



**Hewlett Packard**  
Enterprise

# **HPE ArcSight Security Solution Guide**

Compliance Insight Package for Sarbanes-Oxley 4.0

ArcSight Logger

June 13, 2011

## Warranty

The only warranties for Hewlett Packard Enterprise products and services are set forth in the express warranty statements accompanying such products and services. Nothing herein should be construed as constituting an additional warranty. HPE shall not be liable for technical or editorial errors or omissions contained herein. The information contained herein is subject to change without notice.

The network information used in the examples in this document (including IP addresses and hostnames) is for illustration purposes only.

HPE Security ArcSight products are highly flexible and function as you configure them. The accessibility, integrity, and confidentiality of your data is your responsibility. Implement a comprehensive security strategy and follow good security practices.

This document is confidential.

## Restricted Rights Legend

Confidential computer software. Valid license from HPE 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

© Copyright 2012 Hewlett Packard Enterprise Development LP

Follow this link to see a complete statement of copyrights and acknowledgements:

<https://www.protect724.hpe.com/docs/DOC-13026>

## Contact Information

---

<b>Phone</b>	A list of phone numbers for HPE ArcSight Technical Support is available on the HPE Enterprise Security contacts page: <a href="http://www.hpe.com/software/support/contact_list">www.hpe.com/software/support/contact_list</a>
<b>Support Web Site</b>	<a href="http://www.hpe.com/software/support">www.hpe.com/software/support</a>
<b>Protect 724 Community</b>	<a href="https://www.protect724.hpe.com">https://www.protect724.hpe.com</a>

---

# Contents

---

<b>About This Book</b>	<b>vii</b>
Who Should Read this Guide	vii
How to Use this Guide	vii
Text Conventions	viii
Related Documentation	ix
 <b>Chapter 1: Overview of Logger CIP for SOX</b>	 <b>1</b>
About ArcSight Logger™	2
Sarbanes-Oxley Act and Security Monitoring Requirements	2
Logger CIP for SOX	2
Architecture of Logger CIP for SOX	3
How the Logger CIP for SOX Identifies SOX-Related Events	3
SOX Report Category Filter	4
SOX Device Group	4
Storage Group	4
Specific SOX-Related Devices	5
About the Logger CIP for SOX Reports	5
Anatomy of a Report	5
What's Next	6
 <b>Chapter 2: Deployment and Configuration</b>	 <b>7</b>
Before Deploying	7
Verify the Software Logger Version	7
Verify the Logger Appliance Version	8
Supported Devices	8
Connectors Needed for Non-CEF Devices	13
Deploy Logger CIP for SOX	15
Deploy Logger CIP for SOX on the Software Logger	15
Deploy Logger CIP for SOX on the Logger Appliance	16
Verify Logger CIP for SOX Content	18
Configure Logger CIP for SOX	19
Identify SOX-Related Devices	19
Classify SOX-Related Devices in SOX Device Group	19
Create SOX Report Category Filter(s)	20

---

Designate a Storage Group for SOX-Related Events .....	21
Select Specific Devices Individually .....	21
Configure Reports with Site-Specific Data .....	21
Providing Site-Specific Data for Reports Using Parameters .....	22
Providing Site-Specific Data for Reports Requiring Customization .....	23
Run a Logger CIP for SOX Report .....	23
Schedule a Logger CIP for SOX Report .....	26
Uninstall Logger CIP for SOX .....	27
<b>Chapter 3: Logger CIP for SOX Contents .....</b>	<b>31</b>
Parameters .....	31
adminUsers .....	31
allowedPorts .....	32
databaseAdminAccounts .....	32
databaseAdminUsers .....	32
destinationUserName .....	32
developmentNetwork .....	33
internalNetwork .....	33
productionNetwork .....	33
testingNetwork .....	33
thirdPartyNetwork .....	34
wirelessNetwork .....	34
Reports and Queries .....	34
ISO 4: Risk Assessment and Treatment .....	35
Resources .....	35
ISO 5: Security Policy .....	35
Resources .....	35
ISO 6: Organization of Information Security .....	36
Resources .....	36
ISO 7: Asset Management .....	38
Resources .....	38
ISO 8: Human Resources Security .....	38
Resources .....	38
ISO 9: Physical and Environmental Security .....	39
Resources .....	39
ISO 10: Communications and Operations Management .....	39
Resources .....	40
ISO 11: Access Control .....	45
Resources .....	45
ISO 12: Information Systems Acquisition Development and Maintenance .....	49
Resources .....	49
ISO 13: Information Security Incident Management .....	51
Resources .....	51

---

ISO 14: Business Continuity Management .....	52
Resources .....	52
ISO 15: Compliance .....	53
Resources .....	53
<b>Index .....</b>	<b>57</b>

---

# About This Book

---

ArcSight Logger™ is a hardware storage solution optimized for extremely high event throughput. An event is a time-stamped log entry, either sent by protocols such as syslog, or appended to a log file. ArcSight Logger receives and stores events, and can optionally forward selected events.

ArcSight Logger™ Compliance Insight Package for Sarbanes-Oxley (Logger CIP for SOX) is a stand-alone solution that is installed on ArcSight Logger. Logger CIP for SOX is used in combination with ArcSight Logger to meet the security monitoring requirements of a Sarbanes-Oxley (SOX) compliance program.

- [“Who Should Read this Guide” on page vii](#)
- [“How to Use this Guide” on page vii](#)
- [“Related Documentation” on page ix](#)

## Who Should Read this Guide

This guide is intended for ArcSight Logger™ administrators and users who need to use ArcSight Logger to meet security management requirements as part of a Sarbanes-Oxley compliance program. Users should have knowledge of:

- Sarbanes-Oxley security monitoring requirements
- Your company's security monitoring practices
- SQL query building principles

## How to Use this Guide



This guide provides an overview of Logger CIP for SOX, instructions about how to install and configure the CIP, and instructions about how to use it. Use the table below to assist you in finding the information you need.

Chapter	Description
Preface	Describes the scope of Logger CIP for SOX, the audience for this book, and related documentation.
1	<b>Overview.</b> Provides a brief description of ArcSight Logger and the Sarbanes-Oxley standard. Describes how the Logger CIP for SOX obtains event data from devices that are subject to SOX compliance, and provides an overview of the Logger CIP for SOX setup and usage process.


Chapter	Description
2	<b>Installation and Configuration.</b> Describes how to install and configure Logger CIP for SOX and run reports. Includes uninstall instructions.
3	<b>Logger CIP for SOX Contents.</b> Lists all the reports available with Logger CIP for SOX, including a description and configuration instructions.
Index	<a href="#">"Index" on page 57</a>

## Text Conventions

The following text conventions appear throughout the ArcSight™ Compliance Insight Package Guide Sarbanes-Oxley v4.0.

Text	Description and Example
<b>Bold</b>	Bold is used to indicate an on-screen element that a user should click. <ul style="list-style-type: none"><li>Enter a value and click <b>OK</b>.</li></ul>
<code>Code</code>	A code character tag indicates code elements. <ul style="list-style-type: none"><li>The timestamp value is made up of seven elements: <code>dd_mmm_yyyy_hh:mm:ss_utc</code>, for example, <code>21 Oct 2007 17:28:02 PDT</code></li></ul>
<i>Emphasis or BookName</i>	<i>Italics</i> indicate emphasis or a book name. <ul style="list-style-type: none"><li><i>Do not</i> perform this procedure until you have backed up your data.</li><li>For more information, see the <i>ArcSight Logger™ Administrator's Guide</i>.</li></ul>
<b>menu &gt; submenu</b>	Right angle brackets are used to indicate steps in a command sequence and online Help topic sequences. <ul style="list-style-type: none"><li>command &gt; subcommand &gt; subcommand</li><li>Authoring &gt; Rules &gt; Rule Actions &gt; Updating Session Lists</li></ul>
tab   subtab	Vertical bars are used to separate multi-level editor-tab sequences. <ul style="list-style-type: none"><li>tab   subtab   subtab</li></ul>
/ Forward slash /	Forward slashes are used to separate resource URI strings and other file paths. <ul style="list-style-type: none"><li>All Reports/System Reports/Asset/All Assets</li></ul>
	The exclamation point icon represents a <b>caution</b> . Cautions provide information that when ignored may cause system damage, data loss, or bodily injury.
	The lightbulb icon represents a <b>tip</b> . Tips provide helpful suggestions and best practices about how to get optimum results from a feature or procedure.



Text	Description and Example
	The speech bubble icon represents a <b>note</b> . Notes provide additional information about a feature or procedure that might help the user make decisions, or inform users about outcomes they can expect.

## Related Documentation

The following ArcSight Logger documentation is included with ArcSight Logger.

Document Title	Description
ArcSight Logger™ Quickstart Guide	Initial starting point for getting started with the ArcSight Logger. A printed copy of this guide is provided with ArcSight Logger.
ArcSight™ Hardware Setup Guide	Describes how to physically install the ArcSight Logger appliance into the rack. A printed copy of this guide is provided with ArcSight Logger.
ArcSight Logger™ Administrator's Guide and Online Help	Describes ArcSight Logger, how to install, initialize, and deploy it in your network environment and how to use it to find and analyze events using reports. The <i>ArcSight Logger™ Online Help</i> is the <i>ArcSight Logger™ Administrator's Guide</i> in a context-sensitive, online format and is available from the ArcSight Logger™Web console. The <i>ArcSight Logger™ Administrator's Guide</i> is available as a PDF book from the Online Help.



# Overview of Logger CIP for SOX

---

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 below. Logger CIP for SOX is a stand-alone package that is installed on ArcSight Logger™.

- [“About ArcSight Logger™” on page 2](#)
- [“Sarbanes-Oxley Act and Security Monitoring Requirements” on page 2](#)
- [“Logger CIP for SOX” on page 2](#)
- [“About the Logger CIP for SOX Reports” on page 5](#)

## 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 throughput. 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*. The *ArcSight Logger™ Online Help* is the *ArcSight Logger™ Administrator's Guide* in a context-sensitive, online format and is available from the ArcSight Logger™ Web console. The *ArcSight Logger™ Administrator's Guide* is available as a PDF book from the *Online Help*.

## 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 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.

## Logger CIP for SOX

ArcSight Logger™ Compliance Insight Package for Sarbanes-Oxley (Logger CIP for SOX) provides an immediate structure to support Sarbanes-Oxley security-monitoring requirements. Logger CIP for SOX provides a set of comprehensive reports designed to evaluate risk, initiate immediate response, and provide comprehensive reporting of high and low-risk activity to help companies immediately address common Sarbanes-Oxley security-monitoring requirements.

Logger CIP for SOX is a layered solution that supports a strong approach to compliance through the combination of the ISO-17799:2005 and the NIST 800-53 standards. The NIST 800-53 control standard is leveraged to provide comprehensive technical checks for the assessment and monitoring of IT controls, including access control and authorization, log monitoring and change management. These technical checks are then automatically mapped to the ISO 17799:2005 standard to place them in the proper risk and operational context.

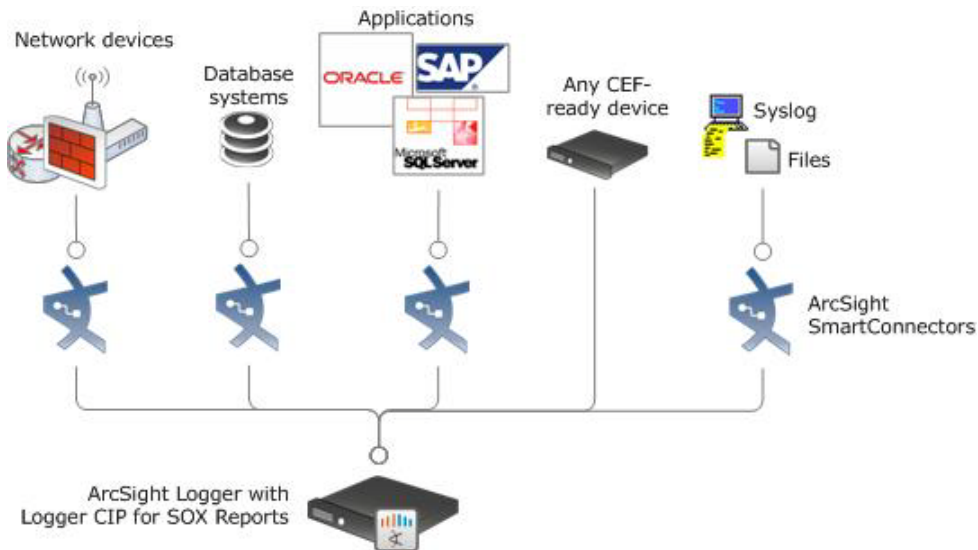
For Sarbanes-Oxley compliance, companies must collect and monitor security-related events, such as user and account management, access control and authorization and change management for financial applications and supporting IT systems. This also includes monitoring other systems that interact with and protect these systems, such as ERP applications, databases, firewalls, and intrusion detection systems. Logger CIP for SOX was designed to provide comprehensive query functionality for systems and devices that are regulated by Sarbanes-Oxley, including:

- Financial applications, such as Oracle, SAP, Peoplesoft, JD Edwards and Siebel
- Databases that store financial data
- Operating systems
- Host and network-based IDS systems
- Perimeter security solutions
- Other supporting applications, such as spreadsheets and system reports

## 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.



**Figure 1-1** Logger CIP for SOX operates on events received from devices on the network in CEF format. SOX-relevant devices that are not already CEF-ready should be run through an ArcSight SmartConnector.

