

---

# **Micro Focus Security**

# **ArcSight Logger CIP for PCI**

Software Version: 4.02

## **Solutions Guide**

Document Release Date: June, 2018

Software Release Date: June, 2018



## Legal Notices

### Warranty

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

### Restricted Rights Legend

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

### Copyright Notice

© 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

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

# Contents

Chapter 1: Logger CIP for PCI Overview .....	7
Logger CIP for PCI Architecture .....	9
PCI Resources .....	9
Alerts .....	9
Queries .....	10
Reports .....	10
Dashboards .....	10
Supported Devices .....	11
Chapter 2: Installing Logger CIP for PCI .....	12
Installing Logger CIP for PCI on the Logger Appliance .....	12
Installing Logger CIP for PCI on the Software Logger .....	13
Chapter 3: Configuring Logger CIP for PCI .....	14
Processing All Events .....	14
Limiting Events Processed .....	16
Classifying PCI-Related Devices in a PCI Device Group .....	16
Creating a PCI Filter to Limit the Events Processed .....	17
Limiting Events Processed by Alerts .....	18
Limiting Events Processed by Reports .....	20
Configuring Alerts .....	21
Configuring Reports .....	26
Sending Virtualization Component Events to ArcSight ESM .....	28
Sending Payment Application Events to ArcSight ESM .....	29
Chapter 4: PCI Alerts .....	31
Requirement 1 Alerts .....	32
Requirement 2 Alerts .....	35
Requirement 3 Alerts .....	37
Requirement 4 Alerts .....	39
Requirement 5 Alerts .....	40

Requirement 6 Alerts .....	41
Requirement 7 Alerts .....	43
Requirement 8 Alerts .....	44
Requirement 9 Alerts .....	45
Requirement 10 Alerts .....	46
Requirement 11 Alerts .....	52
Requirement 12 Alerts .....	53
PA-DSS Requirement 4 Alerts .....	54
 Chapter 5: PCI Reports by Category .....	 56
Build and Maintain a Secure Network and Systems .....	58
Do not use vendor-supplied defaults for system passwords and other security parameters .....	60
Protect stored cardholder data .....	61
Encrypt transmission of cardholder data across open public networks .....	62
Protect all systems against malware and regularly update anti-virus software or programs .....	62
Develop and maintain secure systems and applications .....	64
Restrict access to cardholder data by business need to know .....	66
Identify and authenticate access to system components .....	67
Restrict physical access to cardholder data .....	68
Track and monitor all access to network resources and cardholder data .....	69
Regularly test security systems and processes .....	75
Maintain a policy that addresses information security for all personnel .....	80
PA-DSS .....	81
Helper Utils .....	84
 Chapter 6: PCI Dashboards .....	 86
Requirement 1 Dashboard .....	87
Requirement 2 Dashboard .....	88
Requirement 3 Dashboard .....	89
Requirement 4 Dashboard .....	90
Requirement 5 Dashboard .....	91
Requirement 6 Dashboard .....	92

Requirement 7 Dashboard .....	93
Requirement 8 Dashboard .....	94
Requirement 9 Dashboard .....	96
Requirement 10 Dashboard .....	97
Requirement 11 Dashboard .....	98
Requirement 12 Dashboard .....	99
 Chapter 7: PCI Parameters .....	 100
ANONYMOUS_ACCOUNTS .....	100
CDE_ALLOWED_PORTS .....	100
CDE_AUTHORIZED_USERS .....	100
CDE_ZONES .....	100
CUSTOM_ACCOUNTS .....	100
DATABASE_ADDRESSES .....	101
DATABASE_ADMIN_USERS .....	101
destinationZone .....	101
DMZ_ALLOWED_PORTS .....	101
DMZ_ZONES .....	101
pciAdminUsers .....	101
pciDestAddress .....	102
pciDestHostName .....	102
pciDestUserName .....	102
pciDeviceAddress .....	102
pciDeviceHostName .....	102
pciEventId .....	102
pciEventName .....	103
pciPaymentApplications .....	103
pciSourceAddress .....	103
pciSrcUserName .....	103
pciVirtualizationProducts .....	103
PERIMETER_FIREWALL .....	103
UNSECURED_PORTS .....	104

UNSECURED_PROCESSESSES .....	104
WIRELESS_ZONES .....	104
Appendix A: Uninstall Logger CIP for PCI .....	105
Send Documentation Feedback .....	106

# Chapter 1: Logger CIP for PCI Overview

The Payment Card Industry (PCI) Data Security Standard (DSS) 3.1 is a comprehensive standard defined by the Payment Card Industry Security Standards Council to help organizations protect customer account data and to advance the broad adoption of consistent data security measures across the globe. The standard includes twelve requirements, each with many sub-requirements, for security management, policies, procedures, network architecture, software design, and other key protective measures.

The following table lists the PCI DSS requirements.

**Note:** Excerpts from the PCI DSS and related control statements are provided courtesy of PCI Security Standards Council, LLC and/or its licensors. © 2014 PCI Security Standards Council, LLC. All Rights Reserved.

Objectives	PCI DSS Requirements
<b>Build and Maintain a Secure Network</b>	<b>1.</b> Install and maintain a firewall configuration to protect cardholder data <b>2.</b> Do not use vendor-supplied defaults for system passwords and other security parameters
<b>Protect Cardholder Data</b>	<b>3.</b> Protect stored cardholder data <b>4.</b> Encrypt transmission of cardholder data across open, public networks
<b>Maintain a Vulnerability Management Program</b>	<b>5.</b> Use and regularly update anti-virus software or programs <b>6.</b> Develop and maintain secure systems and applications
<b>Implement Strong Access Control Measures</b>	<b>7.</b> Restrict access to cardholder data by business need to know <b>8.</b> Identify and authenticate access to system components <b>9.</b> Restrict physical access to cardholder data
<b>Regularly Monitor and Test Networks</b>	<b>10.</b> Track and monitor all access to network resources and cardholder data <b>11.</b> Regularly test security systems and processes
<b>Maintain an Information Security Policy</b>	<b>12.</b> Maintain a policy that addresses information security for all personnel

ArcSight Logger Compliance Insight Package for Payment Card Industry (Logger CIP for PCI) is a package of reports, alerts, and dashboards that can assist you in complying with the PCI requirements

specified in Payment Card Industry Data Security Standard 3.1 and the Payment Application Data Security Standard (PA-DSS) 3.1.

Logger CIP for PCI leverages the litigation-quality, long-term repository of log and event data of ArcSight Logger to facilitate better PCI compliance audits, security forensics, and system maintenance using the Logger reporting and alerting capability.

Logger CIP for PCI addresses the PCI standard by providing:

- Detailed reports on the 12 requirements defined in the PCI Standard and Requirement 4 of the Payment Application Standard (PA-DSS)
- Alerts that monitor incoming events in real time and notify PCI analysts when events of interest are detected
- Dashboards that show compliance for the 12 requirements defined in the PCI Standard using graphs and bar charts

The PCI reports, alerts, and dashboards helps demonstrate to stakeholders and auditors that controls are implemented on the systems in your company that contain credit card data and show due diligence to comply with the PCI standard.

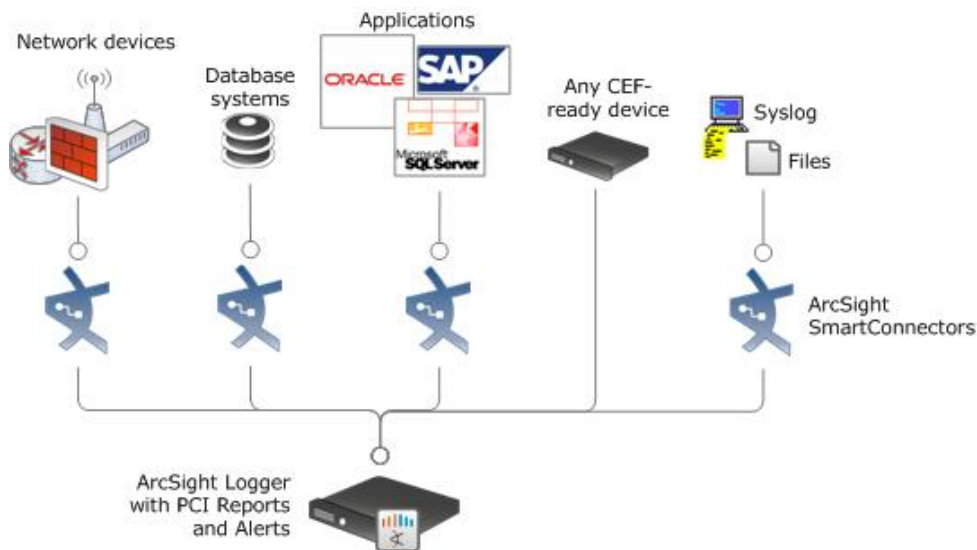


## Logger CIP for PCI Architecture

Logger CIP for PCI reports work on events in Common Event Format (CEF) format, an industry standard for the interoperability of event or log-generating devices.

CEF events can come from a device that is already configured to post events in CEF format, or they can come from any network device whose events are first run through an ArcSight SmartConnector.

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



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

## PCI Resources

Logger CIP for PCI provides alerts, queries, reports, and dashboards to help you demonstrate that controls are implemented on the systems in your company that contain credit card data and that you comply with the PCI standard.

### Alerts

Alerts monitor incoming events in real time and notify PCI analysts when events of interest are detected. Some PCI alerts are enabled by default and the rest are disabled. You can view the list of PCI alerts by selecting the **Configuration** tab and then **Alerts** in the left menu panel. To enable an alert, click the **Disabled** (🚫) icon.

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

## Queries

The SQL queries that support the PCI reports have similar names as the reports themselves. For example, the *Requirement 1-External to PCI System Activity - All* report invokes the *PCI 1-External To PCI Systems* query. The queries can be viewed from the *Reports* tab by selecting **Queries** from the left panel menu. For information on configuring a query see the *Logger Administrator's Guide*.

## Reports

Logger CIP for PCI reports consist of the following:

- **PCI Standard Reports** are optimized to help companies and PCI auditors determine the status of your systems for each PCI requirement addressed by the solution report. In addition to detailed report results, each report contains a summary of the PCI requirement it addresses, how the report supports the requirement, and testing criteria an auditor can use to determine your organization's compliance with the requirement.
- **Drill-down Reports**  
Several reports contain hyperlinks to *drill-down reports* (the report output format must be HTML). Drill-down reports provide additional information to help you pinpoint events that can jeopardize the security of cardholder data. Some drill-down reports link to other drill-down reports to provide more than one perspective of an event. During an investigation, it can be useful to run a drill-down report directly, rather than from a hyperlink in another report. To run a drill-down report directly, you pass the drill-down field name from the calling report as a parameter. For example, to run the *Requirement 5 - Detailed Anti-Virus Report per Host* report, you specify the Destination Host Name as a parameter.
- The **PCI Executive Report** shows an executive overview of the vulnerabilities, database access, attacked hosts and virus events in the PCI environment.

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

## Dashboards

The PCI dashboards show PCI compliance separately in the pie charts to help you demonstrate appropriate risk management and monitoring practices.

## Supported Devices

Logger CIP for PCI acts on events from systems that store and process credit card data, and the systems that interact with and protect those systems, including the following:

- Applications that process cardholder data
- Anti-virus solutions
- Databases that store cardholder data
- Content Security and Web Filtering systems
- Operating systems
- Physical Security systems
- Virtual Management systems
- Virtual Private Networks
- Host and network-based IDS
- Firewalls
- Wireless systems

**Note:** Logger CIP for PCI reports and alerts operate on events from the devices in your environment. HP recommends that you use an ArcSight SmartConnector for devices that are not CEF-enabled so that the reports yield the most accurate results.

# Chapter 2: Installing Logger CIP for PCI

You can install Logger CIP for PCI on the Logger Appliance or the Software Logger. Follow the appropriate procedure below for your Logger type.

## Installing Logger CIP for PCI on the Logger Appliance

Logger Appliance is the preconfigured hardware version of Logger.

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

### To install Logger CIP for PCI on the Logger Appliance:

1. Download the Logger CIP for PCI .enc file (for example, ArcSight-ComplianceInsightPackage-Logger-PCI.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 warning that the update process may take some time is displayed.

7. Click **OK**.

A message displays indicating that the upgrade is progressing. After the contents of the .enc file are installed, another message displays indicating that the upgrade is a success. The .enc file installs PCI 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 **Payment Card Industry** to see the report categories, then click a category to see the list of reports.
  - To view the installed dashboards, select **Dashboards**. Click the drop-down arrow in the top left field.

# Installing Logger CIP for PCI on the Software Logger

Software Logger is the downloadable version of Logger installed on your hardware.

## To install Logger CIP for PCI 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 PCI .bin file (for example, ArcSight-ComplianceInsightPackage-Logger-PCI.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-PCI.x.x.nnnn.0.bin
```

5. Run the installer:

```
./ArcSight-ComplianceInsightPackage-Logger-PCI.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 PCI 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 **Payment Card Industry** to see the report categories, then click a category to see the list of reports.
  - To view the installed dashboards, select **Dashboards**. Click the drop-down arrow in the top left field.

# Chapter 3: Configuring Logger CIP for PCI

This section describes how to configure Logger CIP for PCI to work in your environment.

## Processing All Events

If all the devices in your environment are subject to PCI compliance, configure the Logger so all received events are processed by the Logger CIP for PCI reports and alerts.

**PCI Reports** are ready to process all events received by the Logger and no configuration is required.

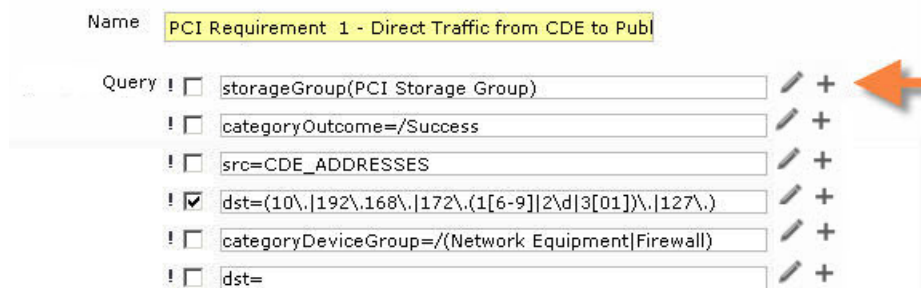
**PCI Alerts** require some configuration to process all the events received by the Logger. By default, all PCI alerts contain the following placeholder condition (Query Term) `storageGroup(PCI Storage Group)`. If you want all the enabled PCI alerts to process all the events received, edit each enabled PCI alert and remove this Query Term (condition) as described in the procedure below.

**Note:** You can enable a maximum of 25 alerts on Logger at one time. Configure only those alerts that you plan to enable. To enable an additional alert, you might need to disable another alert.

If you want to limit the events processed by the Logger CIP for PCI reports and alerts, see ["Limiting Events Processed" on page 16](#).

### To configure alerts to process all events:

1. Select **Configuration** on the top-level menu bar, then click **Alerts** in the **Data** section.
2. Click a PCI alert in the Name column.
3. Find the placeholder Query Term with the text: `storageGroup(PCI Storage Group)`, as shown in the following figure.



4. Remove all the text in the Query Term field, as shown in the following figure.

Name	PCI Requirement 1 - Direct Traffic from CDE to Publ		
Query	<input type="checkbox"/>		+
	<input type="checkbox"/>	categoryOutcome=/Success	+
	<input type="checkbox"/>	src=CDE_ADDRESSES	+
	<input checked="" type="checkbox"/>	dst=(10\.,192\.,168\.,172\.,(1[6-9] 2\d 3[01])\.\.127\.)	+
	<input type="checkbox"/>	categoryDeviceGroup=/(Network Equipment Firewall)	+
	<input type="checkbox"/>	dst=	+

5. Click **Save**.
6. Repeat this procedure for each alert you plan to enable.
7. Configure the alerts with site-specific data. See ["Configuring Alerts" on page 21](#).

## Limiting Events Processed

If only some of your devices are subject to PCI compliance, you can limit the events processed by the Logger CIP for PCI reports and alerts to improve system performance, and obtain more accurate and PCI-relevant information. You can limit the events processed by PCI reports and alerts, in one or more of the following ways:

- Create a PCI-specific device group and only process events from devices in the device group.
- Use a PCI-related *Storage Group* to limit the events processed. This option is available only if a 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 *ArcSight Logger Administrator's Guide*.
- Process events from specified devices only.

Which strategy you choose depends on how your environment is set up, and how you want to organize your PCI compliance program. These limiting strategies can be combined.

**Tip:** Reducing the amount of data a resource has to process translates to better performance. If only a small subset of the overall data feeding into Logger is subject to PCI compliance, using a different Storage Group to store events from PCI-related devices yields the best performance results.

