L E I C A B I O S Y S T E M S I M A G I N G

APERIO GT 450

DIGITAL PATHOLOGY SLIDE SCANNER

IT MANAGER AND LAB ADMINISTRATOR GUIDE

(NOT for use in China)

Advancing Cancer Diagnostics
Improving Lives

Leica BIOSYSTEMS

Aperio GT 450 IT Manager and Lab Administrator Guide

MAN-0394, Revision F | December 2024

This manual applies to Aperio GT 450 Controller, Aperio GT 450 Console, and Aperio GT 450 SAM versions 1.4 and later.

Original Instructions.

Copyright Notice

Customer Resources

- For the latest information on Leica Biosystems Aperio products and services, please visit 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 or service request. https://www.leicabiosystems.com/contact-us/

Importers	
Leica Biosystems Deutschland GmbH Heidelberger Straße 17-19 69226 Nussloch, Germany	Leica Microsystems (UK) Limited Larch House, Woodlands Business Park Milton Keynes, England, United Kingdom, MK14 6FG

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

CE UKCA

UDI 00815477020228, 00815477020464, 00815477020471, 00815477020563, 00815477020495

REF 23GT450, 23GT450SAM, 23GT450SAMSW, 23GT450ZSTACKSW, 23GT450-R

Table of contents

Notices

Important message

Service personnel and distributors who have access to protected patients' information must treat all such information as confidential in accordance with professional ethics, accreditation standards, and legal requirements.

Revision Record

Rev.	Issued	Sections Affected	Detail
F	December 2024	Copyright page	Added UKCA symbol and CE mark on page 2
		Aperio GT 450 network architecture	Added Image types supported (on page 19) Replaced the "Aperio GT 450 Recommended Network Configuration" section with the following sections: Overview of recommended network configurations (on page 20); Aperio GT 450 with DICOM C-STORE and third-party PACS support (on page 21); Aperio GT 450 with Aperio eSlide Manager integration from image file share; Aperio GT 450 with third-party PACS support from image share Aperio GT 450 Network Configuration Ports (on page 25) Added Aperio GT 450 with Aperio iQC Software Module (on page 24)
		System configuration	Reorganized and revised this chapter to reflect the current SAM UI and configuration settings. Added the Server configuration: Settings pages (on page 50)Added Configuring the scanner to send images to Aperio iQC Software Module (on page 60) Revised Enabling DICOM image output (on page 59)
		Cybersecurity and network recommendations	Added Data protection (on page 74); Revised and provided additional information to Protecting the Aperio GT 450 SAM server (on page 74)
E	March 2022	Front matter, Chapter 5, “User Management”	Added revision history, cautions and notes. Chapter 5: Added steps to unlock a user account.
D	January 2021	Chapter 3, “Configuring the Aperio GT 450”	Updated for patch 1.0.1.8000. Added information on specifying characters to replace non-printable barcode characters.
C	April 2020	Chapter 1, "Introduction"	Changed references to two monitors to “monitor(s)” to accommodate change in product configuration.

Rev.	Issued	Sections Affected	Detail
B	October 2019	Chapter 3, "Configuring the Aperio GT 450"	Added Time Zone setting information. Added new Image page section on setting image file name format and barcode identifier.
A	June 2019	All	New document.

Cautions and Notes

- Serious Incidents Reporting – Any serious incident that has occurred in relation to the Aperio GT 450 shall be reported to the manufacturer and the competent authority of the member state in which the user is established.
- Specifications and Performance – For device specifications and performance characteristics, see the document *Aperio GT 450 Specifications*.
- Installation – Aperio GT 450 must be installed by a trained Leica Biosystems Technical Services representative.
- Repair – Repairs may be done only by a trained Leica Biosystems Technical Services representative. After repairs are done, ask the Leica Biosystems technician to perform operation checks to determine the product is in good operating condition.
- Accessories – For information on using Aperio GT 450 with third-party accessories such as a Laboratory Information System (LIS) not provided by Leica Biosystems, contact your Leica Biosystems Technical Services representative.
- Quality Control – For information on image quality checks, see the *Aperio GT 450 User's Guide*.
- Maintenance and Troubleshooting – For information on maintenance and troubleshooting, see the *Aperio GT 450 User's Guide*.
- Cybersecurity – Be aware that workstations are susceptible to malware, viruses, data corruption, and privacy breaches. Work with your IT administrators to protect workstations by following your institution's password and security policies.

  To protect workstations and servers from malware intrusion, use caution when inserting USB drives and other removable devices. Consider disabling USB ports that are not in use. If you plug in a USB drive or other removable device, you should scan the devices with an anti-malware utility. For Aperio recommendations on protecting your workstations and servers, see Chapter 6: Cybersecurity and network recommendations in this guide.

  Leica Biosystems has standard procedures and processes for identifying, evaluating, and responding to cybersecurity vulnerabilities and threats that involve our systems and their operating environments. For more information, you can visit the Product Security Overview on the Leica Biosystems website at:

  - https://www.leicabiosystems.com/us/about/product-security/

  If a suspected Aperio GT 450 cybersecurity vulnerability or incident is detected, contact Leica Biosystems Technical Services for assistance.

  As a system security measure, Leica Biosystems products capture and log external attempts to access system data. For more information, contact your Leica Biosystems representative.

- **Training** – This manual is not a substitute for the detailed operator training provided by Leica Biosystems or for other advanced instruction.
- **Safety** – This device is intended for indoor use only. Safety protection may be impaired if this device is used in a manner not specified by the manufacturer.

For additional information on this product, including intended use, see the primary instructions for use, *Aperio GT 450 User's Guide*.

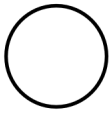
Intended Use

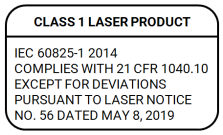
For research use only. Not for use in diagnostic procedures.

Symbols

The following symbols appear on your product label or in this user guide:

Symbol	Regulation/Standard	Description
	ISO 15223-1 - 5.4.3	Consult instructions for use
	ISO 15223-1 - 5.1.1	Manufacturer
	ISO 15223-1 - 5.1.3	Date of manufacture
	ISO 15223-1 - 5.1.8	Importer
	21 CFR 809.10(c)(2)(i)	For research use only. Not for use in diagnostic procedures.
	ISO 15223-1 - 5.1.7	Serial number
	ISO 15223-1 – 5.1.6	Catalog number
	ISO 15223-1 – 5.7.10	Unique Device Identifier
	Machinery Directive 2006/42/EC	Device carries the CE (Conformitè Europëenne) Mark and fulfils the requirements of Machinery Directive 2006/42/EC and additional EU Directives, as shown in Machinery and Materials.
	Electromagnetic Compatibility Regulations 2016 and Low Voltage Electrical Equipment Regulations 1989	UK Conformity Assessment Device is in compliance with UK Conformity Assessment requirements.
	ISO 15223-1 - 5.4.4	Caution
	ISO 7010 – W001	General warning

Symbol	Regulation/Standard	Description
	IEC 61010-1	TÜV Product Services have certified that the listed products comply with both U.S. and Canadian safety requirements.
	IEC 60417 - 5031	This device is suitable for direct current only.
	IEC 60417 - 5007	On. To indicate connection to the mains, at least for mains switches or their positions, and those cases where safety is involved.
	IEC 60417 - 5008	Off. To indicate disconnection from the mains, at least for mains switches, and all those cases where safety is involved.
	ISO 15523-1 5.7.3	Temperature limitation
	ISO 15223-1 5.3.8	Humidity limitation
	2012/19/EU	Device is regulated under 2012/19/EU (WEEE Directive) for Electrical and Electronic Equipment Waste and must be discarded under special conditions.
	People's Republic of China Electronic Industry Standard SJ/T11364	Device contains certain toxic or hazardous elements and can be used safely during its environmental protection use period. The number in the middle of the logo indicates the environmental protection use period (in years) for the product. The outer circle indicates that this product can be recycled.
	National Standard of the People's Republic of China Requirements of concentration limits for certain restricted substances in electrical and electronic products GB/T 26572-201	Device contains certain toxic or hazardous elements and can be used safely during its environmental protection use period. The "e" inside circle indicates product is compliant with Requirements of concentration limits for certain substances in electrical and electronic products GB/T 26572-2011. The outer circle indicates that the product can be recycled.

Symbol	Regulation/Standard	Description
	IEC 60825-1	Device is a Class 1 Laser Product that is in compliance with international standards and US requirements.
	CA Proposition 65	This product can expose you to chemicals known to the State of California to cause Cancer and Reproductive Harm. For more information go to https://www.P65Warnings.ca.gov.
	N/A	Device is made in the USA of U.S. and foreign components.

1 Introduction

In this section:

This chapter introduces the Aperio GT 450 Scanner Administration Manager (Aperio GT 450 SAM) for use with one or more Aperio GT 450 scanners.

The Aperio GT 450 is a high performance, brightfield whole slide scanner that includes continuous loading with 450-slide capacity across 15 racks, priority rack scanning, automated image quality check and a scan speed of ~32 seconds at 40x scanning magnification for a 15 mm x 15 mm area. The Aperio GT 450 scanner was designed to fit into your network environment and offer the best in security and performance.

This system is intended for use by trained histotechnicians, IT professionals, and pathologists. Ensure you follow appropriate good laboratory practices and the policies and procedures required by your institution for slide preparation, processing, storage, and disposal. Use this equipment only for this purpose and in the manner described in the *Aperio GT 450 User's Guide*.

Component	Description
Aperio GT 450 Scanner Administration Manager (Aperio GT 450 SAM) Server	The Aperio GT 450 SAM server connects to multiple Aperio GT 450 scanners and runs the Aperio GT 450 SAM Client Application Software.
Aperio GT 450 SAM Client Application Software	The Aperio GT 450 SAM client application software enables IT implementation, PIN configuration, and service access of multiple scanners from a single desktop client location for IT professionals.
Workstation, monitor, and keyboard	A workstation, monitor, and keyboard are required to be connected to your Local Area Network (LAN) with access to the Aperio GT 450 SAM server to use Aperio GT 450 SAM to manage the Aperio GT 450 scanners.

The Aperio GT 450 includes the Aperio GT 450 Scanner Administration Manager (Aperio GT 450 SAM) that enables IT implementation and service access of multiple scanners from a single desktop client location. Aperio GT 450 SAM facilitates setup, configuration, and monitoring of each scanner. Aperio GT 450 SAM is installed on a server that resides on the same network as the scanner(s) as well as other components for image management.

Features of Aperio GT 450 SAM include:

- Web-based user interface, compatible with most current browsers to allow access throughout your facility network.
- Role-based user access. An operator role allows users to view configuration settings, while an administrative role allows the user to change the settings.
- Scanner-specific configuration settings for user-access PINs and timeouts. Access to each scanner on the system can be configured with separate access PINs.
- Central display of statistics and event logs. Information for each scanner on the system can be displayed and reviewed from the Aperio GT 450 SAM interface for comparison.
- Support for multiple scanners, with centralized configuration and monitoring.
- Immediate display of scanner status. The home page displays which scanners are online and which are not.
- Services to process log data and events via MI7K to a database on the file system.

About this guide

This guide is intended for laboratory administrators, IT managers, and anyone else responsible for managing the Aperio GT 450 scanner on their facility network. For general information on how to use the scanner, see the *Aperio GT 450 User's Guide*.

The next chapter of this guide explains the Aperio GT 450 network architecture and shows how data flows from one component of the system to another.

Chapters that follow discuss using the Aperio GT 450 SAM application to configure the Aperio GT 450 scanner(s), including how to add user accounts to Aperio GT 450 SAM, and configure access PINs for each scanner. Tasks that are only available to Leica Support personnel are beyond the scope of this manual.

For information on specific tasks, use the following table.

Task	See…
Learn how the Aperio GT 450 scanners and the Aperio GT 450 SAM server fit into your network	Overview of recommended network configurations (on page 20)
Learn how data flows between the Aperio GT 450 scanner, the Aperio GT 450 SAM server, and optional image and data management servers.	Overview of recommended network configurations (on page 20)
Log in to the Aperio GT 450 SAM client application software	Log into Aperio GT 450 SAM (on page 15)
Adjust configuration settings for DICOM or DSR communication with the Aperio GT 450 SAM server and scanner	Scanner configuration: Configuration pages (on page 35)
Display information about a scanner on the system	System configuration (on page 30)
Check to see if a scanner is online	The Aperio GT 450 SAM user interface (on page 16)
Display the serial number, software version, or firmware version for a scanner on the system	System Information: Info page (on page 33)
Review scanner statistics and history	Displaying scanner statistics (on page 65)
Review advanced configuration options such as camera settings	Displaying scanner information and settings (on page 64)
Add a new user for Aperio GT 450 SAM access or as a scanner operator	Managing users (on page 69)
Delete a user account from Aperio GT 450 SAM	Managing users (on page 69)
Change the password for a user	Managing users (on page 69)
Diagnose a problem by reviewing the event and error logs	Working with the Event Log (on page 65)
Check for updates to the software	Displaying scanner information and settings (on page 64)

Task	See…
Review cybersecurity and network recommendations for the Aperio GT 450	Cybersecurity and network recommendations (on page 72)

Related documents

Videos available through the Aperio GT 450 touchscreen provide instructions for basic scanning tasks such as loading and unloading racks.

For additional information on operating the Aperio GT 450, see the following documents:

- *Aperio GT 450 Quick Reference Guide* — Get started with the Aperio GT 450.
- *Aperio GT 450 User's Guide* — Learn more about the Aperio GT 450.
- *Aperio GT 450 Specifications* — Detailed specifications on the Aperio GT 450.

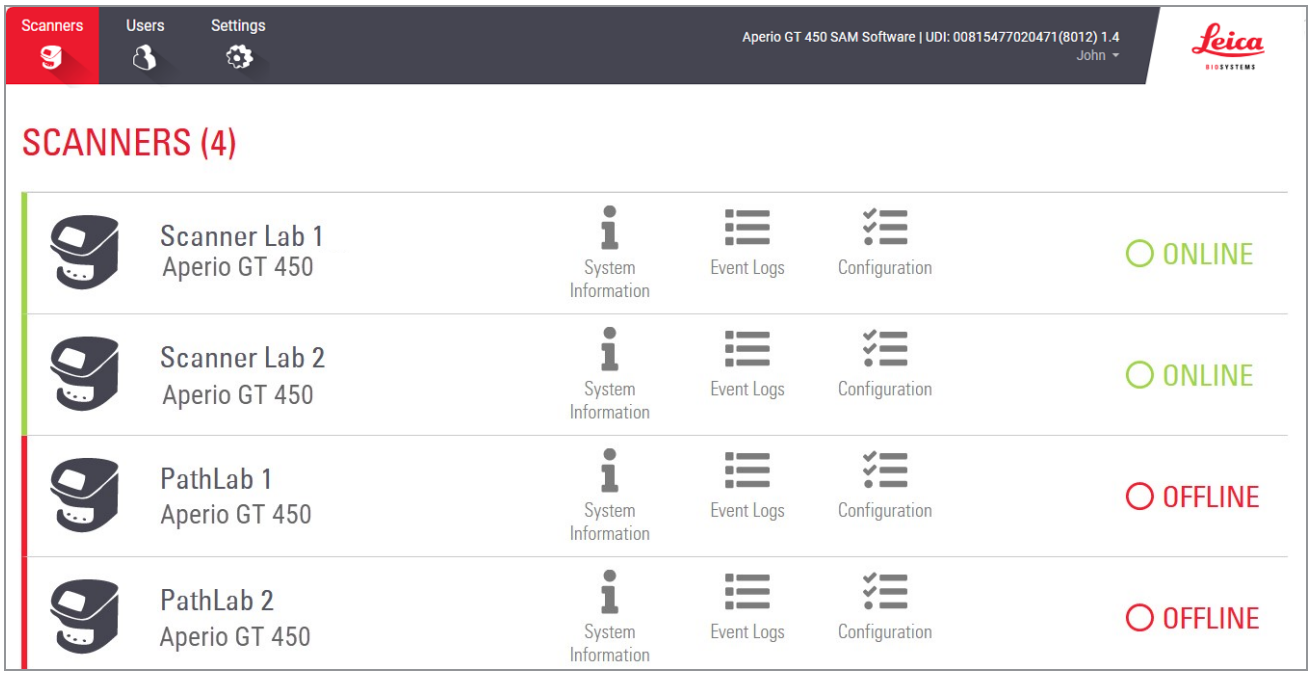
Log into Aperio GT 450 SAM

After the Aperio GT 450 is installed and configured, the next step is to use the Aperio GT 450 SAM to manage the Aperio GT 450 scanners and users.

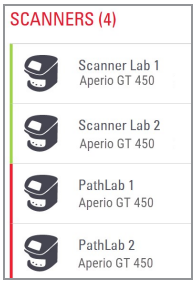
1. Open an Internet browser and enter the address of the Aperio GT 450 SAM server. (The Leica installation representative provides this address to the IT representative at the facility when the system is installed. Contact your IT staff for this address if you don't have it.)
2. Enter your login (user) name and password. If this is the first time you are logging in, use the login information provided by your system administrator or the Leica Biosystems installer.
3. Click **Log In**.

The Aperio GT 450 SAM user interface

The Aperio GT 450 SAM home page with the scanner list is shown below. Note that users with the Operator role will not see the **Users** or **Settings** icons in the top banner or the **Configuration** icons.



The four general areas of the page are described below.

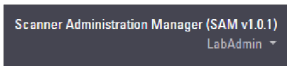


Scanner List

This list displays each scanner in the system, including the custom or “friendly” name, and the scanner model. Lab Admin users can click a scanner name in this area to display the Edit Scanner options.

Scanner Status Area

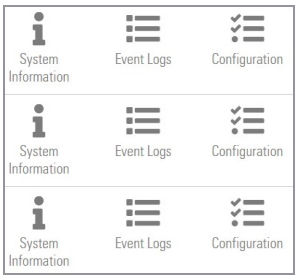
This area displays the status of each scanner.



User Login

This displays the user name for the current Aperio GT 450 SAM user.

Select your login name to display links for changing the password and logging out.



Commands Area

The icons used to display System Information, Event Log, and Configuration pages are included in this area.

Note that the Configuration icons are only available to users with the Lab Admin role.

2 Aperio GT 450 network architecture

In this section:

This chapter presents a basic architectural overview of how the Aperio GT 450 scanner and the Aperio GT 450 SAM server fit in your network.

Aperio GT 450 architecture

The Aperio GT 450 was designed with IT ease of use and security in mind. It is integration-ready for your image and data management system (IDMS), an LIS, and other networked systems.

The Aperio GT 450 includes an Aperio GT 450 scanner, Aperio GT 450 SAM server, cables, and plugs. Each instance of the Aperio GT 450 SAM server can accommodate multiple Aperio GT 450 scanners, and multiple Aperio GT 450 SAM servers can exist on your network.

The Aperio GT 450 SAM client application software resides on the Aperio GT 450 SAM server, and includes the following:

- Aperio GT 450 SAM software for configuration of the scanner
- Web-based user interface for scanner administration and configuration
- Logging and messaging services for events and errors

For customers who require SMB file shares or SVS images, a DICOM service is installed alongside the Aperio GT 450 SAM Client Application Software.

Image types supported

The Aperio GT 450 creates SVS files or DICOM images. The .svs image format is the default.

Before you can enable DICOM image output, your IT environment must meet the requirements detailed in the *Aperio GT 450 DICOM Conformance Statement*. Also, a Leica Biosystems Technical Services representative will need to log into Aperio GT 450 SAM as a Leica Admin and enable **Optional Features** for the scanner you want to configure for DICOM. See Enabling DICOM (on page 1) for details.

