How Do You Share Devices in UEM

VMware Workspace ONE UEM services

vmware by Broadcom

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

https://docs.vmware.com/

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

Contents

How Do You Share Devices in UEM

Workspace ONE UEM supports shared devices scenarios for Android, macOS, and iOS platforms. Examples of scenarios that use a shared pool of devices include shared mobile nursing devices for healthcare and shared mobile point of sale devices for retail. For information on how to configure Workspace ONE UEM, find use cases that outline how to set user accounts, how to set up device enrollment, and how to configure and deploy profiles to facilitate your shared devices deployment.

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

Functionality

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

Security

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

Platforms That Support Shared Devices

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

- Android 4.3 or later
- iOS devices with Workspace ONE Intelligent Hub 4.2 or later.
- MacOS devices with Workspace ONE Intelligent Hub 2.1 or later.

Configure Shared Android Devices for your Shift Workers

You can configure Workspace ONE UEM to provide your shift workers, and other roles that share devices, access to corporate resources. Configure and use different apps, policies, and branding based on a user's role. To ensure user privacy, certain apps can have their app data cleared between user sessions. You can use the launcher native to Android or you can use the Workspace ONE UEM Launcher.

Configure Shared iOS Devices for Shift Workers

Workspace ONE UEM offers different solutions to enable iOS devices for shared purposes. You can configure Workspace ONE UEM to provide your shift workers access to corporate resources. This use case outlines how to configure and assign different apps and policies to shift workers based on their roles.

Configure Shared iPads for Business

Shared Device capabilities are available natively on Apple iPads integrated with Apple Business Manager. This functionality called Shared iPads for Business leverages the user's Managed Apple ID for login and does not take place in the Workspace ONE Intelligent Hub for login and logout. For more information, see Shared iPads for Business

Log In and Log Out of Shared Devices

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

Log In and Log Out of Shared iOS Devices

You can log in to and out of an iOS device that is shared across multiple users.

1. Run the Workspace ONE Intelligent Hub on the device.
2. Enter the end-user credentials.

   If the device is already logged in to Workspace ONE Intelligent Hub, then the user is prompted to enter an SSO Passcode. If the device is not logged in, then the user is prompted to enter a user name and password. The profiles assigned to each user are pushed down based on the smart group and user group association.

   Note: If **Prompt User for Organization Group** is enabled, then end users are required to enter a **Group ID** to log in to a device.
3. Select **Login** and accept the **Terms of Use**.

   Note: If prompted for a passcode, users can create one in the Self-Service Portal. These passcodes are subject to an expiration period. As the expiration period nears, the Workspace ONE Intelligent Hub prompts users to change the passcode on the device. If users do not a change their passcode before it expires, users must return to the Self-Service Portal to create another passcode.

Log In and Log Out of Shared macOS Devices

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

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

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

Define the Shared Device Hierarchy in UEM

While strictly optional, making an organization group (OG) specific to shared devices offers many benefits due to multi-tenancy and inherited device settings.

If you have a large number of shared devices in your fleet and you want to manage them apart from single user devices, you can make a shared device-specific OG. Making a shared device hierarchy in your OG structure is optional. Features like smart groups and user groups mean you do not have to rely strictly on OG hierarchy design to simplify device management.

However, having a shared device OG (or nested OGs) simplifies device management by enabling you to standardize device functionality through profiles, policies, and device inheritance without the processing overhead required by a smart group or a user group.

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

Setting	Description
Name	Enter a name for the child organization group (OG) to be displayed. Use alphanumeric characters only. Do not use odd characters.
Group ID	Enter an identifier for the OG for the end users to use during the device login. Group IDs are used during the enrollment of group Devices to the appropriate OG. Ensure that users sharing devices receive the Group ID as it might be required for the device to log in depending on your Shared Device configuration. If you are not in an on-premises environment, the Group ID identifies your organization group across the entire shared SaaS environment. For this reason, all Group IDs must be uniquely named.
Type	Select the preconfigured OG type that reflects the category for the child OG.
Country	Select the country where the OG is based.
Locale	Select the language classification for the selected country.
Customer Industry	This setting is only available when Type is Customer. Select from the list of Customer Industries.
Time Zone	Select the time zone for the OG's location.

5. Select **Save**.

Configure Shared Android Devices for your Shift Workers

Workspace ONE UEM can be configured to provide your shift workers, and other roles that share devices, access to corporate resources. Different apps, policies, and branding can be provided based on a users role. To ensure user privacy, certain apps can have their app data cleared between user sessions.

There are two prominent ways to configure your shared devices:

- Workspace ONE Launcher VMware Workspace ONE UEM Launcher provides a highly customizable experience for your shift workers. You can add custom branding, set app icon positioning, and configure which device settings they should have access to.
- Native Android Using Native Android for shared devices supports simpler use cases that do not require as much customization as Launcher. You can create secondary users, use simple branding, implement restrictions, and limit applications.

Example Uses

- Shared Bank Teller Android device in Financial Services
- Shared Nurse Android device in Healthcare
- Shared mobile Point of a Sale Android device in the retail industry.

Prerequisites

This guide assumes you have knowledge of certain workflows in the Workspace ONE UEM console, and have completed certain steps already:

- The Android EMM registration is complete using managed Google accounts.
- Smart groups are already created. If a certain group of users need a different set of policies and/ or apps, separate smart groups are created for them.
- Internal and/ or private apps for your users are added into the Workspace ONE UEM Console.
- Android devices are running OS version 5.0 or higher. For Workspace ONE Launcher, use Android 5.0 or higher. For Native Android, use Android 9.0 or higher.
- User accounts for your users have been added to the Workspace ONE UEM Console.
- Profiles for applying device policies and network configuration should be created and assigned to your users.

Enrollment Configuration

The best option for the shared device use case is to use Work Managed enrollment with device based accounts. This is based on two key assumptions:

1. Devices used for shared devices typically do not have a single end user associated with them.
2. The enrollment occurs at a central location and then shipped to the location where the devices are used.

Configure Device-based Accounts

Device based accounts is only available when Android EMM is registered using managed Google Accounts.

Device based accounts adds a unique managed Google account on each device, even if the enrollment user is the same. This is important because Google limits how many devices can be used by a single user (limited to 10). With device based accounts, any number of devices can be enrolled with the same user.

