Solutions Guide for ArcSight Compliance Pack GDRP

Tuesday, December 7, 2021

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

The European Union (EU) adopted the General Data Protection Regulation (GDPR) to ensure that businesses and organizations protect the data privacy and security of individuals. If your enterprise processes the personal data of EU citizen or residents or offers goods and services to such individuals, then you must comply with the GDPR.

- "What's New" on the next page
- "Adding and Removing the Compliance Pack" on page 5
- "Specifying Your GDPR Assets" on page 6
- "Viewing Report and Dashboard Details" on page 9
- "Known Issues" on page 10

What's New

The following sections outline the key features and functions provided in this release.

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.

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.

Reports and Dashboards

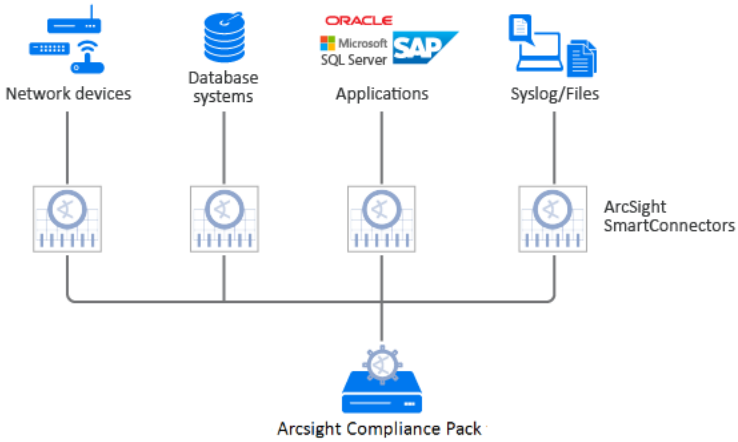
This compliance pack provides a library of reports and dashboards to help you to address the following objectives.

Compliance Reporting	Supports the presentation of requirements to internal and external audit teams, as well as upper management.
Real-time Detection of Compliance Breaches	Pro-actively and Actionable Dashboards addressing compliance violations.
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.

Architecture

The ArcSight Compliance Pack for GDPR 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. This GDPR solution 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.

- 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 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 **GDPR**, 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 **GDPR**, right-click, and select **Remove**.

   A confirmation pop-up window displays.
7. Click **OK**.

Removing Logical Model Content

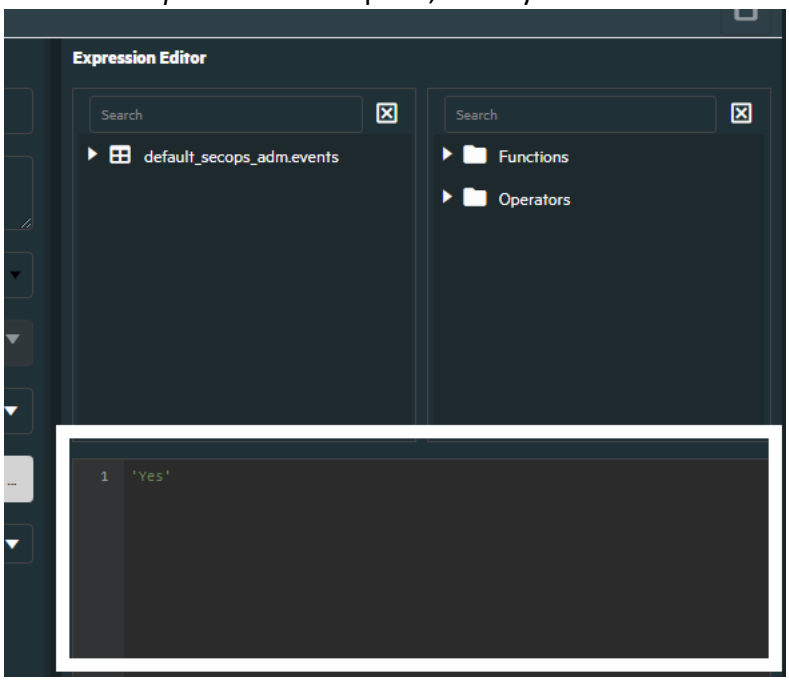
1. Select **Reports** > **Portal**.
2. Click the **Data** icon.
3. Select **Data Source** > **Database** > **Events**.
4. Select the content, such as **GDPR**, right-click, and select **Delete**.

   A confirmation pop-up window displays.
5. 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 the *Events* drop-down list and select the value you want to modify.
5. Below the *Expression Editor* pane, modify the value.



6. Click the **save**  icon.

For more examples, see:

- 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:

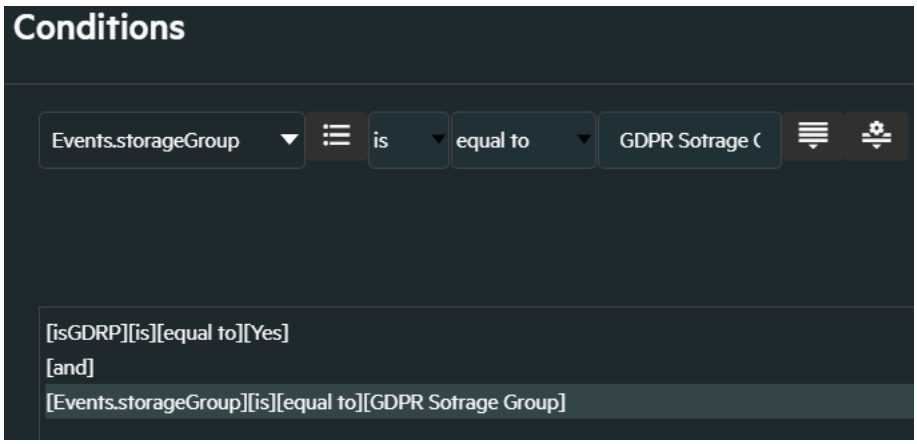
Field	Old Value	New Value
isAgentAddressGDPR	No	No
isAgentZoneGDPR	No	CASE WHEN default_secops_adm.events.agentZoneURI IN ('/All Zones/ArcSight System/Public Address Space Zones/ARIN/142.0.0.0-144.255.255.255 (ARIN)') THEN 'Yes 'Else 'No' END

- 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.



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.

- "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

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