Building a BYOD Program Using Jamf Pro

Technical Paper
Jamf Pro 10.2.0 or Later
2 February 2018

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 devices with Jamf Pro (formerly the Jamf Software Server) 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 build 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.

Important Concepts

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

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

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

Additional Resources

For more information on the management capabilities available for personally owned iOS devices, see Management Capabilities for Personally Owned Devices in the *Jamf Pro Administrator's Guide*.

Overview

As organizations adopt Bring Your Own Device (BYOD) programs to secure and manage personal devices in their environments, IT departments are increasingly faced with challenges due to BYOD program complexities and dismal user acceptance.

The Jamf Pro solution for personal device management is specifically designed to mitigate these challenges, with a simplified management toolset and user-focused features that help to accelerate BYOD program adoption. This allows organizations to balance the enterprise security needs of IT with the personal needs of the user.

A user-focused BYOD program implemented using Jamf Pro includes the following key benefits:

- Users can review the IT management capabilities for a personally owned iOS device, with transparency regarding everything IT has access to.
- Users can securely and easily access institutional resources such as email, contacts, calendars, Wi-Fi, and VPN, while enjoying a native experience on their preferred device.
- 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 building and maintaining a BYOD program using Jamf Pro:

1. Customize the user experience and enable personal device enrollment. You can customize the user-initiated enrollment messaging to provide distinct messages for each device ownership type—institutional ownership and personal ownership. You can also enable device enrollment for the iOS platform, and configure enrollment access for specific LDAP groups.

2. Define site-specific settings and apps for personal devices. Personal device profiles in Jamf Pro provide a single location for defining all settings and apps for personal devices. You can define settings for passcode policies, Wi-Fi, VPN, email, contacts, calendars, certificates, and security. You can also select managed apps to distribute to personal devices.

3. Direct users to the enrollment portal to enroll personal devices. This allows you to provide the enrollment URL to users in the way that best fits their environment. Optionally, you can integrate Jamf Pro with a network access management service that automatically prompts users to enroll when their device is detected on the network.

4. View and report on personal devices in inventory. You can perform an advanced mobile device search to identify personal devices enrolled in your environment and view a subset of basic inventory information for a device. You can also identify whether a personal device has the most up-to-date personal device profile installed.

5. Remotely perform management commands on a personal device. You can remotely update inventory for a personal device, and remotely lock a device. In addition, you can wipe only institutional data and settings from a personal device. This protects the user's personal data, such as photos and documents.

Requirements

To enroll and manage personally owned iOS devices with Jamf Pro using the instructions in this guide, you need:

- Jamf Pro 9.4 or later
- A push certificate in Jamf Pro
- Mobile devices with iOS 4 or later (iOS 7 or later is recommended)
- An LDAP server set up in Jamf Pro

In addition, to distribute managed apps to personal devices, the devices must have iOS 5 or later and an MDM profile that supports managed apps.

Customizing the User Experience and Enabling Personal Device Enrollment

Enrollment is the process of adding mobile devices to Jamf Pro to establish a connection between the devices and Jamf Pro. 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 personal device 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 Knowledge Base article.
- Enable user-initiated enrollment for personally owned iOS devices.
- Configure enrollment access for specific LDAP groups.

Note: Enrolling a personal device using user-initiated enrollment requires an enabled personal device profile for the site that the user belongs to, or an enabled personal device profile for the full Jamf Pro. Instructions for creating a personal device profile are included in the "Defining Site-Specific Settings and Apps for Personal Devices" section in this 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 and to skip certificate installation.

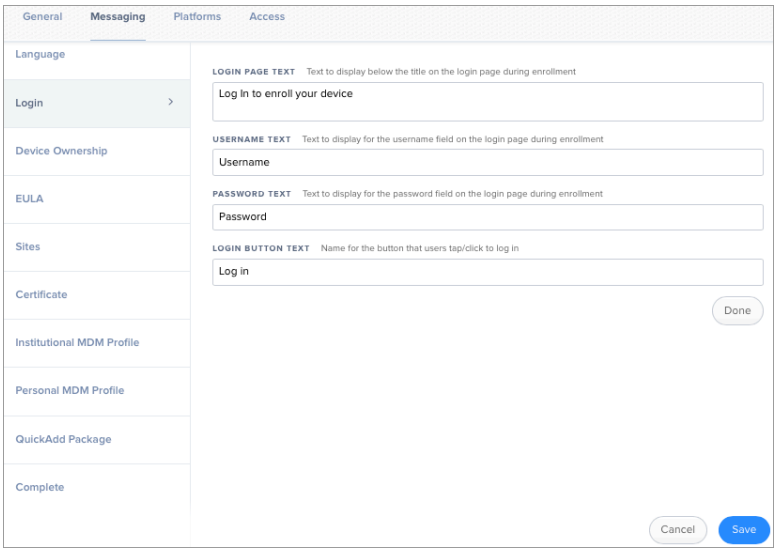
7. On the Messaging pane, do the following to customize the text displayed during the enrollment experience and add languages:

   a. Do one of the following:

      - To add a language, click **Add** + 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.

