snare
TOTAL EVENT VISIBILITY

Best practices with Snare Enterprise Agents

snare

About this document

The Payment Card Industry Data Security Standard (PCI/DSS) documentation provides guidance on a set of baseline security measures that are designed to reduce fraud relating to credit cards, and to encourage the adoption of consistent security countermeasures across a range of businesses that are linked by the need to store or process payment card data.

This document discusses the role of Snare agents in meeting PCI/DSS requirements.

Introduction

If you are dealing with any form of payment card data you will need to comply with the PCI/DSS. From May 2018, security audits need to prove compliance with the current PCI/DSS 3.2.1. The Snare Enterprise agent is configured to address these PCI/DSS requirements. Simply review the Enterprise Agent network destination and, if the host holds sensitive data in files or directories, then instigate the Snare FIM option (https://www.snaresolutions.com) to audit and monitor the relevant directories or files.

The agents allow collection of local privileged user activity as well as key log files from systems to send them to a centralized logging system such as the Snare Server or third-party SIEM system. The Snare agent logging and auditing features meet the needs of PCI/DSS requirements for all Windows, Linux, MAC OSX and Solaris-based systems.

If you are running the unsupported Snare Open Source agent software for event logging, you will most likely fail your audit as they do not address two key aspects of the PCI/DSS V3 audit requirements:

1. There is no technical, product, vendor or customer support because you are on an unsupported security tool/platform.

2. More than half of the critical event log data is in the custom event logs, which are not processed by the Open Source agents, so forensic evidence is lost.

Banks and regulators are stepping up their action in the face of recent significant breaches. Open Source agents are not supported and will not stand up to compliance or auditing standards (e.g. PCI/DSS), with more than half of the critical logs not being captured including:

- privileged user activity
- system and group policy changes
- DHCP logs
- system time changes
- host firewall policy changes and access logs
- terminal service access
- print logs.

Therefore, using Snare Open Source agents will risk failing audits and will not be able to detect all serious malicious attacks or unauthorized changes on your systems. This can lead to loss of customer data, major brand damage and significant financial penalties, depending on which standard has been failed and the degree of damage caused. There are approximately 70 system event logs that will be missed by the Open Source agents.

Security standard overview

The latest iteration of the PCI/DSS documentation (version 3.2.1), was released in May 2018. The security standard highlights a wide range of security practices that are designed to enhance the security of credit card information and client details. PCI/DSS requirements should be considered a baseline requirement, and can be enhanced with additional controls to further mitigate risk. A full copy of the standard can be found at https://www.pcisecuritystandards.org/security_standards/documents.php.

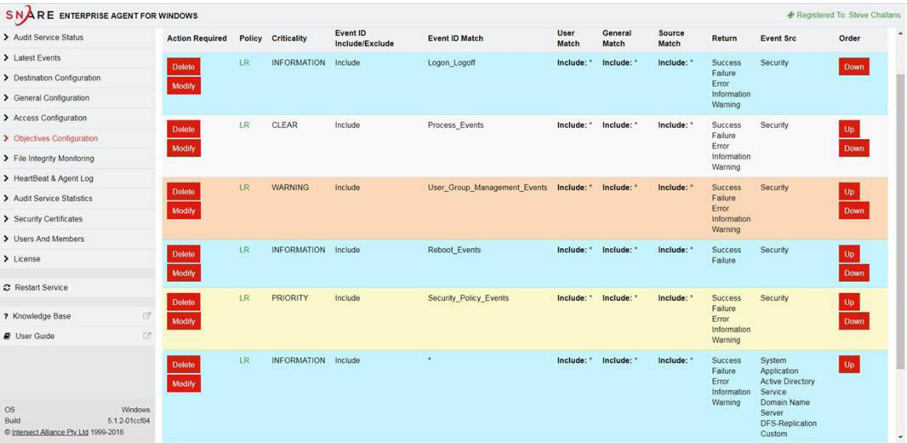
PCI/DSS requirements apply if a primary account number (PAN) is stored, processed, or transmitted. If a PAN is not stored, processed, or transmitted, PCI/DSS requirements do not apply.

