An Oracle White Paper
January 2010

Using Oracle Enterprise Manager Configuration Management Pack for PCI Compliance

ORACLE

Disclaimer

The following is intended to outline our general product direction. It is intended for information purposes only, and may not be incorporated into any contract. It is not a commitment to deliver any material, code, or functionality, and should not be relied upon in making purchasing decisions. The development, release, and timing of any features or functionality described for Oracle's products remains at the sole discretion of Oracle.

Executive Overview

This white paper provides guidance to Oracle customer who would like to use Oracle Enterprise Manager Configuration Management Pack for Payment Card Industry Data Security Standard (PCI DSS) compliance.

Configuration Management Pack

Introduction

The Configuration Management Pack discovers and tracks configuration data for all elements of the software stack from the OS up to packaged applications. This pack lowers your application support costs by simplifying and automating manual tasks for managing configuration settings. It also improves service levels by reducing the largest source of application outages—configuration errors. And it enforces regulatory compliance with automated, real-time change detection and reporting. Forrester Consulting says that Oracle's Configuration Management Pack gives companies a 124% ROI pays back in 15 months.

Key Features

Simplify Management

- Automate discovery of IT configuration data
- Streamline delivery of new application instances using 'gold master' templates
- Enforce configuration consistency across environments (QA, Staging, Production, DR, etc) thereby reducing configuration errors which cause outages
- Determine the impact of changes before they are made

Improve Service

- Reduce troubleshooting time and costs via in-depth configuration comparisons
- Improve time-to-market for new applications and upgrades
- Reduce application outages owing to configuration errors

Enforce Compliance

- Detect configuration changes in real time
- Utilize policy-based compliance monitoring to avoid configuration drift
- Automate reporting for compliance (SOX, PCI, etc)

Throughout the rest of the document, we use two acronyms viz. GC for Grid Control and CCC for Configuration Change Console to refer to specific functionality within the Oracle Enterprise Manager Configuration Management Pack.

Payment Card Industry Data Security Standard (PCI DSS) Compliance

PCI DSS is data security standard mandated by major firms in the Payment Card Industry viz. American Express, Discover Financial Services, JCB International, MasterCard Worldwide and Visa Inc. International. The goal of PCI DSS is to help merchants secure their customers' payment data by implementing policies and procedures that safeguard hardware, software, network, and other entities that store or process payment data.

Many of Oracle's customers are required to implement PCI DSS compliance. Failure to implement PCI DSS not only increases risk to business but may also subject the corporation to hefty fines from the Payment Card Industry for non-compliance.

Oracle offers a broad-based solution to the PCI DSS compliance problem. The Oracle Enterprise Manager Configuration Management Pack is part of the overall solution. In the following sections of the document, we suggest how our existing as well as potential customers can use Configuration Management Pack to implement PCI DSS compliance. We first provide detailed usage scenarios for Configuration Management Pack as they apply to Requirement 10 and 11 of PCI DSS v1.21. We then complete the discussion by providing suggestions on the remaining PCI requirements.

Oracle has been investing heavily to provide an even broader coverage for PCI compliance using Configuration Management Pack. Customers should check newer versions as they may contain enhanced functionality for PCI compliance. In addition, Oracle has one of the broadest suites of products that support PCI compliance2.

Requirement 10: Track and monitor all access to network resources and cardholder data.

Logging mechanisms and the ability to track user activities are critical in preventing, detecting, or minimizing the impact of a data compromise. The presence of logs in all environments allows thorough tracking, alerting, and analysis when something does go wrong. Determining the cause of a compromise is very difficult without system activity logs.

1 The requirements and testing procedures are as described in the document "Payment Card Industry (PCI) Data Security Standard, Requirements and Security Assessment Procedures Version 1.2". Please visit https://www.pcisecuritystandards.org/ for more details.
2 For example, customer may want to look at Audit Vault and Database Vault to meet audit and database protection requirements.

