This Miro was last updated on October 23, 2023

The Basics: Username, Password, Profiles and Domains

The Microsoft Windows OS is built on the foundation of a shared device. Every user of the device needs a unique user name and password which is combined with a unique set of configuration options called a profile. Profiles consist of the Documents, My Pictures, Desktop, Shortcuts, and many other user specific configuration items. To ensure privacy with each profile, Microsoft created the "NT File System," or NTFS, which controls the permissions to the individual files and folders that make up a user profile. With a username, a password, a profile, and NTFS you have the foundation of the Windows OS security model. In practice, an end user turns on a computer, is asked to enter in the username and the password and the Windows OS chooses the corresponding user profile and the end user is off and running. Over time the requirement to type in a username and password is being augmented with biometric solutions like Windows Hello or device pin codes.

Microsoft provides IT Administrators two choices for username, password, and profile management :

Option 1: Workgroup

In this de-centralized approach the user name, password, and profile is created on the device. This method is seeing a resurgence in the industry as companies move away from Microsoft solutions and implement technologies like Okta Universal Directory

Option 2: Domain

In this centralized approach the user name and password is created on a Windows Server named a Domain Controller (DC). User profiles are created locally on the device, but access to the profile is controlled through the Domain Controller. There are two types of Domains: Active Directory (AD) and Azure Active Directory (AAD). The core difference between AD and AAD is that with AD the DC is installed in a customer's datacenter; but with AAD, the DC is running in Microsoft's Azure Cloud infrastructure. A third method often referenced is Hybrid Domain. In a Hybrid Domain, the computer is joined to AD and joined to AAD.

When configuring Windows 10 the 2 options above become 1 of 4 choices that must be determined during OS Setup:

1. Workgroup
2. Active Directory Domain (AD)
3. Azure Active Directory Domain (AAD)
4. Hybrid (this is a combination of AD + AAD)

What is VMware Workspace ONE UEM's role in Windows OS Provisioning:

Workspace ONE UEM does not install the Windows Operating System (OS) on a computer hard drive.

It is up to the OEM or the IT Administrator to install the Windows OS. There are various methods to install the OS on a hard drive. One of the most common techniques is for the IT Administrator to copy the OS install files to a USB key, then boot the computer from the USB key which triggers the OS installation to begin. For a step-by-step guide to creating a USB key for this purpose, reference Brooks Peppin's blog:
https://brookspeppin.com/2019/01/12/create-a-zero-touch-windows-10-setup-usb-key/

!!! The workflows below assume that the OS has already been installed on the hard drive !!!

Once the OS has been installed on the hard drive, part of the OS configuration steps involve choosing a user management model. VMware Workspace ONE UEM's role is to automate the user management model choice, and then finish the configuration of the OS. In summary... Workspace ONE UEM configures the OS, it does not install the OS.

IT Administrators have 3 primary options to choose from to automate the Windows 10/11 OS configuration:

1. Image the computer / Traditional. Most PC LifeCycle Management (PCLM) solutions like Microsoft's System Center Configuration Manager (SCCM) use this approach
2. Microsoft Out-of-box Experience (OOBE) with our without MIcrosoft AutoPilot
3. Workspace ONE UEM Drop-Ship Provisioning

In a perfect world the three OS provisioning options would support the four Microsoft models (Workgroup, AD, Entra ID, Hybrid), but they do not. For this reason it is critical to choose the right configuration model based on the customer's user profile management model. The workflows below will detail each of the 3 methods to illustrate what choices are available.

Before continuing there are a couple more concepts to understand:

To automate many of the decisions necessary to complete the OS installation, Microsoft has created a template file. The template file is an XML file named the unattend.xml. For automating the installation of applications during the OS Setup, a second automation tool named a Provisioning Package (.PPKG) can be used. Workspace ONE UEM includes a method to create the unattend.xml and .PPKG file for this purpose.

With the above background in mind, what follows below is a visual flow for each OS provisioning method. We begin with a high level summary of the decision points. Each path below uses a color coded set of arrows to illustrate the choices available.

As a final note, it is possible to combine some of the workflows described below. For example Drop Ship Provisioning OFFLINE and OOBE/AutoPilot could be combined. The purpose of the illustrations below are to document the base level configurations.

