VMware AirWatch macOS Platform Guide

Deploying and Managing macOS Devices

Workspace ONE UEM v9.6

Have documentation feedback? Submit a Documentation Feedback support ticket using the Support Wizard on support.air-watch.com.

Table of Contents

Chapter 1:
Introduction to Workspace ONE UEM for macOS

Overview

Workspace ONE UEM provides complete management solutions for macOS devices. Workspace ONE UEM's Mobile Device Management (MDM) solution enables enterprises to manage Corporate-Dedicated, Corporate-Shared or Employee Owned (BYOD) macOS devices throughout the entire device lifecycle.

Workspace ONE UEM supports macOS versions 10.9 and higher, and all devices running those operating system versions.

This guide shows administrators how to enroll devices or allow end users to enroll themselves, create profiles to manage compliance, configure the AirWatch Agent, manage applications, manage devices through the Workspace ONE UEM console and on the Self-Service Portal, integrate with macOS tools like File Vault 2, and enable Product Provisioning.

Workspace ONE UEM macOS Management Prerequisites

Before reading this guide, Workspace ONE UEM recommends having the following materials ready:

- **Active Environment** – This is your active Workspace ONE UEM environment and access to the UEM console.
- **Appropriate Admin Permissions** – This type of permission allows you to create profiles, policies and manage devices within the UEM console.
- **Enrollment URL** – This is the web address entered into Safari to begin the enrollment procedure. This location is specific to your company's enrollment environment. For example, this enrollment URL will follow the format of https://<companyspecificdeviceservicesurl>/enroll.
- **Group ID** – This is a unique identifier for the organization group where the device is enrolled that defines all configurations the device receives.
- **Credentials** – This a username and password combination used to identify and authenticate the user account to which the device belongs. This can be AD/LDAP user credentials.

- **Apple ID for Volume Purchase Program (VPP)** – An Apple ID is needed to purchase managed distribution or the user-based licenses when using the Volume Purchase Program with a macOS deployment.
- **Apple ID for Device Enrollment Program** – An Apple ID is needed to enroll macOS device through Device Enrollment Program (DEP).

  Note: Apple ID that is used for VPP or DEP should not be entered in the settings or preferences on the device. For example, do not use for iTunes or iCloud.

- **Apple Push Notification service (APNs) Certificate** – This is a certificate issued to your organization to authorize use of Apple's cloud messaging services.

Supported Devices

Workspace ONE UEM currently supports devices running mac 10.9 and higher, including:

- mac Book
- mac Book Pro
- mac Book Air
- iMac Pro
- imac
- mac mini
- mac Pro

Chapter 2:
macOS Device Enrollment

Overview

Each device in your organization's deployment must be enrolled in your organization's environment before it can communicate with Workspace ONE UEM and access internal content and features. macOS devices enroll using MDM functionality built into the native OS in conjunction with Workspace ONE UEM functionality.

Enrollment Methods

There are three ways to initiate enrollment for macOS devices:

- Enroll a device using the AirWatch Agent
- Sideload devices with an MDM profile
- Utilize Apple's Device Enrollment Program

End user Enrollment Using the AirWatch Agent

The agent-based enrollment process secures a connection between macOS devices and your Workspace ONE UEM environment through the AirWatch Agent app. The AirWatch Agent application facilitates User-Approved Device Enrollment, and then allows for real-time management and access to device information.

For more information, see:

- Apps for macOS Devices on page 92
- Enroll with macOS Agent on page 10

Admin Enrollment Using a Sideloaded Staging Profile

Device Staging on the Workspace ONE UEM console allows a single admin to outfit devices for other users on their behalf, which can be particularly useful for IT admins provisioning a fleet of devices. Admins can sideload a staging profile for a

single user devices and multi-user devices.

Single-User Staging

Single-user staging allows an admin to stage devices for a single user, such as a company-issued laptop. LDAP binding or pre-registration is required when staging devices for single users.

For more information, see Stage macOS Devices for Single User Enrollment on page 12.

Single Staging with Pre-Registration and Local User

Workspace ONE UEM also supports a new single staging enrollment flow for a local user with pre-registration to help macOS admins who are moving towards a deployment model without domain join. For more information, see Single Staging with Pre-Registration and Non-Domain Joined Local User on page 15.

Multi-User Staging

Multi-user device staging allows an admin to provision devices intended to be used by more than one user, such as a customer service kiosk computer. Multi-user staging allows the device to dynamically change its assigned user as the different network users log into that device.

For more information, see Configure Multi-User Staging for macOS Devices on page 14.

Bulk Device Enrollment

Depending on your deployment type and device ownership model, you may want to enroll devices in bulk. Workspace ONE UEM provides bulk enrollment capabilities for macOS devices using the Apple Device Enrollment Program (DEP) and Automated Enrollment.

Bulk Enrollment with Apple Device Enrollment Program

Deploying a bulk enrollment through the Apple Device Enrollment Program (DEP) allows you to install a non-removable MDM profile on a device, which prevents end users from being able to remove the profile from their devices. You can also provision devices in Supervised mode to access additional security and configuration settings.

For more information, see Apple Device Enrollment Program on page 17.

Enroll with macOS Agent

The agent-based enrollment process secures a connection between macOS devices and your Workspace ONE UEM environment. Install the AirWatch Agent application to facilitate enrollment and enable real-time management and access to relevant device information.

Download the AirWatch Agent from **awagent.com**. As soon as the Agent is installed, the device begins prompting the user for enrollment authentication.

1. Navigate to **awagent.com** and download the AirWatch Agent application on the device.
2. Open the .dmg file and follow the prompts to install the application. An Workspace ONE UEM authentication window appears.

3. Enter the credentials as required.

   You may be notified at this time if your user account is not allowed or blocked because your account is blacklisted and not approved for enrollment.

4. Follow the prompts in the AirWatch Agent.

   a. For devices running macOS 10.13.1 and below, proceed to step 7.

   b. For devices running macOS 10.13.2 and above, proceed to step 6.

5. The device switches to the System Preferences page. Continue to follow the on-screen prompts.

6. Enter admin username and password to install the MDM profile.

7. Once the process is completed, the Agent shows an Enrollment Complete screen and the device immediately begins receiving configurations assigned by the administrator.

8. Quit the enrollment app.

AirWatch macOS Agent Download

Download the AirWatch Agent from **awagent.com**. However, you can also download the AirWatch Agent for macOS devices at any time by logging into either UEM console or Self-Service Portal (SSP).

Download options:

- **Workspace ONE UEM console** – Navigate to **Groups & Settings > All Settings > Devices & Users > Apple > Apple macOS > Agent Application** and select **Download Agent**.
- **Self-Service Portal** – Log into the SSP and select **Download Agent** from the top action menu.

Once the Agent is installed, the icon  appears at the top of the display indicating it is active and no additional end user interaction is necessary.

Enable the Agent for Web-based Enrollment on macOS Devices

If you are utilizing web-based enrollment, enable the AirWatch Agent to be downloaded before or after enrollment through the UEM console. For web enrollment using the UEM console v7.3 and higher, make sure that the **Require Agent Enrollment for macOS** option is enabled (Navigate to **Groups & Settings > All Settings > Devices & Users > General > Enrollment** and select the check box).

1. From the UEM console Dashboard, navigate to **Devices > Device Settings > Apple > Apple macOS > Agent Application**.

2. Select the **Download macOS Agent Post Enrollment** check box for web-based enrollment.

3. Select **Save**.

4. Navigate to **awagent.com** to download the AirWatch Agent and begin the enrollment process.

Stage macOS Devices for Single User Enrollment

Single-User Device Staging on the Workspace ONE UEM Console allows a single administrator to outfit devices for other users on their behalf, which can be useful for IT administrators provisioning a fleet of devices.

Device staging through Workspace ONE Direct Enrollment is not supported. If you must stage a device, whether for single or multiple users, you must enroll the device using AirWatch Agent instead of Workspace ONE Direct Enrollment.

Important: LDAP binding is required when staging devices. To create this payload, see Binding a Device to the Directory Service in this guide.

1. Navigate to **Accounts > Users > List View** and select **Edit** for the user account for which you want to enable device staging.
2. In the **Add / Edit User** page, select the **Advanced** tab.
   a. Scroll down to the **Staging** section.
   b. Select **Enable Device Staging**.
   c. Select the staging settings that apply to this staging user.
3. **Single User Devices** stages devices for a single user. This user is the next Network User to log into the device. Toggle the type of single user device staging mode to either **Standard** or **Advanced**. Standard staging requires an end user to enter login information after staging, while Advanced means that the staging user can enroll the device on behalf of another user.
4. Ensure that **Multi User Devices** is set to **Disabled**.
5. Enroll the device using one of the two following methods.
   - Enroll using the AirWatch Agent by entering a server URL and Group ID.
   - Open the device's Internet browser, navigate to the enrollment URL, and enter the proper Group ID.
6. Enter your staging user's credentials during enrollment. If necessary, specify that you are staging for **Single User Devices**. You will only have to do this if multi-user device staging is also enabled for the staging user.
7. Complete enrollment for either Advanced or Standard staging.
   - If you are performing Advanced staging, you are prompted to enter the user name of the end-user device owner who is going to use the device. Proceed with enrollment by installing the Mobile Device Management (MDM) profile and accepting all prompts and messages.
   - If you are performing Standard staging, then when the end user completes the enrollment, they are prompted to enter their own credentials in the login window.

The device is now staged and ready for use by the new user.

Configure a Sideloading Enrollment Profile for macOS Devices

Obtain the MDM profile to prepare to sideload devices.

Do this by using Automated Enrollment functionality to generate an enrollment profile for the desired organization group. Then, enroll devices using the MDM profile for standard or advanced staging. Last, download the AirWatch Agent to complete enrollment and authenticate devices.

To configure an enrollment profile:

1. Configure a **Staging** user account in the UEM console, if you have not already. This can be a **Basic** user account you manually create or a **Directory** user account that is enabled with staging. If configuring Multi-user staging for macOS devices, then choose a **Directory** user account. For more information on creating users, see the **VMware Workspace ONE UEM Mobile Device Management Guide**.
2. Navigate to **Devices > Device Settings > Devices & Users > Apple > Automated Enrollment**.
3. Select **Enabled** for **Automated Enrollment**. You may need to **Override** the current organization group to do this.
4. Choose **macOS** as the **Platform**.
5. Select the **Staging Mode** drop-down menu.
   - **Single user device** – Stage the device for one user.
   - **Multi-user device** – Stage the device for multiple users.
6. Choose the **Default Staging User**.
   - Only staging users are available as Default Enrollment User options. Later, when staging is completed, the user's device details are updated in the UEM console and the device is associated with that end user.
7. Select **Save and Copy URL > OK** to save the .mobileconfig file that includes the name of the organization group.
8. Select **Export** to export the .mobileconfig file. This profile is needed when staging devices.
9. Navigate to **Groups & Settings > All Settings > Devices & Users > Apple > Apple macOS > Agent Application** and select **Download Agent Download** to install the AirWatch Agent.
10. Enroll using a local account and install the AirWatch Agent. At this time, all profiles are pushed to the device.
11. Distribute the device to the end user. The end user must log in from the device's Login Window to complete the staging process.

Configure Multi-User Staging for macOS Devices

Multi-user device/shared device staging allows an IT administrator to provision devices intended to be used by more than one user. Multi-User staging allows the device to change its assigned user dynamically as the different network users log into that device.

Device staging through Workspace ONE Direct Enrollment is not supported. If you must stage a device, whether for single or multiple users, you must enroll the device using AirWatch Agent instead of Workspace ONE Direct Enrollment.

1. Navigate to **Accounts > Users > List View** and select **Edit** for the user account for which you want to enable device staging.
2. In the **Add / Edit User** page, select the **Advanced** tab.
   a. Scroll down to the **Staging** section.
   b. Select **Enable Device Staging**.
   c. Select the staging settings that apply to this staging user.
3. **Single User Devices** stages devices for a single user. Toggle the type of single user device staging mode to either **Standard** or **Advanced**. Standard staging requires an end user to enter login information after staging, while Advanced means that the staging user can enroll the device on behalf of another user.
4. Ensure that **Multi User Devices** is set to **Enabled**.
5. Enroll the device using one of the two following methods.
   - Enroll using the AirWatch Agent by entering a server URL and Group ID.
   - Open the device's Internet browser, navigate to the enrollment URL, and enter the proper Group ID.
6. Enter your staging user's credentials during enrollment. If necessary, specify that you are staging for **Single User Devices**. You only have to do this if multi-user device staging is also enabled for the staging user.
7. Complete enrollment for either Advanced or Standard staging.
   - If you are performing Advanced staging, you are prompted to enter the user name of the end-user device owner who is going to use the device. Proceed with enrollment by installing the Mobile Device Management (MDM) profile and accepting all prompts and messages.
   - If you are performing Standard staging, then when the end user completes the enrollment, they are prompted to enter their own credentials in the login window.

The device is now staged and ready for use by the new users.

Single Staging with Pre-Registration and Non-Domain Joined Local User

Before VMware Workspace ONE UEM version 9.3, Workspace ONE UEM Staging for macOS required a macOS to be domain joined to a directory service (Multi-Staging or Single-Staging). After the staging enrollment, an end user logs into the macOS with Domain credentials. The device then gets checked out to the corresponding directory user within the UEM console.

From VMware Workspace ONE UEM version 9.3, macOS admins are moving towards a deployment model without a domain join. VMware Workspace ONE UEM now supports this deployment model by providing a new single staging enrollment flow for a local user with the pre-registration in the UEM console. Because Workspace ONE UEM MDM can only manage one local user, the new enrollment flow to map the staging user APNs token to the directory user that is pre-registered to the device is created.

Use Cases for Single-Staging with Pre-Registration

- Admin needs the device before the end user, but does not want to domain join and use the existing local account.
- Admin does not want to domain join, but uses Enterprise Connect or NoMAD to keep the password synced.
- Admin wants the device for setup, then integrate the API to an internal device checkout system.
- Admin creates their own custom GUI authentication dialog box which calls a Workspace ONE UEM API to switch the device to the end user.

Create Single-Staging Flow with Pre-Registration

Create a single-staging user in the UEM console before pre-registering the device.

To begin with single staging flow with pre-registration:

1. Create Single-Staging User on page 15 in the UEM console.
2. Pre-Register Device to the Enrollment User on page 16 (basic or directory user in the UEM console)
3. Enroll the device to the single staging user (DEP staging or Web enrollment or Agent enrollment)

Pre-Requistites

- Pre-registration is only supported for Single-Staging
- Device must be assigned to a staging user before the pre-registration or API flow to work

Create Single-Staging User

1. Navigate to **Accounts > Users > List View** and then select **Add > Add User**.
2. Enter the general information such as Username, Password, Full name, email address in the **General** tab for a single staging user in the **Add/Edit User** page.
3. In the **Advanced** tab, under **Staging**, enable **Device Staging** and **Single User Devices**.
4. Select **Save** to save the enrollment user.

Once single staging user is created, the next step is to pre-register the macOS device. In the UEM console, pre-register the device through the device identifiers (such as serial, udid, and so on) to the directory or basic enrollment user.

Pre-Register Device to the Enrollment User

1. Navigate to **Devices > Lifecycle > Enrollment Status**. Select **Add** and then select **Register Device**.
2. In the **User** tab, enter a **basic user** or **directory user** in the User's **Search Text** text box and select the user from the search list.
3. Enable **Show Advanced Device Information Options** check box and enter the device identifiers of the device.
4. Select **Save**.

After the pre-registration of the device is complete, the next step is to enroll device to the Workspace ONE UEM single-staging user.

Device Enrollment to the Single-Staging User

Log into the macOS device with a local user and enroll through DEP Staging, Agent Enrollment, Web Enrollment, Apple Configurator with a Workspace ONE UEM single-staging user. If using DEP, the managed local user must be the user created during Setup Assistant process. For more information, refer the enrollment sections.

After enrollment completes, the UEM console automatically checks out the user from the staging use to the pre-registered basic user. All assigned user profiles, commands, or applications start installing onto the device.

Single Staging with API

As an alternative to pre-registration, use Single-Staging with API to switch the user from the Workspace ONE UEM staging user to the Workspace ONE UEM directory or basic user. Before using Single-Staging with API, ensure that the device is enrolled through Agent enrollment, Web enrollment, or Apple Configurator with a Workspace ONE UEM single-staging user.

Use the following (v2) API to switch the device assignment:

```
PATCH /api/mdm/devices/{id}/enrollmentuser/{enrollmentuserid}
```

where,

- id – Workspace ONE UEM device ID
- enrollmentuserid – Workspace ONE UEM user ID

The header request must be:

```
Accept – application/json;version=2
```

Ensure you receive 200 OK as a return response which indicates that the device switching is complete with no errors. All assigned user profiles, commands, or applications start coming down to the device.

Apple Device Enrollment Program

Devices can also be staged through Apple's Device Enrollment Program (DEP). Apple DEP is a streamlined staging method that is best for corporate-owned devices.

DEP on macOS enables you to:

- Apply standard staging to devices.
- Configure Setup Assistant panes to skip during installation.
- Enforce enrollment for all end users.
- Customize and streamline the enrollment process to meet your organization's needs.
- Hold a device in the Awaiting Configuration state when it reaches the Setup Assistant screen.
- Create a local Hidden Admin account and allow end users to skip the Account Creation screen.

For more information, see the **VMware Workspace ONE UEM Guide for Apple Device Enrollment**.

For additional Apple information, see the Apple Deployment Programs' Device Enrollment Program Guide or contact your Apple Representative.

Custom Bootstrap Packages for Device Enrollment

In a typical device enrollment, the AirWatch Agent must be installed on a device before any other installer packages can be executed. The Bootstrap Package allows installer packages to deploy to a device immediately after the device is enrolled.

Bootstrap Packages

Bootstrap Packages use the Apple MDM command `InstallApplication`, which allows an MDM to natively install .pkg files to an enrolled device. Historically, the AirWatch Agent handles the download and installation of application files. Bootstrap Packages allow .pkg files to install immediately after enrollment whether or not the AirWatch Agent is installed.

You may want to use alternative tools for device and application management in addition to the AirWatch Agent. Bootstrap package enrollment comprises an enrollment flow paired with a bootstrap package that installs the alternative tooling and configures the device before the end user begins using the device.

Bootstrap Package Use Cases

Bootstrap Packages may be useful in certain deployment scenarios. This list is not exhaustive.

- You want to create a custom-branded end user experience, such as launching a window as soon as enrollment completes, to inform the user about the installation process and instruct them to wait to use the device until provisioning and installation complete.
- Your deployment does not include the AirWatch Agent, but you still have critical software to deploy to devices.
- You want to use Munki for Application Management, and need the Munki client to install immediately after enrollment so the user can begin installing apps, rather than going through the AirWatch Agent and AirWatch Catalog.
- Your deployment only uses MDM for certificate management and software management, and uses Chef or Puppet for configuration management. In this configuration, Chef or Puppet must be installed as soon as enrollment completes to finish configuring the device.

Bootstrap Package Creation

Bootstrap packages are deployed to the device as soon as enrollment completes. Bootstrap packages deployed from the Console will not deploy to existing enrolled devices unless the devices are specifically queued using the Assigned Devices list for the package.

You must create packages before you deploy them. There are several tools available that can create a package for use in the Bootstrap Package functionality. Created packages must meet two criteria:

- The package must be signed with an Apple Developer ID Installer Certificate. Only the package needs to be signed, not the app, since the Apple Gatekeeper does not check apps installed through MDM.
- The package must be a distribution package (product archive), not a flat component package.

When you have created a bootstrap package, you must deploy the package to your devices. For more information, see Deploy a Bootstrap Package on page 19.

Deploy a Bootstrap Package

Bootstrap packages allow you to make your end users' devices usable sooner after the device enrolls than a traditional enrollment. Once you have created a bootstrap package, you must deploy the package to your devices.

You must create bootstrap packages before you deploy them. There are several tools available that can create a package for use in the Bootstrap Package functionality. For more information, see Custom Bootstrap Packages for Device Enrollment on page 18.

To deploy a bootstrap package:

1. Navigate to **Apps & Books > Internal > Add Application**.
2. Upload a .pkg file that meets these requirements:
   - Package must be signed with an Apple Developer ID Installer certificate.
   - Package must be a distribution package.

   For more information about the bootstrap package requirements, see Custom Bootstrap Packages for Device Enrollment on page 18.
3. Select **Continue** and modify the items in the **Details** tab and the **Images** tab if necessary.
4. Select **Save & Assign**, and then select **Add Assignment** to configure the **App Delivery Method**.

   By default, the **App Delivery Method** is set to **Auto**. In this configuration, the assigned bootstrap package will only install on newly-enrolled devices.

   To install the bootstrap package on enrolled devices, select **On Demand**. On-Demand package deployments require you to manually push the package to devices.

   To manually deploy a bootstrap package to enrolled devices, navigate to **Applications > Internal Apps > List View**. Select the package you want to assign to open the **Application Details**. Use the **Devices** tab to select devices to push the package to.

Chapter 3:
Software Distribution and Management

Overview

Before Workspace ONE UEM console v9.3, most of the macOS applications or software were deployed through Product Provisioning. From v9.3, Workspace ONE UEM also offers a flexible deployment through an integration with Munki, an widely renowned open source tool. Now all macOS application file types (.dmg, .pkg, .mpkg) can be managed in the Internal Applications section on the UEM console (**Apps & Books > Applications > Native > Internal**.