PCI DSS REQUIREMENTS	TESTING PROCEDURES	CONFIGURATION MANAGEMENT PACK USAGE
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.	10.1 Verify through observation and interviewing the system administrator, that audit trails are enabled and active for system components.	GC3 Policies – 'Enable Database Auditing', 'Secure OS Audit Level'
10.2 Implement automated audit trails for all system components to reconstruct the following events:	10.2 Through interviews, examination of audit logs, and examination of audit log settings, perform the following:	
10.2.1 All individual accesses to cardholder data	10.2.1 Verify all individual access to cardholder data is logged.	CCC4 Controls - to monitor and record accesses made to cardholder data files and database tables
10.2.2 All actions taken by any individual with root or administrative privileges	10.2.2 Verify actions taken by any individual with root or administrative privileges is logged.	GC Policy - 'Auditing of SYS Operations Enabled' CCC Controls - to monitor activities of elevated-privilege users on databases (DBAs) and to production OSes, applications and utilities.
10.2.3 Access to all audit trails	10.2.3 Verify access to all audit trails is logged.	CCC Controls - to monitor and record accesses made to audit trails - files and Oracle DB tables
10.2.4 Invalid logical access attempts	10.2.4 Verify invalid logical access attempts are logged.	GC Policy – 'Audit Insert Failure' Custom GC Policy - UDM to collect audit setting and UDP to check that metric is set for both (on-success and on-failure)
10.2 5 Use of identification and authentication mechanisms	10.2.5 Verify use of identification and authentication mechanisms is logged.	CCC Controls - provide information as to how the user connected e.g. SQL Plus. CCC also provides the OS and DB username used to connect.
10.2.6 Initialization of the audit logs	10.2.6 Verify initialization of audit logs is logged.	CCC Controls – to monitor and record accesses and modifications made to audit trails - files and tables to capture initialization
10.2.7 Creation and deletion of system-level objects	10.2.7 Verify creation and deletion of system level objects are logged.	CCC Controls – to monitor and record accesses and modifications made to system objects - files, database tables, objects, registry entries, user accounts in LDAP repository, etc.
10.3 Record at least the following audit trail entries for all system components for each event:	10.3 Through interviews and observation, for each auditable event (from 10.2), perform the following:	
10.3.1 User identification	10.3.1 Verify user identification is included in log entries.	CCC Controls capture user identification
10.3.2 Type of event	10.3.2 Verify type of event is included	CCC Controls capture type of event

[3] Oracle Enterprise Manager Grid Control
[4] Configuration Change Console

	in log entries.	
10.3.3 Date and time	10.3.3 Verify date and time stamp is included in log entries.	CCC Controls capture date and time
10.3.5 Origination of event	10.3.5 Verify origination of event is included in log entries.	CCC Controls capture: For DB change - source host, OS user For OS change - original user in the case of sudo
10.3.6 Identity or name of affected data, system component, or resource	10.3.6 Verify identity or name of affected data, system component, or resources is included in log entries.	CCC component-application structure helps identify components that are affected
10.4 Synchronize all critical system clocks and times.	10.4 Obtain and review the process for acquiring and distributing the correct time within the organization, as well as the time-related system-parameter settings for a sample of system components. Verify the following is included in the process and implemented:	
	10.4.c Verify that specific external hosts are designated from which the timeservers will accept NTP time updates (to prevent a malicious individual from changing the clock). Optionally, those updates can be encrypted with a symmetric key, and access control lists can be created that specify the IP addresses of client machines that will be provided with the NTP service (to prevent unauthorized use of internal time servers). See www.ntp.org for more information	CCC Control - to monitor the ntp daemon, monitor 'date' command that may be used to change time, and monitor changes to configuration files such as /etc/inet/ntp.conf.
10.5 Secure audit trails so they cannot be altered.	10.5 Interview system administrator and examine permissions to verify that audit trails are secured so that they cannot be altered as follows:	
10.5.1 Limit viewing of audit trails to those with a job-related need.	10.5.1 Verify that only individuals who have a job-related need can view audit trail files.	Custom GC Policy – to check if users are assigned direct access vs. role-based CCC Control – to monitor and record accesses and modifications made to audit trails - files and tables - by users other than those expected (system or application).
10.5.2 Protect audit trail files from unauthorized modifications.	10.5.2 Verify that current audit trail files are protected from unauthorized modifications via access control mechanisms, physical segregation, and/or network segregation.	CCC Controls - to monitor and record accesses and modifications made to audit trails - files and tables - by users other than those expected (system or application).
10.5.3 Promptly back up audit trail files to a centralized	10.5.3 Verify that current audit trail files are promptly backed up to a	Custom GC Policy – to check for prompt backup if RMAN is used with Oracle Database

