Hewlett Packard
Enterprise

# HPE Security ArcSight HIPAA CIP for Logger

Software Version: 1.0

Solutions Guide

July 27, 2016

# Legal Notices

## Warranty

The only warranties for Hewlett Packard Enterprise products and services are set forth in the express warranty statements accompanying such products and services. Nothing herein should be construed as constituting an additional warranty. Hewlett Packard Enterprise shall not be liable for technical or editorial errors or omissions contained herein.

The information contained herein is subject to change without notice.

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

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

This document is confidential.

## Restricted Rights Legend

Confidential computer software. Valid license from Hewlett Packard Enterprise 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



Follow this link to see a complete statement of copyrights and acknowledgements:
https://www.protect724.hpe.com/docs/DOC-13026

# Support

## Contact Information

| | |
|---|---|
| **Phone** | A list of phone numbers is available on the HPE Security ArcSight Technical Support Page: https://softwaresupport.hp.com/documents/10180/14684/esp-support-contact-list |
| **Support Web Site** | https://softwaresupport.hp.com |
| **Protect 724 Community** | https://www.protect724.hpe.com |

# Contents

# Overview

Compliance with the Health Insurance Portability and Accountability Act (HIPAA) is an important part of any security regime. The HIPAA Compliance Insight Package (CIP) provides a set of Logger reports designed for the detailed examination of HIPAA-related data, which are highly customizable to meet your needs.

For a description of the included reports, see "Running HIPAA Compliance Reports" on page 6.

# Installation

Install the HIPAA Compliance Insight Package (CIP) with the installer file downloaded from the HPE ArcSight Marketplace. The Logger HIPAA CIP is supported on Logger v6.0 and later versions.

### To install the HIPAA Compliance Insight Package for Logger:

1. In Logger, on the main menu, click **Reports**.
2. Click **Deploy Report Bundle.**
3. Under **Step 1: Upload and View Cab Information**, browse to the file <*TBD*>, and then click **Upload**.
4. Under **Step 2: Deploy Objects on Report Server**, review the objects that will be deployed to your report server. Then click **Deploy**. The objects are added to your server.

# Running HIPAA Compliance Reports

By running and reviewing the reports included in the HIPAA Compliance Insight Package, you can easily ensure compliance with HIPAA sections 164-167.

Before running a report, verify that the report's period (start and end date) is for the desired time frame. Period can be retained from previously run reports.

**To access any HIPAA report:**

1. On the Logger main menu, click **Reports**.
2. In the navigation menu, click **Report Explorer.**
3. Select **HIPAA**
4. Select a report to run.
5. Filter the report results by choosing an appropriate filter criterion from each drop-down list specific to the report. (The default, "*" , returns all results for the criterion.)
6. Under **Actions**, select an action to take with the report, such as **Run with Default Options.**

You can run reports, customize, copy or take other actions with any of these reports as you would with other Logger reports. For detailed instructions on how to run, edit, and manage Logger reports, see the *Logger Administrator's Guide*.

You can schedule these reports to run automatically in Logger under **Scheduled Reports** in the navigation menu.

# Report Types

The following report types are available for the HIPAA CIP:

- "164.308 Administrative Safeguards Reports" on the next page
- "164.310 Physical Safeguards Reports" on page 11
- "164.312 Technical Safeguards Reports" on page 12

# 164.308 Administrative Safeguards Reports

The following reports are available for HIPAA 164.308, Administrative Safeguards.

