Advanced Networking + Security

Advanced Networking

If your users will be using a firewall that blocks traffic except from whitelisted IP’s/ports, please contact us at sdk@zello.com to obtain a copy of our IP address list.

Security

For more information, please see Zello | Technical and Organizational Security Measures

Voice and rich media data transits the public internet encrypted by 256 bit AES, passing from sender device to receiver device through Zello servers. Under no circumstances do we store this data, EXCEPT:

- When Message Vault is enabled by the customer, in which case encrypted data will be saved—along with the original client key—for up to 2 years
- When a voice message is a direct 1:1 communication and the recipient is offline, in which case the encrypted data will be stored for redelivery for up to 7 days. Once redelivered, the data is deleted

Voice and rich media data will be stored on the recipient device UNLESS:

- It is prevented by configuration
- It is automatically deleted by policy (expiration time)
- It is manually deleted by the user

Voice and rich media data on a recipient device is encrypted at the operating system level on iOS and suitably configured versions of Android 7+

Additionally, we use:

- 1024 bit RSA for authentication, digital signatures and secure media session keys exchange
- TLS for control traffic encryption between Zello client and Zello server
- All API communication occurs over HTTP/S

IBM Cloud erases data using a DOD 5220.22-M grade algorithm. This ensures that any residual drive data is destroyed. This process is monitored, logged and tracked. Once complete the drive is ready to be redeployed to a new customer.

If a drive fails the wipe process or reaches end of life, it is taken out of commission and physically destroyed