Solutions Guide for ArcSight Compliance Pack IT Governance

Monday, August 9, 2021

Version 1.0.0.0

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

We support IT Gov standards ISO 27002-2013. 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*.

ArcSight Compliance Pack IT Governance leverages the ArcSight litigation-quality, long-term repository of log and event data to facilitate IT Governance compliance with the IT ISO 27002:2013 and reporting of high, medium, and low-risk activity standards using ArcSight reporting.

What's New

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

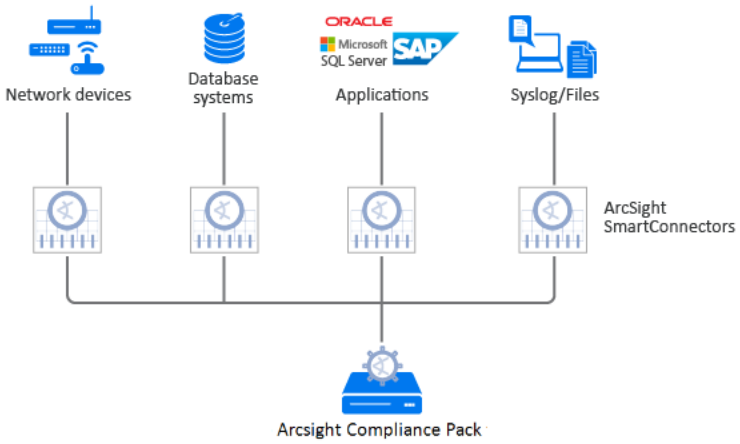
This compliance pack facilitates compliance by providing detailed reports that help evaluate risk and provide comprehensive reporting of high and low-risk activity.

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.

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.

- 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

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

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 **ITGov**, 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 **ITGov**, 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 **ITGov**, right-click, and select **Delete**.

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

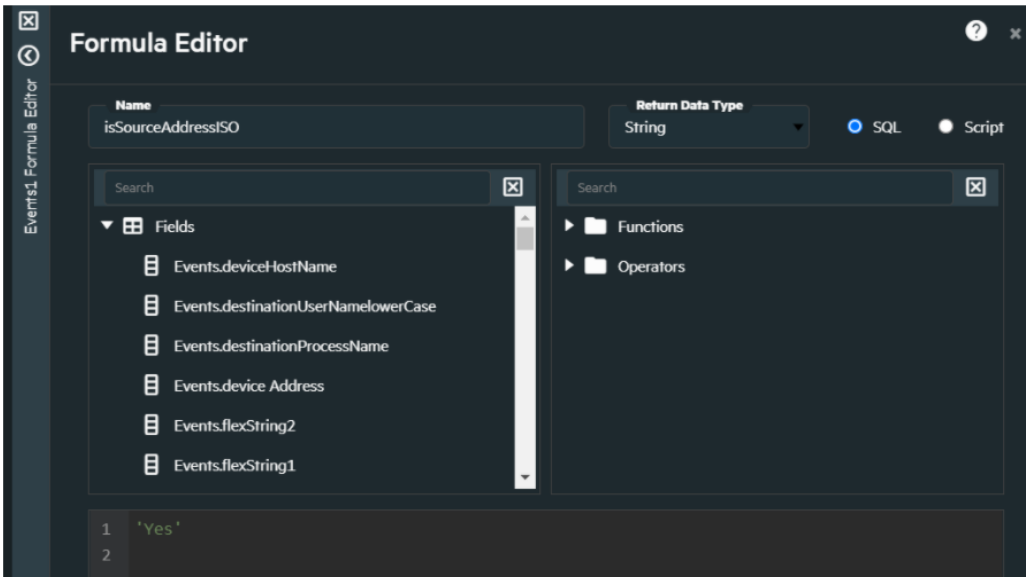
Specifying Your IT Governance Assets

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

1. Select **Reports** > **Portal**.
2. Click the **Data**  icon.

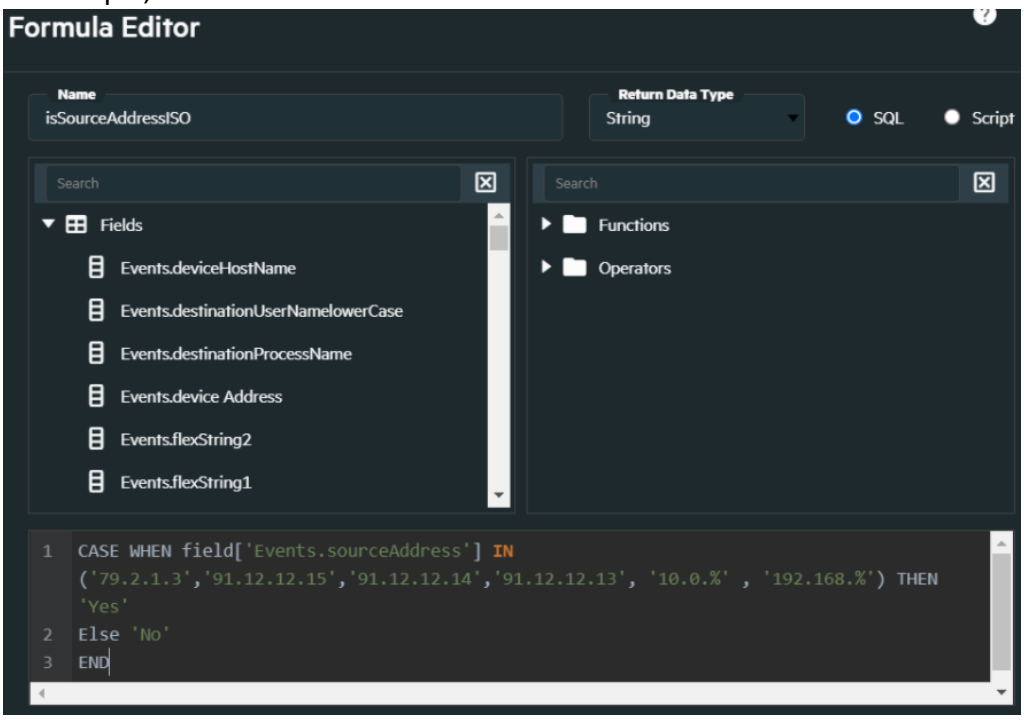
3. In the navigation pane, expand **Data Worksheet** > **Standard Content** > **ITGov** > **ISO Systems**.
4. Click the worksheet to open. Multiple fields and variables display in the lower pane.
5. To define the assets for this compliance pack, select the variable to modify, and then click the **formula** icon.

   The *Formula Editor* pop-up displays.



6. Modify the formula to add the case condition.

   For example, source IP address is shown below.



For more examples, see:

- 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**, and then click the **save** icon.

Preserving Your IT Governance Assets

This section describes how to preserve your IT Governance assets should you need to re-import the compliance pack. If you do not back up your assets, all of the content you added will be overwritten with a Yes value. Hence, its always a best practice to backup your assets.

1. Select **Reports** > **Content**.
2. In the navigation pane, expand **Data Worksheets** > **Standard Content** > **ITGov**.
3. Select the worksheet to export.
4. Click the **Export Asset** icon.
5. Type a zip file name for the asset.
6. Click **Export**.

Viewing Report Details

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

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.

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

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