Building a BYOD Program with User Enrollment and Jamf Pro

Technical Paper
Jamf Pro 10.17.0 or Later
18 October 2021

jamf

Jamf has made all efforts to ensure that this guide is accurate.

Jamf
100 Washington Ave S Suite 1100
Minneapolis, MN 55401-2155
(612) 605-6625

Contents

Introduction

Target Audience

This guide is designed for IT administrators who want to allow users to enroll their personally owned iOS or iPadOS devices with Jamf Pro so that the devices can be managed by Jamf Pro.

What's in This Guide

This guide provides step-by-step instructions on how to use Jamf Pro to help create a Bring Your Own Device (BYOD) program in your organization. It also provides information on the management capabilities available with Jamf Pro for personally owned mobile devices enrolled using User Enrollment.

Important Concepts

Before you can use Jamf Pro to build a BYOD program, you should be familiar with the following concepts:

- Push certificates
- User-initiated enrollment for mobile devices
- Managed apps
- Advanced mobile device searches
- Remote commands for mobile devices

Additional Resources

For more information on these concepts, see the Jamf Pro Administrator's Guide.

Overview

Apple's preferred method for enrolling personally owned iOS and iPadOS devices in Jamf Pro is by using Account-Driven User Enrollment or User Enrollment. Personal Device Profiles have been deprecated and are no longer recommended as a method of enrolling personally owned devices. You can migrate devices enrolled using Personal Device Profiles to Account-Driven User Enrollment or User Enrollment as well.

Enrolling devices using Account-Driven User Enrollment or User Enrollment in a BYOD program allows administrators to secure and manage personal devices in their environments without having access to the user's personal data. Account-Driven User Enrollment and User Enrollment keep personal and institutional data separate by associating a personal Apple ID with personal data and a Managed Apple ID with corporate data. This allows for a limited management of devices using a set of configurations that associate management with the user, not the entire device. The user can access their corporate data without the administrator erasing, modifying, or viewing personal data. This separation allows users to keep their personal data protected and intact once the device is removed from Jamf Pro, while the corporate data is deleted.

A BYOD program implemented using Jamf Pro has the following advantages:

- Users can review the IT management capabilities for a personally owned iOS and iPadOS devices before enrolling their device.
- Users can securely and easily access institutional resources such as email, contacts, calendars, Wi-Fi, and VPN.
- IT can only remove institutional data from the device, ensuring protection of the user’s personal data, such as photos and documents.

There are several steps involved in enrolling and managing personally owned iOS and iPadOS devices using Jamf Pro:

1. **Customize the user experience and enable Account-Driven User Enrollment or User Enrollment.** You can customize the user-initiated enrollment messaging for personally owned mobile devices. You can also enable Account-Driven User Enrollment or User Enrollment.

2. **(Optional) Remove the MDM profile from devices enrolled using Personal Device Profiles.** To migrate devices from Personal Device Profiles to Account-Driven User Enrollment or User Enrollment, you must un-enroll the device.

3. **Allow users to enroll personally owned devices.** Users can enroll devices by authenticating to the device using a Managed Apple ID (Account-Driven User Enrollment) or you can provide the enrollment URL to users so they can enroll their device with Jamf Pro (User Enrollment).

4. **Define settings and apps for personal devices.** You can create configuration profiles and select managed apps to distribute to personal devices enrolled using Account-Driven User Enrollment or User Enrollment.

5. **Manage personal devices.** You can perform a subset of mobile device management capabilities, such as remote commands and viewing inventory information, on personally owned mobile devices.

Requirements

To allow personally owned mobile devices to be enrolled using Account-Driven User Enrollment or User Enrollment via user-initiated enrollment, you need the following:

- A push certificate in Jamf Pro (For more information, see Push Certificates in the *Jamf Pro Administrator's Guide*.)
- User-initiated enrollment enabled (For more information, see User-Initiated Enrollment Settings in the *Jamf Pro Administrator's Guide*.)
- (LDAP login only) An LDAP server set up in Jamf Pro (For more information, see Integrating with LDAP Directory Services in the *Jamf Pro Administrator's Guide*.)
- (Account-Driven User Enrollment) Jamf Pro 10.33.0 or later; personally owned mobile devices with iOS 15 or later, or iPadOS 15 or later
- (User Enrollment) Jamf Pro 10.17 or later; personally owned mobile devices with iOS 13.1 or later, or iPadOS 13.1 or later

> **Note:** Personally owned mobile devices must also have free storage space to use for corporate data.

To create Managed Apple IDs for Account-Driven User Enrollment or User Enrollment, you must either use federated authentication to link Apple School Manager or Apple Business Manager to your instance of Microsoft Azure Active Directory (AD) or create them manually in Apple School Manager or Apple Business Manager. For more information, see the following Apple documentation:

- Intro to federated authentication with Apple School Manager in the *Apple School Manager User Guide*
- Intro to federated authentication with Apple Business Manager in the *Apple Business Manager User Guide*
- Create Managed Apple IDs in Apple School Manager in the *Apple School Manager User Guide*
- Create Managed Apple IDs in Apple Business Manager in the *Apple Business Manager User Guide*

> **Note**: For Account Driven User Enrollment, Managed Apple IDs must belong to a verified domain. For more information , see the following:
>
> - For more information about existing domains in Apple School Manager, see the Apple School Manager User Guide.
> - For more information about how to verify domains in Apple Business Manager and Apple School Manager, see Verify domains in Apple Business Manager and Apple School Manager from Apple's support website.

Before you can allow users to enroll personally owned mobile devices using Account-Driven User Enrollment, you must define the Jamf Pro enrollment information in a .JSON file and host it on a web server that is accessible to any device you want enrolled with Jamf Pro. To set this up, you need the following:

- The web server must have the same fully qualified domain name (FQDN) as the verified domain that the Managed Apple IDs belong to, and web services must be enabled.
- The .JSON file must be hosted on a server which supports HTTPS GET requests.
- The SSL certificate for the web server must be issued by a trusted certificate authority. For a list of trusted root certificates on iOS devices, see Lists of available trusted root certificates in iOS from Apple's support website.

For more information about defining the Jamf Pro enrollment information in a .JSON file and hosting it on a web server, see Account-Driven User Enrollment for Personally Owned Mobile Devices in the *Jamf Pro Administrator's Guide*.

Customizing the User Experience and Enabling User Enrollment

Enrollment is the process of adding mobile devices to Jamf Pro to establish a connection between the devices and the Jamf Pro server. User-initiated enrollment allows users to initiate this process by logging in to an enrollment portal and following the onscreen instructions to enroll a device. Personally owned devices can only be enrolled via user-initiated enrollment.

When configuring Account-Driven User Enrollment or User Enrollment using the User-Initiated Enrollment settings in Jamf Pro, you can do the following:

- Customize messaging displayed for each step in the enrollment process, including adding different languages.

  Note: You can use Markdown, a text-to-HTML conversion tool, to specify formatting for the text displayed to users during enrollment. For more information, see the Using Markdown to Format Text article.

- Enable Account-Driven User Enrollment or User Enrollment for personally owned mobile devices.

For more information on what User-Initiated Enrollment settings you can configure for devices enrolled using Account-Driven User Enrollment or User Enrollment, see User-Initiated Enrollment Settings in the *Jamf Pro Administrator's Guide*.

Configuring the User-Initiated Enrollment Settings

1. Log in to Jamf Pro.
2. In the top-right corner of the page, click **Settings**  .
3. Click **Global Management**.
4. Click **User-Initiated Enrollment**  .
5. Click **Edit**.
6. Use the General pane to restrict re-enrollment, skip certificate installation, or upload a third-party signing certificate to be used during enrollment.
7. On the Messaging pane, do the following to customize the text displayed on devices during the enrollment experience and add languages:
   a. Do one of the following:
      - To add a language, click **Add** and then choose the language from the Language pop-up menu.

        Note: English is the default language if the mobile device does not have a preferred language set on it.

- To customize the text for a language already listed, click **Edit** next to the language.

b. In the **Page Title for Enrollment** field, enter a page title to display at the top of all enrollment pages.

c. On the **Login** tab, use the fields provided to customize how you want the Login page to be displayed to users.