General information

The following guidelines apply:

- The network share where images are stored (DSR) can exist on the same server as the Aperio eSlide Manager, or it may reside elsewhere on the local network.
- Messaging includes an instance of MI7K and the deployment of various channels used to transform and route scanner messages (scan events and logs).

Before the installation of the Aperio GT 450 scanners, Aperio GT 450 SAM client application software, the Aperio GT 450 SAM server, and Aperio Viewing Station, the Leica Biosystems technical representative determines the best architecture for the installation based on projected usage, current network configuration, and other factors. This includes deciding which components (Aperio GT 450 SAM, DICOM converter, etc.) are installed on each physical server in the network. The various components and services can be installed on different servers, or co-located on a single server.

Network bandwidth requirements

For the connection between the Aperio GT 450 and the Aperio GT 450 SAM server, the required minimum bandwidth is a gigabit ethernet with a speed equal to or greater than 1 gigabit per second (Gbps). For the connection between the Aperio GT 450 SAM server and the image repository (DSR), the required minimum bandwidth is 10 gigabits per second.

How the Aperio GT 450 fits into your network

These are the major components of the Aperio GT 450 and Aperio GT 450 SAM system:

- Aperio GT 450 scanner – One or more Aperio GT 450 scanners can be connected to a Aperio GT 450 SAM server through the network. Each Aperio GT 450 SAM server can support multiple scanners.
- Digital Slide Repository (DSR) Server – This server (also known as an Image Management System) contains the whole slide images from the scanner and the infrastructure to manage them.
- Aperio GT 450 SAM Client Application Software – Accessed through a web browser (Firefox, Chrome, or Edge) on PC or laptop on your network, administrators and operators use the Aperio GT 450 SAM client application software to view event data and statistics. Administrators can also add user accounts, configure PINs, and make configuration changes.
- Database – The MS SQL Server Database that contains user data, settings data, the data and events reported via the statistical reports, and the errors reported in the logs.
- Network File Share – The location on your network where event logs are stored.

Secure access

Access via the Aperio GT 450 SAM user interface is secured using SSL. Self-signed SSL certificates are provided at installation. To avoid security messages from the browser, customers may provide their own security certificates.

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

Overview of recommended network configurations

The following three network configuration diagrams and port list describe the most common configuration scenarios for the Aperio GT 450, Aperio GT 450 SAM hosting server, Aperio eSlide Manager hosting server, image share, and third-party Picture and Archiving Communications System (PACS) with and without DICOM C-STORE image transfer support.

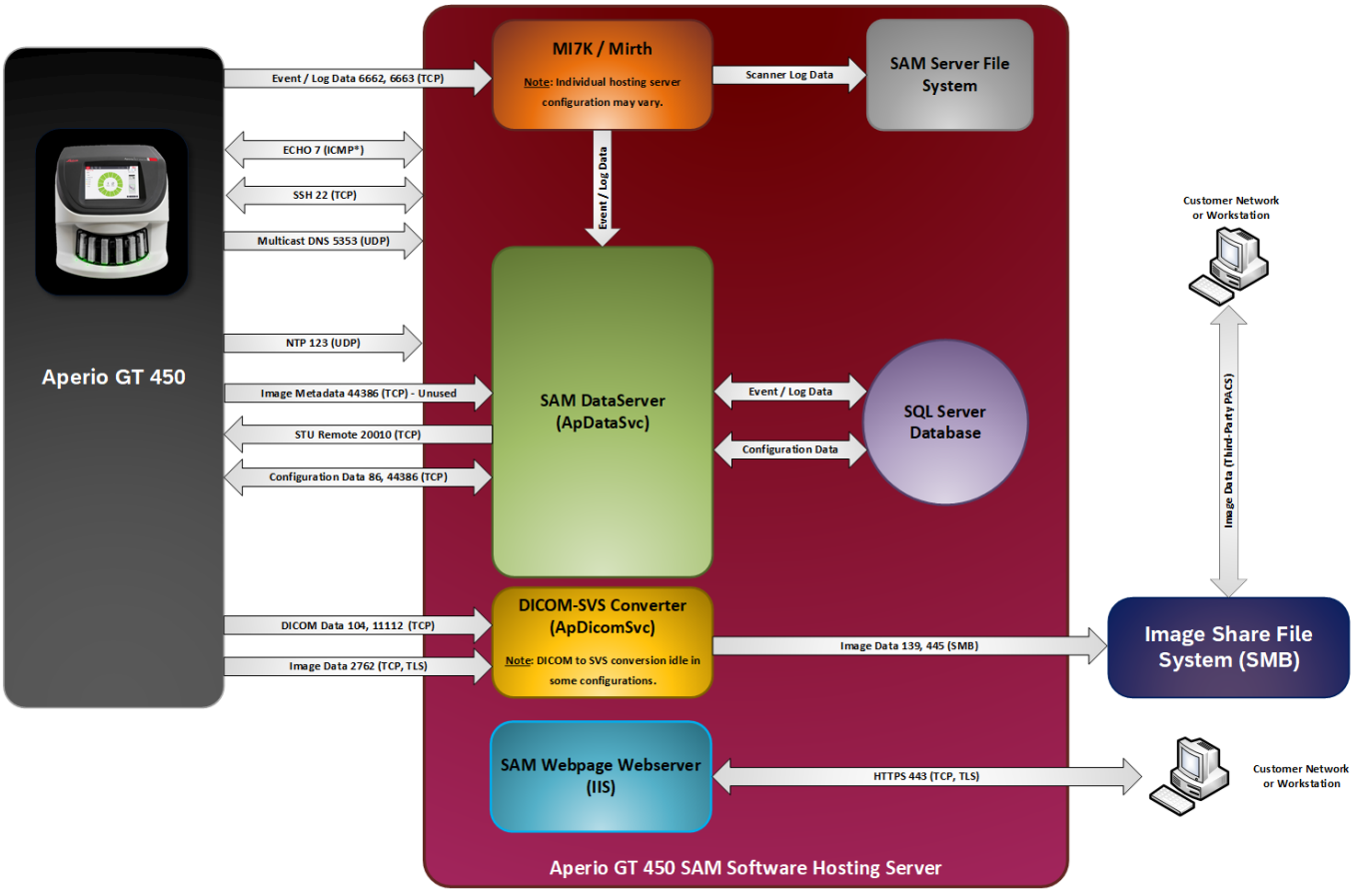
This section provides the most common configurations, and your site's configuration may differ. Work with your Leica Biosystems representative to address any questions or concerns.

Aperio GT 450 with DICOM C-STORE and third-party PACS support

The configuration shown in this section represents a typical configuration and use case where the Aperio GT 450 and Aperio GT 450 SAM software configuration transmits DICOM images direct to a customer Laboratory Information Management System (LIMS), Laboratory Information System (LIS), Vendor Neutral Archive (VNA), or third-party Picture and Archiving Communication System (PACS) using the DICOM C-STORE protocol.

This configuration is applicable only to those organizations who are using the optional DICOM upgrade. This configuration does not produce ScanScope Virtual Slide (SVS) images by default. The DICOM-SVS conversion service (ApDicomSvc) on the Aperio GT 450 SAM hosting server is idle. Image metadata is not transmitted to Aperio GT 450 SAM. For more information on the optional DICOM upgrade, including system setup details, see the *Aperio GT 450 DICOM Upgrade Guide*.

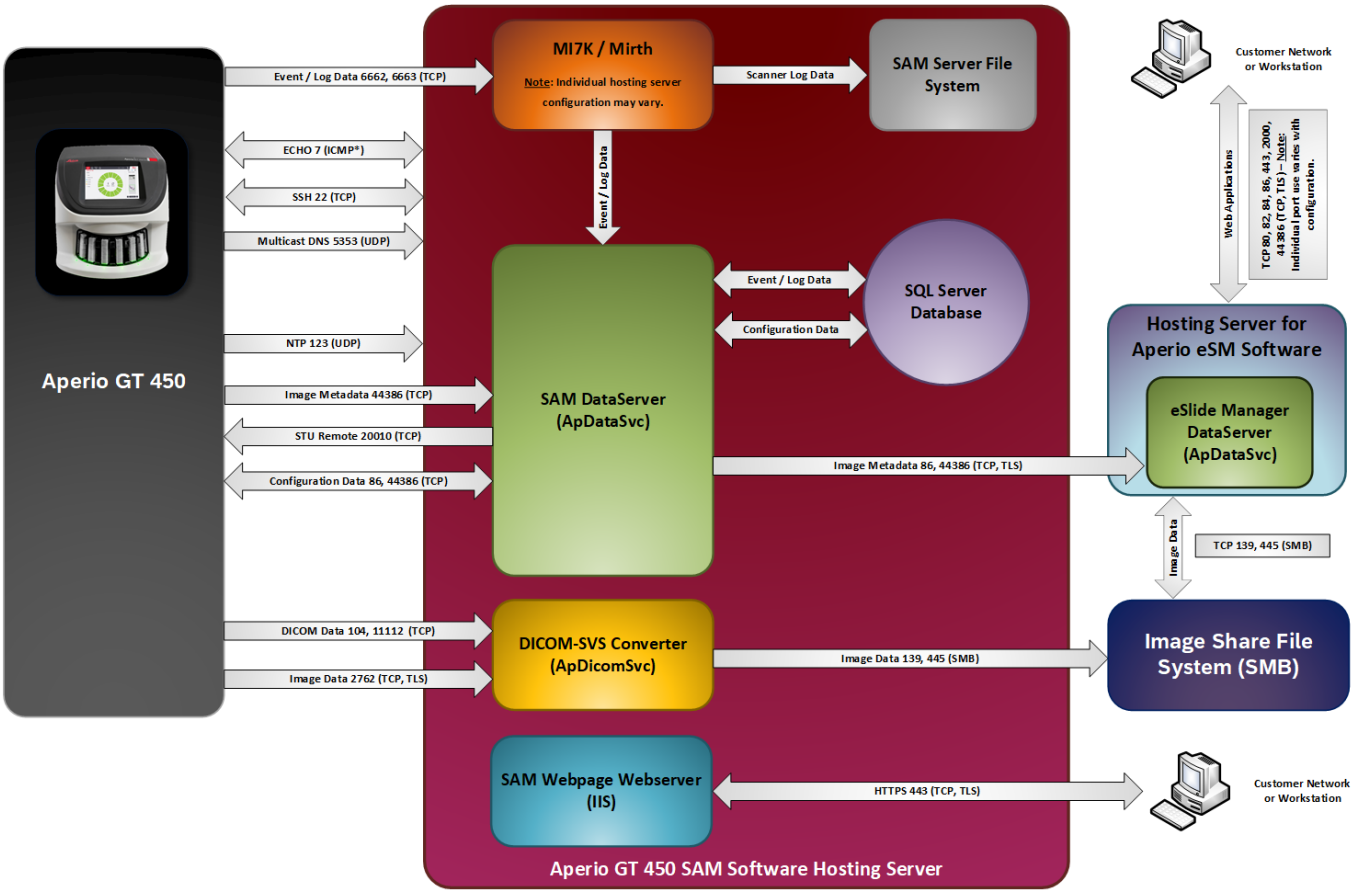
The scanner must be licensed and configured with the optional DICOM upgrade. Refer to the *Aperio GT 450 DICOM Upgrade Guide* for details. Contact your Leica Biosystems representative with any specific questions.



Aperio GT 450 with Aperio eSlide Manager integration from image file share

The configuration shown in this section represents a typical configuration and use case where the Aperio GT 450 interface with an image share that provides data to an instance of Aperio eSlide Manager running on a physical or virtualized hosting server separate from the device with Aperio GT 450 SAM installed. There are multiple configurations of Aperio eSlide Manager (such as Hub and Spoke) that are not described in this guide.

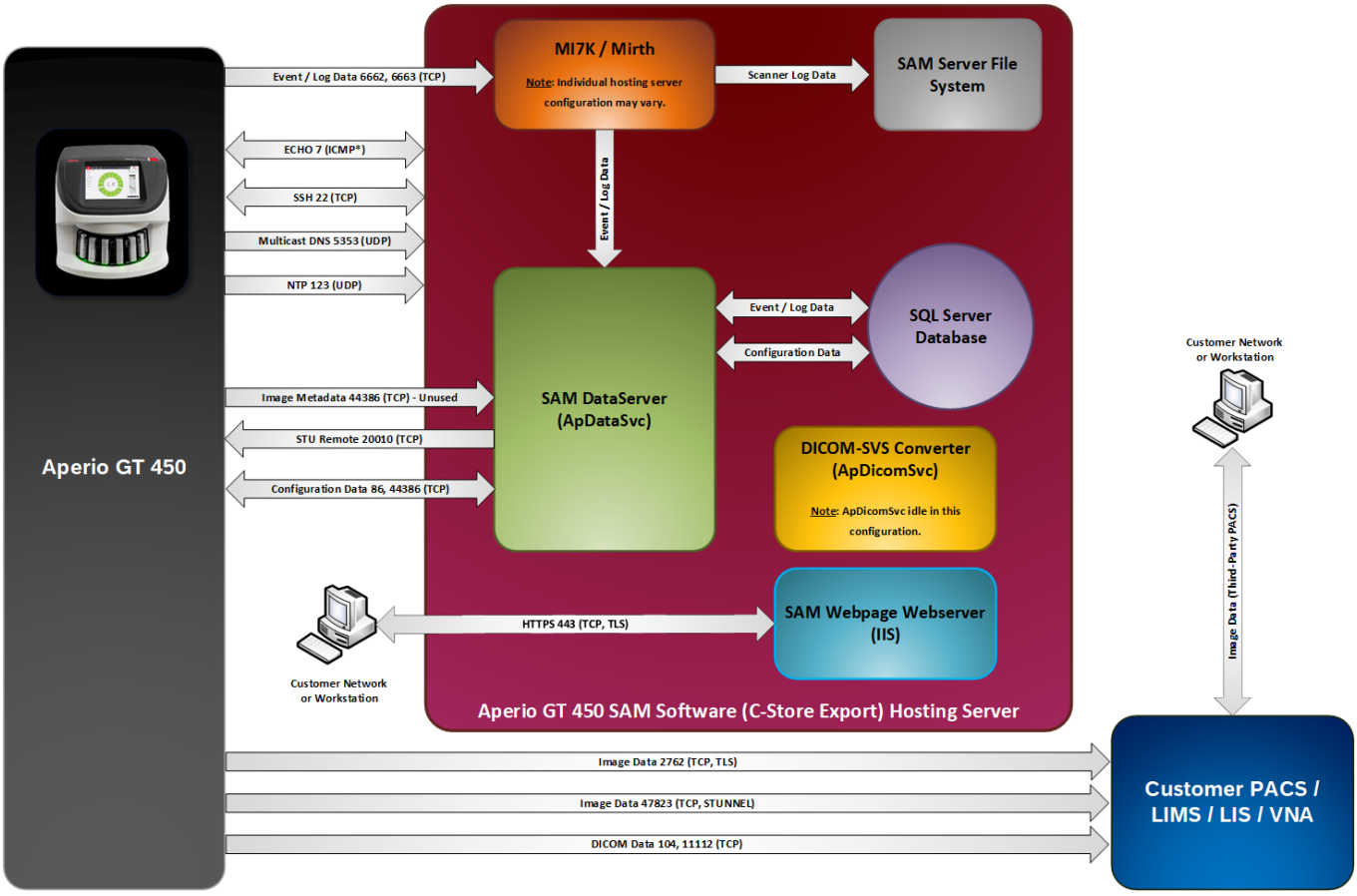
This configuration produces only SVS images, as other image formats are not compatible with Aperio eSlide Manager.



Aperio GT 450 with third-party PACS support from image share

The configuration shown in this section represents a typical configuration and use case where the Aperio GT 450 interface with an image share monitored by a third-party PACS, LIS, or LIMS using an instance of Aperio GT 450 SAM with no Aperio eSlide Manager.

This configuration exports SVS or DICOM images to the image share, depending on your Aperio GT 450 SAM hosting server configuration. Enabling DICOM export is applicable only to those organizations that are using the optional DICOM upgrade. Image metadata is not transmitted to Aperio GT 450 SAM.



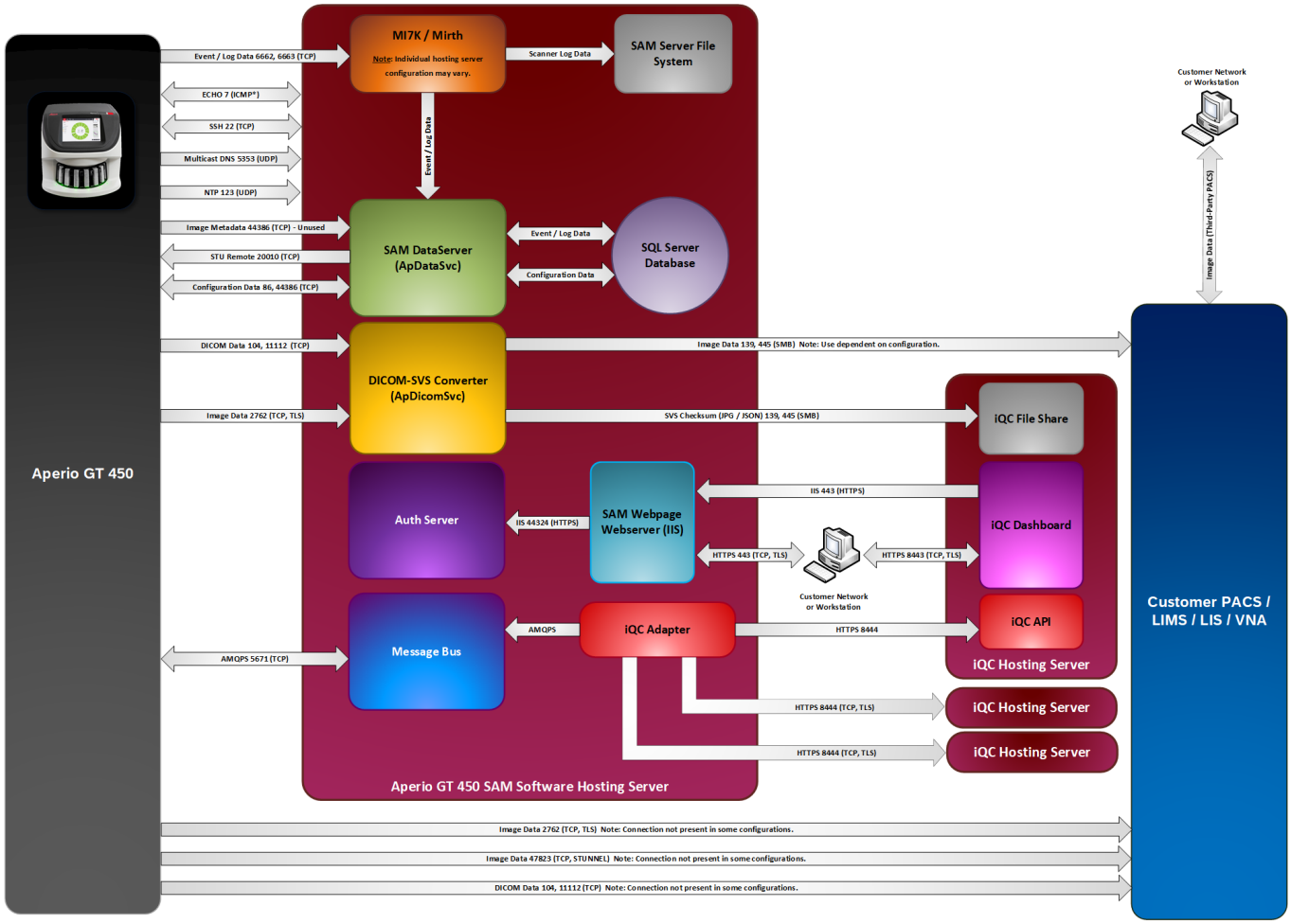
Aperio GT 450 with Aperio iQC Software Module

This section shows how the Aperio GT 450 interfaces with the Aperio iQC Software Module. The Aperio iQC 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 the configurations described previously.