The flexible deployment feature resides in the **Assign** sections of the application area and offers advantages to the assigning process.

- Configure deployment assignments.
- Assign multiple deployments simultaneously.
- Order assignments so that critical deployments are not missed due to the limited bandwidth.
- Customize assignments for multiple smart groups.

Requirements to Deploy macOS Applications for Software Distribution

To deploy macOS applications with the software distribution, use the supported file types, platform version, and agents.

Supported Platform Version

macOS 10.10+

Supported File Types

PKG, DMG, MPKG

Supported Agents

- AirWatch Agent for macOS 3.0
- (Optional) Workspace ONE 1.0 native application

Considerations

- **pkginfo metadata file generation** – You can upload all primary macOS software file types through **Books & Apps > Internal Applications**. A PKG file can be a Bootstrap package, or it can be managed through full lifecycle management. To configure advanced management features for macOS software through the integrated Open-Source Munki library in the agent, you must generate a metadata file for the application before uploading the application to the UEM console. You can generate a pkginfo metadata file using Generate Metadata Using VMware AirWatch Admin Assistant Tool on page 21.
- **Third-Party Integration** – Apart from using the Admin Assistant tool to generate metadata or a pkginfo file, you can also integrate with AutoPkg and AutoPkgr tools that have ready-made software with configuration features. They perform periodic checks for updates to the third-party software and notify the admins.
- **Migration from Munki setup to Workspace ONE UEM** – You can add the existing application with the direct link of the application on your current Munki Repository server. This method is advantageous, as there is no requirement for an actual upload of the file to Workspace ONE UEM, which uses Workspace ONE UEM File Storage space.
- **CDNs and File Storage Systems** – All deployments use a content delivery network (CDN) to deploy applications. This method has the advantage of sending the content to devices in the network and to remote devices. It also offers increased download speed and reduces the bandwidth on the Workspace ONE UEM servers. However, in some scenarios, a CDN is not a viable choice. For these instances, use a file storage system.

Configure Software Management

Configure Workspace ONE UEM to recognize the deployment of macOS applications through the software distribution method. To initiate the software management lifecycle for macOS applications, enable the software management feature (SaaS or on-premises) on the UEM console.

1. Navigate to **Settings > Devices & Users > Apple > Apple macOS > Software Management**.
2. Enable Software Management. At this point, make sure that you verify if the **File Storage** is enabled. If there is no file storage enabled, you are requested to enable it.

On-Premises environments use a file storage system to store the large macOS applications and also use a CDN to download the applications and to reduce the bandwidth on other servers.

Generate Metadata Using VMware AirWatch Admin Assistant Tool

The VMware Admin Assistant tool uses a Munki command-line utility to give admins an easy way to create the pkginfo metadata files that you must enforce software management. Workspace ONE UEM requires pkginfo metadata file with the application file to manage the deployment in the UEM console.

Note: The VMware Admin Assistant Tool is available in the UEM console, and at https://awagent.com/AdminAssistant/VMwareWorkspace ONE UEMAdminAssistant.dmg. The Admin Assistant is also built with an auto-update mechanism, which updates to the latest version based on the AppCast.XML file available at https://awagent.com/AdminAssistant/VMwareWorkspace ONE UEMAdminAssistant.xml.

To generate a metadata file using the Admin Assistant:

1. Click open the Admin Assistant tool. The Assistant dialog box asks you to upload the application installer files for the Assistant to parse.
2. Upload an application installer file by dragging and dropping a .pkg, .dmg, .app, or .mpkg file, or browse your local files for an installer file.
    - When you drop or select a file, the tool initiates the process. If needed, you can add more files during this time.
    - If you select an .app file, the tool creates a .dmg containing the file.

After the parsing is finished, the tool prompts you to reveal the parsed metadata files in Finder. Store the metadata files in a local folder where you can easily retrieve them during the Software distribution procedure.

Upload Applications to Deploy to macOS Devices

Deploy internal applications to your mobile network by upload internal applications with local files in the UEM console.

To deploy applications:

1. Navigate to **Apps & Books > Applications > Native > Internal** and select **Add Application**.
2. Select **Upload > Local File** and browse for the application file on your system. Select the .dmg, .pkg, or .mpkg file to upload.
3. Upload the required application metadata file (.plist).

   To create a metadata file, download and install the VMware Workspace ONE UEM Admin Assistant Tool to your macOS computer. For more information about how to use the VMware AirWatch Admin Assistant Tool, see Generate Metadata Using VMware AirWatch Admin Assistant Tool on page 21.
4. Complete the **Images** tab.

Setting	Description
Icon	Upload or drag the images of the application to display in the AirWatch Catalog as the icon for the application

5. Configure **Scripts** settings to run the installation, uninstallation, and verification of the application. By providing pre-install scripts and post-install scripts, you can perform additional configuration tasks or install additional items without the need of repacking the applications or software. Simply paste the script and Workspace ONE UEM formats it to be used by Munki. For more information on the exit behavior of each script type, see Software Distribution Scripts on page 26.

Setting	Description
Install Scripts	
Pre-Install Script	Define a pre-install script to run before attempting installation. See Software Distribution Scripts on page 26 for information on the exit code behavior of the script.
Post-Install Script	Define a post-install script to run after a successful installation. See Software Distribution Scripts on page 26 for information on the exit code behavior of the script.
Uninstall Scripts	
Pre-Uninstall Script	Define a pre-uninstall script to run before an attempted uninstall. See Software Distribution Scripts on page 26 for information on the exit code behavior of the script.

Setting	Description
Uninstall Method	Select from the drop-down and customize the behavior of the Uninstall Methods on page 25. The options are: • Remove Packages • Remove Copied items • Remove app • Uninstall script See Software Distribution Scripts on page 26 for information on the exit code behavior of the script.
Post Uninstall Script	Define a post-uninstall script to run after a successful uninstall. See Software Distribution Scripts on page 26 for information on the exit code behavior of the script.
Note: Failure of the pre-install script cancels the installation attempt and failure of the post-install script logs errors, but the install is considered complete.	
Verification Scripts	
With some software, you have to configure what exactly defines a successful install or uninstall. Munki allows software configuration through setting an Install or Uninstall Check Script.	
Install Check Script	If present, the script runs to determine if the application must be installed. A return code of 0 means install is needed, any other return code causes install to be skipped.
Uninstall Check Script	If present, the script runs to determine if the application must be uninstalled. A return code of 0 means uninstall is needed, any other return code causes uninstall to be skipped.

6. Configure the **Deployment** tab settings.

Setting	Description
Restart Action	Select the restart action for the application. The available actions are: • Require Shutdown • Require Restart • Recommend Restart • Require Logout
Condition	Define the condition for the application to be installed on the device.

Setting	Description
Desired State Management	Currently when installing macOS software, administrators have an option to enable or disable the Desired State Management settings based on the business needs. Desired State Management is enabled by default to enforce application management during macOS software installation. If enabled, and if the end-user deletes the app, the application is automatically reinstalled on the next Agent sync. If disabled, and if the end-user deletes the app, the application is not automatically reinstalled, unless pushed from the UEM Console or Catalog.

7. Configure the **Terms of Use** tab.

   Terms of use states specifically how users are expected to use the application. When the application pushes to devices, users view the terms of use that they must accept to use the application. If users do not accept, they cannot access the application.

8. Select **Save & Assign**.

Uninstall Methods

There are multiple methods available for the uninstallation of software and the appropriate method is selected by default by the VMware Admin Assistant tool based on the file type. If needed, you can override the default with any of the following methods.

Remove Copied Items

The Remove Copied Items method is primarily used for DMG file types, where it pulls from the ***items_to_copy array [dicts]*** array in the pkginfo file and deletes all file paths in the array.

Remove App

The Remove App method pulls from the installs array [dicts] in the pkginfo file and deletes all file paths in the array.

Remove Packages

The Remove Packages method is used primarily for PKG file types. This method:

- Uses receipts and analyzes the packages to remove
  - Tries to determine what all files were installed through Bom file
  - Deletes receipt
- Removes non-associated packages only

Uninstall Script

Uninstall scripts are written in a shell script. This method is:

- Used for any installer type
- Used to perform custom uninstall operation. If you have a customized deployment for an application, then write a corresponding uninstall script to remove the custom configurations.

Software Distribution Scripts

Use macOS software distribution scripts to perform additional configurations or validation of tasks in the **Script** section of the **Add or Edit Application** page of the console.

By inserting scripts, you can:

- Avoid repacking installers by using pre-install scripts
- Avoid post-install user prompts by scripting additional configurations
- Perform validation
- Customise uninstallation

The following table provides exit code behavior for each script type.

Script Type	Exit Code 0 Behavior	Other exit Code Behavior
Pre-Install	Continue Install	Skip Install
Post-Install	Successfully Installed	Installed Successfully with Warnings
Pre-Uninstall	Continue Uninstall	Skip Uninstall
Post-Uninstall	Uninstall Successfully	Uninstall successfully with Warnings
Install Check Script	Install is Needed	Skip Install
Uninstall Check Script	Uninstall is Needed	Skip Uninstall

Software Distribution Conditions

Conditions are a set of attributes provided by the integrated open source Munki library for determining install applicability. Conditions are defined at a per-application level and are evaluated before download and install of the software. There are some built-in conditions supported by Munki.

Conditions Format

Conditions are written in the format:

```
machine_type == "laptop" AND os_vers BEGINSWITH "10.7"
```

Conditional Comparison Attributes

Attribute	Type	Description	Example Comparison
hostname	String	Hostname	hostname=="Lobby imac"
arch	String	Processor architecture. For example: 'powerpc', 'i386', 'x86_64'	arch=="x86_64"
os_vers	String	Full OS Version. For example: "10.7.2"	os_vers BEGINSWITH "10.7"
os_vers_major	Integer	Major OS Version. For example: '10'	os_vers_major == 10

os_vers_minor	Integer	Minor OS Version. For example:'7'	os_vers_minor == 7
os_vers_patch	Integer	Point release version. For example: '2'	os_vers_patch >=2
machine_model	String	'MacMini1,1', 'iMac4,1', 'MacBookPro8,2'	machine_model == "iMac4,1"
machine_type	String	'laptop' or 'desktop'	machine_type == "laptop"
ipv4_address	Arrays of string	This contains current IPv4 addresses for all interfaces	ANY ipv4_address CONTAINS '192.168.161.'
munki_version	String	Full version of the installed munkitools	munki_version LIKE '*0.8.3*'
serial_number	String	machine serial number	serial_number =="W9999999U2P"
date	UTC date string	Date and time. Note the special syntax required to cast a string into an NSDate object.	date>CAST("2013-01-02T00:00:00Z", "NSDATE")

Assign Applications to macOS Devices

Once you configure an application, add a single assignment or multiple assignments. If you add multiple assignments, prioritize the importance of the assignment by moving its place in the list up for most important or down for least important.

To assign applications:

1. Navigate to **Apps & Books > Applications > Native > Internal** or **Public**.
2. Upload an application and select **Save & Assign** or select the application and choose **Assign** from the actions menu.
3. Select **Add Assignment** and complete the following options.

Setting	Description
Select Assignment Groups	Type a smart group name to select the groups of devices to receive the assignment.
App Delivery Method	• **On Demand** – Deploys content to a catalog or other deployment agent and lets the device user decide if and when to install the content. This option is the best choice for content that is not critical to the organization. Allowing users to download the content when they want helps conserve bandwidth and limits unnecessary traffic. • **Automatic** – Deploys content to a catalog or other deployment agent on a device upon enrollment. After the device enrolls, the Agent automatically installs the app without needing user interaction. This option is the best choice when it is critical to your organization and its mobile users.
Deployment Begins On Internal Applications	Set a day of the month and a time of day for the deployment to start. The **Priority** setting governs which deployments push first. Workspace ONE UEM then pushes deployments according to the **Effective** configuration. To set a beginning date with enough bandwidth for successful deployment, consider the traffic patterns of your network .

4. Select **Add**.
5. Use the **Move Up** and **Move Down** options to order assignments if you have more than one. Place critical assignments at the top of the list. This configuration displays as the **Priority**.
6. Select **Save & Publish**.

Manage Software Distribution Updates

Once the macOS application or software is deployed, the deployed application or software can be managed from the UEM console. You can manage updates by uploading a new version of the file onto the UEM console.

To update the application or software:

1. Navigate to **Apps & Books > Native.**
2. Select the application that you want to update. .
3. On the top right of the **Details** page, select **Add Version**.
4. Upload the installer and the .pkginfo file of the new version.
5. If necessary, perform additional changes and then **Save**.
6. Select **Save & Assign**.

Methods used by Munki to Install Applications

Munki uses the information in the pkginfo file and looks for the software items to decide whether or not a given item must be installed. To create a functional pkginfo items, understand the methods used by Munki to check the list of software items.

Important: Most of the content under this section are obtained from Munki website.

Methods

In the order of precedence, listed below are the methods used by Munki in determining whether the given item should be installed (or removed):

- Install Check Script on page 31
- Install Items on page 32
- Receipts on page 35

When combining these methods, only the highest priority method is used. For example, if a given pkginfo item has both an "installs" list and a "receipts" list, the receipts will be ignored for purposes of determining installation status. Even in this case, though, receipts may be used when removing an item, as they help Munki determine exactly which files were installed.

Install Check Script

A pkginfo item may optionally contain an **installcheck_script**. Install ckeck script provides a method for determining if an software item needs to be installed, where providing **installs/receipts** is inadequate or impractical. Command-line tools typically installed through port (macports) or Python modules installed using easy_install or pip are prime examples as they provide no easy method for determining their installed version.

An install check_script should be written such that an exit code of 0 indicates that the item is currently not installed and should therefore be installed. All non-zero exit codes indicate that the item is installed.

An example of installcheck_script illustrating a check to determine if the current version of the argparse Python module is installed.

```
#!/bin/sh
# Grab current version of installed python module
version="$(python -c 'import argparse;print argparse.__version__' 2>/dev/null)"
# Compare with the version we want to install
if [ ${version:-0} < 1.2.1 ]; then
exit 0
else
exit 1
fi
```

Uninstall Check Script

Optionally, an explicit **uninstallcheck_script** can be provided to determine whether or not an software item should be removed. In this case, the script with an exit code of 0 indicate that the item is currently installed and that removal should occur. All non-zero exit codes indicate that the item is not installed.

Install Items

The install items list is generated by the VMware AirWatch Admin Assistant for some types of installation items(.dmg), but not for Apple packages (.pkg or .mpkg). You can generate (or modify) this list and is the most flexible mechanism for determining installation status.

The **installs** list can contain any number of items such as applications, preference panes, frameworks, or other bundle-style items, info.plists, simple directories, or files. You can use any combination of items to help Munki determine if an item is installed or not.

An example of an auto-generated "installs" list for Firefox 6.0

```
<key>installs</key>
<array>
    <dict>
    <key>CFBundleIdentifier</key>
    <string>org.mozilla.firefox</string>
    <key>CFBundleName</key>
    <string>Firefox</string>
    <key>CFBundleShortVersionString</key>
    <string>6.0</string>
    <key>minosversion</key>
    <string>10.5</string>
    <key>path</key>
    <string>Applications/Firefox.app</string>
    <key>type</key>
    <string>application</string>
    </dict>
</array>
```

To determine if Firefox 6 is installed or not, Munki checks for an application with a CFBundleIdentifier of *org.mozilla.firefox* and if found, verifies that its version (CFBundleShortVersionString) is at least 6.0. If Munki cannot find the application or its version is lower than 6.0, it considers Firefox-6.0 as not installed. Installs lists can contain multiple items. If any item is missing or has an older version, the item is considered not installed. You can manually generate items to add to an **installs** list using the following makepkginfo,

```
/Library/Application\ Support/AirWatch/Data/Munki/bin/makepkginfo -f
/Library/Interne
t\ Plug-Ins/Flash\ Player.plugin
```

```
<?xml version="1.0" encoding="UTF-8"?>
<!DOCTYPE plist PUBLIC "-//Apple//DTD PLIST 1.0//EN"
"http://www.apple.com/DTDs/Prope
rtyList-1.0.dtd">
<plist version="1.0">
```

```
<dict>
    <key>installs</key>
    <array>
        <dict>
            <key>CFBundleShortVersionString</key>
            <string>10.3.183.5</string>
            <key>path</key>
            <string>/Library/Internet Plug-Ins/Flash Player.plugin</string>
            <key>type</key>
            <string>bundle</string>
        </dict>
    </array>
</dict>
</plist>
```

Copy and paste the entire **installs** key and value, or copy just the dict value and add it to an existing installs list inside your pkginfo file. Munki checks for the existence of */Library/Internet Plug-Ins/Flash Player.plugin* and if found, check its version. If the version is lower than 10.3.183.5, the item would be considered not installed. You can generate installs items for any filesystem item, but Munki only knows how to determine the versions for bundle-style items that contain an Info.plist or version.plist with version information.

For other filesystem items, Munki can only determine existence (in the case of a non-bundle directory), or can calculate a checksum (for files). For files with checksums, the test fails (and therefore the item will be considered not installed) if the checksum for the file on disk does not match the checksum in the pkginfo.

```
<key>installs</key>
<array>
    <dict>
        <key>md5checksum</key>
        <string>087fe4805b63412ec3ed559b0cd9be71</string>
        <key>path</key>
        <string>/private/var/db/dslocal/nodes/MCX/computergroups/loginwindow.pli
        st</s
        tring>
        <key>type</key>
        <string>file</string>
    </dict>
</array>
```

If you want Munki to only check for the existence of a file and do not care about its contents, remove the generated md5checksum information in the installs item info. Make sure the provided path is intact.

```
<key>installs</key>
<array>
```

```
    <dict>
    <key>path</key>
    <string>/private/var/db/dslocal/nodes/MCX/computergroups/loginwindow.plist
    </string>
    <key>type</key>
        <string>file</string>
    </dict>
</array>
```

Receipts

When an Apple-style package is installed, generates a receipt on the machine. Metapackages generate multiple receipts. The VMware AirWatch Admin Assistant adds the names and versions of those receipts to a receipts array in the pkginfo for a package. Following is a receipts array for the Avid LE QuickTime codecs, version 2.3.4.

```
<key>receipts</key>
<array>
    <dict>
        <key>filename</key>
        <string>AvidCodecsLE.pkg</string>
        <key>installed_size</key>
        <integer>1188</integer>
        <key>name</key>
        <string>AvidCodecsLE</string>
        <key>packageid</key>
        <string>com.avid.avidcodecsle</string>
        <key>version</key>
        <string>2.3.4</string>
    </dict>
</array>
```

If Munki is using the receipts array to determine installation status, it checks for the existence and the version of each receipt in the array. If any receipt is missing or has a lower version number than the version specified for that receipt in the receipts array, the item is considered not installed. Only if every receipt is present and all versions are the same as the ones in the pkginfo (or higher) is the item considered installed. To troubleshoot issues, use the pkgutil tool to examine the installed receipts.

```
# pkgutil --pkg-info com.avid.avidcodecsle
No receipt for 'com.avid.avidcodecsle' found at '/'.
```

In this case, the receipt for the Avid LE QuickTime codecs was not found on this machine. A common complication with receipts is, with many metapackages, the installation logic results in only a subset of the subpackages being installed. Generally, the receipts list contains a receipt for every subpackage in a metapackage (and needs this info if Munki is asked to remove the software item based on package receipts). But if it is normal and expected that not every subpackage will actually be installed, Munki will continually mark the item as not currently installed and offer to install it again and again. One solution for this issue is to add an *optional* key with the value of *true* to the receipts that are optionally installed. Munki will then not consider these receipts when determining installation status.

```
<key>receipts</key>
<array>
    <dict>
        <key>filename</key>
```

```
        <string>mandatory.pkg</string>
        <key>installed_size</key>
        <integer>1188</integer>
        <key>name</key>
        <string>Mandatory</string>
        <key>packageid</key>
        <string>com.foo.mandatory</string>
        <key>version</key>
        <string>1.0</string>
    </dict>
    <dict>
        <key>filename</key>
        <string>optional.pkg</string>
        <key>installed_size</key>
        <integer>1188</integer>
        <key>name</key>
        <string>Optional</string>
        <key>optional</key>
        <true/>
        <key>packageid</key>
        <string>com.foo.optional</string>
        <key>version</key>
        <string>1.0</string>
    </dict>
</array>
```

Another solution for this situation is to provide an **installs** array that lists items that are installed by the package. Munki can use installs array information instead of the receipts to determine installation status.

Troubleshooting macOS Software Distribution

This section helps you understand how to troubleshoot problems related to the macOS software distribution process. It also details you on the path to verify the logs.

Troubleshooting Issues

- How to verify on the device locally that an application is assigned?

  All assigned applications are shown in the */Library/Application\ Support/Workspace ONE UEM/Data/Munki/Munki_Repo/manifests/device_manifest.plist* in the managed_installs array.

  Furthermore, all assigned applications have their corresponding pkginfo stored in the catalog plist at */Library/Application\ Support/Workspace ONE UEM/Data/Munki/Munki_Repo/catalogs/device_catalog.plist*

- How to verify on the console that an application is assigned?

  In the internal applications **List View** page, select the application to go to the application **Details** page. Then select the **Devices** tab. This page shows the application install statuses for all assigned and enrolled devices.

