Securing Devices

Overview

In the event a device belonging to the school or district is lost or stolen, there are remote management methods to lock the device, secure data stored, and/or prevent further use of the device.

Available options via the MDM include:

- Lost Mode (iOS & iPadOS): Lock a device with a specified message. Once locked, ping the device's location or play a sound to assist with locating the device.
- Activation Lock (iOS, iPadOS, & macOS): Lock the device so that once erased, it cannot be reactivated and set up until the user enters the Apple ID credentials to authorize the unlock or Activation Lock is disabled via the MDM. Available only for devices in Apple School Manager that are owned by the school or district.
- FileVault (macOS): Enforce FileVault to encrypt the disk and prevent unauthorized access.
- Firmware Password (macOS): Lock the device with a firmware password to block the ability to use startup key combinations and prevent users from starting up any internal or external storage device other than the selected startup disk. Available only for Mac computers with an Intel processor.
- Recovery Lock (macOS): Set a recovery lock password to prevent unauthorized access to the recovery partition on macOS devices. Available only for Mac computers with Apple silicon running macOS 11.5 or later.
- Lock device (macOS): Lock a device with a 6-digit PIN. The device cannot be accessed until the 6-digit PIN is entered. To lock Mac computers with Apple silicon, macOS 11.5 or later is required.

IMPORTANT NOTE: Mosyle will retain the Activation Lock bypass codes, FileVault Personal Recovery Key, and Lock PIN for the duration of time the device remains in the Mosyle system. If the device is removed from the MDM, the data will be removed from all Mosyle systems and cannot be recovered. Before removing devices from the Mosyle MDM, please be sure to take note of any codes, keys, or passwords that may be needed in the future.

Lost Mode (iOS/iPadOS)

To enable Lost Mode on a device, go to Management > Devices Overview > Select any/all devices to enable Lost Mode. From the More dropdown menu, choose “Activate Lost Mode”. Enter the desired message to be displayed on the device screen when it is locked (required), as well as a phone number or footnote (optional). In order for Lost Mode to be enabled on the device, it must have a valid network connection so it can receive the command from the MDM.

When Lost Mode is enabled, a banner will be presented under the Security Info tab in Device Information for the iPhone or iPad.

lost-mode.png

After turning on Lost Mode, the device will be locked. To play a sound or request the device location, click the More dropdown menu and choose: Request Location or Play Sound.

location-or-sound.png

Enabling Lost Mode will not prevent someone from erasing the device. If erased and the device is part of Apple School Manager and assigned to Mosyle, it will automatically re-enroll in the MDM after connecting to a network and will re-apply Lost Mode. If the device is not part of Apple School Manager, or is not assigned to the Mosyle MDM server, it can be erased and the user will be able to proceed with normal setup.

To disable Lost Mode, go to Management > Devices Overview > Select any/all devices to turn off Lost Mode. From the More dropdown menu, choose “Disable Lost Mode”. Again, devices will need a valid network connection to receive the command to release Lost Mode.

Activation Lock

Activation Lock is a built-in security mechanism on iOS, iPadOS, and macOS devices which prevents users from being able to activate and set up a device without knowing the Apple ID credentials that enabled Activation Lock. If Activation Lock is enabled and the device is erased, the user will be presented with a screen requesting the Apple ID credentials used to enable Activation Lock in order to proceed with setup. The device will be locked and unusable until Activation Lock is released or unlocked.

Activation Lock can be managed on devices owned by the school or district, and exist in Apple School Manager. Devices can be locked with Activation Lock in two forms:

- User-initiated: Users turn on Activation Lock in Find My or iCloud with their personal Apple ID
- MDM-initiated: The MDM turns on Activation Lock

Note: A T2 chip or Apple silicon is required on macOS devices for Activation Lock.

User-initiated Activation Lock

By default, devices enrolled in Mosyle MDM using Automated Device Enrollment will be blocked from User-initiated Activation Lock being enabled, in other words users enabling Activation Lock with their personal Apple ID. If the school or district prefers users to have access to enabling Activation Lock, check the box to “Allow User-initiated Activation Lock” in the Automated Device Enrollment profile.