Aperio GT 450 Network Configuration Ports

The table below provides a list and description of the ports used with the Aperio GT 450 configurations.

Port Number	Protocol	Use by SAM /Aperio GT 450 / DSR	Source	Destination	Description
7	ICMP	Internet Control Message Protocol (ICMP)	SAM	Aperio GT 450	ICMP echo requests from SAM to the Aperio GT 450 (when configured.)
7	ICMP	Internet Control Message Protocol (ICMP)	Any	SAM	ICMP echo requests from external systems to Scanner Administration Manager (SAM, when configured.)
22	TCP	Secure Shell Connections	SAM	Aperio GT 450	SSH service provides remote command and file transfer services on the Aperio GT 450. The Aperio GT 450 firewall only permits SSH traffic from SAM (when configured.)
80	TCP	Hypertext Transfer Protocol (HTTP)	Any	DSR / Image Share	Display of unencrypted web pages. Only in use in certain configurations.
82	TCP	ImageServer service used for image viewing.	Any	DSR / Image Share	Only in use with instances of Electronic Slide Manager (eSM.)
84	TCP	Digital slide conferencing.	Any	DSR / Image Share	Only in use with instances of Electronic Slide Manager (eSM.)
86	TCP	DICOM Data Tool (Image Metadata)	Any	DSR / Image Share	DataServer API. SAM DataServer sends image metadata to eSlide Manager DataServer. Connections encrypted via TLS.

Port Number	Protocol	Use by SAM /Aperio GT 450 / DSR	Source	Destination	Description
86	TCP	DICOM Data Tool (Image Metadata)	Aperio GT 450	SAM	Heartbeat verification from Aperio GT 450 to SAM.
104	TCP	DICOM Data Tool	Aperio GT 450	SAM	DICOM TLS SCP for receiving image data from the GT 450.
123	UDP	Network Time Protocol (NTP) synchronization.	Aperio GT 450	SAM	Aperio GT 450 Network Time Protocol Daemon (NTPD) synchronization.
137	UDP	SAM requires UDP access to this port for image data transmission.	Any	DSR / Image Share	NETBIOS service discovery.
138	UDP	SAM requires UDP access to this port for image data transmission.	Any	DSR / Image Share	NETBIOS service discovery.
139	TCP	SAM requires TCP access to this port for image data transmission.	Any	DSR / Image 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)	Any	DSR / Image Share	HTTPS access to eSlide Manager (eSM) hosting server webpage webserver (IIS.) Connections encrypted via TLS.
443	TCP	Secure Hypertext Transfer Protocol (HTTPS)	SAM	Aperio GT 450	HTTPS access to GT 450 console from SAMused to collect logs and Saved Scan Data (SSD.) Connections encrypted via TLS.

Port Number	Protocol	Use by SAM /Aperio GT 450 / DSR	Source	Destination	Description
443	TCP	Secure Hypertext Transfer Protocol (HTTPS)	Any	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.	Any	DSR / Image 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.
1433	TCP	Microsoft SQL services.	Aperio GT 450	SAM	SQL server data traffic.
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.
5353	UDP	Multicast DNS	Aperio GT 450	SAM	Resolves hostnames on networks without dedicated domain name services (DNS.)
5671	AMQPS	Events from Aperio iQC Services	Aperio iQC	SAM	Message bus installation for receiving event data from Aperio iQC.
6662	TCP	Used by MI7K for status logging and messaging between the SAM server and connected GT 450 scanners.	Aperio GT 450	SAM	Aperio GT 450 sends device logging data to SAM. No sensitive data transferred via this port.
6663	TCP	Used by MI7K for status logging and messaging between the SAM server and connected GT 450 scanners.	Aperio GT 450	SAM	Aperio GT 450 sends device logging data to SAM. No sensitive data transferred via this port.
10000	TCP	Interactive Connectivity Establishment (ICE)	SAM	Aperio GT 450	Remote troubleshooting utility (Scanner Test Utility, STU,) log collection tool.

Port Number	Protocol	Use by SAM /Aperio GT 450 / DSR	Source	Destination	Description
10001	TCP	Interactive Connectivity Establishment (ICE)	SAM	Aperio GT 450	Remote troubleshooting utility (Scanner Test Utility, STU,) log collection tool.
10002	TCP	Interactive Connectivity Establishment (ICE)	SAM	Aperio GT 450	Remote troubleshooting utility (Scanner Test Utility, STU,) log collection tool.
10003	TCP	Interactive Connectivity Establishment (ICE)	SAM	Aperio GT 450	Remote troubleshooting utility (Scanner Test Utility, STU,) log collection tool.
10004	TCP	Interactive Connectivity Establishment (ICE)	SAM	Aperio GT 450	Remote troubleshooting utility (Scanner Test Utility, STU,) log collection tool.
10005	TCP	Interactive Connectivity Establishment (ICE)	SAM	Aperio GT 450	Remote troubleshooting utility (Scanner Test Utility, STU,) log collection tool.
10006	TCP	Interactive Connectivity Establishment (ICE)	SAM	Aperio GT 450	Remote troubleshooting utility (Scanner Test Utility, STU,) log collection tool.
10010	TCP	Interactive Connectivity Establishment (ICE)	SAM	Aperio GT 450	Remote troubleshooting utility (Scanner Test Utility, STU,) log collection tool.
11112	TCP	DICOM Data Tool II	Aperio GT 450	SAM	DICOM TLS SCP for receiving image data from the GT 450.
20000	TCP	Interactive Connectivity Establishment (ICE)	SAM	Aperio GT 450	Remote troubleshooting utility (Scanner Test Utility, STU,) log collection tool.
20001	TCP	Interactive Connectivity Establishment (ICE)	SAM	Aperio GT 450	Remote troubleshooting utility (Scanner Test Utility, STU,) log collection tool.
20002	TCP	Interactive Connectivity Establishment (ICE)	SAM	Aperio GT 450	Remote troubleshooting utility (Scanner Test Utility, STU,) log collection tool.

Port Number	Protocol	Use by SAM /Aperio GT 450 / DSR	Source	Destination	Description
20003	TCP	Interactive Connectivity Establishment (ICE)	SAM	Aperio GT 450	Remote troubleshooting utility (Scanner Test Utility, STU,) log collection tool.
20004	TCP	Interactive Connectivity Establishment (ICE)	SAM	Aperio GT 450	Remote troubleshooting utility (Scanner Test Utility, STU,) log collection tool.
20005	TCP	Interactive Connectivity Establishment (ICE)	SAM	Aperio GT 450	Remote troubleshooting utility (Scanner Test Utility, STU,) log collection tool.
20006	TCP	Interactive Connectivity Establishment (ICE)	SAM	Aperio GT 450	Remote troubleshooting utility (Scanner Test Utility, STU,) log collection tool.
20010	TCP	Interactive Connectivity Establishment (ICE)	SAM	Aperio GT 450	Remote troubleshooting utility (Scanner Test Utility, STU,) log collection tool.
44386	TCP	Used by SAM for image metadata and GT 450 configuration data transfer.	Any	DSR	DataServer API. SAMDataServer sends image metadata to eSlide Manager DataServer. Connections encrypted via TLS.
44386	TCP	Used by SAM for image metadata and GT 450 configuration data transfer.	Aperio GT 450	SAM	Aperio GT 450 sends a call to the SAMDataServer to request configuration data. The SAMDataServer returns the configuration data to the Aperio GT 450. Connections encrypted via TLS.
47823	TCP	STUNNEL default port for image transmission. (Use dependent on device and hosting server softwar configuration.)	Aperio GT 450	SAM	Used for third-party secure image transmission. (Requires specific version and configuration of SAM and device software.) (This configuration requires the optional DICOM upgrade package.)

3 System configuration

In this section:

This chapter provides information you will use if you need to change the scanner settings, system information, or configuration.

The scanner configuration defines how the scanner communicates with Aperio GT 450 SAM, and how Aperio GT 450 SAM, in turn, communicates with the various components on the network, including the Aperio eSlide Manager server, the DICOM Image converter, the Aperio iQC Software Module, and others. Also included are procedures for assigning scanner access PINs.

General instructions

Only a user who is assigned the Lab Admin role can make configuration changes. Operators can view configuration settings, but they cannot change them.

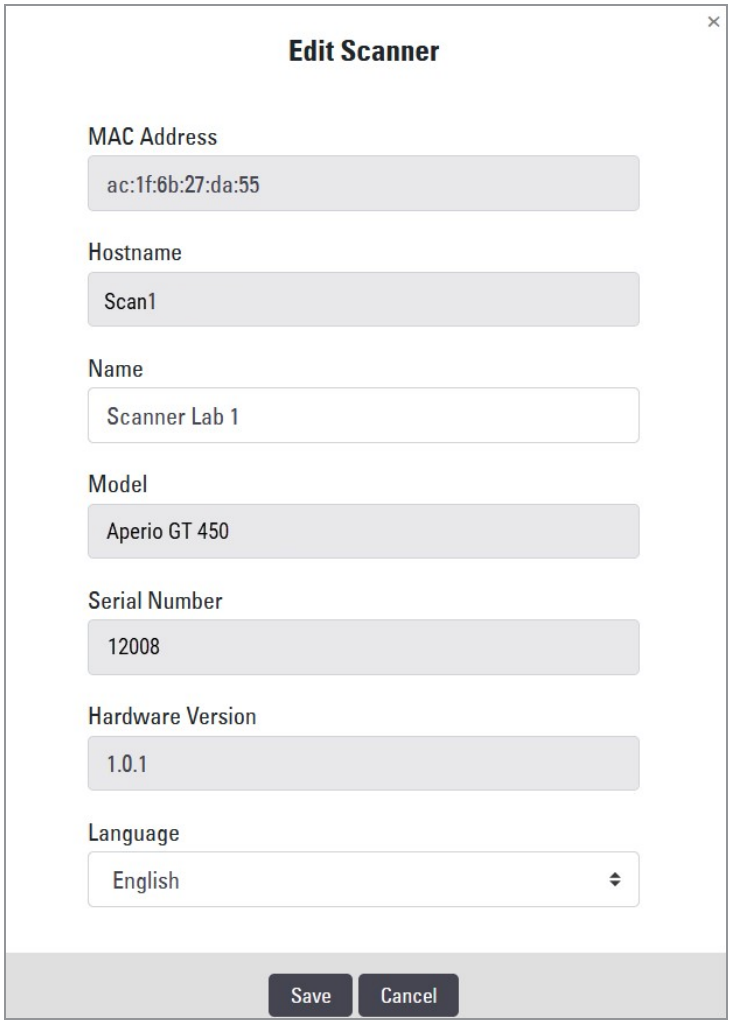
Some of the configuration settings define how the scanner communicates with Aperio GT 450 SAM, such as the **MAC Address** and **Hostname**. The **Serial Number** uniquely identifies the scanner. Calibration settings define how the scanner operates. These settings can only be changed by Leica Support personnel, and are displayed in shaded fields.

There are three sets of scanner configuration parameters:

- **Basic scanner settings**, such as the network address, name, and display language
- **Scanner system information**, such as general information and detailed scanner and camera settings
- **Scanner configuration settings**, such as communication settings for the DICOM Image converter and the DSR server, event management, time zone, and PIN management
- **Server configuration settings**, such as system endpoints, barcode rules, and Aperio iQC Software Module related configuration

Each set of parameters is discussed in this chapter.

Basic scanner settings

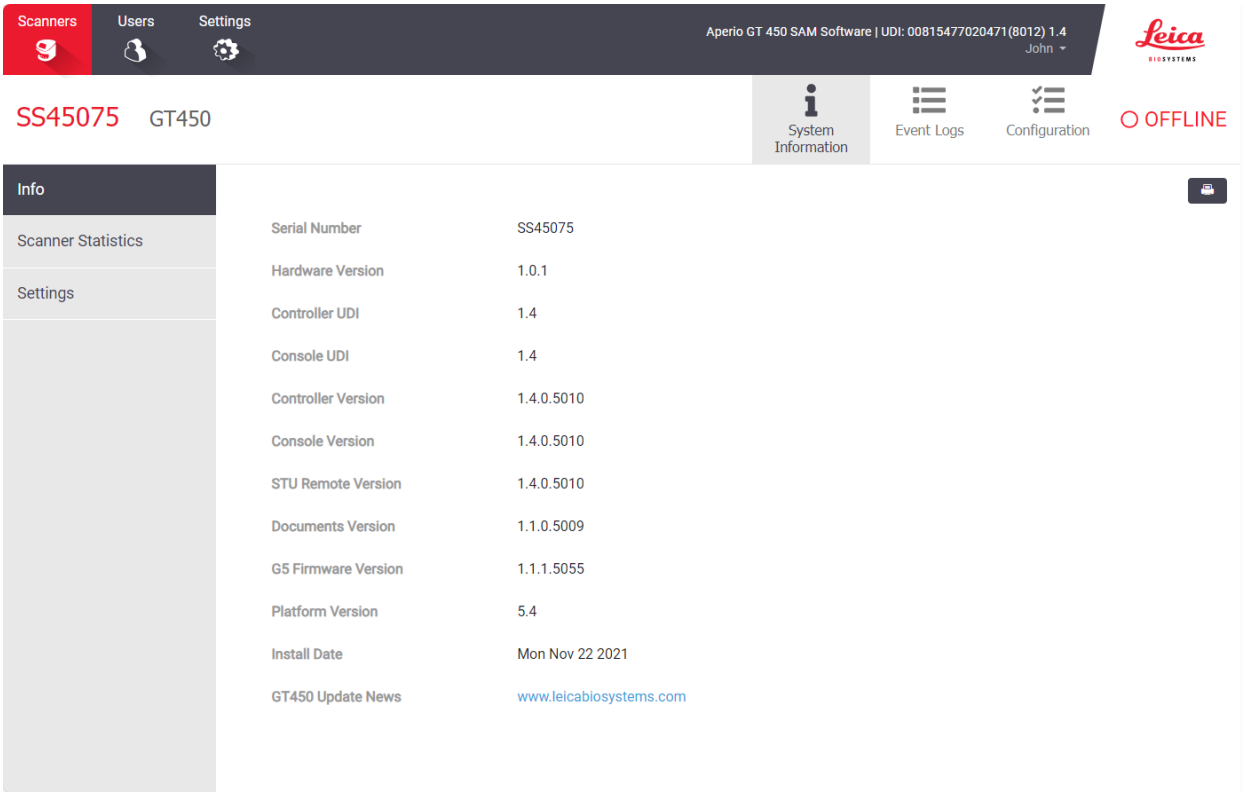


To display the **Edit Scanner** dialog box:

1. Confirm that the **Scanners** icon in the banner is selected, and the page shows the list of scanners. Click the **Scanners** icon to display the list, if necessary.
2. Hover over the name of the scanner until the edit symbol appears, then click the scanner name.
3. Customize the available settings as needed:
   - Enter a "friendly" name to identify the scanner for your facility. (This name is shown on the main page.)
   - Select a new language for the scanner control panel messages, if you wish.
   - For additional information on each option, see Summary of scanner setting and configuration options (on page 87).
4. Click **Save** to save your changes.

If you are setting up a new scanner or need to change how the scanner communicates with other servers on the network, continue with Scanner configuration: Configuration pages (on page 35).

System Information: Info page



To display the **Info** page:

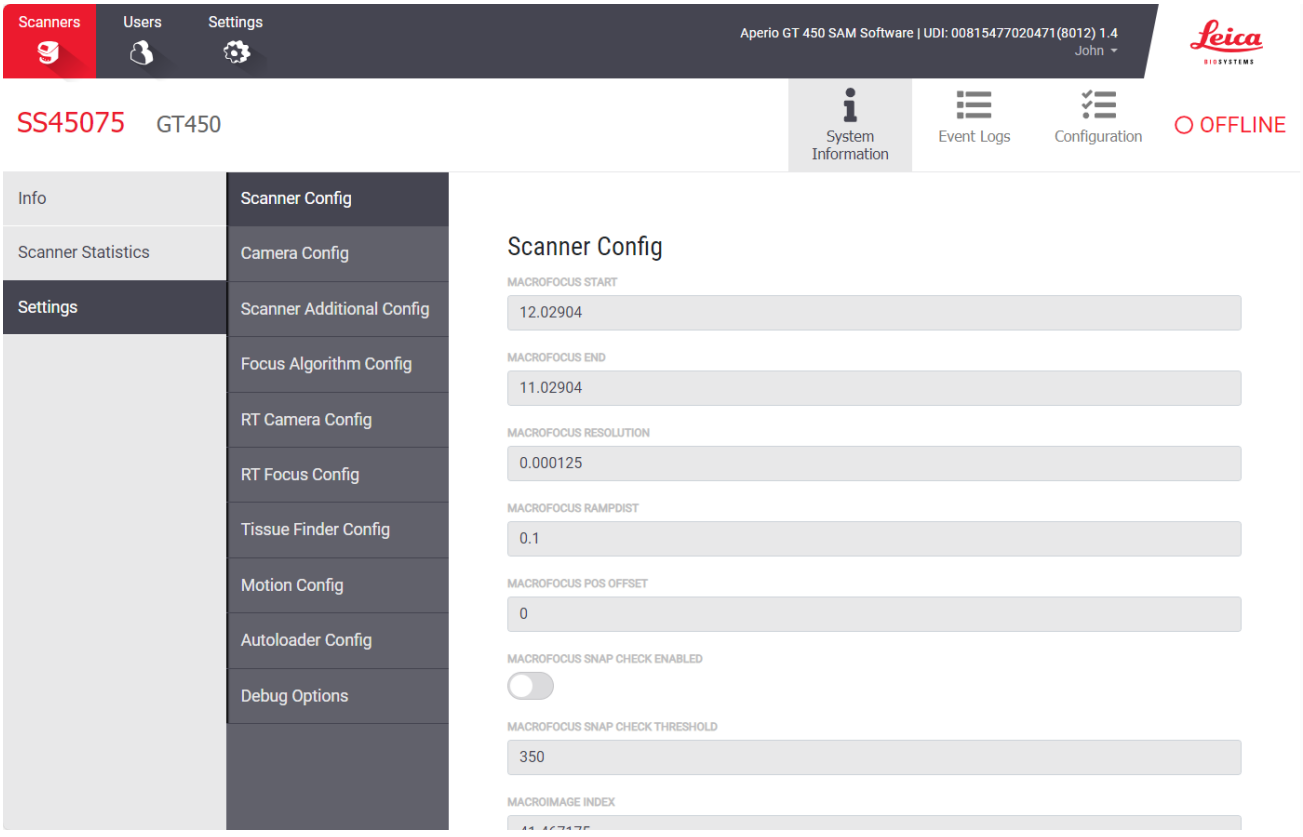
1. Confirm that the **Scanners** icon in the banner is selected, and the page shows the list of scanners. Click the **Scanners** icon to display the list, if necessary.
2. Click the **System Information** icon to the right of the scanner you want to review.
3. Click **Info** in the side menu.

Use the **Info** page to review the scanner settings. (You cannot make changes on this page.)

The firmware and hardware versions are automatically updated once Aperio GT 450 SAM establishes communication with the scanner.

