

Quest Solutions for PCI Compliance

Effective Data Access Controls and Data Protection
Management for Complying with the Payment Card
Industry Data Security Standard

Written by
Quest Software, Inc.

© 2010 Quest Software, Inc.

ALL RIGHTS RESERVED.

This document contains proprietary information protected by copyright. No part of this document may be reproduced or transmitted in any form or by any means, electronic or mechanical, including photocopying and recording for any purpose without the written permission of Quest Software, Inc. ("Quest").

The information in this document is provided in connection with Quest products. No license, express or implied, by estoppel or otherwise, to any intellectual property right is granted by this document or in connection with the sale of Quest products. EXCEPT AS SET FORTH IN QUEST'S TERMS AND CONDITIONS AS SPECIFIED IN THE LICENSE AGREEMENT FOR THIS PRODUCT, QUEST ASSUMES NO LIABILITY WHATSOEVER AND DISCLAIMS ANY EXPRESS, IMPLIED OR STATUTORY WARRANTY RELATING TO ITS PRODUCTS INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTY OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, OR NON-INFRINGEMENT. IN NO EVENT SHALL QUEST BE LIABLE FOR ANY DIRECT, INDIRECT, CONSEQUENTIAL, PUNITIVE, SPECIAL OR INCIDENTAL DAMAGES (INCLUDING, WITHOUT LIMITATION, DAMAGES FOR LOSS OF PROFITS, BUSINESS INTERRUPTION OR LOSS OF INFORMATION) ARISING OUT OF THE USE OR INABILITY TO USE THIS DOCUMENT, EVEN IF QUEST HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES. Quest makes no representations or warranties with respect to the accuracy or completeness of the contents of this document and reserves the right to make changes to specifications and product descriptions at any time without notice. Quest does not make any commitment to update the information contained in this document.

If you have any questions regarding your potential use of this material, contact:

Quest Software World Headquarters

LEGAL Dept

5 Polaris Way

Aliso Viejo, CA 92656

www.quest.com

E-mail: **legal@quest.com**

Refer to our Web site for regional and international office information.

Trademarks

Quest, Quest Software, the Quest Software logo, AccessManager, ActiveRoles, Aelita, Akonix, AppAssure, Benchmark Factory, Big Brother, BridgeAccess, BridgeAutoEscalate, BridgeSearch, BridgeTrak, BusinessInsight, ChangeAuditor, ChangeManager, Defender, DeployDirector, Desktop Authority, DirectoryAnalyzer, DirectoryTroubleshooter, DS Analyzer, DS Expert, Foglight, GPOAdmin, Help Desk Authority, Imceda, IntelliProfile, InTrust, Invirtus, iToken, I/Watch, JClass, Jint, JProbe, LeccoTech, LiteSpeed, LiveReorg, LogADmin, MessageStats, Monosphere, MultSess, NBSpool, NetBase, NetControl, Npulse, NetPro, PassGo, PerformaSure, Point,Click,Done!, PowerGUI, Quest Central, Quest vToolkit, Quest vWorkSpace, ReportADmin, RestoreADmin, ScriptLogic, Security Lifecycle Map, SelfServiceADmin, SharePlex, Sitraka, SmartAlarm, Spotlight, SQL Navigator, SQL Watch, SQLab, Stat, StealthCollect, Storage Horizon, Tag and Follow, Toad, T.O.A.D., Toad World, vAutomator, vControl, vConverter, vFoglight, vOptimizer, vRanger, Vintela, Virtual DBA, VizionCore, Vizioncore vAutomation Suite, Vizioncore vBackup, Vizioncore vEssentials, Vizioncore vMigrator, Vizioncore vReplicator, WebDefender, Webthority, Xaffire, and XRT are trademarks and registered trademarks of Quest Software, Inc in the United States of America and other countries. Other trademarks and registered trademarks used in this guide are property of their respective owners.

Updated – February 2010

Contents

- Introduction.....3
- About PCI DSS4
 - Best Practice Areas and Requirements4
 - Required Validation Activities5
 - Definition of System Components6
- Becoming PCI DSS Compliant with Quest7
 - Choosing the Right Solution for Your Needs8
 - Requirement 1: Install and maintain a firewall configuration to protect cardholder data.10
 - Requirement 2: Do not use vendor-supplied defaults for system passwords and other security parameters.....11
 - Requirement 4: Encrypt transmission of cardholder data across public networks.....12
 - Requirement 5: Use and regularly update anti-virus software or programs.....13
 - Requirement 6: Develop and maintain secure systems and applications.....14
 - Requirement 7: Restrict access to cardholder data by business need-to-know.15
 - Requirement 8: Assign a unique ID to each person with computer access.....16
 - Requirement 10: Track and monitor all access to network resources and cardholder data.....22
 - Requirement 11: Regularly test security systems and processes.....27
 - Requirement 12: Maintain a policy that addresses information security for employees and contractors.....28
 - Appendix A, Requirement A.1: Shared hosting providers must protect the cardholder data environment.29
 - Appendix B, Requirement 3: [Compensating controls must] be “above and beyond” other PCI DSS requirements.30
- For More Information30

Introduction

After collaborating to adopt a common data security standard for the payment card industry, the five major payment card brands - Visa International, MasterCard Worldwide, American Express, Discover Financial Services and JCB International - announced the formation of an official industry council, the PCI Security Standards Council. Their charter requires all merchants that handle payment card transactions with their brand (including credit cards and signature debit cards embossed with a council member's logo), as well as all associated third-party transaction processors, IT service and payment device providers, to comply with the Payment Card Industry Data Security Standard (PCI DSS).

