Integration with Apple Business Manager

VMware Workspace ONE UEM

You can find the most up-to-date technical documentation on the VMware website at:

https://docs.vmware.com/

VMware, Inc.
3401 Hillview Ave.
Palo Alto, CA 94304
www.vmware.com

Contents

Introduction to Apple Business Manager

1

Apple Business Manager is a portal for administrators to manage the Device Enrollment program (DEP), Volume Purchase Program (VPP), Apple IDs, and content distribution in their organizations. Apple Business Manager with Workspace ONE UEM powered by AirWatch Mobile Device Management (MDM) solution makes it easy to enroll devices and deploy content.

Apple Business Manager has consolidated the management features that you have been using through the DEP and VPP portals. Once your organization upgrades to Apple Business Manager from Apple Deployment programs, the DEP and VPP portals will no longer be used to manage devices, assignments, apps purchases, or manage content.

For more information, see Apple Business Manager or contact your Apple representative.

Prerequisites

- If you are using DEP, upgrade to Apple Business Manager.

  Note Once upgraded to new Apple Business Manager portal, you will have no access to the Apple Deployment programs.

- If you are using only Volume Purchase Program, you need to first enroll in Apple Business Manager and then invite VPP purchasers to your new Apple Business Manager account.

Apple Business Manager Services

To maximize the benefits of Apple devices enrolled in Mobile Device Management (MDM), Apple has introduced Apple Business Manager with combined services of the Device Enrollment Program (DEP) and the Volume Purchase Program (VPP) services.

Apple Business Manager's DEP service

Through Apple Business Manager's DEP service, you can perform the following.

- Install a non-removable MDM profile on a device, preventing end users from being able to delete it.
- Provision devices in Supervised mode (iOS only). Devices in Supervised mode can access additional security and configuration settings.
- Enforce an enrollment for all end users.
- Meet your organization's needs by customizing and streamline the enrollment process.

- Prevent iCloud back up by disabling users from signing in with their Apple ID when generating a DEP profile.
- Force OS updates for all end users.

For more information, see the Apple Business Support Portal portal or the Apple Business Manager Guide, or contact your Apple representative.

Note Integration with any third-party software product is not guaranteed, and is dependent upon the proper functioning of those third-party solutions.

App Security Features for DEP Devices

Devices managed by Workspace ONE UEM and enrolled through the Apple Device Enrollment Program can receive security measures to protect corporate data on Workspace ONE productivity applications and Third-party applications leveraging Workspace ONE SDK.

Maximum App Passcode Attempts

You can configure your Workspace ONE productivity applications and Third-party applications leveraging Workspace ONE SDK to require the end user to enter a passcode to access app on the device. You can also set a maximum number of attempts to enter the passcode correctly. If this feature is enabled and a user exceeds the maximum device passcode attempts, regular Bring Your Own Devices (BYOD) perform enterprise wipe, while corporate dedicated DEP devices are quarantined and the devices lock into Lost Mode. A device in Lost Mode can only be unlocked from the UEM console. This way corporate dedicated DEP assets continue to be managed from the UEM console for tracking purposes while the user is locked out of the device.

To configure the app passcode settings, navigate to **Groups & Settings > All Settings > Apps > Security Policies** in the UEM console.

For more information, see *Create or Edit the DEP Enrollment Profile* in Apple Business Manager - Device Enrollment Program section.

Workspace ONE Intelligent Hub Unenroll Protection

If an end user attempts to unenroll a supervised DEP device through the Workspace ONE Intelligent Hub, the device locks into Lost Mode. A device in Lost Mode can only be unlocked from the UEM console.

For more information, see *Perform Remote Actions on All Devices* in DEP Device Management section .

Apple Business Manager Integration Prerequisites

To utilize the features of Apple Business Manager, make sure you have the following prerequisites in place.

- **An Apple Business Manager account** – Register for a Apple Business Manager account. If needed, enroll with Apple using the Apple Enrollment Procedure.
- **Apple devices** – Any macOS, iOS, and tvOS devices that you want to be managed through DEP service, you must have devices associated with Apple Business Manager account.
  - Devices purchased from a Third party or reseller must be associated with your Apple Business Manager account.
  - Starting iOS 11 and tvOS 11, any iOS and tvOS device can be added to device enrollment program of Apple Business Manager using Apple Configurator.
  - When enrolling devices, you must have Internet connectivity.
- When integrating with the Apple Business Manager portal, ensure that the network is set up to communicate with **mdmenrollment.apple.com** on port **443**, as for some on-premise clients.

Apple Business Manager - Device Enrollment Program

2

Integrating with Apple's Device Enrollment Program (DEP) requires completing tasks in both the UEM console and in Apple Business Manager portal.

Your organization must already be registered with Apple Business Manager Deployment Programs. During the integration, Workspace ONE UEM suggests you not use Internet Explorer as your browser. Also, once you begin configuring the Apple Business Manager wizard in the UEM console, keep the browser session open. You cannot save your activity until you complete the final configuration step, so it is important to finish the entire configuration in one browser session.

Configure the Apple Business Manager Portal

Start in the UEM console to begin integrating your Workspace ONE UEM deployment with Apple Business Manager. Then move to the Apple Business Manager portal to create a virtual MDM server container for your organization's devices. You must download the Publick Key to integrate with Apple Business Manager.

To configure the Apple Business Manager Portal, begin integrating with the Apple DEP program by creating a virtual MDM server for devices that links to your own MDM servers, so you can manage devices directly in the UEM console. Workspace ONE UEM does not encourage using Internet Explorer to complete this process.

Prerequisites

You must download the public key (.pem) that allows Workspace ONE UEM and Apple to mutually authenticate with each other to sync devices. This key is uploaded to the Apple portal later.

1 Log into the UEM console and navigate to **Groups & Settings > All Settings > Devices & Users > Apple > Device Enrollment Program** and select **Configure**. A **Device Enrollment Program** window appears.

2 Download the public key by selecting the **MDM_DEP_PublicKey.pem** file.

3 Save the public key in a convenient location. This is used to complete the DEP setup process.

Procedure

Using the public key you have downloaded, you must next enable and configure the Apple Business Manager Portal so that you can manage your DEP-enrolled devices in the Workspace ONE UEM console.

1 Log into Apple Business Manager portal.

2 Sign in with your organization's Apple credentials.

3 Confirm your identity by entering the verification code. The Device Enrollment Program portal screen appears.

4 Navigate to **Settings** > **Device Management Settings** > **Add a MDM Server**.

5 Enter the **MDM Server Name**.

6 In MDM Server Settings, upload the public key by browsing from your local repository.

7 Click **Save**.

What next : Configure your devices and the UEM console to create an initial profile.

Create or Edit the DEP Enrollment Profile

After assigning devices to the Apple Business Manager portal, use the Device Enrollment Program wizard in the Workspace ONE UEM console to create an initial DEP profile to configure authentication, MDM features, and the Setup Assistant to push down to devices.

You must assign this DEP profile before configuring the device's Setup Assistant that appears after you switch on the device for the first time. Devices only reach out to Apple's server once after configuring Wi-Fi to receive the DEP profile. If the correct DEP profile is not assigned to the device prior to Wi-Fi configuration, a factory wipe is required (using iTunes or directly on the device).

After you register devices with the Apple Business Manager portal, use the DEP Enrollment Program wizard to create a DEP enrollment profile in Workspace ONE Express or Workspace ONE UEM powered by AirWatch. An enrollment profile is a collection of DEP settings assigned to your registered devices. To provide a customized experience to users enrolling into Workspace ONE UEM with devices added to Apple Business Manager, see *Custom Enrollment in DEP*.

Create a DEP enrollment profile or edit an existing profile. If needed, you can create more profiles later.

1 In the Workspace ONE UEM console, navigate to **Groups & Settings > All Settings > Devices & Users > Apple > Device Enrollment Program**.

2 Select **Upload** and select Apple Server Token File (.p7m). Select **Next**. Now Workspace ONE UEM and Apple can authenticate each other.

   For clarity, use only one token at the customer organization group. Only add multiple tokens if your organization has a complex configuration, or if you are enrolling devices with multiple DEP accounts.

3 Configure the **Authentication** settings, based on whether you turn authentication **On** or **Off**. Authentication settings are only available for devices running iOS 7.1 or later. If devices running iOS 7.0 and earlier are assigned an authentication profile, the devices are automatically enrolled using staging authentication.

- If you turn on **Authentication**, each user must tie a DEP device to their own user account.
- If you turn off **Authentication**, you can enable staging of all devices under a single user account, and extra configuration options appear on the Settings page to accommodate this option.

If you set Authentication to **On**, then configure:

Setting	Description
Device Ownership Type	Determines the ownership type of the device upon enrollment, which can be either Corporate-Dedicated or Employee-Owned.
Device Organization Group	Select the organization group your where your end users authenticate. Only end-user accounts created at this level or a parent above it can authenticate their devices. End users can authenticate using either their Active Directory credentials or basic Workspace ONE UEM credentials, depending on which authentication type you have enabled under Enrollment settings.
Custom Prompt	Turn **On** Custom Prompt to enable custom text to appear on the device authentication screen during the Setup Assistant. Authentication occurs when end users are prompted for their credentials. For Apple School Manager, turn **Off** Custom Prompt if you are deploying shared iPads.
Message Template	Select a message template to send as a Custom Prompt. (Supported for English-language only.) This option is not available when **Custom Prompt** is **Off**.

If you turn Authentication **Off**, then configure:

Setting	Description
Default Staging User	Select the Enrollment User assigned to the device.
Device Ownership Type	Select the ownership type of the device upon enrollment, which can be either Corporate-Dedicated or Employee-Owned.
Device Organization Group	Select the organization group where your devices are enrolled.

4 Configure **MDM features** of the device.

Setting	Description
Profile Name	Enter the name of the profile as it appears in the UEM console.
Department	Enter the name of your department as it appears in the device's **About Configuration** panel upon setup and enrollment.
Support Number	Enter your organizational support contact phone number as it appears in the device's **About Configuration** panel upon setup and enrollment.
Require MDM Enrollment	Select **Enable** and require end users to enroll into Workspace ONE UEM MDM. Use this setting to ensure end-user devices cannot be activated unless they enroll into Workspace ONE UEM MDM.