> Note: This is the only tab that you can customize for Account-Driven User Enrollment.

d. Click the **Device Ownership** tab and use the fields provided to customize the text that is displayed to users based on their device ownership type. The text displayed and the enrollment page that the text displays on depends on the enrollment options that you enable:

- **If you enable user-initiated enrollment for both institutionally owned and personally owned mobile devices**—Customize the text that prompts users to choose the appropriate device ownership type, and customize the device management description that explains the IT management capabilities for each device ownership type. When users select the personal or institutional device ownership type, the respective device management description is displayed.
- **If you enable user-initiated enrollment for personally owned devices only**—Customize the device management description that explains the IT management capabilities for personal device ownership. This description is accessible to users by tapping the **Information** icon displayed on the Personal MDM Profile page during enrollment.

e. Click the **End User License Agreement** tab and use the fields provided to specify an End User License Agreement (EULA) for personally owned devices. If the EULA fields are left blank, a EULA page is not displayed to users during enrollment.

f. Click the **Certificate** tab and use the fields provided to customize the message that prompts users to install the CA certificate for mobile devices to trust at enrollment.

g. Click the **User Enrollment MDM Profile** tab and use the fields provided to customize the message that prompts users to install the MDM profile, including guidance for users on what to enter for their Managed Apple ID.

h. Click the **Complete** tab and use the fields provided to customize the messages that are displayed to users if enrollment is successful or if it fails.

i. Click **Save**.

8. On the Platforms pane, click the iOS tab and do one of the following:
   - (Account-Driven User Enrollment) In the Account-Driven User Enrollment settings, select Enable for personally owned devices.
   - (User Enrollment) In the User-Initiated Enrollment via URL settings, select Enable for personally owned devices, and then select User Enrollment.
9. Click **Save**.

Enabling Users to Enroll Personally Owned Devices

(Account-Driven User Enrollment only) To ensure users initiate the enrollment process, they must sign in with their Managed Apple ID. This action redirects the user to the enrollment portal where they are prompted to install the MDM profile on their device.

(User Enrollment only) To direct users to the enrollment portal, you need to provide them with the enrollment URL. The enrollment URL is the full URL for the Jamf Pro server followed by "/enroll". For example:

- https://instancename.jamfcloud.com /enroll (hosted in Jamf Cloud)
- https://jamf.instancename.com:8443/enroll (hosted on-premise)

You can provide the enrollment URL to users in the way that best fits your environment.

Note: Users must use Safari to access the enrollment URL.

Users can then log in to the enrollment portal using an LDAP directory account or a Jamf Pro user account. When a user logs in with an LDAP directory account, user and location information is submitted to Jamf Pro during enrollment. When a user logs in with a Jamf Pro user account, it allows an LDAP user to be assigned to the mobile device.

Migrating Devices from Personal Device Profiles to User Enrollment

Disclaimer: Personal device profiles have been deprecated and are no longer recommended as a method of enrolling personally owned devices. User Enrollment is the Apple-preferred method for enrolling personally owned devices in a Bring Your Own Device (BYOD) program. For legacy documentation about Personal Device Profiles, see version 10.27.0 or earlier of the Jamf Pro Administrator's Guide.

If you have personally owned devices currently enrolled in Jamf Pro using a Personal Device Profile, you can migrate those devices to User Enrollment. When migrating to User Enrollment, keep in mind that devices enrolled using User Enrollment count as regular managed devices for your license count. To re-enroll devices in Jamf Pro using User Enrollment, you must first remove the MDM profile from the device.

Warning: When removing the MDM profile from a device enrolled using a Personal Device Profile, any local corporate data will be deleted. It is recommended that you back up corporate data in iCloud before unenrolling the device.

Removing the MDM Profile from a Device Enrolled Using a Personal Device Profile

Before you enroll a personally owned device in Jamf Pro using User Enrollment, users must first remove the MDM profile from the device.

Important: Users may lose access to VPN and Mail while their personal device is in an unenrolled state. It is recommended that you unenroll the device and re-enroll using User Enrollment when the user does not need access to these resources.

1. On the device you want to remove the MDM profile from, navigate to **Settings**.
2. Tap **General**, and then tap **Device Management**.
3. Tap the MDM profile and tap **Remove Management**.
4. If the device has a passcode, enter the passcode.
5. Tap **Remove Management** to confirm.
   The MDM profile is removed from the device.

Enrollment Experience for Personally Owned Mobile Devices

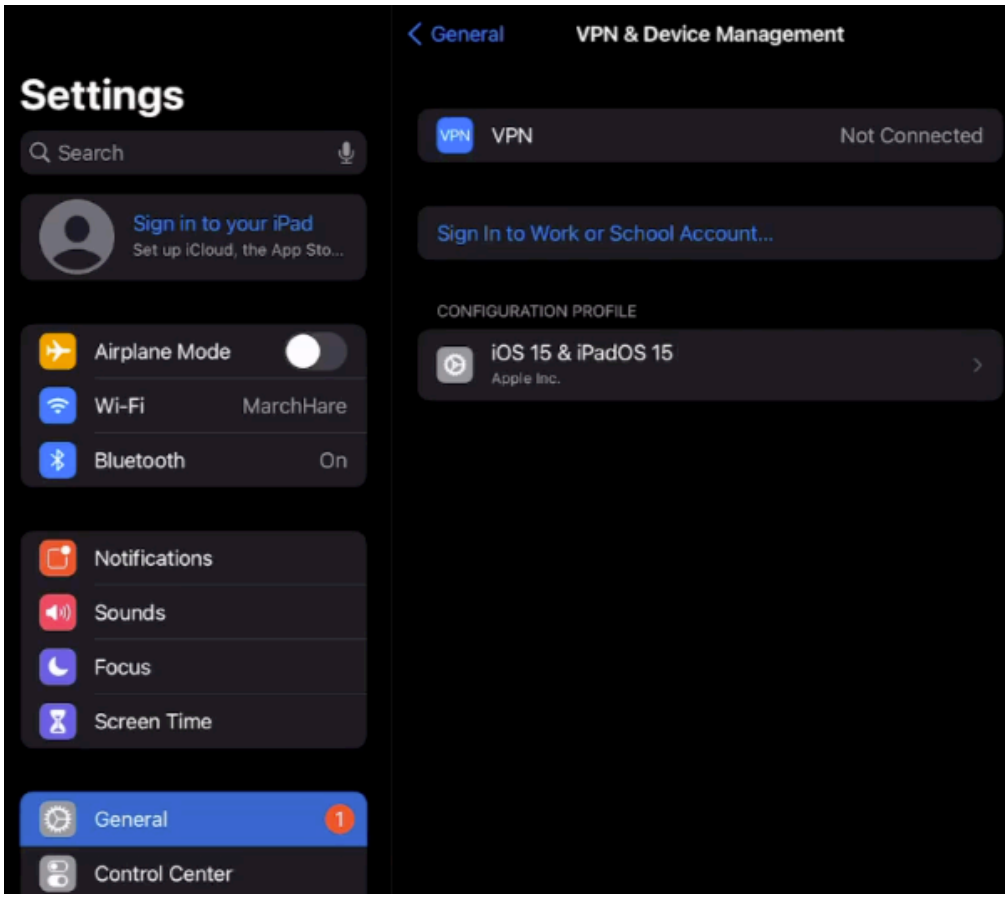
User Experience for Account-Driven User Enrollment

When a user authenticates to their device with a Managed Apple ID, the enrollment process initializes. Users are redirected to the enrollment portal and prompted to install the MDM profile on their device. The text displayed in the enrollment portal may vary depending on if the text or languages are customized in the User-Initiated Enrollment settings. For more information, see User-Initiated Enrollment Settings.

