

## Firewall requirements for Vscene 2.x

For standards-based video conferencing using Vscene web-based communication, V-Room Systems and H.323/SIP endpoints.

Component	Name	Application	IP	TCP Ports	UDP Ports
H.323 Calling	H.323/SIP Gateway	H.323 Call Signalling, Setup and Media	212.219.85.150 to 212.219.85.177	1719 to 65535 (Bi-directional)	1719 to 65535 (Bi-directional)
SIP Calling	H.323/SIP Gateway	SIP / Secure SIP Signalling	212.219.85.150 to 212.219.85.177	5060 & 5061 (Bi-directional)	50000 to 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)
V-Room Registration & Calling	V-Room Registrar	Endpoint Registration and Media	212.219.85.128/25 46.249.221.4 - 46.249.221.13 46.249.221.132 - 46.249.221.141	80, 443, 17990 to 17992 (Outbound)	50000 to 65535 (Outbound)
WebRTC – Native	Native WebRTC Pool	Media & Client Signalling	212.219.85.128/25 46.249.221.4 - 46.249.221.13 46.249.221.132 - 46.249.221.141	443, 17990 (Outbound)	50000 to 65535 (Outbound)
WebRTC – Native	Native WebRTC Pool	TURN & WebSocket Signalling	212.219.85.128/25 46.249.221.14 - 46.249.221.33 46.249.221.142 - 46.249.221.161	443 (Outbound)	n/a

\* Any firewall UDP time-out should be 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 organisation's usage.

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

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