Setting	Description
Supervision	Enable the option to set the device in Supervised mode, which is an alternative to configuring Supervised devices using Apple Configurator. Supervision is required for shared devices.
Shared Devices	Enable the option to use Shared iPads for Business or Shared iPads for Education. This option must be enabled for shared devices using Apple Business Manager or Apple School Manager, respectively.
Lock MDM Profile	Select **Enable** and prevent end users from unenrolling from Workspace ONE UEM MDM. This setting ensures that end users cannot remove the Workspace ONE UEM MDM profile installed on the device. This option can only be enabled if Supervision is enabled.
Anchor Certificate	Enable this option to upload the certificate as a trusted anchor certificate and push to devices during the DEP enrollment. These certificates are used as trusted anchor certificates when evaluating the trust of the connection to the MDM server URL. If no certificate is uploaded, the built-in root certificates are used.
Device pairing	Enable the option to allow the device to sync with any Workstation through iTunes, Configurator, and iPCU. Optionally, set Device Pairing to **Disable** when deploying education functionality, and **Upload** a **Device Pairing Certificate** for supervised identities. From Workspace ONE UEM 9.2.2, you can upload Device Pairing Certificates whether Device Pairing is set to Enabled or Disabled.
Await Configuration.	Enable this setting if the MDM server is expected to send extra commands before the device can allow the user to proceed in the Setup Assistant. Await Configuration is required for the education functionality. To override the Await Configuration setting on a device, navigate to **Device > Details View** and select the device to override. Select **More Actions > Device Configured**, note the device as configured, and skip the Awaiting Configuration screen during enrollment. If you enable **Await Configuration**, more options appear in the **Setup Assistant** section.
Auto Advance Setup	Enable this setting to apply the DEP configuration automatically to an enrolling device. Users can skip all setup panes, and the device is automatically set to the most restrictive option by default within around 30 seconds after network active. Applies to ethernet-connected macOS 11.0+ and tvOS devices only.

5 Select the items seen by end users during the Apple **Setup Assistant** workflow that appears after the device is powered on for the first time. For Apple School Manager, **Skip** all Setup Assistant options.

Setting	Description
Passcode	Select **Don't Skip** and require the user to set a passcode during setup. If an MDM passcode profile is already set up through Workspace ONE UEM, select **Skip**.
Touch ID	Select **Don't Skip** and prompt the user to configure Touch ID during setup.
Location Services	Select **Don't Skip** and prompt user to enable or deactivate Location Services during setup. If you plan on tracking GPS locations for your devices, select **Don't Skip**.
Restoring from Backup	Select **Don't Skip** and prompt user to restore from the backup during setup. You must select **Don't Skip** to allow users to move data from a previous device, including an Android Device.
Move from Android	If **Restoring from Backup** is set to **Don't Skip**, select **Don't Skip** in this pane to prompt users to move accounts and data from an Android device during setup.

Setting	Description
Sign in with Apple ID and iCloud	Select **Don't Skip** and prompt the user to sign in with an Apple ID and iCloud account during setup.
Terms of Use and Conditions	Select **Don't Skip** and prompt users to read and accept the Terms of Use and Conditions during setup.
Siri	Select **Don't Skip** to prompt the user to configure Siri. If you select **Skip**, Siri is deactivated on enrolled devices.
Diagnostics	Select **Don't Skip** and prompt the user to enable or deactivate sending diagnostic data to Apple. If you select **Skip**, sending diagnostic data is deactivated on enrolled devices.
Registration	Select **Don't Skip** and prompt the user to register the device with Apple during setup.
Apple Pay	Select **Don't Skip** and prompt the user to set up an Apple Pay account during setup. If you select **Skip**, Apple Pay is deactivated on enrolled devices.
Zoom	Select **Don't Skip** and prompt the user to enable the zoom functionality during setup.
FileVault 2	Select **Don't Skip** and prompt the user to set up a FileVault account. The device determines whether or not to display this setup step.
Display Tone	Select **Skip** and allow users to skip the display tone setup step for enrolling iOS devices.
Home Button Sensitivity	Select **Skip** and allow users to enroll devices without configuring the Home button sensitivity on enrolling iOS devices.
Tap to Setup	Select **Skip** and allow enrolling tvOS devices to enroll without an associated iOS device.
Screen Saver	Select **Skip** and allow users to enroll a tvOS device without configuring a screen saver.
Keyboard	Select **Skip** and omit the prompt for users to select a keyboard type during the Setup Assistant process.
Onboarding	Select **Skip** and prevent users from viewing on-boarding informational screens for the user education during the Setup Assistant process.
Watch Migration	Set to **Skip** and prevent users from viewing options for the watch migration during the Setup Assistant process.
Device to Device Migration	Set to **Skip** and prevent the users from being informed about device to device migration during setup.
iCloud Analytics	Set to **Skip** and omit a user prompt to send analytics to iCloud during setup.
iCloud Documents and Desktop	Set to **Skip** and prevent users from viewing iCloud Documents and Desktop screen in macOS.
TV Home Screen Sync	Set to **Skip** and prevent users from toggling the TV home screen layout during setup.
TV Provider Sign In	Set to **Skip** and prevent users from signing in to a TV provider during setup.
Where is the TV?	Set to **Skip** and omit the **Where is this Apple TV** screen on tvOS devices enrolling through DEP.
Privacy	Set **Skip** and omit the **Privacy** screen in the DEP setup assistant while onboarding.
iMessage And FaceTime	Set to **Skip** and prevent the iMessage and FaceTime prompt during setup.
Software Update	Set to **Skip** and prevent informing users about Software Updates during setup.
Screen Time	Set to **Skip** and prevent informing users about Screen Time during setup.

Setting	Description
SIM Setup	Set to **Skip** and prevent users from viewing the SIM Setup screen during setup.
Welcome	Set to **Skip** the Get Started screen during setup.
Express Language	Set to **Skip** the Express Language Setup screen during setup.
Preferred Language	Set to **Skip** the Preferred Language Order screen during setup.
Appearance	Set to **Skip** the Choose Your Look screen during setup.
Primary Account Setup	This item appears only if **Await Configuration** is set to **Enabled**. Select **Don't Skip** to require users to create an account during setup. Configure the type of account the user creates in **Account Type**. Select **Skip** if you have created a Directory Profile for the user and they do not need to create an account. Configure the admin account for this selection in the **Admin Account Creation** section and auto log in after the Setup Assistant is deactivated.

6 For certain configurations detailed in the **Setup Assistant** configuration, use the **Primary User Account** section to define the type of account the end users are allowed to create at the end of the setup. create an admin account for local and remote macOS device admin actions.

Setting	Description
Primary Account Creation	
Account Type	This item appears only if the **Primary Account Setup** is set to **Don't Skip**. Select **Standard** and give users access to a standard user account on their macOS device. If you select Standard, you must create an admin account to manage the Standard account. Select **Administrator** and allow users to create an Administrator account on their macOS device.
Autofill	Enable the option to auto populate the primary account information.
User Name	Enter the account name for the primary account. To automatically populate the enrollment user's organization user name, use the lookup values, such as {EmailUserName}, {EnrollmentUser}.
Full Name	Enter the full name for the primary account. To automatically populate the enrollment user's first and last name, use the default lookup values, such as {FirstName}, {LastName}.
Allow Editing	If the option is deactivated and the primary account user name and full name is predefined, the user cannot modify the User Name and Full Name fields in Setup Assistant. **Note** Allow editing is applicable only if Autofill is enabled.
Create New Admin Account	Enable the option to create a managed admin account during the DEP enrollment. Currently, on macOS only one managed admin account can be created.
Admin Account Creation	
User Name	Enter the account name for the admin account.
Full Name	Enter the full name for the admin account.
Unique Random Password	Generate a unique random password of 14 characters, with at least 2 symbols, 1 lowercase, 1 uppercase, and 1 digit. If enabled, cannot be changed back to static password. (macOS 10.11)

Setting	Description
Password	Deactivate Unique Random Password toggle to create a static password for the account. This password will be used for all assigned devices that enroll with this configuration.
Hidden	Select **Enabled** and hide the admin account on the macOS device. Hidden accounts are not visible in the Login Window to end-users. Select **Disabled** and make the admin account visible when a user logs in.

7 Select **Save** to view the **Summary** page and review the settings you have selected. Assign the settings to devices registered in the Device Enrollment Program.

Setting	Description
Sync Now and Assign to All Devices	Select **Yes** and save and deploy the DEP profile settings to all devices that are currently registered with the MDM server that you just created in the DEP portal. Selecting **No** saves the DEP profile settings but does not deploy them to devices.
Auto Assign Default Profile	Select **Yes** and push the DEP profile settings to all devices that are currently registered once they are synced with Workspace ONE UEM**and** any devices from that point on as they are newly registered with Apple and synced with Workspace ONE UEM. Selecting **No** means that the newly registered devices do not automatically receive the DEP profile settings. Enable this setting if you plan to create multiple DEP profiles for different devices.

8 Once the deployment options are configured, select **Save**. You are now ready to manage profiles on DEP-enabled devices from the UEM console.

What next: Assign devices to the virtual MDM container in Apple Business Manager portal, so they can be managed through the UEM console.

Assign and Manage Devices

Associate and Disassociate Devices in Apple Business Manager Portal

Associate devices with the MDM server in the DEP portal so that they can be synced and managed with Workspace ONE UEM. You can assign additional devices later using these same steps, if necessary.

Associate Devices in ABM

Perform the following steps:

1 Log into the Apple Business Manager portal and select Apple's Device Enrollment Program.

2 Select **Device Assignment > Manage Devices** in the left pane to assign DEP-enabled devices to the MDM Server you already created.

3 Select the method for associating devices and **Choose Devices**:

- **Serial Number** – You can enter a list of device serial numbers.

- **Order Number** – You can enter your Apple Purchase Order number and have devices added automatically.
- **Upload a .csv File** – Upload a CSV file listing the serial numbers.

4 Select **Assign to Server** as the **Action** and select the **MDM server group**.

5 Click **Done**.

You have successfully associated the devices to the MDM server group.

Disassociate Devices in ABM

If necessary, you can manually disassociate a device from the Apple Business Manager. Do this if the device was lost or stolen.

1 Return to the Apple Business Manager portal and manually disassociate it from the MDM server that you initially created.

2 Navigate to **Device Assignments** > **Choose Devices**.

3 Enter the **Serial Number**.

4 In Choose Action, select **Unassign Devices** and click **Done**.

5 To sync the devices in the Workspace ONE UEM, navigate to **Devices** > **Enrollment Status**.

6 In the **ADD** dropdown menu, select **Sync Devices** and click **Sync**. Follow the prompt to complete the process.

Apple Business Manager Device Enrollment

3

Enroll devices to Apple Business Manager portal to use with the Workspace ONE UEM MDM profile and settings provisioned onto the device.

