# ICUFL—Tech—Client—iPadWebex

Author: PJ McKenna

Contributors: "Galway 'ICU FamilyLink' Contributor Group", consisting of Irial Conroy, Dr. Aoife Murray, Brian O'Donoghue, Breda McColgan, PJ McKenna, Frank Kirrane, Leonie Cullen

Acknowledgements: We acknowledge the assistance of the following in the preparation of this document - National University of Ireland Galway, University Hospital Galway & Saolta University Healthcare Group, IBM, Cisco



Version 1.0
8th June 2020

# 1 Intent

This document details how to set up iPads as test-clients for the 'ICU FamilyLink' system, where that system is based on Cisco Webex. These instructions are subject to change due to updates to the software concerned.

It is intended that the reader has first read the document 'ICUFL—Logical Architecture', which sets the context for 'ICU FamilyLink', both in terms of use-case and technical considerations.

# 2 Table of Contents

# 3 Intended audience

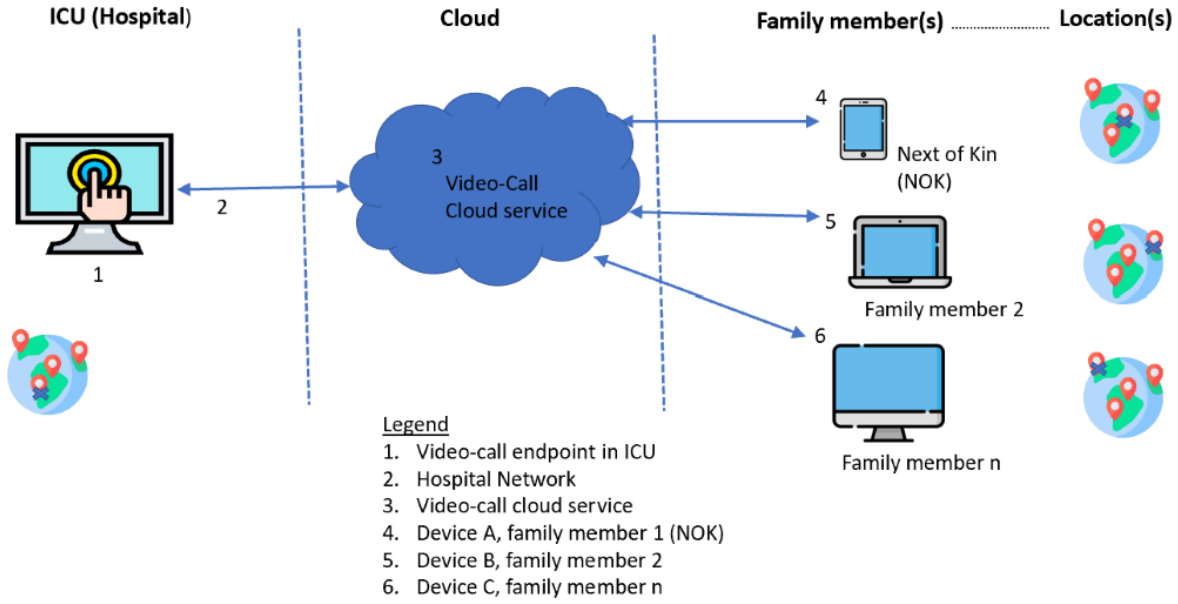
This document is intended to assist in system planning and implementation, and is written for two audiences:

- The system planner who needs to know the requirements for device configuration and management.
- The implementation engineer who will provision the iPads.

The implementation engineer must have an understanding of modern interconnected mobile device operating systems and Internet Protocol networking but does not need to be an expert in either.

# 4 System overview

Logical System Overview




# 5 Client Devices (iPads)

As part of the ICU FamilyLink system, the iPad devices play a role in the following use cases:

1. Testing the 'Virtual Family Room' configuration and performance
2. Training ICU staff members in video-call facilitation

Given the use cases, and the skill sets and priorities of those involved, the iPads' configuration must focus on robustness and ease of use.

It is recommended that the iPads should be configurable remotely by a Mobile Device Management (MDM) system. The local IT team can guide on which MDM is in place locally – consider leveraging

that MDM. This document provides pertinent configuration and usage instructions for one specific MDM: that is, Cisco Meraki.

