Gesamtübersicht

V. 1.3

ISONA Fernwartungssystem

Das **ISONA Fernwartungssystem** ist eine innovative Lösung, die mit einem hohen Sicherheitsstandard alle erdenklichen Anforderungen in unterschiedlichsten Einsatzszenarien abdeckt. Durch das flexible Konzept des Systems lassen sich auch komplexe, kundenspezifische Prozesse abbilden.
Speziell für Firmen mit Maschinenparks unterschiedlicher Hersteller aber auch für Firmen mit heterogenen Serverumgebungen, die externe Dienstleister zu Wartungszwecken sicher auf ihre Maschinen / Server zugreifen lassen möchten, ist das **ISONA Fernwartungssystem** optimal geeignet.

Die folgende Grafik erläutert den Aufbau des ISONA Fernwartungssystems:

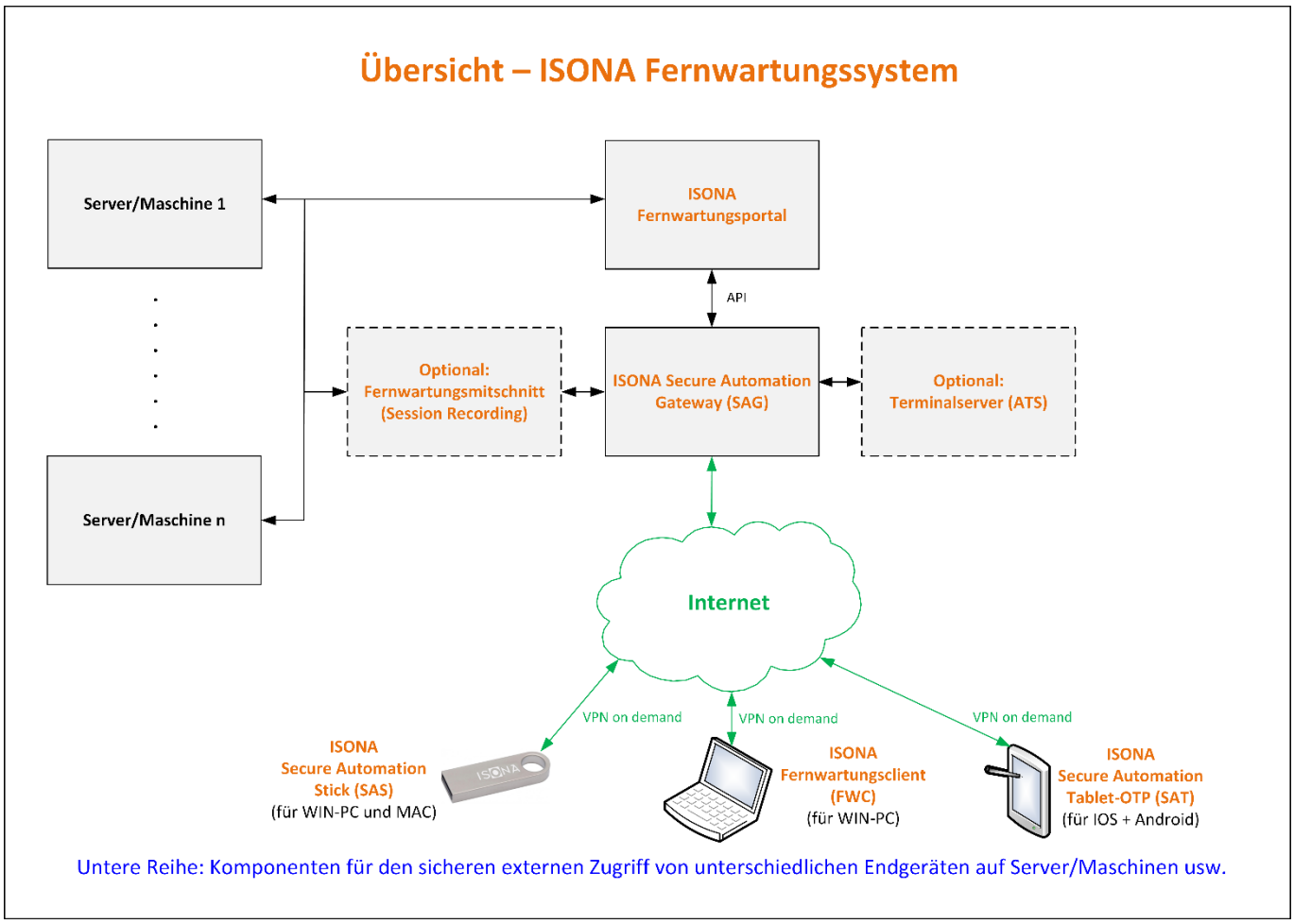

Abb. 1: Komponenten des ISONA Fernwartungssystems

Das ISONA Fernwartungssystem umfasst folgende Funktionen:

⇨ Login von externen Servicetechnikern im Fernwirkportal, um Fernwartungsanfrage zu stellen
⇨ Freigabe einer Fernwartungsanfrage durch einen Authentikator in der Firma (auch via Smartphone möglich)
⇨ Zeitliche Limitierung der Fernwartungssitzung durch automatische Beendigung des VPN-Tunnels
⇨ Revisionssicherer Mitschnitt der Fernwartungssitzung mit dem optionalen Session Recording System
⇨ Inventarsystem, in dem alle Informationen über Server und Maschinen erfasst sind
⇨ Adressverwaltung mit den Kontaktdaten von Herstellern, Servicepartnern usw.
⇨ Webportal basierend auf einer SQL-Datenbank mit Schnittstellen zu übergeordneten Applikationen
⇨ Einfache VPN-Erstkonfiguration von Tablets durch den Endbenutzer über das Fernwartungsportal

