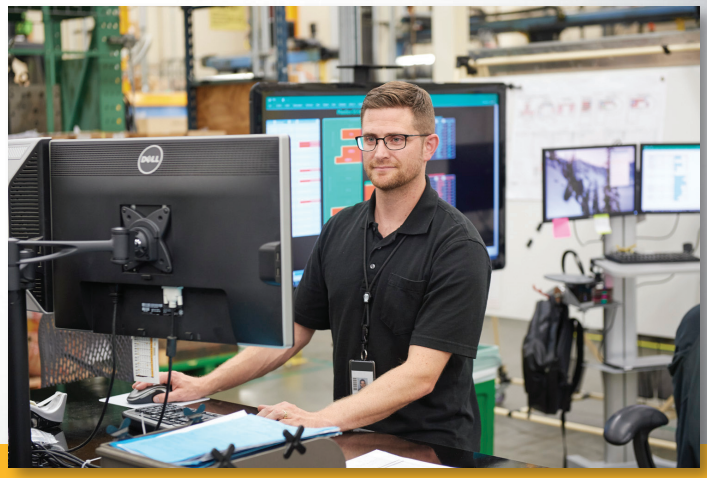
# Fluke 3563 Analysis Vibration Sensor IT and security

Frequently asked questions



## Data collection and storage

| | |
|---|---|
| **Q:** Where is all my data hosted and stored? | **A:** The data is hosted on AWS. |
| **Q:** How does Fluke 3563 ensure the security of data at rest? | **A:** Our database backups are encrypted when at rest. |
| **Q:** How does Fluke 3563 ensure the security of data in transit? | **A:** Fluke ensures data in transit is secure by using TLS and https protocols to transmit sensitive data. |
| **Q:** How is the availability of data guaranteed? | **A:** Our cloud storage vendor provides Fluke three types of service:<br>1. For Relational Database Service # (RDS), the service level agreement (SLA) commitment is a Monthly Uptime Percentage of at least 99.95%.<br>2. For Simple Storage Service, the SLA commitment is a Monthly Uptime Percentage of at least 99.9% during any monthly billing cycle.<br>3. For Elastic Compute Cloud, the SLA commitment is a Monthly Uptime Percentage of at least 99.95%. Uptime on the Fluke 3563 app may vary. |
| **Q:** How long will the data be available for an active account? | **A:** Under the current terms of service, your data remains on the system until you tell us to delete it. Fluke retains the right to impose a time limit. |
| **Q:** How long will the data persist in storage for a non-active account (what if a user who did not log in for a year)? | **A:** Under the current terms of service, data in non-active accounts is not deleted unless specifically requested by the administrator. Fluke retains the right to impose a time limit. |

FLUKE Reliability

## Data Security

| | |
|---|---|
| Q: Who can view my data? | A: Once the information is transmitted to the Fluke Cloud™ Storage for a team account, only those people specifically given access by the administrator can view the data. The administrator specifies who has access to the information for that team, which helps prevent unauthorized users from accessing data. |
| Q: Who owns the right to manage (create, update, delete, download etc.) customer data? | A: Fluke eventually owns the data per EULA. |
| Q: Physical and environmental security of Fluke 3563 Infrastructure. | A: Our data center is cloud based and managed by AWS, they have security documents that we can refer them to. |
| Q: How is the app data protected from hackers? | A: Fluke Cloud™ storage is hosted on a cloud infrastructure architected to be one of the most secure cloud computing environments available today. Our cloud service provider uses state-of-the-art electronic surveillance, multi-factor access control systems, and 24x7 staffing at its data centers. Furthermore, the servers have built-in firewalls, encrypted data storage and secure access specifically de-signed to protect your data. Data transfers from smartphones to the cloud and back are encrypted to prevent interception of the data by an unauthorized user. |

## Identity and access management

| | |
|---|---|
| Q: What password policies are enforced? | A: • Min 8 characters required<br>• At least one uppercase character<br>• At least one special character |
| Q: What if someone on my team loses their phone? | A: The Fluke 3563 app requires a personal login. None of the information on the app or in the cloud can be accessed without that login. We further recommend that all smart devices used for company business have a mandatory overall login code, and that any proprietary information be locked behind additional security tools and measures. Users also have the option to change their app password via the Web user interface, blocking access by any unauthorized person who may have obtained the phone and learned the original password. |
| Q: What happens to the data on the phone and in the cloud the moment a person is removed from a team? | A: If an administrator removes a person from the team, all of that person's data stays with the team, including any data collected before they joined the team. The individual loses access to data on the cloud, and the data cached on that person's phone will be wiped the next time they attempt to connect to the cloud. The remaining Fluke 3563 account can be used to save new data to the cloud. |
| Q: Can I easily block or empty my account in case of a stolen phone or password? | A: If a phone is lost or a password is compromised, the administrator or team member related to the phone can change the password immediately. If the phone is company-issued, the company's IT department may have the ability to wipe it remotely, which will also remove the Fluke 3563 app and cached data. |