For more about CEF events and how they are used by Logger, see *Appendix A: Common Event Format* in the *ArcSight Logger™ Administrator's Guide*.

## 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 19](#).

## 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 20](#).

For instructions about how to run a report, see ["Run a Logger CIP for SOX Report" on page 23](#).

## 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 19](#).

For instructions about how to run a report, see ["Run a Logger CIP for SOX Report" on page 23](#).

## 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 23](#).

## 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 21](#).

For instructions about how to run a report using this method, see [“Run a Logger CIP for SOX Report” on page 23](#).

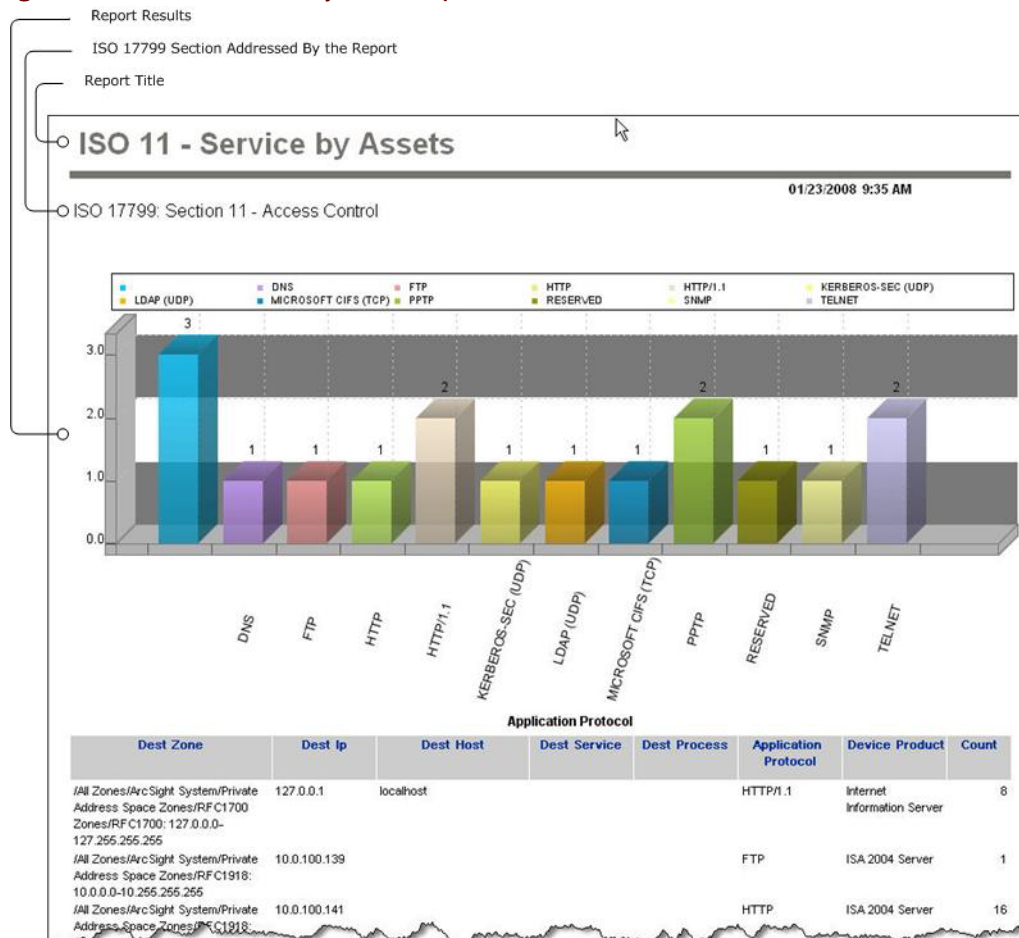
## About the Logger CIP for SOX Reports

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 21](#).

## 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 in [Figure 1-2 on page 5](#).

**Figure 1-2 ISO 11 - Service by Assets Report**



For details about how to run reports, see [“Run a Logger CIP for SOX Report” on page 23](#).

## What’s Next

The next chapter describes how to deploy Logger CIP for SOX to your existing ArcSight Logger v2.0 appliance, and how to set up the device groups and/or filters required to trigger Logger CIP for SOX reports.



## Chapter 2

# Deployment and Configuration

---

This section describes how to deploy Logger CIP for SOX v4.0, and how to configure it to work in your environment.

- [“Before Deploying” on page 7](#)
- [“Deploy Logger CIP for SOX” on page 15](#)
- [“Verify Logger CIP for SOX Content” on page 18](#)
- [“Configure Logger CIP for SOX” on page 19](#)
- [“Uninstall Logger CIP for SOX” on page 27](#)

## Before Deploying

Before deploying Logger CIP for SOX v4.0, verify the ArcSight Logger is running the correct version for the appropriate Logger type:

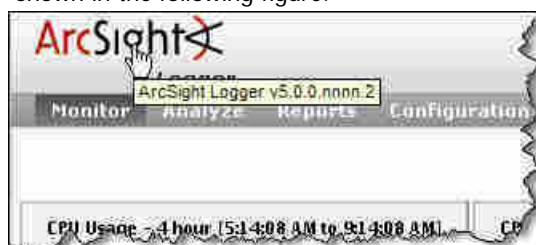
- [“Verify the Software Logger Version” on page 7](#)—Software Logger is the downloadable version of Logger installed on your hardware.
- [“Verify the Logger Appliance Version” on page 8](#)—Logger Appliance is the preconfigured hardware version of Logger.

## Verify the Software Logger Version

Before deploying Logger CIP for SOX v4.0, verify that the software Logger is installed and running ArcSight Logger v5.0 Patch 2 or greater.

**To verify that the Software Logger is running ArcSight Logger v5.0 Patch 2 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*.
- 2 Place the cursor over the ArcSight logo located at the top-left corner of the panel as shown in the following figure.



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.



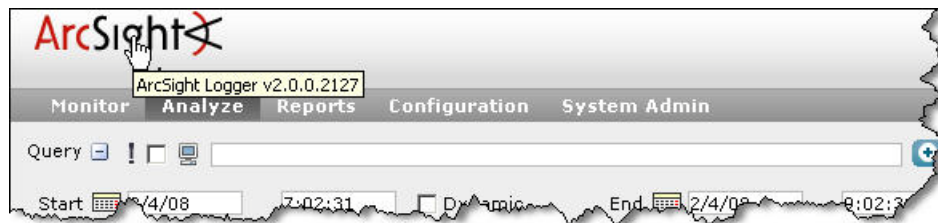
If the version string does not display, move the cursor away from the logo and then back onto the logo.

## Verify the Logger Appliance Version

Before deploying Logger CIP for SOX v4.0, verify that the Logger appliance is running ArcSight Logger v2.0 Patch 1 (2.0.0.2127) or greater.

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

- 3 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*.
- 4 From the Logger navigation bar, click **Analyze**.
- 5 Place the cursor over the ArcSight logo located at the top-left corner of the panel as shown in the following figure.



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



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

## Supported Devices

The device groups listed in [Table 2-1 on page 9](#) 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.

**Table 2-1** 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	
ISO 6 - Administrative Logins and Logouts to Third-Party Hosts	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										
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	

Report Name	IDS/IPS	NBAD	DB	OS	FW	VPN	VA	IDM	PM	NE	CS, WF	AV	W	App	PSS
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	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	X	
ISO 10 - Administrator Actions	X	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	
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										
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					

Report Name	IDS/IPS	NBAD	DB	OS	FW	VPN	VA	IDM	PM	NE	CS, WF	AV	W	App	PSS
<a href="#">ISO 10 - Number of Successful Administrative Logins</a>	X	X	X	X	X	X	X	X	X	X	X	X	X	X	
<a href="#">ISO 10 - Number of Successful User Logins</a>	X	X	X	X	X	X	X	X	X	X	X	X	X	X	
<a href="#">ISO 10 - Number of Unsuccessful Administrative Logins</a>	X	X	X	X	X	X	X	X	X	X	X	X	X	X	
<a href="#">ISO 10 - Number of Unsuccessful User Logins</a>	X	X	X	X	X	X	X	X	X	X	X	X	X	X	
<a href="#">ISO 10 - Operating System Configuration Changes</a>				X											
<a href="#">ISO 10 - Production Network Not Segregated</a>	X	X	X	X	X	X			X	X	X		X	X	
<a href="#">ISO 10 - Resource Exhaustion</a>			X	X	X					X					
<a href="#">ISO 10 - Successful Brute Force Logins</a>	X	X													
<a href="#">ISO 10 - System Restarted</a>				X											
<a href="#">ISO 10 - Test Network Not Segregated</a>	X	X	X	X	X	X			X	X	X		X	X	
<a href="#">ISO 10 - Top Unsuccessful Administrative Logins</a>	X	X	X	X	X	X	X	X	X	X	X	X	X	X	
<a href="#">ISO 10 - Top Unsuccessful User Logins</a>	X	X	X	X	X	X	X	X	X	X	X	X	X	X	
<a href="#">ISO 10 - Unsuccessful User Logins</a>	X	X	X	X	X	X	X	X	X	X	X	X	X	X	
<a href="#">ISO 10 - User Logins and Logouts</a>	X	X	X	X	X	X	X	X	X	X	X	X	X	X	
<a href="#">ISO 10 - Virus Summary by Hosts</a>												X			
<a href="#">ISO 10 - Virus Summary by Virus Name</a>												X			
<a href="#">ISO 10 - VPN Access Summary</a>						X									
<a href="#">ISO 11 - Account Activity by User</a>	X	X	X	X	X	X	X	X	X	X	X	X	X	X	
<a href="#">ISO 11 - Blocked Firewall Traffic</a>					X										
<a href="#">ISO 11 - Database Privilege Violation</a>			X												
<a href="#">ISO 11 - Default Vendor Account Used</a>	X	X	X	X	X	X	X		X	X	X	X	X		
<a href="#">ISO 11 - Insecure Services</a>	X	X	X	X	X	X	X			X	X		X		
<a href="#">ISO 11 - Login From Multiple IPs - Detail</a>	X	X	X	X	X	X	X	X	X	X	X	X	X	X	
<a href="#">ISO 11 - Login From Multiple IPs - Overview</a>	X	X	X	X	X	X	X	X	X	X	X	X	X	X	
<a href="#">ISO 11 - Multiple User Login - Detail</a>	X	X	X	X	X	X	X	X	X	X	X	X	X	X	
<a href="#">ISO 11 - Multiple User Login - Overview</a>	X	X	X	X	X	X	X	X	X	X	X	X	X	X	
<a href="#">ISO 11 - Network Routing Configuration Changes</a>					X					X					
<a href="#">ISO 11 - Privileged Account Changes - All</a>	X	X	X	X	X	X		X	X	X	X	X	X		
<a href="#">ISO 11 - Privileged Account Changes - Successful</a>	X	X	X	X	X	X		X	X	X	X	X	X		
<a href="#">ISO 11 - Removal of Access Rights</a>	X	X	X	X	X	X		X	X	X	X	X	X		

Report Name	IDS/IPS	NBAD	DB	OS	FW	VPN	VA	IDM	PM	NE	CS, WF	AV	W	App	PSS
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		
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											
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		
ISO 13 - Internal Reconnaissance - Top 20 Targets	X				X		X			X	X		X		

Report Name	IDS/IPS	NBAD	DB	OS	FW	VPN	VA	IDM	PM	NE	CS, WF	AV	W	App	PSS
<a href="#">ISO 14 - Availability Attacks</a>	X	X			X					X	X		X		
<a href="#">ISO 15 - Email Receivers by Amount - Top 100</a>	X				X						X			X	
<a href="#">ISO 15 - Email Receivers by Size - Top 100</a>	X				X						X			X	
<a href="#">ISO 15 - Email Senders by Amount - Top 100</a>	X				X						X			X	
<a href="#">ISO 15 - Email Senders by Size - Top 100</a>	X				X						X			X	
<a href="#">ISO 15 - Information Leaks - Organizational</a>	X	X			X										
<a href="#">ISO 15 - Information Leaks - Personal</a>	X	X			X										
<a href="#">ISO 15 - Information System Audit Tool Logins</a>	X	X			X										
<a href="#">ISO 15 - Largest Emails - Top 20</a>	X				X						X			X	
<a href="#">ISO 15 - Peer to Peer Ports Count</a>	X	X			X			X	X	X			X		
<a href="#">ISO 15 - Peer to Peer Sources by Machine - Detail</a>	X	X			X			X	X	X			X		
<a href="#">ISO 15 - Peer to Peer Sources by Machine - Overview</a>	X	X			X			X	X	X			X		
<a href="#">ISO 15 - Policy Breaches</a>	X			X	X	X		X	X	X	X	X	X		
<a href="#">ISO 15 - Possible Intellectual Property Rights Violation</a>	X	X							X		X				

### Key

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 [Table 2-1 on page 9](#). 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 [Table 2-1 on page 9](#) 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 v4.0 on an ArcSight Logger, follow the appropriate procedure for your Logger type:

- [“Deploy Logger CIP for SOX on the Software Logger” on page 15](#)—Software Logger is the downloadable version of Logger installed on your hardware.
- [“Deploy Logger CIP for SOX on the Logger Appliance” on page 16](#)—Logger Appliance is the preconfigured hardware version of Logger.

