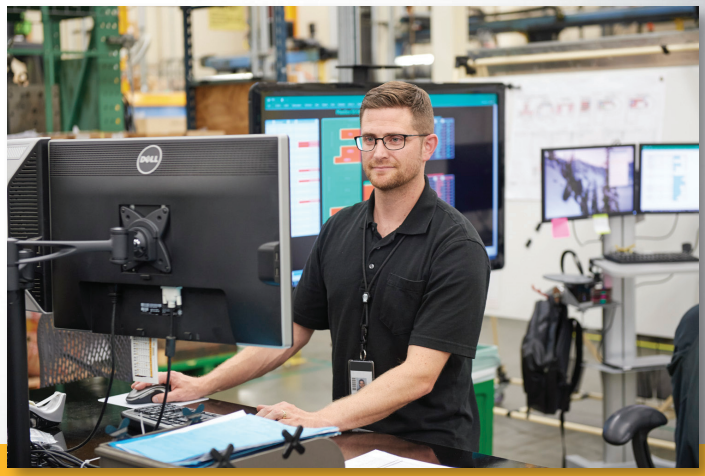
Fluke Connect IT and security

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 Connect ensure the security of data at rest?	**A:** Our database backups are encrypted when at rest.
Q: How does Fluke Connect ensure the security of data in transit?	**A:** Fluke ensures data in transit is secure by using TLS, SSL, 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: 1. For Relational Database Service # (RDS), the service level agreement (SLA) commitment is a Monthly Uptime Percentage of at least 99.95%. 2. For Simple Storage Service, the SLA commitment is a Monthly Uptime Percentage of at least 99.9% during any monthly billing cycle. 3. For Elastic Compute Cloud, the SLA commitment is a Monthly Uptime Percentage of at least 99.95%. Uptime on the Fluke Connect 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.

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 Connect 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: The Fluke Connect app requires a six character password. Users should follow their internal company guidelines for character complexity and frequency of change.
Q: What if someone on my team loses their phone?	A: The Fluke Connect 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 Connect 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 Connect 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/SSL 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 Connect 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 Connect 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	Wireless Lan/Wi-Fi
Standard	IEEE 802.11 b/g
Certifications	FCC/CE/IC
Supported network security protocols	Open (no security) Wi-Fi protected assets II • WPA-2 Personal (AES-256 packet encryption) • 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 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®

Q: Can someone hack into the Gateway and from there access my network?	**A:** No. The point of access for a smart device into the Gateway is isolated from the Gateway's access to the client network. Even if someone did somehow get access to the Gateway via a device, they couldn't get from there to the network.
Q: Can unauthorized people connect to the Fluke 3501 FC or 3502 FC Gateway? I'm concerned about malicious interference with a monitoring session and loss of data.	**A:** Only people who have the password can access the Gateway.
Q: Is the data transfer encrypted? I'm concerned about unauthorized access to or corruption of restricted/sensitive maintenance data.	**A:** • Data is encrypted between the phone and the gateway, via WiFi network encryption, and between the gateway and the cloud, via SSL (standard practice). • Data is not encrypted between the short-range sensor and the gateway but it is very difficult for unauthorized parties to access. ✦ Unauthorized parties using the Fluke Connect app can't see the data stream from connected sensors. BLE scanner apps may be able to see sensors that are turned on but not connected to the gateway. ✦ The short-range point-to-point signal from the sensors is not a target for signal jammers or scrapers, due to the restrictive 30 meters (90 feet) range. • To change a Gateway recording session or see connected sensors or measurements, a person must have the Gateway password.
Q: How do I protect my operations systems from being compromised by Fluke Connect?	**A:** The Fluke Connect app and data are completely separate from operations, SCADA, and HMI systems. There is no point of intersection so malicious users cannot access your internal networks from the Fluke Connect app.
Q: Can unauthorized parties connect to Fluke connect enabled sensors and tools? I'm concerned about malicious interference with a monitoring session and loss of data.	**A:** The Fluke connect enabled tool and sensor network is initially configured via an extremely limited BLE interface. Within close physical proximity (up to 90 feet), there's no password required for the BLE so, theoretically, someone could reset the module and create a new password. After configuration, the sensors uses secure communications through your network to reach Fluke's servers and perform its assignment so it's extremely unlikely that an outside entity can access your data.
Q: Is the data transfer encrypted? I'm concerned about unauthorized access to or corruption of restricted/sensitive maintenance data.	**A:** Data is encrypted between the sensors/gateway and the cloud via SSL. Data is not encrypted between the phone and the tools/sensors but it is very difficult for unauthorized parties to gain access. BLE scanner apps may be able to see tools/sensors that are turned on but the data available for scanning is extremely limited in scope. The short-range, point-to-point signal from the sensors is not a target for signal jammers or scrapers, due to the restrictive 90-foot range. To change a recording session or see connected sensors or measurements, a person must have a Fluke Connect® login and password.

