

GEA IIOT AND REMOTE ACCESS SERVICES

General Information Guide (Version 1.4)



What is the GEA IIoT Edge Solution?

It's a powerful all-in-one device that combines remote access, data logging, edge computing, and advanced IIoT features. It provides secure remote maintenance functionality and real-time monitoring, enabling GEA experts to quickly address issues or optimize performance.



Why does this matter to you?

1. What if something goes wrong?

Things happen—equipment might fail or act up. Instead of waiting for an engineer to travel, we connect remotely to your equipment. This saves time and gets you back up and running faster. Plus, our 24/7 condition monitoring can catch issues before they become problems.

2. Why combine IIoT and Remote Access?

Historically, these features required separate systems. Not anymore. The GEA IIoT Edge Solution integrates everything into one device, simplifying your setup and maximizing your benefits.



Why should I choose a GEA Edge Device?

1. Managed for You:

Our Edge Gateway is always up-to-date with the latest security patches and updates. Using an Edge Management System, we ensure all connected devices remain secure and optimized.

2. Built for Your Needs:

It's compatible with various GEA equipment and supports industrial-grade capabilities like Azure IoT integration and robust security features.



Why GEA?

Because we make it simple for you. Our IIoT and Remote Access Services give you fast, secure, and effective solutions to keep your operations running smoothly. With GEA, you're always one step ahead.

How to get started?

1. Connection:

The Edge Gateway can connect via your network (DMZ or WAN).

2. Simple Setup:

The device uses Zero-Touch Provisioning, configuring itself automatically during installation.

3. Ongoing Support:

Once installed, GEA handles updates, monitoring, and troubleshooting remotely, so you don't have to worry.



How does Remote Access work?

1. Secure and Reliable Connectivity: Our VPN technology ensures your equipment is securely accessible from anywhere. Each device gets a unique IP address, and granular access controls ensure that only the right person connects to the right machine.

2. Easy Device Management: We automate VPN setups, firmware updates, and security patches, so you can focus on your operations.

3. What's the Benefit for you? You get 24/7 remote access to all connected devices worldwide, including both Edge Gateway and GEA equipment. This ensures faster response times and reduced downtime, keeping your operations running smoothly.



How does IIoT Connectivity work?

1. Clarity and Transparency: We define what data will be collected, how it will be used, and secure your approval upfront. Your data stays private and compliant with regulations like the EU Data Act.

2. Smart Data Handling: The Edge Gateway collects and processes data either locally or in the cloud. It's flexible and supports industry-standard protocols like Siemens, Modbus, OPC UA, Ethernet/IP and IFM VSE.

3. Custom Modules for Your Needs: From AI and analytics to system interfacing, we can tailor modules to fit your exact requirements.



What are the Security Benefits?

1. Built-In Protection: With features like hardened operating systems, secure hardware chips (TPM), and Azure IoT security, your devices are well-guarded against threats.

2. Automatic Updates: We regularly apply patches and updates over the air, keeping your system resilient and secure without disrupting your operations.

3. Zero-Trust Approach: Our internal firewall restricts edge gateway traffic to a set of known ports only. In addition, we share a list of cloud endpoints that are required by the edge gateway. This transparency allows customers IT to manage their firewall so that only this limited number of endpoints are white-listed.

GEA IIOT GATEWAY

Secure, Reliable, and Efficient Data Management for Your Operations

This is a summary of GEA's IIoT Gateway White Paper. For full details, refer to the original document: "The IIoT Gateway, Its Management Platform, and Security Features."



What is the IIoT Gateway?

Think of the IIoT Gateway as a smart device that securely connects your GEA equipment to the digital world. It collects valuable data about your equipment's performance and sends it to the Cloud, allowing GEA engineers to monitor and manage assets remotely.



How does it benefit you?

By using the IIoT Gateway, GEA engineers can check and troubleshoot your equipment remotely. This means they can fix issues without having to be on-site, keeping your equipment running smoothly and reducing downtime, saving you time and money. It could also help preventing unexpected failures by enabling predictive maintenance, which catches problems early.



What makes the IIoT Gateway safe to use?

You might be wondering, "How do I know my data is safe?" That's where GEA comes in, your Security is our top priority. The IIoT Gateway isn't just any device; it's built with top-notch security features to protect your data from being compromised. GEA is even working on making sure the Gateway meets the highest industry standards (IEC 62443) for cybersecurity.



How GEA manages your Gateway and makes sure it's Safe?

GEA doesn't just plug in random services. The IIoT Gateway uses several trusted third-party services (Welotec & Microsoft Azure) to help manage and monitor everything from afar. These services are rigorously tested and certified to meet the same high security standards as the Gateway itself.



How Can You Use the IloT Gateway?

Wired Setup: This is the most common way. Your Gateway connects to your existing internet network and uses your current security measures like firewalls. Just whitelist specific hostnames to ensure connectivity with GEA Cloud Services. It's simple, secure, and reliable.



Why choose GEA's IloT Gateway?

With the IloT Gateway, you get a simple, secure, and smart way to manage your GEA equipment from anywhere. It's packed with powerful security features that protect your data, making it easier and safer to keep things running smoothly.

For a hassle-free experience, trust GEA to keep your equipment and data safe



What makes the IloT Gateway so secure?

The IloT Gateway has multiple built-in security features to be tough against cyber attacks & minimize vulnerabilities:

- **Customizable Operating System:** The Gateway uses a special, secure operating system Yocto OS that only lets necessary features run, making it harder for hackers to get in.
- **Easy to Set Up Security:** The Gateway always initiates communication, so no ports need to be open permanently. Its predictable communication makes it easy to configure firewalls securely to block unwanted traffic.
- **Proactive Monitoring & Updates:** GEA continuously monitors the health of the Gateway, and any issues are addressed proactively. Regular security updates and critical patches are rolled out to ensure the Gateway remains secure.
- **Safe Storage of Credentials:** The Gateway uses the Trusted Platform Module (TPM) to securely store its immutable device identity keys, so no one can steal or misuse them.

Why do we advise white-listing fully qualified domain names (FQDN) instead of IP addresses?

Azure Cloud Services offer a wide range of IP addresses to ensure resilience and uptime and white-listing all these IP addresses would be additional overhead for customer IT to manage. Using hostnames (like companynames.com) instead of IP addresses (that may change) help changing server addresses. It makes sure your system stays up and running smoothly to avoid issues.

Why does GEA need third-party services?

GEA works with trusted partners like Microsoft Azure to store your data and provide extra security. These services are securely managed by GEA, so your information stays safe, and the data remains protected. GEA is moving toward self-hosting more of these services for additional security.

Why no SSL inspection?

The IloT Gateway uses something called mutual TLS to ensure confidentiality and integrity for secure communication. This is a super-secure way to keep data safe between devices. Enabling SSL inspection would compromise this security, so GEA does not support it. But don't worry – your data is still protected!