

# What is the intent of "administrative access" in PCI DSS?

PCI SSC FAQ | Article 1454 | October 2017

---

Accounts with administrative access are those assigned with specific privileges or abilities in order for that account to manage systems, networks and/or applications. As a general rule, the functions or activities considered to be administrative are beyond those performed by regular users as part of routine business functions. For example, activities related to normal processing of card payments and providing customer service would not be considered administrative.

Examples of accounts that are typically considered as administrative include:

- Accounts used for system administration. Depending on the operating system (OS), common names for these accounts might include root, administrator, admin or supervisor.
- Accounts with the ability to make unrestricted, potentially adverse, or system-wide changes.
- Accounts with the ability to install, remove or edit executable files.
- Accounts with the ability to assign or take ownership of sensitive data, system files, and/or programs.
- Accounts with ability to directly access or query databases containing cardholder data – for example, Database Administrators.
- Accounts with the ability to override or change security controls – for example;
- Turn security controls on or off, such as anti-virus software, firewalls, IDS/IPS or audit logs.
- Change or configure security policy settings, such as password policies (session timeouts, password expiry, etc.), role definitions, or firewall rules.
- Change other administrative accounts or passwords, including elevating privileges to administrator-level.
- Maintain logs, including setting log retention periods or changing or deleting logs.
- Alter access permissions to systems and/or data.
- Change cryptographic keys or encryption settings.

In addition to the above, each entity should identify any roles within their organization with elevated privileges that require additional protection. When determining whether an account should be considered administrative, the entity should consider the potential impact if that account is compromised. For example, an application-level account that creates user IDs only within the application, where those user IDs do not impact other systems or applications, might not be considered administrative. Conversely, an account with the ability to create or edit other accounts that themselves perform administrative tasks, or that have access to multiple applications or systems, would be considered administrative.

Some solutions encapsulate administrative access to a system component within a single sign-on solution, such as a remote access portal, that also provides non-administrative access to other system components. If a single sign-on account provides administrative access to any system component(s), this account would be considered administrative only for access to that system component(s).

Source: <https://www.pcisecuritystandards.org/faqs/1454/>