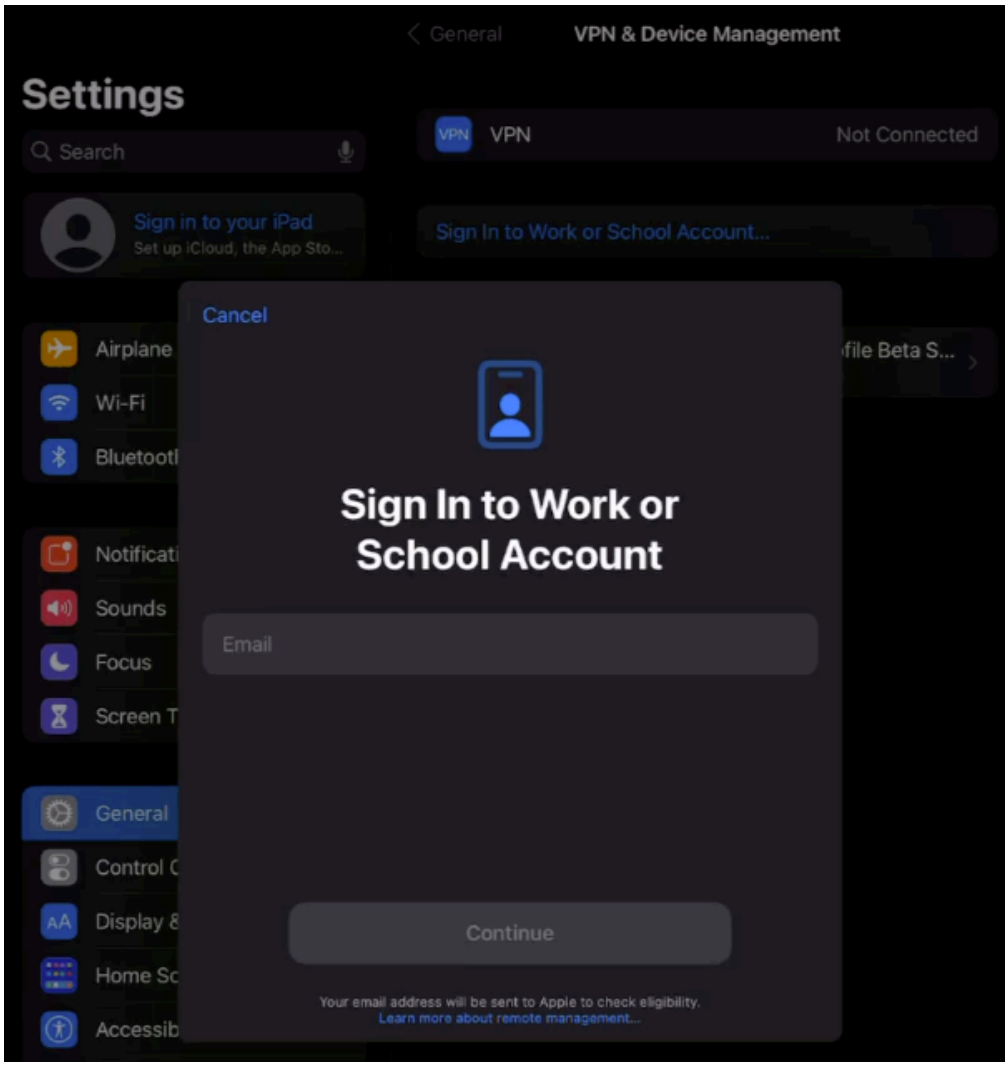
> **Note**: If you are re-enrolling a device that was previously enrolled using the deprecated method of using a Personal Device Profile, it is recommended that you first remove the device's previous record from Jamf Pro. For more information about how to re-enroll a device enrolled using a Personal Device Profile, see "Migrating Devices from Personal Device Profiles to User Enrollment" in the Building a BYOD Program with User Enrollment and Jamf Pro technical paper.

The following workflow describes how Account-Driven User Enrollment can be used to enroll personally owned mobile devices with Jamf Pro:

1. The user authenticates to the device using a Managed Apple ID by navigating to **Settings** > **General** > **VPN & Device Management** > **Sign In to Work or School Account**:



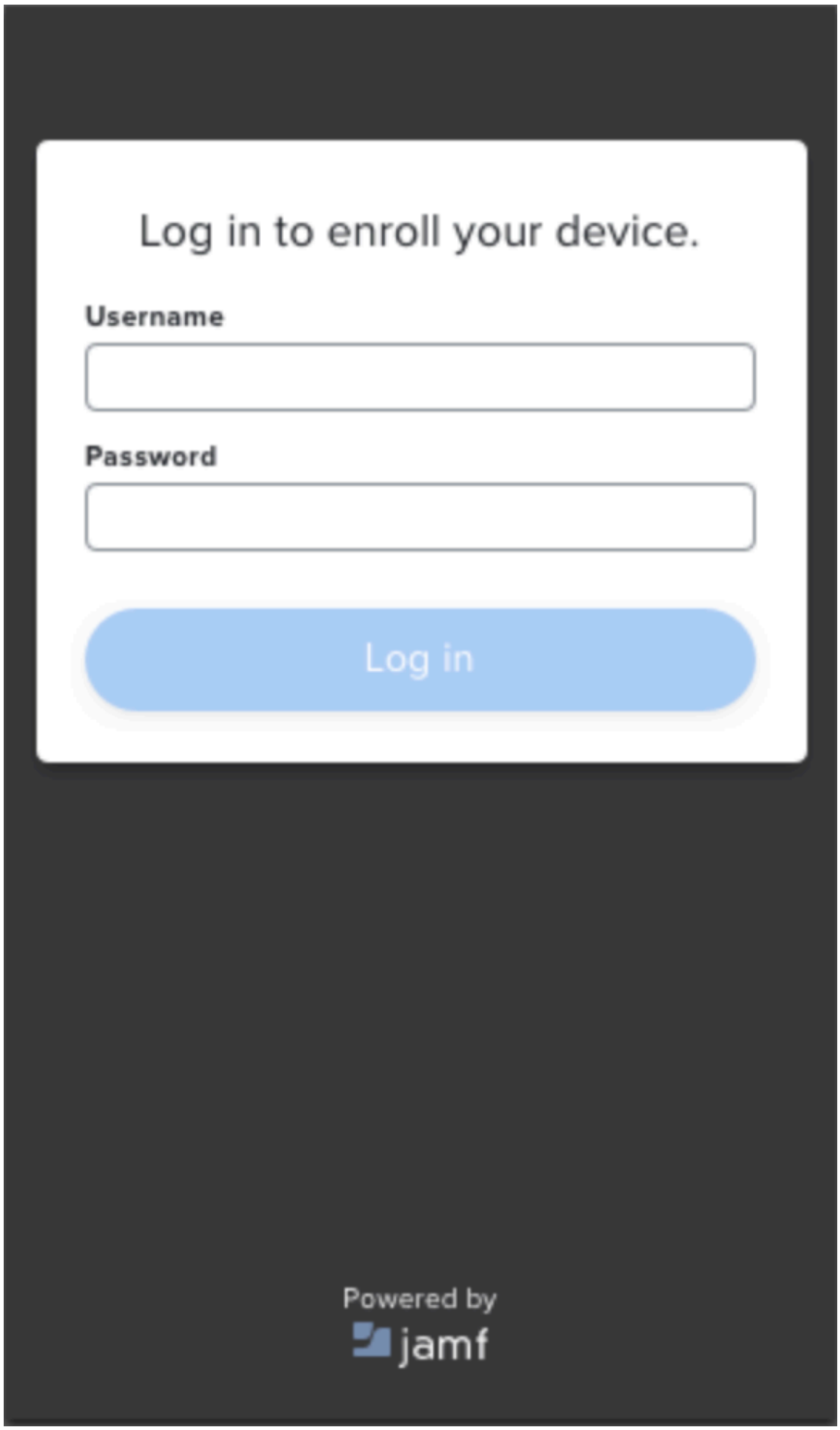
2. The user is prompted to enter a Managed Apple ID:



Important: The user must enter the full Managed Apple ID. For example, "samantha.johnson@mycompany.com"

