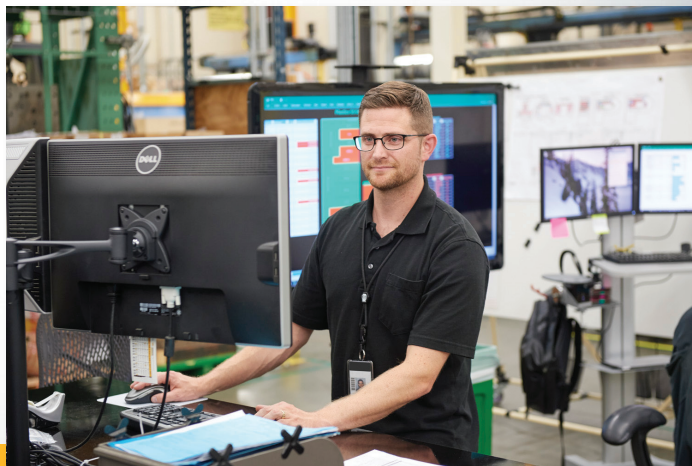


Fluke 3563- Sensor zur Schwingungsanalyse: IT und Sicherheit

FLUKE

Reliability

Häufig gestellte Fragen



Datenerfassung und -speicherung

F: Wo werden meine Daten gehostet und gespeichert?

A: Die Daten werden über AWS gespeichert.

F: Wie gewährleistet Fluke 3563 die Sicherheit von Daten im Ruhemodus?

A: Unsere Datenbank-Backups werden im Ruhemodus verschlüsselt.

F: Wie gewährleistet Fluke 3563 die sichere Datenübertragung?

A: Fluke gewährleistet die sichere Übertragung vertraulicher Daten durch Verwendung von TLS- und HTTPS-Protokollen.

F: Wie wird die Datenverfügbarkeit sichergestellt?

A: Unser Cloud-Anbieter stellt Fluke drei Arten von Service zur Verfügung:

1. Für Relational Database Service # (RDS) wird im Rahmen der Servicevereinbarung (SLA) ein monatlicher Verfügbarkeitsprozentsatz von mindestens 99,95 % sichergestellt.
2. Für Simple Storage Service wird im Rahmen der Servicevereinbarung (SLA) ein monatlicher Verfügbarkeitsprozentsatz von mindestens 99,9 % in jedem Abrechnungsmonat sichergestellt.
3. Für Elastic Compute Cloud wird im Rahmen der Servicevereinbarung (SLA) ein monatlicher Verfügbarkeitsprozentsatz von mindestens 99,95 % sichergestellt. Die Verfügbarkeit in der Fluke 3563-App kann variieren.

F: Wie lange bleiben die Dateien zu einem aktiven Konto verfügbar?

A: Im Rahmen der gegenwärtigen Geschäftsbedingungen des Dienstes verbleiben die Daten im System, bis Sie uns einen Löschauftrag erteilen. Fluke behält sich das Recht vor, die Dauer der Speicherung zu begrenzen.

F: Wie lange bleiben die Daten zu einem inaktiven Konto gespeichert (wenn sich z. B. ein Benutzer seit einem Jahr nicht angemeldet hat)?

A: Im Rahmen der gegenwärtigen Geschäftsbedingungen des Dienstes werden Daten zu inaktiven Konten nicht gelöscht, es sei denn, dies wird explizit vom Administrator angefordert. Fluke behält sich das Recht vor, die Dauer der Speicherung zu begrenzen.

Datensicherheit

F: Wer kann meine Daten einsehen?

A: Sobald Informationen für ein Teamkonto in die Fluke Cloud™ übertragen wurden, können die Daten nur von den Personen eingesehen werden, die vom Administrator entsprechende Zugriffsrechte erhalten haben. Der Administrator legt fest, wer Zugriff auf die Informationen dieses Teams hat. Auf diese Weise wird unbefugter Zugriff auf die Daten verhindert.

F: Wer ist dazu berechtigt, Kundendaten zu verwalten (erstellen, aktualisieren, löschen, herunterladen etc.)?

A: Gemäß der Lizenzvereinbarung für Endanwender ist Fluke der Eigentümer der Daten.

F: Wie wird die physische Sicherheit und Umgebungssicherung der Fluke 3563 Infrastruktur gewährleistet?

A: Unser Rechenzentrum ist cloudbasiert und wird über AWS verwaltet. Der Anbieter stellt Sicherheitsdokumente zur Verfügung, auf die wir verweisen können.

F: Wie werden die App-Daten vor Hackern geschützt?

