Aperio iQC Software Module

IT Administrator's Guide

This document provides guidance on how to deploy the Aperio iQC Software Module into the laboratory environment in a way that is secure and robust.

Introduction

For research use only. Not for use in diagnostic procedures.

The Aperio iQC Software Module is a standalone software application intended to assist in identifying artifacts in whole slide images (WSIs) produced by the Aperio GT 450 Scanner. It is installed on the customer's server. The Aperio iQC Software Module analyzes copies of WSIs of hematoxylin and eosin (H&E) and immunohistochemistry (IHC) stained slides in SVS and DICOM formats.

When Aperio iQC Software Module is running, copies of WSIs from connected Aperio GT 450 Scanners are automatically analyzed. The WSIs, along with the artifact detection results, are displayed on the iQC dashboard for laboratory staff review and disposition. The user can accept or reject the Aperio iQC Module results and add comments for each scan.

To analyze images, Aperio iQC Module algorithms use static AI. The Aperio iQC Software Module is executed on copies of the original images. The Aperio iQC Software Module does not modify those images.

Network configuration

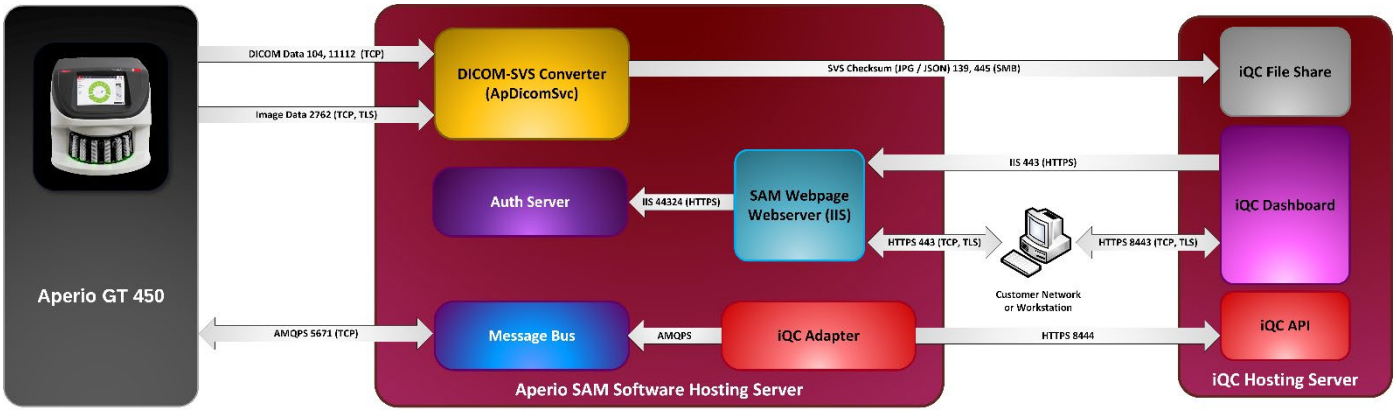
This section shows how the Aperio iQC (hosting server) interfaces with Aperio GT 450. The Aperio iQC Software Module resides on a separate server, but it requires connections to the SAM server and a dedicated file system.

To integrate with the Aperio iQC Software Module, the Aperio GT 450 uses an iQC Support Package, which is installed on a SAM hosting server to facilitate communication with the Aperio GT 450. The scanner console displays artifact information provided by the Aperio iQC Module.

User authentication for the Aperio iQC Software Module is through the SAM authentication server. The Aperio iQC Module user logs in with their SAM credentials.

The DICOM-SVS converter sends a copy of image data both to a dedicated Aperio iQC file system and to the IMS file system. The data stream to the dedicated Aperio iQC Software Module includes metadata and other files used by iQC. IMS integration is achieved by leveraging one of several configurations described in the *Aperio GT 450 Lab Manager and IT Administrator's Guide*, MAN-0394.

To protect your network from cybersecurity attacks, we recommend that you disable unused ports and services on your network.



Aperio iQC Software Module port descriptions

The table below provides a list and description of the ports used with the Aperio iQC Software Module configurations.