Upon enrollment, Mosyle requests an Activation Lock bypass code from the device. This code can be used to unlock a device which has been Activation Locked by a user. Please note, Mosyle MDM is unable to manage or unlock Activation Lock if it was enabled prior to enrolling in the MDM.

If devices have already been enrolled and you wish to either allow or block User-initiated Activation Lock:

- iOS/iPadOS: Go to Management > Devices Overview > Click the device name to bring up Device Info > More dropdown menu > Allow User-Initiated Activation Lock.
- macOS: Go to Management > Devices Overview > MDM Options > Select or deselect Allow User-initiated Activation Lock.

If a device is User-Initiated Activation Locked after being enrolled in the Mosyle MDM, it can be turned off using one of the methods below:

- Within the Mosyle console: Management > Devices Overview > Click the device name to bring up Device Info > More dropdown menu > Disable Activation Lock.
- On the Activation Lock screen on the device, enter the Managed Apple ID and password of the ASM Admin user into the Apple ID and password fields. The credentials should be for the ASM Admin user who integrated and assigned devices to the Mosyle MDM server.
- Using the Activation Lock Bypass Code:
  - iOS/iPadOS: On the Activation Lock Screen on the device, leave the Apple ID field blank and enter the User-Initiated Activation Lock Bypass Code from Mosyle in the password field.
  - macOS: From the Activation Lock Screen on the device, click the Recovery Assistant menu option in the top left and select "Activate with MDM Key". Enter the User-Initiated Activation Lock Bypass Code from Mosyle in the field presented.

MDM-initiated Activation Lock

The MDM can enable MDM-initiated Activation Lock on any enrolled device that was enrolled via Automated Device Enrollment and is part of the school or district's Apple School Manager account. When enabling Activation Lock, the device is not required to have a network connection as the Activation Lock request is simply an API call between the Mosyle servers and Apple servers.

To enable Activation Lock, go to Management > Devices Overview > Click a device name to bring up Device Info > More dropdown menu: Enable MDM-Initiated Activation Lock.

If a device is MDM-Initiated Activation Locked, it can be turned off using one of the methods below:

- Within the Mosyle console: Management > Devices Overview > Click the device name to bring up Device Info > More dropdown menu > Disable MDM-Initiated Activation Lock.
- On the Activation Lock screen on the device, enter the Managed Apple ID and password of the ASM Admin user into the Apple ID and password fields. The credentials should be for the ASM Admin user who integrated and assigned devices to the Mosyle MDM server.
- Using the Activation Lock Bypass Code:
  - iOS/iPadOS: On the Activation Lock Screen on the device, leave the Apple ID field blank and enter the MDM-Initiated Activation Lock Bypass Code from Mosyle in the password field.
  - macOS: From the Activation Lock Screen on the device, click the Recovery Assistant menu option in the top left and select "Activate with MDM Key". Enter the MDM-Initiated Activation Lock Bypass Code from Mosyle in the field presented.

Activation Lock Bypass Code

Each device will have two Activation Lock Bypass Codes. One code is to bypass User-Initiated Activation Lock, the other is to bypass MDM-initiated Activation Lock (if MDM Activation Lock was enabled). Be sure to use the appropriate Activation Lock Bypass Code depending on how Activation Lock was enabled. To view the Bypass Codes, go to Management > Devices Overview > Click on a device's name to bring up Device Info > Click Security Info tab.

If Activation Lock is unable to be removed, the device will need to be taken to an Apple Store with proof of purchase in order to be unlocked.

activation-lock.png

FileVault (macOS)

The Security profile in Mosyle will enforce the enablement of FileVault. Find the profile by going to Management > Security & Privacy > Security tab > Add new profile. The FileVault settings are available under the FileVault tab.

