

FAQs – Advantage In Touch™ | Externe Version

Generische Fragen

1. Was ist Advantage In Touch?

Advantage In Touch ist unser intelligentes Mix aus Fernwartung in Verbindung mit Vor-Ort-Services für Brandschutz, Sicherheit und Gebäudeautomation zur Steigerung der Servicequalität, Flexibilität und Systemverfügbarkeit. Advantage In Touch für ganzheitliche und schnelle services.

2. Wie funktioniert Fernwartung?

Aus der Ferne bereitgestellte Dienstleistungen werden über eine sichere Remote-Verbindung zu Ihren Systemen erbracht. So können Siemens-Servicetechniker umgehend reagieren und Überprüfungen anstellen, indem Sie Softwareanpassungen vornehmen oder bei Bedarf mit den erforderlichen Instrumenten und Ersatzteilen vor Ort erscheinen.

3. Wie viel Erfahrung hat Siemens mit Fernwartung?

Siemens bietet seit mehr als zehn Jahren Fernwartungs-Services basierend auf der Siemens Remote Service-Plattform (SRS) an. Dabei hatten Datensicherheit, Zugriffsschutz, Verfügbarkeit und Servicequalität stets absolute Priorität für uns. Dank seiner hohen Sicherheitsstandards und Zuverlässigkeit ist SRS das ideale System, sogar für die komplexen Anforderungen von Siemens Healthcare mit seinen sensiblen Patientendaten oder für die Fernprojektierung von Offshore-Windparks im Energiesektor. Aktuelle Anzahl an Systemen pro Sektor, die über SRS verbunden sind:

Gesundheitswesen: 105.000

Energiesektor: 61.000

Infrastrukturen und Städte: 17.000 (Gebäudetechnik: 7.000)

Industriesektor: 9.000

4. Wie stellt Siemens hochwertige Fernwartung sicher?

Siemens verfügt über dedizierte Servicetechniker, die in Advantage Service Centern (ASC) arbeiten. Sie richten sich nach klar definierten Prozessen und nehmen an regelmäßigen Schulungen teil.

5. Wie sicher ist Fernwartung?

Datensicherheit, Datenschutz sowie Zugriffsschutz und Zugriffsüberwachung haben für uns höchste Priorität. Sie verfügen jederzeit über komplette Zugriffskontrolle und Transparenz. Die Remote-Verbindung basiert auf einem sicheren Virtual Private Network (VPN).

6. Wer kann über das Remote-System auf mein(e) System(e) zugreifen?

Von befristetem Zugriff auf Anfrage bis hin zu überwachtem oder sogar uneingeschränktem Zugriff – im Rahmen Ihres Dienstleistungsvertrags legen wir mit Ihnen gemeinsam die Systemzugriffsstufe für unsere Servicetechniker fest. Darüber hinaus wird jeder Systemzugriff dokumentiert.

7. Ist die Remote-Verbindung gegen Viren oder Hackerangriffe geschützt?

Sicherheit, Datenschutz und Zugriffsschutz haben für uns höchste Priorität. Die Technologien, die für den Schutz des Remote-Zugriffs auf Ihre Systeme verwendet werden, nutzen modernste Sicherheitstechnologien gegen unbefugten Zugriff. Jeder der drei SRS-Zugangsserver (Proxyserver, die nur dann externe Daten zulassen, wenn diese zuvor von einem System oder Nutzer des Siemens-Netzwerks angefordert wurden) befindet sich in einer entmilitarisierten Zone (Demilitarized Zone, DMZ), in der

eine Firewall zwischen dem Internet und dem Zugangsserver sowie zwischen dem Siemens-Intranet und dem Zugangsserver aufgestellt ist. Kundendaten werden permanent nur innerhalb des geschützten Siemens-Intranets gespeichert.

8. Wie kann der Zugriff auf das System durch Siemens gesteuert werden?

Die Grundvoraussetzung für Fernwartungseingriffe ist die Genehmigung durch den Kunden. Der vom Kunden festgelegte Zugriff (Nutzer und Stufen) ist Teil eines rechtsverbindlichen Vertrags.

