

Support système. Disponible quand vous en avez besoin.

Introduction

Siemens propose des services distants à l'aide d'une connexion distante sécurisée vers un système client. Nous garantissons une disponibilité supérieure du système grâce à un service proactif et plus rapide.

Dès le début, nous avons accordé la priorité à la sécurité des données et à la protection des accès. Notre concept de sécurité s'articule en deux parties. La première concerne l'aspect opérationnel général et présente le concept de base de Siemens Remote Service (SRS), la mise en œuvre de nos services et le support des applications, ainsi que les capacités techniques de nos produits. Elle s'adresse principalement aux administrateurs informatiques et aux responsables techniques souhaitant obtenir une compréhension de base de la façon dont le concept SRS fonctionne et des actions que nous mettons en œuvre pour sécuriser et préserver la confidentialité des données. Dans la seconde partie, nous abordons l'aspect technique et organisationnel. Les spécialistes informatiques et les experts de la sécurité des données y découvrent en détail les mesures de sécurité technique et organisationnelle que nous prenons pour atteindre un niveau élevé de sécurité et de confidentialité des données système. Nous expliquons également comment s'établit la connexion via notre plate-forme SRS, l'apparence de notre infrastructure de sécurité et les actions que nous mettons en place pour prévenir les attaques malveillantes. Ce document présente également les mesures offertes par SRS en matière de sécurité informatique.

L'avantage SRS

Face à une complexité grandissante, le service distant constitue une aide supplémentaire pour mener une prise en charge optimale de vos systèmes de protection incendie, de sécurité et d'automatisation des bâtiments.

Les avantages de SRS sont les suivants :

- Surveillance à distance pour détecter de manière proactive et corriger les interruptions afin de

réduire au maximum les temps d'arrêt des systèmes.

- Définition plus rapide et efficace de l'origine des problèmes des systèmes.
- Correction rapide et intelligente des problèmes par une intervention à distance.
- Les techniciens de service arrivent sur site en étant déjà munis des informations nécessaires et de l'équipement approprié.
- Support rapide des utilisateurs en cas de problèmes avec les applications.

Priorité à la sécurité des données

Nous nous engageons à établir un partenariat de long terme basé sur la confiance – et c'est pourquoi la sécurité des données et de toute première importance à nos yeux. Lors de l'installation de la plate-forme SRS, nous effectuons une analyse détaillée de la situation en tenant compte des réglementations internationales et nationales ainsi que de l'infrastructure technique avant de compléter notre offre de service par une connectivité distante. Notre équipe de service évalue soigneusement et au cas par cas les besoins de chaque client en matière de sécurité des informations et de protection des systèmes.

Voici une sélection des besoins que Siemens a l'habitude de traiter :

- **Confidentialité des données** : SRS a toujours développé une approche profondément respectueuse de la confidentialité des données des clients et continuera de le faire. Les problèmes potentiels et les mesures de sécurité sont tous et toutes expliqué(e)s avant l'établissement d'une connexion distante.
- **Accès sous surveillance** : nos clients peuvent surveiller et interrompre quand ils le souhaitent tout accès d'un service à distance.
- **Piste d'audit traçable** : le détail de chaque session individuelle est facilement retraçable à la demande des clients ou du législateur.
- **Accès sélectif** – administration individuelle des droits des utilisateurs et de l'accès aux données : les clients peuvent définir des droits d'accès à leurs systèmes et leurs données.

Avantage In Touch

Des réponses pour votre infrastructure.

SIEMENS

Sécurité des informations par un concept de sécurité en plusieurs étapes.

Accès contrôlé par le client

L'autorisation du client constitue la condition préalable principale de toute activité de service à distance. Seuls nos clients peuvent définir quel technicien de service est autorisé à accéder à telle partie de tel système dans le cadre d'un contrat juridiquement contraignant.

Nos clients définissent également quand et dans quelle mesure un technicien de service est autorisé à accéder à leur système.

Voici certains des modèles d'accès les plus courants choisis par nos clients :

- **Accès sur demande** : notre technicien de service peut accéder au système d'un client seulement sur la base d'une demande individuelle. Par exemple, un technicien de service peut demander un accès limité dans le temps afin de résoudre un problème spécifique. Cet accès n'est pas permanent. Ce type d'utilisation peut avoir fait l'objet d'un accord contractuel, et peut même figurer dans le paramétrage du pare-feu du client.
- **Accès contrôlé** : le client peut surveiller en temps réel le technicien de service lorsqu'il travaille sur le système via un partage d'écran à distance. La palette de services où cette option est nécessaire et les moyens techniques employés pour restreindre l'accès à ce niveau font l'objet d'un accord mutuel.
- **Accès complet** : un technicien de service expressément autorisé a la permission du client de se connecter à tout moment au système. Chaque accès au système est automatiquement notifié dans un journal pour que le client puisse en prendre connaissance. En général, les clients optent pour l'accès complet lorsqu'ils privilégient la maintenance préventive proactive et la disponibilité maximum du système.
- **Communication extérieure** : le système du client est autorisé à envoyer des informations en temps réel ou à des intervalles préalablement convenus au Siemens Service Center via la plate-forme SRS. Ceci permet de recueillir des données statistiques pour l'optimisation du système, la gestion proactive des incidents et les services de maintenance préventive. Siemens s'assure, en étroite collaboration avec le client, que la transmission se limite

au type de données et aux systèmes convenus.