Q: What sort of network access does the sensor need to operate?

A: To connect the gateway/sensor to the internet, your IT department needs to allow the gateway/sensor to connect to a local Wi-Fi network and must also allow http protocol to Fluke.com, MQTT protocol over TCP port 8883 and access to Fluke Connect® Cloud storage for measurements.

Q: What are the data transmission sizes?

A:

Typical Overall Measurement (Up)	80 Bytes
Typical Spectrum Measurement (Up)	800 Bytes
Zeep Message (Down)	FCC/CE/IC
Over-The-Air Firmware Upgrade (Down)	9 Bytes (Typical) + Additional payload if instruction requires (Payload < 120 Bytes Typical)

Incident management

Q: In case of a data integrity compromise, (accidental update/deletion of data by a privileged user) how will Fluke Connect restore the data?

A: We have hourly backups and would need to restore from that data the information, this would also refer to DR/BC plans.

Cloud security

Q: Can I connect to the cloud via a cellular network?

A: Yes, but only if you're using a cell phone as a Wi-Fi hotspot, a practice known as tethering. Once you've turned tethering on,your sensor can send data to the cloud via your smartphone's connection. The gateway/sensors needs Wi-Fi access to send data to the cloud.

Q: What are the roles, responsibilities and ation methods?

A: Each team is responsible for some part of the security policy in that each team has responsibility to secure the communication between client and server, also access to AWS resources made available to Fluke Employees.

Q: What are the transmission specifications for the tools?

A:

Service	Team	Responsibilities	Authentication Methods
Web Service API	Web Services	Provide authentication services for all Fluke Connect client calls	FC user authentication in the DB level with hashed user password
Fluke Connect Web Application	WebApp	Secure access to the Fluke Connect Web Console	Secure connection to the Web Service API, uses WebSVC API for authentication
Fluke Connect Android	Android Mobile	Secure access to Fluke Connect Android mobile application	Secure connection to WebSVC API, uses user/password from WebSVC API
Fluke Connect iOS	iOS Mobile	Secure access to Fluke Connect iOS mobile application	Secure connection to WebSVC API, uses user/password from WebSVC API
Fluke Connect Desktop	FC Desktop	Secure access to Fluke Connect Desktop application	Secure connection to WebSVC API, uses user/password from WebSVC API
AWS Console Access	Ops	Secure access to AWS and its resources allocated to Fluke Connect	Username and Password, with Multi Factor Authentication to Web Console

Regulatory compliance

Q: Is Fluke Connect's hosting solution SAS 70 type II/SOC 3 certified?	**A:** Yes.
Q: Are Fluke Connect's data centers ISO 27001 certified?	**A:** Yes.

Business continuity

Q: How does Fluke Connect protect against loss of power, loss of network access, loss of other key infrastructural elements, non-availability of personnel due to severe weather events, and so on?	**A:** Data centers are built in clusters in various global regions. All data centers are online and serving customers; no data center is "cold." In case of failure, automated processes move customer data traffic away from the affected area. Core applications are deployed in an N+1 configuration, so that in the event of a data center failure, there is sufficient capacity to enable traffic to be load-balanced to the remaining sites. Each availability zone is designed as an independent failure zone. This means that availability zones are physically separated within a typical metropolitan region and are located in lower risk flood plains (specific flood zone categorization varies by Region). In addition to discrete uninterruptable power supply (UPS) and onsite backup generation facilities, they are each fed via different grids from independent utilities to further reduce single points of failure. Availability zones are all redundantly connected to multiple tier-1 transit providers.

For more information, visit: www.fluke.com/conditionmonitoring
or call 1-844-427-2269