TECH PAPER

Watchman Platform IT Requirements – Azure

Azima DLI, a Fluke Reliability Company, is committed to providing a safe and secure environment for all product applications hosted in the Microsoft Azure cloud environment.

Brief Summary:

This document is intended for company IT professionals to understand the security, setups and configurations required for connecting to WATCHMAN hosted programs. This document covers IT Security Protocols for the WATCHMAN Data Center Infrastructure, Security and Protection of WATCHMAN Data, and connecting to or accessing the WATCHMAN sites and services, including: This document covers:

- WATCHMAN Reliability Portal™ Web Pages (User Portal)
- ExpertALERT™ Cloud Subscription (EA-C)
- Online Wireless Vibration Sensor and Mesh Network (Accel Wireless)
- Online System Data Transfer (Message Queuing)
- Database Synchronization to WATCHMAN Data Center (WATCHMAN Sync Utility)

Program Component IT Requirements – Microsoft Azure

Web Access:

Your web subscription provides full access to your plant's machine health and program statistics through a Secure Socket Layer (SSL) encrypted Internet connection to the SIAI Azure Cloud Servers. A pre-assigned user name and strong password are required. User passwords are managed by the customer.

Access to your securely encrypted data requires:

- **Outbound Internet connections via ports 443 (HTTPS)**
  - **IP Address: 20.49.172.200**
- **Supported browsers: Microsoft Internet Explorer 11, Google Chrome, Microsoft Edge. Other browsers may function but are not tested or directly supported.**

WATCHMAN Reliability Portal Web Page Access:

The Portal web subscription provides full access to your plant's machine health and program statistics through a Secure Socket Layer (SSL) encrypted Internet connection to the SIAI web servers. A pre-assigned user name and strong password are required. User passwords are managed by the customer.

Access to the WATCHMAN Reliability Portal requires:

- **Outbound Internet connections via ports 443 (HTTPS)**
  - **IP Address: 13.66.252.42**
  - **URL: https://expert.watchmanportal.com/eavweb/desktop/logon.aspx**
- **Supported browsers: Microsoft Internet Explorer 11, Google Chrome, Microsoft Edge. Other browsers may function but are not tested or directly supported.**
  - **User link: https://expert.watchmanportal.com**

ExpertALERT Cloud-subscription – Terminal Service Web Access:

ExpertALERT Cloud-subscription (EA-C) provides full access to your machine vibration data through a Remote Desktop connection natively built into most Microsoft operating systems and an .RDP file supplied from the Portal website. EA-C is accessed through a remote Windows Terminal Services session. To access this session, one must also establish a secure VPN tunnel and use Multi-factor Authentication (MFA) to establish a session.

Sophos VPN client

To secure the connection between end users and their data, a VPN tunnel needs to be established. Each end user will need to install the Sophos VPN client on their computer and install the MFA agent on an android, Apple or desktop simulator.

The Sophos SSL VPN client uses AES 128 based encryption with SHA2 256 based authentication.

Access to ExpertALERT Cloud-subscription via Remote Terminal Session require:

- **Outbound VPN connectivity then (Terminal Services Web Access) via Sophos VPN Tunnel**
  - **IP Address: 13.66.252.42 (VPN connection)**
  - **Computer: 10.10.10.21 (Terminal Server connection)**

Online Wireless Vibration Sensors and Mesh Gateway Network:

Azima DLI supports a Wirepas Mesh Network vibration sensor system manufactured for SIAI by Treon of Finland. These high-resolution vibration sensors and pre-configured to communicate with the Watchman platform and Portals.

- **The gateway requires internet access for data transfer, system configuration and occasional firmware updates**
- **The gateway is Wi-Fi capable and has a built in ethernet port for WLAN/LAN configurations, and accommodates a SIM card for a cellular network data connection option**
- **If using Ethernet or Wi-Fi, direct access to the internet must be allowed by the network**
- **For LAN or WLAN firewall configuration, HTTPS traffic on TCP port 443 and MQTT traffic on port 8883 must be allowed**

WATCHMAN Online System Data Transfer:

Vibration and process data that is collected on-site with online data acquisition systems is transferred to the WATCHMAN Data Center through Microsoft Message Queuing and encrypted though SSL.

