Aperio GT 450
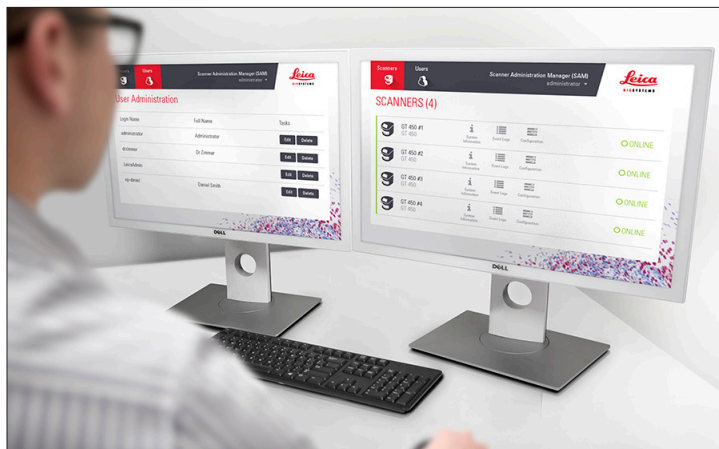
IT Manager and Lab Administrator Guide

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

Copyright Notice

- Copyright © 2019-2021 Leica Biosystems Imaging, Inc. All Rights Reserved. LEICA and the Leica logo are registered trademarks of Leica Microsystems IR GmbH. Aperio is a trademark of the Leica Biosystems group of companies in the USA and optionally in other countries. Other logos, product and/or company names might be trademarks of their respective owners.

- This product is protected by registered patents. For a list of patents, contact Leica Biosystems.

Customer Resources

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

Disclaimers

- This manual is not a substitute for the detailed operator training provided by Leica Biosystems Imaging or for other advanced instruction. Leica Biosystems Imaging Field Representatives should be contacted immediately for assistance in the event of any instrument malfunction. Installation of hardware should only be performed by a certified Leica Biosystems Imaging Service Engineer.

Contact Information – Leica Biosystems Imaging, Inc.

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

Customer Service Contacts

Please contact the office for your country for technical assistance.

Australia:
96 Ricketts Road
Mount Waverly, VIC 3149
AUSTRALIA
Tel: 1800 625 286 (toll free)
Between 8:30 AM-5 PM, Monday-Friday, AEST
Email: lbs-anz-service@leicabiosystems.com

Austria:
Leica Biosystems Nussloch GmbH
Technical Assistance Center
Heidelberger Strasse 17
Nussloch 69226
GERMANY
Tel: 0080052700527 (toll free)
In-country Tel: +43 1 486 80 50 50
Email: support.at@leicabiosystems.com

België/Belgique:
Tel: 0080052700527 (toll free)
In-country Tel: +32 2 790 98 50
Email: support.be@leicabiosystems.com

Canada:
Tel: +1 844 534 2262 (toll free)
Direct International Tel: +1 760 539 1150
Email: TechServices@leicabiosystems.com

China:
17F, SML Center No. 610 Xu Jia Hui Road, Huangpu District
Shanghai, PRC PC:200025
CHINA
Tel: +86 4008208932
Fax: +86 21 6384 1389
Email: service.cn@leica-microsystems.com
Remote Care email: tac.cn@leica-microsystems.com

Danmark:
Tel: 0080052700527 (toll free)
In-country Tel: +45 44 54 01 01
Email: support.dk@leicabiosystems.com

Deutschland:
Leica Biosystems Nussloch GmbH
Technical Assistance Center
Heidelberger Strasse 17
Nussloch 69226
GERMANY
Tel: 0080052700527 (toll free)
In-country Tel: +49 6441 29 4555
Email: support.de@leicabiosystems.com

Eire:
Tel: 0080052700527 (toll free)
In-country Tel: +44 1908 577 650
Email: support.ie@leicabiosystems.com

España:
Tel: 0080052700527 (toll free)
In-country Tel: +34 902 119 094
Email: support.spain@leicabiosystems.com

France:
Tel: 0080052700527 (toll free)
In-country Tel: +33 811 000 664
Email: support.fr@leicabiosystems.com

Italia:
Tel: 0080052700527 (toll free)
In-country Tel: +39 0257 486 509
Email: support.italy@leicabiosystems.com

Japan:
1-29-9 Takadannobaba, Sinjuku-ku
Tokyo 169-0075
JAPAN

Nederland:
Tel: 0080052700527 (toll free)
In-country Tel: +31 70 413 21 00
Email: support.nl@leicabiosystems.com

New Zealand:
96 Ricketts Road
Mount Waverly, VIC 3149
AUSTRALIA
Tel: 0800 400 589 (toll free)
Between 8:30 AM-5 PM, Monday-Friday, AEST
Email: lbs-anz-service@leicabiosystems.com