To configure device-based accounts in the Workspace ONE UEM console:

1. Navigate to **Groups & Settings > All Settings > Devices & Users > Android > Android EMM Registration > Enrollment Settings**.
2. Set the Work Managed Enrollment Type to Device-Based.

Create a Multi-user Staging Account for Enrollment

Enrolling a device using a multi-user staging account sets up the device for shared use. Once you enable multi user devices, you can check in and check out shared Android devices using native Android capability or Workspace ONE Launcher (see sections below for more information on each option). Additionally, the multi-user staging account simplifies bulk enrollment by enabling you to enroll all your shared devices with this account.

To create a multi-user staging account, follow these steps:

1. Navigate to **Accounts > Users > List View > Add User**.
2. Add the **Username**, **Full Name**, **E-mail**, and **Password** for the account in the **General** tab.
3. Enable **Multi User Devices** under **Advanced > Staging**.
4. Choose **Native** or **Launcher** under **Android Shared Device Mode**. If you select Launcher, proceed to select **Save**.

   When you select **Native**, additional settings display to configure Native Android settings.

Setting	Description
System Apps	Allow end users to access system apps
Admin Passcode Mode	Specify an alphanumeric passcode to troubleshoot a device in admin mode. Tap the Hub icon on the login screeen 5 times to access admin mode.
Confirm Admin Passcode	Reenter admin passcode.

5. Select **Save**

Creating a QR code for Enrollment

To ensure that the enrollment is easy to perform in bulk, the best option is to use a QR code. A QR code can be created within the Workspace ONE UEM console that includes server details, group ID and authentication details. By simply scanning the QR code during the out of box setup, the device enrolls without any further interaction.

To create a QR code in the Workspace ONE UEM console:

1. Navigate to **Lifecycle > Staging > List view**.
2. Select **Configure Enrollment**.
3. Navigate to **Android > QR Code** and select **Configure**.
4. Connect the device to Wi-Fi prior to enrollment by enabling the Wi-Fi toggle. This enabling action displays the following options.

Setting	Description
SSID	Enter the Service Set Identifier, more commonly known as the name of the Wi-Fi Network.
Password	Enter the Wi-Fi password for the entered SSID.

5. Select **Next**.
6. Select the Workspace ONE Intelligent Hub to push to devices during staging. The default selection is **Use latest Workspace ONE Intelligent Hub**. If you do not have an Workspace ONE Intelligent Hub added, select **Hosted on an external URL** and enter the address in the URL text box to point to an externally-hosted Workspace ONE Intelligent Hub Package.
7. Select **Next**.
8. Set the Enrollment Details settings. To use token-based authentication, leave both options disabled.
9. Configure **Organization Group**

Setting	Description
Organization Group	Enable and select the organization group to enroll the device into.

10. Configure **Login Credentials**

Setting	Description
Username	Enable to configure login credentials. Enter the username of the staging account created earlier.
Password	Enter the corresponding password for the staging user.

11. Select **Next**
12. The **Summary** page allows you to the download the QR code as a PDF file.

You can use this QR code for enrolling your Android devices into Work Managed mode.

Native Android Configuration

Using Native Android for shared devices supports simpler use cases that do not require as much customization as Launcher.

Prerequisites

Native Android is supported on the following:

- Android 9.0 or later devices
- Workspace ONE UEM Console 2102
- Workspace ONE Intelligent Hub 2102 for Android

How It Works

To use Native Android Check-In Check-Out, during enrollment the Workspace ONE Intelligent Hub for Android creates a primary user that is set as the Device Owner, which manages the device and the lifecycle of any secondary users created later.

Once a user checks out a device, a secondary user is created silently in the background that contains all the apps and data. The secondary user can only modify or interact with the device as the secondary user. After the user checks in, or logs out, all associated data is cleared from the device and the device is ready for the user displaying the log in screen.

Applications

Consider assigning all apps to the Staging User which originally enrolled the device. This allows pre-loading of applications to the primary user so they are available when your secondary users log in without having to repush from the UEM console or having the user spend time downloading anything.

Migration from Launcher to Native Check-In Check-Out

You can migrate any existing devices meeting the above pre-requisites that are using Workspace ONE Launcher to a Native Android experience by changing the setting in the Staging section of the enrolled Staging user in the Workspace ONE UEM console.

To change the setting:

1. Navigate to **Accounts > Users > List View > Edit User** for the Staging user with which the devices you would like to migrate are associated.
2. Switch to **Advanced > Staging**, and under **Multi User Devices** choose **Native** under **Android Shared Device Mode**.
3. Select **Save**.

On the device side, once the logged in user checks in (logs out of Launcher), the Workspace ONE Intelligent Hub receives the new settings from the UEM console, exits the device out of Launcher, and Intelligent Hub for Android is locked into the foreground to begin the Native Android experience for secondary users to log in.

How to End a User Session

There are several ways to end a session or switch between users when using Native Android Check-In Check-Out:

- Users long press the power button and the **End Session** displays in the available options. The device switches back to the device owner and the login screen for Intelligent Hub for Android is ready for the next user.
- When the device is locked, a native **End Session** option appears on the homescreen. This is useful in the event the secondary user forgets to log out and the next user does not have access to an admin passcode. Once **End Session** is selected, the device switches back to the device owner and the login screen for Intelligent Hub for Android is ready for the next user.

Workspace ONE UEM Launcher Configuration

VMware Workspace ONE UEM Launcher provides a highly customizable experience for your shift workers. You can add custom branding, set app icon positioning, and configure which device settings they should have access to.

Prior to creating a Launcher profile, you should add any internal and/ or public applications that will be used by your shift workers into the Workspace ONE UEM console.

If your shift workers need to have a different set of apps or settings available to them based on their role, you must create multiple Launcher profiles and assign them to the different smart group(s) created based on the role.

Create a Launcher Profile

1. Navigate to **Devices > Profiles & Resources > Profiles > Add > Add Profile > Android**.
2. Under the **General** Tab, provide a name for the profile and assign the profile to smart group(s) that include your shift workers.
3. Select the Launcher payload, select **Configure**.
4. Select **Multi App**.
5. Drag and drop applications from the left to the canvas on the right.
    - Adjust the positioning of the app icon to ensure that shift workers get a consistent experience on any device they sign into at the start of the shift.
    - You can use the **Create Folder** option at the top of the canvas to organize your apps for your shift workers.
6. Under the **Layout**, add a custom wallpaper, if desired.
7. Under the **Settings** dropdown, you can enter an administrative passcode that enables you to exit out of the launcher screen for troubleshooting.
    - Additionally, you can also customize which settings your users can access. Once you're done customizing settings, select **Save**.

