

APERIO GT 450 DX

DIGITAL PATHOLOGY SLIDE SCANNER

IT MANAGER AND LAB ADMINISTRATOR GUIDE



Advancing Cancer Diagnostics
Improving Lives

Aperio GT 450 DX IT Manager and Lab Administrator Guide

MAN-0507, Revision A | April 2024

This manual applies to Aperio GT 450 DX and Aperio GT 450 SAM DX Software version 1.2.


Copyright Notice


- Copyright © Leica Biosystems Imaging, Inc. 2024. All Rights Reserved. LEICA and the Leica logo are registered trademarks of Leica Microsystems IR GmbH. Aperio, GT, and GT 450 are trademarks of Leica Biosystems Imaging, Inc. in the USA and optionally in other countries. Other logos, products, 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 [LeicaBiosystems.com/Aperio](https://www.leicabiosystems.com/Aperio).

Contact Information – Leica Biosystems Imaging, Inc.

Headquarters	Customer Support
 <p>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</p>	<p>Contact your local support representative with any query and service request.</p> <p>https://www.leicabiosystems.com/contact-us/</p>

IVD 

UDI 815477020525, 815477020518

REF 23GT450DXUS, 23SAMSWDXUS

Table of contents

Notices	6
Revision Record	6
Cautions and Notes	6
Intended Use	8
Symbols	9
1 Introduction	11
About this guide	13
Related documents	14
Log into SAM DX	14
The SAM DX user interface	15
2 Aperio GT 450 DX network architecture	17
Aperio GT 450 DX architecture	18
Image types supported	18
General information	18
Network bandwidth requirements	19
How the Aperio GT 450 DX fits into your network	19
Secure access	19
Aperio GT 450 DX recommended network configuration	20
3 Configuring the Aperio GT 450 DX	23
General instructions	24
Basic scanner settings	25
Scanner system information: Info page	26
Scanner system information: Settings page	27
Scanner configuration settings	28
Images page	30
Image file name format	31
Barcode management	31
PIN management	32
Configuring a PIN and timeout	32
Enabling DICOM image output	33
4 Viewing system information	37
Displaying scanner information and settings	38

Displaying scanner statistics	39
Working with the Event Log	39
Back up log files	39
Login alerts	40
5 User management	41
Understanding roles	42
Managing users	43
Add a user	43
Edit a user	44
Delete a user	44
Unlock a user account	44
Changing your user password	45
6 Cybersecurity and network recommendations	46
Aperio GT 450 DX and SAM DX cybersecurity features	47
Data protection	48
Data Backup	48
Physical safeguards for Aperio GT 450 DX	48
Protecting the Aperio SAM DX server	48
Password, login, and user configuration safeguards	49
Physical safeguards for the SAM DX server	49
SAM DX server administrative safeguards	49
Require SMB encryption with Windows Admin Center	50
Additional security controls	51
Recommended registry settings to secure Windows Server 2019 and Windows Server 2022	52
Use of off-the-shelf software	55
Support and cybersecurity patches	55
A Troubleshooting	56
Scanner Administration Manager DX (SAM DX) server troubleshooting	57
Restart the DataServer	58
Verify Mirth is running	58
IIS configuration error	58
Scanner network troubleshooting	59

B	Summary of scanner setting and configuration options	61
	Basic scanner information	62
	Scanner configuration	62
C	Binding an SSL certificate to Aperio SAM DX	65
	Assign the SSL certificate to your website	66
	Bind the SSL certificate	67
	Index	70

Notices

Revision Record

Rev.	Issued	Sections Affected	Detail
A	April 2024	All	New manual for Aperio GT 450 DX 1.2.

Cautions and Notes

- **Serious Incidents Reporting** – Any serious incident that has occurred in relation to the Aperio GT 450 DX shall be reported to the manufacturer and the competent authority of the member state in which the user and/or the patient is established.
- **Specifications and Performance** – For device specifications and performance characteristics, see the document *Aperio GT 450 DX Specifications*.
- **Installation** – Aperio GT 450 DX 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 DX 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 DX User's Guide*.
- **Maintenance and Troubleshooting** – For information on maintenance and troubleshooting, see the *Aperio GT 450 DX 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 of 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 DX 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 DX User’s Guide*.

Intended Use

The Aperio GT 450 DX is an automated digital slide creation and viewing system. The Aperio GT 450 DX is intended for in vitro diagnostic use as an aid to the pathologist to review and interpret digital images of surgical pathology slides prepared from formalin-fixed paraffin embedded (FFPE) tissue. The Aperio GT 450 DX is for creation and viewing of digital images of scanned glass slides that would otherwise be appropriate for manual visualization by conventional light microscopy.

Aperio GT 450 DX is comprised of the Aperio GT 450 DX scanner, which generates images in the Digital Imaging and Communications in Medicine (DICOM) and in the ScanScope Virtual Slide (SVS) file formats, the Aperio WebViewer DX viewer, and the displays. The Aperio GT 450 DX is intended to be used with the interoperable components specified in Table 1.














Table 1: Interoperable components of Aperio GT 450 DX

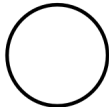



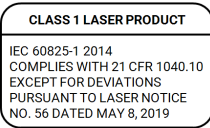
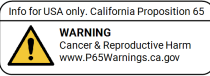

Scanner Hardware	Scanner Output file format	Interoperable Viewing Software	Interoperable Displays
Aperio GT 450 DX	SVS	Aperio WebViewer DX	Barco MDPC-8127 Dell UP3017 Dell U3023E Dell U3223QE
Aperio GT 450 DX	SVS	Sectra Digital Pathology Module (3.3)	Dell U3223QE
Aperio GT 450 DX	DICOM	Sectra Digital Pathology Module (3.3)	Dell U3223QE

The Aperio GT 450 DX is not intended for use with frozen section, cytology, or non-FFPE hematopathology specimens. It is the responsibility of a qualified pathologist to employ appropriate procedures and safeguards to assure the validity of the interpretation of images obtained using the Aperio GT 450 DX.

