

Solutions Guide for ArcSight Compliance Pack PCI

Thursday, May 13, 2021

Version 1.0.0.0

*You must have **ArcSight Recon 1.2** to use this compliance pack.*



We support PCI Standard 3.2. This package provides a limited set of reports for checking compliance. For a full set of reports and dashboards, see the packages provided for [ArcSight Enterprise Security Manager \(ESM\)](#) or [ArcSight Logger](#).

The Payment Card Industry (PCI) Data Security Standard (DSS) 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 sub-requirements: for security management, policies, procedures, network architecture, software design, and other key protective measures.

- ["What's New" on the next page](#)
- ["Adding and Removing the Compliance Pack" on page 4](#)
- ["Specifying Your PCI Assets" on page 5](#)
- ["Viewing Report and Dashboard Details" on page 7](#)
- ["Known Issues" on page 7](#)
- ["Send Documentation Feedback" on page 9](#)
- ["Additional Documentation" on page 10](#)

What's New

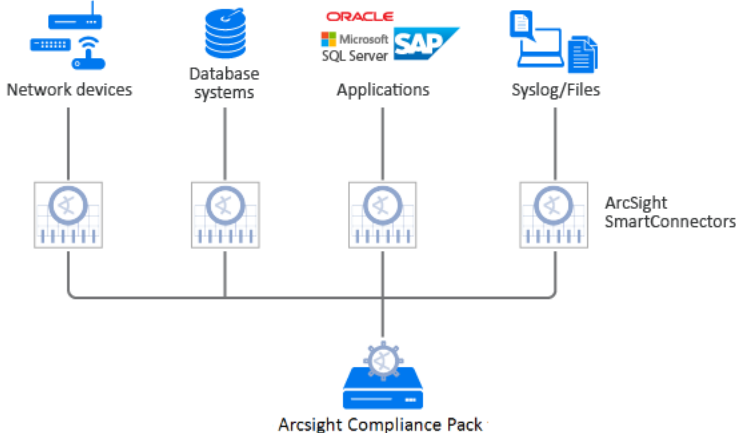
This new compliance pack is a package of reports that can assist you in complying with PCI DSS requirements. This package leverages the litigation-quality, long-term repository of log and event data to facilitate better PCI compliance audits, security forensics, and system maintenance using the reporting.

PCI reports demonstrate stakeholders and auditors that controls are implemented on their credit card systems. Hence, they are PCI compliant and show due diligence to comply with PCI standards. This compliance pack provides a library of reports for specific standards and requirements.

Architecture

The ArcSight Compliance Pack reports operate on events in Common Event Format (CEF), 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, or they can come from any network device whose events are first run through an ArcSight SmartConnector.

This compliance pack operates on events received from devices on the network in CEF. IT Governance devices that are not already CEF-ready must be run through an ArcSight SmartConnector. For more about CEF events and how they are used, see the [Administrator's Guide for ArcSight Platform](#).



Supported Devices

The following lists the supported devices that may generate events used by the compliance pack.

PCI Requirement	Supported Devices	PCI Requirement	Supported Devices
Requirement 1	Network Equipment Firewall Devices	Requirement 7	Firewall Intrusion Detection System
Requirement 2	Network Equipment Firewall Devices Operating System Devices	Requirement 8	Operating Systems Vulnerability Scanner
Requirement 3	Intrusion Detection System Intrusion Prevention System Vulnerability Scanner Application	Requirement 9	Physical Security Systems
Requirement 4	Vulnerability Scanner Wireless Intrusion Detection System	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 5	Anti-Virus	Requirement 11	Vulnerability Assessment Intrusion Detection System File Integrity Tools
Requirement 6	Vulnerability Scanner Firewall Intrusion Detection System Operating System Devices	Requirement 12	Policy Management

Resources

This compliance pack consists of standard reports. These reports are optimized to help companies and PCI auditors determine the status of your systems for each PCI requirement addressed by the solution report.


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.

For information about running, formatting, publishing, and scheduling reports, see the *Help* or the [User's Guide for Recon in the ArcSight Platform](#).

Adding and Removing the Compliance Pack

This section describes adding and removing the compliance pack.


Adding Content

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.

Removing Reports Content



1. Select **Reports > Portal**.
2. Select **Repository > Standard Content**.
3. Select the content, such as **PCI**, right-click, and select **Delete**.
A confirmation pop-up window displays.
4. Click **OK**.

Removing Worksheets Content

1. Select **Reports > Portal**.
2. Click the **Create**  icon.
3. Click **Data Worksheet**. The *New Data Worksheet* pop-up window displays.
4. Click **Cancel**.
5. In the navigation pane, select **Data Worksheet > Standard Content**.
6. Select the content, such as **PCI**, right-click, and select **Remove**.
A confirmation pop-up window displays.
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 Worksheet > Standard Content > PCI > PCI Systems**.
4. Click the worksheet to open. Multiple fields and variables display in the lower pane.
5. To define the assets for this compliance pack, select the variable to modify, and then click the **formula** icon, which is identified with an .

