
Micro Focus Security

ArcSight Logger CIP for IT Gov

Software Version: 5.02

Solutions Guide

Document Release Date: June, 2018

Software Release Date: June, 2018



Legal Notices

Warranty

The only warranties for products and services of Micro Focus and its affiliates and licensors (“Micro Focus”) are set forth in the express warranty statements accompanying such products and services. Nothing herein should be construed as constituting an additional warranty. Micro Focus shall not be liable for technical or editorial errors or omissions contained herein. The information contained herein is subject to change without notice.

Restricted Rights Legend

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

Copyright Notice

© Copyright 2018 Micro Focus or one of its affiliates.

Trademark Notices

Adobe™ is a trademark of Adobe Systems Incorporated.

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

UNIX® is a registered trademark of The Open Group.

Support

Contact Information

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

Contents

Chapter 1: Overview	6
ArcSight Logger CIP for IT Governance Architecture	8
Logger CIP for IT Gov Resources	8
Alerts	9
Queries	9
Dashboards	9
Reports	9
Supported Devices	11
 Chapter 2: Installing Logger CIP for IT Gov	13
 Chapter 3: Configuring Logger CIP for IT Gov	15
Processing Events	15
Limiting the Events Processed	15
Classifying Logger CIP for IT Gov-Related Devices in a Device Group	16
Creating a Filter to Limit Events Processed	17
Limiting Events Processed by Alerts	18
Limiting Events Processed by Reports	19
Configuring Alerts	19
Configuring Reports	20
 Chapter 4: Logger CIP for IT Gov Alerts	31
 Chapter 5: Logger CIP for IT Gov Reports	35
ISO 27002	35
ISO 6 - Organization of information security	35
ISO 8 - Asset management	37
ISO 9 - Access control	38
ISO 10 - Cryptography	40
ISO 11 - Physical and environmental security	40
ISO 12 - Operations security	41
ISO 13 - Communications security	56

ISO 14 - System acquisition development and maintenance	58
ISO 16 - Information security incident management	59
ISO 17 - Information security aspects of business continuity management	60
ISO 18 - Compliance	61
NIST 800-53	61
 Chapter 6: Logger CIP for IT Gov Dashboards	 85
IT Governance - Account Management Activity	85
IT Governance - Firewall Activity	86
IT Governance - Configuration Changes	87
IT Governance - Administrative Activity	88
IT Governance - Malicious Activity	89
IT Governance - Physical Security Activity	90
IT Governance - Vulnerability Management	91
IT Governance - DoS and Port Scanning Activity	92
IT Governance - Technical Controls Activity	92
IT Governance - User Activity Dashboard	93
 Chapter 7: Logger CIP for IT Gov Parameters	 94
adminUsers	94
allowedPorts	94
destinationAddress	94
databaseAdminAccounts	94
databaseAdminUsers	95
destinationHostName	95
destinationUserName	95
developmentNetwork	96
deviceEventClassId	96
deviceProduct	96
eventName	96
eventPriority	96
internalNetwork	97

productionNetwork	97
sourceDestUserName	97
sourceUserName	97
testingNetwork	98
thirdPartyNetwork	98
variable	98
virusName	98
wirelessNetwork	99
Appendix A: Uninstalling Logger CIP for IT Gov	100
Send Documentation Feedback	101

Chapter 1: Overview

ArcSight Logger CIP for IT Governance leverages the Logger litigation-quality, long-term repository of log and event data to facilitate IT Governance compliance with the IT ISO 27002:2013 and NIST 800-53 Governance standards using the Logger reporting and alerting capability. Logger CIP for IT Gov facilitates compliance by providing detailed reports that help evaluate risk and provide comprehensive reporting of high and low-risk activity, and alerts that monitor incoming events in real time and notify analysts when events of interest are detected. Dashboards are also provided to show a holistic overview of the IT Governance controls in your organization.

ISO/IEC 27002:2013 Standard

Compliance with the components that apply to your business can best be demonstrated by using a cohesive framework, such as the Code of Practice for information security management, also known as ISO/IEC 27002:2013. This standard was developed by the International Organization for Standardization (ISO) and the International Electrotechnical Commission (IEC) and covers the controls and guidelines a company should consider implementing to follow due diligence and best practices in IT security. The standard covers the following security categories, from 5 to 18:

- 5 Information Security Policies
- 6 Organization of Information Security
- 7 Human Resource Security
- 8 Asset Management
- 9 Access Control
- 10 Cryptography
- 11 Physical and Environmental Security
- 12 Operation Security
- 13 Communication Security
- 14 System Acquisition, Development, and Maintenance
- 15 Supplier Relationships
- 16 Information Security Incident Management
- 17 Information Security Aspects of Business Continuity Management
- 18 Compliance

NIST 800-53 Standard

The National Institute of Standards and Technology (NIST) is responsible for developing and publishing a set of standards and guidelines for securing information systems known as Federal Information Processing Standards or FIPS. NIST has developed a FIPS document called [NIST Special](#)

[Publication 800-53 Recommended Security Controls for Federal Information System \(NIST 800-53\)](#) to define standards and guidelines for providing information security for agency operations and assets.

NIST 800-53 defines the selection and employment of appropriate security controls for an information system. NIST 800-53 defines security controls as the management, operational, and technical safeguards or countermeasures prescribed for an information system to protect the confidentiality, integrity, and availability of the system and its information.

NIST 800-53 defines the following three general classes of security controls:

- Management
- Operational
- Technical

In addition, NIST 800-53 defines eighteen security control families as defined by the following table. Each security control family contains a set of related security controls. For example, the Access Control family contains twenty security controls. Each security control has a unique identifier that contains two characters representing the security control, a hyphen (-) followed by a number. For example, the first security control in the Access Control family is called *Access Control Policy and Procedure* and is referenced using the *AC-1* identifier.

The security control families defined in NIST 800-53 are closely aligned with the security areas found in FIPS 200.

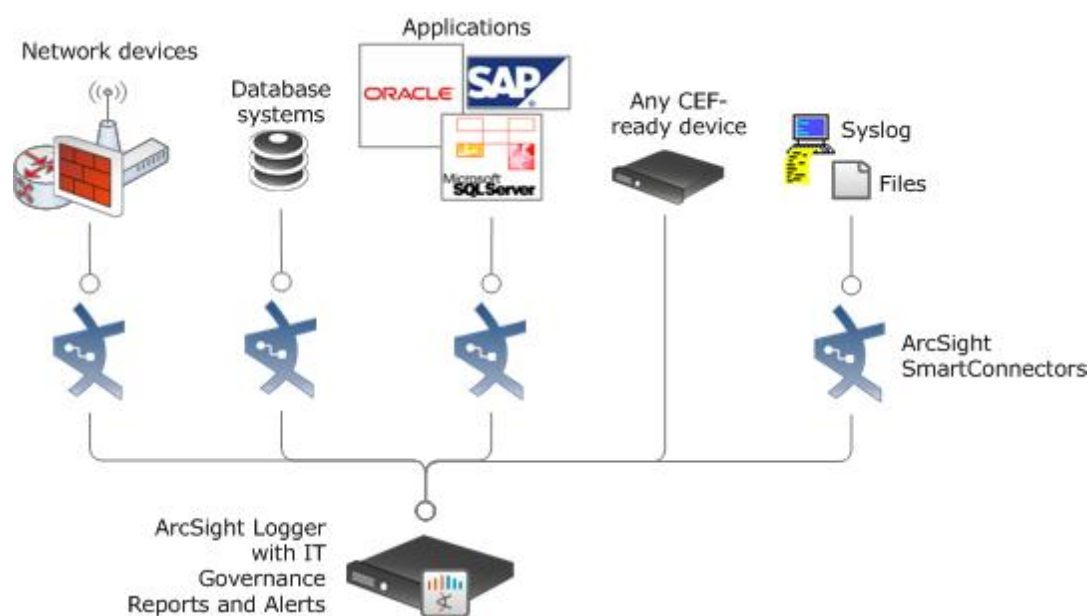
The following table defines the security controls defined by the NIST.

Family	Identifier	Class
Access Control	AC	Technical
Awareness and Training	AT	Operational
Audit and Accountability	AU	Technical
Certification, Accreditation, and Security Assessments	CA	Management
Configuration Management	CM	Operational
Contingency Planning	CP	Operational
Identification and Authentication	IA	Technical
Incident Response	IR	Operational
Maintenance	MA	Operational
Media Protection	MP	Operational
Physical and Environmental Protection	PE	Operational
Planning	PL	Management
Personnel Security	PS	Operational
Program Management	PM	Management

Family	Identifier	Class
Risk Assessment	RA	Management
System and Services Acquisition	SA	Management
System and Communications Protection	SC	Technical
System and Information Integrity	SI	Operational

ArcSight Logger CIP for IT Governance Architecture

Logger CIP for IT Gov reports operate on events in Common Event Format (CEF), an industry standard for the interoperability of event or log-generating devices. CEF events can come from a device that is already configured to post events in CEF, or they can come from any network device whose events are first run through an ArcSight SmartConnector. Logger CIP for IT Gov operates on events received from devices on the network in CEF. IT Governance devices that are not already CEF-ready must be run through an ArcSight SmartConnector.



For more about CEF events and how they are used, see the *ArcSight Logger Administrator's Guide*.

Logger CIP for IT Gov Resources

Logger CIP for IT Gov provides alerts, queries, reports, and dashboards.

Alerts

Alerts monitor incoming events in real time and notify analysts when events of interest are detected. Some Logger CIP for IT Gov alerts are enabled by default and the rest are disabled. You can view the list of Logger CIP for IT Gov alerts by selecting **Configuration** on the top-level menu bar, then clicking **Alerts** in the **Data** section. To enable an alert, click the **Disabled** (🚫) icon.

For information about creating alert destinations and sending notifications, see the *ArcSight Logger Administrator's Guide*.

Queries

Logger CIP for IT Gov queries are invoked by the Logger CIP for IT Gov reports and have similar names as the reports themselves. You can view the queries by clicking **Reports** on the top-level menu bar, then clicking **Query Explorer** in the **Navigation** section. For information on configuring queries, see the *ArcSight Logger Administrator's Guide*. Queries are not described in this guide.

Dashboards

The Logger CIP for IT Governance dashboards provide a quick high level overview of the compliance status of different controls on the organization in various chart formats to help you demonstrate appropriate risk management and monitoring practices. You can view the dashboards by clicking **Dashboards** on the top-level menu bar.

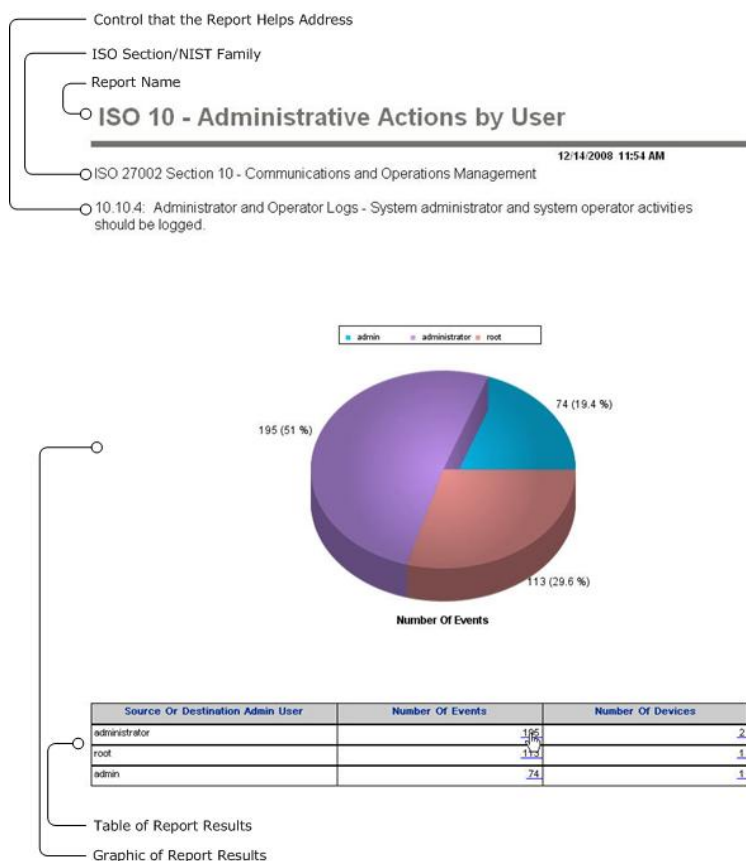
Reports

Logger CIP for IT Gov reports consist of the following:

- **Standard Reports**

Logger CIP for IT Gov standard reports are optimized to provide information that can be used to satisfy monitoring and reporting requirements of ISO 27002 and NIST 800-53 controls. You can view the Logger CIP for IT Gov standard reports by clicking **Reports** on the top-level menu bar, then clicking **Report Explorer** in the **Navigation** section. Each standard report has a SQL query associated with it that queries the database for the specified conditions. Certain reports prompt you to provide site-specific information at run time; this information is passed from the report to the query via parameters. Some queries contain default values, which you can customize to match conditions

relevant to your environment.



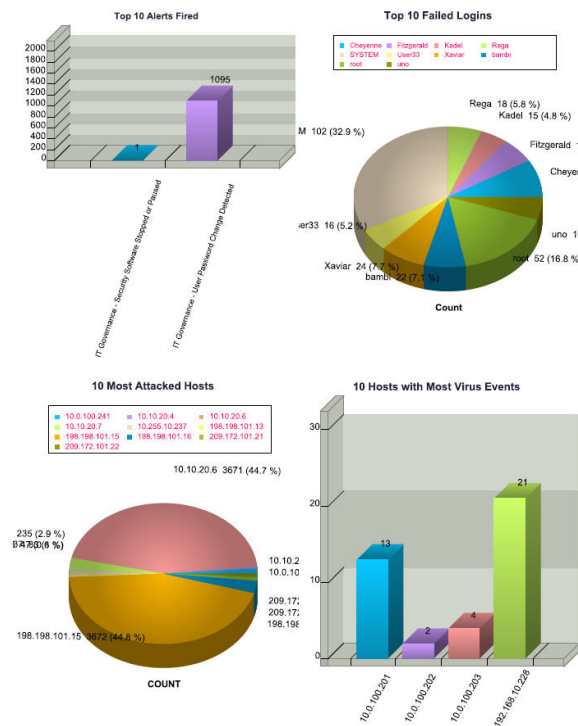
• Drill-down Reports

Some standard reports are enabled with additional investigative links that drill down to other reports and provide a different perspective about the behavior of an item on the network. For example, drilling down can provide more detail or generate a higher level overview about a certain event. Some drill-down reports are designed to be accessed by reference only from the reports that provide special hyperlinks to them. Other drill-down reports are top-level reports called entry drill-downs. Run these entry drill-downs first and use them to drill down to the other drill-down reports to avoid generating reports with a large number of pages. During an investigation, however, you might want to run a drill-down report directly; for example, to investigate a specific host or event name.

• Executive Reports

Logger CIP for IT Gov provides two executive reports, ISO Executive and NIST Executive. These executive reports show an executive overview of the alerts fired, attacked hosts, failed logins, and virus-infected machines at your site.

