

Solutions Guide for ArcSight Compliance Insight Package for SOX

Tuesday, December 7, 2021

*You must have **ArcSight Recon 1.4** to use this compliance package.*

The Sarbanes-Oxley Act (SOX) is a United States federal law that was enacted in 2002. The stated purpose of the law is to protect investors by improving the accuracy and reliability of corporate disclosures made pursuant to the securities laws and for other purposes.

- [What's New](#)
- [Adding and Removing the Compliance Pack](#)
- [Specifying Your SOX Assets](#)
- [Viewing Report and Dashboard Details](#)

What's New

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

Section 404 (Management Assessment of Internal Controls) of the Sarbanes-Oxley Act (SOX) states that a corporation must assess the effectiveness of its internal controls and report this assessment annually to the Securities and Exchange Commission. An outside auditing firm must also review and judge the assessment.

The SOX Auditing Standard No. 2, published by the Public Company Accounting Oversight Board (PCAOB), further mandates that organizations and the parties who audit them assess “control risk” in order to determine the effectiveness of internal controls.

These regulations do not describe exactly how to demonstrate the effectiveness of internal controls. The ArcSight Compliance Insight Package for SOX is based on ISO27002:2013, which is the clearly-defined industry standard and accepted globally.

The ArcSight Compliance Insight Package for SOX is a package of reports and dashboards that assist you in complying with SOX requirements. This compliance package 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.

Reports and Dashboards

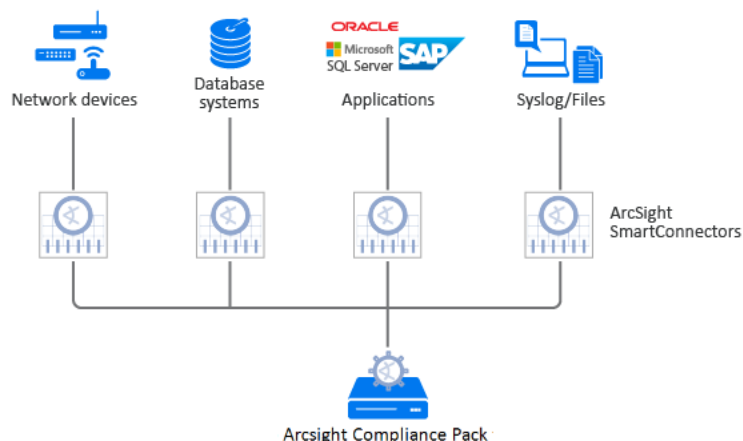
This compliance package provides a library of reports and dashboards to help you to address the following objectives.

Compliance Reporting	Supports the presentation of requirements to internal and external audit teams, as well as upper management.
Real-time Detection of Compliance Breaches	Includes Actionable Dashboards for addressing compliance violations.
Security Best Practices	Helps implement, monitor, and manage a best practices approach to information security management, as well as ensure that SOX security controls are in place and enforced.
Harmful User and Machine Monitoring	Tracks potentially harmful users and machines.
Visualizing Security Events	Displays security events graphically, which allows analysts to quickly analyze situations.
Vulnerabilities and Configuration Changes Monitoring	Tracks vulnerabilities and configuration changes on SOX systems.

Architecture

The ArcSight Compliance Insight Package for SOX operates 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 package operates on events received from devices on the network in CEF. This SOX 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 can generate events used by the compliance package.

- 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 Data Compliance Content folder.


Removing Reports Content

1. Select **Reports > Portal**.
2. Select **Repository > Data Compliance Content**.
3. Select the content, such as **SOX**, 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 > Data Compliance Content**.
6. Select the content, such as **SOX**, right-click, and select **Remove**.
A confirmation pop-up window displays.
7. Click **OK**.

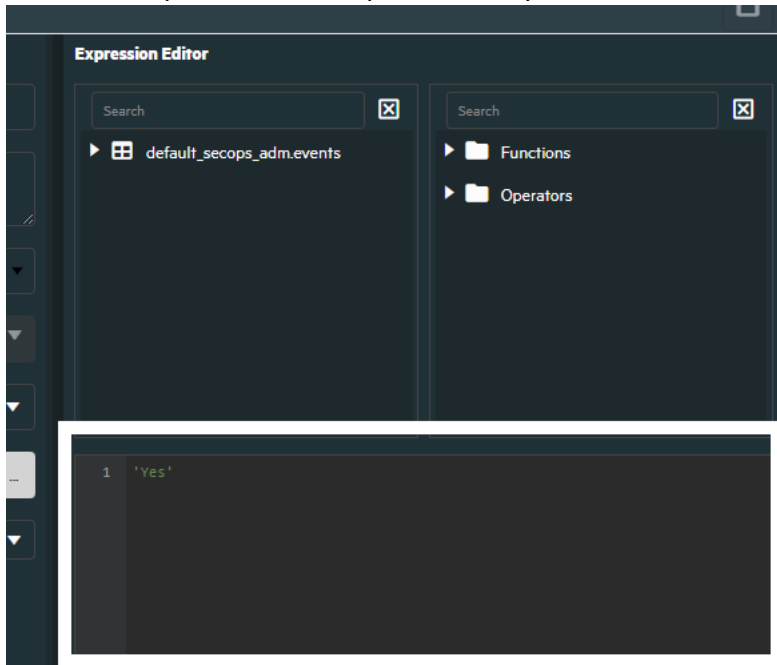
Removing Logical Model Content

1. Select **Reports > Portal**.
2. Click the **Data**  icon.
3. Select **Data Source > Database > Events**.
4. Select the content, such as **SOX**, right-click, and select **Delete**.
A confirmation pop-up window displays.
5. Click **OK**.

