Device Restrictions & Passcode Policies

Device Restrictions

The Restrictions profile configures restrictions on iOS, iPadOS, macOS, and tvOS devices. Features may vary based on the type and OS version of the device, and some may require supervision.

To create a Restrictions profile go to Management > Restrictions. Select the restrictions to be applied, and choose the Application time (Full time or according to a time profile). Assign the profile to users and/or devices and click Save.

If multiple Restriction profiles are installed on a device, the OS will combine all settings for the most restrictive configuration.

Common iOS/iPadOS Restrictions

Below is a list of common restrictions applied to iOS/iPadOS devices:

- Do not allow device name change: Users cannot modify the name of the device in Settings (iOS 9 or higher)
- Do not allow Wallpaper change: Users cannot modify the device wallpaper (iOS 9 or higher)
- Do not allow passcode change: Users cannot add, change, or remove a passcode to access the device (iOS 9 or higher). This includes Touch ID or Face ID.
- Do not allow News: Users will not have access to the News App (iOS 9 or higher)
- Do not allow modifications to account settings: Users can't create new accounts or change user name, password, or other settings associated with their account. Accounts include-- Apple ID, Mail, Twitter, Facebook, Flickr and Vimeo

- Do not allow Find my Device: It turns off Find My Device in Find My App. This restriction requires supervision.
- Don't allow the installation of apps via App Store: Users will not be able to install apps from the App Store
- Do not allow access files on Network Drive: Users will not be able to access files on Network Drive. This restriction requires supervision
- Do not allow USB Files Drive: Users will not be able to access USB Files Drive. This restriction requires supervision
- Force Wifi Power On: The user will not be able to turn off WiFi
- Force automatic Date & Time: The Date & Time setting is set automatically
- Do not allow AutoFill Passwords: Users cannot use the AutoFill Passwords feature. Users also won't be prompted with the option to pick a saved password to use in password fields in Safari or other apps.
- Do not allow nearby iOS devices to share requests for a password: Users' devices will not be able to advertise themselves to nearby devices for passwords by using the Proximity AutoFill capability.
- Do not allow password sharing: Users cannot share their passwords with the AirDrop Passwords feature

Common macOS Restrictions

The macOS Restriction profile is organized into six categories/tabs. Use the option 'Do not configure the options on this tab' in the Restrictions profile to ensure any settings or restrictions within the tab are not applied and the default or manual configuration that's present on the macOS devices will remain unchanged. This feature is important in prevention of accidental deployment of configurations and impact of devices assigned to the profile.

The tabs are organized with their corresponding restrictions. After making any changes to a Restriction profile and reinstalling the profile on devices, the Mac may require a reboot for the new restriction configurations to be applied.

macOS Restrictions Tabs

- Preferences: Restrict users from accessing areas of System Preferences or System Settings on the Mac. For devices running macOS versions earlier than macOS 13, configure the System Preferences tab. For devices running macOS 13 or later, configure the System Settings tab.
- Apps: Restrict settings for applications such as Game Center, Safari Autofill, and restrictions for the installation and updates of applications. This tab also allows you to restrict applications from launching. The Allowed and Disallowed Folders options have been deprecated in macOS 10.15 and later.
- Widgets: Allow specific widgets to run. This restriction option has been deprecated in macOS 10.15 and later.

- Media: Configure media types that are allowed, such as network media (AirDrop), internal disks, external disks, disk images, DVD-RAM, CDs & CD-ROMs, DVDs, and recordable disks. This restriction has been deprecated with macOS 11.
- Sharing: Configure services to be available in the sharing menu. For devices running macOS 10.13 or later, you can configure these services using the Extensions profile.
- Functionality: Configure specific settings to allow or disallow on the Mac. Some examples include iCloud services, password sharing, password AutoFill, requiring Admin credentials for network changes, erase all content and settings, AirPrint, and content caching.

Passcode Policies

The Passcode Policies profile configures passcode criteria on iOS, iPadOS and macOS devices. It supports the system scope and user scopes on macOS devices. If user scope is chosen, please assign only users to the profile. If existing passcodes do not meet the policy standards, users will be prompted to reset their password.

The Passcode Policy profile does not create or set passcodes and is not compatible with Apple Shared iPad devices. To set the PasscodeLockGracePeriod on Apple Shared iPad devices, configure the Apple Shared iPad Shared Device Group settings.