System Information: Settings pages

The **Settings** pages are not visible to the operator.



The **Settings** pages display camera, scanner, focus algorithm, motion, and autoloader configuration settings. (The illustration above displays only some of the available settings.) Most or all of the settings on this page will be configured for you by a Leica Biosystems representative when the scanner is installed. However, you may be asked to check the settings during a troubleshooting procedure.

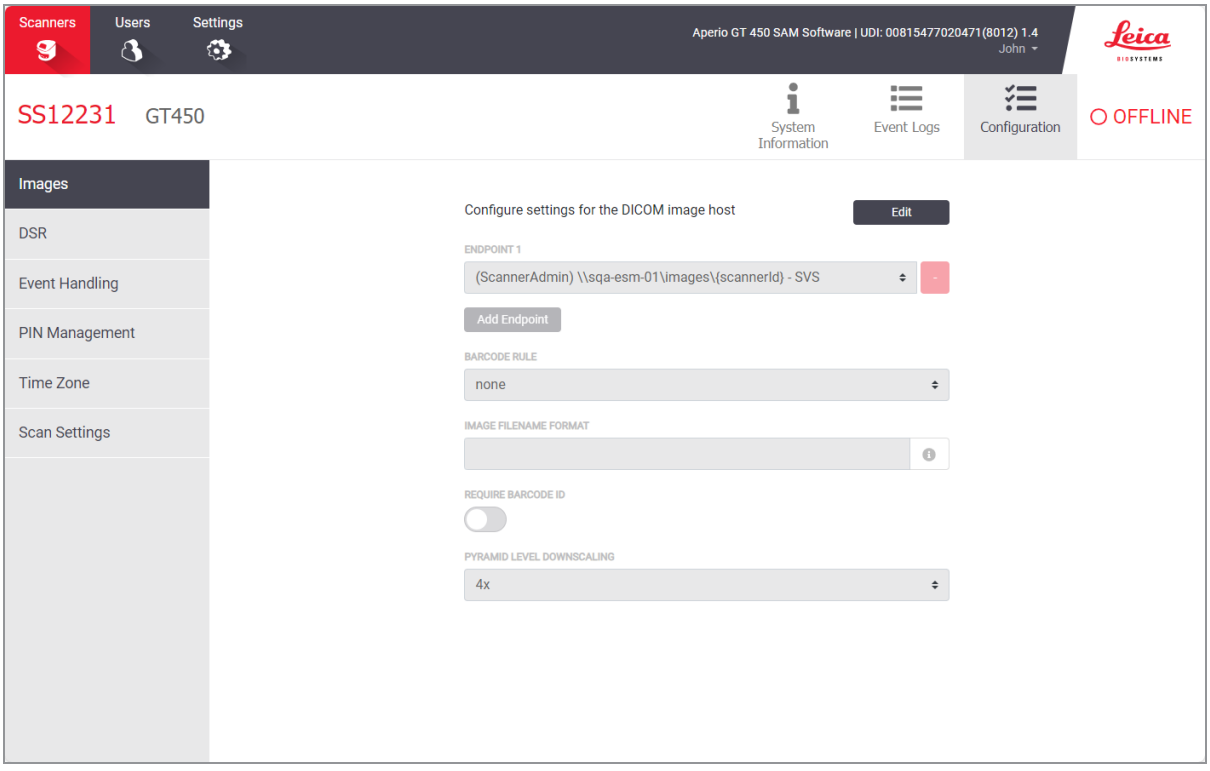
If a change must be made, you will be given specific instructions by a Leica Biosystems technical representative. Never make changes to these settings except when directed to do so by a Leica Biosystems technical representative.

To use the **Settings** page to view or edit settings:

1. Confirm that the **Scanners** icon in the banner is selected, and the page shows the list of scanners.
2. Click the **System Information** icon to the right of the scanner you want to review.
3. Click **Settings** in the side menu bar.
4. Use the scroll bar to display the list of available settings.

Scanner configuration: **Configuration** pages

The **Configuration** pages are not visible to the operator.



The settings on these pages will be configured for you by a Leica Biosystems representative when the scanner is installed. However, you may be asked to check the settings during a troubleshooting procedure. You may also need to change settings if there are changes to your network that impact one or more of the communication settings. Only a user who is assigned the Lab Admin role can make configuration changes.

There are several **Configuration** pages, one each for **Images**, **DSR**, **Event Handling**, **PIN Management**, **Time Zone**, and **Scan Settings**.

- The **Images** settings enable Lab Administrators to assign the endpoints where the scanner will send images. You can also configure other items. For more information on this page, see Images (on page 37).
- The **DSR** (Digital Slide Repository) settings control communication with the image storage system, or DSR, where the image metadata is stored.
- The **Event Handling** settings control communication with the server where scanner messages and events are processed (MI7K). For information on event logs, see Working with the Event Log (on page 65).
- The **PIN Management** settings allow lab administrators to create one or more PINs to be used to access the scanner. See PIN Management (on page 41) for more information.
- The **Time Zone** setting allows you to select the time zone for the scanner.

- The **Scan Settings** page enables you to set 20x as the default scan magnification, enable the use of the default calibration point, enable Auto Narrow Stripe scanning, enable Extended Focus Image Output, and configure z-stack and/or Extended Focus scanning parameters. Only features that are licensed for the scanner are available to configure.

To use the **Configuration** pages to view or edit settings:

1. Confirm that the **Scanners** icon in the banner is selected, and the page shows the list of scanners.
2. Click the **Configuration** icon to the right of the scanner you want to configure. The **Images** configuration page displays.
3. Click the desired configuration setting in the side menu bar.
4. To add, delete, or modify PINs or change the timeout, see PIN Management (on page 41) .

   For other configuration settingss, click **Edit**, and change the setting as desired. Note that you cannot make changes to settings in shaded fields.
5. If you made changes, click **Save** to save the changes and return to viewing mode.

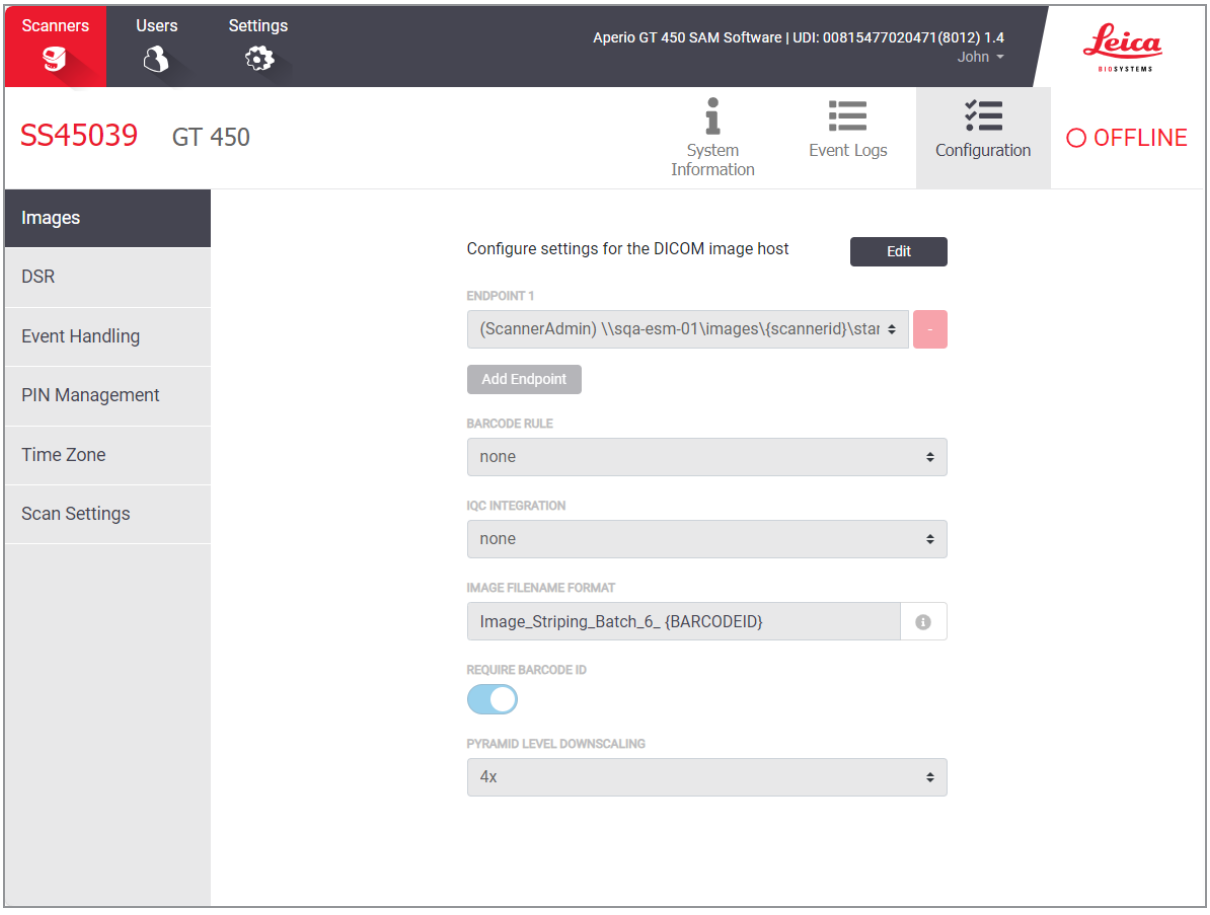
For more details on each option, see Summary of scanner setting and configuration options (on page 87).

Images

The **Images** page allows lab administrators to configure settings related to image generation, including:

- Endpoint(s) for the DICOM image host
- The image file name format
- Barcode management
- 2x pyramid downscaling

The Lab Admin can click the **Edit** button to modify the settings on this page.



Selecting endpoints

From the Images page you select the endpoint(s) where scanned images should be sent. To be selectable, the endpoint must have been set up already through the **Settings** icon in the top banner. To populate SAM with endpoints, see Endpoint management (on page 50).

Depending on the scanner licenses, you may have the option to add an additional endpoint. This feature is currently available for scanners with iQC integration.

Managing barcodes

The **Images** page includes several settings related to barcode management. Here you specify whether a barcode ID is required when scanning a slide, and you select the barcode rule used to extract the barcode from the label. To be selectable, the barcode rule must have been set up already through the **Settings** icon in the top banner. To create and edit barcode rules, see Barcode Rules (on page 53).

iQC integration

If the Aperio iQC Software Module is licensed, you will see the **iQC INTEGRATION** field on the **Images** page. This field allows for selection of the hosting server for the Aperio iQC Software Module. To be selectable, the endpoint must have been set up already through the **Settings** icon in the top banner. To populate SAM with endpoints, see Endpoint management (on page 50).

Image file name format

By default, the file name of the scanned image begins with the image's numeric ImageID followed by an underscore and a six-digit time code, and it ends with a file extension indicating the format of the file.

You can enter your own text at the beginning of this field and then use any of these keywords in any order. The keywords must be in all capitals and surrounded by { } symbols. We suggest separating the keywords with underscores for readability.

- BARCODEID — Barcode value identifier (see the next section)
- RACK — Rack number
- SLIDE — Slide position in the rack
- IMAGEID — Unique identifier for the image

For example, if you want to identify all of the scanned images from this scanner as coming from ScannerA, and also want to indicate what rack and what position in the rack the slide came from, you might create an image file name format like this:

```
ScannerA_{RACK}_{SLIDE}
```

The file name will begin with the text "ScannerA" followed by the rack number and the slide position in the rack. Following this will be an underscore, a six-digit code, and the file extension. For example:

```
ScannerA_5_2_210164.SVS
```

Setting barcode ID requirement

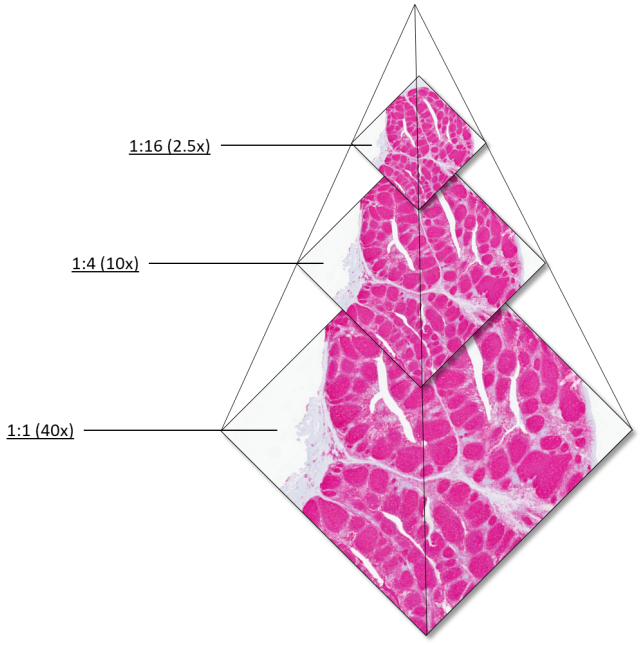
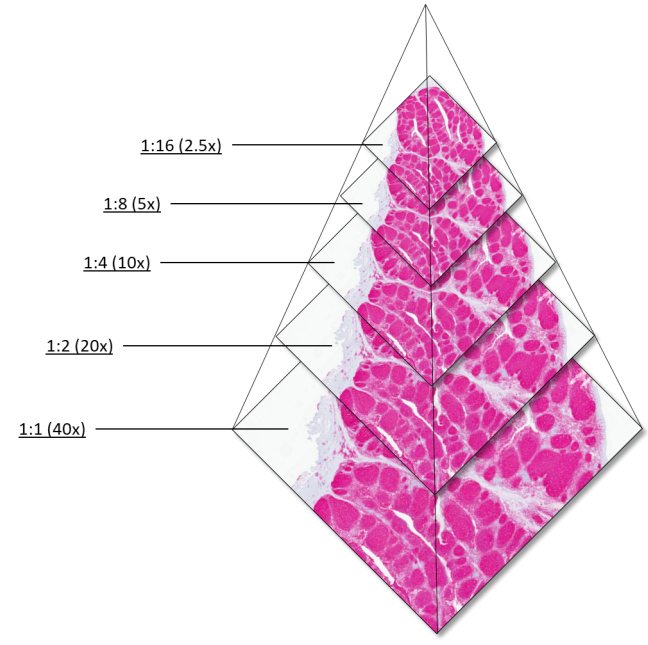
If your procedures require each scanned image to be saved with a barcode, move the **REQUIRE BARCODE ID** slider to the right. When the barcode ID is enabled, the scanner will skip a slide if the slide does not have a barcode or if the scanner cannot read the barcode.

Pyramid level downscaling

You have the option of changing the pyramid level downscaling from the default of 4x to 2x.

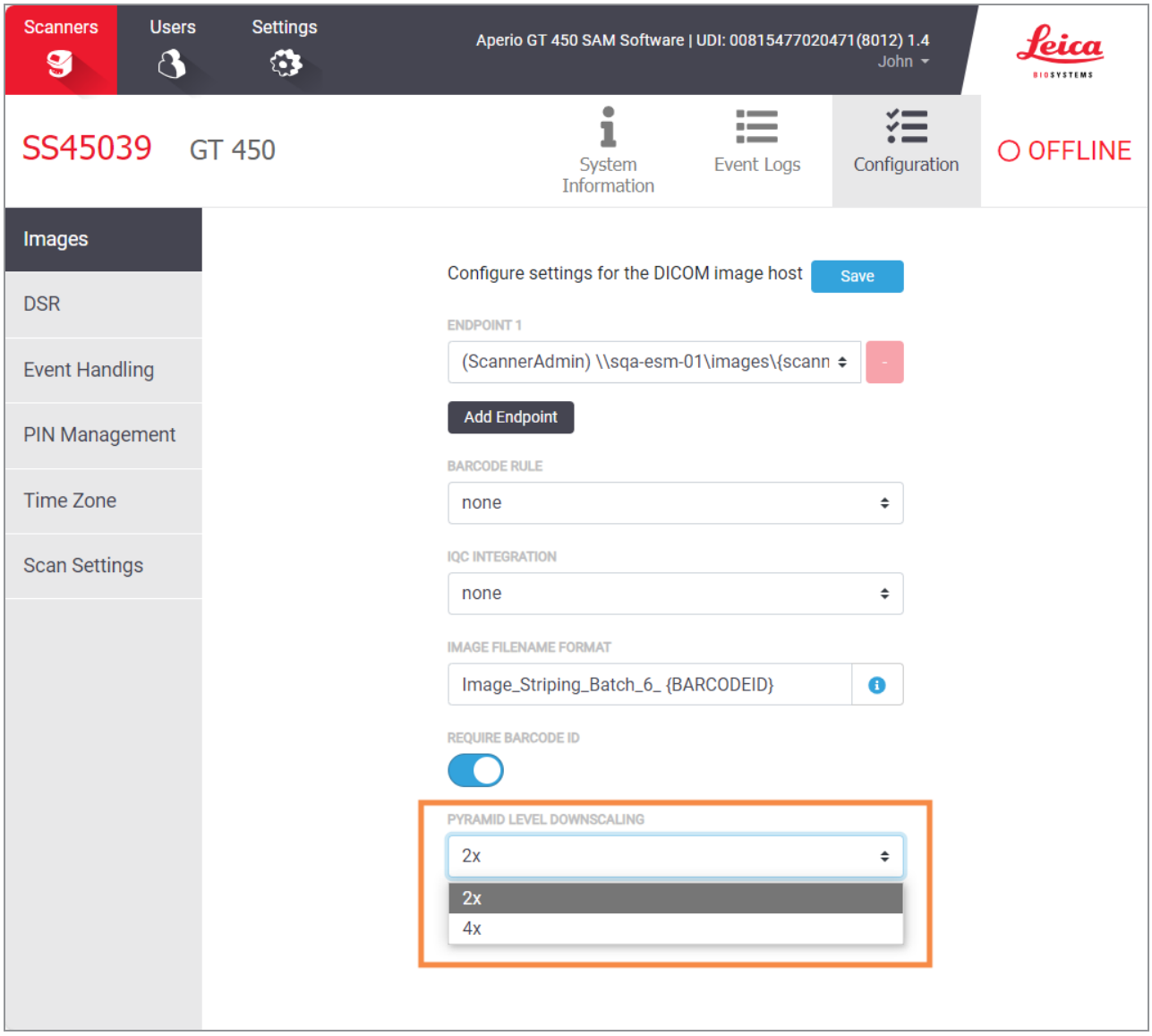
When displaying Aperio GT 450 scanned images, some third-party viewing software solutions must interpolate the image data as the user navigates through the available magnification levels. This interpolation process can cause a decrease in viewing performance. Setting the pyramid level downscaling to 2x can increase viewing performance by enabling third-party viewing software solutions to display all available magnification levels with less interpolation of the image data.

The illustrations below show how 2x pyramid level downscaling provides the viewing software direct access to a greater range of magnification levels.

4x pyramid level downscale	2x pyramid level downscale
	

When you enable the 2x pyramid level downscaling option, the image size for 2x downscaled images is approximately 15% to 20% greater than the default 4x downscaled images, depending on the slide image.

To configure 2x pyramid level downscaling from the Images page, click **Edit**. In the **PYRAMID LEVEL DOWNSCALING** field, select 2x to enable the 2x Pyramid Level Downscaling option, then click **Save**.



1 Click **Save**.

DSR (Digital slide repository)

The **DSR** page is used to configure the hostname and port for the Digital Slide Repository.

Event Handling

The **Event Handling** settings control communication with the server where scanner messages and events are processed (MI7K). For information on event logs, see Working with the Event Log (on page 65).

