
Micro Focus Security

ArcSight Logger CIP for PCI

Software Version: 5.0

Solutions Guide

Document Release Date: December 05, 2018

Software Release Date: December 05, 2018



Legal Notices

Warranty

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

Restricted Rights Legend

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

Copyright Notice

© Copyright 2018 Micro Focus or one of its affiliates.

Trademark Notices

Adobe™ is a trademark of Adobe Systems Incorporated.

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

UNIX® is a registered trademark of The Open Group.

Support

Contact Information

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

Contents

Chapter 1: Logger CIP for PCI Overview	5
Chapter 2: Installation and Uninstallation	7
Installation	7
Installing Logger CIP for PCI on the Logger Appliance	7
Installing Logger CIP for PCI on Software Logger:	8
Uninstall Logger CIP for PCI	9
Chapter 3: Configuring Logger CIP for PCI	10
Processing All Events	10
Classifying PCI-Related Devices in a PCI Device Group	10
To classify PCI-related devices in the PCI device group:	10
Limiting the Events Processed	11
Creating a Filter to Limit the Events Processed	11
To create a filter:	12
Limiting Events Processed by Alerts	13
Adding a filter to an alert:	13
Adding a query term to an alert:	13
Limiting Events Processed by Saved Searches	13
To limit events processed by a saved search:	14
Limiting Events Processed by Reports	14
To limit the events using a filter:	14
To limit events at report run time:	14
Supported Devices	14
Configuring Reports	16
Configuring Alerts	19
Chapter 4: PCI Reports by Category	20
Requirement 1: Install and maintain a firewall configuration to protect cardholder data	22
Requirement 2: Do not use vendor-supplied defaults for system passwords and other security parameters	24
Requirement 3: Protect stored cardholder data	25

Requirement 4: Encrypt transmission of cardholder data across open, public networks	25
Requirement 5: Protect all systems against malware and regularly update anti-virus software or programs	27
Requirement 6: Develop and maintain secure systems and applications	28
Requirement 7: Restrict access to cardholder data by business need to know	29
Requirement 8: Identify and authenticate access to system components	30
Requirement 9: Restrict physical access to cardholder data	31
Requirement 10: Track and monitor all access to network resources and cardholder data	32
Requirement 11: Regularly test security systems and processes	33
Requirement 12: Maintain a policy that addresses information security for all personnel	34
Chapter 5: PCI Dashboards	35
Chapter 6: PCI Alerts	37
Requirement 1 Alerts	37
Requirement 2 Alerts	40
Requirement 3 Alerts	41
Requirement 4 Alerts	43
Requirement 5 Alerts	45
Requirement 6 Alerts	46
Requirement 7 Alerts	48
Requirement 8 Alerts	49
Requirement 9 Alerts	50
Requirement 10 Alerts	51
Requirement 11 Alerts	55
Requirement 12 Alerts	56
Send Documentation Feedback	57

Chapter 1: Logger CIP for PCI Overview

The Payment Card Industry (PCI) Data Security Standard (DSS) 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 sub-requirements: for security management, policies, procedures, network architecture, software design, and other key protective measures.

The following table lists PCI DSS requirements.

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

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 for the twelve requirements defined in the PCI DSS Standard.
- Alerts that monitor incoming events in real time and notify PCI analysts when events of interest are detected.
- Dashboards with graphics and bar charts that display compliance information for the twelve requirements defined in the PCI Standard.

PCI reports, alerts, and dashboards demonstrate stakeholders and auditors that controls are implemented on their credit card systems. Hence, they are PCI compliant and show due diligence to comply with PCI standards.

Chapter 2: Installation and Uninstallation

Installation

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

Installing 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 machine in which you plan to log into the Logger user interface.

Note: Check the Release Notes for the exact version of the file.

2. Log into Logger's user interface.
3. From the top-level menu bar, click **System Admin**.
4. Go to **System** and select **License & Update**.
5. Click **Browse** to locate and open the .enc file you downloaded.
6. Click **Upload Update**.

A dialog with the warning "The process may take some time", is displayed.

7. Click **OK**.

A message is displayed, indicating that the upgrade is progressing. After the contents of the .enc file are installed, a confirmation message pops. 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 **Realtime 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 Software Logger:

1. Log into the system running the Software Logger with the same ID 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).

Note: 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 the Software Logger was installed. For example, if the directory is /opt/logger, the installation folder should be /opt/logger.

The .bin file installs 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 **Realtime 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.

Uninstall Logger CIP for PCI

If you need to uninstall Logger CIP for PCI, follow these steps:

1. Delete all reports, queries, and parameters in the Payment Card Industry:
 - a. From the **Reports** top-level menu bar, click **Explorer**.
 - b. Right-click **PCI**.
 - c. Click **Delete**.
2. Delete each Logger CIP for PCI alert individually:
 - a. Select **Configuration** from the top-level menu bar, then select **Realtime Alerts** in the **Data** section.
 - b. For each alert that is prefixed with PCI requirements, 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 requirements, 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 requirements, click the **Remove** ✕ icon.

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

PCI reports, saved searches and alerts process all the events received by Logger and no configuration is required.

If only some of your devices are subject to PCI compliance, you can limit the events processed by reports, alerts, and saved searches. For more information, see ["Limiting the Events Processed" on the next page](#)

Classifying PCI-Related Devices in a PCI Device Group

If using Device Group to limit the events processed by reports, alerts, and saved searches, create a PCI device group and classify the PCI-related devices as described in following procedure.

After the PCI-related devices are categorized, the device group can be set to filter alerts and reports of the events processed.

To classify PCI-related devices in the 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, select the 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 Filter to Limit the Events Processed" on the next page](#)

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

Limiting the 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:

Tip: You may consider your environment setup and PCI compliance program details. These limiting strategies may be combined.

- Create a PCI-specific device group and only process events from the devices in the device group.
- Use a PCI-related *Storage Group* to limit the events processed. This option is only available if a Storage Group (in addition to the Default Storage and Internal Event Storage Groups) is created during the Logger initialization process. After the Logger initializes, no additional Storage Groups can be allocated. For details, see the *ArcSight Logger Administrator's Guide*.
- Process events from specified devices only.

Note: If only a small subset of all of your reporting devices to Logger are subject to PCI compliance, you may keep those events on a specific storage group. In that way, your Logger may run queries in that storage group, reducing the amount of data and increasing its performance.

To limit the events processed by the Logger CIP for PCI reports and alerts, implement one or more of these limiting strategies:

- Classify PCI-related devices in a PCI device group. See [Classifying PCI-Related Devices in a PCI Device Group](#).
- Create a PCI filter that constrains the events processed by the alerts and reports. See [Creating a Filter to Limit the Events Processed](#).
- 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](#).
- Apply the PCI filter to the entire PCI report category or specify at report run time. See [Limiting Events Processed by Reports](#).
- Configure a saved search for PCI-related events only. See, "[Limiting Events Processed by Saved Searches](#)" on page 13.

Creating a Filter to Limit the Events Processed

You can create filters to identify PCI -related events in your environment and use them to limit events processed by PCI alerts, reports and saved searches. A filter can limit events as follows:

- **Using a PCI-related device group**—Only those events from the devices listed in the device group are processed.
- **Using a PCI-related storage group**—Only those events stored in the specified storage group are processed.
- **By specific devices**—Only events from specific devices are processed.


