NEW!

COMARK
A Fluke Company

Diligence™ Cloud

Security Overview

20714-1 | February 2022

Diligence™ Cloud

COMARK
A Fluke Company

Introduction

We have designed this document as supporting material, for those, such as corporate IT departments or technical personnel, charged with investigating or implementing a Comark WiFi Monitoring System, including the Diligence Cloud data storage and management platform.

It sets out the technology and infrastructure in place as well as the data protection mechanisms in place. The information contained herein will be directly relevant to those charged with ensuring the continued security of your own systems.

Our Service Provider

The Comark Diligence Cloud data storage and management platform is managed by an approved, UK based third-party supplier.

All access to the Diligence Cloud database as well as to customer information is strictly controlled.

All procedures and work are carried out in accordance with the guidelines of the UK Data Protection Act 1988 and EU General Data Protection Regulation (GDPR).

Any Questions?

Get the answers from our team of experts

comarkinstruments.com/temperature-monitoring-system-enquiry/

Diligence Cloud

COMARK
A Fluke Company

Server & Network Provider

The Diligence Cloud is currently hosted on a dedicated 'bare metal' server provided by OVH Cloud in London (UK). OVH act as an infrastructure-as-a-service (IaaS) supplier to our service provider. They provide all the network connectivity, routing, firewalling, as well as the physical server.

OVHcloud

The 'bare metal' hardware provided by OVH, has been customised to our service provider's specifications and they configure and manage all installed software, including BIOS/UEFI, RAID, Operating System (OS), and the Diligence Cloud software stack (Nginx, PHP, MariaDB). OVH has no access to the server other than purely physical access.

Our server and network provider (OVH) carries the following certifications for all their data centers, including the London (UK) data center which we are currently hosted in:

- ISO/IEC 27001:2013, 27701:2019, 27017, 27018
- CSA Star Level 1,
- SOC I-II Type 2

Should we expand to use additional 'bare-metal' solutions in other OVH data centers in the future, then additional compliance coverage is available to us, such as HIPAA in the USA and HDS in France.

For more information, please refer to OVH:
https://www.ovhcloud.com/en-gb/enterprise/certification-conformity/

OVH Limited
Becket House
1 Lambeth Palace Road
London SE1 7EU

Registered in England as 05519821

OVH Limited is a subsidiary of OVH Groupe SAS, a company registered with the Lille company registry under the number 537 407 926 sise 2, rue Kellermann, 59100 Roubaix (France).

More information about OVH's Data Processing Agreement (DPA) can be found here - https://www.ovh.co.uk/personal-data-protection/

For the purposes of data processing, our service provider utilises services from both OVH Limited (UK) and OVH Groupe SAS (France), therefore both companies may need to be listed/considered.

Our Service Provider is a member of the OVH Partner Programme.

CDN & Security Provider

All Diligence Cloud customer-facing traffic passes through our Content Delivery Network (CDN) which is provided by a third-party provider, Cloudflare.

Cloudflare also provides the security (WAF, Anti-DDoS) and performance services which we utilise for the Diligence Cloud.

Cloudflare carries the following certifications:

- ISO/IEC 27001:2013, 27701:2019
- SOC 2 Type II

Further compliance information can be found here:
https://www.cloudflare.com/trust-hub/compliance-resources/

More information about Cloudflare's GDPR policies can be found here:
https://www.cloudflare.com/en-gb/gdpr/introduction/

This solution is provided by

Cloudflare Limited
County Hall
The Riverside Building
Belvedere Road
Westminster Bridge Road, 6th Floor,
London
SE1 7PB

Registered in England as 08778322

Cloudflare Limited is a subsidiary of Cloudflare, Inc. 101 Townsend St., San Francisco, CA, 94107 (USA).

Our service provider is a Cloudflare certified and Cloudflare optimised partner.

Diligence™ Cloud

COMARK
A Fluke Company

Back-Up Storage

Our service provider currently utilises a number of back-up solutions and for our Diligence Cloud, the primary off-platform backup of both files and database will be Google Cloud Storage.

Google Cloud Storage

Where possible, data will be located in European locations, which includes the UK and several EU countries.

Should the platform evolve to include international servers we may look to utilise additional locations in order to keep data in the same country as the customer.

