xtendx®
corporate media solutions

simplex Meeting

Firewall Requirements

xtendx AG | Adlikerstrasse 246, CH-8105 Regensdorf
t +41 43 299 92 92 **e** support@xtendx.com **w** www.xtendx.com

20.07.2020

Index

1 Introduction

simplex Meeting leverages the official WebRTC standard for its audio and video conferencing solution. To conduct successful audio and video conferences, certain minimal requirements need to be covered by a corporate firewall.

1.1 Web server (WEB)

IP: ***46.231.206.225***

Normally HTTP traffic is not blocked by firewalls. Certain high-risk verticals prevent documents upload. To allow documents sharing in simplex meeting, documents upload must be allowed.

1.2 STUN/TURN (ICE)

IP: **46.231.206.8** & **46.231.206.9**

STUN and TURN are technologies used to establish peer-to-peer connections between participants. These types of connections are used in standard meeting room types.

1.3 Video Bridge (VB)

IP: **94.126.19.216**

The video bridge is used for Boardroom, Classroom and Dial-in Meeting rooms. The browser will communicate with the video bridge through HTTP and will also establish an SRTP session to send and receive media.

2 Firewall rules

Webinars only	P2P full	Server	Ports	Protocol*
✓	✓	WEB & VB	443	TCP
✓	✓	VB	32768-MAX*	TCP/UDP
	✓	ICE	32768-MAX*	TCP/UDP
	✓	ICE	443	TCP/UDP
	✓	ICE & VB	3478-3479	TCP/UDP

2.1 [Protocol*]

Unfiltered / no DPI: The STUN protocol is different to the HTTP protocol that usually uses the ports 80 and 443. That is why technologies such as DPI might prevent STUN protocol traffic to these ports.

2.2 [MAX*]

The upper port limit is the sum of the beginning port and the maximum expected concurrent participants. simplex meeting skips ports already in use by other applications.

For Webinars only, an upper port limit of at least 33068 is recommended.

For p2p meetings, an upper port limit of 65535 is recommended.