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

- **PCI Device Group Filter**—It returns events from devices categorized as PCI devices.
- **PCI Storage Group Filter**—It returns events stored in a designated storage group.
- **PCI Devices Filter**—It returns events from specified devices.
- **PCI Storage Group and Devices Filter**—It returns events 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. From the *Add Filter* page, enter the following information and click **Next**:

Field	Description
Name	Name the filter with Logger CIP for PCI and the purpose of the filter, such as <code>PCI Device Group Filter</code> , <code>PCI Storage Group Filter</code> , or <code>PCI Devices Filter</code> .
Type	From the drop-down menu, select: <ul style="list-style-type: none"> Search Group —It can be used can by both alerts and reports to constrain events. Regex —It can be used can by alerts to constrain events. Unified —It can be used can by saved searched to constrain events.

4. Create a query, using one of the following options:
 - In the Query field, enter a regular expression, for example: `storageGroup(Default Storage Group) | deviceGroup(PCIDeviceGroup)`
 - From the *Constrain search by* dialog, click the  icon and select one of the following options:
 - To process events from devices listed in the device group. Click **Device Groups**. Select a Device Group from the list and click **Submit**.
 - To process events saved in a designated storage group. Click **Storage Groups**. Select a storage group from the list and click **Submit**.
 - To 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 created to limit the events processed by both reports and alerts, as described in [Limiting Events Processed by Alerts](#) and [Limiting Events Processed by Reports](#).


Limiting Events Processed by Alerts

To limit the events alerts process, you may add a filter or add a query term to the alert.

Adding a filter to an alert:

1. From **Configuration**, go to **Data** and select **Realtime Alerts**.
2. Click on a PCI alert in the Name column.
3. From **Filters**, select the filter you created in [Creating a Filter to Limit the Events Processed](#) that limits the events processed by the alert.
4. Click **Save**.

Adding a query term to an alert:

1. Select **Configuration** from the top-level menu, then select **Realtime Alerts** from the **Data** section.
2. To edit the alert, click the PCI alert in the Name column.
3. On the top-level Query Term field, click the Add (+) icon.
A new empty Query term is displayed.
4. 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)`
 - From *Constrain search by* dialog, click on the  icon and select one of the following options:
 - Configure 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**.
 - Configure alerts to only process events saved in a designated Storage Group. Click **Storage Groups**. Select a Storage Group from the list and click **Submit**.
 - Configure 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.
5. Click **Save**.

Limiting Events Processed by Saved Searches

To limit the events that a saved search processes, focus the saved search on PCI-related events.

To limit events processed by a saved search:

1. Select **Configuration** from the top-level menu.
2. Click **Saved Searches**.
3. To edit the saved search, click the PCI saved search in the Name column.
4. In the query section, click **Advanced**.
5. Do one or more of the following:
 - Configure Saved Searches to only process events from devices listed in the Device Group: Click **Device Groups**. Select a Device Group from the list and click **Submit**.
 - Configure Saved Searches to only process events saved in a designated Storage Group: Click **Storage Groups**. Select a Storage Group from the list and click **Submit**.
 - Configure Saved Searches 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**.


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:

1. Select **Reports < Administration < Report Category** filters from the top-level menu bar.
2. On the **Report Category Enforced Filter** page, apply a report category (search group) filter to a whole report category.

To limit events at report run time:

1. Run the report using Run or Quick Run ()
2. From **Data**, go to **Device < Device Groups** or **Storage groups**, select the constrain.

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

Supported Devices

The following table lists the supported devices that may generate events used by CIP for each PCI Requirement.

PCI Requirement	Supported Devices
Requirement 1	Network Equipment Firewall devices
Requirement 2	Network Equipment Firewall devices Operating System devices
Requirement 3	Intrusion Detection System Intrusion Prevention System Vulnerability Scanner Application
Requirement 4	Vulnerability Scanner Wireless Intrusion Detection System
Requirement 5	Anti-Virus
Requirement 6	Vulnerability Scanner Firewall Intrusion Detection System Operating System Devices
Requirement 7	Firewall Intrusion Detection System
Requirement 8	Operating Systems Vulnerability Scanner
Requirement 9	Physical Security Systems

Requirement 10	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
Requirement 11	Vulnerability Assessment Intrusion Detection System File Integrity tools
Requirement 12	Policy Management

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 Payment Card Industry\Helper Utils that require configuration

Parameter	Description	Configuration
PCI_ADMIN_USERS	List of administrative users on lower case separated by comma.	Populate it with the usernames that have administrative privileges in your environment.
PCI_AD_DOMAIN	Active Directory Domain	Populate it beforehand or supply it on the reports at runtime.
PCI_ANONYMOUS_ACCOUNTS	List of Anonymous accounts	By default, it contains a list of anonymous and custom accounts that should not be used. It could be also populated with relevant custom accounts.

PCI_BUILDING	PCI Physical Building	Supply it at run time by running the following reports : 1. Successful Physical Facility Accesses by Building 2. Failed Physical Facility Accesses by Building
PCI_CDE_AUTHORIZED_USERS	Cardholder data environment authorized users separated by commas and quotes For example, if the authorized users are admin and john, then the value at run time should be : 'admin,john'	Before running the following report : Unauthorized Access to Cardholder Data Environment. This variable must be properly configured.
PCI_CDE_PORTS	List of authorized ports on the cardholder's environment for both outbound and inbound communications.	Default ports are 443, 80 and 25. To edit the list please add/remove ports from the Dropdown Source.
PCI_CDE_ZONES	Cardholder's data environment zones	Default zone is RFC1918. More zones may be added Replace REGEX string with the REGEX of your PCI_DEVELOPMENT_ZONE addresses
PCI_CUSTOM_ACCOUNTS	List of custom accounts	Default custom account is: dev,test,tester This variable may be edited if you wish to add more custom accounts
PCI_CVE_ID	Used by this report : "Vulnerability Summary by CVE. The valid CVE ID should be provided at report runtime	
PCI_DEVELOPMENT_ZONES	Development environment zones	Default zone is RFC1918 More zones may be added Replace REGEX string with the REGEX of your PCI_DEVELOPMENT_ZONE addresses
PCI_DMZ_PORTS	The list of allowed ports on the DMZ environment both outbound and inbound communications	Default ports are 443, 80 and 25 To edit the list please add/remove ports from the Dropdown Source