GDPR, compliance and certification information for Google Cloud services is available here:

https://cloud.google.com/privacy/gdpr
https://cloud.google.com/security/compliance

Secondary backups which may contain personally identifiable information (PII), such as those made for testing or during development, may be stored in a number of additional locations, which can include:

- Service Provider Office NAS (UK)
  Protected with firewall and IPS/IDS, Physical protection by means of CCTV, monitored alarm, and shutters/railings on windows & doors.

- Service Provider Staff Computers
  Data Encrypted at rest via FileVault with T2 Secure Enclave.

- Google Drive (via Google Workspace) - (EU)
  Protected with mandatory two-factor authentication for all users.

Diligence™ Cloud

COMARK
A Fluke Company

Code Storage, Integrity & Continuous Integration (CI/CD)

The Diligence Cloud backend, frontend, and device API source code is version-controlled using Git, hosted in a private GitHub repository under the service provider's organisation.

The Git repository contains all source code and compiled code, including example configurations and set-up documentation.

The Git repository also stores a history of all changes, including what was affected, when the changes were made, and who the changes were made by. This includes the service provider developer's name, email address, and in some cases a digital signature (GPG).

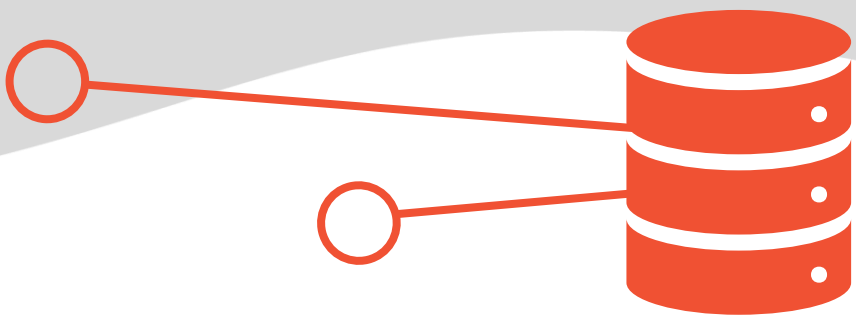
The git repository does not contain any personally identifiable information (PII) related to customers, such as passwords, keys, tokens, production configuration files, or database data other than empty database structure migrations.

GitHub's Data Protection Agreement (DPA) can be found here:
https://docs.github.com/en/github/site-policy/github-data-protection-agreement

GitHub's Continuous Integration (CI) service (GitHub Actions) is utilised for monitoring code quality, vulnerability scanning, and testing changes. Third-party services such as Dependabot and Snyk are used for automated code and vulnerability analysis.

Our service provider mandates that all developer accounts use two-factor authentication (2FA) in order to access the repository.

Releases to the development or production platforms are additionally restricted to 'signed commits', which requires a service provider developer to have access to a physical security key (hardware token) in order to 'sign' the code and approve the deployment. Automations then run to deploy this code to the server (Webhooks). A log of these deployments is kept in GitHub.