Portugal:
Tel: 0080052700527 (toll free)
In-country Tel: +35 1 21 388 9112
Email: support.pt@leicabiosystems.com

The Russian Federation
BioLine LLC
Pinsky lane 3 letter A
Saint Petersburg 197101
THE RUSSIAN FEDERATION
Tel: 8-800-555-49-40 (toll free)
In-country Tel: +7 812 320 49 49
Email: main@bioline.ru

Sweden:
Tel: 0080052700527 (toll free)
In-country Tel: +46 8 625 45 45
Email: support.se@leicabiosystems.com

Switzerland:
Tel: 0080052700527 (toll free)
In-country Tel: +41 71 726 3434
Email: support.ch@leicabiosystems.com

United Kingdom:
Tel: 0080052700527 (toll free)
In-country Tel: +44 1908 577 650
Email: support.uk@leicabiosystems.com

USA:
Tel: +1 844 534 2262 (toll free)
Direct International Tel: +1 760 539 1150
Email: TechServices@leicabiosystems.com

Contents

1 Introduction

This chapter introduces the Aperio Scanner Administration Manager (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
Scanner Administration Manager (SAM) Server	The SAM server connects to multiple Aperio GT 450 scanners and runs the SAM Client Application Software.
SAM Client Application Software	The Scanner Administration Manager (SAM) client application software enables IT implementation, PIN configuration, and service access of multiple scanners from a single desktop client location for IT professionals.
Aperio Viewing Station	The viewing station includes monitor(s) and a workstation with Aperio ImageScope version 12.4 or higher.

The Aperio GT 450 system includes the Aperio Scanner Administration Manager (SAM) that enables IT implementation and service access of up to 4 scanners from a single desktop client location. SAM facilitates setup, configuration, and monitoring of each scanner. 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 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 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.

▸ Integration with Aperio eSlide Manager for image management, if desired. The interface can be configured to use SSL or another communication method.

▸ Services to process log data and events via Mirth Connect 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, refer to 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 Scanner Administration Manager (SAM) application to configure the Aperio GT 450 scanner(s), including how to add user accounts to 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 GT 450 scanners and the Scanner Administration Manager (SAM) server fit into your network	*"Aperio GT 450 Network Architecture" on page 13*
Learn how data flows between the Aperio GT 450 scanner, the SAM server, and image storage and optional Aperio eSlide Manager servers	*"Data Communication Pathways" on page 15*
Log in to the Scanner Administration Manager (SAM) client application software	*"Log Into SAM" on page 10*
Adjust configuration settings for DICOM (ImageServer) or DSR communication with the SAM server and scanner	*"Scanner Configuration Settings" on page 22*
Display information about a scanner on the system	*"Configuring the Aperio GT 450 Scanner" on page 18*
Check to see if a scanner is online	*"The SAM User Interface" on page 11*
Display the serial number, software version, or firmware version for a scanner on the system	*"Scanner System Information: Info Page" on page 20*
Review scanner statistics and history	*"Displaying Scanner Statistics" on page 29*
Review advanced configuration options such as camera settings	*"Displaying Scanner Information and Settings" on page 28*
Add a new user for Scanner Administration Manager (SAM) access or as a scanner operator	*"Adding, Editing, and Deleting Users" on page 31*

Task	See...
Delete a user account from SAM	*"Adding, Editing, and Deleting Users" on page 31*
Change the password for a user	*"Edit a User" on page 32*
Diagnose a problem by reviewing the event and error logs	*"Working With the Event Log" on page 29*
Check for updates to the software	*"Displaying Scanner Information and Settings" on page 28*
Review cybersecurity and network recommendations for the Aperio GT 450 system	*"Cybersecurity and Network Recommendations" on page 33*

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 scanner, refer to 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.

Aperio GT 450 System Components

The diagram below illustrates the components of a typical Aperio GT 450 scanner system, using a DSR server and Aperio eSlide Manager for image file management. Other configurations may be possible. Consult with your Leica Biosystems technical representative for more information.

Deploying the Aperio GT 450 System

The following diagram shows how the Aperio GT 450 system fits into the different departments of your organization.
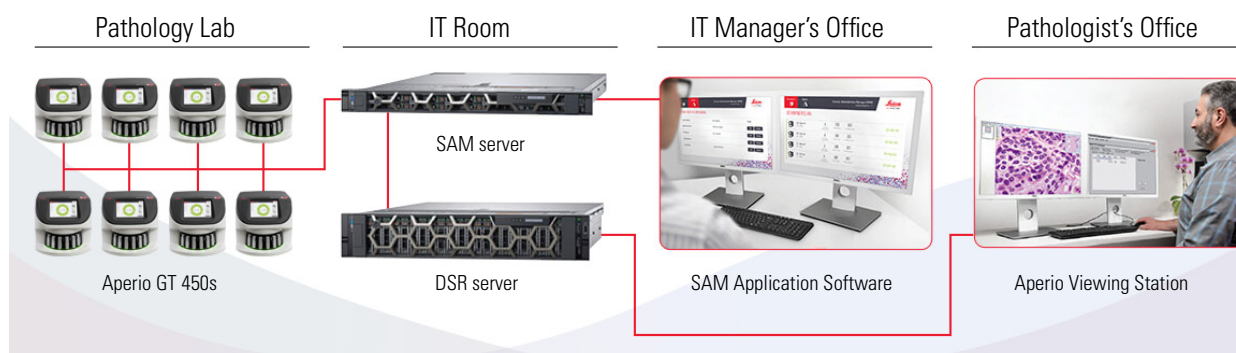
SAM Server
‣ Microsoft Windows Server software
‣ SAM software
‣ DICOM converter software
‣ Mirth Connect server software
‣ Storage for logs and events

