Micro Focus Security ArcSight Logger CIP for SOX

Software Version: 4.02

Solutions Guide

Document Release Date: June, 2018
Software Release Date: June, 2018

Legal Notices

Warranty

The only warranties for products and services of Micro Focus and its affiliates and licensors (“Micro Focus”) 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. The information contained herein is subject to change without notice.

Restricted Rights Legend

Confidential computer software. Except as specifically indicated otherwise, a valid license from Micro Focus is required for possession, use or copying. Consistent with FAR 12.211 and 12.212, Commercial Computer Software, Computer Software Documentation, and Technical Data for Commercial Items are licensed to the U.S. Government under vendor's standard commercial license.

Copyright Notice

Trademark Notices

Adobe™ is a trademark of Adobe Systems Incorporated.

Microsoft® and Windows® are U.S. registered trademarks of Microsoft Corporation.

UNIX® is a registered trademark of The Open Group.

Support

Contact Information

Phone	A list of phone numbers is available on the Technical Support Page: https://softwaresupport.softwaregrp.com/support-contact-information
Support Web Site	https://softwaresupport.softwaregrp.com/
ArcSight Product Documentation	https://community.softwaregrp.com/t5/ArcSight-Product-Documentation/ct-p/productdocs

Contents

Chapter 1: Overview 5
About ArcSight Logger 5
Sarbanes-Oxley Act and Security Monitoring Requirements 5
Architecture of Logger CIP for SOX 6
How the Logger CIP for SOX Identifies SOX-Related Events 7
About the Logger CIP for SOX Reports 8
Anatomy of a Report 8

Chapter 2: Deployment and Configuration 10
Before Deploying 10
Verify the Software Logger Version 10
Verify the Logger Appliance L7700 Version 11
Supported Devices 12
Connectors Needed for Non-CEF Devices 21
Deploy Logger CIP for SOX 21
Deploy Logger CIP for SOX on Software Logger or Logger Appliance L8000 21
Deploy Logger CIP for SOX on the Logger Appliance L7700 22
Verify Logger CIP for SOX Content 24
Uninstall Logger CIP for SOX 25

Chapter 3: Configure Logger CIP for SOX 28
Identify SOX-Related Devices 28
Configure Reports with Site-Specific Data 31
Providing Site-Specific Data for Reports Using Parameters 31
Providing Site-Specific Data for Reports Requiring Customization 33
Run a Logger CIP for SOX Report 33
Schedule a Logger CIP for SOX Report 36

Chapter 4: Logger CIP for SOX Contents 38
Parameters 38
adminUsers 38
allowedReports 39

databaseAdminAccounts ... 39
databaseAdminUsers ... 39
destinationUserName ... 40
developmentNetwork ... 40
internalNetwork ... 40
productionNetwork ... 41
testingNetwork ... 41
thirdPartyNetwork ... 42
Reports and Queries ... 42
ISO 4: Risk Assessment and Treatment ... 43
ISO 5: Security Policy ... 43
ISO 6: Organization of Information Security ... 44
ISO 7: Asset Management ... 46
ISO 8: Human Resources Security ... 46
ISO 9: Physical and Environmental Security ... 47
ISO 10: Communications and Operations Management ... 48
ISO 11: Access Control ... 53
ISO 12: Information System Acquisition Development and Maintenance ... 57
ISO 13: Information Security Incident Management ... 59
ISO 14: Business Continuity Management ... 61
ISO 15: Compliance ... 61

Send Documentation Feedback ... 64

Chapter 1: Overview

ArcSight Logger Compliance Insight Package for Sarbanes-Oxley (Logger CIP for SOX) is a package of coordinated reports that support Sarbanes-Oxley security monitoring requirements as described in this section. Logger CIP for SOX is a stand-alone package that is installed on ArcSight Logger.

Topics in this section:

- "About ArcSight Logger" below
- "Sarbanes-Oxley Act and Security Monitoring Requirements" below
- "Logger CIP for SOX" on page 1
- "Architecture of Logger CIP for SOX" on the next page
- "About the Logger CIP for SOX Reports" on page 8

About ArcSight Logger

ArcSight Logger is a scalable, high performance log management platform for collection, cost-effective storage, and analysis of all log data across the enterprise for use cases ranging from security and compliance to IT operations and networking.

ArcSight Logger is optimized for extremely high event throughout. An event is a time-stamped text message, either a syslog message sent by a host or a line appended to a log file. ArcSight Logger receives and stores events, supports search and retrieval, and can optionally forward selected events to any syslog-ready device.

For more about ArcSight Logger, see the *ArcSight Logger Administrator's Guide*.

Sarbanes-Oxley Act and Security Monitoring Requirements

Congress passed the Sarbanes-Oxley Act in 2002 to help restore investor confidence and deter corporate fraud. Since its passage, the law has had tremendous impact on the way organizations approach security and compliance management. As a result of sections 302 and 404, management is now held accountable for the implementation, assessment and effectiveness of an internal control framework for financial reporting.

Sarbanes-Oxley (SOX) compliance includes the requirement to consolidate and review log activity for all in-scope systems and devices. These log review controls include

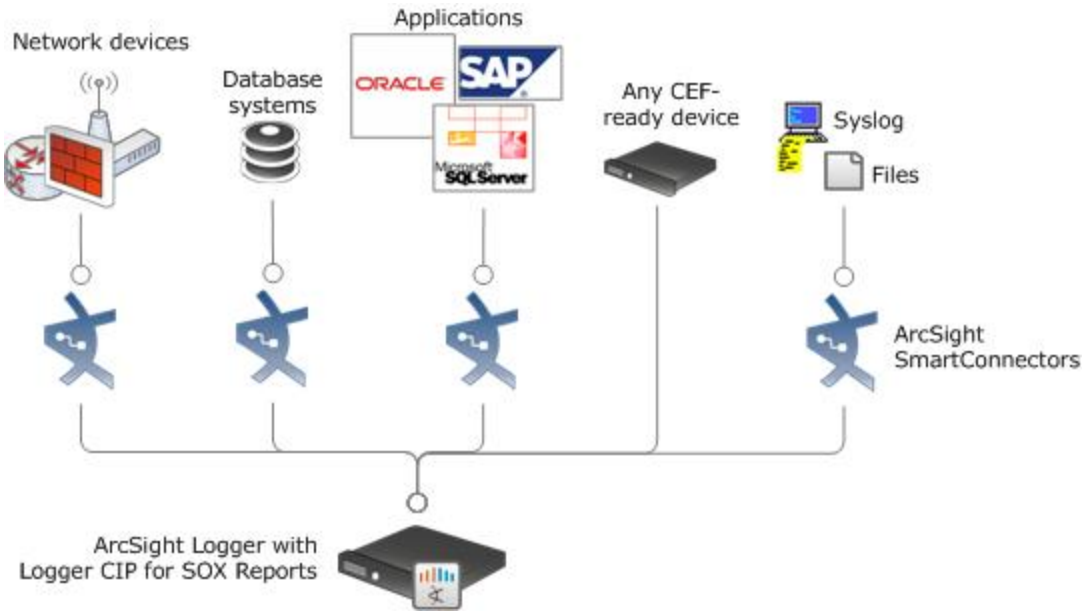
monitoring of change requests and authorization, user account authorizations and application and system access controls.

Long-term data retention requirements to support Sarbanes-Oxley necessitate a cost-effective means to collect and store audit-relevant log data from all in-scope systems, applications and devices. Given the wide variety of log formats and ever-growing volume of logs generated, enterprises need a log management infrastructure that can support the rapid collection of large log volumes. Aggregated log information also has to be quickly accessible to support compliance and audit requests across the entire IT infrastructure.

Architecture of Logger CIP for SOX

The reports contained in Logger CIP for SOX work on events in Common Event Format (CEF) format, 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 format, or they can come from any network device whose events are first run through an ArcSight SmartConnector.



For more about CEF events and how they are used by Logger, see the *ArcSight Common Event Format (CEF) Implementation Guide* for your type of deployment.

How the Logger CIP for SOX Identifies SOX-Related Events

By design, the reports in Logger CIP for SOX are ready to operate on events from all devices reporting to ArcSight Logger. If all the devices in your environment are subject to SOX compliance, then it is not necessary to configure any methods to focus the Logger CIP for SOX reports on specific systems.

If only a segment of your systems are subject to SOX compliance, however, and you wish to focus the results of the Logger CIP for SOX reports to those systems, there are several ways to select events from only those devices:

- Write a SOX report category filter that specifies which device's events you want to evaluate at report run time; or
- Create a SOX-related device group that you would assign your SOX-relevant devices to and specify it as a parameter when you run the report; or
- Create a SOX-related storage group (or select an existing one) that you want the reports to evaluate at run time; or
- Select specific devices individually at report run-time

Which method you choose depends on how your environment is set up, and how you want to organize your Sarbanes-Oxley compliance program. Each method is outlined below. Methods can also be combined. Details and instructions about how to use each method appear in "Identify SOX-Related Devices" on page 28.

SOX Report Category Filter

With ArcSight Logger v2.0 Patch 1, you can use a report category filter to focus reports on SOX-related devices. The report category filter is applied to the whole SOX category, and focuses each report on any parameter available during query building, such as a device group or specific devices.

For instructions about how to write a SOX-specific report category filter, see "Create SOX Report Category Filter(s)" on page 29.

For instructions about how to run a report, see "Run a Logger CIP for SOX Report" on page 33.

SOX Device Group

ArcSight Logger v2.0 provides a method for organizing the devices that report to Logger in containers called device groups. Using this method, you would classify your SOX-related assets in a SOX device group, and specify that device group as a parameter when you run the report.

For instructions about how to create a SOX device group and use it to classify your SOX-related devices, see "Classify SOX-Related Devices in SOX Device Group" on page 29.

For instructions about how to run a report, see "Run a Logger CIP for SOX Report" on page 33.

Storage Group

Storage groups are a method for defining different retention policies for events of different types. Storage groups are created during ArcSight Logger initialization. If you have a storage group created that corresponds with your systems that are subject to SOX compliance, you can specify that storage group as a parameter at report run time.

For instructions about how to run a report using this method, see "Run a Logger CIP for SOX Report" on page 33.

Specific SOX-Related Devices

Another option for focusing Logger CIP for SOX reports on SOX-related devices is to select individual devices as parameters at report run time. For instructions, see "Select Specific Devices Individually" on page 31.

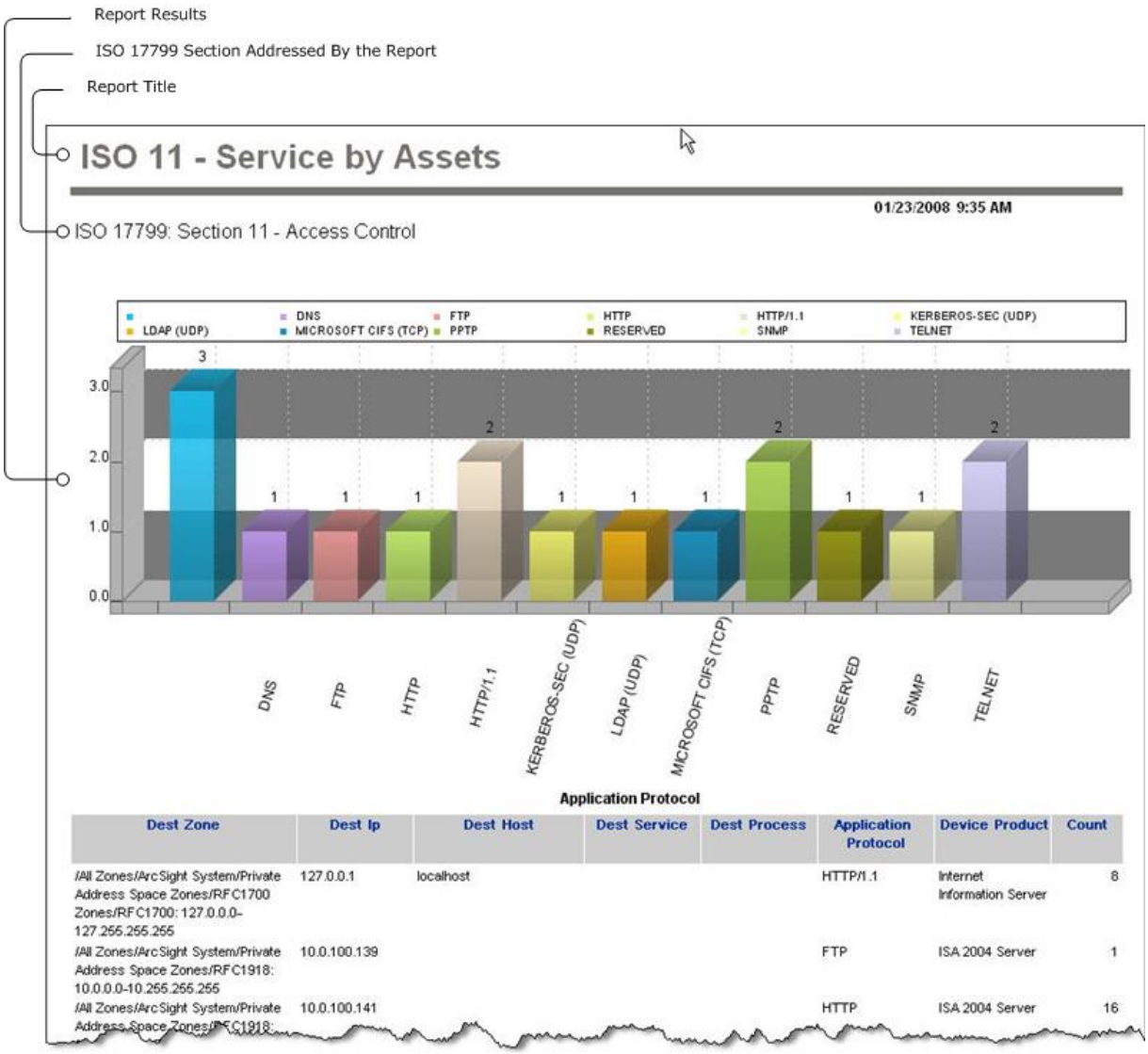
For instructions about how to run a report using this method, see "Run a Logger CIP for SOX Report" on page 33.

