NETWORK CONFIGURATION REQUIREMENT

3561 FC Vibration Sensor

Introduction

Fluke 3561 FC Vibration Sensors are deployed with strict network compliance guidelines. Refer to this document to make sure you are adequately prepared to start a successful vibration monitoring program.

Is my data encrypted and how?

All data sent from mobile phones, gateways, power monitors or other devices is encrypted using SSL/TLS. We are aware of the vulnerabilities with each of these protocols and have updated them to the latest industry recommended version to avoid man-in-the-middle attacks.

What inbound/ingress ports need to be opened?

No inbound ports need to be opened, all our traffic is outbound and should be handled by NAT at the firewall level.

What outbound/egress ports and protocols need to be allowed for FW rules?

We use standard ports registered by IANA and would need the following ports and protocols allowed through the firewall:

Type	Destination Host/IP	Ports	Direction	Purpose	Service/ Product
TCP	service.connect.fluke.com	443 (HTTPS)	Egress	Rest API	Fluke Connect mobile app
TCP	measurement.connect.fluke.com	443 (HTTPS)	Egress	Rest API	Fluke Connect mobile app
TCP	streaming.connect.fluke.com	443 (HTTPS)	Egress	Rest API	Fluke Connect mobile app
TCP	notification.connect.fluke.com	443 (HTTPS)	Egress	Rest API	Fluke Connect mobile app
TCP	bzio.connect.fluke.com	443 (HTTPS)	Egress	Rest API	Fluke Condition Monitoring 3502 Gateway (Nocturne)
UDP	0.pool.ntp.org 1.pool.ntp.org 2.pool.ntp.org 3.pool.ntp.org	123 (NTP)	Egress	NTP (time synchronization)	3502 Gateway (Nocturne)

Notes:

- The servers listed are not customer-facing web servers, so you should expect a 404 error (or no response) if you enter URLs into a web browser.
- You will see SSL certificate errors if you input HTTPS list entries into a web browser, as they are aliases for third-party servers. The certificate is issued to the actual name of the server, not our alias.

What are the network requirements to use 3561 FC Vibration Sensor successfully?

- ✓ **Wi-Fi Spectrum Compatibility:** All data sent from mobile phones, gateways, power monitors or other devices is encrypted using SSL/TLS. We are aware of the vulnerabilities with each of these protocols and have updated them to the latest industry recommended version to avoid man-in-the-middle attacks.
- ✓ **Coverage:** Ensure adequate electrical service outlets for the gateways and Wi-Fi coverage at the desired locations.
- ✓ **Security:** Ensure that the Wi-Fi network is using one of the following Wi-Fi security modes: None, WEP, WPA/WPA2 Personal. WPA2 Enterprise / 802.1x is not supported at this time.
- ✓ **MAC Address Whitelisting:** Wireless network may require 3502 FC Gateway's Wi-Fi MAC Address be explicitly added to approved devices table if link layer filtering is used.
- ✓ **M2M Optimized:** Ensure that the Wi-Fi network is machine to machine (M2M) optimized, meaning that it does not implement HTML sign-in prompts or any other forms of authentication that require human interaction (i.e. no captive portals); access should be non-expiring.
- ✓ **Signal Strength:** Ensure Wi-Fi signal strength at gateway location is -75 dBm or stronger.
- ✓ **Connection Speed:** Ensure Wi-Fi connection speeds out to the internet are 2 Mbps download and 2 Mbps upload minimum, sustained.
  - ✓ Each 3502 FC Gateway will be sending about 50 to 100 kbps of data maximum. In general, there should be at least 128 kbps upload bandwidth available on the network for each 3502 installed. Multiply the number of 3502 FC Gateways by 128 kbps to get the required upload bandwidth. This is to avoid any latency in the transmission of data from 3502 FC Gateways to the cloud. Test connection speeds at http://www.speedtest.net. Testing must be done from a smart device or computer using the same wireless network the 3502 Gateway is or will be connected to.
- ✓ **DHCP:** DHCP must be enabled for the Gateways to join Wi-Fi networks; leases to clients will be granted in less than 30 seconds.
- ✓ **Wi-Fi Hotspot:** If using a cellular-based Wi-Fi hotspot for connectivity, ensure the data plan does not throttle bandwidth after a certain amount of data is transferred.
- ✓ **No proxies:** Ensure no HTTP(S) proxies are in use and that connections to bzio.connect.fluke.com are whitelisted with BYPASS directives on port 443.

✓ **Note:** If your available Wi-Fi network uses 802.1X / WPA2 Enterprise, uses captive portals to log on, employs HTTP proxies or is blocking traffic to the Internet, consider broadcasting an additional SSID/network that doesn't have these restrictions but is locked down to just the gateways.

Why don't we have IP addresses for the destinations hosts?

We use Amazon Web Services (AWS) for our cloud platform. These services use virtual IP addresses that could change as Amazon manages its offerings. AWS will have multiple IPs that can change based on demand. The document "aws-ip-ranges" references IP ranges used by AWS to set firewall access to the Fluke Connect services. We recommend saving the JSON document to a source control repository so that backups and version revisions can be done if needed.

Documentation and Syntax:
https://docs.aws.amazon.com/general/latest/gr/aws-ip-ranges.html

JSON document with IP ranges:
https://ip-ranges.amazonaws.com/ip-ranges.json

Accelix. *Connected Reliability.*

Fluke Corporation
PO Box 9090, Everett, WA 98206 U.S.A.

For more information call:
In the U.S.A. 856-810-2700
In Europe +353 507 9741
In UK +44 117 205 0408
Email: support@accelix.com
Web access: http://www.accelix.com