Port Number	Protocol	Use by SAM/Aperio GT 450/DSR	Source	Destination	Description
104	TCP	DICOM Data Tool	Aperio GT 450	SAM	DICOM TLS SCP for receiving image data from the GT 450.
139	TCP	SAM requires TCP access to this port for image data transmission	DICOM/ SVS Converter	IQC File Share	TCP image transmission, encrypted using TLS 1.2 or greater for transmission from the scanner to the hosting server and SMB3 from the hosting server to image share.
443	TCP	Secure Hypertext Transfer Protocol (HTTPS)	iQC Dashboard	SAM	HTTPS access to Scanner Administration Manager (SAM) hosting server webpage webserver (IIS.) Connections encrypted via TLS.
445	TCP	Used by SAM for image data transfer	DICOM/ SVS Converter	IQC File Share	TCP image transmission, encrypted using TLS 1.2 or greater for transmission from the scanner to the hosting server and SMB3 from the hosting server to image share.
2762	TCP	Digital Imaging and Communications in Medicine (DICOM) Transport Layer Security (TLS.) Used by SAM for image data transfer.	Aperio GT 450	SAM	DICOM TLS SCP for receiving image data from the Aperio GT 450.
5761	AMQPS	Events from Aperio iQC Services	Aperio iQC	SAM	Message bus installation for receiving event data from Aperio iQC.
8443	TCP	iQC Dashboard	Aperio iQC	User web browser	iQC Dashboard.
8444	TCP	iQC integration interface APIs	Aperio iQC	SAM	iQC integration interface APIs

Cybersecurity

This chapter discusses how the Aperio iQC Software Module protects image data and provides protections against cybersecurity threats. We also discuss the measures you can take to protect the Aperio iQC Software Module hosting server on your network. This chapter gives information for IT network administrators, Aperio product administrators, and Aperio product end users.

CAUTION: Review all guidelines in this chapter for information on protecting the Aperio iQC Software Module from cybersecurity threats.

The recommendations in this section apply to the Linux-based server used to host the Aperio iQC Software Module. The security and network settings are configured through the Linux operating system and administrative tools. The information here is provided for reference only. Refer to your Linux documentation for specific instructions.

In many cases, your facility may require security settings and configurations more restrictive than those listed here. If that is the case, use the stricter guidelines and requirements dictated by your facility

User authentication and security

A robust authentication and authorization system that leverages industry-standard mechanisms safeguards sensitive data and maintains the integrity of the Aperio iQC Module system.

Authentication of the Aperio iQC Module users is handled by an authentication service, which runs on the SAM server. The system employs the OAuth 2 protocol, an industry-standard protocol that allows users to log in using their existing SAM credentials. Once the user is authenticated, the Aperio iQC Module grants access to the user based on roles and permissions, which are configured in SAM: Operator or Lab Admin. The Lab Admin role can perform all Aperio iQC Module functions. The Operator role can perform all functions except for configuring the sensitivity thresholds for the artifacts.

Aperio iQC Software Module cybersecurity features

Cybersecurity features included in the Aperio iQC Software Module protect critical functionality despite cybersecurity compromise. These cybersecurity features are as follows:

- To reduce cybersecurity vulnerability, the software code base on the Aperio iQC Software Module is scanned for code vulnerabilities, and any vulnerabilities are mitigated.
- The Aperio iQC Software Module is not intended to store sensitive data, only to export/upload data for processing images and publishing results. The connection between the Aperio GT 450 scanner and the Aperio iQC Software Module is secured through an encrypted, secure SSL/TLS connection. In addition, the transient data is erased when the scanner is shut down or loses power.

Data protection

Data at rest (temporary storage) is to be protected by encryption. When the operating system boots up, a unique encryption key for this partition is randomly generated to encrypt all partitions that store sensitive data. The Aperio iQC Software uses BoltDB as its database. BoltDB is an embedded key/value store designed for Go. Go's encryption libraries are used for data encryption.

Sensitive Data Protection – This Leica Biosystems product is capable of input, storage, and handling of sensitive data, including personal identifier information (PII) and/or possibly protected health information (PHI). In addition to personal data such as name, address and other obvious personal identifiers, sensitive data include barcodes, accession numbers diagnostic information, and scan images, such as microscope slide labels and other labels or annotations embedded in image files. Please take appropriate precautions to protect from sensitive data exposure and theft. Handling of sensitive data is subject to local laws. Many countries have a data protection authority to ensure that data protection law is followed. For more information about your privacy rights, or if you are not able to resolve a problem directly with us and wish to make a complaint, contact your local authority.

Protected Health Information Protection - To ensure that Protected Health Information (PHI) data is protected in transit, Leica Biosystems secures all network communications using TLS. All sensitive information is transmitted between the scanner and the Aperio iQC Software Module through up-to-date TLS communications. A unique x509 device certificate is generated by the scanner during first initialization for use in all TLS communications with the Aperio GT 450 SAM and the Aperio iQC Software Module.