ISO 27002 Executive Report



Note: For the executive report to be populated with data during report run time, the following types of events must be received by the ArcSight Logger:

- Internal Logger events indicating that alerts have fired
- Virus events
- Intrusion detection system (IDS) events
- Failed login events

For information about running, formatting, publishing, and scheduling reports, see the *ArcSight Logger Administrator's Guide*.

Supported Devices

The following device categories are capable of generating events to populate the Logger CIP for IT Gov reports and to trigger enabled alerts:

- Anti-virus solutions
- Applications
- Content Security and Web Filtering systems
- Databases

- Firewalls
- Identity Management systems
- Intrusion Detection System/Intrusion Prevention System
- Network equipment
- Operating systems
- Physical Security systems
- Policy Management systems
- Virtual Management systems
- Virtual Private Networks
- Wireless systems

Note: Logger CIP for IT Gov reports and alerts operate on events from the devices in your environment. Micro Focus recommends that you use an ArcSight SmartConnector for devices that are not CEF-enabled to yield the most accurate reports.

Chapter 2: Installing Logger CIP for IT Gov

You can install Logger CIP for IT Gov on the Logger Appliance or the Software Logger. Logger Appliance is the preconfigured hardware version of Logger. Software Logger is the downloadable version of Logger installed on your hardware.

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

Follow the appropriate procedure below for your Logger type.

To install Logger CIP for IT Gov on the Logger Appliance:

1. Download the Logger CIP for IT Gov .enc file (for example, ArcSight-ComplianceInsightPackage-Logger-ITGov.x.x.nnnn.0.enc) to the computer where you plan to log into the Logger user interface. Check the Release Notes for the exact version of the file.
2. Log into the Logger user interface.
3. From the Logger top-level menu bar, click **System Admin**.
4. From the **System** section, select **License & Update**.
5. Click **Browse** to locate and open the .enc file you downloaded.
6. Click **Upload Update**.

A dialog displays indicating that the update process might take some time.

7. Click **OK**.

A message displays indicating that the update is progressing. After the contents of the .enc file are installed, another message displays indicating that the update is a success. The .enc file installs Logger CIP for IT Gov reports, parameters, queries, dashboards, and alerts.

8. Verify that the content is installed.
 - To view the installed alerts, click **Configuration** on the top-level menu bar, then click **Alerts** in the **Data** section.
 - To view the installed reports, click **Reports** on the top-level menu bar, then click **Report Explorer** in the **Navigation** section. Click the arrow to the left of **ISO 27002** to see the ISO 27002 report categories, then click a category to see the list of reports. Click **NIST 800-53** to see the list of NIST 800-53 reports.
 - To view the installed dashboards, click **Dashboards** on the top-level menu and you should see IT Governance Dashboards.

To install Logger CIP for IT Gov on the Software Logger:

1. Log into the system running the Software Logger with the same ID that you used to install the software version of Logger.
2. Download the Logger CIP for IT Gov .bin file (for example, ArcSight-ComplianceInsightPackage-Logger-ITGov.x.x.nnnn.0.bin). Check the Release Notes for the exact version of the file.
3. Go to the directory that contains the .bin file.
4. Change the permissions of the .bin file to be executable:

```
chmod +x ArcSight-ComplianceInsightPackage-Logger-ITGov.x.x.nnnn.0.bin
```