To enforce and require FileVault, check the box for “Require FileVault”. Choose whether to use an Institutional Recovery Key, Personal Recovery Key, or both. Institutional Recovery Keys are not supported on Mac computers

with Apple silicon, so it's recommended to use Personal Recovery Keys.

personal-recovery.png

When using Personal Recovery Keys, it's recommended to escrow the key to the MDM so it's available as needed. To escrow the key, check the box “Escrow Personal Recovery Key”. Enter location information for the key and choose whether or not to show the end user the recovery key locally on the Mac when FileVault is enabled.

escrow.png

Last, choose when to prompt the user to enable FileVault. Select “Defer enabling until logout” to prompt users to enable FileVault when logging out, check the box “Ask at login” to prompt users to enable FileVault when logging in. Set the maximum number of times the user can skip the prompt to enable FileVault before being forced.

prompt-enable.png

Secure Token & Bootstrap Token

Users can only enable FileVault if they have a secure token. Starting with macOS 11, the first user created on the Mac with a plain text password is granted the initial secure token.

Users granted a secure token on macOS 11 and later:

- If the device is enrolled using Automated Device Enrollment and no Local User profiles are assigned, the user created during the Setup Assistant will be granted the initial secure token.
- If a Local User profile is deployed to devices enrolled using Automated Device Enrollment, this could result in the local user account being granted the initial secure token.
- If the device is enrolled using Automated Device Enrollment, no Local User profiles are assigned, and the user is not prompted to create an account during the Setup Assistant, the first user to login on the Mac will be granted the initial secure token. This is the case for deployments using Mosyle Auth 2, devices bound to AD using network/mobile accounts, or devices that only have the admin account created through Automated Device Enrollment and the user logs in to this account.

Because the password for the additional admin account created during Automated Device Enrollment is set using a password hash, the admin account created during Automated Device Enrollment is typically not the first user to be granted a secure token. In order for the admin account created during Automated Device Enrollment to be granted a secure token, the bootstrap token must be generated and escrowed. The bootstrap token is generated and escrowed to Mosyle only after a user with a secure token logs in for the first time. Once the bootstrap token is generated and escrowed, any other user who logs in on the Mac will receive a secure token (macOS 11 and later). This means, in order for the admin account created during Automated Device Enrollment to be granted a secure token, the user account will need to login on the Mac.

Mac computers with Apple silicon, enrolled via Automated Device Enrollment, require the bootstrap token to authorize the installation of kernel extensions and software updates via the MDM. Additionally, the bootstrap token is used to authorize the Erase All Content and Settings (EACS) command on Mac computers with the T2

security chip or Apple silicon running macOS 12.0.1 or later. Mac computers with Apple silicon that are manually enrolled will need to update the Security settings in Recovery mode so the MDM can install kernel extensions, software updates, and authorize EACS.

To allow the bootstrap token, configure your Automated Device Enrollment profile to “Allow Bootstrap Token” by going to:

1. My School > Apple Basic Setup
2. Enrollment > Automated Device Enrollment
3. Click the enrollment profile
4. Check the box to “Allow Bootstrap Token” and save
5. After the device is enrolled and a user with a secure token logs in, the bootstrap token will be created and escrowed in Mosyle.

Apple silicon devices that have already been enrolled via Automated Device Enrollment, but were not enrolled with the option to “Allow Bootstrap Token” can be sent a command after the enrollment to allow bootstrap token. To do this, follow the steps below:

1. Management > Devices > Devices Overview
2. Select the device(s) > More dropdown menu: MDM Options
3. Choose the option “Allow bootstrap Token”
4. After the command goes through, a user with a secure token will need to login to generate and escrow the bootstrap token. Once generated and escrowed, all other users logging in on the Mac will receive a secure token (macOS 11 and later).

Check out Apple's documentation for more information on FileVault, Secure token, and Bootstrap Tokens.

Rotating the Recovery Key

For security reasons, you may need or want to rotate the personal recovery key. You can do this in intervals of 30, 60, 90, or 120 days using the Single Shot profile under the Management tab.