## 5.1 Provisioning process overview

The steps in the iPad provisioning process are:

1. Configure the remote management tools to facilitate the iPads functioning in the intended roles in the expected environment.
2. Enrol each iPad under the Apple Device Enrolment Program, (DEP) using an Apple School Manager (ASM) or Apple Business Manager (ABM) account.
3. Administer the iPads using a Mobile Device Management system; for example, Cisco Meraki.
4. Test the iPads.

**The longest lead time in the provisioning process is likely to be the credentials for the Apple Device Enrolment Program.** If the iPads were sourced from a retailer who purchased the iPads from the Volume Purchase Program, the retailer might be able to remotely reconfigure the iPads to take their configuration from your MDM. If not, apply the necessary iPad profile using a combination of freely available Apple Configurator software, an Apple Mac to run it on, and a cable to connect the two devices.

## 5.2 Configuring the online tools

The two online tools - Apple Device Enrolment Program and Cisco Meraki – must be configured to work together.

The procedure is:

1. On Meraki, hover over **Organisation**. From the list that appears, under the "Configure" heading, select "Create Network". A window will appear asking for information for the new network.
2. For **Network name** enter a descriptive name for the new network.
3. For **Network type** select **EMM (Systems Manager)**.
4. Click the "Create Network" button.
5. On Meraki, hover over **Organisation**. From the list that appears, under the **Configure** heading, select **MDM**.
6. Scroll down to the **Apple Device Enrolment Program** section.
7. Download the Meraki_Apple_DEP_cert.pem file provided.
8. In another browser window, go to the Apple Business Manager or Apple School Manager portal and sign in with the Apple ID tied to the desired organization.
9. Navigate to **Settings > Device Management Settings**.
10. Click **Add MDM Server**.
11. Enter a **Name** for the MDM server in DEP, then click **Next**.

12. Click **Choose File...** and upload the .pem public key downloaded in step 7, then click **Next**.
13. Download the server token provided, then click **Done**.
14. Back in Meraki, click on the **Choose File** button in the DEP section.
15. Select/upload the server token downloaded in step 13.
16. Choose the default Systems Manager network where devices tied to this MDM server in DEP will be enrolled.
17. Click **Save Changes**.
18. You should see a new entry under **Apple DEP Servers** corresponding to the information you entered from steps 11 to 16.

### 5.2.1 Using Apple Configurator to enrol an iPad under Meraki

Before starting this work, please consult the Apple Configurator documentation.

Prerequisites:

- An Apple MacOS workstation (MacBook or iMac) and a cable to connect it to the iPad
- Apple Device Enrolment Program credentials (either Apple School Manager or Apple Business Manager)
- An Apple ID (email address and password) that will be associated with the iPads.
- WiFi credentials in the setup environment
- The Apple Configurator 2 application
- An existing Meraki installation

**Please note that the enrolment procedure will wipe the contents of the iPad.**

### 5.2.2 Assigning the iPads to the Meraki MDM server

Procedure:

1. Obtain the serial number for each iPad that you want to enrol under Meraki.
2. On Apple School Manager or Apple Busines Manager, select "**Device Assignment**".
3. In section 1 **Choose Devices** select **Serial Number**.
4. Enter each serial number you recorded in step 1, separated by a comma.
5. In section 2 **Choose Action** for P**erform** Action select **Assign to Server**, for **MDM Server** select the name of the Meraki server.
6. Click **Done**.

### 5.2.3 Installing and configuring Apple Configurator 2 on the MacOS Workstation

Procedure:

1. Familiarize yourself with the Apple Configurator 2 documentation and the instructions for how to use Configurator to enrol an iPad under Meraki. We will be performing manual enrolment.
2. Install Configurator 2 on the MacOS workstation.
3. In Configurator 2, open the preferences window.
    a. Create a new Organisation definition using your Device Enrolment Program credentials. You might be asked to authenticate against the Apple service. Follow the prompts to create a new supervision identity. Use the credentials you use to access the Device Enrolment Program.
    b. Create a new Server definition using the URL shown by your Meraki interface[1].
4. In Configurator 2, create a new Profile, with a meaningful name. This profile should contain:
    a. In the General section, make an appropriate choice for the Security and Automatically Remove Profile values. In our case for Security we selected "With Authorization" and added a password. Automatically Remove Profile was set to "Never".
    b. In the WiFi section, add a WiFi payload (configuration) for the WiFi network in which the iPad will be initially configured. It should be set to "Auto Join".
    c. Save the Profile in an appropriate place on the MacOS workstation's file system.