Unfortunately, the security features that exist today in many of the system components that make up a merchant's "cardholder data environment" are insufficient to meet the standard. In fact, an increasing number of companies are finding security holes that may compromise cardholder data (for some examples, see <http://seclists.org/dataloss/>). With data breaches on the rise and 100 percent compliance being required, merchants must remediate their deficiencies. Failing to comply with PCI-DSS can result in fines, lost customers and a damaged reputation.

As the premier provider of platform-integrated event and access management solutions on Windows, Unix, and Linux systems, Quest offers the tools and controls you need to easily and efficiently comply with PCI-DSS.

About PCI DSS

Best Practice Areas and Requirements

The PCI DSS is composed of six best practice areas and 12 high-level requirements for securing protected data. These include strong access controls, user activity monitoring, change tracking, and record retention. Table 1 lists the best practice areas and the high-level requirements for each area.

Area 1: Build and Maintain a Secure Network
Requirement 1: Install and maintain a firewall configuration to protect cardholder data.
Requirement 2: Do not use vendor-supplied defaults for system passwords and other security parameters.
Area 2: Protect Cardholder Data
Requirement 3: Protect stored cardholder data.
Requirement 4: Encrypt transmission of cardholder data across public networks.
Area 3: Maintain a Vulnerability Management Program
Requirement 5: Use and regularly update anti-virus software.
Requirement 6: Develop and maintain secure systems and applications.
Area 4: Implement Strong Access Control Measures
Requirement 7: Restrict access to cardholder data by business need-to-know.
Requirement 8: Assign a unique ID to each person with computer access.
Requirement 9: Restrict physical access to cardholder data.
Area 5: Regularly Monitor and Test Networks
Requirement 10: Track and monitor all access to network resources and cardholder data.
Requirement 11: Regularly test security systems and processes.
Area 6: Maintain an Information Security Policy
Requirement 12: Maintain a policy that addresses information security.
Appendix A: Additional PCI DSS Requirements for Shared Hosting Providers
Appendix B: Compensating Controls

Table 1. PCI DSS Best Practice Areas and High-Level Requirements

Required Validation Activities

Merchants who accept credit and signature debit cards are held to different levels of compliance scrutiny by payment brands and acquirers (e.g., merchant banks). These levels are based on the volume of transactions, market segment, acceptance channel and the merchant's risk history. Merchants that fall into the Merchant Level 1 category (the most closely watched group) must accept an annual on-site audit from a Qualified Security Assessor (QSA) and undergo quarterly network scans. Merchants at Levels 2 and 3 are required to submit an annual self- assessment and, like Level 1 merchants, contract with an Approved Scanning Vendor (ASV) to perform quarterly security scans of their corporate network. Most Level 4 merchants are not required to submit proof of compliance, but must self-assess. Regular scans are recommended.

Table 2 defines the various merchant levels and their required validation activities as defined by Visa and MasterCard.

Merchant Level	Description	Required Validation Activities
Level 1	Any merchant that: <ul style="list-style-type: none"> • Processes over six million Visa or MasterCard transactions per year, or • Has suffered a hack or attack resulting in data being compromised, or • Has been deemed by Visa or any other payment card brand to sufficiently merit meeting Level 1 requirements to reduce risk to their systems 	Annual on-site audit and quarterly network scans are required.
Level 2	Any merchant processing 1 million to 6 million Visa or MasterCard transactions per year	Annual PCI Self-Assessment questionnaire and quarterly network scans are required.
Level 3	Any merchant that processes between 20,000 to 1 million Visa or MasterCard e-commerce transactions per year that does not meet Level 1 or 2 criteria	Annual PCI Self-Assessment questionnaire and quarterly network scans are required.
Level 4	Any other merchant	Annual PCI Self-Assessment questionnaire and quarterly network scans may be required by some merchant banks. If not required, an annual PCI self- assessment questionnaire and quarterly network scan conducted by a qualified independent scan vendor are recommended.

Table 2. Visa and MasterCard Merchant Level Definitions

Definition of System Components

The standard's definition of the cardholder data environment is quite broad, stating that the PCI DSS security requirements:

"...apply to all 'systems components'. System components are defined as any network component, server, or application that is included in or connected to the cardholder data environment. The cardholder data environment is that part of the network that possesses cardholder data or sensitive authentication data."

- Payment Card Industry Data Security Standard: Requirements and Security Assessment Procedures, Version 1.2

The PCI DSS definition of "system component[s]" is further clarified to encompass various network components such as firewalls and network appliances as well as all server types including Web, database, authentication, mail, proxy, NTP, DNS, and other servers that possess "cardholder data or sensitive authentication data" or that are connected to components storing this data. According to the DSS, the payment card data that can be stored includes cardholder names and expiration dates. Card numbers (also called PANs) may be stored as long as the latter are obfuscated in an acceptable manner. However, stored data cannot include full magnetic stripe, or track, data, PINs, and CVC2/CVV2/CID codes used for payment card validation.

Becoming PCI DSS Compliant with Quest

Merchants who want their non-consumer users to have controlled, monitored, and secure access to sensitive cardholder data can use Quest's Windows and platform layer management solutions to help satisfy requirements 1, 2, 4, 5, 6, 7, 8, 10, 11 and 12 of the PCI DSS. This data can be managed within a Windows domain, on a Unix, Linux or Mac system, or combination of both. Quest solutions can also help your organization protect and manage access and changes to system components that store this data, regardless of whether your compliance policy requires the data to be encrypted, masked, hashed, or made clearly visible to all authorized users.

