

ISONA Automation WebCenter and the Secure Automation Components

ISONA offers its customers an innovative all-in-one solution by combining the **Automation WebCenter** (web portal) with its **Secure Automation components**.

High IT security standards and a wide range of application scenarios make this solution a benchmark in the industry, meeting virtually all customer requirements.

The ISONA solution is designed for use across various sectors, including energy contracting companies, municipal utilities, building automation firms, plant operators, solar installers, as well as manufacturers of control systems, energy generation units, machinery, and more.

Thanks to its flexible design, the system can be easily customized to meet specific customer needs.

The following diagram illustrates how the **Automation WebCenter (AWC)** interacts with various **Secure Automation components** to enable connectivity for distributed sites and secure remote maintenance access:

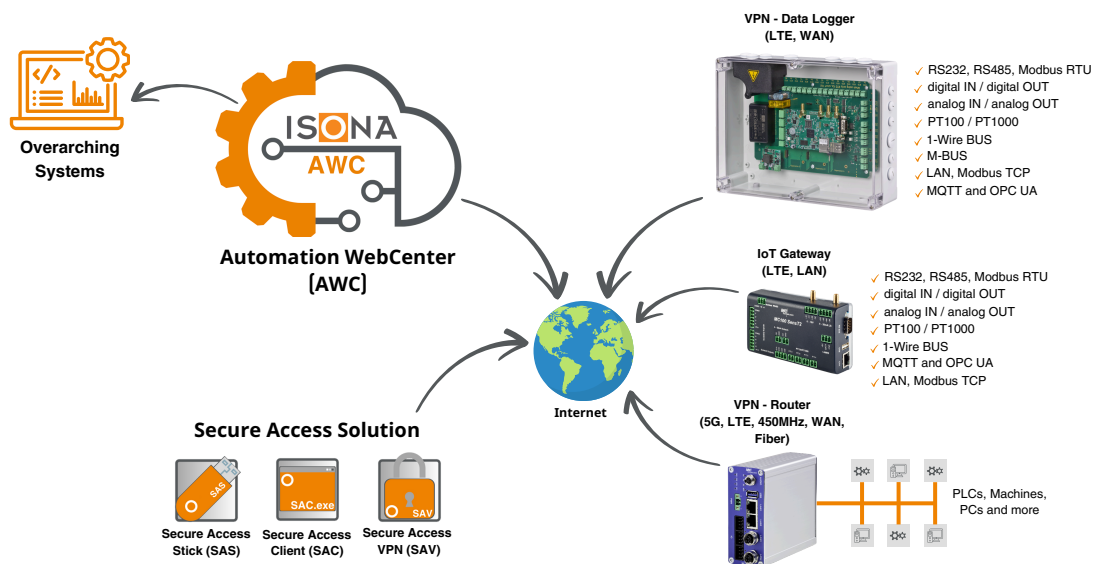


Fig.1: Overview - ISONA Automation WebCenter in Combination with ISONA Secure Access Components

The **ISONA Automation WebCenter** includes the following functions and modules:

- Alarm notifications in the event of faults via email, SMS, or fax
- Centralized collection of meter readings and measurement data across multiple sites in a central PostgreSQL database
- MQTT broker for communication with IoT devices
- Monitoring of firewall and controller availability at distributed locations
- Device management for various VPN routers, VPN data loggers, and miniboxes: initial offline configuration, remote configuration, remote firmware updates, online/offline monitoring
- Inventory system containing all information about installed devices at each site (manuals, schematics, etc.)
- Address management with contact details of manufacturers, service providers, customers, project partners, etc.
- Diagnostic tools for the quick commissioning of new sites
- Easy VPN configuration on tablets by end users
- Automatic certificate renewal upon expiration (typically after 1–3 years of validity)
- Various interfaces to higher-level energy management systems, building automation servers (BMS), billing systems, ERP platforms, control centers, and more

Overview

ISONA Automation WebCenter and the Secure Automation Components

The **ISONA Secure Automation Components** are the ideal complement to the **ISONA Automation WebCenter**. Below is an overview of each **Secure Automation Component**:

Secure Access Gateway (SAG)

The **Secure Access Gateway (SAG)** is the central IT security component of the overall system. It functions as a VPN gateway, remote maintenance server, authentication server, certificate authority (PKI), authorization system, routing server, and central management server for all **Secure Access components**.

The **Secure Access Gateway** is delivered as a virtual appliance and can be deployed on a wide range of virtualization platforms. Depending on customer requirements, it can be hosted either on-premises or on ISONA's data center servers.

A persistent VPN tunnel between the **Secure Access Gateway** and a corporate network allows for a secure and vendor-independent remote maintenance system.

Secure Access Stick (SAS)

The **Secure Access Stick (SAS)** enables secure external access to plant visualizations or control systems. This specialized USB stick requires no installation or administrator rights and leaves no traces on the Windows® guest system, as it runs in a sandboxed environment.

All software required to establish a secure application-layer VPN and access the automation infrastructure is preloaded on the stick.

Combined with a password, the stick provides strong two-factor authentication (2FA), making it immune to keyloggers and viruses that can compromise traditional VPN clients by stealing credentials. Stick configuration and management are handled centrally via the **Secure Access Gateway**.

Secure Access Client (SAC)

The **Secure Access Client (SAC)** is a USB-free alternative to the SAS with identical features. It enables secure access from Windows® PCs where USB usage is restricted.

After successful authentication, all necessary software to establish a secure application-layer VPN is delivered ad hoc via browser by the **Secure Access Gateway (SAG)** and executed in a sandboxed environment.

For 2FA, users can choose between a hardware OTP token or an OTP app on a smartphone (e.g., Google Authenticator).

Secure Access VPN (SAV)

The **Secure Access VPN (SAV)** is used when a transparent VPN tunnel from a PC or tablet to a device on-site is required — for example, to access a controller using a programming tool.

The complete OpenVPN configuration file (.ovpn) can be downloaded from the **ISONA Automation WebCenter** and imported as a profile into the installed OpenVPN client (available at <https://openvpn.net/vpn-client>).

Secure Access VPN is also used to enable access from tablets (iOS, Android) or Macs to servers or machines. Secure user authentication is ensured via 2FA using a one-time password (OTP), with the same authentication options as for the **Secure Access Client**.

Overview

ISONA Automation WebCenter and the Secure Automation Components

Devices for Distributed Sites

To network decentralized facility locations, **ISONA** provides a range of hardware devices (see Fig. 1; further details available on our website www.isona.de)

- Various VPN routers (LTE, DSL, or WAN) for connecting different LAN-capable devices on-site
- Various VPN data loggers (LTE or WAN) for connecting fault contacts, sensors, M-Bus meters, Modbus devices, controllers, third-party routers, etc.
- **ISONA Minibox** (LTE-M or LoRaWAN) for connecting up to two sensors (4–20 mA) and one fault contact. Ideal for monitoring small installations, e.g., with a single burner and a domestic hot water or buffer tank, and for pressure monitoring in heating circuits

Automation Terminal Server (ATS)

This optional Windows-based terminal server is used when tablet or Mac users require remote access to systems, controllers, etc.

The **Secure Access VPN (SAV)** is installed on the end device, which then connects via RDP to the **Automation Terminal Server**. The server acts similarly to a jump server.

All necessary Windows applications for remote access to servers, machines, or controllers are installed on the **Automation Terminal Server**.