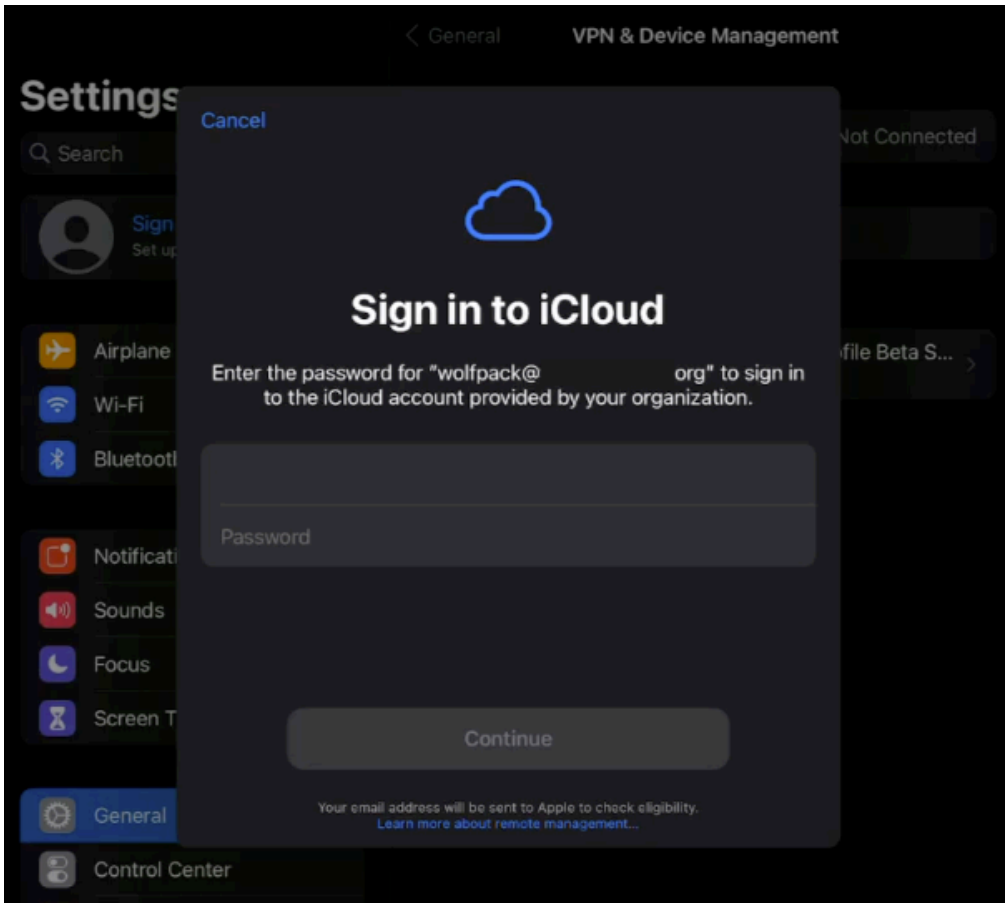
After the user enters the Managed Apple ID, the user must tap **Continue**.

3. The enrollment portal displays and prompts the user to enter their Jamf Pro User Account or directory credentials (for example, LDAP).



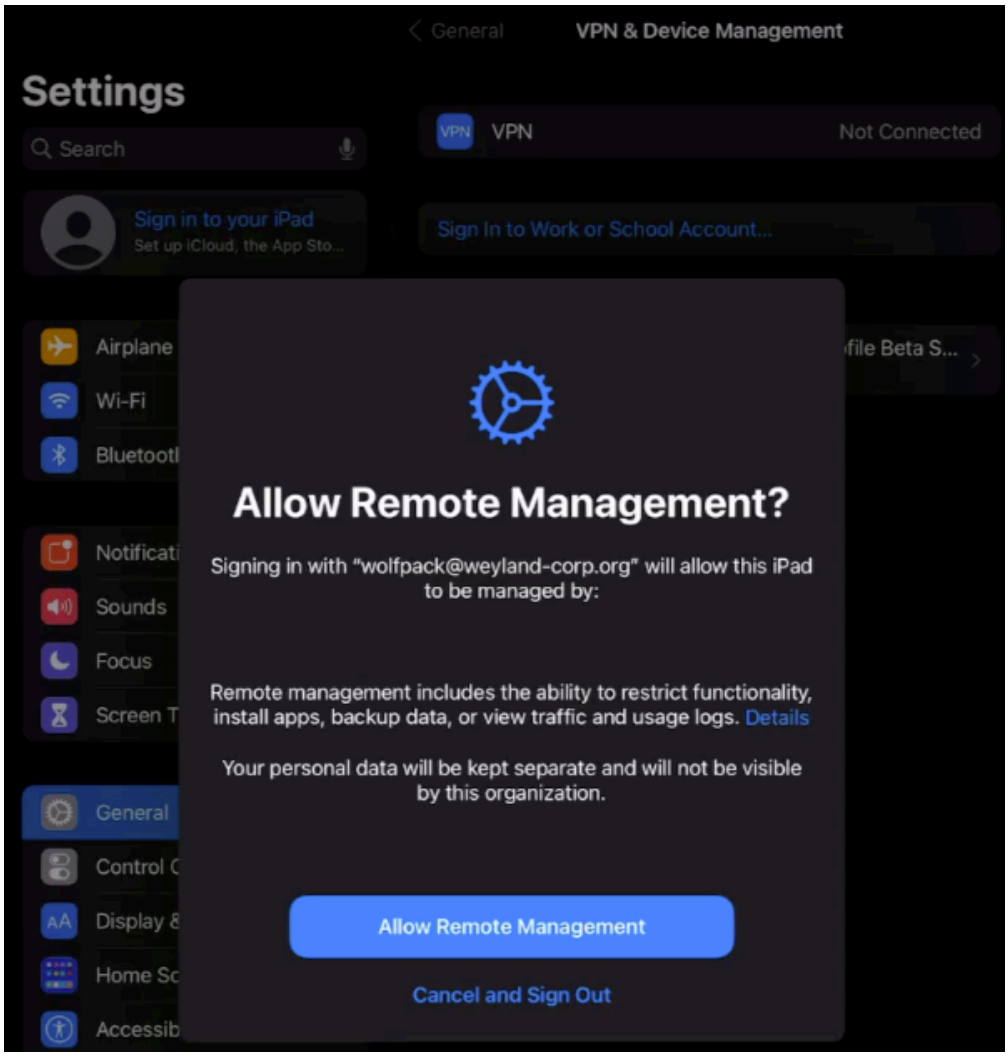
After entering directory credentials, the user must tap **Log In**.

4. The user is directed to the Settings app and must enter their Managed Apple ID email address and password when prompted.

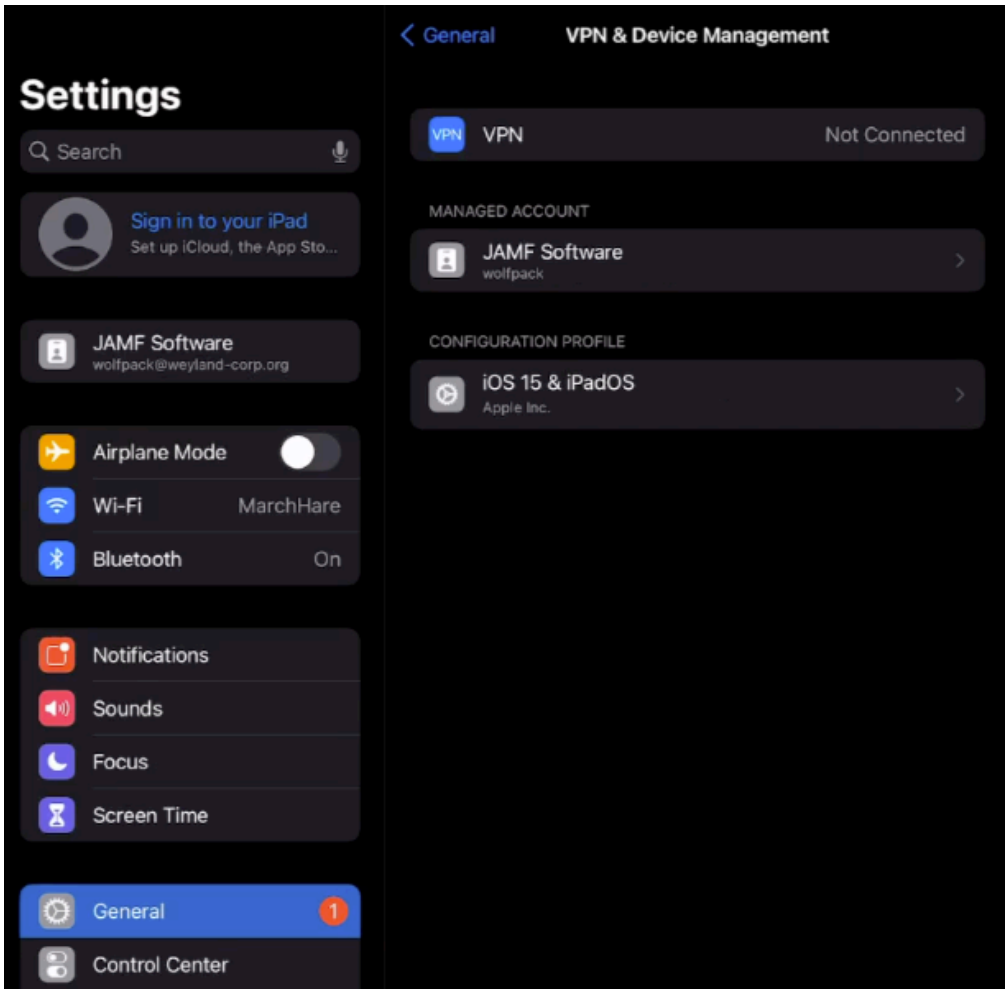


After entering the Managed Apple ID and password, the user must tap **Continue**.