This data is transmitted using Microsoft Message Queuing (MSMQ):

- **Outbound Internet connections via ports 443 (SSL)**
  - **IP Address: 13.66.252.42**
  - **URL: https://expert.watchmanportal.com**
- **Note:** *SpriteMAX™ systems that use Windows XP will not be able to utilize this portal.*

WATCHMAN Database Synchronization – WATCHMAN Sync Utility:

Vibration data that is collected with portable data collectors (TRIO®) is transferred to the WATCHMAN Data Center through a Sybase Data Replication Engine. The data collectors have a Windows operating system; however, these data collectors do not need to be part of your domain or network, but need to periodically reach the Internet to transfer data to the data center.

Data is transmitted and received by ***encrypted message files*** using Secure File Transfer Protocol (FTPS) to the WATCHMAN Data Center:

- **Outbound Internet connections via ports 1750-1761 and 64,000-64,099 (FTPS)**
  - **IP Address: 13.66.252.42**
  - **Dedicated, Secure FTP server ftps://expert.watchmanportal.com**

Alternative Method to Database Synchronization – Replication Batch Transfer:

If secure FTP is not possible, databases can be synchronized using traditional batch replication. In these cases, a replication batch file will be provided which are configured with standard FTP protocols.

- **Outbound Internet connections via ports 20, 21 (FTP)**
  - **IP Address: 13.66.252.42**
  - **Dedicated FTP server ftps://expert.watchmanportal.com**

Alternative Method to Database Synchronization – Survey File Transfer:

Non-replicating systems can use the Survey Transfer File Exchange systems to transfer to the WATCHMAN Data Center through Microsoft Message Queuing and encrypted though SSL.

This data is transmitted using Microsoft Message Queuing (MSMQ):

- **Outbound Internet connections via ports 443 (SSL)**
  - **IP Address: 13.66.252.42**
  - **URL: https://expert.watchmanportal.com**

How Azima DLI Protects Your Data

Introduction

The security of customer data is of the highest priority to Azima DLI.

The WATCHMAN Portal infrastructure was designed to provide a secure environment for the database(s) and database servers that that make up the WATCHMAN Portal system.

The figure below shows the Data Center where customer data is hosted and the connections to it.

