Status: Running or Disabled rule shown below demonstrates one way to do this:



```
On First Event
On Subsequent Events
On Every Event [ Active ]
  Set Event Field Actions
    deviceEventCategory = Compliance Scenario
    deviceCustomString1 = $AssetID
    deviceCustomString2 = $AssetName
    deviceCustomString3 = $AssetZone
    deviceCustomString4 = $Impact
  Add To Active List
    Field: myName
    Field: AssetID
    Field: Impact
    Resource: /All Active Lists/ArcSight Solutions/CIP/General/Scenario State
On First Threshold
On Sub     Thresholds
```

6. Test the rule and, when you are satisfied with the results, save the rule.
7. Deploy the rule to the `Real-time Rules` group.

To map the scenario rule to a PCI DSS control:

1. Add a new entry to the Scenario Controls active list located in:

   `Active Lists/Shared/All Active Lists/ArcSight Solutions/CIP/General/`
2. Provide values for the following fields:
   - **Scenario** - The scenario rule name from step 2 under "To create a scenario rule:" on page 29.
   - **Regulation** - The regulation that the scenario rule pertains to, for example, PCI DSS.
   - **Control ID** - The control that the scenario rule addresses, for example, a PCI sub-requirement number.
   - **Score** - If your rule has an impact type of Y or Y/N and can determine full compliance, specify 1.0. However, if your requirement is complex, for example, it contains multiple conditions, and the rule can determine only partial compliance, specify a score ***between*** 0 and 1.

     If your rule has an impact type of N, specify 0.0.
   - **Scenario Type** - The impact type of Y, N, or Y/N.
3. Click **Add** to add the entry to the active list.

If you created a scenario rule to address a control that does not exist in the Controls active list, add the information about the new control to both the PCI DSS Requirements and Controls active lists for documentation and reporting purposes.

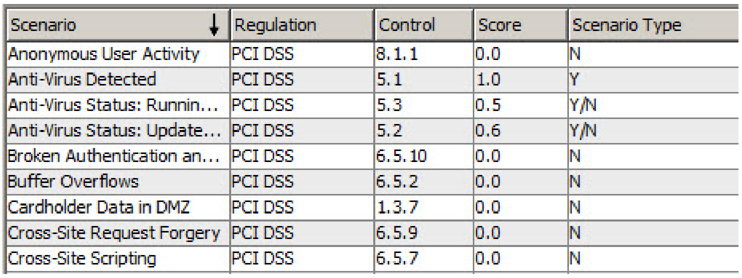
Scenario Impact Type

When a scenario rule triggers, it creates a correlation event that includes an ***impact type,*** as described below:

Y	The scenario determines compliance, but cannot determine non-compliance. For example, if the control states "Anti-Virus must be enabled...", a Y scenario can make sure this is true, but cannot determine that it is false.
N	The scenario determines non-compliance, but cannot determine compliance. For example, if a control states "Anti-Virus must be enabled...", an N scenario can make sure this is false (anti-virus is not enabled), but cannot determine that it is true.
Y/N	The scenario determines compliance and non-compliance. For example, if the control states "Anti-Virus must be enabled...", a Y/N scenario can check whether it is enabled or not.

CIP for PCI uses the impact type in conjunction with the following active lists to determine the compliance score for each control-asset pair:

- The Scenario Controls active list maps each scenario to a control and an initial score, typically 1 or 0 depending on the rule's impact type, as shown below:

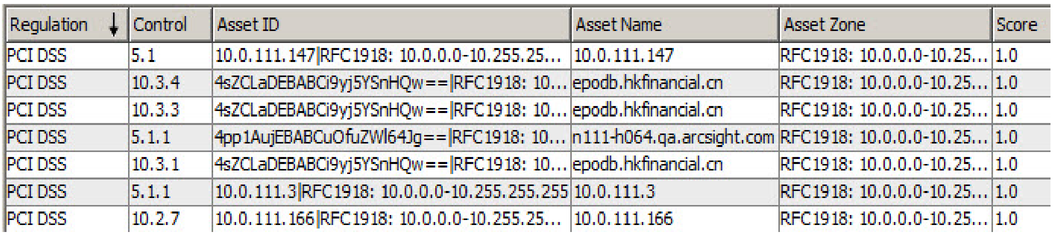
Scenario ↓	Regulation	Control	Score	Scenario Type
Anonymous User Activity	PCI DSS	8.1.1	0.0	N
Anti-Virus Detected	PCI DSS	5.1	1.0	Y
Anti-Virus Status: Runnin...	PCI DSS	5.3	0.5	Y/N
Anti-Virus Status: Update...	PCI DSS	5.2	0.6	Y/N
Broken Authentication an...	PCI DSS	6.5.10	0.0	N
Buffer Overflows	PCI DSS	6.5.2	0.0	N
Cardholder Data in DMZ	PCI DSS	1.3.7	0.0	N
Cross-Site Request Forgery	PCI DSS	6.5.9	0.0	N
Cross-Site Scripting	PCI DSS	6.5.7	0.0	N

  Note that a few scenarios have an initial score between 1 and 0, for example, 0.6, typically because the control contains multiple conditions and CIP for PCI can only determine partial compliance.

  This active list is pre-populated when CIP for PCI is installed and does not change unless you manually add a custom scenario to it.

- The Compliance Score active list maintains a dynamic compliance score for each control-asset pair by using the following process:

  If a scenario has an impact type of N, a value of -1 is put into the Compliance Score active list for the control-asset pair. Otherwise, the initial score from the Scenario Controls active list is put into the Compliance Score active list.

Regulation ↓	Control	Asset ID	Asset Name	Asset Zone	Score
PCI DSS	5.1	10.0.111.147|RFC1918: 10.0.0.0-10.255.25...	10.0.111.147	RFC1918: 10.0.0.0-10.25...	1.0
PCI DSS	10.3.4	4sZCLaDEBABCi9yj5YSnHQw==|RFC1918: 10...	epodb.hkfinancial.cn	RFC1918: 10.0.0.0-10.25...	1.0
PCI DSS	10.3.3	4sZCLaDEBABCi9yj5YSnHQw==|RFC1918: 10...	epodb.hkfinancial.cn	RFC1918: 10.0.0.0-10.25...	1.0
PCI DSS	5.1.1	4pp1AujEBABCuOfuZWl64Jg==|RFC1918: 10...	n111-h064.qa.arcsight.com	RFC1918: 10.0.0.0-10.25...	1.0
PCI DSS	10.3.1	4sZCLaDEBABCi9yj5YSnHQw==|RFC1918: 10...	epodb.hkfinancial.cn	RFC1918: 10.0.0.0-10.25...	1.0
PCI DSS	5.1.1	10.0.111.3|RFC1918: 10.0.0.0-10.255.255.255	10.0.111.3	RFC1918: 10.0.0.0-10.25...	1.0
PCI DSS	10.2.7	10.0.111.166|RFC1918: 10.0.0.0-10.255.25...	10.0.111.166	RFC1918: 10.0.0.0-10.25...	1.0

  CIP for PCI uses the scores in the Compliance Score active list to calculate the scores displayed in the CIP for PCI reports and dashboards.

- The Scenario State active list stores the latest state (either Y or N) of scenarios that have an impact of Y/N, for each asset.

Chapter 3: Compliance Scenario Configuration

This chapter describes the compliance scenario rules and configuration, organized by PCI requirement.

Note: Excerpts from the PCI DSS and related control statements are provided courtesy of PCI Security Standards Council, LLC and/or its licensors. © 2014 PCI Security Standards Council, LLC. All Rights Reserved.

Requirement 1: Firewall Configuration

The PCI DSS 3.2.1 provides the following definition for this requirement.

Requirement 1: Install and maintain a firewall configuration to protect cardholder data

Firewalls are devices that control computer traffic allowed between an entity’s networks (internal) and untrusted networks (external), as well as traffic into and out of more sensitive areas within an entity’s internal trusted networks. The cardholder data environment is an example of a more sensitive area within an entity’s trusted network.

A firewall examines all network traffic and blocks those transmissions that do not meet the specified security criteria.

All systems must be protected from unauthorized access from untrusted networks, whether entering the system via the Internet as e-commerce, employee Internet access through desktop browsers, employee e-mail access, dedicated connections such as business-to-business connections, via wireless networks, or via other sources. Often, seemingly insignificant paths to and from untrusted networks can provide unprotected pathways into key systems. Firewalls are a key protection mechanism for any computer network.

Other system components may provide firewall functionality, as long as they meet the minimum requirements for firewalls as defined in Requirement 1. Where other system components are used within the cardholder data environment to provide firewall functionality, these devices must be included within the scope and assessment of Requirement 1.

Compliance Scenarios

CIP for PCI provides the following compliance scenario rules to determine compliance with Requirement 1:

Requirement 1 Scenario Rules

Compliance Scenario Rule	PCI DSS Requirement	PCI DSS Requirement Description
Successful Disallowed Ports Access in Cardholder Data Environment	1.2.1	Restrict inbound and outbound traffic to that which is necessary for the cardholder data environment.
Successful Disallowed Ports Access from Wireless into Cardholder Data Environment	1.2.3	Install perimeter firewalls between any wireless networks and the cardholder data environment, and configure these firewalls to deny or control (if such traffic is necessary for business purposes) any traffic from the wireless environment into the cardholder data environment.
Implement a DMZ	1.3.1	Implement a DMZ to limit inbound traffic to only system components that provide authorized publicly accessible services, protocols, and ports.
Successful Traffic from Internet into non-DMZ Destination	1.3.2	Limit inbound Internet traffic to IP addresses within the DMZ.
Direct Connections between Internet and Cardholder Data Environment	1.3.3	Do not allow any direct connections inbound or outbound for traffic between the Internet and the cardholder data environment.
Internal IP access from Internet into DMZ	1.3.4	Do not allow internal addresses to pass from the Internet into the DMZ.
Successful Unauthorized Traffic from Cardholder Data Environment to Internet	1.3.5	Do not allow unauthorized outbound traffic from the cardholder data environment to the Internet.

Requirement 1 Scenario Rules, continued

Compliance Scenario Rule	PCI DSS Requirement	PCI DSS Requirement Description
Cardholder Data in DMZ	1.3.7	Place system components that store cardholder data (such as a database) in an internal network zone, segregated from the DMZ and other untrusted networks.
Private IP Protected From Disclosure	1.3.8	Do not disclose private IP addresses and routing information to unauthorized parties. **Note**: Methods to obscure IP addressing may include, but are not limited to: • Network Address Translation (NAT). • Placing servers containing cardholder data behind proxy servers/firewalls. • Removal or filtering of route advertisements for private networks that employ registered addressing. • Internal use of RFC1918 address space instead of registered addresses.
Personal Firewall	1.4	Install personal firewall software on any mobile and/or employee-owned computers with direct connectivity to the Internet (for example, laptops used by employees), which are used to access the organization's network.

Configuration

Configuration for Requirement 1 is provided below.

Asset Categories

- For requirement **1.2.1**, **1.2.3**, **1.3.3**, **1.3.5**, and **1.3.7**, categorize all servers and networks that store sensitive cardholder information in the following category:

  `All Asset Categories/ArcSight Solutions/Compliance Insight Package/Regulations/PCI/Cardholder Data`

- For requirement **1.2.3**, categorize all assets or zones that belong to wireless networks in one of the following categories:

  `All Asset Categories/ArcSight Solutions/Compliance Insight Package/Address Spaces/Wireless`

- For requirement **1.3.2** and **1.3.7**, categorize all network components that are part of the DMZ in the following category:

  `All Asset Categories/ArcSight Solutions/Compliance Insight Package/Address Spaces/DMZ`

  > **Note:** When adding a new asset to the Cardholder Data category, specify the MAC address. The rule (for requirement 1.3.7) detects when an asset from the cardholder data environment is moved to a DMZ segment only if the MAC address for the asset is specified.

- For requirement **1.3.2**, **1.3.3**, and **1.3.5**, categorize all assets or zones that have IP addresses that do not belong to `Private Address Space Zones`, but are considered internal, in the following category:

`All Asset Categories/ArcSight Solutions/Compliance Insight Package/Address Spaces/Protected`

- For requirement **1.3.4**, categorize perimeter firewalls that connect the Internet with the DMZ in the following category:

  `All Asset Categories/ArcSight Solutions/Compliance Insight Package/Infrastructure/Perimeter Firewalls`

  > **Note:** Do not categorize firewalls that are connected to segments other than the DMZ and the Internet in this category.

Active Lists

For requirement **1.2.1**, **1.2.3**, and **1.3.5**, populate the Cardholder Data Environment Allowed Ports active list with ports that allow inbound and outbound traffic. For example, `Port=80, Direction=inbound; and Port=24, Direction=outbound`. All entries must be in lowercase.

See "Configuring Active Lists" on page 24 for information on how to populate active lists.

Rules

Enable the scenario rules in "Requirement 1 Scenario Rules" on page 35. The rules are located in the following group:

`ArcSight Solutions/CIP/Compliance Scenarios/Network Security`

For instructions on enabling rules, see "Deploying and Enabling Rules" on page 22.

Trends

For requirement **1.3.1**, enable the DMZ Assets and DMZ Zones trends.

Requirement 2: Default Security Parameters

The PCI DSS 3.2.1 provides the following definition for this requirement.

Requirement 2: Do not use vendor-supplied defaults for system passwords and other security parameters

Malicious individuals (external and internal to an entity) often use vendor default passwords and other vendor default settings to compromise systems. These passwords and settings are well known by hacker communities and are easily determined via public information.

Compliance Scenarios

CIP for PCI provides the following compliance scenario rules to determine compliance with Requirement 2:

Requirement 2 Scenario Rules

Compliance Scenario	PCI DSS Requirement	PCI DSS Requirement Description
Default Vendor Account Used Successfully	2.1	Always change vendor-supplied defaults and remove or disable unnecessary default accounts before installing a system on the network. This applies to ALL default passwords, including but not limited to those used by operating systems, software that provides security services, application and system accounts, point-of-sale (POS) terminals, Simple Network Management Protocol (SNMP) community strings, etc.).
Multiple Functions Implemented on a Server	2.2.1	Implement only one primary function per server to prevent functions that require different security levels from co-existing on the same server. (For example, web servers, database servers, and DNS should be implemented on separate servers.) Note: Where virtualization technologies are in use, implement only one primary function per virtual system component.
Insecure Services, Protocols or Daemons Detected	2.2.3	Implement additional security features for any required services, protocols, or daemons that are considered to be insecure—for example, use secured technologies such as SSH, S-FTP, SSL, or IPSec VPN to protect insecure services such as NetBIOS, file-sharing, Telnet, FTP, and so on.
Misconfigurations	2.2.4	Configure system security parameters to prevent misuse.
Unnecessary Functionality Detected	2.2.5	Remove all unnecessary functionality, such as scripts, drivers, features, subsystems, file systems, and unnecessary web servers.
Unencrypted Non-Console Administrative Access Detected	2.3	Encrypt all non-console administrative access using strong cryptography. Use technologies such as SSH, VPN, or SSL/TLS for web-based management and other non-console administrative access.

Configuration

Configuration for Requirement 2 is provided below.

Asset Categories

For requirement **2.2.1** and **2.2.5**, categorize the following assets as described in "Categorizing Assets and Zones" on page 22.

- Categorize database assets in the `All Asset Categories/ArcSight Solutions/Compliance Insight Package/Application/Type/Database` category.
- Categorize web server assets in the `All Asset Categories/ArcSight Solutions/Compliance Insight Package/Application/Type/Web Server` category.
- Categorize Domain Name Server (DNS) assets in the `All Asset Categories/ArcSight Solutions/Compliance Insight Package/Application/Type/Domain Name Server` category.

Active Lists

Populate the following active lists, as described in "Configuring Active Lists" on page 24.

- For requirement **2.1**, add vendor user accounts that are not secure and should not be used to the Default Vendor Accounts active list. All the entries in this list must be in lowercase.
- For requirement **2.2.1**, update the following active lists with additional data to improve the rule efficiency:
  - Database Ports
  - Database Processes (all entries in this list must be in lowercase)
  - Domain Name Server Ports
  - Domain Name Server Processes (all entries in this list must be in lowercase)
  - Web Server Ports
  - Web Server Processes (all entries in this list must be in lowercase)
- For requirement **2.2.3**, review the Insecure Ports active list. Remove any justified ports from the active list to eliminate false positives. Add insecure ports for additional protection.
- For requirement **2.2.5** and **2.3**, populate the Administrative Accounts active list with the administrative accounts in your organization. All the entries in this list must be in lowercase.

Rules

Enable the scenario rules in "Requirement 2 Scenario Rules" on the previous page. The rules are located in the following groups:

```
ArcSight Solutions/CIP/Compliance Scenarios/System Hardening
```

```
ArcSight Solutions/CIP/Compliance Scenarios/Vulnerability Management/
```

For instructions on enabling rules, see "Deploying and Enabling Rules" on page 1.

Requirement 3: Protecting Stored Data

The PCI DSS 3.2.1 provides the following definition for this requirement.

Requirement 3: Protect stored cardholder data

Protection methods such as encryption, truncation, masking, and hashing are critical components of cardholder data protection. If an intruder circumvents other security controls and gains access to encrypted data, without the proper cryptographic keys, the data is unreadable and unusable to that person. Other effective methods of protecting stored data should also be considered as potential risk mitigation opportunities. For example, methods for minimizing risk include not storing cardholder data unless absolutely necessary, truncating cardholder data if full PAN is not needed, and not sending unprotected PANs using end-user messaging technologies, such as e-mail and instant messaging.

Compliance Scenarios

CIP for PCI provides the following compliance scenario rules to determine compliance with Requirement 3:

Requirement 3 Scenario Rules

Compliance Scenario	PCI DSS Requirement	PCI DSS Requirement Description
Primary Account Numbers Detected in Clear Text	3.3	Mask PAN when displayed (the first six and last four digits are the maximum number of digits to be displayed), such that only personnel with a legitimate business need can see the full PAN. Note: This requirement does not supersede stricter requirements in place for displays of cardholder data—for example, legal or payment card brand requirements for point-of-sale (POS) receipts.

Configuration

Configuration for Requirement 3 is provided below.

Filters

Add custom network intrusion detection system (NIDS) signatures to the Primary Account Numbers Detected in Clear Text filter.

Rules

Enable the scenario rule in "Requirement 3 Scenario Rules" above. The rule is located in the following group:

```
ArcSight Solutions/CIP/Compliance Scenarios/Privacy Protection
```

For instructions on enabling rules, see "Deploying and Enabling Rules" on page 22.

Requirement 4: Encrypted Transmissions

The PCI DSS 3.2.1 provides the following definition for this requirement.

Requirement 4: Encrypt transmission of cardholder data across open, public networks

Sensitive information must be encrypted during transmission over networks that are easily accessed by malicious individuals. Misconfigured wireless networks and vulnerabilities in legacy encryption and authentication protocols continue to be targets of malicious individuals who exploit these vulnerabilities to gain privileged access to cardholder data environments.

Compliance Scenarios

CIP for PCI provides the following compliance scenario rules to determine compliance with Requirement 4:

Requirement 4 Scenario Rules

Compliance Scenario	PCI DSS Requirement	PCI DSS Requirement Description
Bluetooth Protocol Vulnerability Cryptographic Hash Algorithm Related Vulnerability Cryptographic Public Key Related Vulnerability Cryptographic Symmetric Key Related Vulnerability Cryptographic Weak Protocol Vulnerability Heartbleed Vulnerability Insecure Transmission of Cardholder Data Over Public Networks Poodle Vulnerability SSL|TLS 1.0 Detected SSL|TLS Vulnerability TLS BREACH Vulnerability TLS CRIME Vulnerability	4.1	Use strong cryptography and security protocols to safeguard sensitive cardholder data during transmission over open, public networks, including the following: • Only trusted keys and certificates are accepted. • The protocol in use only supports secure versions or configurations. • The encryption strength is appropriate for the encryption methodology in use. **Notes:** Where SSL/early TLS is used, the requirements in Appendix A2 must be completed. Examples of open, public networks include, but are not limited to: • The Internet • Wireless technologies, including 802.11 and Bluetooth • Cellular technologies, for example, Global System for Mobile communications (GSM), Code division multiple access (CDMA) • General Packet Radio Service (GPRS) • Satellite communications
Wireless Encryption Violation in Cardholder Data Environment Detected	4.1.1	Ensure wireless networks transmitting cardholder data or connected to the cardholder data environment, use industry best practices to implement strong encryption for authentication and transmission.

Configuration

Configuration for Requirement 4.1 is as follows:

For Requirement 4.1 Scenario, Insecure Transmission of Cardholder Data Over Public Networks:

Add custom network intrusion detection system (NIDS) signatures to the Primary Account Numbers Detected in Clear Text filter.

Rules

Enable the scenario rules in the table "Requirement 4 Scenario Rules" on the previous page. The rules are located in the following groups:

```
ArcSight Solutions/CIP/Compliance Scenarios/Cryptography
```

```
ArcSight Solutions/CIP/Compliance Scenarios/ Vulnerability Management
```

For instructions on enabling rules, see "Deploying and Enabling Rules" on page 22.

Data Monitor

For requirement 4.1, enable the Cryptographic Vulnerabilities Graph data monitor.

Additional Resources that Support the 4.1 Requirement

Resource Type	Resource Name
Dashboard	Cryptographic Asset Vulnerabilities
Report	Bluetooth Protocol Vulnerability Detected
Report	Cryptographic Hash Algorithm Related Vulnerability Detected
Report	Cryptographic Public Key Related Vulnerability Detected
Report	Cryptographic Symmetric Key Related Vulnerability Detected
Report	Cryptographic Weak Protocol Vulnerability Detected
Report	Heartbleed Vulnerability Detected
Report	Insecure Cryptography
Report	Poodle Vulnerability Detected
Report	SSL|TLS 1.0 Detected
Report	SSL|TLS Vulnerability Detected
Report	TLS BREACH Vulnerability Detected
Report	TLS CRIME Vulnerability Detected
Report	Top 20 Insecure Transmission of Cardholder Data Over Public Networks

Requirement 5: AntiVirus

The PCI DSS 3.2.1 provides the following definition for this requirement.

Requirement 5: Protect all systems against malware and regularly update anti-virus software or programs

Malicious software, commonly referred to as "malware"—including viruses, worms, and Trojans—enters the network during many business-approved activities including employee e-mail and use of the Internet, mobile computers, and storage devices, resulting in the exploitation of system vulnerabilities. Anti-virus software must be used on all systems commonly affected by malware to protect systems from current and evolving malicious software threats. Additional anti-malware solutions may be considered as a supplement to the anti-virus software; however, such additional solutions do not replace the need for anti-virus software to be in place.