1. Go to Management > Single Shot
2. Choose the action "Rotate FileVault key"
3. Select to rotate the personal recovery key or the institutional recovery key and enter the required information
4. Choose the interval for the rotation: 30, 60, 90, or 120 days
5. Assign the profile to users/devices

To rotate the institutional recovery key, you must enter the username and password for an Admin user on the Mac that has a secure token and upload the new institutional recovery key. To rotate the personal recovery key, you must enter the username and password for an Admin user on the Mac that has a secure token or select the option to use the current recovery key if it is escrowed in Mosyle.

Managing devices that are already encrypted

Devices that are already encrypted can be managed so that the personal recovery is escrowed in Mosyle. Some scenarios that administrators may find the need to do this include:

- If you are migrating to Mosyle from another MDM, are unable to erase and re-enroll the Macs, and they are already encrypted.
- Devices are currently encrypted with an institutional recovery key but need to be changed to be encrypted with a personal recovery key.

Below are options and workflows that can be used to migrate encryption management:

1. Decrypt the Macs, enroll in Mosyle and then install the Security profile to enforce FileVault encryption and escrow the recovery key in Mosyle.
2. If you know the username and password for an Admin user on the Mac with a secure token, once the Security payload from Mosyle is installed, you can configure the Single Shot profile to rotate the recovery key. After it's rotated, it will be escrowed in Mosyle.

If you need assistance with escrowing the personal recovery key, please contact the Mosyle Support Team.

Firmware Password (macOS)

The Firmware Password profile sets a password on the firmware of Intel-based devices running macOS 10.13 or later. A firmware password prevents users who don't have the password from starting up all disks other than the designated startup disk and blocks most startup key combinations.

To add a firmware password to a Mac, go to Management > Click the Firmware Password profile > Enter the new password. If the devices already have a firmware password and it needs to be changed, select “The devices already have a firmware password” and enter the old password. To remove the firmware password, leave the new password field blank and enter the current password.

Mac computers with Apple silicon do not support firmware passwords. Mosyle is unable to remove or change a firmware password if the current password is forgotten. In a scenario where the firmware password is unknown, please contact Apple.

Recovery Lock Password (macOS)

The Recovery Lock profile sets a Recovery Mode password on Apple silicon devices running macOS 11.5 or later. A Recovery Lock password prevents users who don't have the password from booting Apple silicon devices into Recovery Mode. Recovery Lock passwords are removed when a device is erased or removed from the MDM.

To add a recovery lock password to a Mac, go to Management > Click the Recovery Lock Password profile > Enter the new password. If the devices already have a recovery lock password and it needs to be changed, select “The devices already have a recovery lock password” and enter the old password. To remove the recovery lock password, leave the new password field blank and enter the current password.

Lock Device (macOS)

Lock a device with a 6-digit PIN so it cannot be accessed until the correct 6-digit PIN is entered. To send the command to lock the Mac, go to Management > Devices Overview > More dropdown menu: Lock Device. Enter the 6-digit PIN.

lock-device.png

The last 10 Lock PIN codes are available under Management > Devices Overview > Click on the device's name > Has Lock PIN Code? > Click here to see the last Lock PIN Code. If the PIN is entered incorrectly too many times and shows the Mac is “Disabled”, please contact Apple support to unlock the devices.

Reminder: If the device has been sent a command to lock the device with the Lock PIN code and is then removed from Mosyle MDM, the PIN code sent will no longer be able to be retrieved from Mosyle systems if it is forgotten.

Using Dynamic Device Groups

Check device security status using Dynamic Device Group criteria. Criteria listed below can help identify devices that are not meeting security requirements of the school or district and need to be addressed, or assist in identifying devices that have potentially been lost or stolen:

- Activation Lock Status: Disabled or Enabled
- Bootstrap Token: is or is not Present
- Bootstrap Token Allowed for Authentication: is or is not Allowed
- FDE Personal Recovery Key: Disabled, Enabled, or Escrowed
- FileVault Encryption: Disabled or Enabled
- Lost Mode: Disabled or Enabled

Revision #1
Created 2025-10-08 00:32:36 UTC by joliveira
Updated 2025-10-08 00:34:35 UTC by joliveira