Table of Contents

Overview

- Introduction
- Audience

Enrolling macOS Devices

- Introduction
- Prerequisites
- Logging In to the Workspace ONE UEM Console
- Installing the Workspace ONE Intelligent Hub
- Onboarding using User-Initiated Agent-Based Workflow

Configuring macOS Profiles

- Introduction
- Prerequisites
- Configuring a Restrictions Profile for macOS Devices
- Configuring a Dock Profile for macOS Users

Configuring Device Lock for macOS

- Introduction
- Prerequisites
- Configuring Device Lock

Understanding macOS Software Delivery

- Introduction
– **Prerequisites**

– **Deploying macOS Volume-Purchased Apps**

**Summary and Additional Resources**

– **Conclusion**

– **Terminology Used in This Tutorial**

– **Additional Resources**

– **About the Author**

– **Feedback**
OT-WS1-macOS-mgmt

Overview

Introduction
VMware provides this operational tutorial to help you with your VMware Workspace ONE® environment. In this tutorial, you enroll a macOS device, configure a restrictions profile and a dock profile, configure a device lock, and deploy macOS volume-purchased apps.

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 Workspace ONE® Access (formerly VMware Identity Manager) and VMware Workspace ONE® UEM is also helpful.

Enrolling macOS Devices

Introduction
This section covers basic macOS administration using Workspace ONE UEM. This exercise helps you to install the Workspace ONE Intelligent Hub and enroll a macOS device into Workspace ONE UEM.

Prerequisites
Before you can perform the exercises in this tutorial, you must meet the following requirements.

- Workspace ONE UEM version 9.4 or later
- Apple device running macOS version 10.12.6 (Sierra) or later
- Retrieving the Group ID from Workspace ONE UEM Console
- Local macOS account with administrator permissions

This exercise requires admin and end user device authentication during enrollment. Gather the required account information, and record it in the following table. The account information provided in the table is based on a test environment. Your account details will differ.

<table>
<thead>
<tr>
<th>Local Administrator Account Information</th>
</tr>
</thead>
<tbody>
<tr>
<td>User name</td>
</tr>
<tr>
<td>Password</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>User Account Information</th>
</tr>
</thead>
<tbody>
<tr>
<td>User name</td>
</tr>
<tr>
<td>Password</td>
</tr>
<tr>
<td>Email</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Workspace ONE UEM Information</th>
</tr>
</thead>
<tbody>
<tr>
<td>Server URL</td>
</tr>
</tbody>
</table>
Logging In to the Workspace ONE UEM Console
To perform most of the steps in this exercise, you must first log in to the Workspace ONE UEM Console.

1. Launch Chrome Browser

On your desktop, double-click the Google Chrome icon.

2. Navigate to the VMware Workspace ONE UEM Console

For example, navigate to https://<WorkspaceONEUEMHostname> where WorkspaceONEUEMHostname is the host name of the Workspace ONE UEM console.

3. Authenticate In to the Workspace ONE UEM Console
Enter your Username, for example, administrator.

1. Enter your **Username**, for example, administrator.
2. Click **Next**. After you click Next, the Password text box is displayed.
1. Enter your Password, for example, VMware1!
2. Click Login.

**Note:** If you see a Captcha, be aware that it is case sensitive.

**Installing the Workspace ONE Intelligent Hub**

In this exercise, download and install the Workspace ONE Intelligent Hub on your macOS device.

1. Log In to the MacBook - If Needed
Log in to the macOS device with your administrator credentials.

1. Enter the username. For example, administrator.
2. Enter the password. For example, VMware1!.
3. Click the arrow icon or press ENTER.

2. Open the Browser

Click the Safari icon (blue compass) to open the Safari browser.

3. Download the Agent

Workspace ONE Intelligent Hub is the app you use to register your device for access to resources within your organization.

1. Enter https://getwsone.com in the URL field, then press ENTER.
2. Click Download Hub for macOS. The Workspace ONE Intelligent Hub begins to download and will save to the Downloads folder by default.
4. Launch the Installer

1. Click the Downloads folder in the dock (next to the Trash Bin).
2. Click the VMwareWorkspaceONEIntelligentHub.pkg file to begin the installer.

5. Review the Introduction

Click Continue.

6. Review and Accept Licensing Terms
1. In the Installer, click Continue.
2. Click Agree (to the license terms).

7. Select Destination for the Installer
Click Continue.

8. Define Install Location and Provide Administrator Credentials
Click **Install** to perform a standard installation.

1. Enter the admin user name, for example, **Administrator**.
2. Enter the password.
3. Click **Install Software**.

9. **Complete Installation**
1. Click **Close** when the installer finishes.
2. Click **Move to Trash** to move the installer to the trash.