Diligence Cloud

COMARK
A Fluke Company

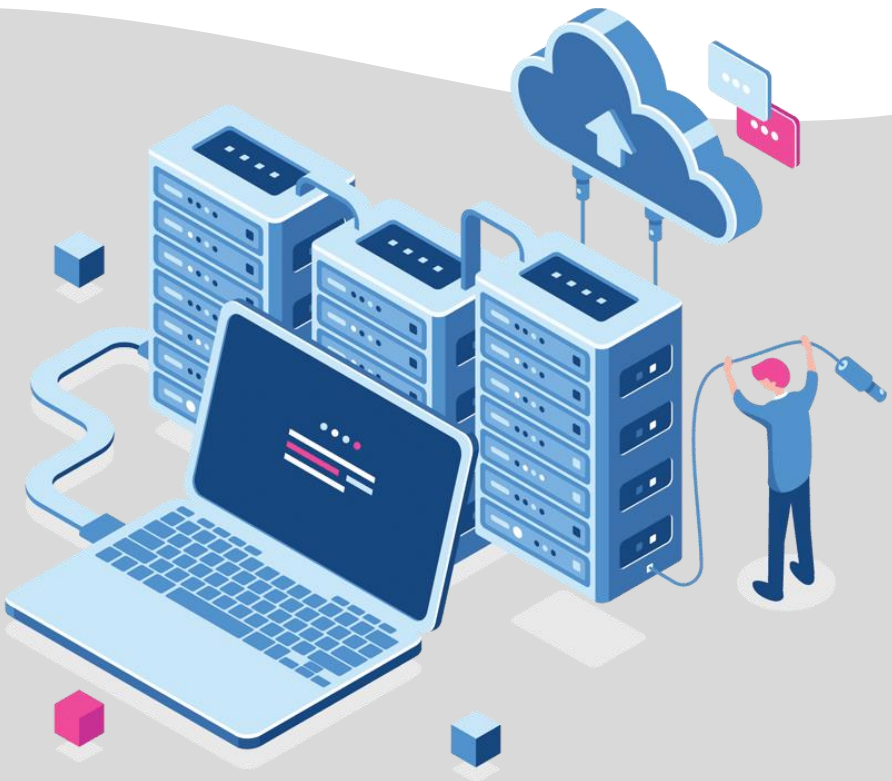
Back-Up Storage

The Diligence Cloud stack and infrastructure is monitored using a third-party solution provided by New Relic. Our server and software utilises a combination of monitoring agent software packages, which record and transmit data to New Relic for analysis and alerting purposes.

New Relic®

The system regularly transmits analytical data, such as request counts, timings, hardware utilisation, network connections, and other key performance indicators (KPIs) which are used internally by our service provider to uphold any support contract and related service level agreements (SLAs). In the case of an error with the system, error traces including request and response information, stack traces, error messages, and affected source code may be transmitted to New Relic, in order to provide error analysis and alerting.

Where possible, any secrets (i.e. passwords or tokens) are scrubbed from data server-side before being transmitted to New Relic.



New Relic Data Processing Addendum FAQ:
https://newrelic.com/termsandconditions/dataprotectionFAQ

Diligence™ Cloud

COMARK
A Fluke Company

Off-Platform Logging & Log Retention

The Diligence Cloud stack and server generate log data during normal operation. At a server level, this can include information about running services, maintenance events, system errors, and access attempts.

At a software level, the Diligence Cloud logs information about back-end errors, and in some cases verbose information from the device API, including all commands transmitted and received from a Comark WiFi Transmitter. Log files retrieved from a Comark WiFi Transmitter in the event of an error are also included. This data includes IP addresses, MAC addresses, serial numbers, firmware versions, commands, responses and errors. This includes the 'status' response from each Transmitter, which in newer firmware versions can include the WiFi SSID.

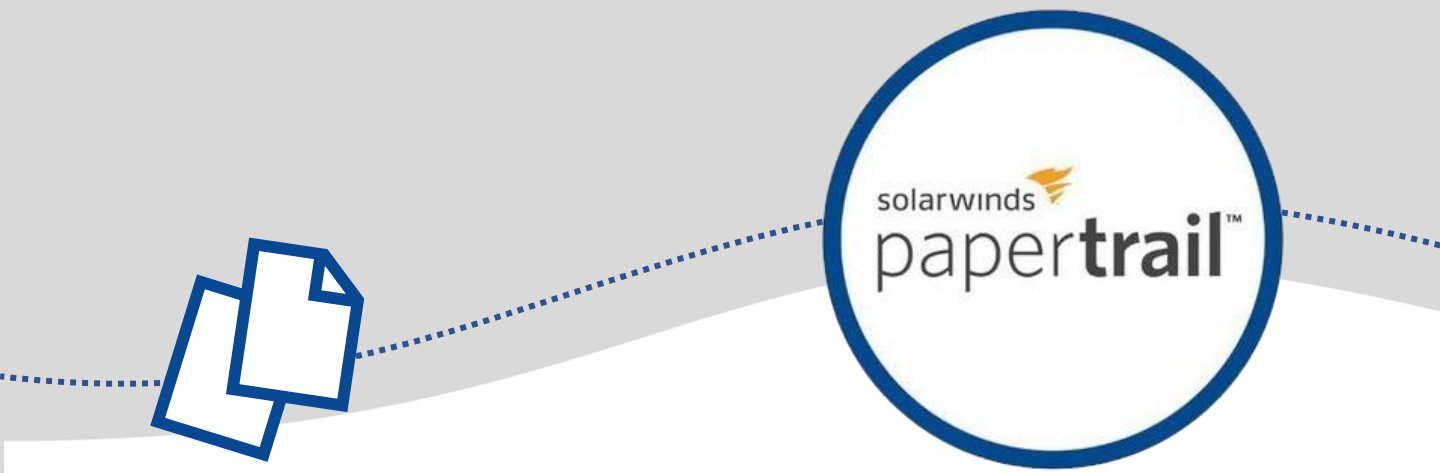
These logs are retained on the server, and also transmitted to a third-party log service Papertrail provided by SolarWinds. Off-platform logging allows better security information and event management (SIEM) in the case of a security incident. The logs cannot be erased by the server or an attacker. In addition to log retention, our service provider team utilises Papertrail to view and search converged logs, when troubleshooting an issue.