PCI_DMZ_ZONES	This variable list the DMZ zones	Default zone is RFC1918 More zones may be added Replace REGEX string with the REGEX of your PCI_DMZ_ZONE addresses
PCI_HOST_NAME	This variable used across different reports , and didn't require any configuration.	
PCI_MF_PRODUCTS	All reporting Multi Factor Authentication Device Products in your environment separated by comma	Add Multi Factor Authentication reporting devices to this variable
PCI_PERIMETER_FIREWALL	Firewall perimeter address	Cofigure the variable "Private IP Addresses Disclosure" within your perimeter firewall address , or provide the address at report run time when required
PCI_PRODUCTION_ZONES	Production environment zones	Default zone is RFC1918. More zones may be added Replace REGEX string with the REGEX of your PCI_PRODUCTION_ZONE addresses
PCI_TEST_ZONES	Testing environment zones	Default zone is RFC1918. More zones may be added Replace REGEX string with the REGEX of your PCI_TEST_ZONE addresses
PCI_UNSECURED_PORTS	Unsecured ports within the organization	Default ports are: 20, 21, 23, 110, 143 and 137 You can edit it to add more ports which relevant to your environment
PCI_UNSECURED_PROCESSES	Unsecured processes within the organization	By default the following processes defined: ftpd,in.rexecd,itend,nmbd,pop3,rexec,rsh,snmpd,snmptrapd,telnetd More processes may be added
PCI_USER	Used by reports. No configuration required	
PCI_WIRELESS_ZONES	Wireless environment zones	Default zone is RFC1918 More zones may be added Replace REGEX string with the REGEX of your PCI_WIRELESS_ZONE addresses
PCI_ZONES	PCI environment zones	Default zone is RFC1918 More zones may be added Replace REGEX string with the REGEX of your PCI_ZONE addresses

For specific report configuration, see [PCI Reports by Category](#).

Configuring Alerts

All the CIP for PCI Alerts are disabled by default and some of the alerts require specific configuration .

Enabling PCI Alerts :

1. Select the Configuration tab.
2. From the left panel menu, select **Realtime Alerts**.
3. Click the alert to be configured.
4. Mark the “**Enable**” checkbox.
5. Click **Save**.

Configuring alerts with site specific data:

1. Select the **Configuration** top-level menu bar, then select **Realtime 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**.

Chapter 4: 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
Requirement 1: Firewall Configuration Requirement 1 states that companies should install and maintain a firewall configuration that protects cardholder data.	""Requirement 1: Install and maintain a firewall configuration to protect cardholder data" on page 22
Requirement 2: Default Security Parameters 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	Requirement 2: Do not use vendor-supplied defaults for system passwords and other security parameters
Requirement 3: Protect Stored Cardholder Data 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.	Requirement 3: Protect stored cardholder data
Requirement 4: Encrypted Transmissions Requirement 4 states that transmissions from cardholder systems to public networks should be encrypted across open, public networks.	Requirement 4: Encrypt transmission of cardholder data across open, public networks

PCI Requirement	Report Category
Requirement 5: Anti-Virus PCI requires that anti-virus software be used on PCI-governed systems and regularly maintained.	Requirement 5: Protect all systems against malware and regularly update anti-virus software or programs
Requirement 6: System Applications 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.	Requirement 6: Develop and maintain secure systems and applications
Requirement 7: Business Need-To-Know Requirement 7 states that access to critical cardholder data should be restricted only to users who have express authorization.	Requirement 7: Restrict access to cardholder data by business need to know
Requirement 8: Unique User ID 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.	Requirement 8: Identify and authenticate access to system components
Requirement 9: Physical Access 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.	Requirement 9: Restrict physical access to cardholder data

PCI Requirement	Report Category
Requirement 10: Track and Monitor Data Access 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.	Requirement 10: Track and monitor all access to network resources and cardholder data
Requirement 11: Test Systems and Networks 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.	Requirement 11: Regularly test security systems and processes
Requirement 12: Maintain an Information Security Policy 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.	Requirement 12: Maintain a policy that addresses information security for all personnel

Requirement 1: Install and maintain a firewall configuration to protect cardholder data

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

PCI\Install and maintain a firewall configuration to protect cardholder data

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

Report	Requirement IDs	Description	Parameters
Blocked Inbound Traffic to Card Holder Data Environment	12.1	This report provides overview of Blocked Inbound Traffic to the Cardholder Data Environment.	PCI_CDE_ZONES
Blocked Outbound Traffic from Card Holder Data Environment	12.1	This report provides overview of Blocked outbound traffic from the Cardholder Data Environment.	PCI_CDE_ZONES
CardHolder Data within the DMZ	13.6	This report shows all the cardholder data IP addresses within the DMZ range.	PCI_CDE_ZONES , PCI_DMZ_ZONES
External to PCI Systems	1.1.2,1.1.3,1.3.3	This report shows all external systems that are communicating directly with PCI internal systems. This traffic should be justified.	PCI_ZONES
Firewall Configuration Changes	1.1 , 1.1.1 ,1.2,6.4.5	This report shows information about firewall configuration changes.	
Inbound Traffic to Card Holder Data Environment	12.1	Inbound Traffic to the Cardholder Data Environment.	PCI_CDE_ZONES
Internal PCI Systems to External	1.1.2,1.1.3,1.3.3	This report shows all internal PCI systems which communicating directly with External systems. This traffic should be justified.	PCI_ZONES
Network Routing Configuration Changes	1.1 , 1.1.1,1.2 ,1.2.2,6.4.5	This report shows information about network routing configuration changes.	
Accessed Ports Through Firewall	1.1.5 , 1.1.6 , 1.1.7	This report finds all ports that were passed by a firewall, as well as the firewall rule number that it triggered.	
Outbound Traffic from Card Holder Data Environment	12.1	This report shows Outbound Traffic from the Cardholder Data Environment.	PCI_CDE_ZONES,PCI_CDE_PORTS
Private IP Addresses Disclosure	13.7	This report shows RFC1918 IP addresses which communicating with public IP addresses. Before running this report please provide your perimeter firewall while running the report , or configure the following variable PCI_Perimeter_Firewall with your organizational perimeter firewall.	
Unauthorized Inbound Traffic to Card Holder Data Environment	12.1	This report shows unauthorized traffic to card holder data environment.	PCI_CDE_ZONES,PCI_CDE_PORTS

VPN Configuration Changes	1.1, 1.1.1,6.4.5	This report shows information about VPN configuration changes.	
Unauthorized Outbound Traffic from Card Holder Data Environment	1.2.1	This report shows unauthorized outbound traffic from card holder data environment.	PCI_CDE_ZONES
Unauthorized Inbound Traffic to DMZ	1.3.1,1.3.2	This report shows unauthorized traffic to DMZ.	PCI_DMZ_ZONES,PCI_DMZ_PORTS
Personal Firewall Installed	1.4	This report listing all the reported personal firewalls.	
Outbound Traffic from Card Holder Data Environment to Internet	1.3.4	This report shows outbound traffic from card holder data environment to the internet.	PCI_CDE_ZONES, PCI_INTERNAL_ZONE

Requirement 2: 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.

PCI\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.

Report	Requirement IDs	Description	Parameters
Default Vendor Accounts	2.1	This report provides overview of default vendor accounts	
Insecure Services	2.2.2	This report lists unsecure services	PCI_UNSECURED_PORTS PCI_UNSECURED_PROCESSES

Insecure Services by Host	2.2.2	This report provides information about insecure services by host (default localhost)	PCI_UNSECURED_PROCESSES PCI_HOST_NAME
Misconfigured Systems	2.2.4	This report lists all the misconfigured systems	
Multiple Functions Implemented on a Server	2.2.1	This report shows multiple functions implemented on the same server (like DNS and Web Server, Database and Web Server..)	
Software Inventory	2.4	This report lists the software inventory detected	
Unencrypted Administrative Accesses	2.3	This report lists all the unencrypted administrative accesses	PCI_ADMIN_USERS

Requirement 3: Protect stored cardholder data

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

PCI\Protect stored cardholder data

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

Report	Requirement IDs	Description	Parameters
Credit Card Numbers in Clear Text	3.3	This report shows credit card numbers activity in clear text	

Requirement 4: 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.