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 - 5.1.7	Serial number
	ISO 15223-1 - 5.5.1	In Vitro Diagnostic medical device
	ISO 15223-1 - 5.1.6	Catalog number
	21 CFR 809.10(a)(4)	Requires prescription in the United States.
	ISO 15223-1 - 5.7.10	Unique Device Identifier
	ISO 15223-1 - 5.4.4	Caution
	SO 7010 - W001	General warning
	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.

Symbol	Regulation/Standard	Description
	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
	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.
	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:

About this guide	13
Related documents	14
Log into SAM DX	14
The SAM DX user interface	15

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

The Aperio GT 450 DX 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 DX was designed to fit into your network environment and offer the best in security and performance.

The Aperio GT 450 DX is intended for use by trained clinical pathology histotechnicians, while the Aperio GT 450 DX SAM DX software is intended for use by IT professionals and laboratory administrators.

The Aperio GT 450 DX is intended for use in medium- to high-volume clinical pathology laboratories that support the pathology services of a hospital, reference laboratory or other clinical facility.

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 DX User's Guide*.

Component	Description
Scanner Administration Manager DX (SAM DX) Server	The SAM DX Client Application Software resides on a server, which is referred to in this document as the SAM DX server. The SAM DX server connects to multiple Aperio GT 450 DX scanners.
Aperio GT 450 SAM DX Client Application Software	The SAM DX 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 SAM DX server to use SAM DX to manage the Aperio GT 450 DX scanners.

The Aperio GT 450 DX includes the Scanner Administration Manager DX (SAM DX) that enables IT implementation and service access of multiple scanners from a single desktop client location. SAM DX facilitates setup, configuration, and monitoring of each scanner. SAM DX 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 DX 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 DX 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 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 DX on their facility network. For general information on how to use the scanner, see the *Aperio GT 450 DX User's Guide*.

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

Chapters that follow discuss using the SAM DX application to configure the Aperio GT 450 DX scanner(s), including how to add user accounts to SAM DX, 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 DX scanners and the SAM DX server fit into your network	Aperio GT 450 DX network architecture (on page 17)
Learn how data flows between the Aperio GT 450 DX, the SAM DX server, and optional image and data management servers.	Aperio GT 450 DX recommended network configuration (on page 20)
Log in to the SAM DX client application software	Log into SAM DX (on page 14)
Adjust configuration settings for DICOM or DSR communication with the SAM DX server and scanner	Scanner configuration settings (on page 28)
Display information about a scanner on the system	Configuring the Aperio GT 450 DX (on page 23)
Check to see if a scanner is online	The SAM DX user interface (on page 15)
Display the serial number, software version, or firmware version for a scanner on the system	Scanner system information: Info page (on page 26)
Review scanner statistics and history	Displaying scanner statistics (on page 39)
Review advanced configuration options such as camera settings	Displaying scanner information and settings (on page 38)
Add a new user for SAM DX	Add a user (on page 43)
Delete a user account from SAM DX	Delete a user (on page 44)
Change the password for a user	Changing your user password (on page 45)
Unlock a locked user account	Unlock a user account (on page 44)
Diagnose a problem by reviewing the event and error logs	Working with the Event Log (on page 39)

Task	See...
Check for updates to the software	Displaying scanner information and settings (on page 38)
Review cybersecurity and network recommendations for the Aperio GT 450 DX	Cybersecurity and network recommendations (on page 46)

Related documents

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

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

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

Log into SAM DX

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

- 1 Open an Internet browser and enter the address of the SAM DX 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 DX user interface

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

Scanner Name	Model	System Information	Event Logs	Configuration	Status
Scanner Lab 1	Aperio GT 450 DX	System Information	Event Logs	Configuration	ONLINE
Scanner Lab 2	Aperio GT 450 DX	System Information	Event Logs	Configuration	ONLINE
PathLab 1	Aperio GT 450 DX	System Information	Event Logs	Configuration	OFFLINE
PathLab 2	Aperio GT 450 DX	System Information	Event Logs	Configuration	OFFLINE

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.

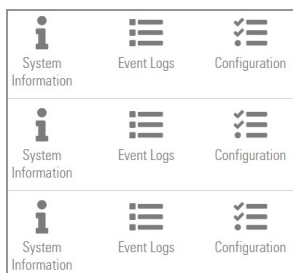
Scanner Status Area

This area displays the status of each scanner.

User Login

This displays the user name for the current SAM DX 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 DX network architecture

In this section:

Aperio GT 450 DX architecture	18
Image types supported	18
General information	18
Network bandwidth requirements	19
How the Aperio GT 450 DX fits into your network	19
Secure access	19
Aperio GT 450 DX recommended network configuration	20

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



IT network failure may lead to delay in diagnosis/prognosis until the network is restored.

Aperio GT 450 DX architecture

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

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

- SAM DX 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 SAM DX Client Application Software.

Image types supported

The Aperio GT 450 DX 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 DX DICOM Conformance Statement*. Also, a Leica Biosystems Technical Services representative will need to log into SAM DX as a Leica Admin and enable **Optional Features** for the scanner you want to configure for DICOM. See [Enabling DICOM image output \(on page 33\)](#) for details.

General information

The following guidelines apply:

- The network share where images are stored (DSR) can exist on the same server as IDMS, 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 DX scanners, SAM DX client application software, and the SAM DX server, 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 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 DX and the SAM DX 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 SAM DX server and the image repository (DSR), the required minimum bandwidth is 10 gigabits per second.

How the Aperio GT 450 DX fits into your network

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

- **Aperio GT 450 DX** – One or more Aperio GT 450 DX scanners can be connected to a SAM DX server through the network. Each SAM DX 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.
- **SAM DX Client Application Software** – Accessed through a web browser (Firefox, Chrome, or Edge) on PC or laptop on your network, administrators and operators use the SAM DX 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 SAM DX 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.

