Network requirements for cloud connected devices

For optimal security, all communication between zencontrol cloud infrastructure is performed on a secure TLS socket. Each connection uses an ephemeral port and is always an outbound connection. The sites network must also be synchronised with an NTP server for the TLS handshake to complete and secure the connection. When commissioning, devices receive network configurations by default via a DHCP server. It is also recommended that the network enables ICMP types 0, 3 and 8 to allow for network diagnostics and discovery of control systems.
For Wi-Fi connected devices, they will need to connect to an **802.11g** network on **channels 1-11** authenticated via **WPA-2 personal security**. There should also be no 'Captive portal' page on the Wi-Fi.

The following table shows the required ports that must be enabled to use the sites internet connection for communication with the zencontrol cloud infrastructure.

Service	Type	Port	Protocol	Network access	Application Layer
Api Server	Commissioning	8901	TCP	Outbound	MNCP 2.0, TLS 1.2 PKI
Api Server	Commissioning	8902	TCP	Outbound	HTTP/2, TLS 1.2 PKI
C2C MNCP	Controller	5110	TCP/UDP	Internal	MNCP 2.0 & TLS 1.2 PSK
Device Upgrade	Controller	5112 & 6396	TCP	Outbound	MNCP 2.0
Zentri OTA	Controller	443	TCP	Outbound	HTTPS
Cloud MNCP	Controller	5113	TCP	Outbound	MNCP 2.0 & TLS 1.2 PKI
API	Controller	5108	UDP	Internal	Third Party Interface

Outbound zencontrol URLS required:
fw-download.zencontrol.com - for the controllers to upgrade their firmware
connect.zencontrol.com - for the controllers to connect to the cloud
ntp.buildinglogin.com - for the controllers to resync their time
mobile.zencontrol.com - for the commissioning app
api.zencontrol.com - for the automated interaction with the cloud
login.zencontrol.com - for web auth
cloud.zencontrol.com - for web portal
developer.zencontrol.com - documentation of api

Note:

1. The IP address those URLs resolve to changes frequently. The outbound filter will need to follow the URL and not the resolved IP address, this is because each of those URLs resolve to an allocated Amazon AWS load balancer and we get shifted between load balancers depending on the server loads.
2. The URLs above use custom ports. The firmware update port is 5112. The Cloud connection port is 5113
3. At a local network level the controllers will communicate with each other on port 5110 and 5108 (TPI applications) These are not external connections, and do not need to be allowed through the firewall, but will need to be allowed locally on the network.
4. The NTP server will use port 123 in accordance with the NTP spec.