About the Logger CIP for SOX Reports

Logger CIP for SOX reports each have an associated SQL query that is evaluated against the set of events saved on the ArcSight Logger. Some queries require that you customize the SQL code in the query to reflect the site-specific data for your environment, while some other queries require that you provide site-specific data using parameters. Some queries do not need to be customized. For more information, see "Configure Reports with Site-Specific Data" on page 31.

Anatomy of a Report

Each Logger CIP for SOX report lists the ISO 17799 section the report addresses in addition to the detailed report results, as shown:



For details about how to run reports, see "Run a Logger CIP for SOX Report" on page 33.

Chapter 2: Deployment and Configuration

This section describes how to deploy Logger CIP for SOX v4.02, and how to configure it to work in your environment.

Topics in this section:

- "Before Deploying" below
- "Deploy Logger CIP for SOX" on page 21
- "Verify Logger CIP for SOX Content" on page 24
- "Uninstall Logger CIP for SOX" on page 25

Before Deploying

This section describes how to deploy Logger CIP for SOX 4.02, and how to configure it to work in your environment.

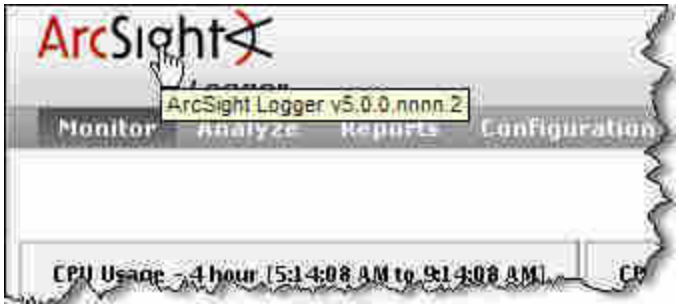
- "Verify the Software Logger Version" below–Software Logger is the downloadable version of Logger installed on your hardware.
- "Verify the Logger Appliance L7700 Version" on the next page–Logger Appliance is the preconfigured hardware version of Logger.

Verify the Software Logger Version

Before deploying Logger CIP for SOX 4.02, verify that the software Logger is installed and running ArcSight Logger 5.0 Patch 1 or greater.

To verify that the Software Logger is running ArcSight Logger v6.6 Patch 1 or greater:

1. Log into the Logger user interface of the software Logger. The Logger user interface is a web browser application. For detailed instructions and browser requirements, see the "Using the User Interface" topic of the *ArcSight Logger Administrator's Guide* for 6.6.
2. Place the cursor over the ArcSight logo located at the top-left corner of the panel as shown:



3. Verify that the version level is 5.0 Patch 2 or greater. For example, the string: `5.0.0.nnnn.2` indicates the software Logger is running ArcSight Logger v5.0 Patch 2, where `nnnn` is the 4 character build number.

Note: If the version string does not appear, move the cursor away from the logo and then back onto the logo.

Verify the Logger Appliance L7700 Version

Before deploying Logger CIP for SOX 4.02, verify that the Logger appliance L7700 is running ArcSight Logger 2.0 Patch 1 (2.0.0.2127) or greater.

To verify that the Logger Appliance L7700 is running ArcSight Logger v2.0 Patch 1 or greater:

1. Log into the Logger user interface. The Logger user interface is a web browser application. For detailed instructions and browser requirements, see the Using the User Interface chapter of the *ArcSight Logger Administrator's Guide* for 5.0.
2. From the Logger navigation bar, click **Analyze**.
3. Place the cursor over the ArcSight logo located at the top-left corner of the panel as shown:

4. Verify that the version level is 2.0.0.2127 or greater. If the version level equals 2.0.0.2127, the Logger appliance L7700 is running ArcSight Logger v2.0 Patch 1.

Note: If the version string does not appear, move the cursor away from the logo and then back onto the logo.

Supported Devices

The device groups listed in this topic are capable of generating events to populate the marked reports. However, it is possible that not all products in the device group category will generate the required events. For example, CheckPoint NG firewalls may generate events that will populate certain reports, whereas Cisco Pix will not, even though they are both under the firewall category.

It is possible that even though a device is capable of generating certain event types, it will not do so frequently, and it may take a long time for the event to appear.

Content in Logger CIP for SOX reports usually depends on more than just the generating device. Other factors such as zones, user names, IP addresses and so on, are part of the variety of factors that the content depends on.

For each Logger CIP for SOX report, the device categories in the matrix are not the only ones that are capable of generating events that will populate it, but are the major and most likely sources for such events.

Supported Devices

Report Name	IDS/IPS	NBAD	DB	OS	FW	VPN	VA	IDM	PM	NE	CS, WF	AV	W	APP	PSS
ISO 4 - High Risk Events	X	X	X	X	X	X		X	X	X	X	X	X		
ISO 4 - High Risk Events by Zone	X	X	X	X	X	X		X	X	X	X	X	X		
ISO 4 - Top 10 High Risk Events	X	X	X	X	X	X		X	X	X	X	X	X		
ISO 5 - Machines Conducting Policy Breaches	X			X	X	X		X	X	X	X	X	X		
ISO 5 - New Hosts		X													
ISO 5 - New Services		X													
ISO 5 - Top 20 Policy Breach Events	X			X	X	X		X	X	X	X	X	X		
ISO 6 - Administrative Logins and Logouts from Third-Party Hosts	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X

Supported Devices, continued

Report Name	IDS/IPS	NBAD	DB	OS	FW	VPN	VA	IDM	PM	NE	CS, WF	AV	W	APP	PSS
ISO 6 - Administrative Logins and Logouts to Third-Party Hosts	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X
ISO 6 - Attacks from Third-Party Systems	X	X			X	X		X			X	X	X	X	X
ISO 6 - Attacks on Third-Party Systems	X	X			X	X		X			X	X	X	X	X
ISO 6 - Compromised Third-Party Systems	X	X						X					X		
ISO 6 - Failed Admin Logins from Third-Party Systems	X	X	X	X	X	X	X	X	X	X	X	X	X	X	
ISO 6 - Failed Admin Logins to Third-Party Systems	X	X	X	X	X	X	X	X	X	X	X	X	X	X	
ISO 6 - Failed User Logins from Third-Party Systems	X	X	X	X	X	X	X	X	X	X	X	X	X	X	
ISO 6 - Failed User Logins to Third-Party Systems	X	X	X	X	X	X	X	X	X	X	X	X	X	X	
ISO 6 - File Activity on Third-Party Systems				X											
ISO 6 - File Creations on Third-Party Systems				X											
ISO 6 - File Deletions on Third-Party Systems				X											
ISO 6 - File Modifications on Third-Party Systems				X											
ISO 6 - Policy Violations from Third-Party Systems	X			X	X	X		X	X	X	X	X	X		
ISO 6 - Services Accessed by Third-Party Systems					X										

Supported Devices, continued

Report Name	IDS/IPS	NBAD	DB	OS	FW	VPN	VA	IDM	PM	NE	CS, WF	AV	W	APP	PSS
ISO 6 - Third-Party Systems Accessed	X	X	X	X	X	X	X	X		X	X	X	X	X	
ISO 6 - User Logins and Logouts from Third-Party Systems	X	X	X	X	X	X	X	X	X	X	X	X	X	X	
ISO 6 - User Logins and Logouts to Third-Party Systems	X	X	X	X	X	X	X	X	X	X	X	X	X	X	
ISO 7 - Network Active Assets	X	X	X	X	X	X	X	X	X	X	X	X	X	X	
ISO 8 - Internet Activity per Device per Machine	X			X	X				X	X	X		X		
ISO 8 - Internet Activity per Device per User	X			X	X				X	X	X		X		
ISO 8 - Summary of Suspicious Activities per User	X	X		X	X	X			X	X	X	X	X	X	
ISO 9 - Failed Building Access Attempts															X
ISO 9 - Successful Building Access Attempts															X
ISO 10 - Account Lockouts by System				X											
ISO 10 - Account Lockouts by User				X											
ISO 10 - Administrative Logins and Logouts	X	X	X	X	X	X	X	X		X	X	X	X	X	
ISO 10 - Administrator Actions	X	X	X	X	X	X	X	X		X	X	X	X	X	
ISO 10 - Application Configuration Modification	X		X	X	X			X	X	X	X	X		X	
ISO 10 - Attacks - Development to Production	X	X		X	X		X			X	X	X	X	X	

Supported Devices, continued

Report Name	IDS/IPS	NBAD	DB	OS	FW	VPN	VA	IDM	PM	NE	CS, WF	AV	W	APP	PSS
ISO 10 - Attacks - Production to Development	X	X		X	X		X			X	X	X	X	X	
ISO 10-Audit Log Cleared	X	X		X	X										
ISO 10 - Changes to Development Network Machines	X		X	X	X	X	X	X	X	X	X	X	X	X	
ISO 10 - Changes to Third-Party Resources	X		X	X	X	X	X	X	X	X	X	X	X	X	
ISO 10 - Database Access - All	X		X						X						
ISO 10 - Database Access - Failed	X		X						X						
ISO 10 - Development Network Not Segregated	X	X	X	X	X	X			X	X	X		X	X	
ISO 10 - Device Configuration Changes										X					
ISO 10 - Device Logging Review	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X
ISO 10 - Failed Anti-Virus Updates	X											X			
ISO 10 - Fault Logs	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X
ISO 10 - File Integrity Changes	X	X		X	X			X	X	X	X	X		X	
ISO 10 - Firewall Configuration Changes - All					X										
ISO 10 - Firewall Configuration Changes - Successful					X										
ISO 10 - Firewall Open Port Review					X										

Supported Devices, continued

Report Name	IDS/IPS	NBAD	DB	OS	FW	VPN	VA	IDM	PM	NE	CS, WF	AV	W	APP	PSS
ISO 10 - Information Interception Events		X													
ISO 10 - Malicious Code Sources	X	X		X			X				X	X			
ISO 10 - Network Device Configuration Changes - All									X						
ISO 10 - Network Device Configuration Changes - Successful									X						
ISO 10 - Number of Successful Administrative Logins	X	X	X	X	X	X	X	X	X	X	X	X	X	X	
ISO 10 - Number of Successful User Logins	X	X	X	X	X	X	X	X	X	X	X	X	X	X	
ISO 10 - Number of Unsuccessful Administrative Logins	X	X	X	X	X	X	X	X	X	X	X	X	X	X	
ISO 10 - Number of Unsuccessful User Logins	X	X	X	X	X	X	X	X	X	X	X	X	X	X	
ISO 10 - Operating System Configuration Changes				X											
ISO 10 - Production Network Not Segregated	X	X	X	X	X	X			X	X	X		X	X	
ISO 10 - Resource Exhaustion			X	X	X					X					
ISO 10 - Successful Brute Force Logins	X	X													
ISO 10 - System Restarted				X											
ISO 10 - Test Network Not Segregated	X	X	X	X	X	X			X	X	X		X	X	