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

- Classify PCI-related devices in a PCI device group. See ["Classifying PCI-Related Devices in a PCI Device Group" below](#).
- Create a PCI filter that constrains the events processed by the alerts and reports. See ["Creating a PCI Filter to Limit the Events Processed" on the next page](#).
- Limit the events that an alert processes by either applying the PCI filter to the alert or adding a condition directly to the alert. See ["Limiting Events Processed by Alerts" on page 18](#).
- Apply the PCI filter to the entire PCI report category or specify at report run time. See ["Limiting Events Processed by Reports" on page 20](#).

## Classifying PCI-Related Devices in a PCI Device Group

If you plan to use a device group to limit the events processed by reports and alerts, create the PCI device group and classify the PCI-related devices into it, as described in following procedure. You can then create a filter that only returns events from devices listed in the PCI device group filter and configure alerts and reports to use that filter.



**To classify PCI-related devices in PCI device group:**

1. Select **Configuration** from the top-level menu panel, 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 PCI.
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 PCI filter to limit the events processed as described in ["Creating a PCI Filter to Limit the Events Processed" below](#)

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

## Creating a PCI Filter to Limit the Events Processed

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

- **Limit using a PCI-related device group**—Only those events from devices listed in the device group are processed. .
- **Limit using a PCI-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 `PCI Device Group Filter` that returns events from devices categorized as PCI devices.
- A filter called `PCI Storage Group Filter` that returns events that are stored in a designated storage group.
- A filter called `PCI Devices Filter` that returns events from specified devices.
- A filter called `PCI Storage Group and Devices Filter` that returns events that are stored in a designated storage group (such as a PCI 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. On the *Add Filter* page, enter the following information, then click **Next**:

Field	Description
Name	Enter a name for the filter that identifies it with Logger CIP for PCI and identifies the purpose of the filter, such as PCI Device Group Filter, PCI Storage Group Filter, or PCI Devices Filter.
Type	From the drop-down menu, select <b>Search Group</b> . 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(PCIDeviceGroup)`
  - 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 PCI 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 create to limit the events processed by both reports and alerts, as described in ["Limiting Events Processed by Alerts" below](#) and ["Limiting Events Processed by Reports" on page 20](#).

## Limiting Events Processed by Alerts



You can constrain the events that an alert processes by adding a filter or a query term to the alert.


**Note:** A maximum of 25 alerts can be enabled on Logger at one time. Configure only those alerts that you plan to enable.


### To add a filter to the alert:


1. Select **Configuration** from the top-level menu, then select **Alerts** from the **Data** section.
2. Click a PCI alert in the Name column.
3. In the **Filters** field, select the filter you created in ["Creating a PCI Filter to Limit the Events Processed" on the previous page](#) that limits the events processed by the alert.
4. Locate and remove the placeholder `storageGroup(PCI Storage Group)` condition:
  - a. Find the Query Terms field with the text: `storageGroup(PCI Storage Group)`, as shown in the following figure.


Name **PCI Requirement 1 - Direct Traffic from CDE to Publ**


Query ! ☐ storageGroup(PCI Storage Group)  + 

! ☐ categoryOutcome=/Success  +

! ☐ src=CDE\_ADDRESSES  +


! ☒ dst=(10\.,192\.,168\.,172\.,(1[6-9]|2\d|3[01])\.\.127\.)  +


! ☐ categoryDeviceGroup=/(Network Equipment|Firewall)  +


! ☐ dst=  +


- b. Remove all the text in the Query Term field, as shown in the following figure.


Name **PCI Requirement 1 - Direct Traffic from CDE to Publ**


Query ! ☐  +

! ☐ categoryOutcome=/Success  +

! ☐ src=CDE\_ADDRESSES  +

! ☒ dst=(10\.,192\.,168\.,172\.,(1[6-9]|2\d|3[01])\.\.127\.)  +

! ☐ categoryDeviceGroup=/(Network Equipment|Firewall)  +


! ☐ dst=  +


5. Click **Save**.
6. Repeat for each alert you plan to enable.


### To add a query term to the alert:


1. Select **Configuration** from the top-level menu, then select **Alerts** from the **Data** section.
2. Click the PCI alert in the Name column.
3. Locate the placeholder storageGroup(PCI Storage Group) condition. Find the Query Terms field with the text: storageGroup(PCI Storage Group) as shown in the preceding figure.
4. Remove all the text in the Query Term field, as shown in the following figure.


Name **PCI Requirement 1 - Direct Traffic from CDE to Publ**


Query ! ☐  +


! ☐ categoryOutcome=/Success  +

! ☐ src=CDE\_ADDRESSES  +

! ☒ dst=(10\.,192\.,168\.,172\.,(1[6-9]|2\d|3[01])\.\.127\.)  +

! ☐ categoryDeviceGroup=/(Network Equipment|Firewall)  +

! ☐ dst=  +


5. In the same 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(PCIDeviceGroup)
  - 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 PCI 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.
6. Click **Save**.
  7. Repeat this procedure for each alert you plan on enabling.

## Limiting Events Processed by Reports

You can limit events processed by the PCI 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 (the PCI report group).

To limit events at report run time, run the report using the Quick Run () option. Select one or more Devices, Device Groups, or 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 PCI 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
<b>PCI Requirement 1 - Direct Traffic from CDE to Public Addresses Alert</b>  <b>PCI Requirement 1 - Direct Traffic from Public Addresses to CDE Alert</b>  <b>PCI Requirement 1 - Destination Address in CDE and DMZ</b>  <b>PCI Requirement 1- Unauthorized Inbound Traffic to the CDE</b>  <b>PCI Requirement 1- Unauthorized Outbound Traffic from the CDE</b>  <b>PCI Requirement 1- Unauthorized Inbound Traffic from Wireless Networks to the CDE</b>  <b>PCI Requirement 8 - Anonymous User Activity</b>	<p>In the Query Terms field that contains the string CDE_ADDRESSES, replace CDE_ADDRESSES with a regular expression that specifies the range of IP addresses for machines in the Cardholder Data Environment (CDE).</p>
<b>PCI Requirement 1 - Unauthorized Inbound Traffic from Public Addresses</b>  <b>PCI Requirement 1-Unauthorized Inbound Traffic from Public IP Addresses to the DMZ</b>  <b>PCI Requirement 2 - Databases in DMZ</b>	<p>Edit the alert: In the Query Terms field that contains the string DMZ, replace DMZ with a regular expression that specifies a range of IP addresses of the machines in the DMZ.</p>
<b>PC Requirement 1- Unauthorized Inbound Traffic from Wireless Networks to the CDE</b>  <b>PCI Requirement 1- Unauthorized Outbound Traffic from the CDE to Wireless Networks</b>	<p>In the Query Terms field that contains the string CDE_ADDRESSES, replace CDE_ADDRESSES with a regular expression that specifies the range of IP addresses for machines in the Cardholder Data Environment (CDE).</p> <p>In the Query Terms field that contains the string WIRELESS_ADDRESSES, replace WIRELESS_ADDRESSES with a regular expression that specifies a range of IP addresses of the machines in wireless networks.</p>

Alert Name	Required Configuration
<b>PCI Requirement 1 - Destination Address in CDE and DMZ</b> <b>PCI Requirement 1 - Source Address in CDE and DMZ</b>	<p>In the Query Terms field that contains the string: CDE_ADDRESSES, replace CDE_ADDRESSES with a regular expression that specifies the range of IP addresses for machines in the Cardholder Data Environment (CDE).</p> <p>In the Query Terms field that contains the string DMZ, replace DMZ with a regular expression that specifies a range of IP addresses of the machines in the DMZ.</p>
<b>PCI Requirement 1- Internal IP Access from the Internet</b> <b>PCI Requirement 1- Disclosed Private IP Addresses</b>	<p>In the Query Terms field that contains the string PERIMETER_FIREWALL, replace PERIMETER_FIREWALL with a regular expression that specifies the IP/a range of IP addresses of your perimeter firewalls.</p>
<b>PCI Requirement 2 - Default Account Usage Alert</b>	<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>
<b>PCI Requirement 6 - Custom Account Detected</b>	<p>In the Query Terms field that contains the string PRODUCTION_ENVIRONMENT, replace PRODUCTION_ENVIRONMENT with a regular expression that specifies a range of IP addresses of the machines in your production environment.</p>
<b>PCI Requirement 7- Unauthorized Access to CDE Detected</b>	<p>In the Query Terms field that contains the string UNAUTHORIZED_USERS, replace UNAUTHORIZED_USERS with a regular expression that specifies a list of unauthorized users that you want to monitor; for example, user1 user2 user3.</p> <p>In the Query Terms field that contains the string: CDE_ADDRESSES, replace CDE_ADDRESSES with a regular expression that specifies the range of IP addresses for machines in the Cardholder Data Environment (CDE).</p>

Alert Name	Required Configuration
<b>PCI Requirement 10 - Virtual Machine Down Alert</b>	Change the following query <code>^CEF:0\ .*\  (VirtualCenter 4.1 ESX VProduct)\ </code> by replacing <code>VirtualCenter 4.1 ESX VProduct</code> with a list of the virtual device products in your environment. The product names are present in the Device Product event field.
<b>PCI Requirement 10 - Virtual Machine Modifications Alert</b>	If you have virtual device products other than VMware, change the alert query conditions to match events from these products, or configure the connector to change the categorization of the specific events to match the alert query conditions.

Alert Name	Required Configuration
<b>PCI Requirement 10 - Excessive Failed Administrative Actions Alert</b>  <b>PCI Requirement 10 - Excessive Failed Administrative Logins Alert</b>  <b>PCI Requirement 10 - Excessive Failed User Actions Alert</b>  <b>PCI Requirement 10 - Excessive Failed User Logins Alert</b>  <b>PCI Requirement 10 - Excessive Successful Administrative Actions Alert</b>  <b>PCI Requirement 10 - Excessive Successful Administrative Logins Alert</b>  <b>PCI Requirement 10 - Excessive Successful User Actions Alert</b>  <b>PCI Requirement 10 - Excessive Successful User Logins Alert</b>	<p>Change the set of default administrative accounts defined in this alert, to reflect the administrative accounts used at your site:</p> <ul style="list-style-type: none"> <li>• admin</li> <li>• root</li> <li>• super</li> <li>• sa&lt;space&gt;</li> <li>• sys&lt;space&gt;</li> <li>• system</li> <li>• manager</li> </ul> <p>Edit the alert and in the Query Terms field that lists the default administrative account names, change the set of default administrative accounts to reflect the set of administrative accounts used at your site. For example, add the CTXSYS account name to the user list:</p> <pre>(duser suser)=(admin root super sa  sys  system manager CTXSYS)</pre> <p>Separate the user names using the pipe character ( ). The pipe character represents an OR operator.</p> <p>All account names are case insensitive. An alert triggers if the account name in the incoming PCI event matches one of the defined administrative accounts and the other conditions in the alert are satisfied.</p> <p>An account name matches if the name starts with the same set of characters as one of the defined administrative accounts—additional characters at the end of the account name are allowed. For example, the account name Administrator matches the account name admin. This type of pattern matching does not occur with the sys&lt;space&gt; and sa&lt;space&gt; account names because these account names are specified with a space at the end of the name. For example, the account name sarah does not match the sa&lt;space&gt; account name.</p>
<b>PA-DSS 4 - Anonymous Payment Application Access to Cardholder Data Alert</b>	<p>Edit the alert and change the query <code>^CEF:0\ .*\ (PAYMENT_APP_1 PAYMENT_APP_2)\ </code> to specify the payment applications to be monitored.</p> <p>Change the query <code>dst=CDE_ADDRESSES</code> to indicate the destination addresses of the cardholder systems.</p>



Alert Name	Required Configuration
<b>PA-DSS 4 - Consecutive Invalid Payment Application Access Attempts Alert</b>  <b>PA-DSS 4 - Payment Application Access to Cardholder Data with no User Name Alert</b>  <b>PA-DSS 4 - Payment Application Access with Anonymous User Name Alert</b>  <b>PA-DSS 4 - Payment Application Access with No User Name Alert</b>	Edit the alert and change the query <code>^CEF:0\ .*\ (PAYMENT_APP_1 PAYMENT_APP_2)\ </code> to specify the payment applications to be monitored.
<b>PA-DSS 4 - Payment Application Audit Log Initialized Alert</b>	Edit the alert and change the query <code>^CEF:0\ .*\ (PAYMENT_APP_1 PAYMENT_APP_2)\ </code> to specify the payment applications to be monitored.  Change the query <code>\ AUDIT_LOG_INITIALIZED\ </code> to indicate the name of the event that identifies audit log initialization.

### To configure an alert with site specific data:

1. Select the **Configuration** top-level menu bar, then select **Alerts** from the **Data** section.
2. Click the alert you want to configure.
3. Find the Query Term with the site specific data and change it to reflect your site.
4. Click **Save**.

## Configuring Reports

Many of the Logger CIP for PCI reports 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. You configure the report query or parameters.

The following table lists the reports that require configuration.

### Configuration Needed for Reports

Report Name	Configuration Required
<b>Requirement 1-External to PCI Systems on Disallowed Ports Report</b>	Configure the <i>PCI 1-External To PCI Systems On Disallowed Ports</i> query with disallowed ports for your site.
<b>Requirement 2-Default Account Usage Report</b>	Configure the <i>PCI 2-Default Account Usage</i> query with the default accounts in use on your site.
<b>Requirement 3-Credit Card Numbers in Clear Text Report</b>	Configure the <i>PCI 3-Credit Card Numbers in Clear Text</i> query with the event and/or identification information for your IDS and IPS systems.
<b>Requirement 4-Outbound Unencrypted Services Report</b>	Configure the <i>PCI 4-Outbound Unencrypted Communication</i> query with any additional unencrypted ports or protocols relevant to your site.
<b>Requirement 4-PCI Systems Providing Unencrypted Services Report</b>	Configure the <i>PCI 4-PCI Systems Providing Unencrypted Services</i> query with any additional unencrypted ports or protocols relevant to your site.
<b>Requirement 10-Administrative Actions Report.</b>	Configure the <i>PCI 10-Administrative Actions</i> query as needed with the names of the admin accounts used at your site.
<b>Requirement 10-Administrative Logins - All Report</b>	Configure the <i>PCI 10-Administrative Logins - All</i> query as needed with the names of the admin accounts used at your site.
<b>Requirement 10-Administrative Logins - Failed Report</b>	
<b>Requirement 10-Administrative Logins - Successful Report</b>	

**Configuration Needed for Reports, continued**

Report Name	Configuration Required
<b>Requirement 6-All Configuration Changes to Virtualization Management Systems Report</b>  <b>Requirement 6-All Configuration Modifications to Virtual Machines Report</b>  <b>Requirement 10-All Detected Virtual Machine MAC Addresses Report</b>  <b>Requirement 10-All Hypervisors per Reporting Device</b>  <b>Requirement 10-All Virtual Machine Creation and Deletion Events Report</b>  <b>Requirement 10-All Virtual Machine Data Manipulations Report</b>  <b>Requirement 10-All Virtualization Infrastructure Events Report</b>  <b>Requirement 10-Detected Virtual Machines with their Hypervisors and Reporting Devices Report</b>  <b>Requirement 10-All Detected Virtual Machine MAC Addresses Report</b>  <b>Requirement 10-Number of Hypervisors Detected per Reporting Device Report</b>  <b>Requirement 10-Number of Virtual Machines by Reporting Device and Hypervisor Report</b>  <b>Requirement 10-Top Hypervisors with the Most VM Activities Report</b>	<p>Specify the virtual device products used in your environment. Edit the <b>Default Value</b> field of the <code>pciVirtualizationProducts</code> parameter and specify a quoted, comma separated list of device products, for example: 'VirtualCenter 4.1', 'ESX'. The product names will be present in the Device Product event field.</p> <p>If you have virtual device products other than VMware, either change the query conditions for this report's query to match the events from those products, or configure the connector to change the categorization of the specific events to match the conditions in this query. See <a href="#">"Sending Virtualization Component Events to ArcSight ESM" on the next page</a>.</p>
<b>Requirement 10-All Detected Virtual Machine IP Addresses Report</b>	<p>Specify the virtual device products used in your environment. Edit the <b>Default Value</b> field of the <code>pciVirtualizationProducts</code> parameter and specify a quoted, comma separated list of device products, for example: 'VirtualCenter 4.1', 'ESX'. The product names will be present in the Device Product event field.</p> <p>Edit the underlying query for this report so that the DHCPAssign section captures IP address assignment events.</p> <p>If you have virtual device products other than VMware, edit the underlying query so that the MACAssign section captures MAC Address to virtual machine assignment events. See <a href="#">"Sending Virtualization Component Events to ArcSight ESM" on the next page</a>.</p> <p>If you change either the MACAssign or DHCPAssign sections of the query, modify the conditions at the bottom of the query accordingly.</p>

**Configuration Needed for Reports, continued**

Report Name	Configuration Required
<b>PA-DSS Requirement 4 - All Administrative Actions in Payment Applications Report</b>	Edit the pciPaymentApplicationsparameter Default Value field to indicate a quoted, comma separated list of all the payment applications, for example: 'Internet Information Server','RealSecure'
<b>PA-DSS Requirement 4 - Summary of Administrative Actions in Payment Applications Report</b>	Edit the pciAdminUsersparameter Default Value field to indicate a quoted, comma separated list of all the administrative users of the payment applications, in lowercase letters, for example:'root','administrator','admin','sys'
<b>PA-DSS Requirement 4 - Anonymous Payment Application Access to Cardholder Data Report</b>	Edit the pciPaymentApplicationsparameter Default Value field to indicate a quoted, comma separated list of all the payment applications, for example: 'Internet Information Server','RealSecure'  Change the conditions in the query to reflect the destination addresses or zones of systems that hold cardholder data.
<b>PA-DSS Requirement 4 - Creations and Deletions of Payment Application Objects Report</b>	Edit the pciPaymentApplicationsparameter Default Value field to indicate a quoted, comma separated list of all the payment applications, for example: 'Internet Information Server','RealSecure'
<b>PA-DSS Requirement 4 - Details of Invalid Payment Application Access Attempts</b>	
<b>PA-DSS Requirement 4 - Individual Access to Payment Applications Report</b>	
<b>PA-DSS Requirement 4 - Insufficient Audit Trail in Payment Application Events Report</b>	
<b>PA-DSS Requirement 4 - Summary of Invalid Payment Application Access Attempts Report</b>	
<b>PA-DSS Requirement 4 - Summary of Payment Applications with Insufficient Audit Trail Report</b>	
<b>PA-DSS Requirement 4 - Anonymous Access to Payment Application Report</b>	

## Sending Virtualization Component Events to ArcSight ESM

The Logger CIP for PCI queries for virtualization components accommodate events from VMware, by default. If you have virtualization products other than VMware in your environment, as an optional step, you can develop a FlexConnector to parse specific events related to the virtualization components on your network. When you develop the FlexConnector, make sure that you use the following field

mappings to map the key event data into the ArcSight event schema. Refer also to the instructions in the *FlexConnector Developer's Guide*.

