

## Firewall requirements for Vscene 2.x

For standards-based video conferencing using H.323/SIP endpoints, VsceneRoom systems and WebRTC for web-based conferencing.

Component	Name	Application	IP	TCP ports	UDP Ports*
H.323 Calling	H.323/SIP Gateway	H.323 Call Signalling, Setup and Media	195.195.245.128/26	1719 to 65535 (Bi-directional)	1719 to 65535 (Bi-directional)
SIP Calling	H.323/SIP Gateway	SIP / Secure SIP signalling	195.195.245.128/26	5060 & 5061 (Bi-directional)	50000-65535 (Bi-directional)
H.323 / SIP Device Registration	H.323 Gatekeepers & SIP Registrar	Endpoint Registration & GK Neighbouring	194.80.134.34 (Primary GK) 194.80.134.35 (Secondary GK) 194.80.134.50 (SIP Registrar)	1719 & 1720 (H.323) 5060 & 5061 (SIP) (All Bi-directional)	1719-65535 (H.323) 50000-65535 (SIP) (All Bi-directional)
VsceneRoom Registration & Calling	VsceneRoom Registrar	Endpoint Registration and Media	212.219.85.131 to 212.219.85.141	80, 443, 17990 to 17992 (Outbound)	50000 to 65535 (Outbound)
WebRTC	WebRTC Cluster	Call Setup, Signalling and Media	195.195.245.128/26	80 & 443, 40000 to 49999 (Outbound)	3478 40000 to 49999 (Outbound)
WebRTC	STUN/TURN Server	Firewall Traversal (optional)	212.219.85.233	3478 (Outbound)	3478 (Outbound)

\* It is also recommended that any firewall UDP time-out is extended to a suitable length to enable conferencing sessions to continue uninterrupted. E.g. 2 or 4 hours, but longer may be required, based on your organisations usage.

If web proxies or DNS filtering are being used on your network, please add the following exceptions: - \*.vscene.net \*.jvcs.ja.net & \*.jisc.ac.uk

If you will be using Skype for Business with Vscene, please whitelist the domain 'vscene.net' in your organisational control panel for Office365.