## Deploy Logger CIP for SOX on the Software Logger

This section describes how to deploy Logger CIP for SOX v4.0 on the software version of Logger.



You must log into software Logger and open the Reports page at least once before installing the Solutions package.

### To deploy Logger CIP for SOX v4.0 on the Software Logger:

- 1 On the system running the software Logger, 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.4.0.nnnn.bin](#) where [nnnn](#) is the four-digit build number) from the ArcSight support site: <https://support.arcsight.com/> to the system that has the software Logger installed.



The four-digit build number is specified in the *Release Notes ArcSight™ Compliance Insight Package SOX v4.0*.

- 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.4.0.nnnn.bin
```
- 5 Run the installer:
 

```
./ArcSight-ComplianceInsightPackage-Logger-SOX.4.0.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 18](#)

## Deploy Logger CIP for SOX on the Logger Appliance

This section describes how to install Logger CIP for SOX v4.0 on a Logger appliance.



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

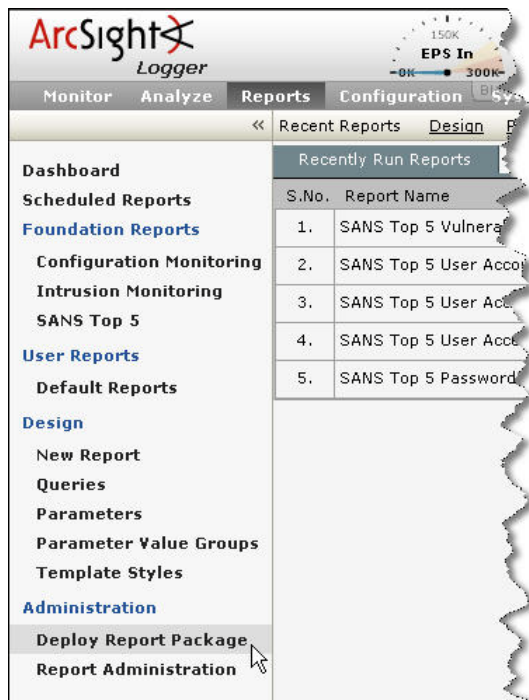
### To install Logger CIP for SOX v4.0 on a Logger Appliance:

- 1 Using the log-in credentials supplied to you by ArcSight, download the Logger CIP for SOX cab file ([ArcSight-ComplianceInsightPackage-Logger-SOX.4.0.nnnn.cab](#), where *nnnn* is the four-digit build number) from the ArcSight support site: <https://support.arcsight.com/> to a local computer to which ArcSight Logger has access.



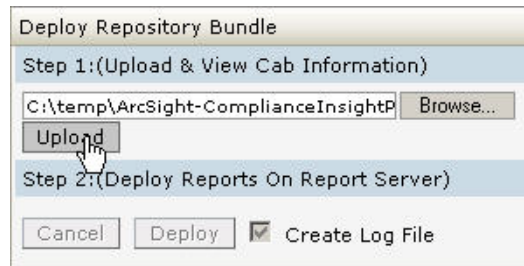
The four-digit build number is specified in the *Release Notes ArcSight™ Compliance Insight Package SOX v4.0*.

- 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* chapter 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 file you downloaded in [Step 1 on page 16](#).

- 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.

**Legends**

- Object will be updated
- Object will not be updated
- New Object
- Deny deploying
- Public Category
- Private Category
- Public Studio Report
- Private Studio Report
- Public Report
- Private Report

**Cab File Information:**

Cab Version	Creation Date	01-30-2008 04:19
Creator	Company	ArcSight Inc.

**Cab Summary:**

Categories	1	Reports	130	Query Objects	126	Parameter Objects	11	Database connections	0
Organizations	0	Users	0	Roles	0	Print Settings	0	Dashboards	0
Schedules	0	Tasks	0	Jobs	0	Client Configuration Files	0	Server Configuration	0
System Files	2	Portal Themes	0	Plugin Files	0				

Report | Users and Roles | Server configuration | Schedules | Client Configuration | Miscellaneous | System Files

**Reports**

**Category Name:** Sarbanes Oxley 130 Reports

Report Name	Version	Previous Version
ISO 10 - Malicious Code Sources	🟢 🏠	
ISO 12 - Vulnerability Scanner Results	🟢 🏠	
ISO 13 - Internal Reconnaissance - Top 20 Targets	🟢 🏠	
ISO 13 - Covert Channel Activity	🟢 🏠	
ISO 10 - Attacks - Production to Development	🟢 🏠	
ISO 6 - Policy Violations from Third-Party Systems	🟢 🏠	



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. Proceed to the next section.

## 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](#).

S.No.	Report Name	Quick Run	Run	Published	Edit	Description	Delete
1.	ISO 4 - High Risk Events						
2.	ISO 4 - High Risk Events by Zone						
3.	ISO 4 - Top 10 High Risk Events						
4.	ISO 5 - Machines Conducting Policy Breaches						
5.	ISO 5 - New Hosts						
6.	ISO 5 - New Services						
7.	ISO 5 - Top 20 Policy Breach Events						
8.	ISO 6 - Administrative Logins and Logouts from Third-Party Hosts						
9.	ISO 6 - Administrative Logins and Logouts to Third-Party Hosts						
10.	ISO 6 - Attacks from Third-Party Systems						
11.	ISO 6 - Attacks on Third-Party Systems						
12.	ISO 6 - Compromised Third-Party Systems						
13.	ISO 6 - Failed Admin Logins from Third-Party Systems						
14.	ISO 6 - Failed Admin Logins to Third-Party Systems						



To refresh the left panel menu and view the [Solution Reports/Sarbanes Oxley](#) reports, you may have to 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.

## 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” on page 19](#)—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 21](#)—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 26](#)—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 23](#).

## 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.



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 21](#).

As outlined in [“How the Logger CIP for SOX Identifies SOX-Related Events” on page 3](#), there are several methods for identifying SOX-related devices:

- [“Classify SOX-Related Devices in SOX Device Group” on page 19](#)
- [“Create SOX Report Category Filter\(s\)” on page 20](#)
- [“Designate a Storage Group for SOX-Related Events” on page 21](#)
- [“Select Specific Devices Individually” on page 21](#)

You can use any of these methods, or some in combination.

## 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™ Online Help* or the *ArcSight Logger™ Administrator's Guide*.

- 6 Click **Save** to create the new Device Group, or **Cancel** to abandon it.

For more information about device groups, see the *Device Groups* topic in the *ArcSight Logger™ Online Help* or the *ArcSight Logger™ Administrator's Guide*.

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 23](#) and use the instructions provided in the procedure called [“To Quick Run a Report:” on page 24](#).

## Create SOX Report Category Filter(s)

Report category filters are a feature available with ArcSight Logger v2.0 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 Add a filter of the type: *Search Group*:
  - a From the Logger navigation bar, select **Configuration**.
  - b From the left panel menu, select **Filters** and click **Add**.
  - c 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 <a href="#">SOX Devices</a> .
Type	From the drop-down menu, select <b>Search Group</b> . 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:  <a href="#">DeviceGroup=SOX</a> or <a href="#">Device=10.10.10.10</a>

- 2 Click **Save**.

- 3 Assign the SOX search group filter you created in [Step 1](#) 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 the drop-down menu associated with the [Sarbanes Oxley](#) reports group, select the filter you created in [Step 1](#) and click **Save**.

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

For instructions about how to schedule reports, see ["Schedule a Logger CIP for SOX Report" on page 26](#).

## 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™ Online Help* or 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 23](#) and use the instructions provided in the procedure called ["To Quick Run a Report:" on page 24](#).

## 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 23](#) and use the instructions provided in the procedure called ["To Quick Run a Report:" on page 24](#).

## 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" on page 22](#).
- 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 23](#).
- 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 34](#).



## 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.

The screenshot shows a text input field with the label "Administrative User(s)\*" and a character count "(30/300 Entered)". The field contains the text "'admin','administrator','root'".

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 in the following figure.

The screenshot shows the same text input field as before, but now it contains the text "'adm','root'", indicating the default value has been updated.

You can specify one or more user names for this field, for example: `'adm','root'`. Each account name must be 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 34](#).

### 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 34](#) 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™ Online Help* or 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 Reports* topic in the *ArcSight Logger™ Administrator's Guide*.

To schedule a report, see [“Schedule a Logger CIP for SOX Report” on page 26](#).

- 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:” on page 24](#)—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 19](#)).
- ◆ [“To Run a Report:” on page 25](#)—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 [Table 2-2 on page 24](#) and click **Run Report**.


**Table 2-2 Report Parameters Panel**

Field	What to enter
Any parameter(s) required by the report	<p>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.</p> <p>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 <a href="#">“Reports and Queries” on page 34</a>.</p> <p>For example, the <a href="#">ISO 11 - Account Activity by User</a> report invokes the <a href="#">ISO 11-Account Activity by User Name</a> query. The <a href="#">ISO 11-Account Activity by User Name</a> query takes as input the <code>destinationUserName</code> parameter. When the <a href="#">ISO 11 - Account Activity by User</a> report is run, you are prompted to provide a User Name value to pass to the query via the <code>destinationUserName</code> parameter.</p> <p>For information about providing a default value for a parameter, see <a href="#">“To change the default value of a parameter:” on page 22</a>.</p>
Start	<p>This indicates the start of the time range of events you want the query to evaluate. The default is the time dynamic value <code>\$Now - 2h</code>, meaning the last two hours of event data starting from the moment you click Run Report.</p> <ul style="list-style-type: none"> <li>Adjust this dynamic timeframe in increments of hours (h), minutes (m), or days (d).</li> <li>Uncheck the <i>Dynamic</i> box to specify a particular date and time.</li> </ul>
End	<p>This indicates the end of the time range of events you want the query to evaluate. The default is the time dynamic value <code>\$Now</code>, meaning the moment you click Run Report.</p> <ul style="list-style-type: none"> <li>Adjust this dynamic timeframe in increments of hours (h), minutes (m), or days (d).</li> <li>Uncheck the <i>Dynamic</i> box to specify a particular date and time.</li> </ul>

Field	What to enter
Device Groups	<p>If all the devices in your environment are subject to SOX compliance, it is not necessary to specify a device group.</p> <p>If you are using device groups to focus your reports, you should have created a SOX device group during the configuration process (see <a href="#">“Classify SOX-Related Devices in SOX Device Group” on page 19</a>). Ctrl + click the SOX device group to select it as a parameter to be used.</p>
Storage Groups	<p>If your environment uses a specific storage policy for SOX-related events (as described in <a href="#">“Designate a Storage Group for SOX-Related Events” on page 21</a>), select (Ctrl + click) the storage group you want the report to query.</p>
Devices	<p>Optionally, you can select (Ctrl + click) particular devices whose events you want the report to evaluate.</p>



### 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 [Table 2-3 on page 25](#) and click **Run**.

**Table 2-3 Run Report Panel**

Field	What to enter
Template	<p>From the drop-down menu, select the report template you want to apply to the report. The default report template is <b>sox</b>.</p> <p>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.</p>
Multipage	<p>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.</p> <p>For online formats, such as HTML, it is easier to view the results as a single, continuous page.</p> <p>The Multipage checkbox is not selected by default.</p>
Report Format	<p>From the drop-down menu, select the output format for your report (HTML, PDF, Microsoft Excel, comma separated, text, Microsoft Word, interactive, XML, raw text).</p>
Max. Rows	<p>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 <a href="#">“Schedule a Logger CIP for SOX Report” on page 26</a>.</p> <p>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.</p> <p>Leave this field blank if you want the report to evaluate all the rows included in a time range.</p>

Field	What to enter
Field	From the drop-down menu, select one of the available fields from the report.
Criteria	From the drop-down menu, select a SQL operator ( <a href="#">above</a> , <a href="#">below</a> , <a href="#">is</a> , <a href="#">is not</a> , <a href="#">starts with</a> , <a href="#">ends with</a> , <a href="#">contains</a> , 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.

The Report Parameter panel displays in a separate window.