Supported Devices, continued

Report Name	IDS/IPS	NBAD	DB	OS	FW	VPN	VA	IDM	PM	NE	CS, WF	AV	W	APP	PSS
ISO 10 - Top Unsuccessful Administrative Logins	X	X	X	X	X	X	X	X	X	X	X	X	X	X	
ISO 10 - Top Unsuccessful User Logins	X	X	X	X	X	X	X	X	X	X	X	X	X	X	
ISO 10 - User Logins and Logouts	X	X	X	X	X	X	X	X	X	X	X	X	X	X	
ISO 10 - Virus Summary by Hosts												X			
ISO 10 - Virus Summary by Hosts												X			
ISO 10 - VPN Access Summary						X									
ISO 11 - Account Activity by User	X	X	X	X	X	X	X	X	X	X	X	X	X	X	
ISO 11 - Blocked Firewall Traffic							X								
ISO 11 - Database Privilege Violation			X												
ISO 11 - Default Vendor Account Used	X	X	X	X	X	X	X		X	X	X	X	X		
ISO 11 - Insecure Services	X	X	X	X	X	X	X			X	X		X		
ISO 11 - Login From Multiple IPs - Detail	X	X	X	X	X	X	X	X	X	X	X	X	X	X	
ISO 11 - Login From Multiple IPs - Overview	X	X	X	X	X	X	X	X	X	X	X	X	X	X	
ISO 11 - Multiple User Login - Detail	X	X	X	X	X	X	X	X	X	X	X	X	X	X	
ISO 11 - Multiple User Login - Overview	X	X	X	X	X	X	X	X	X	X	X	X	X	X	
ISO 11 - Network Routing Configuration Changes					X					X					

Supported Devices, continued

Report Name	IDS/IPS	NBAD	DB	OS	FW	VPN	VA	IDM	PM	NE	CS, WF	AV	W	APP	PSS
ISO 11 - Privileged Account Changes - All	X	X	X	X	X	X		X	X	X	X	X	X		
ISO 11 - Privileged Account Changes - Successful	X	X	X	X	X	X		X	X	X	X	X	X		
ISO 11 - Removal of Access Rights	X	X	X	X	X	X		X	X	X	X	X	X		
ISO 11 - Services by Asset	X	X	X	X	X	X	X	X	X	X	X	X	X	X	
ISO 11 - Suspicious Activity in Wireless Network	X	X		X	X	X		X	X	X	X	X	X		
ISO 11 - Systems Accessed as Root or Administrator	X	X	X	X	X	X	X	X	X	X	X	X	X	X	
ISO 11 - Traffic - Inbound Count	X	X		X	X					X	X				
ISO 11 - Traffic - Inbound on Disallowed Ports - All	X	X		X	X					X	X				
ISO 11 - Traffic - Inbound on Disallowed Ports - Successful	X	X		X	X					X	X				
ISO 11 - Traffic Between Zones - Protocols	X	X		X	X					X	X				
ISO 11 - User Account Creation	X	X	X	X	X	X		X	X	X	X	X	X		
ISO 11 - User Account Deletion	X	X	X	X	X	X		X	X	X	X	X	X		
ISO 12 - Changes to Operating Systems				X											
ISO 12 - Exploit of Vulnerabilities	X	X			X				X	X	X	X	X		
ISO 12 - File Changes in Production				X											

Supported Devices, continued

Report Name	IDS/IPS	NBAD	DB	OS	FW	VPN	VA	IDM	PM	NE	CS, WF	AV	W	APP	PSS
ISO 12 - Invalid Certificate	X			X	X	X	X	X		X			X		
ISO 12 - Invalid Data Input	X	X		X	X	X				X				X	
ISO 12 - Software Changes in Production	X		X	X	X	X			X	X		X			
ISO 12 - Vulnerabilities and Misconfigurations							X								
ISO 12 - Vulnerability Scanner Results							X								
ISO 13 - Attack Events - Top 20	X	X		X	X		X			X	X	X	X	X	
ISO 13 - Attacked Hosts - Top 20	X	X		X	X		X			X	X	X	X	X	
ISO 13 - Attackers - Top 20	X	X		X	X		X			X	X	X	X	X	
ISO 13 - Attacks - Hourly Count	X	X		X	X		X			X	X	X	X	X	
ISO 13 - Attacks Targeting Internal Assets - All	X	X		X	X		X			X	X	X	X	X	
ISO 13 - Confidentiality and Integrity Breach Sources - Count	X	X		X	X		X			X	X	X	X	X	
ISO 13 - Covert Channel Activity	X	X										X			
ISO 13 - DoS Sources	X	X			X					X			X		
ISO 13 - Information System Failures	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X
ISO 13 - Internal Reconnaissance - Top 20 Events	X					X		X		X	X		X		
ISO 13 - Internal Reconnaissance - Top 20 Sources	X					X		X		X	X		X		

Supported Devices, continued

Report Name	IDS/IPS	NBAD	DB	OS	FW	VPN	VA	IDM	PM	NE	CS, WF	AV	W	APP	PSS
ISO 13 - Internal Reconnaissance - Top 20 Targets	X					X		X		X	X		X		
ISO 14 - Availability Attacks	X	X			X					X	X		X		
ISO 15-Email Receivers by Amount	X				X						X			X	
ISO 15-Email Receivers by Size	X				X						X			X	
ISO 15-Email Senders by Amount	X				X						X			X	
ISO 15-Email Senders by Size	X				X						X			X	
ISO 15-Information Leaks - Organizational	X	X			X										
ISO 15-Information Leaks - Personal	X	X			X										
ISO 15-Information System Audit Tool Logins	X	X			X										
ISO 15-Largest Emails	X				X						X			X	
ISO 15-Peer To Peer Ports Count	X	X			X			X	X	X			X		
ISO 15-Peer to Peer Sources By Machine-Detail	X	X			X			X	X	X			X		
ISO 15-Peer to Peer Sources By Machine-Overview	X	X			X			X	X	X			X		
ISO 15-Policy Breaches	X			X	X	X		X	X	X	X	X	X		
ISO 15-Possible IPR Violations	X	X							X		X				

Key to Device Type

IDS = Intrusion Detection System	PM = Policy Management
IPS = Intrusion Prevention System	NE = Network Equipment
NBAD = Network Behavior Anomaly Detection	CS, WF = Content Security, Web Filtering
DB = Database	AV = Antivirus
OS = Operating System	W = Wireless
FW = Firewall	APP = Applications
VPN = Virtual Private Network	PSS = Physical Security Systems
VA = Vulnerability Assessment	
IDM = Identity Management	

Connectors Needed for Non-CEF Devices

Logger CIP for SOX reports operate on events from the devices listed in the table in "Supported Devices" on page 12. If these devices in your environment are not already CEF-enabled, you must apply an ArcSight SmartConnector for these devices so that the Logger CIP for SOX reports yield the most accurate results.

Use the supported devices listed in Supported Devices to determine which non-CEF enabled devices in your environment would benefit from the installation of an ArcSight SmartConnector to optimize results from Logger CIP for SOX.

Deploy Logger CIP for SOX

To deploy Logger CIP for SOX v4.02 on an ArcSight Logger, follow the appropriate procedure for your Logger type:

- "Deploy Logger CIP for SOX on Software Logger or Logger Appliance L8000" below—Software Logger is the downloadable version of Logger installed on your hardware.
- "Deploy Logger CIP for SOX on the Logger Appliance L7700" on the next page—Logger Appliance is the preconfigured hardware version of Logger.

Deploy Logger CIP for SOX on Software Logger or Logger Appliance L8000

This section describes how to deploy Logger CIP for SOX v4.02 on the software version of Logger or Logger Appliance L8000.

Note: You must log into software Logger or Logger Appliance L8000 and open the Reports page at least once before installing the Solutions package.

To deploy Logger CIP for SOX v4.02 on the Software Logger or Logger Appliance L8000:

1. On the system running the software Logger or Logger Appliance L8000, log into the system using the same user that you used to install the software version of Logger.
2. Using the log-in credentials supplied to you by ArcSight, download the Logger CIP for SOX BIN file (ArcSight-ComplianceInsightPackage-Logger-SOX.4.02.nnnn.bin where nnnn is the four-digit build number).

   Note: The four-digit build number is specified in the *Release Notes ArcSight Compliance Insight Package SOX 4.02*.
3. Go to the directory that contains the BIN file.
4. Change the permissions of BIN file to be executable:

   `chmod +x ArcSight-ComplianceInsightPackage-Logger-SOX.4.02.nnnn.bin`
5. Run the installer:

   `./ArcSight-ComplianceInsightPackage-Logger-SOX.4.02.nnnn.bin`
6. Follow the instructions provided by the installer. When prompted to choose an installation folder, enter the same directory you specified when you installed the software Logger. For example, if when installing the software Logger you specified the `/opt/logger` directory, specify `/opt/logger` as the installation folder.

   The BIN file installs the SOX reports, parameters, and queries.
7. Verify that the Logger CIP for SOX content is installed. Skip to "Verify Logger CIP for SOX Content" on page 24.

Deploy Logger CIP for SOX on the Logger Appliance L7700

This section describes how to install Logger CIP for SOX v4.02 on a Logger appliance L7700.

Caution: You must log into Logger appliance L7700 and open the Reports page at least once before installing the Solutions package.

To install Logger CIP for SOX v4.02 on a Logger Appliance L7700:

1. Using the log-in credentials supplied to you by ArcSight, download the Logger CIP for SOX cab file (`ArcSight-ComplianceInsightPackage-Logger-SOX.4.01.nnnn.cab`, where `nnnn` is the four-digit build number) from the support site to a local computer to which ArcSight Logger has access.

   Note: The four-digit build number is specified in the *Release Notes ArcSight Compliance Insight Package SOX 4.02*.

2. Log into the Logger user interface. The Logger user interface is a web browser application. For detailed instructions and browser requirements, see the Using the User Interface topic of the *ArcSight Logger Administrator's Guide*.
3. From the Logger navigation bar, click **Reports**.
4. From the left panel menu, select **Administration/Deploy Report Package**.
5. In the `Step 1:(Upload & View Cab Information)` field, specify the reports package file name with its full path. Click **Browse** to locate the CAB file you downloaded at the start of this procedure.
6. Click **Upload** to load the content and prepare it to be deployed.

   The content in the CAB file is uploaded but not deployed. The list of reports to be deployed into the `Sarbanes Oxley` category are displayed. In addition, the query objects and parameters to be deployed are also displayed.

   The system displays status information about the objects in the package being deployed, and a legend with information about each of the components in respective tabs. A green dot next to each item indicates that it is a new object, and the icon indicates that the report is a public report, which will be viewable by all users with the appropriate permissions.

   Note: Overwrite behaviors are determined when a package is created.

   Logger CIP for SOX reports are given full overwrite behaviors, which means if an updated version of a report is installed (with the same name), the old report is automatically overwritten.

7. Optional–If you want to create a log of the deployment process, select the **Create Log File** option. When this option is selected, a log file is generated during the deploy.
8. Click **Deploy** to initiate the deployment process (or click **Cancel** to stop).

   The contents of the CAB file are deployed.
9. Verify that the Logger CIP for SOX content is installed ("Verify Logger CIP for SOX Content" on the next page).

Verify Logger CIP for SOX Content

This section provides steps to verify that the Logger CIP for SOX content is deployed and applies to both the Logger appliance and software Logger.

To verify that the SOX reports, parameters, and queries have been installed:

1. To view the installed reports, select **Reports**.

   In the left panel menu, Logger CIP for SOX reports are listed under `Solution Reports/Sarbanes Oxley`.

   Note: To refresh the left panel menu and view the `Solution Reports/Sarbanes Oxley` reports, click **Configuration** from the Logger navigation bar. and then click **Reports**.

2. Optional–If the Create Log File option was selected before deploying, a log file was generated during the deploy. To view the log, click the **Download Log** button.

Uninstall Logger CIP for SOX

This section provides instructions for uninstalling Logger CIP for SOX. This section is not part of the initial configuration and is provided if you want to uninstall Logger CIP for SOX at a later date. The following process removes each report component individually.

To uninstall Logger CIP for SOX:

1. From the Logger navigation bar, select **Reports**.
2. From the left panel menu, select **Solution Reports/Sarbanes Oxley**.
3. Delete each report in the Sarbanes Oxley category:
   a. Select a Sarbanes Oxley report (for example: ISO 4 - High Risk Events) and click delete () in the far right column.

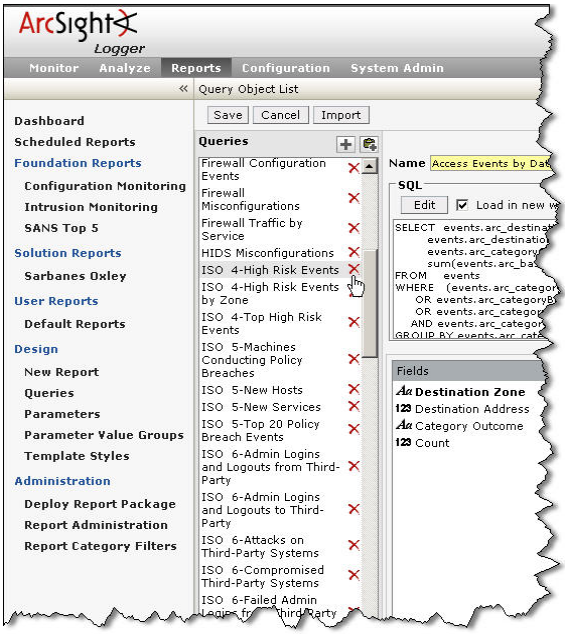
      The system launches a confirmation panel verifying that you want to delete the report.

   b. Click **OK** or press Enter to complete the deletion, or **Cancel** to revert.