Alerting rules are applied through Papertrail to send early warnings to the Service Provider team when certain log entries are found.

In some instances, log data may contain personally identifiable information (PII) where the log entry is the result of an error during registration or login, for example. User passwords are never logged (to disk or otherwise).

For information about Papertrail's compliance and data protection, please refer to the SolarWinds Trust Centre:

https://www.solarwinds.com/trust-center

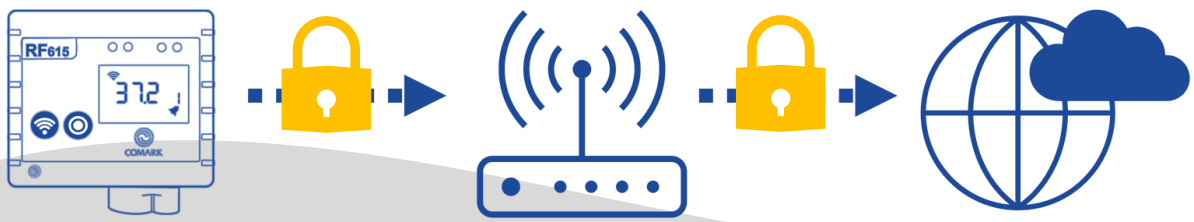


Data Storage & Security of Data in Transit

All data including any personally identifiable information (PII), such as user account details, is stored in the Diligence Cloud database which resides on a server in London (UK).

All data is encrypted (TLS/HTTPS) between the user browser (Client) and our Cloudflare content delivery network (CDN), where it is decrypted for processing (at the CDN Edge). It is then re-encrypted (TLS/HTTPS) when sent back from Cloudflare and our back-end (Origin) server.

Data between Comark WiFi Transmitters and the Diligence Cloud Device API is communicated over a TLS socket, using self-signed certificates with two-way TLS (both server and client certificates are used). Certificates for Comark WiFi Transmitters (Diligence 600) have been issued by our service provider to our specification and are backed by a self-signed CA certificate which resides on a hardware security module (HSM) owned by our service provider.



Data at rest on the server is not encrypted at this time. There is reliance here upon OVH's security certifications to provide physical protection to the data centre, server, and storage systems to prevent access to data at rest.

End user Diligence Cloud passwords are hashed using Argon2 (Argon2i/Argon2id) before being stored in the database. No user passwords are stored in plain text.

Security mechanisms such as key-based authentication are in place to limit access to the server and protect the data at rest from remote access.

Diligence™ Cloud

COMARK
A Fluke Company

Off-Platform Logging & Log Retention

The Diligence Cloud stack and server generate log data during normal operation. At a server level, this can include information about running services, maintenance events, system errors, and access attempts.

At a software level, the Diligence Cloud logs information about back-end errors, and in some cases verbose information from the device API, including all commands transmitted and received from a Comark WiFi Transmitter. Log files retrieved from a Comark WiFi Transmitter in the event of an error are also included. This data includes IP addresses, MAC addresses, serial numbers, firmware versions, commands, responses and errors. This includes the 'status' response from each Transmitter, which in newer firmware versions can include the WiFi SSID.