Not only can Quest solutions increase the efficiency and effectiveness of the authentication and authorization controls available on native platforms, they can also consolidate, log, monitor, report on, and alert on virtually all security events occurring on all system components. For example, Quest solutions can leverage Active Directory's (AD) native capabilities to consolidate its cardholder data access controls with those operating in Unix, Linux, and Mac platforms. This produces a centrally managed practice area of cross-platform identities and access controls, simplifying managing and reporting on PCI's Strong Access Control Measures. In addition, Quest's platform-layer solutions provide full-featured identity and access management to help meet the DSS host, application, and file-level access monitoring requirements for both Windows and non-Windows users.

Quest solutions can improve deficiencies in your data security architectures and IT controls. Combining Quest's solutions with your organization's AD and Unix/Linux infrastructure can help make your data security safeguards more effective and efficient while providing the evidence required to be compliant with the PCI DSS. These solutions secure and monitor access to sensitive data, as well as alert you to any changes within your PCI architecture.

However, even with complete IT control of the architecture's platform layer, Quest solutions are only a part of a successful PCI DSS compliance program. These tools should be used along with additional controls to cover the remaining portions of the PCI DSS.

Choosing the Right Solution for Your Needs

Table 3 provides a quick view of the areas where Quest's Windows and platform layer solutions are helping organizations around the globe meet their PCI DSS requirements.

Use Table 3 as a first step to identifying the PCI DSS requirement coverage you need. Then turn to the sections that follow for a deeper look at how these products can help you meet the specific DSS requirements your organization is facing.

QUEST SOLUTION	PCI DSS v1.2 Requirement Sections													
	1	2	3	4	5	6	7	8	9	10	11	12	App A	App B
Compliance Suite		✓		✓	✓		✓	✓		✓	✓	✓	✓	
Reporter		✓		✓	✓		✓	✓		✓	✓		✓	
InTrust with InTrust Plug-in for Active Directory		✓			✓			✓		✓	✓		✓	
ActiveRoles Server							✓	✓		✓		✓	✓	
Additional Solutions	✓	✓		✓	✓	✓	✓	✓		✓	✓	✓	✓	✓
InTrust Plug-in for File Access							✓	✓		✓	✓			
InTrust Plug-in for Exchange								✓		✓				
Change Auditor for File Systems							✓	✓		✓	✓			
Change Auditor for Active Directory								✓		✓			✓	
Change Auditor for Exchange								✓		✓				
Policy Authority for Unified Communications	✓			✓	✓	✓	✓	✓		✓				

QUEST SOLUTION	PCI DSS v1.2 Requirement Sections													
	1	2	3	4	5	6	7	8	9	10	11	12	App A	App B
Authentication Services	✓	✓					✓	✓		✓		✓		
Defender								✓						✓
GPOAdmin	✓	✓				✓	✓	✓				✓		
Password Manager								✓						
Privilege Manager for Unix							✓	✓		✓	✓	✓		✓
Single Sign-on for Java		✓					✓	✓					✓	
Access Manager							✓			✓		✓		

Table 3. Mapping of Quest products to PCI DSS requirements

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

PCI DSS Section	Requirement	How Quest products help address the requirement
1.1.1	Have a formal process for approving and testing all network connections and changes to the firewall and router configurations.	GPOADmin supports testing changes to Group Policy objects (GPOs) that contain firewall configuration settings.
1.2	Build a firewall configuration that restricts connections between untrusted networks and any system components in the cardholder data environment.	<p>Policy Authority for Unified Communications can limit, filter, or restrict connections between the cardholder data environment and real-time communication networks such as instant messaging (IM), and peer-to-peer applications. It can also block Skype connections. (Filtering includes using policies such as blocking inbound executables).</p> <p>When the capabilities of Windows Group Policy are extended, script policies and file copy policies can be applied using Authentication Services to configure various types of Unix and Linux-based firewall and router solutions (iptables, ipf, etc.).*</p>
1.3	Prohibit direct public access between the Internet and any system component in the cardholder data environment.	
1.4	Install personal firewall software on any mobile or employee-owned computers with direct connectivity to the Internet (for example, laptops used by employees) that are used to access the organization's network.	When the capabilities of Windows Group Policy are extended, script policies and file copy policies can be applied using Authentication Services to configure various types of Unix and Linux-based firewall solutions,* including personal firewalls, assuming the organization has the additional capability to remotely control root access on end-user computers, and the firewalls cannot be altered locally.

