OnTime Network Requirements

OnTime/AirStack Access

For OnTime to transfer time and attendance data, along with transferring/receiving registration templates, there must be an unrestricted network. This is to ensure there is no communication issue between OnTime (connected to the client network) and AirStack (hosted on Allocate Cloud).

This can be achieved by allowing full internet access through the Firewall for SmartHub devices. Where this cannot be achieved, the devices must be allowed to communicate directly with AirStack (hosted on Allocate Cloud). **Specific host/URL/IP requirements should be requested from RLDatix Support.**

CPAir Access

In order for the OnTime application to communicate with our device management system CPAir, **please allow the TimeClock to communicate with https://cpair.uk/login hosted at Server IP: 198.244.229.71**

More information on CPAir can be found here

Google Play Access

The OnTime Application makes use of Google Play Services to register employee templates to location (radius) and to send/receive employee templates within that defined radius.

The following destination host and ports, must be enabled on the clients network/firewall to ensure OnTime can function correctly:

Destination Host	Ports
play.google.com	TCP/443
android.com	TCP, UDP/5228-5230
google-analytics.com	
googleusercontent.com	
*gstatic.com	
*.gvt1.com	

*.ggpht.com dl.google.com dl-ssl.google.com android.clients.google.com *.gvt2.com *.gvt3.com	
*.googleapis.com m.google.com	TCP/443
accounts.google.com accounts.google.[country]	TCP/443
pki.google.com clients1.google.com	TCP/443
clients2.google.com clients3.google.com clients4.google.com clients5.google.com clients6.google.com	TCP/443
omahaproxy.appspot.com	TCP/443
android.clients.google.com	TCP/443
connectivitycheck.android.com connectivitycheck.gstatic.com www.google.com	TCP/443

Source: https://support.google.com/work/android/answer/10513641?hl=en

Remote Support Access (TeamViewer)

The Timeclocks are remotely supported via a remote access tool, TeamViewer. TeamViewer is used by Allocate/ClockedIn Service Desk for long term remote support for software/hardware issues which may arise. Furthermore, Software Updates to OnTime are pushed out and applied via this remote access which does not require interaction on site.

To ensure that TeamViewer is not restricted on your local network, please ensure the below network ports are allowed the relevant access:

TeamViewer's Ports

TeamViewer prefers to make outbound TCP and UDP connections over port 5938 – this is the primary port it uses, and TeamViewer performs best using this port. Your firewall should allow this at a minimum. If TeamViewer can't connect over port 5938, it will next try to connect over TCP port 443. If TeamViewer can't connect over port 5938 or 443, then it will try on TCP port 80.

Destination IP addresses

The following extract has been taken from – https://community.teamviewer.com/English/kb/articles/4139-which-ports-are-used-by-teamviewer

"The TeamViewer software makes connections to our master servers located around the world. These servers use a number of different IP address ranges, which are also frequently changing. As such, we are unable to provide a list of our server IPs. However, all of our IP addresses have PTR records that resolve to *.teamviewer.com. You can use this to restrict the destination IP addresses that you allow through your firewall or proxy server.

Having said that, from a security point-of-view this should not really be necessary – TeamViewer only ever initiates outgoing data connections through a firewall, so it is sufficient to simply block all incoming connections on your firewall and only allow outgoing connections over port 5938, regardless of the destination IP address."

Source: https://community.teamviewer.com/English/kb/articles/4139-which-ports-are-used-by-teamviewer