ArcSight Field	Mapping
deviceCustomString5	The name of the virtual machine.
sourceUserName	The name of the user performing the event.  Note: If only one user name appears in the event, map the name to the <code>destinationUserName</code> field, described below.
destinationUserName	The name of the user on which the event is performed.  Note: If only one user name appears in the event, map the name to this field.
sourceAddress sourceHostName	The network address ( <code>sourceAddress</code> ) or hostname ( <code>sourceHostName</code> ) from which the operation is taking place.  Note: If only one address or hostname appears in the event, map the address or hostname to the <code>destinationAddress</code> or <code>destinationHostName</code> field, described below.
destinationAddress destinationHostName	The network address ( <code>destinationAddress</code> ) or hostname ( <code>destinationHostName</code> ) on which the operation is taking place.  Note: If only one address or hostname appears in the event, map the address to this field.  Note: For events that apply to hypervisors, map the hypervisor address to the <code>destinationAddress</code> field or the hypervisor hostname to the <code>destinationHostName</code> field.

## Sending Payment Application Events to ArcSight ESM

To send payment application audit events to ArcSight ESM, you might need to create payment application FlexConnectors. When you develop the FlexConnectors, make sure that you use the following field mappings to map the key event data into the ArcSight event schema. Refer also to the instructions in the *FlexConnector Developer's Guide*.

ArcSight Field	Mapping
deviceProduct	The name of the application.
deviceVendor	The application vendor.

ArcSight Field	Mapping
sourceUserName	<p>The name of the user performing the event. For example, if user A is changing the access permissions for user B within the payment application, map user A to the sourceUserName field.</p> <p>Note: If only one user name appears in the event, map the name to the destinationUserName field, described below.</p>
destinationUserName	<p>The name of the user on which the event is performed. For example, if user A is changing the access permissions for user B within the payment application, map user B to the destinationUserName field.</p> <p>Note: If only one user name appears in the event, map the name to this field.</p>
sourceAddress	<p>The network address from which the operation is taking place. For example, if a user with address 1.1.1.1 logs into address 2.2.2.2, map 1.1.1.1 to the sourceAddress field.</p> <p>Note: If only one address appears in the event, map the address to the destinationAddress field, described below.</p>
destinationAddress	<p>The network address on which the operation is taking place. For example, if a user with address 1.1.1.1 logs into address 2.2.2.2, map 2.2.2.2 to the destinationAddress field.</p> <p>Note: If only one address appears in the event, map the address to this field.</p>

Use the following event categories for the event types listed:

**Note:** It is a PA-DSS requirement to indicate the outcome in every event.

Event type	Behavior	Device Group	Outcome	Significance
Successful login to the application	/Authentication/ Verify	/Payment Application	/Success	/Informational
Failed login to the application	/Authentication/ Verify	/Payment Application	/Failure	/Informational
An object was created in the payment application (Success assumed; in case of a failure, the Outcome needs to reflect that and the significance is /Informational/Error)	/Create	/Payment Application	/Success	/Informational
An object was deleted in the payment application (Success assumed; in case of a failure, the Outcome needs to reflect that and the significance is /Informational/Error)	/Delete	/Payment Application	/Success	/Informational

# Chapter 4: PCI Alerts

This section lists all the Logger PCI alerts.

## Requirement 1 Alerts

Logger PCI Requirement 1 alerts notify PCI analysts when events occur that indicate the direct flow of traffic between public IPs and the Cardholder Data Environment (CDE).

The following devices are supported for Logger PCI Requirement 1 alerts:

- Network Equipment
- Firewall devices

Alert Name	Description
<b>PCI Requirement 1 - Direct Traffic from CDE to Public Addresses Alert</b>	<p>This alert triggers when a router or firewall reports direct communication from the Cardholder Data Environment (CDE) to public IP addresses. This type of activity is a violation of the PCI Data Security Standard (DSS).</p> <p>This alert is not configured by default.</p> <p>Default <b>Match Count</b>: 1</p> <p>Default <b>Threshold (Sec)</b>: 1</p>
<b>PCI Requirement 1 - Direct Traffic from Public Addresses to CDE Alert</b>	<p>This alert triggers when a router or firewall reports communications from public IP addresses to the Cardholder Data Environment (CDE). This type of activity is a violation of the PCI Data Security Standard (DDS).</p> <p>This alert is not configured by default.</p> <p>Default <b>Match Count</b>: 1</p> <p>Default <b>Threshold (Sec)</b>: 1</p>
<b>PCI Requirement 1 - Firewall Configuration Changes Alert</b>	<p>This alert triggers when changes to a Firewall's configuration file are reported.</p> <p>This alert is not configured by default.</p> <p>Default <b>Match Count</b>: 1</p> <p>Default <b>Threshold (Sec)</b>: 1</p>
<b>PCI Requirement 1 - Network Equipment Configuration Changes Alert</b>	<p>This alert triggers when changes to a network device's configuration file are reported.</p> <p>This alert is not configured by default.</p> <p>Default <b>Match Count</b>: 1</p> <p>Default <b>Threshold (Sec)</b>: 1</p>
<b>PCI Requirement 1 - VPN Configuration Changes Alert</b>	<p>This alert triggers when changes to a VPN device's configuration file are reported.</p> <p>This alert is not configured by default.</p> <p>Default <b>Match Count</b>: 1</p> <p>Default <b>Threshold (Sec)</b>: 1</p>



Alert Name	Description
<b>PCI Requirement 1 - Destination Address in CDE and DMZ</b>	<p>PCI Section: 1.3.7</p> <p>This alert triggers when a destination IP address is found in the Cardholder Data Environment and the DMZ.</p> <p>This alert is not configured by default.</p>
<b>PCI Requirement 1- Internal IP Access from the Internet</b>	<p>PCI Section: 1.3.4</p> <p>This alert triggers when a private IP address is disclosed to unauthorized parties.</p> <p>This alert is not configured by default.</p>
<b>PCI Requirement 1- Disclosed Private IP Addresses</b>	<p>PCI Section: 1.3.8</p> <p>This alert triggers when a private IP address is disclosed to unauthorized parties.</p> <p>This alert is not configured by default.</p>
<b>PCI Requirement 1- Unauthorized Inbound Traffic to the CDE</b>	<p>PCI Section: 1.2.1</p> <p>This alert triggers when unauthorized inbound traffic to the Cardholder Data Environment is detected.</p> <p>This alert is not configured by default.</p>
<b>PCI Requirement 1- Unauthorized Outbound Traffic from the CDE</b>	<p>PCI Section: 1.2.1</p> <p>This alert triggers when unauthorized outbound traffic from the Cardholder Data Environment is detected.</p> <p>This alert is not configured by default.</p>
<b>PCI Requirement 1 - Source Address in CDE and DMZ</b>	<p>PCI Section: 1.3.7</p> <p>This alert triggers when a source IP address is found in the Cardholder Data Environment and the DMZ.</p> <p>This alert is not configured by default.</p>
<b>PCI Requirement 1 - Unauthorized Inbound Traffic from Public Addresses</b>	<p>PCI Section: 1.3.2</p> <p>This alert triggers when unauthorized inbound traffic from public addresses is detected.</p> <p>This alert is not configured by default.</p>

Alert Name	Description
<b>PCI Requirement 1- Unauthorized Inbound Traffic from Public IP Addresses to the DMZ</b>	<p>PCI Section: 1.3.1</p> <p>This alert triggers when unauthorized inbound traffic from public IP addresses to the DMZ is detected.</p> <p>This alert is not configured by default.</p>
<b>PCI Requirement 1- Unauthorized Inbound Traffic from Wireless Networks to the CDE</b>	<p>PCI Section: 1.2.3</p> <p>This alert triggers when unauthorized inbound traffic from wireless networks to the Cardholder Data Environment is detected.</p> <p>This alert is not configured by default.</p>
<b>PCI Requirement 1- Unauthorized Outbound Traffic from the CDE to Wireless Networks</b>	<p>PCI Section: 1.2.3</p> <p>This alert triggers when unauthorized outbound traffic from the Cardholder Data Environment to wireless networks is detected.</p> <p>This alert is not configured by default.</p>

## Requirement 2 Alerts

The Logger PCI Requirement 2 alerts notify PCI analysts when default configuration parameters (such as default vendor accounts) are used.

The following devices are supported for Logger PCI Requirement 2 alerts:

- Network Equipment
- Firewall devices
- Operating System devices

Alert Name	Description
<b>PCI Requirement 2 - Default Account Usage Alert</b>	<p>This alert triggers when the source or destination account name matches one of the following default account names:</p> <p>admin, root&lt;space&gt;, sa&lt;space&gt;, nobody&lt;space&gt;, guest&lt;space&gt;, manager&lt;space&gt;, sys&lt;space&gt;, system&lt;space&gt;, oracle&lt;space&gt;, orcladmin&lt;space&gt;, cisco&lt;space&gt;, pixadmin&lt;space&gt;</p> <p>Where &lt;space&gt; 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 &lt;space&gt; character, for example the account name sa&lt;space&gt; does not match the string sarah</p> <p>This alert is not configured by default.</p> <p>Default <b>Match Count</b>: 1</p> <p>Default <b>Threshold (Sec)</b>: 1</p>
<b>PCI Requirement 2 - Databases in DMZ</b>	<p>PCI Section: 2.2.1</p> <p>This alert is triggered when a Database instance is found in the DMZ.</p>
<b>PCI Requirement 2 - Insecure Services Detected</b>	<p>PCI Section: 2.2.3</p> <p>This alert triggers when an insecure service, such as ftp, tftp, telnet, pop3, or NetBIOS is identified.</p>

Alert Name	Description
<b>PCI Requirement 2 - Misconfiguration Detected</b>	PCI Section: 2.2.4 This alert triggers when a misconfiguration event is detected.
<b>PCI Requirement 2 - Unencrypted Administrative Access</b>	PCI Section: 2.3 This alert triggers when unencrypted administrative access is detected.
<b>PCI Requirement 2 - Insecure SSL Service Detected (Poodle Heartbleed OpenSSL Vulnerabilities)</b>	PCI Section: 2.2.3 This alert triggers when an insecure SSL Service (such as a Poodle, Heartbleed, or Open SSL vulnerability) is detected.

## Requirement 3 Alerts

Logger PCI Requirement 3 alerts notify PCI analysts when events occur that indicate credit card information is not encrypted.

The following devices are supported for Logger PCI Requirement 3 alerts:

- Anti-Virus
- Applications
- Content Security, Web Filtering
- Database
- Firewall
- Identity Management
- Intrusion Detection System
- Intrusion Prevention System
- Network Equipment
- Operating System
- Vulnerability Assessment
- Wireless

Alert Name	Description
<b>PCI Requirement 3 - Credit Card Number in Clear Text Alert</b>	<p>This alert triggers when a credit card number appears in the logs as clear text, using one of the following formats:</p> <p>&lt;n&gt;&lt;n&gt;&lt;n&gt;&lt;n&gt;-&lt;n&gt;&lt;n&gt;&lt;n&gt;&lt;n&gt;-&lt;n&gt;&lt;n&gt;&lt;n&gt;&lt;n&gt;-&lt;n&gt;&lt;n&gt;&lt;n&gt;&lt;n&gt;</p> <p>&lt;n&gt;&lt;n&gt;&lt;n&gt;&lt;n&gt;-&lt;n&gt;&lt;n&gt;&lt;n&gt;&lt;n&gt;&lt;n&gt;-&lt;n&gt;&lt;n&gt;&lt;n&gt;&lt;n&gt;</p> <p>&lt;n&gt;&lt;n&gt;&lt;n&gt;&lt;n&gt;-&lt;n&gt;&lt;n&gt;&lt;n&gt;&lt;n&gt;&lt;n&gt;-&lt;n&gt;&lt;n&gt;&lt;n&gt;&lt;n&gt;&lt;n&gt;</p> <p>Where &lt;n&gt; is single numeric digit.</p> <p>This alert is not configured by default.</p> <p>Default <b>Match Count</b>: 1</p> <p>Default <b>Threshold (Sec)</b>: 300</p>
<b>PCI Requirement 3 - Credit Card Number in Clear Text (TippingPoint) - Updated Alert</b>	<p>This alert triggers when a TippingPoint UnityOne IPS reports that credit card information was sent in clear text.</p> <p>This alert is not configured by default.</p> <p>Default <b>Match Count</b>: 1</p> <p>Default <b>Threshold (Sec)</b>: 1</p>

Alert Name	Description
<b>PCI Requirement 3 - Credit Card Number in Clear Text (Juniper) Alert</b>	<p>This alert triggers when a Juniper Netscreen IDS reports that credit card information was sent in clear text using HTTP.</p> <p>This alert is not configured by default.</p> <p>Default <b>Match Count</b>: 1</p> <p>Default <b>Threshold (Sec)</b>: 1</p>
<b>PCI Requirement 3 - Credit Card Number in Clear Text (Reconnex) Alert</b>	<p>This alert triggers when a Reconnex information monitoring system reports that credit card information was sent in clear text.</p> <p>This alert is not configured by default.</p> <p>Default <b>Match Count</b>: 1</p> <p>Default <b>Threshold (Sec)</b>: 1</p>
<b>PCI Requirement 3 - Credit Card Number in Clear Text (Vericept) Alert</b>	<p>This alert triggers when a Vericept information monitoring system reports that credit card information was sent in clear text.</p> <p>This alert is not configured by default.</p> <p>Default <b>Match Count</b>: 1</p> <p>Default <b>Threshold (Sec)</b>: 1</p>
<b>PCI Requirement 3 - Credit Card Number in Clear Text (Vontu) Alert</b>	<p>This alert triggers when a Vontu information monitoring system reports that credit card information was sent in clear text.</p> <p>This alert is not configured by default.</p> <p>Default <b>Match Count</b>: 1</p> <p>Default <b>Threshold (Sec)</b>: 1</p>
<b>PCI Requirement 3 – Credit Card Number in Clear Text (General)</b>	<p>PCI Section: 3.3</p> <p>This alert triggers when a credit card number appears in logs as clear text using one of the following formats:</p> <ul style="list-style-type: none"> <li>Visa</li> <li>MasterCard</li> <li>American Express</li> <li>Discover</li> <li>Diner's club</li> <li>JCB</li> </ul>
<b>PCI Requirement 3 – Credit Card Number in Clear Text (Snort)</b>	<p>PCI Section: 3.3</p> <p>This alert triggers when Snort IDS reports that credit card information was sent in clear text.</p>

## Requirement 4 Alerts

Logger PCI Requirement 4 alerts notify PCI analysts when events occur that indicate use of non-secure protocols or ports.

