AGFA
RADIOLOGX
SOLUTIONS

Secure Remote Service System (SRSS)

Security information

White paper

AGFA

Table of contents

AGFA RADIOLOGY SOLUTIONS

SRSS INTRODUCTION

Agfa's Secure Remote Service System (SRSS) is a centralized connection infrastructure that helps to reduce a hospital's administrative overheads by keeping its Agfa systems running at top performance. SRSS integrates technology based on industry-accepted best practices (such as demilitarized network design) for maximum security.

Using SRSS, Agfa can also remotely manage and maintain software, throughout its lifecycle on Agfa systems, in a controlled and standardized way, to ensure maximum system uptime and avoid disruptions.

SRSS delivers the following key benefits:

- Faster repair times
- Prevention of unscheduled downtime
- Remote diagnosis
- Improved patient throughput
- Software maintenance

Agfa controls its employees' access in order to protect customer data privacy and security through:

- Rapid authorization administration
- State-of-the-art-technology

SRSS Capabilities

Remote Diagnosis

SRSS is designed to promote safe, remote support for Agfa products, using a secure, persistent IPSec connection between the Agfa service network and the Agfa equipment at the customer's site.

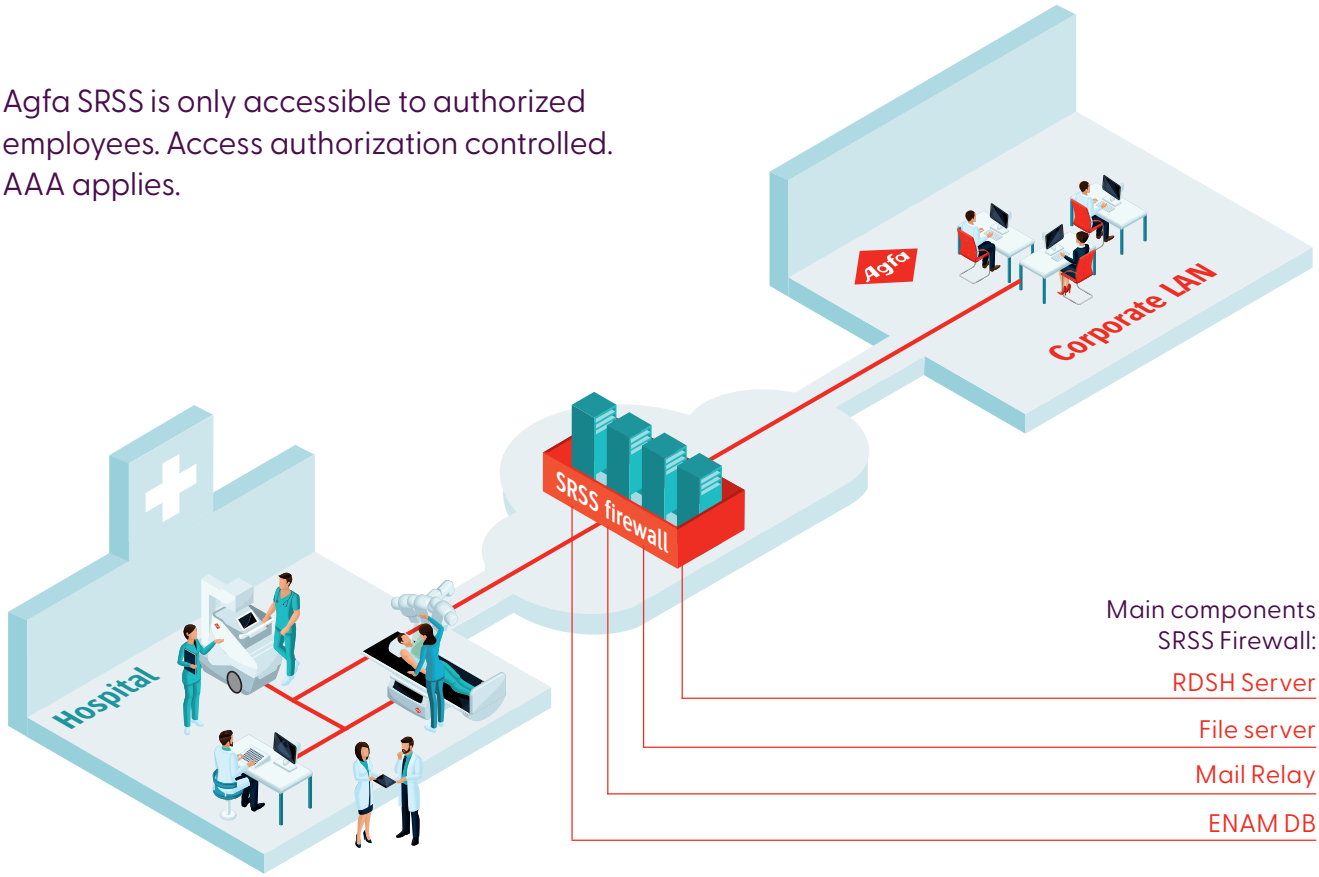
This enables a fast and reliable connection that links the customer's medical devices to the Agfa support centers around the world, via an encrypted network connection across the internet.