Compliance Scenarios

CIP for PCI provides the following compliance scenario rules to determine compliance with Requirement 5:

Requirement 5 Scenario Rules

Compliance Scenario	PCI DSS Requirement	PCI DSS Requirement Description
Anti-Virus Detected	5.1	Deploy anti-virus software on all systems commonly affected by malicious software (particularly personal computers and servers).
Malware or Spyware Detected	5.1.1	Ensure that anti-virus programs are capable of detecting, removing, and protecting against all known types of malicious software.
Anti-Virus Status: Updates or Scans	5.2	Ensure that all anti-virus mechanisms are maintained as follows: • Are kept current, • Perform periodic scans • Generate audit logs which are retained per PCI DSS Requirement 10.7.
Anti-Virus Status: Running or Disabled	5.3	Ensure that anti-virus mechanisms are actively running and cannot be disabled or altered by users, unless specifically authorized by management on a case-by-case basis for a limited time period. Note: Anti-virus solutions may be temporarily disabled only if there is legitimate technical need, as authorized by management on a case-by-case basis. If anti-virus protection needs to be disabled for a specific purpose, it must be formally authorized. Additional security measures may also need to be implemented for the period of time during which anti-virus protection is not active.

Configuration

Configuration for Requirement 5 is provided below.

Rules

Enable the scenario rules in "Requirement 5 Scenario Rules" on the previous page. The rules are located in the following group:

```
ArcSight Solutions/CIP/Compliance Scenarios/Vulnerability Management
```

For instructions on enabling rules, see "Deploying and Enabling Rules" on page 22.

Requirement 6: System Applications

The PCI DSS 3.2.1 provides the following definition for this requirement.

Requirement 6: Develop and maintain secure systems and applications

Unscrupulous individuals use security vulnerabilities to gain privileged access to systems. Many of these vulnerabilities are fixed by vendor-provided security patches, which must be installed by the entities that manage the systems. All systems must have all appropriate software patches to protect against the exploitation and compromise of cardholder data by malicious individuals and malicious software.

Compliance Scenarios

CIP for PCI provides the following compliance scenario rules to determine compliance with Requirement 6:

Requirement 6 Scenario Rules

Compliance Scenario Rule	PCI DSS Requirement	PCI DSS Requirement Description
Security Patch Missing	6.2	Ensure that all system components and software are protected from known vulnerabilities by installing applicable vendor-supplied security patches. Install critical security patches within one month of release. **Note:** Critical security patches should be identified according to the risk ranking process defined in Requirement 6.1.
Custom Account Detected	6.3.1	Remove development, test and/or custom application accounts, user IDs, and passwords before applications become active or are released to customers.
Test Account in Production Environment	6.4.2	Separation of duties between development/test and production environments.

Requirement 6 Scenario Rules, continued

Compliance Scenario Rule	PCI DSS Requirement	PCI DSS Requirement Description
Primary Account Numbers Detected in Testing or Development Environment	6.4.3	Production data (live PANs) are not used for testing or development.
Injection Flaws	6.5.1	Injection flaws, particularly SQL injection. Also consider OS Command Injection, LDAP and XPath injection flaws as well as other injection flaws.
Buffer Overflows	6.5.2	Buffer overflows
Insecure Cryptography	6.5.3	Insecure cryptographic storage
Insecure Communications	6.5.4	Insecure communications
Improper Error Handling	6.5.5	Improper error handling
High Risk Vulnerability Detected	6.5.6	All "high risk" vulnerabilities identified in the vulnerability identification process (as defined in PCI DSS Requirement 6.1).
Cross-Site Scripting	6.5.7	Cross-site scripting (XSS)
Improper Access Control	6.5.8	Improper access control (such as insecure direct object references, failure to restrict URL access, directory traversal, and failure to restrict user access to functions).
Cross-Site Request Forgery	6.5.9	Cross-site request forgery (CSRF)
Broken Authentication and Session Management	6.5.10	Broken authentication and session management. Note: Requirement 6.5.10 is a best practice until June 30, 2015, after which it becomes a requirement.
Critical Network Device Configuration Change Critical Operating System Change	6.4.5	Change control procedures

Configuration

Configuration for Requirement 6 is provided below.

Asset Categories

- For requirement **6.4.2**, categorize assets or network zones that belong to the production environment in the following category:

  ```
  All Asset Categories/ArcSight Solutions/Compliance Insight
  Package/Environments/Production
  ```

- For requirement **6.4.5**, categorize assets or network zones in the following categories:

  ```
  All Asset Categories/System Asset Categories/Criticality/High
  All Asset Categories/System Asset Categories/Criticality/Very-High
  ```

```
All Asset Categories/Site Asset Categories/Business Impact
Analysis/Business Role/Security Devices/Firewall
```

```
Asset Categories/Site Asset Categories/Business Impact Analysis/Business
Role/Infrastructure/Network
```

```
All Asset Categories/Site Asset Categories/Business Impact
Analysis/Business Role/Security Devices/NIDS
```

Active Lists

For requirement **6.3.1** and **6.4.2**, populate the Test and Custom Accounts active list with additional custom accounts that should be disabled in a production environment. All the entries in this list must be in lowercase.

Rules

Enable the scenario rules in "Requirement 6 Scenario Rules" on page 44. The rules are located in the following groups:

```
ArcSight Solutions/CIP/Compliance Scenarios/Access Control
```

```
ArcSight Solutions/CIP/Compliance Scenarios/Cryptography
```

```
ArcSight Solutions/CIP/Compliance Scenarios/Privacy Protection
```

```
ArcSight Solutions/CIP/Compliance Scenarios/System Hardening
```

```
ArcSight Solutions/CIP/Compliance Scenarios/Vulnerability Management
```

For instructions on enabling rules, see "Deploying and Enabling Rules" on page 22.

Trend

For requirement **6.4.5**, enable the Configuration Changes trend.

Additional Resources that Support Requirement 6.4.5

Resource Type	Resource
Dashboard	Configuration Changes Overview
Report	Application Configuration Modifications
Report	Database Configuration Modifications
Report	Firewall Configuration Modifications
Report	Firewall Configuration Modification Summary
Report	Network Device Configuration Modifications
Report	Weekly Trend - Configuration Modification Summary

Requirement 7: Business Need-to-Know

The PCI DSS 3.2.1 provides the following definition for this requirement.

Requirement 7: Restrict access to cardholder data by business need to know

To ensure critical data can only be accessed by authorized personnel, systems and processes must be in place to limit access based on need to know and according to job responsibilities.

“Need to know” is when access rights are granted to only the least amount of data and privileges needed to perform a job.

Compliance Scenarios

CIP for PCI provides the following compliance scenario rules to determine compliance with Requirement 7:

Requirement 7 Scenario Rule

Compliance Scenario	PCI DSS Requirement	PCI DSS Requirement Description
Unauthorized Access to Cardholder Data	7.1	Limit access to system components and cardholder data to only those individuals whose job requires such access.

Configuration

Configuration for Requirement 7 is provided below.

Active Lists

Populate the Users Authorized to Access Cardholder Data active list with the usernames of users who are authorized to access the cardholder data environment. All the entries in this list must be in lowercase.

Rules

Enable the scenario rule in "Requirement 7 Scenario Rule" above. The rule is located in the following group:

```
ArcSight Solutions/CIP/Compliance Scenarios/Access Control
```

For instructions on enabling rules, see "Deploying and Enabling Rules" on page 22.

Requirement 8: Unique User ID

The PCI DSS 3.2.1 provides the following definition for this requirement.

Requirement 8: Identify and authenticate access to system components

Assigning a unique identification (ID) to each person with access ensures that each individual is uniquely accountable for their actions. When such accountability is in place, actions taken on critical data and systems are performed by, and can be traced to, known and authorized users and processes.

The effectiveness of a password is largely determined by the design and implementation of the authentication system—particularly, how frequently password attempts can be made by an attacker, and the security methods to protect user passwords at the point of entry, during transmission, and while in storage.

Compliance Scenarios

CIP for PCI provides the following compliance scenario rules to determine compliance with Requirement 8:

Requirement 8 Scenario Rules

Compliance Scenario	PCI DSS Requirement	PCI DSS Requirement Description
Anonymous User Activity	8.1.1	Assign all users a unique ID before allowing them to access system components or cardholder data.
Terminated User Activity	8.1.3	Immediately revoke access for any terminated users.
Inactive User Account Activity	8.1.4	Remove/disable inactive user accounts at least every 90 days.
Account Lockouts	8.1.6	Limit repeated access attempts by locking out the user ID after not more than six attempts.
Lockout Duration	8.1.7	Set the lockout duration to a minimum of 30 minutes or until an administrator enables the user ID.
Clear Text Password Transmission	8.2.1	Using strong cryptography, render all authentication credentials (such as passwords/phrases) unreadable during transmission and storage on all system components.

Requirement 8 Scenario Rules, continued

Compliance Scenario	PCI DSS Requirement	PCI DSS Requirement Description
Password Management: Successful Changes or Expirations	8.2.4	Change user passwords/passphrases at least every 90 days.
Non Multi Factor Access to CDE by Admin Account	8.3..1	Incorporate multi-factor authentication for all non-console access into the CDE for personnel with administrative access.
Unauthorized Direct Cardholder Database Access	8.7	All access to any database containing cardholder data (including access by applications, administrators, and all other users) is restricted as follows: • All user access to, user queries of, and user actions on databases are through programmatic methods. • Only database administrators have the ability to directly access or query databases. • Application IDs for database applications can only be used by the applications (and not by individual users or other non-application processes).

Configuration

Configuration for Requirement 8 is provided in this section.

Categories

Categorize the following assets and zones, as described in "Categorizing Assets and Zones" on page 22.

For requirement **8.3.1**, categorize all servers and networks that store sensitive cardholder information in the following category:

```
All Asset Categories/ArcSight Solutions/Compliance Insight
Package/Regulations/PCI/Cardholder Data
```

Active Lists

- For requirement **8.1.1**, populate the Anonymous Accounts active list with usernames that cannot be linked to an individual user. All the entries in this list must be in lowercase.
- For requirement **8.1.3**, populate the Terminated Users active list with the user accounts of former employees. User accounts in this active list are retained indefinitely. All the entries in this list must be in lowercase.
- For requirement **8.1.4**, change the default time-to-live (TTL) value of 90 days for the Active Accounts active list to comply with your organization’s policy if necessary.

Populate the Inactive Accounts active list with additional user accounts that are known to be inactive. This active list is populated automatically, but you can also add entries manually. All the entries in this list must be in lowercase.

- For requirement **8.7**, populate the Database Administrators active list with the usernames of the database administrators in the organization. All the entries in this list must be in lowercase.
- For requirement **8.3.1**:
  a. Populate the Multi Factor Authentication Devices active list with all multi factor authentication devices on your organization. All the entries in this list must be in lowercase.
  b. If you have non multi authentication devices that you want to exclude from this compliance scenario, you can populate them with the Non Multi Factor Authentication Devices - Exception active list.
  c. Populate the Administrative Accounts active list with the administrative accounts in your organization. All the entries in this list must be in lowercase.

Trends

For requirement **8.2.4**, enable the Password Expired trend.

Rules

- For requirement **8.1.7**: If necessary, change the account lockout duration to comply with your organization's policy by editing the Lockout Duration scenario rule and changing the **Impact** local variable.
- Enable the scenario rules in "Requirement 8 Scenario Rules" on page 48. The rules are located in the following groups:

  ```
  ArcSight Solutions/CIP/Compliance Scenarios/Access Control
  ArcSight Solutions/CIP/Compliance Scenarios/Privacy Protection
  ```

  For instructions on enabling rules, see "Deploying and Enabling Rules" on page 22.

Additional resources

Resources that Support 8.3.1 Requirements

Resource Type	Resource
Dashboard	Non Multi Factor Administrative Authentication
Report	Non Multi Factor Access to CDE by Admin Accounts

Requirement 9: Physical Access

The PCI DSS 3.2.1 provides the following definition for this requirement.

Requirement 9: Restrict physical access to cardholder data

Any physical access to data or systems that house cardholder data provides the opportunity for individuals to access devices or data and to remove systems or hardcopies, and should be appropriately restricted. For the purposes of Requirement 9, "onsite personnel" refers to full-time and part-time employees, temporary employees, contractors and consultants who are physically present on the entity's premises. A "visitor" refers to a vendor, guest of any onsite personnel, service workers, or anyone who needs to enter the facility for a short duration, usually not more than one day. "Media" refers to all paper and electronic media containing cardholder data.

Compliance Scenarios

CIP for PCI provides the following compliance scenario rules to determine compliance with Requirement 9:

Requirement 9 Scenario Rules

Compliance Scenario	PCI DSS Requirement	PCI DSS Requirement Description
Failed Physical Access Attempt	9.1	Use appropriate facility entry controls to limit and monitor physical access to systems in the cardholder data environment.
Physical Access Events	9.1.1	Use video cameras and/or access control mechanisms to monitor individual physical access to sensitive areas. Review collected data and correlate with other entries. Store for at least three months, unless otherwise restricted by law. Note: "Sensitive areas" refers to any data center, server room or any area that houses systems that store, process, or transmit cardholder data. This excludes public-facing areas where only point-of-sale terminals are present, such as the cashier areas in a retail store.

Configuration

Configuration for Requirement 9 is provided below.

Rules

Enable the scenario rules in "Requirement 9 Scenario Rules" above. The rules are located in the following group:

```
ArcSight Solutions/CIP/Compliance Scenarios/Physical Security
```

For instructions on enabling rules, see "Deploying and Enabling Rules" on page 22.

Requirement 10: Tracking and Monitoring Data Access

The PCI DSS 3.2.1 provides the following definition for this requirement.

Requirement 10: Track and monitor all access to network resources and cardholder data

Logging mechanisms and the ability to track user activities are critical in preventing, detecting, or minimizing the impact of a data compromise. The presence of logs in all environments allows thorough tracking, alerting, and analysis when something does go wrong. Determining the cause of a compromise is very difficult, if not impossible, without system activity logs.

Compliance Scenarios

CIP for PCI provides the following compliance scenario rules to determine compliance with Requirement 10:

Requirement 10 Scenario Rules

Compliance Scenario Rule	PCI DSS Requirement	PCI DSS Requirement Description
Accesses to Cardholder Data Environment by Identified Users	10.2.1	Implement automated audit trails for all system components to reconstruct the following events: all individual user accesses to cardholder data.
Failed Logical Access Attempts	10.2.4	Implement automated audit trails for all system components to reconstruct the following events: invalid logical access attempts.
Audit Log Cleared	10.2.6	Implement automated audit trails for all system components to reconstruct the following events: initialization, stopping, or pausing of the audit logs.
Creation and Deletion of Objects	10.2.7	Implement automated audit trails for all system components to reconstruct the following events: creation and deletion of system-level objects.
Identified User Account in Event	10.3.1	Record at least the following audit trail entries for all system components for each event: user identification.
Event Time: Empty or Non-empty	10.3.3	Record at least the following audit trail entries for all system components for each event: date and time.
Success or Failure Indication in Event	10.3.4	Record at least the following audit trail entries for all system components for each event: success or failure indication.
Non-empty Origination of Event	10.3.5	Record at least the following audit trail entries for all system components for each event: origination of event.

Requirement 10 Scenario Rules, continued

Compliance Scenario Rule	PCI DSS Requirement	PCI DSS Requirement Description
Time Consistency Issues	10.4.1	Critical systems have the correct and consistent time.
Events from External-Facing Technologies	10.5.4	Write logs for external-facing technologies onto a secure, centralized, internal log server or media device.
Information System Failures	10.8	Implement a process for the timely detection and reporting of failures of critical security control systems, including but not limited to failure of: • Firewalls • IDS/IPS • FIM • Anti-virus • Physical access controls • Logical access controls • Audit logging mechanisms • Segmentation controls (if used)

Configuration

Configuration for Requirement 10 is provided below.

Categories

Categorize the following assets and zone, as described in "Categorizing Assets and Zones" on page 22.

For requirement **10.8**, categorize all the critical servers and networks that store sensitive cardholder information in the following category:

```
/All Asset Categories/System Asset Categories/Criticality/High
```

```
/All Asset Categories/System Asset Categories/Criticality/Very High
```

Rules

Enable the scenario rules in "Requirement 10 Scenario Rules" on the previous page. The rules are located in the following groups:

```
ArcSight Solutions/CIP/Compliance Scenarios/Access Control
```

```
ArcSight Solutions/CIP/Compliance Scenarios/Monitoring
```

For instructions on enabling rules, see "Deploying and Enabling Rules" on page 22.

Additional resources supporting Requirement 10.8

Resource Type	Resource
Dashboard	Information System Failures
Report	Information System Failures

Requirement 11: Testing Systems and Processes

The PCI DSS 3.2.1 provides the following definition for this requirement.

Requirement 11: Regularly test security systems and processes

Vulnerabilities are being discovered continually by malicious individuals and researchers, and being introduced by new software. System components, processes, and custom software should be tested frequently to ensure security controls continue to reflect a changing environment.

Compliance Scenarios

CIP for PCI provides the following compliance scenario rules to determine compliance with Requirement 11:

Requirement 11 Scenario Rules

Compliance Scenario	PCI DSS Requirement	PCI DSS Requirement Description
Unauthorized Access Point Detected	11.1	Implement processes to test for the presence of wireless access points (802.11), and detect and identify all authorized and unauthorized wireless access points on a quarterly basis. **Note:** Methods that may be used in the process include but are not limited to wireless network scans, physical/logical inspections of system components and infrastructure, network access control (NAC), or wireless IDS/IPS. Whichever methods are used, they must be sufficient to detect and identify both authorized and unauthorized devices.
Network IDS Detected	11.4	Use intrusion-detection and/or intrusion prevention techniques to detect and/or prevent intrusions into the network. Monitor all traffic at the perimeter of the cardholder data environment as well as at critical points in the cardholder data environment, and alert personnel to suspected compromises. Keep all intrusion-detection and prevention engines, baselines, and signatures up to date.

Requirement 11 Scenario Rules, continued

Compliance Scenario	PCI DSS Requirement	PCI DSS Requirement Description
File Integrity Tool Detected	11.5	Deploy a change-detection mechanism (for example, file-integrity monitoring tools) to alert personnel to unauthorized modification of critical system files, configuration files, or content files; and configure the software to perform critical file comparisons at least weekly. **Note:** For change detection purposes, critical files are usually those that do not regularly change, but the modification of which could indicate a system compromise or risk of compromise. Change detection mechanisms such as file-integrity monitoring products usually come pre-configured with critical files for the related operating system. Other critical files, such as those for custom applications, must be evaluated and defined by the entity (that is, the merchant or service provider).
Penetration Testing not Performed for Longer than Policy Standard	11.3.4.1	If segmentation is used, confirm PCI DSS scope by performing penetration testing on segmentation controls at least every six months and after any changes to segmentation controls/methods. **Note:** This requirement is a best practice until January 31, 2018, after which it becomes a requirement.

Configuration

Configuration for Requirement 11 is provided below.

Active Lists

For requirement **11.3.4.1**, change the default time-to-live (TTL) value of 60 days for the Vulnerability Scanned Assets active list to comply with your organization’s policy if necessary.

Rules

- Enable the scenario rules in "Requirement 11 Scenario Rules" on the previous page. The rules are located in the following groups:
  - `ArcSight Solutions/CIP/Compliance Scenarios/Monitoring`
  - `ArcSight Solutions/CIP/Compliance Scenarios/Network Security`
  - `ArcSight Solutions/CIP/Compliance Scenarios/Vulnerability Management`

  For instructions on enabling rules, see "Deploying and Enabling Rules" on page 22.
- For requirement 11.3.4.1: Make sure the below rule ***is*** enabled and deployed:

  `ArcSight Solutions/CIP/Compliance Scenarios/Vulnerability Management/Vulnerability Scans`

Requirement 12: Maintaining an Information Security Policy

The PCI DSS 3.2.1 provides the following definition for this requirement.

Requirement 12: Maintain a policy that addresses information security for all personnel.

A strong security policy sets the security tone for the whole entity and informs personnel what is expected of them. All personnel should be aware of the sensitivity of data and their responsibilities for protecting it. For the purposes of Requirement 12, “personnel” refers to full-time and part-time employees, temporary employees, contractors and consultants who are “resident” on the entity’s site or otherwise have access to the cardholder data environment.

Compliance Scenarios

CIP for PCI provides the following compliance scenario rules to determine compliance with Requirement 12:

Requirement 12 Scenario Rule

Rule	PCI DSS Requirement	Description
Policy Violations	12.4	Ensure that the security policy and procedures clearly define information security responsibilities for all personnel.

Configuration

Configuration for Requirement 12.4 is as follows:

Enable the scenario rules in "Requirement 12 Scenario Rule" above. The rule is located in the following group:

```
ArcSight Solutions/CIP/Compliance Scenarios/Monitoring
```

For instructions on enabling rules, see "Deploying and Enabling Rules" on page 22.

Additional Resources that Support the 12.4 Requirement

Resource Type	Resource
Dashboard	Policy Violations
Report	Policy Violations

Chapter 4: Using CIP for PCI

This section explains how to use these CIP for PCI dashboards:

- **PCI DSS Compliance Status**
- **Unauthorized Cardholder Data Accesses**
- **Negative Impact Compliance Scenarios In the Last 7 Days**

Many of the features demonstrated in this chapter are available on other CIP for PCI dashboards.

Using the PCI DSS Compliance Status Dashboard

The **PCI DSS Compliance Status** dashboard is a good starting point for determining PCI compliance in your organization.

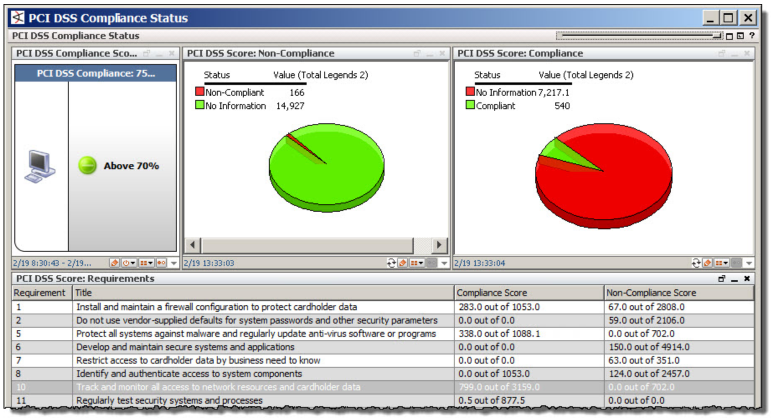
Note: Make sure the CIP for PCI rules, trends, and data monitors are enabled, as described in "Configuring CIP for PCI " on page 20 and "Compliance Scenario Configuration" on page 33.

To use the dashboard:

1. Click the **Use Cases** tab in the Navigator panel and open the **PCI DSS Compliance Status** use case located in:

   ```
   Use Cases/Shared/All Use Cases/ArcSight Solutions/CIP
   ```

2. Open the PCI DSS Compliance Status dashboard.


PCI DSS Compliance Status
PCI DSS Compliance Status
PCI DSS Compliance Sco...
PCI DSS Compliance: 75...
Above 70%
2/19 8:30:43 - 2/19...
PCI DSS Score: Non-Compliance
2/19 13:33:03
PCI DSS Score: Compliance
2/19 13:33:04
PCI DSS Score: Requirements

Status	Value (Total Legends 2)
🟥 Non-Compliant	166
🟩 No Information	14,927

Status	Value (Total Legends 2)
🟥 No Information	7,217.1
🟩 Compliant	540

Requirement	Title	Compliance Score	Non-Compliance Score
1	Install and maintain a firewall configuration to protect cardholder data	283.0 out of 1053.0	67.0 out of 2808.0
2	Do not use vendor-supplied defaults for system passwords and other security parameters	0.0 out of 0.0	59.0 out of 2106.0
5	Protect all systems against malware and regularly update anti-virus software or programs	338.0 out of 1088.1	0.0 out of 702.0
6	Develop and maintain secure systems and applications	0.0 out of 0.0	150.0 out of 4914.0
7	Restrict access to cardholder data by business need to know	0.0 out of 0.0	63.0 out of 351.0
8	Identify and authenticate access to system components	0.0 out of 1053.0	124.0 out of 2457.0
10	Track and monitor all access to network resources and cardholder data	799.0 out of 3159.0	0.0 out of 702.0
11	Regularly test security systems and processes	0.5 out of 877.5	0.0 out of 0.0

The dashboard shows compliance and non-compliance separately in the pie charts.

