Micro Focus Security
ArcSight Logger CIP for HIPAA

Software Version: 1.01

Solutions Guide

Document Release Date: June, 2018
Software Release Date: June, 2018

Legal Notices

Warranty

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

Restricted Rights Legend

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

Copyright Notice

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/ct-p/productdocs

Contents

Chapter 1: Overview

In 1996, the Health Insurance Portability and Accountability Act (HIPAA) was enacted by the United States Congress. Title II of HIPAA has standardized the way electronic health care information is transmitted among providers and insurers by defining a set of standard transactions.

For example, when a consumer visits a medical clinic, the clinic sends an electronic inquiry to the health care insurance company to verify that the patient is insured. Such electronic transfer of patient information streamlines the health care industry but it introduces a risk that health care and claim information about an individual could be misused. To protect this Protected Healthcare Information (PHI), HIPAA Title II defines the following rules:

- *The Privacy Rule:* This rule establishes national standards for protecting healthcare information. The rule specifies that covered entities (such as health insurers, hospitals, medical providers) put appropriate safeguards into place to protect the privacy of health care information about an individual.
- *The Security Rule:* This rule specifies that covered entities (such as health insurers, hospitals, medical providers) put appropriate safeguards in place to protect the Electronic Protected Healthcare Information (EPHI). These safeguards listed in the next section.

ArcSight Logger CIP for HIPAA

ArcSight Logger Compliance Insight Package (CIP) for HIPAA facilitates compliance with the HIPAA standard using Logger's reporting and dashboarding capabilities. Logger CIP for HIPAA addresses the HIPAA standard by providing:

- Detailed reports which covering Administrative, Technical and Physical Safeguards.
- Dashboards which show a detailed overview of the HIPAA requirements.

The Logger Compliance Insight Package for HIPAA helps demonstrate the following to stakeholders and auditors:

- Implementation of HIPAA controls for your company.
- Due diligence in complying with HIPAA standards, as well as security policies and best practices.
- Real-time monitoring and notification of potential hazardous events, harmful user activity, network vulnerabilities, and configuration changes on healthcare assets.
- Reporting that shows compliance to HIPAA Standard.

Chapter 2: Logger CIP for HIPAA Architecture

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

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

Chapter 3: Installation and Uninstallation

The Logger HIPAA CIP is supported on Logger v6.6 and later versions.

Required Installation Files

These files are required for Logger CIP for HIPAA installation.

Reports and Dashboards Installer: You will need to run the installer for HIPAA reports and dashboards.

- For Logger Appliance, the reports and dashboards installer is called `ArcSight-ComplianceInsightPackage-Logger-HIPAA.1.01.1539.0.enc`
- For software Logger, the reports and dashboards installer is called `ArcSight-ComplianceInsightPackage-Logger-HIPAA.1.01.1539.0.bin`

To install reports and dashboards for the HIPAA CIP, follow the appropriate installation procedure below for your Logger form factor.

Filters and Fieldsets Installers: Additionally, you will need to install filters and field sets. These files are the same for both Logger form factors.

- Filters Installer: `HIPAA_1.0_Filters.xml.gz`
- Field sets Installer: `HIPAA_1.0_Fieldsets.xml.gz`

Installation of these files is as explained under "Installation and Uninstallation" above

Prior to the installation process, download all of these files (the reports and dashboard installer for your form factor, the filters installer, and the field sets installer) to a secure network location.

Installation Process

To install the reports and dashboards for the HIPAA CIP on the Logger Appliance:

1. Log into the Logger user interface.
2. From the Logger top-level menu bar, click **System Admin.**
3. From the **System** section, select **License & Update.**
4. Click **Browse** to locate and open the .enc file you downloaded.
5. Click **Upload Update.** A dialog displays indicating that the update process might take some time.

6. Click **OK**. A message displays indicating that the update is progressing. After the contents of the .enc file are installed, another message displays indicating that the update is a success.

Verify that the content is installed, as follows:

- To view the installed reports, click **Reports** on the top-level menu bar, and then click **Report Explorer** in the **Navigation** section. Click the arrow to the left of HIPAA to see the HIPAA report categories, and then click a category to see the list of reports.
- To view the installed dashboards, click **Dashboards** on the top-level menu and you should see HIPAA Dashboards.