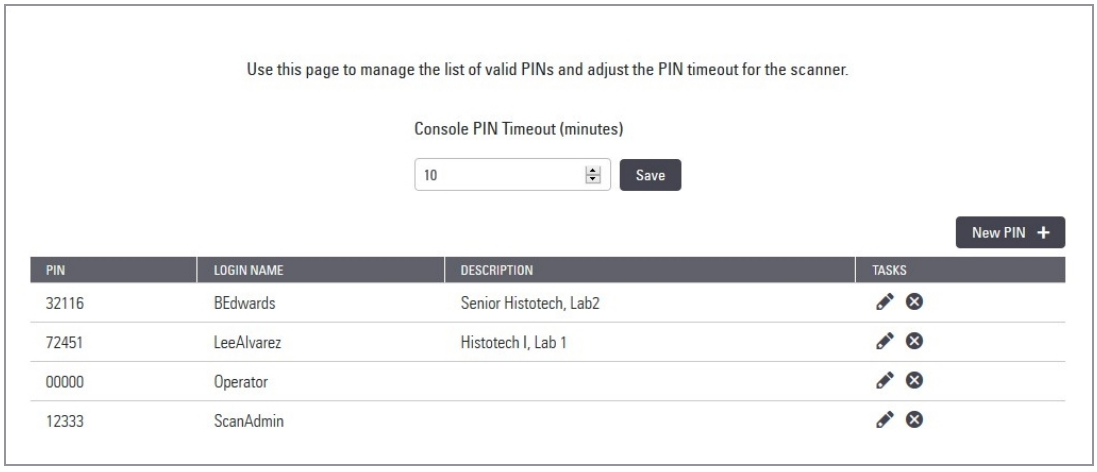
PIN Management

PINs control access to the scanner. (Each operator needs to enter a PIN to unlock the scanner.)

Each PIN is associated with a specific scanner user. When an operator accesses the scanner using a PIN, the scanner records the user name associated with the PIN in the internal scanner log. (The PIN itself is not logged.) The scanner controls remain unlocked as long as there is operator activity. If no one interacts with the scanner before the set time elapses, the scanner locks until an operator enters a valid PIN.

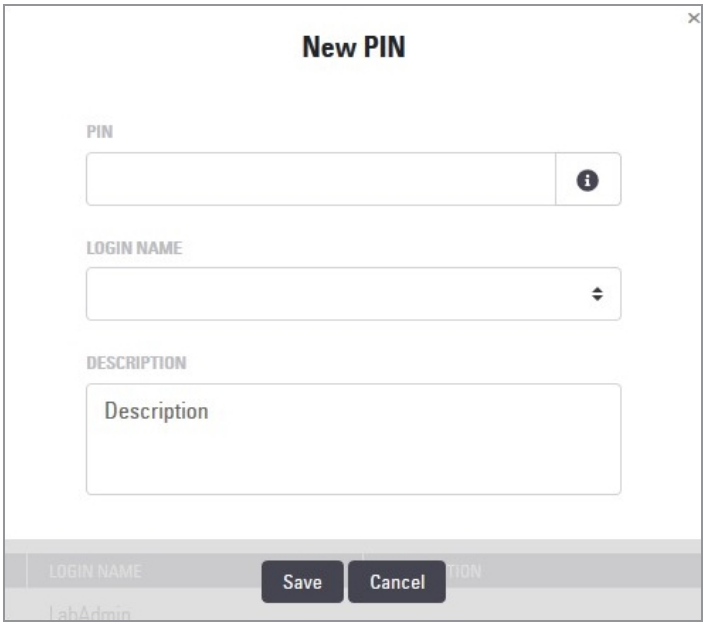
- You must have at least one PIN for each scanner, and PINs are specific to a scanner. You can assign either the same or different PINs to each scanner in the system, depending on what is best for the workflow at your facility.
- A PIN does not limit the features that an operator can access on the scanner.
- When configuring the login timeout, choose a time that is convenient for operators, without being so long that it allows the scanner to be left unattended and vulnerable to misuse.

Configuring a PIN and timeout



1. Confirm that the **Scanners** icon in the banner is selected, and that the page shows the list of scanners.
2. Click the **Configuration** icon to the right of the scanner.
3. Click **PIN Management** in the side menu bar.
4. Enter a value (in minutes) in the **Console PIN Timeout** field. The scanner locks automatically after this period of inactivity.

5 Click **New PIN+** to add a new PIN. The **New PIN** window opens.



6 Populate the window as follows:

- Enter the PIN in the PIN field (five digits). PINs can only contain digits, and may not contain alphabetical or special characters.
- From the **LOGIN NAME** drop-down list, select a user. This list only shows users who do not have a PIN. (For information on adding users, see Add a user (on page 69).
- Optionally add a **DESCRIPTION** to identify the user who will be using this PIN.

7 Click **Save** to return to the list of PINs.

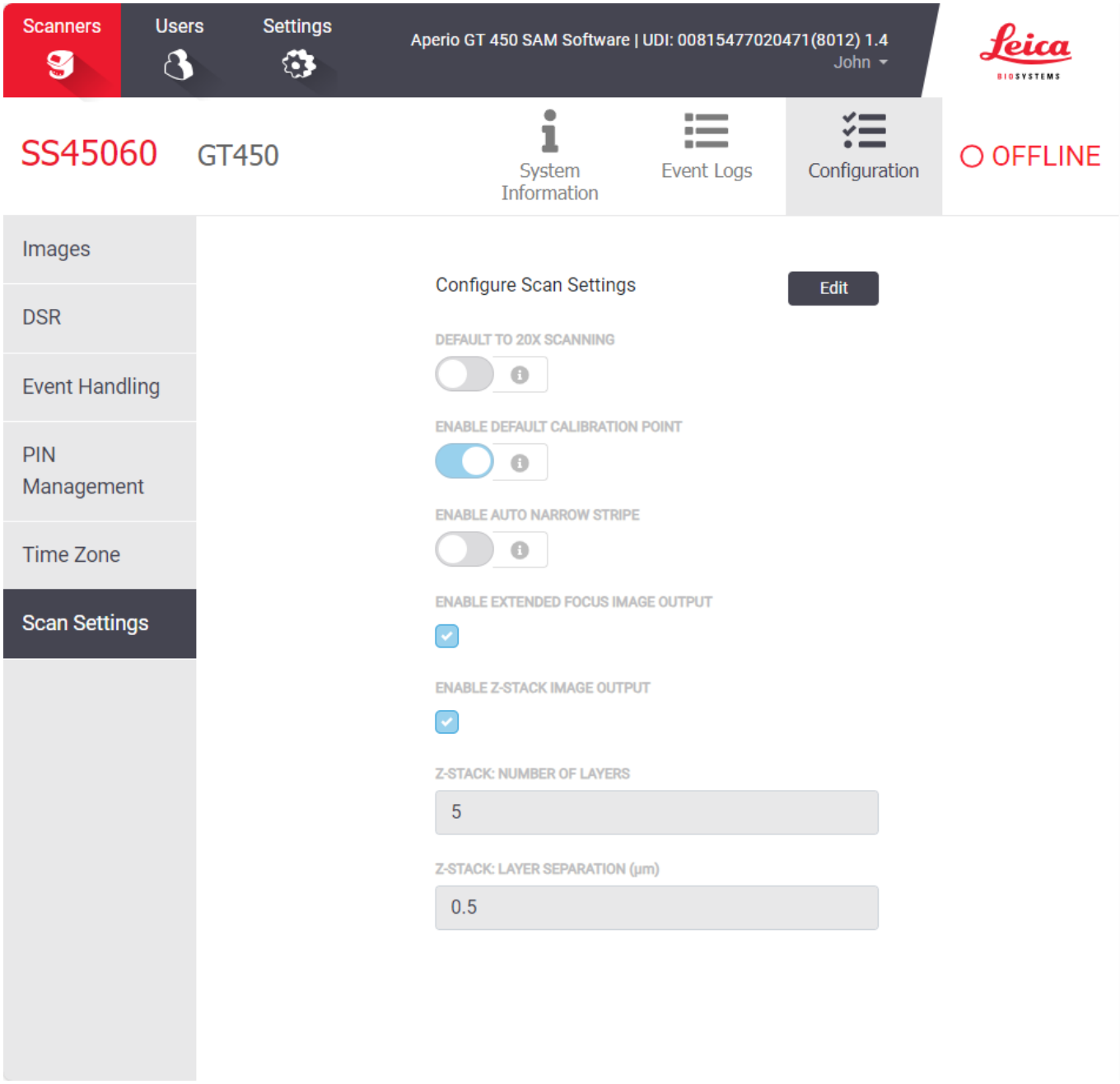
Time Zone

The **Time Zone** is set by the Aperio GT 450 SAM administrator.

Scan Settings

The **Scan Settings** page contains settings for the following:

- Default scan magnification (on page 44)
- Default Calibration Point (on page 45)
- Auto Narrow Stripe scanning (on page 47)
- Extended Focus parameters (on page 47)
- Z-stack parameters (on page 48)



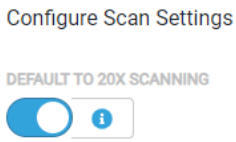
To configure the **Scan Settings**, click **Edit**. Change any settings as desired, and click **Save**.

Default scan magnification

The default scan magnification for the Aperio GT 450 scanner is originally set to 40x. For each Aperio GT 450 scanner, you have the option of changing the default scan magnification from 40x to 20x. The scanner scans all slides using the default magnification. The scanner operator has the option to override the default using the console touch screen during the scanning process.

Follow the steps below to set the default scan magnification for a specific Aperio GT 450 scanner:

1. To set the scan magnification default to 20x, navigate to the Scan Settings page, and click **Edit**.
2. Click to turn on the **DEFAULT TO 20X SCANNING** option. (If this setting is turned off, the scanner uses the default of 40x magnification.)

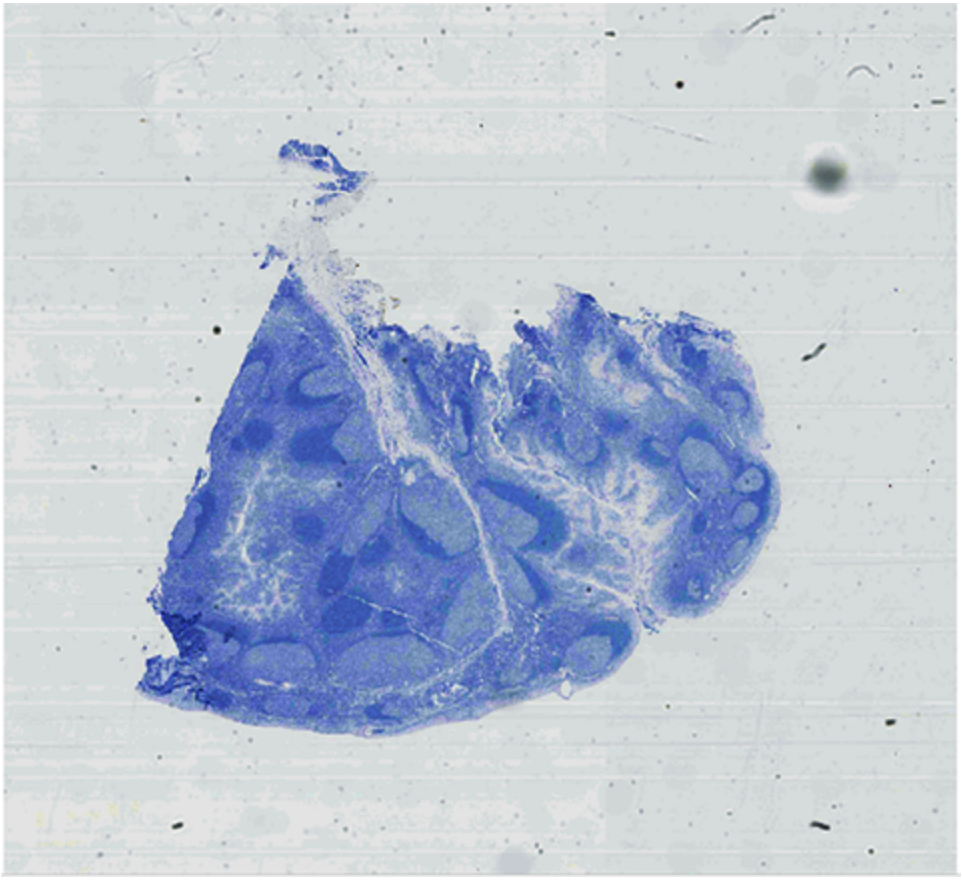


3. To save your settings, click **Save** .

Default Calibration Point

About the Default Calibration Point

As part of the scanning process, the scanner places a calibration point on a clean area of the glass slide, and then takes a "pre-scan" picture of that area. The resulting pre-scan image is used for white balance and illumination correction. If a slide does not contain an area clean enough to take a high-quality pre-scan, repetitive white striping may appear on the final scanned image, as shown in the example below.



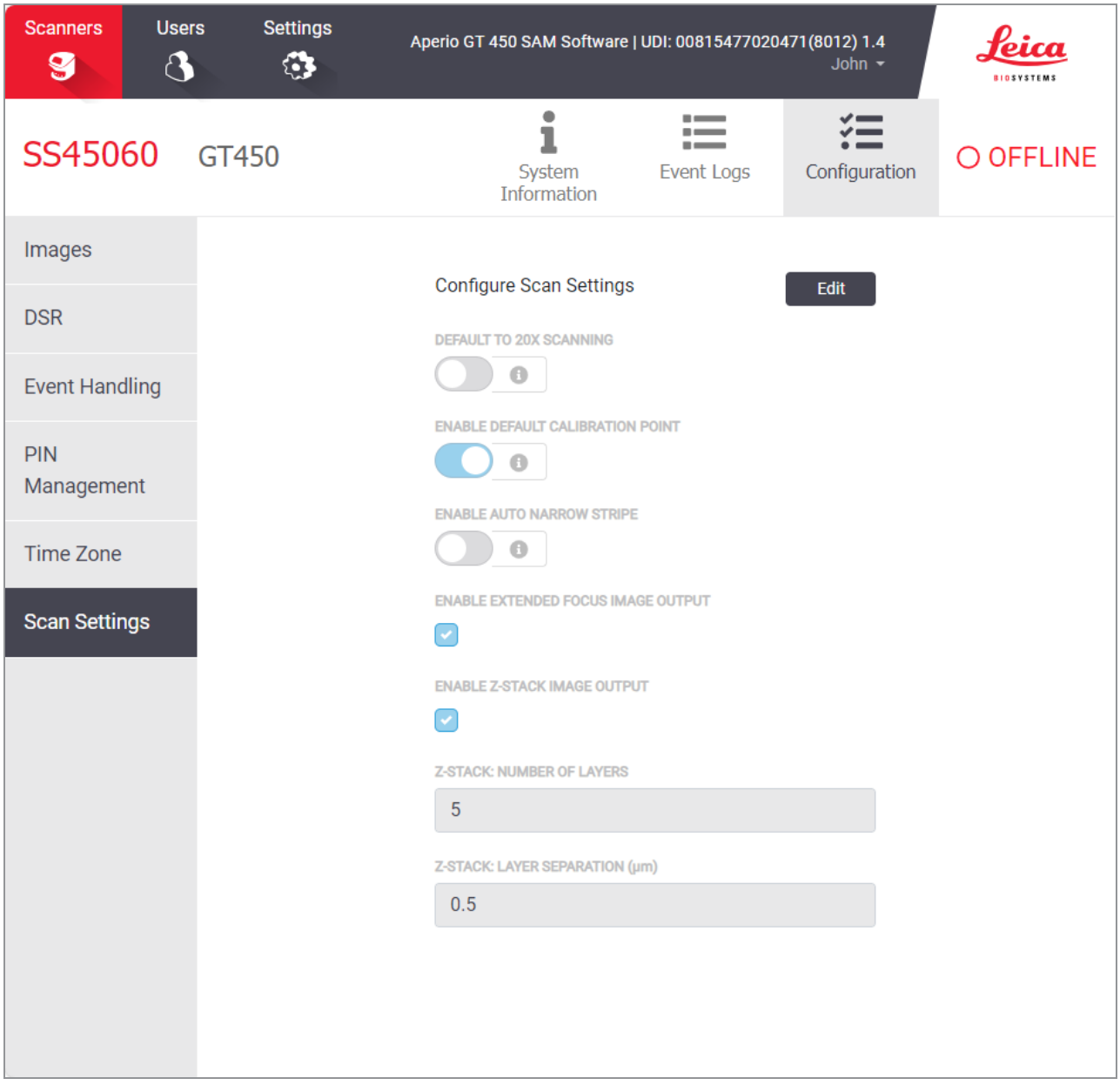
Certain tissue types are more prone to this issue, because there is not enough clear space on the slide. Additionally, artifacts introduced by improper tissue processing, such as microscopic contamination, micro water droplets, or micro air bubbles, can also cause white striping to occur. If your organization experiences frequent white striping on your scanned images, you can enable the Default Calibration Point feature. When the Default Calibration Point is enabled, the scanner checks the quality of the pre-scan during the scan workflow, and if necessary, replaces it with a higher quality default pre-scan that was created specifically for your particular scanner.

Enabling the Default Calibration Point feature

You must have Lab Admin access on the Aperio GT 450 Scanner Administration Manager to access the **Scan Settings** page.

To enable the Default Calibration Ooint feature:

1 Navigate to the **Scan Settings** page, and click **Edit**.



2 Click **ENABLE DEFAULT CALIBRATION POINT** to turn on the feature.

3 Click **Save**.

If you receive an error stating that a default calibration point is not set, contact Leica Biosystems Technical Services to resolve the problem.

If you continue to experience white horizontal striping on your scanned images after enabling the Default Calibration Point feature or if your scanner is using the Default Calibration Point feature more often than expected, contact Leica Biosystems Technical Services. They may need to adjust the internal configuration settings for this feature to better suit your environment.

Auto Narrow Stripe scanning

The Auto Narrow Stripe scanning feature helps mitigate potential image quality issues by enabling the scanner to automatically rescan a slide using an alternative scanning process, Auto Narrow Stripe scanning, when the system detects an excessive tilt of the slide tissue. Excessive slide tissue tilt can occur when the slide does not sit level in the slide tray, or when tissue is not laid flat on the glass surface along the short axis (index axis) of the slide due to poor slide preparation.

This feature works with a tilt threshold that is configured by Leica. When Auto Narrow Stripe scanning is enabled in SAM, the system evaluates every slide during the scanning process according to the tilt threshold. If the slide exceeds the tilt threshold, the scanner automatically rescans the slide using Auto Narrow Stripe scanning.

The Auto Narrow Stripe scanning feature is not leveraged when scanning z-stack images.

Note that the total scan time increases when the scanner rescans one or more slides using Auto Narrow Stripe scanning.

Your Leica Biosystems Technical Services representative can adjust the defined tilt threshold according to the needs of your organization.

Follow the steps below to enable Auto Narrow Stripe on SAM:

1. Navigate to the **Scan Settings** page, and click **Edit**.
2. Click the **ENABLE AUTO NARROW STRIPE** button to turn on the Auto Narrow Stripe workflow feature.

3. To save your changes, click **Save**.

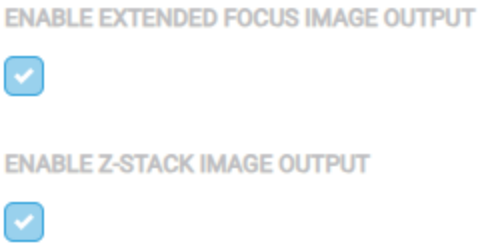
Extended Focus parameters

The optional Extended Focus feature provides an alternative to the real-time focus used by the scanner to capture image data. A z-stack image is captured, then each vertical slice is assessed, and the tile with the best focus is selected to represent that slice. Because it leverages the z-stack engine, settings for EF are shared with z-stack.

