GUIDE – FEBRUARY 2019

PRINTED 26 FEBRUARY 2019

ONBOARDING OPTIONS FOR MACOS: VMWARE WORKSPACE ONE OPERATIONAL TUTORIAL

VMware Workspace ONE

vmware

Table of Contents

OT-WS1-macOS-onboard

Overview

Introduction

VMware provides this operational tutorial to help you with your VMware Workspace ONE® environment. Workspace ONE simplifies access to cloud, mobile, and enterprise applications from supported devices. As an IT professional, you can use Workspace ONE to deploy, manage, and secure applications. At the same time, you can offer a flexible, bring-your-own-device (BYOD) initiative to your end users from a central location.

Purpose

This operational tutorial provides you with discussions and exercises to help with your existing VMware Workspace ONE® production environment. VMware provides operational tutorials to help you with

- Common procedures or best practices
- Complex manual procedures
- Troubleshooting

Note: Before you begin any operational tutorial, you must first deploy a production environment. For information about deployment, see the VMware Workspace ONE Documentation.

Audience

This operational tutorial is intended for IT professionals and Workspace ONE administrators of existing production environments. Both current and new administrators can benefit from using this tutorial. Familiarity with networking and storage in a virtual environment is assumed, including Active Directory, identity management, and directory services. Knowledge of additional technologies such as VMware Identity Manager™ and VMware Workspace ONE® UEM (unified endpoint management), powered by VMware AirWatch, is also helpful.

Understanding macOS Onboarding

Introduction

Users can enroll a macOS device in many ways. This operational tutorial covers a number of enrollment workflows, including user-initiated enrollments, single-user and multi-user staging for network users, and single-user staging without domain binding.

Understanding macOS User Types

MacOS inherently supports a number of discrete user accounts (each with their own data and settings). Although macOS is an inherently multi-user system, the `mdmclient` process built-in to macOS (leveraged by Workspace ONE UEM) is not multi-user capable *unless* the device is bound to a directory service (such as Active Directory).

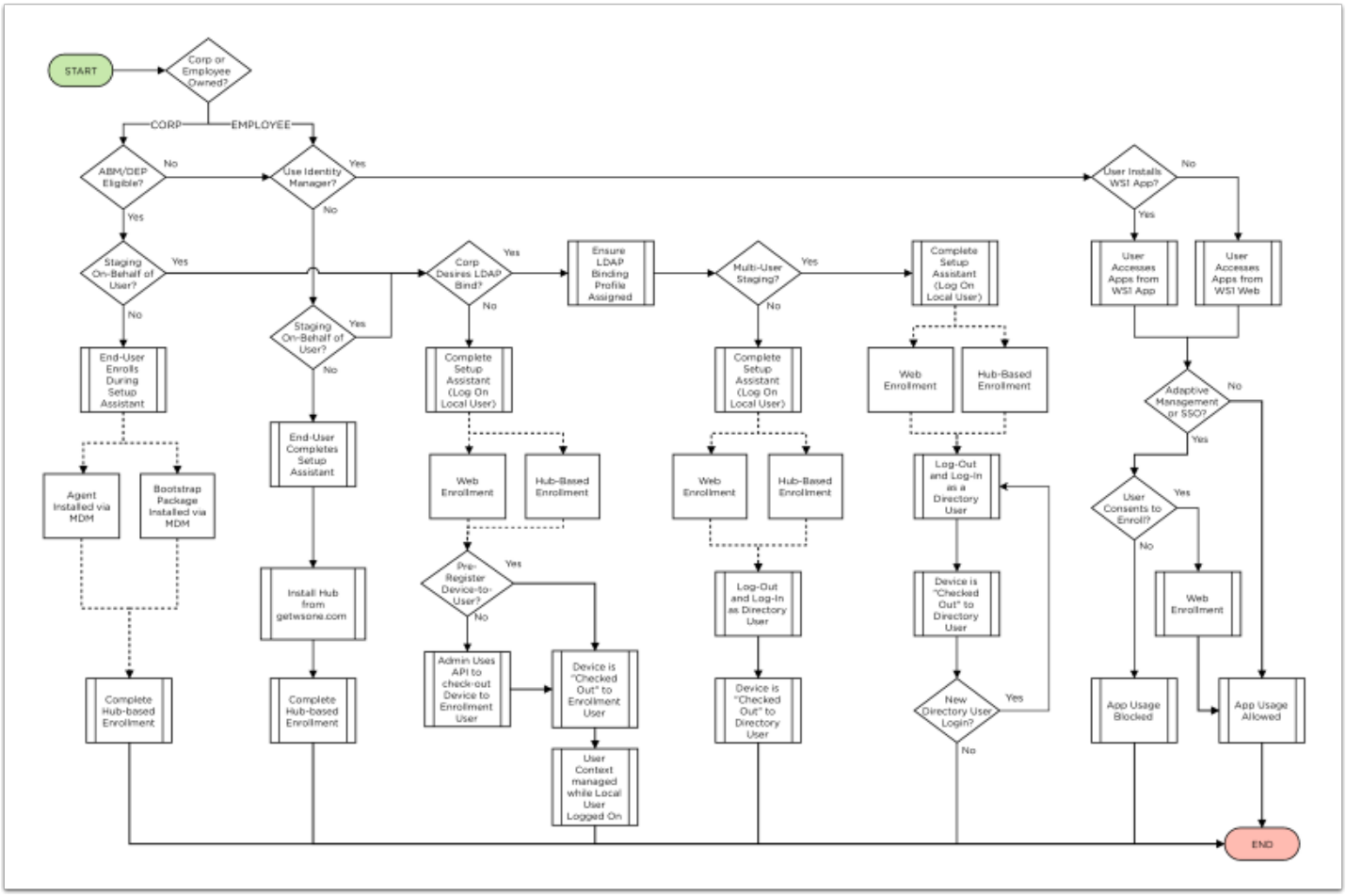
As such, when discussing enrollment workflows for macOS, we must first define three different types of users.