Audit logging capabilities underpin a range of security measures within PCI/DSS, however requirement 10 of the document specifically addresses logging and auditing. Requirement 10 is reproduced at the end of this document for reference.

The Snare Enterprise Agents support organizational PCI/DSS security strategies, particularly requirement 10.

Audit collection

The following recommendations highlight strategies that can be implemented on the Snare agents to meet event collection, analysis and reporting requirements for systems, devices and applications that store or process data covered by PCI/DSS. It is strongly recommended that any recommendations below be considered in the light of an organizational risk assessment and security policy.

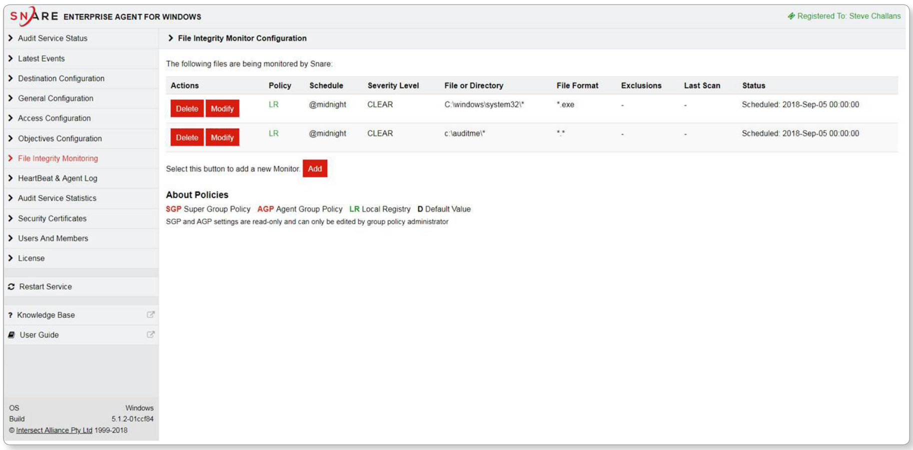


Action Required	Policy	Criticality	Event ID Include/Exclude	Event ID Match	User Match	General Match	Source Match	Return	Event Src	Order
Delete Modify	LR	INFORMATION	Include	Logon_Logoff	Include: *	Include: *	Include: *	Success Failure Error Information Warning	Security	Down
Delete Modify	LR	CLEAR	Include	Process_Events	Include: *	Include: *	Include: *	Success Failure Error Information Warning	Security	Up Down
Delete Modify	LR	WARNING	Include	User_Group_Management_Events	Include: *	Include: *	Include: *	Success Failure Error Information Warning	Security	Up Down
Delete Modify	LR	INFORMATION	Include	Reboot_Events	Include: *	Include: *	Include: *	Success Failure	Security	Up Down
Delete Modify	LR	PRIORITY	Include	Security_Policy_Events	Include: *	Include: *	Include: *	Success Failure Error Information Warning	Security	Up Down
Delete Modify	LR	INFORMATION	Include	*	Include: *	Include: *	Include: *	Success Failure Error Information Warning	System Application Active Directory Service Domain Name Server DFS-Replication Custom	Up

Servers used to host/process cardholder information

In general, the following core event categories should be enabled:

- all management and security events
- logins and logouts (both failed and successful)
- accounts created and deleted
- events pertaining directly to the event/audit log.