      The Sarbanes Oxley reports panel displays the following message confirming the report deletion from the repository at the top of the panel, and the report no longer appears in the right panel.

   c. Repeat the steps to delete reports in Logger CIP for SOX.

      When the process is completed, the Sarbanes Oxley group is empty but still displayed under Solution Groups in the left panel.
4. From the left panel menu, select **Design/Queries**.
5. Delete each Logger CIP for SOX query individually:
   a. In the Queries column, scroll down to the Sarbanes-Oxley queries. (The SOX queries all begin with the prefix: ISO.) Select a Sarbanes-Oxley query (for example: ISO 4 - High Risk Events by Zone) and click delete ().



b. Repeat to delete every Sarbanes-Oxley query.

6. When all Sarbanes-Oxley queries have been deleted, click **Save**.

   At the top of the Query Object List pane, all the deleted report objects (queries) are listed.

7. Optional–You can delete the parameters included with Logger CIP for SOX. Parameters do not affect system performance, but removing them ensures a clean state in case other CAB files with similarly named parameters are imported at a later time:
   a. From the Logger navigation bar, select **Reports**.
   b. From the left panel menu, select **Design/Parameters**.
   c. In the Parameters column, select each of the following Logger CIP for SOX parameters and click delete ( ).

      adminUsers
      allowedPorts
      databaseAdminAccounts
      databaseAdminUsers
      destinationUserName
      developmentNetwork
      internalNetwork
      productionNetwork
      testingNetwork
      thirdPartyNetwork

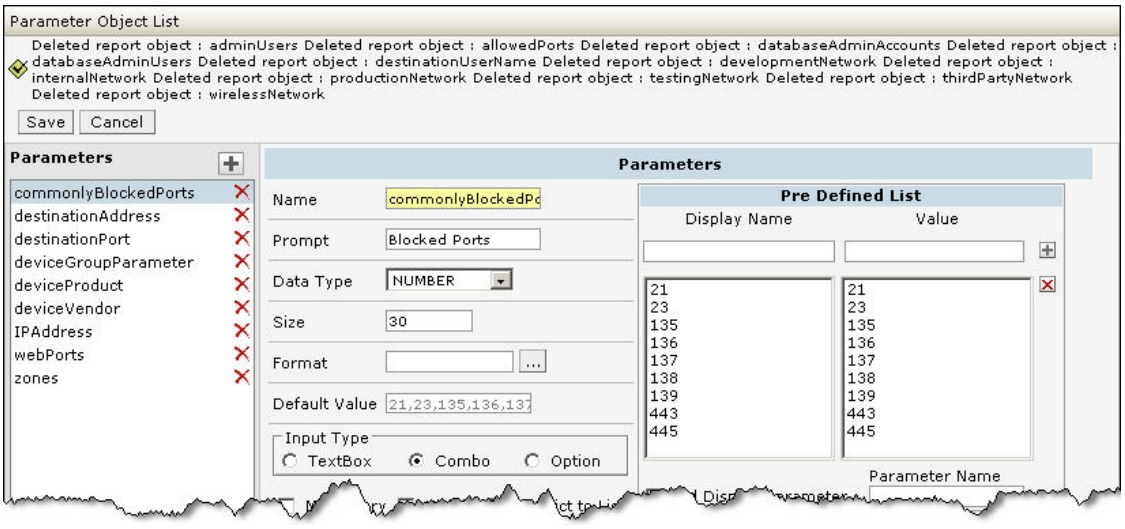
wirelessNetwork

Caution: The following parameters are used by the queries in the Foundation Reports. Do not delete them:

- commonlyBlockedPorts
- destinationAddress
- destinationPort
- destinationGroupParameter
- deviceProduct
- deviceVendor
- IPAddress
- webPorts
- zones

d. Repeat Step c for each of the SOX parameters.

e. When all Sarbanes-Oxley parameters have been deleted, click **Save**. At the top of the Query Object List pane, all the deleted report objects (parameters) are listed:



Chapter 3: Configure Logger CIP for SOX

Although not expressly required, some configuration of Logger CIP for SOX will optimize the results of the reports.

- "Identify SOX-Related Devices" below—If you have devices reporting to ArcSight Logger that are not subject to SOX compliance, follow the instructions in this section to set up device groups and/or filters to identify SOX-related events for Logger CIP for SOX reports.
- "Configure Reports with Site-Specific Data" on page 31—Several Logger CIP for SOX reports refer to site-specific details, such as admin user account names and default ports, which should be configured with details specific to your environment for more accurate results.
- "Schedule a Logger CIP for SOX Report" on page 36—All reports contained in Logger CIP for SOX can be run manually at any time after installation. If you wish to have any of these reports run automatically on a regular schedule, follow the instructions in this section.

For basic instructions about how to use the Logger CIP for SOX reports, see "Run a Logger CIP for SOX Report" on page 33.

Identify SOX-Related Devices

Once Logger CIP for SOX is installed, the reports are ready to run. By design, they will run on all events being processed through ArcSight Logger. If all the devices in your environment are subject to SOX compliance, it is not necessary to create a SOX-specific device group or filter.

However, if only some of your devices are subject to SOX compliance, system performance will improve if you specify which devices the Logger CIP for SOX reports should evaluate.

Tip: Reducing the amount of data a report has to process, translates to better performance.

If only a small subset of the overall data feeding into ArcSight Logger is subject to SOX compliance, using a different storage group for your events from your SOX-related devices will yield the best performance results. See "Designate a Storage Group for SOX-Related Events" on page 30.

As outlined in "How the Logger CIP for SOX Identifies SOX-Related Events" on page 7, there are several methods for identifying SOX-related devices:

- "Classify SOX-Related Devices in SOX Device Group" below
- "Create SOX Report Category Filter(s)" below
- "Designate a Storage Group for SOX-Related Events" on the next page
- "Select Specific Devices Individually" on page 31

Classify SOX-Related Devices in SOX Device Group

1. From the Logger navigation bar, select **Configuration**.
2. From the left panel menu, select **Devices** and select the **Device Groups** tab.
3. Click **Add**.
4. In the Name field, enter a name for the new device group, such as SOX.
5. In the Devices field, click to select devices from the list. Press and hold the Ctrl key when clicking to add additional devices to the selection. To select a range of devices, click to select the first device, then press and hold the Shift key while clicking the last device.

   A Device is a named event source, and is comprised of an IP address (or hostname) and a Receiver name. Devices can be created by autodiscovery or manually. Once a Receiver is enabled and ArcSight Logger starts receiving events, ArcSight Logger automatically creates Devices. This process is called autodiscovery. For more information, see the Devices topic in the *ArcSight Logger Administrator's Guide*.
6. Click **Save** to create the new Device Group, or **Cancel** to abandon it.

For instructions about how to use this device group when running the Logger CIP for SOX reports, see "Run a Logger CIP for SOX Report" on page 33 and use the instructions provided in the procedure called "To Quick Run a Report:" on page 34.

Create SOX Report Category Filter(s)

Report category filters are a feature available with ArcSight Logger v6.6 Patch 1. They enable you to create one or more filters that are applied to a whole report category, in this case, the Sarbanes Oxley report group.

To use this feature to focus the Logger CIP for SOX reports on devices that are subject to SOX compliance, you would create a SOX report category filter to apply a device group to reports that are scheduled to be run automatically.

1. From the Logger navigation bar, select **Configuration**.
2. From the left panel menu, select **Filters** and click **Add**.
3. In the Add Filter panel, enter the information described in the following table:

Field	Description
Name	Enter a name for the Report Category Filter that identifies it with Logger CIP for SOX, such as `SOX Devices`.
Type	From the menu, select Search Group. This makes the filter available to the Report Category Filter panel, and restricts its edit access to those who have administrator privileges.

Query	Use these lines to construct the query that will focus all the reports in the SOX group on the devices subject to SOX compliance, either already grouped in a SOX device group, or individually from a list of devices that report to ArcSight Logger. For example:
	`DeviceGroup=SOX`
	or
	`Device=10.10.10.10`

4. Click **Save**.
5. Assign the SOX search group filter you created at the start of this procedure to the `Sarbanes Oxley` report group:
   a. From the Logger navigation bar, select **Reports**.
   b. From the left panel menu, select **Administration/Report Category Filters**.
   c. In tthe menu associated with the `Sarbanes Oxley` reports group, select the filter you created at the start of this procedure and click **Save**.

For more information about report category filters, see the Filters and Using Report Category Filters topic in the *ArcSight Logger Administrator's Guide*.

For instructions about how to schedule reports, see "Schedule a Logger CIP for SOX Report" on page 36.

Designate a Storage Group for SOX-Related Events

Create a SOX-related storage group (or select an existing one) that you want the reports to evaluate at run time.

- To create a new storage group: To create a new storage group, you must have an unused storage group in reserve from the ArcSight Logger setup process. For details about the setup process, see the Storage Groups topic in the *ArcSight Logger Administrator's Guide*.
- To specify an existing storage group during report run-time: At report run-time, select the Quick Run option. In the Storage Groups field, select the storage group that stores your SOX-related events. For details about running reports, see "Run a Logger CIP for SOX Report" on page 33 and use the instructions provided in the procedure called "To Quick Run a Report:" on page 34.

Select Specific Devices Individually

Another option for focusing the Logger CIP for SOX reports on SOX-related devices is to select individual devices as parameters at report runtime.

At report runtime, select the **Quick Run** option. In the Devices field, select the device(s) that generate your SOX-related events. For details about running reports, see "Run a Logger CIP for SOX Report" on page 33 and use the instructions provided in the procedure called "To Quick Run a Report:" on page 34.

Configure Reports with Site-Specific Data

Some reports require that you provide site-specific data, such as admin account names and default ports. How this data is provided, depends on the report:

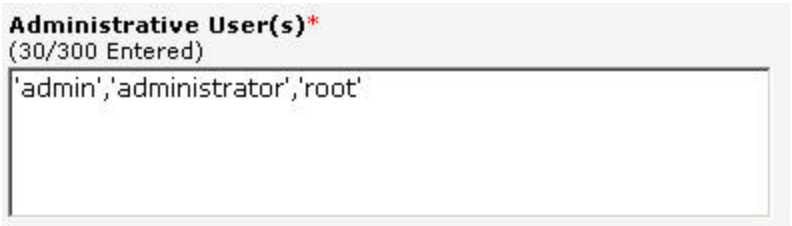
- For some reports, you must provide the site-specific data via parameters–For more information, see "Providing Site-Specific Data for Reports Using Parameters" below.
- For some reports, you must customize the query the report invokes with the site-specific data.–For more information, see "Providing Site-Specific Data for Reports Requiring Customization" on page 33.

Some reports do not need site-specific data or to be customized

The site-specific data that you must provide for each report is described in the Configuration column of the report tables provided in "Reports and Queries" on page 42.

Providing Site-Specific Data for Reports Using Parameters

When some reports are run, you are prompted to provide site-specific information that is passed from the report to the query via parameters. For example, the ISO 11 - Privileged Account Changes - All report invokes the ISO 11-Privileged Account Changed query, which requires Administrative User(s) as input. When the ISO 11 - Privileged Account Changes - All report is run, you are prompted to provide Administrative User(s) as shown in the following figure.



During report runtime, the value in the Administrative User(s) text field is passed to the query via the `adminUsers` parameter. The default value of the parameter is displayed in the text field when the report is run. For this example, the default value of the `adminUsers` parameter is `'admin','administrator','root'`.

To change the value of the parameter, choose one of the following methods:

- When running the report, enter a different value in text field. The new value is used for the single run of the report and is not saved.
- Change the default value of the parameter prior to running the report. For this method, a new value is saved as the default value for parameter. For instructions, see the following procedure.

To change the default value of a parameter:

1. From the Logger navigation bar, select **Reports**.
2. From the left panel menu, select **Design/Parameters**.
3. Select a parameter. For this example, the `adminUsers` parameter is selected.
4. Specify a new default value in **Default Value** text field (for example: **'adm','root'**) and click **Save**.

   The next time a report is run that invokes a query with this parameter, the new default value is displayed in the text field, as shown:

   You can specify one or more user names for this field, for example: **'adm','root'**. Each account name must start and end with a single quote and each user name must be separated by commas.

   When the default value of a parameter is changed, all reports that invoke queries which use this parameter, display the updated default value. For example, all the reports invoking queries that use the `adminUsers` parameter, now display the new default value: **'adm','root'**.

Some parameters expect a regular expression to be defined in the text field. For more information, see Parameters that use Regular Expressions.

For more information about the site-specific data (including the data format), required for each parameter, see the Configuration column of the report tables provided in "Reports and Queries" on page 42.

