FLUKE®

How Fluke Connect safeguards data saved to the cloud

White Paper

The introduction of Fluke Connect™ in 2014 added a new level of efficiency and effective collaboration for maintenance and troubleshooting teams in all kinds of manufacturing, commercial, and retail facilities. Technicians can monitor real time results from more than 20 different Fluke test tools from a smart phone (up to 10 at a time on iPhone and 6 on Android). They can also securely share that information in real time with authorized team members in other locations.

In addition, test results and maintenance data can be collected through the Fluke Connect app and stored by asset in secure Fluke Cloud™ storage. That means that troubleshooting and maintenance staff can access that data in the field to compare new measurements to baseline measurements to more quickly identify problems.

The end result is that technicians can use Fluke Connect to quickly identify and diagnose problems while securely sharing the related data, when they want and with the specific people they have given permission to view it.

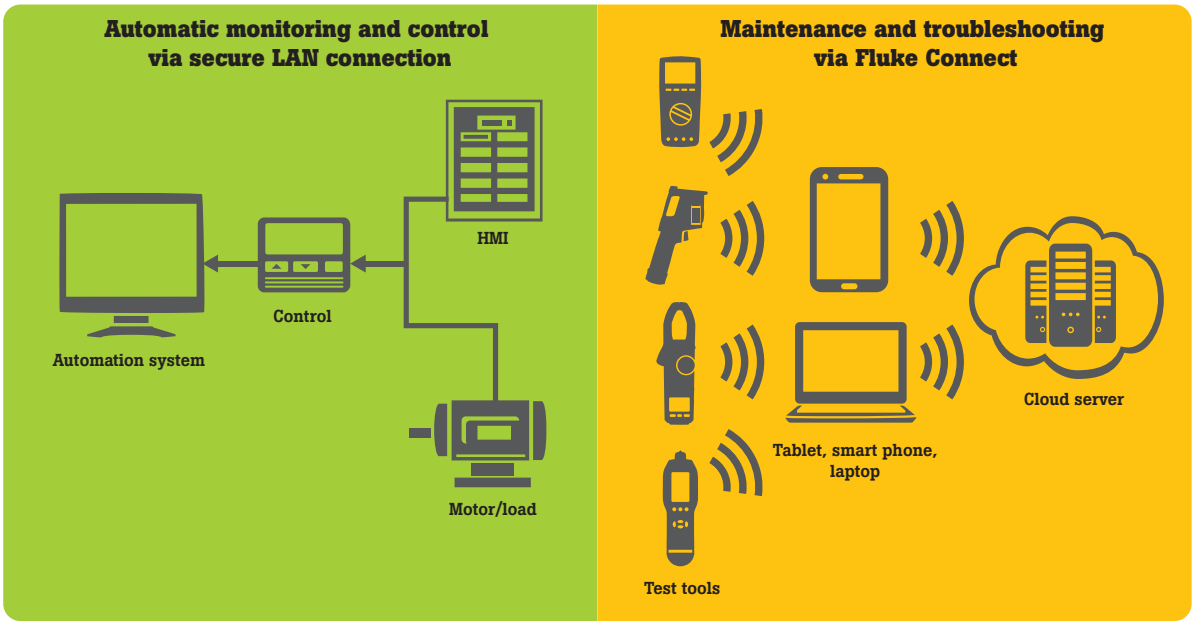
The development of Fluke Connect was shaped by two primary principles. The data needed to be:

- Safeguarded from malicious or accidental loss or changes
- Easily accessible to authorized team members, only

Fluke Connect is designed to support those two goals. This document outlines the measures Fluke has taken to make that happen and provides guidance on best practices for mobile app security.

Safeguarded by world class cloud security

Security breaches primarily occur when internal personnel inappropriately share information; more rarely, external entities gain access to the internal network. The largest security benefit of Fluke Connect is that it is completely separate from the end-user's internal network. The Fluke Connect app does not directly connect with internal systems, from SCADA to individual HMIs, and therefore cannot be used to manipulate those systems. The only primary contact Fluke Connect makes with local operations is in the form of handheld device measurements taken on non-networked components.



Fluke Connect collects measurements from non-networked equipment components and then uses its own network to securely transfer and store the data.

The measurement data collected through Fluke Connect is transmitted to Fluke Cloud™ storage using Transport Layer Security (TLS) encryption, a newer protocol than Secure Sockets Layer (SSL). Fluke Cloud™ storage is a virtual private cloud (VPC) hosted by a world class cloud provider on some of the most secure computing infrastructure on the planet. That infrastructure is designed and managed according to security best practices and complies with stringent security standards, including: SOC 1, 2, and 3; PCI DSS, FIPS 140–2, and ISO 27001.