To create a Passcode Policy, go to Management > Passcode Policies.

Features include:

- Force PIN: Prompts users to set passcode within 1 hour (iOS, iPadOS)
- Allow simple value: Permits repeating, ascending and descending characters
- Require alphanumeric value: Requires passcodes to contain at least one letter and one number
- Force Password Reset (10.13+): Prompts for reset on next user authentication (macOS). This will prompt users anytime the profile is saved and/or reinstalled.
- Minimum passcode length: Sets the minimum of characters allowed
- Minimum number of complex characters: Sets the minimum of non-alphanumeric characters allowed
- Maximum passcode age: Enter 0 to not configure, or 1 day to 730 days
- Maximum Auto-Lock: Narrows times available to users to manually set Auto-Lock. On macOS, this maximum auto-lock value configures the screen-saver settings.
- Passcode history: Enter 0 to not configure, or 1 passcode to 50 passcodes (iOS, iPadOS)
- Maximum grace period for device lock: Longest device lock grace period available to users
- Maximum number of failed attempts: Maximum failed attempts prior to the device erases
- Delay after failed login attempts: Minutes that the device is locked for after maximum failed attempts (macOS)

Additional Considerations

- When an iOS/iPadOS device is locked, some commands may not apply until it is unlocked.
- If an iOS/iPadOS device has a passcode, it will not auto-join the network until it is unlocked after a restart. This can impact commands being delivered to the device if it is not connected to the network.
- If using Mosyle Auth on macOS devices, it's recommended to configure password policies through the identity service provider (IdP).
- Local administrators created from an Automated Device Enrollment profile are not exempt from the Passcode Policies profile on macOS devices. If the policy should not be applied to the Administrator created using Automated Device Enrollment, the profile should be assigned via the User Scope to specific users.
- It's recommended to turn on Force Password Reset to prevent lockout of users whose password does not meet policy standards on macOS devices.
- If the passcode policy still applies after profile uninstallation on macOS devices, please run the following command in Terminal, which is opened from Applications/Utilities, or the Custom Commands profile: pwpolicy -clearaccountpolicies

Removing a passcode on iOS/iPadOS devices

If the passcode is forgotten on an iOS/iPadOS device, it's important to keep the device connected to the network and not restart the device. The device will remain auto-joined to the network as long as it has not been restarted or powered off. As long as the device remains connected it can receive the Remove Lock Passcode command from Mosyle to remove the passcode, Touch ID, and/or Face ID.

To remove the passcode from an iOS/iPadOS device go to Management > Devices Overview > Select the device > More dropdown menu: Remove Lock Passcode.

If the command is sent and the device is connected to the internet, it will remove the passcode and allow the device to be unlocked with the Home button. If the Passcode Policies profile is installed on the device to force a password, it will prompt the user to set a new passcode.

Managing User Accounts on macOS

Administrators can manage User Accounts on Mac computers that are supervised and enrolled in Mosyle.

To access these options, go to Management > Devices Overview > Click on a device's name to bring up the Device Information window > More dropdown: Manage Users. Here you can either change the user's password or unlock the user account after too many failed password attempts.

In order to change a user's password, Administrator credentials for an admin user with a Secure Token is required. The new password must meet password policies, including the Passcode Policies profile or active rules in Security. If FileVault is turned on, the disk must be unlocked for the device to acknowledge the commands. The device must be online at the login window in order for the commands to go through to change the user's password or unlock the device.

If the user's password is unable to be changed through Mosyle, the password can be changed using the Reset Password Assistant in recoveryOS. To reset an account's password, follow the instructions under the heading "Use the Reset Password assistant" in the Apple Support article.

Changing the ADE Admin Password

When creating the Administrator account using the Automated Device Enrollment profile, a password needed to be defined. This password can be changed by sending the Set Admin password in Devices Overview, or using the Single Shot profile to Change the Randomized DEP Admin Password.

- Devices Overview: Go to Management > Devices Overview > Select Devices > More dropdown menu: Set Admin Password. Enter the new password for the DEP Admin account.
- Single Shot: Go to Management > Single Shot profile > Change Randomized DEP Admin Password. Choose the rotation interval of 30, 60, 90, or 120 days. This option ensures that devices are rotating the DEP Admin password on a regular basis to keep devices secure.

Revision #1
Created 2025-10-08 00:29:27 UTC by joliveira
Updated 2025-10-08 00:30:44 UTC by joliveira