DSR Server
‣ Microsoft Windows Server software
‣ Aperio eSlide Manager software
‣ Storage for image data

Aperio GT 450 Scanner

Pathology Lab	IT Room	IT Manager's Office	Pathologist's Office
Aperio GT 450s	SAM server / DSR server	SAM Application Software	Aperio Viewing Station

Log Into SAM

After the Aperio GT 450 system is installed and configured, the next step is to use the Scanner Administration Manager (SAM) to manage the Aperio GT 450 scanners and users.

1. Open an Internet browser and enter the address of the 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 SAM User Interface

The SAM home page with the scanner list is shown below. Note that users with the Operator role will not see the Configuration icons.

The four general areas of the page are described below.
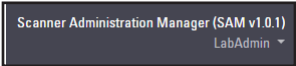

Scanner List

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.

ONLINE

ONLINE

OFFLINE

Scanner Status Area

This area displays the status of each scanner.

Scanner Administration Manager (SAM v1.0.1)
LabAdmin ▼

User Login

This displays the user name for the current SAM user.

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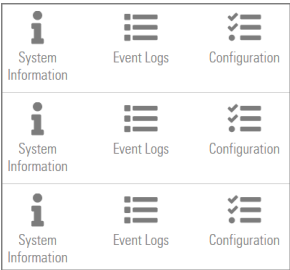
Commands Area

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

This chapter presents a basic architectural overview of how the Aperio GT 450 scanner and the 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 Aperio eSlide Manager, an LIS, and other networked systems.

The Aperio GT 450 system includes an Aperio GT 450 scanner, Aperio Scanner Administration Manager (SAM) server, cables, and plugs. Each instance of the SAM server can accommodate four Aperio GT 450 scanners and multiple SAM servers can exist on your network.

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

- ▶ SAM software for configuration of the scanner
- ▶ Web-based user interface for scanner administration and configuration
- ▶ Logging and messaging services for events and errors
- ▶ DICOM server to convert the DICOM image files to SVS and transfer them to the image storage system

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 Mirth Connect 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, SAM client application software, 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 (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 SAM server, the required minimum bandwidth is a gigabit ethernet with a speed equal to or greater than 1 gigabits per second (Gbps) For the connection between the 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 scanner and SAM system:

▶ **Aperio GT 450 scanner -** One or more Aperio GT 450 scanners can be connected to a SAM server through the network. Each SAM server can support multiple scanners.

▶ **Aperio Scanner Administration Manager (SAM) Server -** The SAM server contains the Scanner Administration Manager client application software, the subject of this guide. The SAM server provides the DICOM Image converter to convert DICOM images to SVS image file format. (Aperio GT 450 scanners stream encrypted DICOM images to the SAM server). SAM also manages scanner configuration settings, and manages messaging using Mirth connections.

▶ **Digital Slide Repository (DSR) Server -** This server (also known as an Image Storage System server) contains the whole slide images from the scanner and the infrastructure to manage them. The repository may be a network share available through a server on your network, or may reside on an optional Aperio eSlide Manager Server.

▶ **SAM Workstation/Console -** Accessed through a web browser (Firefox, Chrome, or Edge) on PC or laptop on your network, administrators and operators use the console 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.

