ICUFL—Tech—Core—Cisco Webex

Author: Irial Conroy, Brian O'Donoghue

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

Version 1.0
June 8th 2020

1 Intent

This document details how to implement the core 'ICU FamilyLink' system using Cisco Webex Meetings and Cisco DX endpoints.

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 Table of Figures

4 Implementation based on Cisco Webex

This section outlines the specific technical implementation at University Hospital Galway (UHG) in Ireland, which uses Cisco Webex Meetings and Cisco DX video endpoint devices as the base technologies.

4.1 System Architecture
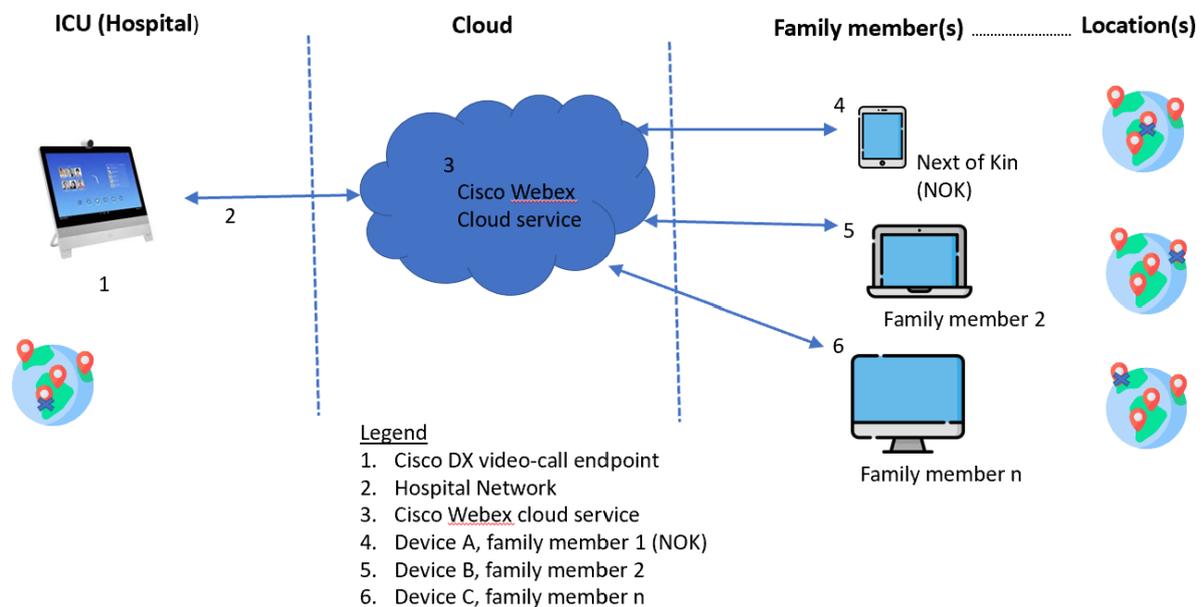
The high-level system architecture is shown in Figure 1.

Figure 1: System Architecture

4.2   System Concepts

Each ICU (Intensive Care Unit) patient area or room covered by the solution is assigned a separate 'virtual conference room' (as a shorthand, let's refer to this as a *'Virtual Family Room'*). Each Virtual Family Room has a specific URL.

Family members who attempt to join a video call will remain in a *'Virtual Waiting Room'* until the staff member leading the call admits them to the video call.

The logical system flow is outlined in the document: 'ICUFL—Logical Architecture'.

The system concepts map to Cisco technical components, as follows:

- 'Virtual Family Room' functionality is provided via Cisco Webex Personal Meeting Rooms:
    - Each distinct 'Virtual Family Room' requires a separate Cisco Webex Personal Meeting Room.
    - The system designer must assess how many 'Virtual Family Room(s)' are required; for example, one per patient area, one per physical room, or other allocation. This in turn determines how many Cisco Webex Personal Meeting Rooms are required for the system.
- 'Virtual Waiting Room' functionality is provided by the Cisco Webex Personal Meeting Room.
- Video endpoint(s) are implemented using a Cisco DX video endpoint.

Subsequent sections provide more detail on each system component.

4.3   System Components

4.3.1   Cisco Webex Meetings

Cisco Webex Meetings is a cloud-based video-conferencing solution that can be joined via desktop, mobile, browser and standards-based IP video devices (see further details at https://www.webex.com/).

For 'ICU FamilyLink' at UHG, Cisco Webex Meetings was customized in several ways (see 4.4).

4.3.2   Cisco Webex Personal Meeting Rooms

Cisco Webex Personal Meetings Rooms is a secure, always-on virtual meeting room mode for a Cisco Webex user. It essentially means that a Cisco Webex meeting does not need to be scheduled in the

Webex or Microsoft Outlook calendar, because it is always available and ready to host a meeting. A Cisco Webex Personal Meeting Room (PMR) allows Cisco DX video endpoints to call into Cisco Webex meetings and take on the Host privileges to control the meeting experience.

See further details at https://www.cisco.com/c/en/us/solutions/collaboration/pervasive-conferencing/index.html.

