

Payment Card Industry Data Security Standard (PCI DSS) states in Requirement 10 that you must "Track and monitor all access to network resources and cardholder data".

It further states, "Logging mechanisms and the ability to track user activities are critical. The presence of logs in all environments allows thorough tracking and analysis if something does go wrong. Determining the cause of a compromise is very difficult without system activity logs."

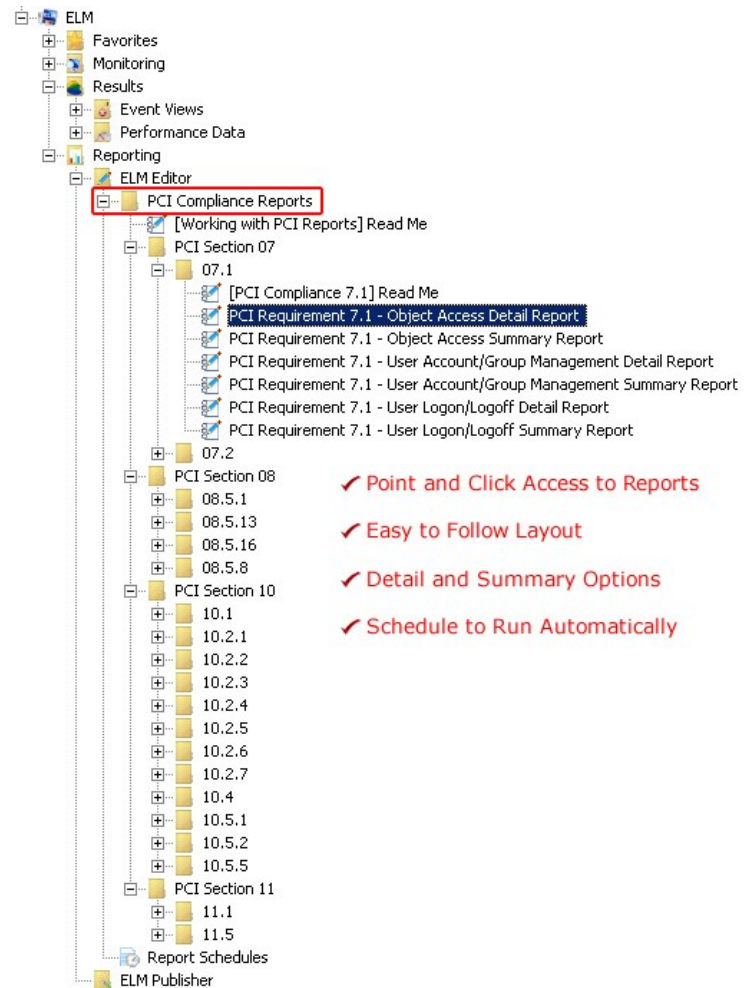
ELM Enterprise Manager supports PCI compliance for payment service providers and merchants who must track and report on all access to their network resources and cardholder data through system activity logs. ELM Enterprise Manager provides support for **PCI Requirement 10.6** as well as several other requirements listed on the next page.

"Review logs for all system components at least daily. Log reviews must include those servers that perform security functions like intrusion-detection system (IDS) and authentication, authorization, and accounting protocol (AAA) servers (for example, RADIUS)."

ELM's real-time monitoring, alerting and reporting provides IT Security and Compliance Managers with the tools they need to help meet this requirement.

All event data is securely stored in Microsoft SQL Server databases. Automatic archive rollover databases provide simplified data retention management and assist in complying with **PCI Requirement 10.7**, keeping 3 months of data readily accessible and one full year of data securely stored and available.

The PCI DSS Reports Management Pack installs a set of **Custom Reports** into the ELM Editor Reporting Container as well as custom PCI Event Views into the Event Views container, allowing quick and easy access to reports and data.



Real-Time Server Monitoring and Event Log Management



- **Requirement 7.1** - Limit access to computing resources and cardholder information only to those individuals whose job requires such access.
- **Requirement 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.
- **Requirement 8.5.1** - Control addition, deletion, and modification of user IDs, credentials, and other identifier objects.
- **Requirement 8.5.8** - Do not use group, shared, or generic accounts and passwords.
- **Requirement 8.5.13** - Limit repeated access attempts by locking out the user ID after not more than six attempts.
- **Requirement 8.5.16** - Authenticate all access to any database containing cardholder data. This includes access by applications, administrators, and all other users. Restrict user direct access or queries to databases to database administrators.
- **Requirement 10.1** - Establish a process for linking all access to system components (especially access done with administrative privileges such as root) to each individual user.
- **Requirement 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 assessment trails.
 - **10.2.4** - Invalid logical access attempts.
 - **10.2.5** - Use of identification and authentication mechanisms.
 - **10.2.6** - Initialization of the assessment logs.
 - **10.2.7** - Creation and deletion of system-level objects.
- **Requirement 10.5** - Secure audit trails so they cannot be altered.
 - **10.5.1** - Limit viewing of assessment trails to those with a job-related need.
 - **10.5.2** - Protect assessment trail files from unauthorized modifications.
 - **10.5.5** - Use file integrity monitoring and change detection software on logs to ensure that existing log data cannot be changed without generating alerts.
- **Requirement 10.6** - Review logs for all system components at least daily. Log reviews must include those servers that perform security functions like intrusion-detection system (IDS) and authentication, authorization, and accounting protocol (AAA) servers (for example, RADIUS).
- **Requirement 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. Use a wireless analyzer at least quarterly to identify all wireless devices in use.
- **Requirement 11.5** - Deploy file-integrity monitoring tools to alert personnel to unauthorized modification of critical system files, configuration files, or content files; and configure the software to perform critical file comparisons at least weekly.
- **Requirement 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.
- **Requirement 10.5** - Secure audit trails so they cannot be altered.
 - **10.5.1** - Limit viewing of assessment trails to those with a job-related need.
 - **10.5.2** - Protect assessment trail files from unauthorized modifications.
 - **10.5.5** - Use file integrity monitoring and change detection software on logs to ensure that existing log data cannot be changed without generating alerts.
- **Requirement 10.6** - Review logs for all system components at least daily. Log reviews must include those servers that perform security functions like intrusion-detection system (IDS) and authentication, authorization, and accounting protocol (AAA) servers (for example, RADIUS).
- **Requirement 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. Use a wireless analyzer at least quarterly to identify all wireless devices in use.
- **Requirement 11.5** - Deploy file-integrity monitoring tools to alert personnel to unauthorized modification of critical system files, configuration files, or content files; and configure the software to perform critical file comparisons at least weekly.