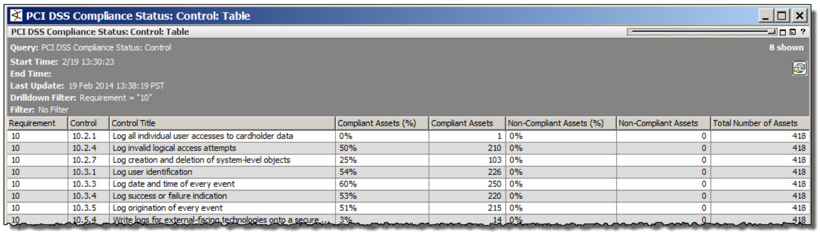
The scores in the dashboard are calculated by CIP for PCI and are derived from the following information:

- the total number of assets sending events from your PCI environment
- the number of events that indicate compliance (those detected by scenario rules that can have a positive impact type of Y or Y/N)
- the number of events that indicate non-compliance (those detected by scenario rules that can have a negative impact type of N or Y/N)
- an estimated maximum, potential compliance score and non-compliance score, based on the above information and the total number of scenario rules

  The **No Information** values represents the difference between the maximum potential compliance/non-compliance scores and the actual scores.

  The lower half of the dashboard provides scores for each PCI DSS requirement.

3. Double-click any requirement row to drill down to information about its sub-requirements (controls).



PCI DSS Compliance Status: Control: Table

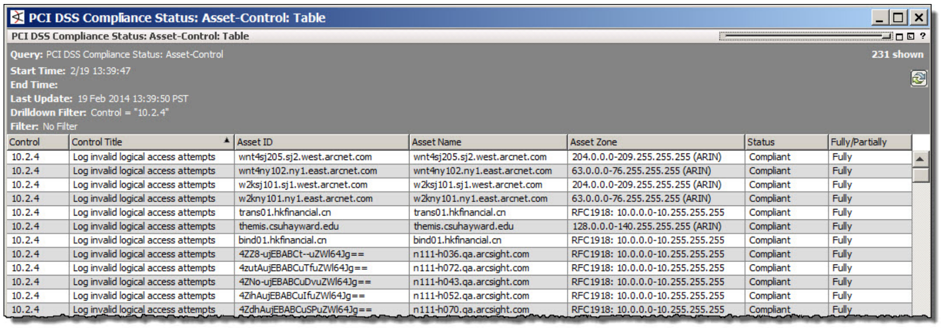
PCI DSS Compliance Status: Control: Table

Query: PCI DSS Compliance Status: Control
Start Time: 2/19 13:30:23
End Time:
Last Update: 19 Feb 2014 13:38:19 PST
Drilldown Filter: Requirement = "10"
Filter: No Filter

8 shown

Requirement	Control	Control Title	Compliant Assets (%)	Compliant Assets	Non-Compliant Assets (%)	Non-Compliant Assets	Total Number of Assets
10	10.2.1	Log all individual user accesses to cardholder data	0%	1	0%	0	418
10	10.2.4	Log invalid logical access attempts	50%	210	0%	0	418
10	10.2.7	Log creation and deletion of system-level objects	25%	103	0%	0	418
10	10.3.1	Log user identification	54%	226	0%	0	418
10	10.3.3	Log date and time of every event	60%	250	0%	0	418
10	10.3.4	Log success or failure indication	53%	220	0%	0	418
10	10.3.5	Log origination of every event	51%	215	0%	0	418
10	10.5.4	Write logs for external-facing technologies onto a secure ...	3%	14	0%	0	418

4. Double-click any sub-requirement to drilldown to a list of assets and the compliance status of each.



PCI DSS Compliance Status: Asset-Control: Table

PCI DSS Compliance Status: Asset-Control: Table

Query: PCI DSS Compliance Status: Asset-Control
Start Time: 2/19 13:39:47
End Time:
Last Update: 19 Feb 2014 13:39:50 PST
Drilldown Filter: Control = "10.2.4"
Filter: No Filter

231 shown

Control	Control Title	Asset ID	Asset Name	Asset Zone	Status	Fully/Partially
10.2.4	Log invalid logical access attempts	wnt4sj205.sj2.west.arcnet.com	wnt4sj205.sj2.west.arcnet.com	204.0.0.0-209.255.255.255 (ARIN)	Compliant	Fully
10.2.4	Log invalid logical access attempts	wnt4ny102.ny1.east.arcnet.com	wnt4ny102.ny1.east.arcnet.com	63.0.0.0-76.255.255.255 (ARIN)	Compliant	Fully
10.2.4	Log invalid logical access attempts	w2ksj101.sj1.west.arcnet.com	w2ksj101.sj1.west.arcnet.com	204.0.0.0-209.255.255.255 (ARIN)	Compliant	Fully
10.2.4	Log invalid logical access attempts	w2kny101.ny1.east.arcnet.com	w2kny101.ny1.east.arcnet.com	63.0.0.0-76.255.255.255 (ARIN)	Compliant	Fully
10.2.4	Log invalid logical access attempts	trans01.hkfinancial.cn	trans01.hkfinancial.cn	RFC1918: 10.0.0.0-10.255.255.255	Compliant	Fully
10.2.4	Log invalid logical access attempts	themis.csuhayward.edu	themis.csuhayward.edu	128.0.0.0-140.255.255.255 (ARIN)	Compliant	Fully
10.2.4	Log invalid logical access attempts	bind01.hkfinancial.cn	bind01.hkfinancial.cn	RFC1918: 10.0.0.0-10.255.255.255	Compliant	Fully
10.2.4	Log invalid logical access attempts	4ZZ8-ujEBABCt--uZWl64Jg==	n111-h036.qa.arcsight.com	RFC1918: 10.0.0.0-10.255.255.255	Compliant	Fully
10.2.4	Log invalid logical access attempts	4zutAujEBABCuTfuZWl64Jg==	n111-h072.qa.arcsight.com	RFC1918: 10.0.0.0-10.255.255.255	Compliant	Fully
10.2.4	Log invalid logical access attempts	4ZNo-ujEBABCuDvuZWl64Jg==	n111-h043.qa.arcsight.com	RFC1918: 10.0.0.0-10.255.255.255	Compliant	Fully
10.2.4	Log invalid logical access attempts	4ZihAujEBABCuIfuZWl64Jg==	n111-h052.qa.arcsight.com	RFC1918: 10.0.0.0-10.255.255.255	Compliant	Fully
10.2.4	Log invalid logical access attempts	4ZdhAujEBABCuSPuZWl64Jg==	n111-h070.qa.arcsight.com	RFC1918: 10.0.0.0-10.255.255.255	Compliant	Fully

Other helpful resources:

- To view the top 50 non-compliant assets, use the following query viewer:

  `/All Query Viewers/ArcSight Solutions/CIP/Regulations/PCI DSS/PCI DSS Top 50 Non-Compliant Assets`

  To see more than 50 assets, edit the query viewer and increase the **Row Limit** parameter.

- To view the compliance status for a specific asset, run the following report and provide the **AssetID** parameter:

  `/All Reports/ArcSight Solutions/CIP/General/Asset Compliance Score`

  The reports shows the controls for the asset and the compliance score for each control.

Using the Unauthorized Cardholder Data Accesses Dashboard

The Compliance Scenario Correlation Events dashboard shows details about access to cardholder data systems and direct access to cardholder databases by unauthorized users. Only users who are identified as a database administrator are considered authorized users.

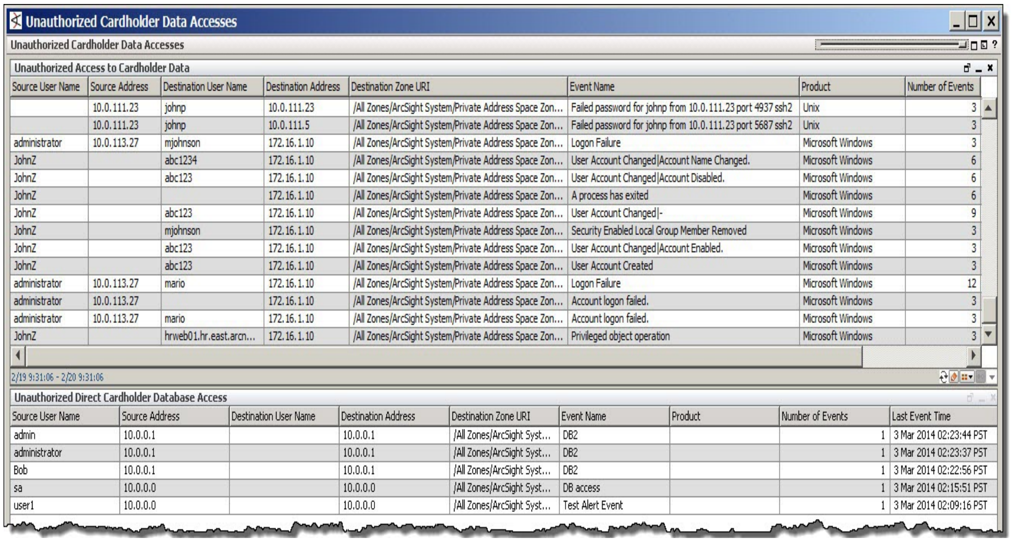
Note: Make sure the **Database Administrators** active list is populated with the user names of the database administrators in your organization.

To use the dashboard:

1. Click the **Use Cases** tab in the Navigator panel and open the Access Control use case located in:

   `Use Cases/Shared/All Use Cases/ArcSight Solutions/CIP`

2. Open the Unauthorized Cardholder Data Accesses dashboard.



Unauthorized Cardholder Data Accesses

Unauthorized Cardholder Data Accesses

Unauthorized Access to Cardholder Data

Source User Name	Source Address	Destination User Name	Destination Address	Destination Zone URI	Event Name	Product	Number of Events
	10.0.111.23	johnp	10.0.111.23	/All Zones/ArcSight System/Private Address Space Zon...	Failed password for johnp from 10.0.111.23 port 4937 ssh2	Unix	3
	10.0.111.23	johnp	10.0.111.5	/All Zones/ArcSight System/Private Address Space Zon...	Failed password for johnp from 10.0.111.23 port 5687 ssh2	Unix	3
administrator	10.0.113.27	mjohnson	172.16.1.10	/All Zones/ArcSight System/Private Address Space Zon...	Logon Failure	Microsoft Windows	3
JohnZ		abc1234	172.16.1.10	/All Zones/ArcSight System/Private Address Space Zon...	User Account Changed|Account Name Changed.	Microsoft Windows	6
JohnZ		abc123	172.16.1.10	/All Zones/ArcSight System/Private Address Space Zon...	User Account Changed|Account Disabled.	Microsoft Windows	6
JohnZ			172.16.1.10	/All Zones/ArcSight System/Private Address Space Zon...	A process has exited	Microsoft Windows	6
JohnZ		abc123	172.16.1.10	/All Zones/ArcSight System/Private Address Space Zon...	User Account Changed|-	Microsoft Windows	9
JohnZ		mjohnson	172.16.1.10	/All Zones/ArcSight System/Private Address Space Zon...	Security Enabled Local Group Member Removed	Microsoft Windows	3
JohnZ		abc123	172.16.1.10	/All Zones/ArcSight System/Private Address Space Zon...	User Account Changed|Account Enabled.	Microsoft Windows	3
JohnZ		abc123	172.16.1.10	/All Zones/ArcSight System/Private Address Space Zon...	User Account Created	Microsoft Windows	3
administrator	10.0.113.27	mario	172.16.1.10	/All Zones/ArcSight System/Private Address Space Zon...	Logon Failure	Microsoft Windows	12
administrator	10.0.113.27		172.16.1.10	/All Zones/ArcSight System/Private Address Space Zon...	Account logon failed.	Microsoft Windows	3
administrator	10.0.113.27	mario	172.16.1.10	/All Zones/ArcSight System/Private Address Space Zon...	Account logon failed.	Microsoft Windows	3
JohnZ		hrweb01.hr.east.arcn...	172.16.1.10	/All Zones/ArcSight System/Private Address Space Zon...	Privileged object operation	Microsoft Windows	3

2/19 9:31:06 - 2/20 9:31:06

Unauthorized Direct Cardholder Database Access

Source User Name	Source Address	Destination User Name	Destination Address	Destination Zone URI	Event Name	Product	Number of Events	Last Event Time
admin	10.0.0.1		10.0.0.1	/All Zones/ArcSight Syst...	DB2		1	3 Mar 2014 02:23:44 PST
administrator	10.0.0.1		10.0.0.1	/All Zones/ArcSight Syst...	DB2		1	3 Mar 2014 02:23:37 PST
Bob	10.0.0.1		10.0.0.1	/All Zones/ArcSight Syst...	DB2		1	3 Mar 2014 02:22:56 PST
sa	10.0.0.0		10.0.0.0	/All Zones/ArcSight Syst...	DB access		1	3 Mar 2014 02:15:51 PST
user1	10.0.0.0		10.0.0.0	/All Zones/ArcSight Syst...	Test Alert Event		1	3 Mar 2014 02:09:16 PST

3. To focus on a particular scenario, return to the Access Control use case and run the appropriate report, for example the Anonymous Access to Cardholder Data Environment report.

Using the Negative Impact Compliance Scenarios In the Last 7 Days Dashboard

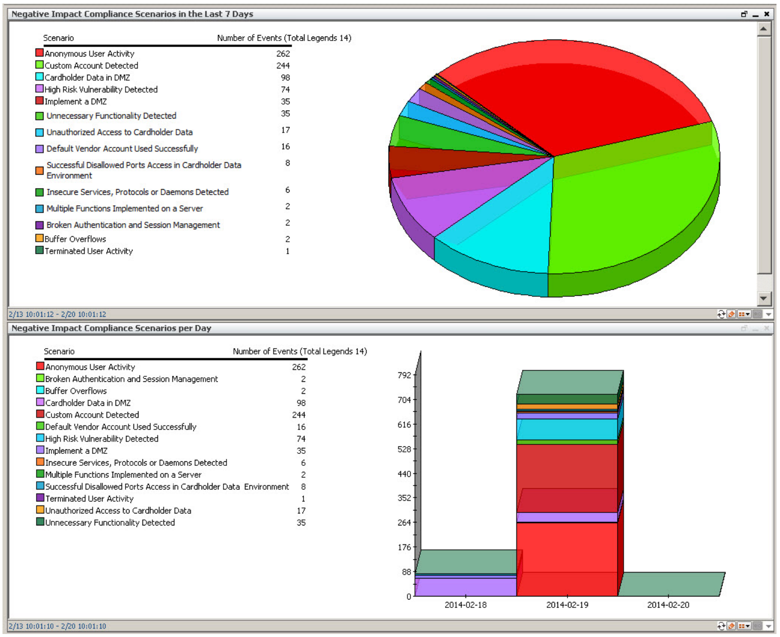
The Negative Impact Compliance Scenarios in the Last 7 Days dashboard graphically represents the number of events that negatively affect compliance, such as terminated user activity and unauthorized access to cardholder data.

To use the dashboard:

1. Click the **Use Cases** tab in the Navigator panel and open the General use case located in:

   `Use Cases/Shared/All Use Cases/ArcSight Solutions/CIP`

2. Open theNegative Impact Compliance Scenarios in the Last 7 Days dashboard.



Negative Impact Compliance Scenarios in the Last 7 Days

	Scenario	Number of Events (Total Legends 14)
🟥	Anonymous User Activity	262
🟩	Custom Account Detected	244
🟦	Cardholder Data in DMZ	98
🟪	High Risk Vulnerability Detected	74
🟥	Implement a DMZ	35
🟩	Unnecessary Functionality Detected	35
🟦	Unauthorized Access to Cardholder Data	17
🟪	Default Vendor Account Used Successfully	16
🟧	Successful Disallowed Ports Access in Cardholder Data Environment	8
🟩	Insecure Services, Protocols or Daemons Detected	6
🟦	Multiple Functions Implemented on a Server	2
🟪	Broken Authentication and Session Management	2
🟧	Buffer Overflows	2
🟩	Terminated User Activity	1

2/13 10:01:12 - 2/20 10:01:12

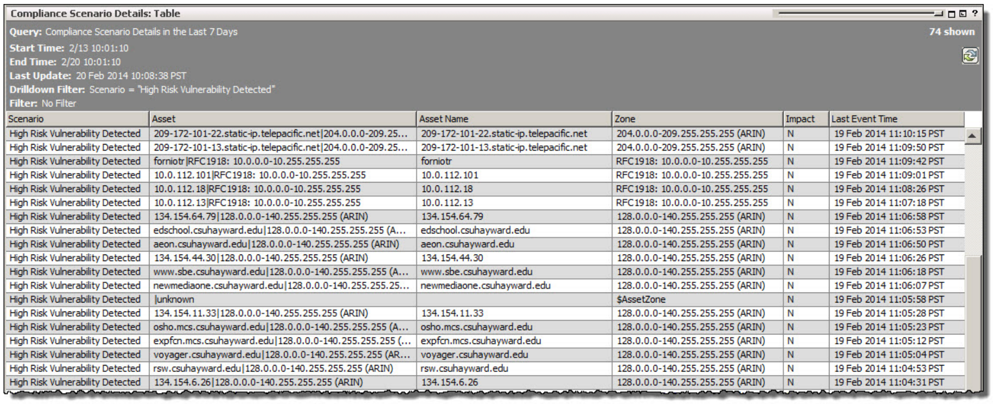
Negative Impact Compliance Scenarios per Day

	Scenario	Number of Events (Total Legends 14)
🟥	Anonymous User Activity	262
🟩	Broken Authentication and Session Management	2
🟦	Buffer Overflows	2
🟪	Cardholder Data in DMZ	98
🟥	Custom Account Detected	244
🟩	Default Vendor Account Used Successfully	16
🟦	High Risk Vulnerability Detected	74
🟪	Implement a DMZ	35
🟧	Insecure Services, Protocols or Daemons Detected	6
🟩	Multiple Functions Implemented on a Server	2
🟦	Successful Disallowed Ports Access in Cardholder Data Environment	8
🟪	Terminated User Activity	1
🟧	Unauthorized Access to Cardholder Data	17
🟩	Unnecessary Functionality Detected	35

2/13 10:01:10 - 2/20 10:01:10

Each colored section in the charts represents the number of events for each scenario, as described in the legends on the left side of the dashboard.

3. Double-click on a section of either chart to see which assets were detected by a particular scenario:



Compliance Scenario Details: Table

Query: Compliance Scenario Details in the Last 7 Days **74 shown**
Start Time: 2/13 10:01:10
End Time: 2/20 10:01:10
Last Update: 20 Feb 2014 10:08:38 PST
Drilldown Filter: Scenario = "High Risk Vulnerability Detected"
Filter: No Filter

Scenario	Asset	Asset Name	Zone	Impact	Last Event Time
High Risk Vulnerability Detected	209-172-101-22.static-ip.telepacific.net|204.0.0.0-209.25...	209-172-101-22.static-ip.telepacific.net	204.0.0.0-209.255.255.255 (ARIN)	N	19 Feb 2014 11:10:15 PST
High Risk Vulnerability Detected	209-172-101-13.static-ip.telepacific.net|204.0.0.0-209.25...	209-172-101-13.static-ip.telepacific.net	204.0.0.0-209.255.255.255 (ARIN)	N	19 Feb 2014 11:09:50 PST
High Risk Vulnerability Detected	forniotr|RFC1918: 10.0.0.0-10.255.255.255	forniotr	RFC1918: 10.0.0.0-10.255.255.255	N	19 Feb 2014 11:09:42 PST
High Risk Vulnerability Detected	10.0.112.101|RFC1918: 10.0.0.0-10.255.255.255	10.0.112.101	RFC1918: 10.0.0.0-10.255.255.255	N	19 Feb 2014 11:09:01 PST
High Risk Vulnerability Detected	10.0.112.18|RFC1918: 10.0.0.0-10.255.255.255	10.0.112.18	RFC1918: 10.0.0.0-10.255.255.255	N	19 Feb 2014 11:08:26 PST
High Risk Vulnerability Detected	10.0.112.13|RFC1918: 10.0.0.0-10.255.255.255	10.0.112.13	RFC1918: 10.0.0.0-10.255.255.255	N	19 Feb 2014 11:07:18 PST
High Risk Vulnerability Detected	134.154.64.79|128.0.0.0-140.255.255.255 (ARIN)	134.154.64.79	128.0.0.0-140.255.255.255 (ARIN)	N	19 Feb 2014 11:06:58 PST
High Risk Vulnerability Detected	edschool.csuhayward.edu|128.0.0.0-140.255.255.255 (A...	edschool.csuhayward.edu	128.0.0.0-140.255.255.255 (ARIN)	N	19 Feb 2014 11:06:53 PST
High Risk Vulnerability Detected	aeon.csuhayward.edu|128.0.0.0-140.255.255.255 (ARIN)	aeon.csuhayward.edu	128.0.0.0-140.255.255.255 (ARIN)	N	19 Feb 2014 11:06:50 PST
High Risk Vulnerability Detected	134.154.44.30|128.0.0.0-140.255.255.255 (ARIN)	134.154.44.30	128.0.0.0-140.255.255.255 (ARIN)	N	19 Feb 2014 11:06:26 PST
High Risk Vulnerability Detected	www.sbe.csuhayward.edu|128.0.0.0-140.255.255.255 (A...	www.sbe.csuhayward.edu	128.0.0.0-140.255.255.255 (ARIN)	N	19 Feb 2014 11:06:18 PST
High Risk Vulnerability Detected	newmediaone.csuhayward.edu|128.0.0.0-140.255.255.25...	newmediaone.csuhayward.edu	128.0.0.0-140.255.255.255 (ARIN)	N	19 Feb 2014 11:06:07 PST
High Risk Vulnerability Detected	|unknown		$AssetZone	N	19 Feb 2014 11:05:58 PST
High Risk Vulnerability Detected	134.154.11.33|128.0.0.0-140.255.255.255 (ARIN)	134.154.11.33	128.0.0.0-140.255.255.255 (ARIN)	N	19 Feb 2014 11:05:28 PST
High Risk Vulnerability Detected	osho.mcs.csuhayward.edu|128.0.0.0-140.255.255.255 (A...	osho.mcs.csuhayward.edu	128.0.0.0-140.255.255.255 (ARIN)	N	19 Feb 2014 11:05:23 PST
High Risk Vulnerability Detected	expfcn.mcs.csuhayward.edu|128.0.0.0-140.255.255.255 (...	expfcn.mcs.csuhayward.edu	128.0.0.0-140.255.255.255 (ARIN)	N	19 Feb 2014 11:05:12 PST
High Risk Vulnerability Detected	voyager.csuhayward.edu|128.0.0.0-140.255.255.255 (AR...	voyager.csuhayward.edu	128.0.0.0-140.255.255.255 (ARIN)	N	19 Feb 2014 11:05:04 PST
High Risk Vulnerability Detected	rsw.csuhayward.edu|128.0.0.0-140.255.255.255 (ARIN)	rsw.csuhayward.edu	128.0.0.0-140.255.255.255 (ARIN)	N	19 Feb 2014 11:04:53 PST
High Risk Vulnerability Detected	134.154.6.26|128.0.0.0-140.255.255.255 (ARIN)	134.154.6.26	128.0.0.0-140.255.255.255 (ARIN)	N	19 Feb 2014 11:04:31 PST

Appendix A: Backing Up and Uninstalling a Package

This chapter provides instructions on how back up a solution package, and uninstall the CIP for PCI.