### 164.308 Administrative Safeguard Reports

| Report | Description |
|---|---|
| **Access Report** | Lists all actions by a particular user account. Narrow down the report by modifying the parameters like Device Vendor, Device Product, Activities, Outcome, Destination Address, Source Address, User Account and Destination Port. |
| **Antivirus Agent Stopped** | Identifies the systems where the antivirus agent is disabled. |
| **Antivirus Signature Updates** | <TBD> |
| **Antivirus Update Deployment Events** | Identifies the assets that have successful and unsuccessful antivirus updated deployed. |
| **Attempted Brute Force Attack** | Shows the tuple of source, user account and destination involved in the attempted brute force attack. If the number of failed login events from a source to a destination using a user account exceeds the threshold (default: 50 failed events/day),this incident is considered an attempted brute force attack. Modify this aggregation parameter as per the organization standards by editing the HAVING section of the Attempted Brute Force Attack query. If the report is run for more than 1 day, the aggregation parameter is multiplied by the number of days. |
| **Authorization Changes** | Shows authorization privilege changes made on the system, sorted by event time.It also shows the last time such events happened.<br>By default, the report will display all the activities of all the users in the system. The default parameter's values can be modified according to the actual parameter values. There are different parameters such as User Name, Source and Destination IP addresses,Destination Port, Outcome (Successful and/or Unsuccessful Events),Device Vendor and Device Product to further narrow down the search result for optimized output. |
| **Cross Site Request Forgery Vulnerabilities** | Identifies the cross site request forgery vulnerabilities reported by the scanners. Prioritizing and patching the vulnerabilities helps in securing the organization. |
| **CVSS Score Vulnerabilities Equal Or Greater Than 6** | Identifies the vulnerabilities having CVSS score equal or greater than 6. Prioritizing and patching the vulnerabilities helps in securing the organization. |
| **ESM Information Security Alerts** | Helps security analysts to identify the correlation events (alerts) triggered across the organization. Narrow down the report by modifying the report parameters like Device Vendor, Device Product, Destination Address, Source Address, User Account, Event Severity and Outcome. |
| **Exploit of Vulnerabilities** | Helps security analysts to identify the events about the exploit of vulnerabilities. These events are reported by the Intrusion Detection System when an attempt to exploit a well-known vulnerability, such as the Unicode vulnerability is detected. Narrow down the report by using the parameters like Device Vendor, Device Product, Destination Address and Source Address. |

### 164.308 Administrative Safeguard Reports, continued

| Report | Description |
|---|---|
| **Failed Login Events** | Helps security analysts to identify the failed logins events to identify trends of user account (s) across the assets. Narrow down the scope of the report by using the parameters like Device Vendor, Device Product, Destination Address, and Source Address. |
| **Failed Logins - Sources Targeting Unique Destinations** | Helps security analysts to get the statistics of Failed Login events - Sources Targeting Unique Destinations to identify the rogue user account or sources and/or Destinations under attack. Narrow down the scope of the report by using the parameters like Device Vendor, Device Product |
| **Failed Logins - Destinations Targeted by Unique Sources** | Helps security analysts to get the statistics of Failed Login events - Destinations targeted by Unique Sources to identify the rogue user account or sources or destinations under attack. Narrow down the scope of the report by using the parameters like Device Vendor or Device Product. |
| **Firewall Configuration Changes** | Identifies the successful configuration changes in Firewall appliances. |
| **Firewall Traffic Monitoring** | Shows details about firewall traffic, sorted by event end time. It also shows the last time such a firewall event happened.<br>By default the report will display all firewall-related activities of all users. The default parameter's values can be modified according to the actual parameter values.There are different parameters such as User Name, Source and Destination IP addresses,Destination Port, Outcome (Successful and/or Unsuccessful Events),Device Vendor and Device Product to further narrow down the search result for optimized output. |
| **High Risk Events** | Helps the security analysts to get the overview of the High Risk Events across the organization. This report can be narrowed down by specifying various report parameters like Device Vendor, Device Product, Destination Address, Source Address, User Account, Outcome and Event Severity. |
| **Improper Access Control** | Details improper access control events (such as insecure direct object references, failure to restrict URL access, directory traversal, and failure to restrict user access to functions). |
| **Malware Treatment Failed** | Identifies the infected hosts where the infection was not removed by the antivirus software. |
| **Network Equipment Configuration Changes** | Identifies the configuration changes in network equipment. Authorizing the changes helps in reducing the risks. |
| **Overflow Vulnerabilities** | Identifies the overflow vulnerabilities reported by the scanners. Prioritizing and patching the vulnerabilities helps in securing the organization. |
| **Password Change Activities** | Helps security analysts to identify the password change activities across the organization. This report helps in identifying failed as well as successful password change events for further investigation. Narrow down the scope of the report by using the parameters like Outcome, Device Vendor, Device Product, Destination Address and User Account. |
| **Redirection Attacks Events** | Identifies the redirection attacks across the critical assets of the organization. |
| **Removal of Access** | Shows details about those user accounts whose access rights were being removed or deleted. |