Leica Biosystems recommends securing the user-facing web server as well. Customers should procure webserver certificates that are valid for the servers that will be hosting Aperio iQC Software Module. If customer-procured webserver certificates are not provided, the servers will be secured with self-signed certificates.

Protecting the Aperio iQC Software Module

The following sections contain recommendations for protecting the Aperio iQC Software Module.

Password, login, and user configuration safeguards

The password requirements for users logging into the server hosting Aperio iQC web-based client are as follows:

- Passwords must be a minimum of ten characters, including:
    - At least one non-alphanumeric character (special character)
    - At least one numeric digit
    - At least one upper-case and lower-case letter
- The last five passwords recently used may not be reused
- After three invalid login attempts, the user account is locked. The user may contact a Aperio iQC administrator to unlock the account.
- We recommend you configure workstations used to log into Aperio iQC to time out screen displays after 15 minutes of inactivity and require users to log in again after that time.
- For security reasons, do not use user names “Admin”, “Administrator” , or “Demo” when adding users to Aperio iQC Software Module.

Aperio iQC hosting server administrative safeguards

- Set up users with permissions that allow them to access only the portions of the system required for their work. For the Aperio iQC hosting server.
- Protect the Aperio iQC hosting server from unauthorized access by using standard IT techniques. Examples include:
    - Allow listing, an administrative tool that allows only authorized programs to run, to be implemented on the Aperio iQC hosting server.
- Use normal care in maintaining and using servers. Interrupting network connections or turning off the servers while they are processing data (such as when they are analyzing digital slides or generating an audit report) can result in data loss.
- Your IT department must maintain the server, applying Linux and Aperio iQC security patches and hot fixes that may be available for the system, and ensure the server is configured securely. You should select a server that can be configured to detect intrusion attempts such as random password attacks, automatically locking accounts used for such attacks, and notifying administrators of such events.
- Follow your institution’s security policy to protect stored data in the database.

- We recommend implementing allow listing on the server so that only authorized applications are allowed to run.

  If you are not using allow listing we strongly recommend installing anti-virus software on the server. Run anti-virus scans at least every 30 days.

  - We also recommend that you configure the anti-virus software to exclude SVS and DICOM file types as well as the file storage from “on access scanning”. Virus scans should be configured to run during non-peak hours, as they are very CPU intensive and can interfere with scanning.

- Periodically back up the hard disks on the server.
- Aperio iQC requires read and write access to SMB storage to obtain images for processing. As a pre-requisite Aperio GT 450 SAM should have read and write access to SMB storage to store image data files.
- We recommend encrypting the contents of the server hard disks.
- The file shares on the server should be protected from unauthorized access using accepted IT practices.
- You should enable Event logging on your server to track user access and changes to data folders that contain patient information and images.
- Routinely back up the Event log file and save the backup in a secure location so you have the information if a compromise occurs that you need to investigate.

Use of off-the-shelf software

While conducting cybersecurity assessments, you may wish to consider which third-party software components are used by Leica Biosystems software. Lists of all off-the-shelf software (OTS) used by Aperio iQC Software Module are maintained by Leica Biosystems. If you would like information on OTS used, contact your Leica Biosystems Sales or Customer Support representative and ask for the Software Bills of Materials for Aperio iQC Software Module.

Support and cybersecurity patches

Note that technical support and cybersecurity patches for the Aperio iQC Software Module may not be available after the product lifetime. Contact Leica Biosystems Technical Support for more information.

Data collection notice

As part of the product use case, the Aperio iQC Software Module requires input of data images from the Aperio GT 450 Scanner. These images may contain personal or sensitive information. Information is retained for the period of 7 days for WSI identification purposes only. Data is stored and retained in the customer environment/premises.

Aperio iQC Software Module IT Administrator's Guide

MAN-0556, Revision A | December 2024

This document applies to Aperio iQC Software Module version 1.0

Copyright Notice

User Resources

- For the latest information on Leica Biosystems Aperio products and services, please visit www.LeicaBiosystems.com/Aperio.

Contact Information – Leica Biosystems Imaging, Inc.

Headquarters	Customer Support
Leica Biosystems Imaging, Inc. 1360 Park Center Drive Vista, CA 92081 USA Tel: +1 (866)-478-4111 (toll free) Direct International Tel: +1 (760) 539-1100	Contact your local support representative with any query and service request. https://www.leicabiosystems.com/contact-us/

Revision Record

Rev.	Issued	Sections Affected	Detail
A	December 2024	All	New document.

For research use only. Not for use in diagnostic procedures.