PCI\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.

Report	Requirement IDs	Description	Parameters
Cryptographic Hash Algorithm Related Vulnerabilities	4.1	This report selects events indicating that potential hash algorithm related vulnerability was detected.	
Cryptographic Public Key Related Vulnerabilities	4.1	This report displays cryptographic public key related flaws reported by vulnerability scanners.	
Cryptographic Symmetric Key Related Vulnerabilities	4.1	This report displays cryptographic symmetric key related flaws reported by vulnerability scanners.	
Cryptographic Weak Protocol Vulnerability Detected	4.1	This report displays cryptographic weak protocol related flaws reported by vulnerability scanners.	
Heartbleed Vulnerabilities	4.1	This report displays heartbleed related flaws reported by vulnerability scanners.	
Insecure Services	2.2.2 4.1	This report lists unsecure services used on the organization.	PCI_UNSECURED_PORTS PCI_UNSECURED_PROCESSES
Insecure Services by Host	2.2.2 4.1	This report provides information about insecure services by host (default localhost).	PCI_UNSECURED_PORTS PCI_UNSECURED_PROCESSES PCI_HOST_NAME
Poodle Vulnerabilities	4.1	This filter detects POODLE vulnerability reported by vulnerability scanners.	
SSL or TLS 1.0 Detected	4.1	This report displays if SSL or TLS 1.0 is supported based on vulnerability scanner events.	
SSL or TLS Vulnerabilities	4.1	This report lists all the SSL or TLS vulnerabilities on the organization.	
TLS BREACH Vulnerabilities	4.1	This report lists all the TLS BREACH vulnerabilities on the organization.	

TLS CRIME Vulnerabilities	4.1	This report lists all the TLS Crime vulnerabilities on the organization.	
Wireless Encryption Violations	4.1	This report lists all the wireless encryption violations on the organization.	
Wireless Encryption Violations by Host	4.1	This report lists all the wireless encryption violations by specific host (default localhost).	PCI_HOST_NAME

Requirement 5: 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.

PCI\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.

Report	Requirement IDs	Description	Parameters
Disabled Anti-Virus Events	5.3	This report shows all anti-virus disabled events.	
Failed Anti-Virus Updates	5.2	This report shows failed Anti-Virus updates events.	
Installed Anti-Viruses	5.1	This report lists all the Anti-Viruses installed on the organization and reporting events.	
Malicious Code Activities from CDE	5.1.1	This report lists malicious code activities originated from the CDE.	PCI_CDE_ZONES
Malware Activity	5.1.1	This report provides overview of malware activity	
Malware Activity by Host	5.1.1	This report provides overview of malware activity by host (default localhost)	
Spyware and Adware Activity	5.1.1	This report lists all spyware or adware activity	
Trojan Activity	5.1.1	This report lists all the trojan activity	
Worm Activity	5.1.1	This report lists all the worm activity	

Requirement 6: Develop and maintain secure systems and applications

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

PCI\Develop and maintain secure systems and applications

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

Report	Requirement IDs	Description	Parameters
Broken Authentication and Session Management	6.5.10	This report provides overview of broken authentication and vulnerabilities	
Buffer Overflows	6.5.2	This report provides overview of buffer overflow vulnerabilities	
Command Injection	6.5.1	This report provides lists command injection attacks	
Configuration Modifications by Host	6.4.5	This report lists all the configuration modifications by host name (default host name).	
Cross-site Request Forgery	6.5.9	This report provides overview of cross site request forgery vulnerabilities	
Cross-site Scripting	6.5.7	This report provides overview of cross site scripting (XSS) vulnerabilities	
Custom Account Detected	6.3.1	This report lists all the events which includes custom accounts.	
Databases Configuration Changes	6.4.5	This report lists database configuration changes.	
High Risk Vulnerabilities	6.5.6	This report provides overview of high risk vulnerabilities	
Improper Access Control	6.5.8	This report provides overview of improper access control vulnerabilities	
Improper Error Handling	6.5.5	This report provides overview of improper error handling vulnerabilities	
Injection Flaws	6.5.1	This report provides overview of injection flaws	
Insecure Cryptographic Storage	6.5.3	This report lists insecure cryptographic storages .	

Meltdown or Spectre Vulnerable Assets	6.1	This report lists Meltdown or Spectre vulnerable assets.	
Operating System Changes	6.4.5	This report lists operating system changes.	
Outbound Communication from Development to Production	6.4.2	This report lists all the outbound communication from development to production.	PCI_ PRODUCTION_ ZONES PCI_ DEVELOPMENT_ ZONES
Security Patch Missing	6.2	This report provides overview of missing security patches	
Sql Injection	6.5.1	This report provides overview of sql injection	
Vulnerability Summary by CVE	6.1	This report lists all the vulnerabilities by specific CVE(Valid CVE id should be provided at report runtime).	
Vulnerability Summary by Host	6.1	This report lists all the vulnerabilities by specific host (default localhost).	
Outbound Communication from Production to Development	6.4.2	This report lists all the outbound communication from production to development.	PCI_ PRODUCTION_ ZONES PCI_ DEVELOPMENT_ ZONES

Requirement 7: 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.

PCI\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.

Report	Requirement IDs	Description	Parameters
All Accesses to Cardholder Data Environment	7.1	This report lists all the accesses to Card Holder Data Environment .	PCI_CDE_ ZONES

All Accesses to Cardholder Data Environment by User	7.1	This report lists all the accesses to Card Holder Data Environment by specific user (default admin).	PCI_CDE_ZONES
Unauthorized Access to Cardholder Data Environment	7.1 7.1.2 7.2	This report lists all the unauthorized accesses to Card Holder Data Environment , please make sure to configure the reports parameters before or during running this report.	PCI_CDE_AUTHORIZED_USERS PCI_CDE_ZONES

Requirement 8: Identify and authenticate access to system components

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

PCI\Identify and authenticate access to system components

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

Report	Requirement IDs	Description	Parameters
Anonymous User Activity	8.1.1	This report provides overview of anonymous user activity	
Clear Text Password Transmission	8.2.1	This report provides overview of clear text password transmission on clear text	
Disabled User Activity	8.1.4	This report lists all the disabled users activity	PCI_AD_DOMAIN
Disabled Users	8.1.4	This reports lists all the disabled users	PCI_AD_DOMAIN
Non Multi Factor Authentication Reporting Devices	8.3.2	This report lists all the non multi factor authentication reporting device	PCI_MF_PRODUCTS
Password Policy Changes Events	8.2.3 8.2.4 8.2.5 8.2.6	This report lists all the password policy changes events	
Password Policy History Length Changed to less than 5	8.2.5	This report lists events indicating that password history changed to less the 5.	