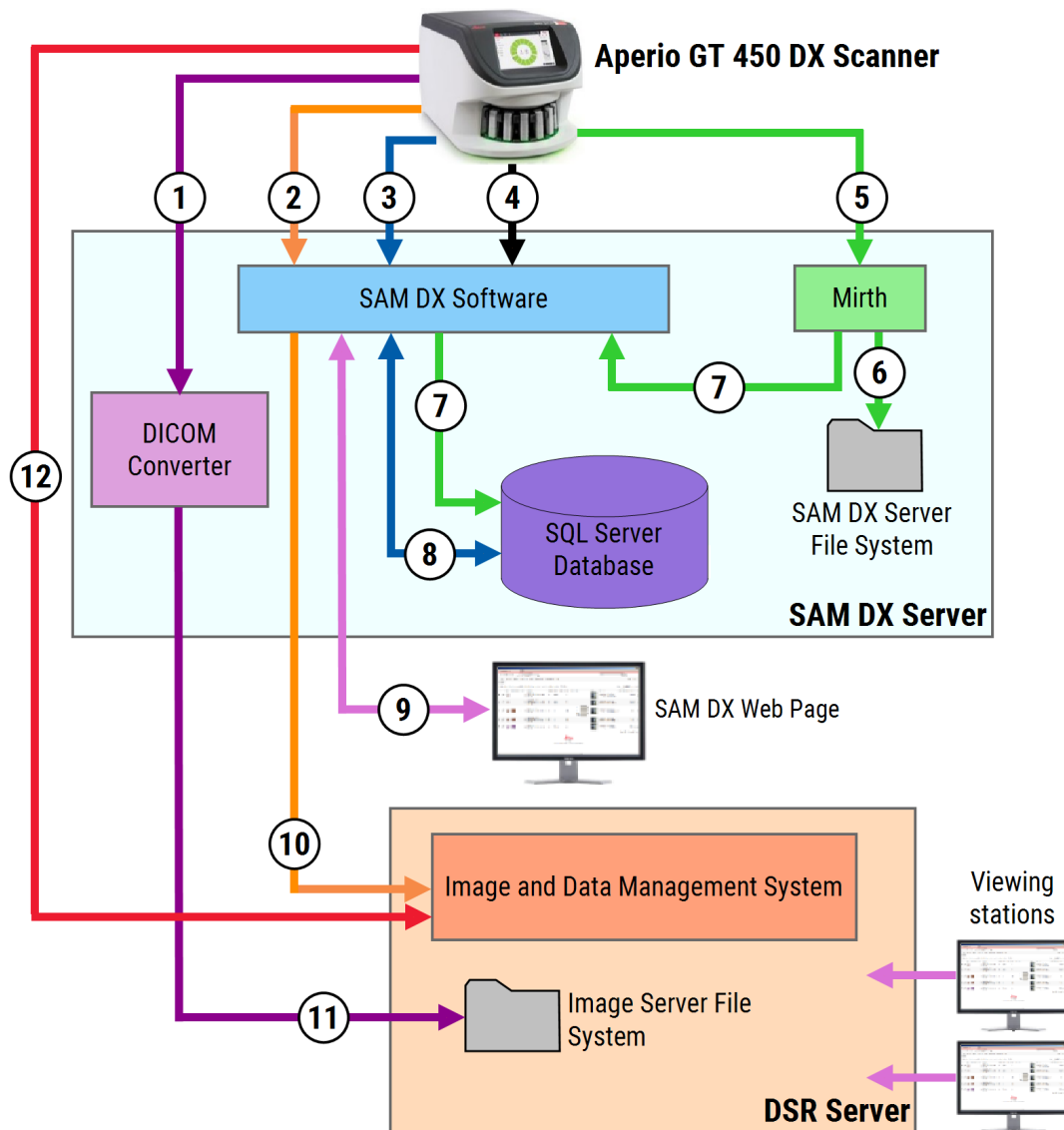


To protect your network from cybersecurity attacks, we recommend that you disable unused ports and services on your network.

Aperio GT 450 DX recommended network configuration

This section describes the recommended way to connect your Aperio GT 450 DX in your IT environment for optimal performance.

Figure 2-1: Recommended network configuration



Legend

1	Image Data, TCP 2762, TLS	7	Events, HTTPS 44386, TLS
2	Image metadata, Port 44386, HTTPS	8	Configuration data
3	Configuration data, Port 44386, HTTPS	9	WebApp, HTTPS 443
4	Time synchronization, Port 123	10	Image metadata, HTTPS 44386
5	Event logs; Ports 6662, 6663	11	Image data; SMB3 (uses UDP 137, 138; TCP 139, 445)
6	Log Data	12	Image data; TCP 2762 (stunnel optional)

Data Type	Description	Port
Image Data	By default, the Scanner sends DICOM image data to the DICOM converter. The data is sent using TLS encryption. Configure the communication between the scanner and the DICOM converter using the Hostname and Port settings on the Images configuration page.	TCP 2762
	By default, the DICOM converter sends the image data (either as a converted SVS file, or as raw DICOM data) to the image and data management system (IDMS) on the DSR Server. The data is sent using SMB3 Encryption. Configure the communication between the DICOM converter and the DSR using the File Location setting on the Images page.	UDP 137, 138 TCP 139, 445
	Alternatively, the scanner may send image data to the Sectra module, bypassing the DICOM Converter. This option is only available when using the Sectra Digital Pathology Module. This connection is not encrypted by default. To secure this connection, you can configure stunnel to create a secure communication tunnel between Sectra and the scanner. DICOM C-Store communication between the scanner and Sectra is configured on SAM DX.	TCP 2762-SSL (default) 47823 (stunnel default)
	Images can be sent to viewing stations connected to the DSR.	HTTP(S) 80/443
Scanner Configuration Data	The scanner sends a call to the SAM DX DataServer to request configuration data. The SAM DX DataServer returns the configuration data to the scanner. The data is sent using TLS Encryption. Communication between the scanner and the SAM DX DataServer is configured on the scanner.	HTTPS 44386
	The SAM DX software stores the configuration data on the SQL Server Database on the SAM DX Server.	TCP 1433
	The SAM DX DataServer displays the configuration data through the SAM DX web page.	HTTP(S) 80/443

