CLEVERTOUCH

CLEVERTOUCH NETWORK REQUIREMENTS, SECURITY AND PRIVACY

The purpose of this document is to quickly assist IT administrators in understanding the basic network requirements (IP's and ports) for each of the Clevertouch services.

Using the information provided below we hope will help with successfully integrating Clevertouch products onto customers networks.

Over-The-Air (OTA) Update Service

- ota.clevertouch.com & ota2.clevertouch.com
- Server IP: 134.213.213.174 & 54.203.29.115
- TCP Port: 80 (HTTP)

NTP Server used on all Clevertouch LUX OS for keeping time in synch

- Server hostname: 2.android.pool.ntp.org
- UDP Port: 123 (NTP)

CleverMessage & Clevertouch Live

Ensure that access on ports 80 (http) and 443 (https) are enabled for connections to:

87.106.215.81

www.Clevertouch Live.com

live.Clevertouch Live.com

CLEVERTOUCH

Cleverstore – On Plus LUX only

The Cleverstore app connects to our servers over port 443 (standard https); The NewRelic and Google Analytics analytic packages use 443 (https) and 80 (http) (but these are not critical for Cleverstore to function)

Cleverstore Hosts:

- prod.sahara-admin.appcarousel.com
- sahara-stage-public.s3.amazonaws.com
- Ports: 80 (HTTP) & 443 (HTTPS)

URL's to whitelist if preferred over the hosts above:

https://prod.sahara-admin.appcarousel.com/api/v1/export-products
https://prod.sahara-admin.appcarousel.com/api/v1/export-categories
https://sahara-stage-public.s3.amazonaws.com

Lynx - Annotation and lesson planning software

Please ensure the firewall permits access to the following websites:

Lynx Hosts:

- auto.saharasupport.com
- registration.saharasupport.com
- Ports: 80 (HTTP) & 443 (HTTPS)

Airserver (Impact Plus and UXPro Gen 2)

Port information

	Inbound		Outbound	
	TCP	**UDP**	**TCP**	**UDP**
All Protocols	32768-61000	5353, 32768-61000	32768-61000	32768-61000
AirPlay	5000-5010, 7000*, 7100			
Google Cast	8008-8019	1900		
Miracast	7250		7236	
Management and updates	53, 80, 123, 443		443	

** This port requirement was added in version 2020.07.09*

CLEVERTOUCH

Bonjour services
AirServer Connect 4K UHD uses the following Bonjour services:

- _airplay._tcp
- _googlecast._tcp
- _display._tcp
- _airserver._tcp
- _raop._tcp

https://support.airserver.com/support/home

Clevershare 2nd & 3rd Generation Service and Applications

Important Note: No matter which Clevershare Generation software or hardware (dongle) being used the Clevershare (server) application on Clevertouch display should be activated first.

Network requirement of activation:

1. TCP Port：80 & 443 & 5224
2. DNS：linkmsg.seewo.com/seewo-link/api/v1/register
3. IP：Access using DNS
    a. IP number you will see are likely to see are
        i. Subnet starting 203.xx.xx.xx
        ii. 116.62.84.143
        iii. 101.37.44.92
        iv. 121.199.255.161
        v. 118.178.158.12

Please Note: If activation fails, you can enter the https://linkmsg.seewo.com/seewo-link/api/v1/register via the Clevertouch Browser to check and test whether or not the network connectivity between Clevertouch and the activation server is ok.

Important Note:
Clevershare previously could only work when both the Clevershare receiver (Clevertouch Display) and the Clevershare client (Windows, Apple or mobile) were on the same subnet*, in our latest version of Clevershare receiver v1.0.8.2070 we removed the boundary within our ‘Advanced Mode’ option within the settings menu of the Clevershare receiver app. This means that the Clevershare receiver and client can now be on totally different subnets on the same LAN, as long as those subnets are routable and the ports are allowed to traverse those subnets. This is accomplished by the new 9 digit code required to be used, it decodes all 32bits of the Clevershare receiver IP instead of just of just the first 13bits as previously.

