FAQs – Advantage In Touch™ | External Version

Generic Questions

1. **What is Advantage In Touch?**
Advantage In Touch is our intelligent mix of remote-based services in combination with on-site services for fire safety, security and building automation to increase service quality, flexibility and system uptime.Advantage In Touch for comprehensive and fast services

2. **How does remote service work?**
Remotely delivered services use a secure remote connection to your systems. This enables Siemens service engineers to check and respond immediately, either by making software adjustments or, if needed, coming on site with the correct tools and replacement parts.

3. **How much experience does Siemens have with remote services?**
Siemens has been offering remote services based on the Siemens Remote Service platform (SRS) for more than 10 years. From the very beginning, we have assigned the highest priority to data security, access protection, availability and service quality. With its high security standards and reliability, SRS is ideal even for the high demands of Siemens Healthcare, handling patient data, or remote engineering in offshore wind parks for the Energy sector.
Current number of systems connected via SRS per sector:
Healthcare: 105,000
Energy: 61,000s
Infrastructure and Cities: 17,000 (Building Technologies: 7,000)
Industry: 9,000

4. **How does Siemens ensure high-quality remote service?**
Siemens has dedicated service engineers working in Advantage Service Centers (ASC) who follow clearly defined processes and undergo regular training.

5. **How secure are remote services?**
We assign the highest priority to data security and privacy as well as access protection and access supervision. You have complete access control and transparency at any given time. The remote connection is based on a secure Virtual Private Network (VPN).

6. **Who can remotely access my system(s)?**
Within the framework of your service contract, we define with you the system access level for our service engineers – from time-limited access upon request to supervised or even full access. In addition, each system access is documented.

7. **Is the remote connection protected against viruses and hacker attacks?**
We have assigned the highest priority to security, privacy and access protection. The technologies used to secure remote access to your systems offer state-of-the-art protection against unauthorized access.
Each of the three SRS access servers – proxy servers which only allow external data previously requested by a system or user into the Siemens network – resides within a demilitarized zone (DMZ), where there is a firewall between the Internet and the access server and a firewall between the Siemens intranet and the access server.
Customer data is stored permanently only within the protected Siemens Intranet.

8. **How can you control Siemens access to your system?**
   The main prerequisite for any remote service activity is customer authorization. Access (users and levels) as defined by the customer is part of a legally-binding contract.

9. **How many access models does Siemens offer?**
   Since each customer's situation is different in terms of network setup, security requirements and regulations, and services provided, there are no clearly defined access models.
   In each solution or service contract, the Remote Service Team will carefully evaluate and define the most appropriate access model, which is then contractually agreed upon and mapped into the Siemens Remote Service Platform.
   For a list of the most commonly used access models, please read this security document.

10. **What happens should the Internet connection fail?**
    When the connection between the Siemens Remote Service Platform and the service system fails, the session is immediately closed on both ends.
    This is also true for idle connectivity sessions: If a connection is not being used for a defined period of time, the session is closed automatically by SRS. The system will automatically restore the last saved software state.

11. **How does Siemens ensure high availability of remote services?**
    The SRS platform is based on three fully redundant data centers located in Germany, Singapore and the USA. The capacity of each center is planned in such a way that the SRS platform is not affected unless two data centers are unexpectedly taken offline at the same time.

12. **What should I take into consideration before I sign up for Advantage In Touch?**
    Before you sign up for Advantage In Touch, we perform a detailed situation analysis of different factors such as industry regulatory requirements, technical infrastructure and national regulations. Only then do we complement our service offer with remote connectivity.

13. **Are there any proactive calls from the service center?**
    We offer to proactively monitor your systems remotely and in real time, 24/7, to detect and correct deviations before they become a problem. This ensures the highest possible system uptime.

14. **Does Advantage In Touch support third-party systems?**
    Advantage In Touch covers all equipment for which you have a maintenance agreement with Siemens. Before you sign up for Advantage In Touch, we will perform a detailed situation analysis. Possible support for third-party products will then be specified.

