UCi2i Video Conference Endpoint Firewall Requirements

Confidentiality Statement and Copyright Notice

This document is published as "Public" and may be freely distributed.

Version Control

Date	Version	Changes	Authorised
28th November 2011	0.1	Draft for review	TK
3rd March 2012	1.0	Released version	TK
6th August 2013	1.1	Brand updates	TK
29th January 2015	2.0	Addition of WebRTC/Brower-based calling	TK
9th February 2015	2.1	Additional IP's added	TK
16th December 2015	2.2	Changed V-Desk support number (UK)	TK
8th December 2016	2.3	Additional IP's for China service added	TK
5th May 2017	2.4	USA Conference node added	TK
7th September 2017	2.5	Updated to suit Support Help Centre	TK
6th July 2018	2.6	Added Google Hangouts information and new graphics	TK
7th September 2018	2.7	Updated USA node IP address	TK
21st November 2019	2.8	Updated with Pinnaca infrastructure IPs	TK

Contents

UCi2i VC Endpoint Firewall Requirements

Due to the implementation of our secure video network, there are a few firewall rules that may be required depending on your network configuration to allow communication with the UCi2i infrastructure. This is to provide our clients with the best technology on the market.

What this means to you

In order for you and your client to take full advantage of our service, we **MAY** require you to make some changes to your firewall to allow communication from your current hardware/software to our Firewall Traversal Servers. Please note that many firewalls work without any modification at all.

If you wish to test your firewall before deploying our managed video service, then call test@dial.vc (more instructions here). and you'll be prompted to speak "1…2…3" and this recording will loop back to you. If you can see and hear this then you're good to go.

What addresses and ports does video conferencing use?

Please see below firewall port requirements. In order to provide resiliency, we will require you to open ports to multiple addresses.

UCi2i address ranges

North America

38.117.72.0/24

185.135.210.0/24

United Kingdom

212.46.142.0/24

185.135.208.0/24

91.244.117.0/24

Hong Kong

64.138.14.224/27

91.233.183.0/24

Note: We provide ranges rather than specific IPs as we may dynamically increase or decrease the size of the video infrastructure estate.