Data Type	Description	Port
Time Synchronization	Timeclock synchronization between SAM DX and multiple scanners is maintained using network time protocol.	UDP 123
Image Metadata	<p>When using Aperio eSlide Manager: The Scanner sends Image Metadata to the SAM DX DataServer using TLS encryption. Communication between the scanner and the SAM DX DataServer is configured on SAM DX. The SAM DX DataServer sends image metadata to the IDMS location on the DSR. Configure the communication between SAM DX DataServer using the Hostname and Port settings on the SAM DX DSR page.</p> <p>When using Sectra Digital Pathology Module: Image Metadata is embedded directly in the DICOM images that are sent to the Sectra module.</p>	HTTPS 44386
Log and Event Data	<p>The scanner sends logs and event data to the Mirth Connect Server. No sensitive data is transferred.</p> <p>Configure the communication between the scanner and the Mirth Connect Server on the Event Handling configuration page.</p>	<p>The Mirth Connect Server copies critical event and error data to the SAM DX DataServer, and then the SAM DX DataServer sends this data to the SQL database. This is the data reported out via the SAM DX Event Logs.</p> <p>The SAM DX DataServer displays the event data through the SAM DX web page.</p> <p>The 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 DX.</p>
		TCP 6662, 6663
		HTTPS 44386
		HTTP(S) 80/443

[Scanner configuration settings \(on page 28\)](#) provides information on how to configure the various connections between the components and services through the SAM DX interface.

3

Configuring the Aperio GT 450 DX

In this section:

General instructions	24
Scanner configuration settings	28
Images page	30
Enabling DICOM image output	33

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 DX, and how SAM DX, in turn, communicates with the various components on the network, including the IDMS 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.



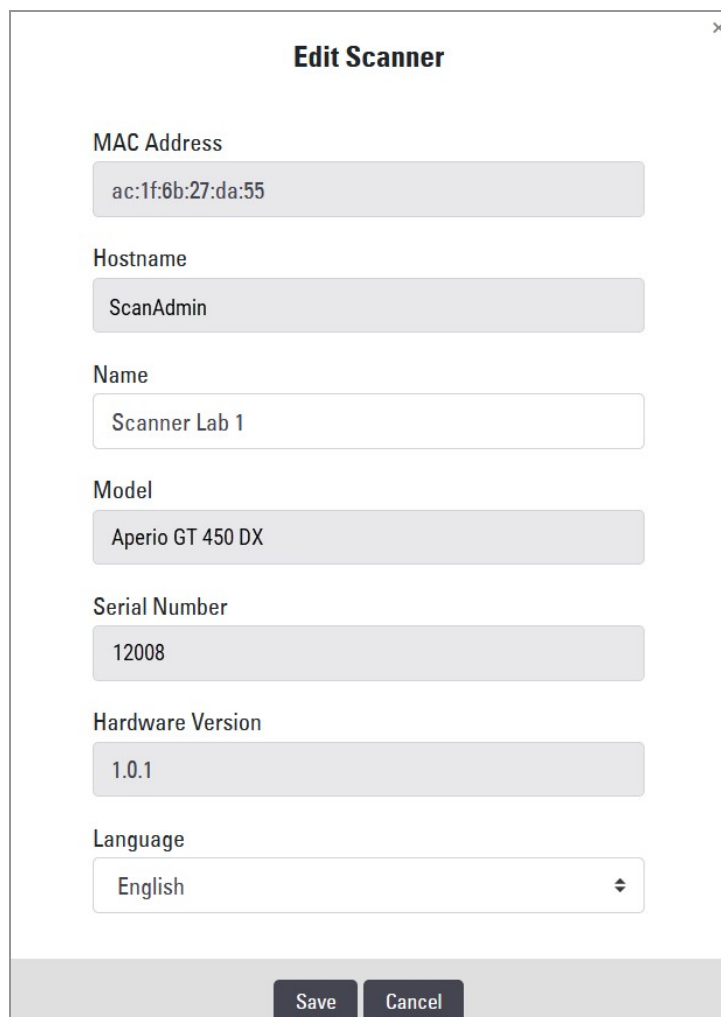
Some of the configuration settings define how the scanner communicates with SAM DX, such as the **MAC Address** and **Hostname**. The **Serial Number** uniquely identifies the scanner. Calibration settings define how the scanner operates. These settings can only be changed by Leica Support personnel,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




The screenshot shows a dialog box titled "Edit Scanner" with a close button (X) in the top right corner. The dialog contains several input fields and a dropdown menu, each with a label above it:

- MAC Address:** ac:1f:6b:27:da:55
- Hostname:** ScanAdmin
- Name:** Scanner Lab 1
- Model:** Aperio GT 450 DX
- Serial Number:** 12008
- Hardware Version:** 1.0.1
- Language:** English (with a dropdown arrow)

At the bottom of the dialog, there are two buttons: "Save" and "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  appears, then click the scanner name.
- 3 Customize the available settings as needed:
 - Enter a Friendly Name to identify the scanner for your facility. (The friendly 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 \(on page 61\)](#).
- 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 \(on page 28\)](#).

Scanner system information: Info page

The screenshot shows the SAM - Scanner Administration Manager interface. The top banner includes 'Scanners' and 'Users' tabs, the SAM version 'SAM - Scanner Administration Manager 00815477020389(8012)1.1', and the user 'LeicaAdmin'. The main header for scanner 'SS45054 GT 450 DX' features icons for 'System Information', 'Event Logs', and 'Configuration', along with an 'ONLINE' status indicator. A left sidebar contains 'Info', 'Scanner Statistics', and 'Settings' sections. The 'Info' section is active, displaying a table of system information. An 'Advanced Maintenance' button is visible in the top right of the content area.

