HP Real User Monitor (RUM) Readiness for PCI-DSS 2.0

The Payment Card Industry Data Security Standard (PCI-DSS) is an accepted set of policies and procedures intended to optimize the security of credit card use and to protect against misuse of cardholder information.

PCI-DSS and RUM Monitoring
This document explains the scope of PCI-DSS 2.0 as relevant to RUM, and how organizations that want to be PCI-DSS 2.0 compliant can configure and use RUM.

Introduction

Overview

The PCI-DSS standard was developed in 2004 by the founding payment brands of the PCI Security Standards Council, including American Express, Discover Financial Services, JCB, MasterCard Worldwide and Visa International, to help facilitate the broad adoption of consistent data security measures on a global basis.
PCI-DSS is a multifaceted security standard that includes requirements for security management, policies, procedures, network architecture, software design and other critical protective measures. This comprehensive standard is intended to help organizations proactively protect customer account data. (The current version of the standard is version 2.0, released on 26 October 2010.)

The standard defines several types of entities and unique requirements for each type. Examples of such entities are:

- A company operating a web site on which credit card transactions can be processed (requires PCI-DSS compliancy).

- A third party payment application that is used for credit card transactions (requires Payment Application Data Security Standard (PA-DSS) compliancy).

- A third party application that does not include payment transactions, but may require card holder data (should be PCI-DSS ready to enable site PCI-DSS certification). In order to be compliant with PCI-DSS or PA-DSS, an entity must pass third party security checks by a Qualified Security Assessor (QSA).

This document explains the scope of PCI-DSS as relevant to RUM and describes RUM readiness for PCI-DSS 2.0. It also provides recommendations for how RUM users can configure and use RUM as part of obtaining PCI-DSS 2.0 compliancy for their organization. This document is intended to act as guidance only and the end user is ultimately responsible for maintaining a compliance program that meets the requirements of PCI-DSS.

May 2013

HP Real User Monitor

RUM is used to collect and analyze data obtained from a web site's network traffic. As RUM can be configured to monitor card holder information, it is important that customers in PCI-DSS governed environments are aware of RUM's status regarding PCI-DSS requirements, and how to configure RUM for PCI-DSS 2.0 readiness.

The Scope of PA-DSS

The Payment Application Data Security Standard (PA-DSS) applies to software vendors and others who develop payment applications that store, process, or transmit cardholder data as part of authorization or settlement, where these payment applications are sold, distributed, or licensed to third parties.
For details on PA-DSS, see: https://www.pcisecuritystandards.org/documents/pa-dss_v2.pdf

Applicability of PA-DSS to RUM

RUM is not a Payment Application and therefore does not require PA-DSS certification. However, an entity that wants to be PCI-DSS 2.0 compliant (for example, a company operating a web site on which credit card transactions can be made) can use a third party non-payment application that is not PA-DSS compliant, as long as that application is PCI- DSS ready. RUM is PCI-DSS ready.

Below is a table describing RUM's readiness for PCI-DSS.

RUM Implementation for PCI-DSS Readiness

PCI-DSS 2.0 Ready	Guideline	RUM Configuration
Build and Maintain a Secure Network	1. Install and maintain a firewall configuration to protect cardholder data. 2. Do not use vendor-supplied defaults for system passwords and other security parameters.	• Firewalls are according to customer policy. • When a probe is installed in DMZ, the card holder name - should not be saved. • Change all default passwords and client certificates as explained in the RUM Hardening Guide: 1. Rum passwords (admin and jmx) 2. Probe client certificate file 3. Integration User 4. MySQL Admin • Create a secure connection to MySQL.

Protect Cardholder Data	3. Protect stored cardholder data. 4. Encrypt transmission of cardholder data across open, public networks.	• Replace the keys periodically according to standard guidelines • Disable saving snapshots or only save snapshots for pages/events that are allowed by the security officer. If you save snapshots: 1. Save only 1 page back 2. Turn off all snapshots saved by default for HTTP error codes 3. Manually define only the exact events /URLs on which to save snapshots • Replace the keys periodically according to standard guidelines • Define the sensitive parameters (or if possible, use the option to mask all parameters values) • Use strong cryptography
Maintain a Vulnerability Management Program	5. Use and regularly update anti-virus software. 6. Develop and maintain secure systems and applications.	• Get security patches from HP as available
Implement Strong Access Control Measures	7. Restrict access to cardholder data on a need to know basis. 8. Assign a unique ID to each person with computer access. 9. Restrict physical access to cardholder data.	• Use the BSM Security User to define sensitive data • Use BSM User Management
Regularly Monitor and Test Networks	10. Track and monitor all access to network resources and cardholder data. 11. Regularly test security systems and processes.	• Use the BSM Auditing mechanism (or any other industry standard solution) to track logs
Maintain Information Security Policy	12. Maintain a policy that addresses information security for all personnel.	• This is an IT process issue and therefore is not directly applicable to RUM