Windows 10/11 Computer Onboarding Options Available

Microsoft Out of Box Experience (OOBE)

Workspace ONE UEM Drop-Ship Provisioning (ONLINE)

Workspace ONE UEM Drop-Ship Provisioning (OFFLINE)

Image (MDT, Ghost, etc)

Windows Autopilot

Without Windows Autopilot

Computer placed in one of the following Microsoft Domain Models

* Microsoft renamed Azure Active Directory (AAD) to Microsoft Entra ID

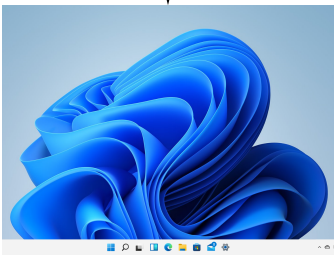
Microsoft Entra ID*

Active Directory (AD)

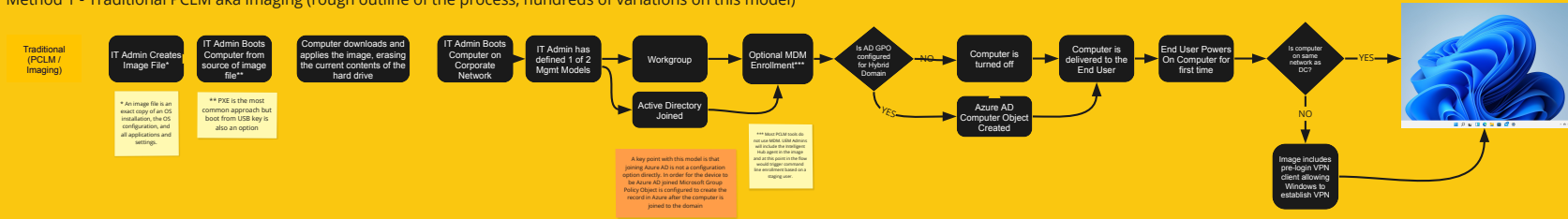
WORKGROUP

OPTIONAL - Both AD and Entra ID (Hybrid)

