

iOS 13 Unlock Token Handling (Historical)

 Historical compatibility note. This page documents iOS 13 unlock-token handling in FileWave 13.1.2 and earlier. Use a currently supported FileWave release for production device management.

FileWave MDM can clear a passcode on a managed device without an administrator knowing the passcode set by the user. This is useful when recovering shared or institution-owned devices.

The device sends FileWave an Unlock Token. FileWave returns that token with the ClearPasscode request, so the enrolled MDM service can clear the passcode without receiving the passcode itself.

In iOS 13, Apple changed unlock-token delivery so that the token is sent during enrollment. Protect the stored token and include FileWave data in the organization's backup plan.

Apple recently clarified how this change would be effective: the device may still send a TokenUpdate message to the MDM server, but the message will not contain the token anymore.

Before FileWave 13.1.3, a `TokenUpdate` message without an `UnlockToken` could clear the token stored by FileWave. Managing iOS 13 devices with an earlier FileWave release could therefore remove the server's ability to clear the device passcode.

It is therefore highly recommended to:

- Back up the FileWave instance regularly so sensitive data, including unlock tokens, is protected.
- Upgrade FileWave 13.1.2 or earlier to at least 13.1.3 before managing iOS 13 devices.
- Ensure iCloud Backup is configured on iOS devices when it is permitted by organizational policy.

You also have the ability to defer software updates by deploying a restriction profile (more information in this [KB article](#))

🔄Revision #3

★Created 2023-07-13 21:12:12 UTC by Andrew Kloosterhuis

✎Updated 2026-08-06 12:58:01 UTC by Josh Levitsky