Overview

Using a registered device, follow the standard iOS Setup Assistant process, including language, country or region, and Wi-Fi network. From this point, the Setup Assistant flow is determined by settings in the DEP profile that was assigned to the device.

The Setup Assistant will not show features that you decided to skip. It only shows screens related to what you choose not to skip. Once automatic configuration and enrollment is complete, the Setup Assistant closes and the device is ready for use.

For iOS devices enrolled using Apple Business Manager, enrollment restrictions do not apply. This is because device information such as OS version, device model and more is only received after the device has been enrolled through DEP.

Enroll Apple Devices Using Apple DEP

Since the device is registered with the Apple Business Manager, follow the Setup Assistant on the device to complete device enrollment using Apple Business Manager.

The Setup Assistant displays the options that were chosen when the DEP profile was created for that device. If you require end users to generate their own enrollment tokens in the Self-Service Portal, they must complete that step before enrolling their devices. For more information about end-user generated tokens, see *Alternate Device Enrollment Flows*.

To enroll a device:

1 When you get a brand new device, complete the steps in the Setup Assistant. If prompted, log in to the device with user credentials. If it is an old device and to enroll the device through automated enrollment, device has to be factory reset.

2 Verify that Supervised status is enabled by navigating to **Settings** in a device. Under the Device Name, you will see a notification that the device is Supervised.

3 Verify that the MDM profile is not removable by navigating to **Settings > General > Profiles** and selecting the Workspace ONE UEM MDM profile. You will see that there is no option in the form of an icon to remove the profile.

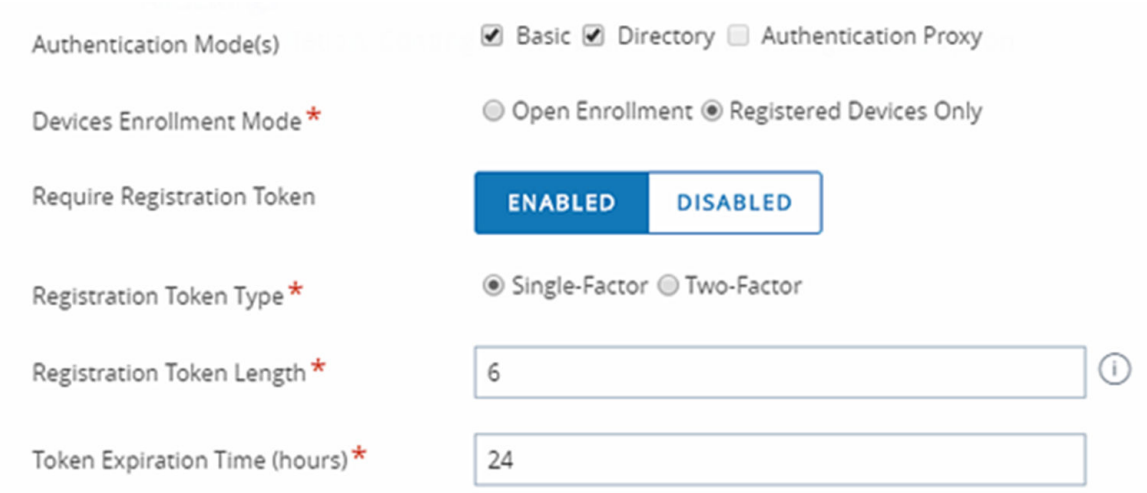
For more information on DEP Enrollment for tvOS devices and macOS devices, see **VMware Workspace ONE UEM Apple tvOS Platform Guide** and **VMware Workspace ONE UEM macOS Platform Guide**.

Enable Registration Tokens for DEP Enrollment

If you restrict enrollment to registered devices only, you have the option of requiring a registration token. This option increases security by confirming that a particular user is authorized to enroll.

To enable token-based enrollment:

1 Select the appropriate organization group and navigate to **Devices > Device Settings > Devices & Users > General > Enrollment** and ensure the **Authentication** tab is selected.Scroll down past the **Getting Started** section and select **Registered Devices Only** as the **Devices Enrollment Mode**. A checkbox labeled **Require Registration Token** will appear in which you should insert a check mark. This will restrict enrollment to only registered devices.



2 Select a **Registration Token Type**.

- **Single-Factor** – The token is all that is needed to enroll.

3 Set the **Registration Token Length**. This required field denotes how complex the Registration Token is and must contain a value between 6 to 20 alphanumeric characters in length.

4 While you can set the **Token Expiration Time** (in hours), note that it does not apply to DEP devices at this time.

Alternative methods for generating an enrollment token exist. For more information, see *Alternate Device Enrollment Flows*.

DEP Profile Settings for Token Enrollment

Use a DEP profile with **Authentication** set to **On** to prompt the user to enter credentials – a username and password – during the Setup Assistant process. If **Require Registration** with a **Single-Factor** token is enabled for the organization group which has DEP configured, the user must enter the one-time token that is sent to them into both the username and password fields.

Use a DEP profile with **Authentication** set to **On** to prompt the user to enter credentials – a username and password – during the Setup Assistant process. If **Require Registration** with a **Single-Factor** token is enabled for the organization group which has DEP configured, the user must enter the one-time token that is sent to them into both the username and password fields.

Generate a Registered Enrollment Token

A DEP token allows your end users to enroll their devices simply and securely.

To generate a DEP token:

1 In the Workspace ONE UEM console, navigate to **Add > Batch Import**.

2 Select Batch type **Users And/Or Devices**. You may chose to use a Simple Template or Advanced Template depending on your need.

3 To generate a Token, map an enrollment user to DEP device serial number. This generates a token and deliver it to the user according to their preferred method of notification, which is specified under User Settings.

- For security reasons, the tokens are not accessible through the UEM console.

Note Once the MDM profile is installed on the device, the token is considered "used" and cannot be used to enroll other devices. If enrollment was not completed, the token can still be used on another device.

Alternate Device Enrollment Flows

Combining the functionalities of the Apple Business Manager's DEP service and the AirWatch Self-Service Portal, you can enable alternate end-user enrollment flows.

Alternate enrollment flows:

- The end users generate their own enrollment tokens in the AirWatch Self-Service Portal.
  - To enable this option, you must have the Self-Service Portal enabled for your end users.
  - The generated token is valid for the expiration time set in Token Enrollment settings in the Admin Portal.

- The admin generates an enrollment token in the UEM console without entering a device serial number.
  - Either the admin or the end user can enroll the device with the generated DEP token, which is configured and sent in the usual way.
  - The generated token is valid for the expiration time set in Token Enrollment settings in the Admin Portal.
  - An advantage of this enrollment flow is that neither admins nor end users are required to enter the device serial number during enrollment. This function is useful in deployments where devices are not preassigned to users, such as in a school setting.
- The admin generates an enrollment token using the bulk upload option in the UEM console, specifying the device serial number.
  - Either the admin or the end user enrolls the device using the generated DEP token, which is configured and sent in the usual way.
  - A token generated using the Bulk Upload method has no expiration date.
  - For more information about uploading device serial numbers in bulk, see *Associate and Disassociate Devices in Apple Business Manager Portal*.

Perform Enrollment with the Registered Enrollment Token

Once you have sent the DEP Registration Token to the end user, perform the enrollment on the device.

To perform the enrollment with a registration token:

1 Turn on the device.

2 Complete the setup screens as part of the Setup Assistant.

  For more information on these settings, see *Create or Edit the DEP Enrollment Profile*.

3 On the authentication screen that requires a username and password, the user must enter the token they received into both the username and password fields. The end user must enter the same token information under both Username and Password. To keep the end user informed you can define the message that will be shown on the authentication screen to direct the user to enter the token under both username and password.

  For more information, see *Enable Registration Tokens*.

Custom Enrollment in DEP

Custom Enrollment is a configurable option within the Automated Enrollment (formerly known as DEP) for admins. Custom Enrollment provides a customized experience to users enrolling into Workspace ONE UEM with devices added to Apple Business Manager. It allows admins to input a custom web view during the Automated Enrollment flow as opposed to the traditional Apple rendered user name and password prompt.

Features of Custom Enrollment

Custom Enrollment provides the option to configure a collection of customized enrollment screens to simplify the user experience and enforce additional security controls. Some of the possible enrollment options you can configure are:

- Terms of Use
- Basic authentication
- Token authentication
- Multi-factor authentication
- SAML federation to an identity provider
- Branding

The Enrollment settings (**Groups & Settings > All Settings > Devices & Users > General > Enrollment**) at an Organization Group determines the enrollment options.

The Branding settings (**Groups & Settings** > **All Settings** > **Settings** > **System** > **Branding**) such as company logo, login page background determines the branding options.

Note The Organization Group is not the Organization Group of the uploaded DEP token.

Enable Custom Enrollment

Enable the Custom Enrollment feature in the DEP wizard while configuring the first DEP profile during the setup.

Prerequisites

Custom Enrollment is available for iOS 13 and macOS 10.15 and later devices only. If you require assistance in setting up the integration to Apple Business Manager, follow the steps in *Configure the Apple Business Manager Portal* and *Download the Public Key to Integrate with Apple Business Manager*.

Procedure

1 Navigate to **Groups & Settings > All Settings > Devices & Users > Apple > Device Enrollment Program**.

2 To create a profile, select **Add Profile** or to update an existing profile, select **Edit Profile**.Enable **Custom Enrollment.**

When the Custom Enrollment is enabled, it demands for authentication and uses some of the settings from the enrollment settings defined at the **Groups & Settings > All Settings > Devices & Users > General > Enrollment** page. For more information about the enrollment authentication and restriction settings, refer to the *Managing Devices* guide

What to do next:

To save the profile, follow instructions from step 3 explained in the *Create or Edit the DEP Enrollment Profile* section.

View Device Enrollment Status

Check the enrollment status of your devices to view DEP-specific information, and generate reports when needed.

To view:

1 Navigate to **Devices > Lifecycle > Enrollment Status**in the UEM console. In addition, DEP-specific devices can have one of the following **Enrollment** statuses:

- **Discovered** – Devices that are synced into Workspace ONE UEM but are not assigned a DEP Profile. These devices would not receive the MDM enrollment prompt during the Setup Assistant.
- **Registered** – Devices are assigned a DEP Profile and you will see the MDM enrollment prompt during the Setup Assistant.
- **Enrolled** – Devices are enrolled into Workspace ONE UEM MDM and can now be managed from the **Devices > List View** page.