The *Formula Editor* pop-up displays.

6. Modify the formula to add the case condition.

For more examples, see:

- Specific Resource Types

By default, the field values below 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 for each specific resource type.

Defines IP Addresses	isSourceAddressPCI
	isDestinationAddressPCI
Defines Host Names	isSourceHostNamePCI
	isDestinationHostNamePCI
Defines Zones	isSourceZonePCI
	isDestinationZonePCI

For Example

IP Address: 10.15.15.15, 10.15.15.16, 192.168.0.0/16

To define assets, modify these values:

Field	Old Value	New Value
isSourceAddressPCI	No	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
isDestinationAddressPCI	No	CASE WHEN field['Events.destinationAddress'] IN ('10.15.15.15','10.15.15.16') or field ['Events.destinationAddress'] like ('192.168.%') THEN 'Yes' Else 'No' END

For Example

Hostname contains PCI

To define assets, modify these values:

Field	Old Value	New Value
isSourceHostNamePCI	No	CASE WHEN field['Events.sourceHostName'] like '%PCI%') THEN 'Yes' Else 'No' END
isDestinationHostNamePCI	No	CASE WHEN field['Events.destinationHostName'] like '%PCI%') THEN 'Yes' Else 'No' END


For Example

Network Zone: /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

To define assets, modify these values:

Field	Old Value	New Value
isSourceZonePCI	No	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

isDestinationZonePCI	No	CASE WHEN field['Events.destinationZoneURI'] 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
----------------------	----	--

7. Click **OK** and then click the **save**  icon.

Viewing Report and Dashboard Details

For information on the available reports and dashboards in this compliance pack, see the *ArcSight Recon Help* or the [User's Guide for Recon in the ArcSight Platform](#).

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 " below](#)
- ["Reports Not Included" below](#)

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)

Reports Not Included

Issue: The following reports are not included in the PCI Compliance Packs currently:

- Standard Content/PCI/PCI Reports/Requirement 1: Firewall Configuration/Cardholder Data Within the DMZ Replet
- Standard Content/PCI/PCI Reports/Requirement 1: Firewall Configuration/Inbound Traffic to the Cardholder Data Environment Replet
- Standard Content/PCI/PCI Reports/Requirement 1: Firewall Configuration/Outbound Traffic From Card Holder Data Environment to Internet Replet
- Standard Content/PCI/PCI Reports/Requirement 1: Firewall Configuration/Outbound Traffic from the Cardholder Data Environment Replet
- Standard Content/PCI/PCI Reports/Requirement 1: Firewall Configuration/Unauthorized Outbound Traffic From Cardholder Data Environment Replet

Workaround: We will include these reports in the future. (OCTCR33I186008)

Send Documentation Feedback

We designed this product in direct response to suggestions from our customers. We thank you for your time and valuable input. We hope that you continue to help us ensure that our products meet all your needs.

The documentation for this product is available on the Documentation website in HTML and PDF formats. If you have suggestions for documentation improvements, click **comment** or **support** on this topic at the bottom of any page in the HTML version of the documentation posted at the [ArcSight Platform Documentation](#) page or the documentation pages for the included products.

We want to hear your comments and suggestions about this document and the other documentation included with this product. You can use the **comment** or **support** on this topic link at the bottom of each page of the online documentation, or send an email to Documentation-Feedback@microfocus.com.

For specific product issues, contact [Micro Focus Customer Care](#).

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

Copyright Notice

© Copyright 2001 - 2021 Micro Focus or one of its affiliates

Confidential computer software. Valid license from Micro Focus required for possession, use or copying. The information contained herein is subject to change without notice.

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

No portion of this product's documentation may be reproduced or transmitted in any form or by any means, electronic or mechanical, including photocopying, recording, or information storage and retrieval systems, for any purpose other than the purchaser's internal use, without the express written permission of Micro Focus.

Notwithstanding anything to the contrary in your license agreement for Micro Focus ArcSight software, you may reverse engineer and modify certain open source components of the software in accordance with the license terms for those particular components. See below for the applicable terms.

U.S. Governmental Rights. For purposes of your license to Micro Focus ArcSight software, "commercial computer software" is defined at FAR 2.101. If acquired by or on behalf of a civilian agency, the U.S. Government acquires this commercial computer software and/or commercial computer software documentation and other technical data subject to the terms of the Agreement as specified in 48 C.F.R. 12.212 (Computer Software) and 12.211 (Technical Data) of the Federal Acquisition Regulation ("FAR") and its successors. If acquired by or on behalf of any agency within the Department of Defense ("DOD"), the U.S. Government acquires this commercial computer software and/or commercial computer software documentation subject to the terms of the Agreement as specified in 48 C.F.R. 227.7202-3 of the DOD FAR Supplement ("DFARS") and its successors. This U.S. Government Rights Section 18.11 is in lieu of, and supersedes, any other FAR, DFARS, or other clause or provision that addresses government rights in computer software or technical data.