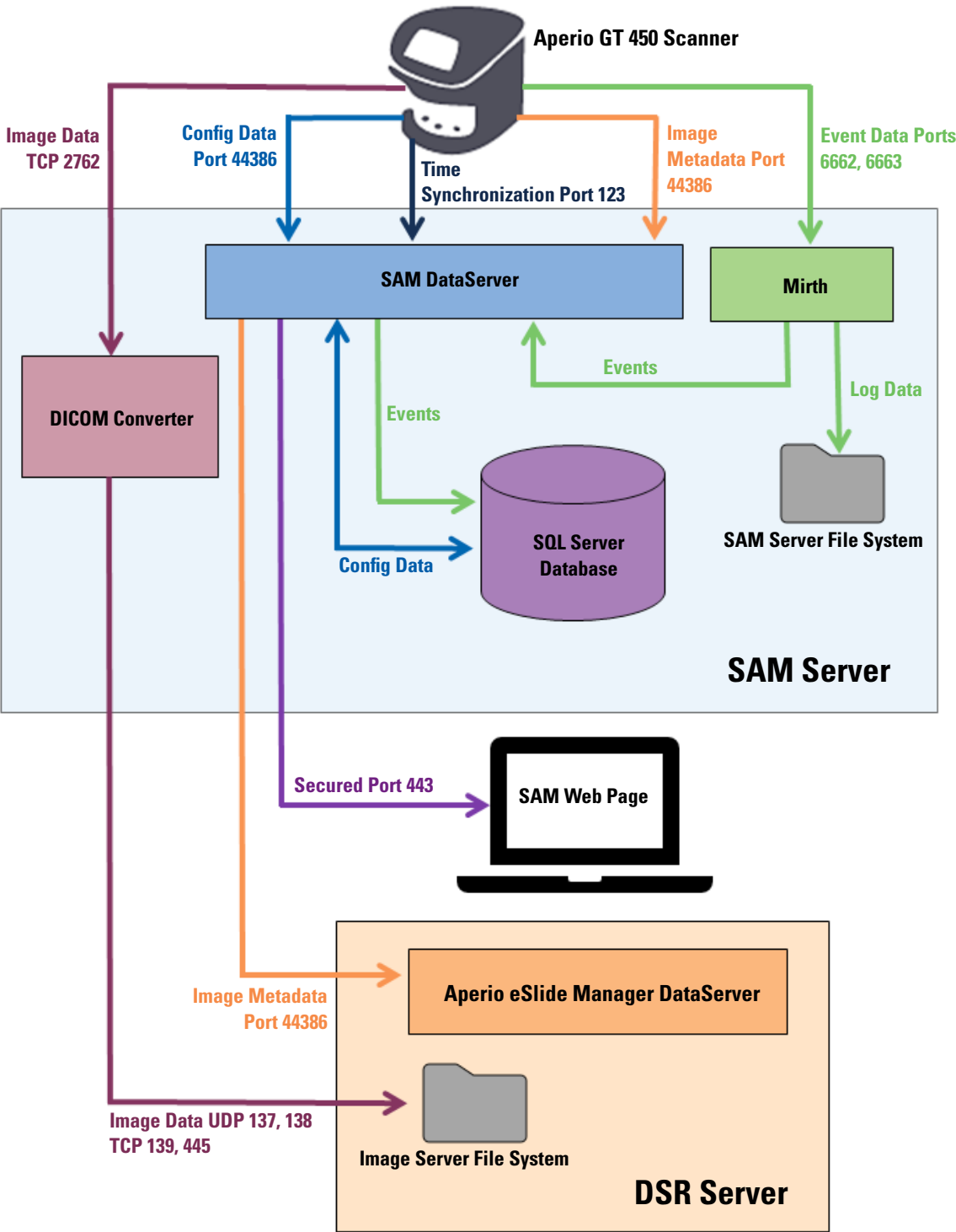▶ **Network File Share -** The location on your network where event logs are stored.

Secure Access

Access via the 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.

Data Communication Pathways

The various components reside on servers on the network. In general, multiple components may be installed on the same physical server, depending on your specific laboratory configuration.

The following diagram shows a standard, secure configuration for the Aperio GT 450 system connected to a SAM server and a DSR server that is running Aperio eSlide Manager. Other configurations may apply to your specific network and use case. This diagram is intended to be used to help you visualize the movement of images and the associated data.