**Note: Achieving this requirement assumes that the target firewall/router software to be configured is sufficiently feature-rich to meet the stated PCI requirement and runs on an OS supported by Authentication Services.*

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

PCI DSS Section	Requirement	How Quest products help address the requirement
2.1	Always change the vendor-supplied defaults before installing a system on the network; for example, include passwords and simple network management protocol (SNMP) community strings, and eliminate unnecessary accounts.	Reporter reports on null passwords, last date of password change, SNMP settings, etc.
2.2	Develop configuration standards for all system components. Ensure that these standards address all known security vulnerabilities and are consistent with industry-accepted system hardening standards.	By creating a system settings change management environment where Group Policy Objects are versioned and tracked, GPOAdmin allows system administrators to set up a system settings test, rollout, rollback, and reporting environment (augmented by Reporter for CIS-benchmarked servers) for safe deployment of system configuration setting changes to conform with industry benchmark configurations. With Reporter's configuration baselining feature, system administrators can compare the settings of their AD and Windows Server configurations with both internally developed and industry standard security benchmarks. Reporter is CIS certified. Once an approved system component configuration is achieved, InTrust can be configured to send alerts when the configuration has been changed.
2.2.1	Implement only one primary function per server.	
2.2.2	Disable all unnecessary and insecure services and protocols (services and protocols not directly needed to perform a device's specified function).	
2.2.3	Configure system security parameters to prevent misuse.	
2.2.4	Remove all unnecessary functionality, such as scripts, drivers, features, subsystems, file systems and unnecessary Web servers.	
2.3	Encrypt all non-console administrative access. Use technologies such as SSH, VPN or SSL/TLS for Web-based management and other non-console administrative access.	With Reporter's configuration baselining feature, system administrators can determine which services and login methods are running for critical servers. Quest provides Unix users a version of OpenSSH that is linked to the Authentication Services security libraries.

Requirement 4: Encrypt transmission of cardholder data across public networks.

PCI DSS Section	Requirement	How Quest products help address the requirement
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.	Policy Authority for Unified Communications supports SSL certificate management for encrypted communication between AOL/AIM clients and is compatible with the MSN/Windows Live Messenger SSL feature. It also supports policy enforcement, content filtering and logging of OCS TLS/MTLS encrypted communication. Reporter's configuration baselining feature enables system administrators to determine which encryption services, if any, are running for Windows servers that transmit and receive cardholder data.
4.2	Never send unencrypted PANs by end-user messaging technologies (for example, e-mail, instant messaging, or chat).	Policy Authority for Unified Communications can block PANs from being sent to external users over real-time messaging technologies or, if desired, it can add security measures to the transmission of already-encrypted PANs that are authorized for end-user messaging technologies.

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

PCI DSS Section	Requirement	How Quest products help address the requirement
5.1	Deploy anti-virus software on all systems commonly affected by malicious software (particularly personal computers and servers).	Policy Authority for Unified Communications provides anti-virus (AV) support for IM-borne viruses found in real-time communication networks. Reporter's configuration baselining feature can ensure AV software is installed and configured on all Windows systems. In addition, InTrust provides AV event log information and reports on AV event data.
5.2	Ensure that all anti-virus mechanisms are current, actively running, and capable of generating audit logs.	

Requirement 6: Develop and maintain secure systems and applications.

PCI DSS Section	Requirement	How Quest products help address the requirement
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.	<p>Policy Authority for Unified Communications includes continuous protocol, SPIM (spam over IM), and malware policy updates for real-time communication networks such as instant messaging, peer-to-peer applications, and Skype. It also implements a challenge/response system to deter zero-day attacks propagated by the transmission of URLs from malicious Web sites.</p>
6.2	Establish a process to identify newly discovered security vulnerabilities (for example, subscribe to alert services freely available on the Internet). Update configuration standards as required by PCI DSS Requirement 2.2 to address new vulnerability issues.	
6.3	<p>Develop software applications in accordance with PCI DSS (for example, secure authentication and logging) and based on industry best practices, and incorporate information security throughout the software development life cycle. These processes must include the following:</p> <p>6.3.1 Test all security patches and system and software configuration changes before deployment.</p> <p>6.3.2 Separate development, test and production environments.</p>	<p>As part of a system configuration change test environment Quest's GPOAdmin can support testing of GPO changes, which could include system configuration setting changes.</p>

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

PCI DSS Section	Requirement	How Quest products help address the requirement
7.1	<p>Limit access to system components and cardholder data to only those individuals whose job requires such access. Access limitations must include the following:</p> <p>7.1.1 Restrict access rights to privileged user IDs to least privileges necessary to perform job responsibilities.</p> <p>7.1.2 Assign privileges based on individual personnel's job classification and function.</p> <p>7.1.3 Require an authorization form signed by management that specifies required privileges</p> <p>7.1.4 Implement an automated access control system</p>	<p>To enforce and automate written access control policies, ActiveRoles Server provides a full-featured solution that greatly enhances the access controls available in AD while Privilege Manager for Unix offers root delegation and granular privilege access management on Unix and Linux systems. Access Manager enables identification and management of user and group access to resources across the Windows enterprise. In addition Single Sign-on for Java enhances and extends AD's access controls for users of Web-based application servers and Authentication Services can extend the access restriction functionality of AD's group memberships to Unix, Linux and Mac systems that compose the organization's cardholder data environment. Policy Authority for Unified Communications includes IM and P2P user privilege settings that can be built on a "block all communications unless allowed by a policy" starting point. InTrust Plug-in for File Access and ChangeAuditor for File Systems offer complete access and permissions history for protected file, folder, share, and NTFS "cardholder data environment" components on Windows file servers. And GPOAdmin can manage the GPOs that contain "deny all" settings for file systems, applications, and system resources that could enable protected cardholder data access.</p>
7.2	<p>Establish an mechanism access control system for systems components with multiple users that restricts access based on a user's need to know and is set to "deny all" unless specifically allowed. This access control system must include the following:</p> <p>7.2.1 Cover all system components.</p> <p>7.2.2 Assign privileges to individuals based on job classification and function.</p> <p>7.2.3 Default "deny-all" setting.</p>	