- Select **Save** to complete the Launcher configuration.
- Select **Save and Publish**.

For advanced use cases that are not available in the Launcher profile, you can refer to Custom XML for Workspace ONE Launcher.

Clear Data Between User Sessions

You can choose to clear app data for all apps between user sessions.

1. Navigate to **Devices & Users > General > Shared Device > Logout Settings**.
2. Enable **Clear Android App Data**, **Clear Android Device Passcode**, and **Clear Android Accounts**.

Enrolling a Device Using a QR Code

1. Power on the device. The setup wizard prompts the user to tap the Welcome screen six times. The taps have to be done in the same place on the screen.
    - For Android 8.0 devices, proceed to step 2 in order to download the QR Code reader.
    - For Android 9.0 and later devices, the camera will open automatically after you complete the six taps, so you can skip to step 3.
2. Connect to Wi-Fi and the setup wizard automatically downloads a QR code reader. The QR code reader app automatically starts once complete.
3. Scan your QR code. For Android 9.0 or later devices, use the QR code option on the camera to scan.
4. The setup wizard automatically downloads the Workspace ONE Intelligent Hub and enrolls the device using the staging user you created earlier.
5. After enrollment is complete, Workspace ONE Launcher then downloads and launches.

The device is now ready for your shift workers to sign in.

Migration From Native Check-In Check-Out to Workspace ONE Launcher

You can migrate any existing devices meeting the above pre-requisites that are using Native Android to Workspace ONE Launcher by changing the setting in the Staging section of the enrolled Staging user in the Workspace ONE UEM console.

To change the setting:

1. Navigate to **Accounts > Users > List View > Edit User** for the Staging user with which the devices you would like to migrate are associated.
2. Switch to **Advanced > Staging**, and under **Multi User Devices** choose **Launcher** under **Android Shared Device Mode**.
3. Select **Save**.

On the device side, once the logged in user checks in (selects **End Session**, the Workspace ONE Intelligent Hub receives the new settings from the UEM console, exits Native Android configuration and Launcher settings are pushed down when a new user logs in.

Shared Device Mode (SDM) for Microsoft Azure Conditional Access Policies on Android Devices

This section discusses Shared Device Mode for Microsoft Azure Conditional Access Policies on Fully Managed Android devices.

This feature allows customers to alert Azure of which user is currently using a shared device and the current compliance status of that device. This allows customers using Azure Conditional Access to configure policies which allow access to certain Microsoft productivity applications under certain conditions, based on any compliance rules supported by Workspace ONE UEM.

Since a device registered in shared device mode allows for access to company resources based on the device compliance, without the need for each user to go through the remediation and registration process, a one-time registration occurs. The device are registered and grants all users logging into that device access to Microsoft 365 apps upon sign-in to their corporate account.

Requirements to use Microsoft Azure Conditional Access Policies on Shared Devices

- Workspace ONE UEM version 23.06 or later
- Workspace ONE Intelligent Hub version 23.07 or later
- Workspace ONE Launcher version 23.02 or later
    - If you are using Launcher, download v23.02 from the Resource portal if it is not already seeded in your console: Resource Portal Download

Setup

To get started, follow the steps pertaining to Android listed in Use Compliance Data in Azure AD Conditional Access Policies then perform a sync with the following steps:

- In Workspace ONE UEM, perform a sync of Azure Services under **Settings > System > Enterprise Integration > Directory Services > Sync Azure Services**.

Configure Shared Device Mode

Devices must be enrolled in Android Enterprise Fully Managed mode. Workspace ONE Launcher is compatible with Shared Device Mode in the following configurations:

- On the sign-in screen in Check-in/Check-out (CICO) mode
- Single App mode (for use with 3rd party launcher applications)

In the Workspace ONE UEM Console

1. Navigate to **Settings > Devices & Users > Android > Intelligent Hub Settings** and turn on **Register as Shared Device with Azure for Conditional Access**.
2. Add **Microsoft Authenticator** as a Public App (from Google Play) and add a new, or configure an existing, assignment.
3. Within the assignment, go to the **Application Configuration** tab and apply following configuration:

- Shared Device Mode: Enable
- Prefill UPN in Shared Device Mode: Leave this field blank.
- Shared Device Mode Tenant Identifier: enter your Microsoft Tenant ID
- Shared Device Mode Registration token: Enter the lookup value `{SharedDeviceRegistrationToken}` This value will be replaced automatically with the correct key by Workspace ONE UEM.

4. Ensure the app is assigned to devices targeted for Shared Device Mode

New Device Setup

During enrollment, Microsoft Authenticator is launched automatically after it is installed. It will wait to receive the registration token (this may take up to one minute). Once the token is received, registration completes and the device compliance status is relayed to Microsoft. Once the process is complete, and the device is marked as Shared and Compliant in Azure, users are able to login to Microsoft apps.

Note:This registration and setup flow only needs to occur one time per device.

Existing Device Setup

On devices that are already enrolled, Microsoft Authenticator will be launched for SDM registration after the configuration steps are completed.There are two different scenarios based on the home screen launcher that is used:

Workspace ONE UEM Launcher with Check-in/Check-out enabled: Microsoft Authenticator launches automatically to complete the registration after the device is checked in (user signs out) so that the user is not disrupted.

Workspace ONE UEM Launcher in Single App Mode: This scenario is primarily for the use of custom launchers as the primary end user interface. Microsoft Authenticator launches automatically after receiving the configuration to perform the registration.

Note: It is possible to migrate from Launcher Multi-App mode to Single App mode and then kick of the Shared Device Mode registration with Microsoft Authenticator, in the case that Check-in/Check-out is not activated. Just make sure to add Microsoft Authenticator as a hidden app in the Launcher configuration.

After the device is registered, it is listed in your Azure tenant and marked as a Shared Device with the current Compliance status. Users will then be able to sign into Microsoft Apps without any additional remediation steps.

Troubleshooting

This section covers common issues you might run into while provisioning shared devices with Microsoft Conditional Access:

- **Microsoft Authenticator App shows expired authentication error** The app configuration must be pushed to that device again. This can be done by re-pushing the app to the device

from the Workspace ONE UEM console. The app will not be reinstalled, but receives the configuration again.

