AGFA
RADIOLOGX
SOLUTIONS

MUSICA® Analytics Data Transfer and Security

Leveraging technology and best practices

White paper

AGFA

Table of contents

AGFA RADIOLOGY SOLUTIONS

Introduction

With MUSICA® Analytics, Agfa Radiology Solutions is putting its long history and expertise as an X-ray equipment vendor to work to help hospitals and imaging departments overcome operational challenges, while increasing imaging quality and workflow.

MUSICA® Analytics delivered as part of MyAgfaRadiologySolutions will provide insight in workstation workflows. Depending on the SMA contract, 2 types of dashboards are available:

- Standard dashboards provide basic information with respect to number of images/exams done, reject rates and dose statistics for the connected MUSICA workstations of the last 6 months. These dashboards will be made available for customers not having a platinum full maintenance agreement.
- Premium Dashboards provide more detailed information on the images/exams done, reject rates, reject reasons and dose statistics. These dashboards will be made available for customers having a platinum full maintenance agreement.

To enable MUSICA® Analytics, Data Analytics from the MUSICA workstation log files are used. And transferred to a secured cloud space where the analytics calculations are performed.

Data protection is the focus of our attention as there is always a great concern surrounding security breaches resulting from missing or ignored procedures and practices. In this document we want to highlight the best practices Agfa put in place and we will answer questions regarding the data transfer, handling and security, specifically:

1. **Data Security and Privacy** - Regulating identities across the globe, such as the European Union with GDPR are taking measures to protect private data.
2. **Data Access** - Registering and documenting all access to sensitive data
3. **Data Collection** - Retrieving periodic log files with utilization data
4. **Data Transfer** - Secure and protected upload of anonymized log file data

Data Security and Privacy (GDPR)

User and connection security are critical aspects of remote access services and tools. To maximize safety, we use technology that integrates industry-recognized best practices, such as secure network design.

In our GDPR-compliant process, the log file data is pseudonymized (which means that only the hospital can trace back the identity of the person) and we do not touch patient data. The solution therefore ignores patient data (such as patient ID, name, RIS/PACS, admission, study IDs etc). We keep the recording of personal information to the strict minimum, and use pseudonymized information only. Agfa will not keep pseudonymization reference data, only the customer will be able to trace back this information.

Data Access Control

Agfa leverages state-of-the-art technology, to control all data access in a granular way. Only our dedicated MUSICA® Analytics consultant and our dedicated administrators can access the data.

Our MFA (Multi Factor Authentication) requires a password as well as a unique code generated via a cell phone to avoid misuse.

Data Collection

The Data Collection Tool software installed on each NX/MUSICA® Acquisition Workstation enables the workstations to upload the usage data from your Agfa direct radiography (DR) system to a secured cloud space where the analytics calculations are performed. Running as a priority B process, uploading can be scheduled for any convenient time.

Access is only needed to a specific set of URLs:

- https://*.amazonaws.com
- https://helicensing.agfa.net/

AGFA
RADIOLOGY
SOLUTIONS

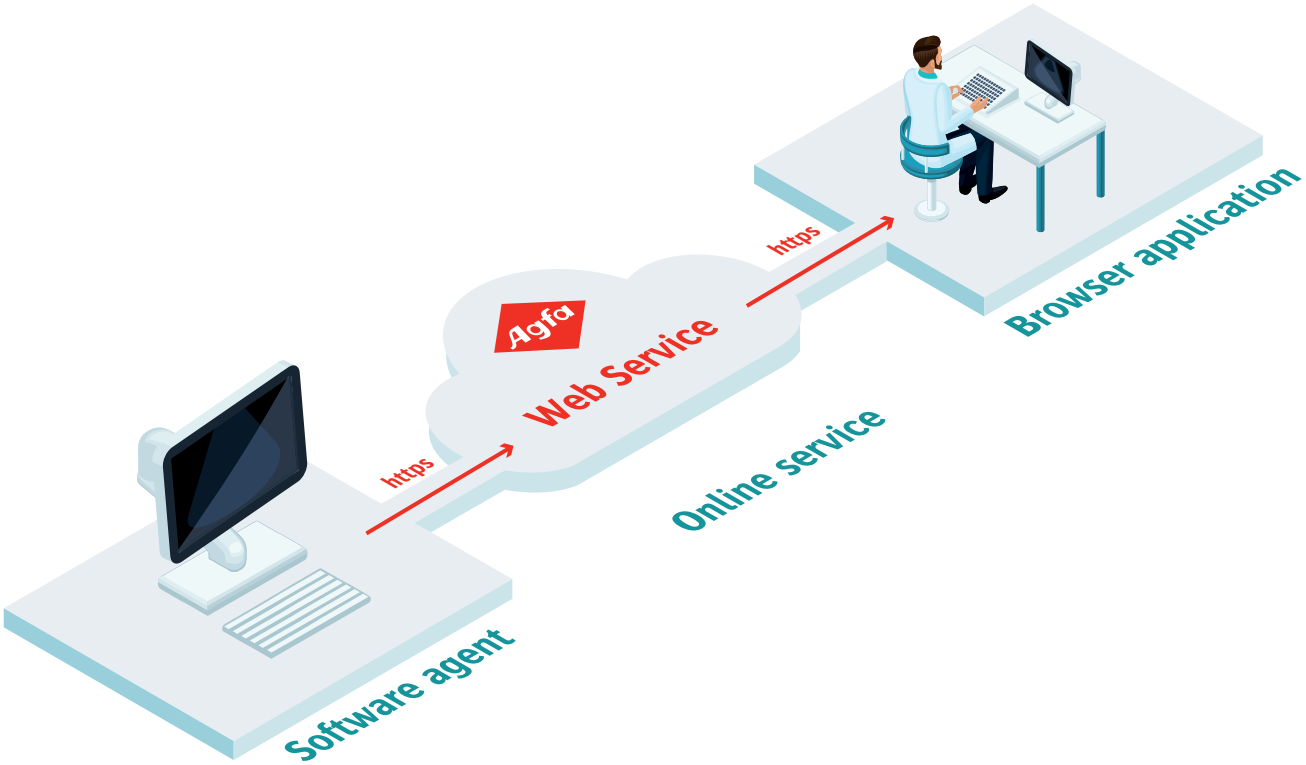
Data Transfer

Security

For the data transfer, all network communication exclusively occurs with the https protocol – unencrypted http is not used anywhere in the solution. Furthermore, the customer's IT department needs to only register the URLs needed for MUSICA Analytics, and restrict them to https on port 443 in the firewall. IP address-based firewall rules should be avoided because IP addresses are not static over time.

The Agfa Web Service encrypts all communications using the AWS IoT (Amazon Web Service - Internet of Things) message broker working with the Transport Layer Security (TLS) 1.2. A 2048-bit length RSA algorithm provides https encryption using TLS version 1.2 or higher; older SSL implementations are not allowed.

Agfa uses the AWS Security Token Service (STS) to create and provide trusted users with temporary security credentials that can (only) upload data to the cloud.