5. Run the installer:

```
./ArcSight-ComplianceInsightPackage-Logger-ITGov.x.x.nnnn.0.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 Logger CIP for IT Gov reports, parameters, queries, dashboards, and alerts.

7. Verify that the content is installed:
 - To view the installed alerts, click **Configuration** on the top-level menu bar, then click **Alerts** in the **Data** section.
 - To view the installed reports, click **Reports** on the top-level menu bar, then click **Report Explorer** in the **Navigation** section. Click the arrow to the left of **ISO 27002** to see the ISO 27002 report categories, then click a category to see the list of reports. Click **NIST 800-53** to see the list of NIST 800-53 reports.
 - To view the installed dashboards, click **Dashboards** on the top-level menu and you should see IT Governance Dashboards.

Chapter 3: Configuring Logger CIP for IT Gov

These topics describe how to configure Logger CIP for IT Gov to work in your environment.

• Processing Events	15
• Limiting the Events Processed	15
• Configuring Alerts	19
• Configuring Reports	20

Processing Events

The **Logger CIP for IT Gov reports** process all events received by the Logger and no configuration is required.

The **Logger CIP for IT Gov alerts** are configured to process all events except events that are stored in the Internal Event Storage Group. Some alerts require configuration with site-specific information; see ["Configuring Alerts" on page 19](#).

Note: You can enable a maximum of 25 alerts on Logger at one time. Only configure the alerts that you plan to enable. See the *ArcSight Logger Administrator's Guide* for information about enabling and disabling alerts.

If only some of your devices are subject to Logger CIP for IT Gov compliance, you can limit the events processed by reports and alerts. See ["Limiting the Events Processed" below](#).

Limiting the Events Processed

If only some of your devices are subject to Logger CIP for IT Gov compliance, you can limit the events processed by the reports and alerts to improve Logger system performance and report more accurate and Logger CIP for IT Gov-relevant information.

You can limit the events processed in one or more of the following ways, depending on how your environment is set up and how you want to organize your ArcSight Logger CIP for IT Governance compliance program.

- Create an Logger CIP for IT Gov-specific *device group* and only process events from devices in that group.
- Use an Logger CIP for IT Gov-related *storage group* to limit the events processed by the ArcSight Logger CIP for IT Governance reports and alerts. This is only appropriate if an additional storage group (in addition to the Default Storage and Internal Event storage groups) was created during the

Logger initialization process. After the Logger initializes, you cannot allocate additional storage groups. For details, see the *ArcSightLogger Administrator's Guide*.

- Process events from specified devices only.

Tip: Reducing the amount of data a resource has to process improves performance. If only a small subset of the overall data feeding into Logger is subject to ArcSight Logger CIP for IT Governance compliance, using a different storage group to store events from Logger CIP for IT Gov-related devices yields the best performance results.

To limit the events processed by the Logger CIP for IT Gov reports and alerts, implement one or more of these limiting strategies by following the configuration steps provided in the following sections.

- Classify IT Governance-related devices in an IT Governance device group. See ["Classifying Logger CIP for IT Gov-Related Devices in a Device Group" below](#).
- Create an IT Governance filter that constrains the events processed by the alerts and reports. See ["Creating a Filter to Limit Events Processed" on the next page](#).
- Limit the events that an alert processes by either applying the IT Governance filter to the alert or adding the condition directly to the alert. See ["Limiting Events Processed by Alerts" on page 18](#).
- Apply the IT Governance filter to the entire Logger CIP for IT Gov report category or specify at report run time. See ["Limiting Events Processed by Reports" on page 19](#).

Classifying Logger CIP for IT Gov-Related Devices in a Device Group

If you plan on using a Device Group to limit the events processed by reports and alerts, create an Logger CIP for IT Gov device group and classify the Logger CIP for IT Gov-related devices into it as described in following procedure. After the Logger CIP for IT Gov-related devices are categorized, you can use the device group to focus on alerts and reports. For example, you can create a filter that only returns events from devices listed in the Logger CIP for IT Gov Device Group filter and then configure alerts and reports to use that filter to limit the events processed.

To classify Logger CIP for IT Gov-related devices into an Logger CIP for IT Gov Device Group:

1. Select **Configuration** on the top-level menu bar, then click **Device Groups** in the **Data** section.
2. Click **Add**.
3. In the **Name** field, enter a name for the new device group, such as Logger CIP for IT Gov.
4. In the **Devices** field, click to select devices from the list. To add additional devices to the selection, press and hold the **Ctrl** key when selecting more devices.
5. Click **Save** to create the new Device Group.

6. Create a filter to limit the events processed, as described in ["Creating a Filter to Limit Events Processed" below](#).

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

Creating a Filter to Limit Events Processed

Create a filter that identifies the IT Governance-related events for your environment. Use the filter to limit the events processed by IT Governance alerts and reports. A filter can limit events as follows:

- **Limit using an Logger CIP for IT Gov-related device group**—Only those events from devices listed in the device group are processed.
- **Limit using an Logger CIP for IT Gov-related storage group**—Only those events stored in the specified storage group are processed.
- **Limit by specific devices**—Only events from specific devices are processed.

For example, you can create any of the following filters:


- A filter called `Logger CIP for IT Gov Device Group Filter` which returns events from devices categorized as ArcSight Logger CIP for IT Governance devices.
- A filter called `Logger CIP for IT Gov Storage Group Filter` which returns events that are stored in a designated storage group.
- A filter called `Logger CIP for IT Gov Devices Filter` which returns events from specified devices.
- A filter called `Logger CIP for IT Gov Storage Group and Devices Filter` that returns events stored in a designated storage group (such as an `Logger CIP for IT Gov Storage Group`) or from a set of specific devices.

To create a filter:

1. Select **Configuration** on the top-level menu bar, then click **Filters** in the **Search** section.
2. Click **Add**.
3. In the **Add Filter** page, enter the following information:

Field	Description
Name	Enter a name for the filter that identifies it with Logger CIP for IT Gov and identifies the purpose of the filter, such as <code>Logger CIP for IT Gov Device Group Filter</code> or <code>Logger CIP for IT Gov Storage Group Filter</code> or <code>Logger CIP for IT Gov Devices Filter</code> .
Type	From the drop-down menu, select Search Group . A filter of type Search Group can be used by both alerts and reports to constrain events.

4. In the Query field, construct a query, using one of the following options:
 - In the **Query** field, directly enter a regular expression, for example: `storageGroup(Default Storage Group)|deviceGroup(Logger CIP for IT Gov Device Group)`

- Use the *Constrain search by* dialog—Select the  icon. In the *Constrain search by* dialog, select from one of the following options:
 - Focus alerts to only process events from devices listed in the device group—Click **Device Groups**. Select a device group from the list and click **Submit**.
 - Focus alerts to only process events saved in a designated storage group—Click **Storage Groups**. Select a storage group from the list and click **Submit**.
 - Focus the alerts to only process events from individual devices subject to ArcSight Logger CIP for IT Governance compliance—Select devices from the lists and click **Submit**. To select more than one device, press and hold the **Ctrl** key while selecting more devices.
- 5. Click **Save**.
- 6. Use the filter you created to limit the events processed by both reports and alerts. See ["Limiting Events Processed by Alerts" below](#) and ["Limiting Events Processed by Reports" on the next page](#)

Limiting Events Processed by Alerts


To limit the events that an alert processes, either add a filter or add a Query Term to the alert.


Note: You can enable a maximum of 25 alerts on Logger at one time. Configure only the alerts that you plan to enable.

To add a filter to the alert:

1. Select **Configuration** on the top-level menu bar, then click **Alerts** in the **Data** section.
2. To edit the alert, click the Logger CIP for IT Gov alert in the Name column.
3. Click **Add**.
4. In the **Filters** field, select the filter you created in ["Creating a Filter to Limit Events Processed" on the previous page](#) that limits the events processed by the alert.
5. Click **Save**.

To add a Query Term to the alert:


1. Select **Configuration** on the top-level menu bar, then click **Alerts** in the **Data** section.
2. To edit the alert, click the Logger CIP for IT Gov alert in the Name column.
3. On the top-level Query Term field, click the Add () icon.
A new empty Query term displays.
4. In the new Query Terms field, add a condition to the alert, using one of the following methods:
 - In the Query Terms field, directly enter a regular expression, for example: `storageGroup (Default Storage Group)|deviceGroup(Logger CIP for IT GovDeviceGroup)`

- Use the *Constrain search by* dialog. Select the  icon and select from one of the following options in the *Constrain search by* dialog:
 - Focus alerts to only process events from devices listed in the device group—Click **Device Groups**. Select a device group from the list and click **Submit**.
 - Focus alerts to only process events saved in a designated storage group—Click **Storage Groups**. Select a storage group from the list and click **Submit**.
 - Focus the alerts to only process events from individual devices subject to Logger CIP for IT Gov compliance. Select devices from the list and click **Submit**. To select more than one device, press and hold the **Ctrl** key while selecting more devices.
5. Click **Save**.

Limiting Events Processed by Reports

You can limit events processed by the Logger CIP for IT Gov reports either with a filter or at report run time.

To limit the events using a filter, apply a report category (search group) filter to a whole report category.

To limit events at report run time, run the report using the Quick Run () option. Select **Configuration** on the top-level menu bar, then click **Devices** or **Device Groups** in the **Data** section to select one or more devices or device groups. Or, select **Configuration** on the top-level menu bar, then click **Storage Groups** in the **Storage** section to select one or more storage groups.

For more information about report category filters and scheduling reports, see the *ArcSight Logger Administrator's Guide*.

Configuring Alerts

Many of the Logger CIP for IT Gov alerts contain site-specific data, such as administrator account names and default ports and protocols, which you need to configure with details specific to your environment.

The following table lists the alerts that require configuration.

Alert Name	Required Configuration
IT Governance - Default Vendor Account Used	<p>In the Query Terms field that lists the default user names, change the set of default account names to reflect the set of account names used by software applications at your site. For example, add the CTXSYS user name to the user list:</p> <pre>user=(admin root sa nobody guest manager sys system oracle orcladmin cisco pixadmin CTXSYS)</pre> <p>Separate the user names using the pipe character (). The pipe character represents an OR operator.</p>
IT Governance - Disallowed Port Access	<p>In the Query Terms field that lists the default ports, change the set of default ports to reflect your site. For example, add the 8080 port to the list:</p> <pre>(d s)pt=(80 443 8080)</pre> <p>Separate the port using the pipe character (). The pipe character represents an OR operator. To specify a unique port number add a space character after the number. For example, specifying port 90 without a space matches any port number that starts with 90 such as 9000 or 9090.</p>

To configure an alert with site specific data:

1. Select the **Configuration** tab.
2. From the left panel menu, select **Alerts**.
3. Click on the alert you need to configure.
4. Find the Query Term with the site specific data and change it to reflect your site.
5. Click **Save**.

Configuring Reports

Some reports require that you provide site-specific data, such as admin account names and default ports.

The following table lists the ISO 27002 reports that require configuration.

Configuring ISO 27002 Reports

Report Name	Required Configuration
ISO 12 - Account Activity by User	This report prompts you to supply values for the destinationUserName parameter.
ISO 12 - Administrative Actions - All Events	This report prompts you to supply values for the deviceProduct, eventName, adminUsers, variable, DeviceEventClassId, and sourceDestUserName parameters.
ISO 12 - Administrative Actions by Event Name	This report prompts you to supply values for the deviceProduct, adminUsers, and sourceDestUserName parameters.

Configuring ISO 27002 Reports, continued

Report Name	Required Configuration
ISO 12 - Administrative Actions by Product	This report prompts you to supply values for the <code>adminUsers</code> and <code>sourceDestUserName</code> parameters.
ISO 12 - Changes to Development Network Machines	This report prompts you to supply a value for the <code>developmentNetwork</code> parameter.
ISO 12 - Failed Administrative Logins per System - Detail ISO 12 - Failed Administrative Logins per User - Detail	These reports prompt you to supply values for the <code>destinationAddress</code> , <code>destinationHostName</code> , <code>adminUsers</code> , <code>deviceProduct</code> , and <code>sourceDestUserName</code> parameters.
ISO 12 - Administrative Actions by User ISO 12 - Administrative Logins and Logouts ISO 12 - Failed Administrative Logins by System ISO 12 - Failed Administrative Logins by User ISO 12 - Failed User Logins by System ISO 12 - Successful Administrative Logins by System ISO 12 - Successful Administrative Logins by User ISO 12 - Successful User Logins by User Name ISO 12 - Successful User Logins by System ISO 9 - Privileged Account Changes	These reports prompt you to supply values for the <code>adminUsers</code> parameter.
ISO 13 - Insecure Services	Customize the list of insecure services listed in the associated query to reflect the devices used in your environment.
ISO 12 - Failed Administrative Logins per System - Summary ISO 12 - Failed User Logins per System - Summary ISO 12 - Successful Administrative Logins per System - Summary ISO 12 - Successful User Logins per System - Summary	These reports prompt you to supply values for the <code>destinationAddress</code> and <code>adminUsers</code> parameters.
ISO 12 - Failed Administrative Logins per User - Summary	This report prompts you to supply values for the <code>destinationAddress</code> , <code>adminUsers</code> , and <code>sourceDestUserName</code> parameters.

Configuring ISO 27002 Reports, continued

Report Name	Required Configuration
ISO 12 - Failed User Logins per System - Detail ISO 12 - Failed User Logins per User Name - Detail ISO 12 - Successful Administrative Logins per System - Detail ISO 12 - Successful Administrative Logins per User - Detail ISO 12 - Successful User Logins per User Name - Detail	These reports prompt you to supply values for the deviceProduct, destinationAddress, destinationHostName, adminUsers, and sourceDestUserName parameters.
ISO 12 - Failed User Logins per User Name - Summary ISO 12 - Successful Administrative Logins per User - Summary ISO 12 - Successful User Logins per User Name - Summary	These reports prompt you to supply values for the destinationAddress, adminUsers, and sourceDestUserName parameters.
ISO 12 - File Changes in Production	This report prompts you to supply a value for the productionNetwork parameter.
ISO 12 - Internet Activity per Device per Machine ISO 12 - Internet Activity per Device per User	Customize the list of ports in the associated query to reflect the internet ports accessed by users at your site.
ISO 12 - Successful User Logins per System - Detail	This report prompts you to supply values for the deviceProduct, destinationAddress, destinationHostName, adminUsers, and sourceDestUserName parameters.
ISO 12 - Systems Accessed as Root or Administrator	Customize the list of account names in the associated query to reflect any additional default administrator account names use by devices at your site.
ISO 13 - Traffic - Inbound on Disallowed Ports	This report prompts you to supply a value for the allowedPorts and internalNetwork parameters.
ISO 12 - User Actions - All Events ISO 12 - User Actions by Event Name	These reports prompt you to supply values for the deviceProduct, eventName, adminUsers, variable, DeviceEventClassId, and sourceUserUserName parameters.
ISO 12 - User Actions by Product	This report prompts you to supply values for the deviceProduct and adminUsers parameters.
ISO 12 - User Actions by User Name and Product	This report prompts you to supply values for the deviceProduct, adminUsers, variable, and sourceUserUserName parameters.

Configuring ISO 27002 Reports, continued

Report Name	Required Configuration
ISO 12 - Viruses per Host ISO 12 - Virus Report - Detail	This report prompts you to supply values for the destinationAddress, destinationHostName, virusName, and eventPriority parameters.
ISO 9 - Database Privilege Violation	This report prompts you to supply values for the databaseAdminUsers and databaseAdminAccounts parameters.
ISO 9 - Default Vendor Account Used	Customize the list of default vendor accounts listed in the associated query to reflect the devices used in your environment.
ISO 13 - Development Network Not Segregated ISO 13 - Production Network Not Segregated ISO 13 - Test Network Not Segregated	These reports prompt you to supply values for the productionNetwork, testing Network, and developmentNetwork parameters.
ISO 13 - Peer to Peer Ports Count ISO 13 - Peer to Peer Sources by Machine - Detail ISO 13 - Peer to Peer Sources by Machine - Overview	Customize the associated query with any additional peer-to-peer destination ports.
ISO 13 - Services by Asset ISO 9 - Traffic from External to Internal Protected Domain ISO 8 - Network Active Assets ISO 9 - Traffic from Internal to External Protected Domain ISO 9 - Traffic - Inbound Count ISO 16 - Attacks - Hourly Count ISO 16 - Internal Reconnaissance - Top 20 Sources ISO 16 - Attacks Targeting Internal Assets ISO 16 - Internal Reconnaissance - Top 20 Events ISO 16 - Internal Reconnaissance - Top 20 Targets	These reports prompt you to supply values for the internalNetwork parameter.
ISO 6- Suspicious Activity in Wireless Network	This report prompts you to supply values for the wirelessNetwork parameter.
ISO 12 - Software Changes in Production	This report prompts you to supply values for the productionNetwork parameter.

Configuring ISO 27002 Reports, continued

Report Name	Required Configuration
ISO 16 - Attacks - Development to Production ISO 16 - Attacks - Production to Development	These reports prompt you to supply values for the <code>productionNetwork</code> and <code>developmentNetwork</code> parameters.
ISO 6 - Administrative Logins and Logouts from Third-Party Hosts ISO 6 - Administrative Logins and Logouts to Third-Party Hosts ISO 6 - Failed Admin Logins from Third-Party Systems ISO 6 - Failed Admin Logins to Third-Party Systems	These reports prompt you to supply values for the <code>adminUsers</code> and <code>thirdPartyNetworkparameters</code> .