CLEVERTOUCH

The Following ports are required to be open between the display network and device network only. There is no requirement to make these ports available externally

- TCP connection, command transmission service, ports are {**7385, 29736, 2067, 39458**}, it will try to open the 4 ports one by one, if one of them get opened successfully, the rest of the ports will not be opened.

- TCP connection, Video stream data transmission service, ports dynamic allocated by the system {**49200-49400**}, if multiple users share the screen, there will be multiple ports are allocated, maximum 4 ports currently.

- TCP connection, Audio stream data transmission service, ports dynamic allocated by the system {**49200-49400**}, if multiple users share the screen, there will be multiple ports are allocated, maximum 4 ports currently.

- TCP connection, Desktop synchronization, ports dynamic allocated by the system {**49200-49400**}. One of the port generated by the system that is not occupied by other services.

- UDP connection, Mouse control, ports dynamic allocated by the system {**49200-49400**}. One of the port generated by the system that is not occupied by other services.

- UDP connection, Touch feedback, ports dynamic allocated by the system {**49200-49400**}. One of the port generated by the system that is not occupied by other services.

- Chromecast function, port occupation (**8008, 8009**, and randomly try from 8009 onwards until an available port is found). Chromecast is UDP connection.

- Airplay function, port occupation (monitoring **7000**, randomly connection after successfully projected). Airpaly video transmission use TCP connection, audio is UDP.

- Airplay/Chromecast function, multicast DNS needs to occupy port {**5353**}

MDM – Mobile Device Management

There are two areas to be considered for network requirements: -

- **Browser Side** = MDM web portal that the Agent Side communicates to.

- **Clevertouch LUX (Android) Agent Side** = The service running on Clevertouch Android Module which communicates to the Browser Side.

Browser Side:

1. **MDM Application Server:** https://clevertouch.glbth.com – If possible we recommend to whitelist https://*.glbth.com (Port: 443 & dynamic IP)
2. **Location resolve by IP service**: https://pro.ip-api.com
3. **Open Street Map**: https://*.tile.openstreetmap.org
4. **Online chat:** https://static-v.tawk.to
5. **Streaming protocol servers to support "Remote" function:** Webrtc over UDP *.glbth.com (Port: 443 & dynamic IP)
    a. 52.11.103.125
    b. 34.240.200.142
    c. UDP ports range: 30100-40000

Clevertouch LUX (Android) Agent Side:

1. **MDM Application Server:** https: //clevertouch.glbth.com – If possible we recommend to whitelist https://*.glbth.com (Port: 443 & dynamic IP)
2. **Streaming protocol servers:** https://*.glbth.com (Port: 443 & dynamic IP)
3. **Push notification system:**
    - **Primary:** Port 443 to clevertouch.glbth.com or preferably *.glbth.com
    - **Secondary:** Should the primary fail or be too slow uses Google's Firebase Cloud Messaging (FCM), for completeness of setup please read the following and allow the three ports either to all public IP's are just the Google ASN ranges as listed below.
    - **The ports to open are:** 5228, 5229, and 5230. GCM typically only uses 5228, but it sometimes uses 5229 and 5230.
    - **Google ASN:**
        - 104.132.0.0/23
        - 104.132.11.0/24
        - 104.132.141.0/24
        - 104.132.34.0/24
        - 104.132.5.0/24
        - 104.132.51.0/24
        - 104.132.7.0/24
        - 104.132.8.0/24
        - 104.133.0.0/24
        - 104.133.2.0/23

CLEVERTOUCH

Clevertouch Live & Clevertouch Technologies Security and Privacy

Clevertouch Technologies provide digital signage solutions for every business sector from primary schools and small businesses through to universities and major corporations. The digital signage requirements of such a large user base are varied as are the security concerns of customers when adding Media Players (or any third-party device) to their network.