9. Wie viele Zugriffsmodelle bietet Siemens?

Da die Situation eines jeden Kunden in puncto Netzwerkeinrichtung, Sicherheitsanforderungen und -vorschriften sowie erbrachte Dienstleistungen unterschiedlich ist, gibt es kleine klar festgelegten Zugriffsmodelle.

Bei jeder Lösung oder jedem Dienstleistungsvertrag wird das Remote Service Team das am besten geeignete Zugriffsmodell ermitteln und festlegen. Dieses wird dann vertraglich vereinbart und in der Siemens Remote Service-Plattform erfasst.

Eine Liste der am meisten verwendeten Zugriffsmodelle finden Sie in diesem [Sicherheitsdokument](#).

10. Was passiert, wenn die Internetverbindung ausfällt?

Wenn die Verbindung zwischen der Siemens Remote Service-Plattform und dem Service-System ausfällt, wird die Sitzung an beiden Enden sofort geschlossen. Dies gilt auch für Sitzungen mit Leerlaufverbindungen: Wenn eine Verbindung für eine festgelegte Zeitspanne nicht verwendet wird, wird die Sitzung automatisch von SRS geschlossen. Das System stellt automatisch den zuletzt gespeicherten Software-Zustand wieder her.

11. Wie stellt Siemens die hohe Verfügbarkeit von Fernwartungsservices sicher?

Die SRS-Plattform basiert auf drei vollständig redundanten Rechenzentren, die sich in Deutschland, Singapur und den USA befinden. Die Kapazität eines jeden Rechenzentrums ist auf eine Weise konzipiert, dass die SRS-Plattform von Ausfällen nicht betroffen ist, es sei denn zwei Rechenzentren werden gleichzeitig offline geschaltet.

12. Was sollte ich berücksichtigen, bevor ich mich für Advantage In Touch anmelde?

Bevor Sie sich für Advantage In Touch anmelden, führen wir eine detaillierte Situationsanalyse unter Berücksichtigung verschiedener Faktoren durch, wie z. B. branchenspezifische regulatorische Anforderungen, technische Infrastruktur sowie landesrechtliche Vorschriften. Erst dann vervollständigen wir unser Service-Angebot mit der Remote-Verbindung.

13. Werden proaktive Anrufe vom Service-Center erfolgen?

Wir bieten Ihnen die proaktive, ferngesteuerte Überwachung Ihres Systems in Echtzeit, täglich rund um die Uhr, damit Abweichungen entdeckt und korrigiert werden, bevor sie zu einem Problem werden. Dadurch wird die höchstmögliche Systemverfügbarkeit gewährleistet.

14. Unterstützt Advantage In Touch Systeme von Drittanbietern?

Advantage In Touch deckt alle Systeme ab, für die Sie eine Wartungsvereinbarung mit Siemens haben. Bevor Sie sich für Advantage In Touch anmelden, führen wir eine detaillierte Situationsanalyse durch. Dabei wird auch die mögliche Unterstützung von Drittanbieter-Produkten angegeben.

15. Spricht das Advantage Service Center meine Sprache?

Wir bieten lokalen Service. Somit wird sichergestellt, dass unser Service-Team Ihre Sprache beherrscht.

16. Wie schnell ist die Remote-Verbindung?

Das Herstellen einer Verbindung, d. h. einer Verbindung zu einem bereits konfigurierten System, erfolgt beinahe unverzüglich. Es dauert nur einige Sekunden, den Tunnel herzustellen und die erforderliche Anwendung zu starten.

Änderungen, die am System über eine Remote-Verbindung vorgenommen werden, unterliegen denselben Verzögerungszeiten wie Änderungen, die lokal vorgenommen werden.

Die Übertragungsgeschwindigkeit und der Datendurchsatz hängen hauptsächlich von der Geschwindigkeit der Internetverbindung am Standort des Kunden ab. Die Plattform hat kein festgelegtes Maximum.

17. Ist eine Anmeldung für Advantage In Touch auch dann sinnvoll, wenn ich nur ein Brandmeldesystem von Siemens habe und ansonsten über kein Gebäudeautomations- und/oder Sicherheitssystem verfüge?

Ja, da Advantage In Touch für eine höhere Systemverfügbarkeit und verbesserte operative Effizienz sorgt.