Password Policy Lockout Threshold Changed to more than 6	8.1.6	This report lists all the events which indicating that password policy lockout threshold changed to more than 6	
Password Policy Minimum length Changed to less the Seven Characters Events	8.2.3	This report lists events indicating that minimum password length changed to less the 7 characters .	
Successful Password Changes	8.2.4	This report lists all the successful password changes	
Successful Password Changes by User	8.2.4	This report lists all the successful password changes by user	
Terminated User Activity	8.1.3	This report shows the terminated user activity	PCI_AD_DOMAIN
Terminated Users	8.1.3	This report shows the terminated user events	PCI_AD_DOMAIN
Windows Account Lockouts by System	8.1.6	This report shows all account lockouts on Windows systems	
Windows Account Lockouts by User	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.	
Password Policy Minimum age Changed to more than 90 days Events	8.2.4	This report lists events indicating that minimum age changed to more than 90 days events	

Requirement 9: Restrict physical access to cardholder data

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

PCI\Restrict physical access to cardholder data

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

Report	Requirement IDs	Description	Parameters
Failed Physical Facility Access	9.1	This report shows an overview of all failed authentication events involving physical access systems	
Failed Physical Facility Accesses by Building	9.1	This report provides overview of failed physical facility accesses by building	
Successful Physical Facility Accesses by User	9.1	This report provides overview of failed physical facility accesses by building	
Physical Access Events Reporting Devices	9.1.1	This report lists all the physical access events reporting devices	
Physical Facility Access Attempts	9.1	This report shows all authentication events involving physical access systems and their division by outcome per hour	
Successful Physical Facility Accesses by Building	9.1	This report provides overview of successful physical facility accesses by building	
Successful Physical Facility Access	9.1	This report shows an overview of all successful authentication events involving physical access systems.	

Requirement 10: 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.

PCI\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.

Dashboard	Requirement IDs	Description	Parameters
PCI Requirement 10 - Failed Administrative Actions	10.2.2	Provides overview of failed administrative actions	
PCI Requirement 10 - Account Creations and Deletions	10.2.7	Provides overview of account creations and deletions	
PCI Requirement 10 - Failed Administrative Logins Overview	10.2.4	Provides overview of failed Administrative logins	
PCI Requirement 10 - Failed Logins Overview	10.2.4	Provides overview of failed logins	

Requirement 11: Regularly test security systems and processes

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

PCI\Regularly test security systems and processes

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

Report	Requirement IDs	Description	Parameters
Attacks and Suspicious Events-Overview	11.4	This report provides overview of attacks and suspicious events	
Rogue Wireless AP Detected	11.1	This report lists all the rogue wireless AP stations detected	
File Integrity Tools Events	11.5	This report provides overview of file integrity reporting tools	
IDS Events	10.6.1 11.4	This reports provides overview of events categorized as IDS events This report Linked to requirement 10 “IDS Events” report	
Traffic Anomaly on Application Layer	11.4	This report lists all the traffic anomaly on the application layer	
Traffic Anomaly on Network Layer	11.4	This report lists all the traffic anomaly on the network layer	
Traffic Anomaly on Transport Layer	11.4	This report lists all the traffic anomaly on the transport layer	
Information Interception Events	11.4	This report lists all the information interception events	
Vulnerability Summary Overview	11.2.1	This report provides overview of vulnerability summary	
Exploit of Vulnerability	11.3.3	This report lists events indicating an exploit of vulnerability detected	

High Risk Vulnerabilities	6.5.6 11.2 11.2.1	This report provides overview of high risk vulnerabilities. This report linked to requirement 6 “High Risk Vulnerabilities” Report	
Vulnerability Summary by CVE	6.1 11.2	This report lists all the vulnerabilities by specific CVE(Valid CVE id should be provided at report runtime). This report linked to requirement 6 “Vulnerability Summary by CVE” Report	
Vulnerability Summary by Host	6.1 11.2	This report lists all the vulnerabilities by specific host (default localhost) This report linked to requirement 6 “Vulnerability Summary by Host” Report	

Requirement 12: 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.

PCI\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.

Report	Requirement IDs	Description	Parameters
Windows Domain Policy Changes	12.1.1	This report lists windows domain policy changes	
All Reporting Devices	12.3.7	This report shows all devices that report into Logger This can be used for inventory purposes	
Policy Violations	12.4	This report provides overview of policy violation	

Chapter 5: PCI Dashboards

This section lists all the Logger PCI dashboards.

Dashboard Name	Description	Requirement IDs
PCI Requirement 1 - Overview	Overview of PCI requirement 1	1.1 , 1.1.1 ,1.2,6.4.5,1.2.1
PCI Requirement 2 – Insecure Services	Overview of insecure services	2.2.2
PCI Requirement 2 - Default Vendor Accounts	Overview of default vendor accounts	2.2.1
PCI Requirement 3 - Clear Text Credit Card Numbers	Overview of Credit Cards in clear text activity	3.3
PCI Requirement 4 - Insecure Communications	Overview of insecure communication	4.1
PCI Requirement 4 - SSL or TLS Flaw	Overview of SSL or TLS Flaws	4.1
PCI Requirement 5 - Anti Virus Activity	Overview of Anti-Virus activity	5.1 5.2 5.3
PCI Requirement 5 - Malware Activity	Overview of malware activity	5.1.1
PCI Requirement 6 - Vulnerability Scanning	Overview of vulnerability scanning	6.1
PCI Requirement 6 - Vulnerabilities by Type	Overview of vulnerabilities by type, focusing on XSS,XSRF,Buffer overflow and SQL Injection.	6.5.1 6.5.2 6.5.7 6.5.9
PCI Requirement 7 - User Access	Overview of user accesses	7.1
PCI Requirement 8 - Password Management	Overview of Password Management	8.2.3 8.2.4 8.2.5 8.2.6
PCI Requirement 8 - Windows Account Lockouts	Overview of Windows account lockouts.	8.1.6
PCI Requirement 9 - Physical Security Overview	Overview of physical security accesses	9.1
PCI Requirement 10 - Failed Administrative Actions	Overview of failed administrative actions	10.2.2
PCI Requirement 10 - Account Creations and Deletions	Overview of account creations and deletions	10.2.7
PCI Requirement 10 - Failed Administrative Logins Overview	Overview of failed administrative logins	10.2.4

PCI Requirement 10 - Failed Logins Overview	Overview of failed logins	10.2.4
PCI Requirement 11 - Attacks and Suspicious Activity	Overview of attacks and suspicious activity	11.4
PCI Requirement 12 - Policy Violations	Overview of policy violations.	12.4

Chapter 6: PCI Alerts

This section lists all the Logger PCI alerts.

