Policies - Apple

- Apple policies
- Apple policy: Passcode
- Apple policy: Restrictions
- Apple policy: Apps & profiles

Apple policies

Apple policies define management settings that Cerberus Enterprise applies to Apple devices via MDM. These settings are configured from the dashboard in the Apple policy editor.

Before you start

Apple device management requires Apple Management (APNs) to be configured. If needed, read the Apple Management setup (APNs) page.

Open the Apple Policy Editor

In the dashboard, open **Policies** and click **Create new Apple policy**. To edit an existing Apple policy, click its row in the policies table.

Editor layout

The Apple Policy Editor is organized as a set of expandable sections. At the top of the page you can always edit:

- **Name** (required)
- **Id** (read-only)
- **Description** (optional)

Policy sections

The sections below match the panels currently available in the Apple Policy Editor:

- **App management**: configure app-related restrictions and managed apps.
- **Passcode settings**: configure passcode requirements and related rules.
- **Security**: control features such as Auto Unlock and biometric unlocking.
- **iCloud**: allow or disallow specific iCloud services (backup, keychain sync, private relay, etc.).
- **Multimedia**: allow/disallow camera and related features.
- **Cellular**: control cellular-related settings (app cellular data settings, eSIM, plan changes).
- **Networking**: control AirDrop/AirPrint/AirPlay and other connectivity settings.

- **Accounts**: restrict account modification and (optionally) configure Google and Mail accounts.

> Many options in the Apple Policy Editor include a tooltip that documents requirements and supported OS versions.

Save, delete, and associated devices

Use **Save policy** to apply your changes. The button is disabled when there are no pending edits, or when the license is expired.

When editing an existing policy, the page also shows a **Delete policy** action. The editor can show an **Associated devices** list at the bottom, so you can see how many devices are currently using the policy.

Next pages

- Passcode: configure passcode requirements and related security options.
- Restrictions: define allowed features and OS-level limitations.
- Apps & profiles: configure installed apps and configuration profiles.

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).

Apple policy: Restrictions

The Restrictions sections control which OS features are allowed on managed Apple devices. In the Apple Policy Editor, these options are exposed as grouped panels with multiple toggles.

> Many restrictions are only supported on specific OS versions and may require supervised devices. Use the tooltips in the dashboard for authoritative requirements.

Security

- **Allow auto unlock**
- **Allow Fingerprint for Unlock**
- **Allow Fingerprint Modification**

iCloud

- **Allow iCloud address book**
- **Allow iCloud backup**
- **Allow iCloud bookmarks**
- **Allow iCloud calendar**
- **Allow iCloud desktop and documents**
- **Allow iCloud document sync**
- **Allow iCloud Freeform**
- **Allow iCloud keychain sync**
- **Allow iCloud Mail**
- **Allow iCloud Notes**
- **Allow iCloud Photo Library**
- **Allow iCloud Private Relay**
- **Allow iCloud Reminders**

Multimedia

- **Allow camera**
- **Allow File Sharing Modification**
- **Allow Files USB Drive Access**

Cellular

- **Allow app cellular data modification**
- **Allow cellular plan modification**
- **Allow eSIM modification**
- **Allow eSIM outgoing transfers**

Networking

- **Allow AirDrop**
- **Allow AirPlay incoming requests**
- **Allow AirPrint**
- **Allow AirPrint credentials storage**
- **Allow AirPrint iBeacon discovery**
- **Allow Bluetooth modification**
- **Allow Bluetooth Sharing modification**
- **Allow Files Network Drive Access**
- **Allow Internet Sharing Modification**

Accounts (restriction)

The Accounts panel contains both a restriction and (optionally) account configuration. The restriction toggle controls whether the user can modify system accounts.

- **Allow account modification**

Apple policy: Apps & profiles

This section documents how to configure managed applications and account payloads for Apple devices.

App management

The **App management** panel contains both general app-related restrictions and a list of managed apps.

General app restrictions

- **Allow app clips**
- **Allow app installation**
- **Allow app removal**
- **Allow automatic app downloads**
- **Allow apps to be hidden**
- **Allow apps to be locked**
- **Allow In-App Purchases**

Managed apps

Use **Add application** to add an app to the policy. Each managed app is displayed as a card. You can expand the card to edit its settings and remove the app using the delete action.

- **App Store ID**: the App Store identifier of the managed app.
- **Bundle ID**: the app bundle identifier.
- **Install behavior**: controls whether the app must remain installed or can be installed/removed by the user.
- **Assignment**: license assignment type.
- **VPP license**: VPP license type used for installation through the App Store.

Accounts

The **Accounts** panel lets you configure accounts that are applied to managed devices. It also includes a restriction toggle for account modification.

Restriction

- **Allow account modification**: when disabled, users cannot modify accounts such as Apple Accounts and internet accounts.

Add accounts

Use **Add Google account** or **Add mail account** to add account payloads to the policy. Each account appears as a card with its configuration fields.

Account credentials from users

Both Google and Mail account cards provide a **Account credentials from users** toggle. When enabled, the system applies account credentials on a per-user basis. When disabled, you enter the account identity in the policy.

Google account fields

- **Visible name**: the name shown to the user for the account.
- **Google email address**: the user email address.
- **Full name**: the user’s full name.

Mail account fields

Mail accounts include identity fields plus incoming/outgoing server configuration. Host names are required.

- **Visible name**: the name shown to the user for the mail account.
- **Email address**: the user email address.
- **Full name**: the user’s full name.

Incoming server

- **Server type**: mail protocol (for example IMAP or POP).
- **Authentication Method**: authentication method for the server.
- **IMAP path prefix**: shown only when Server type is IMAP.
- **Host name**: required.
- **Port**: server port (1–65535).

Outgoing server

- **Authentication Method**
- **Host name**: required.

- **Port**: server port (1–65535).

S/MIME options

For Mail accounts, you can also configure S/MIME encryption and signing behavior.

Encryption

- **S/MIME encryption**
- **Identity user-overrideable**
- **Per-message switch enabled**
- **User overrideable**

Signing

- **S/MIME Signing**
- **Identity user-overrideable**
- **User overrideable**

> Account and restriction options include tooltips in the dashboard that document prerequisites and supported OS versions.