Passcode

The **Passcode settings** section controls device passcode requirements and related security rules (for example, minimum length and complexity). On a Mac (macOS 13 or later, not with User Enrollment) the rules apply to the login password of the users.

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

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

Numeric fields

- **Failed attempts reset (minutes)**: minutes before the failed-attempts counter resets (requires Maximum failed attempts).
- **Maximum failed attempts**: failed attempts allowed before an iPhone or iPad is erased, or a Mac is locked (range: 2–11).
- **Maximum grace period (minutes)**: how long the device can be unlocked without requiring the passcode (0 = none).
- **Maximum inactivity (minutes)**: idle time before the device locks (range: 0–15).
- **Maximum passcode age (days)**: max passcode age before a forced change (range: 0–730).
- **Minimum complex characters**: minimum number of “complex” characters (range: 0–4).
- **Minimum length**: minimum passcode length (range: 0–16).
- **Passcode reuse limit**: passcode history length to prevent reusing old passcodes (range: 1–50).

Revision #60
Created 2026-01-15 15:41:17 UTC by Admin
Updated 2026-11-12 09:51:55 UTC by Admin