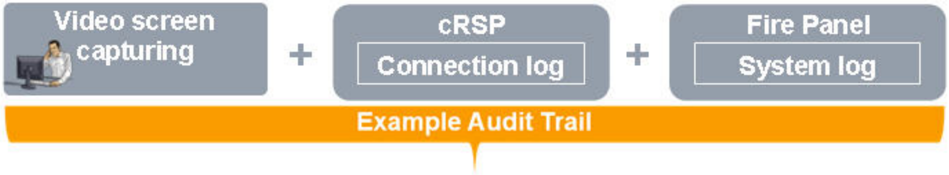
15. **Does the Advantage Service Center team speak my language?**
    We provide local service. This ensures that our service team speaks your language.

16. **How fast is the remote connection?**
    Establishing a connection, i.e. a connection to an already configured system, is almost instantaneous. It only takes a few seconds to establish the tunnel and start up the required application.
    Changes that are made to systems via remote connectivity follow the same delays as changes applied locally.
    The transmission speed and data throughput largely depend on the speed of the Internet connection used at the customer site. The platform has no defined caps.

17. **Does a subscription to Advantage In Touch make sense even though I only have a fire detection system from Siemens, i.e. no building automation and/or security system?**
    Yes, because Advantage In Touch gives you higher system availability and operational efficiency.

18. **Why should I invest in Advantage In Touch services?**
    As an Advantage In Touch customer, you benefit from higher system availability, faster service response and increased operational efficiency.

19. **What is an audit trail?**
    An audit trail consists of all information available to reconstruct what was done in a system (e.g. a fire panel or a PC). In the context of remote services, the audit trail contains elements from multiple sources to enable comprehensive logging, for example the cRSP connection log and a fire panel’s system log. Knowing and defining the elements of the audit trail with the customer gives them the confidence that the root causes can be determined no matter what happens. Additionally, the audit trail demonstrates the service provider’s readiness to make their activities transparent even if they are not supervised by the customer at all times. In addition, the audit trail protects our employees from unjustified claims.



20. **Which report formats are provided by the Performance reporting package?**
    The available formats are csv, PPT, PDF, html.

21. **Can I define customized reports?**
    We offer customized reports based on your requirements.

22. **Can I run the reports myself? How does it work?**
    Yes, you can generate reports yourself. We will be happy to show you how.

23. **How often can I get reports?**
    Depending on your needs, we offer monthly or/and quarterly reports, etc.

24. **Which service modules does Advantage In Touch offer?**
    Depending on your needs we offer Operational Assistance combined with Diagnosis & Repair, Performance Reporting, Performance Consulting and Event Monitoring & Response.

25. **How quickly can I upgrade or downgrade my service contract for Advantage In Touch?**
    Should your requirements change, you can simply modify or upgrade your existing service contract with additional modules.

Technical / IT-Related Questions

1. **How is my data transmitted?**
   The remote connection is based on a secure VPN. Furthermore, our platform utilizes state-of-the-art encryption methods to protect your data from unauthorized access during transmission. Should you require elevated security in response to specific threats, our

platform can also provide hardware-based router-to-router encryption solutions for data transfer.

2. **What is VPN and how does it work?**
   Virtual Private Network (VPN) is a network technology that creates a secure network connection over the Internet. The connection between the SRS portal and the installed system at your site is established through a VPN tunnel. This ensures highest security. VPN technology employs sophisticated encryption to ensure security and prevent any unintentional interception of data between private sites. All traffic over a VPN is encrypted using algorithms to secure data integrity and privacy. VPN architecture is governed by a strict set of rules and standards to ensure a private communication channel between sites.

3. **Which encryption methods are used for the VPN connection?**
   SRS offers various encryption methods and levels to make sure it can accommodate a wide range of customer requirements. For example, it can use DES encryption for legacy devices and AES265 for state-of-the-art encryption for current systems.
   For a comprehensive list of encryption methods per connectivity type, click here.