2 Go to **Layout** and make column selections to view specific information about enrolled devices.

- **Serial Number** – Device's unique serial tracking number.
- **Asset Number** – Internally allocated device tracking number.
- **Profile** – DEP profile assigned to the device.
- **Department** – Department attached to the DEP profile assigned to the device.
- **Source** – Designates whether the device is associated with the Device Enrollment Program.

DEP Device Management

4

Before you can manage any DEP-enabled devices, you must sync them from the UEM console after you register them with Apple.

Sync Apple DEP Devices Manually

If you selected **Sync Now and Assign to All Devices**, then the registered devices are automatically synced when you save your DEP Profile. If you decide to add more devices later, perform a manual sync using the instructions below or wait for the DEP sync scheduler to run.

1 Navigate to **Devices** > **Lifecycle** > **Enrollment Status.**

2 Select the devices to sync.

3 Navigate to **Add** > **Sync Devices** and follow the prompt to complete the process.

- **Sync Devices** – This option is available only after the DEP is set up in the console. Selecting this option populates the UEM console with any newly registered devices from Apple Business Manager. It also automatically assigns the current **Default Profile Assigned for Newly Synced Devices** to devices, if the feature was configured earlier.

Note The Workspace ONE UEM console supports the ability to **Fetch All Devices**. See the *Best Practices for Using Tokens* topic to know when to use each option.

Use the DEP Sync Scheduler

While manual sync can be issued at any time, Workspace ONE UEM syncs with Apple services to add or remove devices to UEM to match what is configured in Apple Business Manager or Apple School Manager every 24 hours by default. Configure the sync schedule by accessing the DEP Scheduler in the UEM console. The Scheduler settings are only available to System Administrators at the Global organization group level.

To use the DEP Sync Scheduler:

1 Navigate to **Groups & Settings** > **All Settings** > **Admin** > **Scheduler**.

2 In the Scheduler page, click the pencil icon next to the job name **Device Enrollment Program Update**.

3 In the **Device Enrollment Program Update**, determine the **recurrence type** and enter the following.

- Schedule Type - Enter the type of the scheduler. For example, Daily/Monthy/Weekly.
- Frequency - Enter the frequency greater than or equal to 10 minutes.
- Interval Type - Enter the interval type. For example, hours/minutes.

4 Determine the range for the schedule. Enter the start date and time.

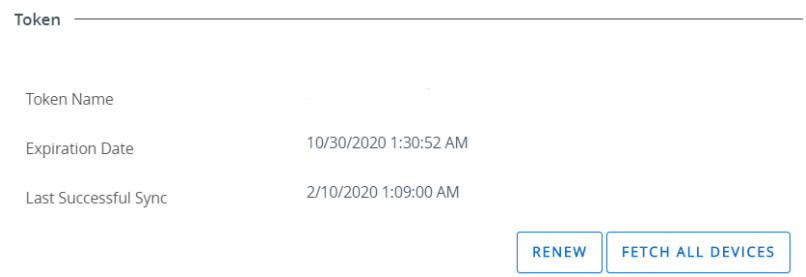
5 Select **Save** to add this schedule to the list.

Renew Your Apple Server Token for DEP Deployments

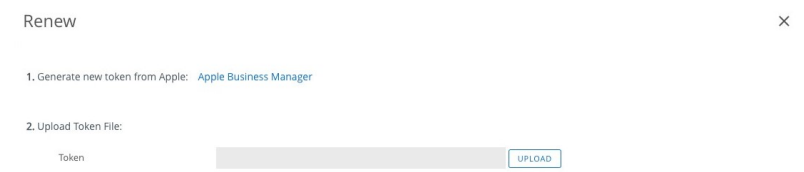
Your Apple server token file is valid for one year, after which time you must renew it. To renew your Apple server token after configuring the DEP, perform the following steps:

1 Go to **Groups & Settings** > **All Settings** > **Devices & Users** > **Apple** > **Device Enrollment Program**

2 Click the **Renew** button and the following screen appears.



Note **Last Successful Sync** indicates the last time a successful DEP device sync was completed for a DEP account. The **Fetch All Devices** synchronizes all the Apple Business Manager enrolled devices with the UEM console, including the devices that were already synchronized. The **Fetch All Devices** option must be used when the devices are not synchronizing even after using the **Sync Devices** from the **Enrollment Status** page. Use the **Fetch All Devices** as a final alternative to synchronize devices.



3 Navigate to the Apple Business Manager, click **Settings**, select your MDM server, and download the Apple server token.

4 Navigate to the Workspace ONE UEM console and click **UPLOAD** to upload the token file.

5 Click **Save** to renew your Apple server token.

Best Practices for Using Server Tokens

Follow the best practices for uploading tokens to any organization group in the UEM console.

- The token determines which device you can assign that profile to. Administrators can add profiles for the tokens at the current, parent, or child organization groups where the DEP is configured.
- Administrators can override DEP settings and add a new token at the child organization groups.
- Review the **Last Successful Sync** time to view when the most recent successful DEP device synchronization was completed for a DEP account.
- Use the **Sync Devices** option on the **Enrollment Status** page to manually synchronize the new devices and updates into Workspace ONE UEM.
- The **Fetch All Devices** option synchronizes all the devices assigned to this token in Apple Business Manager with the UEM console, including the devices that are already synchronized. This option must only be used as a final alternative to fully refresh and resynchronize all your devices from Apple Business Manager.

Perform Remote Actions on All Devices

You can perform various remote actions on devices that are enrolled to Apple Business Manager using DEP.

1 Navigate to **Devices > List View > Select Device**.The **Details View** appears.

2 Select **More Actions** and choose from the following education-specific actions.

Table 4-1.

Option	Description
Device Configured (Admin)	Send this command if a device is stuck in an Awaiting Configuration state.
iOS updates (Admin)	Select individual devices or devices in bulk to update devices.
Enable/Disable Lost Mode	Lock a device and send a message, phone number, or text to the lock screen. Lost Mode is disabled by administrators only. When Lost Mode is disabled, the device returns to normal functionality. Users are sent a message that tells them that the location of the device was shared.
Request Device Location	Query a device in Lost Mode, and then access the Location tab to find the device. (iOS 9.3 + Supervised)

Delete DEP Device Records

You can remove DEP-enabled device records from the Device List View in the UEM console for enrolled devices while the device remains registered with the Device Enrollment Program in the Apple Business Manager portal.

It is recommended that you do not delete an enrolled DEP device. Instead, you must device wipe it and then you can delete it from the console. Once this device record is deleted, the device status changes from enrolled to unenrolled. Simply factory wipe the device and re-enroll it.

1 Navigate to **Devices** > **List View.**

2 Select the devices to delete.

3 Navigate to the **More** drop-down menu.

4 Select **Admin** > **Delete** .

Note The UEM console only allows you to delete a device record from the **Devices** page. You are prevented from manually deleting a DEP-enabled device from the **Enrollment Status** page. To manually delete a device, see *Associate and Disassociate Devices in Apple Business Manager Portal*. If you delete a device that is enrolled, it sends an enterprise wipe.

Wiping DEP-enrolled Devices

You should not perform an enterprise wipe through Workspace ONE UEM on an enrolled device. Instead, perform a device wipe, so the user is forced to re-enroll when it is reactivated.

To discourage an enterprise wipe on DEP enrolled devices, Workspace ONE UEM displays an additional warning in the UEM console when performing the command.

Apple Business Manager DEP Profile Management

5

After the first DEP profile is initially created, create profiles quickly without having to return to the DEP wizard. This allows you to create multiple profiles to use for different deployments.

To create and push DEP profile:

1 Navigate to **Groups & Settings > All Settings > Devices & Users > Apple > Device Enrollment Program**. Since you already configured a DEP profile using the Workspace ONE UEM Setup Wizard, a new screen displays.

2 Select **Add Profile**.

3 Configure the settings for a new DEP profile, as described when using when using the profile wizard earlier.

4 **Save** the profile. This profile is added to the list of other profiles.

5 From the **Default Profile Assigned for Newly Synced Devices** menu, select the DEP profile you want to automatically assign to all devices upon being synced into Workspace ONE UEM. If you do not wish to push a DEP profile to new devices, select **None**.

Edit an Existing DEP Profile

Modify existing DEP profiles to more closely meet the needs of your organization or deployment.

To edit an existing DEP profile:

1 Navigate to **Groups & Settings > All Settings > Devices & Users > Apple > Device Enrollment Program**. The DEP profiles you have already created appear.

2 Select the **pencil icon** to edit the profile. The **Edit Profile** window appears.

3 Edit the DEP profile settings from this window. Settings are not applied until the changes register during the Setup Assistant.

4 Select **Save**.

Manually Assign or Remove a DEP Profile

For Apple School Manager deployments, you must assign profiles to the appropriate devices after creating them for both Shared iPad and one-to-one configurations.

1 Navigate to **Devices > Lifecycle > Enrollment Status.**

2 Select the devices needed for the action.

3 Select the **More Actions > DEP Profile** and select one of the following options:

- **Assign Profile** – Assign new or additional DEP profiles to selected devices. The DEP profile is not updated on a device until the device is factory wiped or re-connected to Wi-Fi.
- **Remove Profile** – Removes existing DEP profiles from selected devices.

Volume Purchase Program (VPP) Application Management

6

To distribute public applications and custom applications to large deployments of Apple iOS and macOS devices, integrate Workspace ONE UEM with Apple Business Manager. Apple Business Manager is a portal for administrators to manage the Device Enrollment program (DEP), Volume Purchase Program (VPP), Apple IDs, and content distribution in their organizations. Apple Business Manager with Workspace ONE UEM powered by Workspace ONE UEM Mobile Device Management (MDM) solution makes it easy to enroll devices and deploy content. Apple Business Manager has consolidated the management features that you have been using through the DEP and VPP portals. Once your organization upgrades to Apple Business Manager from Apple Deployment programs, the DEP and VPP portals will no longer be used to manage devices, assignments, apps purchases, or manage content.

For information on the Device Enrollment Program (DEP) and the Volume Purchase Program (VPP), see Apple Business Manager .

Volume Purchase Program (VPP)

To distribute App Store applications and custom applications to Apple iOS and macOS devices, utilize Volume Purchase Program by integrating Apple Business Manager and Workspace ONE UEM.

The Apple Business Manager enables organizations to purchase publicly available applications for distribution. Any paid application from the App Store is available for purchase, in volume, at the existing App Store price. Custom applications can be free or purchased at a price set by the developer.

See Apple's website for the availability by country and for other details.

Supported Content for Purchased Applications

Workspace ONE UEM supports various content types in the purchased section. The level of management varies according to the method used to get the content and the platform.