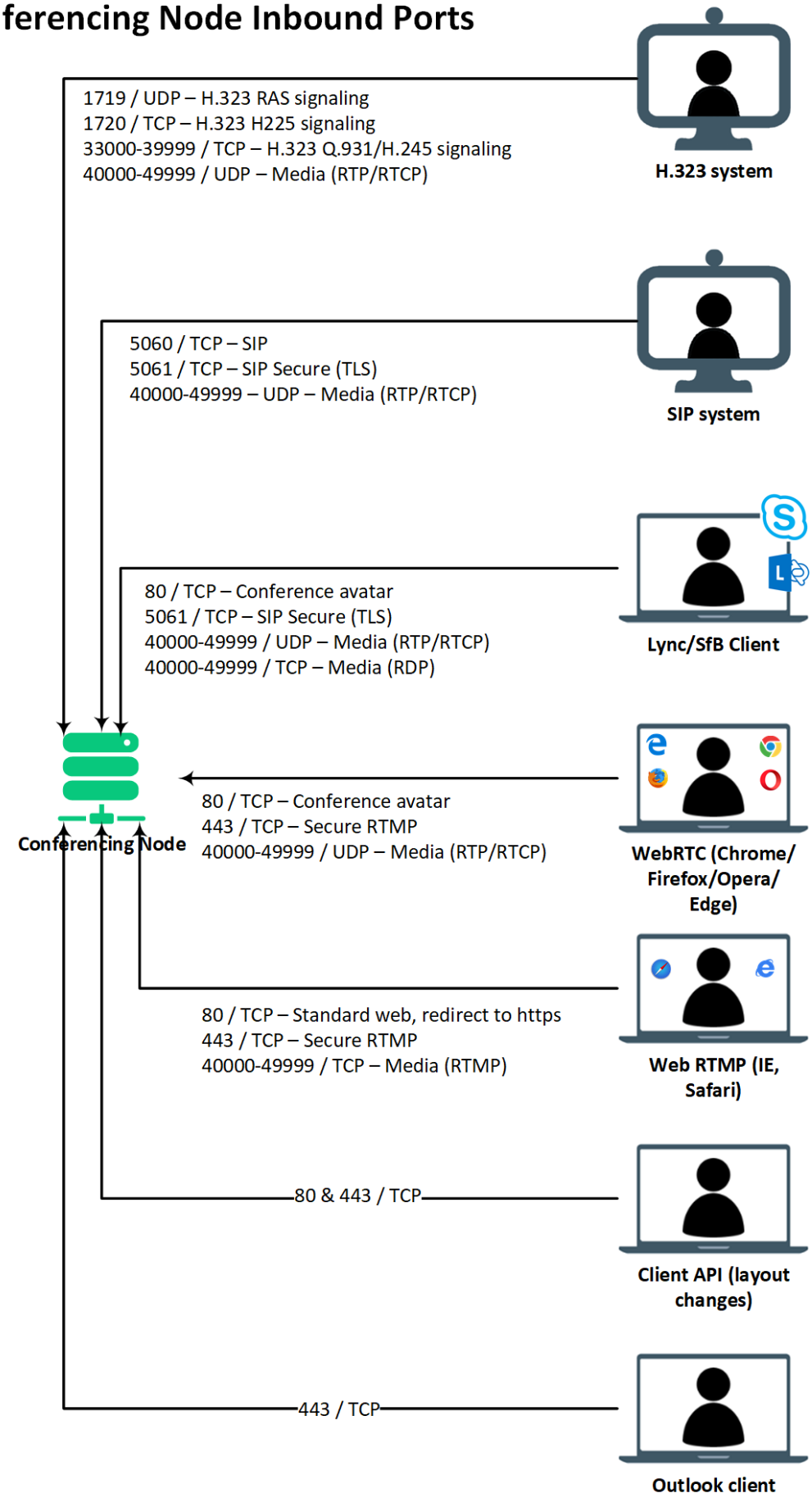
Complete Firewall Port List

To enable the UCi2i service a complete list of the ports required is below. Should, you require information on the individual protocol requirements then please see the next section for a breakdown of services.

Inbound (to UCi2i)

Protocol	Source-Port	Dest-Port	Description	Device
TCP	<any>	80	HTTP	Web browser / API interface / Skype for Business / Lync system (for conference avatar)
TCP	<any>	443	HTTPS	Web browser/ API interface / VC-Connect mobile client / Outlook client/add-in (VMR scheduling)
TCP	<any>	1720	H.323 (H.225 signaling)	Endpoint / call control system
TCP/UDP	<any>	5060	SIP	Endpoint / call control system
TCP	<any>	5061	SIP/TLS	Endpoint / call control system
TCP	<any>	33000-39999	H.323 (Q.931/H.245 signaling)	Endpoint / call control system
TCP/UDP	<any>	40000-49999	RTP / RTCP / RDP / VbSS / DTLS / RTMP / STUN / TURN	Endpoint / call control system / Skype for Business / Lync system / VC-Connect
UDP	<any>	1719	H.323 (RAS signaling)	Endpoint / call control system