5. The user is prompted to allow remote management.



The MDM Profile downloads on the device when the user taps **Allow Remote Management**.



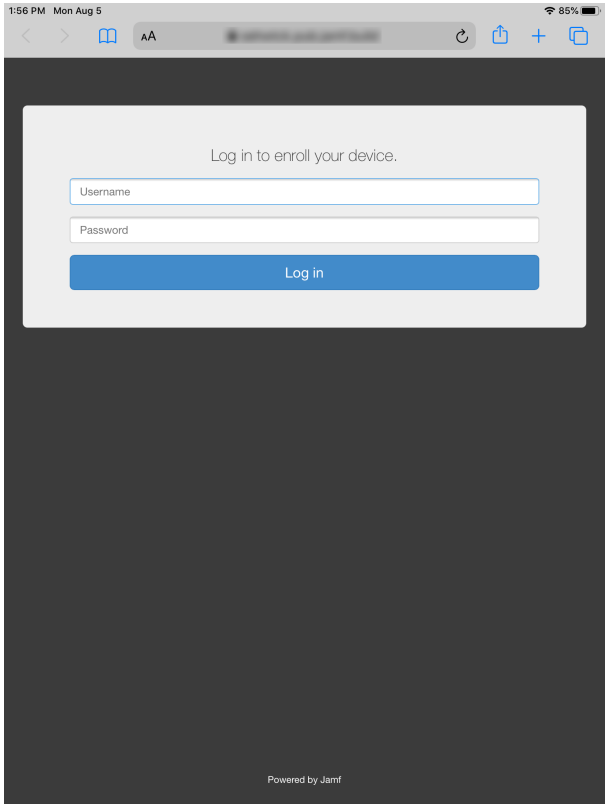
User Experience for User Enrollment

When a user accesses the enrollment URL from a mobile device using Safari, they are guided through a series of steps to enroll the device.

Note: If you are re-enrolling a device that was enrolled using a Personal Device Profile, it is recommended that you remove the device's previous record from Jamf Pro.

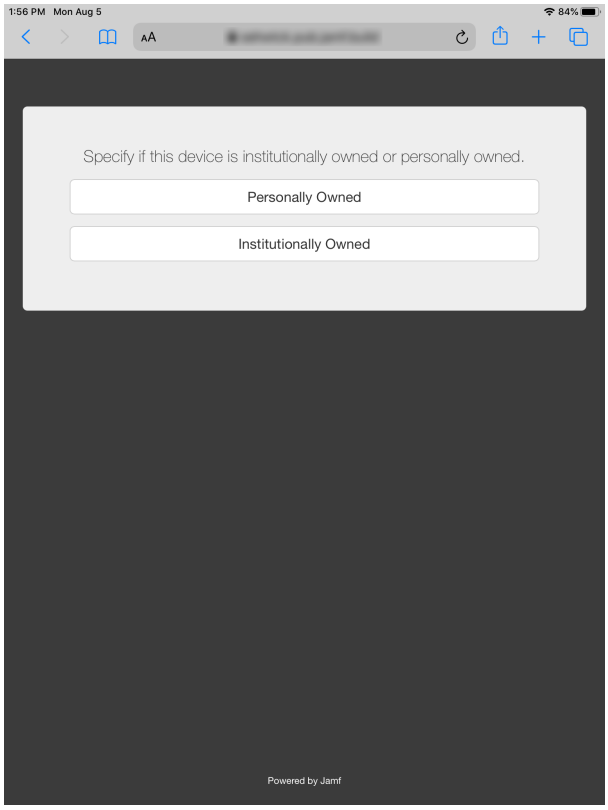
1. The user must enter a Jamf Pro administrator's account credentials on their mobile device. This allows users to enroll the device in Jamf Pro.

Note: You can create a Jamf Pro user account with only enrollment privileges specifically for enrolling devices via user-initiated enrollment.

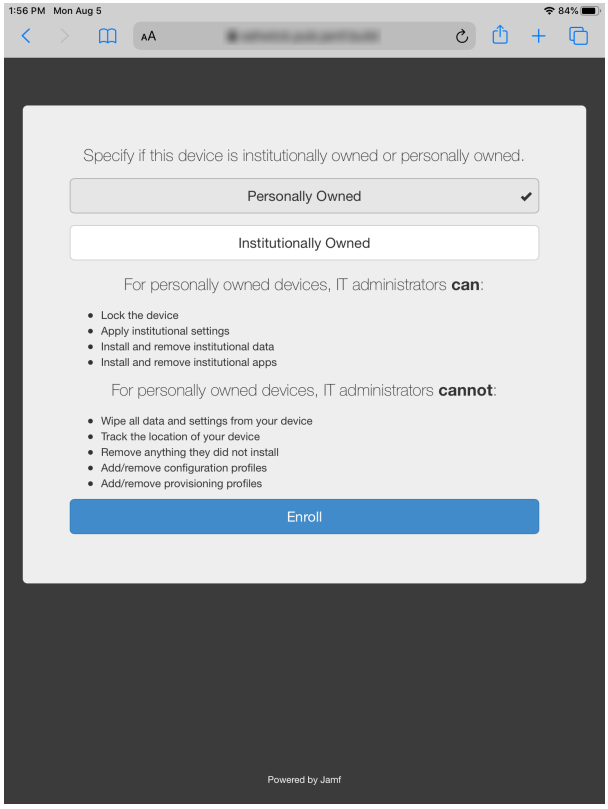


Note: If notified that the device cannot verify the identity of the Jamf Pro server when navigating to the enrollment URL, the user must proceed to the website to log in to the enrollment portal. This notification only appears if the Jamf Pro server uses an untrusted SSL certificate.

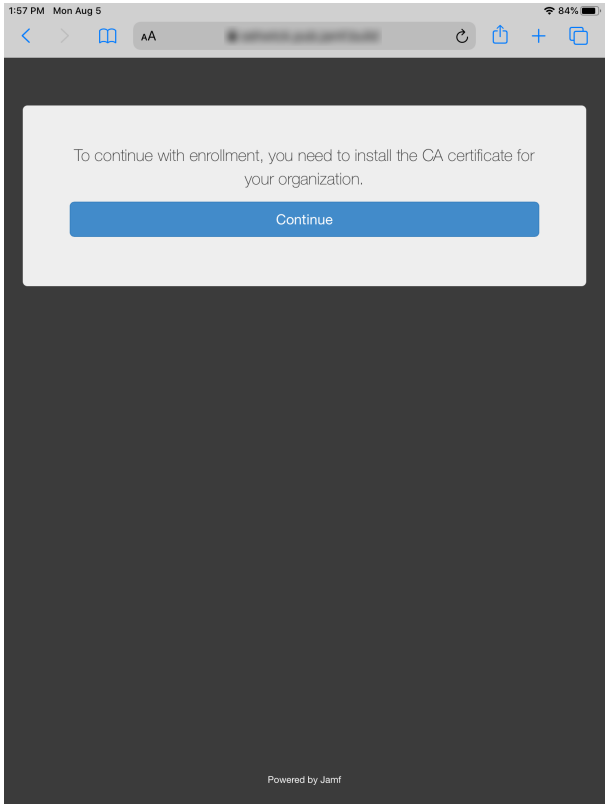
2. The user is prompted to enroll the device as a personally owned device or an institutionally owned device.
   This step is only displayed if both institutionally owned device enrollment and personally owned device enrollment are enabled in Jamf Pro.



You can display a description to users who enroll a personally owned device.

