ArcSight Compliance Insight Package GDPR

Software Version: 1.0.0.1

Solutions Guide for ArcSight Compliance Insight Package

Document Release Date: October 2023
Software Release Date: October 2023

Contents

About this Compliance Pack

Micro Focus solutions help manage and protect your data in accordance with GDPR enabling you to grow your business with confidence. For more information on GDPR, see our General Data Protection Regulation (GDPR) Solutions. ArcSight Compliance Pack GDPR is a package of reports and dashboards that assist you in complying with GDPR requirements. This compliance pack leverages the litigation-quality, long-term repository of log and event data to facilitate better compliance audits, security forensics, and system maintenance using the reporting capability.

This compliance pack addresses the GDPR standard by providing:

- Detailed reports for the requirements defined in the GDPR Standard.
- Dashboards with graphics and bar charts that display compliance information for the requirements defined in the GDPR Standard.

The General Data Protection Regulation (GDPR) provides a single set of rules for protecting the personal data of all European Union (EU) residents and visitors.

GDPR consists of two components:

- Articles (99) - The articles constitute the legal requirements organizations must follow to demonstrate compliance.
- Recitals (173) - The recitals provide additional information and supporting context to supplement the articles.

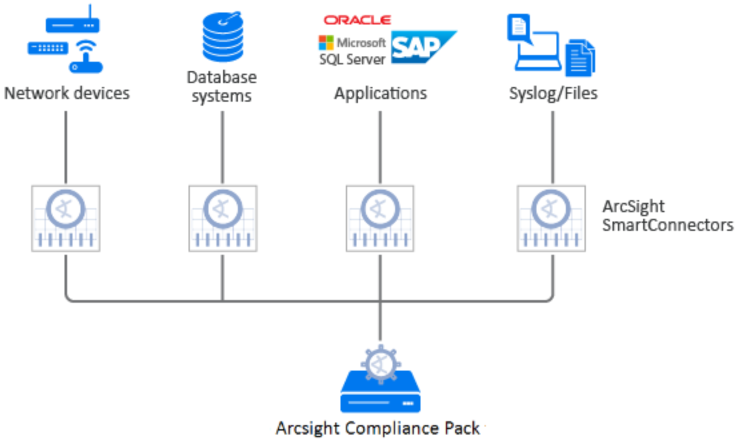
The regulation sets out standards for any action, automatic or manual, that processes on a person’s data. These standards include requiring that the individuals in your enterprise who control, manage, or make decisions about data processing must be able to demonstrate that they are GDPR compliant.

- "About this Compliance Pack" above
- "Adding and Removing the Compliance Pack" on page 5
- "Specifying Your GDPR Assets" on page 7
- "Viewing Dashboard and Report Details" on page 11
- "Known Issues" on page 12

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.

- Anti-virus solutions and EDR products
- Databases
- Content Security and Web Filtering systems
- Operating systems
- Physical Security systems
- Host and network-based IDS
- Firewalls
- Wireless systems
- Vulnerability and assessment tools

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 GDPR 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** > **GDPR**.
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.

   F**Examples:**

   - Specific Resource Types

     By default, the field values below are equal to **Yes**, which means reports and dashboards work against all environments. If you want reports and dashboards 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	isSourceMacGDPR
	isDestinationMacGDPR
Defines IP Addresses	isSourceAddressGDPR
	isDestinationAddressGDPR
Defines GDPR Host Names	isSourceHostNameGDPR
	isDestinationHostNameGDPR
Defines GDPR Zones	isSourceZoneGDPR
	isDestinationZoneGDPR

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
isSourceMacGDPR	Yes	No
isSourceAddressGDPR	Yes	CASE WHEN v6_ntoa(field['default_secops_ adm.events.sourceAddressBin']) 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
isSourceZoneGDPR	Yes	No
isSourceHostNameGDPR	Yes	No
isDestinationMacGDPR	Yes	No
isDestinationAddressGDPR	Yes	CASE WHEN v6_ntoa(field['default_secops_ adm.events.destinationAddressBin']) 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
isDestinationZoneGDPR	Yes	No
isDestinationHostNameGDPR	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
isSourceMacGDPR	Yes	No
isSourceAddressGDPR	Yes	CASE WHEN v6_ntoa(field['default_secops_ adm.events.sourceAddressBin']) 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
isSourceZoneGDPR	Yes	CASE WHEN default_secops_adm.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
isSourceHostNameGDPR	Yes	No
isDestinationMacGDPR	Yes	No
isDestinationAddressGDPR	Yes	CASE WHEN v6_ntoa(field['default_secops_ adm.events.destinationAddressBin']) 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
isDestinationZoneGDPR	Yes	CASE WHEN default_secops_adm.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
isDestinationHostNameGDPR	Yes	No

- Agent Zone Resource Type

By default, the field values below are equal to **No**. If you want to bring additional data from additional connectors, modify the values.

Defines Agent Zones	isAgentZoneGDPR
	isAgentAddressGDPR

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:

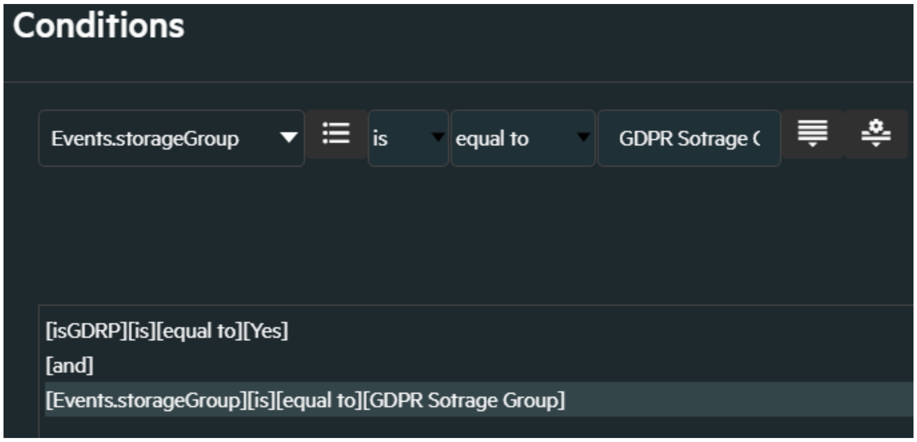
Field	Old Value	New Value
isAgentAddressGDPR	No	No
isAgentZoneGDPR	No	CASE WHEN default_secops_adm.events.agentZoneURI IN ('/All Zones/ArcSight System/Public Address Space Zones/ARIN/142.0.0.0-144.255.255.255 (ARIN)') THEN 'Yes 'Else 'No' END

- Adding Specific Storage Groups to Worksheets

  If you want your reports and dashboards to work against a specific storage group, you can add it to the relevant worksheet.

  For Example:

  The image below displays a GDPR worksheet working against a storage group named GDPR Storage Group.



[isGDRP][is][equal to][Yes]
[and]
[Events.storageGroup][is][equal to][GDPR Sotrage Group]

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.

- "Issue with Report Formatting " below
- "Issue with the After Hours Access Activity on GDPR Systems Summary Report" below

Issue 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)

Issue with the After Hours Access Activity on GDPR Systems Summary Report

Issue: When using running the **After Hours Access Activity on GDPR Systems Summary** report, when including a longer time frame, the report fails to run.

Workaround: Remove the Day of the Week variable by right-clicking on the report and selecting **Edit Table** Then, right-click on the **dayOfWeek** variable and select **Remove**. (OCTCR33I186011)

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 GDPR 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