- How to get direct access to Munki logs?

  Munki Logs can also be directly accessed on the device in the path:

  /Library/Application Support/Workspace ONE UEM/Data/Munki/Managed\Installs/Logs/, where they are saved as ManagedSoftwareUpdate.log files.

- Where to look for device report data on the UEM console?

  The UEM console reports data from the device in a few locations.

  - Navigate to **Apps & Books > Applications > Native > Internal**. Select an application and access **Application Details > Devices** tab to view the install statuses for each device.
  - Navigate to **Devices & Users > Devices > List View** and select a device to access **Device Details > Troubleshooting** tab. You can view the activities performed on the device and filtering options to show the information relating to the software distribution.

Chapter 4:
macOS Device Profiles

Overview

Profiles are the primary means to manage devices. Configure profiles so your macOS devices remain secure and configured to your preferred settings. You can think of profiles as the settings and rules that, when combined with compliance policies, help you enforce corporate rules and procedures. They contain the settings, configurations, and restrictions that you want to enforce on devices.

A profile consists of the general profile settings and a specific payload. Profiles work best when they contain only a single payload.

macOS profiles apply to a device at either the user level or the device level. When creating macOS profiles, you select the level the profile applies to. Some profiles can only be applied to the user level or device level.

Device Access

Some device profiles configure the settings for accessing a macOS device. Use these profiles to ensure that access to a device is limited only to authorized users.

Some examples of device access profiles include:

- Secure a device with a Passcode profile. For more information, see Configure a Passcode Policy Profile (macOS) on page 39
- Configure Apple's Gatekeeper functionality, which secures application downloads and controls specific settings related to user passwords. For more information, see Configure a Security and Privacy Settings Profile (macOS) on page 58.
- Configure accessibility options to accommodate end users' needs. For more information, see Configure an Accessibility Profile (macOS) on page 64.

Device Security

Ensure that your macOS devices remain secure through device profiles. These profiles configure the native macOS security features or configure corporate security settings on a device through Workspace ONE UEM.

Some examples of device security profiles include:

- Use a Wi-Fi profile to connect enrolled devices to your corporate Wi-Fi without sending the network credentials to users. For more information, see Configure a Network Access Profile (macOS) on page 40.
- Implement digital certificates to protect corporate assets. For more information, see Configure a SCEP/Credentials Profile (macOS) on page 49
- Ensure access to internal resources for your devices with the VPN profile. For more information, see Configure a VPN Profile (macOS) on page 42 and Configure a VPN On Demand Profile (macOS) on page 43.

Device Configuration

Configure the various settings of your macOS devices with the configuration profiles. These profiles configure the device settings to meet your business needs.

Some examples of device configuration profiles include:

- Set up access to Microsoft Outlook and corporate files with an Exchange Web Services profile. For more information, see Configure an Exchange Web Services Profile (macOS) on page 45.
- Integrate VMware Fusion with VMware Workspace ONE UEM MDM capabilities to allow for management of both the host device and corporate applications in a virtual machine scenario. For more information, see Configure a VMware Fusion Profile (macOS) on page 71.
- Ensure that the devices remain up to date with the macOS Updates profile. For more information, see Configure a Software Update Server Profile (macOS) on page 53.

Configure a Passcode Policy Profile (macOS)

Device passcode profiles secure macOS devices and their content. Choose strict options for high-profile employees, and more flexible options for other devices or for those part of a BYOD program.

If multiple profiles enforce separate policies on a single device, the most restrictive policy is enforced. If your password policy is being managed by your directory for network users logging into the devices, Workspace ONE UEM does not recommend a passcode policy.

To create a passcode profile:

1. Navigate to **Devices > Profiles & Resources > Profiles** and select **Add**. Select Apple macOS, and then select whether this profile will apply to only the enrollment user on the device (**User Profile**), or the entire device (**Device Profile**).
2. Configure the profile's **General** settings.
3. Select the **Passcode** payload.

4. Configure Passcode settings:

Setting	Description
Require passcode on device	Enable mandatory passcode protection.
Allow simple value	Allow the end user to apply a simple numeric passcode.
Require Alphanumeric Value	Restrict the end user from using spaces or non-alphanumeric characters in their passcode.
Minimum Passcode Length	Select the minimum number of characters required in the passcode.
Maximum Passcode Age (days)	Select the maximum number of days the passcode can be active.
Auto-lock (min)	Select the amount of time the device can be idle before the screen is locked automatically.
Passcode History	Enter the number of passwords to store in order to prevent end users from recycling passwords.
Maximum Number of Failed Attempts	Select the number of failed attempts allowed. If the end user enters an incorrect passcode for the set number of times, the device locks.
Delay after failed login attempts	Enter the length of the delay in minutes before allowing another chance to login again after the end user has reached the maximum number of failed passcode attempts.

5. Select **Save & Publish** when you are finished to push the profile to devices.

Note: End users are only prompted to change their password if the AirWatch Agent is installed and the **Enforce Passcode** check box is selected in the Agent settings in the UEM console. For more information about configuring the Agent, see Apps for macOS Devices on page 92.

Configure a Network Access Profile (macOS)

A network profile allows devices connect to corporate networks, even if they are hidden, encrypted, or password protected. This can be useful for end users who travel and use their own unique wireless network or to end users in an office setting where they need to automatically connect their devices to a wireless on-site.

1. Navigate to **Devices > Profiles & Resources > Profiles** and select **Add**. Select Apple macOS, and then select whether this profile will apply to only the enrollment user on the device (**User Profile**), or the entire device (**Device Profile**).
2. Configure the profile's **General** settings.
3. Select the **Network** payload.
4. Choose to configure **Wi-Fi** or **Ethernet** settings.

Setting	Description
Network Interface	Choose to connect to connect to network using Wi-Fi or Ethernet.

Setting	Description
Service Set Identifier	Enter the name of the network to which the device connects.
Connectivity	Select the type of connectivity. **Hidden** – This allows a connection to network that is not open or broadcasting. **Auto-Join** – This determines whether the device automatically connects to the network.
Security Type	Choose the method for connection encryption to the wireless network.
Use as login window configuration	Allow the user to authenticate to the network at login. This option appears when **WiFi** and **Security Type** is **Enterprise** This option also appears when **Ethernet** is selected.
Protocols	Choose protocols for network access. • This option appears when **WiFi** and **Security Type** is any of the **Enterprise** choices. This option also appears when **Ethernet** is selected.
Password	Enter the password required to join the **Wi-Fi** network.

5. Configure **Authentication** settings that vary by protocol including but not limited to:

Setting	Description
Use as Login Window Configuration	For **Device Profiles** only. Select this if any enterprise protocols were selected for the network. Allow authentication with the target machine's directory credentials.
Username	Enter the username for the account.
User Per-Connection Password	Request the password during the connection and send with authentication
Password	Enter the password for the connection.
Identity Certificate	Select the certificate for authentication.
TLS Minimum Version	Select the minimum TLS version 1.0, 1.1, and 1.2. If no value is selected, the minimum TLS version defaults to 1.0 **Note:** Minimum and Maximum TLS versions can be configured only for TLS , TTLS, EAP-Fast, and PEAP protocol types.
TLS Maximum Version	Select the maximum TLS version 1.0, 1.1, and 1.2. If no value is selected, the maximum TLS version defaults to 1.2
Inner identity	Select the inner identification method.
Outer identity	Select the external authentication method.

6. Enter the name(s) of server certificates.
7. Select **Allow Trust Exceptions** to enable the end user to make trust decisions.
8. Configure **Proxy** settings for either **Manual** or **Auto** proxy types
9. Select **Save & Publish** when you are finished to push the profile to devices.

Configure a VPN Profile (macOS)

Virtual private networks (VPNs) provide devices with a secure and encrypted tunnel to access internal resources. VPN profiles enable each device to function as if it were connected through the on-site network.

1. Navigate to **Devices > Profiles & Resources > Profiles** and select **Add**. Select Apple macOS, and then select whether this profile will apply to only the enrollment user on the device (**User Profile**), or the entire device (**Device Profile**).
2. Configure the profile's **General** settings.
3. Select the **VPN** payload.
4. Configure **Connection** settings.

> **Note:** The following settings vary depending on the type of connection selected.

Settings	Description
Connection Name	Enter the name of the connection name to be displayed on the device.
Connection Type	Use the drop-down menu to select the network connection method. The available options are: • L2TP • PPTP • IPSec (Cisco) (applicable for VPN On Demand) • F5 SSL (applicable for VPN On Demand) • Custom SSL (applicable for VPN On Demand) • F5 Access (applicable for VPN On Demand)
Identifier	Enter the identifier for the VPN connection.
Server	Enter the hostname or IP address of the server to which to connect.
Account	Enter the name of the VPN account.
Encryption Level	Select the level of encryption, either **Automatic** or **Maximum Bit**.
Send All Traffic	Select this check box to force all traffic through the specified network.
Per App VPN	For macOS v10.9 devices, use Per-App VPN to choose what apps should connect to what networks.
Connect Automatically	Select this check box to allow the VPN to connect automatically to chosen Safari Domains.

Settings	Description
Enable Safari Domains	Enable this setting to set specific domains or hosts that open the secure VPN connection in the Safari browser. **Add** domains as needed. If you configure a VMware Tunnel Per-App Tunnel network traffic rule for the Safari app for macOS, Workspace ONE UEM disables this setting. The network traffic rules override any configured Safari Domain rules.
App Mapping	Enable this setting to allow specific applications to open a secure VPN connection. **Add** app bundle ID(s) for applications allowed to open a secure VPN connection.
Web Logon	Select this checkbox to allow F5 Access application to render a browser-based login page instead of a dialog box for VPN authentication. This feature also gives the administrators the ability to configure fields required for the authentication.

5. Configure **Authentication** information including:

Setting	Description
User Authentication	Select the radio button to indicate how to authenticate end users through the VPN, through either password or RSA SecurID.
Password	Enter the password for the VPN account.
Machine Authentication	Select the type of machine authentication to authorize end users for the VPN access.
Identity Certificate	Enter the credentials to authorize end users for the VPN connection (if Certificate is selected as machine authentication).
Shared Secret	Enter the Shared Secret key to be provided to authorize end users for the VPN connection (if Shared Secret is selected as machine authentication).

6. Select either **Manual** or **Automatic** proxy and the appropriate settings.
7. Select **Save & Publish** when you are finished to push the profile to devices.

Configure a VPN On Demand Profile (macOS)

VPN on demand is the process of automatically establishing a VPN connection for specific domains. For increased security and ease of use, VPN on demand uses certificates for authentication instead of simple passcodes.

To distribute certificates through the UEM console during configuration and set up of VPN on demand:

1. Ensure your certificate authority and certificate templates in the Workspace ONE UEM are properly configured for certificate distribution.
2. Make your third-party VPN application of choice available to end users by pushing it to devices or recommending it in your enterprise App Catalog.
3. Navigate to **Devices > Profiles & Resources > Profiles** and select **Add**. Select Apple macOS, and then select whether this profile will apply to only the enrollment user on the device (**User Profile**), or the entire device (**Device Profile**).
4. Configure the profile's **General** settings.

5. Select the **VPN** payload and configure settings as outlined above.
6. Specify the Connection Info for a connection type that supports certificate authentication: IPSec (Cisco), F5 SSL, Custom SSL, or F5 Access.
   - **Server** – Enter the hostname or IP address of the server for connection.
   - **Account** – Enter the name of the VPN account.
7. **Authentication** – Select a certificate to authenticate the device.
8. **Identity Certificate** – Select the appropriate credentials.
9. **Include User PIN** – Select this check box to ask the end user to enter a device PIN.
10. Check the **Enable VPN On Demand** box. **Add** the **Domains**, and choose the **On-Demand Action.**
    - **Always Establish** – Initiates a VPN connection regardless of whether the page can be accessed directly or not.
    - **Never Establish** – Does not initiate a VPN connection for addresses that match the specified the domain. However, if the VPN is already active, it may be used.
    - **Establish if Needed** – Initiates a VPN connection only if the specified page cannot be reached directly.

    Important: For wildcard characters, do not use the asterisk (*) symbol. Instead, use a dot in front of the domain. For example, .air-watch.com.
11. Select **Save and Publish**. After the profile installs on a user's device, a VPN connection prompt will automatically display whenever the user navigates to a site that requires it, such as SharePoint.

Configure an Email Profile (macOS)

Configure an email profile for macOS devices to configure email settings on the device.

1. Navigate to **Devices > Profiles & Resources > Profiles** and select **Add**. Select Apple macOS, and then select **User Profile**, since email settings can only apply to a single user.
2. Configure the profile's **General** settings.
3. Select the **Email** payload.

4. Configure **Email** settings, including:

Settings	Description
Account Description	Enter a brief description of the email account.
Account Type	Use the drop-down menu to select either IMAP or POP.
Path Prefix	Enter the name of the root folder for the email account (IMAP only).
User Display Name	Enter the name of the end user.
Email Address	Enter the address for the email account.
Incoming Mail	
Host Name	Enter the name of the email server.
Port	Enter the number of the port assigned to incoming mail traffic.
Username	Enter the username for the email account.
Authentication Type	Use the drop-down menu to select how the email account holder is authenticated.
Password	Enter the password required to authenticate the end user.
Use SSL	Select this check box to enable Secure Socket Layer usage for incoming email traffic.
Outgoing Mail	
Host Name	Enter the name of the email server.
Port	Enter the number of the port assigned to incoming mail traffic.
Username	Enter the username for the email account.
Authentication Type	Use the drop-down menu to select how the email account holder is authenticated.
Outgoing Password Same As Incoming	Select this to auto-populate the password field.
Password	Enter the password required to authenticate the end user. Select **Show Character**s if you want users to see characters as they type.
Use SSL	Select this check box to enable Secure Socket Layer usage for incoming email traffic.

5. Select **Save & Publish** when you are finished to push the profile to devices.

Configure an Exchange Web Services Profile (macOS)

An Exchange Web Services profile allows the end user to access corporate email infrastructures and Microsoft Outlook accounts from the device.

Note: This payload is fully supported on macOS v.10.9 and higher, however, macOS will only configure Contacts when this is installed on v10.7 and v10.8.

To create an Exchange Web Services profile:

1. Navigate to **Devices > Profiles & Resources > Profiles** and select **Add**. Select Apple macOS, and then select **User Profile**, since email settings can only apply to a single user.
2. Configure the profile's **General** settings.
3. Select the **Exchange Web Services** payload.
4. Configure **Exchange Web Services** settings including:

Setting	Description
Email Client	Configure the native mail client or Microsoft Outlook on the device. Outlook requires AirWatch Agent v.1.1.0+ to be installed on the device.
Account Name	Enter the name for the EWS account.
Exchange Host	Enter the name of the Exchange host. This option appears when **Microsoft Outlook** is selected.
Exchange Port	Enter the port number for the Exchange Host. This option appears when **Microsoft Outlook** is selected.
Use SSL	Select to enable Secure Socket Layer usage for communication. This option appears when **Microsoft Outlook** is selected.
Delete all user data when profile is removed	Select to erase all user information, mail, settings, and accounts in Outlook, whether the user is managed or unmanaged. This option appears when **Microsoft Outlook** is selected. **Caution:** Do not make this selection if deploying to a personal computer. This forces Outlook to quit and deletes all information from the computer's Microsoft User Data folder.
Login Information	
Username	Enter the username for the email account.
Email Address	Enter the email address for the email account.
Full Name	Enter the first and last name associated with the account. This option appears when **Microsoft Outlook** is selected.
Password	Enter the password required to authenticate the end user.
Payload Certificate	Select the certificate upload for EAS use. This option appears when **Native Mail Client** is selected.
Domain	Enter the domain for the email account. This option appears when **Microsoft Outlook** is selected.

5. Configure more options for **Native Mail Client**:

Setting	Description
Internal Exchange Host	The name of the secure server for EAS use. This option and following appear when **Native Mail Client** is selected.

Setting	Description
Port	Enter the number of the port assigned for communication with the internal Exchange host.
Internal Server Path	The location of the secure server for EAS use.
Use SSL For Internal Exchange Host	Select this check box to enable Secure Socket Layer (SSL) usage for communication with the Internal Exchange Host.
External Exchange Host	The name of the external server for EAS use.
Port	Enter the number of the port assigned for communication with the External Exchange Host.
External Server Path	The location of the external server for EAS use.
Use SSL For External Exchange Host	Select this check box to enable Secure Socket Layer (SSL) usage for communication with the External Exchange Host.

6. Configure **Directory Services** for **Microsoft Outlook.**

Settings	Description
Directory Server	Enter the location of the secure server.
Directory Server Port	Enter the port number of the secure server.
Search Base	Enter the search base of the secure server.
Directory Server Requires SSL	Select this check box if the directory server requires Secure Socket Layer (SSL).

7. Select **Save & Publish** when you are finished to push the profile to devices.

Configure an LDAP Profile (macOS)

An LDAP profile allows end users to access and integrate with your corporate LDAPv3 directory information.

1. Navigate to **Devices > Profiles & Resources > Profiles** and select **Add**. Select Apple macOS, and then select **User Profile**, since these settings can only apply to a single user.
2. Configure the profile's **General** settings.
3. Select the **LDAP** payload.

4. Configure LDAP settings:

Setting	Description
Account Description	Enter a brief description of the LDAP account.
Account Hostname	Enter/view the name of the server for Active Directory use.
Account Username	Enter the username for the Active Directory account.
Account Password	Enter the password for the Active Directory account.
Use SSL	Select this check box to enable Secure Socket Layer usage.
Search Settings	Select **Add** and enter settings for Active Directory searches executed from the device.

5. Select **Save & Publish** when you are finished to push the profile to devices.

Configure a CalDAV or CardDAV Profile (macOS)

Configure a CalDAV or CardDAV profile to allow end users to sync corporate calendar items and contacts. To create these profiles:

1. Navigate to **Devices > Profiles & Resources > Profiles** and select **Add**. Select Apple macOS, and then select **User Profile**, since email settings can only apply to a single user.
2. Configure the profile's **General** settings.
3. Select the **CalDAV or CardDAV** payload.
4. Configure CalDAV or CardDAV settings, including:

Setting	Description
Account Description	Enter a brief description of the account.
Account Hostname	Enter/view the name of the server for CalDAV use.
Port	Enter the number of the port assigned for communication with the CalDAV server.
Principal URL	Enter the web location of the CalDAV server.
Account Username	Enter the username for the Active Directory account.
Account Password	Enter the password for the Active Directory account.
Use SSL	Select this check box to enable Secure Socket Layer usage.

5. Select **Save & Publish** when you are finished to push the profile to devices.

Configure a Web Clips Profile

Web Clips are web bookmarks that you can push to devices that display as icons and point to commonly used or recommended web resources.

To deploy a Web Clip:

1. Navigate to **Devices > Profiles & Resources > Profiles** and select **Add**. Select **Apple macOS**, and then select **User Profile.**
2. Configure the profile's **General** settings.
3. Select the **Web Clips** payload.
4. Configure Web Clip settings, including:

Setting	Description
Label	Enter the text displayed beneath the Web Clip icon on an end user's device. For example: "AirWatch Self-Service Portal."
URL	Enter the URL the Web Clip that will display. Below are some examples for Workspace ONE UEM pages: • For the SSP, use: **https://<AirWatchEnvironment>/mydevice/**. • For the app catalog, use: **https://<Environment>/Catalog/ViewCatalog/{SecureDeviceUdid}/{DevicePlatform}**. • For the book catalog, use: **https://<Environment>/Catalog/BookCatalog?uid={DeviceUid}**
Icon	Select this option to upload as the Web Clip icon. Upload a custom icon using a .gif, .jpg, or .png format, for the application. For best results, provide a square image no larger than 400 pixels on each side and less than 1 MB in size when uncompressed. The graphic is automatically scaled and cropped to fit, and converted to .png format if necessary. Web Clip icons are 104 x 104 pixels for devices with a Retina display or 57 x 57 pixels for all other devices.
Show in App Catalog	Select this option to list the application in your App Catalog.

5. Select **Save & Publish** when you are finished to push the profile to devices.

Configure a SCEP/Credentials Profile (macOS)

Even if you protect your corporate email with Wi-Fi and VPN with strong passcodes and other restrictions, your infrastructure still remains vulnerable to brute force and dictionary attacks or employee error. For greater security, you can implement digital certificates to protect corporate assets.

To do this, you must first define a certificate authority. Then configure a **Credentials** payload alongside your **Exchange Web Service**, **Wi-Fi**, or **VPN** payload. Each of these payloads has settings for associating the certificate authority defined in the Credentials payload.

To push certificates down to devices, you need to configure a **Credentials** or **SCEP** payload as part of the profiles you created for EAS, Wi-Fi and VPN settings. Use the following instructions to create a credentials payload:

1. Navigate to **Devices > Profiles & Resources > Profiles > Add > Add Profile**. Select Apple macOS, and then select whether this profile will apply to only the enrollment user on the device (**User Profile**), or the entire device (**Device Profile**).