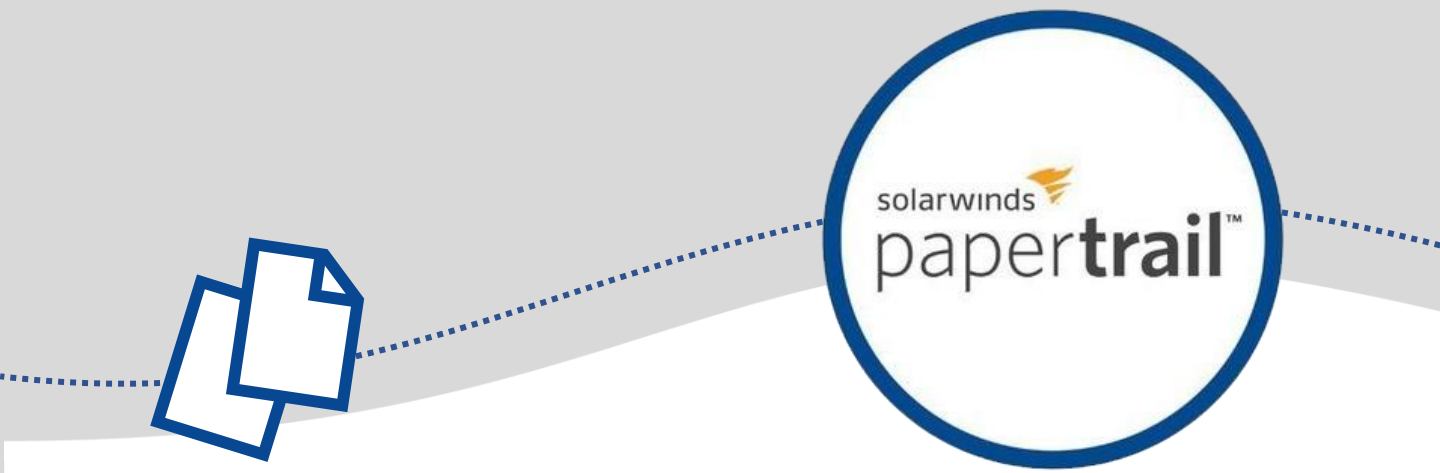
These logs are retained on the server, and also transmitted to a third-party log service Papertrail provided by SolarWinds. Off-platform logging allows better security information and event management (SIEM) in the case of a security incident. The logs cannot be erased by the server or an attacker. In addition to log retention, our service provider team utilises Papertrail to view and search converged logs, when troubleshooting an issue.

Alerting rules are applied through Papertrail to send early warnings to the Service Provider team when certain log entries are found.

In some instances, log data may contain personally identifiable information (PII) where the log entry is the result of an error during registration or login, for example. User passwords are never logged (to disk or otherwise).

For information about Papertrail's compliance and data protection, please refer to the SolarWinds Trust Centre:

https://www.solarwinds.com/trust-center



Firewall Access

The use of a fully qualified domain name (FQDN) is preferable to using the Diligence Cloud IP address, as it allows changes to servers/infrastructure without breaking your firewall configuration.

We would recommend allowing the following:

For Transmitter Connections (M2M / Device API) - single port:

- **Name:** Diligence Cloud Device API
- **Type:** TCP
- **Port:** 8080
- **Destination (FQDN):** ingress-api.comarkinstruments.net
- **Use:** Transmitters open outbound TCP connections to send and receive TLS-encrypted data including time, recordings, alarms, settings and firmware updates.
- **Note:** TLS is two-way using both client and server certificates, and the communication format is proprietary. Firewalls and content filters that intercept TLS traffic should not do so on this port. There is no human-readable service on this port.

For the Web Front-End (Dashboard) - two ports:

- **Name:** Diligence Cloud Dashboard HTTPS
- **Type:** TCP + UDP
- **Port:** 443 (HTTPS)
- **Destination (FQDN):** diligence.cloud
- **Use:** Web based front end for accessing transmitter data over HTTPS using TLS 1.2/1.3
- **Note:** TCP is used for HTTP/1.1 and HTTP/2 connections, UDP is used for HTTP/3 (QUIC) connections in supported browsers.

- **Name:** Diligence Cloud Dashboard HTTP (Redirect)
- **Type:** TCP + UDP
- **Port:** 80 (HTTP)
- **Destination (FQDN):** diligence.cloud
- **Use:** Web based frontend for accessing transmitter data; redirects to HTTPS version on port 443.
- **Note:** All web traffic on this port will be redirected to the HTTPS service where HSTS is enforced, however HTTP should be allowed where possible to ensure users can access the site without typing the URL scheme the first time they use the Diligence Cloud.