Aperio GT 450 Scanner

**Image Data
TCP 2762**

**Config Data
Port 44386**

**Time
Synchronization Port 123**

**Image
Metadata Port
44386**

**Event Data Ports
6662, 6663**

SAM DataServer

Mirth

DICOM Converter

Events

Events

Log Data

**SQL Server
Database**

Config Data

SAM Server File System

SAM Server

Secured Port 443

SAM Web Page

**Image Metadata
Port 44386**

Aperio eSlide Manager DataServer

**Image Data UDP 137, 138
TCP 139, 445**

Image Server File System

DSR Server

Data Type	Description	Port
Image Data	The Scanner sends DICOM image data to the DICOM Converter. The data is sent using TLS encryption.	TCP 2762
	Configure the communication between the scanner and the DICOM converter using the Hostname and Port settings on the **Images** configuration page.	
	The DICOM Converter sends the image data (either as a converted SVS file, or as raw DICOM data) to the Image File System on the DSR Server. The data is sent using SMB3 Encryption.	UDP 137, 138
		TCP 139, 445
	Configure the communication between the DICOM converter and the DSR using the File Location setting on the **Images** page.	
Scanner Configuration Data	The scanner sends a call to the SAM DataServer to request configuration data. The SAM DataServer returns the configuration data to the scanner. The data is sent using TLS Encryption. Communication between the scanner and the SAM DataServer is configured on the scanner.	44386
	The SAM DataServer stores the configuration data on the SQL Server Database on the SAM Server.	
	The SAM DataServer displays the configuration data through the SAM web page.	
Time Synchronization	Timeclock synchronization between SAM and Multiple Scanners is maintained using network time protocol.	UDP 123
Image Metadata	The Scanner sends Image Metadata to the SAM DataServer. The data is sent using TLS encryption. Communication between the scanner and the SAM DataServer is configured on the scanner.	44386
	The SAM DataServer sends image metadata to the Aperio eSlide Manager DataServer located on the DSR. The data is sent using TLS encryption.	
	Configure the communication between the SAM DataServer and the scanner using the Hostname and Port settings on the **DSR** page.	
Messaging and Event Data	The scanner sends logs and event data to the Mirth Connect Server. No sensitive data is transferred.	6662, 6663
	Configure the communication between the scanner and the Mirth Connect Server on the **Event Handling** configuration page.	
	The Mirth Connect Server copies critical event and error data to the SAM DataServer then the SAM DataServer sends this data to the SQL database. This is the data reported out via the SAM Event Logs.	
	The SAM DataServer displays the event data through the SAM web page.	
	Mirth Connect Server processes the Log data and appends the Event Log, which resides on the file system. The communication between Mirth and the Event Log is configured within the Mirth Application setup. It is not accessible through SAM.	

"Scanner Configuration Settings" on page 22 provides information on how to configure the various connections between the components and services through the SAM interface.

3 Configuring the Aperio GT 450 Scanner

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 SAM, and how SAM, in turn, communicates with the various components on the network, including the Aperio eSlide Manager server, the DICOM Image converter, 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 cannot change them.
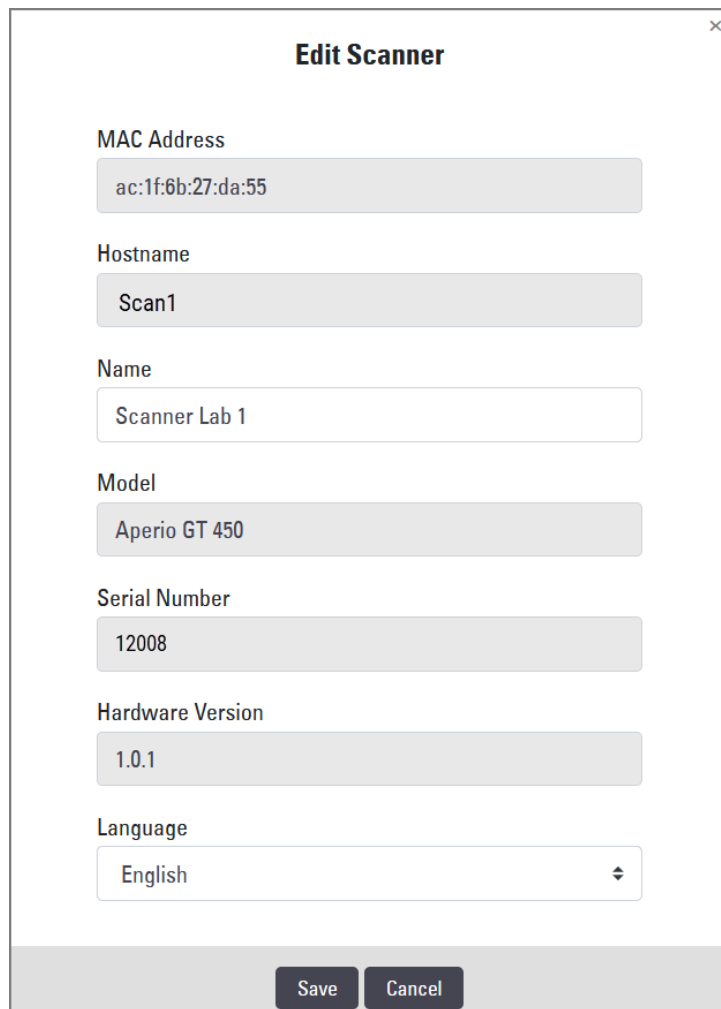
> *Some of the configuration settings define how the scanner communicates with SAM, such as the Mac Address and Hostname. The Serial Number uniquely identifies the scanner. Calibration settings define how the scanner operates. These settings can only be changed by Leica Support personnel, and are displayed 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

Each set of parameters is discussed in this chapter.

Basic Scanner Settings

Edit Scanner   ×

MAC Address

ac:1f:6b:27:da:55

Hostname

Scan1

Name

Scanner Lab 1

Model

Aperio GT 450

Serial Number

12008

Hardware Version

1.0.1

Language

English   ⇕

Save   Cancel

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 [edit icon] appears, then click the scanner name.