Note that Z-Stack and Extended Focus features are licensed separately. If a scanner is licensed for both, then users will presented with options to decide which images should be produced by the scanner – z-stack, EF, or both.

Follow the steps below to enable Extended Focus on SAM:

1. Navigate to the **Scan Settings** page, and click **Edit**.
2. Click the **ENABLE EXTENDED FOCUS IMAGE OUTPUT** button to turn on the Extended Focus Image Output workflow feature.



3. To save your changes, click **Save**.

Z-stack parameters

You configure the default z-stack scan settings by telling the scanner how many layers you want to scan and the distance between the layers (layer separation) in microns. For example, if you configure the z-stack to use five layers separated by 0.5 micron, there are two layers above the best focus layer and two layers below it. These settings are also used for the optional Extended Focus feature.

Follow the steps below to change the z-stack parameter settings:

1. On the **Scan Settings** page, click **Edit**.
2. In the **Z-STACK NUMBER OF LAYERS** field, enter the default number of layers (focal planes) used for scanning z-stack images. You can select from 3 and 25 layers. (The number of layers includes odd numbers only.) Typically, the number of layers you choose depends on the type of tissue you are scanning. The scanner operator can adjust this setting on the scanner console when scanning a rack of slides.

Note that scan time and file sizes increase based on number of focus planes you select.

3 In the **Z-STACK LAYER SEPARATION (µm)** field, enter the default distance between planes from 0.25 to 1.0 micron. This setting controls the focus offset between layers. The scanner operator can adjust this setting on the scanner console when scanning a rack of slides.

4 To save your changes, click **Save**.

Server configuration: **Settings** pages

The server configuration **Settings pages** pages are not visible to the operator.

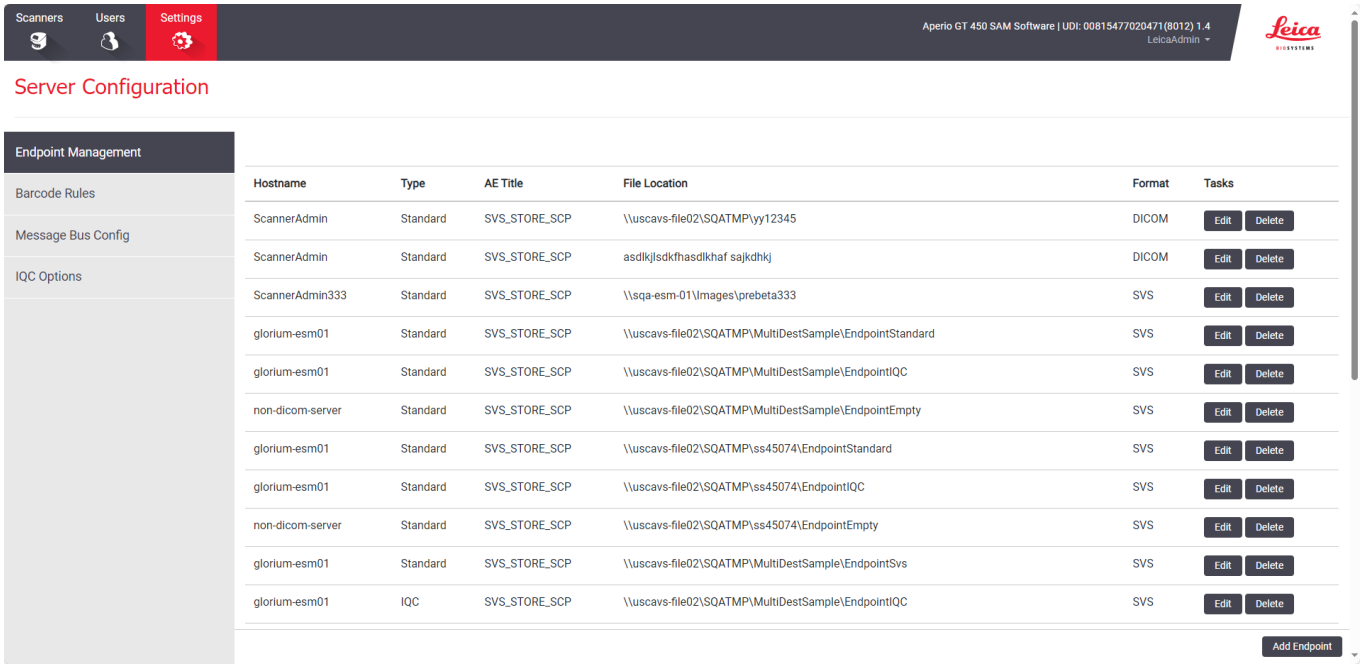
On the **Settings** pages you make these general server configurations:

- You populate Aperio GT 450 SAM with all the endpoints used by connected Aperio GT 450 scanners
- You define any barcode rules used by connected Aperio GT 450 SAM scanners
- You configure the Aperio iQC Software Module message bus
- You define the URL for the iQC API server (where the scanner can poll for iQC results so any artifacts can be displayed on the console UI)

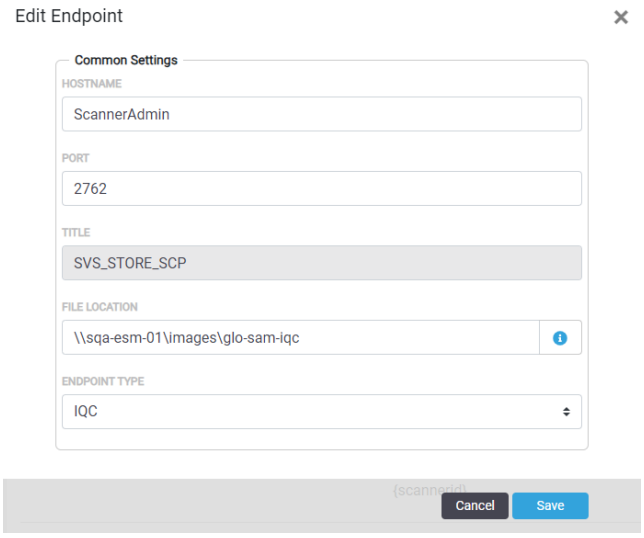
The **Settings** pages are available to the Lab Admin role.

Endpoint management

The **Endpoint Management** page allows you to configure where connected Aperio GT 450 scanners can send images. You can configure options such as hostname, port, title, and file location.



1 Click **Edit** to view or change settings for the selected endpoint, or click **Add Endpoint** to configure a new endpoint. The Endpoint window opens.



2 Populate the window with new or changed settings as described below, and click **Save**.

Common Settings:

HOSTNAME: The server hostname

PORT: The port that the server is configured to use

TITLE: Application entity title. Set by Leica Biosystems Technical Support.

FILE LOCATION: The file share where the images are stored. Available only if connected to the Leica DICOM Service.

ENDPOINT TYPE: Available only if the system is licensed for iQC. This field is used to indicate whether files are being sent to an IMS (**Standard**) or to iQC.

DICOM options:

If the scanner is licensed to support saving DICOM files, additional configuration options will be available:

IMAGE OUTPUT FORMAT: Either DICOM or SVS

SLIDE ID FORMAT: Use a regular expression to tell the system how to extract a Slide ID from the barcode.

A regular expression, regex or regexp, is a sequence of characters that define a search pattern. If you are not familiar with regular expressions, contact Leica Biosystems Technical Support for assistance.

CASE ID FORMAT: Use a regular expression to tell the system how to extract a Case ID from the barcode.

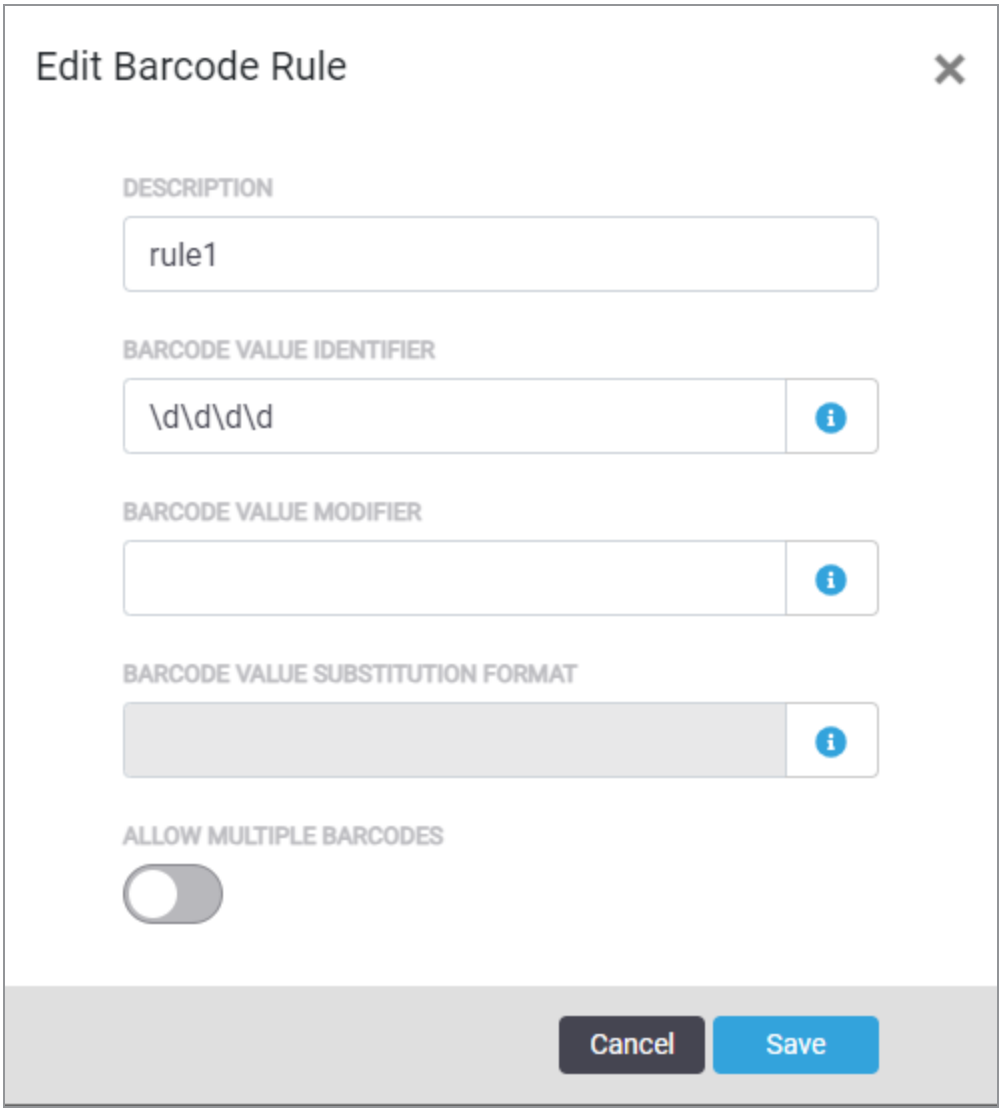
DIMENSION ORG TYPE: Specifies the structure of the image. Supports two options:

- **Full** : Tiles are sequentially encoded as successive frame in an implicit order.
- **Sparse**: Tiles are sparsely arranged and spaital positions of tiles are explicitly encoded.

Barcode Rules

The **Barcode Rules** page defines the barcode rules that are applied in the Aperio GT 450 system

1 Click **Edit** to view or change a barcode rule, or click **Add Barcode Rule** to configure a new rule. The **Barcode Rule** window opens.



2 Populate the window with new or changed settings as described below, and click **Save**.

DESCRIPTION: This is a user-defined field. Because regular expressions are challenging to recognize at a glance, use this field to provide a "friendly name" to help identify your barcode rule. This can be helpful if your institution has many types of barcodes with different rulesets.

BARCODE VALUE IDENTIFIER: If your institution uses multiple barcodes, you will want to identify which barcode will be associated with the scanned image and displayed in the digital slide management system. To do this, enter a search string in regular expression format in the **BARCODE VALUE IDENTIFIER** field.

A regular expression, regex or regexp, is a sequence of characters that define a search pattern. For example, "\d{6}" specifies that a barcode with six digits in a row will be used. If you are not familiar with regular expressions, contact Leica Biosystems Technical Support for assistance.

BARCODE VALUE MODIFIER: Some institutions embed control (non-printable) characters in their barcodes. If you want to filter out or replace these characters, enter the characters you want to modify in regular expression format in the **BARCODE VALUE MODIFIER** field. For example, [\x00-\x1f\x7f] specifies that all non-printable characters will be modified.

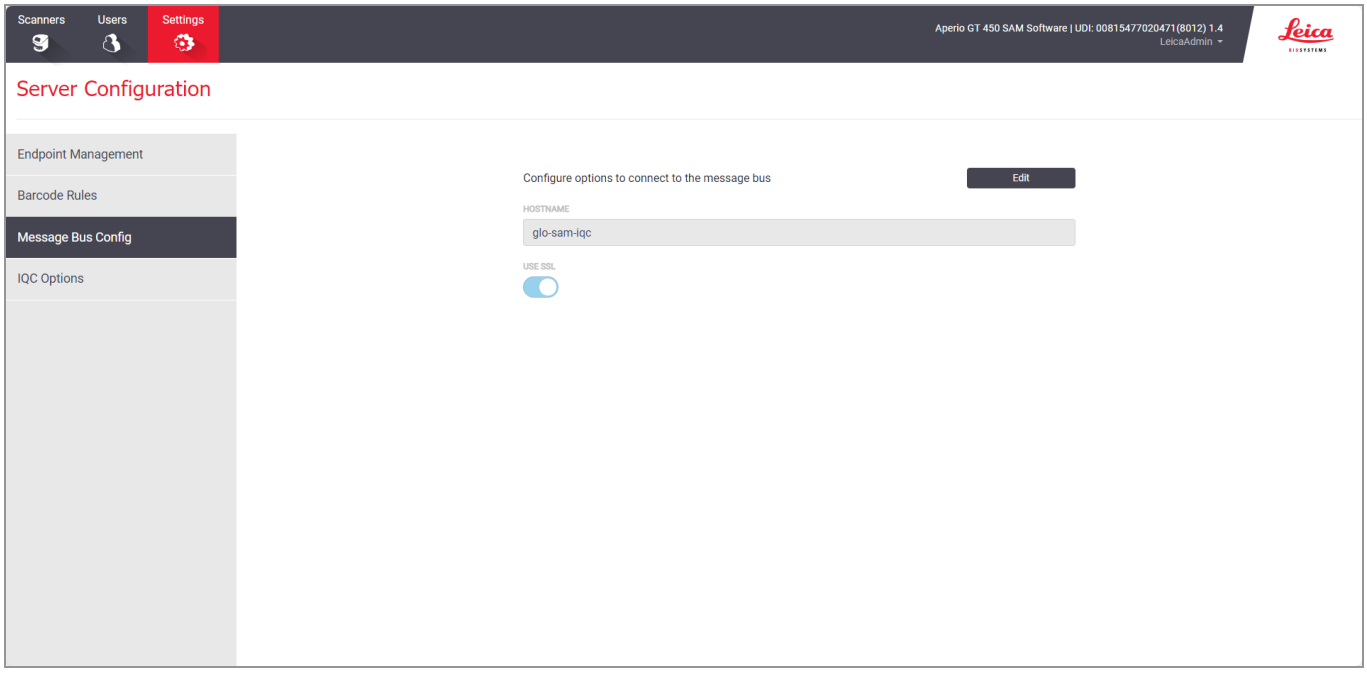
BARCODE VALUE SUBSTITUTION FORMAT: If there are non-printable characters you want to replace that are matched by the **BARCODE VALUE MODIFIER** field, specify that value in the **BARCODE VALUE SUBSTITUTION FORMAT** field. For example, a value of "?" combined with a **BARCODE VALUE MODIFIER** field value of [\x00-\x1f\x7f] replaces all non-printable characters with a question mark "?". Leave this value empty to remove characters matched by characters in the **BARCODE VALUE MODIFIER** field.

ALLOW MULTIPLE BARCODES: Depending on your institution's procedures, you may have more than one barcode on the glass slide label. Click **ALLOW MULTIPLE BARCODES** to enable this feature.

The features discussed in this section allow for more advanced modifications to the barcode. If you require additional control over the barcode string returned by the Aperio GT 450, contact Leica Biosystems Technical Services.

Message Bus Config

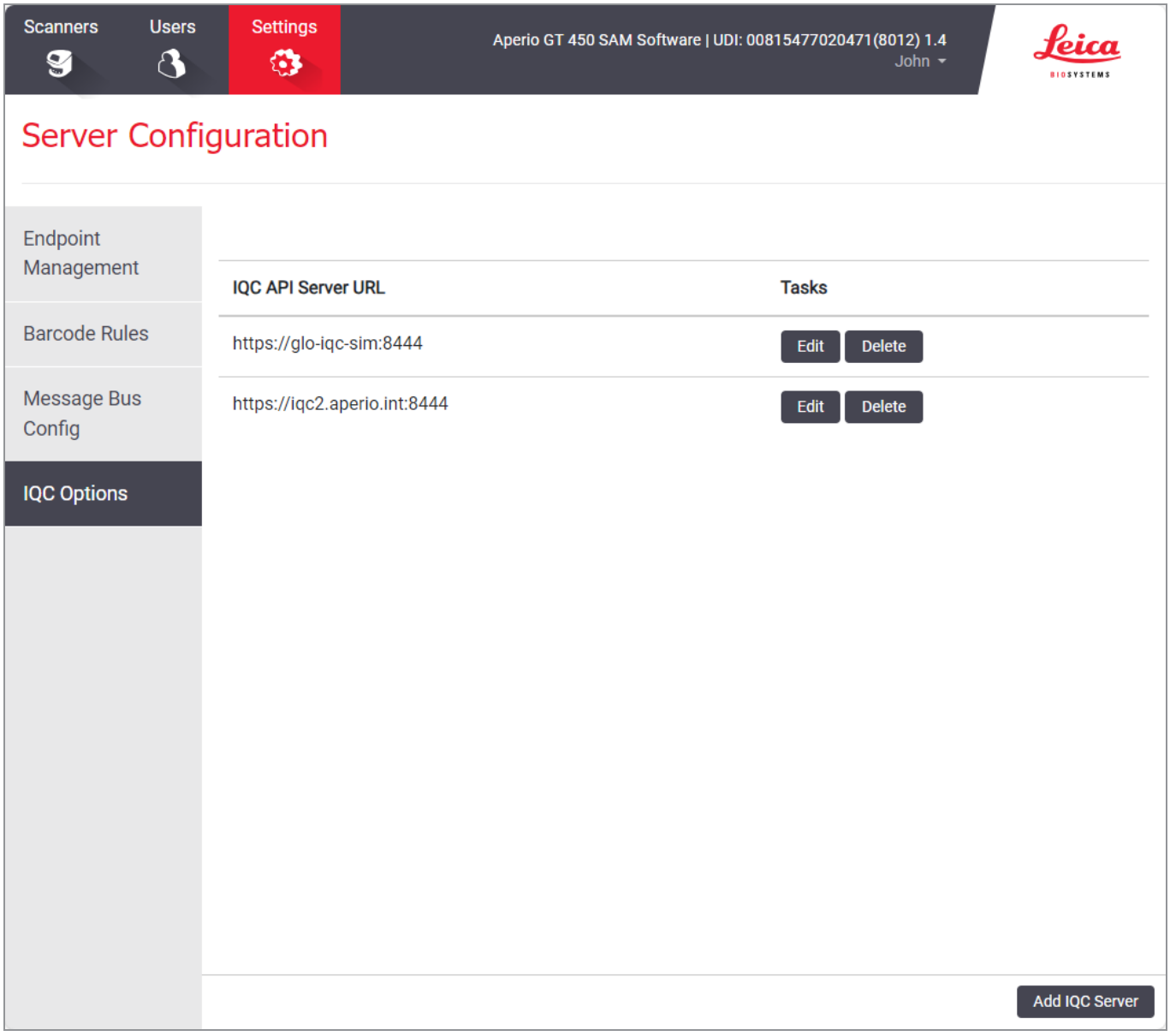
The **Message Bus Config** page is available only if the Aperio iQC Software Module is licensed on one or more connected scanners. It defines the hostname of the iQC message bus and enables SSL encryption for the message bus.