The above should allow access through a Firewall. It is anticipated that most companies already allow 80 and 443 outbound with content scanning / IDS thus customers with firewalls or next-gen firewalls (NGFW) will only need to configure port 8080 for the device API.

Firewall Access (continued)

The Diligence Cloud web front-end connects to a number of external third-party services for performance monitoring and error reporting.

This list is subject to change, but is currently as follows:
(all services accessed over HTTPS, port 443)

- help.comarkinstruments.net - Diligence Cloud Help Guide Content
- www.comarkinstruments.net - Diligence Cloud Licensing (Global) and Comark E-Commerce Account Management (UK Only)
- support.comarkinstruments.net - Comark Instruments Support Desk (Ticketing System)
- gambitnash.report-uri.com - Content Security Policy (CSP) Violation Reporting and Monitoring
- js-agent.newrelic.com – New Relic Application Performance Monitoring (Script)
- bam.nr-data.net – New Relic Application Performance Monitoring (Data endpoint)
- browser.sentry-cdn.com - Sentry Application Error Reporting (Script)
- *.ingest.sentry.io (eg. o132413.ingest.sentry.io) - Sentry Application Error Reporting (Data endpoint)

Additional Useful Information:
- Transmitters can operate on separate VLANs to users, as they do not communicate directly with the browser (only to the Diligence Cloud Device API)
- Transmitters can operate in device-isolated networks, as they do not inter-communicate
- MAC address filtering (allow lists) can be used, by getting the MAC address of the transmitter from "AP Mode".

From a security perspective, we advise that transmitters are on their own VLAN with device isolation, MAC filtering, and only have outbound access to ingress-api.comarkinstruments.net as described above would be most secure - for both the customer/end-user and for the transmitters, as this will protect your network from a malicious transmitter (a number of attack vectors this could be) and in turn would protect the transmitter from other devices on the customer's network (even simple things like pings and port scans, which could slow down the radio session when the WiFi is active).

Other Information

User Passwords

Passwords for Diligence Cloud user accounts must be at least eight characters long and must contain a number, an upper-case letter and a special character. Passwords for access to the servers are independent to that of users.

Data Deletion

Should a customer decide to close their Comark Diligence Cloud account, their data, including full account details, will be permanently deleted from the Comark Diligence Cloud database. Once data has been deleted from the Diligence Cloud database, it is not possible for it to be recovered beyond that of a backup.

Auto Logout

After signing in to the Comark Diligence Cloud no activity is detected on a user account, the user will be automatically logged out. Each user can individually configure the auto logout interval from the following selection: 15, 30, 60 or 120 minutes.

Data Transmission

All user access to the Diligence Cloud is using HTTPS, an encrypted version of HTTP. Only port 8080 is available for HTTPS communications. HTTPS data uses TLS encryption methods. Our (Diligence 600) WiFi Transmitters do not serve a web page and will not respond to any request on any port other than required by essential network services (DHCP) and will not respond to requests on typical HTTP ports 80.

Our WiFi Transmitters will turn their radio off between WiFi transmissions and will not respond to communication. When the Transmitter is ready to send logged data to the Diligence Cloud it will enable the radio, re-establish connection to the WiFi network and initiate a TCP connection on port 8080 to the Diligence Cloud. The Diligence Cloud never initiates, polls or pings any connection to the Transmitter.

Our WiFi Transmitters do require a DNS service and will use the DNS service IP address as directed by DHCP to resolve the URL https://ingress-api.comarkinstruments.cloud Port 8080.

WiFi Transmitters

Our (Diligence 600) WiFi Transmitters are 2.4GHz WiFi (IEEE 802.11b/g/n) compatible and support the WPA-2 personal WiFi encryption and authentication method.

All information such as access point passwords are stored securely in our WiFi Transmitters and it is not possible to read out such information.

Comark Instruments
P.O. Box 500
Beaverton, OR 97077, USA
Tel: +1 (503) 643 5204
Toll Free: (800) 555 6658
Email: sales@comarkUSA.com

Comark Instruments
52 Hurricane Way
Norwich, Norfolk, NR6 6JB
United Kingdom
Tel: +44 (0) 207 942 0712
Email: sales@comarkinstruments.com