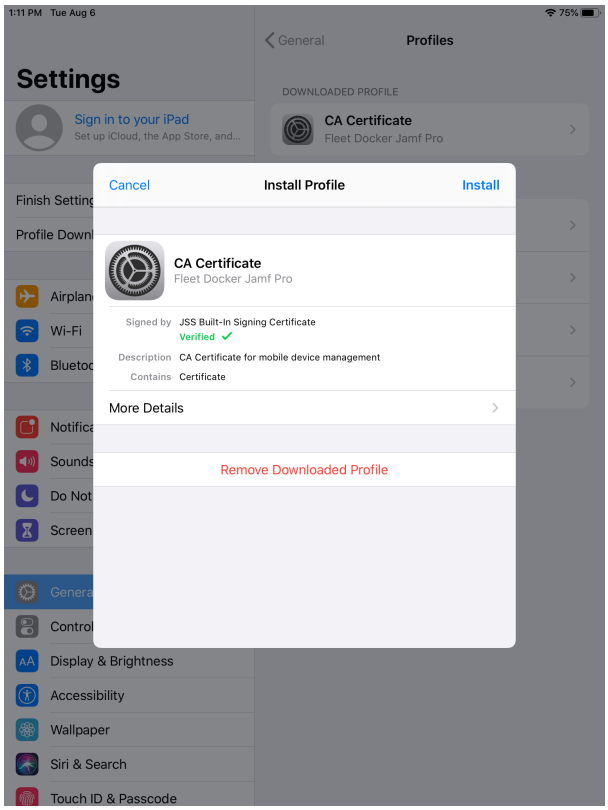


3. The user is prompted to continue to the CA certificate installation.

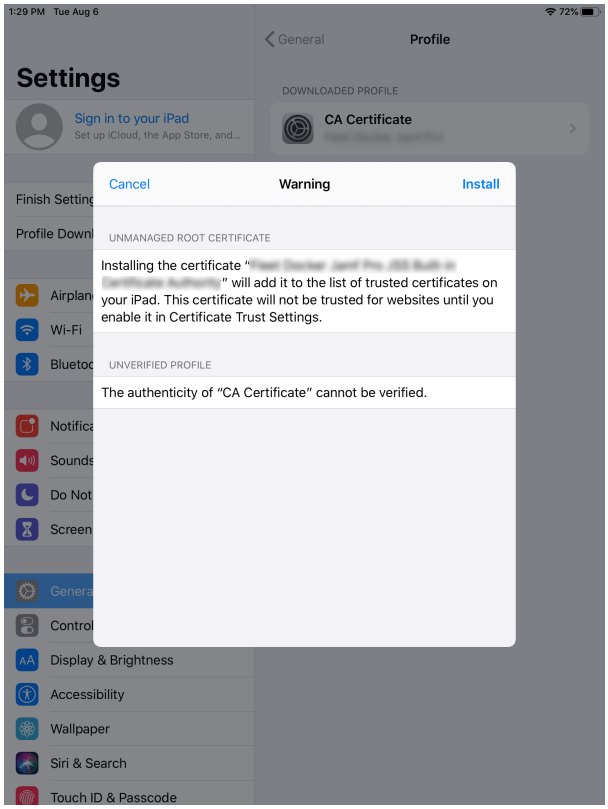


Note: For mobile devices with iOS 11 or later, a pop-up window will appear notifying users, “This website is trying to open Settings to show you a configuration profile. Do you want to allow this?” The user must tap **Allow**. For devices with iOS 12.2 or later, an additional message is displayed notifying users, "Complete installation of this profile in the Settings app." The user must tap **Close**, and then navigate to the Settings app to complete the installation.

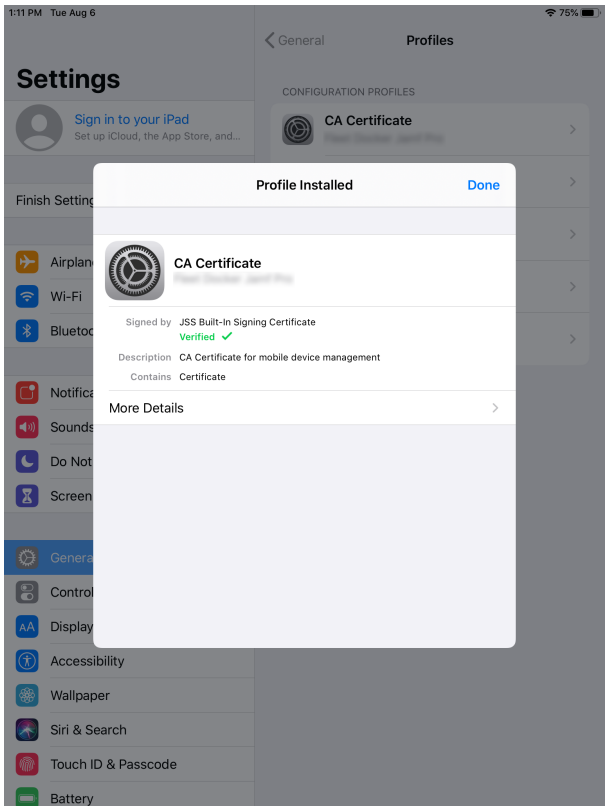
4. The user must tap **Install** to continue.



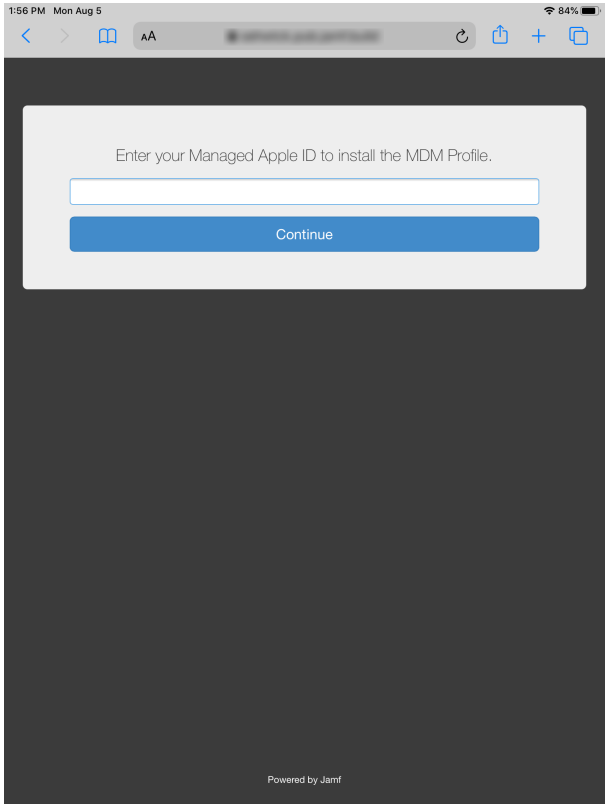
5. When notified that the profile will change settings on the device, the user must tap **Install**. If the device has a passcode, the user must enter the passcode.



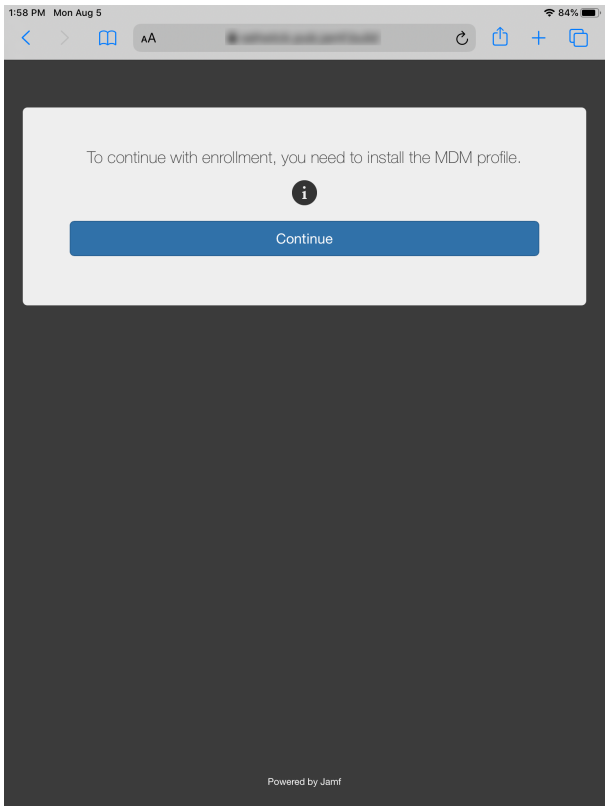
6. To complete the installation, the user must tap **Done**.