- 3 In the Report Parameters panel, enter the values listed in [Table 2-2 on page 24](#) 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	<p>Set the frequency for the scheduled run of the report.</p> <p>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".</p> <p>You can choose to run the report at a certain hour every day "Hour of the Day" or "Every" hour so many hours.</p>
Report Name	<p>Select a report from the list, and click <b>Go</b> to load the report.</p> <p> You must click <b>Go</b> 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.</p>


Option	Description
Delivery Options	<p>Depending on which delivery option you choose, the associated parameters are displayed. Click to enable (check) or disable (uncheck) these options.</p> <p>Both E-mail and Publish options for scheduled reports are the same as those provided after you run a report "on demand".</p> <p>Select a delivery option:</p> <ul style="list-style-type: none"> <li>• <b>Email</b> - For details on setting e-mail delivery options, see the <i>ArcSight Logger™ Administrator's Guide</i>.</li> <li>• <b>Publish</b> - For details on setting publishing options, see the <i>ArcSight Logger™ Administrator's Guide</i>.</li> </ul>
Report Format	<p>Select a report format (Acrobat PDF, HTML, and so forth).</p> <p>For details on report formats, see the <i>ArcSight Logger™ Administrator's Guide</i>.</p>
Report Parameters	<p>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.</p> <p>For more information about the site-specific data parameters, see the report tables provided in <a href="#">"Reports and Queries" on page 34</a>.</p> <p>For more information about providing a default value for a parameter, see <a href="#">"To change the default value of a parameter:" on page 22</a>.</p> <p>For information on specifying report parameters, see the <i>ArcSight Logger™ Administrator's Guide</i>.</p>

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

## 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 at the top of the panel, and the report no longer appears in the right panel:

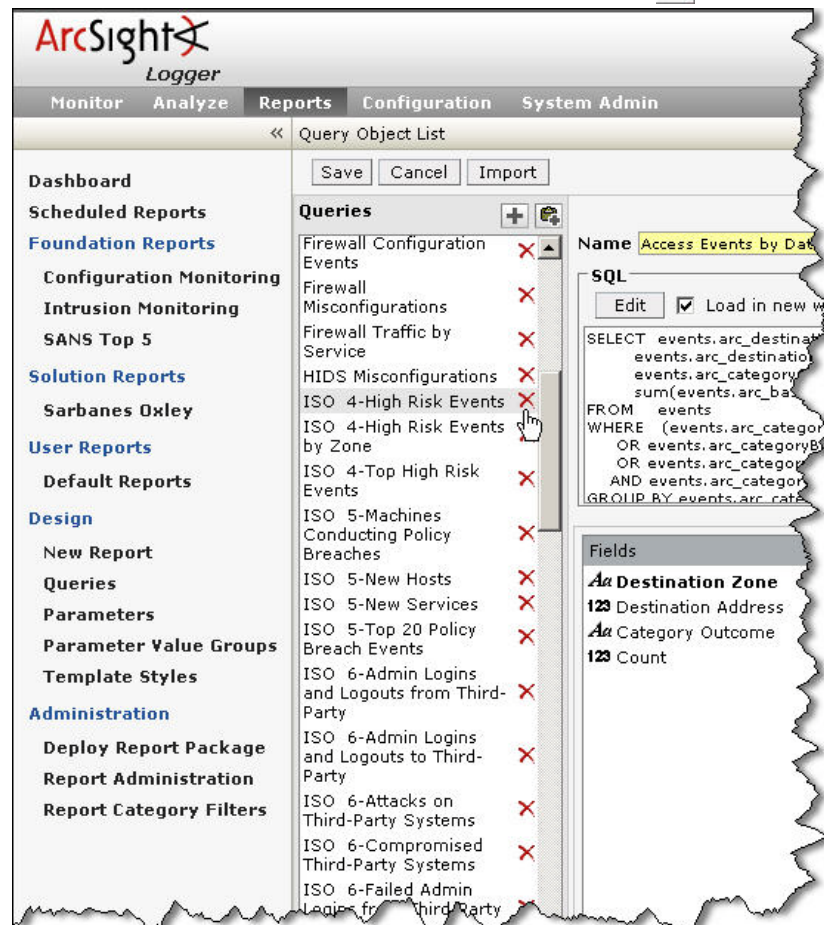


Report successfully deleted from the repository.

- c Repeat [Step a](#) and [Step b](#) for every report 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 (**X**).



- b Repeat [Step a](#) for 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.

- From the Logger navigation bar, select **Reports**.
- From the left panel menu, select **Design/Parameters**.
- 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`



The following parameters are used by the queries in the Foundation Reports and should not be deleted:

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

- Repeat [Step c](#) for each of the SOX parameters.
- 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

Parameter Object List

Deleted report object : adminUsers Deleted report object : allowedPorts Deleted report object : databaseAdminAccounts Deleted report object : databaseAdminUsers Deleted report object : destinationUserName Deleted report object : developmentNetwork Deleted report object : internalNetwork Deleted report object : productionNetwork Deleted report object : testingNetwork Deleted report object : thirdPartyNetwork Deleted report object : wirelessNetwork

Save Cancel

**Parameters**

commonlyBlockedPorts destinationAddress destinationPort deviceGroupParameter deviceProduct deviceVendor IPAddress webPorts zones

**Parameters**

Name `commonlyBlockedPorts`

Prompt Blocked Ports

Data Type NUMBER

Size 30

Format

Default Value 21,23,135,136,137

Input Type ☐ TextBox ☒ Combo ☐ Option

**Pre Defined List**

Display Name	Value
21	21
23	23
135	135
136	136
137	137
138	138
139	139
443	443
445	445

Parameter Name



# 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.

- [“Parameters” on page 31](#)
- [“Reports and Queries” on page 34](#)

## 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” on page 31](#)
- [“allowedPorts” on page 32](#)
- [“databaseAdminAccounts” on page 32](#)
- [“databaseAdminUsers” on page 32](#)
- [“destinationUserName” on page 32](#)
- [“developmentNetwork” on page 33](#)
- [“internalNetwork” on page 33](#)
- [“productionNetwork” on page 33](#)
- [“testingNetwork” on page 33](#)
- [“thirdPartyNetwork” on page 34](#)
- [“wirelessNetwork” on page 34](#)

## 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 via the `adminUsers` parameter. Supply the set of administration 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 22](#).

## allowedPorts

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 via 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 22](#).

## 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 via the `databaseAdminAccounts` parameter. Supply the set of database administration 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 22](#).

## 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 via the `databaseAdminUsers` parameter. Supply the network accounts used to administer 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 22](#).

## 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 via 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 22](#).

## 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 via 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 23](#).

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 22](#).

## 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 via the `internalNetwork` 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 23](#).

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 22](#).

## 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 23](#).

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 22](#).

## 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 via 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 23](#).

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 22](#).

## 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 via 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 23](#).

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 22](#).

## wirelessNetwork

When a report is run that invokes a query which expects the `wirelessNetwork` parameter as input, the Wireless Network(s) prompt is displayed during report runtime. The value in the Wireless Network(s) text field is passed to the query via the `wirelessNetwork` 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 23](#).

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 22](#).

## Reports and Queries

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

- [“ISO 4: Risk Assessment and Treatment” on page 35](#)
- [“ISO 5: Security Policy” on page 35](#)
- [“ISO 6: Organization of Information Security” on page 36](#)
- [“ISO 7: Asset Management” on page 38](#)
- [“ISO 8: Human Resources Security” on page 38](#)
- [“ISO 9: Physical and Environmental Security” on page 39](#)
- [“ISO 10: Communications and Operations Management” on page 39](#)
- [“ISO 11: Access Control” on page 45](#)

- [“ISO 12: Information Systems Acquisition Development and Maintenance” on page 49](#)
- [“ISO 13: Information Security Incident Management” on page 51](#)
- [“ISO 14: Business Continuity Management” on page 52](#)
- [“ISO 15: Compliance” on page 53](#)



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 v4.0*), 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:

**Table 3-1** 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:

**Table 3-2** 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

Report	Description	Associated Query	Configuration
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 - 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:

**Table 3-3 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	This report prompts you to supply values for the following parameters: <ul style="list-style-type: none"> <li>• <a href="#">“adminUsers” on page 31</a></li> <li>• <a href="#">“thirdPartyNetwork” on page 34</a></li> </ul>
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	This report prompts you to supply values for the following parameters: <ul style="list-style-type: none"> <li>• <a href="#">“adminUsers” on page 31</a></li> <li>• <a href="#">“thirdPartyNetwork” on page 34</a></li> </ul>
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	This report prompts you to supply a value for the following parameter: <ul style="list-style-type: none"> <li>• <a href="#">“thirdPartyNetwork” on page 34</a></li> </ul>
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	This report prompts you to supply a value for the following parameter: <ul style="list-style-type: none"> <li>• <a href="#">“thirdPartyNetwork” on page 34</a></li> </ul>
ISO 6 - Compromised Third-Party Systems	This report displays all successful compromise attempts targeting third-party systems.	ISO 6-Compromised Third-Party Systems	This report prompts you to supply a value for the following parameter: <ul style="list-style-type: none"> <li>• <a href="#">“thirdPartyNetwork” on page 34</a></li> </ul>

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 Sys	This report prompts you to supply values for the following parameters: <ul style="list-style-type: none"> <li>• <a href="#">“adminUsers” on page 31</a></li> <li>• <a href="#">“thirdPartyNetwork” on page 34</a></li> </ul>
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 Sys	This report prompts you to supply values for the following parameters: <ul style="list-style-type: none"> <li>• <a href="#">“adminUsers” on page 31</a></li> <li>• <a href="#">“thirdPartyNetwork” on page 34</a></li> </ul>
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	This report prompts you to supply a value for the following parameter: <ul style="list-style-type: none"> <li>• <a href="#">“thirdPartyNetwork” on page 34</a></li> </ul>
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	This report prompts you to supply a value for the following parameter: <ul style="list-style-type: none"> <li>• <a href="#">“thirdPartyNetwork” on page 34</a></li> </ul>
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	This report prompts you to supply a value for the following parameter: <ul style="list-style-type: none"> <li>• <a href="#">“thirdPartyNetwork” on page 34</a></li> </ul>
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	This report prompts you to supply a value for the following parameter: <ul style="list-style-type: none"> <li>• <a href="#">“thirdPartyNetwork” on page 34</a></li> </ul>
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	This report prompts you to supply a value for the following parameter: <ul style="list-style-type: none"> <li>• <a href="#">“thirdPartyNetwork” on page 34</a></li> </ul>
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	This report prompts you to supply a value for the following parameter: <ul style="list-style-type: none"> <li>• <a href="#">“thirdPartyNetwork” on page 34</a></li> </ul>
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 Sys	This report prompts you to supply a value for the following parameter: <ul style="list-style-type: none"> <li>• <a href="#">“thirdPartyNetwork” on page 34</a></li> </ul>
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	This report prompts you to supply a value for the following parameter: <ul style="list-style-type: none"> <li>• <a href="#">“thirdPartyNetwork” on page 34</a></li> </ul>

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	This report prompts you to supply a value for the following parameter: <ul style="list-style-type: none"> <li>• <a href="#">"thirdPartyNetwork" on page 34</a></li> </ul>
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	This report prompts you to supply a value for the following parameter: <ul style="list-style-type: none"> <li>• <a href="#">"thirdPartyNetwork" on page 34</a></li> </ul>
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	This report prompts you to supply a value for the following parameter: <ul style="list-style-type: none"> <li>• <a href="#">"thirdPartyNetwork" on page 34</a></li> </ul>

## 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:

**Table 3-4** 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	This report prompts you to supply a value for the following parameter: <ul style="list-style-type: none"> <li>• <a href="#">"internalNetwork" on page 33</a></li> </ul>

## 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:



**Table 3-5 ISO:8 Human Resources 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 <a href="#">"Providing Site-Specific Data for Reports Requiring Customization"</a> on page 23.
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 <a href="#">"Providing Site-Specific Data for Reports Requiring Customization"</a> on page 23.
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 Section 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:

**Table 3-6 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:

**Table 3-7 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	This report prompts you to supply a value for the following parameter: <ul style="list-style-type: none"> <li>• <a href="#">“adminUsers” on page 31</a></li> </ul>
ISO 10 - Administrator Actions	This report displays all actions taken by administrator accounts.	ISO 10- Administrator Actions	This report prompts you to supply a value for the following parameter: <ul style="list-style-type: none"> <li>• <a href="#">“adminUsers” on page 31</a></li> </ul>
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

Report	Description	Associated Query	Configuration
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	This report prompts you to supply values for the following parameters: <ul style="list-style-type: none"> <li>• <a href="#">“developmentNetwork” on page 33</a></li> <li>• <a href="#">“productionNetwork” on page 33</a></li> </ul>
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	This report prompts you to supply values for the following parameters: <ul style="list-style-type: none"> <li>• <a href="#">“productionNetwork” on page 33</a></li> <li>• <a href="#">“developmentNetwork” on page 33</a></li> </ul>
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	This report prompts you to supply a value for the following parameter: <ul style="list-style-type: none"> <li>• <a href="#">“developmentNetwork” on page 33</a></li> </ul>
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	This report prompts you to supply a value for the following parameter: <ul style="list-style-type: none"> <li>• <a href="#">“thirdPartyNetwork” on page 34</a></li> </ul>
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

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	This report prompts you to supply values for the following parameters: <ul style="list-style-type: none"> <li>• <a href="#">“developmentNetwork” on page 33</a></li> <li>• <a href="#">“testingNetwork” on page 33</a></li> <li>• <a href="#">“productionNetwork” on page 33</a></li> </ul>
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

Report	Description	Associated Query	Configuration
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 - 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	This report prompts you to supply a value for the following parameter: <ul style="list-style-type: none"> <li>• <a href="#">"adminUsers" on page 31</a></li> </ul>
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	This report prompts you to supply a value for the following parameter: <ul style="list-style-type: none"> <li>• <a href="#">"adminUsers" on page 31</a></li> </ul>
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	This report prompts you to supply a value for the following parameter: <ul style="list-style-type: none"> <li>• <a href="#">"adminUsers" on page 31</a></li> </ul>
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	This report prompts you to supply a value for the following parameter: <ul style="list-style-type: none"> <li>• <a href="#">"adminUsers" on page 31</a></li> </ul> 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