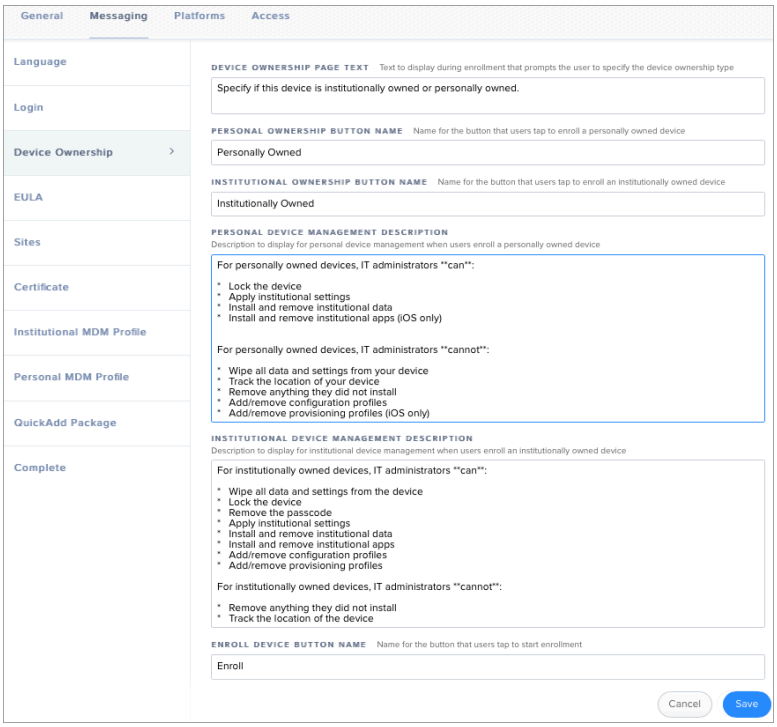
   c. On the **Login** tab, use the fields provided to customize how you want the Login page to be displayed to users.



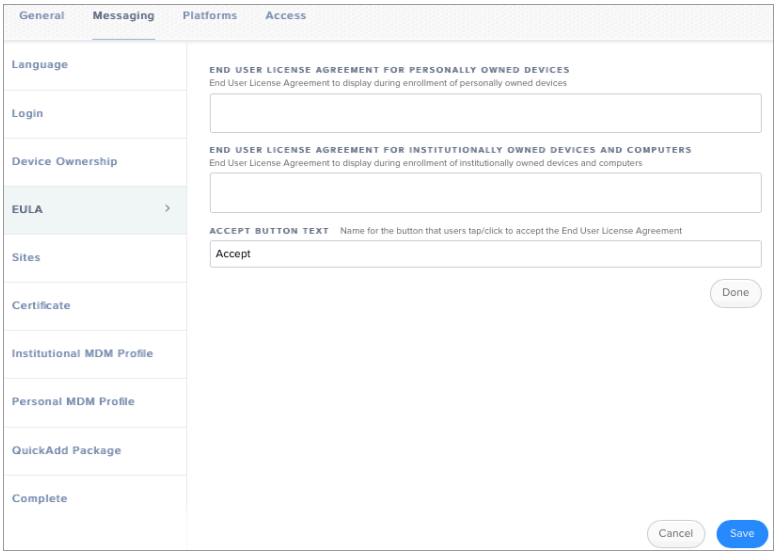
   d. Click the **Device Ownership** tab and use the fields provided to customize the text that is displayed to users based on their device ownership type. The text displayed and the enrollment page that the text displays on depends on the enrollment options that you enable:

      - **If you enable user-initiated enrollment for both institutionally owned and personally owned iOS 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.

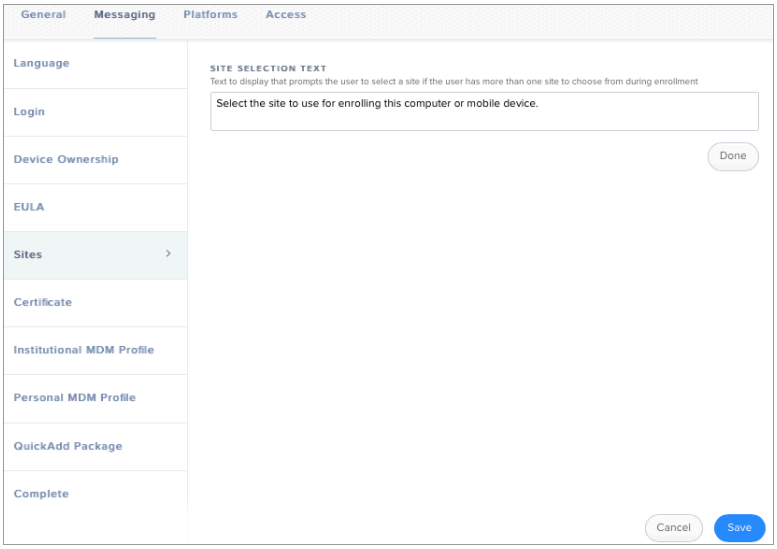
   (For instructions on enabling user-initiated enrollment, see step 8 later in this procedure.)



