opentext™

ArcSight Compliance Pack PCI

Software Version: 1.0.0.1

Solutions Guide for ArcSight Compliance Pack PCI

Document Release Date: October 2023
Software Release Date: February 2022

About this Compliance Pack

This compliance pack provides a set of dashboards and reports that can assist you in complying with PCI DSS 160 requirements established by the PCI Security Standards Council. This package leverages the litigation-quality, long-term repository of log and event data to support better PCI compliance audits, security forensics, and system maintenance using the reporting.

In addition to detailed report results, each report contains a summary of the PCI requirement it addresses, how the report supports the requirement, and testing criteria an auditor can use to determine your organization’s compliance with the requirement.

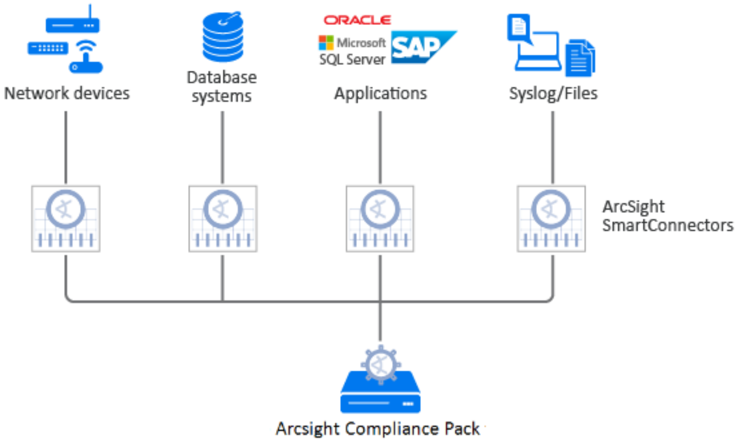
- "How Events Flow to this Compliance Pack" below
- "Supported Devices" on the next page

For information about running, formatting, publishing, and scheduling reports, see the *Help* or the *User’s Guide for Recon in the ArcSight Platform*.

How Events Flow to this Compliance Pack

The dashboards and reports available with this ArcSight Compliance Pack operate on events in Common Event Format (CEF), which is an industry standard for the interoperability of event or log-generating devices. CEF events can come from a device that is already configured to post events in CEF. For devices in your network that are not already CEF-ready, the events must run through an ArcSight SmartConnector.

For more information about CEF events and how they are used, see the *Administrator's Guide for ArcSight Platform*.



Supported Devices

The following table lists the devices that could generate events used by this compliance pack per PCI requirement.

PCI Requirement	Supported Devices
Requirement 1	Network Equipment Firewall devices
Requirement 2	Network Equipment Firewall devices Operating System devices
Requirement 3	Intrusion Detection System Intrusion Prevention System Vulnerability Scanner Application
Requirement 4	Vulnerability Scanner Wireless Intrusion Detection System
Requirement 5	Anti-Virus
Requirement 6	Vulnerability Scanner Firewall Intrusion Detection System Operating System Devices
Requirement 7	Firewall Intrusion Detection System
Requirement 8	Operating Systems Vulnerability Scanner
Requirement 9	Physical Security Systems

Requirement 10	Anti-Virus Applications Content Security, Web Filtering Database Firewall Identity Management Intrusion Detection System Intrusion Prevention System Network Equipment Operating System Physical Security Systems Policy Management Virtual Private Network Virtual Private Network Vulnerability Assessment Wireless
Requirement 11	Vulnerability Assessment Intrusion Detection System File Integrity tools
Requirement 12	Policy Management

Adding and Removing the Compliance Pack

This section describes how to download, add, and remove this compliance pack.

- "Downloading this Pack" below
- "Installing this Pack" below
- "Uninstalling this Pack" below

Downloading this Pack

To purchase this pack, please contact your account or sales representative.

After you purchase this pack, you can download the package from the Software Licenses and Downloads (SLD) portal. Log in to the portal using your active service contract ID.

Installing this Pack

1. Select Reports > Content.
2. Click the Import Asset ⬆ icon.
3. Select the zip file for the compliance pack from the stored location.
4. Click Next.
5. Follow the prompt to import and continue with the installation.
6. To verify the installation is complete, locate the compliance pack folder under the Standard Content folder.

Uninstalling this Pack

To uninstall this compliance pack, you must remove both the content (reports and dashboards) from the Reports repository and the worksheets that support the content.

- "Removing Reports Content" on the next page
- "Removing Worksheets Content" on the next page

Removing Reports Content

1. Select Reports > Portal.
2. Select Repository > Standard Content.
3. Right-click the folder that you want to remove, then select Delete.
4. Click OK.

Removing Worksheets Content

1. Select Reports > Portal.
2. Click the Create ✨ icon.
3. Click Data Worksheet.
4. In the *New Data Worksheet*, click Cancel.
5. In the navigation pane, select Data Worksheet > Standard Content.
6. Right-click on the content, such as PCI, then select Remove.
7. Click OK.

Specifying Your PCI Assets

This section describes how to define assets using variables and case conditions.

1. Select Reports > Portal.
2. Click the Data icon.
3. In the navigation pane, expand Data Source > Database > Events > PCI.
4. In the **Logical Model** pane, expand Events.
5. Select the field that you want to define.

   The ƒ symbol indicates the fields that you can modify.
6. To add the case condition, modify the formula for the field.