Requirement 1 Alerts

Alert	Requirement #1	Configuration	Requirement IDs
PCI Requirement 1 - Destination Address in CDE and DMZ	The alert triggers when a destination address found on both the DMZ and CardHolder Data Environment	1. Replace DMZ string with regex of your DMZ IP addresses 2. Replace CDE_ADDRESSES string with regex of your CardHolder environment IP addresses	13.6
PCI Requirement 1 - Source Address in CDE and DMZ	The alert triggers when a source address found on both the DMZ and CardHolder Data Environment	1. Replace DMZ string with regex of of your DMZ IP addresses 2. Replace CDE_ADDRESSES string with regex of your CardHolder environment IP addresses	13.6
PCI Requirement 1 - VPN Configuration Changes	The alert triggers when changes to a VPN device's configuration file are reported		1.1, 1.1.1,6.4.5
PCI Requirement 1 - Network Equipment Configuration Changes	The alert triggers when changes to a network device's configuration file are reported		1.1, 1.1.1,1.2,1.2.2,6.4.5
PCI Requirement 1 - Firewall Configuration Changes	The alert triggers when changes to a Firewall's configuration file are reported.		1.1, 1.1.1,1.2,6.4.5

PCI Requirement 1 - Direct Traffic from CDE to Public Addresses	The 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).	Replace CDE_ADDRESSES string with the regex of your CardHolder environment IP addresses	1.3
PCI Requirement 1 - Direct Traffic from Public Addresses to CDE	The 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).	Replace CDE_ADDRESSES string with the regex of your cardholder environment IP addresses	1.3
PCI Requirement 1 - Unauthorized Inbound Traffic to the CDE	The alert triggers when unauthorized inbound traffic to the Cardholder Data Environment is detected.	1. Replace CDE_ADDRESSES string with the regex of your cardholder environment IP addresses 2. Change the regex ports on dpt=(433 22) to the permitted inbound ports to the cardholder data environment	1.2.1
PCI Requirement 1 - Unauthorized Outbound Traffic from the CDE	The alert triggers when unauthorized outbound traffic from the Cardholder Data Environment is detected.	1. Replace CDE_ADDRESSES string with the regex of your CardHolder environment IP addresses 2. Change the regex ports on dpt=(433 22) to the permitted outbound ports from the cardholder data environment	1.2.1
PCI Requirement 1 - Unauthorized Inbound Traffic from Public IP Addresses to the DMZ	The alert triggers when unauthorized inbound traffic from public IP addresses to the DMZ is detected	1. Replace DMZ_ADDRESSES string with the regex of your DMZ IP addresses 2. Change the regex ports on dpt=(433 22) to the permitted inbound ports from public addresses to DMZ	1.3.1,1.3.2

PCI Requirement 1- Unauthorized Inbound Traffic from Wireless Networks to the CDE	This alert triggers when unauthorized inbound traffic from wireless networks to the Cardholder Data Environment is detected	1. Replace WIRELESS_ADDRESSES string with the regex of your wireless addresses 2. Replace CDE_ADDRESSES string with the regex of your CDE addresses 3. Change the regex ports on dpt=(433 22) to the permitted inbound ports from wireless network to the CDE	12.3
PCI Requirement 1- Unauthorized Outbound Traffic from the CDE to Wireless Networks	The alert triggers when unauthorized outbound traffic from the Cardholder Data Environment to wireless networks is detected.	1. Replace WIRELESS_ADDRESSES string with the regex of your wireless addresses 2. Replace CDE_ADDRESSES string with the regex of your CDE addresses 3. Change the regex ports on dpt=(433 22) to the permitted outbound ports from CDE to wireless networks	12.3
PCI Requirement 1 - Disclosed Private IP Addresses	The alert triggers when a private IP address is disclosed to unauthorized parties.	Replace PERIMETER_FIREWALL with your perimeter firewall address	13.7
PCI Requirement 1- Internal IP Access from the Internet	The alert triggers when traffic originating from the internet within an internal ip address as source	Replace PERIMETER_FIREWALL with your perimeter firewall address	13.3
PCI Requirement 1 - Unauthorized Inbound Traffic from Public Addresses	The alert triggers when unauthorized inbound traffic from public addresses is Detected and targeting the DMZ .	Replace DMZ_ADDRESSES string with the regex of your DMZ IP addresses	13.2

Requirement 2 Alerts

Report	Requirement #2	Configuration	Requirement IDs
PCI Requirement 2 -Default Account Usage Alert	<p>This alert triggers when the source or destination account name matches one of the following default account names:</p> <p>admin, root<space>, sa<space>, nobody<space>, guest<space>, manager<space>, sys<space>, system<space>, oracle<space>, orcladmin<space>, cisco<space>, pixadmin<space></p> <p>Where <space> represents the space character. Account names are case insensitive.</p> <p>The "Query Terms" field, specifies account names. If the admin account name is specified without a trailing space, any account name that begins with the same set of characters may match.</p> <p>For example, the account name <i>admin</i>, matches any string beginning with admin including Administrator or admins. This scenario does not occur to those account names that end with the <space> character.</p>	Update and add the list to include default vendor accounts.	2.1
PCI Requirement 2 -Databases in DMZ	This alert is triggered when a Database instance is found in the DMZ.	Replace DMZ string with regex of your DMZ IP addresses	2.2.1
PCI Requirement 2 - Insecure Services Detected	This alert triggers when an insecure service, such as ftp, tftp, telnet, pop3, or NetBIOS is identified.		2.2.2
PCI Requirement 2 - Misconfiguration Detected	This alert triggers when a misconfiguration event is detected		2.2.4
PCI Requirement 2 – Unencrypted Administrative Access	This alert triggers when unencrypted administrative access is detected.		2.3

Requirement 3 Alerts

Alert	Description	Requirement IDs
PCI Requirement 3 - Credit Card Number in Clear Text (Juniper)	This alert triggers when a Juniper Netscreen IDS reports that credit card information was sent in clear text using HTTP.	3.3
PCI Requirement 3 - Credit Card Number in Clear Text (Vericept)	This alert triggers when a Vericept information monitoring system reports that credit card information was sent in clear text.	3.3
PCI Requirement 3 - Credit Card Number in Clear Text (Vontu)	This alert triggers when a Vontu information monitoring system reports that credit card information was sent in clear text.	3.3
PCI Requirement 3 - Credit Card Number in Clear Text (TippingPoint)	This alert triggers when a TippingPoint UnityOne IPS reports that credit card information was sent in clear text.	3.3
PCI Requirement 3 - Credit Card Number in Clear Text (Snort)	This alert triggers when Snort IDS reports that credit card information was sent in clear text.	3.3
PCI Requirement 3 - Credit Card Number in Clear Text (Reconnex)	This alert triggers when a Reconnex information monitoring system reports that credit card information was sent in clear text.	3.3

PCI Requirement 3 - Credit Card Number in Clear Text	<p>This alert triggers when a credit card number appears in the logs as clear text,</p> <p>using one of the following formats:</p> <pre><n><n><n><n>-<n><n><n><n>-<n><n><n><n>-<n><n><n><n></pre> <pre><n><n><n><n>-<n><n><n><n><n><n>-<n><n><n><n></pre> <pre><n><n><n><n>-<n><n><n><n><n><n>-<n><n><n><n></pre> <p>Where <n> is single numeric digit.</p>	<p>3.3</p>
PCI Requirement 3 - Credit Card Number in Clear Text (Nessus)	<p>This alert triggers when Nessus reports that credit card information was sent in clear text</p>	<p>3.3</p>
PCI Requirement 3 - Credit Card Number in Clear Text (Card Association)	<p>This alert triggers when a credit card number appears in logs as clear text using one of the following formats:</p> <p>Visa</p> <p>MasterCard</p> <p>American Express</p> <p>Discover</p> <p>Diner's club</p> <p>JCB</p>	<p>3.3</p>