log server or media that is difficult to alter.	centralized log server or media that is difficult to alter.	CCC Controls- to monitor and record accesses and modifications made to audit trails - files and tables - by users other than those expected (system or application).
10.5.5 Use file-integrity monitoring or change-detection software on logs to ensure that existing log data cannot be changed without generating alerts (although new data being added should not cause an alert).	10.5.5 Verify the use of file-integrity monitoring or change-detection software for logs by examining system settings and monitored files and results from monitoring activities.	CCC Controls – to monitor critical system log files filtering out change made by "the system" user vs. other users that have access
10.7 Retain audit trail history for at least one year, with a minimum of three months immediately available for analysis (for example, online, archived, or restorable from back-up).	10.7.a Obtain and examine security policies and procedures and verify that they include audit log retention policies and require audit log retention for at least one year.	
	10.7.b Verify that audit logs are available for at least one year and processes are in place to restore at least the last three months' logs for immediate analysis.	Maintain CCC event data (audit logs) for required time period (configurable). Monitor changes to audit logs (deletions, accesses, etc.)

Requirement 11: Regularly test security systems and processes.

Vulnerabilities are being discovered continually by malicious individuals and researchers, and being introduced by new software. System components, processes, and custom software should be tested frequently to ensure security controls continue to reflect a changing environment.

PCI DSS REQUIREMENTS	TESTING PROCEDURES	CONFIGURATION MANAGEMENT PACK USAGE
11.2 Run internal and external network vulnerability scans at least quarterly and after any significant change in the network (such as new system component installations, changes in network topology, firewall rule modifications, product upgrades).	11.2.a Inspect output from the most recent four quarters of internal network, host, and application vulnerability scans to verify that periodic security testing of the devices within the cardholder data environment occurs. Verify that the scan process includes rescans until passing results are obtained. Note: External scans conducted after network changes, and internal scans, may be performed by the company's qualified internal personnel or third parties.	GC Policies - Critical Patch Advisories for Oracle Homes, Execute Stack, Insecure Services, NTFS File System, Open Ports GC Reports - 'Oracle Home Patch Advisories' for applicable patchsets, applied patchsets, and interim patches. CCC Controls – to monitor and record system, software and utility upgrades, patches and firewall rule changes and reconcile w/ change management system requests. CCC Controls - to record if and when vulnerability scanner ran
11.5 Deploy file-integrity monitoring software 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. Note: For file-integrity monitoring purposes, critical files are usually those that do not regularly change, but the modification of which could indicate a system compromise or risk of compromise. File-integrity monitoring products usually come pre-configured with critical files for the related operating system. Other critical files, such as those for custom applications, must be evaluated and defined by the entity (that is, the merchant or service provider).	11.5 Verify the use of file-integrity monitoring products within the cardholder data environment by observing system settings and monitored files, as well as reviewing results from monitoring activities. Examples of files that should be monitored: System executables Application executables Configuration and parameter files Centrally stored, historical or archived, log and audit files	GC Comparison Function – compare configurations against gold standards CCC Controls – to monitor and record changes to critical system or content files CCC Report – File Change Report

Requirement 1: Install and maintain a firewall configuration to protect cardholder data

A firewall examines all network traffic and blocks those transmissions that do not meet the specified security criteria.

All systems must be protected from unauthorized access from untrusted networks, whether entering the system via the Internet as e-commerce, employees' Internet access through desktop browsers, employees' e-mail access, dedicated connection such as business to business connections, via wireless networks, or via other sources. Often, seemingly insignificant paths to and from untrusted networks can provide unprotected pathways into key systems. Firewalls are a key protection mechanism for any computer network.

PCI DSS REQUIREMENTS	TESTING PROCEDURES	CONFIGURATION MANAGEMENT PACK USAGE
1.1.5 Documentation and business justification for use of all services, protocols, and ports allowed, including documentation of security features implemented for those protocols considered to be insecure	1.1.5.b Identify insecure services, protocols, and ports allowed; and verify they are necessary and that security features are documented and implemented by examining firewall and router configuration standards and settings for each service. An example of an insecure service, protocol, or port is FTP, which passes user credentials in clear-text.	GC Policy – Open Ports and Insecure Services GC Custom Policy – for supported target types CCC Control – real-time change detection using SNMP traps
1.2.2 Secure and synchronize router configuration files.	1.2.2 Verify that router configuration files are secure and synchronized—for example, running configuration files (used for normal running of the routers) and start-up configuration files (used when machines are re-booted), have the same, secure configurations.	GC Compare Function – define gold standard and compare CCC Control – real-time change detection using SNMP traps

Requirement 2: Do not use vendor-supplied defaults for system passwords and other security parameters

Malicious individuals (external and internal to a company) often use vendor default passwords and other vendor default settings to compromise systems. These passwords and settings are well known by hacker communities and are easily determined via public information.

