Emerald 5

Payment Card Industry (PCI)
Security Standards Compliance

Emerald Management Suite

IEA Software, Inc.

Introduction

The purpose of this document is to assist those seeking PCI compliance from the perspective of Emerald version 5. Only questions and responses relevant to the Emerald Management Suite are provided. There are many remaining organizational and management requirements outside the scope of this document. All questions in this document are from the PCI self-assessment questionnaire available via the Internet: https://www.pcisecuritystandards.org/

Requirements

Requirement 2: Use of default passwords

2.1 Have all default passwords been changed or disabled before placing the system into production?

Be sure to change the default operator admin account password from 'pass1' to a secure password as soon as possible after installing Emerald.

2.3 Is remote access for system management secure?

Emerald supports TLS encryption. You should either obtain an TLS certificate from a trusted third party or create a self-signed certificate installing public key to each browsers trusted certificate store. Avoid using sample TLS certificate included with Emerald. This private key is well known and offers no protection.

Requirement 3: Protection of stored data

3.1 Is sensitive data removed as soon as it is no longer needed?

Automatic clearing of sensitive data from accounts when no longer needed is configured from the Emerald Admin / Reports & Logs / Log Trimming / Trim days for Sensitive Data options.

3.2.1 Card track data must not be stored.

Yes, Emerald does not store full stripe track data.

3.2.2 Card security/CVV2 codes must not be stored.

Yes, CVV2 is recorded only long enough to complete the transaction and then all references to it are cleared.

3.2.3 Storage of account PIN codes prohibited

Yes, this information is not stored

3.3 Masking of account numbers

To enable masking of all but last four see the Emerald Admin / Security / Group Rights / CC/EFT visibility option.

3.4 System wide secure storage of sensitive account data

While largely an implementation question you can enable encrypted storage of sensitive information such as account passwords and account numbers from the Emerald Admin / Security / Encryption menu. Please be sure to read all dialogues before encrypting your database.

3.5 Encryption key management

Encryption keys for Emerald can be stored in the operating systems key chain or encrypted file systems.

3.6 Sensitive information should not be recorded to audit logs

Yes, Emerald does not record account numbers in audit logs.

Requirement 4: Encrypt transmission of cardholder data and sensitive information across public networks

4.1 Secure transmission of CC/EFT transactions over the Internet?

Yes, all transactions over public networks are encrypted using TLS with validation of the trust chain.

4.2 Is encryption used when account numbers transmitted via email?

Emerald does not transmit account numbers via email.

Requirement 6: Secure applications

6.1, 6.2 Latest security related patches applied?

The latest version of emerald is available for download from the Emerald product site:
http://www.iea-software.com/emerald#download

Release histories are also available from the IEA Software document site:
http://www.iea-software.com/docs

You may subscribe to receive email notification of important updates by clicking the forum link from the IEA Software web site.

6.5 Secure coding guidelines for web applications

Emerald is a secure application designed to protect against a wide range of threats including input validation, database injection, XSS, CSRF, exception handling, DoS countermeasures, buffer management and circumvention of access controls.

Requirement 8: One operator account per operator

8.4 Encryption of stored passwords for operator access

Use TLS, Encrypted storage of sensitive information such as account passwords and account numbers can be enabled from the Emerald Admin / Security / Encryption menu. Please be sure to read all dialogues before encrypting your database.

8.5.2 Prompt for current password before setting new password

Yes, Emerald requires entry of current password to set new password

8.5.4 Immediate interruption of operator access

Yes, If an operator is online when their access is revoked the operators session can be disconnected from the Emerald Admin / Web Interface / Active Sessions menu.

8.5.9 Password change policy for operators

Emerald does not currently enforce a password change policy for operators and therefore should be handled administratively.

8.5.10, 8.5.11, 8.5.12 Establish operator password policy on length, complexity and reuse of previous passwords.

Password length requirements are configurable from the Emerald Admin / Web Interface / Client Settings menu. Emerald does not store previously used operator passwords and is not able to enforce either policy in terms of determining password strength or reuse of previous passwords.

8.5.13 Lockout for failed access attempts to mitigate brute force password guessing.

Yes, Emerald logons are protected by a short-term lockout interval configured via the Emerald Admin / Web Interface / Operator Settings / Bad Password lockout interval option.

8.5.15 Enforcement of a 15-minute session idle disconnect policy.

Session idle timeout is configured from the Emerald Admin / Web Interface / Operator Settings / Idle timeout (seconds) option.

8.5.16 Authenticate all system accesses

All access to Emerald data requires authentication.

Requirement 10: Monitoring data access

10.2 Is all access involving sensitive data logged?

Yes, to enable detailed client access logging enable the Access logging debug option from the Debug options menu of the Emerald configuration server. (/settings URL)

10.0.3.1-10.0.3.6 Does access logging provide operator, type of operation, its status and timestamp?

This information is available from the Emerald access log.

10.6 Logging of network devices and authentication systems

Emerald includes a syslog server that can be used to centrally collect log data from various network devices for review from the Emerald Client / Reports / System logs menu of Emerald. Authentication failures are also available from the globally sourced daily error summary report.

10.7 Maintenance of audit logging. At least 3-month online, 1-year offline.

Options controlling the retention of logs stored in the Emerald database are configurable from the Emerald Admin / Reports & Logs / Log Trimming menu.

Appendix A: Resellers / VISPs

A.1.1, A.1.2 each reseller limited to subset of accounts?

Make sure that each organization only has MBR object group access to the billing groups they control.

A.1.3 Logging of all reseller actions.

Yes, Emerald access logging applies to all operators of all organizations.

A.1.4 Capability to investigate system compromise.

See Emerald access and audit logs