To install the reports and dashboards for the HIPAA CIP on the Software Logger:

1. Log into the system running the Software Logger with the same ID that you used to install the software version of Logger.
2. Go to the directory that contains the .bin file.
3. Change the permissions of the .bin file to be executable:

```
chmod +x ArcSight-ComplianceInsightPackage-Logger-HIPAA.1.01.1539.0.bin
```

4. Run the installer:

```
./ArcSight-ComplianceInsightPackage-Logger-HIPAA.1.01.1539.0
```

5. Follow the instructions provided by the installer to complete the installation. When prompted to choose an installation folder, enter the same directory you specified when you installed the software Logger. For example, if when installing the Software Logger you specified the `/opt/logger` directory, specify `/opt/logger` as the installation folder.

Verify that the content is installed, as follows:

- To view the installed reports, click **Reports** on the top-level menu bar, and then click **Report Explorer** in the Navigation section. Click the arrow to the left of **HIPAA** to see the HIPAA report categories, and then click a category to see the list of reports.
- To view the installed dashboards, click **Dashboards** on the top-level menu.

Installing Filters and Fieldsets

To install filters and fieldsets on Logger Appliance or Software Logger:

1. In Logger, on the main menu, click **Configuration -> Import Content**.

2. Under **Select File to Upload**, click **Browse.**

3. Browse to the file `HIPAA_1.0_Filters.xml.gz`, and then click **Upload Update**.

4. Repeat step 3 for `HIPAA_1.0_Fieldsets.xml.gz.`

5. The HIPAA filter and fieldset CIP content is installed.

Uninstallation

To uninstall Logger CIP for HIPAA content, you must delete each resource individually.

To delete reports:

1. Delete each report in the HIPAA report category:
   - From the **Reports** top-level menu bar, click **Category Explorer** from the **Navigation** section.
   - Right click on **HIPAA**.
   - Click **Delete**.

To delete dashboards:

1. Delete each Product component short name dashboard individually:
   - From the **Configuration** top-level menu bar, click **Dashboards**.
   - For each Product component short name dashboard, click **Tools > Delete Dashboard**.
   - In the confirmation dialog, click **OK** to complete the deletion.

To delete filters:

1. Delete each HIPAA filter individually:
   - From the **Configuration** top-level menu bar, click **Filters** from the **Search** section.
   - For each Product component short name filter, click the **Remove** ✖ icon.
   - In the confirmation dialog, click **OK** to complete the deletion.

To delete fieldsets:

1. Delete each HIPAA fieldset individually:
   - From the **Configuration** top-level menu bar, click **Fieldsets** from the **Search** section.
   - For each HIPAA fieldset, click the **Remove** ✖ icon.
   - In the confirmation dialog, click **OK** to complete the deletion.

Chapter 4: 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 14
- "164.312 Technical Safeguards Reports" on page 15

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 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. 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. 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.

164.308 Administrative Safeguard Reports, continued

Report	Description
Removal of Access Rights	Shows details about those user accounts whose access rights were being removed or deleted. 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.

164.308 Administrative Safeguard Reports, continued

Report	Description
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, 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.

164.312 Technical Safeguard Reports, continued

Report	Description
Host Operating System Modification Events	Tracks the host operating system modification.
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.

Chapter 5: Dashboards

Dashboards give graphic access to data trends.

To view HIPAA CIP dashboards:

1. In Logger, on the main menu bar, click **Dashboards**.
2. From the dashboards drop-down list, select a set of HIPAA dashboards to view.

The HIPAA CIP includes the following dashboards.

HIPAA - Physical Access System Dashboards

Top Failed Destinations (Last 4 Hours)
Top Failed User Accounts (Last 4 Hours)
Failed Login Attempt Count per Hour (Last 24 Hours)
User Account Management Activities (Last 4 Hours)

HIPAA -Technical Safeguard Activity

Failed Logins - Top Source & Destination Pairs
Firewall Monitoring - Denied Conections by Destination Address
Firewall Monitoring - Denied Conections by Source Address

HIPAA - Unencrypted Network Communication

Top Internal Sources to External Network (Last 1 Hour)
Top Internal Sources to Internal Network (Last 1 Hour)
Top Internal Destinations Providing Unencrypted Network Services (Last 1 Hour)

HIPAA - Antivirus Monitoring

Top Failed Antivirus Updates (Last 4 Hours)
Top Failed Antivirus Clean or Quarantine Count per Hour (Last 4 Hours)
Zones with the Most Virus Infections (Last 4 Hours)
Malware Infection Activity per Hour (Last 4 Hours)