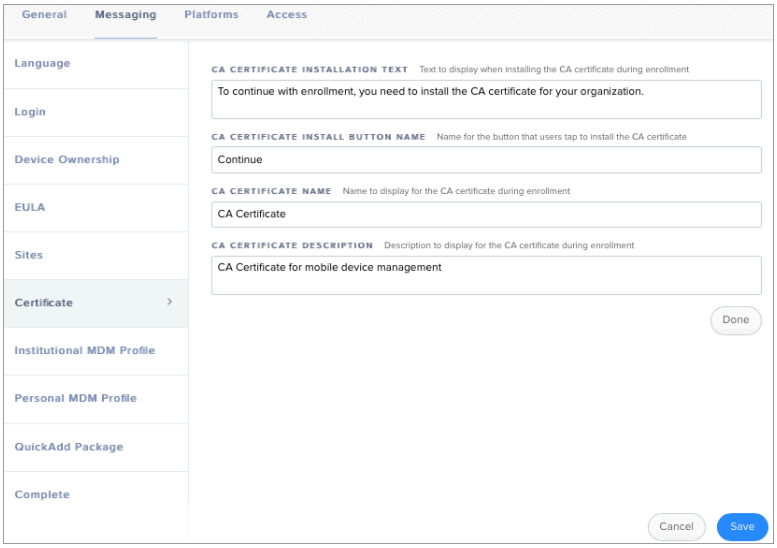
e. Click the **EULA** tab and use the fields provided to specify an End User License Agreement (EULA) for personally owned devices. If the EULA fields are left blank, a EULA page is not displayed to users during enrollment.
Note: The EULA page is not displayed for users logging in with a Jamf Pro user account.



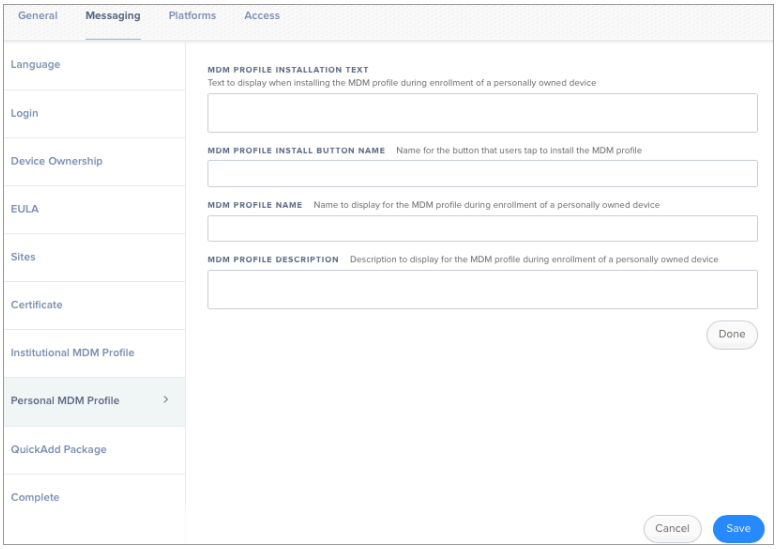
f. Click the **Sites** tab and customize the message that prompts users to choose a site.



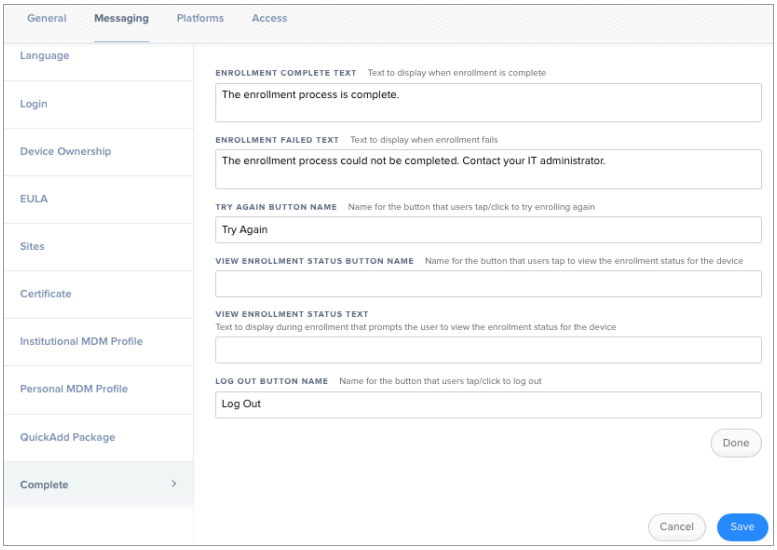
g. Click the **Certificate** tab and use the fields provided to customize the message that prompts users to install the CA certificate for mobile devices to trust at enrollment.



h. Click the **Personal MDM Profile** tab and use the fields provided to customize the message that prompts users to install the MDM profile for personally owned devices.
You can also specify the MDM profile name and description to display during enrollment.



i. 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.



j. Click **Done**.