### 164.308 Administrative Safeguard Reports, continued

| Report | Description |
|---|---|
| **Rights** | By default the report is sorted by event end time. |
| **Security Patch Missing** | Identifies the systems with missing security updates. |
| **SSL Vulnerabilities** | Identifies the SSL vulnerabilities reported by the scanners. Prioritizing and patching the vulnerabilities helps in securing the organization. |
| **Successful Brute Force Attack** | Identifies the successful login of user accounts after an attempted brute force attack attempts. If the number of failed login events from a source to a destination using a user account exceeds the threshold (default 50 failed events/day), we consider this incident as the attempted brute force attempt. Modify this aggregation parameter as per the organization standards by editing the HAVING section of the Attempted Brute Force Attack query. If the report is run for more than 1 day, the aggregation parameter gets multiplied by the number of days. |
| **Successful Brute Force Attack** | Tracks the successful login after attempted brute force attack. By default, the aggregation parameter for attempted brute force attack is 50. Modify this aggregation parameter as per the organization standards by editing the HAVING section of the Attempted Brute Force Attack query. If the report is run for more than 1 day, the aggregation parameter gets multiplied by the number of days. |
| **System Misconfiguration** | Helps security analysts to determine risk by identify misconfigured systems. Misconfigured systems poses a greater risk of getting exploited in an organization. |
| **System Restarted Events** | Tracks the reboot of critical assets of the organization. |
| **User Account Created and Deleted Within a Time Frame** | Helps security analysts to identify the user accounts created and deleted within a particular time frame. Hackers usually prefer to create a temporary user account for a task. After the task, they delete it to keep the chance of detection as low as possible. Narrow down the scope of the report by using the parameters like Device Vendor, Device Product, Destination Address and User Account. |
| **User Account Created or Deleted** | Helps security analysts to identify the user accounts created or deleted for getting the statistics of user accounts creation and deletion. Narrow down the scope of the report by using the parameters like Device Vendor, Device Product, Destination Address and User Account. |
| **User Account Enabled and Disabled Within a Time Frame** | Helps security analysts to identify the user accounts enabled and disabled within a particular time frame. Hackers usually prefer to enable the user account and once their task is completed, they disable it to keep the detection as minimum as possible. User Account enabled and disabled event is also generated when the user account is created and deleted respectively. Morever, when the existing user account is enabled/disabled, this event is generated respectively. Narrow down the scope of the report by using the parameters like Device Vendor, Device Product, Destination Address and User Account. |
| **User Account Enabled or Disabled** | Helps the security analysts to identify the user accounts enabled and disabled. Hackers usually prefer to enable the user account and once their task is completed, they disable it to keep the detection as minimum as possible. User Account enabled and disabled event is also generated when the user account is created and deleted respectively. Morever, when the existing user account is enabled/disabled, this event is generated respectively. Narrow down the scope of the report by using the parameters like Device Vendor, Device Product, |

### 164.308 Administrative Safeguard Reports, continued

| Report | Description |
|---|---|
| | Destination Address and User Account. |
| **Virus Activities** | Identifies the virus infection activities across the organization. |
| **VPN Connection Summary** | Shows count information about VPN connections for each user. Details of each user's connection counts are provided, including connection count and systems accessed. |
| **Vulnerabilities** | Helps security analysts to identify all the vulnerabilities reported by scanners. Prioritizing and patching vulnerabilities helps in securing the organization. Narrow down the report by using the report parameters like Device Vendor, Device Product and Destination Address. |
| **Windows Domain Policy Changes** | Identifies the domain policy changes in the Windows environment. |
| **Windows Group Policy Changes** | Identifies the group policy changes in the Windows environment. |

# 164.310 Physical Safeguards Reports

The following reports are available for HIPAA 164.310, Physical Safeguards.

### 164.310 Physical Safeguard Reports

| Report | Description |
|---|---|
| **After Work Hours Building Access Report** | Tracks the after-work hours building access report. |
| **Badge Access Report** | Reports on badge access events. |
| **Data Written To Removable Storage – Microsoft** | Tracks the data written to the removable storage for Microsoft devices. |
| **New External Device Was Recognized By The System** | Tracks new external devices recognized by the system. |
| **Physical Access System Configuration Changes** | Tracks configuration changes in physical access systems. |
| **Physical Access System Events – All** | Collects and tracks all the events reported by physical access systems. |
| **Physical Access System User Account Management Activities** | Tracks user account management activities in physical access systems. |
| **Physical Access System User Account Privilege Management Activities** | Tracks privilege management activities for the user accounts for physical access systems. |
| **Removable Storage Devices Activities** | Tracks removable storage device activities. |

# 164.312 Technical Safeguards Reports

The following reports are available for HIPAA 164.312, Technical Safeguards.