4. **What software does Siemens use for remote system operation?**
   A number of applications are supported to remotely operate systems via the Siemens Remote Service Platform. The main difference between these applications lies in the serviced systems themselves:
   For systems with a full operating system and a desktop shell, the following desktop visualization applications are currently supported: UltraVNC, RealVNC, NetOP, NetViewer, RDP.
   For embedded systems, i.e. non-PC-based systems such as fire panels or automation level panels, a proprietary engineering tool is used, such as XWorks for Desigo, SintesoWorks for Sinteso, Nox for Guarto3000, or ACS for Synco.

5. **Which prerequisites need to be met for Advantage In Touch?**
   All you need is a service contract, an Internet connection and a compatible system. We take care of the rest.

6. **How does the authentication process work between me as the caller and the service center?**
   Together with you we predefine the system access model for our service engineers – from time-limited access upon request to supervised or even full access. Each time a service engineer logs onto the platform, their user ID and password are verified against their corresponding access rights. This mechanism ensures that service engineers can access only those parts of your systems for which they are expressly authorized. In addition, Siemens maintains constant readiness to inform its customers about which service engineer had access to which data as well as when which communication activities were performed on which system.

   How does the authentication process work with the SRS platform?
   The Siemens Remote Service Platform offers various authentication methods, depending on the access model and the kind of service provided.
   For internal access by service technicians, strong authentication with a smart card token is used. Their credentials are verified against the corporate Active Directory from Siemens to ensure that only active employees can log in. For external access, strong authentication using a one-time password (sent via SMS) together with a username and password is available, depending on the kind of information or access you prefer.
   Authentication key exchange between the Siemens Remote Service Platform and the

system can be transmitted using the Diffie-Hellman method and up to 1536-bit encryption.

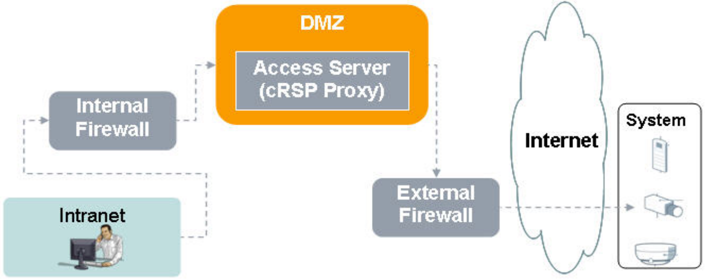
7. **How can I find out which service package is best suited for my requirements?**
   Your sales representative's helps you define the ideal service offering based on your needs and business requirements.

8. **What is the difference between IPsec VPN and SSL VPN?**
   Both IPSec and SSL are simply encryption methods. Both can be used to secure a VPN tunnel. In the Siemens Remote Service Platform, IPSec VPN is implemented using a hardware-based setup. This means that there is a router on both ends of the VPN tunnel. SSL VPN is implemented in a client/server setup. This means that on the customer side, you will find a piece of software (the SSL VPN client) installed on a PC, which establishes the connection to the SSL VPN server residing in the cRSP DMZ. For more detailed information about the technical differences between the two, click here.

9. **What is the difference between the SOA router and the COA router?**
   SOA stands for Siemens Owned Access. In such a scenario, Siemens provides the router which establishes the VPN tunnel from the customer site to the Siemens Remote Service Platform. For more information about the different SOA options, click here.
   COA stands for Customer Owned Access. This means that with the help of the cRSP help desk, we configure a router owned by the customer to establish the VPN connection to the Siemens Remote Service Platform. Generally, this router must offer IPSec support.