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	This report prompts you to supply values for the following parameters: <ul style="list-style-type: none"> <li>• <a href="#">“productionNetwork” on page 33</a></li> <li>• <a href="#">“testingNetwork” on page 33</a></li> <li>• <a href="#">“developmentNetwork” on page 33</a></li> </ul>
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	This report prompts you to supply values for the following parameters: <ul style="list-style-type: none"> <li>• <a href="#">“testingNetwork” on page 33</a></li> <li>• <a href="#">“developmentNetwork” on page 33</a></li> <li>• <a href="#">“productionNetwork” on page 33</a></li> </ul>

Report	Description	Associated Query	Configuration
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	This report prompts you to supply a value for the following parameter: <ul style="list-style-type: none"> <li>• <a href="#">“adminUsers” on page 31</a></li> </ul>
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	This report prompts you to supply a value for the following parameter: <ul style="list-style-type: none"> <li>• <a href="#">“adminUsers” on page 31</a></li> </ul> Login attempts by the specified administrative users are not reported.
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	This report prompts you to supply a value for the following parameter: <ul style="list-style-type: none"> <li>• <a href="#">“adminUsers” on page 31</a></li> </ul> 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:

**Table 3-8 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	This report prompts you to supply a value for the following parameter: <ul style="list-style-type: none"> <li><a href="#">"destinationUserName" on page 32</a></li> </ul>
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	This report prompts you to supply values for the following parameters: <ul style="list-style-type: none"> <li><a href="#">"databaseAdminAccounts" on page 32</a></li> <li><a href="#">"databaseAdminUsers" on page 32</a></li> </ul>
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. For more information about customizing the query, see <a href="#">"Providing Site-Specific Data for Reports Requiring Customization" on page 23</a> .
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. For more information about customizing the query, see <a href="#">"Providing Site-Specific Data for Reports Requiring Customization" on page 23</a> .
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



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	This report prompts you to supply a value for the following parameter: <ul style="list-style-type: none"> <li>• <a href="#">“adminUsers” on page 31</a></li> </ul>
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	This report prompts you to supply a value for the following parameter: <ul style="list-style-type: none"> <li>• <a href="#">“adminUsers” on page 31</a></li> </ul>

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. For more information about customizing the query, see <a href="#">“Providing Site-Specific Data for Reports Requiring Customization” on page 23</a> .
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	This report prompts you to supply a value for the following parameter: <ul style="list-style-type: none"> <li>• <a href="#">“wirelessNetwork” on page 34</a></li> </ul>
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. For more information about customizing the query, see <a href="#">“Providing Site-Specific Data for Reports Requiring Customization” on page 23</a> .
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	This report prompts you to supply a value for the following parameter: <ul style="list-style-type: none"> <li>• <a href="#">“internalNetwork” on page 33</a></li> </ul>
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	This report prompts you to supply values for the following parameters: <ul style="list-style-type: none"> <li>• <a href="#">“allowedPorts” on page 32</a></li> <li>• <a href="#">“internalNetwork” on page 33</a></li> </ul>

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	This report prompts you to supply values for the following parameters: <ul style="list-style-type: none"> <li>• <a href="#">“allowedPorts” on page 32</a></li> <li>• <a href="#">“internalNetwork” on page 33</a></li> </ul>
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 Systems 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:

**Table 3-9** ISO:12 Information Systems 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

Report	Description	Associated Query	Configuration
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 were changed on each host.	ISO 12-File Changes in Production	This report prompts you to supply a value for the following parameter: <ul style="list-style-type: none"> <li>• <a href="#">“productionNetwork” on page 33</a></li> </ul>
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 - 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	This report prompts you to supply a value for the following parameter: <ul style="list-style-type: none"> <li>• <a href="#">“productionNetwork” on page 33</a></li> </ul>
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:

**Table 3-10** 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 - 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	This report prompts you to supply a value for the following parameter: <ul style="list-style-type: none"> <li><a href="#">"internalNetwork" on page 33</a></li> </ul>
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	This report prompts you to supply a value for the following parameter: <ul style="list-style-type: none"> <li><a href="#">"internalNetwork" on page 33</a></li> </ul>
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

Report	Description	Associated Query	Configuration
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	This report prompts you to supply a value for the following parameter: <ul style="list-style-type: none"> <li>• <a href="#">"internalNetwork" on page 33</a></li> </ul>
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	This report prompts you to supply a value for the following parameter: <ul style="list-style-type: none"> <li>• <a href="#">"internalNetwork" on page 33</a></li> </ul>
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	This report prompts you to supply a value for the following parameter: <ul style="list-style-type: none"> <li>• <a href="#">"internalNetwork" on page 33</a></li> </ul>

## 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:

**Table 3-11** 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 e-mail utilization.

### Resources

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

**Table 3-12** ISO:15 Compliance Reports and Queries

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

Report	Description	Associated Query	Configuration
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 e-mails sent in the organization. The chart displays the number of large e-mails 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. For more information about customizing the query, see <a href="#">"Providing Site-Specific Data for Reports Requiring Customization"</a> on page 23.
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. For more information about customizing the query, see <a href="#">"Providing Site-Specific Data for Reports Requiring Customization"</a> on page 23.



Report	Description	Associated Query	Configuration
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. For more information about customizing the query, see <a href="#">"Providing Site-Specific Data for Reports Requiring Customization"</a> on page 23.
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



# Index

---

## Numerics

- 10 ISO section: Communications and Operations Management 39
- 11 ISO section: Access Control 45
- 12 ISO section: Information Systems Acquisition Development and Maintenance 49
- 13 ISO section: Information Security Incident Management 51
- 14 ISO section: Business Continuity Management 52
- 15 ISO section: Compliance 53
- 4 ISO section: Risk Assessment and Treatment 35
- 5 ISO section: Security Policy 35
- 6 ISO section: Organization of Information Security 36
- 7 ISO section: Asset Management section 38
- 8 ISO section: Human Resources 38
- 9 ISO section: Physical and Environmental Security 39

## A

- access control 45
- account management 45
- Administrative User(s) prompt
  - adminUsers 31
- adminUsers parameter 22, 29, 31, 36, 37, 40, 43, 45, 47
- Allowed Port(s) prompt
  - allowedPorts 32
- allowedPorts parameter 29, 32, 48, 49
- anti-virus
  - devices 13
- antivirus updates 39
- applications 13
- ArcSight Hardware Setup Guide ix
- ArcSight Logger 2
- ArcSight Logger Administrator's Guide ix
- ArcSight Logger Online Help ix
- ArcSight Logger Quickstart Guide ix
- ArcSight SmartConnector 3
- asset inventory 38
- asset management 38
- autodiscovery of devices 20

## B

- business continuity management 52

## C

- CAB file 16
  - deploy 17
  - download 16
  - upload 17

## CEF

- devices 13
- events 3
- format 3
- clauses: ISO 35
- Common Event Format (CEF) 3
- commonlyBlockedPorts parameter 30
- communications and operations management 39
- compliance 53
- configure
  - logger CIP for SOX 19
- content security, web filtering 13

## D

- data retention 2
- database 13
- Database Administration Account(s) prompt
  - databaseAdminAccounts 32
- Database Administrative User(s) prompt
  - databaseAdminUsers 32
- databaseAdminAccounts parameter 29, 32, 46
- databaseAdminUsers parameter 29, 32, 46
- databases 3
- deploy
  - CAB file 17
  - logger CIP for SOX 15
- destinationAddress parameter 30
- destinationGroupParameter parameter 30
- destinationPort parameter 30
- destinationUserName parameter 29, 32, 46
- Development Network(s) prompt
  - developmentNetwork 33
- developmentNetwork parameter 29, 33, 41, 42, 44
- device groups 4, 8, 20, 25
- deviceProduct parameter 30
- devices 25
  - anti-virus 13
  - applications 13
  - autodiscovery 20
  - CEF-enabled 13
  - CEF-ready 3
  - content security, web filtering 13
  - creating 20
  - database 13
  - databases 3
  - ERP applications 3
  - firewalls 3, 13
  - generate using CEF format 3
  - identity management 13
  - IDS 3
  - intrusion detection system 13

- intrusion prevention system 13
- network behavior anomaly detection 13
- network equipment 13
- non-CEF 13
- operating system 13
- operating systems 3
- physical security systems 13
- policy management 13
- SOX 19
- supported 9
- syslog-ready 2
- virtual private network 13
- vulnerability assessment 13
- wireless 13
- deviceVendor parameter 30
- documentation
  - Administrator's Guide ix
  - Hardware Setup Guide ix
  - logger ix
  - Online Help ix
  - Quickstart Guide ix
- download
  - CAB file 16

## E

- employment 38
- ERP applications 3
- events
  - CEF format 3
  - identify SOX-related events 3

## F

- fault logging 39
- filters
  - SOX report category 20
- firewalls 3, 13, 39, 45

## G

- Getting Started Guide ix

## H

- human resources 38

## I

- identity management 13
- IDM 13
- IDS 3, 13
- information security incident management 51
- information systems acquisition development and maintenance 49
- insecure services 45
- Internal Network(s) prompt
  - internalNetwork 33
- Internal Reconnaissance 51
- internalNetwork 29
- internalNetwork parameter 29, 33, 38, 48, 49, 51, 52
- Internet usage 38
- intrusion detection system 13
- intrusion detection systems 3
- intrusion prevention system 13
- invalid certificates 49

- inventory. 38
- IPAddress parameter 30
- IPS 13
- ISO 10 - Account Lockouts by System report 40
  - devices 10
- ISO 10 - Account Lockouts by User report 40
  - devices 10
- ISO 10 - Administrative Logins and Logouts report 40
  - configure 40
  - devices 10
- ISO 10 - Administrator Actions report 40
  - configure 40
  - devices 10
- ISO 10 - Application Configuration Modification report 40
  - devices 10
- ISO 10 - Attacks - Development to Production report 41
  - configure 41
  - devices 10
- ISO 10 - Attacks - Production to Development report 41
  - configure 41
  - devices 10
- ISO 10 - Audit Log Cleared report 41
  - devices 10
- ISO 10 - Changes to Development Network Machines report 41
  - configure 41
  - devices 10
- ISO 10 - Changes to Third-Party Resources report 41
  - configure 41
  - devices 10
- ISO 10 - Database Access - All report 41
  - devices 10
- ISO 10 - Database Access - Failed report 41
  - devices 10
- ISO 10 - Development Network Not Segregated report 42
  - configure 42
  - devices 10
- ISO 10 - Device Configuration Changes report 42
  - devices 10
- ISO 10 - Device Logging Review report 42
  - devices 10
- ISO 10 - Failed Anti-Virus Updates report 42
  - devices 10
- ISO 10 - Fault Logs report 42
  - devices 10
- ISO 10 - File Integrity Changes report 42
  - devices 10
- ISO 10 - Firewall Configuration Changes - All report 42
  - devices 10
- ISO 10 - Firewall Configuration Changes - Successful report 42
  - devices 10
- ISO 10 - Firewall Open Port Review report 43
  - devices 10
- ISO 10 - Information Interception Events report 43
  - devices 10
- ISO 10 - Malicious Code Sources report 43
  - devices 10
- ISO 10 - Network Device Configuration Changes - All report 43
  - devices 10
- ISO 10 - Network Device Configuration Changes - Successful report 43
  - devices 10