> By default, if the field values are equal to **No**, the reports and dashboards will be empty. If you want reports and dashboards to work against specific resource types, modify the values.

Resource Type	Fields	Example
IP address	isSourceAddressPCI isDestinationAddressPCI	If you have these IP addresses: 10.15.15.15, 10.15.15.16, 192.168.0.0/16 Then you enter: `CASE WHEN field ['Events.sourceAddress'] IN ('10.15.15.15','10.15.15.16') or field['Events.sourceAddress'] like ('192.168.%') THEN 'Yes' Else 'No' END`
Host name	isDestinationHostNamePCI isSourceHostNamePCI	If the host name contains "PCI" Then you enter: `CASE WHEN field ['Events.sourceHostName'] like '%PCI%') THEN 'Yes' Else 'No' END`

Zones	isDestinationZonePCI isDestinationZonePCIDevelopment isDestinationZonePCIProduction isSourceZonePCI isSourceZonePCIDevelopment isSourceZonePCIProduction	If the network zone is /All Zones/ArcSight System/Private Address Space Zones/RFC1918: 192.168.0.0-192.168.255.255, /All Zones/ArcSight System/Private Address Space Zones/RFC1918: 10.0.0.0-10.255.255.255 Then you enter: `CASE WHEN field ['Events.sourceZoneURI'] IN ('/All Zones/ArcSight System/Private Address Space Zones/RFC1918: 192.168.0.0-192.168.255.255','/All Zones/ArcSight System/Private Address Space Zones/RFC1918: 10.0.0.0-10.255.255.255') THEN 'Yes' Else 'No' END`
Users	isDestinationAdminUser isSourceAdminUser	If you want to watch specific users with administrative privileges including fsmith@extremelyfocused.com Then you add the account to: `CASE WHEN field ['default_secops_adm.events.sourceUserName']) IN ('admin','administrator','root','system', 'fsmith@extremelyfocused.com') THEN 'Yes' Else 'No' END`
Other	isDestinationNTDomainPCI isInsecurePorts isInsecureProcesses	If you want to identify the ports 123, 234, 345 as insecure ports Then you add them to: `CASE WHEN (field ['default_secops_adm.events.destinationPort'] IN ('20','21','23','110','143','137', '433', '123', '234', '345') THEN 'Yes' Else 'No' END`
Buildings	PCI Buildings	If you have five buildings that have restricted access Then you enter: `CASE WHEN (field['PCI Events.deviceCustomString1']) IN ('PCI_BUILDING','PCI_BUILDING_2','PCI_BUILDING_3','PCI_BUILDING_4', 'PCI_BUILDING_5') THEN 'Yes' Else 'No' END`

7. Click OK
8. Save your changes.

Viewing Dashboard and Report Details

This compliance pack provides a library of reports and dashboards to help you to address the following objectives.

Compliance Reporting	Supports the presentation of requirements to internal and external audit teams, as well as upper management.
Security Best Practices	This compliance pack can be used to help implement, monitor and manage a best practices approach to information security management as well as ensuring GDPR security controls are in place and enforced.
Harmful User and Machine Monitoring	Tracks potentially harmful users and machines.
Visualizing Security Events	Displaying security events graphically which allows analysts to quickly analyze situations.
Vulnerabilities and Configuration Changes Monitoring	Tracking vulnerabilities and configuration changes on GDPR systems.

For more information on the available dashboards and reports in this compliance pack, see the *Help* in ArcSight Recon or the *User’s Guide for Recon in the ArcSight Platform*.

For additional reports and dashboards, see the PCI packages provided for *ArcSight Enterprise Security Manager (ESM)* or *ArcSight Logger*.

Known Issues

We are currently researching the following issues that are common to all capabilities that you can deploy in the Compliance Packs.

Micro Focus strives to ensure that our products provide quality solutions for your enterprise software needs. If you need assistance with any issue, visit Micro Focus Support, then select the appropriate product category.

Issues with Report and Dashboards Formatting

Issue: When using the **Export Asset** feature, the formatting for the reports and dashboards might have issues such as:

- Dark backgrounds
- Dark fonts
- Dark table cells

Workaround: Currently, no workaround is available. (OCTCR33I186007)

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 computer, click the link above and an email window opens with the following information in the subject line:

Feedback on Solutions Guide for ArcSight Compliance Pack PCI (Compliance Pack PCI 1.0.0.1)

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 MFI-Documentation-Feedback@opentext.com.

We appreciate your feedback!

Additional Documentation

The ArcSight Platform documentation library includes the following resources.

- Administrator's Guide for ArcSight Platform, which contains installation, user, and deployment guidance for the ArcSight software products and components that you deploy in the containerized platform.
- User’s Guide for Fusion 1.3 in the ArcSight Platform, which is embedded in the product to provide both context-sensitive Help and conceptual information.
- Product Support Lifecycle Policy, which provides information on product support policies.

Legal Notices

Open Text Corporation

275 Frank Tompa Drive, Waterloo, Ontario, Canada, N2L 0A1

Copyright Notice

The only warranties for products and services of Open Text and its affiliates and licensors (“Open Text”) are as may be set forth in the express warranty statements accompanying such products and services. Nothing herein should be construed as constituting an additional warranty. Open Text shall not be liable for technical or editorial errors or omissions contained herein. The information contained herein is subject to change without notice.

Trademark Notices

“OpenText” and other Open Text trademarks and service marks are the property of Open Text or its affiliates. All other trademarks or service marks are the property of their respective owners.