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

PCI DSS Section	Requirement	How Quest products help address the requirement
8.1	<p>Assign each user a unique user name before allowing the user to access system components or cardholder data.</p>	<p>Policy Authority for Unified Communications can ensure all unidentified real-time messaging users are blocked from communicating with authorized IM users with access to system components. Privilege Manager for Unix helps to enforce unique user IDs by delegating anonymous supervisor privileges to individual users and then auditing all actions performed by those users. In addition, Authentication Services supports corporate policies implemented in AD that require unique user names. Authentication Services also provides tools to consolidate existing non-unique user accounts in AD.</p>
8.2	<p>In addition to assigning a unique ID, employ at least one of the following methods to authenticate all users:</p> <ul style="list-style-type: none"> • Password or passphrase • Two-factor authentication (for example, token devices, smart cards, biometrics, or public keys) 	<p>Defender enables users two-factor authentication using both hardware and software tokens. Privilege Manager for Unix can make additional authentication calls to any PAM-enabled system or security mechanism. Single Sign-on for Java extends AD's Kerberos password authentication for users of Web-based application servers, while Authentication Services provides Kerberos-based authentication of Unix and Linux systems (or PAM-enabled Unix-based biometric applications) via password or smart card login.</p>
8.3	<p>Incorporate two-factor authentication for remote access (network-level access originating from outside the network) to the network by employees, administrators and third parties. Use technologies such as remote authentication and dial-in service (RADIUS); terminal access controller access control system (TACACS) with tokens; or VPN (based on SSL/TLS or IPSEC) with individual certificates.</p>	<p>Defender leverages Active Directory to provide two-factor RADIUS authentication for any system, application, or resource. In addition, an optional feature of Authentication Services is available to support multi-factor authentication of Unix and Linux systems using smart cards. Also, Reporter can report on users that are leveraging smart cards.</p>
8.4	<p>Render all passwords unreadable during transmission and storage on all system components using strong cryptography based on approved standards (defined in PCI DSS Glossary, Abbreviations, and Acronyms).</p>	<p>AD offers this functionality natively within Windows. Authentication Services extends this basic functionality to Unix, Linux and Mac systems, while Single Sign-on for Java extends this functionality to users of Web-based application servers.</p>

PCI DSS Section	Requirement	How Quest products help address the requirement
8.5	Ensure proper user authentication and password management for non-consumer users and administrators, on all system components	
8.5.1	Control addition, deletion, and modification of user IDs, credentials, and other identifier objects	<p>AD offers basic user ID, computer ID and password administration. ActiveRoles Server enhances AD's user provisioning functionality by providing an automated change approval environment for all user changes, including user rights, permissions, modification, creation and deletion. Policy Authority for Unified Communications can extend the user rights approval process by requiring users who have been authenticated on the network and who attempt to log into Internet-based communications networks with personal logins (e.g., IM, P2P, or Skype) to link their screen names with their network user IDs. InTrust Plug-in for Active Directory supports object locking to protect against unwanted changes to user objects within AD. GPOAdmin supports testing GPO changes, which could include user group attributes. Single Sign-on for Java extends AD's basic user account management functionality to users of Web-based application servers, while Authentication Services permits Unix-enabled user IDs and passwords in AD to be administered using either standard AD tools or the vastool utility. Privilege Manager for Unix provides for the management of user IDs and credentials of Unix users regardless of whether they are also managed within AD. Reporter can report on user access to validate that access has been granted in accordance with a corresponding authorization form.</p>
8.5.2	Verify user identity before performing password resets	<p>Authentication Services extends AD's basic functionality to require Unix, Linux and Mac users to log in with existing credentials before resetting passwords in response to password reset requests. Single Sign-on for Java does the same for users of Web-based application servers. Defender can be used with Single Sign-on requiring a user to enter a token code in order to be permitted to perform a password reset. Quest Password Manager provides additional self-service password reset and change capabilities for users managed in AD, as well as administrative password reset and management. For example, Password Manager enables organizations to set up a series of security questions before a user can change or update his or her password. Privilege Manager for Unix verifies the identity of Unix users regardless of whether they are also managed within AD.</p>

PCI DSS Section	Requirement	How Quest products help address the requirement
8.5.3	Set first-time passwords to a unique value for each user and change them immediately after the first use.	AD offers this functionality natively within Windows. Authentication Services extends this basic functionality to Unix, Linux and Mac systems, while Single Sign-on for Java does the same for users of Web-based application servers.
8.5.4	Immediately revoke access for any terminated users.	The definitive record of terminated employees and contractors is stored in the HR database, which often requires an additional step of revoking of access within AD. Authentication Services enforces revoked access for users disabled in or removed from AD on Unix, Linux and Mac systems, and Single Sign-on for Java does the same for users of Web-based application servers. However, ActiveRoles Server , which provides extra user provisioning and de-provisioning controls, can empower one designated authority (such as HR) to make termination and access revocation an immediate, one-step process with ActiveRoles Quick Connect Reporter can report on users that have not logged in within a period of time (such as 180 days) and through action-enabled reporting, easily disable or remove them from AD.
8.5.5	Remove or disable inactive user accounts at least every 90 days.	Reporter can report on users that have been inactive for 90 days. Authentication Services works with AD to enable administrators to know which Unix-enabled accounts are inactive for 90 days or more. Single Sign-on for Java does the same for users of Web-based application servers. ActiveRoles Server automates this control and serves as a complete de-provisioning solution. Recovery Manager for Active Directory allows companies to meet this requirement while preserving their internal policy of making historical user account credentials available (for rehires, SEC inquiries, legal investigations, etc.).