Caution: There is no migration path from CIP for PCI 3.x or earlier. If you are running CIP for PCI 3.x or earlier and you need to keep your current data, do not **uninstall** your earlier version; instead install CIP for PCI 4.1 on a different system.

Generating a List of Resource Changes

Before backing up a solution package, you can generate a list of the resource changes since the last time the package was exported to a package bundle. The current resources associated with the selected package are compared against the resources saved in the package bundle and any new, modified or deleted resources are reported.

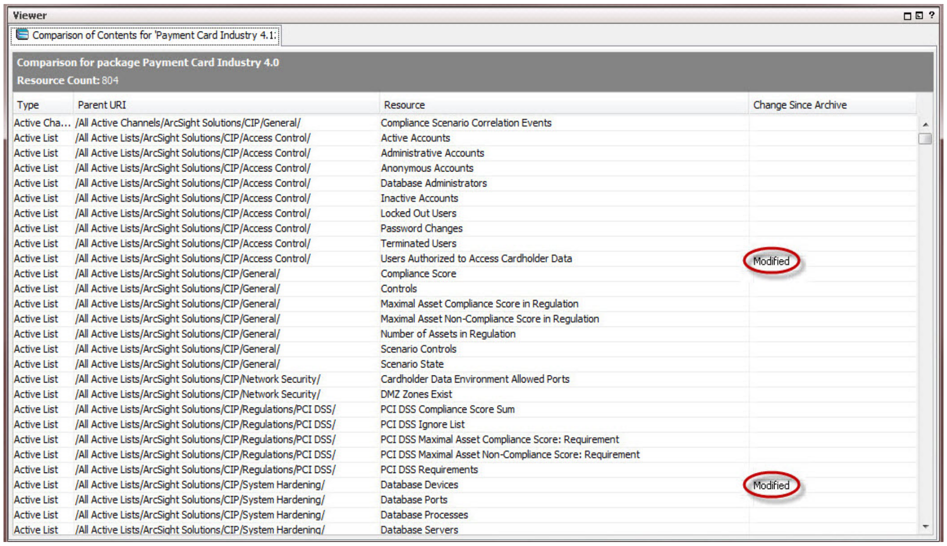
Note: Every time a package is exported, the change history resets.

To generate a list of resource changes:

1. Log into the ArcSight Console with an account that has administrative privileges.
2. In the **Packages** tab of the Navigator panel, navigate to the solution group.

   For CIP for PCI, navigate to `ArcSight Solutions`.
3. Right-click the package for which you want to generate resource changes (▤) and select **Compare Archive with Current Package Contents.**

   In the Viewer panel, a list of resources associated with the package are displayed. In the right column called `Change Since Archive`, any changes with the resource since the last export are displayed, either `Added`, `Modified`, or `Removed`.



Comparison for package Payment Card Industry 4.0
Resource Count: 804

Type	Parent URI	Resource	Change Since Archive
Active Cha...	/All Active Channels/ArcSight Solutions/CIP/General/	Compliance Scenario Correlation Events	
Active List	/All Active Lists/ArcSight Solutions/CIP/Access Control/	Active Accounts	
Active List	/All Active Lists/ArcSight Solutions/CIP/Access Control/	Administrative Accounts	
Active List	/All Active Lists/ArcSight Solutions/CIP/Access Control/	Anonymous Accounts	
Active List	/All Active Lists/ArcSight Solutions/CIP/Access Control/	Database Administrators	
Active List	/All Active Lists/ArcSight Solutions/CIP/Access Control/	Inactive Accounts	
Active List	/All Active Lists/ArcSight Solutions/CIP/Access Control/	Locked Out Users	
Active List	/All Active Lists/ArcSight Solutions/CIP/Access Control/	Password Changes	
Active List	/All Active Lists/ArcSight Solutions/CIP/Access Control/	Terminated Users	
Active List	/All Active Lists/ArcSight Solutions/CIP/Access Control/	Users Authorized to Access Cardholder Data	Modified
Active List	/All Active Lists/ArcSight Solutions/CIP/General/	Compliance Score	
Active List	/All Active Lists/ArcSight Solutions/CIP/General/	Controls	
Active List	/All Active Lists/ArcSight Solutions/CIP/General/	Maximal Asset Compliance Score in Regulation	
Active List	/All Active Lists/ArcSight Solutions/CIP/General/	Maximal Asset Non-Compliance Score in Regulation	
Active List	/All Active Lists/ArcSight Solutions/CIP/General/	Number of Assets in Regulation	
Active List	/All Active Lists/ArcSight Solutions/CIP/General/	Scenario Controls	
Active List	/All Active Lists/ArcSight Solutions/CIP/General/	Scenario State	
Active List	/All Active Lists/ArcSight Solutions/CIP/Network Security/	Cardholder Data Environment Allowed Ports	
Active List	/All Active Lists/ArcSight Solutions/CIP/Network Security/	DMZ Zones Exist	
Active List	/All Active Lists/ArcSight Solutions/CIP/Regulations/PCI DSS/	PCI DSS Compliance Score Sum	
Active List	/All Active Lists/ArcSight Solutions/CIP/Regulations/PCI DSS/	PCI DSS Ignore List	
Active List	/All Active Lists/ArcSight Solutions/CIP/Regulations/PCI DSS/	PCI DSS Maximal Asset Compliance Score: Requirement	
Active List	/All Active Lists/ArcSight Solutions/CIP/Regulations/PCI DSS/	PCI DSS Maximal Asset Non-Compliance Score: Requirement	
Active List	/All Active Lists/ArcSight Solutions/CIP/Regulations/PCI DSS/	PCI DSS Requirements	
Active List	/All Active Lists/ArcSight Solutions/CIP/System Hardening/	Database Devices	Modified
Active List	/All Active Lists/ArcSight Solutions/CIP/System Hardening/	Database Ports	
Active List	/All Active Lists/ArcSight Solutions/CIP/System Hardening/	Database Processes	
Active List	/All Active Lists/ArcSight Solutions/CIP/System Hardening/	Database Servers	

4. Optional—For future reference, you can copy and paste the cells from this table into a spreadsheet.

Backing Up the Solution Package

Keep a backup of the current state before making content changes or installing and uninstalling solution packages. Before backing up a solution, you can obtain a list of changed resources. You can then back up only those resources that have been modified or added. For detailed instructions, see "Generating a List of Resource Changes" on page 62.

You can back up the solution content to a package bundle file that ends in the `.arb` extension as described in the process below.

To back up a solution package:

1. Log into the ArcSight Console with an account that has administrative privileges.
2. In the **Packages** tab of the Navigator panel, navigate to the solution group.

   For CIP for PCI, navigate to `ArcSight Solutions/`.
3. Right-click the package (▤) and select **Export Package(s) to Bundle**.

   The Package Bundle Export dialog displays.
4. In the Package Bundle Export dialog, browse for a directory location, specify a file name and click **Next**.

   The Progress tab of the Export Packages dialog displays the progress of the export.
5. When the export is complete, click **OK**.

   The resources are saved into the package bundle file that ends with the `.arb` extension. You can restore the contents of this package at a later time by importing this package bundle file.

Uninstalling the CIP for PCI

Before uninstalling the CIP for PCI, back up all the packages (▤) for all the solutions currently installed on the ArcSight Manager. For example, if the CIP for PCI and the CIP for SOX solution are both installed on the same ArcSight Manager, export the package for each solution before uninstalling either solution. Back up the CIP for SOX package into a package bundle (ARB) file and then back up the CIP for PCI into a different package bundle (ARB) file before uninstalling either solution. For detailed instructions, see "Backing Up the Solution Package" on the previous page. To generate a list of resource changes before the uninstall, see "Generating a List of Resource Changes" on page 62.

To uninstall the CIP for PCI:

1. Log into the ArcSight Console with an account that has administrative privileges.

   Do not uninstall CIP for PCI as the systemuser. Doing so uninstalls resources that are intentionally locked.

2. Click the **Packages** tab in the Navigator panel.
3. Navigate to `ArcSight Solutions`, right-click the CIP for PCI package (▤), and select **Uninstall Package**.
4. In the Uninstall Packages dialog, click **OK**. The progress of the uninstall displays in the Progress tab of the Uninstalling Packages dialog.

   If a message indicates that resources are locked, select the **Skip** option in the **Resolution Options** area and click **OK**.

   If a message indicates a conflict about changed package content, select the **Continue without saving changes** option and click **OK**.

5. When the uninstall is complete, review the summary and click **OK**.
6. Right-click the CIP for PCI package and select **Delete Package.**

Appendix B: Compliance Insight Package for the Payment Card Industry Resources by Type

This appendix lists all the Compliance Insight Package for the Payment Card Industry resources by type.

Active Channels

The following table lists all the active channels in Compliance Insight Package for the PCI.

Active Channels Resources

Resource	Description	URI
Compliance Scenario Correlation Events	This active channel shows all correlation events that are related to compliance scenarios.	`ArcSight Solutions/CIP/General/`

Active Lists

The following table lists all the active lists in Compliance Insight Package for the Payment Card Industry.

Active Lists Resources

Resource	Description	URI
Active Accounts	This active list stores usernames that have successfully logged in within the last 90 days. Customize the Time-To-Live (TTL) field of this active list to match the definition of stale (inactive) accounts in your environment.	`ArcSight Solutions/CIP/Access Control/`
Administrative Accounts	This active list stores the account names of administrative users. All the entries in this list must be in lowercase.	`ArcSight Solutions/CIP/Access Control/`
Anonymous Accounts	This active list stores the account names of anonymous users that are not unique and do not belong to a single individual user. All the entries in this list must be in lowercase.	`ArcSight Solutions/CIP/Access Control/`
Cardholder Data Environment Allowed Ports	This active list contains all permissible inbound and outbound ports (all permissible services). Populate this active list according to your policy and the PCI DSS regulation, which requires restricted connections between untrusted networks and any system components in the cardholder data environment. Direction is either inbound or outbound, and must be lowercase.	`ArcSight Solutions/CIP/Network Security/`
Compliance Score	This active list maintains compliance score for the system assets.	`ArcSight Solutions/CIP/General/`
Controls	This active list maintains a list of controls for all the supported regulations in the solution.	`ArcSight Solutions/CIP/General/`
DMZ Zones Exist	This active list indicates if there are zones that belong to the DMZ category. If such zones exist in the system, the active list holds a single value: 1. Otherwise, the active list is empty. Do not update this active list manually.	`ArcSight Solutions/CIP/Network Security/`
Database Administrators	This active list stores the usernames of the database administrators. All the entries in this list must be in lowercase.	`ArcSight Solutions/CIP/Access Control/`
Database Devices	This active list maintains a list of Device Product names for database devices.	`ArcSight Solutions/CIP/System Hardening/`
Database Ports	This active list maintains a list of database ports. Populate this active list with other database ports in the network.	`ArcSight Solutions/CIP/System Hardening/`
Database Processes	This active list maintains a list of database processes.	`ArcSight Solutions/CIP/System Hardening/`
Database Servers	This active list maintains a list of new database servers (database servers that do not belong to the Database category).	`ArcSight Solutions/CIP/System Hardening/`

Active Lists Resources, continued

Resource	Description	URI
Default Vendor Accounts	This active list contains some well-known vendor-supplied default accounts. Populate this active list with other vendor accounts in the network. All the entries in this list must be in lowercase.	`ArcSight Solutions/CIP/System Hardening/`
Domain Name Server Devices	This active list maintains a list of Device Product names for DNS devices.	`ArcSight Solutions/CIP/System Hardening/`
Domain Name Server Ports	This active list maintains a list of DNS ports. Populate this active list with other DNS ports in the network.	`ArcSight Solutions/CIP/System Hardening/`
Domain Name Server Processes	This active list maintains a list of DNS processes.	`ArcSight Solutions/CIP/System Hardening/`
Domain Name Servers	This active list maintains a list of new Domain Name Servers (Domain Name Servers that do not belong to the Domain Name Server category).	`ArcSight Solutions/CIP/System Hardening/`
Inactive Accounts	This active list stores user names that have not appeared in login events for the time specified by the Active Accounts active list TTL value.	`ArcSight Solutions/CIP/Access Control/`
Insecure Ports	This active list includes ports related to unencrypted (insecure) communication services.	`ArcSight Solutions/CIP/System Hardening/`
Insecure Processes	This active list includes the names of processes that provide unencrypted (insecure) communication.	`ArcSight Solutions/CIP/System Hardening/`
Locked Out Users	This active list maintains a list of users that have been locked out of their accounts.	`ArcSight Solutions/CIP/Access Control/`
Maximal Asset Compliance Score in Regulation	This active list stores the maximum potential compliance score for a single asset, for each regulation. Do not manually update this active list.	`ArcSight Solutions/CIP/General/`
Maximal Asset Non-Compliance Score in Regulation	This active list stores the maximum potential non-compliance score for a single asset, for each regulation. Do not manually update this active list.	`ArcSight Solutions/CIP/General/`
Multi Factor Authentication Devices	This active list stores the multi factor authentication devices. All the entries in this list must be in lowercase.	`ArcSight Solutions/CIP/Access Control/`
Non Multi Factor Authentication Devices - Exception	This active list stores non multi factor authentication devices which you want to exclude. All the entries in this list must be in lowercase.	`ArcSight Solutions/CIP/Access Control/`

Active Lists Resources, continued

Resource	Description	URI
Number of Assets in Regulation	This active list stores the number of assets that were reported for compliance or non-compliance for at least one control in a regulation. This active list is updated by a trend and is used by solution reports. Do not manually update this active list.	`ArcSight Solutions/CIP/General/`
PCI DSS Compliance Score Sum	This active list stores PCI DSS compliance and non-compliance score summations for all control-asset pairs in the system. It has one row duplicated three times, each time for a different Status column value, as follows: *Compliant: *Non-compliant *No Information This information is required to build the top level compliance/non-compliance reports for the PCI DSS regulation. Do not manually update this active list.	`ArcSight Solutions/CIP/Regulations/PCI DSS/`
PCI DSS Ignore List	This active list stores assets or network zones that are not relevant for PCI DSS regulation. * Identify an asset by either its IP address, host name, or ESM resource ID. The ESM resource ID must be used if the asset is known to ESM and, therefore, has been assigned an ESM resource ID. * Host names must be entered in lowercase text. * ESM resource IDs, IP addresses, and zone names must be added as is, in their original case. * Both the Asset ID and Asset Zone fields must be specified. * An asterisk (*) indicates all assets or all zones, as shown in the examples below. To ignore an asset by IP address in a zone: Asset ID 10.0.0.0, Asset Zone = RFC1918: 10.0.0.0-10.255.255.255 To ignore all assets in a zone: Asset ID = *, Asset Zone = RFC1918: 10.0.0.0-10.255.255.255 To ignore an asset by host name in all zones: Asset ID = myhostname, Asset Zone = * To ignore an asset by ESM resource ID in a zone: Asset ID = 4K5yF+EMBABCU--70AvXMzg==, Asset Zone = RFC1918: 10.0.0.0-10.255.255.255	`ArcSight Solutions/CIP/Regulations/PCI DSS/`

Active Lists Resources, continued

Resource	Description	URI
PCI DSS Maximal Asset Compliance Score: Requirement	This active list stores the maximum potential PCI DSS compliance score for a single asset, for each PCI DSS requirement. Do not manually update this active list.	`ArcSight Solutions/CIP/Regulations/PCI DSS/`
PCI DSS Maximal Asset Non-Compliance Score: Requirement	This active list stores the maximum potential PCI DSS non-compliance score for a single asset, for each PCI DSS requirement. Do not manually update this active list.	`ArcSight Solutions/CIP/Regulations/PCI DSS/`
PCI DSS Requirements	This active list stores the titles and descriptions of PCI DSS requirements.	`ArcSight Solutions/CIP/Regulations/PCI DSS/`
Password Changes	This active list is updated with the user and asset information when a successful password change occurs. The entries in this active list expire after 90 days.	`ArcSight Solutions/CIP/Access Control/`
Scenario Controls	This active list maintains the mappings between the compliance scenarios and the regulation controls. Scenario Type field can have the following values: Y indicates the scenario determines compliance, therefore the Score value must be between 0 and 1. N indicates the scenario determines non-compliance, therefore -1 will be used as compliance score and Score value are ignored. Y/N indicates the scenario determines compliance or non-compliance, therefore the Score value must be between 0 and 1.	`ArcSight Solutions/CIP/General/`
Scenario State	This active list stores the latest state of Y/N compliance scenarios, per asset.	`ArcSight Solutions/CIP/General/`
Terminated Users	This active list stores user accounts of former employees. User accounts in this active list are retained indefinitely. All the entries in this list must be in lowercase.	`ArcSight Solutions/CIP/Access Control/`
Test and Custom Accounts	This active list stores names of development, test, or custom application or user accounts. Populate this active list with additional custom accounts that should be disabled in a production environment. All the entries in this list must be in lowercase.	`ArcSight Solutions/CIP/System Hardening/`
Users Authorized to Access Cardholder Data	This active list stores the usernames of the individuals who are authorized to access the cardholder data environment. All the entries in this list must be in lowercase.	`ArcSight Solutions/CIP/Access Control/`

Active Lists Resources, continued

Resource	Description	URI
Vulnerability Scanned Assets	This active list stores all the assets that were scanned by vulnerability scanners on the last x days, default 60 days. Do not manually update this active list.	`ArcSight Solutions/CIP/Vulnerability Management/`
Web Server Devices	This active list maintains a list of Device Product names for Web server devices.	`ArcSight Solutions/CIP/System Hardening/`
Web Server Ports	This active list maintains a list of Web server ports. Populate this active list with other Web server ports in the network.	`ArcSight Solutions/CIP/System Hardening/`
Web Server Processes	This active list maintains a list of Web server processes.	`ArcSight Solutions/CIP/System Hardening/`
Web Servers	This active list maintains a list of new Web servers (Web servers that do not belong to the Web Server category).	`ArcSight Solutions/CIP/System Hardening/`

Dashboards

The following table lists all the dashboards in Compliance Insight Package for the Payment Card Industry.

Dashboards Resources

Resource	Description	URI
Accounts Lockouts and Failed Logical Access	This dashboard displays information about most products with failed logical access and account lockouts.	`ArcSight Solutions/CIP/Access Control/`
Activities by Illegitimate User Accounts	This dashboard displays activities by illegitimate user accounts, such as terminated users, inactive users, and anonymous users.	`ArcSight Solutions/CIP/Access Control/`
Administrators Activity	This dashboard displays information about administrator activity and the most unsuccessful administrative logins.	`ArcSight Solutions/CIP/Monitoring/`
Anti-Virus Update Status	This dashboard displays information about anti-virus updates by anti-virus products and outcomes.	`ArcSight Solutions/CIP/Vulnerability Management/`
Asset Vulnerabilities	This dashboard displays information about assets and vulnerabilities detected.	`ArcSight Solutions/CIP/Vulnerability Management/`
Audit Log Cleared	This dashboard displays information about audit logs cleared from a host.	`ArcSight Solutions/CIP/Monitoring/`
Cardholder Data Environment Traffic	This dashboard displays cardholder data environment traffic.	`ArcSight Solutions/CIP/Network Security/`
Configuration Changes Overview	This dashboard provides overview of configuration changes.	`ArcSight Solutions/CIP/System Hardening/`
Cryptographic Asset Vulnerabilities	This dashboard displays information about assets and cryptographic vulnerabilities detected.	`ArcSight Solutions/CIP/Vulnerability Management/`
Default Vendor Account Used Successfully	This dashboard displays successful default vendor account usage events.	`ArcSight Solutions/CIP/System Hardening/`
File Changes	This dashboard displays file change activity and the top 10 file activities.	`ArcSight Solutions/CIP/Monitoring/`

Dashboards Resources, continued

Resource	Description	URI
Illegitimate Internet Communications	This dashboard displays information about illegitimate Internet communications, such as direct connections between the Internet and the cardholder data environment, and successful traffic from the Internet into a non-DMZ destination.	`ArcSight Solutions/CIP/Network Security/`
Information System Failures	This dashboard displays information system failures.	`ArcSight Solutions/CIP/Monitoring/`
Insecure Processes and Ports	This dashboard displays information about insecure processes and ports.	`ArcSight Solutions/CIP/System Hardening/`
Negative Impact Compliance Scenarios in the Last 7 Days	This dashboard displays information about negative impact compliance scenarios within the last seven days. The information is based on trends and taken from scenario correlation events. Negative means that device custom string4 equals to N.	`ArcSight Solutions/CIP/General/`
Non Multi Factor Administrative Authentication	This dashboard provides overview of non multi factor administrative authentication.	`ArcSight Solutions/CIP/Access Control/`
Overview of Insecure Transmissions and Cryptography	This dashboard displays insecure cryptography and insecure transmission of cardholder data over public networks.	`ArcSight Solutions/CIP/Cryptography/`

Dashboards Resources, continued

Resource	Description	URI
PCI DSS Compliance Status	This dashboard displays information about PCI DSS compliance status. This includes the following: *PCI DSS Compliance (%) - compliance score/(compliance score + non-compliance score). *PCI DSS Score: Compliance - actual compliance score out of the maximum potential compliance score. *PCI DSS Score: Non-Compliance - actual non-compliance score out of the maximum potential non-compliance score. *PCI DSS Score: Requirements - compliance and non-compliance scores per PCI DSS requirement. If this dashboard displays negative numbers, run manually the following trends in this order: 1)PCI DSS Number of Assets 2)PCI DSS Maximal Asset Compliance Score 3)PCI DSS Maximal Asset Compliance Score: Requirement 4)PCI DSS Maximal Asset Non-Compliance Score 5)PCI DSS Maximal Asset Non-Compliance Score: Requirement 6)PCI DSS Compliance Score Sum	`ArcSight Solutions/CIP/Regulations/PCI DSS/`
Password Changes	This dashboard displays information about failed password changes and all password changes.	`ArcSight Solutions/CIP/Access Control/`
Physical Accesses Overview	This dashboard displays after hours physical accesses and the last 30 physical access attempts.	`ArcSight Solutions/CIP/Physical Security/`
Policy Violations	This dashboard displays policy violations activity.	`ArcSight Solutions/CIP/Monitoring/`
Positive Impact Compliance Scenarios in the Last 7 Days	This dashboard displays information about positive impact compliance scenarios within the last seven days. The information is based on trends and taken from scenario correlation events. Positive means that device custom string4 equals to Y.	`ArcSight Solutions/CIP/General/`
Privacy Protection Overview	This dashboard displays an overview of insecure cryptography and cardholder data transmissions.	`ArcSight Solutions/CIP/Privacy Protection/`
Servers with Unnecessary Functionality	This dashboard displays information about servers with unnecessary functionality. This dashboard shows three types of servers: database servers, domain name servers, and web servers.	`ArcSight Solutions/CIP/System Hardening/`

Dashboards Resources, continued

Resource	Description	URI
Successful Disallowed Ports Access	This dashboard displays information about successful disallowed ports access, such as successful disallowed port access from a wireless network into the cardholder data environment and successful disallowed port access in the cardholder data environment.	`ArcSight Solutions/CIP/Network Security/`
Unauthorized Cardholder Data Accesses	This dashboard displays unauthorized cardholder data accesses.	`ArcSight Solutions/CIP/Access Control/`
User Accounts with Expired Passwords	This dashboard displays accounts for which the password was not changed for longer than the policy standard permits.	`ArcSight Solutions/CIP/Access Control/`

Data Monitors

The following table lists all the data monitors in Compliance Insight Package for the Payment Card Industry.

