Apple's Automated Device Enrolment

What

From inception known as Device Enrolment Programme (DEP), Apple's Automated Device Enrolment (ADE) is a zero touch enrolment method for Apple devices.

This article aims to cover the generic processes.

When/Why

Typically this process is used with new devices or those erased.

Registration

The basics:

- Devices, purchased from a supplier signed up to Apple's programme, are registered with Apple
- FileWave MDM server is registered with Apple
- Devices are assigned to the FileWave MDM server within the Apple Business or School account: ABM or ASM

Enrolment Profile

Enrolment Profile has options, e.g which Setup Assistant items are shown. When an Enrolment Profile is associated with one or more devices, the Enrolment Profile is sent to Apple; differing Enrolment Profiles may be configured and associated with different devices.

Working with Apple's Device Enrollment Program (DEP)

How

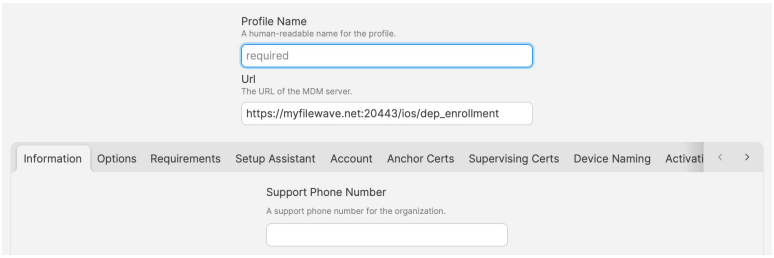
Enrolment Stages

Enrolment Profile delivery

When the device is first connected to a network, the device will initially communicate with Apple. Apple observe the identity of the device and if there is an associated Enrolment Profile with this device, the Profile is sent to the device.

> Once the Enrolment Profile is delivered, it will remain on the device, even if rebooted. Only a subsequent erase of the device will remove the Enrolment Profile and the process be re-triggered from scratch.

A key item in the Enrolment Profile is the MDM Server URL.



Check-in

The device reads the MDM Server URL and the enrolment process can then begin.

Authentication

The next requirement from check-in is authentication.

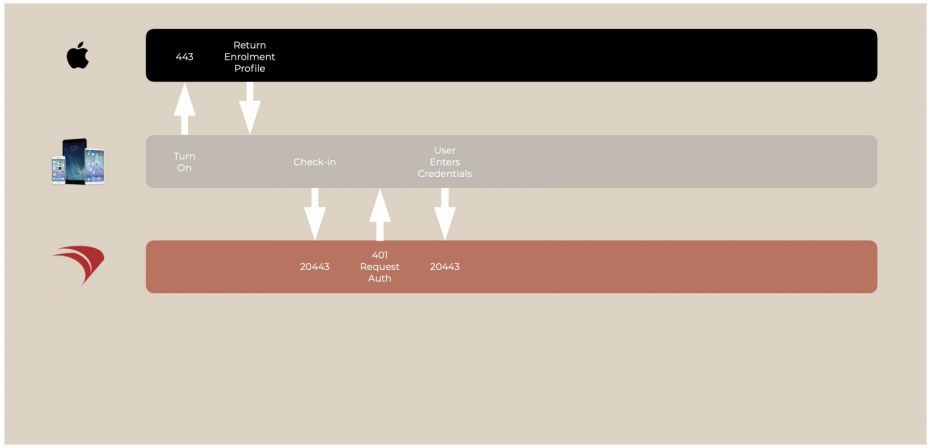
> On initial check-in, FileWave server returns a 401 due to no authentication and then informs the device how to authenticate.

Local Authentication	FileWave is configured with a local username and password encrypted on the FileWave Server (Default)
No Authentication	FileWave Server is configured to allow devices to enrol with no authentication required

No Authentication	FileWave Server is configured to allow devices to enrol with no authentication required
LDAP	An LDAP server, e.g. Active Directory, is configured, allowing directory users to authenticate enrolment
IdP	Okta, Google or Entra users may authenticate enrolment

Local and No authentication are configured through the server command line, LDAP may be configured through FileWave Central, whilst IdP is configured through FileWave Anywhere.

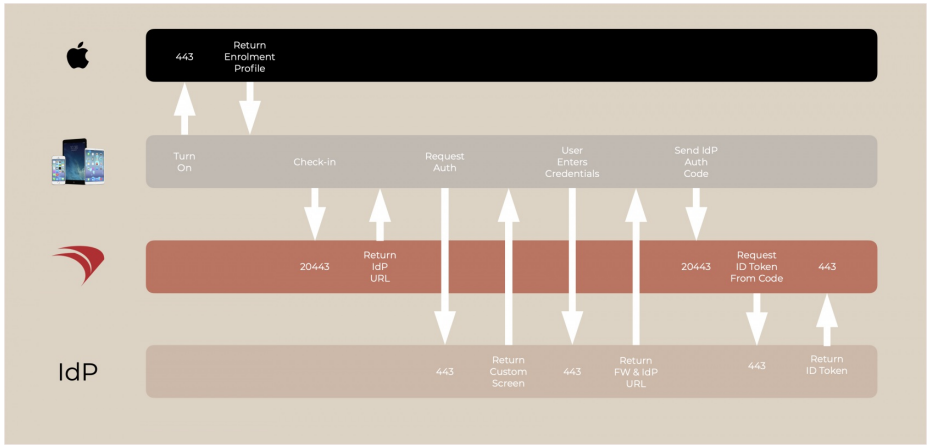
Basic Authentication



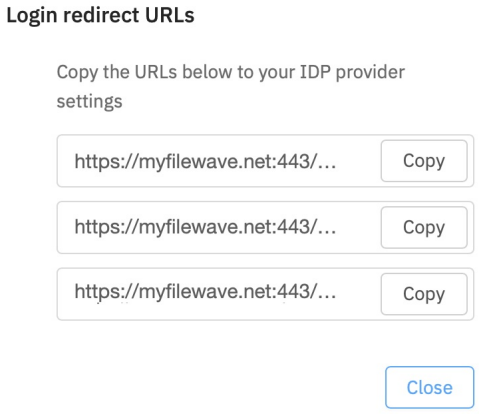
IdP Authentication

IdP requires a special mention here due to the additional steps involved.

FileWave server informs the device with a URL to direct the authentication; the IdP. The IdP custom authentication screen should be presented to the user and on entering details, if successful, the IdP uses the configured redirect, to contact the FileWave server to inform of success.



Redirects provided to IdP for connection with FileWave Server may be viewed from FileWave Anywhere, for example:



FileWave Server informs the IDP where to respond to the FileWave Server once complete. The FileWave returned URL to send on the code from the device will be through port 20443 and includes the auth code as a parameter within the URL.

Federated Authentication

An extension of IdP, Federated Authentication is an offering from Apple, which allows Apple IDs/passwords to be synchronised with an IdP. This is configured within Apple's Management portal; FileWave is not involved with this configuration.

https://support.apple.com/en-gb/guide/apple-business-manager/axmb19317543/web

---

Revision #8
★Created 16 August 2024 09:15:53 by Sean Holden
✎Updated 13 September 2024 10:02:25 by Sean Holden