1. **Workspace ONE UEM Enrollment User**
    - If not staging a device, this is a user account (either basic or directory-based) within Workspace ONE UEM (under **Accounts > Users > List View**) whose credentials were entered at the time the device was enrolled.
    - If staging a device, this is the user account to which the device is assigned within Workspace ONE UEM (under **Devices > Details View > User)**
    - This is the user account Workspace ONE is using to determine membership within assignment groups.
    - In other words, this is the user account to which Workspace ONE UEM considers the device assigned.
2. **macOS Logged-On User**
    - This is a user account (either local to macOS or based from a directory service such as Active Directory) that is currently logged-on and active on the device.

3. **Workspace ONE Managed User**
    - This is the user account (either local to macOS or based from a Network Account Server) that was logged-on and active on the device when enrollment occurred.
    - This is the macOS user account Workspace ONE UEM can target using Apple Push Notifications when it is also the logged-on user.
    - In other words, this is the user account that must be logged-on within macOS in order for Workspace ONE to deliver items assigned to the Workspace ONE UEM enrollment user.

It is important to note the subtle differences between these three types of users as we begin discussing enrollment scenarios.

Reviewing Onboarding Options



As detailed in the screenshot, users can enroll a macOS device in numerous ways. The following operational tutorial provides guidance on the different settings an administrator should configure to enable these workflows.

Non-Staging, User-Initiated macOS Enrollment

Introduction

In a user-initiated enrollment (such as Bring Your Own Device), macOS device enrollment with a Workspace ONE UEM user's credentials (*enrollment user*) makes that currently logged in macOS user (*logged-in user*) the Workspace ONE *managed user*. In other words, the *managed user* is the macOS user account that enrolled with Workspace ONE credentials.

This means that any profiles and applications targeting the **user** *only apply when that specific macOS user is logged in*. If the managed user logs out from a non-staged device and another macOS user logs in, Workspace ONE *does not* apply any **user** items to that new logged-in user. User profiles are not delivered/applied to the non-staged device until the managed user account logs in again. The user enrolling the device in a user-initiated enrollment workflow must have administrative permissions on the device. Administrative permissions are required to install the device management profile.

A non-staged, user-initiated enrollment qualifies as a User-Approved MDM Enrollment flow for macOS High Sierra (and later) when performed through the Profiles preference pane or the VMware Workspace ONE Intelligent Hub for macOS.

Note: The reason for the one local user limitation can be found in Apple's MDM Protocol Documentation:

- The local user that installed the profile *will be managed.*
- *No other local users will be managed.* The server never receives requests from a local user other than the one that installed the enrollment profile.
- Network users logging into the device will be managed if the server responds successfully to their `UserAuthenticate` messages .

Prerequisites

Before you can perform the procedures in this tutorial, you must satisfy the following requirements.

- Apple device running macOS version 10.12.6 (Sierra) or later
- VMware Workspace ONE Intelligent Hub for macOS version 3.0 or later
- Workspace ONE UEM version 9.4 or later

For more information, see the VMware Identity Manager Documentation and VMware Workspace ONE UEM Documentation.

You must also meet the following prerequisites, before configuring *any* type of macOS enrollment workflow:

1. To manage an Apple device with Workspace ONE UEM, you must generate an APNS certificate for your Workspace ONE UEM environment.
2. Create a basic user account or directory user account to Workspace ONE UEM as enrollment ties a device to an enrollment user account.
    - To correlate the logged-on macOS user to a directory-based user account, you must integrate Workspace ONE UEM with your Directory Service.
3. To enable Device Enrollment integration, you must sign up for an Apple Business Manager (or Apple School Manager) account.
4. To enroll devices using Apple Business Manager or Apple School Manager, you must perform the following:
    - Download the Public Key to Integrate with Apple Business Manager
    - Configure the Apple Business Manager Portal
    - Associate devices in Apple Business Manager

Onboarding Using User-Initiated, Agent-Based Enrollment

The following video demonstrates a basic non-staged, user-initiated enrollment.

Note: The web-based enrollment flow is similar to agent-based, except that the user would initiate their enrollment by navigating to `https://deviceservices.url.com/enrollment` in a web browser, (where `deviceservices.url.com` is the fully qualified domain name for your Workspace ONE UEM device services endpoint).