4.3.3   Cisco DX

Cisco DX is high-quality video-conferencing endpoint, with touchscreen operation (see further details at https://www.cisco.com/c/en/us/products/collaboration-endpoints/dx80/index.html).

For the UHG 'ICU FamilyLink' project, we used two models of DX: DX80 & DX70.

Figure 2 shows a generic DX, highlighting the controls.

Front View and the Home Screen

❶ Camera with privacy shutter, turn counter-clockwise to shut and clockwise to open

❷ Microphone mute button, loudspeaker volume controls and USB socket on the right side of the unit.

❸ Power On/Off

❹ Loudspeaker

❺ Microphone in each leg. As default, the microphones are set in *Focused* mode. This mode suppresses extraneous noise without affecting your voice.

Figure 2: Generic Cisco DX - controls

Figure 3 shows a Cisco DX80, with an example of a customised menu.

Figure 3: Cisco DX with customized menu

4.4 System Configuration and Customisation

4.4.1 Cisco Webex Account setup

The setup flow for Cisco Webex Accounts is outlined in Figure 4. All Cisco Webex administration (Site, DX Endpoint and User accounts) is done using the Cisco Webex Control Hub (accessible via https://www.webex.com).

Email Account Setup
- Unque hospital Email A/C per 'Virtual Family Room'

Cisco Webex Account setup
- Email A/C is a pre-req
- Webex A/C per 'Virtual Family Room' required

Cisco Webex Account customisation
- Rooms locked on startup
- Record & Share disabled
- etc.

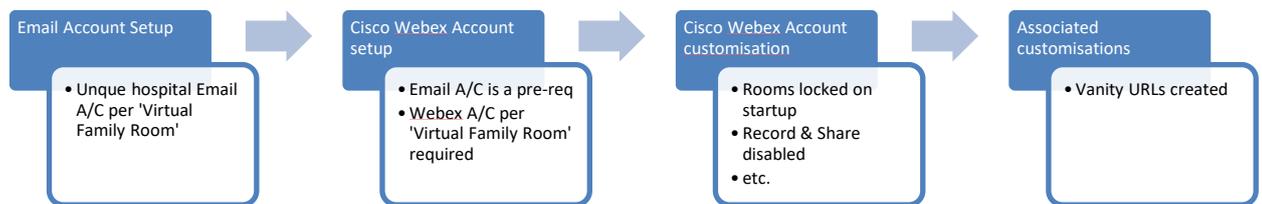**Associated customisations**
- Vanity URLs created

Figure 4: Cisco Account setup overview

Notes:

- Email accounts are set up via the Hospital Email system. These are linked to each Webex Personal Meeting Room (one email account per Webex Personal Meeting Room)
- Vanity URLs (such as http://cs.co/icu-101) are short URLs that are easy to remember and type. These URLs make it easier for family members to access the Personal Meeting Rooms, when they type the URL into a browser (for example, instead of typing https://hostA.webex.com/meet/icu-101). If you want to shorten the Webex URLs, you should pick a preferred URL shortening service (the cs.co URL shortener tool might only be available to certain individuals, such as Cisco employees and partners).

4.4.2 Cisco Webex Account customisation

Webex Account customisations are applied at two levels:

i.   Cisco Webex Site: Applied by Cisco Webex site administrator (via http://admin.webex.com)

ii. Cisco Webex Meetings Personal Meeting Room (PMR): Applied by Cisco Webex PMR account owner (via http://www.webex.com)

Level	Property/Setting	Modify To	Notes
Cisco Webex Site	Recording	Disabled	Applied to applicable Webex Accounts on the site
	Email Address (for attendees)	Optional	This means that family members don't need to enter an email address to attend the video call
	Share	Disabled	
	Chat	Disabled	
	End Meeting once Host leaves	Enabled	
	Encryption for voice & video in transit	Enabled	
Cisco Webex Meetings PMR	My Personal Room: 'Personal Room Name'	Modify so that it reflects the 'Virtual Family Room' name that you want family members to see in the 'Virtual Waiting Room'	Example: Change 'XXX ICU-101 Personal Room' to 'ICU-101'
	My Personal Room: 'Personal Room Link'	Modify so that the last section of the URL solely reflects the 'Virtual Family Room' name (without extraneous prefix)	Example: Change https://hostA.webex.com/meet/*ZZZ*.icu-101 to https://hostA.webex.com/meet/icu-101
	My Personal Room: Automatic Lock	Enable (that is, selected) [0 minutes after meeting starts]	Ensures that each family member must be admitted to the video-call by ICU staff
	'My Personal Room': Alternate Host	Disable (that is, not selected)	
	'My Personal Room': Host PIN	<see note>	Host PINs provide an additional layer of security, whilst offering device flexibility. The JavaScript macro (on the DX – see 4.4.3) has a variable that enters the Host PIN, to streamline the start experience on the DX.

Figure 5 Cisco Webex Account/PMR

4.4.3 Cisco DX customisation and configuration

4.4.3.1 Cisco DX customisation

Custom Menus

A custom menu is developed for each Cisco DX.