View support by operating system, application type, acquirement method, Managed Distribution (**MD**), or Redemption Codes (**RC**). The letters **DB' represents** systems that can retrieve applications without an Apple ID, and an **X** represents no support.

Table 6-1. Supported Purchased Content by Platform and OS Version

Operating System	Free Public Apps	Purchased Public Apps	Free Custom Apps	Purchased Custom Apps
Apple iOS 7.x – 8.x	MD & RC	MD & RC	MD & RC	MD & RC
Apple iOS 9+	MD, RC, & DB	MD, RC, & DB	MD & RC	MD & RC
macOS 10.9 – 10.10	MD	MD	X	X
macOS 10.11-10.15	MD & DB	MD & DB	X	X
macOS 11.0+	MD & DB	MD & DB	MD & DB	MD & DB

Deploy Volume Purchase Program 7

To purchase and deploy content with Apple Business Manager's Volume Purchase Program (VPP), enroll and acquire content on the Apple Business Manager site and then use Workspace ONE UEM to distribute content.

1 Content Purchase – Purchase content in the bulk through the App & Books in Apple Business Manager.

2 Application Deployment – Distribute the assets throughout your device fleet using redemption codes or managed distribution service token files (sTokens).

- Redemption Code Method
- Managed Distribution by Apple IDs
- Custom Applications
- Managed Distribution by Device Serial Number

Redemption Code Method

This method uses redemption codes to allocate the content to devices, and it does not support revoking the codes from Apple iOS devices. Once the redemption code is redeemed, it cannot be recycled. Also, Workspace ONE UEM cannot delete content bought using redemption codes off devices.

Devices older than Apple iOS 7 must use this method for purchasing VPP content because the managed distribution is not available for older systems.

You cannot use redemption codes for macOS systems.

Complete All Tasks to Distribute Redemption Codes

For the successful distribution of the Apple's Volume Purchase Program (VPP) content to end users, perform all steps of the deployment process. In return, end users must complete all steps on their devices to receive the VPP content.

1 Admins send VPP content to end users.

   a Purchase your applications and download your redemption code spreadsheet from the Apple iTunes Store.

   b Upload the spreadsheet to Workspace ONE UEM.

c Allocate redemption codes to organization groups and smart groups in the Workspace ONE UEM console and save the settings.

2 End-Users receive content.

This step occurs automatically when admins publish the content.

a Obtain a redemption code from Workspace ONE UEM.

b Install the content from the catalog.

Upload a Redemption Code Spreadsheet

You can use Workspace ONE UEM to manage and distribute applications and books purchased through the VPP to your Apple iOS devices. Apple uses Web services to manage redemption codes. For the Workspace ONE UEM console to access Apple's Web services, you must first upload the redemption code spreadsheet.

1 Navigate to either **Resources > Apps > Orders** or **Resources > Books > Orders**.

2 Select **Add** or **Order** to add a redemption code spreadsheet.

3 Select **Purchased Public App** or **Purchased Custom App** (Custom app), for applications.

This option is not available for books.

4 Select **Choose File** to upload the **CSV** or **XLS** file that you downloaded from the Apple portal.

This action creates the order.

5 Select **Save** to continue to the **Product Selection Form**.

6 Locate the appropriate product and choose **Select** to finish uploading the spreadsheet. If your spreadsheet contains an Adam ID, Workspace ONE UEM does not display this step.

- If your spreadsheet contains an Adam ID, you do not have to locate the product. Workspace ONE UEM automatically adds applications and books from the app store when the spreadsheet contains the Adam ID. Adam IDs are specific to iTunes, are components of the Apple Search API, and are unique for each application.
- If the Apple VPP redemption code spreadsheet contains codes for multiple applications or books, Workspace ONE UEM lists several products on this form. You can select only one per order.

iTunes uses Adam IDs, which are item identifiers, to automate connections to content. If your spreadsheet contains an Adam ID, then you do not have to locate applications and books in the app store. For custom applications, the Adam ID enables Workspace ONE UEM to update application IDs in the UEM console.

Assign Content to Users

You must enable the Workspace ONE UEM console to assign redemption codes to users and devices. Select the applicable organization groups and smart groups to which to assign redemption codes.

1 Navigate to the organization group where you uploaded the redemption code spreadsheet.

2 Go to **Resources > Apps > Native > Purchased**.

3 Select the application you want to assign.

4 On the **Orders Assignment** tab, complete the following options.

Table 7-1. Orders Assignment Tab Options - General

Setting	Description
Redemption Codes On Hold	Enter the number of redemption codes that you want to place on hold. Use this option to save the redemption codes for later use.
SDK Profile	If you use AirWatch SDK functionality, assign an SDK profile to the application.
Add Assignment By	Assign redemption codes to organization groups or smart groups. ■ **Organization Group** – Allocate redemption codes to an organization group. Select **All Users** to include all users in that organization group, or choose Selected **Users** to display a list of users in the organization group. Use the **Add** and **Remove** buttons to choose the specific users to receive the application. ■ **Smart Group** – Allocate redemption codes to a smart group by typing the name of the group. Options display and you can select the appropriate smart group from the list. You can create a new smart group, if necessary. ■ You can apply redemption codes to organization groups and to smart groups simultaneously. However, you can only specify the users for organization groups of the **Customer** type. ■ You cannot specify users for smart groups. However, you can edit the smart group so that it contains the necessary users. ■ Verify the information in the following columns for each assignment rule: ■ **Users** – View the number of users for the order. ■ **Allocated** – Enter the number of licenses to allocate to the selected users. Do not exceed the total number in the order. ■ **Redeemed** – View the number of licenses that have already been redeemed, if any.

Table 7-2. Orders Assignment Tab Options - Deployment

Setting	Description
Assignment Type	■ **On Demand** – Deploys content to a catalog or other deployment agent. The device user can 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.

Table 7-2. Orders Assignment Tab Options - Deployment (continued)

Setting	Description
	■ **Automatic** – Deploys content to a catalog or other deployment Hub on a device upon enrollment. After the device enrolls, the system prompts users to install the content on their devices. This option is the best choice for content that is critical to your organization and its mobile users. You can only use **On-Demand** for custom B2B applications acquired using redemption codes. When the **Assignment Type** is **Auto**, only eligible Apple iOS 7+ devices receive the application or book automatically.
Remove On Unenroll	Set the removal of the application from a device when the device unenrolls from Workspace ONE UEM. Workspace ONE UEM enables this option by default. If you choose to enable this option, supervised devices are restricted from silent app installation because the device is locked and the provisioning profile installation is in the command queue which requires a device to be unlocked to complete the installation. If you choose to deactivate this option, provisioning profiles are not pushed along with the installed application. That is, if the provisioning profile is updated, the new provisioning profile is not automatically deployed to devices. In such cases, a new version of the application with the new provisioning profile is required. Removing an application when a device is unenrolled does not recover the redeemed code. When installed, the application is associated to the app store account of the user.
Prevent Application Backup	Deactivate backing up the application data to iCloud. However, the application can still back up to iCloud. This restriction will work only for managed Apps. It will not work for unmanaged Apps.
Make App MDM Managed if User Installed	Assume management of applications previously installed by users on their devices, supervised and unsupervised. Enable this feature so that users do not have to delete the application version installed on the device. Workspace ONE UEM manages the application without having to install the AirWatch Catalog version on the device.

Table 7-2. Orders Assignment Tab Options - Deployment (continued)

Setting	Description
Use VPN	Configure a VPN at the application level, and select the **Per-App VPN Profile**. Users access the application using a VPN, which helps ensure that application access and use is trusted and secure.
Send Application Configuration	Send application configurations to Apple iOS devices, so users do not have to configure these specified values themselves.

5 Select **Save** when you finish allocating codes.

Application configurations are vendor-specific key-value pairs you can deploy with an application to preconfigure the application for users.

Redemption Code Information

Access information about your redemption codes so that you can manage and track your VPP deployments.

To access orders of applications you acquired using redemption codes, navigate to **Resources > Orders > Redemption Codes**.

- View the availability status of the code.

  Table 7-3. Redemption Code Status Descriptions

Status	Description
Available	Identifies an available key code to use to distribute the purchased content. You can make this key code unavailable or delete it.
Externally Redeemed	Identifies a key code that was assigned and redeemed outside of the Workspace ONE UEM Purchased (VPP) system. You cannot perform actions for this key code.
Redeemed	Identifies a key code that was assigned and redeemed within the Workspace ONE UEM Purchased (VPP) system. You can make this key code unavailable or delete it.
Unavailable	Identifies a key code that was explicitly made unavailable for various reasons. Reasons include separating codes that you want to save for users who might not be in your Workspace ONE UEM deployment.

- View each redemption code and the order number.
- View the date the redemption code was redeemed.
- View to whom the code is assigned.
- Delete a redemption code.

Managed Distribution by Apple IDs

This method uses service token files, also called sTokens, to authenticate assignments. It allows you to assign license codes to Apple IDs to allocate content to devices, and the method supports the revocation and recycling of these license codes.

Introduction

With Apple's Managed Distribution system integration with Workspace ONE UEM, you can distribute your free and purchased Volume Purchase Program (VPP) applications and books. The managed distribution model uses service tokens (also called sTokens) to retrieve your VPP contents and to distribute them to devices using the Workspace ONE UEM console.

Revoke Managed Distribution Licenses

Workspace ONE UEM can revoke licenses for applications but it cannot revoke licenses for books.

Complete All Tasks For Managed Distribution by Apple IDs

For successful distribution of VPP content to end users, perform all steps of the deployment process. In return, end users must complete all steps on their devices to receive VPP content.

1 Admins send VPP content to end users.

   a Purchase content and download your sToken from the Apple iTunes Store.

   b Upload the sToken to Workspace ONE UEM.

      You can use multiple sTokens within your Workspace ONE UEM hierarchy but you can only have one sToken in each organization group.

   c Sync licenses to display the content in the console.

   d Add the bundle IDs for custom applications. This action activates management.

      This step is unnecessary for non-B2B applications and books.

   e Allocate licenses and assign licenses to smart groups, and enable eligible applications for device-based assignment, if applicable. Then publish managed distribution content with the flexible deployment feature.

      Publishing content triggers invitations to end users whose content is tied to their Apple IDs.

2 End-Users accept invitations and receive content.

   a Accept the invitation and register with the Apple VPP.

      This step is not necessary for device-based use. This step ensures that they have the terms of agreement for participating in the program.

   b Obtain the license from Workspace ONE UEM.

   c Install content from the catalog.

