

Does PCI DSS Requirement 8.2.2 allow users to share authentication credentials?

PCI SSC FAQ | Article 1080 | September 2024

Yes, but use of any shared authentication credentials such as group, shared, or generic IDs (including for administrator accounts such as admin or root) must be prevented unless needed for an exceptional circumstance and must be managed in accordance with all elements of PCI DSS Requirement 8.2.2.

PCI DSS Requirement 8.2.2 applies to all shared authentication credentials, not only those used by administrators. The intent of the PCI DSS requirements for strict management of user identification and accounts (requirements under 8.2) and strong authentication (requirements under 8.3) is to ensure each user is uniquely identified such that every action taken is attributable to an individual user ID. This allows organizations to maintain individual accountability for user actions and provide an effective audit trail per user ID. This will help speed issue resolution and containment if misuse or malicious use occurs.

For administrative functions, tools or password vaults can be used to facilitate management, security, and limited use of shared IDs, including confirming the identity of individual users and maintaining individual accountability and audit trails. A password vault is an example of a technology that can be used when a shared ID is needed for emergency use or “break the glass” administrator access.

Source: <https://www.pcisecuritystandards.org/faqs/1080/>