Deploying iPad to Patients

Setup Guide

Contents

Overview

Healthcare institutions are increasingly focused on engaging patients and delivering a great experience throughout their stay in the hospital. Deploying iPad with patient-centered apps enables hospitals to enhance each step of the patient journey, from check-in through discharge. With third-party iOS apps, hospitals can empower patients to access their daily schedule, connect with their care team, track their progress, get educated on their treatment plan, and personalize their entertainment—putting patients in the center of care.

This Setup Guide offers guidance to the hospital IT staff who are configuring and deploying iPad for patients to use. iPad can be preconfigured with minimal setup so patients have access to iOS apps, and IT can use mobile device management (MDM) to protect patient data while also preserving a great user experience. Once a patient has been discharged, the iPad can be securely wiped so all patient-generated data is removed, and reset to factory settings so it's ready for the next patient to use.

A key decision when deploying iPad to patients is to choose between in-room versus centralized storage of the device (described in the In-Room Storage and Centralized Storage sections). In-room storage is enabled by over-the-air (OTA) wiping and resetting of iPad, which allows devices to stay in the patient room at all times. Many hospitals prefer this deployment because it minimizes the work required from nurses or other staff members. At the same time, there may be compelling reasons for centralized storage deployment, such as when there are fewer iPad devices than rooms or when there are readily available staff or volunteers who can help keep track of devices as patients are admitted or discharged.

Regardless of which deployment scenario you choose, the preparation steps described in this paper are important for any successful deployment.

Getting Prepared

This section outlines four steps to follow when preparing to deploy devices and apps in the hospital.

Evaluate your infrastructure

The first step is to evaluate your network infrastructure. The physical layout of the hospital and how people interact within the physical space is critical to how you design your network and plan for Wi-Fi coverage and capacity.

Wi-Fi and networking

Consistent and dependable access to a wireless network is key to setting up and configuring iOS devices. Confirm that your hospital's Wi-Fi network can support multiple devices with simultaneous connections from all your users. You might also need to configure your web proxy or firewall ports if devices are unable to access Apple's activation servers or the iTunes Store. Apple and Cisco are optimizing the network experience for devices running iOS 10 or later. Talk to your Apple or Cisco representative to get the latest information about these networking features.

Content Caching

An integrated feature of macOS, Content Caching stores a local copy of frequently requested content from Apple servers, helping to minimize the amount of bandwidth needed to download content on your network. Content Caching speeds up the download and delivery of software through the App Store, Mac App Store, iTunes Store, and iBooks Store. It can also cache software updates for faster downloading to multiple iOS devices. Content Caching includes the tethered caching service, which allows a Mac to share its Internet connection with many iOS devices connected via USB.

Invest in an MDM solution

MDM gives organizations the ability to securely enroll iOS devices in the hospital environment, wirelessly configure and update settings, establish policies, deploy and manage apps, as well as remotely wipe or lock managed devices. These features are built into iOS and are enabled by third-party MDM solutions. MDM solutions are available from a wide range of vendors and can be cloud hosted or installed on-premise. MDM solutions come with different features and pricing, so you have flexibility in deciding which solution best fits your needs. Some MDM solution providers also offer predefined settings that make it even easier to configure devices for patient use.

Create a configuration

Once you have selected an MDM solution, you'll need to create a configuration that's specifically optimized for the patient use case and can be installed by your MDM solution over the air. A configuration will typically contain settings and restrictions that set up the device in a posture that's appropriate for patient use. These settings will help streamline the initial patient experience and also disable features or services that might store personal data or be unnecessary.

Restrictions

The following are examples of restrictions you're likely to disable so that no personal information is left on the device. **Note:** Descriptions may vary by MDM solution.

Device management: Disallow manual profile installation, disallow configuring of restrictions, disallow device name changing, disallow account modification, force Limit Ad Tracking, and disallow pairing with non-Configurator hosts.