ISO 6 - Attacks from Third-Party Systems ISO 6 - Attacks on Third-Party Systems ISO 6 - Compromised Third-Party Systems ISO 6 - Failed User Logins from Third-Party Systems ISO 6 - Failed User Logins to Third-Party Systems ISO 6 - File Activity on Third-Party Systems ISO 6 - File Creations on Third-Party Systems ISO 6 - File Deletions on Third-Party Systems ISO 6 - File Modifications on Third-Party Systems ISO 6 - Policy Violations on Third-Party Systems ISO 6 - Services Accessed by Third-Party Systems ISO 6 - User Logins and Logouts from Third-Party Systems ISO 6 - User Logins and Logouts to Third-Party Systems	These reports prompt you to supply values for the <code>thirdPartyNetwork</code> parameters.

The following table lists the NIST 800-53 reports that require configuration.

Configuring NIST 800-53 Reports

Report Name	Required Configuration
NIST AC - Account Activity by User	This report prompts you to supply values for the <code>destinationUserName</code> parameter.
NIST AC - Administrative Actions - All Events	This report prompts you to supply values for the <code>deviceProduct</code> , <code>eventName</code> , <code>adminUsers</code> , <code>deviceEventClassID</code> , and <code>sourceDestUserName</code> parameters.
NIST AC - Administrative Actions by Event Name	This report prompts you to supply values for the <code>deviceProduct</code> , <code>adminUsers</code> , and <code>sourceDestUserName</code> parameters.
NIST AC - Administrative Actions by Product	This report prompts you to supply values for the <code>adminUsers</code> and <code>sourceDestUserName</code> parameters.
NIST AC - Administrative Actions by User NIST AC - Administrative Logins and Logouts NIST AC - Failed Administrative Logins by System NIST AC - Failed Administrative Logins by User NIST AC - Failed User Logins by System NIST AC - Failed User Logins by User Name NIST AC - Privileged Account Changes NIST AC - Successful Administrative Logins by System NIST AC - Successful Administrative Logins by User NIST AC - Successful User Logins by System NIST AC - Successful User Logins by User Name	These reports prompt you to supply values for the <code>adminUsers</code> parameter.
NIST AC - Database Privilege Violation	This report prompts you to supply values for the <code>databaseAdminUsers</code> and <code>databaseAdminAccounts</code> parameters.
NIST AC - Development Network Not Segregated	This report prompts you to supply values for the <code>productionNetwork</code> and <code>testingNetwork</code> and <code>developmentNetwork</code> parameters.

Configuring NIST 800-53 Reports, continued

Report Name	Required Configuration
NIST AC - Failed Administrative Logins per System - Detail NIST AC - Failed Administrative Logins per User - Detail NIST AC - Successful Administrative Logins per System - Detail NIST AC - Successful Administrative Logins per User - Detail	These reports prompt you to supply values for the deviceProduct, destinationAddress, destinationHostName, adminUsers, and sourceDestUserName parameters.
NIST AC - Failed Administrative Logins per User - Summary NIST AC - Successful Administrative Logins per User - Summary	This report prompts you to supply values for the destinationAddress, adminUsers and sourceDestUserName parameters.
NIST PS - Failed User Logins from Third-Party Systems	This report prompts you to supply values for the thirdPartyNetwork parameter.
NIST AC - Failed Administrative Logins per System - Summary NIST AC - Failed User Logins per System - Summary NIST AC - Failed User Logins per User Name - Summary NIST AC - Successful Administrative Logins per System - Summary NIST AC - Successful User Logins per System - Summary NIST AC - Successful User Logins per User Name - Summary	These reports prompt you to supply values for the destinationAddress and adminUsers parameters.

Configuring NIST 800-53 Reports, continued

Report Name	Required Configuration
NIST PS - Failed User Logins to Third-Party Systems	These reports prompt you to supply values for the <code>thirdPartyNetwork</code> parameter.
NIST AC - File Activity on Third-Party Systems	
NIST AC - File Creations on Third-Party Systems	
NIST AC - File Deletions on Third-Party Systems	
NIST AC - File Modifications on Third-Party Systems	
NIST AC - User Logins and Logouts from Third-Party Systems	
NIST AC - User Logins and Logouts to Third-Party Systems	
NIST CM - Changes to Third-Party Resources	
NIST IR - Compromised Third-Party Systems	
NIST IR - Policy Violations from Third-Party Systems	
NIST PS - Attacks from Third-Party Systems	
NIST PS - Attacks on Third-Party Systems	
NIST PS - Services Accessed by Third-Party Systems	
NIST AC - Third-Party Systems Accessed	

Configuring NIST 800-53 Reports, continued

Report Name	Required Configuration
NIST AC - Internal Reconnaissance - Top 20 Events NIST AC - Internal Reconnaissance - Top 20 Sources NIST AC - Internal Reconnaissance - Top 20 Targets NIST AC - Services by Asset NIST CM - Network Active Assets NIST AC - Traffic - Inbound Count NIST AC - Traffic from External to Internal Protected Domain NIST AC - Traffic from Internal to External Protected Domain NIST IR - Attacks - Hourly Count NIST IR - Attacks Targeting Internal Assets	These reports prompt you to supply values for the <code>internalNetwork</code> parameter.
NIST AC - Internet Activity per Device per Machine NIST AC - Internet Activity per Device per User	Customize the list of ports in the associated query to reflect the internet ports accessed by users at your site.
NIST AC - Failed User Logins per System - Detail NIST AC - Successful User Logins per System - Detail NIST AC - Successful User Logins per User Name - Detail NIST AC - Failed User Logins per User Name - Detail	This report prompts you to supply values for the <code>deviceProduct</code> , <code>destinationAddress</code> , <code>destinationHostName</code> , and <code>adminUsers</code> parameters.
NIST AC - Suspicious Activity in Wireless Network	This report prompts you to supply values for the <code>wirelessNetwork</code> parameter.
NIST AC - Test Network Not Segregated	This report prompts you to supply values for the <code>productionNetwork</code> and <code>testingNetwork</code> and <code>developmentNetwork</code> parameters.
NIST AC - User Actions - All Events NIST AC - User Actions by Event Name	This report prompts you to supply values for the <code>deviceProduct</code> , <code>eventName</code> , <code>adminUsers</code> , <code>variable</code> , <code>deviceEventClassID</code> , and <code>sourceDestUserName</code> parameters.

Configuring NIST 800-53 Reports, continued

Report Name	Required Configuration
NIST AC - User Actions by Product	This report prompts you to supply values for the <code>deviceProduct</code> and <code>adminUsers</code> parameters.
NIST AC - User Actions by User Name and Product	This report prompts you to supply values for the <code>deviceProduct</code> , <code>adminUsers</code> , <code>variable</code> , and <code>sourceUserName</code> parameters.
NIST CM - Changes to Development Network Machines	This report prompts you to supply values for the <code>developmentNetwork</code> parameter.
NIST CM - File Changes in Production	This report prompts you to supply values for the <code>productionNetwork</code> parameter.
NIST IA - Default Vendor Account Used	Customize the list of default vendor accounts listed in the associated query to reflect the devices used in your environment.
NIST IA - Systems Accessed as Root or Administrator	Customize the list of account names in the associated query to reflect any additional default administrator account names use by devices at your site.
NIST IR - Attacks - Development to Production NIST IR - Attacks - Production to Development	These reports prompt you to supply values for the <code>productionNetwork</code> and <code>developmentNetwork</code> parameters.
NIST IR - Traffic - Inbound on Disallowed Ports	This report prompts you to supply values for the <code>allowedPorts</code> and <code>internalNetwork</code> parameters.
NIST PS - Administrative Logins and Logouts from Third-Party Hosts NIST PS - Administrative Logins and Logouts to Third-Party Hosts NIST PS - Failed Admin Logins from Third-Party Systems NIST PS - Failed Admin Logins to Third-Party Systems	These reports prompt you to supply values for the <code>adminUsers</code> and <code>thirdPartyNetwork</code> parameters.
NIST SA - Peer to Peer Ports Count NIST SA - Peer to Peer Sources by Machine - Detail NIST SA - Peer to Peer Sources by Machine - Overview	Customize the associated query with any additional peer-to-peer destination ports.

Configuring NIST 800-53 Reports, continued

Report Name	Required Configuration
NIST SC - Insecure Services	Customize the ports and processes listed in the associated query to reflect the ports and processes that are considered insecure in your environment.
NIST SI - Software Changes in Production	This report prompts you to supply values for the <code>productNetwork</code> parameter.
NIST SI - Viruses per Host NIST SI - Virus Report - Detail	This report prompts you to supply values for the <code>destinationAddress</code> , <code>destinationHostName</code> , <code>virusName</code> and <code>eventPriority</code> parameters.

Chapter 4: Logger CIP for IT Gov Alerts

Logger CIP for IT Gov alerts monitor incoming events and notify analysts when events of interest are detected. After you customize and enable an alert, it is ready to be triggered.

When the alert triggers, an internal alert event is generated. You can search and view these internal alert events in real-time from the **Analyze** tab of the Console. For more information, see the *ArcSight Logger Administrator's Guide*.

The Logger CIP for IT Gov alerts are listed in the table below.

Note: The table below specifies the default Match Count and the default Threshold (Sec) for each alert. The Match Count and Threshold (sec) fields determine when an enabled alert triggers. An alert triggers when the specified number of matches is seen within the specified time threshold. You can customize these settings. For more information, see the *ArcSight Logger Administrator's Guide*.

Alert Name	Description
IT Governance - Access Right Removed	<p>This alert triggers when an access right or privilege is successfully removed from an account.</p> <p>Default Match Count: 1</p> <p>Default Threshold (Sec): 1</p>
IT Governance - Account Lockout	<p>This alert triggers when an account lockout is detected on a Windows system. A account lockout occurs when there are too many failed login attempts into an account.</p> <p>Default Match Count: 1</p> <p>Default Threshold (Sec): 1</p>
IT Governance - Audit Log Cleared	<p>This alert triggers when the Windows audit log is cleared.</p> <p>Default Match Count: 1</p> <p>Default Threshold (Sec): 1</p>

Alert Name	Description
IT Governance - Default Vendor Account Used	<p>This alert triggers when the source or destination account name matches one of the following default account names: admin, root<space>, sa<space>, nobody<space>, guest<space>, manager<space>, sys<space>, system<space>, oracle<space>, orcladmin<space>, cisco<space>, pixadmin<space>.</p> <p>Where <space> represents the space character. All account names are case insensitive.</p> <p>In the Query Terms field that specifies the account names, the admin account name is specified without a trailing space. Specifying an account name without a trailing space means any account name that starts with the same set of characters is matched; for example, the account name admin matches any string beginning with admin including Administrator or admins. This pattern matching does not occur with the account names that end with the <space> character, for example the account name sa<space> does not match the string sarah.</p> <p>Default Match Count: 1</p> <p>Default Threshold (Sec): 1</p>
IT Governance - Disallowed Port Access	<p>This alert triggers when traffic is detected over ports not specified in the list of allowed ports. Traffic over the default ports of 80 and 443 are allowed.</p> <p>Default Match Count: 1</p> <p>Default Threshold (Sec): 1</p>
IT Governance - Exploit of Vulnerability Detected	<p>This alert triggers when an exploit of a known vulnerability is detected.</p> <p>Default Match Count: 1</p> <p>Default Threshold (Sec): 1</p>
IT Governance - Failed File Access	<p>This alert triggers when a failed attempt to access a file occurs.</p> <p>Default Match Count: 1</p> <p>Default Threshold (Sec): 1</p>
IT Governance - Failed File Deletion	<p>This alert triggers when a failed attempt to delete a file occurs.</p> <p>Default Match Count: 1</p> <p>Default Threshold (Sec): 1</p>
IT Governance - Information Leak	<p>This alert triggers when a leak of high, medium or low classified information is detected.</p> <p>Default Match Count: 1</p> <p>Default Threshold (Sec): 1</p>

Alert Name	Description
IT Governance - Insecure Services Use Detected	<p>This alert triggers when insecure services are running on an internal system or a connection is made to insecure port on an internal system. These services are defined as insecure: telnetd, ftpd, rexec, pop3, rsh, imapd.</p> <p>An insecure port is a port number that is commonly used by an insecure service. These ports are defined as insecure: 20, 21, 25, 110, 143, 23.</p> <p>Default Match Count: 1</p> <p>Default Threshold (Sec): 1</p>
IT Governance - Internal Recon Detected	<p>This alert triggers when evidence of an internal network reconnaissance is detected. Employees might be attempting to prove suspected security weaknesses on the network.</p> <p>Default Match Count: 1</p> <p>Default Threshold (Sec): 1</p>
IT Governance - Low Severity Scanner Events	<p>This alert triggers when low severity scanner events are reported.</p> <p>Default Match Count: 1</p> <p>Default Threshold (Sec): 1</p>
IT Governance - Malicious Code Detected	<p>This alert triggers when malicious code has been detected.</p> <p>Default Match Count: 1</p> <p>Default Threshold (Sec): 1</p>
IT Governance - Multiple Invalid Data Input Attempts Detected	<p>This alert triggers when multiple attempts at entering invalid data into application(s) are detected.</p> <p>Default Match Count: 3</p> <p>Default Threshold (Sec): 30</p>
IT Governance - New Host Detected Alert	<p>This alert triggers when new hosts are found on the network.</p> <p>Default Match Count: 1</p> <p>Default Threshold (Sec): 60</p>
IT Governance - New Service Detected	<p>This alert triggers when new network services are found on machines in the network.</p> <p>Default Match Count: 1</p> <p>Default Threshold (Sec): 1</p>
IT Governance - New User Account Created	<p>This alert triggers when new accounts are created.</p> <p>Default Match Count: 1</p> <p>Default Threshold (Sec): 1</p>

Alert Name	Description
IT Governance - Outbound IM Traffic	<p>This alert triggers when outbound instant messenger traffic is detected.</p> <p>Default Match Count: 1</p> <p>Default Threshold (Sec): 1</p>
IT Governance - Possible Information Interception	<p>This alert triggers when possible information interception such as spoofing attempts or man-in-the-middle attacks are detected.</p> <p>Default Match Count: 1</p> <p>Default Threshold (Sec): 1</p>
IT Governance - Security Software Stopped or Paused	<p>This alert triggers when security software has been disabled.</p> <p>Default Match Count: 1</p> <p>Default Threshold (Sec): 1</p>
IT Governance - Successful Attack - Brute Force	<p>This alert triggers when a successful brute force attack is detected.</p> <p>Default Match Count: 1</p> <p>Default Threshold (Sec): 1</p>
IT Governance - Successful File Access Alert	<p>This alert triggers when a successful attempt to access a file occurs.</p> <p>Default Match Count: 1</p> <p>Default Threshold (Sec): 1</p>
IT Governance - Successful File Deletion	<p>This alert triggers when a successful attempt to delete a file occurs.</p> <p>Default Match Count: 1</p> <p>Default Threshold (Sec): 1</p>
IT Governance - System with Vulnerabilities	<p>This alert triggers when system(s) with known vulnerabilities are detected.</p> <p>Default Match Count: 1</p> <p>Default Threshold (Sec): 1</p>
IT Governance - User Account Deletion	<p>This alert triggers when the deletion of a user account is detected.</p> <p>Default Match Count: 1</p> <p>Default Threshold (Sec): 1</p>
IT Governance - User Password Change Detected	<p>This alert triggers when a password change for a user account is detected.</p> <p>Default Match Count: 1</p> <p>Default Threshold (Sec): 1</p>

Chapter 5: Logger CIP for IT Gov Reports

Logger CIP for IT Gov reports are described below.

• ISO 27002	35
• ISO 6 - Organization of information security	35
• ISO 8 - Asset management	37
• ISO 9 - Access control	38
• ISO 10 - Cryptography	40
• ISO 11 - Physical and environmental security	40
• ISO 12 - Operations security	41
• ISO 13 - Communications security	56
• ISO 14 - System acquisition development and maintenance	58
• ISO 16 - Information security incident management	59
• ISO 17 - Information security aspects of business continuity management	60
• ISO 18 - Compliance	61
• NIST 800-53	61

ISO 27002

The ISO 27002 category executive report is listed below.

ISO 27002

Report	Description	Drill Down
ISO Executive Report	This report is made up of 4 charts:1. Top 10 Alerts Fired2. Top 10 Failed Logins3. 10 Most Attacked Hosts4. 10 Hosts with Most Virus Events	none

ISO 6 - Organization of information security

The ISO 6 - Organization of information security category is located under the following path.

ISO 27002\ISO 6 - Organization of information security

The ISO 6 - Organization of information security category reports are listed in the following table.

ISO 6 - Organization of information security

Report	Description	Drill Down
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.	none
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.	none
ISO 6 - Attacks from Third-Party Systems	This report displays the event, time, source, and destination of attacks originating from third-party systems.	none
ISO 6 - Attacks on Third-Party Systems	This report displays source and destination information from attacks against third-party systems.	none
ISO 6 - Compromised Third-Party Systems	This report displays all successful compromise attempts targeting third-party systems.	none
ISO 6 - Failed Admin Logins from Third-Party Systems	This report displays all failed administrative logins from third-party systems.	none
ISO 6 - Failed Admin Logins to Third-Party Systems	This report displays all failed administrative logins to third-party systems.	none
ISO 6 - Failed User Logins from Third-Party Systems	This report displays all failed user logins from third-party systems.	none
ISO 6 - Failed User Logins to Third-Party Systems	This report displays all failed user logins to third-party systems.	none
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.	none

ISO 6 - Organization of information security, continued

Report	Description	Drill Down
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.	none
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.	none
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.	none
ISO 6 - Misconfigured Wireless Devices	This report shows a list of wireless devices that are configured incorrectly.	none
ISO 6 - Policy Violations from Third-Party Systems	This report displays the events indicating policy violations from third-party systems.	none
ISO 6 - Services Accessed by Third-Party Systems	This report displays the port, service, and destination information of services accessed by third-party systems.	none
ISO 6 - 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.	none
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.	none
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.	none

ISO 8 - Asset management

The ISO 8 - Asset management category is located under the following path.

ISO 27002\ISO 8 - Asset management

The ISO 8 - Asset management category reports are listed in the following table.

ISO 8 - Asset management

Report	Description	Drill Down
ISO 8 - 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.	none
ISO 8 - New Hosts	This report displays all new hosts on the network detected by traffic analysis systems.	none
ISO 8 - New Services	This report displays all new services detected on the network by traffic analysis systems.	none

ISO 9 - Access control

The ISO 9 - Access control category is located under the following path.

ISO 27002\ISO 9 - Access control

The ISO 9 - Access control category reports are listed in the following table.

ISO 9 - Access control

Report	Description	Drill Down
ISO 9 - 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.	none
ISO 9 - 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.	none
ISO 9 - Authorization Changes	This report shows authorization changes made on systems and the number of events per host name.	none
ISO 9 - 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\'.	none

