



ArcSight Compliance Insight Package

Software Version: 1.0.0.1

Solutions Guide for ArcSight Compliance Insight Package

Document Release Date: October 2023

Software Release Date: February 2022

About This Compliance Pack

This compliance pack facilitates compliance by providing detailed dashboards and reports that help you evaluate risk and provide comprehensive reporting of high and low-risk activity.

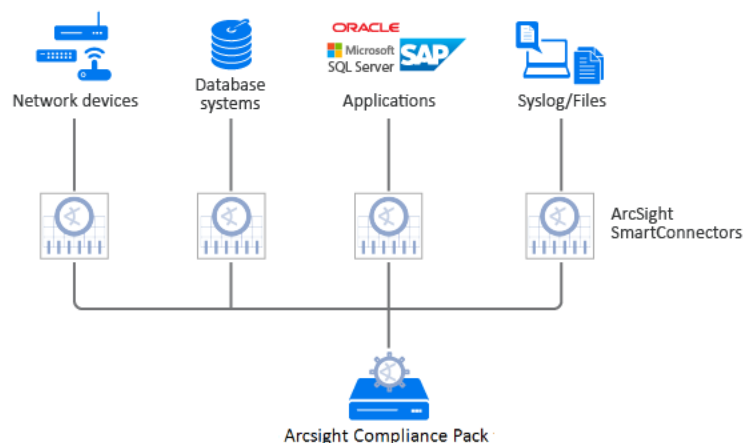
Compliance with the components that apply to your business can best be demonstrated by using a cohesive framework, such as the Code of Practice for information security management, also known as ISO/IEC 27002:2013. This standard was developed by the International Organization for Standardization (ISO) and the International Electrotechnical Commission (IEC) and covers the controls and guidelines a company should consider implementing to follow due diligence and best practices in IT security. This package provides reports for Control 12 - Operations Security. Additional reports will be released in the future.

- ["How Events Flow to this Compliance Pack" below](#)
- ["Supported Devices" on the next page](#)

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.

- Anti-virus solutions
- Applications
- Content Security and Web Filtering systems
- Databases
- Firewalls
- Identity Management systems
- Intrusion Detection System/Intrusion Prevention System
- Network equipment
- Operating systems
- Physical Security systems
- Policy Management systems
- Virtual Management systems
- Virtual Private Networks
- Wireless systems



The IT Governance Compliance Pack reports and alerts operate on events from the devices in your environment. To yield the most accurate reports, we recommend that you use an ArcSight SmartConnector for devices that are not CEF-enabled.

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 IT Governance 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 > IsoSystems.
4. In the **Logical Model** pane, expand EventsISO.
5. Select the field that you want to define.
The  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.

Examples:

- Specific Resource Types

By default, the field values below are equal to **Yes**, which means reports work against all environments. If you want reports to work against specific resource types, modify the values from **Yes** to **No** for each specific resource type. Also, be sure the specific resource types expression return **Yes** for your asset list (Below examples).

Defines MAC Addresses	isSourceMacISO
	isDestinationMacISO
Defines IP Addresses	isSourceAddressISO
	isDestinationAddressISO
Defines Host Names	isSourceHostNameISO
	isDestinationHostNameISO
Defines IP Zones	isSourceZoneISO
	isDestinationZoneISO

For Example:

IP Address: 89.2.1.4,79.2.1.3,91.12.12.15,91.12.12.14,91.12.12.13

To define assets, modify these values:

Field	Old Value	New Value
isSourceMacISO	Yes	No
isSourceAddressISO	Yes	No
isSourceZoneISO	Yes	No
isSourceHostNameISO	Yes	No
isDestinationMacISO	Yes	No
isDestinationAddressISO	Yes	CASE WHEN field['Events.destinationAddress'] IN ('89.2.1.4','79.2.1.3','91.12.12.15','91.12.12.14','91.12.12.13') THEN 'Yes' Else 'No' END
isDestinationZoneISO	Yes	No
isDestinationHostNameISO	Yes	No

For Example:

IP Address: 89.2.1.4,79.2.1.3,91.12.12.15,91.12.12.14,91.12.12.13

Zone: /All Zones/ArcSight System/Public Address Space Zones/ARIN/142.0.0.0-144.255.255.255 (ARIN)