The menu covers a discrete set of 'Virtual Family Rooms'. The exact set of 'Virtual Family Rooms' per DX is based on several local factors, including (but not limited to): overall number of 'Virtual Family Rooms' (see 4.2), number of DXs being deployed, etc.

The custom menu is implemented via a combination of a JavaScript web dial application macro and an XML-based touch screen menu.

JavaScript web dial macros application menu

- It leverages the following API:
  https://www.cisco.com/c/dam/en/us/td/docs/telepresence/endpoint/ce82/dx70-dx80-api-reference-guide-ce82.pdf
- The JavaScript web dial application menu is uploaded to the DX via
  https://<DX_ip_address>/web/macros (you will require administrator access to the DX to upload the file)

XML-based DX80 UI Menu

- The XML file is created for the UI menu layout, and invokes the JavaScript file, and is uploaded to the DX also.
- Browse to https://<DX_ip_address>/web/roomcontrol to upload the XML file (you will require administrator access to the DX to upload the file).

Note: Both files must be uploaded from a PC that is on the same network as the DX devices.

Samples of both files are hosted at this location:

https://github.com/CiscoDevNet/xapi-samples/tree/master/controls/family_link

Example DX menus
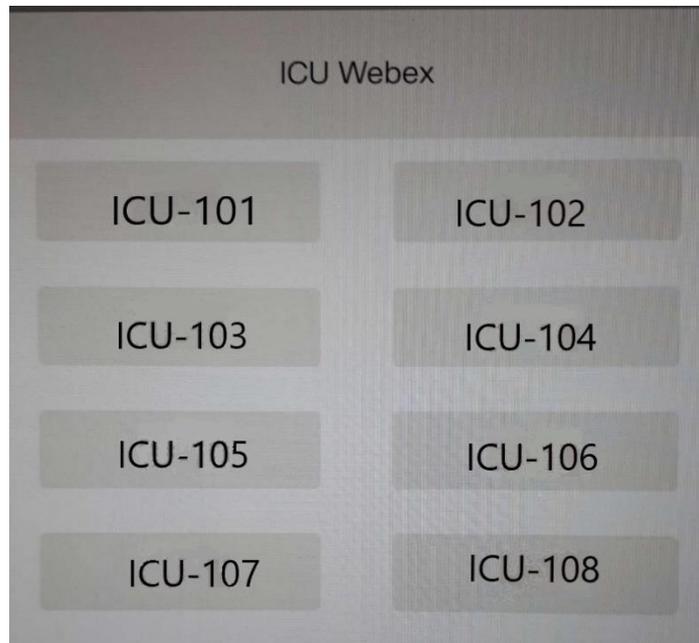
- o DX-A: Menu with ICU-101, ICU-102…ICU-108

Figure 6: Customized menu on DX-A

- o DX-B: Menu with ICU-201, ICU-202…ICU-208
- o etc.

Custom Dial Icon

- A new button is added via Macros.
- Its name is set to 'Join Webex'.
- This button is configured to bring up the menu of 'Virtual Family Room's when clicked.

4.4.3.2   Other Cisco DX configuration

Setting	Set To	Reference link / Notes
Ultrasound Pairing (Intelligent Proximity/Proximity Ultrasound)	0 (that is, Disabled)	https://www.cisco.com/c/en/us/products/collaboration-endpoints/intelligent-proximity.html
Default Feature Icons	Remove	(Call | Whiteboard | Join Webex)
Video Layout	'Equal'	
Self-view	On | Top Right	

Settings Menu	Locked	Lock the Settings menu so that the configuration is not accidentally changed

4.5 Other Technical aspects

4.5.1 Networking

Ethernet

Links to Cisco firewall requirements:

https://help.webex.com/en-us/WBX264/How-Do-I-Allow-Webex-Meetings-Traffic-on-My-Network

https://help.webex.com/en-us/WBX000028782/Network-Requirements-for-Webex-Teams-Services

Bandwidth planning for Webex

https://www.cisco.com/c/en/us/products/collateral/conferencing/webex-meetings/white_paper_c11-691351.html

Wifi as backup

While Wifi might result in good video calls, we recommend to hard-wire the DX units where possible, as there is less likelihood for service disruption. We do not recommend connecting the DX to a guest Wifi network that has web-portal sign-on, and limited duration per session. At a minimum, you should connect the DX to a Wifi network that supports WPA2 PSK.

4.5.2 Security

For the latest Cisco Webex security information, see www.cisco.com.

A current snapshot of Cisco Webex security posture is:

- In addition to complying with stringent internal standards, Cisco Webex also continually maintains third-party validations to demonstrate our commitment to information security. Cisco Webex is:
  - ISO 27001 certified
  - Service Organization Controls (SOC) 2 Type II audited
  - FedRAMP certified
  - Cloud Computing Compliance Controls Catalogue (C5) attestation
  - Privacy Shield Framework certified

- Webex Security Whitepaper:
  https://www.cisco.com/c/dam/en/us/products/collateral/conferencing/webex-meeting-center/white-paper-c11-737588.pdf

5 Appendices

5.1 Credits

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