The following devices are supported for Logger PCI Requirement 4 alerts:

- Database
- Network Equipment

Alert Name	Description
<b>PCI Requirement 4 - Internal Systems Running Insecure Services Alert</b>	<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. The following services are defined as insecure: telnet, ftpd, rexec, pop3, rsh, imapd.</p> <p>An insecure port is a port number that is commonly used by an insecure service. The following ports are defined as insecure: 20, 21, 25, 110, 143, 23</p> <p>According to PCI Data Security Standard (DSS), use of such services has to be justified and cannot be used to transmit cardholder or sensitive information.</p> <p>This alert is not configured by default.</p> <p>Default <b>Match Count</b>: 1</p> <p>Default <b>Threshold (Sec)</b>: 300</p>
<b>PCI Requirement 4 - Internal Systems Using Insecure Public Services Alert</b>	<p>This alert triggers when internal systems are using public insecure services or ports available on the Internet. The following 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 insecure service. The following ports are defined as insecure: 20, 21, 25, 110, 143, 23.</p> <p>According to PCI Data Security Standard (DSS), use of such services has to be justified and cannot be used to transmit cardholder or sensitive information.</p> <p>This alert is not configured by default.</p> <p>Default <b>Match Count</b>: 1</p> <p>Default <b>Threshold (Sec)</b>: 300</p>
<b>PCI Requirement 4 - Misconfigured Wireless Devices</b>	<p>PCI Section: 4.11</p> <p>This alert triggers when a misconfigured wireless device is detected.</p>

## Requirement 5 Alerts

Logger PCI Requirement 5 alerts notify PCI analysts when events occur that indicate systems are infected with viruses.

The following devices are supported for Logger PCI Requirement 5 alerts:

- Anti-Virus

Alert Name	Description
<b>PCI Requirement 5 - Failed Virus Quarantine or Clean or Deletion Alert</b>	<p>This alert triggers when anti-virus software is not able to quarantine, clean or delete virus files. When notified, PCI analysts should quickly investigate this issue.</p> <p>This alert is not configured by default.</p> <p>Default <b>Match Count</b>: 1</p> <p>Default <b>Threshold (Sec)</b>: 1</p>
<b>PCI Requirement 5 - Network Traffic matching a Virus Signature is Detected Alert</b>	<p>This alert triggers when an IDS detected network traffic that matches a virus signature.</p> <p>This alert is not configured by default.</p> <p>Default <b>Match Count</b>: 1</p> <p>Default <b>Threshold (Sec)</b>: 1</p>
<b>PCI Requirement 5 - Successful Virus Quarantine or Clean or Deletion Alert</b>	<p>This alert triggers when anti-virus software quarantined, cleaned or deleted virus files.</p> <p>This alert is not configured by default.</p> <p>Default <b>Match Count</b>: 1</p> <p>Default <b>Threshold (Sec)</b>: 1</p>
<b>PCI Requirement 5 - Virus Discovered Alert</b>	<p>This alert triggers when anti-virus software discovered a virus on a machine.</p> <p>This alert is not configured by default.</p> <p>Default <b>Match Count</b>: 1</p> <p>Default <b>Threshold (Sec)</b>: 1</p>
<b>PCI Requirement 5 – Anti Virus Disabled</b>	<p>PCI Section: 5.3</p> <p>This alert triggers when an anti-virus disabled action is detected.</p>
<b>PCI Requirement 5 – Anti Virus Failed Update</b>	<p>PCI Section: 5.2</p> <p>This alert triggers when a failed anti-virus update event is detected.</p>



## Requirement 6 Alerts

Logger PCI Requirement 6 alerts notify PCI analysts when events occur that indicate excessive numbers of unsuccessful changes to applications and operating systems have been attempted.

The following devices are supported for Logger PCI Requirement 6 alerts:

- Applications
- Anti-Virus
- Content Web
- Firewall
- Database
- Identity Management
- Intrusion Detection System
- Intrusion Prevention System
- Operating System
- Policy Management
- Virtual Private Network

Alert Name	Description
<b>PCI Requirement 6 - Excessive Failed Application Level Changes Alert</b>	<p>This alert triggers when an excessive number of unsuccessful changes to applications are attempted.</p> <p>This alert is not configured by default.</p> <p>Default <b>Match Count</b>: 30</p> <p>Default <b>Threshold (Sec)</b>: 300</p>
<b>PCI Requirement 6 - Excessive Failed Operating System Changes Alert</b>	<p>This alert triggers when an excessive number of unsuccessful changes to operating systems are attempted.</p> <p>This alert is not configured by default.</p> <p>Default <b>Match Count</b>: 30</p> <p>Default <b>Threshold (Sec)</b>: 300</p>
<b>PCI Requirement 6 - Broken Authentication and Session Management Detected</b>	<p>PCI Section: 6.5.10</p> <p>This alert triggers when a Broken Authentication and Session Management vulnerability is detected.</p>
<b>PCI Requirement 6 - Cross Site Request Forgery Detected</b>	<p>PCI Section: 6.5.9</p> <p>This alert triggers when a Cross Site Request Forgery vulnerability is detected.</p>

Alert Name	Description
<b>PCI Requirement 6 - Cross Site Scripting Detected</b>	PCI Section: 6.5.7  This alert triggers when a Cross Site Scripting vulnerability is detected.
<b>PCI Requirement 6 - Custom Account Detected</b>	PCI Section: 6.3.1  This alert triggers when a custom account is detected.
<b>PCI Requirement 6 - Improper Access Control Detected</b>	PCI Section: 6.5.8  This alert triggers when improper access control is detected.
<b>PCI Requirement 6 - Improper Error Handling Detected</b>	PCI Section: 6.5.5  This alert triggers when improper error handling is detected.
<b>PCI Requirement 6 - Injection Flaw Detected</b>	PCI Section: 6.5.1  This alert triggers when an Injection Flaw vulnerability is detected.
<b>PCI Requirement 6 -Insecure Communications Detected</b>	PCI Section: 6.5.4  This alert triggers when insecure communications are detected.
<b>PCI Requirement 6 - Insecure Cryptographic Storage Detected</b>	PCI Section: 6.5.3  This alert triggers when an Insecure Cryptographic Storage event is detected.
<b>PCI Requirement 6 - Security Patch Missing</b>	PCI Section: 6.2  This alert triggers when a Missing Security Patch event is detected.
<b>PCI Requirement 6 - Vulnerability with CVSS SCORE Larger or Equal to 4</b>	PCI Section: 6.5.6  This alert triggers when a vulnerability with a CVSS score of 4 or higher is detected.
<b>PCI Requirement 6 - Vulnerability with High Severity Detected</b>	PCI Section: 6.5.6  This alert triggers when a vulnerability with a high score is detected.

## Requirement 7 Alerts

Logger PCI Requirement 7 alerts

Alert Name	Description
<b>PCI Requirement 7- Unauthorized Access to CDE Detected</b>	PCI Section: 6.5.6  This alert triggers when an unauthorized user tries to access the Cardholder Data Environment.

## Requirement 8 Alerts

Logger PCI Requirement 8 alerts

Alert Name	Description
<b>PCI Requirement 8 - Anonymous User Activity</b>	PCI Section: 8.1.1  This alert triggers when anonymous user activity is detected in the Cardholder Data Environment.
<b>PCI Requirement 8 - Clear Text Password Transmission</b>	PCI Section: 8.2.1  This alert triggers when a clear text password transmission is detected on a web application.

## Requirement 9 Alerts

Logger PCI Requirement 9 alerts notify PCI analysts when events occur that indicate too many failed access, creation or modification attempts have occurred to a physical access system such as a badge reader.

The following devices are supported for Logger PCI Requirement 9 alerts:

- Physical Security Systems

Alert Name	Description
<b>PCI Requirement 9 - Excessive Failed Physical System Access Attempts Alert</b>	<p>This alert triggers when too many failed access attempts to a physical access system occur.</p> <p>This alert is not configured by default.</p> <p>Default <b>Match Count</b>: 20</p> <p>Default <b>Threshold (Sec)</b>: 300</p>
<b>PCI Requirement 9 - Excessive Failed Physical System Account Creation or Modification Alert</b>	<p>This alert triggers when too many failed attempts to create or modify an account on a physical access system occur.</p> <p>This alert is not configured by default.</p> <p>Default <b>Match Count</b>: 5</p> <p>Default <b>Threshold (Sec)</b>: 300</p>

## Requirement 10 Alerts

Logger PCI Requirement 10 alerts notify PCI analysts when events occur that indicate failed log-ins or access to resources, user authentications and authorizations, audit log management and audit trails, and clock synchronization.

The following devices are supported for Logger PCI Requirement 10 alerts:

- Anti-Virus
- Applications
- Content Security, Web Filtering
- Database
- Firewall
- Identity Management
- Intrusion Detection System
- Intrusion Prevention System
- Network Equipment
- Operating System
- Physical Security Systems
- Policy Management
- Virtual Private Network
- Virtual Private Network
- Vulnerability Assessment
- Wireless

Alert Name	Description
<b>PCI Requirement 10 - Device Clock Synchronization Problems Alert</b>	<p>This alert triggers when ArcSight SmartConnectors are reporting source events with an incorrect time stamp.</p> <p>This alert <b>is</b> disabled by default.</p> <p>Default <b>Match Count</b>: 20</p> <p>Default <b>Threshold (Sec)</b>: 300</p>
<b>PCI Requirement 10 - Excessive Failed Account Creations Alert</b>	<p>This alert triggers when an excessive number of unsuccessful attempts to create computer accounts occur.</p> <p>This alert is not configured by default.</p> <p>Default <b>Match Count</b>: 3</p> <p>Default <b>Threshold (Sec)</b>: 300</p>

Alert Name	Description
<b>PCI Requirement 10 - Excessive Failed Account Deletions Alert</b>	<p>This alert triggers when an excessive number of unsuccessful attempts to delete computer accounts occur.</p> <p>This alert is not configured by default.</p> <p>Default <b>Match Count</b>: 3</p> <p>Default <b>Threshold (Sec)</b>: 300</p>
<b>PCI Requirement 10 - Excessive Failed Account Modifications Alert</b>	<p>This alert triggers when an excessive number of unsuccessful attempts to modify computer accounts occur.</p> <p>This alert is not configured by default.</p> <p>Default <b>Match Count</b>: 3</p> <p>Default <b>Threshold (Sec)</b>: 300</p>
<b>PCI Requirement 10 - Excessive Failed Administrative Actions Alert</b>	<p>This alert triggers when an excessive number of failed actions occur by administrative user accounts.</p> <p>This alert <b>is</b> disabled by default.</p> <p>Default <b>Match Count</b>: 20</p> <p>Default <b>Threshold (Sec)</b>: 300</p>
<b>PCI Requirement 10 - Excessive Failed Administrative Logins Alert</b>	<p>This alert triggers when an excessive number of failed login attempts occur by administrative user accounts.</p> <p>This alert <b>is</b> disabled by default.</p> <p>Default <b>Match Count</b>: 3</p> <p>Default <b>Threshold (Sec)</b>: 300</p>
<b>PCI Requirement 10 - Excessive Failed Authorization Changes (Including Windows 2008) Alert</b>	<p>This alert triggers when an excessive number of failed attempts to change authorizations occur—such as changes to access lists.</p> <p>This alert is triggered for both Windows 2003 and Windows 2008 events.</p> <p>This alert is not configured by default.</p> <p>Default <b>Match Count</b>: 10</p> <p>Default <b>Threshold (Sec)</b>: 300</p>
<b>PCI Requirement 10 - Excessive Failed Database Access Alert</b>	<p>This alert triggers when an excessive number of unsuccessful database access attempts occur. Database access attempts can be logins or queries.</p> <p>This alert is not configured by default.</p> <p>Default <b>Match Count</b>: 10</p> <p>Default <b>Threshold (Sec)</b>: 300</p>

Alert Name	Description
<b>PCI Requirement 10 - Excessive Failed File Creations Alert</b>	<p>This alert triggers when an excessive number of unsuccessful attempts to create files occur.</p> <p>This alert is not configured by default.</p> <p>Default <b>Match Count</b>: 20</p> <p>Default <b>Threshold (Sec)</b>: 300</p>
<b>PCI Requirement 10 - Excessive Failed File Deletions Alert</b>	<p>This alert triggers when an excessive number of unsuccessful attempts to delete files occur.</p> <p>This alert is not configured by default.</p> <p>Default <b>Match Count</b>: 20</p> <p>Default <b>Threshold (Sec)</b>: 300</p>
<b>PCI Requirement 10 - Excessive Failed File Modifications Alert</b>	<p>This alert triggers when an excessive number of unsuccessful attempts to modify files occur.</p> <p>This alert is not configured by default.</p> <p>Default <b>Match Count</b>: 10</p> <p>Default <b>Threshold (Sec)</b>: 300</p>
<b>PCI Requirement 10 - Excessive Failed Resource Access Alert</b>	<p>This alert triggers when an excessive number of failed attempts to access resources occur. For example, an excessive number of failed attempts to create ssh tunnels occur.</p> <p>This alert is not configured by default.</p> <p>Default <b>Match Count</b>: 10</p> <p>Default <b>Threshold (Sec)</b>: 300</p>
<b>PCI Requirement 10 - Excessive Failed User Actions Alert</b>	<p>This alert triggers when an excessive number of failed actions occur by non-administrative user accounts. This alert is triggered for any accounts that are <i>not</i> listed as an administrative account in the alert.</p> <p>This alert is not configured by default.</p> <p>Default <b>Match Count</b>: 20</p> <p>Default <b>Threshold (Sec)</b>: 300</p>
<b>PCI Requirement 10 - Excessive Failed User Logins Alert</b>	<p>This alert triggers when an excessive number of failed login attempts occur by non-administrative user accounts. This alert is triggered for any accounts that are <i>not</i> listed as an administrative account in the alert.</p> <p>This alert is not configured by default.</p> <p>Default <b>Match Count</b>: 10</p> <p>Default <b>Threshold (Sec)</b>: 300</p>



Alert Name	Description
<b>PCI Requirement 10 - Excessive Successful Administrative Actions Alert</b>	<p>This alert triggers when an excessive number of successful actions by administrative user accounts occur.</p> <p>This alert <b>is</b> disabled by default.</p> <p>Default <b>Match Count</b>: 300</p> <p>Default <b>Threshold (Sec)</b>: 300</p>
<b>PCI Requirement 10 - Excessive Successful Administrative Logins Alert</b>	<p>This alert triggers when a large number of successful logins by administrative user accounts occur.</p> <p>This alert <b>is</b> not configured by default.</p> <p>Default <b>Match Count</b>: 10</p> <p>Default <b>Threshold (Sec)</b>: 300</p>
<b>CI Requirement 10 - Excessive Successful Authorization Changes (Including Windows 2008) Alert</b>	<p>This alert triggers when a large number of authorization changes occur—such as changes to access lists. The alert is triggered for both Windows 2003 and Windows 2008 events.</p> <p>This alert is not configured by default.</p> <p>Default <b>Match Count</b>: 100</p> <p>Default <b>Threshold (Sec)</b>: 300</p>
<b>PCI Requirement 10 - Excessive Successful Account Creations Alert</b>	<p>This alert triggers when a large number of computer accounts are successfully created.</p> <p>This alert is not configured by default.</p> <p>Default <b>Match Count</b>: 5</p> <p>Default <b>Threshold (Sec)</b>: 300</p>
<b>PCI Requirement 10 - Excessive Successful Account Deletions Alert</b>	<p>This alert triggers when a large number of computer accounts are successfully deleted.</p> <p>This alert is not configured by default.</p> <p>Default <b>Match Count</b>: 5</p> <p>Default <b>Threshold (Sec)</b>: 300</p>
<b>PCI Requirement 10 - Excessive Successful Account Modifications Alert</b>	<p>This alert triggers when a large number of computer accounts are successfully modified.</p> <p>This alert is not configured by default.</p> <p>Default <b>Match Count</b>: 5</p> <p>Default <b>Threshold (Sec)</b>: 300</p>

Alert Name	Description
<b>PCI Requirement 10 - Excessive Successful Database Access Alert</b>	<p>This alert triggers when a large number of successful database accesses are reported. Database access attempts can be logins or queries.</p> <p>This alert is not configured by default.</p> <p>Default <b>Match Count</b>: 100</p> <p>Default <b>Threshold (Sec)</b>: 300</p>
<b>PCI Requirement 10 - Excessive Successful File Creations Alert</b>	<p>This alert triggers when a large number of files are successfully deleted.</p> <p>This alert is not configured by default.</p> <p>Default <b>Match Count</b>: 500</p> <p>Default <b>Threshold (Sec)</b>: 300</p>
<b>PCI Requirement 10 - Excessive Successful File Deletions Alert</b>	<p>This alert triggers when a large number of files are successfully deleted.</p> <p>This alert is not configured by default.</p> <p>Default <b>Match Count</b>: 500</p> <p>Default <b>Threshold (Sec)</b>: 300</p>
<b>PCI Requirement 10 - Excessive Successful File Modifications Alert</b>	<p>This alert triggers when a large number of files are successfully modified.</p> <p>This alert is not configured by default.</p> <p>Default <b>Match Count</b>: 1000</p> <p>Default <b>Threshold (Sec)</b>: 300</p>
<b>PCI Requirement 10 - Excessive Successful Resource Access Alert</b>	<p>This alert triggers when a large number of successful resource access attempts occur. For example, the successful creation of an excessive number of ssh tunnels.</p> <p>This alert is not configured by default.</p> <p>Default <b>Match Count</b>: 50</p> <p>Default <b>Threshold (Sec)</b>: 300</p>
<b>PCI Requirement 10 - Excessive Successful User Actions Alert</b>	<p>This alert triggers when a large number of successful actions occur by non-administrative user accounts. This alert is triggered for any accounts that are <i>not</i> listed as an administrative account in the alert.</p> <p>This alert is not configured by default.</p> <p>Default <b>Match Count</b>: 2000</p> <p>Default <b>Threshold (Sec)</b>: 300</p>
<b>PCI Requirement 10 - Excessive Successful User Logins Alert</b>	<p>This alert triggers when a large number of successful logins by non-administrative user accounts occur. This alert is triggered for any accounts that are <i>not</i> listed as an administrative account in the alert.</p> <p>This alert is not configured by default.</p> <p>Default <b>Match Count</b>: 30</p> <p>Default <b>Threshold (Sec)</b>: 300</p>