There are many solutions to customer's potential security concerns, the most secure but least recommended digital signage solution is to have a stand-alone system not connected to the customer's network. Whilst this is effective, and in use by a number of Clevertouch Technologies customers, it defeats the major advantage of being able to update sales or communications messages across your business, in seconds and without having to leave your desk.

Clevertouch Technologies solutions are designed on top of the Microsoft windows operating system in order that they can be

- Easily added to your network using standard procedures
    - In most networks they simply need plugging in and will connect automatically using DHCP

- Any network administrator can add standard security policies, such as adding the player to their domain, although to do this it is essential they follow the Clevertouch Technologies recommended procedure to ensure 24/7 signage operation. For example your standard PC build might save power by turning the screen off after an hour, or turn on a screen saver, which would stop the system working

- Players can be added to VLANs, WAN, connected over VPNs or in any other way IT want to operate

LAN versus Cloud

Clevertouch Technologies offer LAN base signage solutions where all the software required to operate a complete signage solution is installed on the Clevertouch Technologies Players and/or on the customer own PCs.

By containing all the software within the customer's network there is no requirement to access the internet, unless wishing to show internet content such as news or the weather, which removes the security risk of having a connection from inside the network to the internet.

CLEVERTOUCH

There are many advantages of using a Clevertouch Live Cloud attached digital signage systems such as

- Ease of use
- Ease of scalability to larger networks
- Ease of use across multiple geographic sites
- Clevertouch Technologies managed maintenance
- Automated Software updates
- Global access

The very low cost of controlling a network of players via Clevertouch Live means that the only reason not to do so are security concerns of using a Cloud based solution.

Clevertouch Live Methodology

The wide spread adoption of Cloud solutions such as Office365, Dropbox, OneDrive, Salesforce, EMIS Web and many more shows that most businesses accept that correctly designed Cloud solutions can be used and trusted with business data held off-premises and also having that off-site data kept synchronised with date on-site.

This is identical to the way the Clevertouch Live works

1. You upload your digital signage channels, images and messages to Clevertouch Live, which acts like a digital signage equivalent of Dropbox/OneDrive.

2. All your Clevertouch Technologies players connect to your Clevertouch Live account and are instructed to download the content you have uploaded, exactly like synchronising multiple computers using Dropbox/OneDrive

3. You then login to your Clevertouch Live control panel and tell which screen to play which channel

It's beautifully simple and very reliable.

Every player holds a copy of the data on Clevertouch Live and plays it out as requested. There is no bandwidth required to stream the data off the network as only new updates needs to be downloaded.

If the internet fails the player continues to play perfectly (although won't be updated with new content) Hence there are three sides to the system which need to be addressed to understand potential security

CLEVERTOUCH

1. Player connecting to Clevertouch Live and downloading content
2. Users uploading (updating) content on the site
3. Data storage on the site

Player connecting to Clevertouch Live (and downloading content)

Clevertouch Live uses 2048 bit SSL encryption for communication between Clevertouch Live.com and a Clevertouch Technologies Cloud connected player inside the customer's network.

When a brand new player is connected to the internet it makes a connection request to www.Clevertouch Live.com which generates a unique 8 digit alpha-numeric pin code. When this pin code is typed into a Clevertouch Live account that in turn generates an industry standard OAuth2.0 authentication token which is send to the player. Both the player and Clevertouch Live then destroy the 8 digit code and use the OAuth token to validate all communications between them giving a fully secure, authenticated and encrypted communications mechanism. Digital signage media, as well as server client communications messages, are send via this mechanism.

The server always validates that the token is correct before allowing any communication with the player.

For network security, all communications between the customer's player and the Clevertouch Live server originate on the player. Hence for firewalls there are no unsolicited in-bound communications from the internet. The player continually issues requests to the Clevertouch Live server using long-polling requests lasting up to 30 seconds. When the server has new instruction for the player that need to be acted upon it responds and the instructions are received and processed by the player.

If the instruction includes a requirement to download updated content then a new secure connection is created and the media is downloaded.