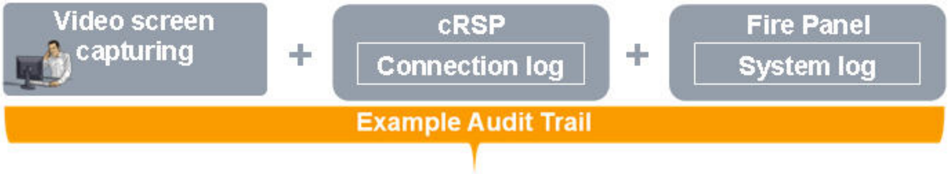
10. **How securely is my data transmitted and stored?**
    Customer data is stored only on the Siemens intranet. There it is backed up and protected from unauthorized access. We have implemented different technical and organizational measures to ensure maximum data protection, such as an ISO 27001-certified Information Management System and strong authentication for data access. Transmission of any data is always encrypted via a VPN connection.
    For a comprehensive list of security elements involved in the Siemens Remote Service Platform, click here.

11. **What is a demilitarized zone (DMZ)?**
    Some software services need to be reachable from the (unsecure) Internet. Rather than opening our (secure) intranet, we place those services outside of our intranet. This is done by separating a certain network area from the internet using a firewall.



12. **What is an audit trail?**
    An audit trail consists of all information available to reconstruct what was done in a system (e.g. a fire panel or a PC). In the context of remote services, the audit trail contains elements from multiple sources to enable comprehensive logging, for example the cRSP connection log and a fire panel's system log. Knowing and defining the elements of the audit trail with the customer gives them the confidence that the root causes can be determined no matter what happens. Additionally, the audit trail demonstrates the service provider's readiness to make their activities transparent even if they are not supervised by the customer at all times. In addition, the audit trail protects

our employees from unjustified claims.



13. What does ISO 27001 stand for?

ISO/IEC 27001 formally specifies a management system intended to bring information security under explicit management control. Being a formal specification means that it mandates specific requirements. Organizations that claim to have adopted ISO/IEC 27001 can therefore be formally audited and certified to be compliant with the standard. The standard formulates requirements for an Information Security Management System (ISMS). Additionally, it defines how those requirements are measured and assessed
A certified organization proves conformity with these requirements by passing the assessments of a certification body (e.g. TÜV for Germany).
Certification demonstrates to an interested party (e.g. a customer) that your IT security (via implementation of the ISMS) complies with internationally recognized standards. Certified organizations are listed on www.iso27001certificates.com.

14. Why is it necessary to connect via SRS?

While handling may be more complex during the initial setup process as compared to a third-party solution, cRSP offers the maximum level of security available and fully complies with the Siemens security standards.

15. Can I also use my own platform for the remote connection?

The Siemens Remote Service Platform is able to interface with other connectivity or authentication platforms in various ways and on different levels. Examples are integration of a customer's authentication portal via cRSP, or utilizing a customer's network infrastructure to connect to the Siemens Remote Service Platform in case of Customer Owned Access (COA).
The possibilities and limitations will always depend on the individual requirements and context and need to be reviewed as part of the preliminary assessment conducted before establishing any remote connection to a customer.

16. Do I need several remote connections when I have several plants?

Assuming that there is equipment in each plant which is subject to service enabled by remote connectivity, the number of connections, or entry points, depends on whether or not those plants are connected in a routable network.
With one remote connection, all systems residing in the same network and configured for remote service can be reached, regardless of their geographic location. Consequently, we need as many connections as there are individual networks we want to connect to.

17. Which infrastructure do I need? Modem or router?

The Siemens Remote Service Platform can provide connectivity to any kind of equipment at the customer site. It offers packages for dial-up modem/ISDN and broadband-based Internet connectivity.
Whether or not a router or integrated router/modem infrastructure is required, solely depends on the complexity of the network at the customer site. For example, if only one PC system needs to be connected to the Siemens Remote Service Platform, one dial-up modem may suffice. Should the same connection be used for multiple PC systems in the customer network, a router will be required at a minimum.

18. **Are the agents at the Advantage Service Center just operators who only record my problem or do they have in-depth expertise?**
    ASC engineers are well trained and highly skilled. Additionally, they are backed by our global service expertise.