Alert Name	Description
<b>PCI Requirement 10 - Microsoft Audit Log Cleared (including Windows 2008) Alert</b>	<p>This alert triggers when the Microsoft Audit Log is cleared.</p> <p>This alert is not configured by default.</p> <p>Default <b>Match Count</b>: 1</p> <p>Default <b>Threshold (Sec)</b>: 120</p>
<b>PCI Requirement 10 - Virtual Machine Down Alert</b>	<p>This alert triggers when a virtual machine is powered off or suspended.</p> <p>This alert is not configured by default.</p> <p>Default <b>Match Count</b>: 1</p> <p>Default <b>Threshold (Sec)</b>: 120</p>
<b>PCI Requirement 10 - Virtual Machine Modifications Alert</b>	<p>This alert triggers when virtual machine modifications occur (including deletions and relocations).</p> <p>This alert is not configured by default.</p> <p>Default <b>Match Count</b>: 1</p> <p>Default <b>Threshold (Sec)</b>: 120</p>
<b>PCI Requirement 10 - Virtual Machine Data Manipulations Alert</b>	<p>This alert triggers when manipulation of virtual machine data (images, snapshots, and so on) occurs.</p> <p>This alert is not configured by default.</p> <p>Default <b>Match Count</b>: 1</p> <p>Default <b>Threshold (Sec)</b>: 120</p>
<b>PCI Requirement 10 - Virtual Management System Alerts Alert</b>	<p>This alert triggers when alerts from virtualization management systems occur.</p> <p>This alert is not configured by default.</p> <p>Default <b>Match Count</b>: 1</p> <p>Default <b>Threshold (Sec)</b>: 120</p>
<b>PCI Requirement 10- Audit Log Cleared (General)</b>	<p>PCI Section: 10.2.6</p> <p>This alert triggers when an audit log is cleared.</p>

## Requirement 11 Alerts

Logger PCI Requirement 11 alerts notify PCI analysts when events occur that indicate suspicious behavior, hostile behavior, a compromise or vulnerabilities.

The following devices are supported for Logger PCI Requirement 11 alerts:

- Vulnerability Assessment

Alert Name	Description
<b>PCI Requirement 11 - Suspicious Events Alert</b>	<p>This alert triggers when there are events that are categorized as suspicious behavior, hostile behavior, or a compromise.</p> <p>This alert is not configured by default.</p> <p>Default <b>Match Count</b>: 30</p> <p>Default <b>Threshold (Sec)</b>: 300</p>
<b>PCI Requirement 11 - Vulnerabilities Alert</b>	<p>This alert triggers when more that 10 vulnerabilities are reported in less that 5 minutes.</p> <p>This alert is not configured by default.</p> <p>Default <b>Match Count</b>: 30</p> <p>Default <b>Threshold (Sec)</b>: 300</p>
<b>PCI Requirement 11 - Unauthorized Access Point Detected</b>	<p>PCI Section: 11.1</p> <p>This alert triggers when an unauthorized access point event is detected.</p>

## Requirement 12 Alerts

Logger PCI Requirement 12 alerts

Alert Name	Description
<b>PCI Requirement 12 - Shellshock Vulnerability Detected</b>	PCI Section: 12.3  This alert triggers when a Shellshock vulnerability is detected.

## PA-DSS Requirement 4 Alerts

The Logger PA-DSS Requirement 4 alerts notify PCI analysts of events that indicate problems with payment application activity.

The following devices are supported for Logger PA-DSS Requirement 4 alerts:

- Applications

See also: ["Configuring Alerts" on page 21](#).

Alert Name	Description
<b>PA-DSS 4 - Anonymous Payment Application Access to Cardholder Data Alert</b>	<p>This alert is triggered when an anonymous user attempts to access cardholder data via a payment application.</p> <p>This alert is not enabled by default.</p> <p>Default <b>Match Count</b>: 1</p> <p>Default <b>Threshold (Sec)</b>: 120</p>
<b>PA-DSS 4 - Consecutive Invalid Payment Application Access Attempts Alert</b>	<p>This alert is triggered when an anonymous user attempts to access cardholder data via a payment application.</p> <p>This alert is not enabled by default.</p> <p>Default <b>Match Count</b>: 7</p> <p>Default <b>Threshold (Sec)</b>: 60</p>
<b>PA-DSS 4 - Payment Application Access to Cardholder Data with no User Name Alert</b>	<p>This alert is triggered when an event indicates access to cardholder data via a payment application but the event contains no username.</p> <p>This alert is not enabled by default.</p> <p>Default <b>Match Count</b>: 1</p> <p>Default <b>Threshold (Sec)</b>: 120</p>

Alert Name	Description
<b>PA-DSS 4 - Payment Application Access with Anonymous User Name Alert</b>	<p>This alert is triggered when an anonymous user attempts to access a payment application.</p> <p>This alert is not enabled by default.</p> <p>Default <b>Match Count</b>: 1</p> <p>Default <b>Threshold (Sec)</b>: 120</p>
<b>PA-DSS 4 - Payment Application Access with No User Name Alert</b>	<p>This alert is triggered when an event indicates access to a payment application but the event contains no username.</p> <p>This alert is not enabled by default.</p> <p>Default <b>Match Count</b>: 1</p> <p>Default <b>Threshold (Sec)</b>: 120</p>
<b>PA-DSS 4 - Payment Application Audit Log Initialized Alert</b>	<p>This alert is triggered when a payment application log has been initialized.</p> <p>This alert is not enabled by default.</p> <p>Default <b>Match Count</b>: 1</p> <p>Default <b>Threshold (Sec)</b>: 60</p>

# Chapter 5: PCI Reports by Category

The table below lists all the Logger PCI report categories by PCI Requirement. The PCI reports are described under each category in the following sections.

PCI Requirement	Report Category
<b>Requirement 1: Firewall Configuration</b>  Requirement 1 states that companies should install and maintain a firewall configuration that protects cardholder data.	<a href="#">Build and Maintain a Secure Network and Systems</a>
<b>Requirement 2: Default Security Parameters</b>  Newly deployed systems are often left with default configuration parameters enabled, such as default accounts and passwords. These can leave open known, easily exploitable vulnerabilities. Requirement 2 states that companies should not use vendor-supplied defaults for system passwords and other security parameters	<a href="#">Do not use vendor-supplied defaults for system passwords and other security parameters</a>
<b>Requirement 3: Protect Stored Cardholder Data</b>  Even if someone breaks through the outer defenses of your network, encrypted data is still unreadable, which makes encryption the ultimate protection mechanism. PCI requirement 3 provides guidelines for safeguarding encrypted data and its keys.  ArcSight specifically addresses section 3.3 of this requirement by recommending how certain security devices, such as network intrusion detection and prevention systems, can be set up to detect cardholder data that makes it to the wire, where it should not be.	<a href="#">Protect stored cardholder data</a>
<b>Requirement 4: Encrypted Transmissions</b>  Requirement 4 states that transmissions from cardholder systems to public networks should be encrypted across open, public networks.	<a href="#">Encrypt transmission of cardholder data across open public networks</a>



PCI Requirement	Report Category
<b>Requirement 5: Anti-Virus</b>  PCI requires that anti-virus software be used on PCI-governed systems and regularly maintained.	<a href="#">Protect all systems against malware and regularly update anti-virus software or programs</a>
<b>Requirement 6: System Applications</b>  Requirement 6 states that companies should develop and maintain secure systems and applications. This requirement is concerned with ensuring that you have adequate processes in place to maintain the security of your systems and applications. This includes maintaining the latest patch levels, vulnerability reports, in-house software security, change control procedures, and web application security.	<a href="#">Develop and maintain secure systems and applications</a>
<b>Requirement 7: Business Need-To-Know</b>  Requirement 7 states that access to critical cardholder data should be restricted only to users who have express authorization.	<a href="#">Restrict access to cardholder data by business need to know</a>
<b>Requirement 8: Unique User ID</b>  Requirement 8 states that each user with access to cardholder data systems has a unique user ID so that any actions taken on systems that affect cardholder data can be traced to known and authorized users.	<a href="#">Identify and authenticate access to system components</a>
<b>Requirement 9: Physical Access</b>  Requirement 9 states that companies should restrict physical access to cardholder data. This requirement ensures restricted physical access to data or systems that house cardholder data.  Most of the items in PCI Requirement 9 address safeguarding physical access to buildings and equipment, and maintaining control over access to paper and electronic media.	<a href="#">Restrict access to cardholder data by business need to know</a>

PCI Requirement	Report Category
<b>Requirement 10: Track and Monitor Data Access</b>  Requirement 10 states that companies should track and monitor all access to network resources and cardholder data. This requirement ensures that system activity logs adequately track, monitor, and test all access to network resources and cardholder data.	<a href="#">Track and monitor all access to network resources and cardholder data</a>
<b>Requirement 11: Test Systems and Networks</b>  Requirement 11 states that companies should regularly test security systems and processes.  New vulnerabilities are discovered every day. Requirement 11 focuses on regular monitoring and testing practices to keep up with these changes over time.	<a href="#">Regularly test security systems and processes</a>
<b>Requirement 12: Maintain an Information Security Policy</b>  Requirement 12 states that companies should maintain a policy that addresses information security for employees and contractors. This requirement ensures an information security policy and procedures that enable employees and contractors to uphold their responsibility in protecting sensitive cardholder data.	<a href="#">Maintain a policy that addresses information security for all personnel</a>
<b>PA-DSS Requirement 4: Log Payment Application Activity</b>  PA-DSS Requirement 4 states that companies should log all payment application activity.	<a href="#">PA-DSS</a>

## Build and Maintain a Secure Network and Systems

The Build and Maintain a Secure Network and Systems category is located under the following path.

Payment Card Industry\Build and Maintain a Secure Network and Systems

The Build and Maintain a Secure Network and Systems category reports are listed in the following table.

## Build and Maintain a Secure Network and Systems

Report	Description	Drill Down	Parameters
Requirement 1-Cardholder Data within the DMZ	13.7 Place system components that store cardholder data (such as a database) in an internal network zone, segregated from the DMZ and other untrusted networks.	none	CDE_ZONES DMZ_ZONES
Requirement 1-Disclosed Private IP Addresses	13.8 Do not disclose private IP addresses and routing information to unauthorized parties.	none	PERIMETER_FIREWALL
Requirement 1-External to PCI System Activity - All	Section 13.3 - This report shows all external systems that are communicating directly with PCI systems. This traffic should be justified.	none	none
Requirement 1-External to PCI Systems on Disallowed Ports	Section 11.6/12.1 - This report shows all traffic from external sources to PCI systems that is not explicitly allowed based on commonly used ports. The list of ports should be configured within the query.	none	none
Requirement 1-Firewall Configuration Changes	Section 11.7 / 11.2 - This report shows all firewall configuration changes.	none	none
Requirement 1-Internal IP Access from the Internet to the DMZ	Section 13.4 : Implement anti-spoofing easures to detect and block forged source IP addresses from entering the network.	none	PERIMETER_FIREWALL
Requirement 1-Network Equipment Configuration Changes	Section 11.7/6.4 - This report shows all PCI network equipment configuration changes, including changes to routers and switches.	none	none
Requirement 1-Open Ports by Device	Section 11.6 / 11.1 - This query finds all ports that were passed by a firewall, as well as the firewall rule number that it triggered.	none	none
Requirement 1-PCI Systems to External - All	Section 13.3/13.5/13.8 - This report shows PCI systems that are communicating with external systems. This traffic should be justified.	none	none
Requirement 1-Personal Firewall Installed	1.4 Install personal firewall software on any mobile and/or employee-owned devices that connect to the Internet when outside the network	none	none
Requirement 1-Unauthorized Direct Inbound Traffic from Public IP Addresses to the CDE	Section 13.3 Do not allow any direct connections inbound or outbound for traffic between the Internet and the cardholder data environment	none	CDE_ZONES
Requirement 1-Unauthorized Direct Outbound Traffic from the CDE to Public IP Addresses	Section 13.3 Do not allow any direct connections inbound or outbound for traffic between the Internet and the cardholder data environment	none	CDE_ZONES
Requirement 1-Unauthorized Inbound Traffic from Public IP Addresses	Section 13.2 : unauthorized inbound traffic from public addresses	none	DMZ_ZONES

### Build and Maintain a Secure Network and Systems, continued

Report	Description	Drill Down	Parameters
Requirement 1-Unauthorized Inbound Traffic from Public IP Addresses to the DMZ	Section 1.3.1: unauthorized inbound traffic from public addresses to DMZ	none	DMZ_ZONES  DMZ_ALLOWED_PORTS
Requirement 1-Unauthorized Inbound Traffic from Wireless Networks to the CDE	Section 1.2.3 : unauthorized Inbound traffic from wireless networks to card holder data	none	CDE_ALLOWED_PORTS  CDE_ZONES  WIRELESS_ZONES
Requirement 1-Unauthorized Inbound Traffic to the CDE	Section 1.2.1: Unauthorized Inbound Traffic to the Cardholder Data Environment	none	CDE_ZONES  CDE_ALLOWED_PORTS
Requirement 1-Unauthorized Outbound Traffic from the CDE	Section 1.2.1: Unauthorized Outbound Traffic from the Cardholder Data Environment	none	CDE_ZONES  CDE_ALLOWED_PORTS
Requirement 1-Unauthorized Outbound Traffic from the CDE to Wireless Networks	Section 1.2.3 : unauthorized outbound traffic from card holder data to Wireless Networks	none	WIRELESS_ZONES  CDE_ZONES  CDE_ALLOWED_PORTS
Requirement 1-VPN Configuration Changes	Section 1.1.7/ 6.4 - This report shows all configuration changes made to PCI related VPN devices.	none	none

## Do not use vendor-supplied defaults for system passwords and other security parameters

The Do not use vendor-supplied defaults for system passwords and other security parameters category is located under the following path.

Payment Card Industry\Do not use vendor-supplied defaults for system passwords and other security parameters

The Do not use vendor-supplied defaults for system passwords and other security parameters category reports are listed in the following table.

**Do not use vendor-supplied defaults for system passwords and other security parameters**

Report	Description	Drill Down	Parameters
Requirement 2-Default Account Usage	Section 2.1/PA-DSS 3.1.1 - This report shows default account usage. To view or modify the default account names and vendors, see the "Default Account Usage" query.	none	none
Requirement 2-Insecure Services	Section 2.2.3 - list of insecure services used.	none	UNSECURED_PORTS UNSECURED_PROCESSES
Requirement 2-Misconfigured Systems	Section 2.2.4 - Configure system security parameters to prevent misuse.	none	none
Requirement 2-Multiple Functions Implemented on a Server	Section 2.2.1 - Implement only one primary function per server to prevent functions that require different security levels from co-existing on the same server. (For example, web servers, database servers, and DNS should be implemented on separate servers.)	none	none
Requirement 2-Unencrypted Administrative Access	Section 2.3/PA-DSS 12.1 - This query finds all the Unencrypted Administrative Accesses	none	pciAdminUsers

## Protect stored cardholder data

The Protect stored cardholder data category is located under the following path.

Payment Card Industry\Protect stored cardholder data

The Protect stored cardholder data category reports are listed in the following table.

**Protect stored cardholder data**

Report	Description	Drill Down	Parameters
Requirement 3-Credit Card Numbers in Clear Text	Section 3.3 - This report presents occasions of credit card transmission in clear text. It is based on IDS reports and information leakage prevention systems. The query should be customized with the appropriate event and/or identification information for your IDS and IPS systems.	none	none

## Encrypt transmission of cardholder data across open public networks

The Encrypt transmission of cardholder data across open public networks category is located under the following path.

Payment Card Industry\Encrypt transmission of cardholder data across open public networks

The Encrypt transmission of cardholder data across open public networks category reports are listed in the following table.

### Encrypt transmission of cardholder data across open public networks

Report	Description	Drill Down	Parameters
Requirement 4-Misconfigured Wireless Devices	4.1.1/PA-DSS 6.2 Ensure wireless networks transmitting cardholder data or connected to the cardholder data environment, use industry best practices (for example, IEEE 802.11i) to implement strong encryption for authentication and transmission.	none	none
Requirement 4-Outbound Unencrypted Services	Section 4.1 - This report shows systems (clients) that communicate with servers with an external address over unencrypted protocols and the number of such events recorded. An unencrypted protocol is defined as one of the following: 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	none
Requirement 4-PCI Systems Providing Unencrypted Services	Section 4.1 - This report shows PCI 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. A PCI system is defined as one with an internal IP address.	none	none

## Protect all systems against malware and regularly update anti-virus software or programs

The Protect all systems against malware and regularly update anti-virus software or programs category is located under the following path.

