



PCI DSS and GFI EventsManager 7

PCI DSS requirements	Auditing	Monitoring and reporting	Alerting	Enforcing	Notes
Requirement 1: Install and maintain a firewall configuration to protect cardholder data					
1.3 Build a firewall configuration to restrict connections to cardholder data					
1.3.1 Restricting inbound Internet traffic to IP addresses within the DMZ		●	●		Create new rules
1.3.6 Securing and synchronizing router configuration files		✓	✓		Customize default rules and reports **
1.3.7 Denying all other inbound and outbound traffic not specifically allowed		●	●		Create new rules
Requirement 2: Do not use vendor-supplied default passwords					
2.2 Develop configuration standards for all system components					
2.2.2 Disable all unnecessary and insecure services and protocols		●	●		Requirement not supported by default *
Requirement 3: Protect stored cardholder data					
3.5 Protect encryption keys used for encryption of cardholder data against both disclosure and misuse:					
3.5.1 Restrict access to keys to the fewest number of custodians necessary		✓	✓		Customize default rules and reports **
3.6 Fully document and implement all key management processes and procedures for keys used for encryption of cardholder data					
3.6.3 Secure key storage		✓	✓		Customize default rules and reports **
Requirement 7: Restrict access to cardholder data by business need-to-know					
7.1 Limit access to computing resources and cardholder information only to those individuals whose job requires such access		✓	✓		Customize default rules and reports **
7.2 Establish a mechanism for systems with multiple users that restricts access based on a user's need to know, and is set to "deny all" unless specifically allowed		✓	✓		Customize default rules and reports **
Requirement 8: Assign a unique ID to each person with computer access					
8.5 Ensure proper user authentication and password management for non-consumer users and administrators					
8.5.1 Control addition, deletion, or modification of user IDs, credentials, and other identifier objects		✓	✓		Default rules and reports
8.5.2 Verify user identity before performing password resets		✓	✓		Default rules and reports
8.5.3 Set first-time passwords to a unique value for each user & change immediately after first use		✓			Default reports
8.5.4 Immediately revoke access for any terminated users		✓	✓		Default rules and reports
8.5.5 Remove inactive user accounts at least every 90 days		✓			Default reports
8.5.6 Enable accounts used by vendors for remote maintenance only during the time period needed		✓	✓		Default rules and reports

PCI DSS requirements	Auditing	Monitoring and reporting	Alerting	Enforcing	Notes
8.5.13 Limit repeated access attempts by locking out the user ID after not more than six attempts		✓			Default reports
8.5.16 Authenticate all access to any database containing cardholder data		✓	✓		Default rules and reports
Requirement 10: Track and monitor all access to network resources and cardholder data					
10.1 Log all individual user access to system components, especially administrative users	✓	✓			Customize default rules and reports **
10.2 Implement automated audit trails for all system components to reconstruct the following events:					
10.2.1 All individual accesses to cardholder data	✓	✓		✓	Customize default rules and reports **
10.2.2 All actions taken by any individual with root or administrative privileges	✓	✓		✓	Default rules
10.2.3 Access to all audit trails	✓	✓		✓	Default rules and reports
10.2.4 Invalid logical access attempts	✓	✓		✓	Default rules and reports
10.2.5 Use of identification and authentication mechanisms	✓	✓		✓	Default rules and reports
10.2.6 Initialization of the audit logs	✓	✓		✓	Default rules and reports
10.2.7 Creation and deletion of system-level objects	✓	✓		✓	Default rules and reports
10.3 Record audit trail details for all system component related events	✓			✓	
10.4 Synchronize all critical system clocks and times		✓	✓		Default rules
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		✓	✓		Default rules and reports
10.5.2 Protect audit trail files from unauthorized modifications		✓	✓		Default rules and reports
10.5.5 Use file integrity monitoring and change detection software on logs to ensure that existing log data cannot be changed (except for new data) without generating alerts		✓	✓	✓	Default rules and reports
10.6 Review logs for all system components at least daily		✓		✓	Schedule default reports
Requirement 11: Regularly test security systems and processes					
11.1 Test security controls, limitations, network connections, and restrictions annually to assure the ability to adequately identify and to stop any unauthorized access attempts		●	●		
11.4 Use network intrusion detection systems, host-based intrusion detection systems, and intrusion prevention systems to monitor all network traffic and alert personnel to suspected compromises		●	●	●	Create new rules
11.5 Deploy file integrity monitoring software to alert personnel to unauthorized modification of critical system or content files			✓	✓	Default rules and reports

* Necessitates the creation of a new event processing rule which cannot directly enforce this requirement but supports administrators through monitoring, reporting and alerting.

** Necessitates changing the configuration settings of default rules and reports, by specifying parameters consistent with your network environment.

Legend

- ✓ Requirement fully supported
- Requirement partially supported through reporting or product customization. Certain conditions may apply.

Note: Conditions apply which include, but are not limited to:

- Windows Security Settings, such as Password Policy and Audit Policy
- User account settings
- Third-party software and devices, such as firewalls, being properly installed and configured