Requirement 4 Alerts

Alert	Description	Configuration	Requirement IDs
PCI Requirement 4 - Heartbleed Vulnerability Detected	This alert triggers when a heartbleed vulnerability detected		4.1
PCI Requirement 4 - Internal Systems Running Insecure Services	<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.</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>1.The following services are defined as insecure:</p> <p>telnet, ftpd, rexec, pop3, rsh, imapd.</p> <p>2.The following ports are defined as insecure:</p> <p>20, 21, 25, 110, 143, 23</p> <p>3. Default Match Count: 1</p> <p>Default Threshold (Sec): 300</p>	4.1
PCI Requirement 4 - Internal Systems Using Insecure Public Services	<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>Default Match Count: 1</p> <p>Default Threshold (Sec): 300</p>		4.1

PCI Requirement 4 - TLS CRIME Vulnerability Detected	This alert triggers when a TLS CRIME vulnerability detected		4.1
PCI Requirement 4 - Wireless Encryption Violation	This alert triggers when a wireless encryption violation detected		4.1.1
PCI Requirement 4- Poodle Vulnerability Detected	This alert triggers when a poodle vulnerability detected		4.1
PCI Requirement 4 - SSL or TLS 1.0 Detected	This alert triggers when a SSL or TLS 1.0 service detected		4.1
PCI Requirement 4- SSL or TLS Flaw Detected	This alert triggers when a ssl or tls vulnerability detected		4.1
PC Requirement 4 - TLS BREACH Vulnerability Detected	This alert triggers when a TLS BREACH vulnerability detected		4.1

Requirement 5 Alerts

Alert	Description	Requirement IDs
PCI Requirement 5 - Anti-Virus Disabled	This alert triggers when an anti-virus disabled action is detected.	5.1
PCI Requirement 5 - Anti-Virus Failed Update	This alert triggers when a failed anti-virus update event is detected.	5.2
PCI Requirement 5 - Failed Virus Quarantine or Clean or Deletion	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.	5.2
PCI Requirement 5 - Malware Activity Detected	This alert triggers when a malware activity detected	5.1.1
PCI Requirement 5 - Network Traffic matching a Virus Signature is Detected	This alert triggers when a network traffic detected that match a virus signature	5.1.1
PCI Requirement 5 - Successful Virus Quarantine or Clean or Deletion	This alert triggers when anti-virus software quarantined, cleaned or deleted virus files.	5.1.1
PCI Requirement 5 - Virus Discovered	This alert triggers when anti-virus software discovered a virus on a machine.	5.1.1
PCI Requirement 5 - Worm Activity Detected	This alert triggers when a worm activity detected	5.1.1

Requirement 6 Alerts

Alert	Description	Configuration	Requirement IDs
PCI Requirement 6 - Broken Authentication and Session Management Detected	This alert triggers when a Broken Authentication and Session Management vulnerability is detected.		6.5.10
PCI Requirement 6 - Cross Site Request Forgery Detected	This alert triggers when a Cross Site Request Forgery vulnerability is detected		6.5.9
PCI Requirement 6 - Cross Site Scripting Detected	This alert triggers when a Cross Site Scripting vulnerability is detected.		6.5.7
PCI Requirement 6 - Improper Access Control Detected	This alert triggers when improper access control is detected.		6.5.8
PCI Requirement 6 - Improper Error Handling Detected	This alert triggers when improper error handling is detected.		6.5.5
PCI Requirement 6 - Injection Flaw Detected	This alert triggers when an Injection Flaw vulnerability is detected.		6.5.1
PCI Requirement 6 - Insecure Communications Detected	This alert triggers when insecure communications are detected.		6.5.4
PCI Requirement 6 - Insecure Cryptographic Storage Detected	This alert triggers when an Insecure Cryptographic Storage event is detected.		6.5.3
PCI Requirement 6 - Security Patch Missing	This alert triggers when a Missing Security Patch event is detected.		6.2

PCI Requirement 6 - Custom Account Detected	This alert triggers when a custom account is detected on production environment.	1. Replace PRODUCTION_ENVIRONMENT string with the regex of your production environment IP addresses	6.3.2
PCI Requirement 6 - Excessive Failed Application Level Changes	<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 Match Count: 30</p> <p>Default Threshold (Sec): 300</p>		6.4.5
PCI Requirement 6 - Excessive Failed Operating System Modifications	<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 Match Count: 30</p> <p>Default Threshold (Sec): 300</p>		6.4.5
PCI Requirement 6 - Vulnerability with CVSS SCORE Larger or Equal to 4	This alert triggers when a vulnerability with a CVSS score of 4 or higher is detected		6.5.6
PCI Requirement 6 - Vulnerability High Severity Detected	This alert triggers when a vulnerability with a CVSS score of 4 or higher is detected.		6.5.6
PCI Requirement 6 - Custom Vulnerability Detected	This alert triggers when a custom CVE vulnerability is detected	1. Replace CVE_ID string with the custom CVE	6.5 6.5.6

Requirement 7 Alerts

Alert	Description	Configuration	Requirement IDs
PCI Requirement 7-Unauthorized Access to CD Detected	This alert triggers when an unauthorized user tries to access the Cardholder Data Environment.	1. Replace AUTHORIZED_USERS string with the regex of your authorized users 2. Replace CDE_ADDRESSES string with the regex of your cardholder data environment	7.1

Requirement 8 Alerts

Alert	Description	Configuration	Requirement IDs
PCI Requirement 8 - Anonymous User Activity	This alert triggers when anonymous user activity is detected in the Cardholder Data Environment.	1. Replace: .CDE_ ADDRESSES string with the regex of your CDE addresses	8.1.1
PCI Requirement 8 - Clear Text Password Transmission	This alert triggers when a clear text password transmission is detected on a web application		8.2.1
PCI Requirement 8 - Password Policy Minimum age Changed to more than 90 days	This alert triggers when password policy minimum age changed to more than 90 days.		8.2.4
PCI Requirement 8 - Password Policy History Length Changed to less than 5	This alert triggers when password policy History Length changed to less than 5.		8.2.5
PCI Requirement 8 - Password Policy Lockout Threshold Changed to more than 6	This alert triggers when password policy lockout threshold changed to more than 6.		8.1.6
PCI Requirement 8 - Password Policy Lockout Duration Changed to less than 30	This alert triggers when password policy lockout duration changed to less than 30.		8.1.7
PCI Requirement 8 - Password Policy Minimum length Changed to less the Seven Characters	This alert triggers when password policy minimum length changed to less than seven characters		8.2.3
PCI Requirement 8 -Web Form Sending Credentials Using Get	This alert triggers when Nessus detects web form sending credentials using Get		8.2.1

Requirement 9 Alerts

Alert	Description	Configuration	Requirement IDs
PCI Requirement 9 - Excessive Failed Physical System Access Attempts	This alert triggers when too many failed access attempts to a physical access system occur.	Default Match Count: 20 Default Threshold (Sec) 300	9.1