Sélection du personnel

Seuls les employés ayant été formés à la sécurité informatique et à la protection des données sont autorisés à travailler dans notre unité SRS. Nous disposons de critères de sélection stricts et nos techniciens de service doivent participer à des formations et des procédures de validation permanentes.

Authentification et autorisation

À chaque fois qu'un technicien de service se connecte à notre plate-forme SRS, son ID et son mot de passe sont comparés aux droits d'accès correspondants.

Les modèles d'accès définis par le client sont répercutés sur notre plate-forme SRS et convertis en niveaux autorisés d'accès au système informatique. Ces niveaux d'accès sont ensuite comparés avec l'identité vérifiée du technicien de service. Grâce à ce mécanisme, les techniciens de service accèdent uniquement aux espaces des systèmes client pour lesquels ils disposent d'une autorisation expresse

Piste d'audit traçable

Siemens se tient constamment prêt à informer ses clients sur l'identité du technicien de service, les données auxquelles il a accès, les activités de communication menées sur chaque système et leur chronologie. Cette piste d'audit est rendue possible par les mesures suivantes :

- Chacun des accès à un système client est enregistré. Un horodatage d'entrée et de sortie ainsi que l'identité du technicien sont consignés.
- Des journaux de rapport sont conservés sur fichiers pendant au moins douze mois et leur conservation peut être étendue sur demande du client.

Les demandes d'ajout d'informations à la piste d'audit des clients sont envisageables dans la mesure où elles sont techniquement réalisables.

Accès réservé aux seuls partenaires agréés

Certains services peuvent nécessiter le recours à des partenaires techniques et de service externes.

Pour garantir un niveau de sécurité tout aussi fiable en pareil cas, notre plate-forme SRS dispose d'un mécanisme d'accès pour les partenaires. Ce n'est qu'après s'être soumis avec succès à une procédure d'authentification très rigoureuse et strictement mise en œuvre que les partenaires commerciaux agréés reçoivent l'autorisation d'accéder à une zone spécialement définie d'un système client via la plate-forme SRS.

Tous les services de partenaires agréés sont enregistrés avec la même précision que les accès système effectués par nos techniciens de service.

Protection de la transmission des données

Notre plate-forme SRS utilise des méthodes de cryptage de haut niveau pour protéger les données des clients de tout accès non-autorisé durant la transmission. L'accent est tout particulièrement mis sur le cryptage intégré en tant que condition préalable à toute communication sur Internet.

Si un client demande une élévation du niveau de sécurité en réponse à des menaces spécifiques, notre plate-forme SRS peut également fournir des solutions matérielles de cryptage routeur à routeur pour le transfert des données.

Architecture sécurisée du réseau

La plate-forme centrale SRS est située dans l'infrastructure de réseau Siemens et est protégée des accès extérieurs non-autorisés.

Dans une zone démilitarisée (DMZ), un serveur d'accès SRS se comporte comme un point d'entrée sécurisé entre Internet et le réseau Siemens, où sont stockées les données du client. Il établit une connexion sécurisée entre le système du client et le système du technicien de service.

Un DMZ avec une technologie de serveur Proxy constitue une architecture réseau éprouvée qui garantit la transmission au réseau Siemens des seules données précédemment demandées par une procédure de service distante authentifiée par Siemens. Ceci empêche tout accès Internet non-autorisé ou frauduleux aux données du client.