Parameters that use Regular Expressions

Some parameters expect a regular expression compatible with the MySQL REGEXP operator. Using regular expressions, you can specify a pattern that specifies a range of values. For example you could specify a regular expression that defines a range of addresses. For example, the regular expression: `192\\.168\\.|10\\.` matches either the `192.168.0.0 /16` or the `10.0.0.0 /8` network, while the regular expression: `172\\.168\\.(1[6-9]|2[0-9]|3[0-1])\\.` matches addresses in the range of `172.168.16-31`.

More information about creating regular expressions compatible with MySQL REGEXP operator, see the following URL:

http://dev.mysql.com/doc/refman/5.0/en/regexp.html

The Configuration column of the report tables provided in "Reports and Queries" on page 42 defines which reports expect a regular expression.

Providing Site-Specific Data for Reports Requiring Customization

Some reports require you to customize the SQL code in a query as described in the following procedure.

To modify the SQL code in a query:

1. From the Logger navigation bar, select **Reports**.
2. From the left panel menu, select **Design/Queries**.
3. From the Queries panel, select a query.
4. In the SQL panel, click Edit.
   The SQL editor displays in a separate window.
5. Customize the SQL code.
6. Click **OK** to exit the SQL editor.
7. In the Query Object List panel, click **Save**.

For more information, see the "Setting up Queries" topic in the *ArcSight Logger Administrator's Guide*.

Run a Logger CIP for SOX Report

These instructions describe how to run a Logger CIP for SOX report on demand. For more information, see the Running, Viewing, and Publishing Reportstopic in the *ArcSight*

Logger Administrator's Guide.

To schedule a report, see "Schedule a Logger CIP for SOX Report" on page 36.

1. From the Logger navigation bar, select **Reports**.
2. From the left panel menu, select **Solution Reports/Sarbanes Oxley**.
3. Choose the appropriate procedure to invoke the report:
   - To Quick Run a Report:—Use this procedure if all your devices are subject to SOX compliance, or if you created a special device group for SOX devices (see "Classify SOX-Related Devices in SOX Device Group" on page 29).
   - To Run a Report:—Use this procedure if you want to apply specific filter conditions to this run of the report only.

To Quick Run a Report:

1. From the Logger CIP for SOX reports listed in the right panel, choose the report you want to run, such as ISO 11 - Account Activity by User, and click **Quick Run** ().

2. In the Report Parameters panel, enter the values listed in the following table:

Report Parameters Pane

Field	What to Enter
Any parameter (s) required by the report	At the top of the panel, any parameters required by the query invoked by the report, are displayed. Some reports invoke a query that does not have any parameters and for these reports, no parameters are listed. Enter an appropriate value for each parameter. For more information about the site-specific data (including the data format), required for each parameter, see the report tables provided in"Reports and Queries" on page 42. For example, the ISO 11 - Account Activity by User report invokes the ISO 11-Account Activity by User Name query. The ISO 11-Account Activity by User Name query takes as input the `destinationUserName` parameter. When the ISO 11 - Account Activity by User report is run, you are prompted to provide a User Name value to pass to the query via the `destinationUserName` parameter. For information about providing a default value for a parameter, see "To change the default value of a parameter:" on page 32.
Start	This indicates the start of the time range of events you want the query to evaluate. The default is the time dynamic value `$Now - 2h`, meaning the last two hours of event data starting from the moment you click **Run Report**. • Adjust this dynamic timeframe in increments of hours (h), minutes (m), or days (d). • Uncheck the Dynamic box to specify a particular date and time.
End	This indicates the end of the time range of events you want the query to evaluate. The default is the time dynamic value `$Now`, meaning the moment you click Run Report. • Adjust this dynamic timeframe in increments of hours (h), minutes (m), or days (d). • Uncheck the `Dynamic` box to specify a particular date and time.
Device Groups	If all the devices in your environment are subject to SOX compliance, it is not necessary to specify a device group. If you are using device groups to focus your reports, you should have created a SOX device group during the configuration process (see "Classify SOX-Related Devices in SOX Device Group" on page 29). Ctrl + click the SOX device group to select it as a parameter to be used.
Storage Groups	If your environment uses a specific storage policy for SOX-related events (as described in "Designate a Storage Group for SOX-Related Events" on page 30), select (Ctrl + click) the storage group you want the report to query.
Devices	Optionally, you can select (Ctrl + click) particular devices whose events you want the report to evaluate.

3. Click **Run Report**.

To Run a Report:

Use this procedure if you want to apply specific filter conditions or parameters to this run of the report only.

1. From the Logger CIP for SOX reports listed in the right panel, choose the report you want to run, such as ISO 11 - Account Activity by User, and click **Run** ().
2. In the Run Report panel, enter the values listed in the following table:

Run Report Panel

Field	What to enter
Template	From the menu, select the report template you want to apply to the report. The default report template is sox. The SOX template includes the field that contains the ISO section title. To give reviewers the most information, use this template for the SOX reports.
Multipage	Select this checkbox if you want the report to span multiple pages if it has many rows. This feature applies only to Microsoft Excel, PDF, and HTML. For online formats, such as HTML, it is easier to view the results as a single, continuous page. The Multipage checkbox is not selected by default.
Report Format	From the menu, select the output format for your report (HTML, PDF, Microsoft Excel, comma separated, text, Microsoft Word, interactive, XML, raw text).
Max. Rows	This feature only applies to reports that are run on demand; this field is not considered when a report is scheduled. For more about scheduling reports, see "Schedule a Logger CIP for SOX Report" below. The Max Rows field limits the number of rows scanned when the report is run. If the data for the report time range contains more rows than the number specified in this box, the rows that exceed the number will not be reflected in the report results. Leave this field blank if you want the report to evaluate all the rows included in a time range.
Field	From the menu, select one of the available fields from the report.
Criteria	From the menu, select a SQL operator (`above, below, is, is not, starts with, ends with, contains`, and so forth).
Value	Enter a value to complete the filter expression.
	Add another row to the filter expression.
	Remove this filter row from the expression.

3. Click **Run**.
   The Report Parameter panel opens in a separate window.
4. In the Report Parameters panel, enter the values listed in "Report Parameters Pane" on the previous page and click **Run Report**.

Schedule a Logger CIP for SOX Report

Once the reports have been configured and return the results that satisfy your needs, you can schedule the reports to run on a regular basis.

1. From the Logger navigation bar, select **Reports**.
2. From the left panel menu, select **Scheduled Reports**. The panel displays the list of currently scheduled report jobs, if any.
3. Click **Add** to bring up the *Add Report Job* panel.
4. On the *Add Report Job* panel, enter the values listed in the following table and click **Save**:

Option	Description
Name	Provide a name for the report job. This is the name that will be displayed on the Scheduled Jobs list.
Schedule	Set the frequency for the scheduled run of the report. For example, you can specify to run the report on specified “Days of the Week” like Sa, Su, M, T, and so forth, or “Everyday”. You can choose to run the report at a certain hour every day “Hour of the Day” or “Every” hour so many hours.
Report Name	Select a report from the list, and click **Go** to load the report. You must click **Go** to load the selected report at the Report Name field before you save the scheduled report job. Attempting to save the scheduled job without first loading the report name will result in an error, and the report will not be saved.
Delivery Options	Depending on which delivery option you choose, the associated parameters are displayed. Click to enable (check) or disable (uncheck) these options. Both email and Publish options for scheduled reports are the same as those provided after you run a report “on demand”. Select a delivery option: • Email • Publish For details on setting email delivery and publishing options, see the *ArcSight Logger Administrator’s Guide*.
Report Parameters	You can either accept the default parameters, or modify them here. These are the same parameters that can be specified for an on-demand report run. For more information about the site-specific data parameters, see the report tables provided in "Reports and Queries" on page 42. For more information about providing a default value for a parameter, see "To change the default value of a parameter:" on page 32. For information on specifying report parameters, see the *ArcSight Logger Administrator’s Guide*.

For a complete description of the report scheduling feature, see the *ArcSight Logger Administrator’s Guide*.

Chapter 4: Logger CIP for SOX Contents

Logger CIP for SOX contains reports, parameters, and queries. This section describes these resources and any configuration that is required.

Topics in this section:

- "Parameters" below
- "Reports and Queries" on page 42

Parameters

This section lists the parameters used in the Logger CIP for SOX queries. When a report is run which invokes a query that requires parameter(s) as input, the report prompts for value(s) for the parameter(s). For example, the ISO 11 - Privileged Account Changes - All report invokes the ISO 11-Privileged Account Changed query, which requires the adminUsers parameter as input. When the ISO 11 - Privileged Account Changes - All report is run, the Administrative User(s) prompt is displayed. The value entered at the Administrative User(s) prompt is passed to the query using the `adminUsers` parameter.

The Logger CIP for SOX queries use following parameters:

- "adminUsers" below
- "allowedReports" on the next page
- "databaseAdminAccounts" on the next page
- "databaseAdminUsers" on the next page
- "destinationUserName" on page 40
- "developmentNetwork" on page 40
- "internalNetwork" on page 40
- "productionNetwork" on page 41
- "testingNetwork" on page 41
- "thirdPartyNetwork" on page 42
- "wirelessNetwork" on page 1

adminUsers

When a report is run that invokes a query which expects the `adminUsers` parameter as input, the Administrative User(s) prompt is displayed during report runtime. The value in

the Administrative User(s) text field is passed to the query thethe `adminUsers` parameter. Supply the set of adminstration accounts used at your site, for example: **'adm', 'root'**. Each user name must start and end with a single quote and each name must be separated by commas.

To change the value of the parameter that is passed to the query, you can enter a new value when prompted by the report during runtime or you can change the default value of the parameter. For more information, see "Providing Site-Specific Data for Reports Using Parameters" on page 31.

allowedReports

When a report is run that invokes a query which expects the `allowedPorts` parameter as input, the Allowed Port(s) prompt is displayed during report runtime. The value in the Allowed Port(s) text field is passed to the query through the `allowedPorts` parameter. Supply the set of allowed ports for your site, for example: **80,25,110**. Each port number must be separated by comma.

To change the value of the parameter that is passed to the query, you can enter a new value when prompted by the report during runtime or you can change the default value of the parameter. For more information, see "Providing Site-Specific Data for Reports Using Parameters" on page 31.

databaseAdminAccounts

When a report is run that invokes a query which expects the `databaseAdminAccounts` parameter as input, the Database Administration Account(s) prompt is displayed during report runtime. The value in the Database Administration Account(s) text field is passed to the query through the `databaseAdminAccounts` parameter. Supply the set of database adminstration accounts used at your site, for example: **'internal','sysman','sys'**. Each user name must start and end with a single quote and each name must be separated by commas.

To change the value of the parameter that is passed to the query, you can enter a new value when prompted by the report during runtime or you can change the default value of the parameter. For more information, see "Providing Site-Specific Data for Reports Using Parameters" on page 31.

databaseAdminUsers

When a report is run that invokes a query which expects the `databaseAdminUsers` parameter as input, the Database Administrative User(s) prompt is displayed during report runtime. The value in the Database Administrative User(s) text field is passed to

the query through the `databaseAdminUsers` parameter. Supply the network accounts used to adminsister the database at your site, for example: **'admin','jdoe'**. Each user name must start and end with a single quote and each name must be separated by commas.

To change the value of the parameter that is passed to the query, you can enter a new value when prompted by the report during runtime or you can change the default value of the parameter. For more information, see "Providing Site-Specific Data for Reports Using Parameters" on page 31.

destinationUserName

When a report is run that invokes a query which expects the `destinationUserName` parameter as input, the User Name prompt is displayed during report runtime. The value in the User Name text field is passed to the query through the `destinationUserName` parameter. Supply the destination user name to report on, for example: **'sys'**. The user name must start and end with a single quote.

To change the value of the parameter that is passed to the query, you can enter a new value when prompted by the report during runtime or you can change the default value of the parameter. For more information, see "Providing Site-Specific Data for Reports Using Parameters" on page 31.

developmentNetwork

When a report is run that invokes a query which expects the `developmentNetwork` parameter as input, the Development Network(s) prompt is displayed during report runtime. The value in the Development Network(s) text field is passed to the query through the `developmentNetwork parameter`.

Specify a regular expression that is compatible with the MySQL REGEXP operator. For example, the regular expression: **192\\.168\\.|10\\.** matches either the 192.168.0.0 /16 or the 10.0.0.0 /8 network. For more information, see "Parameters that use Regular Expressions" on page 33.

To change the value of the parameter that is passed to the query, you can enter a new value when prompted by the report during runtime or you can change the default value of the parameter. For more information, see "Providing Site-Specific Data for Reports Using Parameters" on page 31.

internalNetwork

When a report is run that invokes a query which expects the `internalNetwork parameter` as input, the Internal Network(s) prompt is displayed during report runtime. The value in

the Internal Network(s) text field is passed to the query through the `internalNetwork` parameter.

This snippet is used when a parameter uses regular expressions for IP addresses.Specify a regular expression that is compatible with the MySQL REGEXP operator. For example, the regular expression: **192\\.168\\.|10\\.** matches either the 192.168.0.0 /16 or the 10.0.0.0 /8 network. For more information, see "Parameters that use Regular Expressions" on page 33.