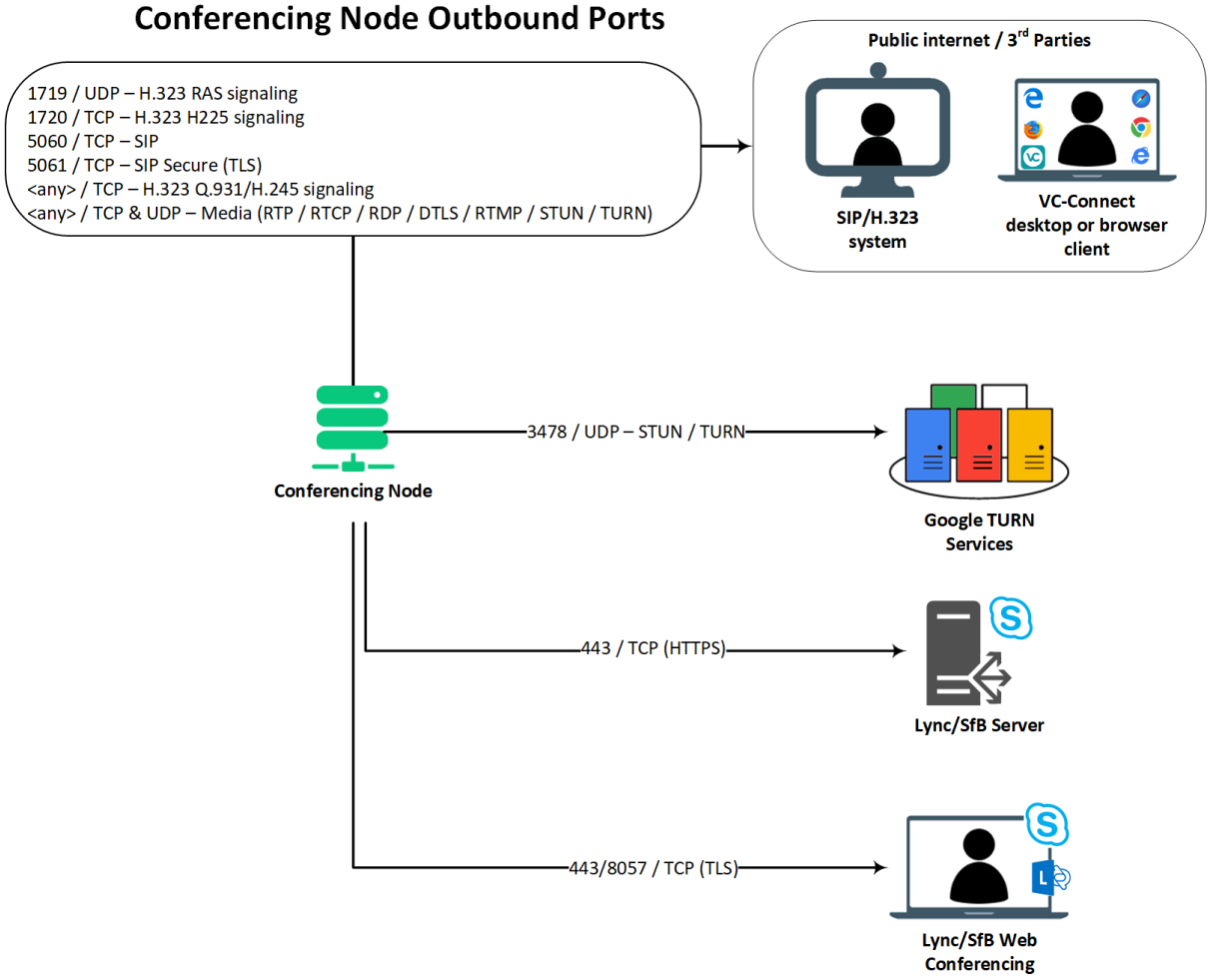
Conferencing Node Inbound Ports



Outbound (from UCi2i)

Protocol	Source-Port	Dest-Port	Description	Device
TCP	33000-39999	1720	H.323 (H.225 signaling)	Endpoint / call control system
TCP/UDP	33000-39999	5060	SIP	Endpoint / call control system
TCP	33000-39999	5061	SIP/TLS	Endpoint / call control system
TCP	33000-39999	<any>	H.323 (Q.931/H.245 signaling)	Endpoint / call control system
TCP/UDP	40000-49999	<any>	RTP / RTCP / RDP / VbSS / DTLS / RTMP / STUN / TURN	Endpoint / call control system / Skype for Business / Lync system / Infinity Connect
TCP	40000-49999	1935	RTMP	RTMP streaming server
UDP	40000-49999	19302-19309	SRTP	Google Hangouts Meet
TCP (TLS)	55000-65535	443/8057	PSOM (PowerPoint presentation from SfB/Lync)	SfB/Lync Web Conferencing service
TCP (TLS)	55000–65535	443	HTTPS (PowerPoint presentation from SfB/Lync)	SfB/Lync Front End Server or Edge Server and WAC/OWA/OOS server
UDP	33000-39999	1719	H.323 (RAS signaling)	Endpoint / call control system
UDP	40000-49999	3478	STUN / TURN	STUN / TURN server

Conferencing Node Outbound Ports



Defined Services Firewall List

SIP Proxies

Please ensure that the correct ports are open depending on the video conferencing system you are using. There are different port requirements for SIP depending on what signalling method your system is using. The media requirements are the same regardless of the signalling method. Note these outbound exceptions are required to establish a UDP/TCP session. There are absolutely no inbound pinholes required.