Gestion des données

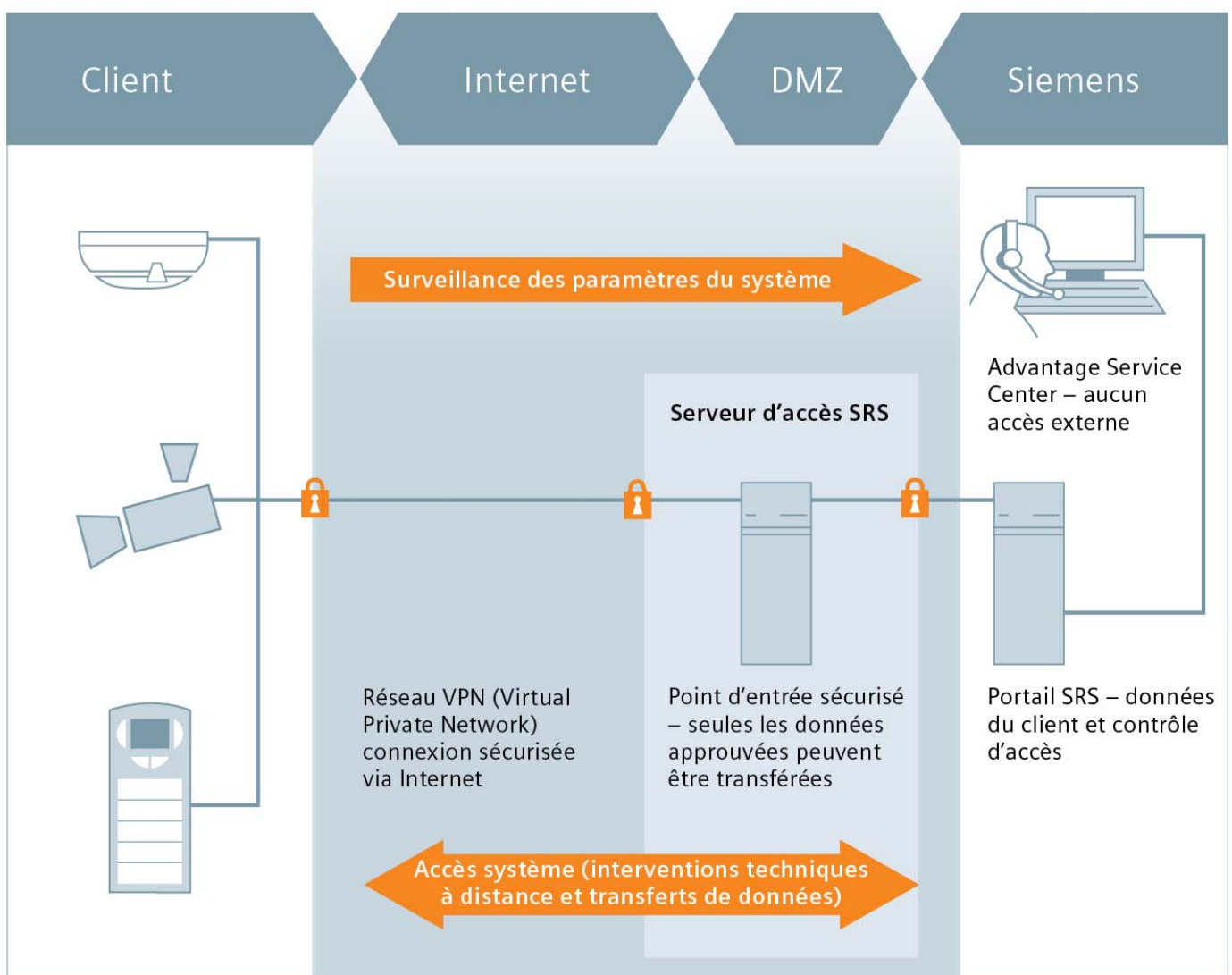
Nous classons de façon hautement confidentielle les données du client et n'accordons un accès à ces dernières qu'aux seules personnes qui en ont besoin. L'application de ce principe est sous-tendue par des mécanismes de contrôle d'accès réglementés et rattachés à une infrastructure, ainsi que par un ensemble d'outils spécialement développés à cet effet.

Les mesures de gestion des données mises en œuvre dépendent des besoins individuels d'un client (protection des données, type de données et exigences de la législation en vigueur). Nous pouvons fournir des conseils complets sur les solutions individuelles de conservation, de sauvegarde, de destruction des données et les droits de propriété associés.

Disponibilité de la plate-forme

La disponibilité de notre plate-forme SRS est garantie par trois centres de données totalement redondants situés en Allemagne, à Singapour et aux États-Unis. La capacité de chaque centre est planifiée de façon à ce qu'en cas de déconnexion inattendue totale de deux centres de données du réseau, la plate-forme SRS reste totalement préservée des éventuelles perturbations.

L'intégration de plans supplémentaires de reprise après sinistre (DR) et de gestion de la continuité d'activité (BCM) garantit un temps d'arrêt réduit au minimum, même en cas de sinistre simultané de nos centres de données.



Audit et certification.

ISO 27001

Siemens a été l'une des premières entreprises dans le monde à disposer d'un système internationalement accepté de gestion de la sécurité des informations pour ses services distants, lequel a reçu la certification ISO/IEC 27001:2005. Notre plate-forme SRS bénéficie d'un renouvellement permanent de sa certification par le TÜV Süd en Allemagne, et figure dans le Registre international des certifications ISMS disponible à l'adresse www.iso27001certificates.com

Audit Siemens CERT

Le Siemens Cyber Emergency Readiness Team (CERT) est un partenaire interne, indépendant et fiable qui élabore des mesures de sécurité préventives et évalue la sécurité des informations de l'infrastructure informatique. Notre plate-forme SRS est soumise à des audits réguliers pour garantir sa bonne protection et son amélioration permanente.

Matériel réseau fourni par Siemens

Lorsque l'utilisation de matériel Siemens pour le cryptage de routeur à routeur se révèle la meilleure solution, vous pouvez compter sur une technologie conforme aux normes du secteur en termes de protection des données. Des routeurs conformes aux normes et dotés de fonctionnalités IPSec, VPN et HTTPS Proxy certifiées sont exclusivement utilisés.

Contacts et informations

Pour obtenir plus d'informations sur notre plate-forme SRS et notre offre de services distants, veuillez contacter votre représentant commercial Siemens local.

Nous serons ravis de vous aider à configurer votre équipement pour mettre en place une connexion SRS sécurisée.