18. Warum sollte ich in Advantage In Touch-Services investieren?

Als Advantage In Touch-Kunde profitieren Sie von einer höheren Systemverfügbarkeit, schnelleren Servicereaktion und besseren operativen Effizienz.

19. Was ist ein Audit-Trail?

Ein Audit-Trail besteht aus den gesamten Informationen, die zur Wiederherstellung der in einem System (z. B. einer Brandmeldezentrale oder einem PC) durchgeführten Aktionen verfügbar sind. Im Zusammenhang mit Remote-Services beinhaltet Audit-Trail Elemente aus mehreren Quellen, um die umfassende Protokollierung, z. B. das cRSP-Verbindungsprotokoll und ein Systemprotokoll des Brandmeldezentrum zu ermöglichen. Wenn der Kunde die Elemente des Audit-Trail kennt und sie festlegt, kann er sicher sein, dass die Grundursache in jedem Fall bestimmt werden kann. Darüber hinaus bestätigt der Audit-Trail die Bereitschaft des Service-Anbieters, seine Aktivitäten transparent zu machen, auch wenn diese nicht jederzeit vom Kunden überwacht werden. Zudem schützt der Audit-Trail unsere Mitarbeiter vor unberechtigten Forderungen.

**20. Welche Berichtsformate stellt das Performance Reporting-Paket bereit?**

Die verfügbaren Formate sind csv, PPT, PDF und html.

21. Kann ich individuelle Berichte definieren?

Wir bieten benutzerdefinierte Berichte, die an Ihre Anforderungen angepasst sind.

22. Kann ich die Berichte selbst ausführen? Wie funktioniert es?

Ja, Sie können Berichte selbst generieren. Wir zeigen Ihnen gerne, wie das geht.

23. Wie oft kann ich Berichte erhalten?

Ausgehend von Ihren Anforderungen bieten wir Ihnen monatliche oder/und vierteljährliche Berichte, usw.

24. Welche Service-Module umfasst Advantage In Touch?

Entsprechend Ihren Anforderungen bieten wir Operational Assistance in Kombination mit Diagnosis & Repair, Performance Reporting, Performance Consulting und Event Monitoring & Response.

25. Wie schnell kann ich ein Upgrade oder Downgrade von meinem Dienstleistungsvertrag für Advantage In Touch durchführen?

Sollten Ihre Anforderungen sich ändern, können Sie Ihren bestehenden Dienstleistungsvertrag einfach ändern oder ein Upgrade mit zusätzlichen Modulen durchführen.

Technische / IT-Relevante Fragen**1. Wie werden meine Daten übertragen?**

Die Remote-Verbindung basiert auf einem sicheren VPN. Zudem verwendet unsere Plattform modernste Verschlüsselungsmethoden, um Ihre Daten vor unbefugtem Zugriff während der Übertragung zu schützen. Falls Sie aufgrund spezieller Bedrohungen höhere Sicherheitsstandards wünschen, kann unsere Plattform auch Hardware-gestützte Router-zu-Router-Verschlüsselungslösungen für die Datenübertragung anbieten.

2. Was ist VPN und wie funktioniert es?

Virtual Private Network (VPN) ist eine Netzwerktechnologie, die eine sichere Netzwerkverbindung über das Internet herstellt. Die Verbindung zwischen dem SRS-Portal und dem an Ihrem Standort installierten System wird durch einen VPN-Tunnel hergestellt. Dadurch wird höchste Sicherheit gewährleistet. VPN-Technologie verwendet komplexe Verschlüsselungstechnologien, die für Sicherheit sorgen und das unbeabsichtigte Abfangen von Daten zwischen privaten Standorten verhindern. Der gesamte Verkehr über ein VPN ist durch Algorithmen verschlüsselt, wodurch Datensicherheit und Datenschutz gewährleistet werden. Die VPN-Architektur unterliegt strikten Regelungen und Standards, um einen privaten Kommunikationskanal zwischen zwei Standorten sicherzustellen.