To define assets, modify these values:

Field	Old Value	New Value
isSourceMacISO	Yes	No
isSourceAddressISO	Yes	CASE WHEN field['Events.sourceAddress'] IN ('89.2.1.4','79.2.1.3','91.12.12.15','91.12.12.14','91.12.12.13') THEN 'Yes' Else 'No' END
isSourceZoneISO	Yes	CASE WHEN field['Events.sourceZoneURI'] IN ('/All Zones/ArcSight System/Public Address Space Zones/ARIN/142.0.0.0-144.255.255.255 (ARIN)') THEN 'Yes' Else 'No' END
isSourceHostNameISO	Yes	No
isDestinationMacISO	Yes	No
isDestinationAddressISO	Yes	CASE WHEN field['Events.destinationAddress'] IN ('89.2.1.4','79.2.1.3','91.12.12.15','91.12.12.14','91.12.12.13') THEN 'Yes' Else 'No' END
isDestinationZoneISO	Yes	CASE WHEN field['Events.destinationZoneURI'] IN ('/All Zones/ArcSight System/Public Address Space Zones/ARIN/142.0.0.0-144.255.255.255 (ARIN)') THEN 'Yes' Else 'No' END
isDestinationHostNameISO	Yes	No

- Agent Zone Resource Types

By default, the field values below are equal to **Yes**. If you want to bring additional data from additional connectors, modify the values.

Defines Agent Zones	isAgentZoneISO
	isAgentAddressISO

For Example:

Zone: /All Zones/ArcSight System/Public Address Space Zones/ARIN/142.0.0.0-144.255.255.255 (ARIN)

To define assets, modify these values:

Field	Old Value	New Value
isAgentAddressISO	Yes	No
isAgentZoneISO	Yes	CASE WHEN default_secops_adm.events.agentZoneURI IN ('/All Zones/ArcSight System/Public Address Space Zones/ARIN/142.0.0.0-144.255.255.255 (ARIN)') THEN 'Yes' Else 'No' END

- **Specific Admin Types**

If you want your reports to work against a specific admins.

For Example:

To define ISO assets by Specific Admins, modify this value to work against additional specific admins. We assume the admins to be: admin, administrator, root.

Field	Old Value	New Value
isAdministrativeISO	Yes	CASE WHEN field ['Events.destinationUserNameLowerCase'] IN ('admin','administrator','root') THEN 'Yes' Else 'No' END

7. Click OK
8. Save your changes.

Configuring the Username Variable

This section describes configuring the `isAdminsSourceNameLowerIso` variable. This variable identifies the source username that is an admin user or a non-admin user.

The following [reports](#) use this variable:

- [Administrative Actions All Events Report](#)
- [User Actions Summary Report](#)
- ["User Logins and Logouts Report" on the next page](#)






An additional variable, `isAdministratorISO`, performs the same function as `isAdminsSourceNameLowerIso`. However, instead of using the source username, this variable uses the destination usernames. You need to configure both variables according to the users you want to view in the reports.

Administrative Actions All Events Report and User Actions Summary Report

The reports Administrative Actions All Events and User Actions Summary might have an aggregation and grouping enabled. Therefore, you need to change the view first.


To configure the variable:

1. Select **Reports > Content**.
2. Click the **Change View**  icon.
3. Select **Meta Detail View**.
4. Scroll to the right until you locate the `isAdminsSourceNameLowerIso` variable.
5. Click the **formula** icon, which is identified with an .

The *Formula Editor* pop-up displays.
6. Modify the formula as needed.
7. Click **OK** to save the data worksheet.
8. To change the view back to the original display, click the **Change View**  icon, and select **Meta Data View**.

User Logins and Logouts Report

To configure the variable:

1. Select **Reports > Content**.
2. Scroll to the right until you locate the **isAdminsSourceNameLowerIso** variable.
3. Click the **formula** icon, which is identified with an .
The *Formula Editor* pop-up displays.
4. Modify the formula as needed.
5. Click **OK** to save the data worksheet.

Viewing Dashboard and Report Details

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](#).

Known Issue

We are currently researching the following issue that is 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 Formatting

Issue: When using the **Export Asset** feature, the formatting for the reports 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 Insight Package (Compliance Insight Package 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

Copyright 2001 - 2023 Open Text.

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.