Serial Number	SS45054
Hardware Version	1.0.1
Controller UDI	00815477020372(8012)1.1
Console UDI	00815477020365(8012)1.1
Controller Version	1.1.0.5072 [C]
Console Version	1.1.0.5017 [C]
STU Remote Version	1.1.0.5050 [C]
Documents Version	1.1.0.5017 [C]
G5 Firmware Version	1.1.0.5069 [C]
Platform Version	5.4
Install Date	Thu May 06 2021
GT 450 DX Update News	www.leicabiosystems.com

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 DX establishes communication with the scanner.

Scanner system information: Settings page

The screenshot shows the SAM - Scanner Administration Manager (SAM v1.0.0-pred.5020) interface. The top banner includes 'Scanners' and 'Users' tabs, and the 'Scanners' tab is active. The main header displays 'SCANNER LAB 1 Aperio GT 450 DX'. On the right, there are icons for 'System Information', 'Event Logs', and 'Configuration', along with an 'ONLINE' status indicator. The left sidebar menu has 'Settings' selected. The main content area is titled 'Scanner Config' and lists several settings:

- MACROFOCUS START: 1175105
- MACROFOCUS END: 1075185
- MACROFOCUS RESOLUTION: 0.000125
- MACROFOCUS RAMPOIST: 0.1
- MACROFOCUS POS OFFSET: 0
- MACROFOCUS SNAP CHECK ENABLED:
- MACROFOCUS SNAP CHECK THRESHOLD: 350

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 screenshot displays the SAM web interface for configuring the DICOM image host. The top navigation bar includes 'Scanners' and 'Users' tabs, the system name 'PATHLAB 1 Aperio GT 450 DX', and a 'Configuration' menu. The left sidebar lists various configuration categories, with 'Images' selected. The main configuration area is titled 'Configure settings for the DICOM image host' and includes an 'Edit' button. The settings are as follows:

Setting	Value
SCAN SCALE FACTOR	1
HOSTNAME	ScannerAdmin
PORT	2762
TITLE	SVS_STORE_SCP
FILE LOCATION	\\us:cavs-eng-fs1\eng-share\Image_Quality\ss12011\RMA_TS
IMAGE FILENAME FORMAT	
BARCODE VALUE IDENTIFIER	
BARCODE VALUE MODIFIER	
BARCODE VALUE SUBSTITUTION FORMAT	
REQUIRE BARCODE ID	<input type="checkbox"/>

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 (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. You can also configure other items. For more information on this page, see [Images page \(on page 30\)](#).

- 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). For information on event logs, see [Working with the Event Log \(on page 39\)](#).
- The **PIN Management** settings allow you to create one or more PINs to be used to access the scanner. See [PIN management \(on page 32\)](#) 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 Images (DICOM), DSR, and Event Handling.
 - Click **Images**, **DSR**, **Event Handling**, or **Time Zone** in the side menu bar.
 - Click **Edit** to make changes on the corresponding page. Note that you cannot make changes to settings in shaded fields.
 - For details on how to add, delete, or modify PINs or change the timeout, see [PIN management \(on page 32\)](#).
- 4 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 \(on page 61\)](#).

Images page

Scanners Users SAM - Scanner Administration Manager (SAM v1.0.1-prod.6005) LeicaAdmin Leica BIOSYSTEMS