### 5.2.4 Enrolling an iPad device in Meraki

1. Connect the iPad to the MacOS workstation.
2. Select "All Devices" from the Configurator 2 UI. You should see the iPad as a large icon.
3. Select the device you want to enrol and right-click on it. From the options displayed, choose "Prepare" to bring up the "Prepare Devices" window.
4. Select the following options on the window:
    a. Prepare with Manual Configuration.
    b. Select "Add to Device Enrolment Program" but do not select "Activate and complete enrolment".
    c. "Supervise devices" should be active, along with "Allow devices to pair with other computers".
5. Click "Next" to bring up the "Enroll in MDM Server" window.
6. Select the server you specified at step 4(b) above.
7. Click "Next" to move to the "Assign to Organization" window.
8. Select the Organization you created in step 4(a) above.
9. Click "Next" to move to the "Configure iOS Setup Assistant" window.
10. For the "Setup Assistant" field, select "Don't show any of these steps".

[1] From the Meraki web interface, select Systems Manager > Manage > Add Devices > iOS > Apple Configurator > Enrollment URL (AC2+)

11. Click “Next” to move to the “Choose Network Profile” window.
12. Select the profile you created in section 5.2.3, step 4 above.
13. Click “Next” to move to the “Automated Enrolment Credentials” window.
14. In our Meraki installation, we did not need to enter “User Name” or “Password”. To verify if you need to enter Meraki credentials, consult your Meraki web interface and navigate SM > Configure > General.
15. Select the “Prepare” button and follow the instructions. Do not disconnect the iPad until the process is complete.
    It is possible that the iPad you are enrolling was already prepared to a different configuration. In this case you will see a window pop up on the MacOS workstation entitled “Configurator could not perform the requested action because <device name> has already been prepared”. Select the “Erase” button to continue.
16. Follow the instructions on the iPad to complete the procedure. You will have to sign in using an Apple ID.
17. After the iPad contacts Meraki using the local WiFi network, it will appear on the Meraki web interface. Find it by navigating System Manager > Devices.

## 5.3 iPad administration using Meraki

### 5.3.1 Applications

The iPads will be configured to have these applications installed:

- Cisco Webex Meetings
  This program allows the iPads to connect to a ‘Virtual Family Room’.
- Meraki Systems Manager
  This program allows the device to be managed remotely. It is not intended to be invoked by the user.
- WebClip
  This application allows a labelled button to appear on the device that causes a browser on the device to load the internet address of a specific ‘Virtual Family Room’.
- Safari
  This application is a web browser where the user can enter a ‘Virtual Family Room’s internet address to initiate a video call.
- Notes
  This application is provided so that the user can take notes as needed. This application is optional.

### 5.3.2 Network access

The iPads connect to the Cisco Webex server and to the Mobile Device Management system via the internet. The most practical way to do this is by WiFi. Configure the network access carefully, because if the iPads are not able to connect to the internet, then they cannot be used for training and testing purposes, and they cannot be reconfigured with corrected WiFi credentials.

The iPads might be initially provisioned and enrolled onto the Mobile Device Management system on a different WiFi network. The iPads should have credentials for each WiFi network that they might need to access.

### 5.3.3 Mobile Device Management

We used Cisco Meraki as the Mobile Device Management tool. Other comparable MDM systems should work in an analogous way.

iPads can be managed by an MDM solution under two different levels of control, *supervised* and *nonsupervised*. *Supervised* devices are more tightly managed. *Nonsupervised* iPads are more difficult to restrict, and a user could remove the iPad from being under the MDM. We configured the iPads as *supervised*, which requires extra setup steps before connecting the iPads to the MDM system.

When an iPad boots for the first time as a supervised device, it connects to the internet to retrieve its initial configuration. The iPad needs to know how to connect to the internet and where to go for its configuration. This information is contained in a "Profile", which we directly add to each iPad as the first step in the implementation process, using a wired connection between an Apple Mac computer and the iPad.

## 5.4 Configuration in detail

Meraki is a Cisco Mobile Device Management tool that allows remote management of various types of internet-connected device. Each device that Meraki manages has an agent program running on it. The agent contacts a central Meraki server using the internet to request the configuration it should impose. The agent makes this request only when it is running and awake. If the agent cannot communicate with the Meraki server, then no configuration change will occur on the device.

