sectona

Solution Brief

Leverage Sectona to Comply with PCI DSS Requirements

Payment Card Industry Data Security Standard (PCI DSS v3)

The Payment Card Industry Data Security Standard (PCI DSS) is a set of requirements intended to ensure that all companies that process, store, or transmit credit card information maintain a secure environment. The standard specifically mandates protecting the cardholder data environment by taking preventive measures to secure privileged account access and passwords.

Sectona helps you achieve compliance with this standard by delivering and ensuring administrative access to your cardholder data environment is controlled, secured, and monitored. It further helps add value by providing rich analytics to improve visibility around user access to your cardholder data environment. Enterprises must be compliant with the PCI-DSS v3.2.1 around clauses of privileged access as highlighted below:

Requirements

Clause 2

Build and Maintain a Secure Network and Systems

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

Clause 7

Implementing Strong Access Control Measures

Restrict access to cardholder data by business need to know

Clause 8

Implement Strong Authentication Measures

Identify and authenticate access to system components

Clause 10

Regular Monitoring

Track and monitor all access to network resources and cardholder data

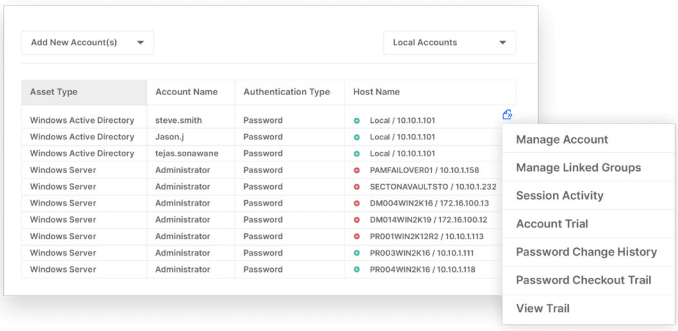
Explore How Sectona Helps You achieve Compliance with PCI DSS

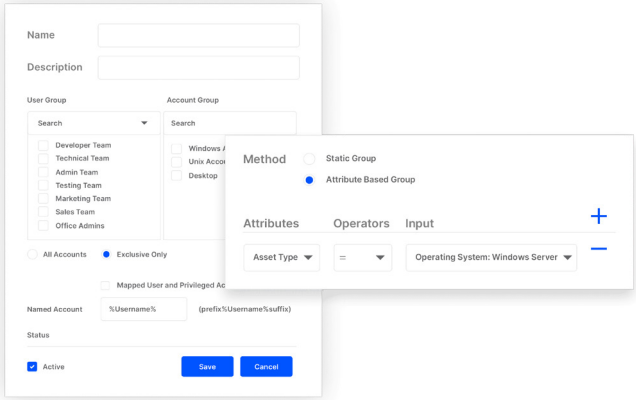
Sectona privileged access management solution addresses the PCI DSS standard requirements in and around clauses related to privileged or administrative account access. It also provides pre-defined and customizable reports out of the box that can help you provide evidence to prove compliance with PCI requirements.

Addressing Clause 2

Automate Password Management

Manage and Inventorize privileged accounts across infrastructure. Leverage strong password change capabilities from discovery, onboarding to rotation for all vendor supplied default accounts.





Addressing Clause 7

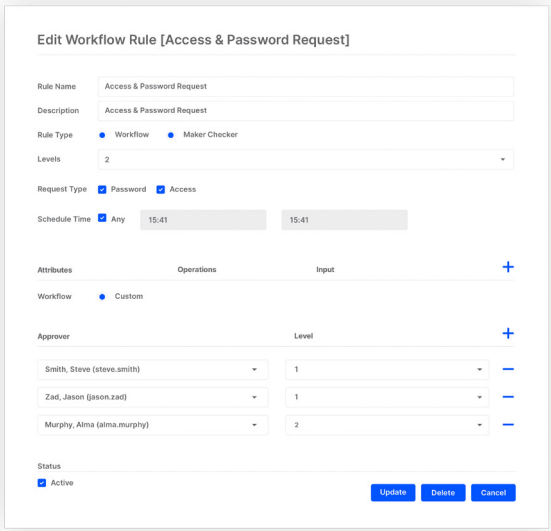
Defining Need-Based Access

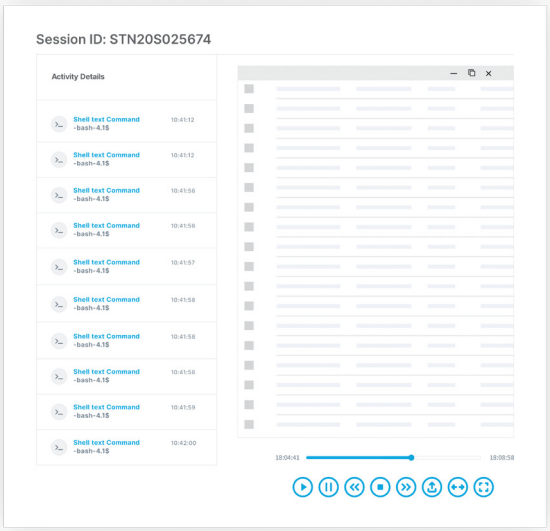
Configure access policy definitions based on user roles & functions. Define access to critical data and enforce restrictions on a need-to-know, need-to-access basis with strong workflow based access.

Addressing Clause 8

Authorized Access Provision with Built-in Multi Factor Authentication

Leverage deep integration with Active Directory for faster provisioning and de-provisioning of access. Control third-party vendor access by defining hybrid access mechanisms. Configure customizable MFA options to enforce second level of authentication for users.





Addressing Clause 10

Risk-Based Session Monitoring

Capture comprehensive logs of all critical sessions in both command and video format. Logs are stored in an encrypted format and provide auditable insights accessible only to authorized personnel.

---

sectona

Sectona is the leading Privileged Access Management company focused on protecting access to enterprise privileged accounts spread across data centers and the cloud. We have a global footprint, with a diverse client base from industries including Banking, Insurance, Government Institutions, Telecom Services, and Information Technology.

For more information, visit www.sectona.com and follow @SectonaTech on X (Twitter) or @Sectona on linkedin