8. On the Platforms pane, click the **iOS** tab and then select the **Enable user-initiated enrollment for personally owned iOS devices** checkbox.
9. On the Access pane, do the following to configure enrollment access for all LDAP users and/or specific LDAP groups:
   a. Do one of the following:
      - To configure enrollment access for a specific LDAP user group, click **Add** + Add and then search for the group.

- To configure enrollment access for a group already listed, click **Edit** next to the group.

b. To allow the group to enroll personally owned devices, select the **Allow group to enroll personally owned devices** checkbox.

c. (Optional) If there are one or more sites in Jamf Pro, choose the site you want to allow the LDAP user group to select during enrollment.
If an LDAP user belongs to more than one LDAP user group in Jamf Pro, the user will have the option to choose a site from a pop-up menu of sites assigned to each of those groups.

d. Click **Done**.

10. Click **Save**.

Defining Site-Specific Settings and Apps for Personal Devices

Personal device profiles are used to enroll personally owned devices with Jamf Pro via user-initiated enrollment. Personal device profiles are also used to perform management tasks on personally owned devices, including defining settings and distributing managed apps to personal iOS devices.

You can create one personal device profile for each site in Jamf Pro, and one profile for the full Jamf Pro. A personal device profile is only used to enroll and manage devices if the profile is enabled in the General payload.

The personal device profile used to enroll and manage a device is based on the site that the mobile device user has access to. Site access is determined by the LDAP directory account or Jamf Pro user account credentials entered during user-initiated enrollment.

If a profile has been enabled for the site, that profile is used to enroll the device and add the device to the site. If a profile has not been enabled for the site, or if sites have not been added to Jamf Pro, the profile for the full Jamf Pro is used if it is enabled.

Note: Changing the site that a personal device belongs to automatically changes the profile that is used to perform management tasks on the device. If a profile has not been enabled for the new site, the device will continue to be managed by Jamf Pro, but all settings and apps that were previously defined by the old profile are removed.

Personal Device Profile Payloads

The payloads and settings that you can configure using a personal device profile represent a subset of the iOS configuration profile payloads and settings available for institutionally owned mobile devices.

Before creating a personal device profile, you should have basic knowledge of configuration profile payloads and settings, and how they affect mobile devices. For detailed information about each payload and setting, see Apple's iOS Deployment Reference at:

http://help.apple.com/deployment/ios/#/cad5370d089

Managed App Distribution to Personal iOS Devices

When creating or editing a personal device profile, you can specify managed in-house apps and App Store apps to distribute to personal devices. Available apps include all managed apps that have been added to the site that the profile is assigned to, and all managed apps that have been added to the full Jamf Pro.

When a managed app is distributed to personal iOS devices, the personal device profile automatically applies settings to do the following:

- Distribute the app using the Install Automatically/Prompt Users to Install distribution method
- Remove the app when the MDM profile is removed
- Prevent backup of app data
- Prevent opening documents from managed apps in unmanaged apps

When selecting managed apps to distribute, you have the option to clone an unmanaged app and make it managed. This adds a managed version of the app to Jamf Pro and leaves the original app unmanaged.