Based on the Service Level Agreement and the type or severity of the issue, systems are proactively monitored around the clock by the software, and a support engineer can run diagnostics and take necessary corrective actions to restore normal operations to customers.

SRSS can be used for:

> Monitoring equipment operation and system status
> Running diagnostics
> Log File Analysis: most problems can be detected and corrected based on retrieved data
> Resetting subsystems in the shortest amount of time possible to restore normal operations to customers

Agfa SRSS is only accessible to authorized employees. Access authorization controlled. AAA applies.



Security and privacy

Data security and protection are Agfa's top priority when maintaining and servicing equipment, whether on site or remotely. Agfa has developed a multi-layered approach to data protection.

Agfa does not touch patient data and all data is pseudo anonymized. Agfa always addresses data isolated on a device, and not on the whole network. Connections occur via terminal servers, which act like proxies and provide an additional layer of security.

Agfa's seven layers of parallel security:

1. Connection via VPN (virtual private network), so there is no direct link to the internet.

2. Agfa equipment can only be accessed with specific access rights.

3. Agfa employees must create an account on the equipment before they can access it. This is done via Agfa's Triple-A access system, which enables a very granular determination of who has accessed what and when. All access is documented.

4. For customers using a VPN or DMVPN (Cisco Dynamic Multipoint-VPN), Agfa requires access to the hospital network before employees can access the devices. For customers using BeyondTrust1 or TeamViewer, Agfa does not require access to the customer network.

5. Agfa remote service engineers require access to the utility tool ENAM (Enterprise Access Management) in order to be able to access any customer device. If BeyondTrust or Teamviewer is used for the connectivity, an account in these systems is also required.

6. Agfa's SRSS and ENAM network architecture requires its own access credentials.

7. Agfa protects the data in its own network. Agfa's data centers are ISO 27K certified.

SRSS takes into account the technical feasibility for customer organizations of differing complexities, as well as the basic legal requirements in the USA (HIPAA) and Europe (GDPR). This simplifies customers' adherence to the applicable legal requirements.

SRSS capabilities are implemented to meet the demands of international safety standards:

> defined by HIPAA (Health Insurance Portability and Accountability Act 1996)
> defined by other information authorities, like ISO-IEC-17799.

SRSS patching policy

All SRSS systems are patched with OS security patches, according to the following policies:

> Agfa uses the Microsoft Severity Rating System.
> All servers are updated and patched with Microsoft SUS.
> Critical security patches process in place, they are to be applied within two weeks.

SRSS access policies

Agfa remote service engineers are technical experts specially trained and screened to deliver remote services.

All connections are logged (reason, user, time, etc.) regardless of who is connecting or why. On request, the hospital can be informed about connection details.

User identification

Agfa uses the most up-to-date encryption methods to protect customer data from unauthorized access during transmission.

Most commonly, Triple-A (Authentication, Authorization and Accounting) access control is followed.

> **Authentication** is the verification of the identity of the person initiating the connection. SRSS performs a thorough identification and authentication, and checks whether the user is entitled to this access.
> **Authorization** can range from a simple one-time authorization, up to a granular authorization for multiple applications and networks.
> **Accounting** refers to the network resource tracking of users.

AGFA RADIOLOGY SOLUTIONS

Typically, the following information is gathered and documented:

> User identity
> Reason for the service
> Applications used
> Beginning and end of access

After passing the Triple-A access control, access is granted to SRSS, and the user may access customer systems according to their specific authorization.

Granting/changing access

SRSS user authorization management is handled through the User Administration Tool (UAT): Agfa's standard tool for requesting new or additional services, hardware, and software. It offers a direct and efficient method for managing SRSS roles.

The procedure for granting SRSS access is as follows:

> The user starts a request for SRSS access.
> The Line Manager approves the request.
> The request is sent to an SRSS Administrator for review.
> The SRSS Administrator or a colleague responsible for dedicated roles or a regional organization gives the final approval.
> ICS Operations updates the user profile.

Access closure

If a user account is closed, UAT automatically starts the delete request for all associated software, hardware and services including SRSS.

Active Directory accounts are closed via script. As a result, the user can no longer access the Agfa network or SRSS.

Connection technologies

SRSS connection technologies

Customers can choose between different options for a connection using SRSS:

> Site-to-Site VPN (Virtual Private Network):
> Cisco DMVPN (Dynamic Multipoint VPN)
> BeyondTrust/ TeamViewer (SSL/TLS VPN)

The choice depends upon the customer's deployment preferences and existing IT infrastructure.

Site-to-Site VPN

Connecting source authentication is ensured through standard Internet Key Exchange (IKE), using pre-shared keys. IKE peers authenticate each other by computing and sending a keyed hash of data that includes the pre-shared key. If the receiving peer can independently create the same hash using its pre-shared key, it 'knows' both peers must share the same secret, thus authenticating the other peer.