3. Welche Verschlüsselungsmethoden werden für die VPN-Verbindung verwendet?

SRS bietet verschiedene Verschlüsselungsmethoden und -stufen, um den unterschiedlichsten Anforderungen der Kunden gerecht zu werden. So kann z. B. DES-Verschlüsselung für Altgeräte und AES256 als moderne Verschlüsselungsmethode für aktuelle Systeme verwendet werden.

Für eine umfassende Liste der Verschlüsselungsmethoden und der entsprechenden Verbindungstypen [klicken Sie hier](#).

4. Welche Software verwendet Siemens für den Betrieb des Remote-Systems?

Zahlreiche Anwendungen werden für den ferngesteuerten Betrieb von Systemen über die Siemens Remote Service-Plattform unterstützt. Der wichtigste Unterschied zwischen diesen Anwendungen besteht in den ferngesteuerten Systemen selbst:

Für Systeme mit einem kompletten Betriebssystem und einer Desktop-Shell werden aktuell die folgenden Desktop-Visualisierungsanwendungen unterstützt: UltraVNC, RealVNC, NetOP, NetViewer, RDP.

Für eingebettete Systeme, z.B. nicht PC-basierte Systeme wie Brandmeldezentralen oder Steuerungen auf Automationsebene wird ein proprietäres Engineering-Tool verwendet, z.B. XWorks für Desigo, SintesoWorks für Sinteso, Nox für Guarto3000 oder ACS für Synco.

5. Welche Bedingungen müssen für Advantage In Touch erfüllt sein?

Alles, was Sie benötigen, sind ein Dienstleistungsvertrag, eine Internetverbindung und ein kompatibles System. Wir kümmern uns um den Rest.

6. Wie funktioniert der Authentifizierungsprozess zwischen mir, dem Anrufer, und dem Service-Center?

Von befristetem Zugriff auf Anfrage bis hin zu überwachtem oder sogar uneingeschränktem Zugriff – wir legen mit Ihnen gemeinsam das Systemzugriffsmodell für unsere Servicetechniker fest. Jedes Mal, wenn ein Servicetechniker sich in der Plattform anmeldet, wird seine Benutzer-ID und sein Kennwort im Hinblick auf seine Zugriffsrechte überprüft. Dank diesem Mechanismus wird sichergestellt, dass Servicetechniker nur auf solche Komponenten Ihres Systems zugreifen können, für die sie eine ausdrückliche Genehmigung haben. Darüber hinaus bietet Siemens die konstante Bereitschaft, seine Kunden darüber zu informieren, welche Servicetechniker auf welche Daten Zugriff hatten und zu welchem Zeitpunkt bestimmte Kommunikationen auf bestimmten Systemen stattfanden.

Wie funktioniert der Authentifizierungsprozess mit der SRS-Plattform?

Je nach Zugriffsmodell und Art der erbrachten Dienstleistungen bietet die Siemens Remote-Plattform verschiedene Authentifizierungsmethoden.

Für den internen Zugriff durch Servicetechniker wird eine starke Authentifizierung mit einem Smartcard-Token verwendet. Ihre Anmeldedaten werden im Hinblick auf die Active-Richtlinie von Siemens für Unternehmen überprüft, um sicherzustellen, dass nur aktive Mitarbeiter sich anmelden können. Für den externen Zugriff steht, je nach der bevorzugten Informationsart oder dem Zugriff, die starke Authentifizierung mit einem einmaligen Kennwort (das über SMS gesendet wird) und einem Benutzernamen und Kennwort zur Verfügung.

Für den Austausch des Authentifizierungsschlüssels zwischen der Siemens Remote Service-Plattform und dem System kann die Diffie-Hellman-Methode und Verschlüsselung bis zu 1536 Bit verwendet werden.

7. Wie finde ich heraus, welches Service-Paket für meine Anforderungen am besten geeignet ist?

Ihr Vertriebsbeauftragter hilft Ihnen dabei, anhand Ihrer Bedürfnisse und Geschäftsanforderungen das ideale Service-Angebot für Sie zu ermitteln.