Users that have multiple Apple iOS devices must select and apply a single Apple ID to all the devices. If admins make content available on demand, then users can accept the invitation and join and register with the VPP. They install the content from the catalog to any of their devices.

Upload VPP sTokens to Retrieve Managed Distribution Licenses and Content

Apple uses Web services to manage license codes. The Workspace ONE UEM console accesses Apple's Web services with the service token, or sToken, you upload to the console. Workspace ONE UEM retrieves your VPP content with the license data on the sToken.

You can upload an sToken at the top Customer level and below. The Workspace ONE UEM system prompts you to register your sToken, so thatWorkspace ONE UEM can detect if the sToken is used in other environments.

1 Navigate to **Groups & Settings > All Settings > Devices & Users > Apple > VPP Managed Distribution**.

2 Configure the following settings.

Table 7-4.

Setting	Description
Description	Enter your VPP Account ID. Using your VPP Account ID as the description has several advantages. ■ If you use multiple sTokens, it identifies the correct account. ■ Reminds you the correct account when you renew the sToken. ■ Identifies the correct account to others in your organization who assume management of the VPP account.
sToken Upload	Select **Upload** to navigate to the sToken on your network. VPP accounts in Apple School Manager and Apple Business Manager can now be associated to locations to allow moving licenses from one VPP account to another. If an sToken that is associated to a location is uploaded, the location name is displayed in the console.

Table 7-4. (continued)

Setting	Description
Automatically Send Invites	Send invitations to all the users immediately after you save the token. The invitation request users to join and register with Apple's VPP. Registration gives users access to the terms of use to participate in the program. Use the **Message Preview** option to review the invitation. If your environment includes VPP applications set to the **Assignment Type, Auto**, then Workspace ONE UEM sends invitations no matter how you configure this option. This behavior facilitates quick access to applications upon enrollment. Workspace ONE UEM automatically sends users of Apple iOS v7.0.3+ and macOS 10.9+ (if supported) an invite command when you enable this option. It does not send them an email message. You do not have to enable this option immediately. You can leave it deactivatedd and still upload your token. Return and enable this feature to send invitations to all the enrolled devices whose users have not yet accepted to join the VPP. For Device-Based VPP, deactivated this check box for the device-based VPP system because invitations are not necessary. If you assign a device-based VPP device to a regular VPP app (a user-based VPP app), devices still receive invitations.
Message Template	Select an email template for an email message invitation for Apple iOS devices on Apple iOS v7.0.0 through v7.0.2.

3 **Save** the sToken and confirm the addition of the token.

Sync Managed Distribution Content

Workspace ONE UEM has two methods that sync-managed distribution content, by assets and by license.

The assets function syncs the metadata on an sToken and claimed licenses information. The license function syncs information for a single asset. It is useful for sTokens that contain thousands of licenses and you only want to sync the licenses applied to one asset.

- Sync Licenses
  a Go to the organization group where you uploaded the sToken.
  b Navigate to one of the following areas.
    - **Resources > Apps > Native > Purchased**
    - **Resources > Books > List View > Purchased**

c Select the asset check box and select **Sync Licenses** option from the actions menu.

- Sync Assets
  a Go to the organization group where you uploaded the sToken.
  b Navigate to one of the following areas.
    - **Resources > Apps > Native > Purchased**
    - **Resources > Books > List View > Purchased**
  c Select **Sync Assets**.
  d Confirm to register an sToken with Workspace ONE UEM, if applicable. The system prompts for registration if it detects an sToken is used in another environment.
  e To select that the sync completed, refresh the screen.

    Workspace ONE UEM syncs purchased asset meta data and if there are claimed licenses, the system syncs for those assets of the claimed licenses. Workspace ONE UEM makes the sync features inaccessible until reconciliation completes.

Custom Applications and VPP

You can upload custom applications acquired through Apple Business Manager's Volume Purchase Program (VPP) to Workspace ONE UEM. Workspace ONE UEM works with the redemption code method and with the managed distribution method.

The ability of Workspace ONE UEM to manage custom applications, depends upon the VPP system used to get the applications.

- **Redemption codes** – Workspace ONE UEM can install custom B2B applications bought using redemption codes on to devices. End users can install these applications on-demand, but Workspace ONE UEM cannot manage these applications. Upload custom B2B applications acquired with redemption codes like other applications acquired with redemption codes.

  Go to *Redemption Code Method* for details.

- **Managed distribution** – Workspace ONE UEM can install custom B2B applications bought using managed distribution. End users can install these applications on-demand or you can push these applications automatically. Workspace ONE UEM can manage these applications. Upload custom B2B applications acquired with the managed distribution like other applications acquired with the managed distribution. However, between the sync-steps and assign-steps, activate management of the applications.
  - Go to *Managed Distribution by Apple IDs* for details on uploading applications acquired with the managed distribution.
  - Go to *Activate Management of Custom B2B Applications* for details to activate management.

VPP, Custom Applications, and Push Mode

Workspace ONE UEM can manage custom applications acquired with managed distribution codes but it cannot manage custom applications acquired with redemption codes.

The ability of Workspace ONE UEM to manage the custom application determines the push modes available to distribute the application.

Table 7-5. Push Mode Depends on VPP Management

VPP Method	Management Ability	Available Push Mode
Managed distribution	Manage Workspace ONE UEM can manage custom applications acquired with managed distribution codes.	Auto On-Demand
Redemption code	Cannot manage Workspace ONE UEM cannot manage custom applications acquired with redemption codes.	On-Demand

Activate Management of Custom Applications

When you acquire applications from Apple's Volume Purchase Program (VPP) with managed distribution codes, Workspace ONE UEM automatically displays all metadata for all applications it deems as custom applications. The systems retrieve the metadata such as the icon, the name, and the bundle ID from an Apple metadata service for App Store apps (public and custom).

As an admin, you have the option to edit the metadata text box. The Bundle Id text box should be deactivated if the custom application information is retrieved from the content metadata service. Applications you do not activate for management display as **Inactive** in the UEM console.

Note To update to the latest version of a custom application, as an admin, you can navigate to the **Resources > Apps > Native > List View > Purchased** option and select the custom application from the purchased applications list view and click the **UPDATE APP** option. The devices with a lower version of the custom application installed automatically get updated to the latest version and the devices with the latest custom application version already installed have no impact.

Managed Distribution by Device Serial Number

If your VPP deployment consists of iOS 9+ or macOS 10.11+ devices, consider enabling the assignment of Volume Purchase Program (VPP) applications by device serial number. This method removes the need to invite users to the VPP.

Deploy device-based VPP applications using the outlined processes in *Managed Distribution and Workspace ONE UEM*.

Workspace ONE UEM does not migrate applications to the device-based system. VPP applications already assigned to Apple IDs remain assigned as such.

Benefits

The device-based system offers several advantages.

- Users do not have to accept invitations and register with the VPP.

- Admins with multiple sTokens in their VPP deployment do not have to manage invitations.
- Admins do not have to manage Apple IDs.

Uses

Device-based assignment is the best choice for deployments in the following scenarios.

- Shared devices with check-in and check-out systems
- Corporate owned devices
- Staged environments with one-device-to-one-user ratios
- Devices in Workspace ONE UEM for Education deployment

The user-based system is the best choice for the following scenarios.

- Multiple devices assigned to a single Apple ID
- Need to conserve licenses

Supported Platforms and Operating Systems

Configure a supported OS to use the device-based method to distribute applications acquired through Apple's Volume Purchase Program (VPP).

- iOS 9+
- macOS 10.11+

App Eligibility

Developers of VPP applications must enable the applications for use in the device-based VPP.

Invitations

With the Apple ID removed from the process, the device-based method no longer relies on invitations to register Apple IDs. However, if a device meets the requirements, the system still sends invitations.

- Device does not use iOS 9+ or macOS 10.11+
- App is not enabled for device-based VPP use
- Device receives a user-based VPP application
- **Automatically Send Invites** is enabled in Workspace ONE UEM

Deploy Device-Based VPP

The process to upload device-based (serial number) applications is similar to uploading user-based (Apple ID) VPP applications. The only difference is that the device-based method does not involve sending invitations.

Important Once an application is enabled for device-based use in the Workspace ONE UEM console, you cannot reverse its status and use it in the user-based system.

1 Upload or register an sToken in the desired organization group in Workspace ONE UEM.

Skip this step if you already have sTokens in Workspace ONE UEM

a If you do not want Workspace ONE UEM to send invitations to devices, deactivated **Automatically Send Invites**.

Workspace ONE UEM prompts you to register an sToken with the Workspace ONE UEM environment. It sends invitations automatically for user-based applications that have an **Auto** push mode.

2 Assign and publish device-based VPP applications with the flexible deployment feature

During the assignment process, Workspace ONE UEM prompts you to enable applications for the device-based method with the setting **Enable Device Assignment**.

3 Access license and application information using the Licenses page, the Device Details page, and the Manage Devices page.

4 Revoke licenses with various management functions.

- Unenroll devices.
- Select the revoke action on the information pages (Licenses, Device Details, and Manage Devices pages).
- Deactivate and delete assignments.
- Remove devices from smart groups assigned to the VPP application.

Update Device-Based VPP Applications Manually or Automatically

Configure automatic updates or manually push updates to device-based VPP applications at the application level. This feature offers management of updates by Workspace ONE UEM or allows you to push updates as a way to control application versions.

This feature does not work for the managed distribution by Apple ID. The VPP application must be enabled for the device-based distribution, also called distribution by device serial number. For general information about the managed distribution method by device serial number, see *Managed Distribution by Device Serial Number*. This topic includes supported operating systems, benefits, and the need for no VPP invitations.

Note The non-device-based VPP applications are tagged as **Not Applicable**, such VPP applications are not supported for this feature.

System Behavior on Initial Setup

The system automatically queues application installation commands at the time you first configure the **Enable Auto Updates**. Workspace ONE UEM stores the currently available application version number from the App Store in the database. Workspace ONE UEM can automatically trigger install commands for devices to perform application updates if they report a version below the currently available version from the App Store. Workspace ONE UEM system regularly checks the App Store for updates and records any new versions in the database to continue the process.

Update Challenge for Device-Based VPP Applications

Device-based VPP applications had update issues due to their disassociation from the Apple ID. Workspace ONE UEM developed a system to help with the updates of device-based applications. You can configure automatic updates or manually push updates.

Challenge

In the device-based VPP method of managed distribution, the device serial number is the connection between licenses and the application. It replaces the Apple ID. However, the update of the application is still tied to the Apple ID because the Apple ID is tied to the purchase history. Device-based applications can miss updates because the Apple ID is removed from the license-assignment process.