File Integrity Monitor Configuration

The following files are being monitored by Snare:

Actions	Policy	Schedule	Severity Level	File or Directory	File Format	Exclusions	Last Scan	Status
Delete Modify	LR	@midnight	CLEAR	C:\windows\system32\*	*.exe	-	-	Scheduled: 2018-Sep-05 00:00:00
Delete Modify	LR	@midnight	CLEAR	c:\auditme\*	*.*	-	-	Scheduled: 2018-Sep-05 00:00:00

Select this button to add a new Monitor. Add

About Policies

SGP Super Group Policy AGP Agent Group Policy LR Local Registry D Default Value

SGP and AGP settings are read-only and can only be edited by group policy administrator

File event monitoring should be considered on those directories that store cardholder or sensitive information. Care should be taken in employing file auditing, since it generally results in a large number of system events being generated. File auditing or file integrity monitoring (FIM) should therefore be configured to monitor only those directories or files that store cardholder information and other sensitive areas of the operating system. In situations where cardholder information is stored within a database, or managed exclusively by a custom application, database and/or application logs may be used to either supplement or supplant file related audit data, assuming:

- appropriate file level access controls are in place
- membership of groups that provide unrestricted access to the underlying data used by the database or application are monitored
- the organizational risk assessment deems the risk acceptable.

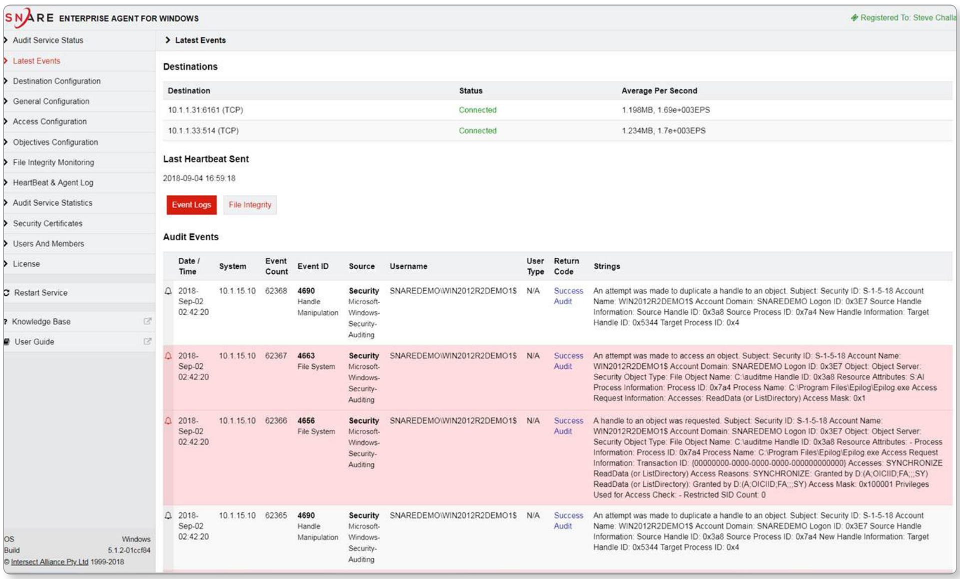
Applications and databases, in general, write audit log data to:

- an operating system log facility (e.g. Windows application log)
- an append-only, rotating, text-format log
- a database auditing log file
- a local or remote syslog server.

Snare agents are available to monitor each of these destinations. Snare Enterprise covers operating systems functions for Windows, Linux, Solaris and MAC OSX. Snare Enterprise Epilog covers application text files and database audit log files. Snare Enterprise for MSSQL covers DBA activity in SQL Server.

The PCI/DSS also requires that “all actions taken by any individual with root or administrative privileges” are logged on any system that processes cardholder information. Unfortunately, older operating systems are generally less capable of auditing at this level of granularity, particularly for file-related events. Most modern operating systems such as Windows and Unix can track user activities to a granular level. However, care should be taken with the objective settings to avoid unnecessary load on the systems.

All systems should be time-synchronized to a central time source for log timestamp consistency.