**Q:** How will users be authenticated, that is, how do we know a user is entitled to use the application?

**A:** User authentication is done by breaking access down into separate parts:

- IOT devices use SSL certificates to be able to communicate to our IOT endpoint, all data is encrypted using SSL.
- Phones uses HTTPS certificate to authenticate the site its communicating with had a valid SSL cert and also that the data is encrypted.
- Web browsers use HTTPS/TLS also to communicate to the back end services and ensure that all data transmitted is encrypted.
- Finally user credentials are stored encrypted at rest and would need a key to un-encrypt it from the database.

**Q:** Is Fluke 3563 accessible from mobile devices such as cell phones and tablets? If so, can access be restricted only to company-owned devices?

**A:** At this time we do not have the abilities to restrict an account based on what phone they are using.

**Q:** Does Fluke 3563 offer multi-factor authentication?

**A:** No, not at this time.

## Fluke Condition Monitoring hardware security and data transmission

**Q:** What are the transmission specifications for the tools?

**A:**

| | |
|---|---|
| **Wireless technology** | Wi-Fi<br>• IEEE 802.11 ac/a/b/g/n<br>• Security: WPA/WPA2-PSK<br>• Transmission rate: 1 – 866.7Mbps<br><br>Wired LAN<br>• Ethernet 1 GBits/s<br><br>Network general (LAN + WIFI)<br>• Protocols: MQTT and HTTP with TLS |
| **Standard** | IEEE 802.11 b/g |
| **Certifications** | FCC/CE/IC |
| **Supported network security protocols** | Open (no security)<br>Wi-Fi protected assets II<br>• WPA-2 Personal (AES-256 packet encryption)<br>• WPA-2 Enterprise (FreeRadius 3.0.X Series WPA-2 Enterprise Server with PEAPv0-MSCHAPv2 options enabled; other types/ options are unsupported) |
| **Transmission rate** | 1-11 Mbit/s with IEEE802.11b |
| **Receive sensitivity** | Nominal: Less than -65dBm<br>Minimal: -83dBm |
| **Output level** | +12dBm |
| **Channels** | 1-14 with 5MHz intervals (default: Channel 6) |
| **Application protocol** | Packet Based Proprietary Protocol |
| **Encryption** | AES-256 with strong 384 bit ECC key generation |
| **Inegrity and uniquity** | Protected with multi-level Signature Hash Algorithm |

FLUKE Reliability

| | |
|---|---|
| **Q:** Can someone hack into the Gateway and from there access my network? | **A:** • With Bluetooth – No. Gateway listens to advertising only. It is not possible to establish a Bluetooth connection to the gateway.<br>• Over Wi-Fi or LAN in normal operation mode – No. Gateway offers no service to access to. MQTT is a pub-sub system and gateway is always subscriber.<br>• Over Wi-Fi in hotspot mode – No. Hotspot mode only active if gateway isn't connected to ADP. While provisioning you need physical access to the gateway because SSID and password is printed on gateway type plate. Individual per gateway. And the gateway offers over hotspot only http REST endpoints which where tested with a special vulnerability scanner for security flaws. |
| **Q:** Can unauthorized people connect to the 3563 gateway? I'm concerned about malicious interferences with a monitoring session and loss of data. | **A:** No - Gateway connects with MQTTS to ADP. There is no service to which you can connect in normal operation mode. |
| **Q:** Is the data transfer encrypted? I'm concerned about unauthorized access to or corruption of restricted/sensitive maintenance data. | **A:** • Data transfer between gateway and cloud is TLS encrypted.<br>• Sensor is paired with the gateway. It's not possible for a second device to connect to the sensor and fetch data from it. |
| **Q:** What sort of network access does the sensor need to operate? | **A:** • LAN or Wi-Fi connection to local network with internet access needed by the gateway.<br>• There is no ingoing connection. Only outgoing connections with MQTTS (port 443) in normal operation mode and HTTPS (port 443) for OTA update. |
| **Q:** What are the data transmission sizes? | **A:** • Default screening config (3 axis, overall acc+vel + temp) ~ 1.8 kByte<br>• TWF for band value computation for all three axis ~440 kByte<br>• Sensor signal status ~ 230 Byte<br>• Gateway update package: up to 180 Mbyte<br>• Sensor update package: 450 kByte |