



Compliance Solutions for the Payment Card Industry Data Security Standard

Quest offers the most extensive set of tools available for Microsoft and Unix/Linux platforms to address your PCI DSS compliance needs. Reasons you should choose Quest:

- Solutions deliver integrated, industry-standard benchmarks
- Single source for PCI DSS compliance data
- Flexible, elaborate reporting capabilities
- Continuous audit, correction and remediation of areas that fall outside set parameters to help prevent fraud
- A solution framework that addresses PCI compliance pains at all levels throughout the organization

A consortium of financial institutions now requires all merchants who accept popular payment cards, such as credit cards and signature debit cards, to comply with a new standard for securing their customers' payment card data. The "Payment Card Industry Data Security Standard" (PCI DSS) has been mandated by all members of the PCI Security Standards Council, which currently includes Visa International, MasterCard Worldwide, American Express, Discover Financial Services and JCB. All banks that process payment transactions associated with these cards are responsible for ensuring their merchants meet the standard, and penalties for failing to comply with the standard can be severe.

For merchants and banks that use Microsoft Activity Directory as part of their identity and access management solution, Quest Software can help satisfy a significant portion of PCI's DSS requirements on not only Windows-based systems but also Unix, Linux and Mac systems. If you are among the many organizations that are struggling to meet the standard's requirements, our solutions can help you automate your compliance efforts and significantly ease the burden of the periodic (quarterly in some cases) audits.

What is PCI DSS?

There are 12 high-level requirements and two special requirement appendices that compose the PCI DSS. These range from mandates for physical server security to very specific IT control objectives. They specify how you must secure, handle, retain and manage your data. You can read the full standard at

https://www.pcisecuritystandards.org/tech/download_the_pci_dss.htm

Meeting PCI DSS Compliance

Quest's award-winning solutions provide the systematic efficiency and audit reports you need to meet the 12 PCI DSS requirements. If you are already familiar with the PCI DSS requirements, refer to the chart below to see how Quest's solutions support each section. If you need to study the requirements, visit www.quest.com/intrust/pci-compliance.aspx.

PCI DSS Mapping Summary														
Quest Solution	PCI Requirement Sections													
	1	2	3	4	5	6	7	8	9	10	11	12	AppA	AppB
Compliance Suite														
Reporter		X		X	X		X	X		X	X		X	
InTrust with InTrust Plug-in for AD				X	X			X		X			X	
ActiveRoles Server							X	X		X		X	X	X
Additional Solutions														
Defender								X						
Authentication Services	X	X		X			X	X		X		X		X
GPOAdmin	X	X				X	X	X				X		
Password Manager								X						
Privilege Manager for Unix				X			X	X		X	X	X		X
Single Sign-on for Java		X		X			X	X					X	X
Access Manager							X			X		X		

Quest's solutions to meet PCI DSS requirements assess the infrastructure and its level of security, track and alert on user and administrator activity, and provide automated remediation policies in case the PCI DSS standards and procedures are violated.

Quest automates the tasks required to meet the PCI DSS requirements, saving the time normally devoted to manual tasks. This allows you to dedicate your IT personnel to more productive activities and achieve greater ROI while meeting this industry standard.

Monitor On-going Security and Compliance Status

You'll have easy access to all the information you need to monitor Windows and Unix system configuration changes, root delegation, access control changes, and user activity patterns for compliance. This minimizes the effort and investment required to achieve and maintain compliance.

Provide Auditors Evidence of Appropriate IT Controls

Continuous processes ensure that audits occur within reasonable time periods. The processes ensure you have secure log files that are small enough to manage and easy to trace, so you'll spend less time and effort on both internal and external audits.

Interpret Data Automatically

Quest solutions allow you to establish rules for interpreting the effectiveness of your Windows and Unix system configurations. They also utilize compliance intelligence and built-in guidance to audit log data and ensure you conform to PCI DSS requirements. You can do more audit evaluation in-house and spend less on the external consultants and auditors. With Quest tools you can confidently maintain a defensible compliance position relative to auditors.

Empower Executives with Complete Reports

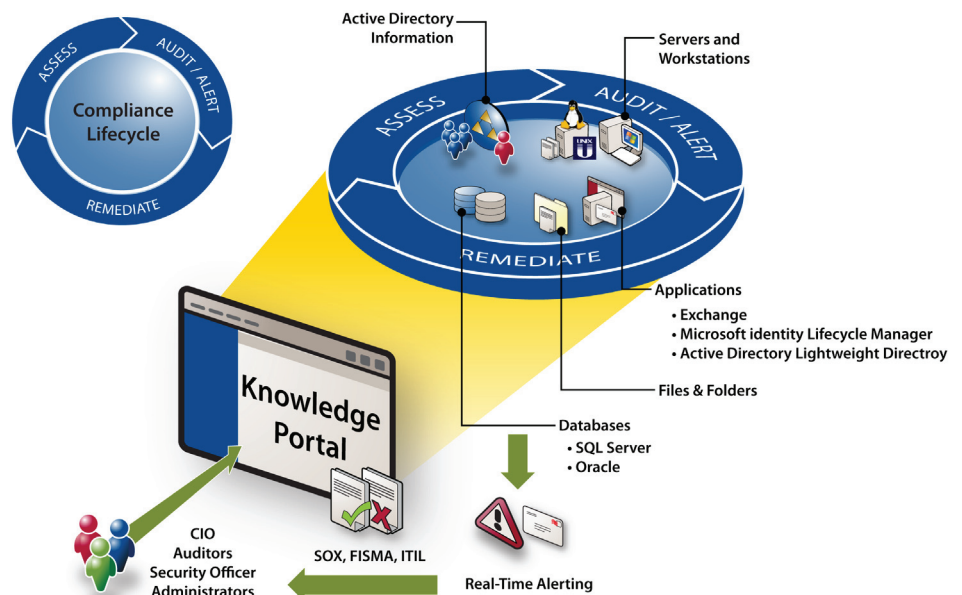
Executives can use compliance reports to confidently address stakeholders, with the knowledge that tools are in place to lower potential for fraud and security breaches, as well as meet compliance requirements.

Fill Compliance Gaps

Quest's solutions allow you to evaluate and recommend remediation measures to address PCI DSS compliance gaps as well as other organizational compliance shortcomings such as control deficiencies and material weaknesses. These same Quest solutions can be leveraged for broad organizational efficiencies to ensure your data structures are "tamper-proof."

Install and Deploy Solutions with Ease

Quest solutions feature an intuitive Quick Start wizard to allow you to quickly get the results you need. A Configuration wizard will guide you through a complete deployment for your event log management solution, including the creation of sites as well as the set up of policies, tasks, and rules.



Quest's integrated system provides a single view of your compliance initiatives.



www.quest.com
e-mail: info@quest.com
Please refer to our Web site for
international office information.

©2009 Quest Software, Inc. All rights reserved. Quest is a registered trademark of Quest Software.
All other brand or product names are trademarks or registered trademarks of their respective companies.