Solution

Workspace ONE UEM checks the app store for updates of your device-based VPP applications and identifies when updates are available in the UI.

Enable automatic updates for device-based VPP applications and Workspace ONE UEM updates these applications whenever it identifies an updated is available.

If you want to control the version of an application, leave automatic updates deactivated and manually push updates when needed.

Configure Licenses and Assign with Flexible Deployment

8

To retrieve the data on the sToken, Workspace ONE UEM syncs with Apple Web services, and then displays the content for assignment and deployment. Workspace ONE UEM distributes licenses by smart group and publishes the content when you save an assignment rule in the flexible deployment feature.

The **Enable Device Assignment** option displays for applications that are eligible for distribution by device serial number. For information about the device-based distribution method, see *Managed Distribution by Device Serial Number*.

For information on flexible deployment and how to prioritize assignment rules, see Add Assignments and Exclusions to your Applications in the *Application Management* guide.

To publish with flexible deployment, assign content acquired from Apple's Volume Purchase Program (VPP) with managed distribution codes to smart groups.

1 Navigate to **Resources > Apps > Native > Purchased**.

2 Select the application and select **Assign**. The Assignment page appears.

3 On the **Assignment** page, select **Add Assignment** and complete the options.

   a In the **Distribution** tab, enter the following information.:

Setting	Description
Name	Enter the assignment name.
Description	Enter the description for the assignment.

Setting	Description
License Distribution	Enter the smart group name to which you want to assign the application and the number of licenses you want to allocate. As you enter the smart group name, options are displayed and you can select the appropriate smart group from the list. The allocated licenses must not exceed the total number of available licenses. You can also view the number of licenses that have already been redeemed, if any. If necessary, you can add more assignment groups.
App Delivery Method	■ **On Demand** – Deploys content to a catalog or other deployment agent. The device user can 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 Hub on a device upon enrollment. After the device enrolls, the system prompts users to install the content on their devices. This option is the best choice for content that is critical to your organization and its mobile users. If the Assignment Type is set to **Auto** when you **Publish**, Workspace ONE UEM sends an invitation to Apple iOS 7.0.3+ and macOS 10.9+ devices. The invitation enables users to register with Apple's VPP.

b In the **Restrictions** tab, enter the following information:

Table 8-1.

Settings	Descriptions
Remove on Unenroll	Set the application to be removed from a device when the device unenrolls from Workspace ONE UEM. Workspace ONE UEM enables this setting by default. If you enable this setting, supervised devices are restricted from silent app installation. This is because the device is locked and the provisioning profile installation is in the command queue which requires a device to be unlocked to complete the installation. If you deactivate this setting, provisioning profiles are not pushed with the installed application. That is, if the provisioning profile is updated, the new provisioning profile is not automatically deployed to devices. In such cases, a new version of the application with the new provisioning profile is required.
Prevent Application Backup	Disallow backing up the application data to iCloud. However, the application can still back up to iCloud.

Table 8-1. (continued)

Settings	Descriptions
Prevent Removal	If you enable this setting, the user is prevented from uninstalling the app. This is supported in iOS 14 and later.
Make App MDM Managed if User Installed	Assume management of applications previously installed by users on their devices, whether applications are supervised or unsupervised. Enable this feature so that users do not have to delete the application version installed on the device. Workspace ONE UEM manages the application without having to install the AirWatch Catalog version on the device.

c In the **Tunnel & Other Attributes** tab, enter the following information.

Settings	Description
Per App VPN Profile	Select a VPN profile that you want to use for the application. Users access the application using a VPN, which helps ensure that application access and use is trusted and secure.
Other Attributes	App attributes provide device-specific details for applications to use. For example, when you want to set a list of domains that are associated to a distinct organization.

d In the **Application Configuration** tab, enter the following information.

Settings	Descriptions
UPLOAD XML	You can upload an XML file that contains the key value pairs supported by the application for the app configuration.

4 Select **Create**.

5 Select **Add Assignment** to add more assignments for your publication.

6 Configure the flexible deployment settings by setting the priority for your app assignments.

Settings	Descriptions
Priority	Select the value from the drop-down menu to set the precedence for the assignments. Devices receive applications from the assignment groups based on the priority set for the assignment groups. Adjusting the priority for a single assignment automatically reprioritizes other assignments.
Copy	From the more options menu, select copy to duplicate the selected assignment.
Delete	From the more options menu, select delete to remove the selected assignment.

7 Select **Save & Publish**.

Methods to Revoke Managed Distribution Licenses

Workspace ONE UEM offers several ways to revoke managed distribution licenses so that you can reuse them. You can manually revoke licenses. The system revokes licenses in response to you deleting or unassigning another system component like organization groups, sTokens, and smart groups.

See what methods are available to you to revoke your managed distribution licenses for reuse.

Table 8-2. Descriptions of Revoking Methods

Revoke Method	Description
Organization Group	Delete an OG and Workspace ONE UEM makes the distribution licenses available for reuse.
User	Unenroll all devices from a user. If another device does not use the unassigned managed distribution license, then the Workspace ONE UEM console revokes it so that it is available for reuse.
Manual	Revoke the license manually off the device. You can use the manual method only for those licenses that are redeemed from an external system. This method is useful for adopting these licenses into Workspace ONE UEM.
App Record	Delete VPP App Record from the UEM console. Once deleted, the license is available for reuse after the scheduler task runs.
sToken	Delete the sToken. Workspace ONE UEM makes all associated licenses available for reuse.
Unassign	Unassign an asset from a user. If that license is not used by anyone else, Workspace ONE UEM revokes the distribution license.
Smart Group	Delete a managed distribution device user from a smart group. If that license is not used by anyone else, Workspace ONE UEM revokes the distribution license.

Workspace ONE UEM makes licenses available immediately after revoking or at a scheduled interval depending on the interval you set in the scheduler task, VPP revoke licenses. Find the scheduler task in **Groups & Settings > All Settings > Admin > Scheduler**.

Managed Distribution Information

You can access managed distribution information from the Device Details, Licenses, and Manage Devices pages. Each page offers various auditing and management actions depending on the type of asset

Device Details

From the **Device Details** page, audit assignments and perform installations and removals.

Go to **Devices > List View > Apps** or to **Devices > List View > More > Books**. The system does not support all management functions for all asset types. The system does not display unsupported options.

- View the content assigned to the device.
- If supported, install and remove the content on the specified device.

Licenses

From the Licenses page, track sync processes, audit licenses available for reuse, and revoke licenses if supported.

Go to **Devices > List View > Apps** or to **Devices > List View > More > Books**. The system does not support all management functions for all asset types. The system does not display unsupported options.

- View the content assigned to the device.
- If supported, install and remove the content on the specified device.
- View when assigned licenses were last synced.
- Filter by **License Owner Type** to access licenses that are available to reuse due to error using the **Not Assigned** option.
- For applications, use the **Revoke** action to make licenses available for reuse. This action is not available for books.

Note Workspace ONE UEM has logic to revoke licenses associated with devices or users for redistribution. If a user removes or uninstalls an application, the status is sent to Workspace ONE UEM. The following scenarios describe where Workspace ONE automatically revokes licenses associated with a device or user.

Scenarios
Administrator triggers removal of application
Administrator unassigns application from the device
Device is unenrolled via enterprise wipe, device wipe, or deletion
User removes the application
User rejects the installation or management request (unsupervised devices only)

Manage Devices

From the Manage Devices page, install and remove content, send invitations to join the VPP if supported, and audit application installations and VPP program registrations.

Go to **Resources > Apps > Native > Purchased > Manage Devices** or to **Resources > Books > List View > Purchased > Manage Devices** to access the page. The system does not support all management functions for all asset types. The system does not display unsupported options.

- For applications, install the content to devices. This action is not available for books.
- For application, remove the content from devices, if supported by the asset. This action is not available for books.
- Notify devices concerning the VPP.
- Reinvite user-based VPP members who have not registered their Apple IDs with the program.
- Filter data using the **Status** option and find devices that have not installed VPP content.
- Filter data using **User Invite** and find those user-based members who have not registered their Apple IDs with the program.

Staging Users and Managed Distribution for VPP

Workspace ONE UEM with Apple Business Manager's Device Enrollment Program (DEP) and Volume Purchase Program (VPP) and Apple Configurator, you can deploy and manage large numbers of Apple iOS devices These programs aim to help maintain and manage bulk device and content.

To reduce the risk of license inconsistencies, review these suggestions and guidelines for deploying VPP content to devices that you stage using Configurator and the DEP.

Note This information does not apply to VPP applications assigned to device serial numbers.

Avoiding License Inconsistencies

Distribute VPP content bought using the managed distribution method:

- Use a service token (sToken) in one MDM environment and not in multiple environments. Some examples include not using an sToken in Workspace ONE UEM and in another MDM system or in a trial environment and in a production environment.
- Use an sToken in one organization group and not in multiple organization groups within Workspace ONE UEM.
- Apply one device to one Apple ID and do not change the Apple ID on the device.

These actions reduce the risk of losing a license in one environment because it was revoked in another environment. However, it cannot be economically possible to have the number of licenses to cover your staged devices using these actions. VPP deployment in a staged environment is still manageable but it can take extra maintenance with special attention paid to the Apple ID.

Apple IDs

When user enrolls with Workspace ONE UEM and then Workspace ONE UEM registers the user with Apple and sends an invitation to join the Apple VPP. The user accepts the invitation and joins the VPP using the Apple ID. Currently, Workspace ONE UEM stores the association of the Apple ID with the user.

It is important to manage the Apple ID in staged environments because the Apple ID controls access to the user's specific set of VPP content. When users change Apple IDs on devices without communicating the change to their admins, they might experience access difficulties. Workspace ONE UEM follows the listed procedure when an admin uploads a service token to the console. This procedure outlines how the system ties the Apple ID users and all that user's licenses.

1 Admin uploads service tokens to Workspace ONE UEM console.

2 Workspace ONE UEM registers all users who have devices enrolled.

3 Workspace ONE UEM sends invitations to users.

4 Users accept invitations with an Apple ID.

5 Workspace ONE UEM ties the Apple ID to the user.

6 Workspace ONE UEM ties all licenses assigned to that user to the Apple ID.

Guidelines for Staging

Use the following processes to reduce license inconsistencies in Workspace ONE UEM.