To change the value of the parameter that is passed to the query, you can enter a new value when prompted by the report during runtime or you can change the default value of the parameter. For more information, see "Providing Site-Specific Data for Reports Using Parameters" on page 31.

productionNetwork

When a report is run that invokes a query which expects the productionNetwork parameter as input, the Production Network(s) prompt is displayed during report runtime. The value in the Production Network(s) text field is passed to the query via the productionNetwork parameter.

Specify a regular expression that is compatible with the MySQL REGEXP operator. For example, the regular expression: **192\\.168\\.|10\\.** matches either the 192.168.0.0 /16 or the 10.0.0.0 /8 network. For more information, see "Parameters that use Regular Expressions" on page 33.

To change the value of the parameter that is passed to the query, you can enter a new value when prompted by the report during runtime or you can change the default value of the parameter. For more information, see "Providing Site-Specific Data for Reports Using Parameters" on page 31.

testingNetwork

When a report is run that invokes a query which expects the `testingNetwork` parameter as input, the Testing Network(s) prompt is displayed during report runtime. The value in the Testing Network(s) text field is passed to the query through the `testingNetwork` parameter.

Specify a regular expression that is compatible with the MySQL REGEXP operator. For example, the regular expression: **192\\.168\\.|10\\.** matches either the 192.168.0.0 /16 or the 10.0.0.0 /8 network. For more information, see "Parameters that use Regular Expressions" on page 33.

To change the value of the parameter that is passed to the query, you can enter a new value when prompted by the report during runtime or you can change the default value of

the parameter. For more information, see "Providing Site-Specific Data for Reports Using Parameters" on page 31.

thirdPartyNetwork

When a report is run that invokes a query which expects the `thirdPartyNetwork` parameter as input, the Third-Party Network(s) prompt is displayed during report runtime. The value in the Third-Party Network(s) text field is passed to the query through the `thirdPartyNetwork` parameter.

Specify a regular expression that is compatible with the MySQL REGEXP operator. For example, the regular expression: **192\\.168\\.|10\\.** matches either the 192.168.0.0 /16 or the 10.0.0.0 /8 network. For more information, see "Parameters that use Regular Expressions" on page 33.

To change the value of the parameter that is passed to the query, you can enter a new value when prompted by the report during runtime or you can change the default value of the parameter. For more information, see "Providing Site-Specific Data for Reports Using Parameters" on page 31.

Reports and Queries

Logger CIP for SOX reports are organized by the ISO section (clause) they address.

- "ISO 4: Risk Assessment and Treatment" on the next page
- "ISO 5: Security Policy" on the next page
- "ISO 6: Organization of Information Security" on page 44
- "ISO 7: Asset Management" on page 46
- "ISO 8: Human Resources Security" on page 46
- "ISO 9: Physical and Environmental Security" on page 47
- "ISO 10: Communications and Operations Management" on page 48
- "ISO 11: Access Control" on page 53
- "ISO 12: Information System Acquisition Development and Maintenance" on page 57
- "ISO 13: Information Security Incident Management" on page 59
- "ISO 14: Business Continuity Management" on page 61
- "ISO 15: Compliance" on page 61

Note: The ISO/IEC 17799 standard defines the twelve security control clauses (ISO 4 - ISO 15). In this document (*ArcSight Compliance Insight Package Guide Sarbanes-Oxley 4.02*), these security control clauses are called sections.

ISO 4: Risk Assessment and Treatment

The ISO Section 4 reports address the ISO controls by allowing analysts to view high risk events occurring on their networks. This helps to identify the immediate risks threatening the network so that security administrators can take actions to mitigate them.

Resources

Logger CIP for SOX includes the following ISO:4 section reports and queries:

ISO 4: Risk Assessment and Treatment Reports and Queries

Report	Description	Associated Query	Configuration
ISO 4 - High Risk Events by Zone	This report displays the number of high or very-high severity events sorted by zone.	ISO 4-High Risk Events by Zone	None required
ISO 4 - High Risk Events	This report displays source and destination information from all events with an agent severity of High or Very-High.	ISO 4-High Risk Events	None required
ISO 4 - Top 10 High Risk Events	This report displays a summary of the top 10 events with an agent severity of High or Very-High.	ISO 4-Top High Risk Events	None required

ISO 5: Security Policy

The ISO Section 5 reports address the ISO controls by identifying users and machines that have violated policies typically included in organizational security policy documents. Top policy violation events are also identified so that administrators can see which policies are most commonly breached and take steps to properly enforce those policies.

Resources

Logger CIP for SOX includes the following ISO:5 section reports and queries:

ISO:5 Security Policy Reports and Queries

Report	Description	Associated Query	Configuration
ISO 5 - Machines Conducting Policy Breaches	This report displays source IP, hostname, and event information from events with a Category Technique of /Policy/Breach.	ISO 5-Machines Conducting Policy Breaches	None required
ISO 5 - New Hosts	This report displays all new hosts on the network detected by traffic analysis systems.	ISO 5-New Hosts	None required

ISO:5 Security Policy Reports and Queries, continued

Report	Description	Associated Query	Configuration
ISO 5 - New Services	This report displays all new services detected on the network by traffic analysis systems.	ISO 5-New Services	None required
ISO 5 - Top 20 Policy Breach Events	This report lists the top 20 events categorized as /Policy/Breach.	ISO 5-Top 20 Policy Breach Events	None required

ISO 6: Organization of Information Security

Communications with customer, partner, and other third-party networks should be closely monitored for suspicious activity and attacks. The ISO Section 6 reports address the ISO controls by reporting on network activities involving third-party assets.

Resources

Logger CIP for SOX includes the following ISO:6 section reports and queries:

ISO:6 Organization of Information Security Reports and Queries

Report	Description	Associated Query	Configuration
ISO 6 - Administrative Logins and Logouts from Third-Party Hosts	This report displays the time, source, destination, and usernames from events indicating administrative logins from a third-party host.	ISO 6-Admin Logins and Logouts from Third-Party	Supply values for: • adminUsers • thirdPartyNetwork
ISO 6 - Administrative Logins and Logouts to Third-Party Hosts	This report displays the time, source, destination, and usernames from events indicating administrative logins to a third-party host.	ISO 6-Admin Logins and Logouts to Third-Party	Supply values for: • adminUsers • thirdPartyNetwork
ISO 6 - Attacks from Third-Party Systems	This report displays the event, time, source, and destination of attacks originating from third-party systems.	ISO 6-Third-Party Sourced Attacks	Supply value for: • adminUsers
ISO 6 - Attacks on Third-Party Systems	This report displays source and destination information from attacks against third-party systems.	ISO 6-Attacks on Third-Party Systems	Supply value for: • adminUsers
ISO 6 - Compromised Third-Party Systems	This report displays all successful compromise attempts targeting third-party systems.	ISO 6-Compromised Third-Party Systems	Supply value for: • adminUsers

ISO:6 Organization of Information Security Reports and Queries, continued

Report	Description	Associated Query	Configuration
ISO 6 - Failed Admin Logins from Third-Party Systems	This report displays all failed administrative logins from third-party systems.	ISO 6-Failed Admin Logins from Third-Party Systems	Supply values for: • adminUsers • thirdPartyNetwork
ISO 6 - Failed Admin Logins to Third-Party Systems	This report displays all failed administrative logins to third-party systems.	ISO 6-Failed Admin Logins to Third-Party Systems	Supply values for: • adminUsers • thirdPartyNetwork
ISO 6 - Failed User Logins from Third-Party Systems	This report displays all failed user logins from third-party systems.	ISO 6-Failed User Logins from Third-Party Systems	Supply value for: • adminUsers
ISO 6 - Failed User Logins to Third-Party Systems	This report displays all failed user logins to third-party systems.	ISO 6-Failed User Logins to Third-Party Systems	Supply value for: • adminUsers
ISO 6 - File Activity on Third-Party Systems	This report displays the host, file, behavior, and outcome of monitored file activity on third-party systems.	ISO 6-File Activity on Third-Party Systems	Supply value for: • adminUsers
ISO 6 - File Creations on Third-Party Systems	This report displays the host, file, behavior, and outcome of monitored file creations on third-party systems.	ISO 6-File Creations on Third-Party Systems	Supply value for: • adminUsers
ISO 6 - File Deletions on Third-Party Systems	This report displays the host, file, behavior, and outcome of monitored file deletions on third-party systems.	ISO 6-File Deletions on Third-Party Systems	Supply value for: • adminUsers
ISO 6 - File Modifications on Third-Party Systems	This report displays the host, file, behavior, and outcome of monitored file modifications on third-party systems.	ISO 6-File Mods on Third-Party Accessible Systems	Supply value for: • adminUsers
ISO 6 - Policy Violations from Third-Party Systems	This report displays the events indicating policy violations from third-party systems.	ISO 6-Policy Violations from Third-Party Systems	Supply value for: • adminUsers
ISO 6 - Services Accessed by Third-Party Systems	This report displays the port, service, and destination information of services accessed by third-party systems.	ISO 6-Services Accessed by Third-Parties	Supply value for: • adminUsers

ISO:6 Organization of Information Security Reports and Queries, continued

Report	Description	Associated Query	Configuration
ISO 6 - Third-Party Systems Accessed	This report displays all events indicating third-party systems were queried or accessed.	ISO 6-Third-Party Systems Accessed	Supply value for: • adminUsers
ISO 6 - User Logins and Logouts from Third-Party Systems	This report displays the time, source, destination, and user information from user login and logout events from third-party systems.	ISO 6-User Logins Logouts from Third-Party Sys	Supply value for: • adminUsers
ISO 6 - User Logins and Logouts to Third-Party Systems	This report displays the time, source, destination, and user information from user login and logout events targeting third-party systems.	ISO 6-User Logins Logouts to Third-Party Sys	Supply value for: • adminUsers

ISO 7: Asset Management

The ISO Section 7 reports address the ISO Controls by analyzing events to identify all assets which participate on the organization's network. This information can be used to find gaps in the asset inventory that might indicate rogue devices or those devices which have not been accounted for in the inventory.

Resources

Logger CIP for SOX includes the following ISO:7 section reports and queries:

ISO 7: Asset Management Reports and Queries

Report	Description	Associated Query	Configuration
ISO 7 - Network Active Assets	This report displays a summary of all hosts that have been included as the source address in logged events; the number of events and last event time are included in the report.	ISO 7-Network Active Assets	Supply a value for internalNetwork

ISO 8: Human Resources Security

The ISO Section 8 reports address the ISO controls by alerting analysts to suspicious activities and Internet usage by employees. This information allows administrators to ensure that employees conform to the terms and conditions of employment, including the organization's acceptable use and information security policies.

Resources

Logger CIP for SOX includes the following ISO:8 section reports and queries:

ISO: Human Resources Security Reports and Queries

Report	Description	Associated Query	Configuration
ISO 8 - Internet Activity per Device per Machine	This report displays a sorted list of Internet Activity per gateway and source machine. The list is sorted by the number of distinct destination IP addresses.	ISO 8-Internet Activity per Device per Machine	Customize the list of ports in the query to reflect the internet ports accessed by users at your site. For more information about customizing the query, see "Providing Site-Specific Data for Reports Requiring Customization" on page 33.
ISO 8 - Internet Activity per Device per User	This report displays a sorted list of Internet Activity per gateway and user. The list is sorted by the number of distinct destination IP addresses.	ISO 8-Internet Activity per Device per User	Customize the list of ports in the query to reflect the internet ports accessed by users at your site. For more information about customizing the query, see "Providing Site-Specific Data for Reports Requiring Customization" on page 33.
ISO 8 - Summary of Suspicious Activities per User	This report displays the number of suspicious events and distinct targets per user, sorted by the time of the last suspicious event.	ISO 8-Summary of Suspicious Activities by User	None required

ISO 9: Physical and Environmental Security

The ISO 9 reports address the ISO controls by reporting on all failed and successful building access events from card reader systems.

Resources

Logger CIP for SOX includes the following ISO:9 section reports and queries:

ISO 9: Physical and Environmental Security Reports and Queries

Report	Description	Associated Query	Configuration
ISO 9 - Failed Building Access Attempts	This report displays all failed building access attempts including user name, id, and badge reader number.	ISO 9-Failed Building Access Events	None required
ISO 9 - Successful Building Access Attempts	This report displays all successful building access attempts including user name, id, and badge reader number. Events are sorted by date.	ISO 9-Successful Building Access Events	None required

ISO 10: Communications and Operations Management

The ISO Section 10 reports address the ISO controls by reporting on configuration changes to operating systems, applications, firewalls, and network equipment. This information can be used to supplement evidence that change control procedures are followed. Additional reports supporting ISO Section 10 include information on malicious code, antivirus updates, network segregation, administrator activities, and fault logging.

