

Aperçu de la technologie et de la sécurité :

Services de gestion à distance CARESTREAM Smart Link

Carestream Health a adopté une technologie innovante afin de fournir l'offre de services à distance la plus efficace du secteur. Ce document est destiné aux clients de Carestream, en particulier aux responsables et administrateurs informatiques, et décrit la configuration, la sécurité et la technologie des services de gestion à distance Smart Link (Smart Link RMS).

Smart Link RMS permet à Carestream de déployer des services à distance en toute sécurité via Internet pour les équipements installés derrière les pare-feux des clients. La solution est conçue pour apporter des performances et une sécurité élevées à tous les niveaux de son architecture.

En utilisant des services Web pour établir une communication sortante sécurisée sur Internet, Smart Link RMS relie les équipements Carestream aux serveurs Smart Link Enterprise de CARESTREAM. Votre équipement peut fournir des données de performance, des alertes et des alarmes à notre équipe d'assistance, ce qui se traduit

par un service et une assistance proactifs et rapides avec des capacités avancées de dépannage à distance. Aucune information sur le patient et l'utilisateur n'est collectée par Smart Link RMS.

Composants de la solution

Les deux principaux composants techniques de Smart Link RMS sont l'agent et le serveur.

Le serveur permet à l'équipe d'assistance Carestream de :

- Consolider et analyser les données.
- Effectuer des diagnostics à distance.
- Définir des règles automatisées pour prendre des mesures lorsque des événements spécifiques se produisent.
- Spécifier la sécurité et l'accès aux dispositifs des clients.
- Configurer les mises à jour logicielles pour la distribution.

Fonction	Avantage
Surveillance des dispositifs	Notifications d'alerte automatiques à l'équipe de service. Aucune action client n'est requise.
Historique consolidé des données du dispositif stocké pour chaque dispositif	Dépannage avancé grâce à un historique complet des performances du dispositif.

Fonction	Avantage
Gestion à distance et contrôle du bureau	Facilité de formation. Dépannage et corrections rapides.
Diagnostic à distance	Dépannage et corrections rapides.
Gestion du logiciel	Mises à jour logicielles pratiques, rapides et sûres.
Service et assistance à distance centralisés	Réponses rapides et capacités d'assistance après les heures de bureau.

Tableau 1 : Fonctions et avantages

Agent	Serveur
Est installé sur les sites des clients ; le logiciel embarqué est installé directement sur le dispositif médical.	Réside dans les centres de données à distance autorisés par Carestream.
Gère les fonctions Smart Link RMS sur le site du client.	Communique avec l'agent à l'aide de services Web sécurisés.
- Établit des communications sécurisées avec le serveur via Internet. - Envoie les données de la machine et les fichiers journaux au serveur. - Surveille les performances de l'appareil et envoie une alarme au serveur. - Prend en charge le téléchargement et le déploiement à distance des mises à jour logicielles à partir de Smart Link Enterprise Server.	- Traite les fichiers de données et les alarmes de l'agent. - Est la console de gestion pour Smart Link Remote Services.

Tableau 2 : Composants techniques

Configuration de la solution

L'agent établit une connexion au Smart Link Enterprise Server à partir de la sécurité de votre pare-feu d'entreprise, en respectant vos politiques de sécurité. Il n'est pas nécessaire d'apporter des modifications spéciales à un serveur proxy.

Au sein de votre réseau, l'agent est comme un autre ordinateur personnel sur le LAN. La configuration de l'agent sur votre site

nécessite :

- Une connexion physique ou sans fil à un LAN existant (TCP/IP)
- Un accès Internet sortant pour l'appareil (ou via un proxy)

Un technicien de maintenance (FE) de Carestream configurera l'Agent sur le ou les appareils et configurera les connexions réseau en fonction de vos besoins informatiques.

Série de fiches techniques | Services de gestion à distance CARESTREAM Smart Link