2. Configure the profile's **General** settings.
3. Select either the **Exchange Web Services**, **Wi-Fi** or **VPN** payload to configure. Configure the payload you selected.
4. Select the **Credentials** (or **SCEP**) payload and **Upload** a certificate or select **Defined Certificate Authority** from the Credential Source drop-down and select the **Certificate Authority** and **Certificate Template** from their respective drop-downs.
5. Navigate back to the previous payload for Exchange Web Services, Wi-Fi or VPN. Specify the Identity Certificate in the payload:
   - **Exchange Web Service** – Select the **Payload Certificate** under Login Information.
   - **Wi-Fi** – Select a compatible **Security Type** (WEP Enterprise, WPA/WPA2 Enterprise or Any (Enterprise)) and select the **Identity Certificate** under Authentication.
   - **VPN** – Select a compatible **Connection Type** (for example, CISCO AnyConnect, F5 SSL) and select **Certificate** from the machine/User Authentication drop-down. Select the **Identity Certificate**.
6. Return to the Credentials payload and choose the following allowances:
   - **Allow access to all applications** – Select whether to allow or prevent applications to access the certificate in the Keychain. When this option is enabled, it is not required for the end users to explicitly select the 'allow access to all applications' to access the installed SCEP Certificate and enter credentials to grant access.
   - **Allow export from the Keychain** – Select whether to allow or prevent users from exporting the private key from the installed certificate.
7. Select **Save and Publish**.

Configure a Dock Profile (macOS)

Configure a Dock profile to manage the look and feel of the dock and the applications that will display on it. Configuring Dock settings from the Console allows for additional control of the users' devices by determining whether or not the users can adjust their own settings later.

To create a Dock profile:

1. Navigate to **Devices > Profiles & Resources > Profiles** and select **Add**. Select Apple macOS, and then select whether this profile will apply to only the enrollment user on the device (**User Profile**), or the entire device (**Device Profile**).
2. Configure the profile's **General** settings.
3. Select the **Dock** payload.
4. Configure **Size & Position** settings, including;

Setting	Description
Dock Size	Use the scale to determine the desired size for the Dock.
Allow user to adjust Dock Size	Allow or prevent users from modifying their own Dock Size settings on their devices.

Setting	Description
Magnification	Use the scale to determine the desired magnification for the Dock.
Allow user to adjust Magnification	Allow or prevent users from modifying their own Magnification settings on their devices.
Position	Use the drop-down menu to select the position of the Dock on the screen.
Allow user to adjust Dock Position	Allow or prevent users from modifying their own Dock Position settings on their devices.

5. Configure **Items** settings, including;

Setting	Description
Dock Applications	Select **Add** to specify applications to appear on the Dock.
Dock Items	Select **Add** to specify files and folders to appear on the Dock.
Add Other Folders	Configure folder for My Applications, Documents, and Network Home in the Dock
Allow user to adjust Dock Applications and Items	Allow or prevent users from modifying their own Dock Applications settings on their devices.

6. Configure **Options** settings, including;

Setting	Description
Minimize Using	Select either **Genie** or **Scale** animation for minimizing the Dock.
Allow user to adjust Minimize effect	Allow user to adjust Minimize effect
Minimize Window Into Application Icon	Select this to create an icon to represent an open window in the Dock when the window is minimized.
Allow user to adjust Minimize into Application icon	Allow or prevent users from modifying their own Minimize windows settings on their devices.
Animate Opening Application	Enable animation when launching an application from the Dock.
Allow user to adjust Animate Opening Application	Allow or prevent users from modifying their own animation settings on their devices.

7. Select **Save & Publish** when you are finished to push the profile to devices.

Configure a Restrictions Profile (macOS)

Use restrictions to secure native functionality on macOS devices, protect corporate information and enforce data-loss prevention. Restriction profiles limit how employees can use their macOS devices and provide the control needed to effectively lock down a device if necessary.

To create a restrictions profile:

1. Navigate to **Devices > Profiles & Resources > Profiles** and select **Add**. Select Apple macOS, and then select whether this profile will apply to only the enrollment user on the device (**User Profile**), or the entire device (**Device Profile**).

2. Configure the profile's **General** settings.
3. Select the **Restrictions** payload.
4. Configure **Preferences** restrictions:

Setting	Description
Restrict System Preferences panes	Select to view and edit the system preference restrictions options (such as Accessibility, App store, Bluetooth, CDs and DVDs, Date & Time, Desktop & Screen Saver, Dictation & Speech, Displays, Dock, Energy Saver, Extensions, Fibre Channel, Flash Player, iCloud, Ink, Internet Accounts, Keyboard, Language & Region, Mission Control, MobileMe, Mouse, Network, Notifications, Parent Controls, Printers & Scanners, Profiles, Security & Privacy, Sharing, Software Update, Sound, Spotlight, Startup Disk, Time Machine, Trackpad, Users and Groups, and Xscan).
Enable selected items	Select to restrict functionality. Then, make restriction selections below.
Disable selected items	Select to allow the preferences. Then, make the selections below.

5. Configure **Application** restrictions:

Setting	Description
Game Center	Select options to restrict or allow the use of Game Center.
Safari	Restrict or allow the use of AutoFill when using Safari to prevent autofilling web forms or storing login information or iCloud Keychain details.
App Store	Restrict or allow the use of the App Store, app store adoption, and use of passwords to install updates. When the **Restrict App Store to Software Updates** is enabled, this prevents third-party app updates from the App Store
Apple Music	Select **Allow Music Service** to permit users to stream music from Apple Music to their devices.
Launch Restrictions	Choose to restrict applications from launching. Use the **Add** buttons to specify allowed applications, allowed folders and disallowed folders.

6. Configure **Widgets** restrictions:

Setting	Description
Allow only configured widgets	Select to allow widgets. Click the **Add** button to specify allowed device widgets.

7. Configure **Media** restrictions:

Setting	Description
Network Access	Allow or restrict network access for AirDrop.
Hard Disk Media Access	Determine what media formats are allowed, require authentication and read-only access for the end user. You can also force to **auto-eject media** at log out.

8. Configure **Sharing** restrictions:

Setting	Description
Restrict which sharing services are enabled	Select which Sharing services, such as AirDrop, Facebook, and Twitter, are enabled on the device. You can also select the **Automatically enable new sharing services** check box as a restriction.

9. Configure **Functionality** restrictions:

Setting	Description
Lock desktop picture	Select to prevent changing the desktop picture.
Desktop picture path	Enter the path for the desktop picture. Leaving the path blank will lock the current desktop picture and prevent it from being changed.
Camera	Restrict or allow the use of the built-in camera. When this is restricted all applications, whether native or enterprise, are unable to access the camera.
iCloud	Restrict or allow the use of iCloud functions. • Allow iCloud documents and data • Allow use of iCloud password for local accounts • Allow backup to My macOS iCloud service • Allow Find My Mac iCloud service • Allow iCloud Bookmark sync • Allow iCloud Mail services • Allow iCloud Calendar services • Allow iCloud Reminder services • Allow iCloud Address Book services • Allow iCloud Notes services • Allow iCloud Keychain sync • Allow iCloud Desktop & Documents Services
Content Caching	Select to allow end users to enable Content Caching on their devices (macOS 10.13 and higher).
Spotlight	Restrict or allow the use of Spotlight suggestions when using Spotlight for searching.

10. Select **Save & Publish** to push the profile to devices. The addition or removal of some **Restrictions** profile payloads may not take effect until the target application or utility is restarted on the device.

Configure a Software Update Server Profile (macOS)

A software update server profile allows you to specify the update server that will be tied to the device for all versioning and update control.

Use this to connect to a macOS server with the AirWatch Agent and configure schedules that actively check and perform updates much more frequently that the system does. If needed, connect to a corporate server to perform updates. Either way, this profile provides a simple solution for managing software updates, restart options and notification updates for end users.

Note: Software update profile only updates minor software update patches and not major software updates.

To create a software update server profile:

1. Navigate to **Devices > Profiles & Resources > Profiles** and select **Add**. Select Apple macOS, and then select **Device Profile**, since this profile is only applicable to the entire device.
2. Configure the profile's **General** settings.
3. Select the **Software Update** payload.
4. Configure Software Update settings:

Setting	Description
Update Source	Choose a server to configure communication with the client computers' .plist. If choosing **Corporate SUS**, enter the hostname of the server (for example, **http://server.net:8088/index.sucatalog**.)
Install macOS updates	Select how and when to check for and control updates. • **Install Updates Automatically:** downloads and installs all updates; sends notifications to the end user. • **Download Updates in Background:** downloads the updates; sends notifications; the end user installs updates when ready. • **Check for updates only:** checks for updates and sends notifications to the end user; the user downloads and installs the updates. • **Don't Automatically Check for Updates:** turns off the ability to update software; monitors .plist settings to match profile only.
Choose Updates	Choose updates to send to the computer. • **Choose All:** sends all updates including Apple updates. • **Recommended only:** sends only security updates.
Allow installation of macOS beta releases	Select this check box to allow beta releases on the server. This option may be best for testing environments only. This does not require the AirWatch Agent.
Install app updates	Select to allow app updates.

Setting	Description
Notify the user updates are installing	Send the end user notifications about receiving updates on the device.
Schedule	Schedule updates with the AirWatch Agent, • **Configure Update Interval**: choose how often to check for updates in two-hour increments. • **Update a Specific Time**: choose specific days and times to check for updates. Choose times to control updates when there are concerns about use during peak business hours or band-width utilization
Force Restart (if required)	Automatically restart the computer if required to complete the software update. • **Grace Period** – Choose to defer a reboot for a certain period of time. After this time expires, the computer automatically reboots. • **Allow user to defer** – Enable the user to choose to defer re-starting the computer for a certain period of time. ◦ **Defer time** – Chose how often to prompt the user to re-start the computer after deferment. After each allowed deferment, a message appears prompting the user to re-start the computer. ◦ **Max number of defers** – Choose how many times the user can defer from re-starting the computer before it is automatically re-started to complete the update process.

5. Determine options if updates are installed automatically.
   - **Force Restart (if required)** – Automatically restart the computer if required to complete the software update.
   - **Grace Period** – Choose to defer a reboot for a certain period of time. After this time expires, the computer automatically reboots.
   - **Allow user to defer** – Enable the user to choose to defer re-starting the computer for a certain period of time.
     - **Defer time** – Chose how often to prompt the user to re-start the computer after deferment. After each allowed deferment, a message appears prompting the user to re-start the computer.
     - **Max number of defers** – Choose how many times the user can defer from re-starting the computer before it is automatically re-started to complete the update process.
6. Select **Save & Publish** when you are finished to push the profile to devices.

Configure a Parental Controls Profile (macOS)

A parental control profile manages settings that limit profanity, blacklist or whitelist specific URLs, time allowances and curfews.

To create a parental controls profile:

1. Navigate to **Devices > Profiles & Resources > Profiles** and select **Add**. Select Apple macOS, and then select whether this profile will apply to only the enrollment user on the device (**User Profile**), or the entire device (**Device Profile**).
2. Configure the profile's **General** settings.
3. Select the **Parental Controls** payload.
4. Configure **Content Filter** settings , including:

Setting	Description
Enable use of Dictation	Select this check box to allow user access to Dictation feature
Hide Profanity in Dictionary and Dictation	Select this check box to remove profane terminology.
Limit Access To Websites By	Select this check box to enable web restrictions. Then, select the applicable radio button for your desired restriction and add blacklisted and whitelisted URLs as needed.

5. Configure **Time Limits** settings:

Setting	Description
Enforce Limit	Select this check box to enable time limit restrictions.
Allowances	Select the applicable check boxes to set allowed device usage to either weekdays or weekends and use the drop-down menus to specify time limits for daily device usage.
Curfews	Select the applicable check boxes to prevent the end user from accessing the device during weekdays or weekends and use the drop-down menus to set specific time frames when device usage is not allowed.

6. Select **Save & Publish** when you are finished to push the profile to devices.

Configure a Directory Profile (macOS)

By binding a device to the directory service, the device comply with any domain policies and password security settings. You may bind a single device to multiple directories by sending multiple directory service profiles.

To create a directory profile for your devices:

1. Navigate to **Devices > Profiles & Resources > Profiles** and select **Add**. Select Apple macOS, and then select **Device Profile**, since this profile is only applicable to the entire device.
2. Configure the profile's **General** settings.
3. Select the **Directory** payload. Then, choose the **Directory Type**, Open Directory or Active Directory.

Note: If multiple profiles enforce separate policies on a single device, the most restrictive policy is enforced. If your password policy is being managed by your directory for network users logging into the devices, Workspace ONE UEM does not recommend a passcode policy.

4. Choose **Authentication** settings including:

Setting	Description
Directory Type	Choose **Active Directory** or **Open Directory or LDAP** from the drop-down menu
Server Hostname	Enter the directory server name.
Username and Password	Enter the credentials of the administrator used to authenticate and bind the device to the server. Administrator credentials should not include the domain. Use "administrator" only, do not use "domain\administrator."
Client ID	Enter the identifier associated with the device in the directory. Enter the Client ID in a format that is allowed by the directory you're attempting to bind. Workspace ONE UEM recommends using {SerialNumber}. Other lookup values (device asset number, etc.) may not generate computer names that comply with Netbios Naming Conventions.

5. Choose **User Experience** settings for Active Directory Accounts:

Setting	Description
Configure a mobile account at login	Select this option to create a mobile account. When this option is selected, the users' data is stored locally and they are automatically logged into a mobile account.
Require confirmation	Send a confirmation message to the end user.
Use UNC path	Select to determine the UNC specified in the Active Directory when mounting the network home.
Mount	Choose either the **AFP** or **SMB** protocols.
Default user shell	Specify the default shell for the user after logging into the computer.

6. Select the **Mappings** tab to specify an attribute to be used for equivalent acronym (GID). By default these are derived from the domain server.

7. Select **Administrative** tab and configure settings including:

Setting	Description
Group Names	Specify groups to determine who has local administrative privileges on the computer.
Preferred domain server	Enter the name of the domain server.
Namespace	Select the primary account naming convention based on **forest** or **domain**.
Packet signing	Choose how to ensure data is secure.

Setting	Description
Packet Encryption	Choose to encrypt data.
Password trust interval	Set to determine how often the computer trust is updated.
Restricts DDNS	Add interfaces to specify updates. Use the format: en0, en1, en2 etc.

8. Select **Save & Publish** to push the profile to the device.

Configure a Security and Privacy Settings Profile (macOS)

The security and privacy settings profile lets you configure Apple's Gatekeeper functionality settings, which are used for secure application downloads. Gatekeeper also controls specific settings related to user passwords.

To create a security and privacy profile:

1. Navigate to **Devices > Profiles & Resources > Profiles** and select **Add**. Select Apple macOS, and then select whether this profile will apply to only the enrollment user on the device (**User Profile**), or the entire device (**Device Profile**).
2. Configure the profile's **General** settings.
3. Select the **Security and Privacy** payload.
4. Choose locations from which apps may be downloaded.
5. Configure OS Updates settings to perform a force delay in updating OS especially from updates being visible to end user for a specified number of days.

Setting	Description
Delay Updates (Days)	Enable this option and specify the number of days to delay the software update. Number of days range from 1 to 90. (macOS 10.13.4+ devices). The number of days dictate the length of time after the release of the software update and not after the time of installation of the profile.

6. Configure **Gatekeeper** settings.

Setting	Description
Gatekeeper	Choose to restrict which types of applications may be downloaded. The available options are: • Mac App Store • Mac App Store and identified developers • Anywhere
Do not allow user to override Gatekeeper setting	Select to prevent the user from modifying settings to Gatekeeper.

7. Configure **Security** settings.

Setting	Description

Allow Apple Watch to Unlock	Select to allow Apple Watch to unlock a paired macOS device (macOS 10.12 and higher).
Allow Touch ID to Unlock	Select to allow Touch ID to unlock a macOS device (macOS 10.12.4 and higher).
Allow user to change Password	Select to allow end users to change their passwords (macOS 10.9+).
Require password after sleep or screensaver begins	Select to require a password after sleep or screen saver begins. Set the grace period to determine when a password should be entered.
Allow user to set lock message	Select to allow end users to set a lock message on their devices (macOS 10.9+).

8. Configure **Privacy** settings to automatically send diagnostic and usage data to Apple.
9. Select **Save & Publish** when you are finished to push the profile to devices.

Configure a Full Disk Encryption Profile (macOS)

Configure encryption on macOS 10.8 with the AirWatch Agent and this profile.

If you are using macOS 10.9 +, configure disk encryption by simply pushing this profile, whether or not the AirWatch Agent is installed. Other Workspace ONE UEM enhancements with 10.9 + include role-based access for recovery keys and the ability to audit who views recovery keys and when.

Important: If you have upgraded console to the latest version 9.3, you have to re-edit and re-publish the disk encryption profile to the device (10.13+) to utilize the recovery key management features of Workspace ONE UEM.

To configure a disk encryption profile:

1. Navigate to **Devices > Profiles & Resources > Profiles** and select **Add**. Select Apple macOS, and then select **Device Profile**, since this profile is only applicable to the entire device.
2. Configure the profile's **General** settings.
3. Select the **Disk Encryption** payload.
4. Configure Disk Encryption settings, including:

Setting	Description
OS Version	Select the appropriate OS version.
Enforce Disk Encryption	Select this check box to enable disk encryption on the device.
Recovery Key Type	Choose the type of recovery key required to decrypt the disk. The options are Personal, Corporate, Personal and Corporate.
File Vault Enterprise Certificate	If configuring **Corporate** or **Personal and Corporate**, choose a certificate for disk encryption that was uploaded through the Credentials payload. For detailed information on using certificates with the Disk Encryption profile, see Full Disk Encryption with FileVault section.

Setting	Description
Store Recovery Key in Workspace ONE UEM	Select this check box to retain the recovery key on the Workspace ONE UEM server. If not selected, choose a **Recovery Key Redirection URL** and **Recovery Key Encryption Certificate** to store the recovery key elsewhere. For more information on recovery keys, see the configuration profile reference guide in the Apple Developer portal.
Require Reboot	Select this check box to force the device to reboot and finish disk encryption. (Agent only) **Note:** If not selected on 10.8 computers, end users are still prompted, but not forced, to reboot the device to complete the encryption process. If not selected on 10.9 + computers, users are not prompted for disk encryption until they log out of the user account.
Require user to unlock the disk after hibernation	Select this to require a password to unlock the disk after hibernation and restore the state of the disk when it was last saved. Workspace ONE UEM recommends this for encryption.

5. Select **Save & Publish** when you are finished to push the profile to devices.

Important: Disk encryption will fail and error out if no CoreStorage logical volume groups are found. This can be determined by running command `diskutil cs list` on an unencrypted device without File Vault 2. If no CoreStorage Volumes are found, the drive needs to be re-formatted using File Vault 2.

Configure a Login Items Profile (macOS)

A Login Items profile enables you to control the behavior of the users' devices when they launch.

To create a Login Items profile:

1. Navigate to **Devices > Profiles & Resources > Profiles** and select **Add**. Select Apple macOS, and then select whether this profile will apply to only the enrollment user on the device (**User Profile**), or the entire device (**Device Profile**).
2. Configure the profile's **General** settings.
3. Select the **Login Items** payload.

4. Configure Login Items settings, including:

Setting	Description
Applications	Specify which applications to launch at login. Enter the full path of the application, for example, /Applications/Contacts.app.
Files and Folders	Specify which files and folders to launch at login. Enter the full path of the file or folder.
Authenticated Network Mounts	Specify which network mounts to authenticate with the user's login name and password. Use Active Directory (AD) credentials for user login. Enter the full mount path and volume, including protocol, for example, smb://server.example.com/volume.
Network Mounts	Specify which volumes to mount at login. Use AD credentials for user login. Enter the full mount path and volume including protocol, for example, smb://server.example.com/volume.
Add network home SharePoint	Select this to enable network home SharePoint configuration on the device.
User may press shift to prevent items from opening	Select this to allow the user to hold shift upon login to prevent items from opening.

5. Select **Save & Publish** when you are finished to push the profile to devices.

Configure a Login Window Profile (macOS)

Configure the Login Window profile to control the look and feel of the login window, including options for logging in, and directory user access to the device.

To configure the Login Window profile:

1. Navigate to **Devices > Profiles & Resources > Profiles** and select **Add**. Select Apple macOS, and then select **Device Profile**, since this profile is only applicable to the entire device.
2. Configure the profile's **General** settings.
3. Select the **Login Window** payload.

4. Configure **Login Window** settings using the tabs, including:

Tab	Description
Window	• Show additional information in the menu bar, including host name, macOS version, and IP address when the menu bar is selected. • Enter custom banner message. • Show local user, mobile accounts, network accounts, device admins and "other" information. • Show device power options, including Shut Down, Restart and Sleep.
Options	• Show password hint and set amount of retries before hint is shown, if available. • Enable automatic login, console access, Fast User Switching • Log out users, enable computer admin to refresh or disable management. • Set computer name to computer record name, enable external accounts, allow guest user. • Set screen saver to start and set actual screen saver.
Access	• Allow or deny specific user accounts from accessing device. • Allow local-only users to log-in; use available workgroup settings and nesting • Combine available work group settings and always show work group dialog during login **Note:** This only works with Directory Users, not local users on the device. The device must be bound to the same directory that Workspace ONE UEM is pulling users from.)
Scripts	• Set EnableMCXLoginScripts to TRUE. • Set MCXScriptTrust to match the binding settings used to connect the client computer to the directory domain.

5. Select **Save & Publish** when you are finished to push the profile to devices.

Configure an Energy Saver Profile (macOS)

An Energy Saver profile enforces the settings for when the computer should sleep and configure wake options.

