



Firewall & Filtering Setup

Network endpoints and ports teamSOS needs to reach

For teamSOS to work reliably, your network and web filtering must allow access to the endpoints below. **These requirements apply to both teamSOS Lockdown and teamSOS Enterprise.**

REQUIRED · HTTP and HTTPS

The teamSOS app requires the following websites to be accessible via HTTPS. We recommend also allowing HTTP for end-user convenience — any HTTP requests we receive are always redirected to HTTPS.

- <https://www.teamsos.co.uk/>
- <https://app.teamsos.co.uk/>
- <https://auth.teamsos.co.uk/>
- <https://api.teamsos.co.uk/>
- <https://portal.teamsos.co.uk/>
- <https://tsoslive.blob.core.windows.net/>
- <https://tsospubliclive.blob.core.windows.net/>
- <https://live-teamsos.service.signalr.net>

MOBILE · Realtime Audio Streaming

Mobile devices need at least one of the following destination UDP ports allowed outbound, with response traffic allowed back to the device:

- 3478/udp
- 8801/udp
- 3479/udp
- 8802/udp
- 5060/udp
- 19302/udp
- 5061/udp
- 19303/udp

teamSOS uses ports common to multiple conferencing services to transmit real-time audio. If you need the full list of ports for security or audit reasons, email help@teamsos.co.uk. To whitelist at IP level (all inbound/outbound UDP), use our real-time audio gateway IP address:

51.140.179.28

Note: teamSOS Web does not use these ports.

USUALLY OK · **WebSocket (via HTTPS)**

This is usually enabled by default on good firewall and filtering products, but can be affected by things like deep packet inspection. It's included here for completeness — only worry about it if teamSOS isn't keeping up to date with new messages while the app is open, or you're stuck connecting after logging in. The hostnames using WebSocket are:

- <https://api.teamsos.co.uk/>
- <https://teamsos.service.signalr.net/>

USUALLY OK · **Push Notification Gateways**

Usually enabled by default in most environments and included here for completeness — only relevant if apps aren't keeping up to date with new messages while closed. These services are operated by Apple, Google and Microsoft and are likely already permitted on your network.

Remember: teamSOS Web does not support offline notifications — it only produces notifications while the web page is open.

Provider reference documentation:

- Apple — support.apple.com/en-gb/HT203609
- Google (Android) — firebase.google.com/docs/cloud-messaging
- Microsoft — [learn.microsoft.com ... firewall-allowlist-config](https://learn.microsoft.com.../firewall-allowlist-config)

IF USING · **Microsoft Entra & Intune**

If you use Entra (Azure AD) sync or SSO for your users, or deploy the Desktop Alerts client via Microsoft Intune, your network must also be able to reach the standard Microsoft 365, Entra and Intune service endpoints. These are typically already allowed on school networks. For the current consolidated list, contact help@teamsos.co.uk.

Need help?

If you encounter any issues, please contact help@teamsos.co.uk