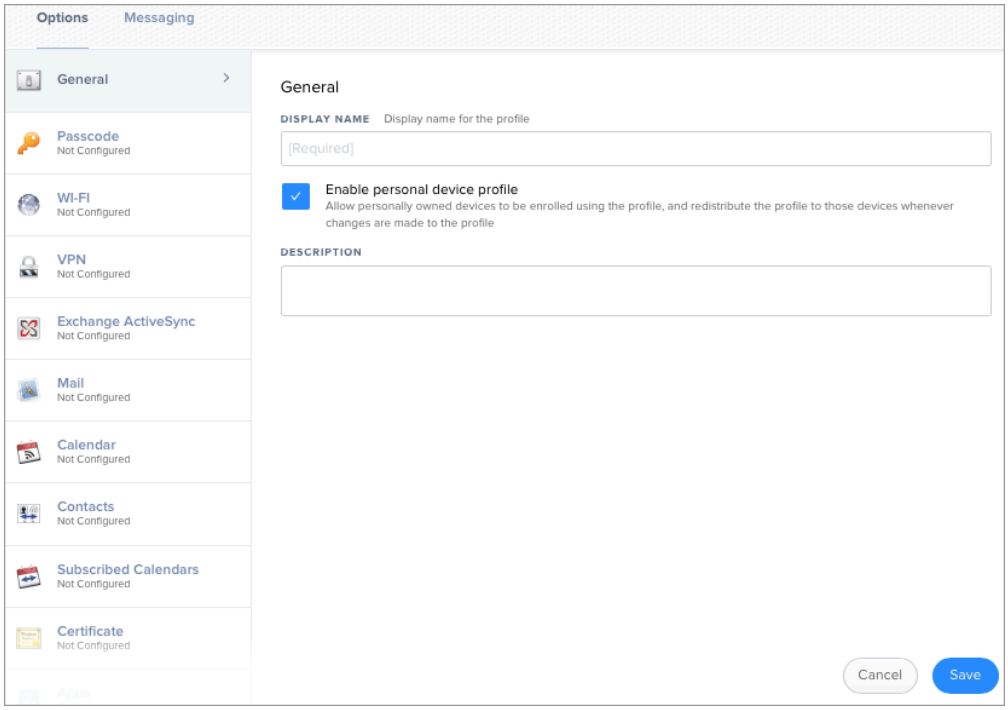
Note: Not all apps can be managed by Jamf Pro. For information on the factors that determine whether an app can be managed, see Understanding Managed Apps in the *Jamf Pro Administrator's Guide*.

Creating a Personal Device Profile

To create a personal device profile, the User-Initiated Enrollment settings must be configured to allow user-initiated enrollment for personally owned devices. In addition, you can only create a personal device profile if there is an available site (or the full Jamf Pro) that does not have a profile assigned to it.

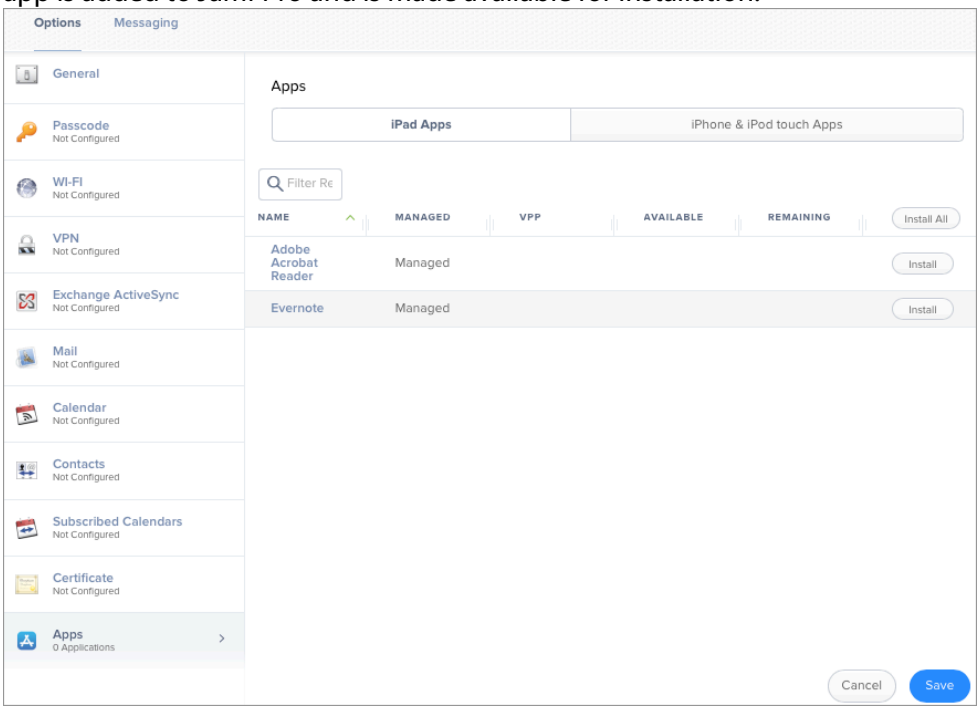
1. Log in to Jamf Pro.
2. Click **Devices** at the top of the page.
3. Click **Personal Device Profiles**.
4. Click **New** + New .
   Note: Only one personal device profile can be created per site in Jamf Pro. If all sites (or the full Jamf Pro) already have an assigned personal device profile, you will not be able to create a new one.

5. Use the General payload to configure basic settings for the profile, including the display name and the site to assign the profile to.
   Note: If you have site access only, the profile is assigned to the applicable site automatically and the **Site** pop-up menu is not displayed.
   To enable this personal device profile, select the **Enable personal device profile** checkbox.