PCI DSS REQUIREMENTS	TESTING PROCEDURES	CONFIGURATION MANAGEMENT PACK USAGE
2.1 Always change vendor-supplied defaults before installing a system on the network—for example, include passwords, simple network management protocol (SNMP) community strings, and elimination of unnecessary accounts.	2.1 Choose a sample of system components, critical servers, and wireless access points, and attempt to log on (with system administrator help) to the devices using default vendor-supplied accounts and passwords, to verify that default accounts and passwords have been changed. (Use vendor manuals and sources on the Internet to find vendor-supplied accounts/passwords.)	GC Policy – policies for account and password checks CCC Controls - Monitor and record account and password changes to firewall configurations via SNMP, LDAP or Active Directory servers and Unix password files. Reconcile to change management system requests if appropriate.
2.2 Develop configuration standards for all system components. Assure that these standards address all known security vulnerabilities and are consistent with industry-accepted system hardening standards.	2.2.c Verify that system configuration standards are applied when new systems are configured.	GC Compare – compare new systems against gold standard

Requirement 3: Protect stored cardholder data

Protection methods such as encryption, truncation, masking, and hashing are critical components of cardholder data protection. If an intruder circumvents other network security controls and gains access to encrypted data, without the proper cryptographic keys, the data is unreadable and unusable to that person. Other effective methods of protecting stored data should be considered as potential risk mitigation opportunities. For example, methods for minimizing risk include not storing cardholder data unless absolutely necessary, truncating cardholder data if full PAN is not needed, and not sending PAN in unencrypted e-mails.

PCI DSS REQUIREMENTS	TESTING PROCEDURES	CONFIGURATION MANAGEMENT PACK USAGE
3.6.7 Prevention of unauthorized substitution of cryptographic keys	3.6.7 Verify that key-management procedures are implemented to require the prevention of unauthorized substitution of keys.	CCC Control - monitor files or database tables containing keys for changes and reconcile to change management system requests

Requirement 4: Encrypt transmission of cardholder data across open, public networks

Sensitive information must be encrypted during transmission over networks that are easily accessed by malicious individuals. Misconfigured wireless networks and vulnerabilities in legacy encryption and authentication protocols can be continued targets of malicious individuals who exploit these vulnerabilities to gain privileged access to cardholder data environments.

PCI DSS REQUIREMENTS	TESTING PROCEDURES	CONFIGURATION MANAGEMENT PACK USAGE
4.1 Use strong cryptography and security protocols such as SSL/TLS or IPSEC to safeguard sensitive cardholder data during transmission over open, public networks.	4.1.a Verify the use of encryption (for example, SSL/TLS or IPSEC) wherever cardholder data is transmitted or received over open, public networks Verify that strong encryption is used during data transmission For SSL implementations: Verify that the server supports the latest patched versions. Verify that HTTPS appears as a part of the browser Universal Record Locator (URL). Verify that no cardholder data is required when HTTPS does not appear in the URL. Select a sample of transactions as they are received and observe transactions as they occur to verify that cardholder data is encrypted during transit. Verify that only trusted SSL/TLS keys/certificates are accepted. Verify that the proper encryption strength is implemented for the encryption methodology in use. (Check vendor recommendations/best practices.)	GC Custom Policy – check if server has latest patched version and the required encryption strength

Requirement 5: Use and regularly update anti-virus software or programs

PCI DSS REQUIREMENTS	TESTING PROCEDURES	CONFIGURATION MANAGEMENT PACK USAGE
5.2 Ensure that all anti-virus mechanisms are current, actively running, and capable of generating audit logs.		CCC Control - monitor antivirus software processes and notify when status changes. Monitor files or registry entries for changes to settings - e.g. auto-update.

Requirement 6: Develop and maintain secure systems and applications

PCI DSS REQUIREMENTS	TESTING PROCEDURES	CONFIGURATION MANAGEMENT PACK USAGE
6.1 Ensure that all system components and software have the latest vendor-supplied security patches installed. Install critical security patches within one month of release.	6.1.a For a sample of system components and related software, compare the list of security patches installed on each system to the most recent vendor security patch list, to verify that current vendor patches are installed.	GC Policy – Critical Patch Advisory for Oracle Homes provides coverage for software in Oracle Homes.
6.3.5 Removal of test data and accounts before production systems become active	6.3.5 Test data and accounts are removed before a production system becomes active.	GC Custom Policy – user-defined metric and policy to check for test accounts

Requirement 7: Restrict access to cardholder data by business need to know

To ensure critical data can only be accessed by authorized personnel, systems and processes must be in place to limit access based on need to know and according to job responsibilities.