ISO 9 - Access control, continued

Report	Description	Drill Down
ISO 9 - 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.	none
ISO 9 - 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.	none
ISO 9 - 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.	none
ISO 9 - Privileged Account Changes	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.	none
ISO 9 - 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.	none
ISO 9 - Successful Brute Force Logins	This report displays the time, user, and host information from successful brute-force logins.	none
ISO 9 - Traffic from External to Internal Protected Domain	This report shows information from all events indicating traffic from external to internal systems.	none
ISO 9 - Traffic from Internal to External Protected Domain	This report shows information from all events indicating traffic from internal to external systems.	none
ISO 9 - 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.	none

ISO 9 - Access control, continued

Report	Description	Drill Down
ISO 9 - 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.	none
ISO 9 - User Account Deletion	This report shows events indicating user accounts have been removed from a system.	none
ISO 9 - VPN Access Summary	This report displays a summary of VPN access by users.	none

ISO 10 - Cryptography

The ISO 10 - Cryptography category is located under the following path.

ISO 27002\ISO 10 - Cryptography

The ISO 10 - Cryptography category reports are listed in the following table.

ISO 10 - Cryptography

Report	Description	Drill Down
ISO 10 - Insecure cryptographic storage	This report shows insecure cryptographic storage detected on your systems.	none
ISO 10 - 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.	none
ISO 10 - Systems Providing Unencrypted Services	This report shows systems that provide unencrypted communications and the number of such events recorded. Unencrypted communication is defined as using one of the following services: telnetd, ftpd, in.rexecd, rexec, pop3, rsh, imapd; or is performed on the following ports: 20, 21, 25, 110, 143, 23. These values are defined in the query and can be adjusted according to the customer's definitions.	none

ISO 11 - Physical and environmental security

The ISO 11 - Physical and environmental security category is located under the following path.

ISO 27002\ISO 11 - Physical and environmental security

The ISO 11 - Physical and environmental security category reports are listed in the following table.

ISO 11 - Physical and environmental security

Report	Description	Drill Down
ISO 11 - Failed Building Access Attempts	This report displays all failed building access attempts including user name, id, and badge reader number.	none
ISO 11 - 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.	none

ISO 12 - Operations security

The ISO 12 - Operations security category is located under the following path.

ISO 27002\ISO 12 - Operations security

The ISO 12 - Operations security category reports are listed in the following table.

ISO 12 - Operations security

Report	Description	Drill Down
ISO 12 - Account Activity by User	This report displays all the events with the specified destination user name. The destination user name is defined at runtime.	none
ISO 12 - Administrative Actions - All Events	This report shows all actions taken by administrators sorted by event time.	none
ISO 12 - Administrative Actions by Event Name	For each event name this reports shows a count of events in which an administrative user appeared either in the source user name or destination user name fields.	The Count field drill downs to the "ISO 12 - Administrative Actions - All Events" above report.
ISO 12 - Administrative Actions by Product	This report shows a count of all actions performed by an administrator for each Product. The report is ordered alphabetically by the product name.	The Count field drill downs to the "ISO 12 - Administrative Actions - All Events" above report. The Distinct Events field drill downs to the "ISO 12 - Administrative Actions by Event Name" above report.

ISO 12 - Operations security, continued

Report	Description	Drill Down
ISO 12 - Administrative Actions by User	This reports shows a count of events in which an administrative user appeared either in the source username or destination username fields.	<p>The Number of Events field drill downs to the "ISO 12 - Administrative Actions - All Events" on the previous page report.</p> <p>The Number Of Devices field drill downs to the "ISO 12 - Administrative Actions by Product" on the previous page report.</p>
ISO 12 - Administrative Logins and Logouts	This report displays administrative logins and logouts. The chart displays the number of such events per system.	none
ISO 12 - Application Configuration Modifications	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.	none
ISO 12 - Audit Log Cleared	This report displays the date, time, system, and user information from all events indicating an audit log has been cleared.	none
ISO 12 - Blocked Firewall Traffic	This report displays events generated by devices that have blocked traffic. The chart displays the number of blocking events.	none
ISO 12 - Changes to Development Network Machines	This report displays all changes to machines in the development network.	none
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.	none
ISO 12 - Changes to Third-Party Resources	This report displays events indicating a change was made to a third-party application or resource.	none
ISO 12 - 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.	none

ISO 12 - Operations security, continued

Report	Description	Drill Down
ISO 12 - Database Access - All	This report displays a count of database access attempts per hour.	none
ISO 12 - Database Access - Failed	This report displays a count of database access attempt failures per hour.	none
ISO 12 - 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.	none
ISO 12 - 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.	none
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.	none
ISO 12 - Failed Administrative Logins by System	This report displays all failed administrative logins, by system.	<p>The Dest IP field drill downs to the "ISO 12 - Failed Administrative Logins per System - Summary" on the next page report.</p> <p>The Count field drill downs to the "ISO 12 - Failed Administrative Logins per System - Detail" on the next page report.</p> <p>This report drills down to itself.</p>

ISO 12 - Operations security, continued

Report	Description	Drill Down
ISO 12 - Failed Administrative Logins by User	This report displays all administrative users that failed to log into systems, the number of failed logins and the number of distinct systems that were attempted to log into.	<p>The Source or Dest User field drill downs to the "ISO 12 - Failed Administrative Logins per User - Summary" on the next page report.</p> <p>The Number of Logins field drill downs to the "ISO 12 - Failed Administrative Logins per User - Detail" below report.</p> <p>This report drills down to itself.</p>
ISO 12 - Failed Administrative Logins per System - Detail	This report displays all the failed administrative logins into a particular system. The chart shows the number of failed administrative logins for each product.	none
ISO 12 - Failed Administrative Logins per System - Summary	This report displays all the administrative users that failed to login into each system and the number of such failed logins.	<p>The User Name field drill downs to the "ISO 12 - Failed Administrative Logins per User - Summary" on the next page report.</p> <p>The Count field drill downs to the "ISO 12 - Failed Administrative Logins per System - Detail" above report.</p> <p>This report drills down to itself.</p>
ISO 12 - Failed Administrative Logins per User - Detail	This report displays all failed logins for the selected administrative user. The chart shows the number of failed logins per product.	<p>The Dest IP field drill downs to the "ISO 12 - Failed Administrative Logins per System - Summary" above report.</p> <p>This report drills down to itself.</p>

ISO 12 - Operations security, continued

Report	Description	Drill Down
ISO 12 - Failed Administrative Logins per User - Summary	This report displays all the systems that the selected administrative users failed to login into, and the number of such failed logins.	<p>The Dest IP field drill downs to the "ISO 12 - Failed Administrative Logins per System - Summary" on the previous page report.</p> <p>The Count field drill downs to the "ISO 12 - Failed Administrative Logins per User - Detail" on the previous page report.</p> <p>This report drills down to itself.</p>
ISO 12 - Failed Anti-Virus Updates	This report displays the date, host, and product information from failed anti-virus update events.	none
ISO 12 - Failed File Access	This report shows information from events indicating failed attempts to access files.	none
ISO 12 - Failed File Deletions	This report shows information from events indicating failed attempts to delete files.	none
ISO 12 - Failed User Logins by System	This report displays all failed non-administrative logins by system.	<p>The Dest IP field drill downs to the "ISO 12 - Failed User Logins per System - Summary" on the next page report.</p> <p>The Count field drill downs to the "ISO 12 - Failed User Logins per System - Detail" on the next page report.</p> <p>This report drills down to itself.</p>

ISO 12 - Operations security, continued

Report	Description	Drill Down
ISO 12 - Failed User Logins by User Name	This report displays all non-administrative users that failed to log into systems, the number of failed logins and the number of distinct systems that were attempted to log into.	<p>The Source or Dest User field drill downs to the "ISO 12 - Failed User Logins per User Name - Summary" on the next page report.</p> <p>The Number of Logins field drill downs to the "ISO 12 - Failed User Logins per User Name - Detail" below report.</p> <p>This report drills down to itself.</p>
ISO 12 - Failed User Logins per System - Detail	This report displays all the failed non-administrative logins into a particular system.	none
ISO 12 - Failed User Logins per System - Summary	This report displays all the non-administrative users that failed to login into each system and the number of such failed logins.	<p>The User Name field drill downs to the "ISO 12 - Failed User Logins per User Name - Summary" on the next page report.</p> <p>The Count field drill downs to the "ISO 12 - Failed User Logins per System - Detail" above report.</p> <p>This report drills down to itself.</p>
ISO 12 - Failed User Logins per User Name - Detail	This report displays all failed logins for the selected non-administrative user.	<p>The Dest IP field drill downs to the "ISO 12 - Failed User Logins per System - Summary" above report.</p> <p>This report drills down to itself.</p>

ISO 12 - Operations security, continued

Report	Description	Drill Down
ISO 12 - Failed User Logins per User Name - Summary	This report displays all the systems that the selected non-administrative user failed to login to, and the number of such failed logins.	<p>The Dest IP field drill downs to the "ISO 12 - Failed User Logins per System - Summary" on the previous page report.</p> <p>The Count field drill downs to the "ISO 12 - Failed User Logins per User Name - Detail" on the previous page report.</p> <p>This report drills down to itself.</p>
ISO 12 - Fault Logs	This report displays all events indicating a system fault has occurred.	none
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.	none
ISO 12 - Firewall Configuration Changes	This report displays all events indicating a configuration file on a firewall has been changed.	none
ISO 12 - 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.	none
ISO 12 - 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.	none
ISO 12 - Machines Conducting Policy Breaches	This report displays source IP, hostname, and event information from events with a Category Technique of /Policy/Breach.	none
ISO 12 - Malicious Code Sources	This report displays the count of malicious code events from particular hosts.	none
ISO 12 - 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.	none

ISO 12 - Operations security, continued

Report	Description	Drill Down
ISO 12 - 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.	none
ISO 12 - Network Device Configuration Changes	This report displays events indicating configuration file changes on network equipment such as routers and switches.	none
ISO 12 - 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.	none
ISO 12 - Operating System Configuration Changes	This report details operating system configuration changes.	none
ISO 12 - Policy Violations	This report displays all policy breaches such as IM use or the downloading of sexual content. The chart displays the number of events per source ip address.	none
ISO 12 - Resource Exhaustion	This report displays a count of events indicating resource exhaustion on particular hosts.	none
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 is determined by the configuration of the productionNetwork parameter, and can be modified by the user at runtime. The chart displays the number of such changes on each host.	none
ISO 12 - Successful Administrative Logins by System	This report displays all successful administrative logins, by system. The chart displays a summary of the number of all administrative logins by product.	<p>The Dest IP field drill downs to the "ISO 12 - Successful Administrative Logins per System - Summary" on the next page report.</p> <p>The Count field drill downs to the "ISO 12 - Successful Administrative Logins per System - Detail" below report.</p> <p>This report drills down to itself.</p>

ISO 12 - Operations security, continued

Report	Description	Drill Down
ISO 12 - Successful Administrative Logins by User	This report displays all administrative users that successfully logged into systems, the number of successful logins and the number of distinct systems that were logged into.	<p>The Source or Dest User field drill downs to the "ISO 12 - Successful Administrative Logins per User - Summary" on the next page report.</p> <p>The Number of Logins field drill downs to the "ISO 12 - Successful Administrative Logins per User - Detail" on the next page report.</p> <p>This report drills down to itself.</p>
ISO 12 - Successful Administrative Logins per System - Detail	This report displays all the events where administrators successfully logged into a particular system.	none
ISO 12 - Successful Administrative Logins per System - Summary	This report displays all the administrative users that successfully logged into each system and the number of such logins.	<p>The User Name field drill downs to the "ISO 12 - Successful Administrative Logins per User - Summary" below report.</p> <p>The Count field drill downs to the "ISO 12 - Successful Administrative Logins per System - Detail" on the previous page report.</p> <p>This report drills down to itself.</p>

ISO 12 - Operations security, continued

Report	Description	Drill Down
ISO 12 - Successful Administrative Logins per User - Detail	This report displays all successful logins for the selected administrative user.	<p>The Dest IP field drill downs to the "ISO 12 - Successful Administrative Logins per System - Summary" above report.</p> <p>This report drills down to itself.</p>
ISO 12 - Successful Administrative Logins per User - Summary	This report displays all the systems that the selected administrative users successfully logged into, and the number of such successful logins.	<p>The Dest IP field drill downs to the "ISO 12 - Successful Administrative Logins per System - Summary" above report.</p> <p>The Count field drill downs to the "ISO 12 - Successful Administrative Logins per User - Detail" above report.</p> <p>This report drills down to itself.</p>
ISO 12 - Successful File Deletion	This report shows information from events indicating successful attempts to delete files.	none
ISO 12 - Successful User Logins by System	This report displays a count of all successful non-administrative logins for each system.	<p>The Dest IP field drill downs to the "ISO 12 - Successful User Logins per System - Summary" on the next page report.</p> <p>The Count field drill downs to the "ISO 12 - Successful User Logins per System - Detail" below report.</p> <p>This report drills down to itself.</p>

ISO 12 - Operations security, continued

Report	Description	Drill Down
ISO 12 - Successful User Logins by User Name	This report displays all non-administrative users that successfully logged into systems, the number of successful logins and the number of distinct systems that were logged into.	<p>The Source or Dest User field drill downs to the "ISO 12 - Successful User Logins per User Name - Summary" on the next page report.</p> <p>The Number of Logins field drill downs to the "ISO 12 - Successful User Logins per User Name - Detail" on the next page report.</p> <p>This report drills down to itself.</p>
ISO 12 - Successful User Logins per System - Detail	This report displays all the events where non-administrators successfully logged in into a particular system.	none
ISO 12 - Successful User Logins per System - Summary	This report displays all the non-administrative users that successfully logged in into each system and the number of such successful logins.	<p>The User Name field drill downs to the "ISO 12 - Successful User Logins per User Name - Summary" below report.</p> <p>The Count field drill downs to the "ISO 12 - Successful User Logins per System - Detail" on the previous page report.</p> <p>This report drills down to itself.</p>
ISO 12 - Successful User Logins per User Name - Detail	This report displays all successful logins for the selected non-administrative user.	<p>The Dest IP field drill downs to the "ISO 12 - Successful User Logins per System - Summary" above report.</p> <p>This report drills down to itself.</p>

ISO 12 - Operations security, continued

Report	Description	Drill Down
ISO 12 - Successful User Logins per User Name - Summary	This report displays all the systems that the selected non-administrative users successfully logged into, and the number of such successful logins.	<p>The Dest IP field drill downs to the "ISO 12 - Successful User Logins per System - Summary" above report.</p> <p>The Count field drill downs to the "ISO 12 - Successful User Logins per User Name - Detail" above report.</p> <p>This report drills down to itself.</p>
ISO 12 - 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.	none
ISO 12 - 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.	none
ISO 12 - Systems Accessed as Root or Administrator	This report shows all systems that users have tried to access directly as root or administrator.	none
ISO 12 - Top 20 Policy Breach Events	This report summarizes the top 20 policy breach events.	none
ISO 12 - Trojan Code Activity	This report shows all trojan activity.	none

ISO 12 - Operations security, continued

Report	Description	Drill Down
ISO 12 - User Actions - All Events	This is a detailed report of all user actions. The report is ordered first by source user name and then by destination user name. Only events where neither the source nor the destination users are administrative users will be shown. Events in which both source and destination users are null will not appear on this report. Run this report with caution, as it can generate enormous amounts of data.	<p>The Source User field drill downs to the "ISO 12 - User Actions by User Name and Product" on page 55 report.</p> <p>The Dest User field drill downs to the "ISO 12 - User Actions by User Name and Product" on page 55 report.</p> <p>The Name field drill downs to the "ISO 12 - User Actions by Event Name" on the next page report.</p> <p>The Event ID field drill downs to the "ISO 12 - User Actions by Event Name" on the next page report.</p> <p>This report drills down to itself.</p>
ISO 12 - User Actions by Event Name	For each event name this report shows a count of events in which a non-administrative user appears either in the source user name or destination user name fields. This reported is ordered alphabetically first by the source user name and then by the destination user name. If either the source or destination user name field is populated with an administrator user name the event will not show up on this report. Run this report with caution as it can generate enormous amounts of data.	<p>The Source User field drill downs to the "ISO 12 - User Actions by User Name and Product" on the next page report.</p> <p>The Dest User field drill downs to the "ISO 12 - User Actions by User Name and Product" on the next page report.</p> <p>The Num of Events field drill downs to the "ISO 12 - User Actions - All Events" on the previous page report.</p> <p>This report drills down to itself.</p>