DMVPN

DMVPN uses encryption (IPSEC, AES256) and other security mechanisms in the same way as the Site-to-Site VPN connections, guaranteeing data protection for the customer and the patient health information.

Incoming remote requests are denied. Unauthorized remote access to the customer devices is not possible.

BeyondTrust

The architecture of the BeyondTrust application environment relies on the BeyondTrust Appliance, which is hosted within the SRSS DMZ as a centralized routing point for all communications between application components. All BeyondTrust sessions between users and remote systems occur through the server components that run on the appliance. To protect the security of the data in transit, BeyondTrust uses 256-bit Advanced Encryption Standard (AES) SSL to encrypt all application communications.

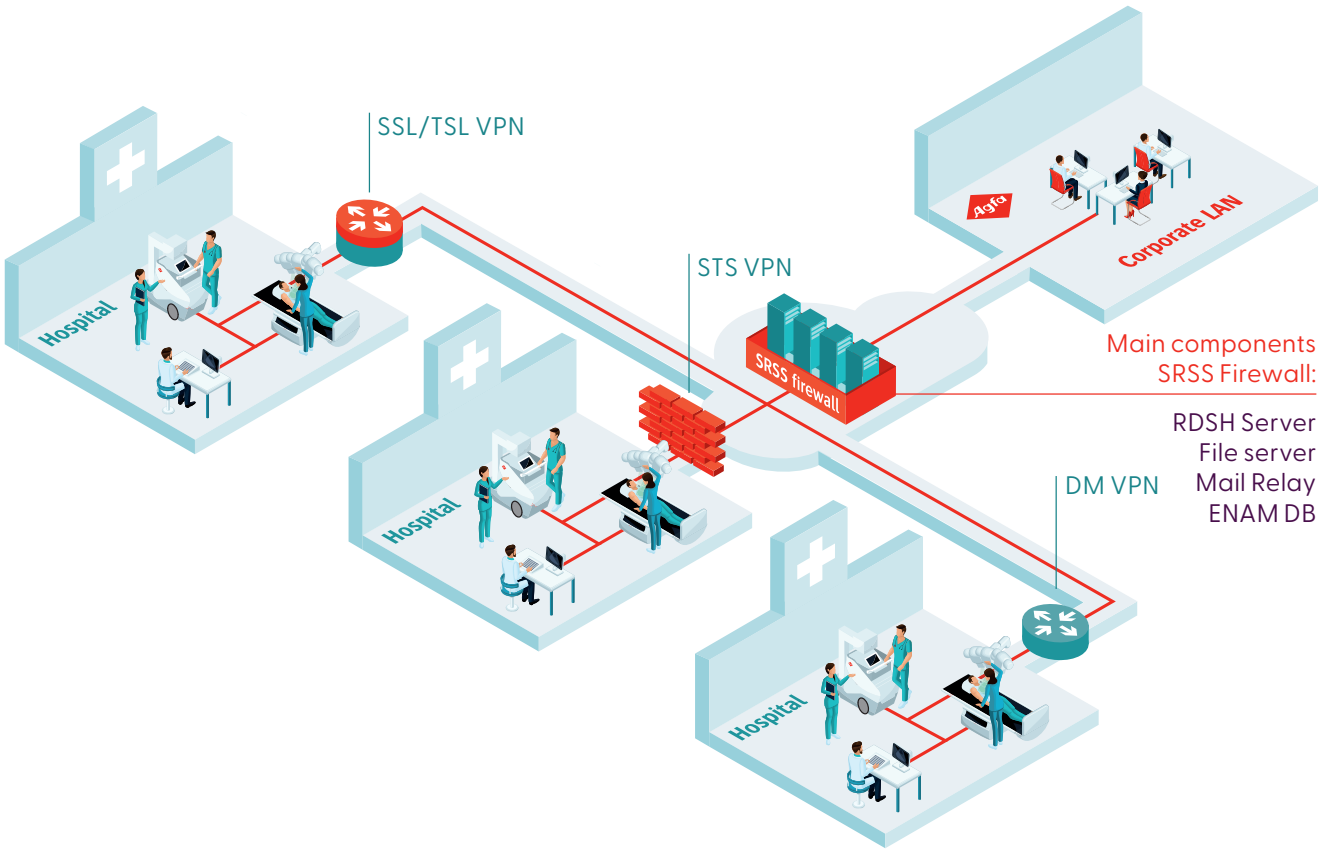
AGFA RADIOLOGY SOLUTIONS

Network performance with SRSS

Agfa service sessions are generally infrequent and brief, typically lasting for only a few minutes and transferring very small amounts of data.

For larger files such as software purchases, upgrades, service packs, hot fixes, patches or trials, the customer determines the timing, and can plan them for when they will have the smallest impact on the network connection.

Agfa SRSS is only accessible to authorized employees. Access authorization controlled. AAA applies.



AGFA RADIOLOGX SOLUTIONS

Follow us:

agfa.com » Septestraat 27 - 2640 Mortsel - Belgium

GB 202409

AGFA