- **The user is not able to sign into any Microsoft app** Admins should check the Azure tenant to make sure that the device record exists and is marked as ‘Shared’ and ‘Compliant'. If the device record shows this, ask the user to try signing in again. If it shows the wrong status, then check the following:
    - Event Log in the Workspace ONE UEM console
    - Device side ADB logs
    - Checking server logs via VMware support
- **Any other registration failure is encountered (device side or server-side)**
    - Admins can check the following:
    - Event Log in the Workspace ONE UEM console
    - Device side ADB logs
    - Checking server logs via VMware support

Configure Shared iOS Devices for your Shift Workers

Mobile devices are often used to facilitate business functions in multiple vertical industries such as Healthcare, Retail, Transportation, and Banks. Some of these functions are performed with a common pool of shared devices. Organizations around the world choose iPhones and iPads to help facilitate these lines of business functions. Workspace ONE offers different solutions to enable iOS devices for shared purposes. Workspace ONE UEM can be configured to provide your shift workers access to corporate resources. Different apps and policies are assigned to shift workers based on their roles.

Workspace ONE offers multiple solutions for enabling shared use of devices in the enterprise depending on the type of devices you want to use and data separation needs.

Type	User Data Separation	Device Requirements
Check-in Checkout with Hub	Limited. Requires removal and reinstallation of apps to clear app data between users	iOS and iPadOS devices
Native iOS Shared iPads for Business	Complete. Data is separated for each user by the operating system	32 GB+ iPadOS devices (13.4 and later)

Example Usage

- Shared Bank Teller iPad in Financial Services
- Shared Nurse iPhone/iPad in Healthcare
- Shared Mobile Point of a Sale iPad in Retail

Check-in and Check-out with Hub

Intelligent Hub can be configured to operate in a multi-user mode allowing any employee to authenticate within Hub to allow Workspace ONE UEM to customize and configure the managed device with the respective policies and applications for that user.

Note: Apps that require user login, such as Microsoft Outlook and Microsoft Teams, are not logged out automatically when the shared device is checked in and made available for another user to check out. Be sure to manually log out of these apps before you check in your shared device. For added security, uninstall these apps to remove app data between users.

Prerequisites

This guide assumes you have knowledge of certain workflows in the Workspace ONE UEM console, and have completed certain steps already:

- iOS, iPadOS devices (preferably running latest version of iOS).
- Intelligent Hub for iOS. See, App Store.
- Supported version of Workspace ONE UEM. Solution available on all Workspace ONE license offerings (Standard, Advanced, and Enterprise). For more information on supported console versions, see VMware Lifecycle Product Matrix .
- Smart groups are already created for your users. If a certain group of users need a different set of policies and/ or apps, separate smart groups are created for them.
- Configured integration with Apple Business Manager for Automated Device Enrollment and distribution of volume purchased applications.
- Internal and/or volume purchased applications through Apple Business Manager for your users are added into the Workspace ONE UEM Console.
- User accounts for your users have been added to the Workspace ONE UEM Console. Intelligent Hub supports the following types of user authentication:
    - Basic Users
    - Directory Users
    - SAML User (using Workspace ONE Access). For more information on integrating Workspace ONE Access, see Integrating Workspace ONE UEM With Workspace ONE Access .
- Profiles for applying device policies and network configuration must be created and assigned to your users.

Enrollment Configuration

For check-in and check-out with Hub use case, the enrollment configuration includes the following:

Create Multi-staging User Account

Enrolling a device using a multi-user staging account sets up the device for shared use. Additionally, the multi-user staging account can simplify bulk enrollment by enabling you to enroll all your shared devices with this account.

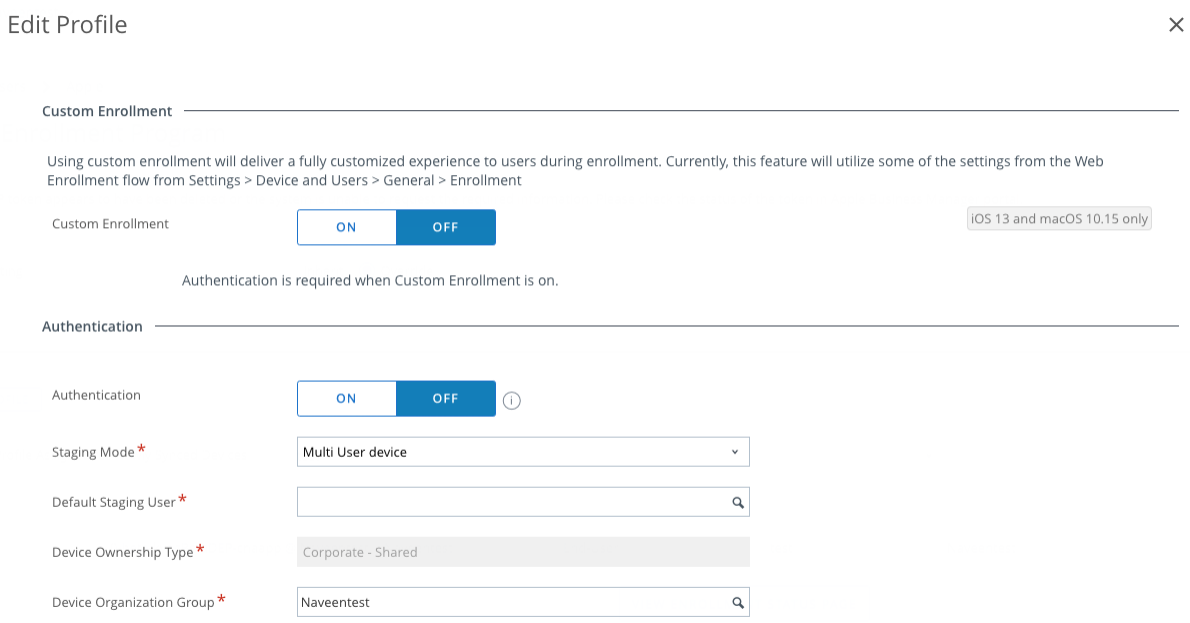
To create a multi-user staging account in the Workspace ONE UEM console:

1. Navigate to **Accounts > Users > List View > Add User.**
2. Add a username, full name, email, and password for the account in the **General** tab.
3. In **Advanced tab > Staging**, enable **Multi User Devices.**
4. Select **Save.**