Data management: Disallow documents from managed sources in unmanaged destinations, disallow documents from unmanaged sources in managed destinations, and enforce AirDrop as an unmanaged destination.

Apps: Disallow the App Store icon on the Home screen, disallow app removal, disallow in-app purchase, disallow user to trust unmanaged enterprise apps, and hide specific apps on the Home screen.

Media: Disallow use of the iTunes Store, disallow use of the iBooks Store, disallow Game Center, uncheck force iTunes Store password entry, and restrict media content as needed.

Home screen layout, Lost Mode, and other settings

You can manage how apps, folders, and web clips are arranged on the Home screen of supervised devices. Enable use of the camera so hospital staff can scan a patient's QR code using a secure patient app or add the patient's photo to an electronic medical record (EMR) app. To track any missing iPad devices, make sure your MDM supports the features related to Lost Mode, such as a lost message text, query location of device, and reenable Lost Mode after reset or restore. Note that Lost Mode will allow an administrator to query the location of a lost device even if the user has disabled location services.

Automate device setup

The Device Enrollment Program (DEP) provides a fast, streamlined way to deploy hospital-owned iOS devices that are purchased directly from Apple or participating Apple Authorized Resellers or carriers. DEP enables automatic MDM enrollment of patient devices on activation. You can also manually enroll iOS devices in DEP using Apple Configurator 2, regardless of how you purchased them. With DEP, devices are always supervised and MDM enrollment is mandatory. However, the user has a 30-day provisional period to remove the device from enrollment, supervision, and MDM.

Configure DEP settings

Associate devices in DEP with your MDM solution and consider implementing the settings below:

- Enable supervision.
- Allow pairing (disable through profile later if required).
- Disallow MDM profile removal.
- Require MDM enrollment.
- Skip all screens in Setup Assistant.

Note: Descriptions and grouping may vary by MDM solution.

Distribute apps

The Volume Purchase Program (VPP) allows you to purchase apps in bulk for distribution to patients through your MDM solution. MDM solutions integrate with VPP and can be used to distribute apps to devices in any country where the app is available.

Assign apps to devices

For in-room and centralized storage deployments, you'll need to assign apps directly to devices using your MDM solution or Apple Configurator 2. Once assigned to a device, an app is pushed to that device by MDM—and no Apple ID or iTunes account is required. Anyone who uses that device has access to the app.

Set up an app catalog

It's highly recommended that you work with your MDM solution provider to create an app catalog for recommended apps you'd like your patients to use. An app catalog presents suggested apps for patients to download as needed, in a self-service fashion.

Typically, only a few essential apps might need to be preinstalled for the patient during the initial setup. By introducing an app catalog, patients can download additional recommended apps as needed. This reduces the load on your Wi-Fi network and reduces deployment time significantly.

In-Room Storage

Once your network and MDM infrastructure are prepared, you'll need to choose your preferred deployment scenario. With an in-room storage deployment, you can leverage over-the-air device setup and software updates, and automatically reset the iPad when the patient is discharged. This deployment scenario enables you to keep your devices in each room, so patients can customize their iPad the moment they arrive.

Initial setup

When the patient is first handed an iPad, the built-in Setup Assistant guides the individual through personalizing the device. From the Hello screen, the patient should select a language, a region, "set up manually," and a public Wi-Fi network. No other steps are required, and all other Setup Assistant screens can be skipped through DEP.

To establish initial connectivity and enrollment, you should provide a public Wi-Fi network without using a captive portal. Once the iPad is enrolled, MDM can automatically transition the device to a private Wi-Fi network for the remaining setup. Using a private Wi-Fi network will also provide better security for the duration of the patient's hospital stay.

Once this has been completed, MDM configures the device settings and installs apps over the air. The amount of time this process takes will depend on your Wi-Fi network, whether you're using Caching Server, and the number of apps you're installing on each iPad.

Reset your device

Once the patient has been discharged, you'll need to reset the iPad for the next patient by erasing all content and settings. You can either remotely wipe the iPad using MDM or manually reset the device.