A: Der Speicher von Fluke Cloud™ wird in einer cloudbasierten Infrastruktur gehostet, die als eine der sichersten heute verfügbaren Cloud-Computing-Umgebungen gilt. Unser Anbieter für Cloud-Dienste nutzt erstklassige Methoden zur elektronischen Überwachung, Systeme für mehrstufige Zugriffssteuerung und besetzt seine Rechenzentren rund um die Uhr mit Personal. Darüber hinaus verfügen die Server über integrierte Firewalls, verschlüsselte Datenspeicher und sichere Zugriffsmethoden, die speziell für den Datenschutz konzipiert wurden. Die Daten werden bei der Übertragung vom Smartphone in die Cloud und zurück verschlüsselt, um unbefugten Zugriff zu verhindern.

Identitäts- und Zugriffsverwaltung

F: Welche Richtlinien gelten für die Erstellung eines Passworts?

A:

- Mindestens 8 Zeichen
- Mindestens ein Großbuchstabe
- Mindestens ein Sonderzeichen

F: Was passiert, wenn jemand in meinem Team sein Smartphone verliert?

A: Um die Fluke 3563-App nutzen zu können, ist eine persönliche Anmeldung erforderlich. Keine der Informationen in der App oder in der Cloud sind ohne diese Anmeldung zugänglich. Wir empfehlen, für alle geschäftlich genutzten Smart Devices einen obligatorischen allgemeinen Anmeldecode zu verwenden und proprietäre Daten mit zusätzlichen Sicherheits-Tools und -Maßnahmen zu schützen. Benutzer haben auch die Möglichkeit, ihr App-Passwort über die webbasierte Oberfläche zu ändern, um unbefugten Zugriff durch eine Person zu verhindern, die möglicherweise in den Besitz des Telefons und des Passworts gelangt ist.

F: Was passiert mit den Daten auf dem Telefon und in der Cloud, wenn eine Person das Team verlässt?

A: Wenn ein Administrator eine Person aus dem Team entfernt, bleiben die Daten dieser Person innerhalb des Teams erhalten, einschließlich aller Daten, die bereits vor der Aufnahme in das Team erfasst wurden. Die Person hat keinen Zugriff mehr auf die Daten in der Cloud, und die Daten, die auf ihrem Telefon zwischengespeichert wurden, werden gelöscht, sobald die Person das nächste Mal versucht, eine Verbindung mit der Cloud herzustellen. Das noch bestehende Fluke 3563-Konto kann genutzt werden, um neue Daten in der Cloud zu speichern.

F: Kann ich mein Konto einfach sperren bzw. meine Daten löschen lassen, wenn mein Smartphone oder Passwort gestohlen wurde?

A: Wenn ein Smartphone verloren gegangen ist oder ein Passwort offengelegt wurde, kann der Administrator oder das Team-Mitglied, dem das Telefon zugewiesen ist, das Passwort sofort ändern. Wenn das Smartphone vom Unternehmen bereitgestellt wird, hat die IT-Abteilung des Unternehmens eventuell die Möglichkeit, alle Daten auf dem Gerät remote zu löschen, wodurch auch die Fluke 3563-App und die zwischengespeicherten Daten entfernt werden.

F: Wie werden Benutzer authentifiziert bzw. wie wissen wir, dass ein Benutzer berechtigt ist, das Programm zu nutzen?

A: Für die Benutzerauthentifizierung wird der Zugriff auf drei Ebenen gesteuert:

- IOT-Geräte verwenden SSL-Zertifikate, um mit unserem IOT-Endpunkt zu kommunizieren. Alle Daten werden mittels SSL verschlüsselt.
- Smartphones verwenden ein HTTPS-Zertifikat, um zu bestätigen, dass die Site, mit der kommuniziert wird, ein gültiges SSL-Zertifikat hat, und dass die Daten verschlüsselt sind.
- Webbrowser verwenden ebenfalls HTTPS/TLS, um mit den Back-End-Diensten zu kommunizieren und sicherzustellen, dass alle übertragenen Daten verschlüsselt werden.
- Anmeldedaten werden im Ruhezustand verschlüsselt gespeichert und können nur mit einem Passwort aus der Datenbank entschlüsselt werden.

F: Ist der Zugriff auf Fluke 3563 auch über Mobilgeräte wie Smartphones und Tablets möglich? Wenn ja, kann der Zugriff auf Firmengeräte beschränkt werden?

A: Derzeit besteht keine Möglichkeit, ein Konto an ein bestimmtes Gerät zu binden.

Condition Monitoring mit Fluke: Hardware-Sicherheit und Datenübertragung

F: Unterstützt Fluke 3563 die Multi-Faktor-Authentifizierung?

A: Nein, im Moment nicht.

F: Wie lauten die technischen Spezifikationen für die Datenübertragung?