PATHLAB 1 Aperio GT 450 DX System Information Event Logs Configuration ONLINE

Images

Configure settings for the DICOM image host Edit

SCAN SCALE FACTOR
1

HOSTNAME
ScannerAdmin

PORT
2762

TITLE
SVS_STORE_SCP

FILE LOCATION
\\uscavs-eng-fs1\eng-share\Image_Quality\ss12011\IRMA_TS

IMAGE FILENAME FORMAT
 ⓘ

BARCODE VALUE IDENTIFIER
 ⓘ

BARCODE VALUE MODIFIER
 ⓘ

BARCODE VALUE SUBSTITUTION FORMAT
 ⓘ

REQUIRE BARCODE ID

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)
- DICOM image settings (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, and 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
```

Barcode management

The barcode is a text string saved with the scanned image file, and can be displayed in your digital slide 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 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.)

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 DX, 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

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 [Add a user \(on page 43\)](#).)
- Optionally add a Description to identify the user who will be using this PIN.
- Click **Save** to return to the list of PINs.

Enabling DICOM image output

The Aperio GT 450 DX has the ability to 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 DX scanner. You must use SAM DX to configure the final storage location for the DICOM images (PACS, IMS, or file share).

Third-party developers retrieve the DICOM images and meta data by accessing the DICOM image file share defined in SAM DX or by using the C-Store protocol. For details on DICOM images and their meta data 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 DX DICOM Conformance Statement*. Also, a Leica Biosystems Technical Services representative will need to log into SAM DX 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 SAM DX as a lab admin.

- 1 Confirm that the Scanners icon in the banner is selected and the page shows the list of scanners.

The screenshot displays the Scanner Administration Manager (SAM) interface. The top navigation bar includes 'Scanners' (selected) and 'Users'. The main content area is titled 'SCANNERS (4)' and lists four scanners:

Scanner Name	Model	System Information	Event Logs	Configuration	Status
Scanner Lab 1	Aperio GT 450 DX	System Information	Event Logs	Configuration	ONLINE
Scanner Lab 2	Aperio GT 450 DX	System Information	Event Logs	Configuration	ONLINE
PathLab 1	Aperio GT 450 DX	System Information	Event Logs	Configuration	OFFLINE
PathLab 2	Aperio GT 450 DX	System Information	Event Logs	Configuration	OFFLINE

- 2 Hover over the name of the scanner you want to configure for DICOM until the **Edit** symbol appears, then click the scanner name.

- Click **Images** in the left-hand pane.

Configure settings for the DICOM image host Edit

HOSTNAME
scanneradmin

PORT
2762

TITLE
SVS_STORE_SCP

FILE LOCATION
\\uscavs-esmmfg\Images\PreBeta6

IMAGE FILENAME FORMAT
{IMAGEID}-{BARCODEID} ⓘ

BARCODE VALUE IDENTIFIER
\d{6} ⓘ

BARCODE VALUE MODIFIER
[(.*)&S ⓘ

BARCODE VALUE SUBSTITUTION FORMAT
\$1&S ⓘ

IMAGE OUTPUT FORMAT
DICOM ▾

SLIDE ID FORMAT
(\d{23})\d{23} ⓘ

CASE ID FORMAT
\d{23}\d{23} ⓘ

DIMENSION ORGANIZATION TYPE
Full ▾ ⓘ

REQUIRE BARCODE ID

- In the **Image Location** box, type the file share where the images will be output.
- In the section labeled **Image Output Format**, select **DICOM**.
- In the **Slide ID Format** box, type the Slide ID format as a regular expression.



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.

- In the **Case ID Format** box, type the Case ID format as a regular expression.

- e 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.

When using a scanner that has been configured to output DICOM images, the Console will show "(DICOM)" at the top of the Console page:

Aperio GT 450 DX (DICOM)

4

Viewing system information

In this section:

Displaying scanner information and settings	38
Displaying scanner statistics	39
Working with the Event Log	39

This chapter explains how to display the various configuration options and settings of the SAM DX 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 (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 DX 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.

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 SAM DX server Downloads folder.



To use the **Download All Logs** button, your workstation must be connected to your institution's Local Area Network with access to the SAM DX server; you cannot access the SAM DX 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 SAM DX server and storing the backups offsite. We also recommend backing up Windows Event logs on the SAM DX 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:

Understanding roles	42
Managing users	43

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

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

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.

Understanding roles

There are three user roles:

- Operator Role
- Lab Admin Role
- Leica Support Role

Role	Description
Operator Role	<p>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:</p> <ul style="list-style-type: none"> • View the status of each scanner • View System Information for each scanner <ul style="list-style-type: none"> • Info page • Scanner Statistics • Settings page • View the Event Log • Change his or her own password <p>Operators cannot view or change the PINs assigned to a scanner.</p> <p>Operators cannot view the list of users, and cannot change settings for other users.</p>
Lab Admin Role	<p>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:</p> <ul style="list-style-type: none"> • Add, modify, and delete other user accounts • Change user passwords • View System Information and edit some of the settings

Role	Description
	<ul style="list-style-type: none"> • Edit the Configuration settings: <ul style="list-style-type: none"> • Images • DSR • Event Handling • PIN Management
Leica Support Role	<p>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.</p> <p>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.</p>

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 SAM DX server, SAM DX 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:

Aperio GT 450 DX and SAM DX cybersecurity features	47
Data protection	48
Physical safeguards for Aperio GT 450 DX	48
Protecting the Aperio SAM DX server	48
Use of off-the-shelf software	55
Support and cybersecurity patches	55

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

The recommendations in this section apply to the Windows-based server used to host SAM DX. 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 DX product, the Leica Biosystems representative will turn over to your IT staff sensitive cybersecurity items such as SSL certificate credentials, SAM DX 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 DX and SAM DX cybersecurity features