6. (Optional) Use the Passcode payload to configure passcode policies.
7. (Optional) Use the Wi-Fi payload to configure how devices connect to your wireless network, including the necessary authentication information.
8. (Optional) Use the VPN payload to configure how devices connect to your wireless network via VPN, including the necessary authentication information.
9. (Optional) Use the Exchange ActiveSync payload to define settings for connecting to your Exchange server.
10. (Optional) Use the Mail payload to define settings for connecting to POP or IMAP accounts.
11. (Optional) Use the Calendar payload to define settings for configuration access to CalDAV servers.
12. (Optional) Use the Contacts payload to define settings for configuration access to CardDAV servers.
13. (Optional) Use the Subscribed Calendars payload to define settings for calendar subscriptions.
14. (Optional) Use the Certificate payload to specify the X.509 certificates (.cer, .p12, etc.) you want to install on devices to authenticate the device access to your network.
15. (Optional) Select the Apps payload and then do any of the following:
    - To distribute a managed app to personal iOS devices added to the site (or the full Jamf Pro) that the profile is assigned to, click **Install** next to the app name. (To distribute all managed apps, click **Install All**.)

- To remove a previously distributed managed app from devices, click **Remove** next to the app name. (To remove all managed apps previously distributed with this profile, click **Remove All**.)
- To clone an unmanaged app to add a managed version of the app to Jamf Pro, click the unmanaged app name and then click **Clone App and Make Managed**. A managed version of the app is added to Jamf Pro and is made available for installation.

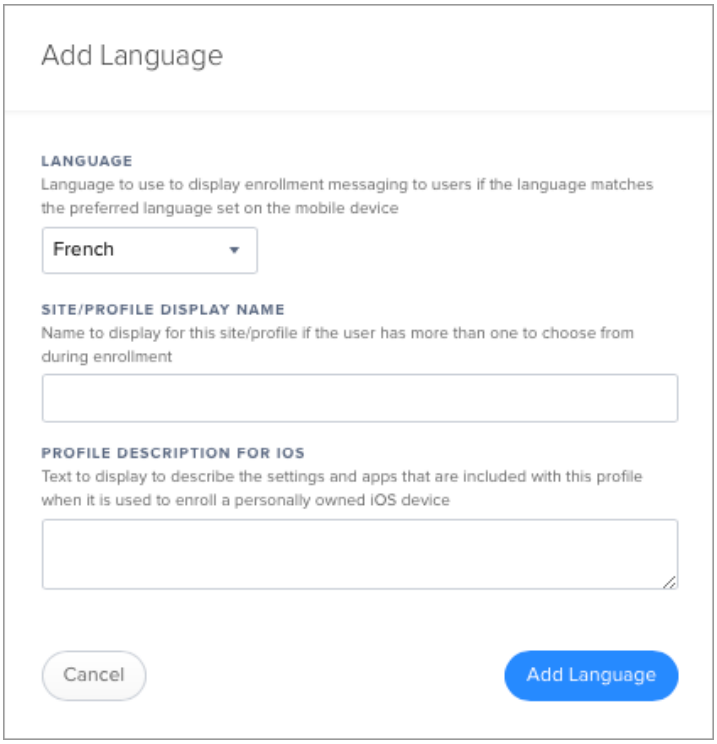


16. (Optional) To add messaging that displays during user-initiated enrollment if the user belongs to multiple LDAP user groups with access to multiple sites, do the following:

    a. Click the **Messaging** tab, and then click **Add** + Add .

    b. Choose a language from the **Language** pop-up menu.

    c. Use the settings on the pane to specify the site/profile display name, as well as the text to describe the settings included with the profile. You can also list any managed apps that will be included with the profile.



    d. Click **Add Language**.

    e. Repeat this process as needed for other languages.

17. Click **Save**.

    If the profile is enabled in the General payload, it will be used to enroll personal devices with Jamf Pro when users enter credentials for an LDAP directory account or a Jamf Pro user account that has access to the site (or to the full Jamf Pro).

Cloning, Editing, or Deleting a Personal Device Profile

Consider the following when cloning, editing, or deleting a personal device profile:

- **Cloning**—You can only clone a personal device profile if there is an available site (or the full Jamf Pro) that does not have a profile assigned to it.
- **Editing**—When a personal device profile is edited and saved, it is automatically redistributed to personal devices belonging to the site (or the full Jamf Pro) that the profile is assigned to.
  When editing an enabled profile, if you deselect the **Enable personal device profile** checkbox in the profile's General payload, all personal devices belonging to the site that the profile is assigned to will continue to be managed by Jamf Pro, but all settings and apps that were previously defined by the profile are removed.
- **Deleting**—When a personal device profile is deleted, all personal devices belonging to the site that the profile is assigned to will automatically be changed to use the profile assigned to the full Jamf Pro if a profile for the full Jamf Pro is enabled. If an enabled profile for the full Jamf Pro does not exist, or if you are deleting the profile assigned to the full Jamf Pro, then the applicable devices will continue to be managed by Jamf Pro, but all settings and apps that were previously defined by the profile are removed.
  Note: A personal device profile is automatically deleted if the site it is assigned to is deleted from Jamf Pro.

