



Connect Device



User / Agent



Cloud Server



Web App



Device Camera



Company / Call Center

The K-Tech Connect system is a complete emergency text messaging and video solution. K-Tech Connect devices and users communicate with each other through a secure web app hosted on a cloud server network.

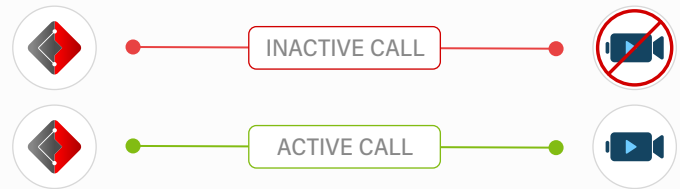
### Communication Protocols

K-Tech Connect devices & users communicate with our cloud servers using encrypted HTTPS and WSS protocols.



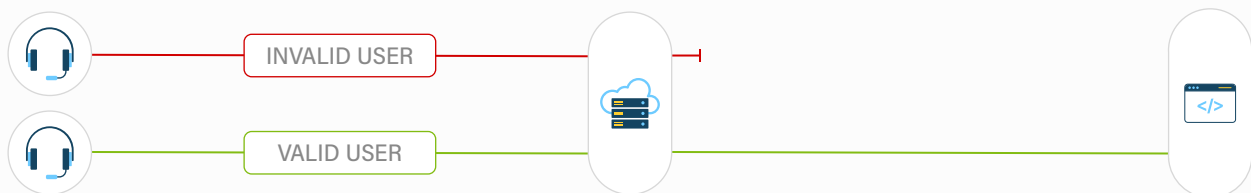
### Camera Activation

The K-Tech Connect emergency device camera is only on during an active emergency call, otherwise it is off.



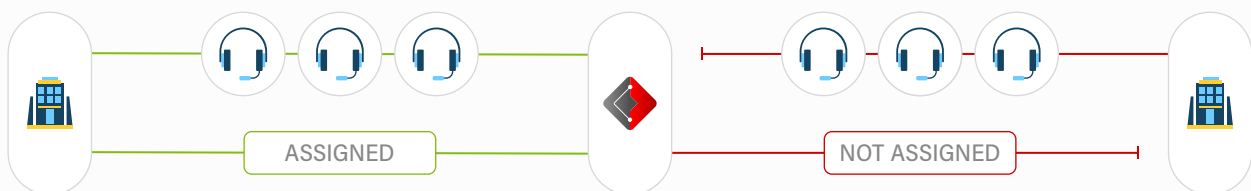
### Web App Access

Our cloud servers handle user authentication, allowing or rejecting the user's web app access based on their credentials. Our web app is an invite-only system. Anonymous users cannot register with the app, which adds to the app's security.



### Connect Device Access

K-Tech Connect devices are assigned to a company or call center within the web app. Only users who belong to that company or call center are allowed access to that device and its features, such as video and texting.



## Outbound Firewall Settings

K-Tech Connect devices access the K-Tech Connect web app in the same way users do, which is through a standard web browser. They only need outbound internet access.

If your firewall is set to filter outbound traffic, you will need to whitelist some destination domains and ports as the devices and web app utilize these for video and text communication. [See the list on the next page.](#)

## Inbound Firewall Settings

Since each K-Tech Connect device acts as a client and has no listening ports, your inbound firewall does not need to be opened for incoming requests to a particular IP address or port.

## Web App Security

### SSL/HTTPS/WSS

The web app is deployed behind HTTPS, and websocket connections are behind WSS to prevent malicious network users from sniffing authentication credentials or any other information transferred between the client and server.

The app also takes advantage of SSL redirects so that requests sent over HTTP are redirected to HTTPS.

### Cross site scripting (XSS) protection

The web app implements data sanitization by escaping specific characters which are particularly dangerous to HTML.

### Cross site request forgery (CSRF) protection

The web app has built-in protection against most types of CSRF attacks by checking for a secret in each POST request. This ensures that a malicious user cannot “replay” a form POST to your website and have another logged in user unwittingly submit that form. The malicious user would have to know the secret, which is user specific (using a cookie).

### SQL injection protection

Database queries in the web app are protected from SQL injection since the queries are constructed using query parameterization. A query's SQL code is defined separately from the query's parameters. Since parameters may be user-provided and therefore unsafe, they are escaped by the underlying database driver.

### Clickjacking protection

The web app contains clickjacking protection in the form of middleware, which in a supporting browser can prevent a site from being rendered inside a frame.

*Even with the above mentioned security measures in place, web apps and networks can still be susceptible to attacks.*



## Destination URLs with Protocol/Ports

K-Tech Connect Devices have no open listening ports whatsoever. This ensures our devices have a 0% attack surface. All of the connections made are outgoing to destination urls. Below is a list of each url, it's purpose, and the protocol/ports that it accesses.

**Web App**

**TCP** 80; 443;  
.ktechonline.com

**jQuery API**

**TCP** 80; 443;  
.jquery.com

**Styling & Icons**

**TCP** 80; 443;  
.ka-f.fontawesome.com  
.jsdelivr.net

**Map API**

**TCP** 80; 443;  
.googleapis.com  
.gstatic.com

**Media Includes**

**TCP** 80; 443;  
.digitaloceanspaces.com

**Video Transmission API**

**TCP** 80; 443; 3433; 4700 - 5000; 5668; 5669; 6080; 6443; 8667; 9667; 30011 - 30013;  
**UDP** 3478; 4700 - 5000;  
.agora.io  
.edge.agora.io  
.sd-rtn.com  
.edge.sd-rtn.com

**NTP Time Sync**

**UDP** 123; **TCP** 80; 443;  
0.debian.pool.ntp.org  
1.debian.pool.ntp.org  
2.debian.pool.ntp.org  
3.debian.pool.ntp.org