**Onboarding using User-Initiated Agent-Based Workflow**

In this exercise, you enroll a macOS device into Workspace ONE UEM. Enrollment is the action that brings a device under management and control by Workspace ONE UEM. There are a number of ways to enroll the various platforms (macOS included), but for this exercise, we cover a basic enrollment scenario.

This enrollment flow is considered **User-Approved** per the functionality introduced in macOS High Sierra.

1. **Initiate Enrollment**
After the Workspace ONE Intelligent Hub finishes installing, the Enrollment Wizard should start automatically. From within the Enrollment wizard window, click **Server Detail**.

**Note:** The Enrollment Wizard may take several minutes to launch. If you do not see the Enrollment Wizard immediately, be patient and wait for it to appear.

### 2. Enter Enrollment Server Details
Enter your Workspace ONE UEM URL, for example, hol.awmdm.com.

1. Enter your Group ID. See Retrieving the Group ID from Workspace ONE UEM Console.
2. Click Continue.

3. Enter Enrollment Credentials
Enter the enrollment username. For example, testuser.
2. Enter the enrollment user password. For example, VMware1!
3. Click Continue.

4. Enable Device Management
Click Enable to enable device management.

5. Install Workspace Services

Click Install.

6. Install the User-Approved Enrollment Profile
Click Install.

7. Enter Credentials

1. When prompted, enter the password for your user account on the Mac. For example, VMware1!
2. Click OK.
8. Quit the Profiles Panel

Click the red dot to close the Profiles panel.

9. Quit the Enrollment Wizard
10. Validate Enrollment

To verify that your MacBook enrolled successfully:

1. In the upper-right corner of your screen, click the Hub icon.
2. In the menu that appears, note your device’s Enrolled status.
3. Click Preferences and review the available options.

Configuring macOS Profiles

Introduction
Profiles are the mechanism by which Workspace ONE UEM manages settings on a macOS device. All profiles are broken down into two basic sections; the General section and the Payload section.

- The General section defines the profile’s name and assignment settings.
- The Payload sections define actions to be taken on the device.
Every profile must have all *required* fields in the General section properly filled out and at least one payload configured.

With Workspace ONE UEM, profile management for macOS can occur on the device level or on the user level.

Device-level profiles apply restrictions and settings to any user logged-on to the device. Device profiles are typically used to control settings that apply system-wide such as VPN and Wi-Fi configurations, Global HTTP Proxy, Disk Encryption, and/or Directory (LDAP) integration.

In contrast, user-level profiles apply settings and restrictions to the specific user logged-on to the device. User profiles typically control settings that apply to the enrolled user such as email configurations, web clips (URL shortcuts), credentials (certificates), and content filtering settings.

**Prerequisites**

Before you can perform the exercises in this tutorial, you must meet the following requirements.

- Workspace ONE UEM version 9.4 or later
- Apple device running macOS version 10.12.6 (Sierra) or later

**Configuring a Restrictions Profile for macOS Devices**

In this exercise, disable Bluetooth and Energy Saver settings on a macOS device by configuring a device-level Restrictions profile. This exercise explores how to modify the macOS device behavior using Profiles.

1. **Close System Preferences if opened**

   ![System Preferences](image)

   This section helps you to create a device profile which will change some system preferences in your Mac. However, to see those changes take place, you must first close any existing System Preference sessions if they are already open.

   If System Preferences are opened, click X to close.

2. **Navigate to Profile Settings**

   ![Workspace ONE UEM Console](image)

   In the Workspace ONE UEM console:
   1. Select Devices.
   2. Select Profiles & Resources.
   3. Select Profiles.
   4. Select Add.
5. Select Add Profile.

3. Select Profile Platform

Add Profile

Select a platform to start:

- Android
- iOS
- macOS

Select macOS.

4. Select the Profile Context

Select Context

- User Profile
- Device Profile

Select Device Profile.

5. Configure General Settings
Configure the device profile as follows:

1. Select **General** if it is not already selected.
2. Enter **macOS Device Restrictions** for the profile name.
3. Select **Auto** for the Assignment Type.
4. Scroll down to view **Assigned Groups**, and click in the search box. From the list of Assignment Groups that appear, select the appropriate group. For example, select **All Devices (your@email.shown.here)**.

**Note:** You do not need to click Save or Save & Publish at this point. This interface allows you to move around to different payload configuration screens before saving.

**6. Select the Restrictions Payload**
7. Configure the Restrictions Payload

Note: When initially setting most payloads, a Configure button will show to reduce the risk of accidentally setting a payload configuration.
Select **Restrict System Preference Panes**.