If the basic prerequisites have been met, Workspace ONE UEM by default can accommodate a user-initiated, agent-based enrollment.

Onboarding Using User-Initiated, Apple Business Manager Enrollment

The following high-level process helps you to successfully configure non-staging, user-initated enrollments for devices enrolling with Apple Business Manager.

1. In your Device Enrollment Profile, set the following options:
    - Set *Authentication* setting to **ON**.
    - Set *Await Configuration* to **Enabled**.
    - Set *Account Setup* to **Don't Skip**.
    - Optionally, set *Create New Admin Account* to **YES** and pre-fill local administrator account details.
2. Assign the Device Enrollment Profile to the device you will be testing.
3. Unbox the macOS device and power it on.
4. Proceed through the macOS Setup Assistant creating a local macOS user.

Important: The macOS user created during the Setup Assistant is the Workspace ONE managed user. Any profiles and applications assigned to the user account (provided to enroll the device) are delivered when the user account created during the Setup Assistant is

logged in to the device.

Staging Single-User, Domain-Bound macOS Enrollment

Introduction

In a network-based user-staging scenario, Workspace ONE UEM receives a message from an LDAP-bound macOS device at a network user's login event. This notification allows Workspace ONE to correlate the newly *logged-in user* (a network user in macOS) to the *enrollment user*. Because the network account in macOS and Workspace ONE UEM are known to be the same (as they are both originating from the same source; LDAP), Workspace ONE UEM can change the *managed user* to be the *new* logged-on user. macOS also reports the APNS token for the Network User's mdmclient process to MDM, allowing Workspace ONE UEM to manage the user context in real time.

In single-user staging scenarios, Workspace ONE UEM associates the device to the enrollment user *only* for the *first* network user login (for example, the managed user). Subsequent network user login events are ignored, and the assigned user for the device is not modified. This means that any user-based assignments (user-level profiles and apps) are only sent to macOS when the managed user (matching the enrollment user) is logged in to the device.

Important: *This is a critical concept to understand, as it directly affects the resultant behavior on a macOS device under MDM management.* If a domain-bound macOS device is enrolled but not receiving *user* profiles/configurations, the logged-in user in macOS may not be the Workspace ONE UEM *managed user*.

Prerequisites

Before you can perform the procedures in this tutorial, you must satisfy the following requirements.

- Apple device running macOS version 10.12.6 (Sierra) or later
- VMware Workspace ONE Intelligent Hub for macOS version 3.0 or later
- Workspace ONE UEM version 9.4 or later

For more information, see the VMware Identity Manager Documentation and VMware Workspace ONE UEM Documentation.

You must also meet the following prerequisites, before configuring *any* type of macOS enrollment workflow:

1. To manage an Apple device with Workspace ONE UEM, you must generate an APNS certificate for your Workspace ONE UEM environment.
2. Create a basic user account or directory user account to Workspace ONE UEM as enrollment ties a device to an enrollment user account.
    - To correlate the logged-on macOS user to a directory-based user account, you must integrate Workspace ONE UEM with your Directory Service.
3. To enable Device Enrollment integration, you must sign up for an Apple Business Manager (or Apple School Manager) account.
4. To enroll devices using Apple Business Manager or Apple School Manager, you must perform the following:
    - Download the Public Key to Integrate with Apple Business Manager
    - Configure the Apple Business Manager Portal
    - Associate devices in Apple Business Manager

Single-User Staging Using Agent-Based Enrollment

The following high-level process helps you to successfully configure single-user staging for devices enrolling with Apple Business Manager:

1. Create a basic Workspace ONE UEM user account configured for Single-User Staging.
2. Configure a macOS Device Profile with the Directory Payload assigned to your devices that should be staged.
    - Note the *Client ID* field can be populated with a lookup value by clicking the **[+]** (plus sign). Ensure you choose a field that contains data allowable for a computer name (for example, conforms to NetBios Naming Restrictions for Microsoft Active Directory), such as `{DeviceSerialNumber}`.
3. Unbox the macOS device and power it on, then proceed through the Setup Assistant as normal.
4. Create a local, administrative macOS account as part of the Setup Assistant.
5. Log in to macOS as the local macOS account created during Setup Assistant.

6. Enroll with macOS Hub using the Staging User credentials you created in Step 1.
    - When the device enrolls, the profile containing the directory payload is installed. This binds macOS to your network-based directory service (such as Microsoft Active Directory).
    - Any other profiles and apps assigned to the device using assignment group is sent to the device.
7. Validate the device is domain bound:
    - Open **Terminal.app**.
    - Enter the command `id <intended user's AD username>` and ensure the command returns information about the user.
8. Log out of the local, administrative macOS account.
9. At the login window, let the intended end-user log in with their domain-based username and password.
10. Workspace ONE UEM assigns the device to the end user and begins sending profiles and apps which are assigned to the user.

Note: The web-based enrollment flow is relatively similar to agent-based, except that the admin would initiate their enrollment by navigating to `https://deviceservices.url.com/enrollment` in a web browser, (where `deviceservices.url.com` is the fully qualified domain name for your Workspace ONE UEM device services endpoint).

