

Apple MDM Enrolment Methods

Description

Enrolling Apple devices involves the installation of an MDM Enrolment Profile.

Installation may be initiated by either the user or the device. This same distinction also applies to the linking of the enrolment.



Initiating Enrolment

This refers to the driving force of enrolment.

Consider Automated Device Enrolment (ADE), delivering the Profile before authentication (if configured). This is an example of profile-driven enrolment.

User-driven enrolment relies on the authentication of a user in advance.

User vs Device Enrolment

Automated Device Enrolment links enrolment with the identity of the device; providing the maximum management options available. The extreme opposite is Bring Your Own Device (BYOD) enrolment. This is an example of the user's identity linking enrolment and provides the minimum amount of control.

User enrolment cryptographically separates organisational data from user data and limits many features of MDM. Further details explained in Apple's KB:

[User Enrolment and MDM](#)

Overview

Therefore, the key methods of enrolment can be categorised as:

- Profile-driven device enrolment
- User-driven device enrolment
- Profile-driven user enrolment
- User-driven user enrolment

Enrolment Methods

Automated Device Enrolment

On startup, the device reaches out to Apple and, where associated, the Enrolment Profile is delivered to the device and installed. The user is then prompted for authentication (if not configured for no authentication).

OTA Enrolment

This enrolment type potentially has two offerings:

- User authenticates to download the Enrolment Profile and then installs the Profile manually.
- An Enrolment Profile is provided to the user, for example by email, and the user manually installs the Profile.

BYOD

BYOD also could be described with two possible options:

- Enrolment Profile is downloaded and then the user authenticates
- User authenticates in Settings and then approves the subsequently downloaded Profile.

Deprecation



Although definitions exist for all enrolment methods above, as of iOS18 and macOS15 Apple will no longer support profile-driven user enrolment. This impacts the first described BYOD enrolment method, meaning BYOD with personal devices must action user-driven enrolment.

User-Driven User Enrolment

Although these are personal devices, this enrolment method requires the user to add credentials into Settings which must be a Managed Apple ID. Federated Authentication links a supported IdP with Apple, matching Managed Apples IDs with IdP usernames

and passwords.

Federated Authentication



User-driven user enrolment is currently targeted for FileWave 15.6. Confirmation of inclusion should be available closer to release.

Related Content

- [Apple Automated Device Enrolment](#)
- [Apple Manual Enrolment](#)

🔄Revision #6

★Created 13 September 2024 07:15:16 by Sean Holden

✎Updated 13 September 2024 14:09:28 by Josh Levitsky