The local player always keep open a long-polling push notification connection with the server. This has added the advantage of allowing almost instantaneous player reaction to requests such as changing channels as well as allowing for a real-time status view of the customer's entire network via the Clevertouch Live control panel.

When a player is removed from the customer's account (by the customer through the Clevertouch Live control panel) the OAuth token is removed and the player cannot be reconnected using it. Hence if the player is physically stolen the customer simply need delete it from their account thereafter there is no potential for connection to their account.

CLEVERTOUCH

For this communication system to work ports 80 (http) and 443 (https) must be open through firewalls and access to the Clevertouch Live servers allowed. A document details the required servers names and IP address can be found here https://www.Clevertouch Live.com/firewall as well as how to use the Clevertouch Live player built in diagnostics to test the firewall is correctly configured.

Users uploading (updating) content on the site

There are two cases for user uploading content using their own PCs and devices

a) Managing the signage network, or uploading content, using a Web browser
b) Creating and uploading signage channels using the Clevertouch Technologies Windows desktop application called ImageFlyer Cloud Master

Managing the signage network, or uploading content, using a Web browser

Clevertouch Live allows users to update content on signage screens, and switch what is playing on screen, by logging into the control panel on their Clevertouch Live account.

The system uses user name and password authorisation. During the session, the customer can upload new content from their device (any device running a modern browser).

All user passwords on Clevertouch Live are hashed and no password is stored in the Clevertouch Live database in plain text. Users are automatically redirected to a secure HTTPS URL even if an attempt is made to login via insecure HTTP

The security system is only as good as the customer's own password policy and the user should choose suitably secure passwords and not reveal these to unauthorised personnel. Passwords for Clevertouch Live must be at least 6 digits in length and can be reset at any time.

To facilitate ease of use, and also security, the admin user can allow unlimited sub users, with their own unique users name and password, to update signage content on zones within channels. This makes the system flexible for admin to limit user privileges and also negates the need to share the administrator credentials.

Creating and uploading signage channels using the Clevertouch Technologies Windows desktop application called ImageFlyer Cloud Master

ImageFlyer Cloud Master is a windows desktop application which allows users to create fully bespoke signage channels.

It works by allowing users to draw, on their own Windows desktop, multiple communications zones in the form of slides shows, text zones, moves, web pages, news feeds and more.
When the user selects to 'publish' the channel they have created (or modified) a connection to the user's Clevertouch Live account is made, all the elements and media are packaged together and everything is uploaded to the account using 2048 bit SSL encryption.

The first time the publish button is used ImageFlyer Cloud master requests a user name and password pair from the user. This is encrypted and passed to Clevertouch Live which checks the credentials for an account of Clevertouch Live. If they match an OAuth security token is returned and all future communications with Clevertouch Live are authenticated. All communications between the ImageFlyer Cloud master and Clevertouch Live are initiated by this software on the user's Desktop.

For this ImageFlyer cloud master system to work ports 80 (http) and 443 (https) must be open through firewalls and access to the Clevertouch Live servers allowed. A document details the required servers names and IP address can be found here https://www.Clevertouch Live.com/firewall The ImageFlyer cloud master does NOT include diagnostics for debugging firewall issues.

Data Storage

All customer's data on Clevertouch Live held on dedicated servers in the EU, at the time of writing (23/03/2017) in Baden Baden Germany. Whilst the data is backed up daily it is the customer's responsibility to ensure they have copies of any media which is of value a Clevertouch Technologies accept no financial responsibility for the loss of Media the event loss. It is worth noting that every player on a customer's network has a copy of the data in their account as if in effect a back-up in its own right.

Privacy concerns

Digital signage is not, under normal circumstances, used to convey very highly sensitive or confidential information. For example, a hospital may use signage to call patients into clinics but would not use it to display the patient's ailments. Most privacy concerns are alleviated if the customer considers what is going to be on screen, bearing in mind the end result is normally shown on a huge screen designed to draw attention to communications in a public, office, retail or educational space.