8. Was ist der Unterschied zwischen IPsec VPN und SSL VPN?

Bei IPsec und SSL handelt es sich einfach um Verschlüsselungsmethoden. Beide können dazu verwendet werden, einen VPN-Tunnel zu schützen. In der Siemens Remote Service-Plattform wird IPsec VPN mithilfe eines Hardware-basierten Setups implementiert. Das bedeutet, dass es an beiden Enden des VPN-Tunnels einen Router gibt. SSL VPN wird in einem Client/Server-Setup implementiert. Somit ist auf der Kundenseite eine Software-Komponente (der SSL VPN-Client) auf einem PC installiert, die die Verbindung zum SSL VPN-Server herstellt, der sich in der cRSP DMZ befindet. Für weitere Informationen zu den technischen Unterschieden zwischen den beiden Methoden [klicken Sie hier](#).

9. Was ist der Unterschied zwischen dem SOA-Router und dem COA-Router?

SOA steht für „Siemens Owned Access“. In diesem Fall stellt Siemens den Router bereit, der den VPN-Tunnel zwischen dem Standort des Kunden und der Siemens Remote Service-Plattform herstellt. Für weitere Informationen über die verschiedenen SOA-Optionen [klicken Sie hier](#).

COA steht für „Customer Owned Access“. Das bedeutet, dass wir mithilfe des cRSP-Help Desk einen Router des Kunden konfigurieren, um die VPN-Verbindung zur Siemens

Remote Service-Plattform zu konfigurieren. Dieser Router muss grundsätzlich IPSec-Unterstützung bieten.

10. Wie sicher werden meine Daten übertragen und gespeichert?

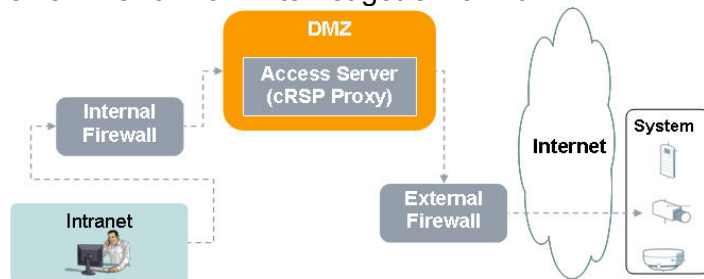
Kundendaten werden ausschließlich im Siemens-Intranet gespeichert. Dort werden sie gesichert und vor unbefugtem Zugriff geschützt. Wir haben verschiedene technische und organisatorische Maßnahmen implementiert, um den maximalen Datenschutz zu gewährleisten, wie etwa das ISO 27001-zertifizierte Informationsmanagement-System und starke Authentifizierung für den Datenzugriff.

Die Übertragung von allen Daten ist stets über eine VPN-Verbindung verschlüsselt.

Für eine umfassende Liste der Sicherheitselemente, die in der Siemens Remote Service-Plattform eingesetzt werden [klicken Sie hier](#).

11. Was ist eine entmilitarisierte Zone (Demilitarized Zone, DMZ)?

Einige Software-Services müssen vom (ungesicherten) Internet erreichbar sein. Anstatt unser (gesichertes) Intranet zu öffnen, stellen wir diese Services außerhalb unseres Intranets zur Verfügung. Dies geschieht, indem ein bestimmter Netzwerkbereich mithilfe einer Firewall vom Internet getrennt wird.



12. Was ist ein Audit-Trail?

Ein Audit-Trail besteht aus den gesamten Informationen, die zur Wiederherstellung der in einem System (z. B. einer Brandmeldezentrale oder einem PC) durchgeführten Aktionen verfügbar sind. Im Zusammenhang mit Remote-Services beinhaltet Audit-Trail Elemente aus mehreren Quellen, um die umfassende Protokollierung, z. B. das cRSP-Verbindungsprotokoll und ein Systemprotokoll des Brandmeldezentrumms zu ermöglichen. Wenn der Kunde die Elemente des Audit-Trail kennt und sie festlegt, kann er sicher sein, dass die Grundursache in jedem Fall bestimmt werden kann. Darüber hinaus bestätigt der Audit-Trail die Bereitschaft des Service-Anbieters, seine Aktivitäten transparent zu machen, auch wenn diese nicht jederzeit vom Kunden überwacht werden. Zudem schützt der Audit-Trail unsere Mitarbeiter vor unberechtigten Forderungen.