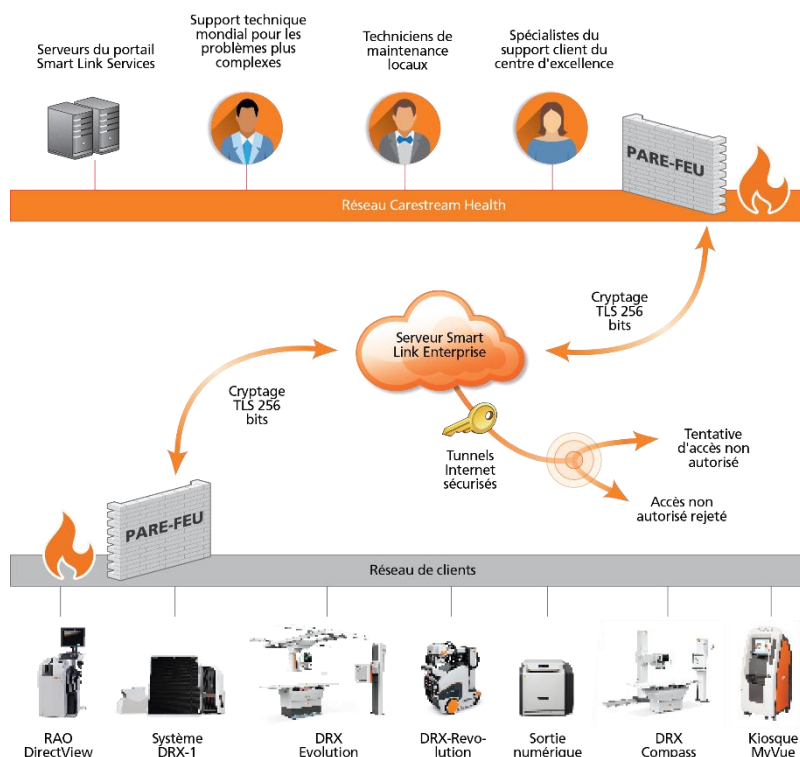


Figure 1 : Les périphériques dotés de l'agent Smart Link RMS sont configurés de la même manière que tout autre périphérique informatique compatible réseau sur votre LAN.

Technologie et sécurité

L'agent est efficace et n'affecte pas les performances optimales de votre équipement, grâce à trois caractéristiques de conception principales :

- L'agent interroge l'appareil à des intervalles gérables de 60 secondes.
- L'agent peut transmettre des données au serveur à des heures planifiées ou lorsqu'un code d'erreur indique qu'une notification immédiate est nécessaire.
- Le protocole de messagerie délivre de petits messages efficaces (0,5 à 3 Ko) ; les communications Smart Link RMS n'affectent pas la bande passante du réseau.

Sécurité du réseau

L'objectif de Smart Link RMS est de prendre en charge vos normes de réseau et vos pratiques de sécurité existantes, tout en maintenant un haut

niveau de sécurité des communications et de confidentialité des données. Smart Link RMS nécessite uniquement une connexion sortante via le port 443 (https). Carestream ne demande pas à votre service informatique de faire des exceptions aux politiques informatiques établies qui compromettraient votre pare-feu. Smart Link RMS applique la sécurité à trois couches : appareil, réseau et entreprise. Les couches sont construites à l'aide d'une technologie conçue pour des communications Smart Link sécurisées et efficaces.

Cette technologie comprend :

- Une conception logicielle renforcée pour la sécurité des applications et des données
- La prise en charge des normes du secteur telles que TCP/IP, HTTPS, SOAP et XML

Couche du dispositif	Couche réseau	Couche entreprise
- Est renforcée pour fonctionner 24 heures sur 24 et 7 jours sur 7 dans des environnements de production ; redémarre automatiquement en cas de défaillance du système ou du logiciel - Fonctionne comme un service système plutôt que comme une application - Prend en charge le cryptage TLS 256 bits - Prend en charge les certificats numériques pour l'authentification des terminaux - Prend en charge l'audit des événements du système de dispositifs médicaux localement, ainsi que sur le serveur Smart Link Enterprise, permettant un accès local aux journaux et aux fichiers d'audit	- Prend en charge le cryptage TLS 256 bits - Utilise les communications basées sur le serveur d'interrogation pour fonctionner dans les pare-feux d'entreprise - Prend en charge l'équilibrage de charge du trafic réseau	- Fournit le cryptage TLS par défaut pour toutes les communications - Nécessite une authentification par nom d'utilisateur et mot de passe - Prend en charge les certificats numériques pour une sécurité accrue - Prend en charge l'autorisation au niveau de l'utilisateur pour les fonctions de l'application, limitant l'accès aux appareils, vues de données et interactions - Prend en charge un audit de l'accès aux appareils, des interactions des utilisateurs et des événements système

Tableau 3 : Spécifications techniques pour la sécurité à chaque couche

Pas de ports spéciaux

Les solutions d'accès à distance d'autres fabricants peuvent imposer l'utilisation d'un numéro de port spécifique. L'administrateur réseau doit ensuite configurer le pare-feu de sorte que les connexions à un port TCP spécifique, tel que 5631, du côté public du pare-feu, soient mappées au port 5631 sur l'appareil, ce qui nécessite une adresse IP statique attribuée à l'appareil. S'il y a plusieurs périphériques sur le réseau local de l'entreprise, des périphériques supplémentaires doivent être affectés à des ports différents, statiques et non standard sur le pare-feu.

Dans ce scénario, le pare-feu doit être configuré de sorte que seuls les périphériques autorisés établissent des connexions sur ces ports spécifiques, ce qui impose une charge supplémentaire à l'administrateur réseau. Les utilisateurs non autorisés pourraient également rechercher le port spécifique et utiliser des protocoles pour découvrir

ce qui se trouve sur cette connexion. L'agent Smart Link RMS ne nécessite pas de port spécial.

Aucune adresse IP fixe n'est requise pour la communication

La capacité de l'agent à communiquer avec le serveur d'entreprise est indépendante de l'adresse IP du périphérique pris en charge. Les configurations de pare-feu typiques permettent aux connexions sortantes de s'initier en toute sécurité derrière le pare-feu, sur le port 443 (https). L'agent communique via le pare-feu à l'aide du port 443 et initie une communication sortante vers le serveur Smart Link RMS Enterprise. Étant donné que toutes les communications sont sortantes, votre réseau d'entreprise n'a pas besoin d'accepter les connexions de l'extérieur ou d'ouvrir des ports supplémentaires. L'équipement activé pour Smart Link RMS n'accepte pas les connexions de n'importe quel système en dehors du pare-feu d'entreprise du client.

