

# Can organizations use alternative password management methods to meet PCI DSS Requirement 8?

PCI SSC FAQ | Article 1467 | May 2019

---

The password requirements in PCI DSS include a minimum level of complexity and strength intended to be met by all types of organizations using a range of technologies. PCI SSC encourages organizations to implement stronger controls or additional security measures as appropriate to meet their security needs.

PCI DSS allows organizations to implement alternative controls than those defined in the standard, as long as the intent of the PCI DSS requirements is met. When considering alternative methods, it is important not to view individual recommendations in isolation but to take all the recommendations as a complete set of controls. For example, when considering the alternative controls described in NIST Special Publication 800-63B, the exclusion of periodic password changes without implementing additional compensating controls would not meet the intent of either the NIST Special Publication or PCI DSS.

Any variation to an authentication method that has been defined in PCI DSS will require that the organization consider how the approach could impact other settings and processes as well as the overall impact to security. Organizations wishing to follow a different combination of password complexity and change frequency than those defined in PCI DSS should document their approach as a compensating control. As part of this process, the organization will need to demonstrate how the risk is mitigated and how the intent of the requirement is met through the implementation of other controls.

PCI SSC continually monitors changes in technologies and payment environments and may incorporate updates in future PCI DSS revisions as needed to support evolving industry best practices.

Source: <https://www.pcisecuritystandards.org/faqs/1467/>