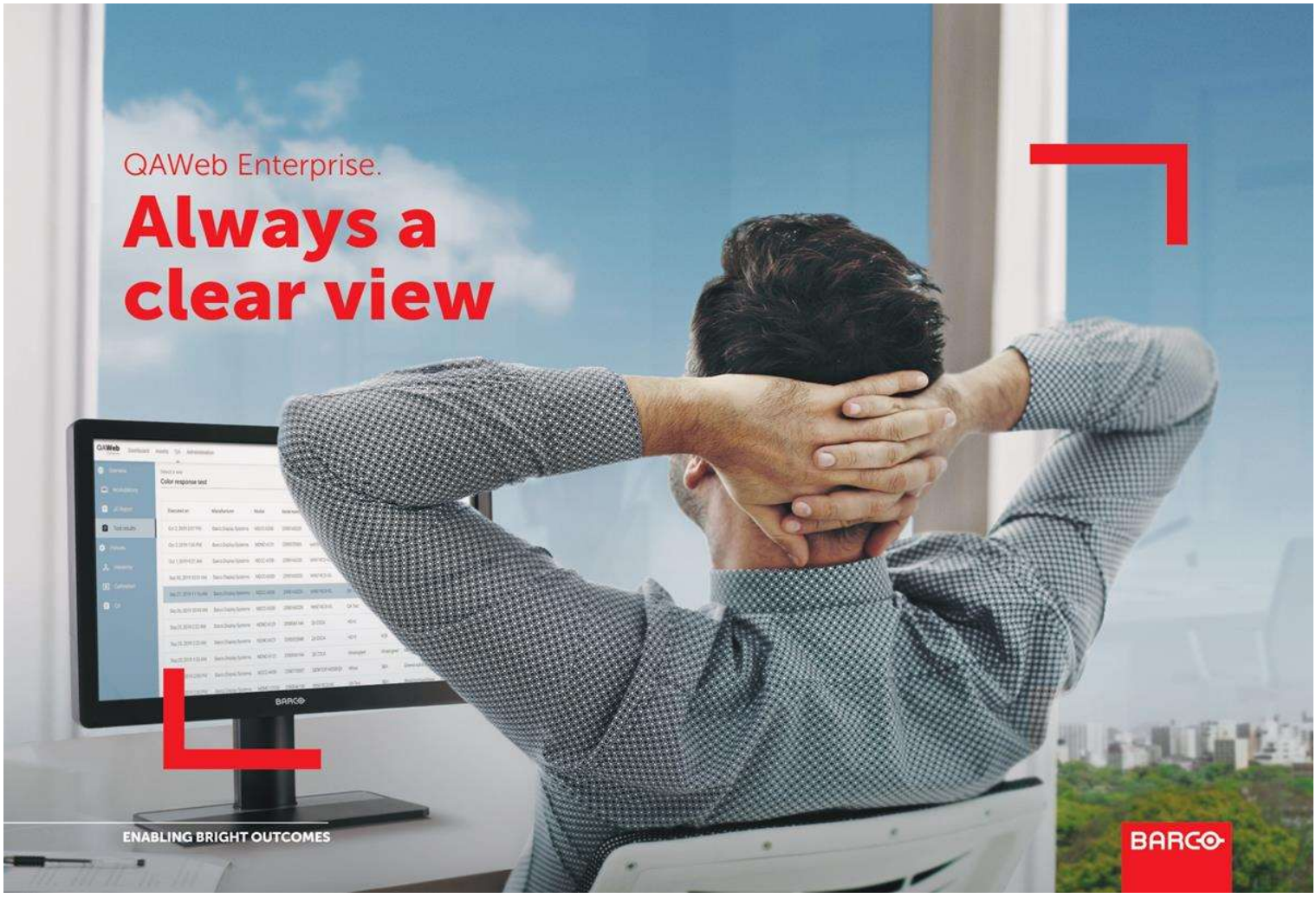
QAWeb Enterprise Security and Connectivity

Frequently Asked Questions

DATE 7/11/2022

AUTHOR **Frederik Vannoote** | Product Owner



Introduction

The purpose of this document is to provide answers to frequently asked questions related to the data handling and security of QAWeb Enterprise.

QAWeb Enterprise is used by healthcare organizations to manage quality and compliance of diagnostic displays used by radiologists and other medical specialists to view medical images throughout the medical imaging workflow. In this document, we'll refer to 'organization' as such a healthcare entity.

QAWeb Enterprise is a solution composed of two main components:

- **QAWeb Enterprise Agent**.The Agent is a low footprint software product that is to be installed on each radiologist workstation using Barco displays. Running primarily as a background process, the Agent is mainly responsible for communicating with the Barco display hardware, verifying settings, and executing periodic calibration and quality assurance tasks. It communicates to the online service using the https protocol.
- **QAWeb Enterprise Portal and Online Service**. The central cloud-hosted platform maintained by Barco fulfills two main functions. (1) The Agents connect to the online service to retrieve their managed settings. They send their status and task results to the online service, which provides central data storage. (2) The Portal is a web application that end-users can log in to using a supported web browser. Using the Portal, users can configure settings, view test results, and troubleshoot issues remotely.