Requirement 10 Alerts

Alert	Description	Configuration	Requirement IDs
PCI Requirement 10 - Audit Log Cleared	This alert triggers when an audit log is cleared.		10.2.6
PCI Requirement 10 - Microsoft Audit Log Cleared	This alert triggers when the Microsoft Audit Log is cleared.		10.2.6
PCI Requirement 10 - Device Clock Synchronization Problems	This alert triggers when ArcSight SmartConnectors are reporting source events with an incorrect time stamp.		10.4
PCI Requirement 10 - Excessive Failed Account Creations	This alert triggers when an excessive number of unsuccessful attempts to create computer accounts occur.	Default Match Count: 3 Default Threshold (Sec): 300	8.1.2 10.2.7
PCI Requirement 10 - Excessive Failed Account Deletions	This alert triggers when an excessive number of unsuccessful attempts to delete computer accounts occur.	Default Match Count: 3 Default Threshold (Sec): 300	8.1.2 10.2.7
PCI Requirement 10 - Excessive Failed Account Modifications	This alert triggers when an excessive number of unsuccessful attempts to modify computer accounts occur.	Default Match Count: 3 Default Threshold (Sec): 300	8.1.2 10.2.7
PCI Requirement 10 - Excessive Failed Administrative Actions	This alert triggers when an excessive number of failed actions occur by administrative user accounts.	Default Match Count: 20 Default Threshold (Sec): 300	10.2.2
PCI Requirement 10 - Excessive Failed Administrative Logins	This alert triggers when an excessive number of failed login attempts occur by administrative user accounts.		10.1 10.2.1 10.2.4

PCI Requirement 10 - Excessive Failed Authorization Changes	<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>Default Match Count: 3</p> <p>Default Threshold (Sec): 300</p> <p>Default Match Count: 10</p> <p>Default Threshold (Sec): 300</p>	10.2.5
PCI Requirement 10 - Excessive Failed Database Access	This alert triggers when an excessive number of unsuccessful database access attempts occur. Database access attempts can be logins or queries.	<p>Default Match Count: 10</p> <p>Default Threshold (Sec): 300</p>	10.2.4
PCI Requirement 10 - Excessive Failed File Creations	This alert triggers when an excessive number of unsuccessful attempts to create files occur.	<p>Default Match Count: 20</p> <p>Default Threshold (Sec): 300</p>	10.5.5
PCI Requirement 10 - Excessive Failed File Deletions	This alert triggers when an excessive number of unsuccessful attempts to delete files occur.	<p>Default Match Count: 20</p> <p>Default Threshold (Sec): 300</p>	10.5.5
PCI Requirement 10 - Excessive Failed File Modifications	This alert triggers when an excessive number of unsuccessful attempts to modify files occur.	<p>Default Match Count: 10</p> <p>Default Threshold (Sec): 300</p>	10.5.5
PCI Requirement 10 - Excessive Failed Resource Access	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>Default Match Count: 10</p> <p>Default Threshold (Sec): 300</p>	10.2.4
PCI Requirement 10 - Excessive Failed User Actions	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 not listed as an administrative account in the alert.	<p>Default Match Count: 20</p> <p>Default Threshold (Sec): 300</p>	10.2.4

PCI Requirement 10 - Excessive Failed User Logins	Non-administrative user accounts. This alert is triggered for any accounts that are not listed as an administrative account in the alert.	Default Match Count: 10 Default Threshold (Sec): 300	10.2.4
PCI Requirement 10 - Excessive Successful Account Creations	This alert triggers when a large number of computer accounts are successfully created.	Default Match Count: 5 Default Threshold (Sec): 300	8.1.2 10.2.7
PCI Requirement 10 - Excessive Successful Account Deletions	This alert triggers when a large number of computer accounts are successfully deleted.	Default Match Count: 5 Default Threshold (Sec): 300	8.1.2 10.2.7
PCI Requirement 10 - Excessive Successful Account Modifications	This alert triggers when a large number of computer accounts are successfully modified.	Default Match Count: 5 Default Threshold (Sec): 300	8.1.2 10.2.7
PCI Requirement 10 - Excessive Successful Administrative Actions	This alert triggers when an excessive number of successful actions by administrative user accounts occur.	Default Match Count: 300 Default Threshold (Sec): 300	10.2.2
PCI Requirement 10 - Excessive Successful Administrative Logins	This alert triggers when a large number of successful logins by administrative user accounts occur.	Default Match Count: 10 Default Threshold (Sec): 300	10.2.1
PCI Requirement 10 - Excessive Successful Authorization Changes	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.	Default Match Count: 100 Default Threshold (Sec): 300	10.2.5
PCI Requirement 10 - Excessive Successful Database Access	This alert triggers when a large number of successful database accesses are reported. Database access attempts can be logins or queries.	Default Match Count: 100 Default Threshold (Sec): 300	10.2.1

PCI Requirement 10 - Excessive Successful File Creations	This alert triggers when a large number of files are successfully deleted.	Default Match Count: 500 Default Threshold (Sec): 300	10.5.5
PCI Requirement 10 - Excessive Successful Account Deletions	This alert triggers when a large number of files are successfully deleted.	Default Match Count: 500 Default Threshold (Sec): 300	10.5.5
PCI Requirement 10 - Excessive Successful Account Modifications	This alert triggers when a large number of files are successfully modified.	Default Match Count: 1000 Default Threshold (Sec): 300	10.5.5
PCI Requirement 10 - Excessive Successful Resource Access	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.	Default Match Count: 50 Default Threshold (Sec): 300	10.2.1
PCI Requirement 10 - Excessive Successful User Actions	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 not listed as an administrative account in the alert.	Default Match Count: 2000 Default Threshold (Sec): 300	10.2.2
PCI Requirement 10 - Excessive Successful User Logins	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 not listed as an administrative account in the alert.	Default Match Count: 30 Default Threshold (Sec): 300	10.2.1
PCI Requirement 10 - Information System Failure	This alert triggers when an information system failure detected		10.7

Requirement 11 Alerts

Alert	Description	Configuration	Requirement IDs
PCI Requirement 11 - Unauthorized Access Point Detected	This alert triggers when an unauthorized access point event is detected.		11.1
PCI Requirement 11 - Traffic Anomaly on Application Layer	This alert triggers when a traffic anomaly detected on the application layer		11.4
PCI Requirement 11 - Traffic Anomaly on Network Layer	This alert triggers when a traffic anomaly detected on the network layer.		11.4
PCI Requirement 11 - Traffic Anomaly on Transport Layer	This alert triggers when a traffic anomaly detected on the transport layer.		11.4
PCI Requirement 11 - Information Interception Events	This alert triggers when an information interception event is detected.		11.4
PCI Requirement 11 - Attacks and Suspicious Events	This alert triggers when there are events that are categorized as suspicious behavior, hostile behavior, or a compromise.	Default Match Count: 30 Default Threshold (Sec): 300	11.4

Requirement 12 Alerts

Alert	Description	Configuration	Requirement 12
PCI Requirement 12 - Policy Violations	This alert triggers when a policy violations detected on the organization.		12.4

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 5.0)

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 arcsight_doc@microfocus.com.

We appreciate your feedback!