3. Customize the available settings as needed:

   ▶ Enter a **Name** to identify the scanner for your facility. (The name is shown on the main page.)

   ▶ Select a new language for the scanner control panel messages, if you wish.

   ▶ Refer to *"Appendix B: Scanner Information Settings and Configuration Options" on page 38* for additional information on each option.

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 Settings" on page 22*.

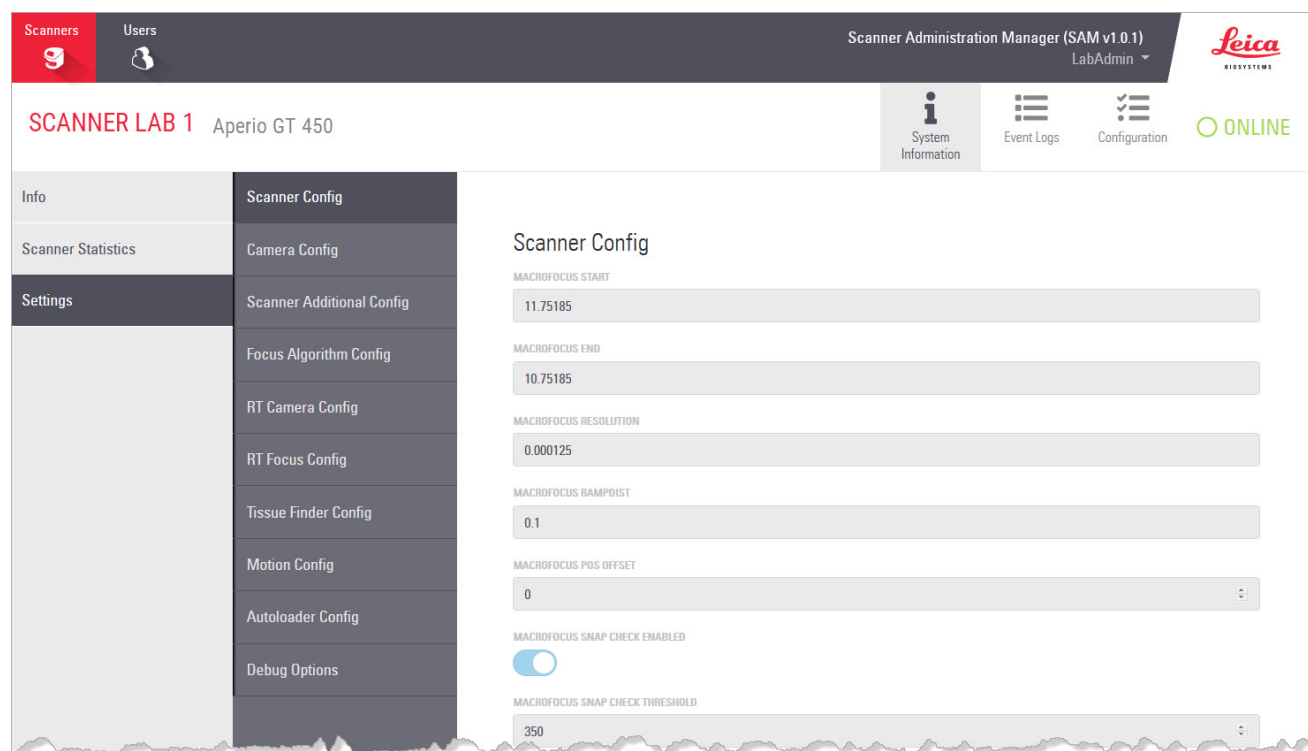## Scanner System Information: Info Page

To display the System Information 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 System Information Info page to review the scanner settings. (You cannot make changes on this page.)

The Firmware and Hardware versions are automatically updated once SAM establishes communication with the scanner.

Scanner System Information: Settings Page

The System Information Settings page displays 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 System Information 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 Settings

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 five Configuration pages, one each for Images (DICOM Converter), DSR, Event handling, PIN Management, and time zone settings.

▶ The **Images** settings control communication with the server that hosts the DICOM converter, as well as defining where the converted SVS image data is stored. For more information on this page, see *"Images Page" on page 24.*

▶ 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 (Mirth).

▶ The **PIN Management** settings allow you to create one or more PINs to be used to access the scanner. See *"PIN Management" on page 26* for more information.

▶ The **Time Zone** setting allows you to select the time zone for the scanner.

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. Enter the configuration settings for DICOM, DSR, and Event Handling.

   ▶ Click **Images**, **DSR**, **Event Handling**, or **Time Zone** in the side menu.

   ▶ Click **Edit** to make changes on the corresponding page. Note that you cannot make changes to settings in shaded fields.

4. Refer to *"PIN Management" on page 26* to add, delete, or modify PINs or change the timeout.

5. If you made changes, click **Save** to save the changes and return to viewing mode.

Refer to *"Appendix B: Scanner Information Settings and Configuration Options" on page 38* for additional information on each option.