1. Select **Disable Selected Items**.
2. Select **Bluetooth**.
3. Select **Energy Saver**.

8. Save and Publish
Click Save and Publish.

9. Publish the Device Profile

View Device Assignment

<table>
<thead>
<tr>
<th>Assignment Status</th>
<th>Friendly Name</th>
<th>User</th>
<th>Platform/OS/Model</th>
<th>Phone Number</th>
<th>Organization Group</th>
</tr>
</thead>
<tbody>
<tr>
<td>Added</td>
<td>testuser MacBook Pro</td>
<td>testuser</td>
<td>macOS / macOS</td>
<td><a href="mailto:your@email.shown.h">your@email.shown.h</a>...</td>
<td></td>
</tr>
</tbody>
</table>

Items 1-1 of 1
Click Publish.

10. Verify the Device Profile Exists

You should now see your macOS Device Restrictions Device Profile within the list of the Profiles window.

Note: If you need to edit the profile, this is where you would do so.

11. Validate Profiles

1. Click the Apple icon in the upper-left corner.
2. Click System Preferences.
3. If System Preferences shows you a specific subpanel, such as Time Machine, click the back button.
4. Note you cannot modify the settings for Bluetooth and Energy Saver as those icons are grayed-out.

Configuring a Dock Profile for macOS Users

In this exercise, change the dock settings for a specific, enrolled user on a macOS device by configuring a user-level profile.
1. Navigate to Profile Settings

1. Select Add.
2. Select Add Profile.

2. Select Profile Platform

Add Profile

Select a platform to start:

- Android
- iOS
- macOS

Select macOS.

3. Select the Profile Context
Select Context

Select User Profile.

4. Configure General Settings

**macOS** macOS User Dock

1. Select General.
2. Enter macOS User Dock in the Name text box.
3. Ensure the Assignment Type is set to Auto.
4. Click in the Assigned Groups field. From the list of Assignment Groups that appear, select the appropriate group. For example, select All Devices (your@email.shown.here).

**Note:** You do not need to click Save or Save & Publish at this point. This interface allows you to move around to different payload
5. Select the Dock Payload

1. Select Dock.
2. Click Configure.

6. Configure the Dock Payload
1. Change the Dock Size to be smaller.
2. Change the Dock Position to Left.

7. Save & Publish

Click Save & Publish.

8. Publish the User Profile
9. Verify the User Profile

You should now see your macOS User Dock user profile in the Profiles window.

Note: If you need to edit the profile, this is where you would do so.

10. Validate Profile
Validation that the Dock has changed size and moved to the left side of the screen.

Configuring Device Lock for macOS

Introduction
Device lock for macOS devices causes the machine to reboot into a firmware-lock screen. This lock screen occurs at the firmware level prior to OS boot. This exercise helps you to configure a macOS device lock.

Prerequisites
Before you can perform the exercises in this tutorial, you must meet the following requirements.

- Workspace ONE UEM version 9.4 or later
- Apple device running macOS version 10.12.6 (Sierra) or later

Configuring Device Lock
Workspace ONE UEM supports a firmware-based device lock for macOS. The device cannot be booted until the device lock code has been entered. This exercise helps you to configure device lock for macOS.

1. Open macOS Device Details
Select Devices.

1. Select List View.

2. Select macOS Device

Select your enrolled macOS device.

Note: In this exercise we are using MacBooks—ensure that you are selecting your enrolled macOS device.

3. Lock Device
Click Lock in the upper-right corner of your device details view.

4. Enter Device Lock Code

Lock Device

You are about to perform the Lock Device action. Please enter a 6-digit unlock PIN below.

Set Unlock PIN: 1 1 1 1 1 1

Warning: This device cannot be unlocked remotely and can only be unlocked using 6-digit PIN entered above. Write this PIN down and store it in a safe place. If you forget your PIN you must contact Apple to unlock your device.

1. Enter 111111 as the firmware lock code.
2. Click Lock Device.

5. Device Reboot

The device reboots after a short delay and the firmware will be locked.

6. Unlock The Device
At the System Lock screen, enter the unlock code 111111.

1. Click the Arrow (--->) to boot the device.

Understanding macOS Software Delivery

Introduction
Workspace ONE UEM supports a few different methods for delivering software to managed macOS devices. This section helps you to volume-purchase app licenses in Apple Business Manager, then assign them to enrolled devices in Workspace ONE UEM.

The following software delivery methods are available for macOS:

- **Apple Business Manager or Apple School Manager** — Delivers macOS App Store applications to devices as volume-licensed, purchased applications.
- **Software Distribution** — Delivers third-party, non-store applications as *internal apps* in Workspace ONE UEM 9.3 and later.
- **Product Provisioning** — Deploys non-store applications and scripts as *products* in AirWatch 9.2 and earlier.