To create an Energy Saver profile:

1. Navigate to **Devices > Profiles & Resources > Profiles** and select **Add**. Select Apple macOS, and then select **Device Profile**, since this profile is only applicable to the entire device.
2. Configure the profile's **General** settings.
3. Select the **Energy Saver** payload.

4. Configure Energy Saver settings, including:

Setting	Description
Desktop	• **Sleep Options** – Set the length of time for the computer or display to go to sleep. • **Wake Options** – Set when the computer will wake depending on Ethernet network administrator access, pressing the power button and automatically after a power failure.
Laptop	Laptop power options are identical to desktop power options. Configure specific configurations when the laptop is using battery power or when connected to a power adapter.
Schedule	Set the computer to start up or go to sleep at specific times. Also set unique schedules depending on weekday, specific day and any day.

5. Select **Save & Publish** when you are finished to push the profile to devices. If you push a laptop profile to a desktop device, or vice versa, the profile is ignored by the receiving device.

Configure a Time machine Profile (macOS)

By creating a Time machine profile you can specify a backup server location used to mount and backup the device.

To create a Time machine profile:

1. Navigate to **Devices > Profiles & Resources > Profiles** and select **Add**. Select Apple macOS, and then select **Device Profile**, since this profile is only applicable to the entire device.
2. Configure the profile's **General** settings.
3. Select the **Time machine** payload.
4. Configure **Time machine** settings, including:

Setting	Description
Backup all volumes	Secure all volumes associated with the device. By default, only the startup volume is backed up.
Backup system files and folders	Secure all system files and folders, which are skipped by default.
Enable automatic backup	Back up the system automatically at determined intervals.
Enable local snapshots (10.8+)	Configure local backup snapshots when device is not connected to the network.
Backup size limit	Set a maximum size allowed to backup the system. Enter 0 (zero) to set unlimited.
Paths to backup	Choose specific filepaths to backup, in addition to the default startup volume.
Paths to skip	Choose specific filepaths to skip during backup from the startup volume.

5. Select **Save & Publish** when you are finished to push the profile to devices.

Once the profile is pushed to the device, the login user's network credentials are used to configure the system keychain for the backup volume defined in the profile. The backup volume will not mount using a local account because network

credentials are required at login to authenticate the drive. After the system keychain is configured the first time, all backups from that computer will be associated with the original user's backup volume.

Configure a Finder Profile (macOS)

A Finder profile controls general settings related to what end users can see on their devices and the actions they are allowed to perform.

To create a Finder profile:

1. Navigate to **Devices > Profiles & Resources > Profiles** and select **Add**. Select Apple macOS, and then select whether this profile will apply to only the enrollment user on the device (**User Profile**), or the entire device (**Device Profile**).
2. Configure the profile's **General** settings.
3. Select the **Finder** payload.
4. Configure settings on the **Preferences**, including:

Setting	Description
Use Regular Finder/Use Simple Finder	Allow user to access either Regular Finder or Simple Finder as a default.
Hard Disk	Show the device's Hard Disk icon on the Desktop.
External Disk	Show any connected external disk icons on the Desktop.
CDs, DVDs, and iPods	Show any inserted media icons on the Desktop.
Connected Server	Show any connected servers icons on the Desktop.
Show warning before emptying the Trash	Present user with prompt before emptying the Trash.

5. Configure settings on the **Commands**, including:

Setting	Description
Connect to server	Allow users to open a dialog box and find servers on a network.
Eject	Allow users to eject removable media and mountable volumes.
Burn Disc	Allow users to write permanent information to a CD or DVD.
Go to Folder	Allow users to open files or folders by typing the path name.
Restart	Allow users to access the restart command from the Apple Menu.
Shut Down	Allow users to access the shutdown command from the Apple Menu.

6. Select **Save & Publish** when you are finished to push the profile to devices.

Configure an Accessibility Profile (macOS)

Configure accessibility options for end users by creating an Accessibility profile.

To create an Accessibility profile:

1. Navigate to **Devices > Profiles & Resources > Profiles** and select **Add**. Select Apple macOS, and then select whether this profile will apply to only the enrollment user on the device (**User Profile**), or the entire device (**Device Profile**).
2. Configure the profile's **General** settings.
3. Select the **Accessibility** payload.
4. Configure options for **Seeing**, including:

Setting	Description
Zoom Options	Enable zoom function using scroll wheel and keyboard, set max/min zoom, smooth images and show preview rectangle when zoomed out.
Display Options	Invert colors, use grayscale, enhance contrast and set cursor size to normal, medium, large or extra large.
Voiceover Options	Enable voiceover for the device.

5. Configure options for **Hearing**, including:

Setting	Description
Flash the screen when an alert occurs	Enable flashing for alerts.
Play stereo audio as mono	Allow stereo to play as mono

6. Configure options for **Interaction**, including:

Setting	Description
Sticky Keys	Enable Sticky Keys, beep when a modifier is set and display pressed keys on screen.
Slow Keys	Enable Slow Keys, use click key sounds and set key acceptance delay.
Mouse Keys	Enable Mouse Keys, set initial delay and max speed, and ignore device's built-in trackpad

7. Select **Save & Publish** when you are finished to push the profile to devices.

Configure a Printer Configuration Profile (macOS)

By creating a Printer configuration profile you can tell devices which default printer to use and set printer access and footer options.

To create a Printer configuration profile:

1. Navigate to **Devices > Profiles & Resources > Profiles** and select **Add**. Select Apple macOS, and then select whether this profile will apply to only the enrollment user on the device (**User Profile**), or the entire device (**Device Profile**).
2. Configure the profile's **General** settings.
3. Select the **Printing** payload.
4. Select **Add Printer**. An **Add Printer** window appears.

5. Configure the **Printer** settings including:

Setting	Description
Name	Enter the name of the printer to add.
Printer address	Enter the printer address.
Location	Specify the friendly location name.
Model/Driver	Choose the printer type. • Set model/driver to **Custom** if the printer does not support generic drivers for macOS devices. If using Custom Driver, the driver text must be the exact name, which can be found by locating the configured printer on the computer and copying the Kind listed under the printer description.
Lock printer settings	Force the user to enter an Admin password to access the printer settings.
Advanced	Unlock the PPD file location and enter it.
Default Printer	Select a printer to be the default printer.
Access	
Allow user to modify printer list	Enable end users to modify printers on the device
Allow printers to connect directly to the device	Enable printers to connect automatically. If checked, you can also require admin passcode.
Only show managed printers	Allow end users to view a list of managed printers available to the device.
Footer	
Print page footer	Select this to auto-populate the footer with user information and time of print.
Include macOS Address	Add a macOS address to show the location of the pages that print and specify the font name and size of the footer.
Font Name	Specify the font name.
Font Size	Specify the size of the footer.

6. Select **Save & Publish** when you are finished to push the profile to devices.

Configure a Messages Profile (macOS)

You can create a Messages profile to pre-configure end user laptops to use a Jabber or AOL Instant Messenger (AIM) account. Accounts can be authenticated through SSL certificates or Kerberos. The ability to use Messages applies to User

Profiles only.

To create a Messages Profile:

1. Navigate to **Devices > Profiles & Resources > Profiles** and select **Add**. Select Apple macOS, and then select (**User Profile**) to apply enrollment to the user's device.
2. Configure the profile's **General** settings.
3. Select the **Messages** payload.
4. Configure **Messages** settings for Jabber , including:

Setting	Description
Account Type	Allow user to access either a **Jabber** or **AIM** account.
Account Description	Configure a brief description of the profile that indicates its purpose. This option appears if **AIM** is selected.
Account Name	Enter the name of the account.
User Name	Enter the user name for this account. Use lookup values (for example, {EnrollmentUser} to pull data from the UEM console.
Password	Optionally enter the password required to authenticate the account. Leave it blank to prompt end users to enter their account password.
Host Name	Enter the name of the account server.
Port	Enter the number of the port assigned to the account.
Use SSL	Select this check box to enable Secure Socket Layer (SSL) usage for authentication.
Use Kerberos v5	Select this check box to enable Kerberos v5 usage for authentication.

5. Select **Save & Publish** when you are finished to push the profile to devices.

Configure a Proxy Profile (macOS)

Direct traffic through a designated proxy server for Wi-Fi connections. Choose from multiple proxy connections to properly route traffic depending on your organizations needs and add proxy exceptions as needed.

1. Navigate to **Devices > Profiles & Resources > Profiles** and select **Add**. Select Apple macOS, and then select whether this profile will apply only to the enrollment user on the device (**User Profile**), or to the entire device (**Device Profile**).
2. Configure the profile's **General** settings.
3. Select the **Proxies** payload from the list.
4. Choose **Network Proxies** for systems running macOS 10.11, or choose **Global HTTP Proxy** for legacy support on systems running macOS 10.9 and 10.10.

- For **Network Proxy** settings, choose:

Setting	Description
Auto Proxy Configuration	Choose this and enter the **Proxy PAC File URL** to automatically configure the device to PAC file settings.
Web Proxy (HTTP)	Choose to enable this and enter the **Host Name** and optionally enter the **Port** used to communicate with the proxy. This tells the device to use this proxy for any HTTP traffic.
Secure Web Proxy (HTTPS)	Choose to enable this and enter the **Host Name** and optionally enter the **Port** used to communicate with the proxy. This tells the device to use this proxy for any HTTPS traffic.
FTP Proxy	Choose to enable this and enter the **Host Name** and optionally enter the **Port** used to communicate with the proxy. This tells the device to use this proxy for any FTP traffic.
SOCKS Proxy	Choose to enable this and enter the **Host Name** and optionally enter the **Port** used to communicate with the proxy. This proxy establishes a TCP traffic connection to a device.
Streaming Proxy	Choose to enable this and enter the **Host Name** and optionally enter the **Port** used to communicate with the proxy. This proxy is configured using a RTSP if needed for applications such as AirPlay.
Gopher Proxy	Choose to enable this and enter the **Host Name** and optionally enter the **Port** used to communicate with the proxy. Gopher proxy enables Gopher-based content.

- For **Global HTTP Proxy** settings, choose:

Setting	Description
Proxy Type	Select the type of proxy. Select **Manual** for proxies that require authentication, or **Auto** to specify a Proxy PAC URL.
Proxy PAC File URL	Only required if the proxy type is **Auto**. This option appears when **Auto** is selected.
Proxy Server	Enter the URL of the Proxy Server. This is required if you selected Manual as the proxy type. This option appears when **Manual** is selected.
Proxy Server Port	Enter the port used to communicate with the proxy. This is required if you selected Manual as the proxy type. This option appears when **Manual** is selected.
Proxy Username/Password	If the proxy requires credentials, you can use look-up values to define the authentication method. This is required if you selected Manual as the proxy type. This option appears when **Manual** is selected.

5. Enter **Proxy Exceptions** as needed.
6. Enable or disable **Passive FTP Mode (PASV)**.
7. Select **Save & Publish** when you are finished to push the profile to devices.

Configure a Mobility Profile (macOS)

Mobility profiles allow configuration of portable home directories for network accounts, so users can log into the network even when they are not connected to the network. With a mobility profile, you can also set home and preference sync settings to optionally sync the home folder with a central server.

To create a Mobility profile:

1. Navigate to **Devices > Profiles & Resources > Profiles** and select **Add**. Select **Apple macOS**, and then select whether this profile will apply to only the enrollment user on the device (**User Profile**), or the entire device (**Device Profile**).
2. Configure the profile's **General** settings.
3. Select the **Mobility** payload.
4. Using the **Account Creation** tab, set up the mobile account profile. When this account is set up, a local copy of the user's network home folder is created for use when they are not connected to the network.

Setting	Description
Configure Mobile account	Select to configure the account for the user to log into the network.
Require Confirmation	Select to send a confirmation message to the end user.
Show "Don't ask me again"	Select to allow end users to skip the confirmation message after the initial prompt to create the mobile account.
Configure Home Using	Choose settings to either **Network home and default sync settings** or **Local home template** from the drop-down navigation menu.
Home folder location	Choose either the **on startup volume folder**, at **path** and enter the **path** location on the user's computer where the home folder will reside, or set the location that the **user chooses.**
Encrypt Contents with FileVault	Select to encrypt contents with FileVault. If you choose to enable Encryption, select the following settings: • Select the **Require computer master password** check box to require a master password. • Select **Restrict Size** to restrict the size of the network home quota. Determine a **Fixed Size** with **megabytes** or a **Percentage of the home network quota** and the **Size** of the percentage.

Setting	Description
Delete mobile accounts	Select to determine how and when to delete the account. • Select the **Delete mobile accounts** check box to configure options for deleting the account. • Choose **After** and select how many hours, days or weeks to delete the account after it expires. Setting the value to 0 causes the account to be deleted as soon as the computer is able to delete it. • Select **Delete only after successful sync** to delete the device after it syncs with the central server.

5. Choose the **Rules** tab to configure sync options:

Setting	Description
Preference Sync	Enable syncing for user preferences. Choose when, what folders to sync and items that do not need to be synced. • Select **Merge with User Settings** check box to add or append the user's sync settings. If this is not selected, the user's settings will be wiped when the new settings are applied.
Home Sync	Enable syncing for desktop preferences. Choose when, what folders to sync and items that do not need to synced and may be skipped. • Select **Merge with User Settings** check box to add or append the user's sync settings. If this is not selected, the user's settings will be wiped when the new settings are applied.
Options	Determine how to sync, how often, and allow syncing status to show in Apple Menu bar.

6. Select **Save & Publish** to push the profile to the device.

Configure a Managed Domains Profile (macOS)

Managed domains are another way Workspace ONE UEM enhances Apple's "open in" security feature on macOS computers. Use the "open in" feature and manage email domains to protect corporate data by helping end users verify which emails are sent to corporate accounts.

To configure a Managed Domains profile:

1. Navigate to **Devices > Profiles & Resources > Profiles > Add > Add Profile**. Select **Apple macOS**, and then select whether this profile will apply to only the enrollment user on the device (**User Profile**), or the entire device (**Device Profile**).
2. Configure the profile's **General** settings.
3. Select the **Managed Domains** payload from the list.

4. Enter **Managed Emails Domains** to specify which email addresses are corporate domains. For example: **mdm.company.com**. Emails sent to other domains are highlighted in the email application to indicate that the address is not part of the corporate domain.
5. Select **Save & Publish**.

Configure a VMware Fusion Profile (macOS)

Integrating VMware Fusion with Workspace ONE UEM's MDM capabilities allows businesses to add flexibility to corporate device management with Bring Your Own Laptop (BYOL) solutions.

Push the VMware Fusion profile from the UEM console to allow for management of both the host device and corporate applications. After the VMware Fusion application is installed, these profile settings allow you to manage the application, including applying volume licenses, configuring UI defaults, and other advanced deployment settings. As needed, administrators can quickly remove the VM application when the laptop is unenrolled.

Important: The application cannot be installed until the profile settings are pushed to the device. Even if the VMware Fusion app is available in the app catalog, the VM Fusion profile must be configured to complete integration.

1. Administrators must upload the VMware Fusion application to the UEM console. For more information about application management, see the **VMware Workspace ONE UEM Mobile Application Management (MAM) Guide**.
2. Navigate to **Devices > Profiles & Resources > Profiles > Add > Add Profile > Apple macOS > Device Profile.**
3. Configure the profile's **General** settings.
4. Select the **VMware Fusion** payload.
5. Configure the VMware Fusion settings.

Setting	Description
Volume License	Enter the volume license key for the VMware Fusion software.
UI Defaults	
Prompt EULA	Select this check box to ask end users to agree to the terms of an End User License Agreement at installation.
Prompt Antivirus Check	Select this check box to ask end users to perform an anti-virus check at installation
Prompt Registration	Select this check box to ask end users to register the software at installation.
Prompt Data Collection	Select this check box to ask end users to agree to data collection at installation.
Show License Key Views	Select this check box to view the license key applied to the application.
Software Update	Choose how the application will be updated from the drop-down menu.

Setting	Description
Locations	
App Directory	Choose to change the default location of the VMware Fusion application.
VM Directory	Choose to change the default location of the virtual machine.
Support	
Support URL	Enter the company URL that directs end users to a website for help. By default this will point to standard Fusion help.
Update	Enter the company server name that will send Fusion updates. By default this will point to standard VMware's software server.

6. Configure **Advanced** settings if needed. The only reason to have an explicit entry in this section is to change the name or location of any specific application or virtual machine by entering its name as it is the (including its **.app** extension) as a key and the absolute path to the destination app as its value.
7. Select **Save & Publish** to push this profile to devices.

Configure a Web Content Filter Profile (macOS)

This payload allows you to configure settings and authentication with third-party web content filters.

1. Navigate to **Devices > Profiles & Resources > Profiles > Add > Add Profile**. Select **Apple macOS**, and then select whether this profile will apply to only the enrollment user on the device (**User Profile)**, or the entire device (**Device Profile**)
2. Configure the profile's **General** settings.
3. Select the **Content Filter** payload.
4. In the **Filter Type**, see that **Plug-in** is enabled.
5. Complete the required **Content Filter** information including:

Setting	Description
Filter Name	Enter the name of the filter that displays in the app and on the device.
Identifier	Enter the bundle ID of the identifier of the plug-in that provides filtering service.
Service Address	Enter the hostname, IP address or URL for service.
Organization	Choose the organization string that is passed to the 3rd party plug-in.
Filter WebKit Traffic	Select this check box to choose whether to filter WebKit traffic.
Filter Socket Traffic	Select this check box to choose whether to filter Socket traffic. **Note:** Either WebKit or Socket traffic needs to be enabled in order for the payload to work.

6. Configure the **Authentication** information including:

Setting	Description
User Name	Use look-up values to pull directly from the user account record. Ensure your Workspace ONE UEM user accounts have an email address and email username defined.
Password	Enter the password for this account.
Payload Certificate	Choose the authentication certificate.

7. Add **Custom Data** which includes keys required by the third-party filtering service. This information goes into the vendor config dictionary.

8. Select **Save & Publish**.

Configure an AirPlay Whitelist Profile (macOS)

Configuring the AirPlay payload allows you whitelist a specific set of devices to receive broadcast privileges according to a device ID. Additionally, if the display access to a device is password-protected, you can pre-enter the password to create a successful connection without revealing the PIN to unauthorized parties.

Note: AirPlay whitelisting currently only pertains to macOS Yosemite devices.

1. Navigate to **Devices > Profiles & Resources > Profiles > Add > Add Profile**. Select **Apple macOS**, and then select whether this profile will apply to only the enrollment user on the device (**User Profile**), or the entire device (**Device Profile**).

2. Configure the profile's **General** settings.

3. Select the **AirPlay Mirroring** payload tab.

4. Select **Add** under Whitelisted AirPlay Destinations.

5. Enter the destinations and device information, including:

Setting	Description
Destination Name	This is the name of the destination display. The name must match the device name and is case-sensitive. The device name can be found on the device.
Allowed Destination Device ID	This is the device ID for the destination display. Device IDs include the BonjourID.)
Password	This is the password that shows on the user's device when attempting to mirror to the destination. This password is only required if a password is required to mirror to the device.

6. Click **Save & Publish** when you are done configuring AirPlay settings.

Configure an AirPrint Profile (macOS)

Configure an AirPrint payload for an Apple device to enable computers to automatically detect an AirPrint printer even if the device is on a different subnet than the AirPrint printer.

To configure the AirPrint payload:

1. Navigate to **Devices > Profiles > List View > Add** and then **Add** the appropriate platform. If you select Apple macOS, then select whether this profile will apply to only the enrollment user on the device (**User Profile**), or the entire device (**Device Profile**).
2. Configure the profile's **General** settings.
3. Select the **AirPrint** payload tab.

Setting	Description
IP address	Enter the IP address (XXX.XXX.XXX.XXX).
Resource Path	Enter the Resource Path associated with the AirPrint printer (ipp/printer or printers/Canon_MG5300_series).

4. Select **Save & Publish**.

Configure an Xsan Storage Profile (macOS)

Apple's Xsan, or storage access network allows macOS with Thunderbolt to Fibre Channel capabilities to quickly access the shared block storage. Configure a payload to manage Xsan directly from the UEM console.

To configure an Xsan:

1. Navigate to **Devices > Profiles & Resources > Profiles** and select **Add**. Select Apple macOS, and then select (**User Profile**) to apply the enrollment to the user's device.
2. Configure the profile's **General** settings.
3. Select the **Xsan** payload.
4. Configure **Connection Info** for Xsan including:

Setting	Description
XSAN name	Enter the name of the storage system.
Authentication Secret	Enter the authentication key for the server.
File System Name Servers	Enter the Hostname or IP address of the file system name servers. Use the **+** button to add additional file system servers as needed.

5. Select **Save & Publish** when you are finished to push the profile to devices.

Configure a Firewall Profile (macOS)

Push a firewall profile with the AirWatch Agent v2.2+ for macOS to filter unauthorized connections to your enterprise network. Using the native firewall combined with the AirWatch Agent, you can monitor firewall settings and revert settings if unauthorized changes occur. Also, use the firewall to control incoming connections and protect computers against probing requests.