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

- To reduce cybersecurity vulnerability, the respective operating systems on the Aperio GT 450 DX VPU and SAM DX software are hardened with CIS (Center for Internet Security) benchmarks.
- The Aperio GT 450 DX scanner and SAM DX 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 DX scanner and the SAM DX 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 DX scanner and recommended for use on the SAM DX server. This prevents unauthorized software from running on these components.
- The daily maintenance for the Aperio GT 450 DX scanner includes rebooting it every day. (See the *Aperio GT 450 DX User's Guide* for details.) This refreshes the firmware and updates allow/deny listings.
- The Aperio GT 450 DX 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 \(on page 39\)](#).

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 Private 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 also protected by encryption. All sensitive information is transmitted between the scanner and 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 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 DX DataServer database which can be a part of your overall backup plan.

The Aperio GT 450 DX 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 \(on page 39\)](#)

Physical safeguards for Aperio GT 450 DX

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

Protecting the Aperio SAM DX server

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

Password, login, and user configuration safeguards

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

Physical safeguards for the SAM DX server

- Protect the SAM DX server and client workstations used to log into SAM DX from unauthorized access by limiting physical access to them.
- To protect the SAM DX 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.

SAM DX 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 SAM DX server, the user roles are "Operator" and "Lab Admin," which have different permissions.
- Protect the SAM DX 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 SAM DX 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 \(on page 52\)](#).
- 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 SAM DX 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.

Require SMB encryption with Windows Admin Center

To further protect your SAM DX 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 \(on page 52\)](#) 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 52](#). (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

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

[HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Hashes\MD5]

"Enabled"=dword:ffffff

[HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Hashes\SHA]

"Enabled"=dword:ffffff

[HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Hashes\SHA256]

"Enabled"=dword:ffffff

[HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Hashes\SHA384]

"Enabled"=dword:ffffff

[HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Hashes\SHA512]

"Enabled"=dword:ffffff

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

[HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\KeyExchangeAlgorithms\Diffie-Hellman]

"Enabled"=dword:ffffff

"ServerMinKeyBitLength"=dword:00000800

[HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\KeyExchangeAlgorithms\ECDH]

"Enabled"=dword:ffffff

[HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\KeyExchangeAlgorithms\PKCS]

"Enabled"=dword:ffffff

[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:ffffff
"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:ffffff
[HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Ciphers\AES 256/256]
"Enabled"=dword:ffffff
[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 DX and SAM DX 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 DX and SAM DX.

Support and cybersecurity patches

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

A

Troubleshooting

In this section:

Scanner Administration Manager DX (SAM DX) server troubleshooting	57
Scanner network troubleshooting	59

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

Scanner Administration Manager DX (SAM DX) server troubleshooting

Symptom	Cause	Solution
"Credentials are Invalid" error message during login	Instance of DataServer used by SAM DX is not running	Restart the DataServer service on the SAM DX server. See Restart the DataServer (on page 58) .
	Incorrect credentials	Check for caps lock, etc. Verify credentials with the Administrator
After update, new features are not available in the SAM DX User Interface	Application is cached in the browser	Exit SAM DX and then clear the browser cache
Scanner is on and connected to SAM DX (retrieves its settings) but SAM DX shows the scanner as offline and no statistical data is being reported (number of scans, etc.)	Mirth on the SAM DX server is not running	See Verify Mirth is running (on page 58) .
	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	Mirth on the SAM DX server is not running	See Restart the DataServer (on page 58) .
	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 DX 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 DX 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 DX_Host) and Port (SAM DX_Port) and are using the correct SSL or non-SSL connection (SAM DX_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.

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.	<ol style="list-style-type: none"> 1 Ensure the LAN cables are connected to the scanner LAN port and to the SAM DX 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. <p>When the issue is resolved, if you have not restarted the scanner, the scanner starts transferring the slide images to the DICOM server.</p>
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.	<ol style="list-style-type: none"> 1 Ensure the LAN cables are connected to the scanner LAN port and to the SAM DX 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.

Symptom	Cause	Solution
		<p>7 If the issue persists, consult with your organization's IT professionals prior to calling Leica Biosystems Technical Services.</p> <p>When the issue is resolved, if you have not restarted the scanner, the scanner starts transferring the slide images to the DICOM server.</p>