Data Monitors Resources

Resource	Description	URI
Cryptographic Vulnerabilities Graph	This data monitor presenting cryptographic vulnerabilities in event graph chart.	`ArcSight Solutions/CIP/Vulnerability Management/`
Last 10 Configuration Modifications	Tracks the most recent system configuration modifications.	`ArcSight Solutions/CIP/System Hardening/`
Last 10 Information System Failures	This data monitor shows last 10 information system failures.	`ArcSight Solutions/CIP/Monitoring/`
Last 30 Failed Physical Access Attempts	This data monitor shows last 30 attempts to enter a building at any time.	`ArcSight Solutions/CIP/Physical Security/`
PCI DSS Compliance Score: Top Level	This percent data monitor displays the ultimate compliance score. The score is calculated using the following formula: Overall compliance score / (Overall compliance score + Overall non-compliance score). Where: Overall compliance score = compliance scores summation for all the control-asset pairs in the system. Overall non-compliance score = non-compliance scores summation for all the control-asset pairs in the system.	`ArcSight Solutions/CIP/Regulations/PCI DSS/`

Filters

The following table lists all the filters in Compliance Insight Package for the Payment Card Industry.

Filters Resources

Resource	Description	URI
Accesses to Cardholder Data Environment by Identified Users	This filter detects accesses to the cardholder data environment by an identified user.	`ArcSight Solutions/CIP/Monitoring/`
Account Creation	This filter identifies account creation events.	`ArcSight Solutions/CIP/Access Control/`
Account Deletion	This filter identifies account deletion events.	`ArcSight Solutions/CIP/Access Control/`
Account Lockouts	This filter identifies account lockouts. By default, the filter identifies lockouts on Microsoft Windows, UNIX, and ArcSight systems.	`ArcSight Solutions/CIP/Access Control/`
Account Modification	This filter identifies account modification events.	`ArcSight Solutions/CIP/Access Control/`
Account Unlocked	This filter identifies account unlock events.	`ArcSight Solutions/CIP/Access Control/`
Administrative User Account in Destination	This filter detects events where the Destination User Name is identified as an administrative account.	`ArcSight Solutions/CIP/Access Control/`
Administrative User Account in Source	This filter detects events where the Source User Name is identified as an administrative account.	`ArcSight Solutions/CIP/Access Control/`
After Hours	This filter defines the after hours time period. Change this filter to adjust the default settings.	`ArcSight Solutions/CIP/General/`
Anonymous User Activity	This filter identifies anonymous user activity.	`ArcSight Solutions/CIP/Access Control/`
Anonymous User in Destination	This filter detects events with an anonymous user in the destination.	`ArcSight Solutions/CIP/Access Control/`
Anonymous User in Source	This filter detects events with anonymous user in the source.	`ArcSight Solutions/CIP/Access Control/`
Anti-Virus Clean or Quarantine Attempt	This filter looks for anti-virus events that indicate a quarantine or cleaning attempt of a detected malware instance.	`ArcSight Solutions/CIP/Vulnerability Management/`

Filters Resources, continued

Resource	Description	URI
Anti-Virus Disabled	This filter detects when an anti-virus service has been disabled. This rule requires Windows event logs for each station you want to monitor.	`ArcSight Solutions/CIP/Vulnerability Management/`
Anti-Virus Events	This filter identifies events reported by anti-virus products in your environment.	`ArcSight Solutions/CIP/Vulnerability Management/`
Anti-Virus Scan Completed Successfully	This filter detects successful anti-virus scans.	`ArcSight Solutions/CIP/Vulnerability Management/`
Anti-Virus Scan Failed	This filter detects when an anti-virus scan failed or stopped.	`ArcSight Solutions/CIP/Vulnerability Management/`
Anti-Virus Update Events	This filter identifies events related to anti-virus product data file updates.	`ArcSight Solutions/CIP/Vulnerability Management/`
Anti-Virus Update Failed	This filter detects failed anti-virus updates.	`ArcSight Solutions/CIP/Vulnerability Management/`
Anti-Virus Updated Successfully	This filter detects all successful anti-virus updates.	`ArcSight Solutions/CIP/Vulnerability Management/`
Audit Log Cleared	This filter detects all events where an audit log is cleared from a host. By default, the filter recognizes events on Microsoft Windows, ISS SiteProtector, and Symantec HostID systems. Modify this filter to include events from other devices.	`ArcSight Solutions/CIP/Monitoring/`
Big Difference Between End Time and Manager Receipt Time	This filter identifies time discrepancies between endTime and managerReceiptTime. By default, the filter identifies events with a difference of more than 600 seconds (10 minutes).	`ArcSight Solutions/CIP/Monitoring/`
Bluetooth Protocol Vulnerability Detected	This query retrieves Bluetooth protocol related vulnerabilities.	`ArcSight Solutions/CIP/Vulnerability Management`
Broken Authentication and Session Management	This filter detects authentication and session management flaws reported by vulnerability scanners.	`ArcSight Solutions/CIP/Vulnerability Management/`
Buffer Overflows	This filter detects buffer overflow flaws reported by vulnerability scanners.	`ArcSight Solutions/CIP/Vulnerability Management/`

Filters Resources, continued

Resource	Description	URI
CVSS Score Greater than or Equal to 4	This filter detects vulnerabilities with a Common Vulnerability Scoring System (CVSS) score greater than or equal to 4.	`ArcSight Solutions/CIP/Vulnerability Management/`
Cardholder Data Environment Destination	This filter identifies events with destination in the cardholder data environment.	`ArcSight Solutions/CIP/General/`
Cardholder Data Environment Inbound Traffic	This filter shows all the cardholder data environment inbound traffic.	`ArcSight Solutions/CIP/Network Security/`
Cardholder Data Environment Outbound Traffic	This filter shows all the cardholder data environment outbound traffic.	`ArcSight Solutions/CIP/Network Security/`
Cardholder Data Environment Source	This filter identifies events with source in the cardholder data environment.	`ArcSight Solutions/CIP/General/`
Cardholder Data in DMZ	This filter identifies cardholder data assets in the DMZ segment.	`ArcSight Solutions/CIP/Network Security/`
Clear Text Password Transmission	This filter identifies a successful login or access to a login page through unencrypted ports, which indicates that a user password might be transferred in clear text over the network.	`ArcSight Solutions/CIP/Privacy Protection/`
Compliance Scenario Correlation Events	This filter filters compliance scenario correlation events.	`ArcSight Solutions/CIP/General/`
Configuration Modifications	Detects non-arcsight configuration modifications events.	`ArcSight Solutions/CIP/System Hardening/`
Creation and Deletion of Objects	This filter identifies object creations and deletions.	`ArcSight Solutions/CIP/Monitoring/`
Cross-Site Request Forgery	This filter detects cross-site request forgery vulnerabilities reported by vulnerability scanners.	`ArcSight Solutions/CIP/Vulnerability Management/`
Cross-Site Scripting	This filter detects cross-site scripting flaws reported by vulnerability scanners.	`ArcSight Solutions/CIP/Vulnerability Management/`
Cryptographic Hash Algorithm Related Vulnerability Detected	Selects events indicating that potential hash algorithm related vulnerability was detected.	`ArcSight Solutions/CIP/Vulnerability Management/`

Filters Resources, continued

Resource	Description	URI
Cryptographic Public Key Related Vulnerability Detected	Selects events indicating that potential public key related vulnerability was detected.	`ArcSight Solutions/CIP/Vulnerability Management/`
Cryptographic Symmetric Key Related Vulnerability Detected	Selects events indicating that potential symmetric key related vulnerability was detected.	`ArcSight Solutions/CIP/Vulnerability Management/`
Cryptographic Vulnerabilities	This filter detects cryptographic vulnerabilities correlation events.	`ArcSight Solutions/CIP/Vulnerability Management/`
Cryptographic Weak Protocol Vulnerability Detected	Selects events indicating that potential cryptographic weak protocol related vulnerability was detected.	`ArcSight Solutions/CIP/Vulnerability Management/`
Custom Account in Destination	This filter detects development, test, or custom application or user accounts in a destination.	`ArcSight Solutions/CIP/System Hardening/`
Custom Account in Source	This filter detects development, test, or custom application or user accounts in a source.	`ArcSight Solutions/CIP/System Hardening/`
DMZ Destination	This filter identifies events with destination asset or zone in the DMZ segment.	`ArcSight Solutions/CIP/General/`
DMZ Source	This filter identifies events with source asset or zone in the DMZ segment.	`ArcSight Solutions/CIP/General/`
Database Configuration Modification	Detects database configuration modifications.	`ArcSight Solutions/CIP/System Hardening/`
Database Server in Destination	This filter detects events with database in a destination.	`ArcSight Solutions/CIP/General/`
Database Server in Device	This filter detects events with database in device.	`ArcSight Solutions/CIP/General/`
Database Server in Source	This filter detects events with database in a source.	`ArcSight Solutions/CIP/General/`
Default Vendor Account Used Successfully	This filter identifies successful default vendor account usage.	`ArcSight Solutions/CIP/System Hardening/`
Development or Test Environment in Destination	This filter detects test or development environment assets in destination.	`ArcSight Solutions/CIP/General/`

Filters Resources, continued

Resource	Description	URI
Development or Test Environment in Source	This filter detects test or development environment assets in source.	`ArcSight Solutions/CIP/General/`
Device Time is Later than Agent Time	This filter identifies events in which the device receipt time is after the connector (agent) receipt time. By default, the filter shows events for which the device receipt time is more than 300 seconds (five minutes) after the connector receipt time.	`ArcSight Solutions/CIP/Monitoring/`
Device is Destination	This filter detects events where device is identical to destination.	`ArcSight Solutions/CIP/General/`
Device is Source	This filter detects events where device is identical to source.	`ArcSight Solutions/CIP/General/`
Direct Connections between Internet and Cardholder Data Environment	This filter identifies successful direct connections between the Internet and the cardholder data environment.	`ArcSight Solutions/CIP/Network Security/`
Domain Name Server in Destination	This filter detects events with Domain Name Server in a destination.	`ArcSight Solutions/CIP/General/`
Domain Name Server in Device	This filter detects events with Domain Name Server in device.	`ArcSight Solutions/CIP/General/`
Domain Name Server in Source	This filter detects events with Domain Name Server in source.	`ArcSight Solutions/CIP/General/`
Empty End Time	This filter detects events with an empty End Time field.	`ArcSight Solutions/CIP/Monitoring/`
Event Limit	This filter limits the events to only the events that are relevant to the solution. This filter is included in the conditions of all other resources in the package, such as rules, queries, and filters, either directly or indirectly. Edit this filter to change the events processed and reported by this solution. See the Solution Guide for more information.	`ArcSight Solutions/CIP/General/`
External Destination	This filter identifies events with an external destination (targeting systems outside the network of your organization).	`ArcSight Solutions/CIP/General/`
External Source	This filter identifies events with an external source (coming from systems outside the network of your organization).	`ArcSight Solutions/CIP/General/`
Failed Logical Access Attempts	This filter detects failed logical access attempts.	`ArcSight Solutions/CIP/Access Control/`
Failed Password Change	This filter identifies unsuccessful password change events.	`ArcSight Solutions/CIP/Access Control/`

Filters Resources, continued

Resource	Description	URI
Failed Physical Access Events	This filter identifies all failed events sent to the ArcSight Manager by physical security systems.	`ArcSight Solutions/CIP/Physical Security/`
File Integrity Tools Events	This filter identifies events from file integrity tools.	`ArcSight Solutions/CIP/Monitoring/`
Firewall Configuration Modifications	Tracks events when the configuration of a firewall is changed.	`ArcSight Solutions/CIP/System Hardening/`
Firewall Events	This filter detects firewall events.	`ArcSight Solutions/CIP/Network Security/`
Heartbleed Vulnerability Detected	This filter detects Heartbleed vulnerability reported by vulnerability scanners.	`ArcSight Solutions/CIP/Vulnerability Management/`
High Risk Vulnerability Detected	This filter detects high and very high risk level flaws reported by vulnerability scanners.	`ArcSight Solutions/CIP/Vulnerability Management/`
Identified User Account in Event	This filter identifies events with a non-empty Source User Name or Destination User Name.	`ArcSight Solutions/CIP/Monitoring/`
Improper Access Control	This filter detects access control flaws reported by vulnerability scanners.	`ArcSight Solutions/CIP/Access Control/`
Improper Error Handling	This filter detects error handling flaws reported by vulnerability scanners.	`ArcSight Solutions/CIP/Vulnerability Management/`
Inactive User Account in Destination	This filter detects events where the Destination User Name is identified as an inactive account.	`ArcSight Solutions/CIP/Access Control/`
Inactive User Account in Source	This filter detects events in which the Source User Name is identified as an inactive account.	`ArcSight Solutions/CIP/Access Control/`
Inbound Cardholder Environment Traffic Allowed by Firewall	This filter identifies all firewall and router accept events that target the cardholder data environment.	`ArcSight Solutions/CIP/Monitoring/`
Information System Failures	This filter identifies information system failures.	`ArcSight Solutions/CIP/Monitoring/`
Injection Flaws	This filter detects injection flaws reported by vulnerability scanners. For example, SQL injection, OS Command Injection, LDAP and XPath injection, and more.	`ArcSight Solutions/CIP/Vulnerability Management/`

Filters Resources, continued

Resource	Description	URI
Insecure Communications	This filter detects insecure communication flaws reported by vulnerability scanners.	`ArcSight Solutions/CIP/Vulnerability Management/`
Insecure Cryptography	This filter detects cryptography flaws reported by vulnerability scanners.	`ArcSight Solutions/CIP/Cryptography/`
Insecure Ports Allowed	This filter detects successful insecure ports access; for example, FTP or Telnet.	`ArcSight Solutions/CIP/System Hardening/`
Insecure Process in Destination	This filter detects insecure processes in an event destination.	`ArcSight Solutions/CIP/System Hardening/`
Insecure Process in Source	This filter detects insecure processes in event source.	`ArcSight Solutions/CIP/System Hardening/`
Insecure Transmission of Cardholder Data Over Public Networks	This filter identifies insecure transmission of sensitive cardholder data over the Internet.	`ArcSight Solutions/CIP/Cryptography/`
Internal Destination	This filter identifies events with an internal destination (targeting the systems inside the network of your organization).	`ArcSight Solutions/CIP/General/`
Internal IP access from Internet into DMZ	This filter identifies events where internal addresses successfully passed from the Internet into the DMZ.	`ArcSight Solutions/CIP/Network Security/`
Internal Source	This filter identifies events with an internal source (coming from the systems inside the network of your organization).	`ArcSight Solutions/CIP/General/`
Login Activity by Inactive User Accounts	This filter identifies login activities by accounts that are in the Inactive Accounts active list.	`ArcSight Solutions/CIP/Access Control/`
Malware Activity	This filter identifies virus and other malware activities reported by either an Intrusion Detection System (IDS) or an anti-virus application.	`ArcSight Solutions/CIP/Vulnerability Management/`
Misconfigurations	This filter detects misconfiguration flaws reported by vulnerability scanners.	`ArcSight Solutions/CIP/Vulnerability Management/`
Multiple Functions Implemented on Destination	This filter identifies destination assets that implement multiple functionality; for example, a database and Web server installed on the same machine.	`ArcSight Solutions/CIP/System Hardening/`
Multiple Functions Implemented on Device	This filter identifies device assets that implement multiple functionality; for example, a database and Web server installed on the same machine.	`ArcSight Solutions/CIP/System Hardening/`

Filters Resources, continued

Resource	Description	URI
Multiple Functions Implemented on Source	This filter identifies source assets that implement multiple functionality; for example, a database and Web server installed on the same machine.	`ArcSight Solutions/CIP/System Hardening/`
NTP Issues	This filter identifies reported alerts related to NTP servers.	`ArcSight Solutions/CIP/Monitoring/`
Network Device Configuration Modifications	Tracks events when the configuration of an infrastructural equipment (router, switch) is changed.	`ArcSight Solutions/CIP/System Hardening/`
Network IDS Configuration Modifications	Tracks events when the configuration of NIDS equipment is changed.	`ArcSight Solutions/CIP/System Hardening/`
Network IDS Events	This filter identifies all events categorized as originating from a network Intrusion Detection System (IDS) or Intrusion Protection System (IPS).	`ArcSight Solutions/CIP/Network Security/`
Network Routing Configuration Modifications	Tracks events when a modification to the routing table of infrastructure equipment (router, switch) is made.	`ArcSight Solutions/CIP/System Hardening/`
New Database Server in Destination	This filter detects new database servers in a destination (database servers that do not belong to the Database category).	`ArcSight Solutions/CIP/General/`
New Database Server in Device	This filter detects new database servers in a device (database servers that do not belong to the Database category).	`ArcSight Solutions/CIP/General/`
New Database Server in Source	This filter detects new database servers in a source (database servers that do not belong to the Database category).	`ArcSight Solutions/CIP/General/`
New Domain Name Server in Destination	This filter detects new Domain Name Servers in a destination (Domain Name Servers that do not belong to the Domain Name Server category).	`ArcSight Solutions/CIP/General/`
New Domain Name Server in Device	This filter detects new Domain Name Servers in device (Domain Name Servers that do not belong to the Domain Name Server category).	`ArcSight Solutions/CIP/General/`
New Domain Name Server in Source	This filter detects new Domain Name Servers in source (Domain Name Servers that do not belong to the Domain Name Server category).	`ArcSight Solutions/CIP/General/`
New Web Server in Destination	This filter detects new Web servers in a destination (Web servers that do not belong to the Web Server category).	`ArcSight Solutions/CIP/General/`
New Web Server in Device	This filter detects new Web servers in device (Web servers that do not belong to the Web Server category).	`ArcSight Solutions/CIP/General/`

Filters Resources, continued

Resource	Description	URI
New Web Server in Source	This filter detects new Web servers in a source (Web servers that do not belong to the Web Server category).	`ArcSight Solutions/CIP/General/`
Non-empty End Time	This filter detects events with a non-empty End Time field.	`ArcSight Solutions/CIP/Monitoring/`
Non-empty Event Source	This filter detects events with a non-empty source.	`ArcSight Solutions/CIP/Monitoring/`
Non Multi Factor Access to CDE by Admin Account	This filter detects events indicating a non multi factor authentication to CDE by admin accounts.	`ArcSight Solutions/CIP/Access Control/`
PCI DSS Ignore	This filter detects assets that should not be reported for PCI DSS compliance. By default, all organizational assets detected by the solution are checked and reported for PCI DSS compliance. A special active list can be used to limit the rule to a specific set of assets; for example, by network zone.	`ArcSight Solutions/CIP/Regulations/PCI DSS/`
Password Change Attempts	This filter identifies password change attempts. By default, the filter only identifies these events on Microsoft Windows systems. Configure this filter to identify password change events from other systems as necessary.	`ArcSight Solutions/CIP/Access Control/`
Password Expired	This filter identifies password expiration events.	`ArcSight Solutions/CIP/Access Control/`
Personal Firewall	This filter identifies events that are reported by a personal firewall.	`ArcSight Solutions/CIP/Network Security/`
Physical Access Events	This filter identifies all events sent to the ArcSight Manager by physical security systems.	`ArcSight Solutions/CIP/Physical Security/`
POODLE Vulnerability Detected	This filter detects POODLE vulnerability reported by vulnerability scanners.	`ArcSight Solutions/CIP/Vulnerability Management/`
Policy Violations	Filter in events with violation of policy.	`ArcSight Solutions/CIP/Monitoring/`
Primary Account Numbers Detected in Clear Text	This filter identifies primary account numbers on the wire as detected by a Network Intrusion Detection System (NIDS). Add custom NIDS signatures to this filter.	`ArcSight Solutions/CIP/Privacy Protection/`
Production Environment in Destination	This filter detects destination assets that belong to the production environment.	`ArcSight Solutions/CIP/General/`
Production Environment in Source	This filter detects source assets that belong to the production environment.	`ArcSight Solutions/CIP/General/`

Filters Resources, continued

Resource	Description	URI
RFC1918 Destination	This filter identifies events with a destination asset that has an IP address within the private IPv4 address space.	`ArcSight Solutions/CIP/General/`
RFC1918 Source	This filter identifies events with a source asset that has an IP address within the private IPv4 address space.	`ArcSight Solutions/CIP/General/`
Security Patch Missing	This filter detects events where vulnerability scanners report a missing security patch.	`ArcSight Solutions/CIP/Vulnerability Management/`
SSL|TLS 1.0 Detected	This filter detects if SSL\TLS 1.0 is supported based on vulnerability scanner events.	`ArcSight Solutions/CIP/Vulnerability Management/`
SSL|TLS Vulnerability Detected	This filter detects ssl flaws reported by vulnerability scanners.	`ArcSight Solutions/CIP/Vulnerability Management/`
Spyware Activity	This filter identifies spyware activity reported by either an Intrusion Detection System (IDS) or an anti-virus application.	`ArcSight Solutions/CIP/Vulnerability Management/`
Success or Failure Indication in Event	This filter detects events with a success or failure indication.	`ArcSight Solutions/CIP/Monitoring/`
Successful Disallowed Ports Access from Wireless into Cardholder Data Environment	This filter identifies successful disallowed port access from a wireless network into the cardholder data environment.	`ArcSight Solutions/CIP/Network Security/`
Successful Disallowed Ports Access in Cardholder Data Environment	This filter identifies all successful connections to disallowed ports within the cardholder data environment (inbound or outbound).	`ArcSight Solutions/CIP/Network Security/`
Successful Login	This filter identifies successful login events.	`ArcSight Solutions/CIP/Access Control/`
Successful Modifications to Operating Systems	Identifies successful configuration modifications to operating systems.	`ArcSight Solutions/CIP/System Hardening/`
Successful Password Change	This filter identifies successful password change events.	`ArcSight Solutions/CIP/Access Control/`
Successful Traffic from Internet into non-DMZ Destination	This filter identifies successful inbound Internet traffic to any destination outside the DMZ segment.	`ArcSight Solutions/CIP/Network Security/`