Gesamtübersicht

V. 1.3

Nachfolgend werden kurz die einzelnen Komponenten des ISONA Fernwartungssystems beschrieben (siehe hierzu auch Abb. 1):

Komponente 1: Secure Automation Gateway (SAG)

Das Secure Automation Gateway (SAG) stellt die zentrale Komponente des ISONA Fernwartungssystems dar. Es dient als VPN-Gateway, Fernwartungsserver, Authentisierungsserver, Berechtigungssystem, Routingserver sowie als zentraler Managementserver für alle Komponenten des ISONA Fernwartungssystems. Das Secure Automation Gateway wird als virtuelle Appliance (lauffähig auf VMware®, Hyper-V®, XenServer®, Oracle VirtualBox®) oder als Hardware-Appliance im 1HE Rack-Gehäuse beim Kunden hinter der Firewall oder in der DMZ installiert.

Komponente 2: Secure Automation Stick (SAS)

Der Secure Automation Stick (SAS) erlaubt es, von extern sicher auf beliebige Server, Maschinensteuerungen usw. per RDP, VNC o.ä. zuzugreifen. Dieser spezielle USB-Stick benötigt keinerlei Installation oder Adminrechte und hinterlässt auf dem Windows®-Gastsystem keine Spuren, da er in einer abgeschirmten Umgebung (Sandbox) läuft. Sämtliche Software, die der Anwender benötigt um eine sichere VPN-Verbindung aufzubauen und auf die vorhandene Infrastruktur zuzugreifen, ist bereits auf dem Stick integriert. Dieser ermöglicht zusammen mit dem Kennwort eine hochsichere 2-Faktor-Authentisierung des Benutzers.
Der Stick bietet auch die Möglichkeit, einen transparenten VPN-Tunnel aufzubauen.

Komponente 3: Fernwartungsclient (FWC)

Der Fernwartungsclient (FWC) ist die USB-sticklose Variante des Secure Automation Stick (SAS) mit identischen Features. Dadurch wird auch ein Zugang von Windows®-PCs aus ermöglicht, bei denen eine Nutzung von USB-Sticks nicht erlaubt ist oder wenn explizit ein alternativer Zugang gewünscht ist.
Sämtliche Software, die der Anwender benötigt um eine sichere VPN-Verbindung aufzubauen und auf die Server/Maschinen zuzugreifen, wird nach der Authentisierung via Browser von dem Secure Automation Gateway (SAG) auf den Gast-PC geladen und in einer abgeschotteten Sandbox ausgeführt.
Für die sichere 2-Faktor-Authentisierung des Benutzers kann je nach Anforderung entweder ein OTP-Token (**O**ne**T**ime**P**assword = Einmalkennwort), ein Soft-Token (Kennwort-Generator auf einem Smartphone wie z.B. Google Authenticator), eine OTP-SMS (Einmalkennwort via SMS) oder „Einmalkennwort via E-Mail“ verwendet werden. Die Verwaltung der unterschiedlichen OTP-Varianten erfolgt zentral im Secure Automation Gateway (SAG).

Komponente 4: Secure Automation Tablet-OTP (SAT)

Mit dem Secure Automation Tablet-OTP (SAT) ist ein sicherer Fernwartungszugriff auf Server/Maschinen von Tablets oder Smartphones aus möglich. Beim iPad®/iPhone® wird dazu der im iOS® integrierte VPN-Client verwendet, erweitert um eine zweistufige Authentisierung mit einem Einmalkennwort. Bei Android®-Tablets/-Smartphones wird die Original OpenVPN-App unterstützt, ergänzt um eine Zwei-Faktor-Authentisierung mit einem Einmalkennwort. Für das Einmalkennwort stehen die gleichen Varianten wie beim Fernwartungsclient (siehe oben) zur Verfügung.

Komponente 5: Fernwartungsmitschnitt

Als optionale Komponente kann eine virtuelle Appliance für den Fernwartungsmitschnitt (Session Recording) in den Datenstrom zu den Servern/Maschinen eingebunden werden. Diese zeichnet die Protokolle HTTP(S), RDP, VNC, ICA, SSH und Telnet auf. Damit lässt sich später genau nachweisen, was der externe Servicetechniker auf dem Server/der Maschine konfiguriert und installiert hat. Das System unterstützt auch das Vier-Augen-Prinzip, bei dem man zeitgleich mitverfolgen kann, was der externe Dienstleister auf dem Zielsystem gerade arbeitet und kann den Zugriff bei Bedarf auch jederzeit unterbrechen.

Komponente 6: Terminalserver (ATS)

Wenn das Secure Automation Tablet-OTP (siehe oben) zum Einsatz kommt, terminiert das Tablet via RDP auf dem Terminalserver, der für die Tabletbenutzer ähnlich einem Jumpserver fungiert. Auf diesem Terminalserver (ATS) werden dann alle benötigten Applikationen für den Fernzugriff auf die Server/Maschinen installiert.

Kontaktdaten

ISONA GmbH
Sant-Ambrogio-Ring 13a
D-55276 Oppenheim (b. Mainz)
Telefon +49 6133 / 509098-0
Internet www.isona.de

Technischer Ansprechpartner:
Wolfgang Heck, heck@isona.de

Vertrieblicher Ansprechpartner:
Ralf Koenigs, koenigs@isona.de