

Firewall Requirements



For standards-based video conferencing using Vscene desktop & web-based communication, room systems and H.323/SIP endpoints.

Support desk: Telephone: +44 (0) 330 020 0404

E-mail: support@vscene.net

Component	Name	Application	Destination	TCP Ports	UDP Ports
Vscene Web, Desktop & Room- Based Client Registration & Calling	Vscene Registrar & Call Routing Pools	Endpoint Registration, Media & Client Signalling	*vscene.net *jvcs.ja.net 212.219.85.128/25 46.249.221.0/25 46.249.221.128/25	443, 17990 to 17992 (Outbound)	50000 to 65535 (Outbound)
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)

PLEASE NOTE:

*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 & *jvcs.ja.net.**

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

*The Vscene web client uses WebSockets to maintain communication between the user's web browser and the call routing pool, so if you are blocking this type of traffic, please allow it through to the ranges specified in the table above.