7. The user is prompted to enter their Managed Apple ID to install the MDM profile.

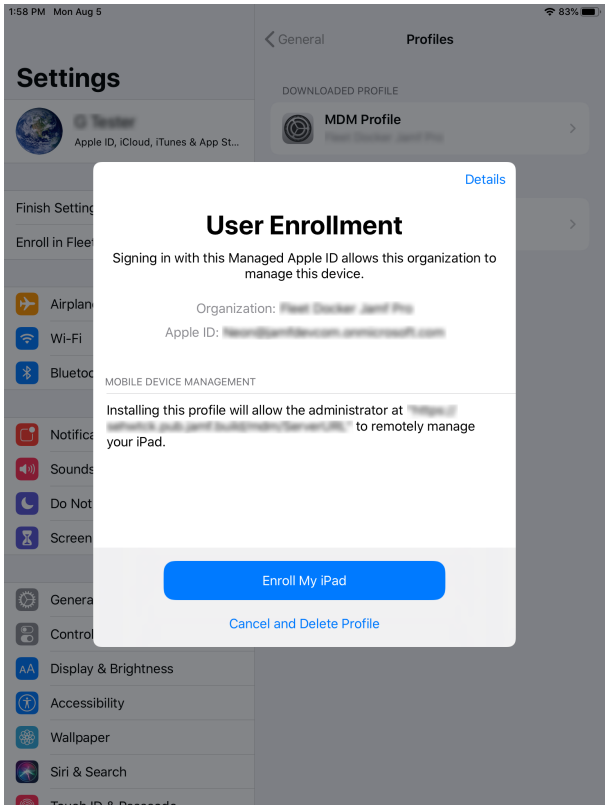


8. The user is prompted to continue to the MDM profile installation.
   Information about enrollment can be accessed by tapping the **Information** icon.

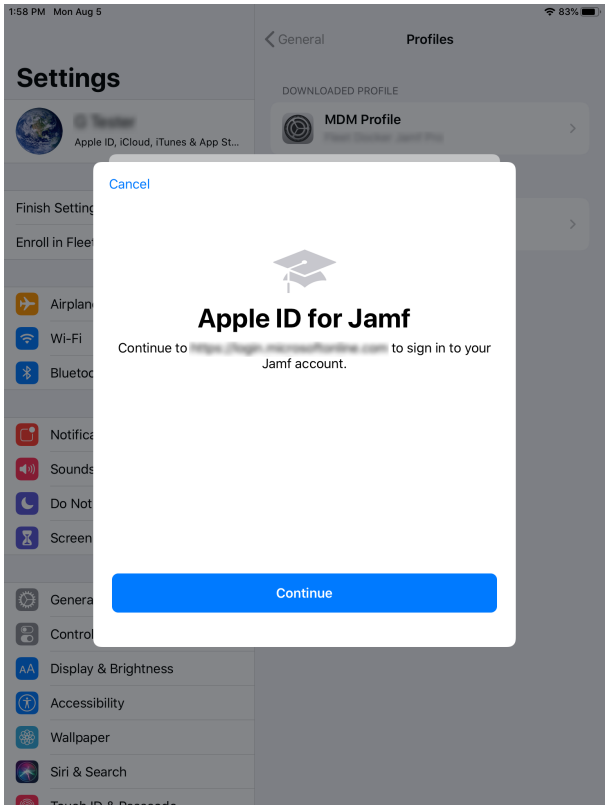


Note: For mobile devices with iOS 11 or later, a pop-up window will appear notifying users, “This website is trying to open Settings to show you a configuration profile. Do you want to allow this?” The user must tap **Allow**. For devices with iOS 12.2 or later, an additional message is displayed notifying users, "Complete installation of this profile in the Settings app." The user must tap **Close**, and then navigate to the Settings app to complete the installation.

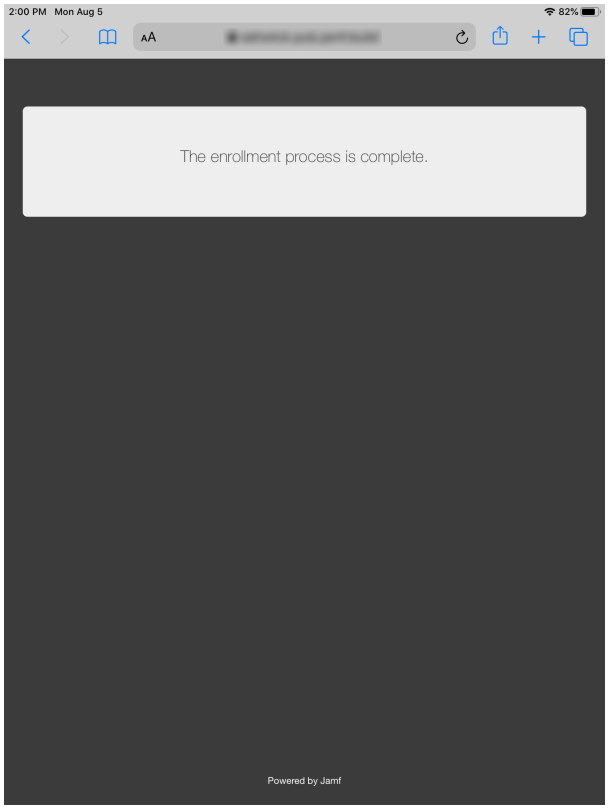
9. The user taps **Enroll My iPad** or **Enroll My iPhone** to continue.
   For more information on the sign-in process for User Enrollment, see User Enrollment into MDM in Apple's *Deployment Reference for iPhone and iPad*.



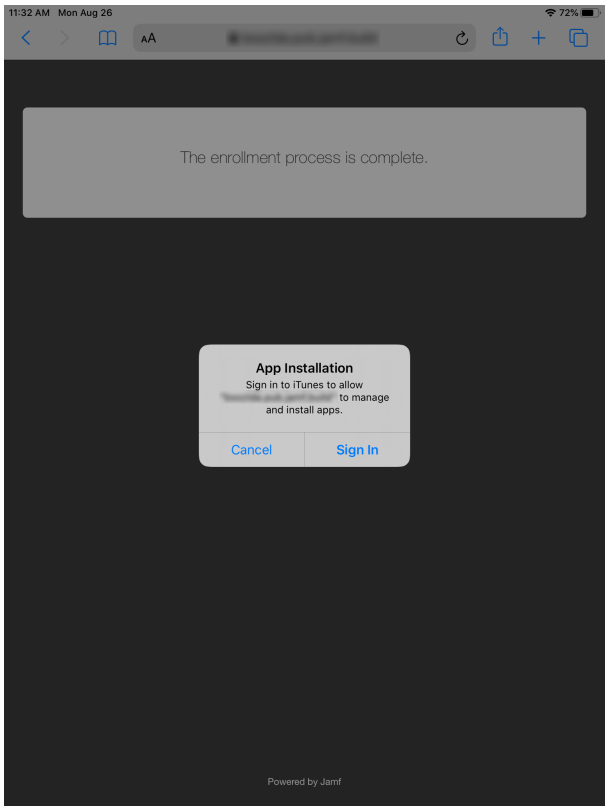
10. The user taps **Continue** to proceed to the Managed Apple ID sign in page. The user is then prompted to enter the password for their Managed Apple ID.



11. When the enrollment is complete, the device is enrolled with Jamf Pro.



If you chose to install Self Service for iOS, users are prompted to install the app from the App Store. For more information, see Jamf Self Service for iOS in the *Jamf Pro Administrator's Guide*.



Managing Personally Owned Devices Enrolled with Jamf Pro

When managing devices enrolled using Account-Driven User Enrollment or User Enrollment, some mobile device management capabilities are not supported because personal data and corporate data are separated on these devices. For more information on the payload settings and restrictions that you can apply to devices enrolled using Account-Driven User Enrollment or User Enrollment, see the following topics in Apple's *Mobile Device Management Settings*:

- User Enrollment MDM payloads for Apple devices
- User Enrollment MDM restrictions for Apple devices

For more information on the management capabilities available for personally owned mobile devices, see Mobile Device Management Capabilities in the *Jamf Pro Administrator's Guide*.