Directing Users to the Enrollment Portal to Enroll Personal Devices

To direct users to the enrollment portal for user-initiated enrollment, you need to provide them with the enrollment URL. The enrollment URL is the full URL for Jamf Pro followed by "/enroll". For example:

https://jss.mycompany.com:8443/enroll

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

Adding a Network Integration Instance

Optionally, you can automatically refer users to the enrollment portal by integrating Jamf Pro with a network access management service, such as Cisco Identity Services Engine. (For more information on integrating Jamf Pro with a network access management service, see Network Integration in the *Jamf Pro Administrator's Guide*.)

1. Log in to Jamf Pro.
2. If you have not already created and saved an advanced mobile device search to be used by the network access management service, do the following to create the search:
   a. Click **Devices** at the top of the page.
   b. Click **Search Inventory**.
   c. Click **New** 

.
   d. On the Search pane, select the **Save this Search** checkbox and enter a display name for the search.
   e. Click the **Criteria** tab.
   f. Click **Add**

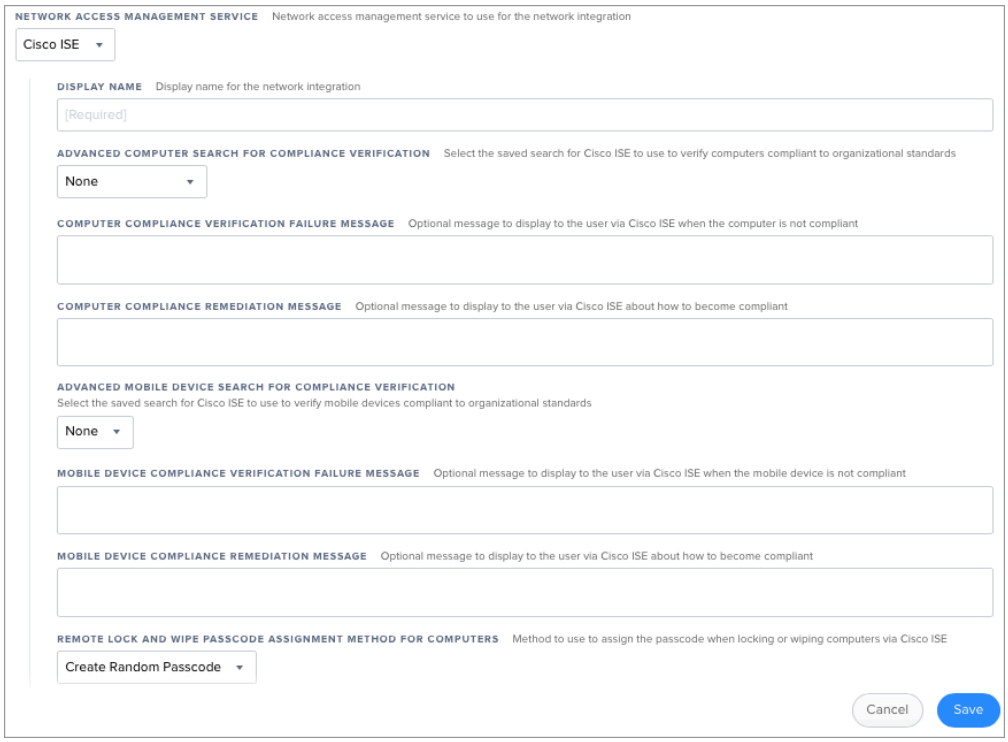
.
   g. Click **Show Advanced Criteria**, and then click **Choose** for "Managed".
   When the "Managed" criteria is displayed, make sure the operator is set to "is".
   h. Click **Browse**
, and then click **Choose** for "Managed".
   i. Click the **Display** tab and select the attribute fields you want to display in your search results.
   j. 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.
   Note: Additional criteria can be added as needed, depending on your organization's compliance standards.
3. In the top-right corner of the page, click **Settings** 
.

4. Click **Network Organization**.

5. Click **Network Integration** .

6. Click **New** .
   Note: Only one network integration instance can be added per site in Jamf Pro. If all sites already have a network integration instance, you will not be able to add a new one.

7. Configure the network integration instance using the settings on the pane, including the site, the advanced mobile device search to be used for compliance verification, and compliance messaging to be displayed to users.



8. Click **Save**.
   After saving the network integration instance, a unique network integration URL appears at the bottom of the pane. This URL will be used by the network access management service to communicate with the specific Jamf Pro network integration instance.

User Experience for Personal Device Enrollment

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

The text displayed in each step of the enrollment experience reflects the customized text that has been entered on the Messaging pane tabs in the User-Initiated Enrollment settings.