The type of software being delivered determines appropriate delivery method. The following table lists different types of software, and their recommended delivery method.

<table>
<thead>
<tr>
<th>Delivery Method</th>
<th>Store Apps</th>
<th>Non-Store Apps</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Apple Business Manager</td>
<td>Software Distribution</td>
</tr>
<tr>
<td>Examples</td>
<td>- xCode</td>
<td>- Adobe Creative Suite</td>
</tr>
<tr>
<td></td>
<td>- Slack</td>
<td>- Microsoft Office 2016 for macOS</td>
</tr>
<tr>
<td></td>
<td>- Microsoft Remote Desktop</td>
<td>- BlueJeans</td>
</tr>
<tr>
<td></td>
<td>- Apple's iWork suite</td>
<td>- Camtasia</td>
</tr>
<tr>
<td></td>
<td>- TextWrangler</td>
<td>- Audacity</td>
</tr>
<tr>
<td></td>
<td>- F5 Access (VPN)</td>
<td>- Shell scripts, Python scripts</td>
</tr>
<tr>
<td></td>
<td>- iBooks Author</td>
<td></td>
</tr>
<tr>
<td></td>
<td>- Microsoft OneDrive</td>
<td></td>
</tr>
<tr>
<td></td>
<td>- Microsoft OneNote</td>
<td></td>
</tr>
<tr>
<td></td>
<td>- Quickbooks</td>
<td></td>
</tr>
<tr>
<td></td>
<td>- VMware Tunnel</td>
<td></td>
</tr>
</tbody>
</table>
Prerequisites
Before you can perform the exercises in this tutorial, you must meet the following requirements.

- Workspace ONE UEM version 9.4 or later
- Apple device running macOS version 10.12.6 (Sierra) or later

Deploying macOS Volume-Purchased Apps
In this section, watch a video that shows how to purchase app licenses in Apple Business Manager, then assign them to enrolled devices in Workspace ONE UEM.

This section shows how to volume-purchase applications through the app store and assign to devices using device-based licensing. However, Workspace ONE UEM also supports non-store, third-party software management. For details, see Deploying Third-Party macOS Applications: VMware Workspace ONE Operational Tutorial on VMware Tech Zone.

Summary and Additional Resources

Conclusion
This operational tutorial provided basic administration steps to manage macOS with Workspace ONE UEM. Procedures included enrolling a macOS device, configuring a restrictions profile and a dock profile, configuring a device lock, and deploying macOS volume-purchased apps.

Terminology Used in This Tutorial
The following terms are used in this tutorial:

<table>
<thead>
<tr>
<th>Term</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>application store</td>
<td>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.</td>
</tr>
<tr>
<td>auto-enrollment</td>
<td>Auto-enrollment simplifies the enrollment process by automatically enrolling registered devices following the Out-of-Box-Experience.</td>
</tr>
<tr>
<td>catalog</td>
<td>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.</td>
</tr>
<tr>
<td>cloud</td>
<td>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.</td>
</tr>
<tr>
<td>device enrollment</td>
<td>The process of installing the mobile device management agent on an authorized device. This allows access to VMware products with application stores, such as Workspace ONE Access (formerly VMware Identity Manager).</td>
</tr>
<tr>
<td>identity provider (IdP)</td>
<td>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.</td>
</tr>
<tr>
<td>mobile device management (MDM) agent</td>
<td>Software installed on an authorized device to monitor, manage, and secure end-user access to enterprise resources.</td>
</tr>
<tr>
<td>one-touch login</td>
<td>A mechanism that provides single sign-on (SSO) from an authorized device to enterprise resources.</td>
</tr>
<tr>
<td>service provider (SP)</td>
<td>A host that offers resources, tools, and applications to users and devices.</td>
</tr>
<tr>
<td>virtual desktop</td>
<td>The user interface of a virtual machine that is made available to an end user.</td>
</tr>
<tr>
<td>virtual machine</td>
<td>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.</td>
</tr>
</tbody>
</table>
For more information, see the VMware Glossary.

Additional Resources
For more information about Workspace ONE, explore the VMware Workspace ONE Activity Path. The activity path provides step-by-step guidance to help you level-up in your Workspace ONE knowledge. You will find everything from beginner to advanced curated assets in the form of articles, videos, and labs.

Additionally, you can check out the VMware Workspace ONE and VMware Horizon Reference Architecture which provides a framework and guidance for architecting an integrated digital workspace using VMware Workspace ONE and VMware Horizon.

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.