To create a firewall profile:

1. Navigate to **Devices > Profiles & Resources > Profiles** and select **Add**. Select Apple macOS, and then select **Device Profile**, since this profile is only applicable to the entire device.
2. Configure the profile's **General** settings.
3. Select the **Firewall** payload.
4. Select **Enable** to allow firewall protection.
5. Configure the following firewall settings:

Setting	Description
Block all incoming connections	Select this to block all incoming connections from sharing services, except for connections required for basic Internet services.
Automatically allow signed software to receive incoming connections	Select this to automatically allow only software signed by a developer and approved by Apple to provide services accessed from their network.
Enable stealth mode	Select this to prevent the computer from responding to or acknowledging requests made from test applications.

6. Select **Save & Publish** to push the profile to the device. All AirWatch Agent functionality continues including Push Notifications even if **Block incoming connections** is selected.

Configure a Firmware Password Profile (macOS)

Enforce a firmware password to increase security at the hardware level when allowing macOS v10.10+ to start up using an external drive, partition, or using Recovery Mode. The AirWatch Agent v2.2+ for macOS is required with this profile that provides enhanced security and allows you to determine when end users need to enter firmware passwords.

Important: If a firmware password is already set on the computer, then profile installation will fail.

To create a firmware password:

1. Navigate to **Devices > Profiles & Resources > Profiles** and select **Add**. Select Apple macOS, and then select **Device Profile**, since this profile is only applicable to the entire device.
2. Configure the profile's **General** settings.

3. Configure the **Firmware Password**:

Setting	Description
Firmware Password	Enter the password for the device.
Mode	Select the **Mode** when end users are required to enter the password: • **Command Mode** – Require the password when attempting to boot to another drive or partition. After the end user enters the password, the computer begins using Command Mode. Then, the macOS Agent prompts the end user to re-start the computer. • **Full Mode** – Require the password every time the computer starts up. After the end user enters the password, the macOS Agent prompts the end user to re-start the computer. When the computer re-starts, it begins using Full Mode. Once the profile is configured, it cannot be removed remotely.

4. Select **Save & Publish** to push the profile to the device.

Configure a Custom Attributes Profile (macOS)

Write a command or script and report it as a custom attribute using the AirWatch Agent for macOS v.2.3 and higher. Choose when to execute the command or script on hourly intervals or during an event.

Custom Attributes can also be used in Assignment Rules for Products. For more information about Products, see the VMware Workspace ONE UEM Product Provisioning for macOS Guide.

To create a Custom Attributes profile, take the following steps.

1. Navigate to **Devices > Profiles & Resources > Profiles** and select **Add** then **Add Profile**. Select Apple macOS, and then select **Device Profile**, since this profile is only applicable to the entire device.
2. Scroll down the menu bar on the left and select **Custom Attributes** followed by **Configure**.
3. Enter the **Attribute Name**.
4. Enter the **Script/Command** to run. Expand the text box as needed.
5. Choose an **Execution Interval** to allow for scheduling to report either in hours or as an event occurs.
6. Use the **+** and **-** buttons at the bottom of the payload to create multiple scripts.
7. Select **Save & Publish** when you are finished to push the profile to devices.

> **Note:** Custom Attribute values cannot return the following special characters: **/ \ " * : ; < > ? |**. If a script returns a value which contains these characters, the value is not reported on the console. Trim these characters from the script's output.

Configure a Custom Settings Profile (macOS)

The **Custom Settings** payload can be used when Apple releases new functionality or features that Workspace ONE UEM does not currently support through its native payloads. If you do not want to wait for the newest release of Workspace ONE UEM to be able to control these settings, you can use the **Custom Settings** payload and XML code to manually enable or disable certain settings.

You can create a "test" organization group to avoid affecting users before you are ready to save and publish the new settings. Also, any device not upgraded to the latest macOS version ignores the enhancements you create. Since the code is now customized, test the profile devices with older macOS versions to verify expected behavior.

1. Navigate to **Devices > Profiles & Resources > Profiles > Add > Add Profile**. Select **Apple macOS > macOS**.
2. Configure the profile's **General** settings.
3. Configure the appropriate payload (for example, Restrictions or Passcode).
4. **Save**, but do not publish, your profile.
5. Select the profile using the radio button next to the profile name. Menu buttons appear about the Profile Details.
6. Select **View XML** from the actions menu for the row of the profile you want to customize.
7. Find and copy the section of text starting with <dict> ... </dict> that you configured previously. See Restrictions or Passcode as an example. The section contains a configuration type identifying its purpose, such as Restrictions.
8. Navigate back to **Custom Settings** profile and paste the XML you copied in the text box. The XML code you paste should contain the complete block of code, from <dict> to </dict>.
9. Remove the original payload you configured by selecting the base payload section, for example, Restrictions, Passcode and selecting the minus [-] button. You can now enhance the profile by adding custom XML code for the new functionality.

Configure a Kernel Extension Policy Profile (macOS)

Use a Kernel Extension Policy to explicitly allow applications and installers that use kernel extensions to load on your end users' devices. This profile controls restrictions and settings for User Approved Kernel Extension Loading on macOS v10.13.2 and later.

To create a kernel extension policy profile:

1. Navigate to **Devices > Profiles & Resources > Profiles** and select **Add**. Select Apple macOS, and then select **Device Profile**.

   This profile is not enabled for the User level.
2. Configure the profile **General** settings.
3. Select the **Kernel Extension Policy** payload.
4. Select the **Allow User Overrides** check box to approve additional kernel extensions not explicitly allowed by configuration profiles.

   This option allows any application to install on the end users' devices without approval for a kernel extension. If you select this option, the extension policy settings below provide no additional functionality.

5. If you choose not to allow users to override kernel extensions, configure the extension policy settings.

Setting	Description
Whitelist Team Identifiers	Team identifiers for which all validly signed kernel extensions will be allowed to load. Use the **Add** button to add additional identifiers.
Whitelist Kernel Extentions	Signed kernel extensions that will always be allowed to load on the machine. Enter a **Team Identifier** and a **Bundle ID** for each app. For unsigned legacy kernel extensions, use an empty key for the team identifier. Use the **Add** button to add additional extensions.

Chapter 5:
Full Disk Encryption with FileVault

Overview

Enforce an encryption policy on macOS computers to protect data on the hard drive and escrowing recovery keys stored in Workspace ONE UEM so the keys can be recovered at later time. With FileVault2, Workspace ONE UEM builds on native capabilities to encrypt the drive and provides functionality within the AirWatch Agent to force the user to complete the encryption process.

Once the decision is made to encrypt your managed devices, you have options that allow you to choose the best recovery model for your deployment. These include recovery keys for Personal use, Corporate use, or a combination of both.

Corporate and Personal Recovery for macOS Devices

Corporate and Personal recovery is useful if the user will benefit from viewing and keeping a Personal Recovery Key, but the company will need a quick way to decrypt the device using a Corporate (Institutional) Recovery Key when necessary.

To encrypt a device using both Corporate and Personal Recovery Keys:

1. Configure a new **Disk Encryption** profile
2. Choose **Personal & Corporate** as the recovery type and configure the recovery key settings as needed.
3. Configure a FileVault Master Keychain. For more information on creating a FileVault Master Keychain, please refer to the section below.
4. Upload the FileVaultMaster.cer to the Disk Encryption profile to encrypt the assigned computers with your Corporate Recovery Key.

Once FileVault is enabled on the device, the Personal Recovery Key will be reported to the server.

Corporate Recovery for macOS Devices

Corporate recovery is beneficial because the network administrator can decrypt any device using a single Corporate Recovery Key, saving time by not needing to enter a unique Personal Recovery Key for each computer.

Generally, corporate recovery is reserved for Corporate Owned, Line-of-Business devices where the user does not have the ability to decrypt the device if they forget the login password.

To encrypt a device using a Corporate Recovery Key:

1. Configure a new **Disk Encryption** profile
2. Choose **Corporate** as the recovery type and configure the recovery key settings as needed.
3. Configure a FileVault Master Keychain. For more information on creating a FileVault Master Keychain, please refer to the section below.
4. Upload the FileVaultMaster.cer to the Disk Encryption profile to encrypt the assigned computers with your Corporate Recovery Key.

Once FileVault is enabled on the device, the Corporate Recovery Key will be reported to the server.

Configure a FileVault Corporate (Institutional) Recovery Key for macOS Devices

A corporate recovery key is a pre-made recovery key that can be installed on a system prior to the encryption process. Corporate recovery keys are not automatically generated and must be manually created before they can be used.

This section explains how to create an Corporate Recovery Key for macOS High Sierra (10.13) and above. However, the steps to create an Corporate Recovery Key for macOS Sierra (10.12) and below can be found at https://support.apple.com/en-us/HT202385.

To distribute the corporate recovery key through AirWatch, first create the FileVault Corporate Recovery Key and then upload it to the configuration profile on AirWatch Console by following the steps:

1. Create FileVault Keychain on page 81
2. Copy FileVaultMaster Keychain to Documents on page 82
3. Unlock FileVaultMaster Keychain on page 82
4. Add FileVaultMaster Keychain to Keychain Access Utility on page 82
5. Validate FileVaultMaster Keychain Unlock on page 84
6. Delete and Confirm Private Key Deletion on page 84
7. Export FileVault Recovery Key Certificate on page 86

Some of the additional steps to perform after exporting FileVaultMaster Recovery Key certificate are to:

1. Re-Lock the FileVaultMaster Keychain
2. Delete keychain from keychain access – To remove references to the FileVaultMaster keychain in Keychain Access.
3. Store the keychain and password – Store both the keychain (containing the certificate and private key) and the Keychain Password in multiple, secure locations. Without both you will be unable to decrypt any FileVault 2 drives encrypted with this Institutional Recovery Key.

Create FileVault Keychain

You can use commands to create a FileVaultMaster keychain in macOS. The keychain contains both private and public keys required for recovering FileVault 2 encrypted devices.

1. On a macOS computer (10.13+), select the **Launchpad** icon and then select **Others** > **Terminal**.
2. In the Terminal window, type the following command to create a FileVaultMaster keychain. Follow the prompts to apply password to the created keychain.

```
sudo security create-filevaultmaster-keychain
/Library/Keychains/FileVaultMaster.keychain
```

3. Once the command is complete, launch the **Finder**.
4. Press **Shift+command+G** and enter */Library/keychains* as the folder name.
5. Select **Go** to access the folder and to fetch the created keychain.

Note: Ensure you make copies and securely store both the keychain file and the password used to create the keychain. This keychain contains the certificate and private key to decrypt any FileVault 2 encrypted devices.

Copy FileVaultMaster Keychain to Documents

Before you start using the created FileVaultMaster keychain, make a copy of it and save in a secure location. Because, you need the modified keychain to encrypt a device and unmodified keychain to recover encryptrd devices.

In Terminal, type the following to copy the keychain file. When prompted, enter your admin account password to elevate your rights.

```
cp /Library/Keychains/FileVaultMaster.keychain
~/Documents/FileVaultMaster.keychain
```

```
sudo cp /Library/Keychains/FileVaultMaster.keychain
/Library/Keychains/FileVaultMaster2.keychain
```

Unlock FileVaultMaster Keychain

Unlock the FileVaultMaster keychain by entering the following command and provide the password you used when the keychain was created.

```
security unlock-keychain /Library/Keychains/FileVaultMaster.keychain
```

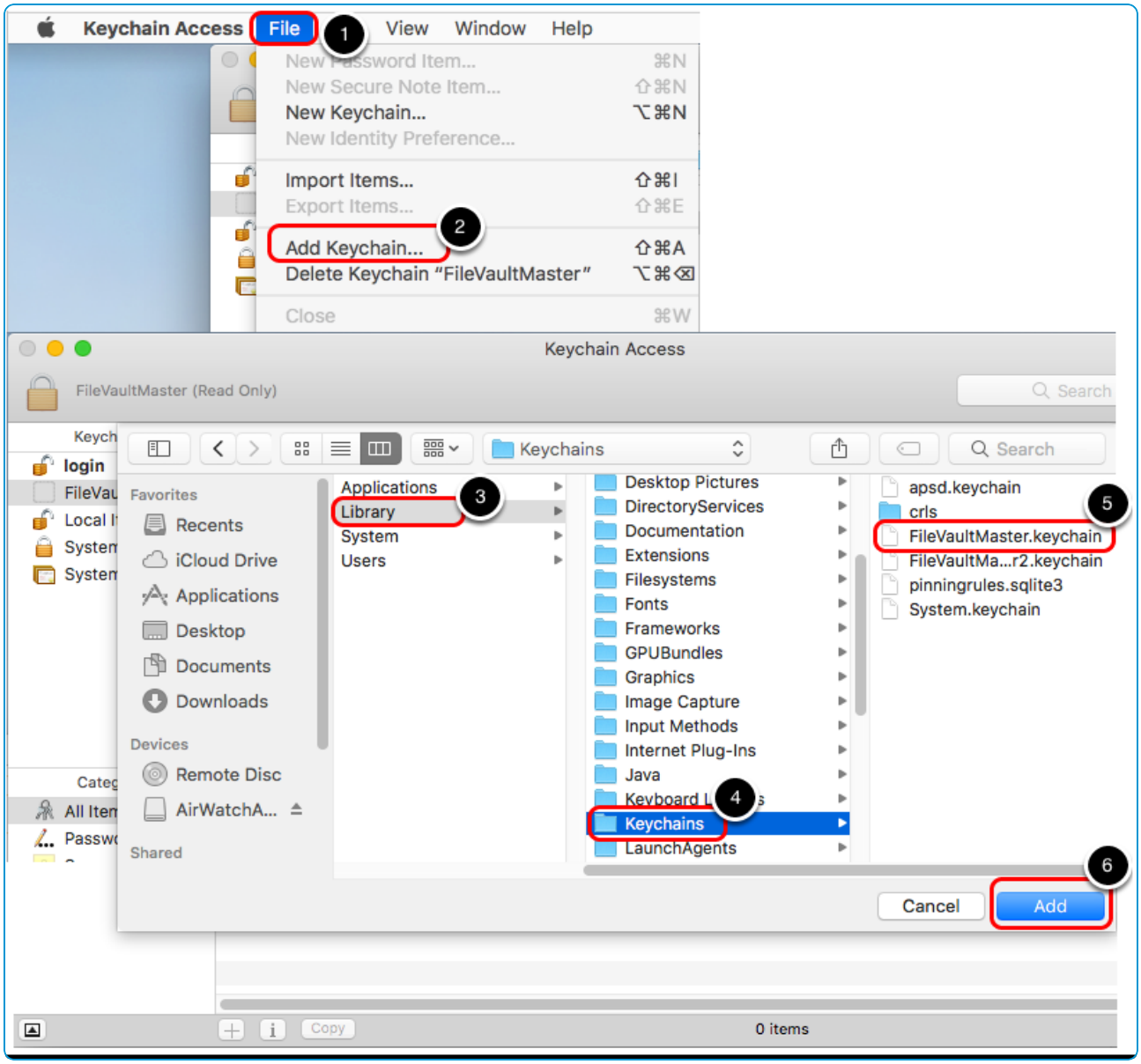
If you get an unexpected result during this step, the unlock idle time might have elapsed. You need to re-issue the unlock command in the Terminal window.

Add FileVaultMaster Keychain to Keychain Access Utility

Before you add the FileVaultMaster keychain to the Keychain Access Utility, open the Keychain Access application through Terminal window using the following command.

```
open /Applications/Utilities/Keychain\ Access.app/
```

Follow the steps to add the FileVaultMaster keychain to the Keychain Access Utility:

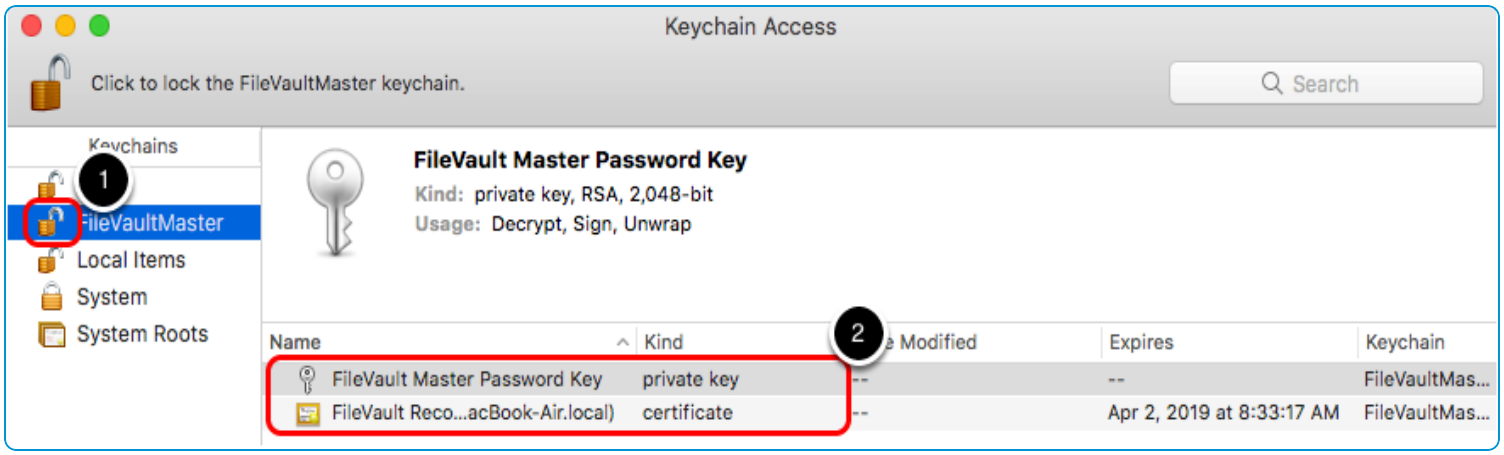


1. Selct File.
2. Select **Add Keychain...**.
3. Browse to the **Library** folder.
4. Select **Keychains**.
5. Select **FileVaultMaster.keychain**.
6. Select **Add**.

Note: If you unlocked the keychain correctly, the keychain should show with the "unlocked" icon in Keychain Access Utility. If it does not, you need to re-issue the unlock and re-add the keychain.

Validate FileVaultMaster Keychain Unlock

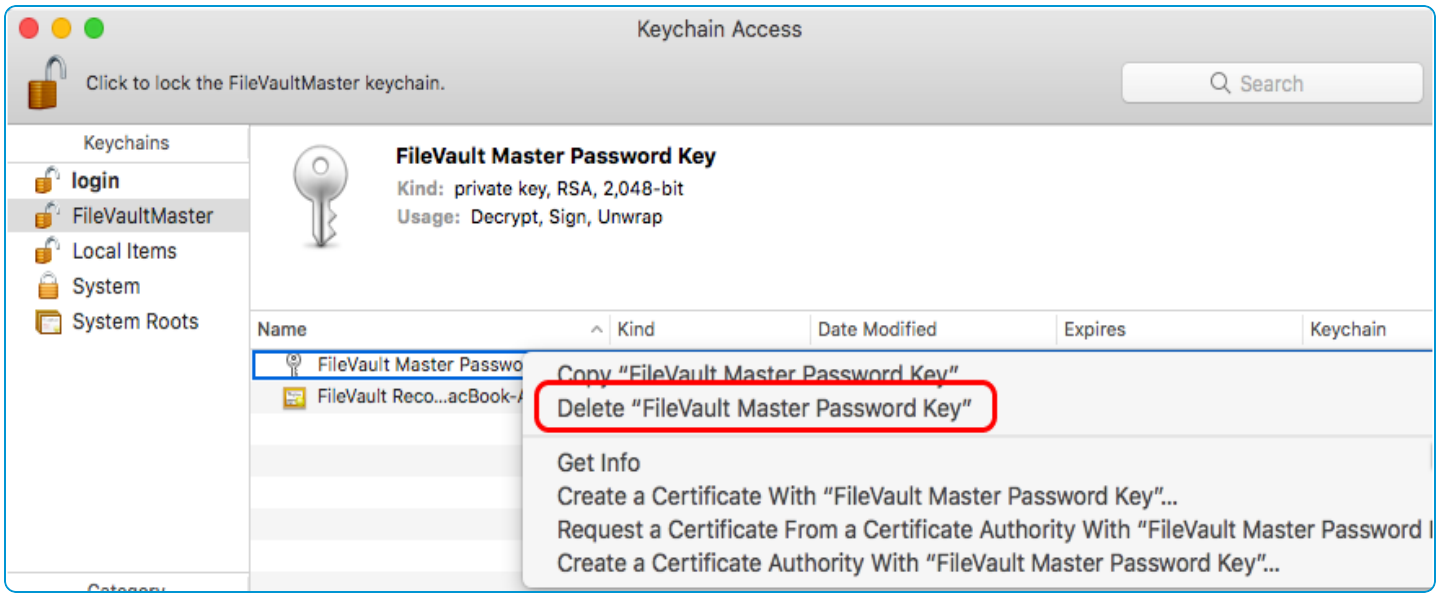
After adding the FileVaultMaster keychain file, validate if it is unlocked by performing the following steps.