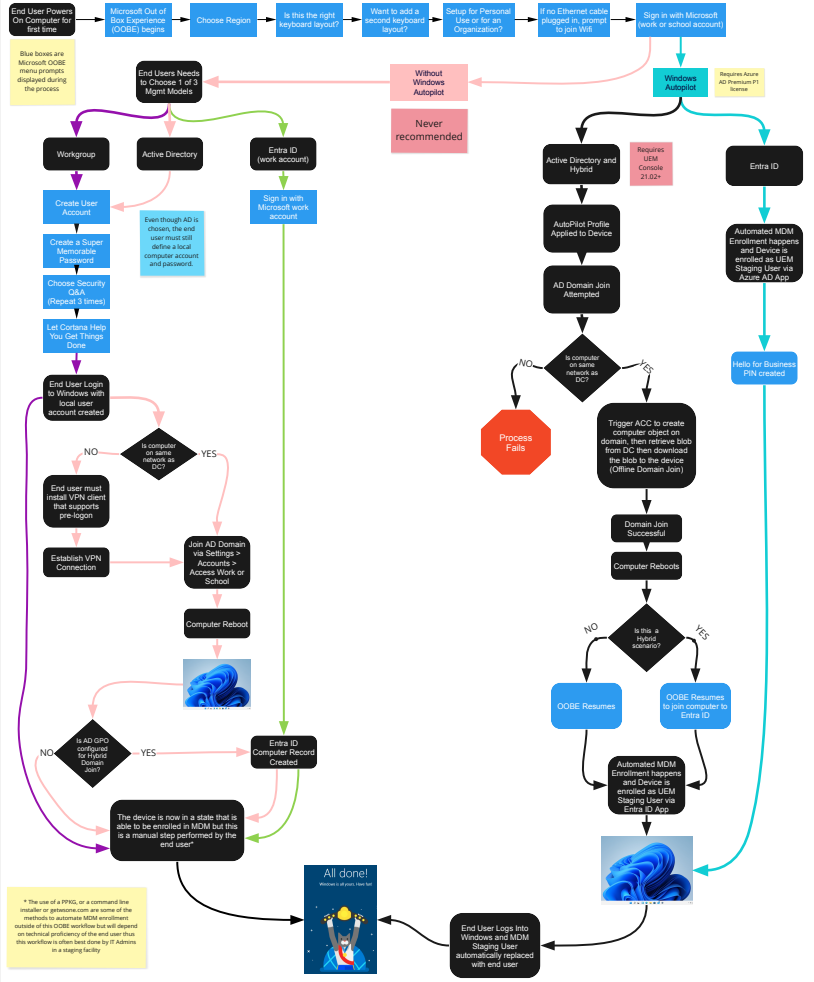
Device is enrolled in MDM



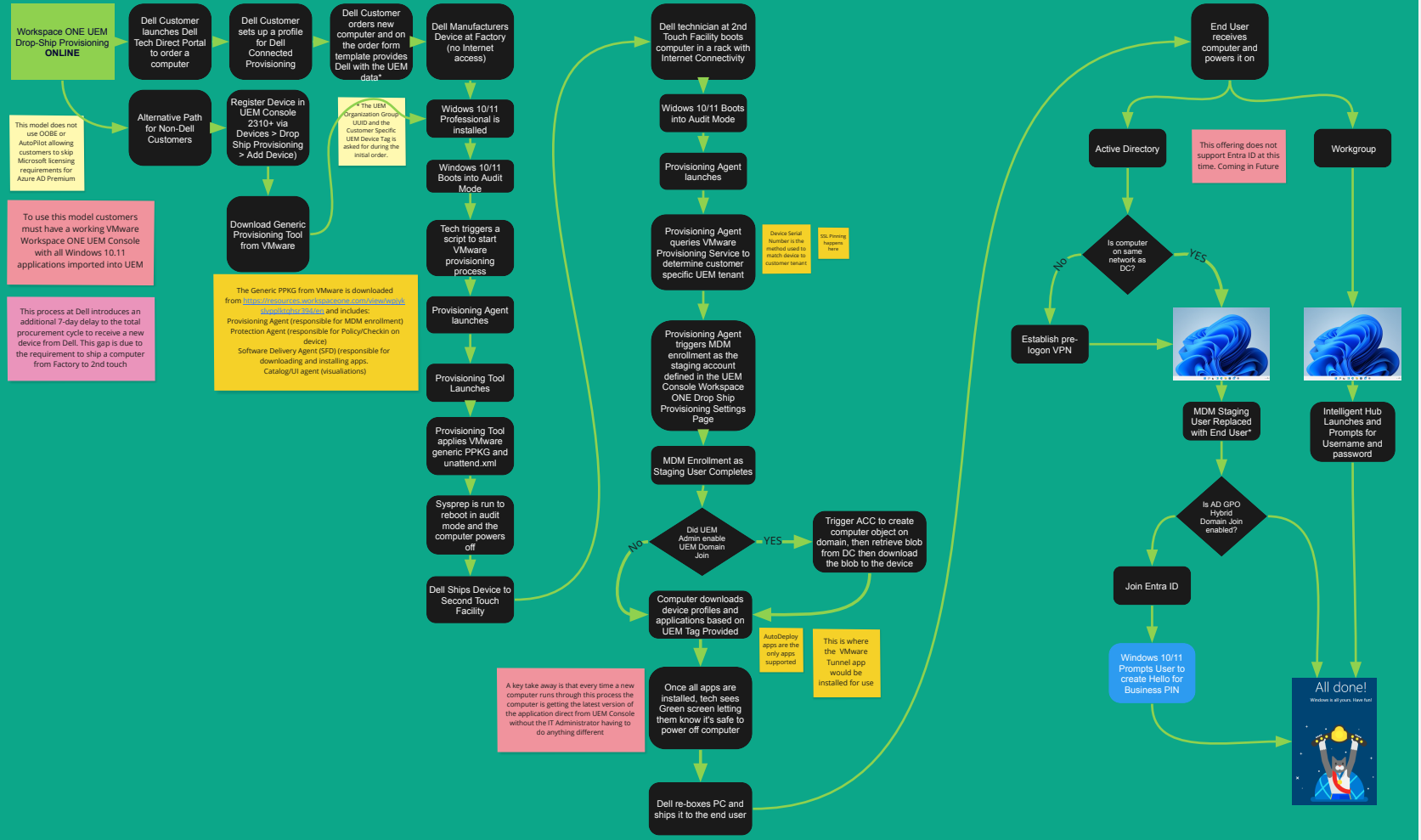
Method 1 - Traditional PCLM aka Imaging (rough outline of the process, hundreds of variations on this model)



Method 2 - Microsoft Out of Box Experience (OOBE) with and without Microsoft AutoPilot



The new provisioning service that drives this entire process is available for all VMware customers worldwide and is not OEM specific. The specific offering through a Dell paid SKU is still in the pilot phase and NOT available for sale at this point. When it is made available it's going to be available from Dell Direct AND this is ONLY available in the United States of America.



Method 3b - Workspace ONE UEM Drop-Ship Provisioning **Offline**

Best Practice is to use this as a last resort - aim for Method 3A DSP ONLINE

(formally named Dell Factory Provisioning then renamed to Factory Provisioning)

Available for purchase via Dell / HP / Lenovo Direct SKU. Available for use by any other OEM or customer