Remote wipe with MDM

To wipe iPad remotely, MDM can perform a full device wipe over the air. Typically an IT administrator would perform this task, but it's better to automate the remote wipe command with your MDM solution. For example, you can trigger a remote wipe in a hospital setting when a patient is discharged by sending a notification from your EMR or other record-keeping system to your MDM solution. This signal can then be used to trigger a remote wipe from the MDM server. There are potentially two approaches to integrating this process:

- MDM vendors can write code that "listens" for a discharge command from an accessible system or a network location, and then initiates a remote wipe.
- EMR systems can have this capability built directly into their products to automatically wipe the iPad the moment a patient has been discharged.

Manual reset

For a manual reset, a staff member can tap Settings > General > Reset > Erase All Content and Settings.

Note: When using a centralized storage deployment, it's not necessary to enable remote wipe. Learn more in the Centralized Storage section.

Centralized Storage

The alternative to in-room storage is to store multiple iPad devices in a secure cart attached to a portable workstation. Each iPad is connected to a Mac by USB, and an automated enrollment process is used to wipe and reset your iOS device to the Home screen before it's assigned to the next patient.

This workflow uses Apple Configurator 2 to enable a hands-free setup process so users don't need to tap the iPad screen, while also making it easy for your staff to check your iOS devices in and out.

Set up Apple Configurator

With this free macOS application, update iOS devices to the latest version of iOS, configure device settings and restrictions, and install apps and other content. After initial setup, you can continue to manage everything remotely using MDM or Apple Remote Desktop. Learn more in the Install Apple Remote Desktop section.

For instructions on creating and exporting a supervision identity in Apple Configurator 2, visit http://configautomation.com/identity-files.html. This identity must be uploaded to MDM for use in supervising DEP-enrolled devices.

Enable automation tools

Automator is used to automate the features of macOS and its applications. The Automator actions for Apple Configurator 2 make it easy to create and apply "automation recipes" for setting up iOS devices. As a result, you can streamline the configuration and setup of multiple connected iPad devices. For more information on using Automator, visit https://configautomation.com.

Ensure that Install Automation Tools has been activated in Apple Configurator 2 by selecting Apple Configurator 2 > Install Automation Tools.

Create a Wi-Fi configuration profile

Using Apple Configurator 2, create a configuration profile containing Wi-Fi credentials. Determine the following:

- Service Set Identifier
  - Hidden Network
  - Auto Join
- Proxy Setup
- Security Type
- Password
- Network Type

Perform initial device enrollment

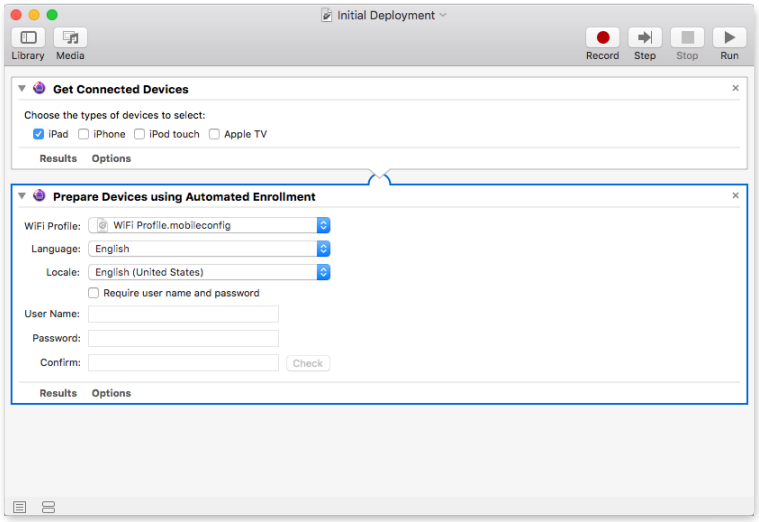
Create the following workflow to perform an initial deployment of devices. In Apple Configurator 2, DEP enrollment is available as an Automator action.