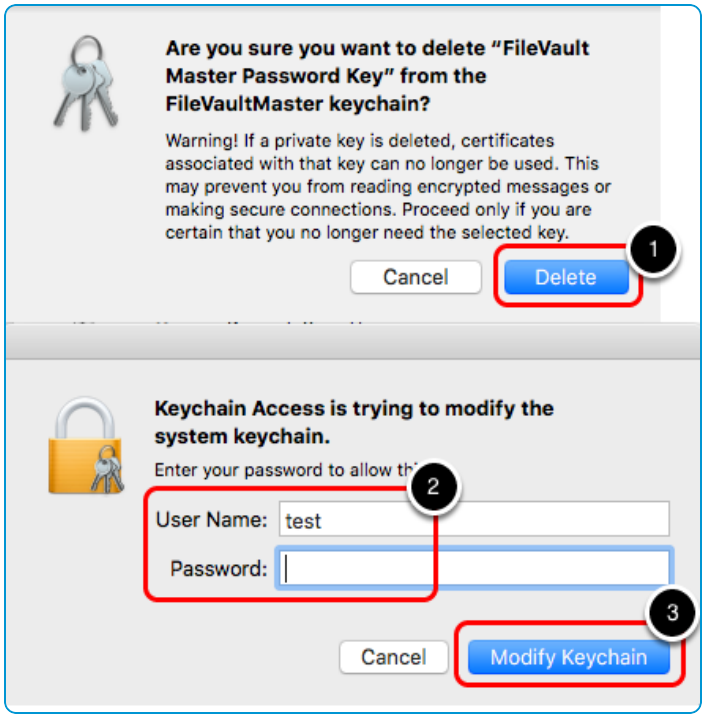


1. Ensure that the FileVaultMaster keychain shows unlocked icon.
2. Ensure that you can view the private key and certificate in the keychain.

Delete and Confirm Private Key Deletion

Once the validation of FileVaultMaster keychain file is complete, ensure you delete the 'FileVaultMaster Password Key' (private key).





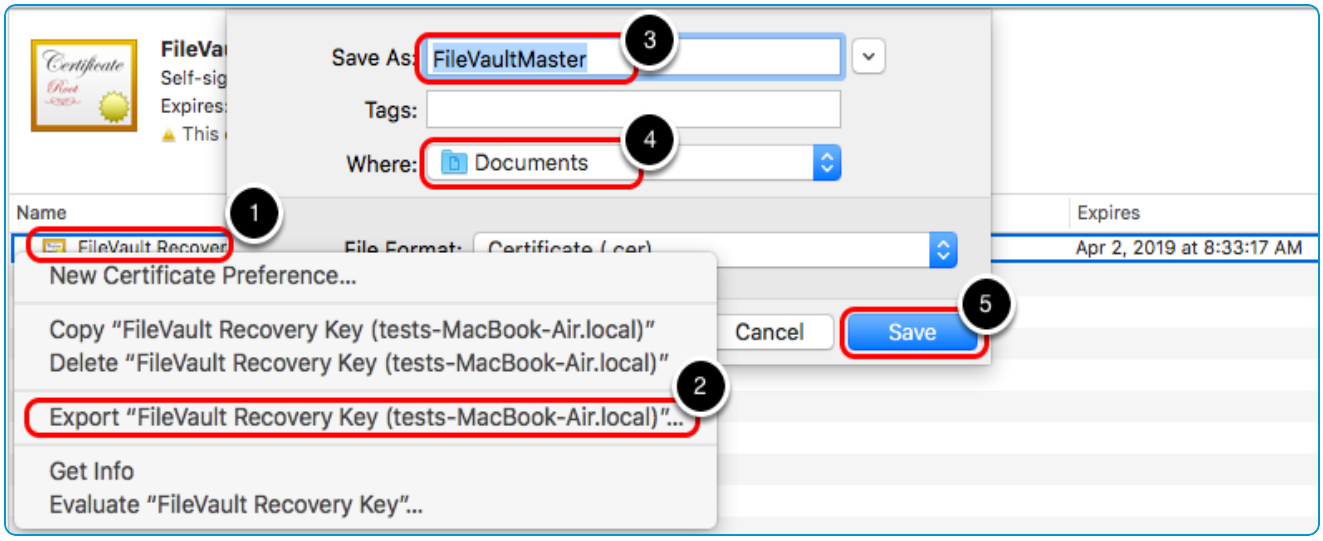
1. Navigate to **FileVault Master Password Key** > **Delete "FileVault Master Password Key"** and select **Delete** to confirm deletion of the private key.
2. Enter your administrative **User Name** and **Password**.
3. Select **Modify Keychain**.

By the end of this step, you have a FileVaultMaster.keychain file which does not contain the private key. This Keychain can be placed in \Library\Keychains in order to manually enable FileVault2 encryption with an Corporate Recovery Key.

Export FileVault Recovery Key Certificate

The configuration profile which configures the corporate recovery key on AirWatch Console requires only the certificate and not the keychain file.

Export the certificate from within the keychain and distribute the corporate recovery key to macOS through AirWatch console by following the steps:



1. Select the **FileVault Recovery Key certificate** in the FileVaultMaster keychain.
2. Select **Export FileVault Recovery Key (....)...**
3. Provide the certificate name as **FileVaultMaster** (in keeping the name consistent with the keychain file that it was created from).
4. Choose the location to save the certificate where you can access the key from your browser. (In this example, ~/Documents/)
5. Select **Save**.

By the end of this step, you now have a certificate file which DOES NOT contain the private key.

Personal Recovery for macOS Devices

Enabling **Personal** as the recovery type will allow the user of the device to use a recovery key to decrypt their device. Additionally, that key can be reported to the UEM console to allow administrators to use the key to decrypt the device if necessary.

Use Personal keys rather than Enterprise keys because Workspace ONE UEM can audit access to these keys, since they are escrowed in the UEM console. Also, Personal keys are beneficial because they are unique to each device. This means that the compromise of one key on one device does not compromise the security of other devices.

Once this profile is deployed to the device, the user will see a prompt from the AirWatch Agent taking them through the process of encrypting the disk. If configured, users may also be shown the recovery key to give them the option of saving it for later use. After a reboot, the device will begin the encryption process in the background and the user can continue their daily tasks normally without fear of interruption.

Enable Personal Recovery Encryption for a macOS Device

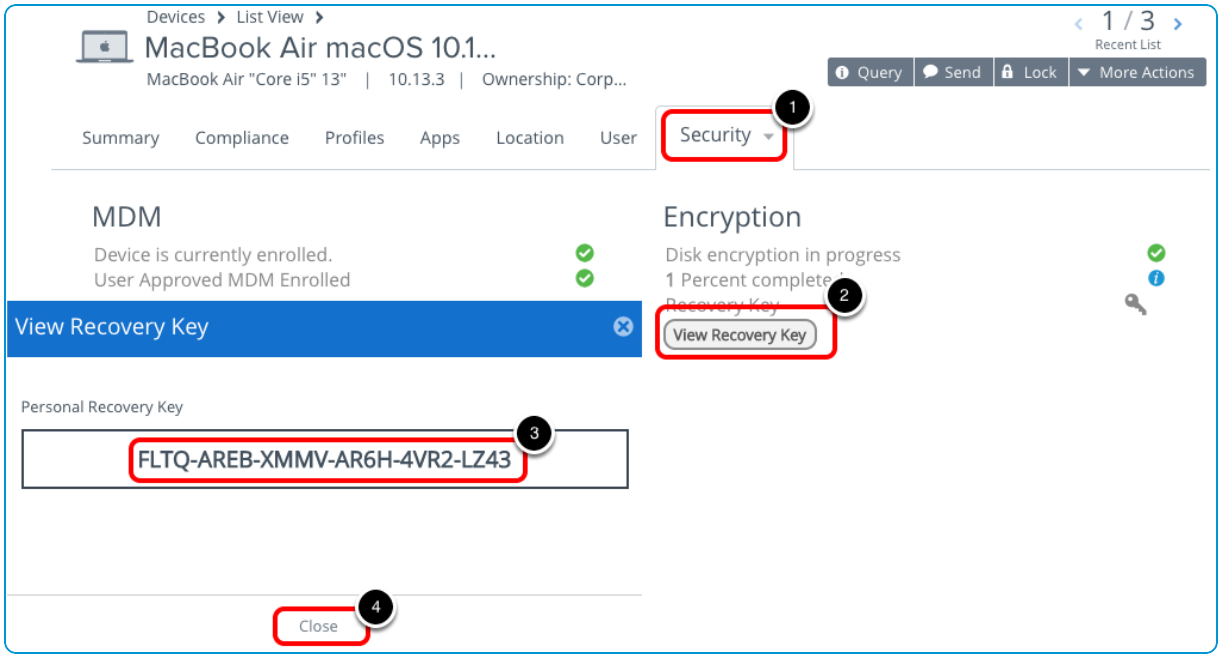
Personal recovery encryption is useful if the user wants the benefit of viewing and keeping a Personal Recovery Key from decrypt. To encrypt a device using a Personal Recovery Key:

1. Configure a new **Disk Encryption** profile.
2. Choose **Personal** as the recovery type and configure the recovery key settings as needed.

Once FileVault is enabled on the device, the Personal Recovery Key will be reported to a Workspace ONE UEM server or another designated server.

View Escrowed Personal Recovery Key

The personal recovery key is generated when FileVault 2 encryption is enabled and remains valid until the personal recovery key is changed or the disk is decrypted using that key.



To view an escrowed recovery key, perform the following within the **Device Details** page on the AirWatch Console.

1. Select the **Security** tab.
2. Select **View Recovery Key**.
3. Note the recovery key that is escrowed.
4. Select **Close** when finished viewing the key.

Note: If an encrypted macOS volume is decrypted and then re-encrypted, the previous personal recovery key would be invalidated and a new one created as part of the re-encryption process.

Recover an Encrypted Disk Using a Personal Recovery Key

If you forget your personal password for FileVault, you can use a Recovery Key to regain access.

To create a FileVault Personal Recovery Key:

1. Start into recovery-mode (**CMD+R** at start), a different partition or connect the disk to another macOS.
2. Access the terminal and run the following command. The command fetches a list of the Logical CoreStorage Volumes.

```
diskutil cs list
```

3. Find the Logical Volume (last on the list) and copy the UUID – it is in the format of XXXXXXXX-XXXX-XXXX-XXXXXXXXXXXX. Logical Volume is used to specify which volume must be unlocked and decrypted.

4. Ensure that you have the Personal Recovery Key available and run the command below. Replace "UUID" with the UUID retrieved in step 3. You are prompted to enter the Passphrase and the Personal Recovery Key.

```
diskutil cs unlockVolume UUID
```

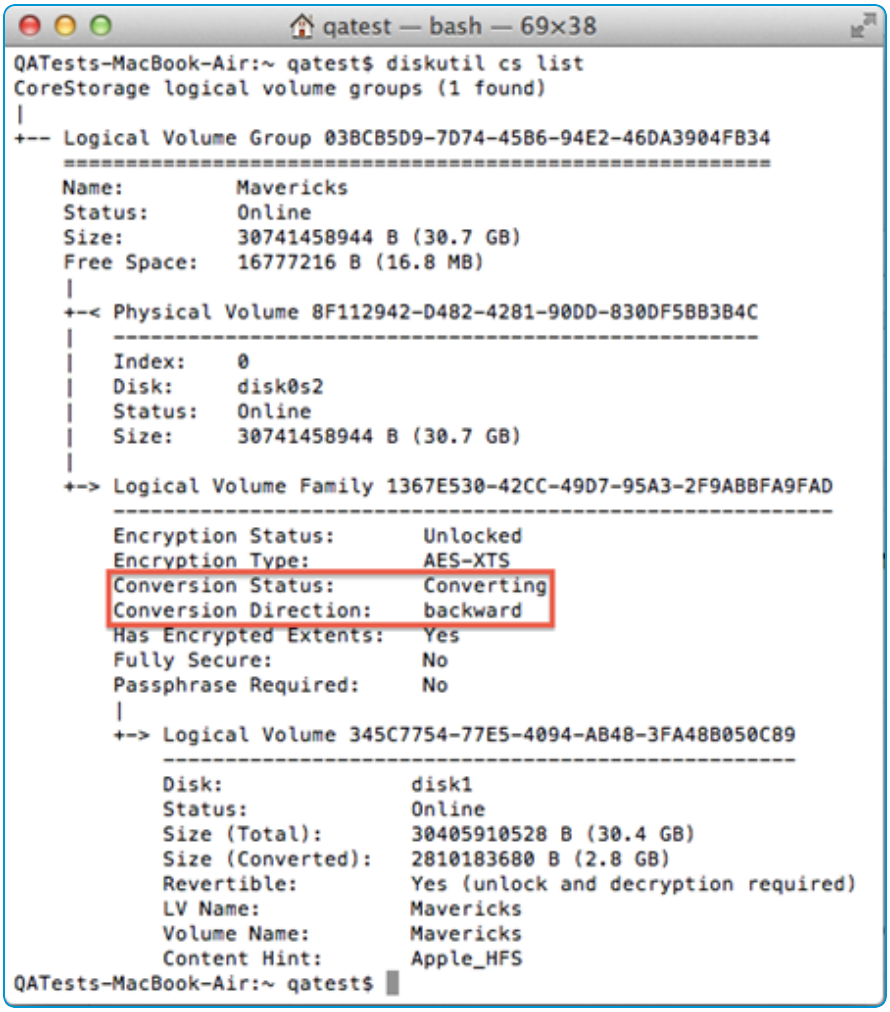
You can now see a response showing that the volume is unlocked and mounted. Now, you can recover any necessary files.

5. Now that the volume is unlocked, you can begin the decryption process by using the following command and replacing "UUID" with the UUID retrieved in step 3. You are prompted to enter the Passphrase and the Personal Recovery Key.

```
diskutil cs revert UUID
```

To monitor the decryption status, use the following command. The status is located in the Logical Volume Family information.

```
diskutil cs list
```



Chapter 6:
Compliance Policies

The compliance engine is an automated tool by Workspace ONE ™ UEM that ensures all devices abide by your policies. These policies can include basic security settings such as requiring a passcode and having a minimum device lock period. For certain platforms, you can also decide to set and enforce certain precautions. These precautions include setting password strength, blacklisting certain apps, and requiring device check-in intervals to ensure that devices are safe and in-contact with Workspace ONE UEM.

Once devices are determined to be out of compliance, the compliance engine warns users to address compliance errors to prevent disciplinary action on the device. For example, the compliance engine can trigger a message to notify the user that their device is out of compliance.

In addition, devices not in compliance cannot have device profiles assigned to it and cannot have apps installed on the device. If corrections are not made in the amount of time specified, the device loses access to certain content and functions that you define. The available compliance policies and actions vary by platform.

For more information about compliance policies, including which policies and actions are supported for a particular platform, refer to the **VMware AirWatch Mobile Device Management Guide**, available on docs.vmware.com.

Chapter 7:
Apps for macOS Devices

AirWatch macOS Agent

Once installed on a macOS device, the AirWatch Agent provides quick access to MDM settings and features you can use to manage your devices.

With the AirWatch Agent, you can perform key device actions:

- Sync Now - Sync the device with the UEM console
- View Enrollment, Connection, and Sync status
- View Preferences
- Uninstall the AirWatch Agent
- View information about the AirWatch Agent

The top line of the menu bar animates when actions are executed, including when products are executed, when the **Sync Now** option is initiated, when data is transmitting, when the disk is encrypting or decrypting, and when the Passcode policy needs updating.

The AirWatch Agent Preferences includes settings and information broken out into four tabs:

- **Status** – Snapshot of device and Workspace ONE UEM information.
    - **Enrollment Overview** – Current enrollment status, Server URL and option to verify enrollment.
    - **Device Information** – Computer name, model, version, serial number, encryption status, processor, memory, graphics and UUID.
    - **Connectivity Status** – Internet connection status, network information and option to test connectivity.
    - **Diagnostics** – Send data to the MDM server, sync with the MDM server, view agent logs, and send logs to Workspace ONE UEM Administrator.
- **Settings** – View MDM-related restrictions. Select the lock icon to make any changes. Changes to restrictions and check-in intervals require the Admin passcode to unlock the settings. Upgrade notifications can be changed even if the Settings are locked.

- **Messages** – View and edit notifications and messages in the Message Center.
- **Activity** – Select **View Log File** to view real-time Activity logs, and **Send Log** to Workspace ONE UEM Administrator.

Configuring Settings for the AirWatch Agent

The AirWatch Agent enhances your ability to monitor and control your device by providing detailed device information to Workspace ONE UEM. You can configure settings specific to the AirWatch Agent and its impact on the installed device through the UEM console.

To configure the Agent settings:

1. From the UEM console Dashboard, navigate to **Devices > Device Settings > Apple > Apple macOS > Agent Settings**.
2. Click the **Override** radio button to enable setting modification, if necessary.

3. Configure the Agent settings:

Setting	Description
General	
Check-in Interval	Enter the time interval for device check-in.
Data Sample Interval	Enter the time interval for sample data to be collected prior to transmission.
Data Transmit Interval	Enter the time interval for the device to automatically transmit data to Workspace ONE UEM.
Administrative Passcode	Enter a passcode to be applied to the app that the end user must enter to access Agent settings.
Enable Agent Uninstall	Select this check box to allow un-installation from the AirWatch Agent's main menu.
Location	
Collect Location Data	Select this check box to enable Workspace ONE UEM to collect GPS information from the device when available. If **Collect Location Data** is enabled, the end user receives a prompt to enable location services for **AirWatchid**. The alert persists until the user enables location services.
Password Enforcement	
Enforce Passcode	Select this check box to enforce passcode policy adherence on the device.
AirWatch Cloud Messaging	
Use AWCM	Select this check box to enable AWCM communication to the AirWatch Agent and device.
Agent Updates	
Enable Automatic Updates	Select this check box to enable automatic updates to the AirWatch Agent when a new version is available.
Upgrade Silently	Select this check box to run silent updates without interruption. If this check box is not selected, users will receive a prompt to begin the upgrade process.

Setting	Description
	Remote Management
Seek Permission	Enable Seek Permission if you want to prompt the end user to accept or decline the remote management request from the admin. When you enable this setting, more options appear. • Enter a **Seek Permission Message** that the end user will see when a remote request is sent. • Enter the **Yes Caption** message for the accept button the end user will see on the Seek Permission request. • Enter the **No Caption** message for the decline button the end user will see on the Seek Permission request.

4. Click **Save**.

Content Locker Sync for macOS Devices

VMware Content Locker Sync is an application that lets your end users sync personal content between VMware Content Locker on their devices, their Self-Service Portal (SSP), and their PC or macOS computers. End users download the application from the SSP and install it on their PC or macOS. From there, they can add files to a folder they designate on their computer, which is then synced with their SSP for viewing on other computers and their VMware Content Locker application on mobile devices.

For more information on enabling, using, and managing content with VMware Content Locker Sync, please refer to the **VMware Workspace ONE UEM Mobile Content Management Guide**.

AirWatch Catalog for macOS Devices

Deploy an app catalog to your end users so that they can access all your enterprise applications that you manage in the UEM console. Your end users can find and access applications based on the settings you establish in the UEM console.

For more information about providing self-service capability for App and Web App installations and the added the ability to manage enterprise applications for macOS, including installation and removal, see the **VMware Workspace ONE UEM Mobile Application Management Guide** .

Native VMware Workspace ONE for macOS Devices

Native VMware Workspace ONE is a unified app catalog that you can access numerous types of applications. Take advantage of Workspace ONE experience by integrating Workspace ONE UEM and VMware Identity Manager (VIDM).

As an admin, you can deploy Workspace ONE as an internal application. After devices enroll through the Workspace ONE UEM macOS agent, the end users can authenticate into the Workspace ONE application using their active directory credentials (such as the VIDM server and user name and password). When Workspace ONE authenticates, the software distribution and management principles are applied to the Workspace ONE application catalog through AirWatch agent.

For more information on how to set device management policies to grant the permission to access the web, remote, and native applications, see the **VMware Workspace ONE UEM Mobile Application Management Guide**.

Chapter 8:
Additional macOS Configurations

Kiosks for macOS Devices

Workspace ONE UEM offers the ability to utilize devices in your mobile fleet as kiosks. Kiosks limit your users to a single website browsing and to specific applications. For example, a retail establishment can deploy devices in device kiosk mode for use in store, utilizing corporate applications for in-store functionality like querying inventory and checking product pricing as well as custom branding to enhance the kiosk functionality.

A kiosk is configured from individual profiles. To build a kiosk, create profiles in the UEM console, and then let the device handle the configuration of a kiosk profile. Use device kiosks to remotely configure allowed applications, desktop wallpapers, allow widgets, specify websites and create other restrictions.

Build a Device Kiosk for a macOS Device

Finder and Dock profile configuration is required in order to lock the file system and manage system commands. Configure these profiles in the UEM console.

- Configure the **Dock** profile.
    - Allow specific applications and items to show on the Dock. By default, user adjustments are disabled, but you can enable these adjustments as needed. Do not select any check boxes that would allow the user to make changes to the settings. Also, do not allow these settings to merge with the user dock. If you choose to override the Dock, it will not be reverted to its original state when the profile is removed or upon an enterprise wipe.
- Configure the **Finder** profile.
    - Restrict access to the file system and commands using the Simple Finder and then choose commands to limit on the computer such as **Shut Down**. De-select the commands to make them unavailable to the user.

Additional macOS Profiles for Kiosk Mode

To use Kiosk mode effectively, enable additional profiles in the UEM console.

Safari browsing

- Configure profiles to control web browsing. Create a content filter within the **Parental Controls** profile and a list of allowed websites. These sites show up as Bookmarks in the Safari browser.
- Optionally, use the **Global HTTP Proxy** profile to limit network access.