- ISO 10 - Number of Successful Administrative Logins report 43
  - configure 43
  - devices 11
- ISO 10 - Number of Successful User Logins report 43
  - configure 43
  - devices 11
- ISO 10 - Number of Unsuccessful Administrative Logins report 43
  - configure 43
  - devices 11
- ISO 10 - Number of Unsuccessful User Logins report 43
  - configure 43
  - devices 11
- ISO 10 - Operating System Configuration Changes report 43
  - devices 11
- ISO 10 - Production Network Not Segregated report 44
  - configure 44
  - devices 11
- ISO 10 - Resource Exhaustion report 44
  - devices 11
- ISO 10 - Successful Brute Force Logins report 44
  - devices 11
- ISO 10 - System Restarted report 44
  - devices 11
- ISO 10 - Test Network Not Segregated report 44
  - configure 44
  - devices 11
- ISO 10 - Top Unsuccessful Administrative Logins report 45
  - configure 45
  - devices 11
- ISO 10 - Top Unsuccessful User Logins report 45
  - configure 45
  - devices 11
- ISO 10 - Unsuccessful User Logins report 45
  - configure 45
  - devices 11
- ISO 10 - User Logins and Logouts report 45
  - devices 11
- ISO 10 - Virus Summary by Hosts report 45
  - devices 11
- ISO 10 - Virus Summary by Virus Name report 45
  - devices 11
- ISO 10 - VPN Access Summary report 45
  - devices 11
- ISO 10-Account Lockouts by System query 40
- ISO 10-Account Lockouts by User query 40
- ISO 10-Administrative Logins and Logouts query 40
  - parameters
  - adminUsers 40
- ISO 10-Administrator Actions query 40
  - parameters
  - adminUsers 40
- ISO 10-Application Configuration Modifications query 40
- ISO 10-Attacks Development to Production query 41
  - parameters
  - developmentNetwork 41
  - productionNetwork 41
- ISO 10-Attacks Production to Development query 41
  - parameters
  - developmentNetwork 41
  - productionNetwork 41
- ISO 10-Audit Log Cleared query 41
- ISO 10-Changes to Development Network Machines query 41
  - parameters
  - developmentNetwork 41
- ISO 10-Changes to Third-Party Resources query 41
  - parameters
  - thirdPartyNetwork 41
- ISO 10-Database Access - All query 41
- ISO 10-Database Access - Failed query 41
- ISO 10-Development to Test or Production query 42
  - parameters
  - developmentNetwork 42
  - productionNetwork 42
  - testingNetwork 42
- ISO 10-Device Configuration Changes query 42
- ISO 10-Device Logging Review query 42
- ISO 10-Failed Anti-Virus Updates query 42
- ISO 10-Fault Logs query 42
- ISO 10-File Integrity Changes Detected query 42
- ISO 10-Firewall Configuration Modifications query 42
- ISO 10-Firewall Open Port Review query 43
- ISO 10-Information Interception query 43
- ISO 10-Malicious Code Sources query 43
- ISO 10-Network Device Configuration Modifications query 43
- ISO 10-Number of Successful Administrative Logins query 43
  - parameters
  - adminUsers 43
- ISO 10-Number of Successful User Logins query 43
  - parameters
  - adminUsers 43
- ISO 10-Number of Unsuccessful User Logins query 43
  - parameters
  - adminUsers 43
- ISO 10-Number Unsuccessful Administrative Logins query 43
  - parameters
  - adminUsers 43
- ISO 10-Operating System Configuration Changes query 43
- ISO 10-Production to Test or Development query 44
  - parameters
  - developmentNetwork 44
  - productionNetwork 44
  - testingNetwork 44
- ISO 10-Resource Exhaustion Detected query 44
- ISO 10-Successful Brute Force Logins query 44
- ISO 10-System Restarted query 44
- ISO 10-Test to Development or Operations query 44
  - parameters
  - developmentNetwork 44
  - productionNetwork 44
  - testingNetwork 44
- ISO 10-Top Unsuccessful Administrative Logins query 45
  - parameters
  - adminUsers 45
- ISO 10-Top Unsuccessful User Logins query 45
  - parameters
  - adminUsers 45
- ISO 10-Unsuccessful User Logins query 45
  - parameters
  - adminUsers 45
- ISO 10-User Logins and Logouts query 45
- ISO 10-Virus Summary by Hosts query 45

- ISO 10-Virus Summary by Virus Name query 45
- ISO 10-VPN Access Summary query 45
- ISO 11 - Account Activity by User report 46
  - configure 46
  - devices 11
- ISO 11 - Blocked Firewall Traffic report 46
  - devices 11
- ISO 11 - Database Privilege Violation report 46
  - configure 46
  - devices 11
- ISO 11 - Default Vendor Account Used report 46
  - configure 46
  - devices 11
- ISO 11 - Insecure Services report 46
  - configure 46
  - devices 11
- ISO 11 - Login From Multiple IPs - Detail report 46
  - devices 11
- ISO 11 - Login From Multiple IPs - Overview report 47
  - devices 11
- ISO 11 - Multiple User Login - Detail report 47
  - devices 11
- ISO 11 - Multiple User Login - Overview report 47
  - devices 11
- ISO 11 - Network Routing Configuration Changes report 47
  - devices 11
- ISO 11 - Privileged Account Changes - All report 47
  - configure 47
  - devices 11
- ISO 11 - Privileged Account Changes - Successful report 47
  - configure 47
  - devices 11
- ISO 11 - Removal of Access Rights report 48
  - devices 11
- ISO 11 - Services by Asset report 48
  - configure 48
  - devices 12
- ISO 11 - Suspicious Activity in Wireless Network report 48
  - configure 48
  - devices 12
- ISO 11 - Systems Accessed as Root or Administrator report 48
  - configure 48
  - devices 12
- ISO 11 - Traffic - Inbound Count report 48
  - configure 48
  - devices 12
- ISO 11 - Traffic - Inbound on Disallowed Ports - All report 48
  - configure 48
  - devices 12
- ISO 11 - Traffic - Inbound on Disallowed Ports - Successful report 49
  - configure 49
  - devices 12
- ISO 11 - Traffic Between Zones - Protocols report 49
  - devices 12
- ISO 11 - User Account Creation report 49
  - devices 12
- ISO 11 - User Account Deletion report 49
  - devices 12
- ISO 11-Account Activity by User Name query 46
  - parameters
    - destinationUserName 46
- ISO 11-Blocked Firewall Traffic query 46
- ISO 11-Database Privilege Violation query 46
  - parameters
    - databaseAdminAccounts 46
    - databaseAdminUsers 46
- ISO 11-Default Vendor Account Used query 46
- ISO 11-Insecure Services query 46
- ISO 11-Login From Multiple IPs-Detail query 46
- ISO 11-Login From Multiple IPs-Overview query 47
- ISO 11-Multiple User Login-Detail query 47
- ISO 11-Multiple User Login-Overview query 47
- ISO 11-Network Routing Changes query 47
- ISO 11-Privileged Account Changed query 47
  - parameters
    - adminUsers 47
- ISO 11-Removal of Access Rights query 48
- ISO 11-Services by Asset query 48
- ISO 11-Suspicious Activity in Wireless Network query 48
  - parameters
    - wirelessNetwork 48
- ISO 11-Systems Accessed as Root or Administrator query 48
- ISO 11-Traffic Between Zones-Protocols query 49
- ISO 11-Traffic-Inbound Count query 48
  - parameters
    - internalNetwork 48
- ISO 11-Traffic-Inbound on Disallowed Ports query 48, 49
  - parameters
    - allowedPorts 48, 49
    - internalNetwork 48, 49
- ISO 11-User Account Creation query 49
- ISO 11-User Account Deletion query 49
- ISO 12 - Changes to Operating Systems report 49
  - devices 12
- ISO 12 - Exploit of Vulnerabilities report 50
  - devices 12
- ISO 12 - File Changes in Production report 50
  - configure 50
  - devices 12
- ISO 12 - Invalid Certificate report 50
  - devices 12
- ISO 12 - Invalid Data Input report 50
  - devices 12
- ISO 12 - Software Changes in Production report 50
  - configure 50
  - devices 12
- ISO 12 - Vulnerabilities and Misconfigurations report 50
  - devices 12
- ISO 12 - Vulnerability Scanner Results report 50
  - devices 12
- ISO 12-Changes to Operating Systems query 49
- ISO 12-Exploit of Vulnerability query 50
- ISO 12-File Changes in Production query 50
  - parameters
    - productionNetwork 50
- ISO 12-Invalid Certificate query 50
- ISO 12-Invalid Data Input query 50
- ISO 12-Software Changes in Production query 50
  - parameters
    - productionNetwork 50
- ISO 12-Vulnerabilities and Misconfigurations query 50
- ISO 12-Vulnerability Scanner Results query 50

- ISO 13 - Attack Events - Top 20 report 51
  - devices 12
- ISO 13 - Attacked Hosts - Top 20 report 51
  - devices 12
- ISO 13 - Attackers - Top 20 report 51
  - devices 12
- ISO 13 - Attacks - Hourly Count report 51
  - configure 51
  - devices 12
- ISO 13 - Attacks Targeting Internal Assets - All report 51
  - configure 51
  - devices 12
- ISO 13 - Confidentiality and Integrity Breach Sources - Count report 51
  - devices 12
- ISO 13 - Covert Channel Activity report 52
  - devices 12
- ISO 13 - DoS Sources report 52
  - devices 12
- ISO 13 - Information System Failures report 52
  - devices 12
- ISO 13 - Internal Reconnaissance - Top 20 Events report 52
  - configure 52
  - devices 12
- ISO 13 - Internal Reconnaissance - Top 20 Sources report 52
  - configure 52
  - devices 12
- ISO 13 - Internal Reconnaissance - Top 20 Targets report 52
  - configure 52
  - devices 12
- ISO 13-Attack Events Count query 51
- ISO 13-Attacked Hosts query 51
- ISO 13-Attackers query 51
- ISO 13-Attacks Targeting Internal Assets-All query 51
  - parameters
    - internalNetwork 51
- ISO 13-Attacks-Hourly Count query 51
  - parameters
    - internalNetwork 51
- ISO 13-CI Breach Sources-Overview query 51
- ISO 13-Covert Channel Activity query 52
- ISO 13-Denial of Service Sources query 52
- ISO 13-Information System Failures query 52
- ISO 13-Internal Reconnaissance-Events query 52
  - parameters
    - internalNetwork 52
- ISO 13-Internal Reconnaissance-Sources query 52
  - parameters
    - internalNetwork 52
- ISO 13-Internal Reconnaissance-Targets query 52
  - parameters
    - internalNetwork 52
- ISO 14 - Availability Attacks report 53
  - devices 13
- ISO 14-Availability Attacks query 53
- ISO 15 - Email Receivers by Amount - Top 100 report 53
  - devices 13
- ISO 15 - Email Receivers by Size - Top 100 report 53
  - devices 13
- ISO 15 - Email Senders by Amount - Top 100 report 53
  - devices 13
- ISO 15 - Email Senders by Size - Top 100 report 53
  - devices 13
- ISO 15 - Information Leaks - Organizational report 53
  - devices 13
- ISO 15 - Information Leaks - Personal report 53
  - devices 13
- ISO 15 - Information System Audit Tool Logins report 54
  - devices 13
- ISO 15 - Largest Emails - Top 20 report 54
  - devices 13
- ISO 15 - Peer to Peer Ports Count report 54
  - configure 54
  - devices 13
- ISO 15 - Peer to Peer Sources by Machine - Detail report 54
  - configure 54
  - devices 13
- ISO 15 - Peer to Peer Sources by Machine - Overview report 55
  - configure 55
  - devices 13
- ISO 15 - Policy Breaches report 55
  - devices 13
- ISO 15 - Possible Intellectual Property Rights Violation report 55
  - devices 13
- ISO 15-Email Receivers by Amount query 53
- ISO 15-Email Receivers by Size query 53
- ISO 15-Email Senders by Amount query 53
- ISO 15-Email Senders by Size query 53
- ISO 15-Information Leaks - Organizational query 53
- ISO 15-Information Leaks - Personal query 53
- ISO 15-Information System Audit Tool Logins query 54
- ISO 15-Largest Emails query 54
- ISO 15-Peer To Peer Ports Count query 54
- ISO 15-Peer to Peer Sources By Machine-Detail query 54
- ISO 15-Peer to Peer Sources By Machine-Overview query 55
- ISO 15-Policy Breaches query 55
- ISO 15-Possible IPR Violations query 55
- ISO 4 - High Risk Events by Zone report 35
  - devices 9
- ISO 4 - High Risk Events report 35
  - devices 9
- ISO 4 - Top 10 High Risk Events report 35
  - devices 9
- ISO 4-High Risk Events by Zone query 35
- ISO 4-High Risk Events query 35
- ISO 4-Top High Risk Events query 35
- ISO 5 - Machines Conducting Policy Breaches report 35
  - devices 9
- ISO 5 - New Hosts report 36
  - devices 9
- ISO 5 - New Services report 36
  - devices 9
- ISO 5 - Top 20 Policy Breach Events report 36
  - devices 9
- ISO 5-Machines Conducting Policy Breaches query 35
- ISO 5-New Hosts query 36
- ISO 5-New Services query 36
- ISO 5-Top 20 Policy Breach Events query 36
- ISO 6 - Administrative Logins and Logouts from Third-Party Hosts report 36
  - configure 36
  - devices 9
- ISO 6 - Administrative Logins and Logouts to Third-Party