Get Connected Devices: Choose types of devices to select.

Prepare Devices using Automated Enrollment: Add the Wi-Fi configuration profile created earlier and set the Language and Locale settings.

Note: Apple Configurator 2 should be running to prevent iTunes and Photos from launching on device connection. Alternatively, use appropriate default commands to disable this behavior.

Connect all devices to the iPad cart or USB hub and run the Initial Deployment workflow.



Configure Automator for device refresh

Create the following workflow to perform a device refresh upon attaching an iPad. Download and install the following attachment actions from http://configautomation.com/attach-workflow.html.

Automator workflow: An attached workflow needs to begin with the Begin Attached Workflow action and end with the End Attached Workflow action.

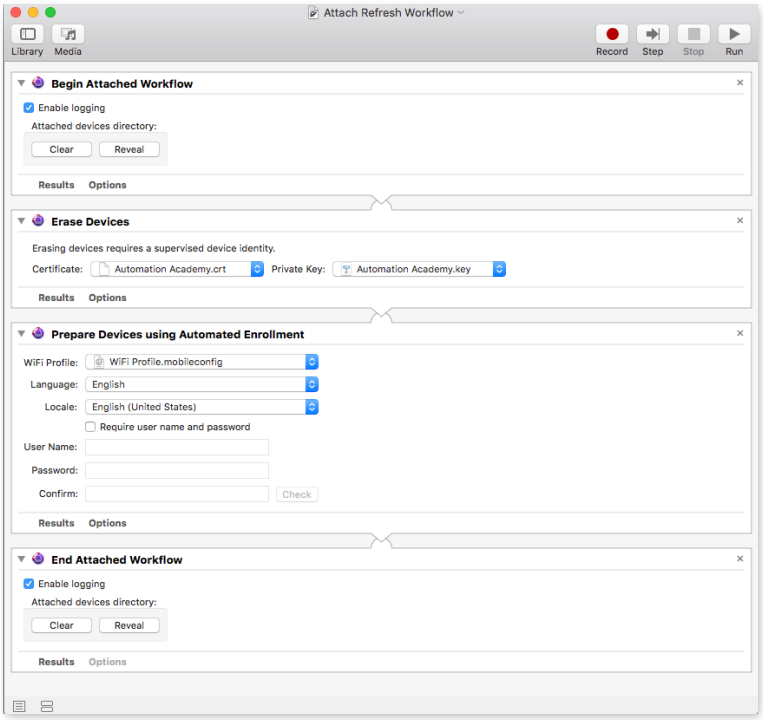
Erase and Restore actions: The first action after the Begin action will be either Erase Devices or Restore Devices.

The Erase Devices action requires the connected device to be either unlocked and paired or supervised. A supervision identity is required for devices not running iOS 9 or later.

If the connected device does not meet these requirements or the supervision identity installed in Apple Configurator 2 does not match the identity used to supervise the device, the workflow will fail.

The Restore action doesn't require the device to be supervised. It will wipe the connected device and install the latest OS if necessary. This process takes approximately five minutes.

Prepare Devices using Automated Enrollment: Configure this action the same way as the initial configuration.