Single-User Staging Using Apple Business Manager Enrollment

The following high-level process helps you to successfully configure single-user staging for devices enrolling with Apple Business Manager:

1. Create a basic Workspace ONE UEM user account configured for Single-User Staging.
2. In your Device Enrollment Profile, set the following options:
    - Set *Authentication* setting to **ON**.
    - Set *Await Configuration* to **ENABLED**.
    - Set *Account Setup* to **SKIP** (as you are forcing the end-user to log in with network credentials).
    - Set *Create New Admin Account* to **YES** and configure Admin Account details.
3. Configure a macOS Device Profile with the Directory Payload assigned to your devices that should be staged.
    - Note the *Client ID* field can be populated with a lookup value by clicking the **[+]** (plus sign). Ensure you choose a field that contains data allowable for a computer name (for example, conforms to NetBios Naming Restrictions for Microsoft Active Directory), such as `{DeviceSerialNumber}`.
4. Unbox the macOS device and power it on, then proceed through the Setup Assistant and select to have the device managed by Workspace ONE UEM.
    - Authenticate to Workspace ONE UEM using the user account configured for Single-User Staging (from step 1).
    - When the device enrolls during the Setup Assistant, the profile containing the directory payload will be installed during the *AwaitConfiguration* phase. This binds macOS to your network-based directory service (such as Microsoft Active Directory).
    - Any other profiles and apps assigned to the device using assignment group are sent to the device.
5. At the login window, ensure network accounts are available.
6. Let the intended end-user log in with their domain-based username and password.
7. Workspace ONE UEM assigns the device to the end user and begins sending profiles and apps which are assigned to the user.

Note: As a reminder, at the point where the device is enrolled to the Single User Staging user, the logged-in user *is not yet* associated to the enrollment user. After the first network directory-based account logs in to the Mac, Workspace ONE UEM associates the logged-in user to a user account in Workspace ONE UEM. The new directory account becomes *both* the enrollment user and managed user.

Important: Although it is possible to set the Authentication setting set to **OFF** in your DEP profile, this is *not* recommended. This setting creates a potential security hole that would allow malicious actors to configure a virtual machine with a serial number of a device from your organization to obtain applications, certificates, and so on. For more information, see Best Practices using Apple Device Enrollment Program (DEP).

Staging Multi-User, Domain-Bound macOS Enrollment

Introduction

In a network-based user-staging scenario, Workspace ONE UEM receives a message from an LDAP-bound macOS device at a network user's login event. This notification allows Workspace ONE to correlate the newly *logged-in user* (a network user in macOS) to the *enrollment user*. Because the network account in macOS and Workspace ONE UEM are known to be the same (as they are both originating from the same source; LDAP), Workspace ONE UEM can change the *managed user* to be the *new* logged-in user. macOS also reports the APNS token for the network user's `mdmclient` process to MDM, allowing Workspace ONE UEM to manage the user context in real time.

In multi-user staging scenarios, Workspace ONE UEM associates the device to a new enrollment user each time a network-based user account logs in (for example, the managed user). With each network user login, Workspace ONE UEM modifies the enrollment user to match the newly logged-in user account. Workspace One UEM also associates the new user's APNS token so that the new user account is managed in real-time. As such, Workspace ONE UEM sends any apps and configurations assigned to the newly logged-in user.

Important: *This is a critical concept to understand, as it directly affects the resultant behavior on a macOS device under MDM management*. Multi-user staging is dependent on both the staging user configuration and the domain bind.

Prerequisites

Before you can perform the procedures in this tutorial, you must satisfy the following requirements.

- Apple device running macOS version 10.12.6 (Sierra) or later
- VMware Workspace ONE Intelligent Hub for macOS version 3.0 or later
- Workspace ONE UEM version 9.4 or later

For more information, see the VMware Identity Manager Documentation and VMware Workspace ONE UEM Documentation.

You must also meet the following prerequisites, before configuring *any* type of macOS enrollment workflow:

1. To manage an Apple device with Workspace ONE UEM, you must generate an APNS certificate for your Workspace ONE UEM environment.
2. Create a basic user account or directory user account to Workspace ONE UEM as enrollment ties a device to an enrollment user account.
    - To correlate the logged-on macOS user to a directory-based user account, you must integrate Workspace ONE UEM with your Directory Service.
3. To enable Device Enrollment integration, you must sign up for an Apple Business Manager (or Apple School Manager) account.
4. To enroll devices using Apple Business Manager or Apple School Manager, you must perform the following:
    - Download the Public Key to Integrate with Apple Business Manager
    - Configure the Apple Business Manager Portal
    - Associate devices in Apple Business Manager

Multi-User Staging Using Agent-Based Enrollment

The following high-level process helps you to successfully configure single-user staging for devices enrolling with Apple Business Manager:

1. Create a basic Workspace ONE UEM user account configured for Multi-User Staging.
2. Configure a macOS Device Profile with the Directory Payload assigned to your devices that should be staged.
    1. Note the *Client ID* field can be populated with a lookup value by clicking the **[+]** (plus sign). Ensure you choose a field that contains data allowable for a computer name (for example, conforms to NetBios Naming Restrictions for Microsoft Active Directory), such as `{DeviceSerialNumber}`.
3. Unbox the macOS device and power it on, then proceed through the Setup Assistant as normal.
4. Create a local, administrative macOS account as part of the Setup Assistant.
5. Log in to macOS as the local macOS account created during Setup Assistant.
6. Enroll with macOS Hub using the Staging User credentials you created in Step 1.
    1. When the device enrolls, the profile containing the directory payload is installed. This binds macOS to your network-based directory service (such as Microsoft Active Directory).
    2. Any other profiles and apps assigned to the device using assignment group are sent to the device.
7. Validate the device is domain bound:

    1. Open **Terminal.app**.
    2. Enter the command `id <intended user's AD username>` and ensure the command returns information about the user.
8. Log out of the local, administrative macOS account.
9. At the login window, let the intended end-user log in with their domain-based username and password.
10. Workspace ONE UEM assigns the device to the end user and begins sending profiles and apps which are assigned to the user.
11. Log out of the domain-based user, and log-in with another domain-based user.
12. Workspace ONE UEM assigns the device to the new end user and begins sending profiles and apps which are assigned to the new user (if different from the previous logged-in user).

Note: The web-based enrollment flow is relatively similar to agent-based, except that the admin would initiate their enrollment by navigating to `https://deviceservices.url.com/enrollment` in a web browser, (where `deviceservices.url.com` is the fully qualified domain name for your Workspace ONE UEM device services endpoint).

Multi-User Staging Using Apple Business Manager Enrollment

The following high-level process helps you to successfully configure multi-user staging for devices enrolling with Apple Business Manager:

1. Create a basic Workspace ONE UEM user account configured for Multi-User Staging.
2. In your Device Enrollment Profile, set the following options:
    1. Set *Authentication* setting to **ON**.
    2. Set *Await Configuration* to **ENABLED**.
    3. Set *Account Setup* to **SKIP** (as you are forcing the end-user to log in with network credentials).
    4. Set *Create New Admin Account* to **YES** and configure Admin Account details.
3. Configure a macOS Device Profile with the Directory Payload assigned to your devices that should be staged.
    1. Note the *Client ID* field can be populated with a lookup value by clicking the **[+]** (plus sign). Ensure you choose a field that contains data allowable for a computer name (for example, conforms to NetBios Naming Restrictions for Microsoft Active Directory), such as `{DeviceSerialNumber}`.
4. Unbox the macOS device and power it on, then proceed through the Setup Assistant as normal.
    1. Authenticate to Workspace ONE UEM using the user account configured for Multi-User Staging (from step 1).
    2. When the device enrolls during the Setup Assistant, the profile containing the directory payload is installed during the *AwaitConfiguration* phase. This binds macOS to your network-based directory service (such as Microsoft Active Directory).
    3. Any other profiles and apps assigned to the device using assignment group are sent to the device.
5. At the login window, let the intended end-user log in with their domain-based username and password.
6. Workspace ONE UEM assigns the device to the end user and begins sending profiles and apps which are assigned to the user.
7. Log out of the domain-based user, and log in with another domain-based user.
8. Workspace ONE UEM assigns the device to the new end user and begins sending profiles and apps which are assigned to the new user (if different from the previous logged-on user).

Note: As a reminder, at the point where the device is enrolled to the multi-user staging user, the device is currently *checked-out* to the multi-user staging user. After the first network directory-based account logs in to the Mac, Workspace ONE UEM associates the logged-in user to a user account in Workspace ONE UEM. This is reflected in the Workspace ONE UEM console whereby the device is assigned to the network-based user. The new directory account becomes *both* the enrollment user (in Workspace ONE UEM) and managed user (in macOS). A subsequent network logout and login event re-assigns the device to the new enrollment user (in Workspace ONE UEM) and begins management of the newly logged-in macOS user (the managed user).

Important: Although it is possible to set the Authentication setting set to **OFF** in your DEP profile, this is *not* recommended. This setting creates a potential security hole that would allow malicious actors to configure a virtual machine with a serial number from your organization to obtain applications, certificates, and so on. For more information, see Best Practices using Apple Device Enrollment Program (DEP).

Staging Single-User, Off-Domain macOS Enrollment

Introduction

Typical, domain-based macOS staging workflows leverage the device's network-based user login event to trigger device assignment to the LDAP-based user. This function is enabled because macOS sends the GUID for the user account to Workspace ONE UEM as part of the *UserAuthenticate* request.

When staging without domain binding, the *only* user account that can be managed by Workspace ONE UEM is the local user that installs the enrollment profile. Per Apple's MDM Protocol Reference, the server *will never* get requests from a local user other than the one that installed the enrollment profile. Any staging scenario without domain binding must ensure the local macOS user account that installs the enrollment profile *must* be the local macOS user account the end-user will be using.

Important: Although it is possible to set the Authentication setting set to **OFF** in your DEP profile, this is *not* recommended. This setting creates a potential security hole that would allow malicious actors to configure a virtual machine with a serial number of a device from your organization to obtain applications, certificates, and so on. For more information, see Best Practices using Apple Device Enrollment Program (DEP).

Prerequisites

Before you can perform the procedures in this tutorial, you must satisfy the following requirements.