Payment Card Industry\Protect all systems against malware and regularly update anti-virus software or programs

The Protect all systems against malware and regularly update anti-virus software or programs category reports are listed in the following table.

**Protect all systems against malware and regularly update anti-virus software or programs**

Report	Description	Drill Down	Parameters
Requirement 5-Anti-Virus Disabled	Section 5.3 - This report shows all anti-virus disabled events as reported by Microsoft systems.	The Dest Host field drill downs to the <a href="#">"Requirement 5-Detailed Anti-Virus Report per Host"</a> below report.	none
Requirement 5-Anti-Virus Installed	5.1 Deploy anti-virus software on all systems commonly affected by malicious software (particularly personal computers and servers).	none	none
Requirement 5-Detailed Anti-Virus Report	Section 5.1.1 - This report shows a detailed listing of anti-virus events (routine maintenance and remediation events) ordered accroding to zone, IP address and virus name.	The Dest Host field drill downs to the <a href="#">"Requirement 5-Detailed Anti-Virus Report per Host"</a> below report.  The Event Name field drill downs to the <a href="#">"Requirement 12-Event in Network"</a> on page 81 report.  This report drills down to itself.	none
Requirement 5-Detailed Anti-Virus Report per Host	Section 5.1.1 - This report was designed as a drill-down report. This report shows a detailed listing of anti-virus events (routine maintenance and remediation events) for a specific host, ordered accroding to time.	The Dest Host field drill downs to the <a href="#">"Requirement 11-Vulnerabilities per Host - All"</a> on page 80 report.  The Event Name field drill downs to the <a href="#">"Requirement 12-Event in Network"</a> on page 81 report.  This report drills down to itself.	none
Requirement 5-Failed Anti-Virus Updates	Section 5.2 - This report shows when anti-virus software fails to retrieve its updates. Is shows the system on which it happened, the minute it happened, and how many failed updates occurred in that minute.	The Dest Host field drill downs to the <a href="#">"Requirement 5-Detailed Anti-Virus Report per Host"</a> above report.	none

### Protect all systems against malware and regularly update anti-virus software or programs, continued

Report	Description	Drill Down	Parameters
Requirement 5-Successful Anti-Virus Updates-Summary	Section 5.2 - This report shows the number of successful times anti-virus updates were performed, for each host in the selected time frame.	The Dest Host field drill downs to the <a href="#">"Requirement 5-Detailed Anti-Virus Report per Host" on the previous page</a> report.	none
Requirement 5-Virus Summary By Host	Section 5.11 - This report shows systems infected with viruses and the number of infections for each system.	The Dest Host field drill downs to the <a href="#">"Requirement 5-Detailed Anti-Virus Report per Host" on the previous page</a> report.	none
Requirement 5-Virus Summary By Virus	Section 5.11 - This report shows detected viruses on systems and the number of such detections, ordered by the viruses that were detected most times.	none	none

## Develop and maintain secure systems and applications

The Develop and maintain secure systems and applications category is located under the following path.

Payment Card Industry\Develop and maintain secure systems and applications

The Develop and maintain secure systems and applications category reports are listed in the following table.

### Develop and maintain secure systems and applications

Report	Description	Drill Down	Parameters
Requirement 6-All Configuration Changes to Virtualization Management Systems	Section 6.4.5 - This report shows all manipulations of virtual machine data via the audit logs of Virtualization Management Systems.	none	pciVirtualizationProducts
Requirement 6-All Configuration Modifications to Virtual Machines	Section 6.4.5 - This report shows all configuration modifications to virtual machines (VMs) that were reported by hypervisors.	none	pciVirtualizationProducts



### Develop and maintain secure systems and applications, continued

Report	Description	Drill Down	Parameters
Requirement 6- Application Modifications	Section 6.4/PA-DSS 5.3 - This report shows modifications made to application configuration files.	none	none
Requirement 6 - Broken authentication and session management	Section 6.5.10/PA-DSS 5.2.10 Broken authentication and session management	none	none
Requirement 6 - Buffer Overflows	Section 6.5.2/PA-DSS 5.2.2 Buffer overflows	none	none
Requirement 6 - Cross-site request forgery	Section 6.5.9/PA-DSS 5.2.9 Cross-site request forgery (CSRF)	none	none
Requirement 6 - Cross-site scripting	Section 6.5.7/PA-DSS 5.2.7 Cross-site scripting (XSS)	none	none
Requirement 6 - Custom Account Detected	Section 6.3.1 Remove development, test and/or custom application accounts, user IDs, and passwords before applications become active or are released to customers.	none	CUSTOM_ACCOUNTS DMZ_ZONES CDE_ZONES WIRELESS_ZONES
Requirement 6- Device Configuration Modifications	Section 6.4 - This report shows device configuration changes on network equipment, such as switches and routers.	none	none
Requirement 6 - High Risk Vulnerability Detected	Section 6.5.6/PA-DSS 5.2.6 All "high risk" vulnerabilities identified in the vulnerability identification process	none	none
Requirement 6 - Improper Access Control	Section 6.5.8/PA-DSS 5.2.8 Improper access control (such as insecure direct object references, failure to restrict URL access, directory traversal, and failure to restrict user access to functions).	none	none
Requirement 6 - Improper error handling	Section 6.5.5/PA-DSS 5.2.5 Improper error handling	none	none
Requirement 6 - Injection Flaws	Section 6.5.1/PA-DSS 5.2.1 Injection flaws, particularly SQL injection. Also consider OS Command Injection, LDAP and XPath injection flaws as well as other injection flaws.	none	none
Requirement 6 - Insecure communications	Section 6.5.4/PA-DSS 5.2.4 Insecure communications	none	none

### Develop and maintain secure systems and applications, continued

Report	Description	Drill Down	Parameters
Requirement 6 - Insecure cryptographic storage	Section 6.5.3/PA-DSS 5.2.3 Insecure cryptographic storage	none	none
Requirement 6- Operating System Changes	Section 6.4 - This report shows changes made to operating system configurations.	none	none
Requirement 6 - Security Patch Missing	Section 6.2 Ensure that all system components and software are protected from known vulnerabilities by installing applicable vendor-supplied security patches. Install critical security patches within one month of release	none	none


## Restrict access to cardholder data by business need to know

The Restrict access to cardholder data by business need to know category is located under the following path.

Payment Card Industry\Restrict access to cardholder data by business need to know

The Restrict access to cardholder data by business need to know category reports are listed in the following table.

### Restrict access to cardholder data by business need to know

Report	Description	Drill Down	Parameters
Requirement 7  Unauthorized Access to the CDE	Section 7.1 Limit access to system components and cardholder data to only those individuals whose job requires such access.	none	CDE_ AUTHORIZED_ USERS  CDE_ZONES
Requirement 7-Users Accessing CDE - All	Section 7.1 - This Report displays all users who accessed the Carholder Data Environment (CDE) and the last time they accessed it.	none	none

## Identify and authenticate access to system components

The Identify and authenticate access to system components category is located under the following path.

Payment Card Industry\Identify and authenticate access to system components

The Identify and authenticate access to system components category reports are listed in the following table.

### Identify and authenticate access to system components

Report	Description	Drill Down	Parameters
Requirement 8-Anonymous User Activity	Section 8.1.1\PA-DSS 3.1.3 Assign all users a unique ID before allowing them to access system components or cardholder data.	The Event Id field drill downs to the <a href="#">"General Event Info by ID" on page 85</a> report.  The Event Name field drill downs to the <a href="#">"General Event Info by Name" on page 85</a> report.	ANONYMOUS_ACCOUNTS  CDE_ZONES
Requirement 8-Clear Text Password Transmission	Section 8.2.1\PA-DSS 3.3 Using strong cryptography, render all authentication credentials (such as passwords/phrases) unreadable during transmission and storage on all system components.	none	none
Requirement 8-Inactive User Account Activity	Section 8.1.4 Remove/disable inactive user accounts at least every 90 days.	none	none
Requirement 8-Successful Password Changes	Section 8.2.4- This report shows which users have changed their passwords and when.	none	none
Requirement 8-Terminated User Activity	Section 8.1.3 Immediately revoke access for any terminated users.	none	none

### Identify and authenticate access to system components, continued

Report	Description	Drill Down	Parameters
Requirement 8- Unauthorized Direct Cardholder Database Access	Section 8.7 All access to any database containing cardholder data (including access by applications, administrators, and all other users) is restricted as follows:Only database administrators have the ability to directly access or query databases.	none	DATABASE_ADDRESSES  DATABASE_ADMIN_USERS
Requirement 8-Windows Account Lockouts by System	Section 8.1.6 - This report shows all account lockouts on Windows systems.	none	none
Requirement 8-Windows Account Lockouts by User	Section 8.1.6 - This report shows all the account lockouts on systems running Windows sorted by user account. It also displays the number of different systems that the user was locked out from and the total number of lockouts for each user.	none	none

## Restrict physical access to cardholder data

The Restrict physical access to cardholder data category is located under the following path.

Payment Card Industry\Restrict physical access to cardholder data

The Restrict physical access to cardholder data category reports are listed in the following table.

### Restrict physical access to cardholder data

Report	Description	Drill Down	Parameters
Requirement 9- Physical Access Event Reporting Devices	9.1.1 Use video cameras and/or access control mechanisms to monitor individual physical access to sensitive areas. Review collected data and correlate with other entries. Store for at least three months, unless otherwise restricted by law	The Device IP field drill downs to the <a href="#">"Events by Device" on page 85</a> report.	none
Requirement 9- Physical Access System Account Creation	Section 9.1 - Shows all new accounts added to physical access systems sorted by user name for the time period you specify when you run the report.	none	none

### Restrict physical access to cardholder data, continued

Report	Description	Drill Down	Parameters
Requirement 9-Physical Access System Account Deletion	Section 9.1 - Shows all deletions of accounts from physical access systems.	none	none
Requirement 9-Physical Access System Account Modification	Section 9.1 - Shows all modifications made to accounts on physical access systems.	none	none
Requirement 9-Physical Facility Access Attempts	Section 9.1 / 9.4 - This report shows all authentication verification events (badge-ins) involving physical access systems.	none	none

## Track and monitor all access to network resources and cardholder data

The Track and monitor all access to network resources and cardholder data category is located under the following path.

Payment Card Industry\Track and monitor all access to network resources and cardholder data

The Track and monitor all access to network resources and cardholder data category reports are listed in the following table.

### Track and monitor all access to network resources and cardholder data

Report	Description	Drill Down	Parameters
Requirement 10-Account Creation	Section 10.2.7 - This report shows user account creations on any type of system sorted by zone and time.	none	none
Requirement 10-Account Deletion	Section 10.2.7 - This report shows user account deletions from any type of system sorted by zone and time.	none	none

### Track and monitor all access to network resources and cardholder data, continued

Report	Description	Drill Down	Parameters
Requirement 10-Administrative Actions	Section 10.2.2 - This report shows all event names of actions involving the administrator user (except logins), sorted by device. It also shows the last time the event happened. Administrative users are defined as admin, administrator, root, superuser, super. The default administrator names should be modified according to the actual administrator user names in the site, in which case this report will show all administrative actions (except logins).	none	none
Requirement 10-Administrative Logins - All	Section 10.2.5 - This report shows all administrative logins to systems. It shows the system to which the login was attempted, the outcome of the attempt, the number of times the attempt happened, and the last time it happened. Administrative users are defined as admin, administrator, root, superuser, super. These administrative user names should be changed to the actual administrator names on site.	none	none
Requirement 10-Administrative Logins - Failed	Section 10.2.5 - This report shows all failed logins to systems performed by default administrative users. It shows the system to which the login was attempted, the number of times the attempt happened, and the last time it happened. Administrative users are defined as admin, administrator, root, superuser, super. The default administrative user names should be changed to the actual administrator names on site.	none	none
Requirement 10-Administrative Logins - Successful	Section 10.2.5 - This report shows all successful logins to systems performed by default administrative users. It shows the system to which the login was attempted, the number of times the attempt happened, and the last time it happened. Administrative users are defined as admin, administrator, root, superuser, super. The default administrative user names should be changed to the actual administrator names on site.	none	none
Requirement 10-All Detected Virtual Machine IP Addresses	Section 10.1 - This report shows the association between virtual machines and their IP addresses.	none	pciVirtualizationProducts
Requirement 10-All Detected Virtual Machine MAC Addresses	Section 10.1 - This report shows the association between virtual machines and their MAC addresses.	none	pciVirtualizationProducts

### Track and monitor all access to network resources and cardholder data, continued

Report	Description	Drill Down	Parameters
Requirement 10-All Hypervisors per Reporting Device	Section 10.1 - This report shows all hypervisors detected per reporting device.	none	pciVirtualizationProducts
Requirement 10-All Virtualization Infrastructure Events	Section 10.1 - This report shows all events from virtualization infrastructure systems.	none	pciVirtualizationProducts
Requirement 10-All Virtual Machine Creation and Deletion Events	Section 10.2.7 - This report shows details of all events that describe the creation and deletion of virtual machines.	none	pciVirtualizationProducts
Requirement 10-All Virtual Machine Data Manipulations	Section 10.2.7 - This report shows all manipulations of virtual machine data (images, snapshots, datastores etc.).	none	pciVirtualizationProducts
Requirement 10-Authorization Changes	Section 10.2.5/8.5.1 - This report shows authorization privilege changes made on systems and the number of times these events happened per host name.	none	none
Requirement 10-Clock Synchronization Problems	Section 10.4 - This report shows all ArcSight SmartConnectors that report inaccurate times. This might be an indication of clocks that are not synchronized with each other in the logging infrastructure and thus affect the credibility of data access reports.	none	none
Requirement 10-Database Access - All	Section 10.2.1 - This report shows all login attempts to all database systems.	none	none
Requirement 10-Database Access - Failed	Section 10.2.1 - This report shows all failed login attempts made to database systems.	none	none

### Track and monitor all access to network resources and cardholder data, continued

Report	Description	Drill Down	Parameters
Requirement 10-Detected Virtual Machines with their Hypervisors and Reporting Devices	Section 10.1 - This report shows all virtual machines that have been detected along with information about their respective hypervisors.	<p>The Hypervisor Address field drill downs to the <a href="#">"Requirement 10-Detected Virtual Machines with their Hypervisors and Reporting Devices"</a> above report.</p> <p>The Reporting Device Address field drill downs to the <a href="#">"Requirement 10-Detected Virtual Machines with their Hypervisors and Reporting Devices"</a> above report.</p> <p>This report drills down to itself.</p>	pciVirtualizationProducts
Requirement 10-Empty Origination of Event	Section 10.3.5/PA-DSS 4.3.5 Verify origination of event is included in log entries.	<p>The Event Id field drill downs to the <a href="#">"General Event Info by ID" on page 85</a> report.</p> <p>The Event Name field drill downs to the <a href="#">"General Event Info by Name" on page 85</a> report.</p>	none
Requirement 10-Events from External-Facing Technologies	Section 10.5.4 Write logs for external-facing technologies onto a secure, centralized, internal log server or media device.	<p>The Event Id field drill downs to the <a href="#">"General Event Info by ID" on page 85</a> report.</p> <p>The Event Name field drill downs to the <a href="#">"General Event Info by Name" on page 85</a> report.</p>	none



### Track and monitor all access to network resources and cardholder data, continued

Report	Description	Drill Down	Parameters
Requirement 10-File Creation Attempts	Section 10.5.5 - This report shows attempts to create files. It displays the machine on which the file creation attempt occurred, the outcome of the attempt, the user involved, the name of the file, and how many times the attempt happened.	none	none
Requirement 10-File Deletion Attempts	Section 10.5.5 - This report shows attempts to delete files. It displays the machine on which the deletion attempt occurred, the outcome of the attempt, the user involved, the name of the file, and how many times the attempt happened.	none	none
Requirement 10-File Manipulations - All	Section 10.5.5 - This report displays all attempts to access, modify or delete files. It is sorted according to zone/host, reporting device and time.	none	none
Requirement 10-File Modification Attempts	Section 10.5.5 - This report shows attempts to modify files. It displays the machine on which the file modification attempt occurred, the outcome of the attempt, the user involved, the name of the file, and how many times the attempt happened.	none	none
Requirement 10-Microsoft Audit Log Cleared	Section 10.5.2 / 10.5.5 / 10.2.6 - This report shows the clearing of windows audit logs, which should usually not be done and could indicate a security problem.	none	none
Requirement 10-Number of Hypervisors Detected per Reporting Device	Section 10.1 - This report shows the number of detected hypervisors per reporting device.	The Hypervisors field drills down to the <a href="#">"Requirement 10-All Hypervisors per Reporting Device" on page 71</a> report.	pciVirtualizationProducts
Requirement 10-Number of Virtual Machines by Reporting Device and Hypervisor	Section 10.1 - This report shows the detected number of virtual machines by their respective hypervisors and reporting devices.	The Virtual Machines field drill downs to the <a href="#">"Requirement 10-Detected Virtual Machines with their Hypervisors and Reporting Devices" on page 72</a> report.  This report drills down to itself.	pciVirtualizationProducts

**Track and monitor all access to network resources and cardholder data, continued**

Report	Description	Drill Down	Parameters
Requirement 10-Resource Access - Failed	Section 10.2.4\PA-DSS 4.2.4 - This report shows failed attempts to access resources systems (except for failed logins which are shown in a separate report) that happened in the report time frame, the number of times these failures occurred, and the last time they occurred. The report is sorted by zone, host and time.	none	none
Requirement 10-Top Hypervisors with the Most VM Activities	Section 10.1 - This report shows the top 10 virtualization hypervisors with the most virtual machine activities (power on, power off, suspension etc.).	none	pciVirtualizationProducts
Requirement 10-Top Hypervisors with the Most VM Creations	Section 10.2.7 - This report shows the top 10 virtualization hypervisors with the most virtual machine creations.	none	pciVirtualizationProducts
Requirement 10-Top Users with the Most VM Activities	Section 10.1 - This report shows the top 10 users with the most virtual machine activities (power on, power off, suspension etc.).	none	pciVirtualizationProducts
Requirement 10-User Logins - All	Section 10.2.1 - This report shows all non-administrative users who attempted to log into a system. The report is sorted first by zone and then by time. A non-administrative user is one whose user name is not Admin, Administrator, root, superuser, or super. This list should be changed according to the actual administrative names on site.	none	none
Requirement 10-User Logins - Failed	Section 10.2.1 - This report shows all failed non-administrative user logins. The report is sorted first by zone and then by time. A non-administrative user is one whose user name is not Admin, Administrator, root, superuser, or super. These names should be changed according to the actual administrative user names on site.	none	none
Requirement 10-User Logins - Successful	Section 10.2.1 - Section 10.2.1 - This report shows all successful non-administrative user logins. The report is sorted first by zone and then by time. A non-administrative user is one whose user name is not Admin, Administrator, root, superuser, or super. This list should be changed according to the actual user names on site.	none	none

## Regularly test security systems and processes

The Regularly test security systems and processes category is located under the following path.

