COMPLIANCE

Payment Card Industry Data Security Standard (PCI-DSS) Compliance with Aldon Lifecycle Manager

The Payment Card Industry requires all organizations that store or process credit card data and transactions to implement technical security requirements on all systems involved in data storage and transmission. These control requirements range from encryption methods, to access rights management, to vulnerability testing.

In typical implementations, Cardholder Data (CHD) would not be stored directly within Rocket® Aldon Lifecycle Manager (LM). However, certain PCI-DSS requirements involve development and change control over PCI systems. Rocket Aldon Lifecycle Manager has robust security controls available to enable a company to design and implement controls to meet PCI-DSS requirements. The relevant requirements and capabilities that LM offers to meet them are listed on the following pages.

PCI-DSS REQUIREMENTS	ROCKET ALDON LIFECYCLE MANAGER CAPABILITIES
2.1 Always change vendor-supplied defaults and remove or disable unnecessary default accounts before installing a system on the network.	Rocket Aldon Lifecycle Manager and its associated modules (LMi, LMe, Rocket Aldon Community Manager (CM), and Security Service Manager) support unique user IDs with customizable passwords for all individuals accessing the systems.
2.3 Encrypt all non-console administrative access using strong cryptography.	Users access the web-based LMe, Security Service Manager, and CM systems using encrypted HTTPS sessions. LMi utilizes encrypted SSH sessions.
6.3 Develop internal and external software applications (including web-based administrative access to applications) securely: • In accordance with PCI DSS (for example, secure authentication and logging) • Based on industry standards and/or best practices • Incorporating information security throughout the software development lifecycle • Removing development, test, and/or custom application accounts, user IDs, and passwords before applications become active or are released to customers • Reviewing custom code prior to release to production or customers, to identify any potential coding vulnerability (using either manual or automated processes) • Ensuring that code changes are reviewed by individuals other than the originating code author, and by individuals knowledgeable about code review techniques and secure coding practices • Ensuring that code is developed according to secure coding guidelines • Implementing appropriate corrections prior to release • Ensuring that code review results are reviewed and approved by management prior to release	CM supports workflows for changes and development activities, such as requests, approvals, testing, acceptance, and any other stages required by an organization's policies. LM supports multiple development environments that are customizable by the organization, such as development, test, staging, and production. Access for individual users to access, modify, or approve code can be assigned for specific projects, release versions, and environments. Developers can be restricted from making changes to software in testing or production. The ability to migrate between development, test, and production environments can also be restricted to appropriately segregated users. All actions within LM and its associated modules, including code changes and promotions, are fully logged and reportable. Changes made to code are highlighted by the Harmonizer module, which supports formal, independent reviews of code changes before promotion to ensure that changes are in accordance with an approved work order.
6.4 Follow change control processes and procedures for all changes to system components. The processes must include the following: • Development/test environments must be separate from production environments, enforced with access controls • Duties between development/test and production environments must be separated • Production data (live PANs) may not be used for testing or development • Test data and accounts must be removed before production systems become active • Change control procedures must include documentation of impact and change approval by authorized parties • Functionality testing must verify that the change does not adversely impact the security of the system • Back-out procedures • Upon completion of a significant change, all relevant PCI DSS requirements must be implemented on all new or changed systems and networks, and documentation must be updated as applicable	LM supports multiple development environments that are customizable by the organization, such as development, test, staging, and production. Access for individual users to access, modify, or approve code can be assigned for specific projects, release versions, and environments. Developers can be restricted from making changes to software in testing or production. The ability to migrate between development, test, and production environments can also be restricted to appropriately segregated users. Emergency changes can be allowed, but this requires approval of a retroactive merge to the development environment.

