SCANCO

Firewall Checklist

innovation
service
experience

NETWORKING/FIREWALL REQUIREMENTS

Objective: Allow requests from Scanco Server to Firewall, forwarded to MAS Server using Port 50,000 to consume a listening service, secured via SSL.

NOTE: *Firewall cannot be tested until after Scanco is installed.* **Sample request:** **https://publicIP:50000/api/test/get**

* There are (2) client apps that may be used for daily scanning:

Scanco Cloud	Scanco Warehouse and MFG 100
Thin Client based. Scanners perform RDP to a cloud server to access the application. Thus, traffic from the Scanco Cloud server routes to your public IP address (firewall). This needs to be configured to allow the traffic and forward it to the Sage Server.	Local based – application sends and receives data directly to the Sage Server. Server and wireless devices should be able to see each other on the local network.

Most customers will be configured for Scanco Warehouse and MFG 100. It does not require the firewall configuration described below. **However, customers who perform the firewall steps outlined below gain additional benefits:**

- A backup application (Scanco Cloud). Used if waiting on Apple to approve the latest update.
- **Increased Support:** Scanco can resolve technical issues faster.

☒ Open port 50,000 on the main firewall.

☒ White list the following IP Addresses:

54.173.192.130 (wms1.scanco.com)
54.173.30.240, 54.173.131.151
54.173.148.207, 54.172.230.152, 54.174.77.240

☒ Forward WAN traffic from Scanco's Cloud servers above to the LAN address of the Sage MAS Server. Destination port 50,000. TCP traffic only.

☒ Public IP Address (or hostname):
65 . 31 . 124 . 237 : 50,000

Signed Complete: _____ Date: 6/12/2019