Images Page

The **Images** page contains settings for:

▶ The location where the scanned images are sent (including server name and file location).

▶ The Title and Scan Scale Factor fields are for internal use. You should not change these unless directed to do so by Leica Biosystems Technical Support.

▶ The image file name format (see below).

▶ Barcode management (see below).

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

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 code ending 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

Barcode Management

The barcode is a text string saved with the scanned image file, and can be displayed in your eSlide management system.

Depending on your institution's procedures, you may have more than one barcode on the glass slide label. In this case, you will want to identify which barcode will be associated with the scanned image and displayed in the eSlide 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.)

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.

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.

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

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.

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

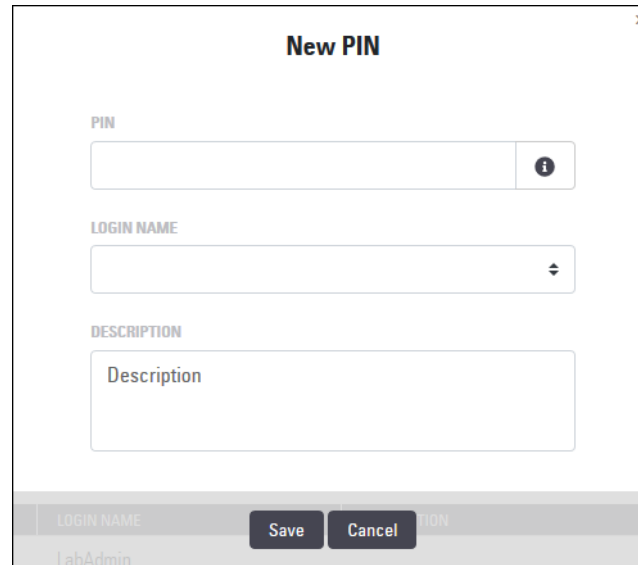Use this page to manage the list of valid PINs and adjust the PIN timeout for the scanner.

Console PIN Timeout (minutes)

| 10 | | Save |

New PIN +

PIN	LOGIN NAME	DESCRIPTION	TASKS
32116	BEdwards	Senior Histotech, Lab2	✏ ⊗
72451	LeeAlvarez	Histotech I, Lab 1	✏ ⊗
00000	Operator		✏ ⊗
12333	ScanAdmin		✏ ⊗

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.

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. You see the New PIN screen.

▶ 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 *"Chapter 5: User Management" on page 30.*)

▶ Optionally add a Description to identify the user who will be using this PIN.

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

4 Viewing System Information

This chapter explains how to display the various configuration options and settings of the 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 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 (Mirth 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 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 three 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 your Downloads folder that contains a set of diagnostic logs. User login events are contained in these logs.

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

5 User Management

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

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

Role	Description
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 • 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.

Adding, Editing, and Deleting 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 8 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**.

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 8 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

This chapter discusses how Aperio products protect electronic protected health information (EPHI) and provide protections against cybersecurity threats. We also discuss the measures you can take to protect client workstations and Aperio servers on your network. This chapter gives information for IT network administrators, Aperio product administrators, and Aperio product end users.

Many of the recommendations in this section apply to the Windows-based workstations that are used in conjunction with the Aperio scanners, and the servers used to host the Aperio applications and components, such as SAM. In these cases, 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.

Password, Login, and User Configuration Safeguards

▶ We recommend the following password complexity requirements:

- Passwords must be a minimum of eight characters, including:

  - At least one non-alpha numeric character (special character)

  - At least one numeric digit

  - At least one lower-case letter

- The last five passwords recently used may not be reused

- Users must change their passwords every 90 days

- Automatic 30 minute system lockout after five invalid login attempts. The operator may contact IT administration to reset the password before the 30 minute lockout expires.

▶ We recommend you configure client workstations 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 client workstations.

Physical Safeguards for Servers and Workstations

▶ We recommend you install and use a disk encryption utility to encrypt the data on client workstation hard disks to protect it.

▶ Be aware that workstations are susceptible to malware, viruses, data corruption and privacy breaches from

physical media such as CDs, DVDs, or USB drives. To reduce the risk of data corruption or unauthorized setting changes, only use physical media that are known to be free from viruses or malware.

▶ Protect the SAM server and client workstations from unauthorized access by limiting physical access to them.

Physical Safeguards for Aperio GT 450 Scanners

▶ Protect the Aperio GT 450 scanners from unauthorized access by limiting physical access to them.

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 server and client workstations from unauthorized access by using standard IT techniques. Examples include:

- Firewalls - We recommend enabling the Windows firewall on client workstations.

- Secure VPNs for remote access of the Aperio server by client workstations

- Whitelisting, an administrative tool that allows only authorized programs to run, should be implemented on Aperio servers and client workstations.