PCI-DSS REQUIREMENTS	ROCKET ALDON LIFECYCLE MANAGER CAPABILITIES
7.1 Limit access to system components and cardholder data to only those individuals whose job requires such access. Define access needs for each role, including system components and data resources needed for job function, and level of privilege required (such as user, administrator) for accessing resources. Restrict access to privileged user IDs to least privileges necessary to perform job responsibilities. Assign access based on individual personnel's job classification and function. Require documented approval by authorized parties specifying required privileges.	Detailed, customizable role-based access levels let an organization define the exact capabilities of each system user. Permissions are granular to support any organization's business needs according to the rule of least privilege and segregation of duties. The CM module supports automated, system-driven workflows that may include access request, authorization, and provisioning processes, as well as termination and offboarding processes. Workflows can be assigned to Security Service Manager administrators for LM, as well as administrators for any other system in use at an organization. Reports are available showing all users with their associated access capabilities and administrative activity performed within the system, including the modification of user access and roles.
7.2 Establish an access control system for system components with multiple users that restricts access based on a user's need to know, and is set to "deny all" unless specifically allowed.	Roles are customizable to meet an organization's specific controls requirements.
8.1 Define and implement policies and procedures to ensure proper user identification management for non-consumer users and administrators on all system components, as follows: • Assign all users a unique ID before allowing them to access system components or cardholder data • Control addition, deletion, and modification of user IDs, credentials, and other identifier objects • Revoke access for any terminated users immediately • Remove/disable inactive user accounts at least every 90 days • Manage IDs used by vendors to access, support, or maintain system components through remote access • Limit repeated access attempts by locking out the user ID after not more than six attempts. • Set the lockout duration to a minimum of 30 minutes or until administrator enables the user ID • Require the user to re-authenticate to re-activate the terminal or session if a session has been idle for more than 15 minutes	ALM and its associated modules (LMi, LMe, CM, and Rocket Aldon Security Service Manager) support unique user IDs for all individuals accessing the systems. Ryan incorrect product terminology System administration is performed through the separate Security Service Manager module, with access restricted to designated administrative users. The Community Manager module supports automated, system-driven workflows that may include access request, authorization, and provisioning processes, as well as termination and offboarding processes.
8.2 In addition to assigning a unique ID, ensure proper user-authentication management for non-consumer users and administrators on all system components by employing at least one of the following methods to authenticate all users: • Something you know, such as a password or passphrase • Something you have, such as a token device or smart card • Something you are, such as biometrics	Passwords are required for users to access each system. LMi also supports integration with IBM i user credentials, and CM supports LDAP integration with Active Directory credentials.
8.5 Do not use group, shared, or generic accounts and passwords, or other authentication methods.	LM and its associated modules (LMi, LMe, CM, and Rocket Aldon Security Service Manager) support unique user IDs for all individuals accessing the systems.
9.1 Use appropriate facility entry controls to limit and monitor physical access to systems in the cardholder data environment.	Systems are installed on premises, and the organization can implement physical and environmental controls as with all other computing equipment.

PCI-DSS REQUIREMENTS	ROCKET ALDON LIFECYCLE MANAGER CAPABILITIES
10.1 Implement audit trails to link all access to system components to each individual user.	All actions within LM and its associated modules are fully logged. Logs are linked to individuals performing the actions.
10.2 Implement automated audit trails for all system components to reconstruct the following events: • All individual accesses to cardholder data • All actions taken by any individual with root or administrative privileges • All audit trails • Invalid logical access attempts • Use of 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 • Initialization, stopping, or pausing of the audit logs • Creation and deletion of system-level objects	All actions within LM and its associated modules, including code changes and promotions, access to or modification or data, and user access management, are fully logged and reportable.
10.3 Record at least the following audit trail entries for all system components for each event: • User identification • Type of event • Date and time • Success or failure indication • Origination of event • Identity or name of affected data, system component, or resource	LM logs include all relevant details of each recorded event.
12.6 Implement a formal security awareness program to make all personnel aware of the cardholder data security policy and procedures. Educate personnel upon hire and at least annually. Require personnel to acknowledge at least annually that they have read and understood the security policy and procedures.	The CM module supports automated, system-driven workflows that may include information security training programs.
12.7 Screen potential personnel prior to hire to minimize the risk of attacks from internal sources. (Examples of background checks include previous employment history, criminal record, credit history, and reference checks.)	The CM module supports automated, system-driven workflows that may include employee onboarding and background check processes.

rocketsoftware.com
info@rocketsoftware.com
US: 1 877 577 4323
EMEA: 0800 520 0439
APAC: 1800 823 405
twitter.com/rocket
www.linkedin.com/company/rocket-software
www.facebook.com/RocketSoftwareInc
blog.rocketsoftware.com