Filters Resources, continued

Resource	Description	URI
Successful Unauthorized Traffic from Cardholder Data Environment to Internet	This filter identifies unauthorized outbound traffic from the cardholder data environment to the Internet.	`ArcSight Solutions/CIP/Network Security/`
Terminated User Activity in Destination	This filter detects events that identify a former employee account in the event destination.	`ArcSight Solutions/CIP/Access Control/`
Terminated User Activity in Source	This filter detects events that identify a former employee account in the event source.	`ArcSight Solutions/CIP/Access Control/`
TLS BREACH Vulnerabiltiy Detected	This filter detects if TLS BREACH (Browser Reconnaissance and Exfiltration via Adaptive Compression of Hypertext) vulnerability detected.	`ArcSight Solutions/CIP/Vulnerability Management/`
TLS CRIME Vulnerabiltiy Detected	This filter detects if TLS CRIME (Compression Ratio Info-leak Made Easy) vulnerability detected.	`ArcSight Solutions/CIP/Vulnerability Management/`
Traffic between Cardholder Data Environment and Internet	This filter identifies traffic between the cardholder data environment and the Internet.	`ArcSight Solutions/CIP/Network Security/`
Traffic between Cardholder Data and Untrusted Environments	This filter identifies traffic between cardholder data and untrusted environments.	`ArcSight Solutions/CIP/Network Security/`
Unauthorized Access Point Detected	This filter identifies events in which a rogue (unauthorized) or soft access point is detected.	`ArcSight Solutions/CIP/Network Security/`
Unauthorized Access to Cardholder Data	This filter detects unauthorized access to the cardholder data environment.	`ArcSight Solutions/CIP/Access Control/`
Unauthorized Direct Cardholder Database Access	This filter detects unauthorized direct access to a cardholder database. A user is not authorized to access a cardholder database directly unless identified as a database administrator. Populate the Database Administrators active list with the usernames of the database administrators in the organization.	`ArcSight Solutions/CIP/Access Control/`
Unencrypted Non-Console Administrative Access Detected	This filter detects the use of clear-text protocols (HTTP, Telnet) for administrative account access.	`ArcSight Solutions/CIP/System Hardening/`

Filters Resources, continued

Resource	Description	URI
Unnecessary Functionality Detected	This filter detects database servers, Web servers and Domain Name Servers that do not belong to a corresponding asset category and therefore are identified as unnecessary functionality within the organizational network.	`ArcSight Solutions/CIP/System Hardening/`
User Account Expired	This filter detects when an entry ages out of the Active Accounts active list. This happens when an account has been inactive for more than the amount of time specified in the time-to-live of this active list.	`ArcSight Solutions/CIP/Access Control/`
VPN Configuration Modifications	Selects events indicating that a VPN configuration change has occurred.	`ArcSight Solutions/CIP/System Hardening/`
Web Server in Destination	This filter detects events with Web server in the destination.	`ArcSight Solutions/CIP/General/`
Web Server in Device	This filter detects events with Web server in device.	`ArcSight Solutions/CIP/General/`
Web Server in Source	This filter detects events with Web server in the source.	`ArcSight Solutions/CIP/General/`
Windows Events with Machine User in Destination	This filter identifies Microsoft Windows events with destination user names that are standard Windows machine users.	`ArcSight Solutions/CIP/General/`
Windows Events with Machine User in Source	This filter identifies Microsoft Windows events with source user names that are standard Windows machine users.	`ArcSight Solutions/CIP/General/`
Wireless Destination	This filter shows all traffic where the destinations are from a wireless environment.	`ArcSight Solutions/CIP/General/`
Wireless Encryption Violation Detected	This filter identifies events where a wireless Intrusion Detection System (IDS) reports a wireless traffic encryption violation.	`ArcSight Solutions/CIP/Cryptography/`
Wireless Source	This filter shows all traffic where the sources are from a wireless environment.	`ArcSight Solutions/CIP/General/`

Global Variabes

The following table lists all the global variables in Compliance Insight Package for the Payment Card Industry.

Global Variables Resources

Resource	Description	URI
solnGetDestinationID	This variable stores the identifier of the destination asset. If Destination Asset ID is present, it is used as the identifier. Otherwise, hostname is examined: if it is NULL as well, then IP address is used. In addition, Destination Zone Name is added to the variable. The asset identifier is in the following format: <Identifier>|<Zone> Examples: 4k0+XPD4BABCIBa0hWgCdtw==|RFC1918: 10.0.0.0-10.255.255.255 somehostname|RFC1918: 192.168.0.0-192.168.255.255 10.0.0.10|RFC1918: 192.168.0.0-192.168.255.255	`ArcSight Solutions/CIP/`
solnGetDestinationName	This variable stores the name of the destination asset. If Destination Asset Name is present, it is used as the asset name. Otherwise, hostname is examined: if it is NULL as well, then IP address is used.	`ArcSight Solutions/CIP/`
solnGetDeviceID	This variable stores the identifier of the device asset. If Device Asset ID is present, it is used as the identifier. Otherwise, hostname is examined: if it is NULL as well, then IP address is used. In addition, Device Zone Name is added to the variable. The asset identifier is in the following format: <Identifier>|<Zone> Examples: 4k0+XPD4BABCIBa0hWgCdtw==|RFC1918: 10.0.0.0-10.255.255.255 somehostname|RFC1918: 192.168.0.0-192.168.255.255 10.0.0.10|RFC1918: 192.168.0.0-192.168.255.255	`ArcSight Solutions/CIP/`
solnGetDeviceName	This variable stores the name of the device asset. If Device Asset Name is present, it is used as the asset name. Otherwise, hostname is examined: if it is NULL as well, then IP address is used.	`ArcSight Solutions/CIP/`

Global Variables Resources, continued

Resource	Description	URI
solnGetSourceID	This variable stores the identifier of the source asset. If Source Asset ID is present, it is used as the identifier. Otherwise, hostname is examined: if it is NULL as well, then IP address is used. In addition, Source Zone Name is added to the variable. The asset identifier is in the following format: <Identifier>|<Zone> Examples: 4k0+XPD4BABCIBa0hWgCdtw==|RFC1918: 10.0.0.0-10.255.255.255 somehostname|RFC1918: 192.168.0.0-192.168.255.255 10.0.0.10|RFC1918: 192.168.0.0-192.168.255.255	`ArcSight Solutions/CIP/`
solnGetSourceName	This variable stores the name of the source asset. If Source Asset Name is present, it is used as the asset name. Otherwise, hostname is examined: if it is NULL as well, then IP address is used.	`ArcSight Solutions/CIP/`
solnPCI_DSS	This variable stores the following string: PCI DSS.	`ArcSight Solutions/CIP/`

Queries

The following table lists all the queries in Compliance Insight Package for the Payment Card Industry.

Queries Resources

Resource	Description	URI
Account Creations	This query returns account creation events within the last 24 hours.	`ArcSight Solutions/CIP/Access Control/`
Account Deletions	This query returns account deletion events within the last 24 hours.	`ArcSight Solutions/CIP/Access Control/`
Account Lockouts	This query returns information about account lockout events within the last hour.	`ArcSight Solutions/CIP/Access Control/`
Account Modifications	This query returns account modification events within the last 24 hours.	`ArcSight Solutions/CIP/Access Control/`
Activity by Anonymous Users	This query retrieves activities performed by anonymous users within the last hour.	`ArcSight Solutions/CIP/Access Control/`
Activity by Inactive Users	This query retrieves activities performed within the last hour by users that have been categorized as inactive.	`ArcSight Solutions/CIP/Access Control/`

Queries Resources, continued

Resource	Description	URI
Activity by Terminated Users	This query retrieves activities performed within the last hour by users that have been categorized as terminated.	`ArcSight Solutions/CIP/Access Control/`
Administrators Activity	This query shows any activity performed by administrative accounts.	`ArcSight Solutions/CIP/Monitoring/`
After Hours Physical Accesses	This query shows the physical access after business hours. The actual time values are defined in the filter referenced in the Conditions tab.	`ArcSight Solutions/CIP/Physical Security/`
All Password Change Events	This query retrieves password change events within the last 24 hours.	`ArcSight Solutions/CIP/Access Control/`
Anonymous Access to Cardholder Data Environment	This query returns anonymous access to the cardholder data environment within the last 24 hours.	`ArcSight Solutions/CIP/Access Control/`
Anti-Virus Disabled Systems	This query detects when the a system has had its anti-virus software disabled.	`ArcSight Solutions/CIP/Vulnerability Management/`
Anti-Virus Events with High Priority - Detailed	This query provides a detailed listing of anti-virus events (routine maintenance and remediation events) with high priority.	`ArcSight Solutions/CIP/Vulnerability Management/`
Anti-Virus Update Failed	This query detects the number of times that anti-virus software failed to retrieve updates.	`ArcSight Solutions/CIP/Vulnerability Management/`
Anti-Virus Updates	This query returns anti-virus software update events.	`ArcSight Solutions/CIP/Vulnerability Management/`
Anti-Virus Updates by Outcome	This query detects the number of times that anti-virus software attempted to update, grouped by outcome.	`ArcSight Solutions/CIP/Vulnerability Management/`
Anti-Virus Updates by Product	This query detects the number of times that anti-virus software attempted to update, grouped by product and outcome.	`ArcSight Solutions/CIP/Vulnerability Management/`
Application Configuration Modifications	Shows any configuration modifications of any application on operations. Default time window: Last 24 hours.	`ArcSight Solutions/CIP/System Hardening/`
Asset Compliance Score	This query returns compliance scores for a selected asset. The results include all the controls that are supported by the solution. The AssetID parameter identifies assets by ESM resource ID, IP address, or hostname.	`ArcSight Solutions/CIP/General/`

Queries Resources, continued

Resource	Description	URI
Asset Vulnerabilities	This query retrieves the number of vulnerabilities per asset.	`ArcSight Solutions/CIP/Vulnerability Management/`
Asset Vulnerabilities Count	This query retrieves the number of vulnerabilities per asset.	`ArcSight Solutions/CIP/Vulnerability Management/`
Audit Log Cleared	This query shows all events where an audit log is cleared from a host.	`ArcSight Solutions/CIP/Monitoring/`
Bluetooth Protocol Vulnerability Detected	This query retrieves Bluetooth protocol related vulnerabilities.	`ArcSight Solutions/CIP/Vulnerabiltiy Management`
CVSS Score Greater than or Equal to 4	This query retrieves vulnerabilities with a Common Vulnerability Scoring System (CVSS) score greater than or equal to 4.	`ArcSight Solutions/CIP/Vulnerability Management/`
Cardholder Data Environment Inbound Traffic	This query identifies all untrusted systems that are communicating directly with cardholder systems. This traffic must be justified.	`ArcSight Solutions/CIP/Network Security/`
Cardholder Data Environment Outbound Traffic	This query identifies all cardholder systems that are communicating with untrusted systems. This traffic must be justified.	`ArcSight Solutions/CIP/Network Security/`
Compliance Scenario Correlation Events - Trend Base	This query retrieves compliance scenario correlation events and is used by trends to aggregate the information.	`ArcSight Solutions/CIP/General/`
Compliance Scenario Details in the Last 7 Days	This query retrieves all fields from trends about compliance scenarios within the last seven days.	`ArcSight Solutions/CIP/General/`
Configuration Changes - Trend Base	Retrieves all configuration changes for the last hour and used as trend base query for the Configuration Changes trend.	`ArcSight Solutions/CIP/System Hardening/`
Critical Configuration Changes Count	This query retrieves the number of critical configuration changes.	`ArcSight Solutions/CIP/System Hardening/`
Cryptographic Asset Vulnerabilities	This query retrieves the number of cryptographic vulnerabilities per asset.	`ArcSight Solutions/CIP/Vulnerability Management/`
Cryptographic Hash Algorithm Related Vulnerability Detected	This query retrieves cryptographic hash algorithm related vulnerabilities.	`ArcSight Solutions/CIP/Vulnerability Management/`
Cryptographic Public Key Related Vulnerability Detected	This query retrieves cryptographic public key related vulnerabilities.	`ArcSight Solutions/CIP/Vulnerability Management/`

Queries Resources, continued

Resource	Description	URI
Cryptographic Symmetric Key Related Vulnerability Detected	This query retrieves cryptographic symmetric key related vulnerabilities.	`ArcSight Solutions/CIP/Vulnerability Management/`
Cryptographic Vulnerabilities Count	This query retrieves the number of cryptographic vulnerabilities.	`ArcSight Solutions/CIP/Vulnerability Management/`
Cryptographic Weak Protocol Vulnerability Detected	This query retrieves cryptographic weak protocol related vulnerabilities.	`ArcSight Solutions/CIP/Vulnerability Management/`
Custom Accounts	This query retrieves information about the use of development, test, or custom application or user accounts outside the test or development environments.	`ArcSight Solutions/CIP/System Hardening/`
DMZ Assets	This query provides a list of detected assets that belong to the DMZ category.	`ArcSight Solutions/CIP/Network Security/`
DMZ Zones	This query provides a list of detected zones that belong to the DMZ category.	`ArcSight Solutions/CIP/Network Security/`
Database Configuration Modifications	Shows all events of database configuration modifications.	`ArcSight Solutions/CIP/System Hardening/`
Default Vendor Account Used Successfully	This query shows successful default vendor account usage.	`ArcSight Solutions/CIP/System Hardening/`
Direct Connections between Internet and Cardholder Data Environment	This query retrieves successful direct connections between the Internet and the cardholder data environment.	`ArcSight Solutions/CIP/Network Security/`
Failed Logins	This query returns all failed logins of non-machine users grouped by product and day.	`ArcSight Solutions/CIP/Access Control/`
Failed Password Changes	This query retrieves failed password change events, listed in order of end time and destination user name.	`ArcSight Solutions/CIP/Access Control/`
Failed Physical Access Events	This query shows failed attempts of physical access at any time.	`ArcSight Solutions/CIP/Physical Security/`
File Changes	This query returns a summary view of file creations, deletions, and modifications in your environment.	`ArcSight Solutions/CIP/Monitoring/`
Firewall Configuration Modifications	Shows any configuration modifications of any firewall. Default time window: Last 24 hours.	`ArcSight Solutions/CIP/System Hardening/`

Queries Resources, continued

Resource	Description	URI
Firewall Configuration Modifications by Name	Shows the top configuration modifications of any firewall.	`ArcSight Solutions/CIP/System Hardening/`
Heartbleed Vulnerability Detected	This query retrieves Heartbleed related vulnerabilities.	`ArcSight Solutions/CIP/Vulnerability Management/`
High Risk Vulnerability Detected	This query provides high and very high risk level flaws reported by vulnerability scanners.	`ArcSight Solutions/CIP/Vulnerability Management/`
Inactive User Accounts	This query shows all user names that are in the Inactive Accounts active list.	`ArcSight Solutions/CIP/Access Control/`
Information System Failures	This query retrieves the number of information failures per asset	`ArcSight Solutions/CIP/Monitoring/`
Information System Failures Assets	This query retrieves the number of information failures per asset	`ArcSight Solutions/CIP/Monitoring/`
Insecure Cryptography	This query finds cryptography flaws reported by vulnerability scanners.	`ArcSight Solutions/CIP/Cryptography/`
Insecure Ports Allowed	This query retrieves successful insecure port access; for example, FTP or Telnet.	`ArcSight Solutions/CIP/System Hardening/`
Insecure Ports Allowed Count by Product	This query retrieves a count of unique ports per product.	`ArcSight Solutions/CIP/System Hardening/`
Insecure Processes	This query shows insecure process events.	`ArcSight Solutions/CIP/System Hardening/`
Login Activity by Inactive User Accounts	This query shows inactive user accounts from which login activity was attempted.	`ArcSight Solutions/CIP/Access Control/`
Negative Impact Compliance Scenarios in the Last 7 Days	This query retrieves information from trends about negative impact compliance scenarios within the last seven days.	`ArcSight Solutions/CIP/General/`
Negative Impact Compliance Scenarios per Day	This query retrieves information from trends about negative impact compliance scenarios per day within the last seven days.	`ArcSight Solutions/CIP/General/`
Network Device Configuration Modifications	Shows all network device configuration changes.	`ArcSight Solutions/CIP/System Hardening/`
Non Multi Factor Access to CDE by Admin Accounts	This query retrieves events indicating a non multi factor authentication to CDE by admin accounts.	`ArcSight Solutions/CIP/Access Control/`
Open Ports by Device	This query identifies all ports that were passed by a firewall, as well as the rule number that it triggered.	`ArcSight Solutions/CIP/Monitoring/`

Queries Resources, continued

Resource	Description	URI
PCI DSS Compliance Score Sum	This query returns PCI DSS compliance and non-compliance score summation for all control-asset pairs in the system. This data is used to build the top level compliance and non-compliance status reports for the PCI DSS regulation.	`ArcSight Solutions/CIP/Regulations/PCI DSS/`
PCI DSS Compliance Status: Asset-Control	This query returns asset compliance scores for PCI DSS controls.	`ArcSight Solutions/CIP/Regulations/PCI DSS/`
PCI DSS Compliance Status: Control	This query returns the number of compliant and non-compliant assets for PCI DSS controls.	`ArcSight Solutions/CIP/Regulations/PCI DSS/`
PCI DSS Maximal Asset Compliance Score	This query returns the maximum potential PCI DSS compliance score for a single asset.	`ArcSight Solutions/CIP/Regulations/PCI DSS/`
PCI DSS Maximal Asset Compliance Score: Requirement	This query returns the maximum potential PCI DSS compliance score for a single asset, for each PCI DSS requirement.	`ArcSight Solutions/CIP/Regulations/PCI DSS/`
PCI DSS Maximal Asset Non-Compliance Score	This query returns the maximum potential PCI DSS non-compliance score for a single asset.	`ArcSight Solutions/CIP/Regulations/PCI DSS/`
PCI DSS Maximal Asset Non-Compliance Score: Requirement	This query returns the maximum potential PCI DSS non-compliance score for a single asset, for each PCI DSS requirement.	`ArcSight Solutions/CIP/Regulations/PCI DSS/`
PCI DSS Non-Compliant Assets	This query returns the list of assets that are non-compliant with PCI DSS controls. For every asset, the number of non-compliant PCI DSS controls is returned.	`ArcSight Solutions/CIP/Regulations/PCI DSS/`
PCI DSS Non-Compliant Controls	This query returns a list of non-compliant PCI DSS controls. For every control, the number of non-compliant assets is returned.	`ArcSight Solutions/CIP/Regulations/PCI DSS/`
PCI DSS Number of Assets	This query returns the number of assets for the PCI DSS regulation. This number includes all assets that were reported as compliant or non-compliant for at least one PCI DSS control.	`ArcSight Solutions/CIP/Regulations/PCI DSS/`
PCI DSS Score: Compliance	This query returns the overall compliance score for PCI DSS compliance in the organization. In addition, the difference between the maximum potential compliance score and the actual overall compliance score is returned.	`ArcSight Solutions/CIP/Regulations/PCI DSS/`

Queries Resources, continued

Resource	Description	URI
PCI DSS Score: Non-Compliance	This query returns the overall non-compliance score for PCI DSS compliance in the organization. In addition, the difference between the maximum potential non-compliance score and the actual overall non-compliance score is returned.	`ArcSight Solutions/CIP/Regulations/PCI DSS/`
PCI DSS Score: Requirements	This query returns compliance and non-compliance score summation per PCI DSS requirement.	`ArcSight Solutions/CIP/Regulations/PCI DSS/`
Password Expired - Trend Base	This query lists accounts for which the password was not changed for longer than the policy standard permits.	`ArcSight Solutions/CIP/Access Control/`
Policy Violation Assets	This query retrieves the number of policy violations per asset.	`ArcSight Solutions/CIP/Monitoring/`
Policy Violations	Provides a listing of events categorized by ArcSight as policy violations which target the various Network Domains by Asset. This query may (and should) be focused based on the Network Domain of interest.	`ArcSight Solutions/CIP/Monitoring/`
POODLE Vulnerability Detected	This query retrieves Poodle vulnerabilities.	`ArcSight Solutions/CIP/Vulnerability Management/`
Positive Impact Compliance Scenarios in the Last 7 Days	This query retrieves information from trends about positive impact compliance scenarios within the last seven days.	`ArcSight Solutions/CIP/General/`
Positive Impact Compliance Scenarios per Day	This query retrieves information from trends about positive impact compliance scenarios per day within the last seven days.	`ArcSight Solutions/CIP/General/`
Primary Account Numbers Detected in Clear Text	This query identifies Network Intrusion Detection System (NIDS) signatures that detected primary account numbers in clear text on the wire.	`ArcSight Solutions/CIP/Privacy Protection/`
Servers with Unnecessary Functionality: Database Servers	This query retrieves a list of new database servers (database servers that do not belong to the Database category) based on the Database Servers active list.	`ArcSight Solutions/CIP/System Hardening/`
Servers with Unnecessary Functionality: Domain Name Servers	This query retrieves a list of new Domain Name Servers (Domain Name Servers that do not belong to the Domain Name Server category) based on Domain Name Server active list.	`ArcSight Solutions/CIP/System Hardening/`

Queries Resources, continued

Resource	Description	URI
Servers with Unnecessary Functionality: Web Servers	This query retrieves a list of new Web servers (Web servers that do not belong to the Web Server category) based on the Web Servers active list.	`ArcSight Solutions/CIP/System Hardening/`
SSL|TLS 1.0 Detected	This query retrieves if SSL\TLS 1.0 is supported based on vulnerability scanner events.	`ArcSight Solutions/CIP/Vulnerability Management/`
SSL|TLS Vulnerability Detected	This query retrieves SSL and TLS flaws reported by vulnerability scanners.	`ArcSight Solutions/CIP/Vulnerability Management/`
Successful Disallowed Ports Access from Wireless into Cardholder Data Environment	This query retrieves successful events with disallowed port access from a wireless network into the cardholder data environment.	`ArcSight Solutions/CIP/Network Security/`
Successful Disallowed Ports Access in Cardholder Data Environment	This query retrieves all successful connection events to disallowed ports within the cardholder data environment (inbound or outbound).	`ArcSight Solutions/CIP/Network Security/`
Successful Password Changes	This query lists successful password change events, listed in order of end time and destination user name.	`ArcSight Solutions/CIP/Access Control/`
Successful Traffic from Internet into non-DMZ Destination	This query retrieves successful inbound Internet traffic events to any destination outside the DMZ segment.	`ArcSight Solutions/CIP/Network Security/`
Time Consistency Issues	This query displays all events in which there are clock synchronization issues between the deviceReceiptTime and agentTime, or the event endTime and managerReceiptTime.	`ArcSight Solutions/CIP/Monitoring/`
TLS BREACH Vulnerability Detected	This query retrieves TLS BREACH (Browser Reconnaissance and Exfiltration via Adaptive Compression of Hypertext) flaws reported by vulnerability scanners.	`ArcSight Solutions/CIP/Vulnerability Management/`
TLS CRIME Vulnerabiltiy Detected	This query retrieves TLS CRIME (Compression Ratio Info-leak Made Easy) flaws reported by vulnerability scanners.	`ArcSight Solutions/CIP/Vulnerability Management/`
Top 10 Admin Users with Non Multi Factor Access to CDE	This query retrieves the top 10 admin users with non multi factor admin accesses.	`ArcSight Solutions/CIP/Access Control/`
Top 10 CDE Assets with Non Multi Factor Admin Accesseses	This query retrieves the top 10 assets with non multi factor admin accesses.	`ArcSight Solutions/CIP/Access Control/`
Top 10 File Changes	This query returns top 10 files changed within the last 24 hours.	`ArcSight Solutions/CIP/Monitoring/`