Attach shell-script command file

For the workflow to run automatically upon attachment of an iOS device, a shell-script command file must be created. This script is executed by the cfgutil application. Details can be found at http://configautomation.com/attach-workflow.html. An example is shown below:

```
    #!/bin/bash
    # set attachPID to Process ID of THIS thread
    export attachPID=$$
    # Set Attached Device Directory Value
    workflowPath=$(echo ~/Library/Workflows/attachment-workflow.workflow)
    automator -i
       "ECID=$ECID&attachPID=$attachPID&PATH=$PATH&UDID=$UDID&dev
       iceName=$deviceName&deviceType=$deviceType&buildVersion=
       $buildVersion&firmwareVersion=$firmwareVersion&locationID=
       $locationID" "${workflowPath}"
    # Check if Cache File exists
    if [ ! -f ~/Library/Caches/com.apple.configurator.AttachedDevices/
    $ECID.plist ];
       then
       echo "Cache file not found - Automator Workflow completed
       successfully"
    else
       # Cache file found - Need to check if the PID matches
       echo "Cache File Found - Test PID"
       # Get the PID from the file
       filePID=$(defaults read ~/Library/Caches/com.apple.configurator.
          AttachedDevices/$ECID.plist attachPID)
       if test $attachPID -eq $filePID
       then
       # The file was created by this PID so the Workflow Failed - Clean up
       echo "PID Match - Workflow has failed - Clean up"
       rm ~/Library/Caches/com.apple.configurator.AttachedDevices/
       $ECID.plist
    else
       # Re-Entry - Do Nothing
       echo "Re-Entry - Do Nothing"
    fi
fi
```

In the command file (attach.command), change the placeholder to the path to the Automator workflow you wish to run on device attachment:

workflowPath=$(echo ~/Library/Workflows/attachment-workflow.workflow)

Save this script with the attached workflow and ensure that it's executable (chmod +x).

Preventing unintended consequences: If using the Restore Devices action, any device connected to the workstation will be wiped without warning.

To limit the execution of the script to known devices, you can check the attached device against a list of devices provided in the script.

To learn more, refer to Specifying Workflows for Device Groups at http://configautomation.com/attach-workflow.html.

Automate device refresh

To automatically run an instance of the specified shell script whenever an iOS device is attached or detached from the host computer, create and install a Launch Services instruction file. Download the provided example files at http://configautomation.com/autoloaunchfiles.zip.

In the provided Launch Services property list (com.example.attached.plist), change the placeholder path to the command file you're using. After making the change, put the property list file in the LaunchAgents folder in the user Library folder. The process will load automatically at next login or can be toggled manually using the launchctl command. Details can be found at http://configautomation.com/attach-workflow.html. The following is an example:

```
<?xml version="1.0" encoding="UTF-8"?>
      <!DOCTYPE plist PUBLIC "-//Apple//DTD PLIST 1.0//
EN" "http://www.apple.com/DTDs/PropertyList-1.0.dtd">
<plist version="1.0">
<dict>
   <key>KeepAlive</key>
   <true/>
   <key>Label</key>
   <string>com.example.attached</string>
   <key>ProgramArguments</key>
   <array>
         <string>/usr/local/bin/cfgutil</string>
         <string>-vvv</string>
         <string>exec</string>
         <string>-a</string>
         <string>'/Users/yourUserName/path/to/
         exampleattachment.command'</string>
   </array>
   <key>RunAtLoad</key>
   <true/>
</dict>
</plist>
```

File permissions for supervision files

For the cfgutil utility to use the supervision certificate and private key, they must be set to be readable by only the user running the script.

In Terminal, use chmod 700 /path/to/file to ensure that this is the case if the supervision files have been moved around on the file system.

Install Apple Remote Desktop

Apple Remote Desktop is a macOS remote desktop management application. It can be used for software distribution, asset management, and remote assistance. With a centralized storage deployment, Apple Remote Desktop allows you to remotely manage multiple Apple Configurator 2 workstations from a single Mac. This enables you to quickly make any required updates to your configuration profiles without having to interrupt your staff from checking in and checking out patient iPad devices. Take an existing package, from either Apple or a third party, and simply use the Install Package to copy and install on multiple workstations within your hospital environment. The screen-sharing features of Apple Remote Desktop allow you to provide immediate help to your remote stations, saving time for both you and the hospital staff.

To learn more about setting up Apple Remote Desktop, visit http://www.apple.com/remotedesktop/pdf/ARD3_AdminGuide.pdf.

Summary

You have options for deploying and managing iPad devices for your patients to use, whether your hospital deploys iPad to a group of users or across the entire organization. And by choosing the right deployment strategies for your organization, you can help your staff focus on what's most important—providing care to your patients.