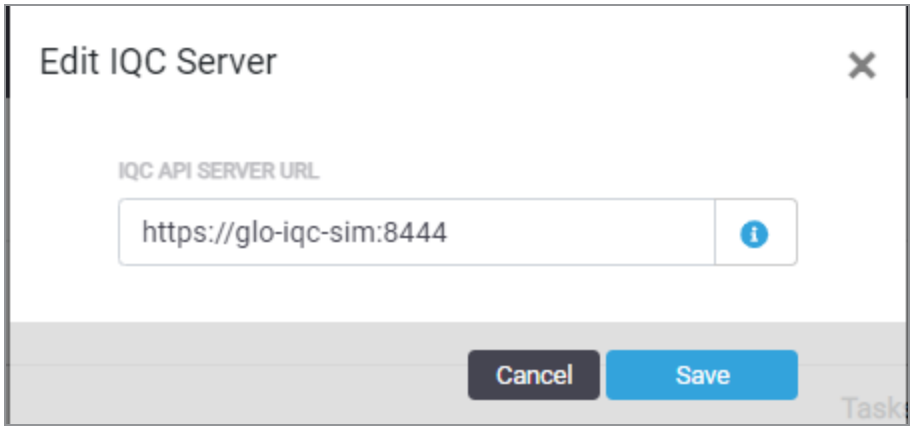
To configure the message bus, click **Edit**, change settings as needed, and click **Save**.

iQC Options

The **iQC Options** page is available only if iQC is licensed on one or more connected scanners. It defines the URL for the iQC API server.



1 Click **Edit** to change the URL for the iQC API Server, or click **Add IQC Server** to configure a new server. The IQC Server window opens.



2 Specify the **IQC API SERVER URL** (typically https://<server-name>:8444), and click **Save**.

Enabling DICOM image output

The Aperio GT 450 can output image files in either SVS or DICOM format. (The default is .SVS image file format.)

The optional DICOM feature is purchased and installed separately for each Aperio GT 450 scanner. You must use Aperio GT 450 SAM to configure the final storage location for the DICOM images (PACS, IMS, or file share).

Third-party developers retrieve the DICOM images and metadata by leveraging the scanner C-STORE interface (or alternatively by accessing the file share defined in Aperio GT 450 SAM). For details on DICOM images and their metadata transmitted to third-party systems, refer to *Aperio DICOM Conformance Statement*, MAN-0465.

Before you can enable DICOM image output, your IT environment must meet the requirements detailed in the *Aperio GT 450 DICOM Conformance Statement*. Also, a Leica Biosystems Technical Services representative will need to log into Aperio GT 450 SAM as a Leica Admin and enable **Optional Features** for the scanner you want to configure for DICOM.

After the DICOM feature pack is installed and configured by Leica Biosystems Technical Support, log into Aperio GT 450 SAM as a Lab Admin.

1. Click **Settings** in the banner at the top of the page.
2. Click **Endpoint Management**.
3. Confirm that the endpoint list includes the DICOM image host. If needed, add an endpoint or edit an existing one.
4. Set the **IMAGE OUTPUT FORMAT** to DICOM.
5. If configuring a third-party DICOM server, specify the **HOSTNAME**, **PORT**, and **TITLE** of the DICOM host.
6. If sending the DICOM image to a file share, accept the default **HOSTNAME**, **PORT**, and **TITLE**.
7. If you want the scanner to populate the Slide and Specimen container headers, type the slide ID format as a regular expression in the **SLIDE ID FORMAT** box.

   A regular expression, regex or regexp, is a sequence of characters that define a search pattern. If you are not familiar with regular expressions, contact Leica Biosystems Technical Support for assistance.

8 If you want the scanner to populate the Study instance UID and Accession Number headers, type the Case ID format as a regular expresion in the **CASE ID FORMAT** box.

   a In the **DIMENSION ORGANIZATION** box, select either **Full** or **Sparse**. The **DIMENSION ORGANIZATION TYPE** box selects how the DICOM images will be organized and encoded.

   Sparse selects the DICOM value TILED_SPARSE in this format:

   - Tile coordinates and position must be explicitly recorded for each tile.
   - Not all tiles need to be present.
   - Frame items can be encoded in the pixel data element in any order.

   Full selects the DICOM value TILED_FULL in this format:

   - A frame must exist for each file of the rectangular total pixel matrix.
   - A frame must exist for every tile.
   - The order in which the tiles are encoded in the pixel data element is predictable.

   Each type of format has advantages and disadvantages in processing speed and file size.

   Due to a technical limitation of the SVS generation process, TILED_FULL is not supported with iQC integration. This limitation will be remediated in a future release.

9 Save the endpoint.

10 Click **Scanners** in the banner at the top of the page.

11 Click **Configuration** for the selected scanner.

12 Click **Edit**.

13 Select the DICOM server from the **ENDPOINT 1** drop-down list.

14 Click **Save**.

Configuring the scanner to send images to Aperio iQC Software Module

1 Make sure that the scanner is licensed for the Aperio iQC Software Module, and that it supports at least two endpoints.

2 Click **Settings** in the banner at the top of the page.

3 Click **Endpoint Management**.

4 When a scanner is licensed for the Aperio iQC Software Module, a new field called **ENDPOINT TYPE** appears in the endpoint dialog. The options are **Standard** and **iQC**. Add at least one **Standard** endpoint for the connected eSM/IMS instance, and one **iQC** endpoint, which is pointed to the file share that iQC Services are watching.

Do not use the {scannerid} key on iQC endpoints. iQC Services do not support nesting folders by scanner. All scanners monitored by the same iQC Service should point to the same path.

5 Click **Message Bus Config**.

6 In the **Message Bus Config** box, set the **HOSTNAME** to the hostname of the server where the message bus is installed.

7 Make sure that **Use SSL** is enabled.

8 Navigate to **iQC Options**.

9 Make sure that at least one iQC API server is added.

Note that the iQC API URL is not the same as the iQC Dashboard URL. Typically, the dashboard is available on port 8443, while the API is available on port 8444. Consult Leica Technical Services for the correct configuration details for your installation.

10 Click the **Scanners** icon, and click **Configuration** for the selected scanner.

11 Click **Edit**.

12 On the **Images** page, select the same two endpoints (Standard and iQC) that you just added to the **Settings** page (for example, as **ENDPOINT 1** and **ENDPOINT 2**).

13 In the **IQC INTEGRATION** box, select the appropriate iQC server.

14 Click **Save**.

15 In the **Dimension Organization Type** box, select either **Full** or **Sparse**. The **DIMENSIONS ORGANIZATION TYPE** box selects how the DICOM images will be organized and encoded.

Sparse selects the DICOM value TILED_SPARSE in this format:

- Tile coordinates and position must be explicitly recorded for each tile.
- Not all tiles need to be present.
- Frame items can be encoded in the pixel data element in any order.

Full selects the DICOM value TILED_FULL in this format:

- A frame must exist for each file of the rectangular total pixel matrix.
- A frame must exist for every tile.
- The order in which the tiles are encoded in the pixel data element is predictable.

Each type of format has advantages and disadvantages in processing speed and file size.

Due to a technical limitation of the SVS generation process, TILED_FULL is not supported with iQC integration. This limitation will be remediated in a future release.

16 Save the endpoint.

17 Click **Scanners** in the banner at the top of the page.

18 Click **Configuration** for the selected scanner.

19 Click **Edit**.

20 Select the DICOM server from the **ENDPOINT 1** drop-down list.

21 Click **Save**.

4 Viewing system information

In this section:

This chapter explains how to display the various configuration options and settings of the Aperio GT 450 SAM server.

Displaying scanner information and settings

Refer to the table below for instructions on how to display scanner and system settings.

In many cases you cannot modify these settings, but Leica Biosystems Technical Support may ask you for the information during troubleshooting or maintenance procedures. Some settings can only be seen by users with the Lab Admin role.

To View:	Do This:
MAC Address	Select the scanner from the main screen to display the Edit Scanner dialog box.
Scanner Hostname	
Scanner Friendly Name	
Scanner Model	
Scanner Language	
Scanner Serial Number	Select the scanner from the main screen to display the Edit Scanner dialog box, or Click **System Information** for the scanner, and then click **Info** from the side menu.
Scanner Firmware Version	Click **System Information** for the scanner, and then click **Info** from the side menu.
Scanner Hardware Version	
Scanner Installation Date	
DICOM Server Settings	Click **Configuration** for the scanner, and then click **Images** from the side menu.
DSR Server Settings	Click **Configuration** for the scanner, and then click **DSR** from the side menu.
Event Handling (MI7K server) Settings	Click **Configuration** for the scanner, and then click **Event Handling** from the side menu.
Camera Configuration Settings	Click **System Information** for the scanner, and then click **Settings** from the side menu.
Scanner Additional Config Settings	
Focus Algorithm Config Settings	
Motion Config XML File	
Autoloader Config XML File	
List of Users	Click the **Users** icon in the top banner.
List of PINs	Click **Configuration** for the scanner, and then click **PIN Management** from the side menu.

Displaying scanner statistics

The Aperio GT 450 SAM console can display the same scanner statistics as those that are available from the scanner control panel display.

Users with either Operator or Lab Admin roles can display the statistics and select from one of the following:

- Display the number of slides scanned in the last 7 days
- Display the number of slides scanned in the last 12 months
- Display all slides, by year

To display the scanner statistics:

1. Confirm that the Scanners icon in the banner is selected, and the page shows the list of scanners.
2. Click the **System Information** icon to the right of the scanner.
3. Click **Scanner Statistics** in the side menu bar.
4. Select the display period from the choices above the grid.
5. Click  to print the statistics. Use the printer dialog to specify the printer and other print options.

Working with the Event Log

To display the Event Log:

1. Confirm that the Scanners icon in the banner is selected, and the page shows the list of scanners.
2. Click the **Event Logs** icon to the right of the scanner.

   The screen displays all of the errors and events since the screen was last cleared. From this screen you can do the following:

   - Click the **Download All Logs** button to save a .zip file in the Aperio GT 450 SAM server Downloads folder that contains a set of diagnostic logs. User login events are contained in these logs.

     To use the **Download All Logs** button, your workstation must be connected to your institution's Local Area Network with access to the Aperio GT 450 SAM server; you cannot access the Aperio GT 450 SAM server remotely from outside the LAN to use this feature.

   - Click **Clear Current Screen** to clear the entries from the screen. Note that this will not delete the entries in the log.

Back up log files

We recommend backing up the scanner log files downloaded to the Aperio GT 450 SAM server and storing the backups offsite. We also recommend backing up Windows Event logs on the Aperio GT 450 SAM server and storing those backups offsite.

Login alerts

The Console.log file contains user login events such as successful logins with user names. It also alerts you to failed logins.

The log can also show “Possible Intrusion Detected” in case of log-in discrepancies that occur while accessing the scanner remotely through SSH.

Note that automated analysis software such as Intrusion Detection System, IDS, can be used to analyze the log files.

5 User management

In this section:

This chapter provides information on how to configure user accounts for Aperio GT 450 SAM.

Before a user can log in to Aperio GT 450 SAM to either view or edit system and scanner settings, they must have an account. Aperio GT 450 SAM user accounts apply to all scanners on Aperio GT 450 SAM.

The administrator creates accounts for each user and assigns a role to the user at that time. The user's role determines what that user can and cannot do on the system.

If you want to assign a PIN to a user to access a scanner, you must first add the user on Aperio GT 450 SAM.

Understanding roles

There are three user roles:

- Operator Role
- Lab Admin Role
- Leica Support Role

Role	Description

Operator Role	This is a general-purpose role, appropriate for most users. Users with the Operator role can view most of the system settings, and do the following:
	• View the status of each scanner
	• View System Information for each scanner
	  • Info page
	  • Scanner Statistics
	  • Settings page
	• View the Event Log
	• Change his or her own password
	Operators cannot view or change the PINs assigned to a scanner.
	Operators cannot view the list of users, and cannot change settings for other users.

Lab Admin Role	This role provides advanced administrative access, and is appropriate for users who will need to add or manage other user accounts, or make changes to the system. In addition to what is available to operators, users with the Administrator role can do the following: • Add, modify, and delete other user accounts • Change user passwords • View System Information and edit some of the settings

Role	Description

	• Edit the Configuration settings:
	  • Images
	  • DSR
	  • Event Handling
	  • PIN Management

Leica Support Role	This is a protected role, and cannot be assigned to users. This role (which has a user name of Leica Admin) cannot be deleted from the system. It is used by Leica Support Representatives for troubleshooting, maintenance, and repair functions, and also provides the ability to add and delete scanners from the system.

Managing users

Only those users with the Lab Admin role can view or modify the list of users or modify existing user accounts.

Add a user

1. Select **Users** from the top ribbon on the main page.
2. Click **Add User** from the bottom of the user list page.
3. Enter the information for the new user account:
   - The login Name (1 to 296 characters, and may include letters, numbers, and special characters)
   - The user's full name
4. Enter an initial password. Passwords have the following requirements:
   - At least 10 characters
   - At least one uppercase letter and one lowercase letter
   - At least one number
   - At least one special character: ! @ # $ % ^ * or _
   - Different from the previous 5 passwords
5. Select a Role: Lab Admin or Operator.
6. Click **Save**.

Edit a user

1. Select **Users** from the top ribbon on the main page.
2. Click **Edit** next to the name of the user you want to edit.
3. Enter the new information.

   Note that you cannot change the Role for an existing user account.
4. Click **Save**.

Delete a user

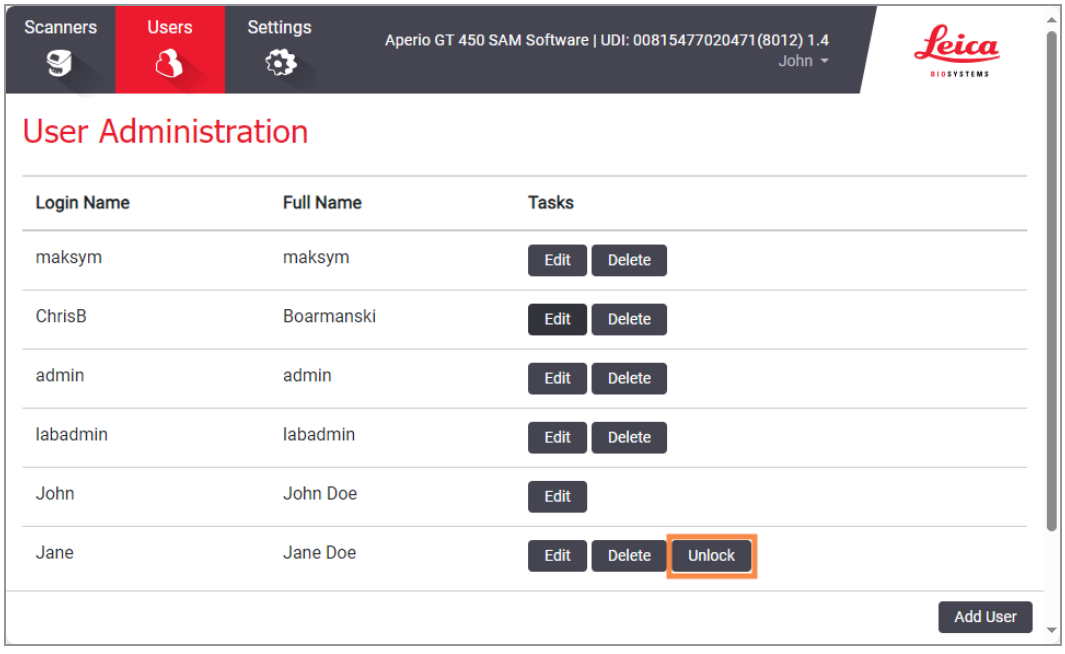
1. Select **Users** from the top ribbon on the main page.
2. Click **Delete** next to the name of the user you want to remove.
3. Confirm that you want to delete the user, or click **Cancel**.

Unlock a user account

After three unsuccessful login attempts to log into the Aperio GT 450 SAM server, Aperio GT 450 SAM locks that user out.

A user with the Lab Admin role can unlock operator accounts. (A LeicaAdmin user can unlock all accounts.)

1. Select **Users** from the top ribbon on the main page.
2. Click **Unlock** next to the name of the user account you want to unlock.



Changing your user password

After successfully logging in, each user can change his or her password:

1. Select the user name shown in the upper right-hand area of the main page.
2. Click the **Change Password** link.
3. Enter a new password. Password requirements are:
    - At least 10 characters
    - At least one uppercase letter and one lowercase letter
    - At least one number
    - At least one special character: ! @ # $ % ^ * or _
    - Different from the previous 5 passwords
4. Confirm the password, and then click **OK**.

6 Cybersecurity and network recommendations

In this section:

This chapter discusses how Aperio GT 450 and Aperio GT 450 SAM protect electronic personal health information (EPHI) and provide protections against cybersecurity threats. We also discuss the measures you can take to protect the Aperio GT 450 SAM 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 Aperio GT 450 and Aperio GT 450 SAM from cybersecurity threats.

The recommendations in this section apply to the Windows-based server used to host Aperio GT 450 SAM. The security and network settings are configured through the Windows operating system and administrative tools. The information here is provided for reference only. Refer to your Windows 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.

After installation of the Aperio GT 450 product, the Leica Biosystems representative will turn over to your IT staff sensitive cybersecurity items such as SSL certificate credentials, Aperio GT 450 SAM server disk encryption key, and so on. The customer assumes ownership of these items, and it is the customer's responsibility to safeguard this information.

Aperio GT 450 and Aperio GT 450 SAM cybersecurity features

Cybersecurity features included in the Aperio GT 450 product protect critical functionality despite cybersecurity compromise. These include:

- To reduce cybersecurity vulnerability, the respective operating systems on the Aperio GT 450 VPU and Aperio GT 450 SAM software are hardened with CIS (Center for Internet Security) benchmarks.
- The Aperio GT 450 scanner and Aperio GT 450 SAM are not intended to store sensitive data, only to export/upload data to connected applications on separate network servers. The connection between the Aperio GT 450 scanner and the Aperio GT 450 SAM server 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.
- The scanner USB ports are not exposed and are disabled during runtime to prevent any insertion of malware.
- Allow/deny listing is used on the Aperio GT 450 scanner and recommended for use on the Aperio GT 450 SAM server. This prevents unauthorized software from running on these components.
- The daily maintenance for the Aperio GT 450 scanner includes rebooting it every day. (See the *Aperio GT 450User's Guide* for details.) This refreshes the firmware and updates allow/deny listings.
- The Aperio GT 450 Console.log file contains user login events with user names. It can also show "Possible Intrusion Detected" in case of log-in discrepancies while accessing the scanner remotely through SSH. For details on downloading the log files, see Working with the Event Log (on page 65).

