Authentication Methods that Align with CIS V 8.1, Control 5.2

Including Alternative Authentication Methods

Overview

The adoption of the CIS Control Framework 8.1 by the Commission on Technology (COT) in June 2025 affected long-standing authentication method requirements, including account management policies. Changes are needed to align to the password guidance contained in the framework. Simultaneously, the increasing ease of deployment for alternative authentication methods such as Virtual Smart Cards, including Windows Hello, presents challenges for interpretating and applying the account management requirements in the framework as written.

Once approved by COT, this document acts as the "minimum acceptable policy" for authentication methods in specific areas that deviate from or are otherwise not mentioned specifically in the CIS Control Framework. Items that match the framework may still be stated for simplicity.

The configurations listed in this document are intended to meet the spirit of CIS Controls while making small adjustments to better suit the branch's user experience and risk profile. Individual courts implementing the CIS Framework and this document may opt to be more stringent in their requirements but may not receive exceptions to be more relaxed. Legacy systems that do not support the requirements listed will be permitted to continue in use up to 5 years after the adoption of this document to provide time to update the system or migrate to a more modern solution.

Tactical Actions

Policy for Password-Only Accounts (including domain accounts that are not required to always use a virtual smart card):

- Minimum Length: 14 characters
- Maximum Length: Unspecified
- Minimum Age: 0 days
- Maximum Age: 0 days (never expires)

    - Password must be expired if known to be exposed or as requested by a user whose identity is validated.
- Complexity: Unspecified
- Password Banning: The system enforces a check on new password creation against a deny list of known bad, weak, or recently used passwords.
- Enforce Password History: 24 passwords remembered

Password/PIN Policy for Virtual Smart Cards (e.g., Windows Hello)

These settings apply specifically to any "gesture" used to unlock the Virtual Smart Card, such as the PIN or password that permits the Virtual Smart Card to be used. These settings do not alter the password requirement for the user account, only the settings related to use of the Virtual Smart Card feature.

- Minimum Length: 6 characters
- Maximum Length: Unspecified
- Minimum Age: 0 days
- Maximum Age: 0 days (never expires)
    - Password/PIN must be expired if known to be exposed or as requested by a user whose identity is validated.
- Complexity: Unspecified
- Biometrics: Biometric methods such as Facial Recognition or Fingerprint may be used to enhance the user experience but are not required. A PIN must always be allowed as a fallback method.
- TPM: Virtual smart cards must be backed by a TPM facility.
- Simple PINs: The virtual smart card must prevent simple PIN usage, either inherently or by policy configuration.

Password/PIN Policy for Hardware Smart Cards (e.g., Common Access Cards, YubiKeys, etc.)

These settings apply specifically to any "gesture" used to unlock a Hardware Smart Card, such as the PIN or password that permits the Hardware Smart Card to be used. These settings do not alter the password requirement for the user account, only the settings related to use of the Hardware Smart Card.

- Minimum Length: 6 characters
- Maximum Length: Unspecified
- Minimum Age: 0 days
- Maximum Age: 0 days (never expires)

    - Password/PIN must be expired if known to be exposed or as requested by a user whose identity is validated.
- Complexity: Unspecified

Account Lockout (for all account/password types)

- Account Lockout Duration: 15 minutes
- Account Lockout Threshold: 5 invalid logon attempts
- Reset Account Lockout Counter, Minimum: 15 minutes

References

- https://www.cisecurity.org/controls/v8
- https://www.cisecurity.org/insights/blog/why-are-authentication-and-authorization-so-difficult
- https://www.cisecurity.org/insights/white-papers/cis-password-policy-guide
- https://learn.microsoft.com/en-us/windows/security/identity-protection/hello-for-business/faq#does-windows-hello-for-business-prevent-the-use-of-simple-pins