Se connecte uniquement au serveur Smart Link Enterprise

Un problème important pour les responsables informatiques est de savoir si une connexion se fait avec Smart Link Enterprise Server ou avec une entité inconnue. Si l'agent écoute sur un port TCP en attendant une connexion, le périphérique peut devenir une cible potentielle pour un accès non autorisé. Avec Smart Link RMS, Carestream peut garantir l'identité du Smart Link Enterprise Server pour l'agent Smart Link qui se connecte à l'aide de certificats numériques. Par conséquent, l'identité n'est jamais un problème. L'agent envoie une demande chiffrée de nouvelles instructions au serveur Smart Link Enterprise de confiance et n'agit ensuite que sur les réponses reçues du serveur Smart Link Enterprise de confiance.

Flexibilité

L'agent de service ne dépend pas d'une adresse IP statique ou de sous-réseaux et prend en charge les infrastructures de réseau d'entreprise qui nécessitent des serveurs proxy Internet (proxy à configuration automatique, proxy HTTP). La flexibilité et la compatibilité de l'agent peuvent s'adapter à l'évolution des infrastructures réseau.

Tunnel sécurisé exclusif aux utilisateurs des services à distance Smart Link

Une fois que l'agent a établi un tunnel point à point sécurisé avec Smart Link Enterprise Server, la connexion n'est visible que pour les clients et services Smart Link RMS (utilisateurs et applications). Les clients et services non autorisés qui tentent d'occuper un port et un protocole TCP libres ne peuvent

pas utiliser la connexion ou établir une nouvelle connexion. Par conséquent, les entités non autorisées ne peuvent pas utiliser la connexion, même si elles peuvent la voir.

Sécurité sans VPN

L'agent initie un tunnel de communication bidirectionnel conforme à l'environnement informatique sécurisé sur le site du client, éliminant ainsi le besoin d'un réseau privé virtuel (VPN) pris en charge par le matériel. L'agent ne nécessite qu'une connexion Internet. C'est moins compliqué et moins coûteux que la fourniture, la configuration et la maintenance du matériel VPN.

Le personnel de service Carestream et l'équipement Carestream se trouvent dans des réseaux différents, tandis que le personnel VPN se trouve dans le même réseau.

De plus, le personnel de service Carestream ne peut accéder à l'équipement Carestream que via les serveurs Smart Link RMS. Tous les autres équipements sur le même réseau ne sont PAS visibles par Carestream. Alors que via VPN, l'ensemble du réseau et toutes les ressources sont ouverts aux utilisateurs.

Transmission sécurisée des données

Toutes les transmissions de données sont cryptées à l'aide du protocole TLS 256 bits, la même technologie que les banques utilisent pour les transactions financières sécurisées en ligne. Les agents du périphérique Smart Link RMS valident les certificats numériques avec le serveur Smart Link Enterprise avant d'accepter les demandes ou d'envoyer des données.

Collecte sécurisée des données

L'agent ne recueille que les données de l'appareil relatives aux performances et à l'utilisation de votre équipement. Carestream ne collecte ni ne stocke vos informations confidentielles ou exclusives. Carestream surveille les données telles que les codes d'erreur, les fichiers journaux et d'autres propriétés de l'appareil qui facilitent le dépannage de l'équipement, les tendances de performance et la résolution des problèmes. L'accès du bureau à distance à l'équipement utilisant Smart Link RMS nécessite un strict respect de la politique de Carestream (comme indiqué dans la formation sur le service), qui est conforme au RGPD car il ne collecte, ne transmet et ne stocke AUCUNE information personnelle.

Accès sécurisé au serveur

Au niveau de l'entreprise, Smart Link Enterprise Server permet uniquement aux utilisateurs autorisés par Carestream de se connecter avec une authentification par nom d'utilisateur et mot de passe. Les profils de connexion des utilisateurs contrôlent les clients, les

équipements et les fichiers auxquels l'utilisateur peut accéder ainsi que le niveau d'accès autorisé. Toutes les sessions d'accès à distance sont enregistrées à des fins d'audit. Les clients peuvent également activer la notification de bureau à distance. Une fois cette option activée, les clients sont avertis lorsqu'une demande de bureau à distance est lancée. Si le client ne répond pas, la demande de bureau à distance est automatiquement rejetée.

Conclusion

Carestream s'engage à améliorer continuellement votre expérience du service en investissant dans de nouvelles méthodes d'assistance et en les mettant en œuvre. Smart Link RMS utilise la technologie actuelle pour fournir une approche de service optimisée et simplifiée pour votre produit Carestream, tout en respectant les réglementations essentielles en matière de sécurité et de confidentialité. Pour plus d'informations, veuillez contacter votre représentant Carestream local ou consulter www.carestream.com/smart-link-services.