"Need to know" is when access rights are granted to only the least amount of data and privileges needed to perform a job.

PCI DSS REQUIREMENTS	TESTING PROCEDURES	CONFIGURATION MANAGEMENT PACK USAGE
7.1.1 Restriction of access rights to privileged user IDs to least privileges necessary to perform job responsibilities	7.1.1 Confirm that access rights for privileged user IDs are restricted to least privileges necessary to perform job responsibilities.	CCC Control – monitor changes to access rights once proper privileges have been setup initially

Requirement 8: Assign a unique ID to each person with computer access.

Assigning a unique identification (ID) to each person with access ensures that each individual is uniquely accountable for his or her actions. When such accountability is in place, actions taken on critical data and systems are performed by, and can be traced to, known and authorized users.

PCI DSS REQUIREMENTS	TESTING PROCEDURES	CONFIGURATION MANAGEMENT PACK USAGE
8.5.5 Remove/disable inactive user accounts at least every 90 days.	8.5.5 Verify that inactive accounts over 90 days old are either removed or disabled.	GC Custom Policy – for several enterprise system such as Oracle database, Weblogic server, and others, custom metric and custom policy can support requirement
8.5.9 Change user passwords at least every 90 days.	8.5.9 For a sample of system components, obtain and inspect system configuration settings to verify that user password parameters are set to require users to change passwords at least every 90 days. For service providers only, review internal processes and customer/user documentation to verify that customer passwords are required to change periodically and that customers are given guidance as to when, and under what circumstances, passwords must change.	GC Policy – database password expiration policy

Requirement 9: Restrict physical access to cardholder data.

Any physical access to data or systems that house cardholder data provides the opportunity for individuals to access devices or data and to remove systems or hardcopies, and should be appropriately restricted.

PCI DSS REQUIREMENTS	TESTING PROCEDURES	CONFIGURATION MANAGEMENT PACK USAGE
9.1 Use appropriate facility entry controls to limit and monitor physical access to systems in the cardholder data environment.	9.1 Verify the existence of physical security controls for each computer room, data center, and other physical areas with systems in the cardholder data environment. • Verify that access is controlled with badge readers or other devices including authorized badges and lock and key. • Observe a system administrator's attempt to log into consoles for randomly selected systems in the cardholder environment and verify that they are "locked" to prevent unauthorized use.	CCC Control – monitor changes to LDAP if LDAP is used to facilitate

Requirement 12: Maintain a policy that addresses information security for employees and contractors.

A strong security policy sets the security tone for the whole company and informs employees what is expected of them. All employees should be aware of the sensitivity of data and their responsibilities for protecting it. For the purposes of this requirement, "employees" refers to full-time and part-time employees, temporary employees and personnel, and contractors and consultants who are "resident" on the company's site.

PCI DSS REQUIREMENTS	TESTING PROCEDURES	CONFIGURATION MANAGEMENT PACK USAGE
12.5.4 Administer user accounts, including additions, deletions, and modifications	12.5.4 Verify that responsibility for administering user account and authentication management is formally assigned.	CCC Control – monitor and record changes to accounts in LDAP or Active Directory. Monitor change/events to password files on systems. Validate against change management system requests. Monitor and record actions of specific (vendor) user IDs against critical resources.

Conclusion

The Oracle Enterprise Manager Configuration Management Pack provides capabilities that customers can immediately use to ensure Payment Card Industry Data Security Standard (PCI DSS) compliance. Many of these GC and CCC capabilities provide direct out-of-box solution to PCI requirements while some GC and CCC capabilities can be customized to solve a specific requirement.

White Paper Title
[Month] 2009
Author: [OPTIONAL]
Contributing Authors: [OPTIONAL]

Oracle Corporation
World Headquarters
500 Oracle Parkway
Redwood Shores, CA 94065
U.S.A.

Worldwide Inquiries:
Phone: +1.650.506.7000
Fax: +1.650.506.7200
oracle.com

Oracle is committed to developing practices and products that help protect the environment

0109