PCI DSS Section	Requirement	How Quest products help address the requirement
8.5.6	Enable accounts used by vendors for remote maintenance only during the time period needed.	AD offers basic management of vendor accounts. Authentication Services works with AD to allow administrators to disable and re-enable (or enable only during specified logon hours) any Unix-enabled AD account used by vendors on demand. Single Sign-on for Java does the same for users of Web-based application servers. ActiveRoles Direct, ChangeAuditor for Active Directory and InTrust Plug-in for Active Directory crisply define, delegate, automate, track, log, audit and easily manage vendor accounts in AD. Privilege Manager for Unix can manage Unix users performing remote maintenance within pre-defined time windows.
8.5.7	Communicate password procedures and policies to all users who have access to cardholder data.	This requirement must be satisfied by the merchant's own data security communication and awareness program.
8.5.8	Do not use group, shared or generic accounts and passwords.	InTrust can be configured to report on activity by generic accounts. InTrust Plug-in for Active Directory can help identify who is using generic accounts by providing a source IP address. Authentication Services supports corporate policies that prohibit group, shared or generic accounts and passwords. Single Sign-on for Java does the same for users of Web-based application servers. Privilege Manager for Unix supports all such policies for Unix users, regardless of whether they are also managed within AD, by eliminating shared privileged account access through delegation of privileges in accordance with defined user roles.

PCI DSS Section	Requirement	How Quest products help address the requirement
8.5.9	Change user passwords at least every 90 days.	<p>Reporter can report on user accounts that have not had a password change within 90 days, and can also report on password-related settings to ensure they are actually applied and in effect. ActiveRoles Server and Password Manager combine to automate all of these password policies. InTrust Plug-in for Active Directory and Change Auditor for Active Directory can both be used to notify administrators when these settings are changed. Authentication Services extends and enforces AD's password policies (or password policies implemented through an AD-based tool such as Password Manager) for users of Unix, Linux and Mac systems. Single Sign-on for Java does the same for users of Web-based application servers. GPOAdmin supports testing of GPO changes, including these password policy settings. Also, GPOAdmin provides an automated way to ensure that all security options are set correctly throughout the domain.</p>
8.5.10	Require a minimum password length of at least seven characters.	
8.5.11	Use passwords containing both numeric and alphabetic characters.	
8.5.12	Do not allow individuals to submit a new password that is the same as any of the last four passwords they have used.	
8.5.13	Limit repeated access attempts by locking out the user ID after not more than six attempts.	
8.5.14	Set the lockout duration to 30 minutes or until administrator enables the user ID	
8.5.15	If a session has been idle for more than 15 minutes, require the user to re-enter the password to re-activate the terminal.	<p>Reporter can report on this setting to ensure it is accurate and in effect. GPOAdmin supports testing of GPO changes, including password re-entry for idle time policy settings. Authentication Services can be used to deploy screensaver configurations through Windows Group Policy to Unix, Linux and Mac systems. This assumes the organization has the additional capability to remotely control root access on end-user computers such that their screensaver configurations are not locally alterable.</p>
8.5.16	Authenticate all access to any database containing cardholder data. This includes access by applications, administrators and all other users.	<p>Authentication Services provides authentication of Unix, Linux, and Mac operating system (OS) users and certain application users (e.g., users of SAP and Oracle). Single Sign-on for Java does the same for users of a broader range of popular Web-based application servers. In cases where an Exchange database contains cardholder data, InTrust Plug-in for Exchange and ChangeAuditor for Exchange can detect instances where access that is authenticated at the application layer is being abused or circumvented, such as can happen with non-owner mailbox access by another Exchange user or Exchange administrator. InTrust Plug-in for File Access and ChangeAuditor for File Systems provide similar controls at the file access level. Policy Authority for Unified Communications can extend the intent of</p>

		<p>this requirement to data transmitted via instant messaging by requiring users with access to cardholder data that attempt to log into real-time communications networks with personal logins (e.g., IM, P2P, or Skype) to associate their “screen names” with their network user IDs. In this way, you not only know who has access to cardholder data, but you know that no one can transmit that data via UC anonymously.</p>
--	--	--

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

PCI DSS Section	Requirement	How Quest products help address the requirement
10.1	Establish a process for linking all access to system components (especially access done with administrative privileges such as root) to an individual user.	<p>ActiveRoles Server links cardholder access to individual users by allowing delegation and tracking of administrative privileges for users managed in AD.</p> <p>Access Manager links user access to specific files, folders, and shares across the Windows enterprise, and Privilege Manager for Unix links cardholder access to individual users by enabling carefully controlled privileged access management (e.g., root delegation) for Unix and Linux users regardless of whether they are also managed within AD. The InTrust and ChangeAuditor families of activity logging solutions enable organizations to forensically analyze all user activity on many different system components, whether that activity is from a general user or administrator. Changes can be tracked to a specific user. Policy Authority for Unified Communications also supports privileged individual user activity logging options for IM messages and file transfers from (or to) the cardholder data environment.</p>
10.2	Implement automated audit trails to reconstruct the following events for all system components.	
10.2.1	All individual user accesses to cardholder data	<p>InTrust, InTrust Plug-in for File Access, and ChangeAuditor for File Systems can track and report on individual user access to the cardholder data stored on Windows file servers. Privilege Manager for Unix can do the same for cardholder data stored on Unix and Linux systems. Policy Authority for Unified Communications can log all IM messages for specific users and their file transfers to or from the cardholder data environment.</p>
10.2.2	All actions taken by any individual with root or administrative privileges	<p>The InTrust and ChangeAuditor families of activity logging solutions can track, report on, and alert on user activity with elevated user privileges on many different system components throughout the organization. Privilege Manager for Unix offers carefully controlled privilege access management (e.g., root delegation) and even keystroke logging for Unix and Linux users regardless of whether they are also managed within AD.</p>