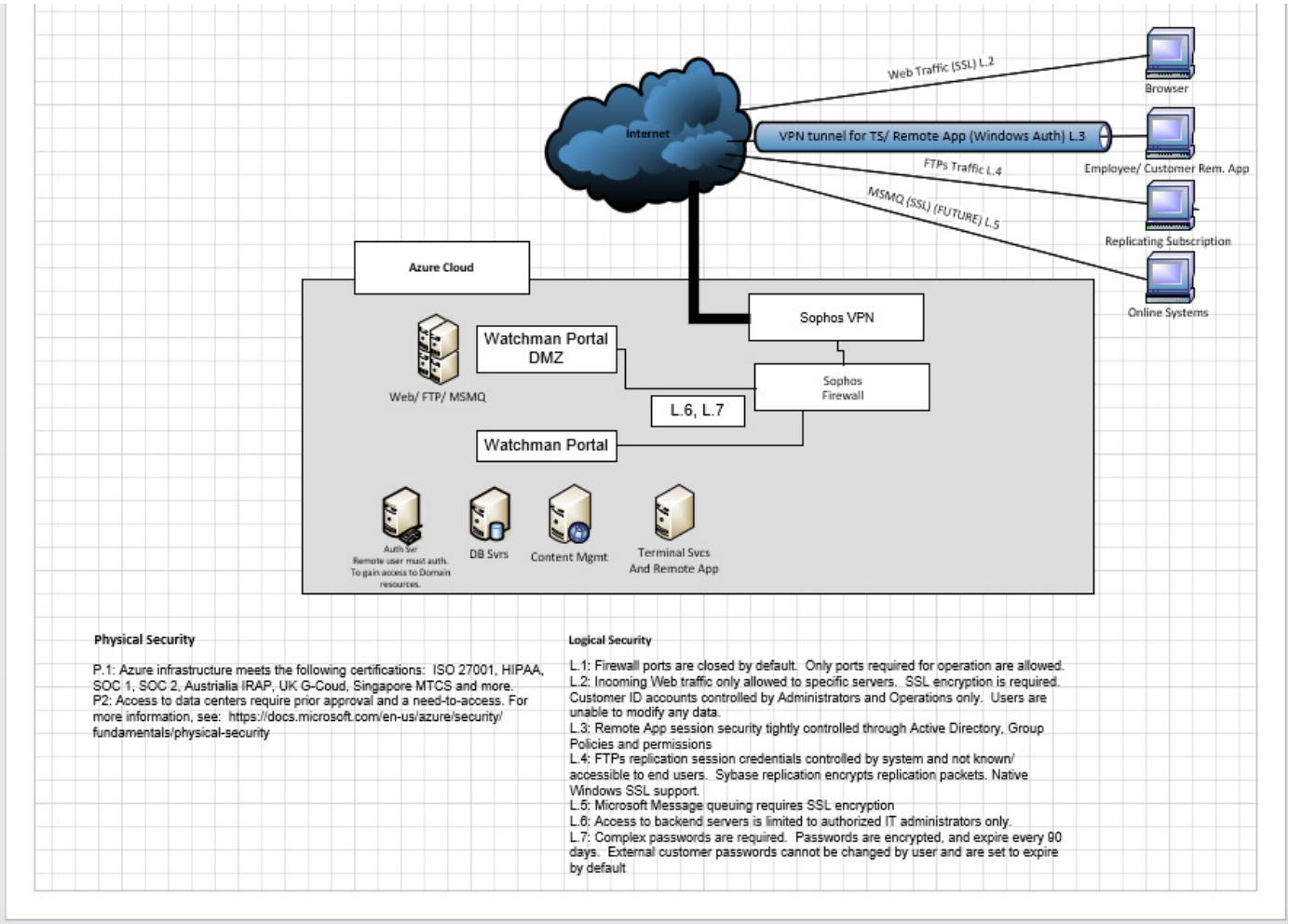


FIGURE 1: WATCHMAN Infrastructure Security Features

Physical Security

The Azima DLI servers are currently located in the West US 2 region. A region is a set of datacenters that is interconnected via a massive and resilient network. The network includes content distribution, load balancing, redundancy, and encryption by default.

Azure regions are organized into geographies. An Azure geography ensures that data residency, sovereignty, compliance, and resiliency requirements are honored within geographical boundaries.

Geographies allow customers with specific data-residency and compliance needs to keep their data and applications close. Geographies are fault-tolerant to withstand complete region failure, through their connection to the dedicated, high-capacity networking infrastructure.

Availability zones are physically separate locations within an Azure region. Each availability zone is made up of one or more datacenters equipped with independent power, cooling, and networking. Availability zones allow you to run mission-critical applications with high availability and low-latency replication.

This is common with all Azure systems. For more information, please see:

https://docs.microsoft.com/en-us/azure/security/fundamentals/physical-security

The region and its data centers have the following certifications:

- ISO 27001
- HIPAA
- SOC 1 and SOC 2
- Australia IRAP
- UK G-Cloud
- Singapore MTCS and more.

See the following for more standards that the Azure platform adheres to:

https://docs.microsoft.com/en-us/microsoft-365/compliance/offering-home

Logical Security

The following safeguards are in place to ensure that only authorized users or systems can access the WATCHMAN Portal database servers. Please see Figure 1 (above) for additional information.

In addition to the logical security features depicted in Figure 1, the Sophos Firewall has specific features to help protect the system and its data.

Firewall Security

- The firewall is responsible for port security for the system.
- Ports are closed by default. Only ports required for operation are allowed. Incoming web traffic is only allowed to specific servers.
- Advanced firewall protections are enabled and intrusions are logged and dropped.
- VPN encryption methods Secure Socket Layer with Multi-factor authentication
- Idle external connections are terminated after 30 minutes.

Web Server & Database Security

The web server and database servers have security protocols in place for protection.

Web Server Security

The web server has been hardened and only has applications installed that are required to operate the system. SSL is required to access the server through a web browser. Only ports required to operate the system are allowed. There are no file shares on the web server.

Database Security

Direct access to customer databases or database servers is limited to system administrators and certain analysts. Default admin passwords are restricted. ODBC connections are tightly managed and individual credentials are required. Replicating subscription credentials are masked by Sybase. Firewalls between edge servers and the database server are configured to only allow specific ports.