- Hosts report 36
  - configure 36
  - devices 9
- ISO 6 - Attacks from Third-Party Systems report 36
  - configure 36
  - devices 9
- ISO 6 - Attacks on Third-Party Systems report 36
  - configure 36
  - devices 9
- ISO 6 - Compromised Third-Party Systems report 36
  - configure 36
  - devices 9
- ISO 6 - Failed Admin Logins from Third-Party Systems report 37
  - configure 37
  - devices 9
- ISO 6 - Failed Admin Logins to Third-Party Systems report 37
  - configure 37
  - devices 9
- ISO 6 - Failed User Logins from Third-Party Systems report 37
  - configure 37
  - devices 9
- ISO 6 - Failed User Logins to Third-Party Systems report 37
  - configure 37
  - devices 9
- ISO 6 - File Activity on Third-Party Systems report 37
  - configure 37
  - devices 9
- ISO 6 - File Creations on Third-Party Systems report 37
  - configure 37
  - devices 9
- ISO 6 - File Deletions on Third-Party Systems report 37
  - configure 37
  - devices 9
- ISO 6 - File Modifications on Third-Party Systems report 37
  - configure 37
  - devices 9
- ISO 6 - Policy Violations from Third-Party Systems report 37
  - configure 37
  - devices 9
- ISO 6 - Services Accessed by Third-Party Systems report 37
  - configure 37
  - devices 9
- ISO 6 - Third-Party Systems Accessed report 38
  - configure 38
  - devices 9
- ISO 6 - User Logins and Logouts from Third-Party Systems report 38
  - configure 38
  - devices 9
- ISO 6 - User Logins and Logouts to Third-Party Systems report 38
  - configure 38
  - devices 9
- ISO 6-Admin Logins and Logouts from Third-Party query 36
  - parameters
    - adminUsers 36
    - thirdPartyNetwork 36
- ISO 6-Admin Logins and Logouts to Third-Party query 36
  - parameters
    - adminUsers 36
    - thirdPartyNetwork 36
- ISO 6-Attacks on Third-Party Systems query 36
  - parameters
    - thirdPartyNetwork 36
- ISO 6-Compromised Third-Party Systems query 36
  - parameters
    - thirdPartyNetwork 36
- ISO 6-Failed Admin Logins from Third-Party Sys query 37
  - parameters
    - adminUsers 37
    - thirdPartyNetwork 37
- ISO 6-Failed Admin Logins to Third-Party Sys query 37
  - parameters
    - adminUsers 37
    - thirdPartyNetwork 37
- ISO 6-Failed User Logins from Third-Party Systems query 37
  - parameters
    - thirdPartyNetwork 37
- ISO 6-Failed User Logins to Third-Party Systems query 37
  - parameters
    - thirdPartyNetwork 37
- ISO 6-File Activity on Third-Party Systems query 37
  - parameters
    - thirdPartyNetwork 37
- ISO 6-File Creations on Third-Party Systems query 37
  - parameters
    - thirdPartyNetwork 37
- ISO 6-File Deletions on Third-Party Systems query 37
  - parameters
    - thirdPartyNetwork 37
- ISO 6-File Mods on Third-Party Accessible Systems query 37
  - parameters
    - thirdPartyNetwork 37
- ISO 6-Policy Violations from Third-Party Sys query 37
  - parameters
    - thirdPartyNetwork 37
- ISO 6-Services Accessed by Third-Parties query 37
  - parameters
    - thirdPartyNetwork 37
- ISO 6-Third-Party Sourced Attacks query 36
  - parameters
    - thirdPartyNetwork 36
- ISO 6-Third-Party Systems Accessed query 38
  - parameters
    - thirdPartyNetwork 38
- ISO 6-User Logins Logouts from Third-Party Sys query 38
  - parameters
    - thirdPartyNetwork 38
- ISO 6-User Logins Logouts to Third-Party Sys query 38
  - parameters
    - thirdPartyNetwork 38
- ISO 7 - Network Active Assets report 38
  - configure 38
  - devices 9
- ISO 7-Network Active Assets query 38
  - parameters
    - internalNetwork 38
- ISO 8 - Internet Activity per Device per Machine report



39  
 configure 39  
 devices 10  
 ISO 8 - Internet Activity per Device per User report 39  
 configure 39  
 devices 10  
 ISO 8 - Summary of Suspicious Activities per User report 39  
 devices 10  
 ISO 8-Internet Activity per Device per Machine query 39  
 ISO 8-Internet Activity per Device per User query 39  
 ISO 8-Summary of Suspicious Activities by User query 39  
 ISO 9 - Failed Building Access Attempts report 39  
 devices 10  
 ISO 9 - Successful Building Access Attempts report 39  
 devices 10  
 ISO 9-Failed Building Access Events query 39  
 ISO 9-Successful Building Access Events query 39  
 ISO clauses 35  
 ISO sections  
 10: Communications and Operations Management 39  
 11: Access Control 45  
 12: Information Systems Acquisition Development and Maintenance 49  
 13: Information Security Incident Management 51  
 14: Business Continuity Management 52  
 15: Compliance 53  
 4: Risk Assessment and Treatment 35  
 5: Security Policy 35  
 6: Organization of Information Security 36  
 7: Asset Management 38  
 8: Human Resources 38  
 9: Physical and Environmental Security 39  
 defined 35  
 ISO/IEC 17799 standard 35  
 ISO-17799:2005 standard 2

## L

log management 2  
 log management platform 2  
 Logger  
 defined 2  
 version level 8  
 Logger Administrator's guide ix  
 logger CIP for SOX  
 configure 19  
 defined 1  
 deploy 15  
 reports 5, 34  
 uninstall 27  
 Logger documentation ix  
 Logger Hardware Setup Guide ix  
 Logger Online Help ix  
 Logger Quickstart Guide ix

## M

malicious code 39  
 Multipage checkbox 25  
 MySQL REGEXP operator 23

## N

NBAD 13  
 network behavior anomaly detection 13  
 network equipment 13  
 network segregation 39  
 NIST 800-53 standard 2  
 non-CEF devices 13

## O

operating systems 3, 13, 39  
 organization of information security 36

## P

parameters  
 adminUsers 22, 29, 31, 36, 37, 40, 43, 45, 47  
 allowedPorts 29, 32, 48, 49  
 changing the default value 22  
 commonlyBlockedPorts 30  
 databaseAdminAccounts 29, 32, 46  
 databaseAdminUsers 29, 32, 46  
 deleting 29  
 destinationAddress 30  
 destinationGroupParameter 30  
 destinationPort 30  
 destinationUserName 29, 32, 46  
 developmentNetwork 29, 33, 41, 42, 44  
 deviceProduct 30  
 deviceVendor 30  
 internalNetwork 29, 33, 38, 48, 49, 51, 52  
 IPAddress 30  
 productionNetwork 29, 33, 41, 42, 44, 50  
 specifying regular expressions 23  
 testingNetwork 29, 33, 42, 44  
 thirdPartyNetwork 29, 34, 36, 37, 38, 41  
 webPorts 30  
 wirelessNetwork 30, 34, 48  
 zones 30  
 performance  
 improving 19  
 perimeter security solutions 3  
 physical and environmental security 39  
 physical security systems 13  
 policy management 13  
 privileged accounts 45  
 Production Network(s) prompt  
 productionNetwork 33  
 productionNetwork parameter 29, 33, 41, 42, 44, 50  
 prompts  
 Administrative User(s) 31  
 Allowed Port(s) 32  
 Database Administration Account(s) 32  
 Database Administrative User(s) 32  
 Development Network(s) 33  
 Internal Network(s) 33  
 Production Network(s) 33  
 Testing Network(s) 33  
 Third-Party Network(s) 34  
 User Name 32  
 Wireless Network(s) 34

## Q

queries 23

- access control 46
- asset management 38
- business continuity management 53
- communications and operations management 40
- compliance 53
- configure 23
- human resources 39
- information security incident management 51
- information systems acquisition development and maintenance 49
- ISO 10
  - supporting 40
  - ISO 10-Account Lockouts by System 40
  - ISO 10-Account Lockouts by User 40
  - ISO 10-Administrative Logins and Logouts 40
  - ISO 10-Administrator Actions 40
  - ISO 10-Application Configuration Modifications 40
  - ISO 10-Attacks Development to Production 41
  - ISO 10-Attacks Production to Development 41
  - ISO 10-Audit Log Cleared 41
  - ISO 10-Changes to Development Network Machines 41
  - ISO 10-Changes to Third-Party Resources 41
  - ISO 10-Database Access - All 41
  - ISO 10-Database Access - Failed 41
  - ISO 10-Development to Test or Production 42
  - ISO 10-Device Configuration Changes 42
  - ISO 10-Device Logging Review 42
  - ISO 10-Failed Anti-Virus Updates 42
  - ISO 10-Fault Logs 42
  - ISO 10-File Integrity Changes Detected 42
  - ISO 10-Firewall Configuration Modifications 42
  - ISO 10-Firewall Open Port Review 43
  - ISO 10-Information Interception 43
  - ISO 10-Malicious Code Sources 43
  - ISO 10-Network Device Configuration Modifications 43
  - ISO 10-Number of Successful Administrative Logins 43
  - ISO 10-Number of Successful User Logins 43
  - ISO 10-Number of Unsuccessful User Logins 43
  - ISO 10-Number Unsuccessful Administrative Logins 43
  - ISO 10-Operating System Configuration Changes 43
  - ISO 10-Production to Test or Development 44
  - ISO 10-Resource Exhaustion Detected 44
  - ISO 10-Successful Brute Force Logins 44
  - ISO 10-System Restarted 44
  - ISO 10-Test to Development or Operations 44
  - ISO 10-Top Unsuccessful Administrative Logins 45
  - ISO 10-Top Unsuccessful User Logins 45
  - ISO 10-Unsuccessful User Logins 45
  - ISO 10-User Logins and Logouts 45
  - ISO 10-Virus Summary by Hosts 45
  - ISO 10-Virus Summary by Virus Name 45
  - ISO 10-VPN Access Summary 45
- ISO 11
  - supporting 46
  - ISO 11-Account Activity by User Name 46
  - ISO 11-Blocked Firewall Traffic 46
  - ISO 11-Database Privilege Violation 46
  - ISO 11-Default Vendor Account Used 46
  - ISO 11-Insecure Services 46
  - ISO 11-Login From Multiple IPs-Detail 46
  - ISO 11-Login From Multiple IPs-Overview 47
  - ISO 11-Multiple User Login-Detail 47
  - ISO 11-Multiple User Login-Overview 47
  - ISO 11-Network Routing Changes 47
  - ISO 11-Privileged Account Changed 47
  - ISO 11-Removal of Access Rights 48
  - ISO 11-Services by Asset 48
  - ISO 11-Suspicious Activity in Wireless Network 48
  - ISO 11-Systems Accessed as Root or Administrator 48
  - ISO 11-Traffic Between Zones-Protocols 49
  - ISO 11-Traffic-Inbound Count 48
  - ISO 11-Traffic-Inbound on Disallowed Ports 48, 49
  - ISO 11-User Account Creation 49
  - ISO 11-User Account Deletion 49
- ISO 12
  - supporting 49
  - ISO 12-Changes to Operating Systems 49
  - ISO 12-Exploit of Vulnerability 50
  - ISO 12-File Changes in Production 50
  - ISO 12-Invalid Certificate 50
  - ISO 12-Invalid Data Input 50
  - ISO 12-Software Changes in Production 50
  - ISO 12-Vulnerabilities and Misconfigurations 50
  - ISO 12-Vulnerability Scanner Results 50
- ISO 13
  - supporting 51
  - ISO 13-Attack Events Count 51
  - ISO 13-Attacked Hosts 51
  - ISO 13-Attackers 51
  - ISO 13-Attacks Targeting Internal Assets-All 51
  - ISO 13-Attacks-Hourly Count 51
  - ISO 13-CI Breach Sources-Overview 51
  - ISO 13-Covert Channel Activity 52
  - ISO 13-Denial of Service Sources 52
  - ISO 13-Information System Failures 52
  - ISO 13-Internal Reconnaissance-Events 52
  - ISO 13-Internal Reconnaissance-Sources 52
  - ISO 13-Internal Reconnaissance-Targets 52
- ISO 14
  - supporting 53
  - ISO 14-Availability Attacks 53
- ISO 15
  - supporting 53
  - ISO 15-Email Receivers by Amount 53
  - ISO 15-Email Receivers by Size 53
  - ISO 15-Email Senders by Amount 53
  - ISO 15-Email Senders by Size 53
  - ISO 15-Information Leaks - Organizational 53
  - ISO 15-Information Leaks - Personal 53
  - ISO 15-Information System Audit Tool Logins 54
  - ISO 15-Largest Emails 54
  - ISO 15-Peer To Peer Ports Count 54
  - ISO 15-Peer to Peer Sources By Machine-Detail 54
  - ISO 15-Peer to Peer Sources By Machine-Overview 55
  - ISO 15-Policy Breaches 55
  - ISO 15-Possible IPR Violations 55
- ISO 4
  - supporting 35
  - ISO 4-High Risk Events 35
  - ISO 4-High Risk Events by Zone 35
  - ISO 4-Top High Risk Events 35
- ISO 5
  - supporting 35