Resources

Logger CIP for SOX includes the following ISO:10 section reports and queries:

ISO:10 Communications and Operations Management Reports and Queries

Report	Description	Associated Query	Configuration
ISO 10 - Account Lockouts by System	This report displays incidents of user accounts locked out by the system, sorted by system name. The chart displays a trend of the number of such incidents per day.	ISO 10-Account Lockouts by System	None required
ISO 10 - Account Lockouts by User	This report displays incidents of user accounts locked out by the system, sorted by user name. The chart displays a trend of the number of such incidents per day.	ISO 10-Account Lockouts by User	None required
ISO 10 - Administrative Logins and Logouts	This report displays administrative logins and logouts. The chart displays the number of such events per system.	ISO 10-Administrative Logins and Logouts	Supply a value for: adminUsers
ISO 10 - Administrator Actions	This report displays all actions taken by administrator accounts.	ISO 10-Administrator Actions	Supply a value for: adminUsers

ISO:10 Communications and Operations Management Reports and Queries, continued

Report	Description	Associated Query	Configuration
ISO 10 - Application Configuration Modification	This report displays events that are categorized as application configuration modifications such as an update of a license file or a program setting change. The chart displays the number of such incidents per day.	ISO 10-Application Configuration Modifications	None required
ISO 10 - Attacks - Development to Production	This report displays events that are categorized as attacks, originating from the development network and targeting the production network. The development and target networks are defined by parameters and can be set in runtime. The chart displays the number of such incidents per day.	ISO 10-Attacks Development to Production	Supply values for: • developmentNetwork • productionNetwork
ISO 10 - Attacks - Production to Development	This report displays events that are categorized as attacks, originating from the production network and targeting the development network. The development and target networks are defined by parameters and can be set in runtime. The chart displays the number of such incidents per day.	ISO 10-Attacks Production to Development	Supply values for: • developmentNetwork • productionNetwork
ISO 10 - Audit Log Cleared	This report displays the date, time, system, and user information from all events indicating an audit log has been cleared.	ISO 10-Audit Log Cleared	None required
ISO 10 - Changes to Development Network Machines	This report displays all changes to machines in the development network.	ISO 10-Changes to Development Network Machines	Supply a value for: • developmentNetwork
ISO 10 - Changes to Third-Party Resources	This report displays events indicating a change was made to a third-party application or resource.	ISO 10-Changes to Third-Party Resources	Supply a value for: • thirdPartyNetwork
ISO 10 - Database Access - All	This report displays a count of database access attempts per hour.	ISO 10-Database Access - All	None required
ISO 10 - Database Access - Failed	This report displays a count of database access attempt failures per hour.	ISO 10-Database Access - Failed	None required

ISO:10 Communications and Operations Management Reports and Queries, continued

Report	Description	Associated Query	Configuration
ISO 10 - Development Network Not Segregated	This report displays events from a development network which target a production or testing network, or vice versa. This indicates lack of segregation between the networks. The development, production and target networks are defined by parameters and can be set in runtime. The chart displays the number of such incidents per day.	ISO 10-Development to Test or Production	Supply values for: • developmentNetwork • productionNetwork • testingNetwork
ISO 10 - Device Configuration Changes	This report displays the date, time, event name, and host information from all events indicating a configuration change has been made on network equipment.	ISO 10-Device Configuration Changes	None required
ISO 10 - Device Logging Review	This report displays all logging devices. For each device, a count of events received and the last time an event was received by the device is reported.	ISO 10-Device Logging Review	None required
ISO 10 - Failed Anti-Virus Updates	This report displays the date, host, and product information from failed anti-virus update events.	ISO 10-Failed Anti-Virus Updates	None required
ISO 10 - Fault Logs	This report displays all events indicating a system fault has occurred.	ISO 10-Fault Logs	None required
ISO 10 - File Integrity Changes	This report displays events indicating changes to monitored files.	ISO 10-File Integrity Changes Detected	None required
ISO 10 - Firewall Configuration Changes - All	This report displays all events indicating a configuration file on a firewall has been changed.	ISO 10-Firewall Configuration Modifications	None required
ISO 10 - Firewall Configuration Changes - Successful	This report displays events indicating a configuration file on a firewall has been successfully changed.	ISO 10-Firewall Configuration Modifications	None required
ISO 10 - Firewall Open Port Review	This report displays the destination ports accepted through firewalls and includes a pie chart showing the most commonly used destination ports.	ISO 10-Firewall Open Port Review	None required

ISO:10 Communications and Operations Management Reports and Queries, continued

Report	Description	Associated Query	Configuration
ISO 10 - Information Interception Events	This report displays the date, source, and destination information from information-interception events.	ISO 10-Information Interception	None required
ISO 10 - Malicious Code Sources	This report displays the count of malicious code events from particular hosts.	ISO 10-Malicious Code Sources	None required
ISO 10 - Network Device Configuration Changes - All	This report displays events indicating configuration file changes on network equipment such as routers and switches.	ISO 10-Network Device Configuration Modifications	None required
ISO 10 - Network Device Configuration Changes - Successful	This report displays events indicating successful configuration file changes on network equipment such as routers and switches.	ISO 10-Network Device Configuration Modifications	None required
ISO 10 - Number of Successful Administrative Logins	This report displays the number of successful administrative logins per host and user.	ISO 10-Number of Successful Administrative Logins	Supply value for: adminUsers
ISO 10 - Number of Successful User Logins	This report displays the number of successful user logins per host and user.	ISO 10-Number of Successful User Logins	Supply value for: adminUsers
ISO 10 - Number of Unsuccessful Administrative Logins	This report displays the number of unsuccessful administrative logins per host and user.	ISO 10-Number Unsuccessful Administrative Logins	Supply value for: adminUsers
ISO 10 - Number of Unsuccessful User Logins	This report displays the number of unsuccessful user logins per host and user.	ISO 10-Number of Unsuccessful User Logins	Supply value for: adminUsers Login attempts by the specified administrative users are not reported.
ISO 10 - Operating System Configuration Changes	This report details operating system configuration changes.	ISO 10-Operating System Configuration Changes	None required

ISO:10 Communications and Operations Management Reports and Queries, continued

Report	Description	Associated Query	Configuration
ISO 10 - Production Network Not Segregated	This report displays events from a production network which target a development or testing network, or vice versa. This indicates lack of segregation between the networks. The development, production and target networks are defined by parameters and can be set in runtime. The chart displays the number of such incidents per day.	ISO 10-Production to Test or Development	Supply values for: • developmentNetwork • productionNetwork • testingNetwork
ISO 10 - Resource Exhaustion	This report displays a count of events indicating resource exhaustion on particular hosts.	ISO 10-Resource Exhaustion Detected	None required
ISO 10 - Successful Brute Force Logins	This report displays the time, user, and host information from successful brute-force logins.	ISO 10-Successful Brute Force Logins	None required
ISO 10 - System Restarted	This report displays events indicating a system or a process on a system has been restarted. The chart displays the number of such incidents per machine.	ISO 10-System Restarted	None required
ISO 10 - Test Network Not Segregated	This report displays events from a test network which target a development or production networks, or vice versa. This indicates lack of segregation between the networks. The development, production and target networks are defined by parameters and can be set in runtime. The chart displays the number of such incidents per day.	ISO 10-Test to Development or Operations	Supply values for: • developmentNetwork • productionNetwork • testingNetwork
ISO 10 - Top Unsuccessful Administrative Logins	This report displays the top administrative usernames with failed logins. A table displays the number of failures per username and the time of the last failure.	ISO 10-Top Unsuccessful Administrative Logins	Supply value for: "adminUsers" on page 38
ISO 10 - Top Unsuccessful User Logins	This report displays the top usernames having failed logins. A table is included which contains the count and last time a login has failed with the username.	ISO 10-Top Unsuccessful User Logins	Supply value for: "adminUsers" on page 38 Login attempts by the specified administrative users are not reported.

ISO:10 Communications and Operations Management Reports and Queries, continued

Report	Description	Associated Query	Configuration
ISO 10 - Unsuccessful User Logins	This report displays the time, name, destination, and user information from unsuccessful user login events.	ISO 10-Unsuccessful User Logins	Supply value for: "adminUsers" on page 38 Login attempts by the specified administrative users are not reported.
ISO 10 - User Logins and Logouts	This report displays the time, name, destination, and user information from user login and logout events.	ISO 10-User Logins and Logouts	None required
ISO 10 - VPN Access Summary	This report displays a summary of VPN access by users.	ISO 10-VPN Access Summary	None required
ISO 10 - Virus Summary by Hosts	This report displays the total virus event count by host in descending order of event count.	ISO 10-Virus Summary by Hosts	None required
ISO 10 - Virus Summary by Virus Name	This report displays the total virus event count by virus name in descending order of event count.	ISO 10-Virus Summary by Virus Name	None required

ISO 11: Access Control

The ISO Section 11 reports address the ISO controls by providing information regarding authorization and authentication, firewall management, and account management. These reports enable analysts to validate changes to privileged accounts, view firewall activity and traffic flows, and identify insecure services in use on the network.

Resources

Logger CIP for SOX includes the following ISO:11 section reports and queries:

ISO 11: Access Control Reports and Queries

Report	Description	Associated Query	Configuration
ISO 11 - Account Activity by User	This report displays all the events with the specified destination user name. The destination user name is defined at runtime.	ISO 11-Account Activity by User Name	Supply a value for: destinationUserName
ISO 11 - Blocked Firewall Traffic	This report displays events generated by devices that have blocked traffic. The chart displays the number of blocking events.	ISO 11-Blocked Firewall Traffic	None required
ISO 11 - Database Privilege Violation	This report displays attempts to access database administrator accounts with non-administrator accounts. For example, if the specified database administrator account is "sys" and the specified database administrator user names are "admin" and "administrator", this report will display attempts to access the user "sys" by users other than "admin" and "administrator".	ISO 11-Database Privilege Violation	Supply values for: • databaseAdminAccounts • databaseAdminAccounts
ISO 11 - Default Vendor Account Used	This report displays usage of default accounts (such as 'root' on Unix systems), if their usage was successful or not, and the number of times they were used. The default account and the systems are defined in the query and should be updated according to the specific environment. The chart displays the total number successful and unsuccessful default account usage attempts.	ISO 11-Default Vendor Account Used	Customize the list of default vendor accounts listed in the query to reflect the devices used in your environment. See "Providing Site-Specific Data for Reports Requiring Customization" on page 33.
ISO 11 - Insecure Services	This report displays systems that are providing insecure services such as FTP or Telnet. The chart displays the number of times each system provided an insecure service.	ISO 11-Insecure Services	Customize the ports and processes listed in the query to reflect the ports and processes that are considered insecure in your environment. See "Providing Site-Specific Data for Reports Requiring Customization" on page 33.
ISO 11 - Login From Multiple IPs - Detail	This report displays logins to the same account on a system, when the logins originated from multiple source IPs. The chart displays the number of times each source IP was involved in such incidents.	ISO 11-Login From Multiple IPs-Detail	None required

ISO 11: Access Control Reports and Queries, continued

Report	Description	Associated Query	Configuration
ISO 11 - Login From Multiple IPs - Overview	This report displays users on specific hosts when the logins originated from multiple IPs, hosts or zones. The count of logins from IPs, hosts or zones is reported. The chart displays for each logged-in IP, the number of different IPs that logins occurred from.	ISO 11-Login From Multiple IPs-Overview	None required
ISO 11 - Multiple User Login - Detail	This report displays logins of one user to multiple accounts on the same host and the number of different accounts that were accessed. The chart displays the number of multiple accounts were accessed by the same user on each host.	ISO 11-Multiple User Login-Detail	None required
ISO 11 - Multiple User Login - Overview	This report displays logins of one user to multiple accounts on the same host and the number of different accounts that were accessed. The chart displays the number of multiple accounts were accessed by the same user on each host.	ISO 11-Multiple User Login-Overview	None required
ISO 11 - Network Routing Configuration Changes	This report displays changes in the network routing configurations. The chart displays the number of times such changes were made to each host.	ISO 11-Network Routing Changes	None required
ISO 11 - Privileged Account Changes - All	This report displays all changes made to privileged accounts such as password changes. Privileged accounts are defined by the 'adminUsers' parameter and can be modified at runtime. The chart shows the hosts these changes were made on and the number of such changes.	ISO 11-Privileged Account Changed	Supply a value for: adminUsers
ISO 11 - Privileged Account Changes - Successful	This report displays all successful changes made to privileged accounts such as password changes. Privileged accounts are defined by the 'adminUsers' parameter and can be modified at runtime. The chart shows the hosts these changes were made on and the number of such changes.	ISO 11-Privileged Account Changed	Supply a value for: adminUsers