ISO 27001 certification is a security management standard that specifies best practices and comprehensive security controls following the ISO 27002 best practice guidance. Our provider also has ISO 9001:2008 certification, which is a global standard for managing the quality of products and services.

In addition, multiple layers of server redundancy and database replication maintain high availability and help guard against accidental deletion of data.

Balancing security and access.
Fluke Connect allows workers to easily collect, access, and analyze measurement data they need to do their jobs. Whether they are troubleshooting, performing maintenance, or supervising others doing those jobs, this application helps increase efficiency and productivity.

At the same time, developers balanced that easy accessibility with the need for strong security so that only authorized team members could access data. To achieve that, Fluke Connect is architected so that the administrator for each team controls who has access to that team's data. The administrator is the first user within an organization to create a Fluke Connect account for that team. The administrator grants access to team members and can remove that access at any time. A team can designate more than one administrator and those administrative designations can be changed.

Accessing Fluke Connect data stored in the cloud requires password authentication. Only authorized team members can see, add, or change data related to their team. They cannot see, add to, or change data for other teams who store data to Fluke Cloud Storage.

Maintaining team integrity
If a team member leaves the team or the company, or loses the phone that holds the Fluke Connect application, the account manager can remove that individual from the team.

If a company-issued phone is lost, the Fluke Connect application and all cached data can be remotely wiped clean, if the company's IT administrator has that capability. In addition, any data cached on an iPhone is deleted from that phone every time the user signs out. However, any data from the phone that was stored in the cloud remains there. So when the user receives a new phone, he or she can reinstall Fluke Connect and access data using the updated password.

Validating security measures
Fluke regularly engages third-party penetration testing to assess the Fluke Connect infrastructure. This assessment includes testing network ranges, applications, and business processes. The results have shown no high risk security issues.

How to make the most of Fluke Connect security features
Fluke Connect supports many standard security features to safeguard against accidental data loss or unauthorized access. To make the most of those features, we recommend that administrators establish best practices for team members that include:

- Creating strong, individual passwords and requiring team members to change them often
- Logging out of Fluke Connect when finished
- Using company-issued smart phones that can be wiped remotely if lost
- Changing the password immediately via the Fluke Connect Web user interface if a phone is lost. When the company issues the user a new phone, the user can reinstall Fluke Connect and immediately access the team data with his new password.

FAQs on Fluke Connect Security

Q **How is the app data protected from hackers?**

A **Fl**uke 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 designed 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.

Q **How do I protect my operations systems from being compromised by this app?**

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 **Where is the data stored?**

A The data is stored on servers in secure data centers in the U.S.

Q **How is the availability of data guaranteed by this provider?**

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 **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 **Is the information collected by the Fluke Connect app secure?**

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 **Can I choose who gets to see my data?**

A The administrator chooses who to share data with. In Fluke Connect, the administrator can invite a team member via email. Typically, one person within an organization is designated the administrator and issues the team invitations, centralizing data sharing and access privileges. Once team members accept, then they can share data. With Fluke Connect, your data options are:

- Share data live among team members and not save it
- Save data to the cloud, unassigned to equipment or work order, where it is not visible to other team members
- Save data to the cloud, assigned to equipment for the team to see
- E-mail saved measurements to anyone, regardless of whether or not they are a team member

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.

Q **What happens to the data on the phone and in the cloud the moment a person leaves 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.

Have more questions?
We're happy to address any additional questions you may have on security measures related to the Fluke Connect app or Fluke Cloud™ storage. Please visit the fluke.com website for the region closest to you and contact our customer support group. We value your feedback and are committed to delivering a secure, wireless, measurement-data management solution.

Fluke. *Keeping your world up and running.*®

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

Fluke Europe B.V.
PO Box 1186, 5602 BD
Eindhoven, The Netherlands

For more information call:
In the U.S.A. (800) 443-5853 or
Fax (425) 446-5116
In Europe/M-East/Africa +31 (0)40 267 5100 or
Fax +31 (0)40 267 5222
In Canada (800)-36-FLUKE or
Fax (905) 890-6866
From other countries +1 (425) 446-5500 or
Fax +1 (425) 446-5116
Web access: http://www.fluke.com

Printed in U.S.A. 3/2015 6004793a-en