Protecting the DSR or Image Storage Server

Here are some recommendations for protecting the server where the scanned images are stored:

▶ 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 eSlides 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.

▶ 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 whitelisting on the server so that only authorized applications are allowed to run.

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

We also recommend that you configure the antivirus software to exclude .SVS, .SCN, .TIF, JPG 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 eSlides. Virus scans should be configured to run during non peak hours as they are very CPU intensive and can interfere with scanning. (In rare circumstances, third-party applications such as virus or security software may prevent Aperio software from connecting to servers or devices. If you are having this problem, contact Leica Biosystems Technical Services for assistance.)

▶ Periodically back up the hard disks on the server.

▶ For the 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.

A   Troubleshooting

This appendix provides causes and solutions for problems related to the 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, refer to the *Aperio GT 450 User's Guide*.

Scanner Administration Manager (SAM) Server Troubleshooting

Symptom	Cause	Solution
"Credentials are Invalid" error message during login	Instance of DataServer used by SAM is not running	Restart the DataServer service on the SAM server. See *"Restart the DataServer" on page 37.*
	Incorrect credentials	Check for caps lock, etc. Verify credentials with the Administrator
After update, new features are not available in the SAM User Interface	Application is cached in the browser	Exit SAM and then clear the browser cache
Scanner is on and connected to SAM (retrieves its settings) but SAM shows the scanner as offline and no statistical data is being reported (number of scans, etc.)	Mirth on the SAM server is not running	See *"Verify Mirth is Running" on page 37.*
	Ports are not open	Ensure port 6663 is open in the firewall and reachable by the scanner.

Symptom	Cause	Solution
Scanner log files are not appearing in the scanner logs folder	Mirth on the SAM server is not running	See *"Restart the DataServer" below..*
	Log output folder configured incorrectly	Check the Configuration Map tab under settings (AppLog_Dir).
	Mirth error	Check the Mirth Dashboard for any errors related to the "ScannerAppLogWriter" channel and refer to the Mirth error log for more details.
	Ports are not open	Ensure port 6663 is open in the firewall and reachable by the scanner.
The 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 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 Mirth is Running

On the server, ensure the Mirth Connect server is running. If it is running, ensure 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 Mirth Connect is reporting errors on "ScannerEventProcessor" channel, refer to the Mirth error logs for more details. If DataServer is not running this could lead to Mirth 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.

B Scanner Information Settings and Configuration Options

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.

Option	Description	View/Edit	
		Admin	Operator
Images Configuration			
Scan Scale Factor	Set by Leica Biosystems Technical Support	View/Edit	None
Hostname	Name of the server where the DICOM Image Converter resides. • Use **ScannerAdmin** if the DICOM Converter is installed on the SAM server. • Otherwise, use the hostname of the server that the DICOM Converter is installed on.	View/Edit	None
Port	The port that the DICOM Converter is configured to use at installation. The default is 2762.	View/Edit	None
Title	Set by Leica Biosystems Technical Support	View/Edit	None
File Location	The complete path to the file share where the converter will place the images after the conversion. This is a location on the network where converted SVS files are stored.	View/Edit	None
DSR Configuration			
Hostname	Hostname of the server where the metadata will be stored. (The "File Location" option, above, is the file share where the images are stored.)	View/Edit	None
Port	The secured port used for the DSR. The default is 44386.	View/Edit	None
Event Handling Configuration			
Hostname	Name of the server where the Mirth Connect Server resides. • Use **ScannerAdmin** if the Mirth Connect Server is installed on the SAM server. • Otherwise, use the hostname of the server where the Mirth instance used for SAM is installed.	View/Edit	None
Log Port	The port that Mirth is configured to use for log data at installation. The default is 6662	View/Edit	None
Event Port	The port that Mirth is configured to use for event data at installation. The default is 6663.	View/Edit	None

Option	Description	View/Edit	
		Admin	Operator
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. Valid value is any whole number greater than zero.	View/Edit	None
Edit Settings: PIN	A 5-digit code to unlock the scanner. Numbers only	View/Edit	None
Edit Settings: 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			
Scanner time zone	Set by SAM administrator.	View/Edit	None

Index

Symbols

‣ The following symbols may appear on your product label or in this user's guide:

[symbol]	Consult instructions for use
[symbol]	Manufacturer
[symbol]	Date of manufacture (year - month - day)
EC REP	European Union Authorized Representative
IVD	In vitro diagnostic device
SN	Serial number
REF	Catalog number
RH	Relative humidity range
[symbol]	Biological risks
[symbol]	Storage temperature range
[symbol]	Electronic and electrical equipment waste disposal
[symbol]	The exclamation point within an equilateral triangle is intended to alert you to the presence of important operating and maintenance (servicing) instructions. *Le point d'exclamation dans un triangle équilatéral vise à avertir l'utilisateur qu'il s'agit d'instructions d'utilisation et d'entretien importantes.*
[symbol]	Class I Laser