Destinations

Destination	Status	Average Per Second
10.1.1.31:6161 (TCP)	Connected	1.198MB, 1.69e+003EPS
10.1.1.33:514 (TCP)	Connected	1.234MB, 1.7e+003EPS

Last Heartbeat Sent

2018-09-04 16:59:18

Audit Events

Date / Time	System	Event Count	Event ID	Source	Username	User Type	Return Code	Strings
2018-Sep-02 02:42:20	10.1.15.10	62368	**4690** Handle Manipulation	**Security** Microsoft-Windows-Security-Auditing	SNAREDEMO\WIN2012R2DEMO1$	N/A	Success Audit	An attempt was made to duplicate a handle to an object. Subject: Security ID: S-1-5-18 Account Name: WIN2012R2DEMO1$ Account Domain: SNAREDEMO Logon ID: 0x3E7 Source Handle Information: Source Handle ID: 0x3a8 Source Process ID: 0x7a4 New Handle Information: Target Handle ID: 0x5344 Target Process ID: 0x4
2018-Sep-02 02:42:20	10.1.15.10	62367	**4663** File System	**Security** Microsoft-Windows-Security-Auditing	SNAREDEMO\WIN2012R2DEMO1$	N/A	Success Audit	An attempt was made to access an object. Subject: Security ID: S-1-5-18 Account Name: WIN2012R2DEMO1$ Account Domain: SNAREDEMO Logon ID: 0x3E7 Object: Object Server: Security Object Type: File Object Name: C:\auditme Handle ID: 0x3a8 Resource Attributes: S:AI Process Information: Process ID: 0x7a4 Process Name: C:\Program Files\Epilog\Epilog.exe Access Request Information: Accesses: ReadData (or ListDirectory) Access Mask: 0x1
2018-Sep-02 02:42:20	10.1.15.10	62366	**4656** File System	**Security** Microsoft-Windows-Security-Auditing	SNAREDEMO\WIN2012R2DEMO1$	N/A	Success Audit	A handle to an object was requested. Subject: Security ID: S-1-5-18 Account Name: WIN2012R2DEMO1$ Account Domain: SNAREDEMO Logon ID: 0x3E7 Object: Object Server: Security Object Type: File Object Name: C:\auditme Handle ID: 0x3a8 Resource Attributes: - Process Information: Process ID: 0x7a4 Process Name: C:\Program Files\Epilog\Epilog.exe Access Request Information: Transaction ID: {00000000-0000-0000-0000-000000000000} Accesses: SYNCHRONIZE ReadData (or ListDirectory) Access Reasons: SYNCHRONIZE: Granted by D:(A;OICIID;FA;;;SY) ReadData (or ListDirectory): Granted by D:(A;OICIID;FA;;;SY) Access Mask: 0x100001 Privileges Used for Access Check: - Restricted SID Count: 0
2018-Sep-02 02:42:20	10.1.15.10	62365	**4690** Handle Manipulation	**Security** Microsoft-Windows-Security-Auditing	SNAREDEMO\WIN2012R2DEMO1$	N/A	Success Audit	An attempt was made to duplicate a handle to an object. Subject: Security ID: S-1-5-18 Account Name: WIN2012R2DEMO1$ Account Domain: SNAREDEMO Logon ID: 0x3E7 Source Handle Information: Source Handle ID: 0x3a8 Source Process ID: 0x7a4 New Handle Information: Target Handle ID: 0x5344 Target Process ID: 0x4

OS	Windows
Build	5.1.2-01ccf84

© Intersect Alliance Pty Ltd 1999-2018

General workstations and servers

All management and security events, logins and logouts both failed and successful, and accounts created and deleted, should be logged from workstations and servers that do not directly store or process cardholder information. The Snare Agents used to collect such events should be configured to collect only those events to support this requirement to reduce the flood of information that would otherwise be sent back to a central collection server for analysis and processing.

Process monitoring and file access auditing (also known as FIM) on these servers and workstations is considered less critical, and the general audit strategy should be to collect event log data that may indicate that these systems are used as a jumping-off point to access other systems that host cardholder information.

In situations where general workstations are used as a transitory storage location for cardholder information (for example, spreadsheets), file auditing on the directories or files containing cardholder information that is used for transitory storage is strongly recommended to meet PCI/DSS compliance.