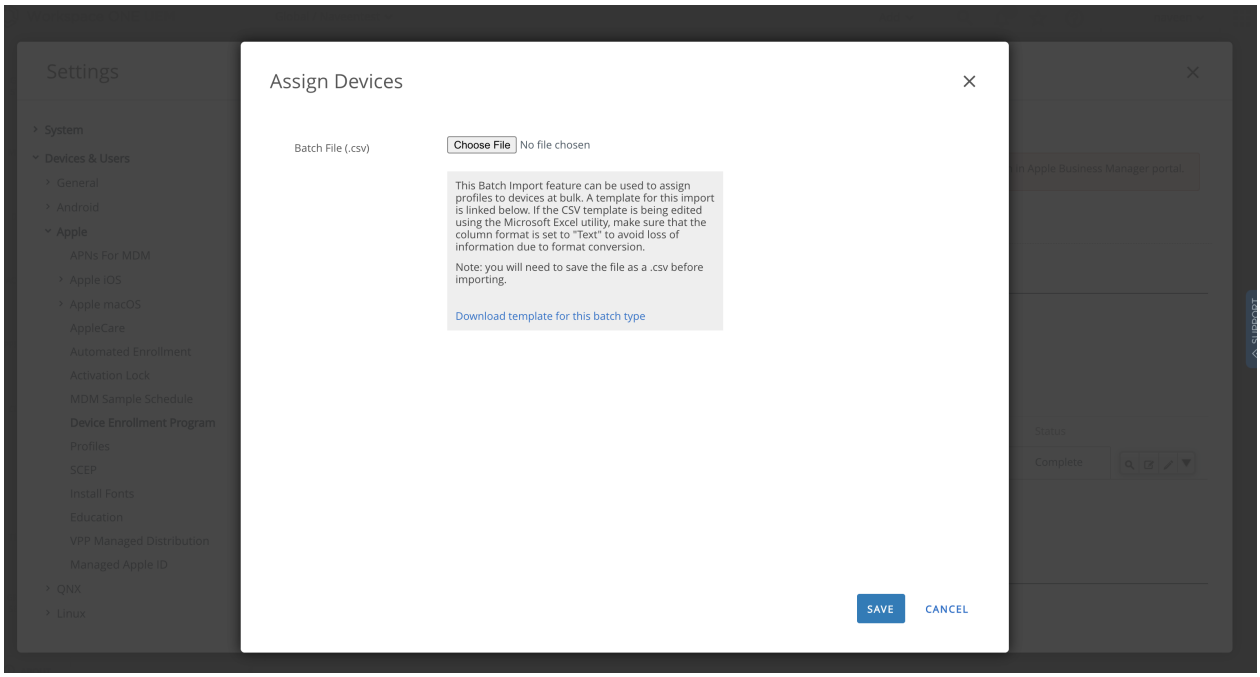
Configure Automated Device Enrollment

To configure automated device enrollment in the Workspace ONE UEM console:

1. Navigate to **Groups and Settings > All Settings > Devices & Users > Apple > Device Enrollment Program**.
2. Create Automated Device Enrollment profile with **Authentication OFF** and Staging Mode set to **Multi User device**.
3. Select **Save**.

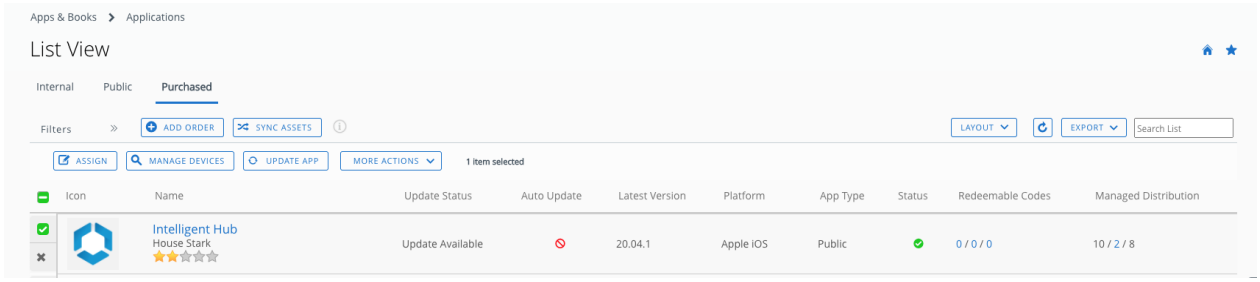


4. Select **Edit Assignment** to assign the Device Enrollment profile to devices.
5. Download the template for this batch type.
6. Add all the serial numbers of devices that are to be provisioned to be used as shared devices.
7. Import .CSV file with list of Serial Numbers.
8. Select **Save**.



Configure Deployment of Intelligent Hub

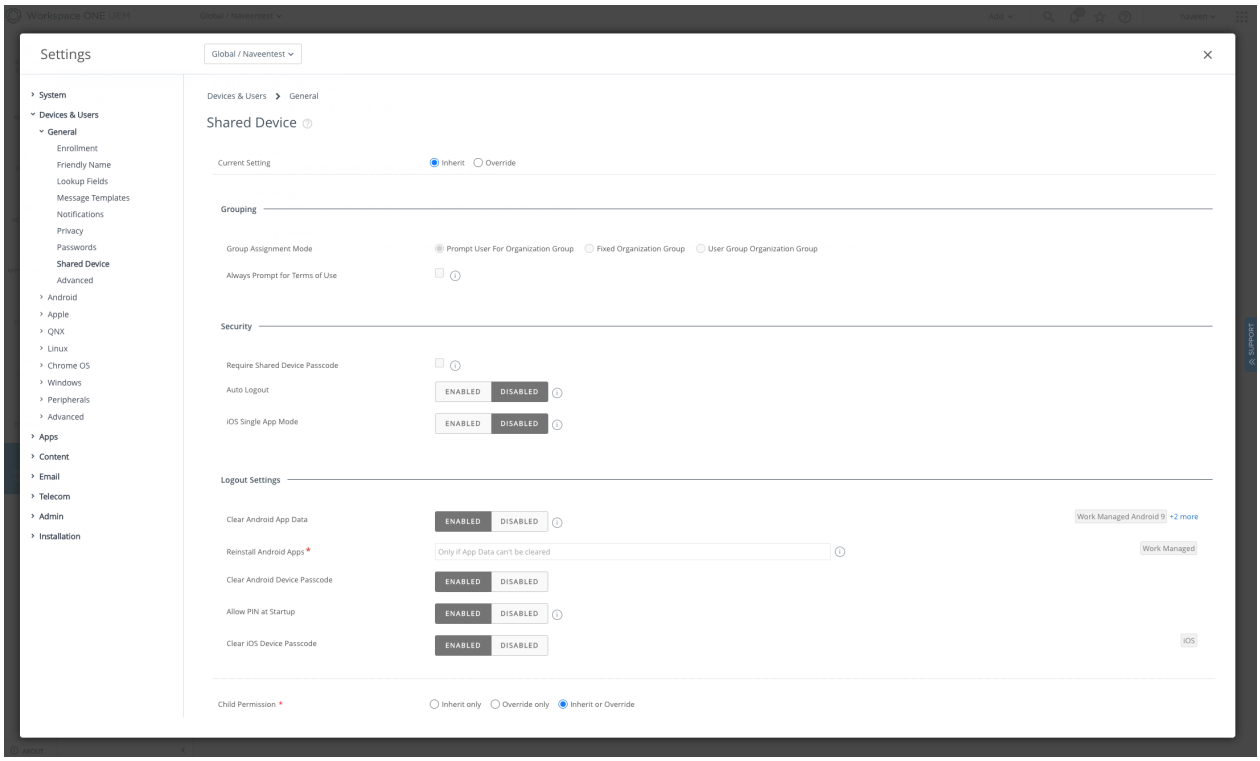
Configure application licensing purchased through Apple Business Manager for **Intelligent Hub** application to be deployed via **Device Based Licensing** to managed devices silently without the need for an Apple ID on the device.