ISO 11: Access Control Reports and Queries, continued

Report	Description	Associated Query	Configuration
ISO 11 - Removal of Access Rights	This report displays events indicating the removal of access rights and user account and group deletion. The chart displays the number of times such events occurred on each host.	ISO 11-Removal of Access Rights	None required
ISO 11 - Services by Asset	This report displays the hosts that are running services and the services they are running. The chart displays the number of hosts that run each service.	ISO 11-Services by Asset	Customize the list of private addresses in the query to focus the report on a particular part of an address space. See "Providing Site-Specific Data for Reports Requiring Customization" on page 33.
ISO 11 - Suspicious Activity in Wireless Network	This report displays events defined as suspicious activity, such as port scanning in the wireless network. The wireless network is defined by the 'wirelessNetwork' parameter and can be changed at runtime. The chart displays a count of the different events that were defined as suspicious.	ISO 11-Suspicious Activity in Wireless Network	Supply a value for: wirelessNetwork
ISO 11 - Systems Accessed as Root or Administrator	This report displays attempts to access systems using the default 'root', 'admin' or 'administrator' account names.	ISO 11-Systems Accessed as Root or Administrator	Customize the list of account names in the query to reflect any additional default administrator account names use by devices at your site. See "Providing Site-Specific Data for Reports Requiring Customization" on page 33.
ISO 11 - Traffic - Inbound Count	This report displays the number of times a device reported communications between public and private IP addresses. The chart shows the number of times each zone has been the target of communication originating in public IP addresses.	ISO 11-Traffic-Inbound Count	Supply a value for: internalNetwork
ISO 11 - Traffic - Inbound on Disallowed Ports - All	This report displays inbound traffic on disallowed ports. Allowed ports are specified at runtime using the 'allowedPorts' parameter. By default, the ports 80 and 443 are specified. The chart displays the number of attempts, successful and failed connections.	ISO 11-Traffic-Inbound on Disallowed Ports	Supply values for: • allowedReports • internalNetwork

ISO 11: Access Control Reports and Queries, continued

Report	Description	Associated Query	Configuration
ISO 11 - Traffic - Inbound on Disallowed Ports - Successful	This report displays successful inbound traffic on disallowed ports. This is traffic with category outcome of 'successful' that should be further investigated. Allowed ports are specified at runtime using the 'allowedPorts' parameter. By default, the ports 80 and 443 are specified. The chart displays the IPs that were the target of this communication.	ISO 11-Traffic-Inbound on Disallowed Ports	Supply values for: • allowedReports • internalNetwork
ISO 11 - Traffic Between Zones - Protocols	This report displays communication protocols that are passed between different zones.	ISO 11-Traffic Between Zones-Protocols	None required
ISO 11 - User Account Creation	This report displays the user, host, and zone information from user-account-creation events. A chart shows the number of such events per zone.	ISO 11-User Account Creation	None required
ISO 11 - User Account Deletion	This report displays the user, host, and zone information from user-account-deletion events. A chart displays the number of such events per zone.	ISO 11-User Account Deletion	None required

ISO 12: Information System Acquisition Development and Maintenance

The ISO Section 12 reports address the ISO controls by providing analysts with reports detailing changes to operating systems and files; invalid data inputs; invalid certificates; and vulnerability exploit attempts. These reports can be used to provide evidence of compliance with maintenance and development related controls.

Resources

Logger CIP for SOX includes the following ISO:12 section reports and queries:

ISO 12: Information System Acquisition Development and Maintenance Reports and Queries

Report	Description	Associated Query	Configuration
ISO 12 - Changes to Operating Systems	This report displays modifications to operating systems such as account changes or change to the security options, and the number of the times these events happened. The chart displays the number of such events per host.	ISO 12-Changes to Operating Systems	None required
ISO 12 - Exploit of Vulnerabilities	This report displays events identified as exploit of vulnerabilities, their source, destination and number of times they occurred. These events are reported by IDSs when an attempt to exploit a well-known vulnerability, such as when a Unicode vulnerability is detected. The chart displays the number of such events per host.	ISO 12-Exploit of Vulnerability	None required
ISO 12 - File Changes in Production	This report displays changes to files made in the production network. The production network address range is defined by the user at runtime. The chart displays the number of times files where changed on each host.	ISO 12-File Changes in Production	Supply value for: productionNetwork
ISO 12 - Invalid Certificate	This report displays events that indicate an error with a server's certificate. The chart displays the number of such occurrences per host.	ISO 12-Invalid Certificate	None required
ISO 12 - Invalid Data Input	This report displays events that indicate corrupt data input such as exceptionally long URLs or SNMP requests that exceed the allowed buffer size.	ISO 12-Invalid Data Input	None required

ISO 12: Information System Acquisition Development and Maintenance Reports and Queries, continued

Report	Description	Associated Query	Configuration
ISO 12 - Software Changes in Production	This report displays events indicating changes to daemons, access policies and other software changes in the production environment. The production network address range is defined by the user at runtime. The chart displays the number of such changes on each host.	ISO 12-Software Changes in Production	Supply value for: productionNetwork
ISO 12 - Vulnerabilities and Misconfigurations	This report displays vulnerability and misconfiguration events such as detected multiple hosts with same IP on the network or vulnerable CGI scripts. The chart displays the number of such events per host.	ISO 12-Vulnerabilities and Misconfigurations	None required
ISO 12 - Vulnerability Scanner Results	This report displays vulnerabilities as reported by vulnerability scanners. The chart displays the number of different kinds of vulnerabilities found.	ISO 12-Vulnerability Scanner Results	None required

ISO 13: Information Security Incident Management

The ISO Section 13 reports address the ISO controls by providing reports detailing information security attacks against the network. The reports provide analysts with up to date information including Top Attack Sources, Internal Reconnaissance events, DoS sources, and activity detected on covert channels.

Resources

Logger CIP for SOX includes the following ISO:13 section reports and queries:

ISO 13: Information Security Incident Management Reports and Queries

Report	Description	Associated Query	Configuration
ISO 13 - Attack Events - Top 20	This report displays the 20 most common attack event names in the report's time frame.	ISO 13-Attack Events Count	None required
ISO 13 - Attacked Hosts - Top 20	This report displays the 20 hosts that were the target for the largest number of events identified as 'attacks'. The chart displays the number of events identified as 'attacks', that targeted each zone.	ISO 13-Attacked Hosts	None required

ISO 13: Information Security Incident Management Reports and Queries, continued

Report	Description	Associated Query	Configuration
ISO 13 - Attackers - Top 20	This report displays the 20 hosts that were the source for the largest number of events identified as 'attacks' . The chart summarizes the number of events identified as 'attacks' per zone.	ISO 13-Attackers	None required
ISO 13 - Attacks - Hourly Count	This report displays the number of attacks that targeted internal IP addresses each hour.	ISO 13-Attacks-Hourly Count	Supply a value for: internalNetwork
ISO 13 - Attacks Targeting Internal Assets - All	This report displays all events with category significance of "Recon", "Compromise", "Hostile" or "Suspicious" that target an internal IP address.	ISO 13-Attacks Targeting Internal Assets-All	Supply a value for: internalNetwork
ISO 13 - Confidentiality and Integrity Breach Sources - Count	This report displays the sources for confidential and integrity attacks and the number of attacks associated with each source. The chart displays the number of such events identified initiated in each zone.	ISO 13-CI Breach Sources-Overview	None required
ISO 13 - Covert Channel Activity	This report displays a count of events identified as covert channel activity. These events are generated by IDS devices and may indicate the use of a 'loki' tool or other tools designed to establish an undetected channel to/from the organization. The chart summarizes the target zones of these events.	ISO 13-Covert Channel Activity	None required
ISO 13 - DoS Sources	This report displays a count of source hosts of Denial of Service attacks and the device that reported the incident.	ISO 13-Denial of Service Sources	None required
ISO 13 - Information System Failures	This report displays a count of failures that happen on machines in the network. The failure to start a service or a denied operation are examples of information system failures. The chart summarizes the number of failures in each zone.	ISO 13-Information System Failures	None required
ISO 13 - Internal Reconnaissance - Top 20 Events	This report displays the 20 events identified mostly as internal reconnaissance events, such as port scanning activity. The chart summarizes the number of such events per reporting device.	ISO 13-Internal Reconnaissance-Events	Supply a value for: internalNetwork
ISO 13 - Internal Reconnaissance - Top 20 Sources	This report displays the 20 hosts that were the source of most internal reconnaissance events, such as port scanning activity.	ISO 13-Internal Reconnaissance-Sources	Supply a value for: internalNetwork
ISO 13 - Internal Reconnaissance - Top 20 Targets	This report displays the 20 hosts that were the target of most internal reconnaissance events, such as port scanning activity.	ISO 13-Internal Reconnaissance-Targets	Supply a value for: internalNetwork

ISO 14: Business Continuity Management

The ISO Section 14 reports address the ISO controls by allowing analysts to report on attacks against the availability of network resources. This enables administrators to identify the attacks and systems targeted so that risks from availability attacks can be mitigated quickly.

Resources

Logger CIP for SOX includes the following ISO:14 section reports and queries:

ISO 14: Business Continuity Management Reports and Queries

Report	Description	Associated Query	Configuration
ISO 14 - Availability Attacks	This report displays a count of DOS and other availability attacks on the network. The chart displays the number of availability attacks in each zone.	ISO 14-Availability Attacks	None required

ISO 15: Compliance

The ISO Section 15 reports address the ISO controls by providing analysts with reports providing evidence of compliance with legal requirements and security policies and standards. Reports can be generated on employee compliance with policies such as peer-to-peer usage, intellectual property protection, and email utilization.

Resources

Logger CIP for SOX includes the following ISO:15 section reports and queries:

ISO 15: Compliance Reports and Queries

Report	Description	Associated Query	Configuration
ISO 15 - Email Receivers by Amount - Top 100	This report displays the top email recipients based on the number of emails received.	ISO 15-Email Receivers by Amount	None required
ISO 15 - Email Receivers by Size - Top 100	This report displays the top email recipients based on the total size (in bytes) of emails received.	ISO 15-Email Receivers by Size	None required
ISO 15 - Email Senders by Amount - Top 100	This report displays the top email senders based on the number of emails sent. The chart summarizes the number of emails sent for each zone.	ISO 15-Email Senders by Amount	None required

ISO 15: Compliance Reports and Queries, continued

Report	Description	Associated Query	Configuration
ISO 15 - Email Senders by Size - Top 100	This report displays the top 100 email senders based on the total size (in bytes) of emails sent. The chart displays the total size (in bytes) of emails sent from each zone based on the table.	ISO 15-Email Senders by Size	None required
ISO 15 - Information Leaks - Organizational	This report displays events that are associated with information leaks as reported by IDSs or Information Monitoring solutions. The chart displays the number of information leak events that occurred in the report timeframe.	ISO 15-Information Leaks - Organizational	None required
ISO 15 - Information Leaks - Personal	This report displays events that are associated with personal information leaks as reported by IDSs or Information Monitoring solutions. The chart displays the number of information leaks that occurred each day in the report timeframe.	ISO 15-Information Leaks - Personal	None required
ISO 15 - Information System Audit Tool Logins	This report displays all logins to ArcSight ESM, ArcSight Logger and other information audit systems. The chart displays the number of successful and unsuccessful logins in the report timeframe.	ISO 15-Information System Audit Tool Logins	None required
ISO 15 - Largest Emails - Top 20	This report displays the 20 largest emails sent in the organization. The chart displays the number of large emails sent per user.	ISO 15-Largest Emails	None required
ISO 15 - Peer to Peer Ports Count	This report displays peer-to-peer ports and the number of times they were used. Additional peer-to-peer ports can be defined in the query.	ISO 15-Peer To Peer Ports Count	Customize the query with any additional peer-to-peer destination ports. See "Providing Site-Specific Data for Reports Requiring Customization" on page 33.

ISO 15: Compliance Reports and Queries, continued

Report	Description	Associated Query	Configuration
ISO 15 - Peer to Peer Sources by Machine - Detail	This report displays sources of peer-to-peer communication and the number of times each peer-to-peer port was used. Additional peer-to-peer ports can be defined in the query. The chart summarizes the number of peer-to-peer events per host.	ISO 15-Peer to Peer Sources By Machine-Detail	Customize the query with any additional peer-to-peer destination ports. See "Providing Site-Specific Data for Reports Requiring Customization" on page 33.
ISO 15 - Peer to Peer Sources by Machine - Overview	This report counts peer-to-peer events per host. Additional peer-to-peer ports can be defined in the query. The chart summarizes the number of peer-to-peer events per zone.	ISO 15-Peer to Peer Sources By Machine-Overview	Customize the query with any additional peer-to-peer destination ports. See "Providing Site-Specific Data for Reports Requiring Customization" on page 33.
ISO 15 - Policy Breaches	This report displays all policy breaches such as IM use or the downloading of sexual content. The chart displays the number of policy breaches that occurred per zone.	ISO 15-Policy Breaches	None required
ISO 15 - Possible Intellectual Property Rights Violation	This report displays snort events indicating that a multimedia application has downloaded a Windows Media file. Such applications can be used for media file sharing which might result in intellectual property rights violation. The chart displays the number of such events per zone.	ISO 15-Possible IPR Violations	None required

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 (Logger CIP for SOX 4.02)

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 documentation-feedback@microfocus.com.

We appreciate your feedback!