PCI DSS Section	Requirement	How Quest products help address the requirement
10.2.3	Access to all audit trails	InTrust is an enterprise audit log solution that enables organizations to connect, collect, store and report on enterprise audit information, including all attempts to access event log (and even its own “raw” audit log) data. When used with an appropriate system configuration and administrative safeguards, Privilege Manager for Unix can protect access to audit trails by offering carefully controlled privileged access management (e.g., root delegation) and even keystroke logging for Unix and Linux users.
10.2.4	Invalid logical access attempts	The InTrust family of activity logging solutions provides failed authentication and other access attempt reporting and alerting on many different system components. This information includes the source machine, username, reason for failure, and date/time.
10.2.5	Use of identification and authentication mechanisms	InTrust can audit and report on the type of authentication mechanisms used to access cardholder data.
10.2.7	Creation and deletion of system-level objects	InTrust provides the ability to report and alert on all system-level activity.
10.3	Record at least the following audit trail entries for each event for all system components	
10.3.1	User identification	By enhancing the native logging capabilities of the OS and of Active Directory, InTrust , ChangeAuditor for Active Directory and Intrust Plug-in for Active Directory are able to determine and secure the recording of the caller account, user ID, or AD user account attributes for every action in the network. Privilege Manager for Unix provides equivalent functionality for Unix and Linux user IDs, regardless of whether they are managed within AD. Policy Authority for Unified Communications records screen name information that can be tied to unique user IDs for IM messages and file transfers of users with access to the cardholder data environment.
10.3.2	Type of event	InTrust enhances the native logging capabilities of the OS by normalizing event information and determining what type of event occurred through either the category or ID. Privilege Manager for Unix also captures and secures the type of event for Unix and Linux users, regardless of whether they are managed within AD.

PCI DSS Section	Requirement	How Quest products help address the requirement
10.3.3	Date and Time	InTrust captures the date and time of each event as it was created. Privilege Manager for Unix does the same for events on Unix and Linux systems. Policy Authority for Unified Communications can record the date and time for all real-time communications of users with access to the cardholder data environment.
10.3.4	Success or failure indication	The InTrust family of activity logging solutions has the ability to determine the difference between successful and failed access or change attempts of many different system components including file access, authentication, and object changes. Privilege Manager for Unix provides the same information for login attempts on Unix and Linux systems.
10.3.5	Origination of event	InTrust is always able to determine the origination of an event, whether that be a computer/server name or an IP address. Privilege Manager for Unix provides equivalent information on Unix and Linux systems.
10.3.6	Identity or name of affected data, system component, or resource	The InTrust family of activity logging solutions provides a complete view into the audit trail of changes to many different system components, including who made the change, when and where the change was made, and what was affected. Privilege Manager for Unix offers granular recording of data, system, and resource changes, down to keystroke and session logging for Unix and Linux users.
10.4	Synchronize all critical system clocks and times	Authentication Services solution provides a utility to synchronize Unix, Linux, and Mac clocks with AD. Reporter provides a report that identifies domain controllers with clocks out of sync.
10.5	Secure audit trails so they cannot be altered	InTrust provides an agent-side caching feature that protects the audit logs from modification while also removing the chance for lost logs. As the information is transferred across the wide area network (WAN), the data is encrypted using 3DES 168-bit encryption. Privilege Manager for Unix includes technology that helps to ensure audit trails cannot be altered.

PCI DSS Section	Requirement	How Quest products help address the requirement
10.5.1	Limit viewing of audit trails to those with a job-related need.	ActiveRoles Server can limit access to audit trail information on Windows systems based on job-related need. InTrust provides reporting through an access-based Web portal, so users can be given access to only the information they need. Privilege Manager for Unix is designed to permit system administrators to limit all user actions on Unix and Linux systems to only those with a job-related need.
10.5.2	Protect audit trail files from unauthorized modifications.	InTrust offers two storage methods, EMC Centera and Windows File Servers. EMC Centera provides data protection through proprietary methods. The information held in the repository is in a proprietary format and can be locked down through native methods. InTrust Plug-in for Active Directory and InTrust for File Access also have lockdown options for audit trails stored on Windows servers. In addition, Privilege Manager for Unix is designed to protect audit trail files from unauthorized modification. Policy Authority for Unified Communications is likewise designed to protect logged information from tampering and accommodates additional tamper-resistant controls at the database level.
10.5.3	Promptly back-up audit trail files to a centralized log server or media that is difficult to alter.	InTrust provides a full consolidation solution that enables organizations to take audit log data from locations from around the globe and consolidate this information in a single location. Privilege Manager for Unix provides for equivalent audit trail back-up functionality for Unix and Linux systems.
10.5.4	Write logs for external-facing technologies onto a log server on the internal LAN.	InTrust can collect and report on all syslog data being created at the network layer. Policy Authority for Unified Communications supports a centralized secure logging architecture for external facing technologies such as real-time communication networks.
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).	InTrust provides real-time alerting for successful and failed access attempts to critical areas. This includes the long-term storage area of audit log information. InTrust Plug-in for File Access or Change Auditor for File Systems can also be used to monitor the integrity of audit log files that reside on Windows servers.