ISO 12 - Operations security, continued

Report	Description	Drill Down
ISO 12 - User Actions by Product	This report shows a count of events triggered by non-administrators for each product and the number of unique source user name and destination user name pairs for each product. It is recommended to run this report first when displaying user events. The report is ordered alphabetically by the product name.	<p>The Total Events field drill downs to the "ISO 12 - User Actions - All Events" on the previous page report.</p> <p>The Num of Source-Destination User Pairs field drill downs to the "ISO 12 - User Actions by User Name and Product" on the next page report.</p> <p>This report drills down to itself.</p>
ISO 12 - User Actions by User Name and Product	This report shows a count of all actions performed by a non-administrator for each Product. The report is ordered alphabetically by the product name. Run this report with caution, as it can generate enormous amounts of data.	<p>The Source User field drill downs to the "ISO 12 - User Actions by User Name and Product" above report.</p> <p>The Dest User field drill downs to the "ISO 12 - User Actions by User Name and Product" above report.</p> <p>The Total Events field drill downs to the "ISO 12 - User Actions - All Events" on page 53 report.</p> <p>The Unique Events field drill downs to the "ISO 12 - User Actions by Event Name" on the previous page report.</p> <p>This report drills down to itself.</p>
ISO 12 - User Logins and Logouts	This report displays the time, name, destination, and user information from user login and logout events.	none

ISO 12 - Operations security, continued

Report	Description	Drill Down
ISO 12 - Viruses per Host	This report shows the number of viruses that infected each host.	<p>The Dest Address field drill downs to the "ISO 12 - Virus Report - Detail" on the next page report.</p> <p>The Dest Host field drill downs to the "ISO 12 - Virus Report - Detail" on the next page report.</p> <p>The Count field drill downs to the "ISO 12 - Virus Report - Detail" on the next page report.</p>
ISO 12 - Virus Report - Detail	This report shows all virus events, the hosts on which they were detected and the time they occurred.	none
ISO 12 - Virus Summary by Virus Name	This report shows all viruses that were detected and the number of hosts each virus was detected on. The table is ordered by priority and then by number of occurrences, while the chart shows the number of occurrences for each virus.	The Total Events field drill downs to the "ISO 12 - Virus Report - Detail" above report.
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.	none
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.	none

ISO 13 - Communications security

The ISO 13 - Communications security category is located under the following path.

ISO 27002\ISO 13 - Communications security

The ISO 13 - Communications security category reports are listed in the following table.

ISO 13 - Communications security

Report	Description	Drill Down
ISO 13 - 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.	none
ISO 13 - Email Receivers by Amount - Top 100	This report displays the top e-mail recipients based on the number of e-mails received.	none
ISO 13 - 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.	none
ISO 13 - 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.	none
ISO 13 - 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.	none
ISO 13 - 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.	none
ISO 13 - High Risk Events	This report displays source and destination information from all events with an agent severity of High or Very-High.	none
ISO 13 - High Risk Events by Zone	This report displays the number of high or very-high severity events sorted by zone.	none
ISO 13 - Information Interception Events	This report displays the date, source, and destination information from information-interception events.	none
ISO 13 - 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.	none
ISO 13 - 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.	none

ISO 13 - Communications security, continued

Report	Description	Drill Down
ISO 13 - 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.	none
ISO 13 - Largest Emails - Top 20	This report displays the 20 largest e-mails sent. The chart displays the size of the largest email sent per user.	none
ISO 13 - 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.	none
ISO 13 - 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.	none
ISO 13 - 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.	none
ISO 13 - 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.	none
ISO 13 - 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.	none
ISO 13 - 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.	none
ISO 13 - Top 10 High Risk Events	This report displays a summary of the top 10 events with an agent severity of High or Very-High.	none
ISO 13 - Traffic Between Zones - Protocol	This report displays communication protocols that are passed between different zones.	none
ISO 13 - Traffic - Inbound on Disallowed Ports	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.	none

ISO 14 - System acquisition development and maintenance

The ISO 14 - System acquisition development and maintenance category is located under the following path.

ISO 27002\ISO 14 - System acquisition development and maintenance

The ISO 14 - System acquisition development and maintenance category reports are listed in the following table.

ISO 14 - System acquisition development and maintenance

Report	Description	Drill Down
ISO 14 - 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.	none

ISO 16 - Information security incident management

The ISO 16 - Information security incident management category is located under the following path.

ISO 27002\ISO 16 - Information security incident management

The ISO 16 - Information security incident management category reports are listed in the following table.

ISO 16 - Information security incident management

Report	Description	Drill Down
ISO 16 - 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 destination ip address.	none
ISO 16 - 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 source ip address.	none
ISO 16 - Attack Events - Top 20	This report displays the 20 most common attack event names in the report\'s time frame.	none

ISO 16 - Information security incident management, continued

Report	Description	Drill Down
ISO 16 - 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.	none
ISO 16 - Attacks - Hourly Count	This report displays the number of attacks that targeted internal IP addresses each hour.	none
ISO 16 - 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.	none
ISO 16 - Attacks Targeting Internal Assets	This report displays all events with category significance of '\Recon\', '\Compromise\', '\Hostile\', or '\Suspicious\' that target an internal IP address.	none
ISO 16 - 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.	none
ISO 16 - Denial of Service Sources	This report shows all the sources involved in denial of service activity.	none
ISO 16 - File Integrity Changes	This report displays events indicating changes to monitored files.	none
ISO 16 - 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 on each host.	none
ISO 16 - Internal Reconnaissance - Top 20 Events	This report displays the top events identified as internal reconnaissance events, such as port scanning activity.	none
ISO 16 - 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.	none
ISO 16 - 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.	none

ISO 17 - Information security aspects of business continuity management

The ISO 17 - Information security aspects of business continuity management category is located under the following path.

ISO 27002\ISO 17 - Information security aspects of business continuity management

The ISO 17 - Information security aspects of business continuity management category reports are listed in the following table.

ISO 17 - Information security aspects of business continuity management

Report	Description	Drill Down
ISO 17 - 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.	none

ISO 18 - Compliance

The ISO 18 - Compliance category is located under the following path.

ISO 27002\ISO 18 - Compliance

The ISO 18 - Compliance category reports are listed in the following table.

ISO 18 - Compliance

Report	Description	Drill Down
ISO 18 - 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.	none
ISO 18 - 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.	none

NIST 800-53

The NIST 800-53 category reports are listed in the following table.

NIST 800-53

Report	Description	Drill Down
NIST AC - Account Activity by User	This report displays all the events with the specified destination user name. The destination user name is defined at runtime.	none
NIST AC - 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.	none
NIST AC - 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.	none
NIST AC - Administrative Actions - All Events	This report shows all actions taken by administrators sorted by event time.	none
NIST AC - Administrative Actions by Event Name	For each event name this reports shows a count of events in which an administrative user appeared either in the source user name or destination user name fields.	The Count field drill downs to the " NIST AC - Administrative Actions - All Events " above report.
NIST AC - Administrative Actions by Product	This report shows a count of all actions performed by an administrator for each Product. The report is ordered alphabetically by the product name.	<p>The Count field drill downs to the "NIST AC - Administrative Actions - All Events" above report.</p> <p>The Distinct Events field drill downs to the "NIST AC - Administrative Actions by Event Name" above report.</p>

NIST 800-53, continued

Report	Description	Drill Down
NIST AC - Administrative Actions by User	This reports shows a count of events in which an administrative user appeared either in the source username or destination username fields.	<p>The Number of Events field drill downs to the "NIST AC - Administrative Actions - All Events" above report.</p> <p>The Number Of Devices field drill downs to the "NIST AC - Administrative Actions by Product" above report.</p>
NIST AC - Administrative Logins and Logouts	This report displays administrative logins and logouts. The chart displays the number of such events per system.	none
NIST AC - Authorization Changes	This report shows authorization changes made on systems and the number of events per host name.	none
NIST AC - Database Access - Failed	This report displays a count of database access attempt failures per hour.	none
NIST AC - 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'.	none
NIST AC - 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.	none
NIST AC - Email Receivers by Amount - Top 100	This report displays the top e-mail recipients based on the number of e-mails received.	none
NIST AC - 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.	none

NIST 800-53, continued

Report	Description	Drill Down
NIST AC - 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.	none
NIST AC - 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.	none
NIST AC - Failed Administrative Logins by System	This report displays all failed administrative logins, by system.	<p>The Dest IP field drill downs to the "NIST AC - Failed Administrative Logins per System - Summary" on the next page report.</p> <p>The Count field drill downs to the "NIST AC - Failed Administrative Logins per System - Detail" below report.</p> <p>This report drills down to itself.</p>
NIST AC - Failed Administrative Logins by User	This report displays all administrative users that failed to log into systems, the number of failed logins and the number of distinct systems that were attempted to log into.	<p>The Source or Dest User field drill downs to the "NIST AC - Failed Administrative Logins per User - Summary" on the next page report.</p> <p>The Number of Logins field drill downs to the "NIST AC - Failed Administrative Logins per User - Detail" on the next page report.</p> <p>This report drills down to itself.</p>

NIST 800-53, continued

Report	Description	Drill Down
NIST AC - Failed Administrative Logins per System - Detail	This report displays all the failed administrative logins into a particular system. The chart shows a count of failed administrative logins per product.	none
NIST AC - Failed Administrative Logins per System - Summary	This report displays all the administrative users that failed to login into each system and the number of such failed logins.	<p>The User Name field drill downs to the "NIST AC - Failed Administrative Logins per User - Summary" below report.</p> <p>The Count field drill downs to the "NIST AC - Failed Administrative Logins per System - Detail" on the previous page report.</p> <p>This report drills down to itself.</p>
NIST AC - Failed Administrative Logins per User - Detail	This report displays all failed logins for the selected administrative user.	<p>The Dest IP field drill downs to the "NIST AC - Failed Administrative Logins per System - Summary" above report.</p> <p>This report drills down to itself.</p>
NIST AC - Failed Administrative Logins per User - Summary	This report displays all the systems that the selected administrative users failed to login into, and the number of such failed logins.	<p>The Dest IP field drill downs to the "NIST AC - Failed Administrative Logins per System - Summary" above report.</p> <p>The Count field drill downs to the "NIST AC - Failed Administrative Logins per User - Detail" above report.</p> <p>This report drills down to itself.</p>

NIST 800-53, continued

Report	Description	Drill Down
NIST AC - Failed File Access	This report shows information from events indicating failed attempts to access files.	none
NIST AC - Failed File Deletions	This report shows information from events indicating failed attempts to delete files.	none
NIST AC - Failed User Logins by System	This report displays all failed non-administrative logins by system.	<p>The Dest IP field drill downs to the "NIST AC - Failed User Logins per System - Summary" on the next page report.</p> <p>The Count field drill downs to the "NIST AC - Failed User Logins per System - Detail" below report.</p> <p>This report drills down to itself.</p>
NIST AC - Failed User Logins by User Name	This report displays all non-administrative users that failed to log into systems, the number of failed logins and the number of distinct systems that were attempted to log into.	<p>The Source or Dest User field drill downs to the "NIST AC - Failed User Logins per User Name - Summary" on the next page report.</p> <p>The Number of Logins field drill downs to the "NIST AC - Failed User Logins per User Name - Detail" on the next page report.</p> <p>This report drills down to itself.</p>
NIST PS - Failed User Logins from Third-Party Systems	This report displays all failed user logins from third-party systems.	none
NIST AC - Failed User Logins per System - Detail	This report displays all the failed non-administrative logins into a particular system.	none

NIST 800-53, continued

Report	Description	Drill Down
NIST AC - Failed User Logins per System - Summary	This report displays all the non-administrative users that failed to login into each system and the number of such failed logins.	<p>The User Name field drill downs to the "NIST AC - Failed User Logins per User Name - Summary" below report.</p> <p>The Count field drill downs to the "NIST AC - Failed User Logins per System - Detail" on the previous page report.</p> <p>This report drills down to itself.</p>
NIST AC - Failed User Logins per User Name - Detail	This report displays all failed logins for the selected non-administrative user.	<p>The Dest IP field drill downs to the "NIST AC - Failed User Logins per System - Summary" above report.</p> <p>This report drills down to itself.</p>
NIST AC - Failed User Logins per User Name - Summary	This report displays all the systems that the selected non-administrative user failed to login into, and the number of such failed logins.	<p>The Dest IP field drill downs to the "NIST AC - Failed User Logins per System - Summary" above report.</p> <p>The Count field drill downs to the "NIST AC - Failed User Logins per User Name - Detail" above report.</p> <p>This report drills down to itself.</p>
NIST PS - Failed User Logins to Third-Party Systems	This report displays all failed user logins to third-party systems.	none
NIST AC - File Activity on Third-Party Systems	This report displays the host, file, behavior, and outcome of monitored file activity on third-party systems.	none

NIST 800-53, continued

Report	Description	Drill Down
NIST AC - File Creations on Third-Party Systems	This report displays the host, file, behavior, and outcome of monitored file creations on third-party systems.	none
NIST AC - File Deletions on Third-Party Systems	This report displays the host, file, behavior, and outcome of monitored file deletions on third-party systems.	none
NIST AC - File Modifications on Third-Party Systems	This report displays the host, file, behavior, and outcome of monitored file modifications on third-party systems.	none
NIST AC - Internal Reconnaissance - Top 20 Events	This report displays the top events identified as internal reconnaissance events, such as port scanning activity.	none
NIST AC - 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.	none
NIST AC - 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.	none
NIST AC - 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.	none
NIST AC - 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.	none
NIST AC - Largest Emails - Top 20	This report displays the 20 largest e-mails sent. The chart displays the size of the largest email sent per user.	none
NIST AC - 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.	none

NIST 800-53, continued

Report	Description	Drill Down
NIST AC - 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.	none
NIST AC - 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.	none
NIST AC - 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.	none
NIST AC - 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.	none
NIST AC - Privileged Account Changes	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.	none
NIST AC - 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.	none
NIST AC - 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.	none
NIST AC - 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.	none

NIST 800-53, continued

Report	Description	Drill Down
NIST AC - Successful Administrative Logins by System	This report displays all successful administrative logins by systems. The chart displays a count of all administrative logins per product.	<p>The Dest IP field drill downs to the "NIST AC - Successful Administrative Logins per System - Summary" on the next page report.</p> <p>The Count field drill downs to the "NIST AC - Successful Administrative Logins per System - Detail" below report.</p> <p>This report drills down to itself.</p>
NIST AC - Successful Administrative Logins by User	This report displays all administrative users that successfully logged into systems, the number of successful logins and the number of distinct systems that were logged into.	<p>The Source or Dest User field drill downs to the "NIST AC - Successful Administrative Logins per User - Summary" on the next page report.</p> <p>The Number of Logins field drill downs to the "NIST AC - Successful Administrative Logins per User - Detail" on the next page report.</p> <p>This report drills down to itself.</p>
NIST AC - Successful Administrative Logins per System - Detail	This report displays all the events where administrators successfully logged in into a particular system.	none

NIST 800-53, continued

Report	Description	Drill Down
NIST AC - Successful Administrative Logins per System - Summary	This report displays all the administrative users that successfully logged into each system and the number of such successful logins.	<p>The User Name field drill downs to the "NIST AC - Successful Administrative Logins per User - Summary" below report.</p> <p>The Count field drill downs to the "NIST AC - Successful Administrative Logins per System - Detail" on the previous page report.</p> <p>This report drills down to itself.</p>