All systems should be time-synchronized to a central time source for log timestamp consistency.

Browsers/proxies

If the primary interface to your cardholder information store is via a web browser, then browser and proxy log data may provide additional information on attacks against your user base.

Monitoring proxy log data for websites that are accessed concurrently with your internal content, searching for known external problem sites that have poor reputation, or scanning logs for cross-site scripting signatures may provide useful information regarding attempts to breach your cardholder data.

Web servers

If the primary interface to your cardholder information store is via a web server/e-commerce system, log data from the web server that hosts the user interface, as well as operating system log files, may provide valuable information on attacks or attempts to scan the server for vulnerabilities.

Monitoring the log data for URL access attempts outside a known authorized subset can highlight attacks against the server itself. Scanning the logs for unexpected data content within 'GET' requests may alert administrators to 'fuzzing' attacks against the web-based application itself and areas that are being targeted for SQL injection, command injection, buffer overflows or cross-site scripting attacks.

All systems should be time-synchronized to a central time source for log timestamp consistency.

Custom applications

Where a custom application provides access to cardholder information, log data from the underlying operating system, or web server in the case of http(s)-based applications, may not provide adequate granularity to meet PCI/DSS requirements.

In situations where the application manages user authentication internally, and/or uses a mechanism to access data that would not be tracked or adequately segregated at the operating system level (e.g. a database or a related amalgamated storage mechanism), it is recommended that the application generates log information that ties authenticated users directly to the activity being performed.

In summary

In the past, Windows-based systems have only relied on three key logs: application; system; and security. With the advent of Windows 2008 and Vista, Windows systems now have many custom Windows event logs that contain administrative activity as well as other valuable logging activity from the host or network. The extra custom event logs are in common use for Windows 2012 and 2016 servers, and Windows 7 and 10 desktop systems. These custom logs also need to be collected from systems.

Administrative user accounts such as Windows administrators/domain admins/unix root user/SQL Server sysadmin users can override technical controls, copy and overwrite data. Therefore, these accounts need to be used only for authorized activity and by trusted staff. However auditing trust is difficult; all we can do is audit user activity. Hence PCI/DSS focuses on these administrative user aspects and ensuring that all relevant logs are kept and stored securely away from the system that generated them, so they can't be tampered with by a compromised account/system or rogue employee.

PCI/DSS standard overview

From the document:

> "The PCI DSS security requirements apply to all system components".
>
> "In the context of PCI DSS, system components are defined as any network component, server, or application that is included in or connected to the cardholder data environment. System components also include any virtualization components such as virtual machines, virtual switches/routers, virtual appliances, virtual applications/desktops, and hypervisors".
>
> "The cardholder data environment is comprised of people, processes and technology that store, process or transmit cardholder data or sensitive authentication data".
>
> "Network components include but are not limited to firewalls, switches, routers, wireless access points, network appliances, and other security appliances".
>
> "Server types include, but are not limited to the following: web, application, database, authentication, mail, proxy, network time protocol (NTP), and domain name server (DNS)".
>
> "Applications include all purchased and custom applications, including internal and external (for example, Internet) applications".
>
> ***Requirement 10: Track and monitor all access to network resources and cardholder data.***
>
> *Logging mechanisms and the ability to track user activities are critical in preventing, detecting, or minimizing the impact of a data compromise.*
>
> *The presence of logs in all environments allows thorough tracking, alerting, and analysis when something does go wrong. Determining the cause of a compromise is very difficult, if not impossible, without system activity logs.*
>
> > *10.1 Implement audit trails to link all access to system components to each individual user.*
> >
> > *10.2 Implement automated audit trails for all system components to reconstruct the following events:*
> >
> > > *10.2.1 All individual user accesses to cardholder data*
> > >
> > > *10.2.2 All actions taken by any individual with root or administrative privileges*
> > >
> > > *10.2.3 Access to all audit trails*
> > >
> > > *10.2.4 Invalid logical access attempts*
> > >
> > > *10.2 5 Use of and changes to identification and authentication mechanisms—including but not limited to creation of new accounts and elevation of privileges—and all changes, additions, or deletions to accounts with root or administrative privileges.*
> > >
> > > *10.2.6 Initialization stopping or pausing of the audit logs*
> > >
> > > *10.2.7 Creation and deletion of system-level objects.*