Drahtlos-Technologie	WLAN <ul style="list-style-type: none"> • IEEE 802.11 ac/a/b/g/n • Sicherheit: WPA/WPA2-PSK • Übertragungsrate: 1 – 866,7 Mbps Kabelgebundenes LAN <ul style="list-style-type: none"> • Ethernet 1 Gbit/s Netzwerk allgemein (LAN + WLAN) <ul style="list-style-type: none"> • Protokolle: MQTT und HTTP mit TLS
Standard	IEEE 802.11 b/g
Zertifizierungen	FCC/CE/IC
Unterstützte Netzwerk-Sicherheitsprotokolle	Offen (kein Schutz) Verschlüsselung für Drahtlosnetzwerk (Wi-Fi Protected Assets II) <ul style="list-style-type: none"> • WPA-2 Personal (AES-256-Verschlüsselung für Datenpakete)
Übertragungsrate	1–11 Mbit/s mit IEEE802.11b
Empfängerempfindlichkeit	Nominal: weniger als -65 dBm Minimal: -83 dBm
Ausgangspegel	+12 dBm
Kanäle	1–14 mit 5 MHz-Intervallen (Standard: Kanal 6)
Anwendungsprotokoll	Paketbasiertes proprietäres Protokoll
Verschlüsselung	AES-256 mit Generierung von 384-Bit-ECC-Schlüssel
Integrität und Unverwechselbarkeit	Geschützt durch Signatur-Hash-Algorithmus auf mehreren Ebenen

F: Kann jemand das Gateway hacken und von dort aus auf mein Netzwerk zugreifen?

- A:**
- Über Bluetooth: nein. Das Gateway hört nur auf Advertisement-Nachrichten. Es ist nicht möglich, eine Bluetooth-Verbindung mit dem Gateway herzustellen.
 - Über WLAN oder LAN im normalen Betriebsmodus: nein. Das Gateway bietet keinen Service, auf den zugegriffen werden kann. MQTT ist ein Publish-Subscribe-System, und das Gateway ist immer Subscriber.
 - Über WLAN im Hotspot-Modus: nein. Der Hotspot-Modus ist nur aktiv, wenn das Gateway nicht mit ADP verbunden ist. Während der Bereitstellung ist physischer Zugriff auf das Gateway erforderlich, weil SSID und Passwort auf dem Typenschild des Gateways abgelesen werden müssen. Individuell je nach Gateway. Und das Gateway bietet über Hotspot nur http-REST-Endpunkte, die mit einem speziellen Vulnerability Scanner auf Sicherheitslücken hin überprüft wurden.

F: Können sich unbefugte Personen mit dem 3563-Gateway verbinden? Ich habe Bedenken, dass Angriffe während einer Monitoring-Sitzung möglich sind und dadurch Datenverlust entsteht.

- A:** Nein. Das Gateway verbindet sich über MQTTS mit ADP. Es gibt keinen Service, mit dem eine Verbindung im normalen Betriebsmodus möglich ist.

F: Werden die Daten bei der Übertragung verschlüsselt? Ich habe Bedenken, dass sich jemand unbefugten Zugriff auf eingeschränkte/vertrauliche Instandhaltungsdaten verschafft oder dass diese beschädigt werden.

- A:**
- Die Daten werden bei der Übertragung zwischen Gateway und Cloud per TLS verschlüsselt.
 - Der Sensor wird mit dem Gateway verbunden. Es ist nicht möglich, dass sich ein anderes Gerät mit dem Sensor verbindet und Daten abfängt.

F: Welche Art von Netzwerkzugriff ist für den Betrieb des Sensors erforderlich?

- A:**
- LAN- oder WLAN-Verbindung zum lokalen Netzwerk mit Internet-Zugang (für das Gateway erforderlich).
 - Es gibt keine eingehende Verbindung, nur ausgehende Verbindungen mit MQTTS (Port 443) im normalen Betriebsmodus und mit HTTPS (Port 443) für Software-Updates per OTA.

F: Wie hoch ist die Datenübertragungsrate?

- A:**
- Standardkonfiguration Screening (3 Achsen, allg. Beschleunigung + Geschwindigkeit + Temp.) ~ 1,8 kByte
 - TWF für Berechnung der Bereichswerte für alle drei Achsen ~ 440 kByte
 - Signalstatus Sensor ~ 230 Byte
 - Gateway-Update-Paket: bis zu 180 Mbyte
 - Sensor-Update-Paket: 450 kByte

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

Weitere Informationen erhalten Sie telefonisch.

USA: 856-810-2700
Europa: +353 507 9741
Großbritannien: +44 117 205 0408
E-Mail: support@accelix.com
Website: <http://www.accelix.com>

©2021 Fluke Corporation. Spezifikationen können ohne vorherige Ankündigung geändert werden.
06/2021 6013904b-de

Eine Änderung dieses Dokuments ist ohne die ausdrückliche schriftliche Genehmigung der Fluke Corporation untersagt.