Newline Cast Technical Overview

Meeting ID and PIN

For each meeting, a unique meeting ID is generated mediated from an SaaS layer, which is used as a means for the clients to connect to that specific meeting. If there is an Internet connection, this meeting ID will be 6 digits long. If no Internet is available (or if 'force local meetings' is checked in settings) the Meeting ID will be 10 digits long. This 10 digit meeting ID is generated using the device's IP address, which enables connection from different subnets on the same network.

If devices connect using the 6 digit meeting ID, connection is attempted locally, however if this is not possible then the connection is made via XMPP.

Cloud Access

If Newline Cast has access to the Cloud, then it will be able to allow devices connecting to it from outside of its local network – e.g. A Chromebook client on a remote network and a Windows client connected on another network within your organization, with voice and video available if those devices are connected using Newline Cast or the Newline Cast Windows Software. This can be restricted by deactivating access to the cloud in Newline Cast's settings.

Updating Newline Cast

An Internet connection is required for updates. The updates are downloaded over a secure connection (using port 443) and are installed on demand. A notification will appear in the user interface to indicate an available update that the user can install. Updates can also be installed via USB drive connected to Newline Cast if Internet cannot be made available.

Security

The clients and boxes are authenticated on our servers using a 4-step authentication process with SASL. At any time, administrators can remove a client or box from the authorized zone temporarily and permanently.

All data transferred between the user's device and Newline Cast is peer to peer (P2P) and is over TLS or DTLS with 2048-bit asymmetric encryption and 256-bit symmetric encryption. If a P2P connection fails to connect between the client and Newline Cast, then the software will relay the data via our TURN server over TLS TCP port 443.

Newline Cast Technical Overview

Firewall & Proxy

Firewall

For remote connections, receiver and clients need to be able to access the Internet through these ports:

- TCP 80
- TCP 443
- UDP 53

For local connections (i.e. clients on the same network or connecting through an Access Point) the following ports are used:

- TCP 1-65535 (It will be selected from available ones)
- UDP 1025 – 65535
- TCP 4700, 7000, 7100 (For Airplay connections)

If there is Layer 7 filtering or proxy with protocol filtering on these ports then the following protocols will need to be allowed:

- HTTP
- HTTPS
- DTLS
- XMPP
- Bonjour protocols
- SRTP
- DNS
- STUN
- TURN
- ICE

Our SaaS provides services at the following FQDNs:

- netcheck.joinmontage.com
- montage.displaynote.com
- xmpp.displaynote.com
- stunturn-prod-ireland.displaynote.com
- stunturn-prod-mumbai.displaynote.com
- stunturn-prod-singapore.displaynote.com
- stunturn-prod-virginia.displaynote.com
- stunturn-prod-california.displaynote.com

Proxy Support

The Montage Linux box and Windows software support proxy configuration. The following proxy types are supported:

- HTTP Proxy (with or without authentication)
- SOCKS 5 (with or without authentication)
- Proxy with Auto-Configuration File (PAC) (with or without authentication)
- System proxy - to inherit proxy settings from Windows

Contact Us

Still need additional assistance?
Contact our Technical Support Team via info_ap@newline-interactive.com.