- Apple device running macOS version 10.12.6 (Sierra) or later
- VMware Workspace ONE Intelligent Hub for macOS version 3.0 or later
- Workspace ONE UEM version 9.4 or later

For more information, see the VMware Identity Manager Documentation and VMware Workspace ONE UEM Documentation.

You must also meet the following prerequisites, before configuring *any* type of macOS enrollment workflow:

1. To manage an Apple device with Workspace ONE UEM, you must generate an APNS certificate for your Workspace ONE UEM environment.
2. Create a basic user account or directory user account to Workspace ONE UEM as enrollment ties a device to an enrollment user account.
    - To correlate the logged-on macOS user to a directory-based user account, you must integrate Workspace ONE UEM with your Directory Service.
3. To enable Device Enrollment integration, you must sign up for an Apple Business Manager (or Apple School Manager) account.
4. To enroll devices using Apple Business Manager or Apple School Manager, you must perform the following:
    - Download the Public Key to Integrate with Apple Business Manager
    - Configure the Apple Business Manager Portal
    - Associate devices in Apple Business Manager

Single-User Staging for Local Users with Pre-Registration Using Agent-Based Enrollment

This section helps you to configure single-user staging for local users with pre-registration using agent-based enrollment.

1. Agent/Web Single-User Staging for Local Users with Pre-Registration

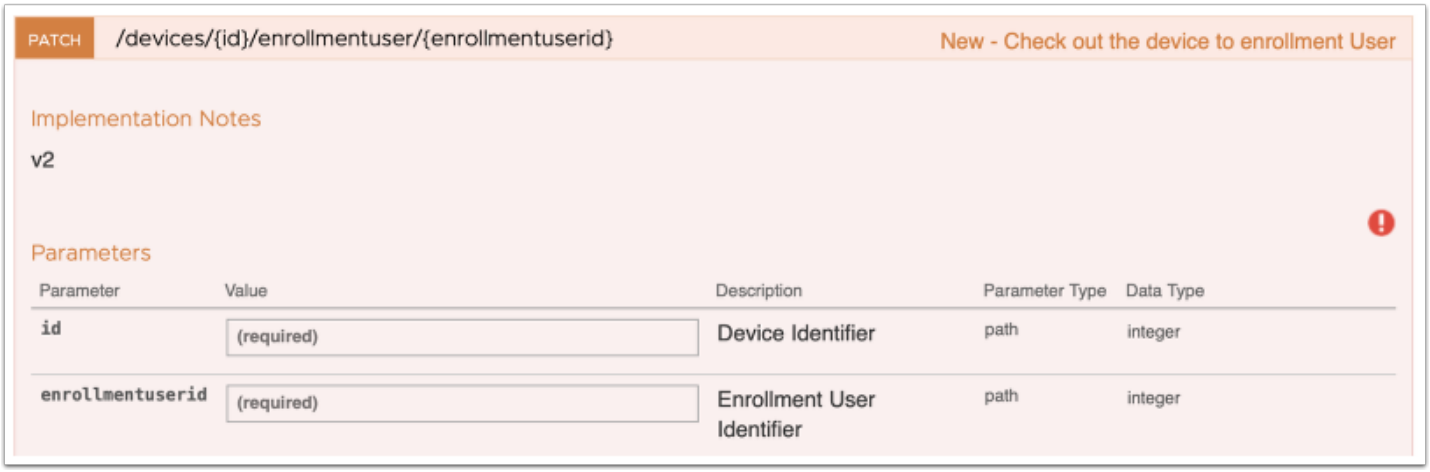
1. Create a basic Workspace ONE UEM user account configured for Single-User Staging.
2. Bulk Import the Device-to-User registration record within the **Devices** > **Lifecycle** > **Enrollment Status** page:
    - Click **Add** > **Batch Import** and use the *Simple template and example for users and/or devices* listed on the Batch Import page.
    - Modify the sample CSV (starting in row 2 of the CSV template) by entering only the **Username**, **FirstName**, **LastName**, **GroupID**, **Security Type** (Directory or Basic), and **DeviceSerial**.
3. Unbox the Mac and power it on. Proceed through the Setup Assistant as normal.
    - Create a local, administrative macOS account as part of the Setup Assistant.

- **ENSURE** the local macOS account created is the username you want to give the end-user of the machine.

4. Log in to macOS as the local macOS account created during Setup Assistant.
5. Enroll with macOS Hub using the Staging User credentials you created in step 1 of this section.
   - When the device enrolls, Workspace ONE UEM assigns the device from the staging user to the user you specified in step 2 using bulk import.
   - Any profiles and apps assigned to the enrollment user specified by bulk import are sent to the device when the local macOS user account you used in step 5 is logged-in.

Note: The web-based enrollment flow is similar to agent-based, except that the admin would initiate their enrollment by navigating to `https://deviceservices.url.com/enrollment` in a web browser (where `deviceservices.url.com` is the fully qualified domain name for your Workspace ONE UEM device services endpoint).