13. Wofür steht ISO 27001?

ISO/IEC 27001 ist die formale Spezifikation eines Managementsystems, deren Ziel darin besteht, Informationssicherheit unter ausdrückliche Managementkontrolle zu bringen. Da es sich dabei um eine formale Spezifikation handelt, sind spezielle Anforderungen erforderlich. Unternehmen, die ISO/IEC 27001 eingeführt haben, können daher formal geprüft werden. Dabei wird ihnen bescheinigt, dass sie den Standard einhalten. Der Standard formuliert Anforderungen im Hinblick auf ein Information Security Management System (ISMS). Zudem legt er fest, wie diese Anforderungen gemessen und bewertet werden.

Ein zertifiziertes Unternehmen beweist die Erfüllung dieser Anforderungen, indem es die

Prüfung einer Zertifizierungsinstanz (z. B. des TÜV in Deutschland) besteht. Die Zertifizierung signalisiert einer interessierten Partei (z. B. einem Kunden), dass Ihre IT-Sicherheit (durch die Implementierung von ISMS) international anerkannte Standards einhält.

Eine Liste mit zertifizierten Unternehmen finden Sie unter www.iso27001certificates.com.

14. Warum ist es notwendig, sich über SRS zu verbinden?

Im Vergleich zu einer Drittanbieter-Lösung kann die Abwicklung während des ersten Setup-Vorgangs mit cRSP komplexer sein. Jedoch bietet cRSP maximale Sicherheit und erfüllt die Siemens Sicherheitsstandards.

15. Kann ich auch meine eigene Plattform für die Remote-Verbindung verwenden?

Die Siemens Remote Service-Plattform kann auf verschiedene Weisen und auf verschiedenen Ebenen mit anderen Verbindungs- oder Authentifizierungsplattformen über eine Schnittstelle verbunden werden. Beispiele sind die Integration des Authentifizierungsportals eines Kunden über cRSP oder die Verwendung der Netzwerkinfrastruktur eines Kunden zur Verbindung mit der Siemens Remote Service-Plattform im Fall von Customer Owned Access (COA).

Die Möglichkeiten und Einschränkungen hängen immer von den individuellen Anforderungen und dem jeweiligen Kontext ab und müssen im Rahmen der vorbereitenden Bewertung, die vor der Herstellung einer Remote-Verbindung zu einem Kunden durchgeführt wird, überprüft werden.

16. Benötige ich mehrere Remote-Verbindungen, wenn ich mehrere Standorte besitze?

Wenn Sie an jedem Standort Systeme haben, die Services über eine Remote-Verbindung benötigen, so hängt die Anzahl der Anschlüsse oder Zugangspunkte davon ab, ob diese Standorte mit einem routbaren Netzwerk verbunden sind.

Mit einer Remote-Verbindung können alle Systeme, die sich im selben Netzwerk befinden und die für Fernwartung konfiguriert sind, erreicht werden, unabhängig von ihrer geografischen Lage. Folglich werden so viele Verbindungen benötigt, wie es individuelle Netzwerke gibt, mit denen eine Verbindung hergestellt werden soll.

17. Welche Infrastruktur benötige ich? Modem oder Router?

Die Siemens Remote Service-Plattform kann mit jedem System auf der Kundenseite verbunden werden. Sie bietet Pakete für Einwahl-Modem/ISDN und Breitband-basierte Internetverbindung.

Ob ein Router oder eine integrierte Router/Modem-Infrastruktur erforderlich ist, hängt lediglich von der Komplexität des Netzwerks auf der Kundenseite ab. Wenn z. B. nur ein PC-System mit der Siemens Remote Service-Plattform verbunden werden muss, ist ein Einwahl-Modem unter Umständen ausreichend. Muss dieselbe Verbindung für mehrere PC-Systeme im Kundennetzwerk verwendet werden, ist mindestens ein Router erforderlich.

18. Sind die Mitarbeiter im Advantage Service Center nur Telefonisten, die lediglich mein Problem aufzeichnen oder verfügen sie über Expertenkenntnisse?

ASC-Mitarbeiter sind gut geschult und verfügen über umfassende Kenntnisse. Darüber hinaus werden sie von unserer Global Service-Erfahrung unterstützt.