Cloud

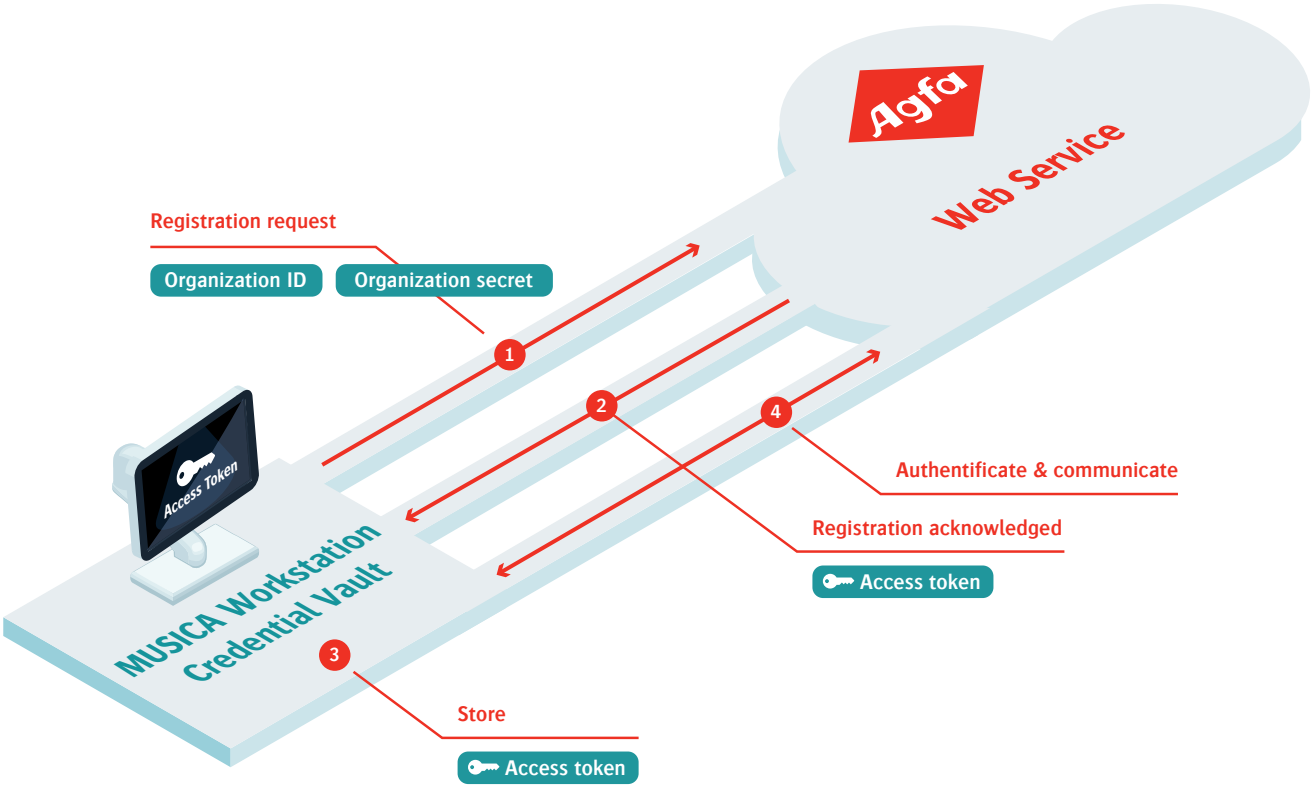
Internet of Things (IoT) technology enables solutions that offer secure connection for many devices in a scalable manner, making the relay/gateway server obsolete.

With no gateway server, Agfa's solution is more secure against cyber-attacks, because:

- The attack surface is reduced; and
- The risk of running a server without the latest security patches is removed.

By using the cloud, and eliminating the need for local server components, deployment is simplified and total cost of ownership significantly reduced. The central cloud-hosted platform is maintained by AWS and Agfa in a shared responsibility; Agfa connects to the online service that provides central data storage functionality and Agfa consultants can log in via the customer portal. Data is stored in Germany.

- customers can only access their own data
- encryption of data in the cloud
- data is deleted after 5 years