2. Agent/Web Single-User Staging for Local Users with API Check-Out



Note: The process to check-out a device to an enrollment user can be used when the device-to-user assignments are not known ahead of time (for example, devices stored in a depot and subsequently assigned out to users). Generally speaking, this is an advanced use case where the code mentioned in step 5 is included in a larger onboarding workflow and/or native application.

1. Create a basic Workspace ONE UEM user account configured for Single-User Staging.
2. Unbox the Mac and power it on. Proceed through the Setup Assistant as normal.
   - Create a local, administrative macOS account as part of the Setup Assistant.
   - **ENSURE** the local macOS account created is the username you want to give the end-user of the machine.
3. Log in to macOS as the local macOS account created during Setup Assistant.
4. Enroll with macOS Hub using the Staging User credentials you created in step 1 of this section.
5. While logged in as the user that enrolled in step 4, call the Workspace ONE UEM Rest API to check-out the device to the correct enrollment user.

REST API Details: `https://<API_Server>/api/help/#!/DevicesV2/DevicesV2_CheckOutDeviceToUser`

```
PATCH /api/mdm/devices/{id}/enrollmentuser/{enrollmentuserid}
* {id} - AirWatch Device ID
* {enrollmentuserid} - AirWatch User ID
* Accept - application/json:version=2
```

- The API call is typically embedded in a workflow control application or script.
- Every time the end-user logs in with the username created during the Setup Assistant, Workspace ONE UEM considers that local macOS user the managed user and sends apps/profiles targeted to the enrollment user.

Note: The web-based enrollment flow is similar to agent-based, except that the admin would initiate their enrollment by navigating to

`https://deviceservices.url.com/enrollment` in a web browser (where `deviceservices.url.com` is the fully qualified domain name for your Workspace ONE UEM device services endpoint).

Single-User Staging for Local Users with Pre-Registration Using Apple Business Manager Enrollment

This section helps you to configure single-user staging for local users with pre-registration using Apple Business Manager enrollment.

1. Apple Business Manager Single-User Staging for Local Users with Pre-Registration

1. Create a basic Workspace ONE UEM user account configured for Single-User Staging.
2. In your Device Enrollment Profile, set the following options:
    - Set *Authentication* setting to **OFF**.
    - Set *Staging Mode* to **Single User Device**.
    - Set the *Default Staging User* as the basic user configured for Single-User Staging.
    - Set *Await Configuration* to **ENABLED**.
    - Set *Account Setup* to **DON'T SKIP**.
    - Optionally, set *Create New Admin Account* to **YES** and configure Admin Account details for a hidden IT administrator account.
3. Validate the device record has synced from Apple Business Manager or Apple School Manager:
    - Navigate to **Devices > Lifecycle > Enrollment Status** in the Workspace ONE UEM console and change the layout to **Custom**.
    - Ensure the device to be staged has synced from Apple Business Manager by scrolling to the right.
    - Check the *Token Type* is **Apple Enrollment**.
    - If the device has no *Token Type*, navigate to **Devices** > **Devices Settings** > **Apple** > **Device Enrollment Program** and click **Sync Devices**.
4. Validate the device record has the correct Device Enrollment profile:
    - Navigate to **Devices** > **Lifecycle** > **Enrollment Status** in the Workspace ONE UEM console and change the layout to **Custom**.
    - Ensure the *Profile Name* matches the profile you created in step 2.
    - If the Profile Name is incorrect, select the check box next to the device(s) to be enrolled and navigate to **More Actions** > **Assign Profile** > Choose the profile you created in step 2 > **Save**.
5. Bulk Import the Device-to-User registration record within the **Devices** > **Lifecycle** > **Enrollment Status**:
    - Click **Add** > **Batch Import** and use the *Simple template and example for users and/or devices* listed on the Batch Import page.
    - Modify the sample CSV (starting in row 2 of the CSV template) by entering only the **Username**, **FirstName**, **LastName**, **GroupID**, **Security Type** (Directory or Basic), and **DeviceSerial**.
    - After the Import completes, reload the Enrollment Status page.
    - Ensure the device to be staged has a *User name* assigned and still has a *Token Type* of **Apple Enrollment**.
6. Unbox the macOS device and power it on. Proceed through the Setup Assistant and select to have the device managed by Workspace ONE UEM:
    - When the device enrolls, Workspace ONE UEM assigns the device from the staging user to the user you specified in step 5 using bulk import (the enrollment user).
    - When the end-user logs in with the username created during the Setup Assistant, Workspace ONE UEM considers that local macOS user the managed user and sends apps/profiles targeted to the enrollment user.

2. Apple Business Manager Single-User Staging for Local Users with API Check-Out

1. Create a basic Workspace ONE UEM user account configured for Single-User Staging.
2. In your Device Enrollment Profile, set the following options:
    - Set *Authentication* setting to **OFF**.

- Set *Staging Mode* to **Single User Device**.
- Set the *Default Staging User* as the basic user configured for single-user staging.
- Set *Await Configuration* to **ENABLED**.
- Set *Account Setup* to **DON'T SKIP**.
- Optionally, set *Create New Admin Account* to **YES** and configure Admin Account details for a hidden IT administrator account.

