

# Overview

## ISONA Remote Access System

The **ISONA Remote Maintenance System** is an innovative solution that meets a wide range of requirements across diverse application scenarios – all while maintaining the highest security standards. Thanks to its flexible architecture, the system can be adapted to support even complex, customer-specific processes.

It is particularly well-suited for critical infrastructure (CRITIS) organizations, companies with machinery and equipment from various manufacturers, and businesses with heterogeneous server environments that need to grant external service providers secure access to their machines or servers for maintenance purposes.

The following graphic illustrates the structure of the **ISONA Remote Access System**:

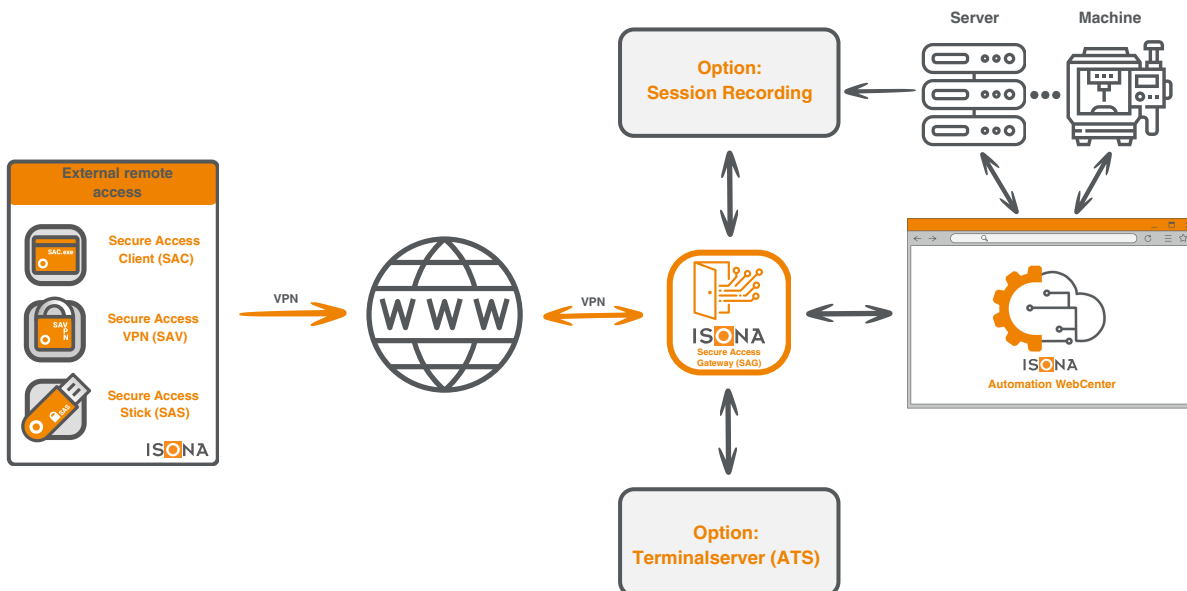


Fig.1: Overview - ISONA Remote Access System

The **ISONA Remote Access System** includes the following features:

- External service technicians can log into the remote access portal to submit a maintenance request
- Maintenance sessions must be approved by an internal employee – even via smartphone
- Time-limited remote sessions through automatic VPN tunnel termination
- Audit-proof recording of remote sessions via the optional Session Recording System
- Integrated asset management system that stores all relevant information about servers and machines
- Contact management for storing details of manufacturers, service partners, and more
- Automation WebCenter (AWC), based on an SQL database, with interfaces to higher-level applications
- User-friendly VPN configuration for end devices via the Automation WebCenter (AWC), directly by the end user

## Overview

### ISONA Remote Access System

Below is a description of the individual components of the ISONA Remote Access System:

#### Component 1: Automation WebCenter (AWC) with integrated Secure Access Gateway (SAG)

The **Secure Access Gateway (SAG)** serves as the central IT security component of the **ISONA Remote Access System**. It functions as a VPN gateway, remote maintenance server, authentication server, authorization system, routing server, and central management server for all system components. The **Secure Access Gateway** is deployed as a virtual appliance (compatible with VMware®, Hyper-V®, XenServer®, Oracle VirtualBox®) either behind the customer's firewall or in the DMZ — following a two-tier security concept.

#### Component 2: Secure Access Stick (SAS)

The **Secure Access Stick (SAS)** enables secure remote access to any server, machine control system, etc., via RDP, VNC, and similar protocols. This special USB stick requires no installation or admin rights and leaves no traces on the Windows® guest system, as it operates within a protected sandbox environment. All the software necessary to establish a secure VPN connection and access the infrastructure is pre-installed on the stick. Together with a password, it enables highly secure two-factor authentication (2FA).

#### Component 3: Secure Access Client (SAC)

The **Secure Access Client (SAC)** is a USB-free alternative to the **Secure Access Stick (SAS)**, offering identical functionality. It enables access from Windows® PCs where USB usage is restricted or where an alternative access method is explicitly required.

All necessary software for secure VPN connection and system access is automatically delivered from the **Secure Access Gateway (SAG)** to the guest PC and executed in a secured sandbox environment.

For two-factor authentication (2FA), users can choose between an OTP token (one-time password), a soft token (authenticator app such as Google Authenticator), OTP via SMS, or OTP via email. All OTP methods are centrally managed via the SAG.

#### Component 4: Secure Access VPN (SAV)

The **Secure Access VPN (SAV)** enables secure remote access to servers and machines from tablets or smartphones. Based on the OpenVPN client, it supports all major operating systems including Windows, macOS, iOS, Android, and Linux.

To ensure secure user authentication, it is combined with a two-factor authentication (2FA) process using a one-time password, with the same authentication options available as in the **Secure Access Client**.

## Overview

### Component 5: Remote Session Recording

To comply with requirements such as those of NIS2, a virtual appliance for session recording is integrated into the data stream between the remote user and the target systems. It records protocols such as HTTP(S), RDP, VNC, ICA, SSH, and Telnet – providing clear evidence of what actions were taken by the external user on the server or machine. The system also supports a four-eyes principle, allowing real-time monitoring of the session and manual interruption if necessary.

### Component 6: Automation Terminal Server (ATS)

This optional Windows-based terminal server is used when tablet or macOS users need remote access to systems or machine controls. The **Secure Access VPN (SAV)** is used on the end device to establish a secure connection. The device then connects via RDP to the **Automation Terminal Server**, which functions like a jump server. All required Windows applications for remote access to servers, machines, or control systems are installed and run on the **Automation Terminal Server**.