The user reports the scanner is indicating it has no network connectivity	The scanner is unable to reach the SAM DX server	<ol style="list-style-type: none"> 1 Ensure the LAN cables are connected to the scanner LAN port and to the SAM DX server. 2 In the area provided on the scanner's touchscreen interface, enter the IP address of the SAM DX server. <div data-bbox="887 704 1275 1183" style="text-align: center;">  </div> <ol style="list-style-type: none"> 3 Verify the network connections are up and working for the Scanner and SAM DX 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:

Basic scanner information	62
Scanner configuration	62

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
Friendly Name	Local administrator's name or description for the scanner, displayed on the Scanners home page	View/Edit	None
Model	Aperio GT 450 DX	View	None
Serial Number	Specified during installation and verified at start up	View	View
Hardware Version	Verified at start up	View	View
Language	Controls the language used for scanner menus and messages	View/Edit	None
Additional version information	Available to Lab Administrator from the Scanner Information page. Some of these fields can be viewed by the Operator from the System Information page.	View	View

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	For internal use. Do not change unless instructed to do so by Leica Biosystems Technical Support.	View/Edit	None
Hostname	Name of the server where the DICOM Image converter resides.	View/Edit	None

Option	Description	View/Edit	
		Admin	Operator
	<ul style="list-style-type: none"> Use ScannerAdmin if the DICOM converter is installed on the SAM DX server. Otherwise, use the hostname of the server that the DICOM converter is installed on. 		
Port	The port that the DICOM converter is configured to use at installation. The default is 2762.	View/Edit	None
Title	For internal use. Do not change unless 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
Image filename format	Sets base file name for the scanned image file.	View/Edit	None
Barcode value identifier	Sets base format for barcode	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. <ul style="list-style-type: none"> Use ScannerAdmin if the Mirth Connect Server is installed on the SAM DX server. Otherwise, use the hostname of the server where the Mirth instance used for SAM DX 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
PIN Management			
Login Timeout	Timeout interval (minutes); the scanner locks the display and control pad when there is no operator interaction for this period of time.	View/Edit	None

Option	Description	View/Edit	
		Admin	Operator
	Valid value is any whole number greater than zero.		
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 DX administrator	View/Edit	None

C

Binding an SSL certificate to Aperio SAM DX

In this section:

Assign the SSL certificate to your website	66
Bind the SSL certificate	67


Access via the Aperio SAM DX 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.

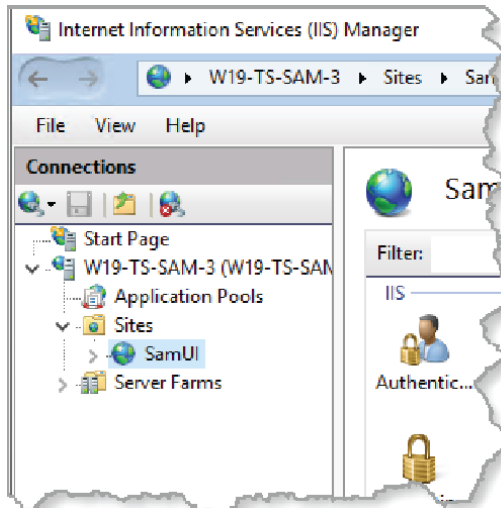
If your institution chooses to use their own SSL certificate to secure the Aperio SAM DX user interface, that SSL certificate will need to be imported and bound to SAM DX.

This section discusses how to update the SSL certificate binding to secure the SAM DX user interface in Microsoft IIS.

Follow the instructions from the SSL certificate provider to import the SSL certificate into Microsoft IIS. Then follow the instructions below to bind the certificate to SAM DX.

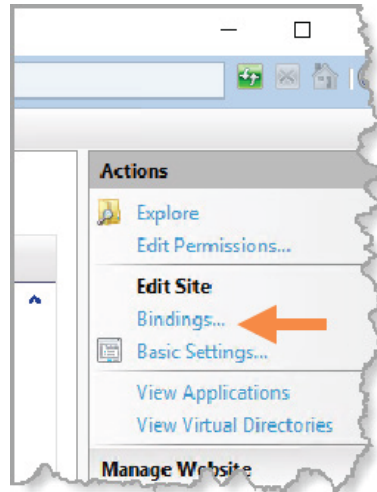
Assign the SSL certificate to your website

- 1 On the SAM DX server click the Windows **Start** button  and type **inetmgr**.
- 2 Assign the SSL certificate to your website by expanding the **Sites** subsection in the **Connections** menu on the left and selecting your website:

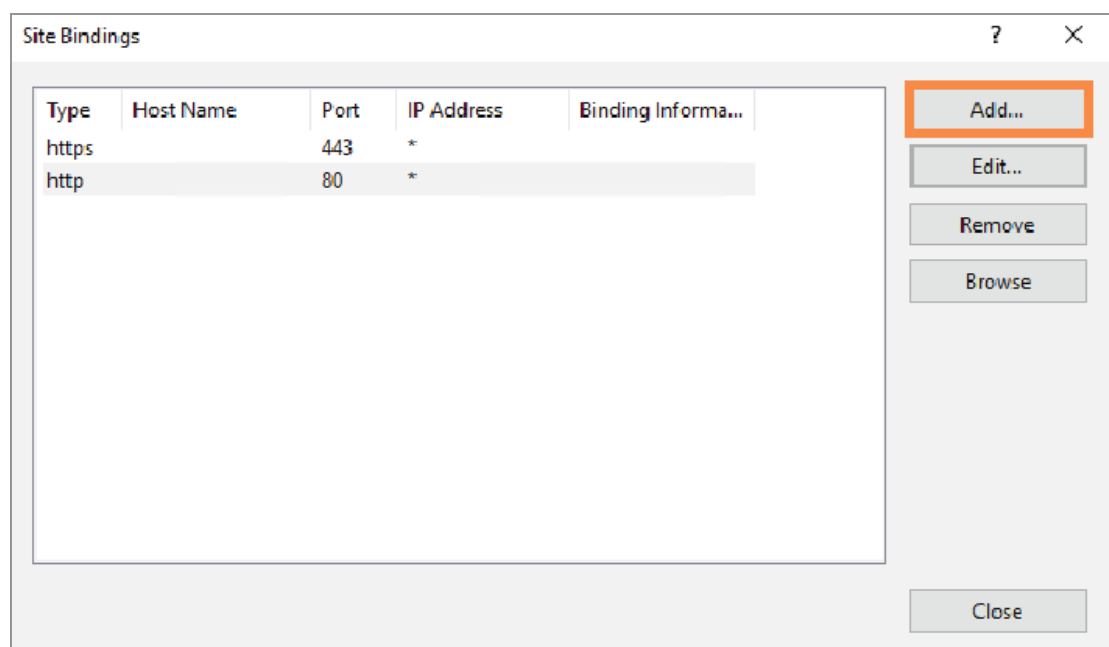


Bind the SSL certificate

- 1 In the Actions panel on the right side, locate the **Edit Site** menu and select the **Bindings** option.



- 2 On the right side of the Site Bindings window, click **Add**:



- 3 In the Add Site Binding window, modify the fields shown below:
 - a In the Type field select **https**.
 - b In the IP address field, select your website's IP address or **All Unassigned**.
 - c In the Port field, specify **443** (default).
 - d In the SSL certificate field, select the previously imported certificate, which can be identified by the friendly name.



The **Require Server Name Indication** box needs to be checked if there are multiple SSL certificates on the server.

- 4 Click **OK** for the new https entry to appear in the Site Bindings window:

Type	Host Name	Port	IP Address	Binding Informa...
https		443	*	
http		80	*	

The certificate is now installed and the SAM DX user interface should be accessible via HTTPS.

Index

A

Administrator role.....	42
allow listing.....	49
architecture.....	18

B

barcode.....	31
requiring.....	31
value identifier.....	31
basic scanner settings.....	62

C

configuration settings	
Scanner.....	28
cybersecurity patches.....	55
cybersecurity protection	
access logging.....	50
administrative safeguards.....	49
DSR, protecting.....	50
IT standards.....	49
physical safeguards.....	49
whitelisting.....	49

D

data backup.....	48
restoring.....	48
DICOM.....	18, 21
configuring DICOM output.....	33
Digital Slide Repository (DSR) server.....	19
documents.....	14

DSR.....	19, 29
settings.....	29, 38, 63

E

event handling settings.....	29, 38, 63
event logs.....	29, 39
events.....	28

F

file name format.....	30-31
-----------------------	-------

H

hostname	
basic scanner setting.....	62
DICOM converter.....	62
Mirth Connect server.....	63
scanner, displaying.....	38

I

image file name format, modifying.....	31
Image Management System.....	19
image types.....	18
images settings.....	28
Intended Use.....	8
intrusion alerts.....	40

L

Lab Admin role.....	42
log files.....	39
downloading.....	39
login timeout.....	32, 63
best practices.....	32

M

- MAC address 38, 62
- Mirth server settings 38

N

- network bandwidth requirements 19
- network configuration 19
 - recommended 20
 - system 21

O

- off-the-shelf software 55
- Operator role 42

P

- passwords 42-43, 45
- patches 55
- PIN 32, 64
 - configuration 32
 - management 29, 32
 - timeout 32
- PIN management
 - settings 64
- PIN, view current 38

R

- related documents 14
- roles 42

S

- SAM
 - logging in 14
 - troubleshooting 57
- SAM DX 12
 - features 12
 - home screen 15
 - user management 42
- scanner
 - event logs 39
 - time zone 64
- scanner settings 25
- settings
 - Images page 28
- SSL 19
- SSL certificate 19
 - assign 66
 - bind 67
- support patches 55
- system information 37
 - Info page 26
 - Settings page 27

T

- time zone 29, 64
- timeout 32, 63
- troubleshooting 56

U

- unlocking user accounts 44
- user interface 15
- user roles 42
 - definitions 42

Lab Admin role	42
Operator role	42
users	
adding	43
deleting	44
editing	44
unlocking accounts	44