Table 8-3. Staging and VPP

Staging Method	Assign VPP Content To	Accepts VPP Invitation	Installs applications	Updates applications	Maintenance	Risks
Single User, Standard (Self-Registration)	Individual devices with unique Apple IDs **Not a staging user**	End users with unique Apple IDs	End-users install applications	End-users update applications	No maintenance of Apple IDs	Least risk because end users maintain their own Apple IDs on individual devices
Single User, Advanced (Pre-Configured)	Pre-configured devices with pre-configured Apple IDs	End users with pre-configured Apple IDs	End-users install applications	End-users update applications	■ Maintain pre-configured Apple IDs ■ Provide pre-configured Apple IDs to end users	■ End-users change Apple IDs ■ End users do not return devices to the pre-configured Apple ID
Multi Users	■ Staging user ■ Individual users	■ Admin with the staging user Apple ID ■ End users with respective unique Apple IDs	■ Admin installs common applications with staging user Apple ID ■ End-users install unique applications with individual Apple IDs	■ Staging user ID must update common applications with staging user Apple ID ■ End users update unique applications with their individual Apple IDs	■ Maintain a staging user Apple ID for a common set of VPP content on all devices selected to staging user ■ Maintain end-user Apple ID at device check-out	■ All devices selected in to the staging user do not have the same Apple ID ■ Admins do not change devices to the staging user Apple ID upon device check-in ■ End users do not change the staging user Apple ID to their unique Apple IDs upon device check-out

Shared iPads for Business

9

Shared iPads for Business is a solution developed by Apple to enable users based on their Managed Apple IDs. Multiple users can check in and check out of the iPad. User's Managed Apple IDs are created in Apple Business Manager often through federation to a third-party Identity Provider such as Azure Active Directory.

As users log in with their Managed Apple ID, the managing MDM provider is notified of this change and can perform personalized actions to only show the resources needed by the targeted user.

When a user signs into an iPad, the user is automatically provisioned with a separate partition of the device's disk space. This ensures that the user's data is separated from all other users and data saved by the user is captured to their Managed Apple ID iCloud storage.

Deployment Prerequisites

Know about the software and hardware requirements for deploying Shared iPads for Business.

Minimum Device Requirements

- iPads with 32 GB storage or higher and iOS 13.4 and later. To know more about device requirements, see Apple documentation here.

Integration Requirements

The following tasks must be completed before you configure Workspace ONE UEM Shared iPad functionality.

Accounts

- **Apple Business Manager** - Register your user id with Apple Business Manager and create an administrator account. See, Apple Documentaion here. For information on integrating DEP with Workspace ONE UEM, see Apple Business Manager Device Enrollment Program in *Integration with Apple Business Manager* Guide.
- **Managed Apple IDs** - Credentials required to sign into Shared iPads to access Apple services. For more information, see *Managed Apple IDs*.

Configuring Shared iPads

Workspace ONE UEM allows you to configure Shared iPads using the UEM console.

Perform the following task to set up a Shared iPad in the Workspace ONE UEM console.

1 Configure a DEP profile. For more information on how to add a DEP profile, see *Create or Edit the DEP Enrollment Profile*.

Note While adding a profile, select the following options specifically to enable shared devices:

- **Custom Enrollment**: OFF
- **Authentication**: OFF
- **Staging Mode**: Multi user device
- **Default Staging User**: Enter the staging user
- **Shared Devices**: Enabled

2 To assign a profile, navigate to **Devices** > **Lifecycle** > **Enrollment Status** > **Select a Device** > **More Actions** > **Assign a Profile**. For more information, see *Manually Assign or Remove a DEP Profile*.

3 If you want to assign smart groups only for shared devices, see Create a Smart Group.

Note In Enrollment Catagory, you must select **Selected** as Apple - Shared iPad.

4 Configure Managed Apple IDs for your enrollment users. For managing Apple IDs, see *Manage Apple IDs*.

5 To select which Organization Group a Shared iPad will move when a user logs in, navigate to **All Settings** > **Devices & Users** > **General** >**Shared Device**. Select the appropriate option.

Note Since there is no method to Prompt User for Group ID, selecting this option will default to using a Fixed Organization Group.

Shared iPad Apps

When any user logs in, the data belonging to that user is accessible and other user's data is securely stored in separate partition. When users log in and out of the Shared iPad, they only want to see the apps that are assigned and applicable to their account. One way to do this is to install all a user's apps when they log in and remove them when they log out. However, this is slow and inefficient because users must wait for apps to install on each login.

Prerequisites

Only Internal and Device Based Licensed apps synced from Apple Business Manager (public and custom) are supported on Shared iPads.

With the Shared iPad for Business in Workspace ONE UEM, apps that are assigned to a user will only be installed on that user's first login to the Shared iPad. Each subsequent login will not reinstall the assigned apps. After the user logs out, these apps will be hidden rather than removed. This provides a better, secure experience as the device is shared among multiple users.

Note Internal apps will install as new apps if the currently installed version is different than the highest assigned version of the logged in user. This occurs even if the new version is lower than the currently installed version. For example, if version2 of an app is installed on the device, but version1 is the highest version assigned to the logged in user, version1 will be installed and replace version2.

Here is a simple workflow to describe the typical Shared iPads app management concept.

1 You get a new iPad and it is enrolled. A first user User1 logs in and that user is assigned App1, App2, and App3 and set for automatic deployment. All three apps are installed for the first time. User1 logs out.

2 User2 logs in and is assigned App3, App4. For User2, App1 and App2 are hidden automatically using a restriction configuration profile. This is managed by Workspace ONE UEM and doesn't require any admin actions to deplo. App3 is displayed because User2 is assigned this app and App4 installs for the first time on user's iPad.

At any point, for any user, only user's assigned apps are visible on the screen and the rest is hidden. Other users' data is inherently secure because each user has their own data partition.

Shared iPad Profiles

Profiles for Shared iPads differ slightly from profiles associated to typical one-to-one enrolled devices in that profiles configured to be automatically deployed are sent down during a user log in rather than immediately after enrollment. Each time a user logs into the Shared iPad the profiles assigned to that user are freshly installed on the device. This is to ensure that all profiles have accurate information relative to that user. For Shared iPads, there are two types of profiles that can be installed. These two types are device channel profiles and user channel profiles.

To deploy profiles to Shared iPads, there are no additional steps that must be taken from the typical profile assignment process. For more information on how to create and assign profiles to iOS device, see *Device Profiles* in *Workpsace ONE UEM iOS Platform Guide*.

To configure a profile for the device vs user channel, perform the following steps:

Device Channel Profiles

Device channel profiles in Shared iPads are sent directly to the device. This means that any user that logs in will have all assigned devices profiles installed and applied. All profiles for non-Shared iPads are deployed as device channel profiles. For Shared iPads, not all profile payloads can be deployed in the device channel for which profiles are available.

User Channel Profiles

User channel profiles in Shared iPads are sent directly to a user instead of the entire device. This means profiles are applied to the users that are logged in. Workspace ONE UEM automatically sends any assigned user profiles to the assigned user when they log into the device.

1 Navigate to **Devices** > **Profiles & Resources** > **Profiles** > **Add Profile**.

2 Select **Device** or **User** to configure the profile for the device channel or user channel, respectively.

3 Configure the profile as normal. For more information on configuring configuration profiles, see *Device Profiles* in *Workpsace ONE UEM iOS Platform Guide*.

Managed Apple IDs

Managed Apple IDs are used in accessing Apple services using Apple Business Manager. These user accounts are created through integration with a third party identity provider (IDP) such as Azure Active Directory. By default, these Apple Business Manager Managed Apple IDs are created using the User Principal Name in the IDP but can be changed by an admin.

For Shared iPad users to receive the correct apps and profiles, the Managed Apple ID of the user logging into the device must match an enrollment user within Workspace ONE UEM. By default, Workspace ONE UEM assumes the Email Address value of the enrollment user is the Managed Apple ID. If your users require a different Managed Apple ID format, you can edit this in the **Settings**.

To know more about Shared iPad with Managed Apple IDs, see Apple Documentation here.

1 Navigate to **Settings** > **Devices and Users** > **Apple** > **Managed Apple ID**.

2 Select **Enable Custom Managed Apple ID Format** as **Enabled**.

3 Enter **Managed Apple ID Format** including Lookup Values.

4 Select the **Child Permission**.

- Inherit only.
- Override only.
- Inherit or Override.

5 Click **Save**.

After clicking **Save**, the Managed Apple ID value of all users at that Organization Group will be updated. This will also occur if the Managed Apple ID settings are inherited at lower Organization Groups.

Shared iPad User Workflow

Users log into Shared iPads using their enterprise Managed Apple ID created by their organization's Apple Business Manager tenant through federation to an IDP such as Azure Active Directory. When this occurs, the device updates Workspace ONE UEM which user has logged in and Workspace ONE UEM assigns the device to the enrollment user with the matching Managed Apple ID.

Prerequisites

To ensure Workspace ONE can appropriately associate the device to an enrollment user, the Managed Apple ID of a user logging into a Shared iPad must exist and be globally unique for that Workspace ONE environment.

Note Never delete the multi-staging enrollment user if there are active Shared iPads. This will leave devices that fall into the above category orphaned and the device will need to be wiped and enrolled to a new multi-staging user.

If a user logs into the device with a Managed Apple ID that doesn't exist in Workspace ONE UEM or is associated with more than one enrollment user, the device remains is associated with the multi-staging user originally used to enroll the device.

This is also the case if the user begins a Temporary Session. When this occurs, Workspace ONE UEM will move the device to the multi-staging user originally used to enroll the device.

It is recommended to assign the minimum required apps and profiles to the multi-staging enrollment user, as any user may have permission to log into the device in this way.

Monitor, Logout, and Delete a User

Workspace ONE allows the administrators to view the list of logged in users, delete a user and forcefully log out a user from a Shared iPad device.

View Current User List

In Workspace ONE UEM, navigate to **Devices** > **Details View** > **User List**.

List of active user and other users who have used the device is displayed with the last logged in time, name, managed Apple Id and so on.

Manually Delete a User

Some users are configured on Shared iPads but have not logged in for a while or have left the company. Admins can select such users from the list and delete them from the device.

In **Device Details** > **Details View** > **User List**, select a user and click **Delete.**

You have successfully deleted a user from the Shared iPad Device.

Manually Logout a User

Shared iPad users, when they are idle, they do not appear to be automatically logged out. Workspace ONE enables the admins to manually log out a user. Once the administrator log outs a user, it returns to the main lock screen. The next user can log in and use the Shared iPad later.

To log out a user from Shared iPad, perform the following steps:

1 In the Workspace ONE UEM, navigate to **Devices** > **Details View** > **More Actions**.

2 Select **Admin**.

3 Select **Log Out User**.