NIST AC - Successful Administrative Logins per User - Detail	This report displays all successful logins for the selected administrative user.	<p>The Dest IP field drill downs to the "NIST AC - Successful Administrative Logins per System - Summary" above report.</p> <p>This report drills down to itself.</p>
NIST AC - Successful Administrative Logins per User - Summary	This report displays all the systems that the selected administrative user successfully logged into, and the number of such successful logins.	<p>The Dest IP field drill downs to the "NIST AC - Successful Administrative Logins per System - Summary" above report.</p> <p>The Count field drill downs to the "NIST AC - Successful Administrative Logins per User - Detail" above report.</p> <p>This report drills down to itself.</p>
NIST AC - Successful Brute Force Logins	This report displays the time, user, and host information from successful brute-force logins.	none

NIST 800-53, continued

Report	Description	Drill Down
NIST AC - Successful File Deletion	This report shows information from events indicating successful attempts to delete files.	none
NIST AC - Successful User Logins by System	This report displays all successful non-administrative logins, by systems.	<p>The Dest IP field drill downs to the "NIST AC - Successful User Logins per System - Summary" on the next page report.</p> <p>The Count field drill downs to the "NIST AC - Successful User Logins per System - Detail" below report.</p> <p>This report drills down to itself.</p>
NIST AC - Successful User Logins by User Name	This report displays all non-administrative users that successfully logged into systems, the number of successful logins and the number of distinct systems that were logged into.	<p>The Source or Dest User field drill downs to the "NIST AC - Successful User Logins per User Name - Summary" on the next page report.</p> <p>The Number of Logins field drill downs to the "NIST AC - Successful User Logins per User Name - Detail" on the next page report.</p> <p>This report drills down to itself.</p>
NIST AC - Successful User Logins per System - Detail	This report displays all the events where non-administrators successfully logged in into a particular system.	none

NIST 800-53, continued

Report	Description	Drill Down
NIST AC - Successful User Logins per System - Summary	This report displays all the non-administrative users that successfully logged in into each system and the number of such successful logins.	<p>The User Name field drill downs to the "NIST AC - Successful User Logins per User Name - Summary" below report.</p> <p>The Count field drill downs to the "NIST AC - Successful User Logins per System - Detail" on the previous page report.</p> <p>This report drills down to itself.</p>
NIST AC - Successful User Logins per User Name - Detail	This report displays all successful logins for the selected non-administrative user.	<p>The Dest IP field drill downs to the "NIST AC - Successful User Logins per System - Summary" above report.</p> <p>This report drills down to itself.</p>
NIST AC - Successful User Logins per User Name - Summary	This report displays all the systems that the selected non-administrative users successfully logged into, and the number of such successful logins.	<p>The Dest IP field drill downs to the "NIST AC - Successful User Logins per System - Summary" above report.</p> <p>The Count field drill downs to the "NIST AC - Successful User Logins per User Name - Detail" above report.</p> <p>This report drills down to itself.</p>
NIST AC - 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.	none

NIST 800-53, continued

Report	Description	Drill Down
NIST AC - 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.	none
NIST AC - 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.	none
NIST AC - Third-Party Systems Accessed	This report displays all events indicating third-party systems were queried or accessed.	none
NIST AC - Traffic Between Zones - Protocol	This report displays communication protocols that are passed between different zones.	none
NIST AC - Traffic from External to Internal Protected Domain	This report shows information from all events indicating traffic from external to internal systems.	none
NIST AC - Traffic from Internal to External Protected Domain	This report shows information from all events indicating traffic from internal to external systems.	none
NIST AC - 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.	none
NIST AC - 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.	none
NIST AC - User Account Deletion	This report shows events indicating user accounts have been removed from a system.	none

NIST 800-53, continued

Report	Description	Drill Down
NIST AC - User Actions - All Events	This is a detailed report of all user actions. The report is ordered first by source user name and then by destination user name. Only events where neither the source nor the destination users are administrative users will be shown. Events in which both source and destination users are null will not appear on this report. Run this report with caution, as it can generate enormous amounts of data.	<p>The Source User field drill downs to the "NIST AC - User Actions by User Name and Product" on page 77 report.</p> <p>The Dest User field drill downs to the "NIST AC - User Actions by User Name and Product" on page 77 report.</p> <p>The Name field drill downs to the "NIST AC - User Actions by Event Name" on the next page report.</p> <p>The Event ID field drill downs to the "NIST AC - User Actions by Event Name" on the next page report.</p> <p>This report drills down to itself.</p>

NIST 800-53, continued

Report	Description	Drill Down
NIST AC - User Actions by Event Name	For each event name this report shows a count of events in which a non-administrative user appears either in the source user name or destination user name fields. This reported is ordered alphabetically first by the source user name and then by the destination user name. If either the source or destination user name field is populated with an administrator user name the event will not show up on this report. Run this report with caution as it can generate enormous amounts of data.	<p>The Source User field drill downs to the "NIST AC - User Actions by User Name and Product" on the next page report.</p> <p>The Dest User field drill downs to the "NIST AC - User Actions by User Name and Product" on the next page report.</p> <p>The Num of Events field drill downs to the "NIST AC - User Actions - All Events" on the previous page report.</p> <p>This report drills down to itself.</p>
NIST AC - User Actions by Product	This report shows a count of events triggered by non-administrators for each product and the number of unique source user name and destination user name pairs for each product. It is recommended to run this report first when displaying user events. The report is ordered alphabetically by the product name.	<p>The Total Events field drill downs to the "NIST AC - User Actions - All Events" on the previous page report.</p> <p>The Num of Source-Destination User Pairs field drill downs to the "NIST AC - User Actions by User Name and Product" on the next page report.</p> <p>This report drills down to itself.</p>

NIST 800-53, continued

Report	Description	Drill Down
NIST AC - User Actions by User Name and Product	This report shows a count of all actions performed by a non-administrator for each Product. The report is ordered alphabetically by the product name. Run this report with caution, as it can generate enormous amounts of data.	<p>The Source User field drill downs to the "NIST AC - User Actions by User Name and Product" above report.</p> <p>The Dest User field drill downs to the "NIST AC - User Actions by User Name and Product" above report.</p> <p>The Total Events field drill downs to the "NIST AC - User Actions - All Events" on page 75 report.</p> <p>The Unique Events field drill downs to the "NIST AC - User Actions by Event Name" on the previous page report.</p> <p>This report drills down to itself.</p>
NIST AC - User Logins and Logouts	This report displays the time, name, destination, and user information from user login and logout events.	none
NIST AC - 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.	none
NIST AC - 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.	none
NIST AC - VPN Access Summary	This report displays a summary of VPN access by users.	none
NIST AU - Audit Log Cleared	This report displays the date, time, system, and user information from all events indicating an audit log has been cleared.	none

NIST 800-53, continued

Report	Description	Drill Down
NIST AU - 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.	none
NIST CM - Application Configuration Modifications	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.	none
NIST CM - Changes to Development Network Machines	This report displays all changes to machines in the development network.	none
NIST CM - 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.	none
NIST CM - Changes to Third-Party Resources	This report displays events indicating a change was made to a third-party application or resource.	none
NIST CM - 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.	none
NIST CM - 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.	none
NIST CM - Firewall Configuration Changes	This report displays all events indicating a configuration file on a firewall has been changed.	none
NIST CM - 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.	none
NIST CM - Network Device Configuration Changes	This report displays events indicating configuration file changes on network equipment such as routers and switches.	none
NIST CM - 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.	none

NIST 800-53, continued

Report	Description	Drill Down
NIST CM - New Hosts	This report displays all new services detected on the network by traffic analysis systems.	none
NIST CM - New Services	This report displays all new services detected on the network by traffic analysis systems.	none
NIST CM - Operating System Configuration Changes	This report details operating system configuration changes.	none
NIST Executive Report	This report is made up of 4 charts:1. Top 10 Alerts Fired2. Top 10 Failed Logins3. 10 Most Attacked Hosts4. 10 Hosts with Most Virus Events	none
NIST IA - Database Access - All	This report displays a count of database access attempts per hour.	none
NIST IA - 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.	none
NIST IA - Systems Accessed as Root or Administrator	This report shows all systems that users have tried to access directly as root or administrator.	none
NIST IR - 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 destination ip address.	none
NIST IR - 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 source ip address.	none
NIST IR - Attack Events - Top 20	This report displays the 20 most common attack event names in the report\'s time frame.	none
NIST IR - 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.	none
NIST IR - Attacks - Hourly Count	This report displays the number of attacks that targeted internal IP addresses each hour.	none

NIST 800-53, continued

Report	Description	Drill Down
NIST IR - 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.	none
NIST IR - Attacks Targeting Internal Assets	This report displays all events with category significance of 'Recon', 'Compromise', 'Hostile', or 'Suspicious' that target an internal IP address.	none
NIST IR - Compromised Third-Party Systems	This report displays all successful compromise attempts targeting third-party systems.	none
NIST IR - 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.	none
NIST IR - 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.	none
NIST IR - High Risk Events	This report displays source and destination information from all events with an agent severity of High or Very-High.	none
NIST IR - High Risk Events by Zone	This report displays the number of high or very-high severity events sorted by zone.	none
NIST IR - Machines Conducting Policy Breaches	This report displays source IP, hostname, and event information from events with a Category Technique of /Policy/Breach.	none
NIST IR - Policy Violations	This report displays all policy breaches such as IM use or the downloading of sexual content. The chart displays the number of events per source ip address.	none
NIST IR - Policy Violations from Third-Party Systems	This report displays the events indicating policy violations from third-party systems.	none
NIST IR - Top 10 High Risk Events	This report displays a summary of the top 10 events with an agent severity of High or Very-High.	none

NIST 800-53, continued

Report	Description	Drill Down
NIST IR - Top 20 Policy Breach Events	This report summarizes the top 20 policy breach events.	none
NIST IR - Traffic - Inbound on Disallowed Ports	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.	none
NIST MA - 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.	none
NIST MA - 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.	none
NIST PE - Failed Building Access Attempts	This report displays all failed building access attempts including user name, id, and badge reader number.	none
NIST PE - 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.	none
NIST PS - 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.	none
NIST PS - 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.	none
NIST PS - Attacks from Third-Party Systems	This report displays the event, time, source, and destination of attacks originating from third-party systems.	none
NIST PS - Attacks on Third-Party Systems	This report displays source and destination information from attacks against third-party systems.	none

NIST 800-53, continued

Report	Description	Drill Down
NIST PS - Failed Admin Logins from Third-Party Systems	This report displays all failed administrative logins from third-party systems.	none
NIST PS - Failed Admin Logins to Third-Party Systems	This report displays all failed administrative logins to third-party systems.	none
NIST PS - Services Accessed by Third-Party Systems	This report displays the port, service, and destination information of services accessed by third-party systems.	none
NIST RA - 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.	none
NIST RA - Vulnerability Scanner Results	This report displays vulnerabilities as reported by vulnerability scanners. The chart displays the number of different kinds of vulnerabilities found.	none
NIST SA - 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.	none
NIST SA - 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.	none
NIST SA - 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.	none
NIST SC - 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.	none
NIST SC - Blocked Firewall Traffic	This report displays events generated by devices that have blocked traffic. The chart displays the number of blocking events.	none
NIST SC - 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.	none

NIST 800-53, continued

Report	Description	Drill Down
NIST SC - Denial of Service Sources	This report shows all the sources involved in denial of service activity.	none
NIST SC - 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.	none
NIST SC - Information Interception Events	This report displays the date, source, and destination information from information-interception events.	none
NIST SC - 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.	none
NIST SC - 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.	none
NIST SC - 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.	none
NIST SC - 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.	none
NIST SI - Failed Anti-Virus Updates	This report displays the date, host, and product information from failed anti-virus update events.	none
NIST SI - Fault Logs	This report displays all events indicating a system fault has occurred.	none
NIST SI - File Integrity Changes	This report displays events indicating changes to monitored files.	none
NIST SI - 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 on each host.	none
NIST SI - 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.	none
NIST SI - Malicious Code Sources	This report displays the count of malicious code events from particular hosts.	none

NIST 800-53, continued

Report	Description	Drill Down
NIST SI - Resource Exhaustion	This report displays a count of events indicating resource exhaustion on particular hosts.	none
NIST SI - 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 is determined by the configuration of the productionNetwork parameter, and can be modified by the user at runtime. The chart displays the number of such changes on each host.	none
NIST SI - Trojan Code Activity	This report shows all trojan activity.	none
NIST SI - Viruses per Host	This report shows the number of viruses that infected each host.	<p>The Dest Address field drill downs to the "NIST SI - Virus Report - Detail" below report.</p> <p>The Dest Host field drill downs to the "NIST SI - Virus Report - Detail" below report.</p> <p>The Count field drill downs to the "NIST SI - Virus Report - Detail" below report.</p>
NIST SI - Virus Report - Detail	This report shows all virus events, the hosts on which they were detected and the time they occurred.	none
NIST SI - Virus Summary by Virus Name	This report shows all viruses that were detected and the number of hosts each virus was detected on. The table is ordered by priority and then by number of occurrences, while the chart shows the number of occurrences for each virus.	The Total Events field drill downs to the "NIST SI - Virus Report - Detail" above report.

Chapter 6: Logger CIP for IT Gov Dashboards

This section describes the Logger IT Governance dashboards.

IT Governance - Account Management Activity

Dashboard Panel	Description
Daily User Account Creations (Past 7 Days)	<p>This panel shows the daily user account creation events for the past 7 days.</p> <p>ISO 27002:2013 control ID: 9.2.1</p> <p>Saved Search: IT Governance - Accounts Creation</p> <p>Type: Area</p>
Daily User Account Deletions (Past 7 Days)	<p>This panel shows the daily user account deletion events for the past 7 days.</p> <p>ISO 27002:2013 control ID: 9.2.1</p> <p>Saved Search: IT Governance - Account Deletion</p> <p>Type: Area</p>

Dashboard Panel	Description
Top Account Lockout Events by User Name (Past Day)	<p>This panel shows the top account lockout events by user name for the past day.</p> <p>Supported Operating Systems: Microsoft Windows 2012, Microsoft Windows 7, Microsoft Windows 8, Microsoft Windows 2003, Microsoft Windows 2000, Microsoft Windows XP, Unix Syslog</p> <p>ISO 27002:2013 control ID: 9.4.2</p> <p>Saved Search: IT Governance - Account Lockouts by User</p> <p>Type: Column</p>
Top Privileged Account Change Events by User Name (Past Day)	<p>This panel shows the top privileged account change events by user name for the past day.</p> <p>Default Privileged Accounts: Admin, Administrator, root.</p> <p>You can customize the saved search to include or exclude privileged accounts from your environment by editing the following section of the saved search:</p> <pre>destinationUserName IN ["Admin", "Administrator", "root"]</pre> <p>ISO 27002:2013 control ID: 9.2.5</p> <p>Saved Search: IT Governance - Top Privileged Account Changes by User Name</p> <p>Type: Column</p>

IT Governance - Firewall Activity

Dashboard Panel	Description
Top Denied Connections by IP Address (Past Day)	<p>This panel shows the top denied connection events by IP address for the past day.</p> <p>ISO 27002:2013 control ID: 13.1.1</p> <p>Saved Search: IT Governance - Denied Connections by Address</p> <p>Type: Column</p>
Top Blocked URLs by Source Address (Past 7 Days)	<p>This panel shows top blocked URLs events by source address for the past day.</p> <p>ISO 27002:2013 control ID: 13.1.1</p> <p>Saved Search: IT Governance – Blocked URLs by Source Address</p> <p>Type: Column</p>

Dashboard Panel	Description
Firewall Events by Application Protocol (Past Day)	<p>This panel shows firewall events by application protocol received for the past day.</p> <p>ISO 27002:2013 control ID: 13.1.1</p> <p>Saved Search: IT Governance - Firewall Events by Application Protocol</p> <p>Type: Pie</p>
Firewall Events by Transport Protocol (Past Day)	<p>This panel shows the firewall events by transport protocol received for the past day.</p> <p>ISO 27002:2013 control ID: 13.1.1</p> <p>Saved Search: IT Governance - Firewall Events by Transport Protocol</p> <p>Type: Pie</p>

IT Governance - Configuration Changes

Dashboard Panel	Description
Top Firewall Configuration Change Events	<p>This panel shows top firewall configuration changes events for the past hour.</p> <p>ISO 27002:2013 control ID: 12.1.2</p> <p>Saved Search: IT Governance – Firewall Configuration Changes</p> <p>Type: Column</p>