PCI DSS Section	Requirement	How Quest products help address the requirement
10.6	<p>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).</p> <p>Note: Log harvesting, parsing, and alerting tools may be used to achieve compliance with Requirement 10.6.</p>	<p>InTrust offers an anomaly analyzer capability that automates significant log review functions such as catching unusual behavior. InTrust reports can be generated on a daily basis and distributed to the necessary persons.</p>
10.7	<p>Retain your 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 backup).</p>	<p>InTrust provides a long-term storage (one to seven years) area at a greatly reduced cost. Privilege Manager for Unix includes functionality to support online and off-line audit trail data retention policies for Unix and Linux systems.</p>

Requirement 11: Regularly test security systems and processes.

PCI DSS Section	Requirement	How Quest products help address the requirement
11.5	<p>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.</p> <p>Examples of files that should be monitored:</p> <ul style="list-style-type: none"> • System executables • Application executables • Configuration and parameter files • Centrally stored, historical or archived, log and audit files 	<p>InTrust, InTrust for File Access, and ChangeAuditor for File Systems can be used to monitor the integrity of Windows system settings and otherwise monitored files of all types on many different system components. Privilege Manager for Unix includes file integrity checking functionality to support policies that require critical file comparisons for Unix and Linux systems. Reporter can report on system settings and file-based attributes to determine if any files have been altered.</p>

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

PCI DSS Section	Requirement	How Quest products help address the requirement
12.4	Ensure the security policy and procedures clearly define information security responsibilities for all employees and contractors.	ActiveRoles Server, Access Manager, Authentication Services, and Privilege Manager for Unix can assist in automating and enforcing this policy.
12.5.4	Administer user accounts, including additions, deletions, and modifications.	ActiveRoles Server, GPOAdmin, and Privilege Manager for Unix can assist in automating and enforcing this policy.

Appendix A, Requirement A.1: Shared hosting providers must protect the cardholder data environment.

PCI DSS Section	Requirement	How Quest products help address the requirement
A.1.1	Ensure that each entity only runs processes that have access to that entity's cardholder data environment.	ActiveRoles Server and Single Sign-on for Java can be used by a hosting service provider to help ensure each hosted entity only has access to its own cardholder data environment.
A.1.2	Restrict each entity's access and privileges to its own cardholder data environment only.	ActiveRoles Server and Single Sign-on for Java can be used by a hosting service provider to help restrict each hosted entity's access and privileges to only its own cardholder data environment.
A.1.3	Ensure logging and audit trails are enabled and unique to each entity's cardholder data environment and are consistent with PCI DSS Requirement 10.	Reporter and InTrust can be used by a hosting service provider to help ensure logging and audit trails are enabled and unique to each entity's cardholder data environment.
A.1.4	Enable processes to provide for timely forensic investigation in the event of a compromise to any hosted merchant or service provider.	InTrust, ChangeAuditor for Active Directory and InTrust Plug-in for Active Directory can be used by a hosting service provider to help provide for timely forensic investigation in the event of a compromise.

Appendix B, Requirement 3: [Compensating controls must] be “above and beyond” other PCI DSS requirements.

(Simply being in compliance with other PCI DSS requirements is not a compensating control.)

PCI DSS Section	Requirement	How Quest products help address the requirement
3 b) and 3 c)(3)	Two-factor authentication from within the internal network can also be considered as a compensating control for non-console administrative access when transmission of encrypted passwords cannot be supported.	Defender leverages Active Directory to provide two-factor RADIUS authentication for any system, application, or resource from within the internal network.
3 c)(2)	[Depending upon the item under review] IP address or MAC address filtering [can be considered as a compensating control when combined with the appropriate existing PCI DSS requirements or other additional controls].	Privilege Manager for Unix can restrict access to cardholder data based on IP address and/or Mac address.

For More Information

For more information about how Quest products can help you with your compliance needs, visit <http://www.quest.com/compliance/>.

About Quest Software, Inc.

Now more than ever, organizations need to work smart and improve efficiency. Quest Software creates and supports smart systems management products—helping our customers solve everyday IT challenges faster and easier. Visit www.quest.com for more information.

Contacting Quest Software

PHONE 800.306.9329 (United States and Canada)

If you are located outside North America, you can find your local office information on our Web site.

E-MAIL sales@quest.com

MAIL Quest Software, Inc.
World Headquarters
5 Polaris Way
Aliso Viejo, CA 92656
USA

WEB SITE www.quest.com

Contacting Quest Support

Quest Support is available to customers who have a trial version of a Quest product or who have purchased a commercial version and have a valid maintenance contract.

Quest Support provides around-the-clock coverage with SupportLink, our Web self-service. Visit SupportLink at <https://support.quest.com>.

SupportLink gives users of Quest Software products the ability to:

- Search Quest's online Knowledgebase
- Download the latest releases, documentation, and patches for Quest products
- Log support cases
- Manage existing support cases

View the Global Support Guide for a detailed explanation of support programs, online services, contact information, and policies and procedures.



5 Polaris Way, Aliso Viejo, CA 92656 | PHONE 800.306.9329 | WEB www.quest.com | E-MAIL sales@quest.com
If you are located outside North America, you can find your local office information on our Web site