Configure Shared Device Settings

To configure shared device settings in the Workspace ONE UEM console:

1. Navigate to **Groups and settings > All Settings > Devices & Users > General > Shared Device**



2. Set the destination **Organization Group** for the device. This provides the flexibility to associate different Organization Group level policies for Shared Devices.
3. Specify the **Group Assignment mode**. This prompts the user to enter the **GroupID** of the **Organization Group** destination.

   Selecting **User Group Organization Group** is an automated approach that Workspace ONE UEM uses to determine the right **Organization Group** based on defined mapping of User Group to Organization Group. For more information on configuring User Group Mapping, see Mapping your User Groups for Enrollment and Console Access.

Prompting end-user to enter GroupID is typically used in scenarios where the user has access to enroll devices into multiple organization groups. For example, for an organization group structure that is organized by a Hospital or a Retail Store location, the user can enter in the code for the respective Hospital or Store they are in that day to login.

- Optionally choose to enforce **Terms of Use** on each login by user, as per organization requirements.
- Optionally configure an Auto-Logout interval to avoid cases of user's forgetting to check the device back in, leaving the device being logged into a last-logged user.
- Optionally enforce **Single App Mode** to lock the device to Hub automatically when the device is checked-in. This prevents anyone from accessing rest of the device or settings until a user can authenticate and check out.
- Optionally disable the automated **Clear Passcode** behavior leaving a static password on the device (Given a passcode configuration is assigned). The default behavior of clearing passcode on each check-in is to prevent users from resetting the passcode to unlock the device that other users might not be aware of.

Native iOS Shared iPads for Business

Shared iPads are a subset of iOS devices that are configured to allow users to natively log in and log out of the iPad using their Managed Apple IDs. Each user that logs in is given their own secure partition of the device where their data is stored and accessed. This partitioning is managed by the OS automatically and is critical in providing a targeted experience to each user logging into the device.

This capability was originally released in iOS 9.3 through integration with Apple School Manager and Managed Apple IDs created on behalf of students. In iOS 13.4, this capability was released to Apple Business Manager as well for use with corporate, federated Managed Apple IDs.

Prerequisites

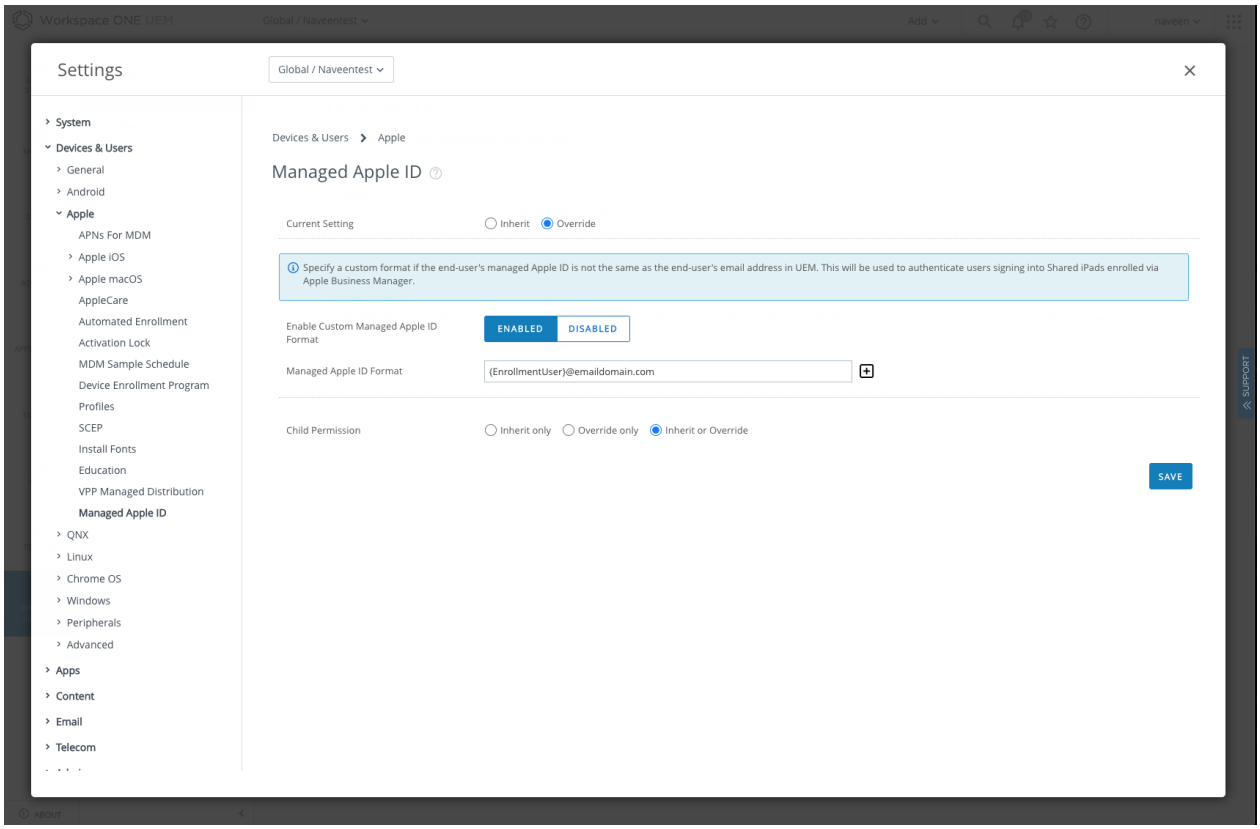
- Workspace ONE UEM 20.07 and later.
- Administrator access to an Apple Business Manager or Apple School Manager tenant.
- 32+ GB iPad on iPadOS 13.4 and later. Each user is given a dedicated partition so the larger the storage, the more space available to each user or maximum number of users that can be configured simultaneously. iPhones and iPods are not supported.
- Domain in Apple Business Manager federated. This is used for the creation of Managed Apple IDs and authentication when users are setting up accounts on new Shared iPads.
- User accounts in Workspace ONE UEM. These accounts can be associated with a Managed Apple ID attribute.