### 164.312 Technical Safeguard Reports

| Report | Description |
|---|---|
| **All Database Access** | Identifies database accesses across the entire organization. |
| **Application Modification** | Tracks all application modifications. |
| **Audit Log Cleared** | Identifies the audit log clearing events. |
| **Confidentiality And Integrity Breach – Overview** | Identifies the events dealing with the confidentiality and integrity breach. |
| **Denial Of Service Sources** | Identifies the sources involved in the denial of service of critical assets of the organization. |
| **Failed Login Event Count – Destination And User Account Pairs** | Identifies the pair of destination and user accounts associated with a failed logins, sorted by count in descending order. Modify the report to include specific number of rows for the report. |
| **Failed Login Event Count – Source And Destination Pairs** | Identifies the pair of sources and destination involved in failed logins, sorted by count in descending order. Modify the report to include specific number of rows for the report. |
| **Failed Login Event Count – Source And User Account Pairs** | Identifies the pair of sources and user accounts, sorted by count in descending order. Modify the report to include specific number of rows for the report. |
| **Failed Login Event Count – Source User Account And Destination Pairs** | Identifies the pair of Source, User Accounts & destination associated with a failed logins, sorted by count in descending order. Modify the report to include specific number of rows for the report. |
| **Failed Login Events** | Identifies the failed login events sorted by the count. The query group the failed login events using source, user accounts and destination column. |
| **Failed Logins – Destination Targeted By Unique User Accounts** | Identifies the destination targeted by unique user accounts, sorted by the count of unique user accounts. Modify the report to include specific number of rows. |
| **Failed Logins – Destinations Targeted By Unique Sources** | Identifies the destinations targeted by unique sources sorted by the count of unique sources. Modify the report to include specific number of rows. |
| **Failed Logins – Sources Attempting Logins With Unique User Accounts** | This reports shows the use of unique user accounts by sources sorted by the count in descending order. |
| **File Creation Deletion And Modification** | This reports lists the creation, deletion and modification activities in system for the files. |
| **Host Operating System** | Tracks the host operating system modification. |

### 164.312 Technical Safeguard Reports, continued

| Report | Description |
|---|---|
| **Modification Events** | |
| **Insecure Cryptographic Storage** | Tracks the vulnerabilities associated with the insecure cryptographic usage. |
| **Invalid Certificate** | Tracks the vulnerabilities dealing with the invalid certificate events. |
| **Logging Devices Review** | Identifies the logging status of the ArcSight SmartConnectors. |
| **Logoff Actions** | Identifies logoff actions from devices. |
| **Microsoft Audit Policy Changes** | Tracks the Microsoft audit policy changes. |
| **Network Equipment Configuration Changes** | Helps security analysts to identify the configuration changes in network equipment. |
| **New Hosts** | This reports Tracks the addition of new hosts to the system. |
| **New Services** | Tracks the services provided by the devices. |
| **No. Of Distinct User Accounts Logged In To A System** | Tracks the number of distinct user accounts logged in to a system, sorted by count in descending order.. |
| **Operating System Configuration Changes** | Tracks the configuration changes in the operation system. |
| **Overflow Vulnerabilities** | Helps security analysts to identify the overflow vulnerabilities reported by the scanners. Prioritizing and patching the vulnerabilities helps in securing the organization. |
| **PHI Systems Providing Unencrypted Services** | Tracks the systems providing unencrypted services. |
| **Traffic Anomaly On Application Layer Events** | Tracks network traffic anomalies on application layer events. |
| **Traffic Anomaly On Network Layer Events** | Tracks network traffic anomalies on network payer events. |
| **Traffic Anomaly On Transport Layer Events** | Tracks network traffic anomalies on transport layer events. |

# 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 system, click the link above and an email window opens with the following information in the subject line:

**Feedback on Solutions Guide (HIPAA CIP for Logger 1.0)**

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 arc-doc@hpe.com.

We appreciate your feedback!