Data Loss Prevention

All databases are backed up nightly. In the unlikely event of catastrophic data loss, SIAI IT engineers are able to restore the previous night's backup. Monthly backups are kept off-site.

System Maintenance Policy & Procedures

Only authorized SIAI IT personnel are responsible for maintaining the entire SIAI IT infrastructure. Only authorized IT Administrators have access to these systems, as needed, to perform their jobs. A vast majority of the maintenance must be performed off hours, so remote maintenance is allowed.

System Audits

- Where applicable, Azima DLI has commissioned audits by reputable third-party vendors to confirm its security protocols provide sufficient protection.
- **SOC-2 Audit** – Not Applicable. No personal or financial information is stored at the Data Center.
- **Vulnerability Assessment** – Third-party assessment found that perimeter controls implemented by SIAI provide adequate protection of sensitive customer information against an Internet-based attacker. All findings/ recommendations from that assessment have been addressed and maintained:
  - Use of weak or default passwords prohibited.
  - Deploy missing security patches to all systems.
  - Implement secure encrypted solutions to minimize exposure on webpage.
  - Outbound firewall rules should be restricted to accept only TCP/UDP ports necessary for operations.
  - Source and destination IP addresses for all inbound and outbound traffic should be as specific as possible.
  - Install anti-virus software on all systems and configure to perform daily file system scans.
  - Implement an automated notification procedure to ensure network anomalies are discovered and responded to in a timely manner.

Wireless Sensor Security

The following security protocols are implemented:

Sensor <--> gateway communication:

- All data is wirelessly transmitted via the Wirepas Mesh Network.
  - https://wirepas.com/what-is-wirepas-mesh/
- All communications on this network are fully encrypted.
- Sensors and gateways are configured to communicate on a given Wirepas Mesh Network via out-of-band authentication at the OEM factory. None of this is negotiated in the field, which eliminates the risk of sensor/gateway spoofing, hijacking or man-in-the-middle attacks.

Gateway <--> cloud communication:

- Gateway communication with the cloud is done by ethernet, wireless internet or cellular.
- SSL encryption and public key infrastructure via Azure IoT hub secure device identity is used.
- Azure Device Provisioning Service is used to configure the gateway upon initial boot to communicate with Azure IoT hub. ateway communication with the cloud is done
  - Uses Azure-verified root, intermediate and device CA certificates to verify gateway's identity and auto-register the gateway as an IoT device.
  - Gateways are configured with device CA certificates at the OEM factory.
- Gateways are also configured to send Wirepas network health information (no customer data) to SIAI Wirepas Network Tool server over a secured connection that uses trusted CA provider or self-signed certificates.

Hardware security:

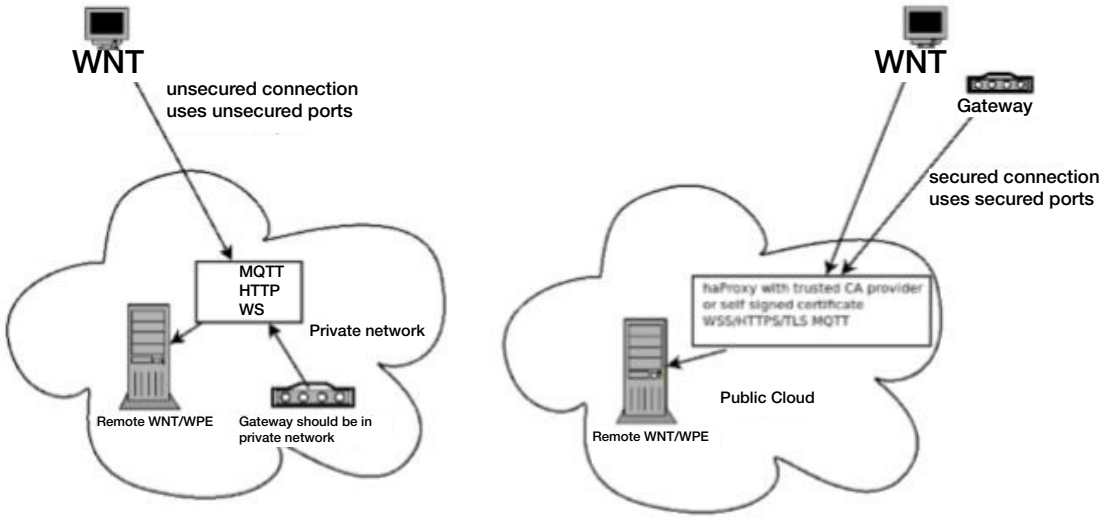
- Sensor
  - No access to gain control of the device – no external ports, fully potted electronics assembly (no access to internal debug ports).
- Gateway
  - ARM-based Linux platform
  - All accounts with user and admin permissions are password protected. Passwords are unique and created by Treon at OEM factory.
  - External USB port – need user or admin account access to interface with USB port.
  - IP information and other network settings can be modified with gateway in WAP mode.
  - Each gateway has unique WAP password. Password is printed on label of gateway.