Performing and Advanced Mobile Device Search for Personally Owned Devices

After enrolling devices using User Enrollment with the instructions in this guide, you can use advanced mobile device searches to identify devices enrolled using Account-Driven User Enrollment or User Enrollment in your environment and view a subset of basic inventory information for a device. For information on the inventory information that you can view and edit for a personal device, see Mobile Device Inventory Information in the *Jamf Pro Administrator's Guide*.

When you create and save an advanced mobile device search, the results of the search are updated each time devices contact Jamf Pro. This allows you to view up-to-date information on the devices in your organization at any time.

1. Log in to Jamf Pro.
2. Click **Devices** at the top of the page.
3. Click **Search Inventory**.
4. Click **New**.
5. On the Search pane, select the **Save this Search** checkbox and enter a display name for the search.
6. Click the **Criteria** tab.
7. To search for personally owned devices in inventory, do the following:
   - Click **Add**.
   - Click **Show Advanced Criteria**, and then click **Choose** for “Device Ownership Type”.
   - Click **Browse**, and then click **Choose** for "Personal (Account-Driven User Enrollment)" or “Personal (User Enrollment)”.
8. Click the **Display** tab and select the attribute fields you want to display in your search results.

9. Click **Save**.
   The results of the search are updated each time mobile devices check in with Jamf Pro and meet or fail to meet the specified search criteria.
10. Click **View**.
    The list of search results is displayed.
11. Do one of the following:
    - To view inventory information for a mobile device in the list, click the device. The device's inventory information is displayed.
    - To export the search results to a file, click **Export** and follow the onscreen instructions to export the data. The report is downloaded immediately.

Distributing Content to Personally Owned Devices

Only managed in-house apps, App Store apps, and books can be distributed to personal devices. App Store apps must be assigned to users (user-based assignment) before distributing them to devices enrolled using Account-Driven User Enrollment or User Enrollment.

You can distribute content to devices individually, or use the previously created advanced mobile device search to distribute apps and books to all devices enrolled via Account-Driven User Enrollment or User Enrollment.

Distributing apps and books to devices enrolled via Account-Driven User Enrollment or User Enrollment involves the following:

1. Integrating with volume purchasing and ensuring users with Managed Apple IDs are automatically registered
2. Creating a smart user group that includes users with Managed Apple IDs and sending an invitation to volume purchasing
3. Creating a volume assignment that includes your smart user group in the scope
4. Distributing mobile devices apps and books to devices

Integrating with Volume Purchasing

Integrating with volume purchasing (formerly VPP) is the first step to using managed distribution.

Keep the following in mind when integrating with Volume Purchasing:

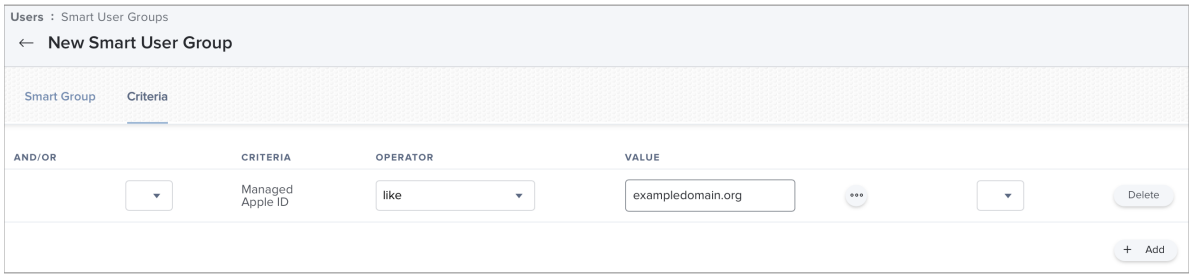
- Before distributing apps and books purchased in volume, you must first add one or more locations to Jamf Pro.
- When you add a location to Jamf Pro, you upload the service token that you obtained from Apple, and specify the country associated with the location. You can also specify other information about the account, such as the contact person and Apple ID.
- You can specify that all content purchased in volume is populated in the app and eBook catalogs.

- Make sure you select the **Automatically register with volume purchasing if users have Managed Apple IDs** checkbox. This setting ensures that users that have Managed Apple IDs are automatically registered with volume purchasing and do not receive an invitation or get prompted to register with volume purchasing. Users that do not have Managed Apple IDs receive the invitation via the method selected from the **Distribution Method** pop-up menu.

For more information, including instructions, see the Integrating with Volume Purchasing section in the *Jamf Pro Administrator's Guide*.

Creating a Smart User Group and Sending an Invitation

1. Create a smart user group that includes users with a Managed Apple ID within your domain. Your criteria should look similar to the following:



   For instructions, see Smart Groups in the *Jamf Pro Administrator's Guide*.

2. Send an invitation to users to register with volume purchasing. When configuring the scope of your invitation, do the following:

   a. Choose "Automatically register only users with Managed Apple IDs and skip invitation" from the **Distribution Method** pop-up menu.

   b. Include the smart user group created in step 1.

   Since the smart group includes users with Managed Apple IDs and the **Automatically register with volume purchasing if users have Managed Apple IDs** checkbox is selected in your Volume Purchasing settings, users will be automatically registered.

   For instructions, see User-Assigned Volume Purchasing Registration in the *Jamf Pro Administrator's Guide*.

Creating Volume Assignments

Create a volume assignment that assigns content to users.

For instructions, see User-Based Volume Assignments in the *Jamf Pro Administrator's Guide*.

Distributing Mobile Device Content to Devices

Once apps and books are assigned to users, you can distribute them to devices. For instructions, see the following sections in the *Jamf Pro Administrator's Guide:*

- In-House Apps
- Apps Purchased in Volume

Keep the following in mind when you distribute apps and books:

- If you want to distribute apps to target devices enrolled using Account-Driven User Enrollment or User Enrollment, you can create a smart device group that defines "Device Ownership Type" criteria as " Personal (Account-Driven User Enrollment)" or "User Enrollment".
- Make sure the **Make app managed if currently installed as unmanaged** checkbox is deselected.
- Distributing content with Jamf Self Service for iOS to devices enrolled via Account-Driven User Enrollment or User Enrollment is recommended. To do this, choose "Make Available in Self Service" from the **Distribution Method** pop-up menu when specifying a distribution method for the app. If you choose "Install Automatically/Prompt Users" as the distribution method and the user ignores the prompt, users will be re-prompted four hours later or during the next inventory update.

For information on installing Self Service, see Jamf Self Service for Mobile Devices in the *Jamf Pro Administrator's Guide*.

Important: To install Self Service 10.10.1 or later on personally owned devices with iOS 13 or later, or iPadOS 13 or later that were enrolled using User Enrollment, include the following in the app configuration:

```
<dict>
<key>INVITATION_STRING</key>
<string>$MOBILEDEVICEAPPINVITE</string>
<key>JSS_ID</key>
<string>$JSSID</string>
<key>SERIAL_NUMBER</key>
<string>$SERIALNUMBER</string>
<key>DEVICE_NAME</key>
<string>$DEVICENAME</string>
<key>MAC_ADDRESS</key>
<string>$MACADDRESS</string>
<key>UDID</key>
<string>$UDID</string>
<key>JSS_URL</key>
<string>$JPS_URL</string>
<key>MANAGEMENT_ID</key>
<string>$MANAGEMENTID</string>
</dict>
```

Sending a Remote Command or Mass Action

After enrolling devices in Jamf Pro using Account-Driven User Enrollment or User Enrollment, you can perform remote commands or mass actions on the devices. You can use the advanced mobile devices search you previously created to perform mass actions on all the devices enrolled using Account-Driven User Enrollment or User Enrollment. For more information on which commands can be sent to devices enrolled using Account-Driven User Enrollment or User Enrollment, see the following pages in the *Jamf Pro Administrator's Guide*:

- Remote Commands for Mobile Devices
- Performing Mass Actions for Mobile Devices

Distributing Configuration Profiles

You can distribute configuration profiles to devices enrolled in Jamf Pro using Account-Driven User Enrollment or User Enrollment. For more information, see Mobile Device Configuration Profiles in the *Jamf Pro Administrator's Guide*. Because of enhanced user data privacy protections on devices enrolled using Account-Driven User Enrollment or User Enrollment, not all payload settings are supported. If an unsupported payload is distributed, you may see an error in Jamf Pro.