Data protection

Data at rest is 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 Personal Health Information (PHI). The key is not saved on any persistent storage that is internal or external to the scanner VPU. As a result, the data on these partitions become inaccessible once the operating system shuts down or the VPU is powered off. These partitions are wiped clean and encrypted again the next time the operating system boots up. This ensures the scanner does not inadvertently expose PHI.

Data in transit is protected by encryption. All sensitive information is transmitted between the scanner and Aperio GT 450 SAM 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.

Data backup

Backing up data is an important element of managing and protecting your data. Although you undoubtedly have your own backup strategy and plan in place, Leica Biosystems has instituted an automatic backup for the Aperio GT 450 DataServer database which can be a part of your overall backup plan.

The Aperio GT 450 database is maintained by Microsoft SQL Server and the automatic backup is created as a SQL Server backup file under the direction of the DataServer.

If you need to restore a backup, you will need to use the Microsoft SQL Server Management Studio or T-SQL statements, so we recommend that someone in your IT department or organization be familiar with managing SQL.

For information on downloading and backing up scanner log files, see Working with the Event Log (on page 65)

Physical safeguards for Aperio GT 450

Protect the Aperio GT 450 scanner from unauthorized access by limiting physical access to it.

Protecting the Aperio GT 450 SAM server

The following sections contain recommendations for protecting the Aperio Aperio GT 450 SAM server.

Password, login, and user configuration safeguards

- The password requirements for users logging into the Aperio GT 450 SAM 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 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 GT 450 SAM administrator to unlock the account.
- We recommend you configure workstations used to log into Aperio GT 450 SAM 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 GT 450 SAM.

Physical safeguards for the Aperio GT 450 SAM server

- Protect the Aperio GT 450 SAM server and client workstations used to log into Aperio GT 450 SAM from unauthorized access by limiting physical access to them.
- To protect the Aperio GT 450 SAM server from malware intrusion, use caution when inserting USB drives and other removable devices. Consider disabling USB ports that are not in use. If you plug in a USB drive or other removable device, you should scan the devices with an anti-malware utility.

Aperio GT 450 SAM 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 GT 450 SAM server, the user roles are “Operator” and “Lab Admin,” which have different permissions.
- Protect the Aperio GT 450 SAM server and client workstations from unauthorized access by using standard IT techniques. Examples include:
  - Firewalls — We recommend enabling the Windows firewall on client workstations.
  - Allow listing, an administrative tool that allows only authorized programs to run, should be implemented on the Aperio GT 450 SAM server.
- Leica Biosystems recommends you use SQL Standard (2019 or later) or Enterprise SQL server which comes with database encryption.
- 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 Windows and Aperio security patches and hot fixes that may be available for the system, and ensure the server is configured securely. See Recommended registry settings to secure Windows Server 2019 and Windows Server 2022 (on page 78).
- 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" as these files can be very large and are accessed continually as they are being scanned and users are viewing the digital slides. 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.
- For the Aperio GT 450 SAM to DSR network connection, we recommend you use a storage server that supports the SMB3 network protocol to protect data in transit. If the DSR server does not support SMB3 or later, mitigation is required to protect data in transit.
- 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 Windows Event logging on your server to track user access and changes to data folders that contain patient information and images.

  Routinely back up the Windows 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.

Require SMB encryption with Windows Admin Center

To further protect your Aperio GT 450 SAM server, Leica Biosystems recommends requiring SMB encryption for shared files. Follow the steps below to enable SMB encryption using Windows Admin Center.

1. Download and install Windows Admin Center (Windows Admin Center Overview | Microsoft Learn).
2. Connect to the file server where the scanner is configured to save images.
3. Select **Files & file sharing**.
4. Select the **File shares** tab.
5. To require encryption on a share, select the share name and choose **Enable SMB encryption**.
6. To require encryption on the server, select **File server settings**.
7. Under **SMB 3 encryption**, select **Required from all clients (others are rejected)**, and then choose **Save**.

Additional security controls

By default, Windows servers enable weak encryption protocols and ciphers to preserve compatibility with older systems. Leica Biosystems recommends disabling these encryption protocols and ciphers by adding the registry entries specified in Recommended registry settings to secure Windows Server 2019 and Windows Server 2022 (on page 78) to your registry.

Follow the steps below to copy and paste the registry entries from this PDF document to a .reg file, which you can then import to your registry using RegEdit.

1. Because the registry settings span more than one page in this document, you need to copy and paste them to your registry document in multiple steps.
2. From this PDF document, select and copy only the registry settings on page 78. (Do not include the section title or the headers and footers from the document.)
3. Paste the content into a text file.
4. Repeat this step for each page of the registry settings, ensuring you copy and paste them in the same order that they appear in this document.
5. Save the text file with a .reg extension.
6. Open the Registry Editor (regedit.exe).
7. From the Registry Editor, go to the **File** menu, and selecting **Import** to import the .reg file you just saved.

Recommended registry settings to secure Windows Server 2019 and Windows Server 2022

```
Windows Registry Editor Version 5.00
[HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Hashes]
[HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Hashes\MD5]
"Enabled"=dword:ffffffff
[HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Hashes\SHA]
"Enabled"=dword:ffffffff
[HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Hashes\SHA256]
"Enabled"=dword:ffffffff
[HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Hashes\SHA384]
"Enabled"=dword:ffffffff
[HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Hashes\SHA512]
"Enabled"=dword:ffffffff
[HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\KeyExchangeAlgorithms]
[HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\KeyExchangeAlgorithms\Diffie-Hellman]
"Enabled"=dword:ffffffff
"ServerMinKeyBitLength"=dword:00000800
[HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\KeyExchangeAlgorithms\ECDH]
"Enabled"=dword:ffffffff
[HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\KeyExchangeAlgorithms\PKCS]
"Enabled"=dword:ffffffff
[HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Protocols]
[HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Protocols\Multi-Protocol Unified Hello]
[HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Protocols\Multi-Protocol Unified Hello\Server]
"Enabled"=dword:00000000
"DisabledByDefault"=dword:00000001
[HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Protocols\PCT 1.0]
[HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Protocols\PCT 1.0\Server]
"Enabled"=dword:00000000
```

"DisabledByDefault"=dword:00000001

[HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Protocols\SSL 2.0]

[HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Protocols\SSL 2.0\Server]

"Enabled"=dword:00000000

"DisabledByDefault"=dword:00000001

[HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Protocols\SSL 3.0]

[HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Protocols\SSL 3.0\Server]

"Enabled"=dword:00000000

"DisabledByDefault"=dword:00000001

[HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Protocols\TLS 1.0]

[HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Protocols\TLS 1.0\Server]

"Enabled"=dword:00000000

"DisabledByDefault"=dword:00000001

[HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Protocols\TLS 1.1]

[HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Protocols\TLS 1.1\Server]

"Enabled"=dword:00000000

"DisabledByDefault"=dword:00000001

[HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Protocols\TLS 1.2]

[HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Protocols\TLS 1.2\Server]

"Enabled"=dword:ffffffff

"DisabledByDefault"=dword:00000000

[HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Ciphers]

[HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Ciphers\AES 128/128]

"Enabled"=dword:ffffffff

[HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Ciphers\AES 256/256]

"Enabled"=dword:ffffffff

[HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Ciphers\DES 56/56]

"Enabled"=dword:00000000

[HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Ciphers\NULL]

"Enabled"=dword:00000000

[HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Ciphers\RC2 128/128]

"Enabled"=dword:00000000

[HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Ciphers\RC2 40/128]

"Enabled"=dword:00000000

[HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Ciphers\RC2 56/128]

"Enabled"=dword:00000000

[HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Ciphers\RC4 128/128]

"Enabled"=dword:00000000

[HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Ciphers\RC4 40/128]

"Enabled"=dword:00000000

[HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Ciphers\RC4 56/128]

"Enabled"=dword:00000000

[HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Ciphers\RC4 64/128]

"Enabled"=dword:00000000

[HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Ciphers\Triple DES 168]

"Enabled"=dword:00000000

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 GT 450 and Aperio GT 450 SAM 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 GT 450 and Aperio GT 450 SAM.

Support and cybersecurity patches

Note that technical support and cybersecurity patches for the Aperio GT 450 and Aperio Aperio GT 450 SAM may not be available after the product lifetime. Contact Leica Biosystems Technical Support for more information.

A Troubleshooting

In this section:

This appendix provides causes and solutions for problems related to the Aperio GT 450 SAM server and related components. It also provides common troubleshooting procedures that may need to be performed by the Aperio GT 450 lab administrator. For general troubleshooting information for the scanner operator, see the *Aperio GT 450 User's Guide*.

Aperio GT 450 SAM server troubleshooting

Symptom	Cause	Solution
"Credentials are Invalid" error message during login	Instance of DataServer used by Aperio GT 450 SAM is not running	Restart the DataServer service on the Aperio GT 450 SAM server. See Restart the DataServer (on page 84).
	Incorrect credentials	Check for caps lock, etc. Verify credentials with the Administrator
After update, new features are not available in the Aperio GT 450 SAM User Interface	Application is cached in the browser	Exit Aperio GT 450 SAM and then clear the browser cache
Scanner is on and connected to Aperio GT 450 SAM (retrieves its settings) but Aperio GT 450 SAM shows the scanner as offline and no statistical data is being reported (number of scans, etc.)	MI7K on the Aperio GT 450 SAM server is not running	See Verify that MI7K is running (on page 84).
	Ports are not open	Ensure port 6663 is open in the firewall and reachable by the scanner.
Scanner log files are not appearing in the scanner logs folder	MI7K on the Aperio GT 450 SAM server is not running	See Restart the DataServer (on page 84).
	Log output folder configured incorrectly	Check the Configuration Map tab under settings (AppLog_Dir).
	MI7K error	Check the MI7K Dashboard for any errors related to the "ScannerAppLogWriter" channel and refer to the MI7K error log for more details.
	Ports are not open	Ensure port 6663 is open in the firewall and reachable by the scanner.
The Aperio GT 450 SAM UI is not reachable or is returning an error code when trying to connect	IIS error	Ensure that IIS and the site are running and the ports Aperio GT 450 SAM is available on are open in the firewall.
	Anonymous Authentication configuration error in IIS	Check the IIS Configuration. See IIS configuration error below.

Restart the DataServer

On the server, go to the Services manager and make sure the “ApDataService” service is running. If the service fails to start or the errors persist, view the DataServer logs for more information (usually found at C:\Program Files (x86)\Aperio\DataServer\ Logs).

Verify that MI7K is running

On the server, ensure that the MI7K server is running. If the server is running, ensure that the Configuration Map Settings are configured to point to the correct DataServer Host (SAM_Host) and Port (SAM_Port) and are using the correct SSL or non-SSL connection (SAM_UriSchema). If the Dashboard in MI7K is reporting errors on “ScannerEventProcessor” channel, refer to the MI7K error logs for more details. If DataServer is not running this could lead to MI7K channel errors. Ensure port 6663 is open in the firewall and reachable by the scanner.

IIS configuration error

To check this setting open the site in IIS and go to the Authentication setting. Find and edit the Anonymous Authentication item and ensure the Specific user is set to “IUSR” (no password). If the site is running and all settings are correct, please see the IIS logs for more details.

Scanner network troubleshooting

Symptom	Cause	Solution
The user reports error 1007: Internal Storage Full	Variable: The system cannot send the images to the DICOM server, or the DICOM server cannot send data to your site's image storage location.	1 Ensure the LAN cables are connected to the scanner LAN port and to the Aperio GT 450 SAM server. 2 Do not restart the scanner. If you restart the scanner, the scanned data is lost, and users have to rescan their slides. 3 Check the connectivity from the scanner to the DICOM server, and from the DICOM server to your site's image storage location. 4 Ensure the DICOM server is running. Restart the DICOM server if necessary. 5 Check if your site's image storage location is full. 6 Check if there is a permissions or account problem with the account running the DICOM server. 7 If the issue persists, consult with your organization's IT professionals prior to calling Leica Biosystems Technical Services. When the issue is resolved, if you have not restarted the scanner, the scanner starts transferring the slide images to the DICOM server.
The user Reports Image Transfer errors on scanner	Variable: The system cannot send the images to the DICOM server, or the DICOM server cannot send data to your site's image storage location.	1 Ensure the LAN cables are connected to the scanner LAN port and to the Aperio GT 450 SAM server. 2 Do not restart the scanner. If you restart the scanner, the scanned data is lost, and users have to rescan their slides. 3 Check the connectivity from the scanner to the DICOM server, and from the DICOM server to your site's image storage location 4 Ensure the DICOM server is running. Restart the DICOM server if necessary. 5 Check if your site's image storage location is full. 6 Check if there is a permissions or account problem with the account running the DICOM server. 7 If the issue persists, consult with your organization's IT professionals prior to calling Leica Biosystems Technical Services.

Symptom	Cause	Solution
		When the issue is resolved, if you have not restarted the scanner, the scanner starts transferring the slide images to the DICOM server.
The user reports the scanner is indicating it has no network connectivity	The scanner is unable to reach the Aperio GT 450 SAM server	1 Ensure the LAN cables are connected to the scanner LAN port and to theAperio GT 450 SAM server. 2 In the area provided on the scanner's touchscreen interface, enter the IP address of the Aperio GT 450 SAM server.  3 Verify the network connections are up and working for the Scanner and Aperio GT 450 SAM server. (Consult your organization's IT professionals if needed.) 4 On the server, go to the Services Manager and restart all services. It may take a few minutes for all the services to restart. 5 Try to connect from the scanner again by manually entering the IP address again. 6 If the issue persists, consult with your organization's IT professionals prior to calling Leica Biosystems Technical Services.

B Summary of scanner setting and configuration options

In this section:

This appendix provides a list of the settings and configuration options. Use these tables as a checklist as you gather the information you will need if you add or reconfigure a scanner. Note that during installation, most of these settings and configuration options will be set for you by the Leica Biosystems representative.

Basic scanner information

Lab Administrators may select the name of the scanner from the scanner page to display the basic scanner settings. (Operators can see some of the settings from the System Information page.) Any setting displayed in a gray box cannot be changed by a Lab Administrator or Operator.

Setting	Description	View/Edit	
		Admin	Operator
MAC Address	Specified during installation	View	None
Hostname	Specified during installation	View	None
Name	Description for the scanner, displayed on the **Scanners** home page	View/Edit	None
Model	Aperio GT 450	View	None
Serial Number	Specified during installation and verified at start-up	View	View
Language	Controls the language used for scanner menus and messages	View/Edit	None

Scanner configuration

Use the following table to gather the information you will need for each scanner on the system. After the Leica Support Representative installs your scanner, you may want to record the settings for future reference.

Not all listed settings may be visible on your system. Setting visibility is based on option licensing and the user's role (Operator or Lab Admin).

Option	Description	View/Edit	
		Lab Admin	Operator
Images			
ENDPOINT *n*	Endpoint (server) that houses the DICOM files.	View/Edit	None
BARCODE RULE	Rule to be applied to barcodes for the DICOM files. For details about barcode rules, see Barcode Rules (on page 53).	View/Edit	None
IQC INTEGRATION	Endpoint (server) that houses the files used by the iQC Software Module.	View/Edit	None
IMAGE FILENAME FORMAT	Sets the base file name for the scanned image file.	View/Edit	None
REQUIRE BARCODE ID	Specifies that only slides with readable barcodes will be scanned.	View/Edit	None

Option	Description	View/Edit	
		Lab Admin	Operator
PYRAMID LEVEL DOWNSCALING	Enables the 2x default Pyramid Level Downscaling option.	View/Edit	None
DSR			
HOSTNAME	Hostname of the server where the metadata is stored.	View/Edit	None
PORT	The secured port used for the DSR. The default is 44386.	View/Edit	None
SEND IMAGE DATA TO ESM	Enables transmission of image data to the eSlide Manager (eSM).	View/Edit	None
Event Handling			
HOSTNAME	Hostname of the server where MI7K resides. • Use ScannerAdmin if MI7K is installed on the Aperio GT 450 SAM server. • Otherwise, use the hostname of the server where the MI7K instance used for Aperio GT 450 SAM is installed.	View/Edit	None
LOG PORT	The port that MI7K is configured at installation to use for log data. The default is 6662.	View/Edit	None
EVENT PORT	The port that MI7K is configured at installation to use for event data. The default is 6663.	View/Edit	None
PIN Management			
Console PIN Timeout	Timeout interval (minutes); the scanner locks the display and control pad when there is no operator interaction for this period of time.		
New PIN	A 5-digit code to unlock the scanner. Numbers only.	View/Edit	None
New PIN: LOGIN NAME		View/Edit	None
New PIN: DESCRIPTION	Identifying information for the PIN. This is a general description field, and can contain numbers, letters, and punctuation characters.	View/Edit	None
Time Zone			
TIME ZONE	Set by Aperio GT 450 SAM administrator.	View/Edit	None
Scan Settings			

Option	Description	View/Edit	
		Lab Admin	Operator
DEFAULT TO 20X SCANNING	Defaults to 20x rather than 40x scanning.	View/Edit	None
ENABLE DEFAULT CALIBRATION POINT	Enables the setting of a default calibration point, which is used during pre-scanning for white balance and illumination correction.	View/Edit	None
ENABLE AUTO NARROW STRIPE	Enables the Auto Narrow Stripe feature.	View/Edit	None
ENABLE EXTENDED FOCUS IMAGE OUTPUT	Enables the Extended Focus feature. This option allows you to scan a slide to generate a single composite image with optimized focus and a greater depth of field than an image of any single layer in a set of z-stack images.	View/Edit	None
Z-STACK: NUMBER OF LAYERS	Default number of layers used in z-stack scanning. The user sets the actual value per rack on the console.	View/Edit	None
Z-STACK: LAYER SEPARATION (µm)	Default distance between layers used for z-stack scanning. The user sets the actual value per rack on the console.	View/Edit	None

Server configuration: Settings

Option	Description	View/Edit	
		Lab Admin	Operator
Endpoint Management			
HOSTNAME	Hostname of the endpoint.	View/Edit	None
PORT	The port that the endpoint is configured to use.	View/Edit	None
TITLE	Application entity title. Set by Leica Biosystems Technical Support. For internal use. Do not change unles instructed to do so by Leica Biosystems Technical Support.	View/Edit	None
FILE LOCATION	The complete path to the file share where the converter will place the converted images. This is a location on the network where converted SVS files are stored.	View/Edit	None
ENDPOINT TYPE	Either Standard or IQC.	View/Edit	None
Barcode Rules			
DESCRIPTION	User-defined description.	View/Edit	None

Option	Description	View/Edit	
		Lab Admin	Operator
BARCODE VALUE IDENTIFIER	A regular expression search pattern used to tell the system which barcodes to save with scanned slide records.	View/Edit	None
BARCODE VALUE MODIFIER	A regular expression used to tell the system to exclude these nonprintable characters from the decoded value. Control (non-printable) characters that you want to filter out or replace. Specify this with a regular expression.	View/Edit	None
BARCODE VALUE SUBSTITUTION FORMAT	A printable character to tell the system to substitute the nonprintable character specified in the BARCODE VALUE MODIFIER field. Control (non-printable) characters that you want to replace that are matched by the BARCODE VALUE MODIFIER field.	View/Edit	None
ALLOW MULTIPLE BARCODES	Enables the use of multiple barcodes.	View/Edit	None
Message Bus Config			
HOSTNAME	Hostname of the iQC hosting server.	View/Edit	None
USE SSL	Enable the use of Secure Sockets Layer (SSL) protocol for the iQC service.	View/Edit	None
IQC Options			
IQC API Server URL	The URL for the IQC hosting server.	View/Edit	None

Index

N

O

P

R

S

T

U

Z