Users and privacy

Does QAWeb Enterprise store patient information?

No. QAWeb Enterprise has no access to PHI (Patient Health Information). The solution is completely agnostic about patient data or other information (e.g. admission numbers, study ID) present in the PACS or RIS software installed on the workstation.

Does QAWeb Enterprise store personal information?

The amount of personal information recorded is kept to the strict minimum:

- For users that have an account (to log in to the web client), the email address is stored because it is the unique account identifier. The name and first name are stored to easily identify users.
- For manually executed QA tests, the person running the test is asked to type in an identifier or callsign, because this is needed as a reference in the report of that QA task execution.

No other types of personal information or sensitive information are processed.

For further details on what data is processed, please consult the product privacy statement available at https://www.barco.com/en/about-barco/legal/privacy-policy/product-privacy-statement#qawebe .

Does each radiologist or workstation user require a QAWeb Enterprise account?

No. Only members of the organization that need to view information or need to manage the application need to have a user account. Typically, this includes:

- PACS/IT administrators
- Imaging technologists
- Medical physicists
- ...

Does QAWeb Enterprise support Single-Sign-On?

Yes, your organization can optionally enable SSO, allowing users to log in to the Portal using your OIDC or SAMLv2 identity provider. More information is available at https://www.barco.com/en/support/knowledge-base/kb12591.

Data storage and security

Where is the QAWeb Enterprise Online Service hosted?

Barco has engaged Amazon Web Services as sub-processor for its cloud services. The online service is hosted in data centers in AWS region eu-west-1 (Europe Ireland Region, see also https://aws.amazon.com/about-aws/global-infrastructure/regions_az/).

Security and compliance of the hosted solution is performed according to the AWS shared responsibility model (https://aws.amazon.com/compliance/shared-responsibility-model/).

What is Barco's approach to cybersecurity and data protection?

The following sources of information are published on the barco.com website to help you evaluate our general cybersecurity approach.

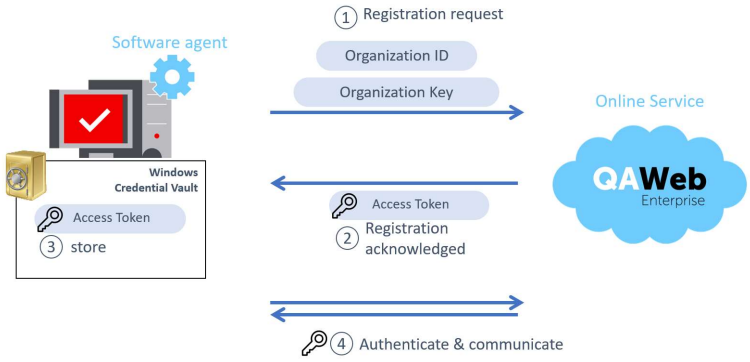
- Our integrated annual reports contain a specific chapter on cybersecurity and data protection: Annual report 2021 page 44 and further: https://ir.barco.com/2021/uploads/files/PDF/Barco-IR2021-PPC.pdf#page=45
- Certifications related to quality and security: https://www.barco.com/en/about-barco/legal/certificates
- Responsible disclosure policy: https://www.barco.com/en/about-barco/legal/responsible-disclosure

Networking requirements

How is the communication between the agent and online service secured?

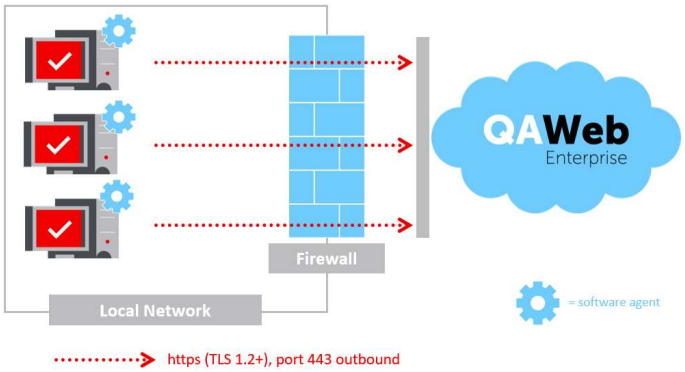
All network communication exclusively uses the https protocol, meaning that data is always encrypted in transit. Strong https encryption is achieved by using a 2048-bit length RSA, and using TLS version 1.2 or higher (older, non-secure SSL implementations are blocked).

Each agent authenticates to the online service using an id and key pair specific to the organization. The returned access tokens are stored in the credential vault of the operating system.



Which URLs need to be allowed in network firewall / routing configuration?

QAWeb Enterprise requires **outbound https access** to a specific set of URLs. The Agent does *not* open extra listening TCP/IP ports, so no inbound firewall rules need to be added.