Payment Card Industry\Regularly test security systems and processes

The Regularly test security systems and processes category reports are listed in the following table.

### Regularly test security systems and processes

Report	Description	Drill Down	Parameters
Requirement 11-All Vulnerabilities by Assets	Section 11.2 - This report shows all vulnerabilities on systems as reported by vulnerability scanners. The report is ordered by zone, host name, scanning device and criticality. By default, the report will show up to 10,000 assets.	<p>The Dest Host field drill downs to the <a href="#">"Requirement 11-Vulnerabilities per Host - All" on page 80</a> report.</p> <p>The Event Name field drill downs to the <a href="#">"Requirement 11-Vulnerability in Network" on page 80</a> report.</p> <p>This report drills down to itself.</p>	none
Requirement 11-Attack in Network	Section 11.4 - This report was designed as a drill-down report. This report shows all the hosts on the network that were targeted by a specific attack or suspicious event, and the number of times the event targeted the host. Attacks and suspicious events are defined by the categorySignificance field.	<p>The Dest Host field drill downs to the <a href="#">"Requirement 11-Attacks and Suspicious Events per Host" on the next page</a> report.</p> <p>The Count field drill downs to the <a href="#">"Requirement 11-Attack on Host - Detail" below</a> report.</p> <p>This report drills down to itself.</p>	none

### Regularly test security systems and processes, continued

Report	Description	Drill Down	Parameters
Requirement 11-Attack on Host - Detail	Section 11.5 - This report was designed as a drill-down report. This report details in what time a specific attack or suspicious event targeted a specific host. Attacks and suspicious events are defined by the categorySignificance field.	<p>The Dest Host field drill downs to the <a href="#">"Requirement 11-Attacks on Host - All" on page 78</a> report.</p> <p>The Event Name field drill downs to the <a href="#">"Requirement 11-Attack in Network" above</a> report.</p> <p>This report drills down to itself.</p>	none
Requirement 11-Attacks and Suspicious Events Overview	Section 11.4/11.5 - This report shows attacks and suspicious events that target PCI systems in the network. Attacks and suspicious events are defined by the categorySignificance field.	<p>The Dest Host field drill downs to the <a href="#">"Requirement 11-Attacks on Host - All" on the next page</a> report.</p> <p>The Count field drill downs to the <a href="#">"Requirement 11-Attacks and Suspicious Events per Host" below</a> report.</p> <p>This report drills down to itself.</p>	none
Requirement 11-Attacks and Suspicious Events per Host	Section 11.5 - This report shows attacks and suspicious events that target a specific PCI Host. Attacks and suspicious events are defined by the categorySignificance field.	<p>The Dest Host field drill downs to the <a href="#">"Requirement 11-Attacks on Host - All" on the next page</a> report.</p> <p>The Event Name field drill downs to the <a href="#">"Requirement 11-Attack in Network" on the previous page</a> report.</p> <p>The Count field drill downs to the <a href="#">"Requirement 11-Attack on Host - Detail" on the previous page</a> report.</p> <p>This report drills down to itself.</p>	none

### Regularly test security systems and processes, continued

Report	Description	Drill Down	Parameters
Requirement 11-Attacks on Host - All	Section 11.5 - This report was designed as a drill-down report. This report details all attacks and suspicious activities that targeted a specific host. Attacks and suspicious events are defined by the categorySignificance field.	<p>The Dest Host field drill downs to the <a href="#">"Requirement 12-Host Event Count" on page 81</a> report.</p> <p>The Event Name field drill downs to the <a href="#">"Requirement 11-Attack in Network" on page 76</a> report.</p> <p>The Device Product field drill downs to the <a href="#">"Requirement 12-Device to Host Event Count" on page 81</a> report.</p> <p>This report drills down to itself.</p>	none
Requirement 11-HIDS Event Review by Device	Section 11.5 - This report shows all events that were triggered on HIDS systems and the number of times each event occurred.	none	none
Requirement 11-NIDS Event Review by Device	Section 11.4 - This report shows the number of different events that were triggered on NIDS systems. The report is sorted by device.	none	none
Requirement 11-Top 20 Vulnerabilities	Section 11.2.a - This report shows the 20 most common vulnerabilities on systems, the number of systems on which they are found, and additional information regarding the vulnerability.	none	none

### Regularly test security systems and processes, continued

Report	Description	Drill Down	Parameters
Requirement 11-Top 20 Vulnerable Assets	Section 11.2.a - This report shows the 20 systems with the most vulnerabilities as reported by vulnerability scanners.	<p>The Dest Host field drill downs to the <a href="#">"Requirement 11-Vulnerabilities per Host - All" on the next page</a> report.</p> <p>The Num of Scanners field drill downs to the <a href="#">"Requirement 11-Vulnerability Count per Scanner" on the next page</a> report.</p> <p>This report drills down to itself.</p>	none
Requirement 11-Unauthorized Access Point Detected	Section 11.1 Implement processes to test for the presence of wireless access points (802.11), and detect and identify all authorized and unauthorized wireless access points on a quarterly basis.	none	none
Requirement 11-Vulnerabilities on Host per Scanner	Section 11.2 - This report was designed as a drill-down report. This report shows all the vulnerabilities on a host for a specific scanner.	<p>The Dest Host field drill downs to the <a href="#">"Requirement 11-Vulnerabilities per Host - All" on the next page</a> report.</p> <p>The Vulnerability field drill downs to the <a href="#">"Requirement 11-Vulnerability in Network" on the next page</a> report.</p> <p>This report drills down to itself.</p>	none

### Regularly test security systems and processes, continued

Report	Description	Drill Down	Parameters
Requirement 11- Vulnerabilities per Host - All	Section 11.2 - This report was designed as a drill-down report. This report shows all the vulnerabilities for a certain host name.	<p>The Dest Host field drill downs to the <a href="#">"Requirement 12-Host Event Count" on the next page</a> report.</p> <p>The Vulnerability field drill downs to the <a href="#">"Requirement 11-Vulnerability in Network" below</a> report.</p> <p>This report drills down to itself.</p>	none
Requirement 11- Vulnerability Count per Scanner	Section 11.2 - This report was designed as a drill-down report. This report shows the number of vulnerabilities found by each scanner that scanned the host.	The Count field drill downs to the <a href="#">"Requirement 11-Vulnerabilities on Host per Scanner" on the previous page</a> report.	none
Requirement 11- Vulnerability in Network	Section 11.2 - This report was designed as a drill-down report. This report shows all the hosts with the selected vulnerability.	<p>The Dest Host field drill downs to the <a href="#">"Requirement 11-Vulnerabilities per Host - All" above</a> report.</p> <p>This report drills down to itself.</p>	none

## Maintain a policy that addresses information security for all personnel

The Maintain a policy that addresses information security for all personnel category is located under the following path.

Payment Card Industry\Maintain a policy that addresses information security for all personnel

The Maintain a policy that addresses information security for all personnel category reports are listed in the following table.

### Maintain a policy that addresses information security for all personnel

Report	Description	Drill Down	Parameters
Requirement 12-All Reporting Devices	Section 12.10.3 - This report shows all devices that report into Logger sorted by Device Vendor, Product, zone, and IP. It also shows the last time an event from the device was received. This can be used for inventory purposes.	The Device Product field drill downs to the <a href="#">"Requirement 12-Device to Host Event Count"</a> below report.	none
Requirement 12-Device to Host Event Count	Section 12.10.3 - This report was designed as a drill-down report. This report shows the number of events per Host that a specific device reported.	The Dest Host field drill downs to the <a href="#">"Requirement 12-Host Event Count"</a> below report.  The Count field drill downs to the <a href="#">"Requirement 12-Device to Host Event Detail"</a> below report.  This report drills down to itself.	none
Requirement 12-Device to Host Event Detail	Section 12.10.3 - This report was designed as a drill-down report. This report shows all the events from a specific device that targeted a specific host.	The Dest Host field drill downs to the <a href="#">"Requirement 12-Host Event Count"</a> below report.  This report drills down to itself.	none
Requirement 12-Event in Network	Section 12.10.3 - This report was designed as a drill-down report. This report shows the hosts that were targeted by a specific event and the number of times they were targeted.	The Dest Host field drill downs to the <a href="#">"Requirement 12-Host Event Count"</a> below report.  This report drills down to itself.	none
Requirement 12-Host Event Count	Section 12.10.3 - This report was designed as a drill-down report. This report shows the number of events different events that targeted a specific host.	The Event Name field drill downs to the <a href="#">"Requirement 12-Event in Network"</a> above report.  This report drills down to itself.	none

## PA-DSS

The PA-DSS category is located under the following path.

Payment Card Industry\PA-DSS

The PA-DSS category reports are listed in the following table.



## PA-DSS

Report	Description	Drill Down	Parameters
Mapping between PA-DSS Requirements and PCI-DSS Reports	Mapping between PA-DSS Requirements and PCI-DSS reports	none	none
PA-DSS 4-All Administrative Actions in Payment Applications	Section 4.2.2 - This report displays details of all actions taken by administrative users in payment applications.	none	pciPaymentApplication pciAdminUsers
PA-DSS 4-Anonymous Access to Payment Application	Section 4.1.a - This report identifies access events to payment applications in which no user name appears.	none	pciPaymentApplication
PA-DSS 4-Anonymous Payment Application Access to Cardholder Data	Section 4.2.1 - This report shows events indicating access of payment applications to cardholder systems without proper identification of the user who is accessing the data. This is a violation of the PA-DSS.	none	pciPaymentApplication
PA-DSS 4-Creations and Deletions of Payment Application Objects	Section 4.2.7 - This report shows events indicating creations and deletions of payment application objects.	none	pciPaymentApplication
PA-DSS 4-Details of Invalid Payment Application Access Attempts	Section 4.2.4 - This report shows details of invalid access events to payment applications.	none	pciPaymentApplication
PA-DSS 4-Individual Access to Payment Applications	Section 4.1.a - This report shows events indicating successful individual access to payment applications.	none	pciPaymentApplication

## PA-DSS, continued

Report	Description	Drill Down	Parameters
PA-DSS 4-Insufficient Audit Trail in Payment Application Events	Section 4.3 - This report displays payment application events with insufficient information, as defined in the PA-DSS. It is intended to help resolve these issues.	<p>The Device Product field drill downs to the <a href="#">"PA-DSS 4-Insufficient Audit Trail in Payment Application Events" above</a> report.</p> <p>This report drills down to itself.</p>	pciPaymentApplication
PA-DSS 4-Summary of Administrative Actions in Payment Applications	Section 4.2.2 - This report displays a summary of all actions taken by administrative users in payment applications.	<p>The Source User field drill downs to the <a href="#">"PA-DSS 4-All Administrative Actions in Payment Applications" on the previous page</a> report.</p> <p>The Destination User field drill downs to the <a href="#">"PA-DSS 4-All Administrative Actions in Payment Applications" on the previous page</a> report.</p>	pciPaymentApplication pciAdminUsers

## PA-DSS, continued

Report	Description	Drill Down	Parameters
PA-DSS 4-Summary of Invalid Payment Application Access Attempts	Section 4.2.4 - This report shows a summary of invalid access events to payment applications.	<p>The Source User field drill downs to the <a href="#">"PA-DSS 4-Details of Invalid Payment Application Access Attempts" on page 82</a> report.</p> <p>The Destination User field drill downs to the <a href="#">"PA-DSS 4-Details of Invalid Payment Application Access Attempts" on page 82</a> report.</p> <p>The Device Product field drill downs to the <a href="#">"PA-DSS 4-Details of Invalid Payment Application Access Attempts" on page 82</a> report.</p> <p>The Device Address field drill downs to the <a href="#">"PA-DSS 4-Details of Invalid Payment Application Access Attempts" on page 82</a> report.</p>	pciPaymentApplication
PA-DSS 4-Summary of Payment Applications with Insufficient Audit Trail	Section 4.3 - This report displays the number of events with insufficient audit trail entries per payment application.	<p>The Device Product field drill downs to the <a href="#">"PA-DSS 4-Insufficient Audit Trail in Payment Application Events" on the previous page</a> report.</p> <p>This report drills down to itself.</p>	pciPaymentApplication

## Helper Utils

The Helper Utils category is located under the following path.

Payment Card Industry\Helper Utils

The Helper Utils category reports are listed in the following table.

## Helper Utils

Report	Description	Drill Down	Parameters
Events by Device	Helper report to get general Event Info using drill downs	none	none
General Event Info by Destination Address	Helper report to get general Event Info using drill downs	none	none
General Event Info by Destination Address and Port	Helper report to get general Event Info using drill downs	none	none
General Event Info by Destination User Name	Helper report to get general Event Info using drill downs	none	none
General Event Info by ID	Helper report to get general Event Info using drill downs	none	none
General Event Info by Name	Helper report to get general Event Info using drill downs	<p>The Dest Address field drill downs to the <a href="#">"General Event Info by Destination Address"</a> above report.</p> <p>The Dest Port field drill downs to the <a href="#">"General Event Info by Destination Address and Port"</a> above report.</p> <p>The Destination User field drill downs to the <a href="#">"General Event Info by Destination User Name"</a> above report.</p> <p>The Source Address field drill downs to the <a href="#">"General Event Info by Source Address"</a> below report.</p>	none
General Event Info by Source Address	Helper report to get general Event Info using drill downs	none	none

# Chapter 6: PCI Dashboards

This section lists all the Logger PCI dashboards.

## Requirement 1 Dashboard

Logger PCI Requirement 1 dashboard panels include charts showing the top network equipment, firewall, and VPN configuration change events by name. A chart showing the top direct outbound communication from the CDE to public addresses is also provided.

Dashboard Component	Description
<b>Top Network Equipment Configuration Change Events</b>	PCI Section: 11.7 This panel shows the top network equipment configuration change events by name.
<b>Top Firewall Configuration Change Events</b>	PCI Section: 11.7 This panel shows the top firewall configuration change events by name.
<b>Top VPN Configuration Change Events</b>	PCI Section: 11.7 This panel shows the top VPN configuration change events by name.
<b>Top Direct Outbound Communications from CDE to Public Addresses</b>	PCI Section: 11.3 This panel shows the top direct communication from CDE to Public addresses by source address.

## Requirement 2 Dashboard

The Logger PCI Requirement 2 dashboard panels include charts showing the top default accounts used, misconfigured systems, insecure services, and unencrypted administrative access.

Dashboard Component	Description
<b>Top Default Account Usage Events by Name and Signature ID</b>	PCI Section: 2.1  This panel shows the top default account usage events by name and signature ID.
<b>Top Misconfigured System Events by IP Address</b>	PCI Section: 2.2.4  This panel shows the top misconfigured system events by IP address.
<b>Top Insecure Service Events by IP Address and Port</b>	PCI Section: 2.2.3  This panel shows the top insecure service events by IP address and port.
<b>Top Unencrypted Administrative Access Events by User, Destination Address, and Port</b>	PCI Section: 2.3  This panel shows the top unencrypted administrative access events by user, destination address, and port.