HIPAA - Critical Devices Groups Configuration Changes

Configuration Changes - VPN (Last 4 Hours)
Configuration Changes - Network Equipment (Last 4 Hours)
Configuration Changes - Firewall (Last 4 Hours)

HIPAA - Failed Login Events - Monitoring_1

Failed Login Events - Top Destinations (Last 4 Hours)
Failed Login Events - Top Sources (Last 4 Hours)
Failed Login Events - User Accounts (Last 4 Hours)

HIPAA - Failed Login Events - Monitoring_2

Failed Login Events - Top Source and User Account Pairs (Last 4 Hours)
Failed Login Events - Top Destination and User Account Pairs (Last 4 Hours)
Failed Login Events - Top Source to Destination Pairs (Last 4 Hours)
Failed Login Events - Top Source User Account and Destination Pairs (Last 4 Hours)

HIPAA - Physical Security Activity

All Failed Physical Access Events
Top Failed Physical Access Events by User
Failed Physical Facility Access Attempts by 30 Minute Intervals
Last 5 Physical Facility Access Attempts for Past 1 Hour

HIPAA - Vulnerabilities

Vulnerability Scanner Events per Device Vendor (Last 4 Hours)
Top Vulnerability Events per Device Vendor (Last 4 Hours)
IP Addresses with CVSS Score 6 (Last 24 Hours)

Appendix A: Filters

The HIPAA CIP includes these filters, which are used as the basis for reports.

HIPAA 164.308 & 164.312 - Failed Login Events
HIPAA 164.308 & 164.312 - Firewall Configuration Changes
HIPAA 164.308 & 164.312 - Firewall Monitoring - Accepted Connections
HIPAA 164.308 & 164.312 - Firewall Monitoring - All Connections
HIPAA 164.308 & 164.312 - Firewall Monitoring - Denied Connections
HIPAA 164.308 & 164.312 - Removal of Access Rights
HIPAA 164.308 & 164.312 - Successful Login Events
HIPAA 164.308 & 164.312 - Unsuccessful Authorization Change Events
HIPAA 164.308 & 164.312 - User Account Created - Microsoft & Unix
HIPAA 164.308 & 164.312 - User Account Deleted Events - Microsoft & Unix
HIPAA 164.308 & 164.312 - User Account Privilege de-Escalation
HIPAA 164.308 & 164.312 - User Account Privilege Escalation
HIPAA 164.308 & 164.312 - VPN Failed Login Events
HIPAA 164.308 & 164.312 - VPN Successful Login Events
HIPAA 164.308 - ESM Information Security Alerts
HIPAA 164.308 - High Risk Events
HIPAA 164.308 - Successful Antivirus Update Deployment Events
HIPAA 164.308 - Successful Exploit of Vulnerabilities
HIPAA 164.308 - Successful Password Change Activities
HIPAA 164.308 - Unsuccessful Antivirus Update Deployment Events
HIPAA 164.308 - Unsuccessful Exploit of Vulnerabilities
HIPAA 164.308 - Unsuccessful Password Change Activities
HIPAA 164.308 - Virus Activities
HIPAA 164.308 - Vulnerabilities - All
HIPAA 164.310 - Badge Access Report - Failed Access Events
HIPAA 164.310 - Badge Access Report - Successful Access Events
HIPAA 164.310 - Physical Access System - All Events

HIPAA 164.310 - Physical Access System Configuration Changes
HIPAA 164.310 - Physical Access System - User Account Created Events
HIPAA 164.310 - Physical Access System - User Account Deleted Events
HIPAA 164.310 - Physical Access System - User Account Privilege Changes
HIPAA 164.312 - Application Modification Events
HIPAA 164.312 - Audit Logs Cleared
HIPAA 164.312 - Authorization Changes
HIPAA 164.312 - Confidentiality and Integrity Breach - Overview
HIPAA 164.312 - File Creation Deletion and Modification
HIPAA 164.312 - Firewall Configuration Changes
HIPAA 164.312 - Logoff Actions
HIPAA 164.312 - Microsoft Audit Policy Changes
HIPAA 164.312 - Network Equipment Configuration Modification
HIPAA 164.312 - Operating System Configuration Changes
HIPAA 164.312 - PHI Systems Providing Unencrypted Services
HIPAA 164.312 - User Account Lockout Events - Windows

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 HIPAA 1.01)

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!