- ISO 5-Machines Conducting Policy Breaches 35
  - ISO 5-New Hosts 36
  - ISO 5-New Services 36
  - ISO 5-Top 20 Policy Breach Events 36
  - ISO 6
    - supporting 36
  - ISO 6-Admin Logins and Logouts from Third-Party 36
  - ISO 6-Admin Logins and Logouts to Third-Party 36
  - ISO 6-Attacks on Third-Party Systems 36
  - ISO 6-Compromised Third-Party Systems 36
  - ISO 6-Failed Admin Logins from Third-Party Sys 37
  - ISO 6-Failed Admin Logins to Third-Party Sys 37
  - ISO 6-Failed User Logins from Third-Party Systems 37
  - ISO 6-Failed User Logins to Third-Party Systems 37
  - ISO 6-File Activity on Third-Party Systems 37
  - ISO 6-File Creations on Third-Party Systems 37
  - ISO 6-File Deletions on Third-Party Systems 37
  - ISO 6-File Mods on Third-Party Accessible Systems 37
  - ISO 6-Policy Violations from Third-Party Sys 37
  - ISO 6-Services Accessed by Third-Parties 37
  - ISO 6-Third-Party Sourced Attacks 36
  - ISO 6-Third-Party Systems Accessed 38
  - ISO 6-User Logins Logouts from Third-Party Sys 38
  - ISO 6-User Logins Logouts to Third-Party Sys 38
  - ISO 7
    - supporting 38
  - ISO 7-Network Active Assets 38
  - ISO 8
    - supporting 39
  - ISO 8-Internet Activity per Device per Machine 39
  - ISO 8-Internet Activity per Device per User 39
  - ISO 8-Summary of Suspicious Activities by User 39
  - ISO 9
    - supporting 39
  - ISO 9-Failed Building Access Events 39
  - ISO 9-Successful Building Access Events 39
    - modifying 23
    - organization of information security 36
    - physical and environmental security 39
    - risk assessment and treatment 35
    - security policy 35
  - quick run reports 24
- R**
- REGEXG operator 23
  - regular expressions 23
  - reports
    - access control 46
    - anatomy 5
    - asset management 38
    - business continuity management 53
    - communications and operations management 40
    - compliance 53
    - focus on SOX systems 4
    - human resources 39
    - information security incident management 51
    - information systems acquisition development and maintenance 49
    - ISO 10
      - supporting 40
    - ISO 10 - Account Lockouts by System 10, 40
    - ISO 10 - Account Lockouts by User 10, 40
    - ISO 10 - Administrative Logins and Logouts 10, 40
      - configure 40
    - ISO 10 - Administrator Actions 10, 40
      - configure 40
    - ISO 10 - Application Configuration Modification 10, 40
    - ISO 10 - Attacks - Development to Production 10, 41
      - configure 41
    - ISO 10 - Attacks - Production to Development 10, 41
      - configure 41
    - ISO 10 - Audit Log Cleared 10, 41
    - ISO 10 - Changes to Development Network Machines 10, 41
      - configure 41
    - ISO 10 - Changes to Third-Party Resources 10, 41
      - configure 41
    - ISO 10 - Database Access - All 10, 41
    - ISO 10 - Database Access - Failed 10, 41
    - ISO 10 - Development Network Not Segregated 10, 42
      - configure 42
    - ISO 10 - Device Configuration Changes 10, 42
    - ISO 10 - Device Logging Review 10, 42
    - ISO 10 - Failed Anti-Virus Updates 10, 42
    - ISO 10 - Fault Logs 10, 42
    - ISO 10 - File Integrity Changes 10, 42
    - ISO 10 - Firewall Configuration Changes 10
    - ISO 10 - Firewall Configuration Changes - All 42
    - ISO 10 - Firewall Configuration Changes - Successful 10, 42
    - ISO 10 - Firewall Open Port Review 10, 43
    - ISO 10 - Information Interception Events 10, 43
    - ISO 10 - Malicious Code Sources 10, 43
    - ISO 10 - Network Device Configuration Changes - All 10, 43
    - ISO 10 - Network Device Configuration Changes - Successful 10, 43
    - ISO 10 - Number of Successful Administrative Logins 11, 43
      - configure 43
    - ISO 10 - Number of Successful User Logins 11, 43
      - configure 43
    - ISO 10 - Number of Unsuccessful Administrative Logins 11, 43
      - configure 43
    - ISO 10 - Number of Unsuccessful User Logins 11, 43
      - configure 43
    - ISO 10 - Operating System Configuration Changes 11, 43
    - ISO 10 - Production Network Not Segregated 11, 44
      - configure 44
    - ISO 10 - Resource Exhaustion 44
    - ISO 10 - Resource Exhaustion report 11
    - ISO 10 - Successful Brute Force Logins 11, 44
    - ISO 10 - System Restarted 11, 44
    - ISO 10 - Test Network Not Segregated 11, 44
      - configure 44
    - ISO 10 - Top Unsuccessful Administrative Logins 11, 45
      - configure 45

- ISO 10 - Top Unsuccessful User Logins 11, 45
  - configure 45
- ISO 10 - Unsuccessful User Logins 11, 45
  - configure 45
- ISO 10 - User Logins and Logouts 11, 45
- ISO 10 - Virus Summary by Hosts 11, 45
- ISO 10 - Virus Summary by Virus Name 11, 45
- ISO 10 - VPN Access Summary 11, 45
- ISO 11
  - supporting 46
- ISO 11 - Account Activity by User 11, 46
  - configure 46
- ISO 11 - Blocked Firewall Traffic 11, 46
- ISO 11 - Database Privilege Violation 11, 46
  - configure 46
- ISO 11 - Default Vendor Account Used 11, 46
  - configure 46
- ISO 11 - Insecure Services 11, 46
  - configure 46
- ISO 11 - Login From Multiple IPs - Detail 11, 46
- ISO 11 - Login From Multiple IPs - Overview 11, 47
- ISO 11 - Multiple User Login - Detail 11, 47
- ISO 11 - Multiple User Login - Overview 11, 47
- ISO 11 - Network Routing Configuration Changes 11, 47
- ISO 11 - Privileged Account Changes - All 11, 47
  - configure 47
- ISO 11 - Privileged Account Changes - Successful 11, 47
  - configure 47
- ISO 11 - Removal of Access Rights 11, 48
- ISO 11 - Services by Asset 12, 48
  - configure 48
- ISO 11 - Suspicious Activity in Wireless Network 12, 48
  - configure 48
- ISO 11 - Systems Accessed as Root or Administrator 12, 48
  - configure 48
- ISO 11 - Traffic - Inbound Count 12, 48
  - configure 48
- ISO 11 - Traffic - Inbound on Disallowed Ports - All 12, 48
  - configure 48
- ISO 11 - Traffic - Inbound on Disallowed Ports - Successful 12, 49
  - configure 49
- ISO 11 - Traffic Between Zones - Protocols 12, 49
- ISO 11 - User Account Creation 12, 49
- ISO 11 - User Account Deletion 12, 49
- ISO 12
  - supporting 49
- ISO 12 - Changes to Operating Systems 12, 49
- ISO 12 - Exploit of Vulnerabilities 12, 50
- ISO 12 - File Changes in Production 12, 50
  - configure 50
- ISO 12 - Invalid Certificate 12, 50
- ISO 12 - Invalid Data 12
- ISO 12 - Invalid Data Input 50
- ISO 12 - Software Changes in Production 12, 50
  - configure 50
- ISO 12 - Vulnerabilities and Misconfigurations 12, 50
- ISO 12 - Vulnerability Scanner Results 12, 50
- ISO 13
  - supporting 51
- ISO 13 - Attack Events - Top 20 12, 51
- ISO 13 - Attacked Hosts - Top 20 12, 51
- ISO 13 - Attackers - Top 20 12, 51
- ISO 13 - Attacks - Hourly Count 12, 51
  - configure 51
- ISO 13 - Attacks Targeting Internal Assets - All 12, 51
  - configure 51
- ISO 13 - Confidentiality and Integrity Breach Sources - Count 12, 51
- ISO 13 - Covert Channel Activity 12, 52
- ISO 13 - DoS Sources 12, 52
- ISO 13 - Information System Failures 12, 52
- ISO 13 - Internal Reconnaissance - Top 20 Events 12, 52
  - configure 52
- ISO 13 - Internal Reconnaissance - Top 20 Sources 12, 52
  - configure 52
- ISO 13 - Internal Reconnaissance - Top 20 Targets 12, 52
  - configure 52
- ISO 14
  - supporting 53
- ISO 14 - Availability Attacks 13, 53
- ISO 15
  - supporting 53
- ISO 15 - Email Receivers by Amount - Top 100 13, 53
- ISO 15 - Email Receivers by Size - Top 100 13, 53
- ISO 15 - Email Senders by Amount - Top 100 13, 53
- ISO 15 - Email Senders by Size - Top 100 13, 53
- ISO 15 - Information Leaks - Organizational 13, 53
- ISO 15 - Information Leaks - Personal 13, 53
- ISO 15 - Information System Audit Tool Logins 13, 54
- ISO 15 - Largest Emails - Top 20 13, 54
- ISO 15 - Peer to Peer Ports Count 13, 54
  - configure 54
- ISO 15 - Peer to Peer Sources by Machine - Detail 13, 54
  - configure 54
- ISO 15 - Peer to Peer Sources by Machine - Overview 13, 55
  - configure 55
- ISO 15 - Policy Breaches 13, 55
- ISO 15 - Possible Intellectual Property Rights Violation 13, 55
- ISO 4
  - supporting 35
- ISO 4 - High Risk Events 9, 35
- ISO 4 - High Risk Events by Zone 9, 35
- ISO 4 - Top 10 High Risk Events 9, 35
- ISO 5
  - supporting 35
- ISO 5 - Machines Conducting Policy Breaches 9, 35
- ISO 5 - New Hosts 9, 36
- ISO 5 - New Services 9, 36
- ISO 5 - Top 20 Policy Breach Events 9, 36
- ISO 6
  - supporting 36
- ISO 6 - Administrative Logins and Logouts from Third-Party Hosts 9, 36
  - configure 36

- ISO 6 - Administrative Logins and Logouts to Third-Party Hosts 9, 36
  - configure 36
- ISO 6 - Attacks from Third-Party Systems 9, 36
  - configure 36
- ISO 6 - Attacks on Third-Party Systems 9, 36
  - configure 36
- ISO 6 - Compromised Third-Party Systems 9, 36
  - configure 36
- ISO 6 - Failed Admin Logins from Third-Party Systems 9, 37
  - configure 37
- ISO 6 - Failed Admin Logins to Third-Party Systems 9, 37
  - configure 37
- ISO 6 - Failed User Logins from Third-Party Systems 9, 37
  - configure 37
- ISO 6 - Failed User Logins to Third-Party Systems 9, 37
  - configure 37
- ISO 6 - File Activity on Third-Party Systems 9, 37
  - configure 37
- ISO 6 - File Creations on Third-Party Systems 9, 37
  - configure 37
- ISO 6 - File Deletions on Third-Party Systems 9, 37
  - configure 37
- ISO 6 - File Modifications on Third-Party Systems 9, 37
  - configure 37
- ISO 6 - Policy Violations from Third-Party Systems 9, 37
  - configure 37
- ISO 6 - Services Accessed by Third-Party Systems 9, 37
  - configure 37
- ISO 6 - Third-Party Systems Accessed 9, 38
  - configure 38
- ISO 6 - User Logins and Logouts from Third-Party Systems 9, 38
  - configure 38
- ISO 6 - User Logins and Logouts to Third-Party Systems 9, 38
  - configure 38
- ISO 7
  - supporting 38
- ISO 7 - Network Active Assets 9, 38
  - configure 38
- ISO 8
  - supporting 39
- ISO 8 - Internet Activity per Device per Machine 10, 39
  - configure 39
- ISO 8 - Internet Activity per Device per User 10, 39
  - configure 39
- ISO 8 - Summary of Suspicious Activities per User 10, 39
- ISO 9
  - supporting 39
- ISO 9 - Failed Building Access Attempts 10, 39
- ISO 9 - Successful Building Access Attempts 10, 39
- logger CIP for SOX 5, 34
- organization of information security 36
- physical and environmental security 39
- quick run 24
- risk assessment and treatment 35
- running 23
- schedule 26
- security policy 35
- resources
  - access control 46
  - asset management 38
  - business continuity management 53
  - communications and operations management 40
  - compliance 53
  - human resources 39
  - information security incident management 51
  - information systems acquisition development and maintenance 49
- ISO 10
  - configure 40
  - listing 40
  - supporting 40
- ISO 11
  - configure 45
  - listing 45
  - supporting 46
- ISO 12
  - configure 49
  - listing 49
  - supporting 49
- ISO 13
  - configure 51
  - listing 51
  - supporting 51
- ISO 14
  - configure 52
  - listing 52
  - supporting 53
- ISO 15
  - configure 53
  - listing 53
  - supporting 53
- ISO 4
  - configure 35
  - listing 35
  - supporting 35
- ISO 5
  - configure 35
  - listing 35
  - supporting 35
- ISO 6
  - configure 36
  - listing 36
  - supporting 36
- ISO 7
  - configure 38
  - listing 38
  - supporting 38
- ISO 8
  - configure 38
  - listing 38
  - supporting 39
- ISO 9
  - configure 39
  - listing 39
  - supporting 39
- organization of information security 36
- physical and environmental security 39
- risk assessment and treatment 35

- security policy 35
- risk assessment and treatment 35
- rogue devices 38
- run reports 25

## S

- Sarbanes-Oxley Act 2
- schedule reports 26
- search group 20
- sections:ISO 35
- security policy 35
- SOX device groups 4, 19
- SOX devices 19
- SOX report category filters 20
- SOX reports 5
- spreadsheets 3
- SQL
  - modifying 23
  - queries 5
- standards
  - ISO-17799:2005 2
  - NIST 800-53 2
- storage groups 4, 25
  - create new 21
- supported devices 9
- syslog
  - device 2
  - message 2
- system reports 3

## T

- Template field 25
- Testing Network(s) prompt

- testingNetwork 33
- testingNetwork parameter 29, 33, 42, 44
- Third-Party Network(s) prompt
  - thirdPartyNetwork 34
- thirdPartyNetwork parameter 29, 34, 36, 37, 38, 41

## U

- uninstall
  - logger CIP for SOX 27
- upload CAB file 17
- User Name prompt
  - destinationUserName 32

## V

- version 8
- virtual private network 13
- VPN 13
- vulnerability
  - assessment 13
- vulnerability exploit attempts 49

## W

- webPorts parameter 30
- wireless 13
- Wireless Network(s) prompt
  - wirelessNetwork 34
- wirelessNetwork parameter 30, 34, 48

## Z

- zones parameter 30