3. Validate that the device record has synced from Apple Business Manager or Apple School Manager:
   - Navigate to **Devices** > **Lifecycle** > **Enrollment Status** in the Workspace ONE UEM console and change the layout to **Custom**.
   - Ensure that the device to be staged has synced from Apple Business Manager by scrolling to the right.
   - Confirm that the *Token Type* is **Apple Enrollment**.
   - If the device has no *Token Type*, navigate to **Devices** > **Devices Settings** > **Apple** > **Device Enrollment Program** and click **Sync Devices**.
4. Validate that the device record has the correct Device Enrollment profile:
   - Navigate to **Devices** > **Lifecycle** > **Enrollment Status** in the Workspace ONE UEM console and change the layout to **Custom**.
   - Ensure that the device to be staged has a *Token Type* of **Apple Enrollment**.
   - Ensure that the *Profile Name* matches the profile you created in step 2.
   - If the Profile Name is incorrect, select the check box next to the device(s) to be enrolled and navigate to **More Actions** > **Assign Profile** > Choose the profile you created in step 2 > **Save**.
5. Unbox the macOS device and power it on. Proceed through the Setup Assistant and select to have the device managed by Workspace ONE UEM:
   - When the device enrolls, Workspace ONE UEM assigns the device to the staging user you created in step 1.
   - When the end-user logs in with the username they create during the Setup Assistant, Workspace ONE UEM does not send any applications/profiles targeted to users as the device is still assigned to the staging account.
6. While logged in as the user that enrolled in step 5, call the Workspace ONE UEM Rest API to check-out the device to the correct enrollment user.

   REST API Details: https://<API_Server>/api/help/#!/DevicesV2/DevicesV2_CheckOutDeviceToUser

```
PATCH /api/mdm/devices/{id}/enrollmentuser/{enrollmentuserid}
* {id} - AirWatch Device ID
* {enrollmentuserid} - AirWatch User ID
* Accept - application/json:version=2
```

- The API call is typically embedded in a workflow control application or script.
- Every time the end-user logs in with the username created during the Setup Assistant, Workspace ONE UEM considers that local macOS user the managed user and sends apps/profiles targeted to the enrollment user.

Note: The process to check-out a device to an enrollment user can be used when the device-to-user assignments are not known ahead of time (for example, devices stored in a depot and subsequently assigned out to users). Generally speaking, this is an advanced use case where the previous code is included in a larger onboarding workflow and/or native application.

Summary and Additional Resources

Conclusion

This operational tutorial provided steps to enroll a macOS device using a number of enrollment workflows. These workflows included user-initiated enrollments, single-user and multi-user staging for network users, and single-user staging without domain binding.

Terminology Used in This Tutorial

The following terms are used in this tutorial:

application store	A user interface (UI) framework that provides access to a self-service catalog, public examples of which include the Apple App Store, the Google Play Store, and the Microsoft Store.
auto-enrollment	Auto-enrollment simplifies the enrollment process by automatically enrolling registered devices following the Out-of-Box-Experience.
catalog	A user interface (UI) that displays a personalized set of virtual desktops and applications to users and administrators. These resources are available to be launched upon selection.
cloud	Asset of securely accessed, network-based services and applications. A cloud can also host data storage. Clouds can be private or public, as well as hybrid, which is both private and public.
device enrollment	The process of installing the mobile device management agent on an authorized device. This allows access to VMware products with application stores, such as VMware Identity Manager.
identity provider (IdP)	A mechanism used in a single-sign-on (SSO) framework to automatically give a user access to a resource based on their authentication to a different resource.
mobile device management (MDM) agent	Software installed on an authorized device to monitor, manage, and secure end-user access to enterprise resources.
one-touch login	A mechanism that provides single sign-on (SSO) from an authorized device to enterprise resources.
service provider (SP)	A host that offers resources, tools, and applications to users and devices.
virtual desktop	The user interface of a virtual machine that is made available to an end user.
virtual machine	A software-based computer, running an operating system or application environment, that is located in the data center and backed by the resources of a physical computer.

For more information, see the VMware Glossary.

Additional Resources

For more information about Workspace ONE, you can explore the following resources:

- VMware Workspace ONE Action Path
- VMware Workspace ONE product page
- VMware Workspace ONE Documentation
- VMware Identity Manager product page
- VMware Identity Manager Documentation
- VMware Workspace ONE UEM, powered by VMware AirWatch product page
- VMware AirWatch Documentation
- VMware Workspace ONE free trial
- VMware Workspace ONE Cloud-Based Reference Architecture
- VMware Workspace ONE and VMware Horizon 7 Enterprise Edition On-premises Reference Architecture
- VMware End-User-Computing Blogs
- Workspace ONE UEM Hands-On Lab

About the Author

This tutorial was written by:

- Robert Terakedis, Senior Technical Marketing Manager, End-User-Computing Technical Marketing, VMware

Feedback

The purpose of this tutorial is to assist you. Your feedback is valuable. To comment on this tutorial, contact VMware End-User-Computing Technical Marketing at euc_tech_content_feedback@vmware.com.

VMware, Inc. 3401 Hillview Avenue Palo Alto CA 94304 USA Tel 877-486-9273 Fax 650-427-5001 www.vmware.com