## Requirement 3 Dashboard

Logger PCI Requirement 3 dashboard panels include charts showing credit card numbers in clear text events received from Tipping Point, Snort, Netscreen, and Qualys devices.

Dashboard Component	Description
<b>Weekly Credit Card Numbers in Clear Text Events (TIPPING POINT)</b>	PCI Section: 3.3  This panel shows credit card numbers in clear text events received from Tipping Point devices per day during the last week.
<b>Weekly Credit Card Numbers in Clear Text Events (Snort)</b>	PCI Section: 3.3  This panel shows credit card numbers in clear text events received from Snort devices per day during the last week.
<b>Monthly Credit Card Numbers in Clear Text Events (General)</b>	PCI Section: 3.3  This panel shows credit card numbers in clear text events received from the following devices per day during the last 30 days: Tipping Point Snort Netscreen Qualys



## Requirement 4 Dashboard

Logger PCI Requirement 4 dashboard panels include charts showing the top unencrypted outbound communications, the top PCI systems that provide unencrypted services, and the top misconfigured wireless devices.

Dashboard Component	Description
<b>Top Unencrypted Outbound Communication by IP Address</b>	PCI Section: 4.1  This panel shows the top unencrypted outbound communication by IP address.
<b>Top PCI Systems Providing Unencrypted Services</b>	PCI Section: 4.1  This panel shows the top PCI systems that provide unencrypted services by IP address and port.
<b>Top Misconfigured Wireless Devices</b>	PCI Section: 4.1.1  This panel shows the top misconfigured wireless devices by MAC address for events received from Motorola AirDefence and AirMagnet devices.

## Requirement 5 Dashboard

Logger PCI Requirement 5 dashboard panels include charts showing the top failed Anti-Virus updates, Anti-Virus clean or quarantine attempts, daily Anti-Virus events by device vendor, and failed Anti-Virus clean or quarantine attempts.

Dashboard Component	Description
<b>Top Failed Anti-Virus Update Events by Agent Address and Device Vendor</b>	PCI Section: 5.2  This panel shows the top failed Anti-Virus update events by agent address and device vendor.
<b>Anti-Virus Clean or Quarantine Attempts per Hour</b>	PCI Section: 5.1.1  This panel shows Anti-Virus clean or quarantine attempts per hour.
<b>Anti-Virus Events by Device Vendor per Day</b>	PCI Section: 5.1  This panel shows daily Anti-Virus events by device vendor.
<b>Failed Anti-Virus Clean or Quarantine Attempts per Hour</b>	PCI Section: 5.1.1  This panel shows failed Anti-Virus clean or quarantine attempts per hour.

## Requirement 6 Dashboard

Logger PCI Requirement 6 dashboard panels include charts showing malicious activity, top IP addresses with CVSS score vulnerabilities larger or equal to 4, top vulnerabilities by vendor signature, and vulnerability scanner events by device vendor .

Dashboard Component	Description
<b>Malicious Malware Activity per Hour (Last 3 Days)</b>	PCI Section: 6.1 /6.2  This panel shows malicious activity per hour during the last three days.
<b>Top IP Addresses with CVSS Score Vulnerabilities Larger or Equal to 4 (Last 30 Days)</b>	PCI Section: 6.5.6  This panel shows the top IP addresses with CVSS score vulnerabilities larger or equal to 4 during the last 30 days using events received from the following devices: <ul style="list-style-type: none"><li>• McAfee Vulnerability Manager</li><li>• Nessus Vulnerability Scanner</li><li>• Qualys vulnerability Manager</li><li>• Rapid7 Nexpose</li></ul>
<b>Top Vulnerability Events by Vendor Signature (Last 14 Days)</b>	PCI Section: 6.5.6\6.1  This panel shows the top vulnerabilities by vendor signature during the last 14 days using events received from the following devices: <ul style="list-style-type: none"><li>• McAfee Vulnerability Manager</li><li>• Nessus Vulnerability Scanner</li><li>• Qualys Vulnerability Manager</li><li>• Rapid7 Nexpose</li><li>• nCircle Vulnerability Manager</li><li>• SAINT Vulnerability Scanner</li></ul>
<b>Vulnerability Scanner Events by Device Vendor per Hour (Last 3 Days)</b>	PCI Section: 6.1\6.2  This panel shows vulnerability scanner events by device vendor per hour during the last three days.

## Requirement 7 Dashboard

Logger PCI Requirement 7 dashboard panels include charts showing the top successful user access, infrequent successful user access, and the last successful user accesses.

Dashboard Component	Description
<b>Top Successful User Access (Last 30 Days)</b>	PCI Section: 7.1  This panel shows the top successful user accesses during the last 30 days.
<b>Infrequent Successful User Access (Last 30 Days)</b>	PCI Section: 7.1  This panel shows infrequent successful user accesses during the last 30 days.
<b>Last Successful User Accesses by User Name (Last Hour)</b>	PCI Section: 7.1  This panel shows the last successful user accesses during the last hour.

## Requirement 8 Dashboard

Logger PCI Requirement 8 dashboard panels include charts showing successful password changes, the top users with Windows account lockouts, the top anonymous user activity, and the top terminated users.

Dashboard Component	Description
<b>Successful Password Changes (Last 90 Days)</b>	<p>PCI Section: 8.2.4</p> <p>This panel shows successful password changes per day during the last 90 days.</p>
<b>Top User Windows Account Lockouts (Last 30 Days)</b>	<p>PCI Section: 8.1.6</p> <p>This panel shows the top users with Windows account lockouts during the last 30 days using events generated from the following SmartConnectors:</p> <ul style="list-style-type: none"><li>• SmartConnector for Microsoft Windows Event Log</li><li>• SmartConnector for Microsoft Windows Event Log-Unified</li></ul>

Dashboard Component	Description
<b>Top Anonymous User Activity (Last Day)</b>	<p>PCI Section: 8.1.1</p> <p>This panel shows the top anonymous user activity during the last day.</p> <p><b>Note:</b> To see the information in this panel, the CIP_Default_Accounts.csv file must be installed on the system.</p> <p>To install the CIP_Default_Accounts file, perform the following procedure:</p> <ol style="list-style-type: none"> <li>1. Download the CIP_Default_Accounts file from the "\"Logger home\"\\solutions\\pci\\V400 directory to the machine where your browser is installed.</li> <li>2. From the Logger user interface, select <b>Configuration &gt; Lookup Files &gt; Add</b>.</li> <li>3. Enter CIP_Default_Accounts in the Lookup File field as shown in the following image:</li> </ol> <div data-bbox="402 674 1421 1083"> <p><b>Add Lookup File</b></p> <hr/> <p>Name <input type="text" value="CIP_Defaults_Accounts"/></p> <p>Lookup File <input type="text"/> <input type="button" value="Browse..."/></p> <p><input type="button" value="Save"/> <input type="button" value="Cancel"/></p> </div> <ol style="list-style-type: none"> <li>4. Click <b>Browse</b> and navigate to where you downloaded the file.</li> <li>5. Click <b>Save</b>.</li> </ol>
<b>Top Terminated User Activity (Last 30 Days)</b>	<p>PCI Section: 8.1.3</p> <p>This panel shows the top terminated users during the last 30 days.</p>

## Requirement 9 Dashboard

Logger PCI Requirement 9 dashboard panels include charts showing the top physical access event reporting devices, physical access system account events, and failed physical access attempts .

Dashboard Component	Description
<b>Top Physical Access Event Reporting Devices (Last Day)</b>	PCI Section: 9.1.1  This panel shows the top physical access event reporting devices during the last day.
<b>Physical Access, System Account Creation, Deletion, and Modification Events (Last Day)</b>	PCI Section: 9.1  This panel shows physical access system account events (creation, deletion, and modification events) by categoryBehavior during the last day.
<b>Failed Physical Facility Access Attempts per 30 Minutes (Last Day)</b>	PCI Section: 9.1/9.4  This panel shows failed physical access attempts at 30 minute intervals during the last day.

## Requirement 10 Dashboard

Logger PCI Requirement 10 dashboard panels include charts showing the top excessive failed administrative logins, the top excessive failed administrative action events, the top excessive failed account creation events, and the top excessive failed database access events.

Dashboard Component	Description
<b>Top Excessive Failed Administrative Login Events (Last Day)</b>	PCI Section: 10.2.5  This panel shows the top excessive failed administrative login events during the last day.
<b>Top Excessive Failed Administrative Action Events (Last Day)</b>	PCI Section: 10.2.5  This panel shows the top excessive failed administrative action events during the last day.
<b>Top Excessive Failed Account Creation Events (Last Day)</b>	PCI Section: 10.2.5  This panel shows the top excessive failed account creation events during the last day.
<b>Top Excessive Failed Database Access Events (Last Day)</b>	PCI Section: 10.2.5  This panel shows the top excessive failed database access events during the last day.



## Requirement 11 Dashboard

Logger PCI Requirement 11 dashboard panels include charts showing network IDS events by device product and IP address, host IDS events by device product and IP address, and the last ten attacks and suspicious events.

Dashboard Component	Description
<b>NIDS Events by Device</b>	PCI Section: 11.4  This panel shows network IDS events by device product and address during the last day.
<b>HIDS Events by Device</b>	PCI Section: 11.5  This panel shows host IDS events by device product and address during the last day.
<b>Last 10 Attacks and Suspicious Events</b>	PCI Section: 11.4/11.5  This panel shows the last ten attacks and suspicious events.

## Requirement 12 Dashboard

Logger PCI Requirement 12 dashboard panels include charts showing all devices reporting events by vendor, the top 20 events, events by categoryOutcome, and the top 20 infrequent events.

Dashboard Component	Description
<b>All Devices Reporting Events by Vendor</b>	PCI Section: 12.10.3  This panel shows all devices reporting events by vendor.
<b>Top 20 Events by Destination Address</b>	PCI Section: 12.10.3  This panel shows the top 20 events by destination address.
<b>Access Events by categoryOutcome (Last Day)</b>	PCI Section: 12.10.3  This panel shows access events by categoryOutcome during the last day.
<b>Top 20 Rare Events by Destination Address</b>	PCI Section: 12.10.3  This panel shows the top 20 infrequent events by destination address.

# Chapter 7: PCI Parameters

The following sections list all the Logger PCI parameters.

## ANONYMOUS\_ACCOUNTS

When a report invokes a query that expects the ANONYMOUS\_ACCOUNTS parameter as input, the Anonymous accounts prompt is displayed during report runtime with a default value of 'admin', 'administrator', 'anonymous', 'dev', 'guest', 'root', 'sys', 'test', 'tester'.

## CDE\_ALLOWED\_PORTS

When a report invokes a query that expects the CDE\_ALLOWED\_PORTS parameter as input, the CDE Allowed ports prompt is displayed during report runtime with all default values listed in the Combo Source panel.

## CDE\_AUTHORIZED\_USERS

When a report invokes a query that expects the CDE\_AUTHORIZED\_USERS parameter as input, the CDE Authorized Users prompt is displayed during report runtime with a default value of 'N/A'.

## CDE\_ZONES

When a report invokes a query that expects the CDE\_ZONES parameter as input, the CDE Zone prompt is displayed during report runtime with a default value of '/All Zones/ArcSight System/Private Address Space Zones/RFC1918: 10.0.0.0-10.255.255.255'.

## CUSTOM\_ACCOUNTS

When a report invokes a query that expects the CUSTOM\_ACCOUNTS parameter as input, the Custom Users prompt is displayed during report runtime with a default value of 'dev', 'test', 'tester'.

## DATABASE\_ADDRESSES

When a report invokes a query that expects the DATABASE\_ADDRESSES parameter as input, the DATABASE\_ADDRESSES prompt is displayed during report runtime with a default value of 'N/A'.

## DATABASE\_ADMIN\_USERS

When a report invokes a query that expects the DATABASE\_ADMIN\_USERS parameter as input, the DataBase Admin Users prompt is displayed during report runtime with a default value of 'N/A'.

## destinationZone

When a report invokes a query that expects the destinationZone parameter as input, the Destination Address prompt is displayed during report runtime with a default value of %.

## DMZ\_ALLOWED\_PORTS

When a report invokes a query that expects the DMZ\_ALLOWED\_PORTS parameter as input, the DMZ Registered ports prompt is displayed during report runtime with all default values listed in the Combo Source panel.

## DMZ\_ZONES

When a report invokes a query that expects the DMZ\_ZONES parameter as input, the DMZ Zone prompt is displayed during report runtime with a default value of '/All Zones/ArcSight System/Private Address Space Zones/RFC1918: 10.0.0.0-10.255.255.255'.

## pciAdminUsers

When a report invokes a query that expects the pciAdminUsers parameter as input, the Administrative Users prompt is displayed during report runtime with a default value of 'root', 'administrator', 'admin', 'sys'.

## pciDestAddress

When a report invokes a query that expects the `pciDestAddress` parameter as input, the Destination Address prompt is displayed during report runtime with a default value of %.

## pciDestHostName

When a report invokes a query that expects the `pciDestHostName` parameter as input, the Destination Host Name prompt is displayed during report runtime with a default value of %.

## pciDestUserName

When a report invokes a query that expects the `pciDestUserName` parameter as input, the Destination User Name prompt is displayed during report runtime with a default value of %.

## pciDeviceAddress

When a report invokes a query that expects the `pciDeviceAddress` parameter as input, the Device Address prompt is displayed during report runtime with a default value of %.

## pciDeviceHostName

When a report invokes a query that expects the `pciDeviceHostName` parameter as input, the Device Host Name prompt is displayed during report runtime with a default value of %.

## pciEventId

When a report invokes a query that expects the `pciEventId` parameter as input, the prompt is displayed during report runtime with a default value of -1.

## pciEventName

When a report invokes a query that expects the `pciEventName` parameter as input, the Event Name prompt is displayed during report runtime with a default value of %.

## pciPaymentApplications

When a report invokes a query that expects the `pciPaymentApplications` parameter as input, the PCI Payment Applications prompt is displayed during report runtime with a default value of `'PAYMENT_APP_1', 'PAYMENT_APP_2'`.

## pciSourceAddress

When a report invokes a query that expects the `pciSourceAddress` parameter as input, the Source Address prompt is displayed during report runtime with a default value of %.

## pciSrcUserName

When a report invokes a query that expects the `pciSrcUserName` parameter as input, the Source User Name prompt is displayed during report runtime with a default value of %.

## pciVirtualizationProducts

When a report invokes a query that expects the `pciVirtualizationProducts` parameter as input, the Virtualization Products prompt is displayed during report runtime with a default value of `'VirtualCenter 4.1', 'ESX', 'VProduct'`.

## PERIMETER\_FIREWALL

When a report invokes a query that expects the `PERIMETER_FIREWALL` parameter as input, the PERIMETER FIREWALL Address prompt is displayed during report runtime with a default value of N/A.

## UNSECURED\_PORTS

When a report invokes a query that expects the UNSECURED\_PORTS parameter as input, the Unsecured ports prompt is displayed during report runtime with all default values listed in the Combo Source panel.

## UNSECURED\_PROCESSESSES

When a report invokes a query that expects the UNSECURED\_PROCESSESSES parameter as input, the Unsecured Processes prompt is displayed during report runtime with a default value of `ftpd,in.rexecd,inetd,nmbd,pop3,rexec,rsh,snmpd,snmptrapd,telnetd`.

## WIRELESS\_ZONES

When a report invokes a query that expects the WIRELESS\_ZONES parameter as input, the WIRELESS Zone prompt is displayed during report runtime with a default value of `'/All Zones/ArcSight System/Private Address Space Zones/RFC1918: 10.0.0.0-10.255.255.255'`.

# Appendix A: Uninstall Logger CIP for PCI

This section provides instructions for uninstalling Logger CIP for PCI. This section is not part of the initial configuration and is provided if you want to uninstall Logger CIP for PCI at a later date.

If you need to uninstall Logger CIP for PCI, follow the steps in this section.

1. Delete all reports, queries, and parameters in the Payment Card Industry:
  - a. From the **Reports** top-level menu bar, click **Category Explorer**.
  - b. Right-click **Payment Card Industry**.
  - c. Click **Delete**.
2. Delete each Logger CIP for PCI alert individually:
  - a. Select **Configuration** from the top-level menu bar, then select **Alerts** in the **Data** section.
  - b. For each alert that is prefixed with PCI or PA-DSS, click the **Remove** ✕ icon.
3. To delete PCI dashboards, delete each dashboard and its saved searches individually:
  - a. Select **Dashboards** from the top-level menu bar.
  - b. For each dashboard that is prefixed with PCI or PA-DSS, click **Tools > Delete Dashboard**.
4. Delete each Logger CIP for PCI Saved Search individually:
  - a. Select **Configuration** from the top-level menu bar, then select **Saved Searches** from the **Search** section.
  - b. For each saved search that is prefixed with PCI or PA-DSS, click the **Remove** ✕ icon.



# 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 PCI 4.02)**

Just add your feedback to the email and click send.

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

We appreciate your feedback!