Apple policy: Passcode

The **Passcode settings** section controls device passcode requirements and related security rules (for example, minimum length and complexity).

Options

In the Apple Policy Editor, passcode options are configured using a mix of toggles and numeric fields. Many fields include tooltips that indicate supported OS versions and supervision requirements.

Passcode toggles

- **ChangeAtNextAuth**: force a password reset the next time the user authenticates.
- **RequireAlphanumericPasscode**: require at least one alphabetic character and one number.
- **RequireComplexPasscode**: require a “complex” passcode (no repeating/sequential patterns and at least one non-alphanumeric character).
- **RequirePasscode**: require a passcode without additional length/quality requirements. Note: setting other passcode keys implicitly requires a passcode.

Numeric fields

- **FailedAttemptsResetInMinutes**: minutes before the failed-attempts counter resets (requires MaximumFailedAttempts).
- **MaximumFailedAttempts**: failed attempts allowed before the device is erased/locked (range: 2–11).
- **MaximumGracePeriodInMinutes**: how long the device can be unlocked without requiring the passcode (0 = none).
- **MaximumInactivityInMinutes**: idle time before the device locks (range: 0–15).
- **MaximumPasscodeAgeInDays**: max passcode age before a forced change (range: 0–730).
- **MinimumComplexCharacters**: minimum number of “complex” characters (range: 0–4).
- **MinimumLength**: minimum passcode length (range: 0–16).
- **PasscodeReuseLimit**: passcode history length to prevent reusing old passcodes (range: 1–50).

Revision #37
Created 2026-01-15 15:41:17 UTC by Admin
Updated 2026-04-22 15:46:22 UTC by Admin