10.3 Record at least the following audit trail entries for all system components for each event:

10.3.1 User identification

10.3.2 Type of event

10.3.3 Date and time

10.3.4 Success or failure indication

10.3.5 Origination of event

10.3.6 Identity or name of affected data, system component, or resource.

10.4 Using time synchronization technology, synchronize all critical system clocks and times and ensure that the following is implemented for acquiring, distributing, and storing time.

10.4.1 Critical systems have the correct and consistent time.

10.4.2 Time data is protected

10.4.3 Time settings are received from industry-accepted time sources.

10.5 Secure audit trails so they cannot be altered.

10.5.1 Limit viewing of audit trails to those with a job-related need.

10.5.2 Protect audit trail files from unauthorized modifications.

10.5.3 Promptly back-up audit trail files to a centralized log server or media that is difficult to alter.

10.5.4 Write logs for external-facing technologies onto a secure centralized internal log server or media device.

10.5.5 Use file integrity monitoring or change detection software on logs to ensure that existing log data cannot be changed without generating alerts (although new data being added should not cause an alert).

10.6 Review logs and security events for all system components to identify anomalies or suspicious activity. Note: Log harvesting, parsing, and alerting tools may be used to meet this Requirement.

10.6.1 Review the following at least daily:

- *All security events*
- *Logs of all system components that store, process, or transmit CHD and/or SAD*
- *Logs of all critical system components*
- *Logs of all servers and system components that perform security functions (for example, firewalls, intrusion-detection systems/intrusion-prevention systems (IDS/IPS), authentication servers, e-commerce redirection servers, etc.).*

10.6.2 Review logs of all other system components periodically based on the organization's policies and risk management strategy, as determined by the organization's annual risk assessment.

10.6.3 Follow up exceptions and anomalies identified during the review process

10.7 Retain audit trail history for at least one year, with a minimum of three months immediately available for analysis (for example, online, archived, or restorable from back-up).

10.8 Additional requirement for service providers only: Implement a process for the timely detection and reporting of failures of critical security control systems, including but not limited to failure of:

- *Firewalls*
- *IDS/IPS*
- *FIM*
- *Anti-virus*
- *Physical access controls*
- *Logical access controls*
- *Audit logging mechanisms*
- *Segmentation controls (if used)*

Note: This requirement is a best practice until January 31, 2018, after which it becomes a requirement.

10.8.1 Additional requirement for service providers only: Respond to failures of any critical security controls in a timely manner. Processes for responding to failures in security controls must include:

- *Restoring security functions*
- *Identifying and documenting the duration (date and time start to end) of the security failure*
- *Identifying and documenting cause(s) of failure, including root cause, and documenting remediation required to address root cause*
- *Identifying and addressing any security issues that arose during the failure*
- *Performing a risk assessment to determine whether further actions are required as a result of the security failure*
- *Implementing controls to prevent cause of failure from reoccurring*
- *Resuming monitoring of security controls*

Note: This requirement is a best practice until January 31, 2018, after which it becomes a requirement

10.9 Ensure that security policies and operational procedures for monitoring all access to network resources and cardholder data are documented, in use, and known to all affected parties

snare

TOTAL EVENT VISIBILITY

Contact Snare

APAC
+61 8 8213 1200
apac@snaresolutions.com

Americas
+1 (800) 834 1060
americas@snaresolutions.com

EMEA
+44 (797) 090 5011
emea@snaresolutions.com

Adelaide (Head Office)
+61 8 8213 1200
Level 1, 76 Waymouth St
Adelaide, SA 5000
Australia

ABN: 84 151 743 976