Queries Resources, continued

Resource	Description	URI
Top 10 Hosts with Most Unsuccessful Administrative Logins	This query returns the top 10 hosts with the most unsuccessful login attempts within the last two hours. This query can (and should) be focused based on the network domain of interest.	`ArcSight Solutions/CIP/Monitoring/`
Top 10 Products with Failed Logical Access Attempts	This query retrieves the top 10 products with failed logical access attempts.	`ArcSight Solutions/CIP/Access Control/`
Top 20 Assets with Failed Logical Access Attempts	This query retrieves the top 20 assets with failed logical access attempts.	`ArcSight Solutions/CIP/Access Control/`
Top 20 Insecure Transmission of Cardholder Data Over Public Networks	This query viewer finds the top 20 suspicious communication between cardholder systems and public systems. Suspicious is defined as protocols that are typically unencrypted.	`ArcSight Solutions/CIP/Cryptography/`
Top Firewalls with Most Successful Configuration Modifications	Shows the top firewalls with most successful configuration modifications.	`ArcSight Solutions/CIP/System Hardening/`
Top Hosts with Most Malware Activities	This query finds the top 10 systems with the most malware activities (routine maintenance and remediation events).	`ArcSight Solutions/CIP/Vulnerability Management/`
Top Hosts with Most Spyware Activities	This query finds the top 10 systems with most spyware activities (routine maintenance and remediation events).	`ArcSight Solutions/CIP/Vulnerability Management/`
Top Internal Hosts Accessed Disallowed Ports	This query returns the top internal hosts that accessed the most disallowed ports.	`ArcSight Solutions/CIP/Network Security/`
Top Internal Hosts Provided Disallowed Ports	This query returns the top internal hosts that provided the most disallowed ports.	`ArcSight Solutions/CIP/Network Security/`
Top Malware Instances	This query provides the names of the top 10 detected malware instances.	`ArcSight Solutions/CIP/Vulnerability Management/`
Top Policy Violators	This query retrieves the top 10 policy violators.	`ArcSight Solutions/CIP/Monitoring/`
Top Spyware Instances	This query provides the names of the top 10 detected spyware instances.	`ArcSight Solutions/CIP/Vulnerability Management/`
Top Successful Disallowed Ports Access in Cardholder Data Environment	This query identifies the top disallowed port access in cardholder data environment.	`ArcSight Solutions/CIP/Network Security/`
Top Users with Most Successful Firewall Modifications	Shows the top users who made most successful configuration modifications.	`ArcSight Solutions/CIP/System Hardening/`

Queries Resources, continued

Resource	Description	URI
Unauthorized Access to Cardholder Data	This query shows details about access to cardholder data systems by unauthorized users.	`ArcSight Solutions/CIP/Access Control/`
Unauthorized Direct Cardholder Database Access	This query retrieves unauthorized direct access to a cardholder database. A user is not authorized to access a cardholder database directly unless identified as a database administrator. Populate the Database Administrators active list with the usernames of the database administrators in the organization.	`ArcSight Solutions/CIP/Access Control/`
User Accounts with Expired Passwords	This query returns user accounts with expired passwords, where password expiration events occurred within the last four weeks.	`ArcSight Solutions/CIP/Access Control/`
Vulnerabilities Count	This query retrieves the number of vulnerabilities.	`ArcSight Solutions/CIP/Vulnerability Management/`
Weekly Trend - Configuration Changes by Address	Shows the top configuration modifications by IP address.	`ArcSight Solutions/CIP/System Hardening/`
Weekly Trend - Configuration Changes by Event Name	Shows the top configuration modifications by event name.	`ArcSight Solutions/CIP/System Hardening/`
Weekly Trend - Configuration Changes by User	Shows the top configuration modifications by user.	`ArcSight Solutions/CIP/System Hardening/`

Query Viewers

The following table lists all the query viewers in Compliance Insight Package for the Payment Card Industry.

Query Viewers Resources

Resource	Description	URI
Account Lockouts	This query viewer shows all account lockout events within the last hour. For more focused results, you can drill down on either the host address or the user name.	`ArcSight Solutions/CIP/Access Control/`
Activity by Anonymous Users	This query viewer shows any activity performed by anonymous users.	`ArcSight Solutions/CIP/Access Control/`
Activity by Inactive Users	This query viewer shows any activity performed by users who are known to have been inactive.	`ArcSight Solutions/CIP/Access Control/`

Query Viewers Resources, continued

Resource	Description	URI
Activity by Terminated Users	This query viewer shows any activity performed by users who are known to have been terminated.	`ArcSight Solutions/CIP/Access Control/`
Administrators Activity	This query viewer shows any activity performed by administrative accounts.	`ArcSight Solutions/CIP/Monitoring/`
After Hours Physical Accesses	This query viewer shows the physical access of a building after business hours.	`ArcSight Solutions/CIP/Physical Security/`
All Password Change Events	This query viewer displays a list of all password change events and their outcome.	`ArcSight Solutions/CIP/Access Control/`
Anti-Virus Updates	This query viewer shows anti-virus software update events.	`ArcSight Solutions/CIP/Vulnerability Management/`
Anti-Virus Updates by Outcome	This query viewer detects the number of times that anti-virus software attempted to update, grouped by outcome.	`ArcSight Solutions/CIP/Vulnerability Management/`
Anti-Virus Updates by Product	This query detects the number of times that anti-virus software attempted to update, grouped by product and outcome.	`ArcSight Solutions/CIP/Vulnerability Management/`
Asset Vulnerabilities	This query viewer shows the number of vulnerabilities per asset. This query viewer uses global variables with 11 filters to detect the type of vulnerability.	`ArcSight Solutions/CIP/Vulnerability Management/`
Asset Vulnerabilities Count	This query viewer displays the number of vulnerabilities per asset.	`ArcSight Solutions/CIP/Vulnerability Management/`
Audit Log Cleared	This query viewer shows all events where an audit log is cleared from a host.	`ArcSight Solutions/CIP/Monitoring/`
Cardholder Data Environment Inbound Traffic	This query viewer shows all untrusted systems that are communicating directly with cardholder systems. This traffic must be justified.	`ArcSight Solutions/CIP/Network Security/`
Cardholder Data Environment Outbound Traffic	This query viewer shows all communication from cardholder systems to untrusted systems. This traffic must be justified.	`ArcSight Solutions/CIP/Network Security/`
CDE Assets with Non Multi Factor Admin Accesses	This Query Viewer shows the number of Non Multi Factor Admin Accesses per asset.	`ArcSight Solutions/CIP/Access Control/`
Compliance Scenario Details	This query viewer displays all fields from trends about compliance scenarios within the last seven days.	`ArcSight Solutions/CIP/General/`

Query Viewers Resources, continued

Resource	Description	URI
Critical Configuration Changes Count	This query viewer displays the number of critical configuration changes.	`ArcSight Solutions/CIP/System Hardening/`
Cryptographic Asset Vulnerabilities	This query viewer shows cryptographic vulnerabilities per asset.	`ArcSight Solutions/CIP/Vulnerability Management/`
Cryptographic Vulnerabilities Count	This query viewer displays the number of cryptographic vulnerabilities.	`ArcSight Solutions/CIP/Vulnerability Management/`
Default Vendor Account Used Successfully	This query viewer shows successful default vendor account usage events.	`ArcSight Solutions/CIP/System Hardening/`
Direct Connections between Internet and Cardholder Data Environment	This query viewer displays successful direct connections between the Internet and the cardholder data environment.	`ArcSight Solutions/CIP/Network Security/`
Failed Password Changes	This query viewer displays failed password change events, listed in order of end time.	`ArcSight Solutions/CIP/Access Control/`
File Changes	This query viewer shows the summary view of file creations, deletions, and modifications in your environment.	`ArcSight Solutions/CIP/Monitoring/`
Information System Failures Assets	This Query Viewer shows the number of information system failures per asset.	`ArcSight Solutions/CIP/Monitoring/`
Insecure Cryptography	This query viewer displays cryptography flaws reported by vulnerability scanners.	`ArcSight Solutions/CIP/Cryptography/`
Insecure Ports Allowed	This query viewer displays events with insecure ports allowed.	`ArcSight Solutions/CIP/System Hardening/`
Insecure Ports Allowed Count by Product	This query retrieves events with insecure ports allowed.	`ArcSight Solutions/CIP/System Hardening/`
Insecure Processes	This query viewer shows events with insecure processes.	`ArcSight Solutions/CIP/System Hardening/`
Negative Impact Compliance Scenarios in the Last 7 Days	This query viewer displays information about negative impact compliance scenarios from trends within the last seven days.	`ArcSight Solutions/CIP/General/`

Query Viewers Resources, continued

Resource	Description	URI
Negative Impact Compliance Scenarios per Day	This query viewer displays information from trends about negative impact compliance scenarios per day within the last seven days.	`ArcSight Solutions/CIP/General/`
PCI DSS Compliance Status: Asset-Control	This query viewer shows control-asset compliance status for PCI DSS controls.	`ArcSight Solutions/CIP/Regulations/PCI DSS/`
PCI DSS Compliance Status: Control	This query viewer shows the following information for every supported PCI DSS control: *The percentage and actual number of assets that are compliant with this control. *The percentage and actual number of assets that are non-compliant with this control. * The total number of PCI DSS assets If the displayed percentages are empty or exceed the allowed range (0-100), run the PCI DSS Number of Assets trend.	`ArcSight Solutions/CIP/Regulations/PCI DSS/`
PCI DSS Score: Compliance	This query viewer shows the overall compliance score for PCI DSS compliance in the organization. In addition, the difference between the maximum potential compliance score and the actual overall compliance score is displayed (No Information).	`ArcSight Solutions/CIP/Regulations/PCI DSS/`
PCI DSS Score: Non-Compliance	This query viewer shows the overall non-compliance score for PCI DSS compliance in the organization. In addition, the difference between the maximum potential non-compliance score and the actual overall non-compliance score is displayed (No Information).	`ArcSight Solutions/CIP/Regulations/PCI DSS/`
PCI DSS Score: Requirements	This query viewer shows the overall compliance and non-compliance scores for every PCI DSS Requirement.	`ArcSight Solutions/CIP/Regulations/PCI DSS/`
PCI DSS Top 10 Non-Compliant Controls	This query viewer shows the top 10 non-compliant PCI DSS controls with the highest number of non-compliant assets.	`ArcSight Solutions/CIP/Regulations/PCI DSS/`
PCI DSS Top 50 Non-Compliant Assets	This query viewer shows top 50 assets with the highest number of non-compliant PCI DSS controls.	`ArcSight Solutions/CIP/Regulations/PCI DSS/`
Policy Violation Assets	This QueryViewer shows the number of policy violations per asset.	`ArcSight Solutions/CIP/Monitoring/`

Query Viewers Resources, continued

Resource	Description	URI
Positive Impact Compliance Scenarios in the Last 7 Days	This query viewer displays information about positive impact compliance scenarios from trends within the last seven days.	`ArcSight Solutions/CIP/General/`
Positive Impact Compliance Scenarios per Day	This query viewer displays information from trends about positive impact compliance scenarios per day within the last seven days.	`ArcSight Solutions/CIP/General/`
Primary Account Numbers Detected in Clear Text	This query viewer shows Network Intrusion Detection System (NIDS) signatures that detected primary account numbers in clear text on the wire.	`ArcSight Solutions/CIP/Privacy Protection/`
Servers with Unnecessary Functionality: Database Servers	This query viewer displays a list of new database servers (database servers that do not belong to the Database category) based on the Database Servers active list.	`ArcSight Solutions/CIP/System Hardening/`
Servers with Unnecessary Functionality: Domain Name Servers	This query viewer displays a list of new Domain Name Servers (Domain Name Servers that do not belong to the Domain Name Server category) based on the Domain Name Server active list.	`ArcSight Solutions/CIP/System Hardening/`
Servers with Unnecessary Functionality: Web Servers	This query viewer displays a list of new Web servers (Web servers that do not belong to the Web Server category) based on the Web Servers active list.	`ArcSight Solutions/CIP/System Hardening/`
Successful Disallowed Ports Access from Wireless into Cardholder Data Environment	This query viewer displays successful events of disallowed port access from a wireless network into the cardholder data environment.	`ArcSight Solutions/CIP/Network Security/`
Successful Disallowed Ports Access in Cardholder Data Environment	This query viewer displays all successful connection events to disallowed ports within the cardholder data environment (inbound or outbound).	`ArcSight Solutions/CIP/Network Security/`
Successful Traffic from Internet into non-DMZ Destination	This query viewer displays successful inbound Internet traffic events to any destination outside the DMZ segment.	`ArcSight Solutions/CIP/Network Security/`

Query Viewers Resources, continued

Resource	Description	URI
Top 10 Admin Users with Non Multi Factor Accesses to CDE	This query viewer displays the top 10 Admin Users with Non Multi Factor Accesses to CDE.	`ArcSight Solutions/CIP/Access Control/`
Top 10 File Changes	This query viewer displays the top 10 files changed within the last 24 hours.	`ArcSight Solutions/CIP/Monitoring/`
Top 10 Hosts with Most Unsuccessful Administrative Logins	This query viewer shows the top 10 hosts with the most unsuccessful administrative logins.	`ArcSight Solutions/CIP/Monitoring/`
Top 10 Policy Violators	This Query Viewer shows the top 10 policy violators.	`ArcSight Solutions/CIP/Monitoring/`
Top 10 Products with Failed Logical Access Attempts	This query viewer displays the top 10 products with failed logical access attempts.	`ArcSight Solutions/CIP/Access Control/`
Top 20 Insecure Transmission of Cardholder Data Over Public Networks	This query viewer displays the top 20 suspicious communication between cardholder systems and public systems. Suspicious is defined as protocols that are typically unencrypted.	`ArcSight Solutions/CIP/Cryptography/`
Top 20 Products with Failed Logical Access Attempts	This query viewer shows the top 20 products with failed logical access attempts.	`ArcSight Solutions/CIP/Access Control/`
Unauthorized Access to Cardholder Data	This query viewer shows details about access to cardholder data systems by unauthorized users.	`ArcSight Solutions/CIP/Access Control/`
Unauthorized Direct Cardholder Database Access	This query viewer displays unauthorized direct access to a cardholder database. A user is not authorized to access a cardholder database directly unless identified as a database administrator. Populate the Database Administrators active list with the usernames of the database administrators in the organization.	`ArcSight Solutions/CIP/Access Control/`
User Accounts with Expired Passwords	This query viewer displays accounts for which the password was not changed for longer than the policy standard permits.	`ArcSight Solutions/CIP/Access Control/`
Vulnerabilities Count	This query viewer displays the number of vulnerabilities.	`ArcSight Solutions/CIP/Vulnerability Management/`

Reports

The following table lists all the reports in Compliance Insight Package for the Payment Card Industry.

Reports Resources

Resource	Description	URI
Account Creations	This report shows all account creations.	`ArcSight Solutions/CIP/Access Control/`
Account Deletions	This report shows all account deletions.	`ArcSight Solutions/CIP/Access Control/`
Account Modifications	This report shows all account modifications.	`ArcSight Solutions/CIP/Access Control/`
Activity by Anonymous Users	This report shows any activity performed by anonymous users.	`ArcSight Solutions/CIP/Access Control/`
Activity by Terminated Users	This report shows any activity performed by users who are known to have been terminated.	`ArcSight Solutions/CIP/Access Control/`
Administrators Activity	This report shows any activity performed by administrative accounts.	`ArcSight Solutions/CIP/Monitoring/`
After Hours Physical Accesses	This report shows the physical access of a building after business hours.	`ArcSight Solutions/CIP/Physical Security/`
All Password Change Events	This report provides a list of all password change events, listed in order of the time that they occurred.	`ArcSight Solutions/CIP/Access Control/`
Anonymous Access to Cardholder Data Environment	This report shows all anonymous access to the cardholder data environment.	`ArcSight Solutions/CIP/Access Control/`
Anti-Virus Disabled Systems	This report shows all incidents when the anti-virus software is disabled.	`ArcSight Solutions/CIP/Vulnerability Management/`
Anti-Virus Report - Detailed	This report shows a detailed listing of anti-virus events (routine maintenance and remediation events) with high priority.	`ArcSight Solutions/CIP/Vulnerability Management/`
Anti-Virus Update Failed	This report shows the number of times that anti-virus software failed to retrieve updates.	`ArcSight Solutions/CIP/Vulnerability Management/`

Reports Resources, continued

Resource	Description	URI
Anti-Virus Updates	This report shows anti-virus software update events.	`ArcSight Solutions/CIP/Vulnerability Management/`
Application Configuration Modifications	Shows any configuration modifications of any application on a system on operations. Default time window: Last 24 hours.	`ArcSight Solutions/CIP/System Hardening/`
Asset Compliance Score	This report shows compliance scores for a selected asset. The results include all the controls that are supported by the solution. The AssetID parameter identifies the asset by ESM resource ID, IP address, or host name.	`ArcSight Solutions/CIP/General/`
Audit Log Cleared	This report shows all events where an audit log is cleared from a host.	`ArcSight Solutions/CIP/Monitoring/`
Bluetooth Protocol Vulnerability Detected	This report displays Bluetooth protocol related flaws reported by vulnerability scanners.	`ArcSight Solutions/CIP/Vulnerability Management`
Cryptographic Hash Algorithm Related Vulnerability Detected	This report displays cryptographic hash algorithm related flaws reported by vulnerability scanners.	`ArcSight Solutions/CIP/Vulnerability Management/`
Cryptographic Public Key Related Vulnerability Detected	This report displays cryptographic public key related flaws reported by vulnerability scanners.	`ArcSight Solutions/CIP/Vulnerability Management/`
Cryptographic Symmetric Key Related Vulnerability Detected	This report displays cryptographic symmetric key related flaws reported by vulnerability scanners.	`ArcSight Solutions/CIP/Vulnerability Management/`
Cryptographic Weak Protocol Vulnerability Detected	This report displays cryptographic weak protocol related flaws reported by vulnerability scanners.	`ArcSight Solutions/CIP/Vulnerability Management/`
CVSS Score Greater than or Equal to 4	This report displays vulnerabilities with a Common Vulnerability Scoring System (CVSS) score greater than or equal to 4.	`ArcSight Solutions/CIP/Vulnerability Management/`
Custom Accounts	This report displays information about the use of development, test, or custom applications or user accounts outside of the test or development environments.	`ArcSight Solutions/CIP/System Hardening/`

Reports Resources, continued

Resource	Description	URI
Database Configuration Modifications	Shows database configuration changes.	`ArcSight Solutions/CIP/System Hardening/`
Default Vendor Account Used Successfully	This report displays successful default vendor account usage.	`ArcSight Solutions/CIP/System Hardening/`
Failed Logins	This report provides a listing of all failed logins of non-machine users grouped by product and day.	`ArcSight Solutions/CIP/Access Control/`
Failed Password Changes	This report displays failed password change events.	`ArcSight Solutions/CIP/Access Control/`
Failed Physical Access Events	This report shows failed attempts to enter a building.	`ArcSight Solutions/CIP/Physical Security/`
Firewall Configuration Modification Summary	Shows several top-level views related to firewall configuration modifications.	`ArcSight Solutions/CIP/System Hardening/`
Firewall Configuration Modifications	Shows any configuration modifications of any firewall.	`ArcSight Solutions/CIP/System Hardening/`
Heartbleed Vulnerability Detected	This report displays heartbleed related flaws reported by vulnerability scanners.	`ArcSight Solutions/CIP/Vulnerability Management/`
High Risk Vulnerability Detected	This report displays high and very high risk level flaws reported by vulnerability scanners.	`ArcSight Solutions/CIP/Vulnerability Management/`
Inactive User Account Detected	This report shows all user names that are in the Inactive Accounts active list.	`ArcSight Solutions/CIP/Access Control/`
Information System Failures	This report shows all information system failure events.	`ArcSight Solutions/CIP/Monitoring/`
Insecure Cryptography	This report shows cryptography flaws reported by vulnerability scanners.	`ArcSight Solutions/CIP/Cryptography/`
Insecure Ports Allowed	This report displays successful insecure port access; for example, FTP or Telnet.	`ArcSight Solutions/CIP/System Hardening/`
Insecure Processes	This report displays events with insecure processes.	`ArcSight Solutions/CIP/System Hardening/`

Reports Resources, continued

Resource	Description	URI
Login Activity by Inactive Users	This report shows login activity by users who are in the Inactive Accounts active list. The information in the report is in order of the outcome of the login event.	`ArcSight Solutions/CIP/Access Control/`
Malware Activities	This report shows an overview of malware activities (including remediation).	`ArcSight Solutions/CIP/Vulnerability Management/`
Network Device Configuration Modifications	Shows network device configuration changes.	`ArcSight Solutions/CIP/System Hardening/`
Non Multi Factor Access to CDE by Admin Accounts	This report shows events indicating a non multi factor authentication to CDE by admin accounts.	`ArcSight Solutions/CIP/Access Control/`
Open Ports by Device	This report shows all ports that were passed by a firewall, as well as the rule number that it triggered.	`ArcSight Solutions/CIP/Monitoring/`
PCI DSS Compliance Score: Asset-Control	This report shows asset compliance scores for the PCI DSS. The compliance is reported per control, per asset, in the following format: 1 - compliant, 0 - non-compliant.	`ArcSight Solutions/CIP/Regulations/PCI DSS/`
Password Expired	This report lists passwords that were not changed for longer than the policy standard.	`ArcSight Solutions/CIP/Access Control/`
Policy Violations	Provides a listing of events categorized by ArcSight as policy violations.	`ArcSight Solutions/CIP/Monitoring/`
Poodle Vulnerability Detected	This report displays poodle related flaws reported by vulnerability scanners.	`ArcSight Solutions/CIP/Vulnerability Management/`
Primary Account Numbers Detected in Clear Text	This report shows Network Intrusion Detection System (NIDS) signatures that detected primary account numbers in clear text on the wire.	`ArcSight Solutions/CIP/Privacy Protection/`
Spyware Activities	This report shows an overview of spyware activities.	`ArcSight Solutions/CIP/Vulnerability Management/`
SSL|TLS 1.0 Detected	This report displays if SSL\TLS 1.0 is supported based on vulnerability scanner events.	`ArcSight Solutions/CIP/Vulnerability Management/`
SSL|TLS Vulnerability Detected	This report displays SSL and TLS flaws reported by vulnerability scanners.	`ArcSight Solutions/CIP/Vulnerability Management/`

Reports Resources, continued

Resource	Description	URI
Successful Disallowed Ports Access	This report shows successful disallowed port access in the cardholder data environment and successful disallowed port access from a wireless network into the cardholder data environment.	`ArcSight Solutions/CIP/Network Security/`
Successful Password Changes	This report displays successful password change events.	`ArcSight Solutions/CIP/Access Control/`
Time Consistency Issues	This report displays all events in which there are clock synchronization issues between the deviceReceiptTime and agentTime, or the event endTime and managerReceiptTime. The report displays the connector (agent) information first and then the device information.	`ArcSight Solutions/CIP/Monitoring/`
TLS BREACH Vulnerability Detected	This report retrieves TLS BREACH (Browser Reconnaissance and Exfiltration via Adaptive Compression of Hypertext) flaws reported by vulnerability scanners.	`ArcSight Solutions/CIP/Vulnerability Management/`
TLS CRIME Vulnerability Detected	This report retrieves TLS CRIME (Compression Ratio Info-leak Made Easy) flaws reported by vulnerability scanners.	`ArcSight Solutions/CIP/Vulnerability Management/`
Top 20 Insecure Transmission of Cardholder Data Over Public Networks	This report shows the top 20 suspicious communications between cardholder systems and public systems. Suspicious is defined as protocols that are typically unencrypted.	`ArcSight Solutions/CIP/Cryptography/`
Weekly Trend - Configuration Modification Summary	Shows several top-level views related to configuration modifications.	`ArcSight Solutions/CIP/System Hardening/`

Rules

The following table lists all the rules in Compliance Insight Package for the Payment Card Industry.