Function	Port (s)	Type	Direction
SIP Signalling(TLS)	5061	TCP	Host ----> UCi2i
SIP Signalling(TCP)	5060	TCP	Host ----> UCi2i
SIP Signalling(UDP)	5060	UDP	Host ----> UCi2i
Media (RTP)	2776	UDP	Host ----> UCi2i
Media (RTCP)	2777	UDP	Host ----> UCi2i
Media	40000 - 54999	UDP	Host ----> UCi2i

H323: Using Assent Firewall Traversal

If your video conference system supports Assent traversal, you **MAY** need to open the ports below in order to register to our firewall traversal server.

Function	Port (s)	Type	Direction
Gatekeeper RAS	1719	UDP	Host ----> UCi2i
Call Signalling	2776	TCP	Host ----> UCi2i
Media (RTP)	2776	UDP	Host ----> UCi2i
Media (RTCP)	2777	UDP	Host ----> UCi2i
Q931/H245 Signalling	33000-39999	TCP	Host ----> UCi2i
Media	40000 - 54999	UDP	Host ----> UCi2i

H323: Using H.460.18/19 Firewall Traversal (used by all Polycom/Lifesize devices)

If your video conference system is not a Cisco Telepresence device and supports H.460.18/19 firewall traversal, you will need to open the ports below in order to register to our firewall traversal server.

Function	Port (s)	Type	Direction
Gatekeeper RAS	1719	UDP	Host ----> UCi2i
H.225 Protocol	1720	TCP	Host ----> UCi2i
H.245 Protocol	2777	TCP	Host ----> UCi2i
Q931/H245 Signalling	33000-39999	TCP	Host ----> UCi2i
Media (RTP)	2776	UDP	Host ----> UCi2i
Media (RTCP)	2777	UDP	Host ----> UCi2i
Media	40000-54999	UDP	Host ----> UCi2i

Browser-based Video Calling (a.k.a. WebRTC)

We offer browser-based video calling - all major browsers are supported. This is typically known as WebRTC but we offer more than that as WebRTC is limited to Google Chrome, Firefox and Opera. We also provide service to any browser that also supports Adobe Flash. To allow this feature to work, the following ports will need to be opened:

Function	Port (s)	Type	Direction
STUN/TURN Media	3478	UDP	Host ----> UCi2i
Media	40000-49999	TCP	Host ----> UCi2i
Media	40000-49999	UDP	Host ----> UCi2i
HTTP	80	TCP	Host ----> UCi2i
HTTPS	443	TCP	Host ----> UCi2i

Key

Please see below explanations of the direction column (where applicable):

Direction	Explanation
Host <----> UCi2i	Ports needs to be opened inbound and outbound to/from your VC endpoint and UCi2i
Host <---- UCi2i	Ports need to be opened inbound to your VC endpoint from the UCi2i address ranges
Host ----> UCi2i	Ports need to be opened outbound from your VC endpoint to the UCi2i address ranges
UCi2i ----> Host	Ports need to be opened inbound to your VC endpoint from the UCi2i address ranges

Finally, if you have any problems, please feel free to contact our support team via one of the follow methods:

Email Address: support@uci2i.com
Video Address: support@uci2i.com
Support Help Centre: https://support.uci2i.com/hc
Telephone: +442038418555 (EMEA) or +852 2281 5300 (APAC)

APAC

t: +852 3008 4422
v/e: support@uci2i.com

21/F, Wyler Centre Phase II
192-200 Tai Lin Pai Road
Kwai Chung, N.T, Hong Kong

EMEA

t: +44 203 841 8555
v/e: support@uci2i.com

Unit 1-3 The Bell Centre
Newton Road
Crawley, RH10 9FZ