Specifying Your SOX 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 > SOX**.
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.

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 type expressions return **Yes** for your asset list.

Defines MAC Addresses	isSourceMacSOX
	isDestinationMacSOX
Defines IP Addresses	IsSourceAddressSOX
	IsDestinationAddressSOX
Defines SOX Host Names	isSourceHostNameSOX
	isDestinationHostNameSOX
Defines SOX Zones	IsSourceZoneSOX
	IsDestinationZoneSOX

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
isSourceMacSOX	Yes	No
IsSourceAddressSOX	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
IsSourceZoneSOX	Yes	No
isSourceHostNameSOX	Yes	No
isDestinationMacSOX	Yes	No
IsDestinationAddressSOX	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
IsDestinationZoneSOX	Yes	No
isDestinationHostNameSOX	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
isSourceMacSOX	Yes	No
isSourceAddressSOX	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
isSourceZoneSOX	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
isSourceHostNameSOX	Yes	No
isDestinationMacSOX	Yes	No
isDestinationAddressSOX	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
isDestinationZoneSOX	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
isDestinationHostNameSOX	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	isAgentZoneSOX
	isAgentAddressSOX

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:

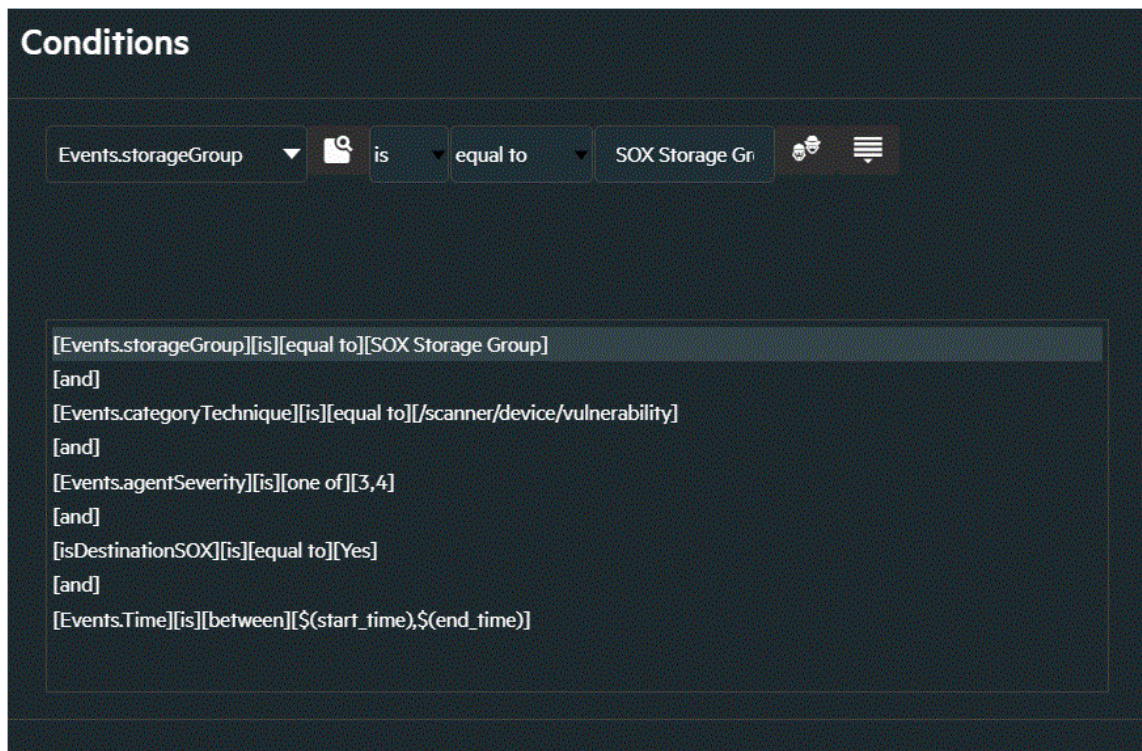
Field	Old Value	New Value
isAgentAddressSOX	No	No
isAgentZoneSOX	No	CASE WHEN default_secops_adm.events.agentZoneURI IN ('/All Zones/ArcSight System/Public Address Space Zones/ARIN/142.0.0.0-144.255.255.255 (ARIN)') THEN 'Yes 'Else 'No' END


- 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 SOX worksheet working against a storage group named SOX 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](#).

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.