Configure Managed Apple ID

Authentication on Shared iPads for business is entirely driven through Managed Apple IDs created or federated through Azure AD as part of Apple Business Manager.

To associate user objects in Workspace ONE UEM with the corresponding Managed Apple ID in Apple Business Manager:

1. Navigate to **Groups and Settings > All Settings > Devices & Users > Apple > Managed Apple ID**.
2. Toggle the **Enable Custom Managed Apple ID Format** to *Enabled*.
3. Enter the format that corresponds to the Managed Apple IDs being created in Apple Business Manager. This can be a combination of lookup values and static values.
4. Select **Save**.

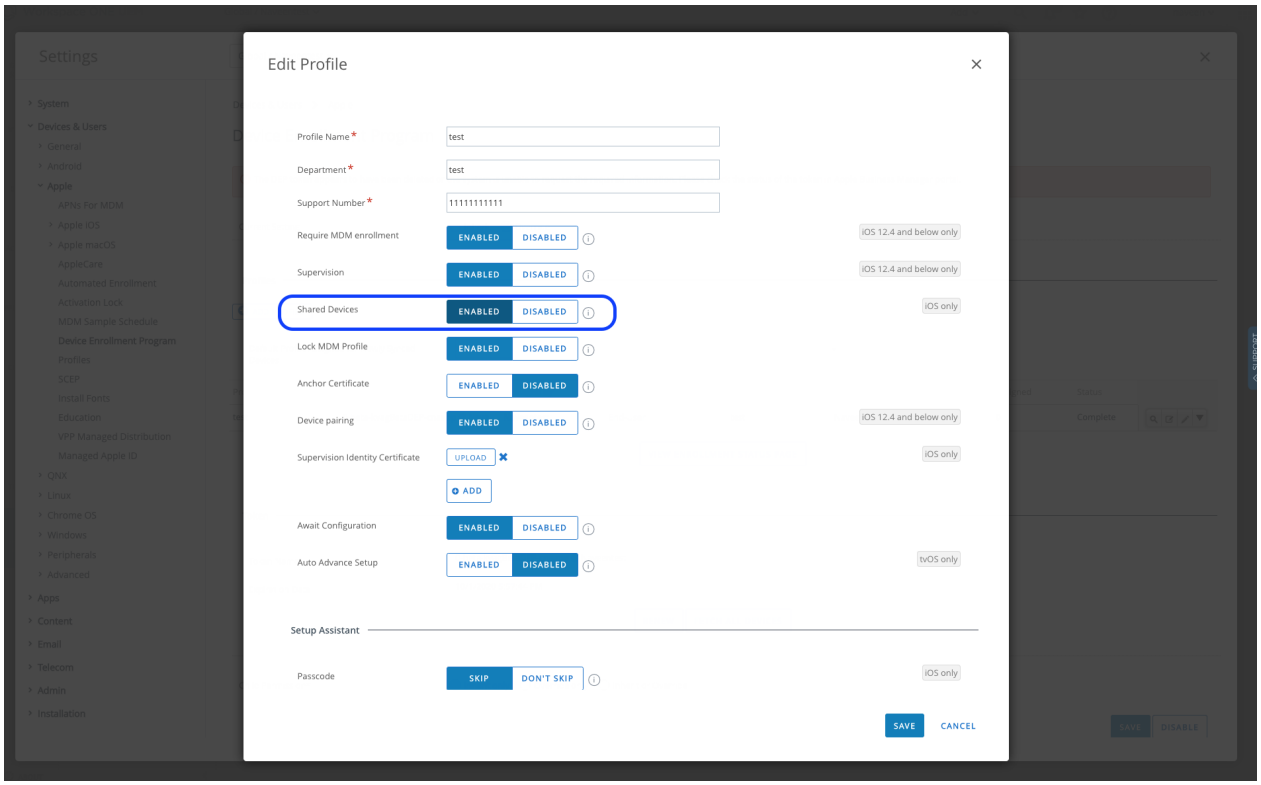


Configure Automated Device Enrollment

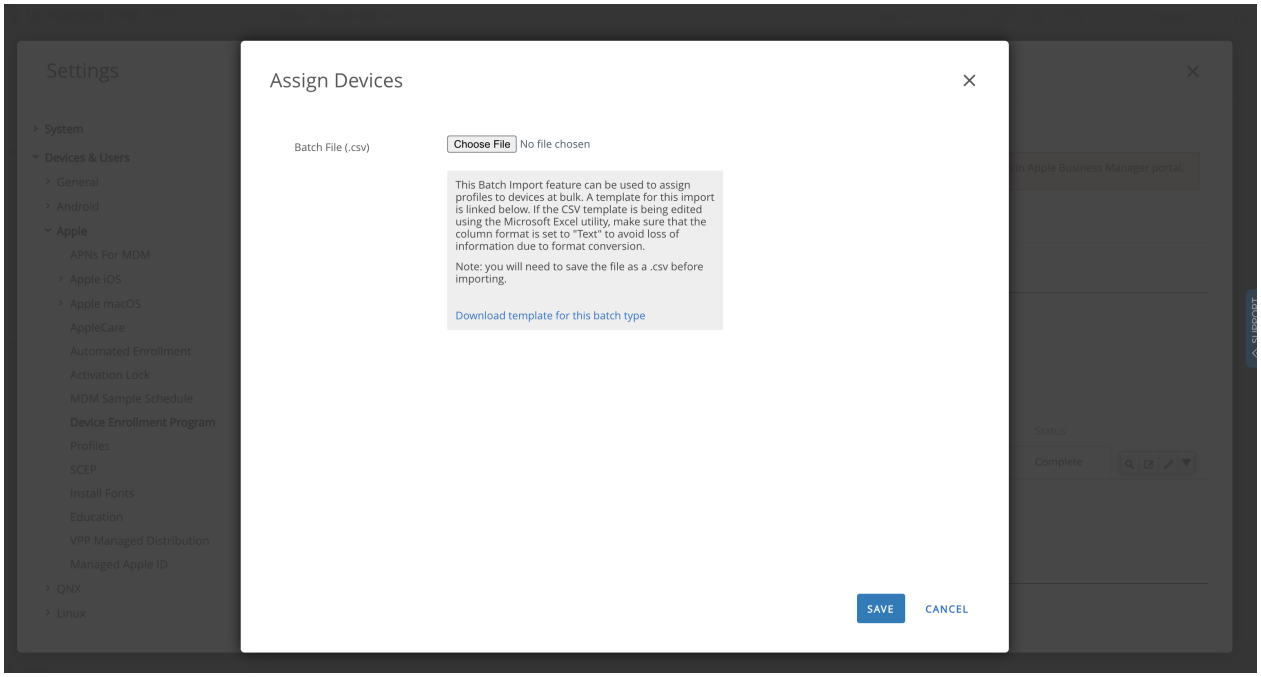
To enable Shared iPad in Enrollment profile in the Workspace ONE UEM console:

Enabling Shared iPad in Enrollment Profile:

1. Log into Workspace ONE UEM and navigate to **Groups and Settings > All Settings > Devices & Users > Apple > Device Enrollment Program**.
2. Select to edit an enrollment profile.
3. Toggle the **Shared iPad** setting to *Enabled*.
4. Save the enrollment profile.



5. Select **Edit Assignment** to assign the Device Enrollment profile to devices.
6. Download the template for this batch type.
7. Add all the serial numbers of devices that are to be provisioned and to be used as shared devices.
8. Import `.csv` file with list of Serial Numbers.
9. Select **Save**.



Note: Devices must be onboarded through Apple Business Manager to be enabled as Shared iPad. This might require a device to be factory wiped and re-enrolled.

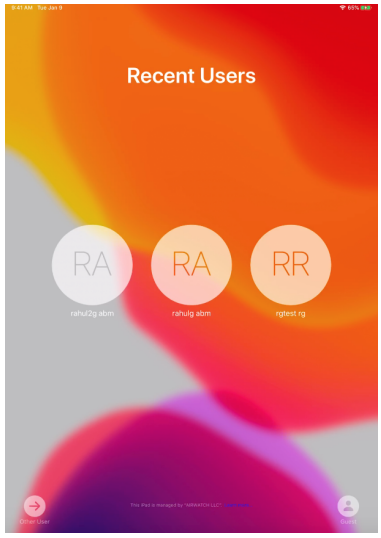
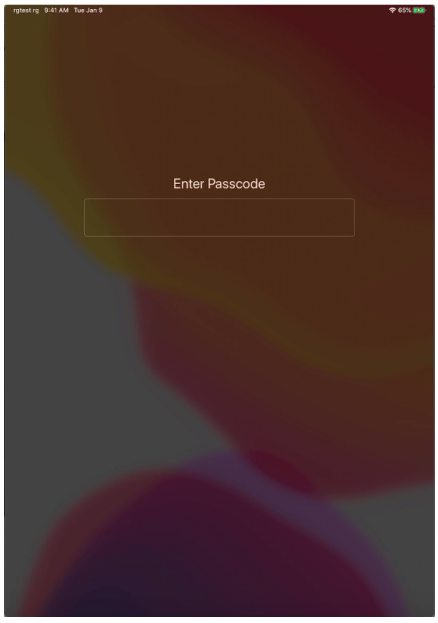
Profiles and configuration Management

Similar to Apps, configuration profiles like restrictions can be assigned and deployed to users. Every user who checks out the device will receive the assigned policies to be applied for their session. For more information about device based and user based policies for Shared iPads, see **Shared iPads for Business** in *Apple Business Manager guide*.

End-User Experience

Shared iPads allow Managed Apple IDs to log in and out of iPads. This allows Workspace ONE UEM to provide unique experiences for each user and preventing sharing data across users. However, this alters the experience away from the typical MDM enrolled iPad. These behaviors are determined by Apple and are active as of iOS 13.4.