Note: For detailed information on the user experience for enrolling a personal device, including screen shots of each enrollment page displaying the default English text, see User-Initiated Enrollment Experience for Mobile Devices in the *Jamf Pro Administrator's Guide*.

User-Initiated Enrollment Experience

The following steps outline the user experience for enrolling a personally owned iOS device:

1. Log in.
When users access the enrollment portal from their device, they must log in by entering credentials for an LDAP directory account or a Jamf Pro user account with user-initiated enrollment privileges.

2. Specify the device ownership type (if applicable).
If both institutionally owned device enrollment and personally owned device enrollment are enabled in Jamf Pro, the user must select the personal device ownership option. When this option is selected, the user can view the personal device management description that has been entered on the Messaging pane Device Ownership tab in the User-Initiated Enrollment settings. This description represents the IT management capabilities for a personal device.

3. Accept the End User License Agreement (if applicable).
If an End User License Agreement (EULA) has been entered on the Messaging pane EULA tab in the User-Initiated Enrollment settings, the user must accept the EULA terms to continue with enrollment.

4. Choose a site (if applicable).
If the user is a member of multiple LDAP user groups and site access has been configured separately for those groups on the Access pane in the User-Initiated Enrollment settings, the user must select the site to use to enroll their personal device. If a profile description was entered on the Messaging pane when creating the personal device profile assigned to the selected site, that profile description is displayed.

5. Install the CA certificate (if applicable).
The user must tap through a series of screens to install the CA certificate.
Note: This step is skipped if the **Skip certificate installation during enrollment** checkbox is selected on the General pane in the User-Initiated Enrollment settings and the user's environment has an SSL certificate that was obtained from an internal CA or a trusted third-party vendor.

6. Install the MDM profile.

The user must tap through a series of screens to install the MDM profile. On the first screen in the series, the user can tap the **Information** icon to view the personal device management description that has been entered on the Messaging pane **Device Ownership** tab in the User-Initiated Enrollment settings. This description represents the IT management capabilities for a personal device.

Enrollment is complete.

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

Viewing and Reporting on Personal Devices in Inventory

After enrolling personal devices using the instructions in this guide, you can use advanced mobile device searches to identify personal devices enrolled in your environment and view a subset of basic inventory information for a device.

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.

Note: For information on the inventory information that you can view and edit for a personal device, see Viewing and Editing Inventory Information for a Mobile Device in the *Jamf Pro Administrator's Guide*.

Performing an Advanced Mobile Device Search for Personal Devices

You can create and save an advanced mobile device search to view all personal devices managed by Jamf Pro. You can also use the advanced search to identify whether those devices have the most up-to-date personal device profile installed.

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".

8. To narrow the search to find personal devices that do not have an up-to-date personal device profile installed, do the following:
   - Click **Add** .
   - Click **Show Advanced Criteria**, and then click **Choose** for “Personal Device Profile Status”.
   - Click **Browse** , and then click **Choose** for “Out of date”.
9. Click the **Display** tab and select the attribute fields you want to display in your search results.
10. 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.
11. Click **View**.
    The list of search results is displayed.
12. 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.

Remotely Performing Management Commands on a Personal Device

The remote commands available in Jamf Pro allow you to remotely perform the following tasks on a personal device:

- **Update Inventory**—Prompts the mobile device to contact Jamf Pro and update its inventory.
- **Lock Device**—Locks the mobile device. If the mobile device has a passcode, the user must enter it to unlock the device.
- **Wipe Institutional Data**—Permanently erases institutional data and settings on the device, removes managed apps, and makes the device unmanaged.
- **Send Blank Push**—Prompts the mobile device to check in with Apple Push Notification service (APNs).

Sending a Remote Command

1. Log in to Jamf Pro.
2. Click **Devices** at the top of the page.
3. Perform a simple or advanced mobile device search.
4. Click the mobile device you want to send the remote command to.
5. Click the **Management** tab, and then click the button for the remote command that you want to send. If you are sending a Lock Device command, enter a lock message and phone number if desired, and then click **Lock Mobile Device**.

   The remote command runs on the mobile device the next time the device contacts Jamf Pro.

Viewing the Status of Remote Commands

1. Log in to Jamf Pro.
2. Click **Devices** at the top of the page.
3. Perform a simple or advanced mobile device search.
4. Click the mobile device you want to view remote commands for.
5. Click the **History** tab.
6. Use the Management History pane to view completed, pending, or failed commands.

Canceling a Remote Command

1. Log in to Jamf Pro.
2. Click **Devices** at the top of the page.
3. Perform a simple or advanced mobile device search.
4. Click the mobile device for which you want to cancel a remote command.
5. Click the **History** tab, and then click **Pending Commands**.
6. Find the command you want to cancel, and click **Cancel** across from it.