Over the air firmware updates:

Firmware for sensors or gateways are digitally signed and authenticated by devices before being allowed to run on the sensor or gateway.

Architectural Drawing

WNT backend configuration diagrams from Wirepas documentation



System Audits

Portal Users

The Portal has two primary types of users, Azima DLI users and Customer end-users. Azima DLI users include administrators to configure the portal experience for each customer account and Azima DLI analysts to support application services as required.

End-users of the Portal are configured by Azima DLI for each account.

User Roles:

- End User: Users who can configure My Dashboard, generate/upload general reports, can update or be assigned an Alert, and can update notification preferences
- Power User: Users who can perform System Configurations, including management of wireless sensors and gateways
- Analyst: User who can perform system configurations and access analytic tools per application entitlement as applicable including unreviewed diagnostic data
- Administrators: User who can add new End Users to the application, can manage token allocations, and can configure integration settings

ExpertALERT-cloud Users

Access to the ExpertALERT cloud application is managed through remote desktop services with users only created by Azima DLI administrators with limited to access to specific associated user database(s) and local resources. Azima DLI maintains domain policy groups to ensure the segregation of system access & controls. Users are automatically logged out of ExpertALERT when application is closed or has been idle for more than 1 hour.

Connecting to ExpertALERT-cloud required two-part authentication, managed by Sophos VPN.

Azima DLI – IT Terminology

WATCHMAN Data Center Data Backup and Transfer

All customer databases are backed up nightly. In the unlikely event of catastrophic data loss, SIAI IT engineers will restore to the previous backup. Monthly backups are secured at an off-site facility.

Technology

The following describes our technology and security for the WATCHMAN™ Reliability Portal and Data Center.

System Software

This refers to the ExpertALERT™ or ViewALERT™ software as made available for desktop installation, embedded into the TRIO data collection hardware, or accessible through an internet Cloud-subscription.

Website Interface / Reliability Portal / PredictivePortal

This refers to the WATCHMAN™ Reliability Portal and PredictivePortal™ which delivers multi-views metrics of plant's machine condition analysis through a secure web browser requiring user authentication. The analysis results, key performance metrics and diagnostic report contents are updated in real time as diagnostic experts complete their analysis on machine data.

Data Transfer

This is the communication or transfer of data either through replication, survey transfer file exchange or data transfer from online systems. This technology allows for two-way data transfer between SIAI and each individual site. Data can be transferred each direction using this technology.

CMMS Connectivity

SIAI has integration with Maximo and other CMMS or SCADA systems through configuration of an integration function in ExpertALERT™. As part of a custom engineered solution, SIAI can provide the required outputs to align with customer's display or management system's API via a COM interface.

PDM Technology Integration

The ExpertALERT™ product databases and associated software are capable and configured to store infrared thermography reports, oil analysis reports, reciprocating equipment inspection reports, and general user defined reports and documentation. These can be stored against a Plant, Area or Machine and in the case of the machine, can be used to drive the current severity value for the machine. These reports are images, doc files or pdf files.

Local Network Boundary

The line which defines responsibility for maintaining an organization's infrastructure and security of the local area network (LAN) on site.

C2C Integration

Cloud-to-Cloud connections to facilitate communication to other applications and tools.

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

For more information about Azima DLI or Fluke Reliability:
visit www. flukereliability.com or
email the team at azimasales@Fluke.com