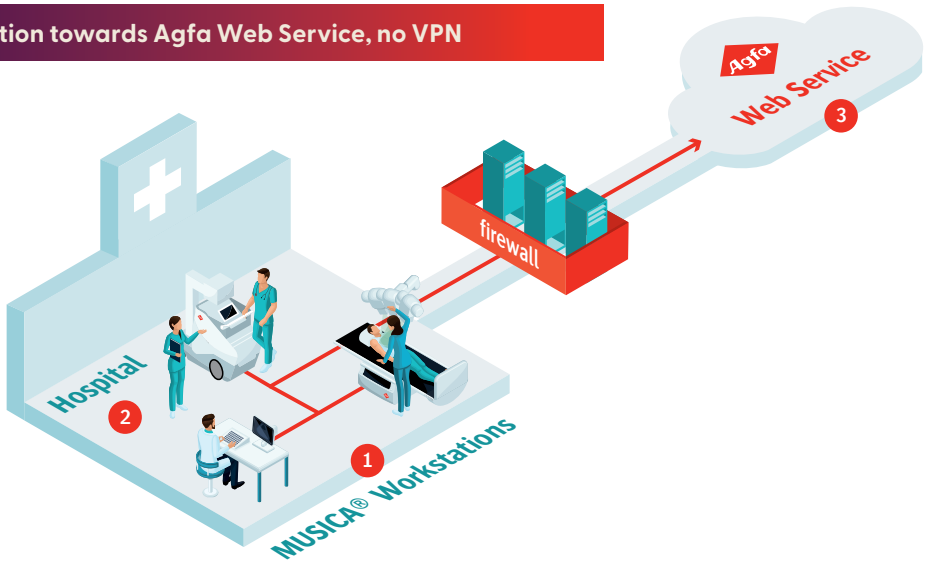


AGFA RADIOLOGY SOLUTIONS

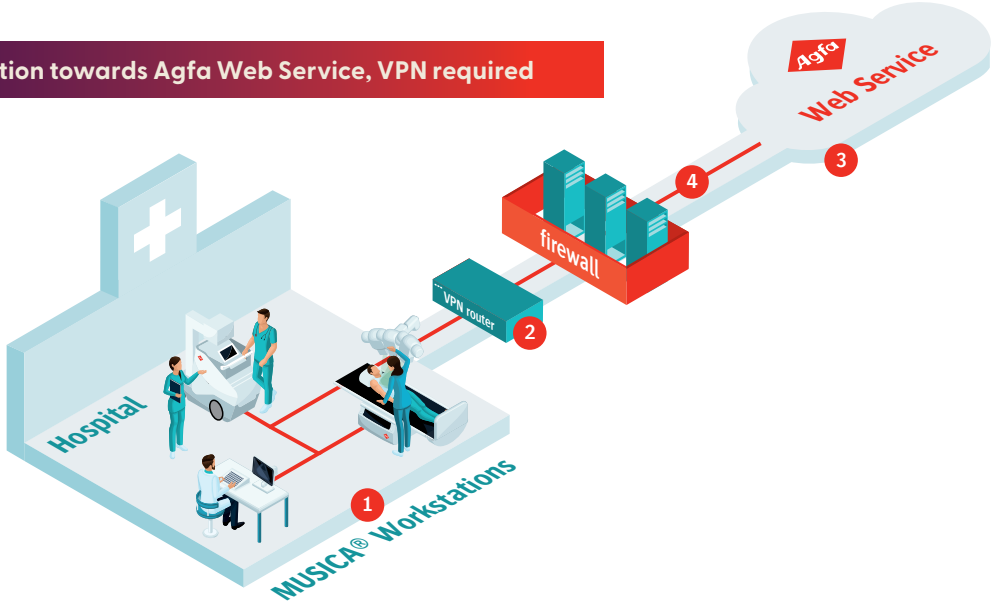
Direct connection

Only strongly encrypted network communication is used, with a direct connection towards the Agfa Web Service, whether with or without a VPN.

Direct connection towards Agfa Web Service, no VPN



Direct connection towards Agfa Web Service, VPN required



1. When a data collection tool is running on MUSICA® NX:
   - data is collected at regular time intervals (between once per day and once per week);
   - patient and operator data is anonymized or pseudo-anonymized;
   - up to 100 Mb/day per workstation can be collected.

2. Data is sent to the cloud in a secure way, using TLS version 1.2 or higher.
   User authentication is required to access the cloud.

3. A cloud can be set up by region, ensuring that data remains within that region (e.g., Germany).

4. A VPN is set up with the cloud.

AGFA RADIOLOGX SOLUTIONS

Follow us:

agfa.com » Septestraat 27 - 2640 Mortsel - Belgium

EN 202311

AGFA