Meraki collects devices into groups based on a set of labels that the user can create and associate with devices. A Meraki user can create device profiles that apply to one or more labels. Each device profile contains one or more settings that are specific to certain aspects of the configuration of a device.

In our system, we created a single label for all of the network environments that the iPads are expected to operate in, as well as separate labels for the iPads' roles. This separation is intended to reduce the likely incidence of accidentally removing the network configuration from the iPads. If this occurred, it would be possible to manually add WiFi credentials to such an iPad to allow it to be used, but this is not ideal.

We created Meraki labels similar to the following (System Manager -> Configure -> Tags):

- *In-hospital-test-device*
    - Applies only to iPad devices that are used as test or demo devices
- *HospitalA*
    - Applies to all iPad devices used in the system.

We created the following Meraki Device Profiles (System Manager -> Manager -> Settings):

- Hospital WiFi
    - Applies to all devices tagged with "*HospitalA"* tag.
    - This profile contained one setting of type "WiFi Settings" – the WiFi credentials to access the network in the hospital.
- Home WiFi
    - Applies to all devices tagged with "*HospitalA"* tag.
    - This profile contained one setting of type "WiFi Settings" – the WiFi credentials to access the network in the location being used to configure the iPads.
- In hospital test / demo
    - Applies to all devices tagged with "*In-hospital-test-device*" tag.
    - This profile contained one setting of type "Restriction "– constraining the device to only allow the applications useful in the test / demo role.
    - For the **Show or hide apps** field we selected **Only allow the following apps**
    - Using the drop-down list, we added the apps **Cisco Webex Meetings**, **Meraki Systems Manager**, **Notes**, **Web Clips** and **Safari.**
- Lock Screen
    - Applies to all devices tagged with "*HospitalA*" tag.
    - One setting of type "Wallpaper".
    - This profile imposes a lock screen graphic tying the device to the Hospital.
- Webex Link Icons
    - Applies to all devices tagged with "*In-hospital-test-device*" tag.
    - This profile contains a number of WebClip settings that put icons on the iPad home page. Each icon corresponds to a Webex account per 'Virtual Family Room'.
    - Each Web Clip setting contains a label for the 'Virtual Family Room' in question, a URL for the corresponding Webex account, and an icon file.
    - The icon file was created with a web tool that creates images from text. The image was designed to legibly show the name of the 'Virtual Family Room' to the iPad user.

## 5.5 Settings that can only be made on the iPads directly

### 5.5.1 Safari/Webex bug workaround

In iOS 13.5 and onwards, when you use Safari to open a link to a Webex meeting room, the Webex app does not open the meeting room. To solve this problem, change the Safari settings from Desktop Mode to Mobile Mode:

1. Open **Settings**, then tap **Safari**.
2. Under **Settings For Website**s, select **Request Desktop Website**.
3. Disable the **All Websites** setting.

### 5.5.2 Webex Meetings application configuration

The test iPad devices are used to mimic the devices used by family members. Use the "Detailed Setup for Family" instructions to set up and test the Webex Meetings software.

## 5.6 Testing

Verify that each test iPad can communicate with each 'Virtual Family Room'. You can simultaneously connect multiple iPads to a specific 'Virtual Family Room' meeting. If possible, the 'Virtual Family Room' should be hosted via a DX device, but this is not strictly necessary.

Procedure:

Repeat the following steps for each 'Virtual Family Room':

1. As described in the "ICUFL—Staff—CiscoDX—Usage Instructions" document, use the DX device to host a meeting for the 'Virtual Family Room'.
2. On each iPad:
    a. Tap the icon that corresponds to the 'Virtual Family Room'.
    b. The corresponding Webex meeting room link opens in a Safari browser window.
    c. When prompted to **Open this page in "Webex Meet"?**, tap **Open**.
    d. The Webex Meetings app starts and prompts you to enter a display name (the name of the 'Family member' participating in the call) and email address.
    e. From this point onwards, the Webex Meetings app will use these credentials when it connects to subsequent Webex Meetings. These credentials can be changed when a meeting is not running, by tapping on the cog icon on the top left of the Webex Meetings display, and then selecting the pen icon to the right of the account information.
    f. Tap **Join**.

# 6 Appendices

## 6.1 Credits

- Icons made by Pixelmeetup ,Freepik from www.flaticon.com