Restrictions

- Customize a **Restrictions** profile to match your control Preferences, widgets and more.
- Apply Media restrictions to prevent mounting of external drives. This prohibits USB or external storage devices from connecting and transferring files. Additionally, disable AirDrop functionality.
- Apply Desktop restrictions to lock wallpaper on the desktop and allow for the configuration of default wallpaper.

Time Limits and Schedules

- Create a device curfew in the **Parental Controls** profile to limit use to operating hours.

Accessibility

- Accommodate all users by configuring settings for enhanced vision, hearing, and keyboard and mouse interactions to further improve the usability of the kiosk.

Mirror Screens with Apple AirPlay on macOS Devices

Apple AirPlay allows administrators to mirror screens from a macOS computer or tvOS on the same subnet. If an end user needs assistance, simply send an AirPlay request to share your screen with an end user's computer running macOS Yosemite or higher.

Adding an AirPlay destination:

1. Navigate to **Devices > List View** and select the device. The device summary screen appears.
2. Select **More > Support > Start AirPlay** in the administrative menu bar. An **AirPlay** window appears.
3. Select **Add a Destination** to start adding destinations to view. An **Add New AirPlay Destination** window appears.
4. Configure the destination information including:
    - **Destination Name** – Friendly name for the device.
    - **Destination Address** – macOS address of the device to view.
    - **Password** – Password for the destination.
    - **Scan Time** – Length of time that the device may search for the destination. The default value is 30 seconds.
    - Select the **Set as Default** check box to make the current destination the default destination. The next time AirPlay is used, the default destination appears as the **Destination Name**. It does not have to be entered again.

5. Select **Save and Start** to send the AirPlay request to the device.
   - This destination is saved for the next request in the **Destination Name** drop-down menu.
6. To **Stop AirPlay** on devices, navigate back to the UEM console. Go to **Devices > List View > Select the Device > Support > More > Stop AirPlay.**

Editing an AirPlay destination:

1. Navigate to **Devices > List View > Select Device > Support > More > AirPlay.** An **AirPlay** window appears.
2. Choose the **Device Destination** to edit from the drop-down menu.
3. Select **Edit** to start editing the destination settings. An **Edit AirPlay Destination** window appears.
4. Select **Save and Start** to send the AirPlay request to the device.

Custom Fonts for macOS Devices

Available to macOS Yosemite and devices running iOS 7 and higher, the UEM console provides a means to upload fonts and install them onto devices. Installing specific fonts allows users to view and read text that is not supported by standard means.

Compatible font file types include .ttf or .otf. There is no limit to the number of fonts you are can install on devices and you can remove a font at any time.

Manage Fonts on macOS Devices

To install and deploy fonts

1. Navigate to **Devices > Device Settings > Apple > Install Fonts**.
2. Drag and drop a supported font file type (.ttf or .otf) onto the screen.
3. Locate the font file and select **Save** to send the font to all devices enrolled in the current organization group.

To delete or view the font file

- Click on the button to delete a font.
- Click on the button to view and export the XML file.

Product Provisioning for macOS Devices

Product provisioning enables you to create, through Workspace ONE ™ UEM, products containing profiles, applications, files/actions, and event actions (depending on the platform you use). These products follow a set of rules, schedules, and dependencies as guidelines for ensuring your devices remain up-to-date with the content they need.

Product provisioning also encompasses the use of relay servers. These servers are FTP(S) servers designed to work as a go-between for devices and the UEM console. Create these servers for each store or warehouse to store product content for distribution to your devices.

For more information on using product provisioning with macOS devices, see the **Product Provisioning for macOS Guide**.

Chapter 9:
macOS Device Management

Overview

After your devices are enrolled and configured, manage the devices using the Workspace ONE ™ UEM console. The management tools and functions enable you to keep an eye on your devices and remotely perform administrative functions.

You can manage all your devices from the UEM console. The Dashboard is a searchable, customizable view that you can use to filter and find specific devices. This feature makes it easier to perform administrative functions on a particular set of devices. The Device List View displays all the devices currently enrolled in your Workspace ONE UEM environment and their status. The **Device Details** page provides device-specific information such as profiles, apps, AirWatch Agent version and which version of any applicable OEM service currently installed on the device. You can also perform remote actions on the device from the Device Details page that are platform-specific.

Device Dashboard

As devices are enrolled, you can manage them from the Workspace ONE ™ UEM **Device Dashboard**. The **Device Dashboard** provides a high-level view of your entire fleet and allows you to act on individual devices quickly.

You can view graphical representations of relevant device information for your fleet, such as device ownership type, compliance statistics, and platform and OS breakdowns. You can access each set of devices in the presented categories by selecting any of the available data views from the **Device Dashboard**.

From the **List View**, you can take administrative action: send messages, lock devices, delete devices, and change groups associated with the device.

Device List View

Select **Devices > List View** to see a full listing of all devices.

The **Last Seen** column displays an indicator showing the number of minutes elapsed since the device has checked-in.

Select a device in the **General Info** column at any time to open the details page for that device.

Sort by columns and configure information filters to review device activity based on specific information. For example, sort by the **Compliance Status** column to view only devices that are currently out-of-compliance and target only those devices. Search all devices for a friendly name or user name to isolate one device or user.

Customize Device List View Layout

Display the full listing of visible columns in the **Device List** view by selecting the **Layout** button and select the **Custom** option. This view enables you to display or hide Device List columns per your preferences.

There is also an option to apply your customized column view to all administrators. For instance, you can hide 'Asset Number' from the **Device List**.

Once all your customizations are complete, select the **Accept** button to save your column preferences and apply this new column view. You can return to the **Layout** button settings at any time to tweak your column display preferences.

Search in Device List View

You can search for a single device for quick access to its information and take remote action on the device.

To run a search, navigate to **Devices > List View**, select the **Search List** bar and enter a user name, device friendly name, or other device-identifying element. This action initiates a search across all devices, using your search parameter.

Device Details Page for macOS Devices

Use the Device Details page to track detailed device information and quickly access user and device management actions. You can access the Device Details page by either selecting a device's Friendly Name from the Device Search page, from one of the available Dashboards or by using any of the available search tools with the UEM console.

Use the Device Details menu tabs to access specific device information.

Tab	Description
Summary	View general statistics on: platform/model/OS, compliance, Workspace ONE UEM Cloud Messaging, enrollment, last seen, firewall, firmware, time machine, contact information, groups, serial number, UDID, asset number, power status, storage capacity, physical memory and virtual memory, and warranty information. If Apple's Global Service Exchange information is accessible, select the warranty link to see when the status was last updated.
Compliance	Display the status, policy name, date of the previous and forthcoming compliance check and the actions already taken on the device. The **Compliance** tab includes advanced troubleshooting and convenience features. • Non-Compliant devices, and devices in pending compliance status, have troubleshooting functions available. You may reevaluate compliance on a per-device basis ( ) or get detailed information about the compliance status on the device ( ). • Users with Read-Only privileges can view the specific compliance policy directly from the **Compliance** tab while Administrators can make edits to the compliance policy.
Profiles	View all MDM profiles currently installed on a device.
Apps	View all apps currently installed or pending installation on the device.

Tab	Description
Location	View current location or location history of a device.
User	Access details about the user of a device as well as the status of the other devices enrolled to this user.

Additional menu tabs are available by selecting **More** from the main Device Details tab.

Tab	Description
Network	View current network status (Cellular, Wi-Fi, Bluetooth) of a device.
Security	View current security status of a device based on security settings.
Restrictions	View all restrictions currently applied to a device. This tab also shows specific restrictions by Device, Apps, Ratings, and Passcode.
Notes	View and add notes regarding the device. For example, note the shipping status or if the device is in repair and out of commission.
Certificates	Identify device certificates by name and issuant. This tab also provides information about certificate expiration.
Products	View complete history and status of all packages provisioned to the device and any provisioning errors.
Custom Attributes	View the Custom Attributes associated with the device.
Files/Actions	View the files and other actions associated with the device.
Shared Device Log	View the history of the shared device including past check-ins and check-outs and status.
Trouble Shooting	View **Event Log** and **Commands** logging information. This page features export and search functions, enabling you to perform targets searches and analysis. • **Event Log** – View detailed debug information and server check-ins, including a **Filter** by **Event Group Type**, **Date Range**, **Severity**, **Module**, and **Category**. In the **Event Log** listing, the **Event Data** column may display hypertext links that open a separate screen with even more detail surrounding the specific event. This information enables you to perform advanced troubleshooting such as determining why a profile fails to install. • **Commands** – View detailed listing of pending, queued, and completed commands sent to the device. Includes a **Filter** enabling you to filter commands by **Category**, **Status**, and specific **Command**.
Status History	View history of device in relation to enrollment status.
Targeted Logging	View the logs for the Console, Catalog, Device Services, Device Management, and Self Service Portal. You must enable Targeted Logging in settings and a link is provided for this purpose. You must then select the **Create New Log** button and select a length of time the log is collected
Attachments	Use this storage space on the server for screenshots, documents, and links for troubleshooting and other purposes without taking up space on the device itself
Terms of Use	View a list of End User License Agreements (EULAs) which have been accepted during device enrollment.

Device Actions

Perform common device actions with the action button cluster including Query, Send, Lock, and other actions accessed through the **More Actions** button.

Device Details Action Button Cluster

Note: Available Device Actions vary by device model, enrollment status and type, and the specific configuration of your Workspace ONE UEM console. For more information on full listing of remote actions that you can invoke using the Console, refer **VMware Workspace ONE UEM Mobile Device Management Guide**.

Run commands remotely to individual (or bulk) devices in your fleet. Each of the following device actions and definitions represents remote commands that you can invoke from the UEM console.

- **Add Tag** – Assign a customizable tag to a device, which can be used to identify a special device in your fleet.
- **Apps (Query)** – Send an MDM query command to the device to return a list of installed apps.
- **Certificates (Query)** – Send an MDM query command to the device to return a list of installed certificates.
- **Change Organization Group** – Change the device's home organization group to another pre-existing OG. Includes an option to select a static or dynamic OG.
- **Change Ownership** – Change the Ownership setting for a device, where applicable. Choices include Corporate-Dedicated, Corporate-Shared, Employee Owned and Undefined.
- **Delete Device** – Delete and unenroll a device from the UEM console. This action performs an Enterprise Wipe and remove its representation in the UEM console.
- **Device Information (Query)** – Send an MDM query command to the device to return basic information on the device such as friendly name, platform, model, organization group, operating system version and ownership status.
- **Device Wipe** – Send an MDM command to wipe a device clear of all data and operating system. This puts the device in a state where recovery partition will be needed to reinstall the OS. This action cannot be undone.
- **Edit Device** – Edit device information such as **Friendly Name**, **Asset Number**, **Device Ownership**, **Device Group** and **Device Category**.
- **Enroll** – Send a message to the device user to enroll their device. You may optionally use a message template that may include enrollment information such as step-by-step instructions and helpful links. This action is only available on unenrolled devices.
- **Enterprise Wipe** – Enterprise Wipe a device to unenroll and remove all managed enterprise resources including applications and profiles. This action cannot be undone and re-enrollment will be required for Workspace ONE UEM to manage this device again. Includes options to prevent future re-enrollment and a **Note Description** field for you to

add any noteworthy details about the action.

  - Enterprise Wipe is not supported for cloud domain-joined devices.

- **Location** – Reveal a device's location by showing it on a map using its GPS capability enabled via the macOS AirWatch Agent. Also requires user approval to enable the functionality in macOS System Preferences.
- **Lock Device** – Send an MDM command to lock a selected device, rendering it unusable until it is unlocked.
- **Profiles (Query)** – Send an MDM query command to the device to return a list of installed device profiles.
- **Query All** – Send a query command to the device to return a list of installed apps (including AirWatch Agent, where applicable), books, certificates, device information, profiles and security measures.
- **Reboot Device** – Send an MDM command to restart macOS 10.13+ devices remotely. This action reproduces the effect of powering the device off and on again.
- **Remote Management** – Take control of a supported device remotely using this action, which launches a console application that enables you to perform support and troubleshoot on the device.
- **Security (Query)** – Send an MDM query command to the device to return the list of active security measures (device manager, encryption, passcode, certificates, etc.).
- **Send Message** – Send a message to the user of the selected device. Choose between **Email**, **Push Notification** (through AirWatch Cloud Messaging), and **SMS**.
- **Start AirPlay** – Stream audiovisual content from the device to an AirPlay mirror destination. The MAC address (format "xx:xx:xx:xx:xx:xx" with no case-sensitive) of the destination is required. A passcode can also be specified if required. Scan Time defines the number of seconds (10-300) to spend searching for the destination. Requires macOS 10.10 or greater.
- **Install macOS AirWatch Agent** – Send an MDM command to the device to install the latest seeded macOS AirWatch agent.
- **Managed settings** – Managed settings lets you enable or disable Bluetooth through an MDM command. Requires macOS 10.13.4 or greater.
- **Shut Down** – Send an MDM command to shut down macOS 10.13+ devices remotely.

Configure and Deploy a Custom Command to a Managed Device

Workspace ONE UEM enables administrators to deploy a custom XML command to managed Apple devices. Custom commands allow more granular control over your devices.

Use custom commands to support device actions that the UEM console does not currently support. Do not use custom commands to send commands that exist in the UEM console as Device Actions. Samples of XML code you can deploy as custom commands are available in the Workspace ONE UEM Knowledge Base at https://support.air-watch.com/kb.

Important: Improperly formed or unsupported commands can impact the usability and performance of managed devices. Test the command on a single device before issuing custom commands in bulk.

To create and deploy a custom command:

1. In the UEM console, navigate to **Devices > List View**.
2. Select one or more macOS devices using the check boxes in the left column.
3. Select the **More Actions** drop-down and select **Custom Commands**. The Custom Commands dialogue box opens.
4. Enter the XML code for the action you want to deploy.

   Browse XML code for Custom Commands on the Workspace ONE UEM Knowledge Base at https://support.air-watch.com/kb.
5. Select **Send** to deploy the command to devices.

If the Custom Command does not run successfully, delete the command by navigating to **Devices > List View**. Select the device to which you assigned the custom command. In the Device **Details View**, select **More > Troubleshooting > Commands**. Select the Command you want to remove, and then select **Delete**. The Delete option is only available for Custom Commands with a Pending status.

AppleCare GSX

Apple Global Service Exchange (GSX) allows administrators to look up device details related to the display model name, the device purchase and warranty status directly from the UEM console.

If any devices in an organization group are missing a display model name, then a time scheduler runs periodically to search and update these names using the GSX information that was configured for the devices at that organization group level.

Only authorized Apple employees or organizations that have registered with Apple's Self-Servicing Account Program can access GSX information.

Create a GSX Account

Before you can integrate your deployment, you must create an Apple GSX account. To apply for a GSX account, you must have a service contract with Apple. Contact your Apple Account Executive to learn more about GSX.

To apply for a GSX account, visit http://www.apple.com/support/programs/ssa/.

Obtain an Apple Certificate to Integrate AppleCare GSX

To integrate AppleCare GSX with your Workspace ONE UEM deployment, you must first obtain an Apple certificates and convert them to .p12 format.

For more information, see Obtain an Apple Certificate to Integrate AppleCare GSX on page 105.

Configure AppleCare in the UEM console

Once you have obtained and configured an Apple Certificate, you must upload the certificate to the UEM console and configure your AppleCare instance.

For more information, see Configure AppleCare GSX in the UEM Console on page 106.

Obtain an Apple Certificate to Integrate AppleCare GSX

To integrate AppleCare GSX with your Workspace ONE UEM deployment, you must first obtain an Apple certificates and convert them to .p12 format.

To integrate, perform the following:

1. Generate a certificate signing request (CSR) using OpenSSL or Java Keytool.
2. Send the CSR and the following GSX account information to Apple to receive Apple certificates (.pem files).
   a. GSX Sold-To account number
   b. Primary IT contact name
   c. Primary IT contact email
   d. Primary IT contact phone number
   e. Outgoing static IP address of the server that sends requests to GSX Production

   
   If your environment is hosted on the AW SaaS, refer to https://support.air-watch.com/articles/115001662168 for the IP address. If the IP range for your environment is not listed, please open a support ticket to have our Network Operations team facilitate it.

   Apple generates the Apple certificate (.pem) and returns a signed certificate and a chain certificate. For ease of use, rename the files “cert.pem” and “chain.pem” for use in subsequent steps.

   You may also receive a file labeled “issuer” that is not needed for this process.
3. Convert the Apple certificates to .p12 format.
   a. Create a .p12 file using the private key and Apple certificates by executing the following command:

   ```
   sudo openssl pkcs12 -export -inkey privatekey.pem -in cert.pem -certfile
   chain.pem -out GSX_Cert.p12
   ```

   b. The certificate saves as a .p12 file in the location you specified.

   If you do not specify a path before the file name when running the conversion command, the file saves to your working directory.

Configure AppleCare GSX in the UEM Console

Once you have obtained and configured an Apple Certificate, you must upload the certificate to the UEM console and configure your AppleCare instance.

1. Navigate to **Groups & Settings > All Settings > Devices & Users > Apple > AppleCare**

   To configure a GSX connection with the UEM console, you must have a GSX account with manager-level access, access to web services, and access to coverage and warranty information.
2. Enter **GSX settings** including:

Setting	Description
GSX User ID	Enter the account user ID.
GSX Password	Enter the account password.
Sold-to Account Number	Enter the 10-digit service account number. This account number can be found in the GSX portal at the bottom of the web page.
Time Zone	Use the drop-down menu to select the appropriate time zone.
Language	Use the drop-down menu to choose a language.

3. Select **Save** to complete the integration with AppleCare.
4. Navigate to the **List View**, select a device, and use the **More** menu to find **AppleCare** information in the UEM console.

Chapter 10:
Shared Devices

Overview

Issuing a device to every employee in certain organizations can be expensive. Workspace ONE ™ UEM lets you share a mobile device among end users in two ways: using a single fixed configuration for all end users, or using a unique configuration setting for individual end users.

Shared Device/Multi-User Device functionality ensures that security and authentication are in place for every unique end user. And if applicable, shared devices allow only specific end users to access sensitive information.

When administering shared devices, you must first provision the devices with applicable settings and restrictions before deploying them to end users. Once deployed, Workspace ONE UEM uses a simple login or log-out process for shared devices in which end users simply enter their directory services or dedicated credentials to log in. The end-user role determines their level of access to corporate resources such as content, features, and applications. This role ensures the automatic configuration of features and resources that are available after the user logs in.

The login or log-out functions are self-contained within the AirWatch Agent. Self-containment ensures that the enrollment status is never affected, and that the device is managed whether it is in use or not.

Shared Devices Capabilities

There are basic capabilities surrounding the functionality and security of devices that are shared across multiple users. These capabilities offer compelling reasons to consider shared devices as a cost-effective solution to making the most of enterprise mobility.

- **Functionality**
  - Personalize each end-user experience without losing corporate settings.
  - Logging in a device configures it with corporate access and specific settings, applications, and content based on the end-user role and organization group (OG).
  - Allow for a log in/log out process that is self-contained in the AirWatch Agent.
  - After the end user logs out of the device, the configuration settings of that session are wiped. The device is then ready for login by another end user.

- **Security**
  - Provision devices with the shared device settings before providing devices to end users.
  - Log in and log out devices without affecting an enrollment in Workspace ONE UEM.
  - Authenticate end users during a login with directory services or dedicated Workspace ONE UEM credentials.
  - Manage devices even when a device is not logged in.

Platforms that Support Shared Devices

The following devices support shared device/multi-user device functionality.

- Android 4.3+,
- iOS devices with AirWatch Agent v4.2+,
- MacOS devices with AirWatch Agent v2.1+.

Define the Shared Device Hierarchy

When you first log in to Workspace ONE ™ UEM, you see a single organization group (OG) that has been created for you using the name of your organization. This group serves as your top-level OG. Below this top-level group you can create subgroups to build out your company hierarchical structure.

1. Navigate to **Groups & Settings > Groups > Organization Groups > Organization Group Details**. Here, you can see an OG representing your company.
2. Ensure the **Organization Group Details** displayed are accurate, and then use the available settings to make modifications, if necessary. If you make changes, select **Save**.
3. Select **Add Child Organization Group**.
4. Enter the following information for the first OG underneath the top-level OG.

Setting	Description
Name	Enter a name for the child organization group (OG) to be displayed. Use alphanumeric characters only. Do not use odd characters.
Group ID	Enter an identifier for the OG for the end users to use during the device login. Group IDs are used during the enrollment of group devices to the appropriate OG. Ensure that users sharing devices receive the **Group ID** as it may be required for the device to log in depending on your Shared Device configuration.
Type	Select the preconfigured OG type that reflects the category for the child OG.
Country	Select the country where the OG is based.
Locale	Select the language classification for the selected country.
Customer Industry	This setting is only available when **Type** is Customer. Select from the list of Customer Industries.

5. Select **Save**.

Log In and log out of Shared macOS Devices

Multiple users can log in to and out of a macOS shared device, activating the automatic push of device profiles.

Log In to a macOS Device

Using assigned Network credentials, log in to a macOS device that has been staged and you receive the profiles assigned to your account in Workspace ONE ™ UEM.

Log out of a macOS Device

The standard macOS log-out procedure also logs the device out of your assigned Workspace ONE UEM user profile.