- Users first sign in with their Managed Apple ID (federated from Azure AD).
- Users must perform initial setup steps before their first sign-in. These steps include selecting the user's preferred Language, Region, and setting a passcode. This passcode is used for unlocking the device when the user signs in.
- Several device settings are removed, hidden, or read-only for users on Shared iPads. See Apple's documentation for more details on settings available to users of Shared iPads.
- Shared iPads allow a temporary, authentication-less session, Guest login. It has no Managed Apple ID associated with it and any data on the device after the session is ended, is removed and is irretrievable.

Login Screen	Recent Users	Authentication
		

Steps for a new user that does not have an account on the iPad:

1. Onboard the iPad through Apple Business Manager with Shared mode enabled in the enrollment profile. Existing devices must be factory wiped to onboard.
2. Select *Other User*.

3. Enter the Managed Apple ID.
4. Complete authentication steps for Managed Apple ID.
5. Select Language, Region, and create a device Passcode.
6. After the device usage, lock the device and select **Sign Out**.

Steps for an existing user that does have an account on the iPad:

1. Select the icon for the account of the Managed Apple ID that must log in.
2. Enter in passcode. This is the same device passcode created when the account was set up for the first time.
3. After the device usage, lock the device and select **Sign Out**.

Shared iPads for Business

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 account related tasks must be completed before you configure Workspace ONE UEM Shared iPad functionality.

- **Apple Business Manager** - Register your user id with Apple Business Manager and create an administrator account. For information on integrating DEP with Workspace ONE UEM, see Apple Business Manager Guide.
- **Managed Apple IDs** - Credentials required to sign into Shared iPads to access Apple services. For more information, see the section on this page below, entitled 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 below.
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**.