Note that URL **firewall rules must be name-based** (and not be based on IP-addresses). The online service makes use of modern web services that are not associated with a single static IP address, which means that the IP address may change over time.

QAWeb Enterprise uses the following URLs:

URL	Purpose / provided functionality
auth.barco.com	Portal authentication.
ciam.cmp.barco.com	Portal user authentication.
qawebdata.healthcare.barco.com	Agent data back-end
a3n9amleodurj6-ats.iot.eu-west-1.amazonaws.com	Secured AWS IoT / MQTT message broker
qaweb.healthcare.barco.com	Portal web application front-end
qawebapi.healthcare.barco.com	Portal web application back-end
documentation-qaweb-agent.healthcare.barco.com	Agent online user guide
documentation-qaweb.healthcare.barco.com	Portal online user guide

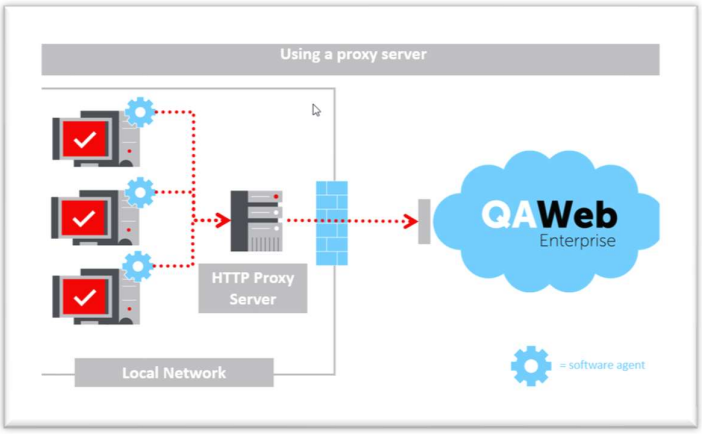
What is the purpose of the HTTPS/WSS URL?

QAWeb Enterprise uses a low-bandwidth messaging service (MQTT over Websocket-Secure) between the Agent and Online Service to provide real-time viewing of the agent's online/offline status and remotely triggering specific Agent tasks through the Portal.

The URL a3n9amleodurj6-ats.iot.eu-west-1.amazonaws.com is used to provide this secure websocket functionality and is uniquely assigned to the Barco QAWeb Enterprise product.

Can we use a proxy server with QAWeb Enterprise?

Yes, you can optionally configure the agent to connect through a proxy server. Proxy user/password authentication is supported.



Migrating from Medical QAWeb (Qaweb1)

Why is there no intermediate relay or gateway server acting as a communications checkpoint between the agent and the online service?

MediCAL QAWeb - the predecessor to QAWeb Enterprise - as well other vendor's QA software solutions require the installation of a local relay / gateway server within the network of the organization, which centralizes traffic between the agent and the online service.

The relay/gateway server was removed from the architecture for two primary reasons:

- Ease of deployment: By eliminating the need for any local server component, the effort to deploy the solution and the total cost of ownership are reduced significantly. This benefits small radiological practices (who might not have a large dedicated IT team) as well as very large entities (where multiple networks would require multiple relay/gateway servers).
- Reduced need due to technological advances: The rise of the 'Internet of Things' has led to the availability of solutions that allow to connect large amounts of devices in a secure and scalable manner, making the role of the relay/gateway server obsolete.

Does the absence of a relay/gateway server, that existed in the Qaweb1 solution, make the solution less secure?

No. As described above, only strongly encrypted network communication is used. If your organization wishes to obtain an extra level of control by directing traffic through a single point of access, you can use a standard HTTP proxy server for that purpose.

Data access

Who has access to the data?

QAWeb Enterprise only stores data on Barco Diagnostic displays. It does not deal with PII, PHI or any kind of patient data.

Every "organization" in QAWeb Enterprise is logically isolated. Users of 1 organization cannot access data in another organization. QAWeb Enterprise Agents are linked to a single organization by means of an organization id and regkey. The regkey is a secret which belongs to a single organization. The organization needs to deal with this regkey as a secret and take appropriate measure to keep it from leaking.

Barco Support staff can access the organization to assist in a support case. All attempts to access the data is logged, linked to the personal account of the individual user. Barco has put measures in place to protect the user accounts of our Support staff (rotating password, MFA, inactivation in case of 3 failed login attempts, cannot use last 5 passwords, …)

Barco uses anonymized data to improve the current version of QAWeb Enterprise and displays. This information is not disclosed with other parties. Full detail can be found in our Product Privacy Statement: https://www.barco.com/en/about-barco/legal/privacy-policy/product-privacy-statement#qawebe

General questions

Where can I find system requirements and user guide?

Please refer to the online documentation:

- Portal user guide: https://documentation-qaweb.healthcare.barco.com
- Agent user guide: https://documentation-qaweb-agent.healthcare.barco.com

Additionally, more resources can be found at https://www.barco.com/support/qaweb-enterprise.