Top Network Equipment Configuration Change Events	<p>This panel shows top network equipment configuration changes events for the past hour.</p> <p>ISO 27002:2013 control ID: 12.1.2</p> <p>Saved Search: IT Governance – Network Equipment Configuration Changes</p> <p>Type: Column</p>
Top VPN Configuration Change Events	<p>This panel shows the top VPN configuration change events for the past hour.</p> <p>ISO 27002:2013 control ID: 12.1.2</p> <p>Saved Search: IT Governance – VPN Configuration Changes</p> <p>Type: Column</p>
Top Application Configuration Change Events	<p>This panel shows the top application configuration changes events for the past hour.</p> <p>ISO 27002:2013 control ID: 12.1.2</p> <p>Saved Search: IT Governance - Application Configuration Changes</p> <p>Type: Column</p>

IT Governance - Administrative Activity

Dashboard Component	Description
Excessive Failed Administrative Logins (Past Day)	<p>This panel shows excessive failed administrative logins events for the past day.</p> <p>ISO 27002:2013 control ID: 12.4.3</p> <p>Saved Search: IT Governance – Excessive Failed Administrative Logins</p> <p>Type: Column</p>
Excessive Failed Administrative Actions (Past Day)	<p>This panel shows top excessive failed administrative actions events for the past day.</p> <p>ISO 27002:2013 control ID: 12.4.3</p> <p>Saved Search: IT Governance – Excessive Failed Administrative Actions</p> <p>Type: Column</p>
Top Failed Administrative Logins for Destination Address (Past Day)	<p>This panel shows top failed administrative logins by destination Address for the past day.</p> <p>ISO 27002:2013 control ID: 12.4.3</p> <p>Saved Search: IT Governance – Top Failed Administrative Logins per Destination Address</p> <p>Type: Column</p>
Excessive Failed Database Administrative Access (Past Day)	<p>This panel shows the top excessive failed database administrative access events for the past day.</p> <p>ISO 27002:2013 control ID: 12.4.3</p> <p>Saved Search: IT Governance – Excessive Failed Database Administrative Access</p> <p>Type: Column</p>

IT Governance - Malicious Activity

Dashboard Panel	Description
Malicious Malware Activity by the Hour (Past 3 Days)	<p>This panel shows the malicious activity events by the hour for the past 3 days.</p> <p>ISO 27002:2013 control ID: 12.2.1</p> <p>Saved Search: IT Governance – Malicious Malware Activity</p> <p>Type: Line</p>
Worm Infected System Events by the Hour (Past 3 Days)	<p>This panel shows the worm infected systems events by the hour for the past 3 days.</p> <p>ISO 27002:2013 control ID: 12.2.1</p> <p>Saved Search: IT Governance – Worm Infected Systems Events</p> <p>Type: Line</p>
Top Infected Systems Reported by Anti-Virus Software (Past Day)	<p>This panel shows top infected systems reported by anti-virus software for the past day.</p> <p>ISO 27002:2013 control ID: 12.2.1</p> <p>Saved Search: IT Governance – Top Infected Systems Reported by Anti-Virus Software</p> <p>Type: Column</p>
Covert Channel Activity (Past 7 Days)	<p>This panel shows the top covert channel activity events for the past 7 days.</p> <p>ISO 27002:2013 control ID: 12.2.1</p> <p>Saved Search: IT Governance - Covert Channel Activity</p> <p>Type: Column</p>

IT Governance - Physical Security Activity

Dashboard Panel	Description
Top Physical Access Event Reporting Devices (Past Day)	<p>This panel shows the top physical access event reporting devices for the past day.</p> <p>ISO 27002:2013 control ID: 11.1.2</p> <p>Saved Search: IT Governance – Physical Access Event Reporting Devices</p> <p>Type: Column</p>
Top Physical Access Events by Name (Past Day)	<p>This panel shows the top physical access events by name for the past day.</p> <p>ISO 27002:2013 control ID: 11.1.2</p> <p>Saved Search: IT Governance – Physical Access Events</p> <p>Type: Column</p>
Failed Physical Facility Access Attempts at 30 Minute Intervals (Past Day)	<p>This panel shows Failed Physical Facility Access Attempts at 30 minute intervals for the past day.</p> <p>ISO 27002:2013 control ID: 11.1.2</p> <p>Saved Search: IT Governance – Failed Physical Facility Access Attempts</p> <p>Type: Line</p>
Last 5 Failed Physical Facility Access Attempts (Past Day)	<p>This panel shows the last 5 failed physical facility access attempts for the past day.</p> <p>ISO 27002:2013 control ID: 11.1.2</p> <p>Saved Search: IT Governance - Last Failed Physical Facility Access Attempts</p> <p>Type: Table</p>

IT Governance - Vulnerability Management

Dashboard Panel	Description
Top IP Addresses with CVSS Score Vulnerabilities Larger or Equal to 4 (Past 30 Days)	<p>This panel shows the top IP addresses with CVSS score vulnerabilities larger or equal to 4 for the past 30 days.</p> <p>ISO 27002:2013 control ID: 12.6.1</p> <p>Saved Search: IT Governance – Top IP Addresses with CVSS Score Larger or Equal 4</p> <p>Type: Column</p>
Top Critical Vulnerability Events by CVE (Past 7 Days)	<p>This panel shows the top critical vulnerability events by CVE ID for the past 7 days.</p> <p>ISO 27002:2013 control ID: 12.6.1</p> <p>Saved Search: IT Governance - Top Critical CVEs</p> <p>Type: Column</p>
Vulnerability Scanner Events by Device Vendor (Past 3 Days)	<p>This panel shows vulnerability scanner events by device vendor for the past 3 days.</p> <p>Supported Devices: McAfee Vulnerability Manager, Nessus Vulnerability Scanner, Qualys Vulnerability Management, Nexpose, SAINT, nCircle</p> <p>ISO 27002:2013 control ID: 12.6.1</p> <p>Saved Search: IT Governance - Vulnerability Scanner Events by Device Vendor</p> <p>Type: Pie</p>
Top Vulnerability Events by Vendor Signature (Past 14 Days)	<p>This panel shows the top received vulnerability events by vendor signature for the past 14 days.</p> <p>Supported Devices: McAfee Vulnerability Manager, Nessus Vulnerability Scanner, Qualys Vulnerability Management, Nexpose, SAINT, nCircle</p> <p>ISO 27002:2013 control ID: 12.6.1</p> <p>Saved Search: IT Governance - Top Vulnerability Events by Vendor Signature</p> <p>Type: Column</p>

IT Governance - DoS and Port Scanning Activity

Dashboard Panel	Description
DoS Attack Events on the Past Day (by the Hour)	<p>This panel shows the DoS attack events for the past day by the hour.</p> <p>ISO 27002:2013 control ID: 16.1.1</p> <p>Saved Search: IT Governance - DoS Attacks on the Last Day</p> <p>Type: Line</p>
Top DoS Attacks by Source Address (Past Day)	<p>This panel shows the top DoS attack events by source address for the past day.</p> <p>ISO 27002:2013 control ID: 16.1.1</p> <p>Saved Search: IT Governance - Dos Attacks by Source Address</p> <p>Type: Column</p>
Port Scan Events for the Past Day (by the Hour)	<p>This panel shows the port scanning events for the past day by the hour.</p> <p>ISO 27002:2013 control ID: 16.1.1</p> <p>Saved Search: IT Governance - Port Scans for the Last Day</p> <p>Type: Line</p>
Top Port Scan Events by Source Address (Past Day)	<p>This panel shows port scanning events by source address for the past day.</p> <p>ISO 27002:2013 control ID: 16.1.1</p> <p>Saved Search: IT Governance - Top Port Scan Events by Source Address</p> <p>Type: Column</p>

IT Governance - Technical Controls Activity

Dashboard Panel	Description
Top Firewall Events (Past Hour)	<p>This panel shows Firewall events by name for the past hour.</p> <p>ISO 27002:2013 control ID: 13.1.1</p> <p>Saved Search: IT Governance – Firewall Events</p> <p>Type: Column</p>
Top Anti Virus Events (Past Hour)	<p>This panel shows Anti Virus events by name for the past hour.</p> <p>ISO 27002:2013 control ID: 12.2.1</p> <p>Saved Search: IT Governance – Anti Virus Events</p> <p>Type: Column</p>

Dashboard Panel	Description
Top IPS/IDS Events (Past Hour)	<p>This panel shows IPS/IDS events by name for the past hour.</p> <p>ISO 27002:2013 control ID: 13.1.1</p> <p>Saved Search: IT Governance – Intrusion Prevention and Detection Events</p> <p>Type: Column</p>
Technical Controls Events by Category (Past Day)	<p>This panel shows technical controls events by categoryDeviceGroup for the past day.</p> <p>ISO 27002:2013 control ID: 12.2.1, 13.1.1</p> <p>Saved Search: IT Governance - Technical Controls Events</p> <p>Type: Pie</p>

IT Governance - User Activity Dashboard

Dashboard Panel	Description
Top Suspicious Activity by User (Past 7 Days)	<p>This panel shows top suspicious activity by user on the past 7 days.</p> <p>ISO 27002:2013 control ID: 12.4.1</p> <p>Saved Search: IT Governance – Suspicious Activity by User</p> <p>Type: Column</p>
Top User Login and Logout Events (Past Day)	<p>This panel shows user login and logout events on the past day.</p> <p>ISO 27002:2013 control ID: 12.4.1</p> <p>Saved Search: IT Governance – User Login and Logout Events</p> <p>Type: Column</p>
Top Failed User Actions Events (Past Hour)	<p>This panel shows failed user actions on the past hour.</p> <p>ISO 27002:2013 control ID: 12.4.1</p> <p>Saved Search: IT Governance – Failed User Actions</p> <p>Type: Column</p>
Top Failed User Login by System (Past Day)	<p>This panel shows failed user login by system on the past day.</p> <p>ISO 27002:2013 control ID: 12.4.1</p> <p>Saved Search: IT Governance - Failed User Login by System</p> <p>Type: Column</p>

Chapter 7: Logger CIP for IT Gov Parameters

Logger CIP for IT Gov uses the parameters described below.

adminUsers

When you run a report that invokes a query that expects the `adminUsers` parameter as input, the Administrative User(s) prompt is displayed during report runtime with a default value of 'admin', 'administrator', 'root'. The value in the Administrative User(s) text field is passed to the query using the `adminUsers` parameter. Supply the set of administration accounts used at your site, for example: 'adm', 'root'. Each user name starts and ends with a single quote and each name is separated by a comma. In addition, specify all names in lower case.

To change the value of the parameter that is passed to the query, enter a new value when prompted by the report during runtime or change the default value of the parameter. For more information, see ["Configuring Reports" on page 20](#).

allowedPorts

When you run a report that invokes a query that expects the `allowedPorts` parameter as input, the Allowed Port(s) prompt is displayed during report runtime with a default value of 80,443. The value in the Allowed Port(s) text field is passed to the query using the `allowedPorts` parameter. Supply the set of allowed ports for your site, for example: 80,25,110. Separate each port number by a comma.

To change the value of the parameter that is passed to the query, enter a new value when prompted by the report during runtime or change the default value of the parameter. For more information, see ["Configuring Reports" on page 20](#).

destinationAddress

This is an internal parameter that passes data from one drill-down report to another. The value in this parameter is not intended to be modified.

databaseAdminAccounts

When you run a report that invokes a query that expects the `databaseAdminAccounts` parameter as input, the Database Administration Account(s) prompt is displayed during report runtime with a default

value of 'sys', 'system', 'sa'. The value in the Database Administration Account(s) text field is passed to the query using the databaseAdminAccounts parameter. Supply the set of database administration accounts used at your site, for example: 'internal', 'sysman', 'sys'. Start and end each user with a single quote and separate each name by a comma.

To change the value of the parameter that is passed to the query, enter a new value when prompted by the report during runtime or change the default value of the parameter. For more information, see ["Configuring Reports" on page 20](#).

databaseAdminUsers

When you run a report that invokes a query that expects the databaseAdminUsers parameter as input, the Database Administrative User(s) prompt is displayed during report runtime with a default value of 'admin', 'administrator'. The value in the Database Administrative User(s) text field is passed to the query using the databaseAdminUsers parameter. Supply the network accounts used to administer the database at your site, for example: 'admin', 'jdoe'. Start and end each user name with a single quote and separate each name by a comma.

To change the value of the parameter that is passed to the query, enter a new value when prompted by the report during runtime or change the default value of the parameter. For more information, see ["Configuring Reports" on page 20](#).

destinationHostName

This is an internal parameter that passes data from one drill-down report to another. The value in this parameter is not intended to be modified.

destinationUserName

When you run a report that invokes a query that expects the destinationUserName parameter as input, the User Name prompt is displayed during report runtime with a default value of 'admin'. The value in the User Name text field is passed to the query using the destinationUserName parameter. Supply the destination user name to report on, for example: 'sys'. Start and end the user name with a single quote.

To change the value of the parameter that is passed to the query, enter a new value when prompted by the report during runtime or change the default value of the parameter. For more information, see ["Configuring Reports" on page 20](#).

developmentNetwork

When you run a report that invokes a query that expects the `developmentNetwork` parameter as input, the Development Network(s) prompt is displayed during report runtime with a default value of `(192\\.168\\. | 10\\.)`. The value in the Development Network(s) text field is passed to the query using 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 ["Configuring Reports" on page 20](#).

To change the value of the parameter that is passed to the query, enter a new value when prompted by the report during runtime or change the default value of the parameter. For more information, see ["Configuring Reports" on page 20](#).

deviceEventClassId

This is an internal parameter that passes data from one drill-down report to another. The value in this parameter is not intended to be modified.

deviceProduct

This is an internal parameter that passes data from one drill-down report to another. The value in this parameter is not intended to be modified.

eventName

This is an internal parameter that passes data from one drill-down report to another. The value in this parameter is not intended to be modified.

eventPriority

This is an internal parameter that passes data from one drill-down report to another. The value in this parameter is not intended to be modified.

internalNetwork

When you run a report that invokes a query that expects the `internalNetwork` parameter as input, the Internal Network(s) prompt is displayed during report runtime with a default value of `(192\\\.168\\\.|10\\\.)`. The value in the Internal Network(s) text field is passed to the query using 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 ["Configuring Reports" on page 20](#)

To change the value of the parameter that is passed to the query, enter a new value when prompted by the report during runtime or change the default value of the parameter. For more information, see ["Configuring Reports" on page 20](#).

productionNetwork

When you run a report that invokes a query that expects the `productionNetwork` parameter as input, the Production Network(s) prompt is displayed during report runtime with a default value of `(192\\\.168\\\.|10\\\.)`. The value in the Production Network(s) text field is passed to the query using 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 ["Configuring Reports" on page 20](#)

To change the value of the parameter that is passed to the query, enter a new value when prompted by the report during runtime or change the default value of the parameter. For more information, see ["Configuring Reports" on page 20](#).

sourceDestUserName

This is an internal parameter that passes data from one drill-down report to another. The value in this parameter is not intended to be modified.

sourceUserName

This is an internal parameter that passes data from one drill-down report to another. The value in this parameter is not intended to be modified.

testingNetwork

When you run a report that invokes a query that expects the `testingNetwork` parameter as input, the Testing Network(s) prompt is displayed during report runtime with a default value of `(192\\\.168\\\.|10\\\.)`. The value in the Testing Network(s) text field is passed to the query using 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 ["Configuring Reports" on page 20](#)

To change the value of the parameter that is passed to the query, enter a new value when prompted by the report during runtime or change the default value of the parameter. For more information, see ["Configuring Reports" on page 20](#).

thirdPartyNetwork

When you run a report that invokes a query that expects the `thirdPartyNetwork` parameter as input, the Third-Party Network(s) prompt is displayed during report runtime with a default value of `(192\\\.168\\\.|10\\\.)`. 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 ["Configuring Reports" on page 20](#)

To change the value of the parameter that is passed to the query, enter a new value when prompted by the report during runtime or change the default value of the parameter. For more information, see ["Configuring Reports" on page 20](#).

variable

This is an internal parameter that passes data from one drill-down report to another. The value in this parameter is not intended to be modified.

virusName

This is an internal parameter that passes data from one drill-down report to another. The value in this parameter is not intended to be modified.

wirelessNetwork

When you run a report that invokes a query that expects the `wirelessNetwork` parameter as input, the Wireless Network(s) prompt is displayed during report runtime with a default value of `(192\\\.168\\. | 10\\.)`. The value in the Wireless Network(s) text field is passed to the query using 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 ["Configuring Reports" on page 20](#).

To change the value of the parameter that is passed to the query, enter a new value when prompted by the report during runtime or change the default value of the parameter. For more information, see ["Configuring Reports" on page 20](#).

Appendix A: Uninstalling Logger CIP for IT Gov

To uninstall Logger CIP for IT Gov, you must delete each resource individually.

To delete the reports, queries, and parameters:

1. Delete each report, query, and parameter in the ISO 27002 and NIST 800-53 report category:
 - a. From the **Reports** top-level menu bar, click **Category Explorer** from the Navigation section.
 - b. Right click on **ISO 27002**.
 - c. Click **Delete**.
 - d. Right click on **NIST 800-53**.
 - e. Click **Delete**.

Caution: Do not delete the `destinationAddress` and `deviceProduct` variables. Both the Foundation reports and the Logger CIP for IT Gov reports use these variables.

To delete the alerts:

1. Delete each Logger CIP for IT Gov alert individually:
 - a. From the **Configuration** top-level menu bar, click **Alerts** from the **Data** section.
 - b. For each Logger CIP for IT Gov alert, click the **Remove (✕)** icon.
 - c. In the confirmation dialog, click **OK** to complete the deletion.

To delete the dashboards:

1. Delete each Logger CIP for IT Gov alert individually:
 - a. From the **Configuration** top-level menu bar, click **Dashboards**.
 - b. For each Logger CIP for IT Gov dashboard, click **Tools > Delete Dashboard**.
 - c. In the confirmation dialog, click **OK** to complete the deletion.

To delete saved searches:

1. Delete each Logger CIP for IT Gov alert individually:
 - a. From the **Configuration** top-level menu bar, click **Saved Searches** from the **Search** section.
 - b. For each Logger CIP for IT Gov saved search, click the **Remove (✕)** icon.
 - c. In the confirmation dialog, click **OK** to complete the deletion.

Send Documentation Feedback

If you have comments about this document, you can [contact the documentation team](#) by email. If an email client is configured on this computer, click the link above and an email window opens with the following information in the subject line:

Feedback on Solutions Guide (Logger CIP for IT Gov 5.02)

Just add your feedback to the email and click send.

If no email client is available, copy the information above to a new message in a web mail client, and send your feedback to arc-doc@hpe.com.

We appreciate your feedback!