Rules Resources

Resource	Description	URI
Accesses to Cardholder Data Environment by Identified Users	This rule detects access to the cardholder data environment by an identified user.	`ArcSight Solutions/CIP/Compliance Scenarios/Monitoring/`
Account Deletion	This rule detects account deletion events. When triggered, the rule adds and deletes users from the appropriate active lists.	`ArcSight Solutions/CIP/General/`
Account Lockouts	This rule detects account lockouts. If both source and destination assets are empty, the username is reported as asset.	`ArcSight Solutions/CIP/Compliance Scenarios/Access Control/`
Anonymous User Activity	This rule triggers when events are detected in which source or destination users cannot be attributed to an individual user.	`ArcSight Solutions/CIP/Compliance Scenarios/Access Control/`
Anti-Virus Detected	This rule detects any events reported by anti-virus products in your environment.	`ArcSight Solutions/CIP/Compliance Scenarios/Vulnerability Management/`
Anti-Virus Status: Running or Disabled	This rule triggers when any anti-virus activity is detected or when an anti-virus is disabled. In the latter case, the impact of the rule is negative, otherwise, the impact is positive.	`ArcSight Solutions/CIP/Compliance Scenarios/Vulnerability Management/`
Anti-Virus Status: Updates or Scans	This rule triggers when an anti-virus update or scan success or failure is detected, or when an anti-virus is disabled.	`ArcSight Solutions/CIP/Compliance Scenarios/Vulnerability Management/`
Audit Log Cleared	This rule triggers when an audit log is cleared from a host.	`ArcSight Solutions/CIP/Compliance Scenarios/Monitoring/`
Bluetooth Protocol Vulnerability	This rule detects Bluetooth flaws reported by vulnerability scanners.	`ArcSight Solutions/CIP/Compliance Scenarios/Vulnerability Management`

Rules Resources, continued

Resource	Description	URI
Broken Authentication and Session Management	This rule detects authentication and session management flaws reported by vulnerability scanners.	`ArcSight Solutions/CIP/Compliance Scenarios/Vulnerability Management/`
Buffer Overflows	This rule triggers when buffer overflow flaws are detected by vulnerability scanners.	`ArcSight Solutions/CIP/Compliance Scenarios/Vulnerability Management/`
Cardholder Data in DMZ	This rule triggers when cardholder data assets are detected in the DMZ segment.	`ArcSight Solutions/CIP/Compliance Scenarios/Network Security/`
Clear Text Password Transmission	This rule triggers when a clear text password transmission is detected.	`ArcSight Solutions/CIP/Compliance Scenarios/Privacy Protection/`
Creation and Deletion of Objects	This rule detects object creations and deletions.	`ArcSight Solutions/CIP/Compliance Scenarios/Monitoring/`
Critical Network Device Configuration Change	This rule triggers when a network device configuration change is detected and has Very-High agent severity. Devices include: Firewalls VPNs Network Equipment Network Routings Network Intrusion Detection Systems	`ArcSight Solutions/CIP/Compliance Scenarios/System Hardening/`
Critical Operating System Change	This rule triggers when operating system change is detected on critical asset and has Very-High agent severity.	`ArcSight Solutions/CIP/Compliance Scenarios/System Hardening/`
Cross-Site Request Forgery	This rule detects cross-site request forgery vulnerabilities reported by vulnerability scanners.	`ArcSight Solutions/CIP/Compliance Scenarios/Vulnerability Management/`
Cross-Site Scripting	This rule detects cross-site scripting flaws reported by vulnerability scanners.	`ArcSight Solutions/CIP/Compliance Scenarios/Vulnerability Management/`
Cryptographic Hash Algorithm Related Vulnerability	Triggers when potential cryptographic hash algorithm related vulnerability is detected.	`ArcSight Solutions/CIP/Compliance Scenarios/Vulnerability Management/`

Rules Resources, continued

Resource	Description	URI
Cryptographic Public Key Related Vulnerability	Triggers when potential cryptographic public key related vulnerability is detected.	`ArcSight Solutions/CIP/Compliance Scenarios/Vulnerability Management/`
Cryptographic Symmetric Key Related Vulnerability	Triggers when potential cryptographic symmetric algorithm related vulnerability is detected.	`ArcSight Solutions/CIP/Compliance Scenarios/Vulnerability Management/`
Cryptographic Weak Protocol Vulnerability	Triggers when potential cryptographic weak protocol algorithm related vulnerability is detected.	`ArcSight Solutions/CIP/Compliance Scenarios/Vulnerability Management/`
Custom Account Detected	This rule detects the use of development, test, or custom application or user accounts outside of the test or development environments.	`ArcSight Solutions/CIP/Compliance Scenarios/System Hardening/`
Default Vendor Account Used Successfully	This rule identifies successful default vendor account usage.	`ArcSight Solutions/CIP/Compliance Scenarios/System Hardening/`
Direct Connections between Internet and Cardholder Data Environment	This rule detects successful direct connection (inbound or outbound) between the cardholder data environment and the Internet.	`ArcSight Solutions/CIP/Compliance Scenarios/Network Security/`
Event Time: Empty or Non-empty	This rule triggers on every event. The impact of this rule is positive if the event time stamp is present. Otherwise, the impact is negative.	`ArcSight Solutions/CIP/Compliance Scenarios/Monitoring/`
Events from External-Facing Technologies	This rule detects events from external-facing technologies. By default, this rule supports firewalls, Domain Name Servers, and network IDS/IPS devices.	`ArcSight Solutions/CIP/Compliance Scenarios/Monitoring/`
Failed Logical Access Attempts	This rule detects failed logical access attempts.	`ArcSight Solutions/CIP/Compliance Scenarios/Access Control/`
Failed Physical Access Attempt	This rule detects a failed physical access attempt.	`ArcSight Solutions/CIP/Compliance Scenarios/Physical Security/`

Rules Resources, continued

Resource	Description	URI
File Integrity Tool Detected	This rule detects an event from a file integrity tool.	`ArcSight Solutions/CIP/Compliance Scenarios/Monitoring/`
Heartbleed Vulnerability	This rule detects Heartbleed vulnerability reported by vulnerability scanners.	`ArcSight Solutions/CIP/Compliance Scenarios/Vulnerability Management/`
High Risk Vulnerability Detected	This rule detects high risk flaws reported by vulnerability scanners.	`ArcSight Solutions/CIP/Compliance Scenarios/Vulnerability Management/`
Identified User Account in Event	This rule triggers when an identified user account is detected in the event.	`ArcSight Solutions/CIP/Compliance Scenarios/Monitoring/`
Identified User Account Lockout	This rule triggers when an account lockout event is detected and the source or destination username is not empty.	`ArcSight Solutions/CIP/General/`
Implement a DMZ	This rule identifies the existence of assets or zones that belong to the DMZ category. This is done by performing the following. For zones that belong to the DMZ category, run the trend to search for events with source or destination zones in the DMZ category. For assets that belong to the DMZ category, run the trend to get a list of assets that belong to the DMZ category. See the Solution Guide for more details.	`ArcSight Solutions/CIP/Compliance Scenarios/Network Security/`
Improper Access Control	This rule detects access control flaws reported by vulnerability scanners.	`ArcSight Solutions/CIP/Compliance Scenarios/Access Control/`
Improper Error Handling	This rule triggers when error handling flaws reported by vulnerability scanners are detected.	`ArcSight Solutions/CIP/Compliance Scenarios/Vulnerability Management/`
Inactive User Account Activity	This rule detects successful activities by accounts that are in the Inactive Accounts active list.	`ArcSight Solutions/CIP/Compliance Scenarios/Access Control/`
Information System Failures	This rule looks for information system failures.	`ArcSight Solutions/CIP/Compliance Scenarios/Monitoring/`
Injection Flaws	This rule detects injection flaws reported by vulnerability scanners. For example, SQL injection, OS Command Injection, LDAP and XPath injection, and more.	`ArcSight Solutions/CIP/Compliance Scenarios/Vulnerability Management/`

Rules Resources, continued

Resource	Description	URI
Insecure Communications	This rule detects insecure communication flaws reported by vulnerability scanners.	`ArcSight Solutions/CIP/Compliance Scenarios/Vulnerability Management/`
Insecure Cryptography	This rule detects cryptography flaws reported by vulnerability scanners.	`ArcSight Solutions/CIP/Compliance Scenarios/Cryptography/`
Insecure Services, Protocols or Daemons Detected	This rule detects insecure services, protocols, or daemons; for example, Telnet or RSH.	`ArcSight Solutions/CIP/Compliance Scenarios/System Hardening/`
Insecure Transmission of Cardholder Data Over Public Networks	This rule detects insecure transmission of sensitive cardholder data over the Internet.	`ArcSight Solutions/CIP/Compliance Scenarios/Cryptography/`
Internal IP access from Internet into DMZ	This rule triggers when internal addresses successfully pass from the Internet into the DMZ.	`ArcSight Solutions/CIP/Compliance Scenarios/Network Security/`
Lockout Duration	This rule detects an unlock event of an identified user account. If the lockout duration is longer than 30 minutes, the impact of this rule is positive, otherwise, the impact is negative. If both source and destination assets are empty, the username is reported as asset.	`ArcSight Solutions/CIP/Compliance Scenarios/Access Control/`
Malware or Spyware Detected	This rule triggers when a spyware or malware activity is reported by either an Intrusion Detection System (IDS) or an anti-virus application.	`ArcSight Solutions/CIP/Compliance Scenarios/Vulnerability Management/`
Misconfigurations	This rule detects misconfiguration flaws reported by vulnerability scanners.	`ArcSight Solutions/CIP/Compliance Scenarios/Vulnerability Management/`
Multiple Functions Implemented on a Server	This rule triggers when an asset with multiple functionality is detected; for example, a database and Web server installed on the same machine.	`ArcSight Solutions/CIP/Compliance Scenarios/System Hardening/`
Network IDS Detected	This rule detects an event categorized as originating from a network Intrusion Detection System (IDS) or Intrusion Protection System (IPS).	`ArcSight Solutions/CIP/Compliance Scenarios/Network Security/`

Rules Resources, continued

Resource	Description	URI
New Database Server Detected in Device	This rule triggers when new database servers are detected in the device (database servers that do not belong to the Database category).	`ArcSight Solutions/CIP/General/`
New Database Server Detected in Source or Destination	This rule triggers when new database servers are detected in the source or destination (database servers that do not belong to the Database category).	`ArcSight Solutions/CIP/General/`
New Domain Name Server Detected in Device	This rule triggers when new Domain Name Servers are detected in the device (Domain Name Servers that do not belong to the Domain Name Server category).	`ArcSight Solutions/CIP/General/`
New Domain Name Server Detected in Source or Destination	This rule detects new Domain Name Servers in the source or destination (Domain Name Servers that do not belong to the Domain Name Server category).	`ArcSight Solutions/CIP/General/`
New Web Server Detected in Device	This rule triggers when new Web servers are detected in the device (Web servers that do not belong to the Web Server category).	`ArcSight Solutions/CIP/General/`
New Web Server Detected in Source or Destination	This rule triggers when new Web servers are detected in the source or destination (Web servers that do not belong to the Web Server category).	`ArcSight Solutions/CIP/General/`
Non-empty Origination of Event	This rule detects events with a non-empty origination.	`ArcSight Solutions/CIP/Compliance Scenarios/Monitoring/`
Non Multi Factor Access to CDE by Admin Account	This Rule detects events indicating a non multi factor authentication to CDE by admin accounts.	`ArcSight Solutions/CIP/Compliance Scenarios/Access Control/`
PCI DSS	This rule detects compliance scenario events that are mapped to PCI DSS controls, and updates the compliance score of the reported assets. If some of the reported assets are not relevant for PCI DSS regulation, a special active list can be used to limit the rule to a specific set of assets; for example, by network zone.	`ArcSight Solutions/CIP/Regulation Rules/`
Password Management: Successful Changes or Expirations	This rule detects successful password change events and password expiration events. Instead of reporting the asset for the compliance status, the username is used.	`ArcSight Solutions/CIP/Compliance Scenarios/Access Control/`

Rules Resources, continued

Resource	Description	URI
Penetration Testing not Performed for Longer than Policy Standard	This rule detects when penetration testing was not Performed for Longer than Policy Standard.	`ArcSight Solutions/CIP/Compliance Scenarios/Vulnerability Management/`
Personal Firewall	This rule triggers when events reported by a personal firewall are detected.	`ArcSight Solutions/CIP/Compliance Scenarios/Network Security/`
Physical Access Events	This rule detects a physical access attempt.	`ArcSight Solutions/CIP/Compliance Scenarios/Physical Security/`
Policy Violations	This rule looks for policy violations.	`ArcSight Solutions/CIP/Compliance Scenarios/Monitoring/`
Poodle Vulnerability	This rule detects POODLE vulnerability reported by vulnerability scanners.	`ArcSight Solutions/CIP/Compliance Scenarios/Vulnerability Management/`
Primary Account Numbers Detected in Clear Text	This rule triggers when primary account numbers are identified on the wire as detected by a Network Intrusion Detection System (NIDS).	`ArcSight Solutions/CIP/Compliance Scenarios/Privacy Protection/`
Primary Account Numbers Detected in Testing or Development Environment	This rule triggers when a Primary Account Number (PAN) is detected in clear text in the testing or development environment.	`ArcSight Solutions/CIP/Compliance Scenarios/Privacy Protection/`
Private IP Protected From Disclosure	This rule detects the use of an RFC1918 address.	`ArcSight Solutions/CIP/Compliance Scenarios/Network Security/`
Security Patch Missing	This rule detects events in which vulnerability scanners report a missing security patch.	`ArcSight Solutions/CIP/Compliance Scenarios/Vulnerability Management/`
SSL|TLS 1.0 Detected	This rule detects if SSL\TLS 1.0 is supported based on vulnerability scanner events.	`ArcSight Solutions/CIP/Compliance Scenarios/Vulnerability Management/`

Rules Resources, continued

Resource	Description	URI
SSL|TLS Vulnerability	This rule detects SSL and TLS flaws reported by vulnerability scanners.	`ArcSight Solutions/CIP/Compliance Scenarios/Vulnerability Management/`
Success or Failure Indication in Event	This rule triggers when a success or failure indication is detected in the event.	`ArcSight Solutions/CIP/Compliance Scenarios/Monitoring/`
Successful Disallowed Ports Access from Wireless into Cardholder Data Environment	This rule detects successful disallowed port access from a wireless network into the cardholder data environment.	`ArcSight Solutions/CIP/Compliance Scenarios/Network Security/`
Successful Disallowed Ports Access in Cardholder Data Environment	This rule triggers when communication with a forbidden destination port within the cardholder data environment is allowed (inbound or outbound).	`ArcSight Solutions/CIP/Compliance Scenarios/Network Security/`
Successful Login by Active Account	This rule detects successful logins from active accounts (users) and puts the account information in the Active Accounts active list.	`ArcSight Solutions/CIP/General/`
Successful Password Change	This rule detects successful password change events and inserts the username into the Password Changes active list.	`ArcSight Solutions/CIP/General/`
Successful Traffic from Internet into non-DMZ Destination	This rule detects successful inbound Internet traffic to any destination outside the DMZ segment.	`ArcSight Solutions/CIP/Compliance Scenarios/Network Security/`
Successful Unauthorized Traffic from Cardholder Data Environment to Internet	This rule detects unauthorized outbound traffic from the cardholder data environment to the Internet.	`ArcSight Solutions/CIP/Compliance Scenarios/Network Security/`
Terminated User Activity	This rule detects any activity of user accounts that have been terminated and placed in the Terminated Users active list.	`ArcSight Solutions/CIP/Compliance Scenarios/Access Control/`
Test Account in Production Environment	This rule detects the use of a test user in the production environment.	`ArcSight Solutions/CIP/Compliance Scenarios/Access Control/`

Rules Resources, continued

Resource	Description	URI
Time Consistency Issues	This rule detects a clock or time related problem.	`ArcSight Solutions/CIP/Compliance Scenarios/Monitoring/`
TLS BREACH Vulnerability	This rule detects if TLS BREACH (Browser Reconnaissance and Exfiltration via Adaptive Compression of Hypertext) vulnerability reported by vulnerability scanners.	`ArcSight Solutions/CIP/Compliance Scenarios/Vulnerability Management/`
TLS CRIME Vulnerability	This rule detects if TLS CRIME (Compression Ratio Info-leak Made Easy) vulnerability reported by vulnerability scanners.	`ArcSight Solutions/CIP/Compliance Scenarios/Vulnerability Management/`
Unauthorized Access Point Detected	This rule triggers when an unauthorized access point is detected in the network.	`ArcSight Solutions/CIP/Compliance Scenarios/Network Security/`
Unauthorized Access to Cardholder Data	This rule detects an unauthorized access to the cardholder data environment.	`ArcSight Solutions/CIP/Compliance Scenarios/Access Control/`
Unauthorized Direct Cardholder Database Access	This rule detects unauthorized direct access to a cardholder database. A user is not authorized to access a cardholder database directly unless identified as database administrator. Populate the Database Administrators active list with the usernames of the database administrators in the organization.	`ArcSight Solutions/CIP/Compliance Scenarios/Access Control/`
Unencrypted Non-Console Administrative Access Detected	This rule detects the use of clear text protocols (HTTP, Telnet) for administrative account access.	`ArcSight Solutions/CIP/Compliance Scenarios/System Hardening/`
Unnecessary Functionality Detected	This rule triggers when database servers, Web servers, and Domain Name Servers that do not belong to a corresponding asset category are detected. These servers are identified as an unnecessary functionality within the organizational network.	`ArcSight Solutions/CIP/Compliance Scenarios/System Hardening/`

Rules Resources, continued

Resource	Description	URI
User Account Expired	This rule triggers every time an entry ages out of the Active Accounts active list. This happens when an account has been inactive for more than the amount of time specified in the time-to-live of this active list.	`ArcSight Solutions/CIP/General/`
Vulnerability Scans	This rule detects vulnerability scans.	`ArcSight Solutions/CIP/Compliance Scenarios/Vulnerability Management/`
Wireless Encryption Violation in Cardholder Data Environment Detected	This rule triggers when a wireless Intrusion Detection System (IDS) reports a wireless traffic encryption violation in the cardholder data environment.	`ArcSight Solutions/CIP/Compliance Scenarios/Cryptography/`

Trends

The following table lists all the trends in Compliance Insight Package for the Payment Card Industry.

Trends Resources

Resource	Description	URI
Compliance Scenario Correlation Events	This trend stores chosen fields from compliance scenario correlation events.	`ArcSight Solutions/CIP/General/`
Configuration Changes	Collects hourly data using the Configuration Changes Trend Base query. Used by other queries to show configuration changes.	`ArcSight Solutions/CIP/System Hardening/`
DMZ Assets	This trend checks whether at least one asset that belongs to the DMZ category was detected during the last 24 hours.	`ArcSight Solutions/CIP/Network Security/`
DMZ Zones	This trend checks whether at least one zone that belongs to the DMZ category was detected during the last 24 hours.	`ArcSight Solutions/CIP/Network Security/`
PCI DSS Compliance Score Sum	This trend stores PCI DSS compliance and non-compliance score summation for all control-asset pairs in the system. This data is used to build the top level compliance and non-compliance status reports for the PCI DSS regulation.	`ArcSight Solutions/CIP/Regulations/PCI DSS/`

Trends Resources, continued

Resource	Description	URI
PCI DSS Maximal Asset Compliance Score	This trend stores the maximum potential PCI DSS compliance score for a single asset.	`ArcSight Solutions/CIP/Regulations/PCI DSS/`
PCI DSS Maximal Asset Compliance Score: Requirement	This trend stores the maximum potential PCI DSS compliance score for a single asset, for each PCI DSS requirement.	`ArcSight Solutions/CIP/Regulations/PCI DSS/`
PCI DSS Maximal Asset Non-Compliance Score	This trend stores the maximum potential PCI DSS non-compliance score for a single asset.	`ArcSight Solutions/CIP/Regulations/PCI DSS/`
PCI DSS Maximal Asset Non-Compliance Score: Requirement	This trend stores the maximum potential PCI DSS non-compliance score for a single asset, for each PCI DSS requirement.	`ArcSight Solutions/CIP/Regulations/PCI DSS/`
PCI DSS Number of Assets	This trend stores the number of assets for the PCI DSS regulation. This number includes all assets that were reported compliant or non-compliant for at least one PCI DSS control.	`ArcSight Solutions/CIP/Regulations/PCI DSS/`
Password Expired	This trend stores all events in the last month of accounts for which the password was not changed for longer than the policy standard permits.	`ArcSight Solutions/CIP/Access Control/`

Use Cases

The following table lists all the use cases in Compliance Insight Package for the Payment Card Industry.

Use Cases Resources

Resource	Description	URI
Access Control	This use case provides a high-level overview of resources that belong to the Access Control domain.	`ArcSight Solutions/CIP/`
Cryptography	This use case provides a high-level overview of resources that belong to the Cryptography domain.	`ArcSight Solutions/CIP/`
General	This use case provides a high-level overview of cross-domain resources. These resources do not belong to a specific domain and may be used by various compliance scenarios.	`ArcSight Solutions/CIP/`
Monitoring	This use case provides a high-level overview of resources that belong to the Monitoring domain.	`ArcSight Solutions/CIP/`

Use Cases Resources, continued

Resource	Description	URI
Network Security	This use case provides a high-level overview of resources that belong to the Network Security domain.	`ArcSight Solutions/CIP/`
PCI DSS Compliance Status	This use case provides a high-level overview of PCI DSS compliance.	`ArcSight Solutions/CIP/`
Physical Security	This use case provides a high-level overview of resources that belong to the Physical Security domain.	`ArcSight Solutions/CIP/`
Privacy Protection	This use case provides a high-level overview of resources that belong to the Privacy Protection domain.	`ArcSight Solutions/CIP/`
System Hardening	This use case provides a high-level overview of resources that belong to the System Hardening domain.	`ArcSight Solutions/CIP/`
Vulnerability Management	This use case provides a high-level overview of resources that belong to the Vulnerability Management domain.	`ArcSight Solutions/CIP/`

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 Solutions Guide (ESM CIP for PCI 4.1)

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 arcsight_doc@microfocus.com.

We appreciate your feedback!