From Eye to Insight

LAS X Systems

LMD Systems

IT Privacy and Security Manual

Product Names	LAS X, LMD
Language	English
Revision Information	2.1
Copyright Information	Leica Microsystems CMS GmbH 2025

Contents

1.0 Introduction

This manual describes Privacy and Security considerations in the use of LAS X and LMD imaging systems. Privacy and Security capabilities, configuration, and appropriate use are described in the following pages.

The reader is expected to have a basic understanding of the concepts of privacy and security. Privacy refers to the protection of users' personal and private data, while security refers to the protection of the system and the information in the system from risks to confidentiality, integrity and availability. The imaging system is not intended as a medical device with access to patient data. However, if the imaging system is used in a healthcare setting, it is strongly recommended that risk management procedures be used to assess and prioritize privacy, security and safety risks. Risk management can be used to determine how to best utilize the imaging system's capabilities.

2.0 Privacy and Security Environment

The system is an imaging, processing and analysis system, which can be used to acquire image data from samples for research purposes; however, it is not intended to collect, store, or use identifiable patient data of any kind. It is also not a medical device and not for use in any clinical procedures or for diagnostic purposes.

This product is intended to be used in a privacy and security environment reasonable for allowing general research purposes by those authorized to access the product via a standard Windows user account and password. It does not collect or store sensitive personal information. Image data collected by this product may be considered confidential by the customer; therefore, the customer may want to consider further measures to ensure any potential identifiable patient information is not entered into the system, such as using file or protocol names or when protecting access to this data.

The following list introduces the components included with the Imaging system which will be discussed within this document in relationship to their Privacy and Security capabilities.

- **Leica Instrument.** An instrument (i.e. Microscope, Camera, Confocal Scanner) used for imaging samples of different types.
- **Imaging Workstation.** The computer used to run the software application that controls the instrument, to store acquired data, and to process and analyze image data. This computer runs a Microsoft Windows 10 or Windows 11 operating system and is connected directly to the Microscope system through physical connection(s) like USB, Ethernet etc.
- **Imaging Software.** The software framework consisting of several separate applications and libraries and their corresponding configuration and log files, stored on the computer hard disk.
- **Imaging System.** A system which consists of a *Imaging Workstation*, the *Imaging Software* and connected *Leica Instrument(s).*

Customer intranet or external internet connectivity is not required for product functionality.
There are few optional modules which need such connectivity (i.e. Remote Care, Remote Analytics, Mobile Solutions) but they are not mandatory and have no impact on the functionality as microscopy imaging system. However, while this configuration provides the greatest protection against network attacks, consistently applying available security updates for the operating system and the application can help protect the product from physical attacks.

If the *Imaging Workstation* is connected to a customer intranet by a local IT administrator, it is strongly recommended the customer implement all relevant privacy and security protocols recommended by local IT staff.

3.0 Privacy and Security Capabilities

The *Imaging system* incorporates a broad assortment of capabilities to enable privacy and security. This section describes each of those capabilities.

3.1 Access Controls

Access controls attempt to limit access to functionality or data to specific and properly authenticated users. The *Imaging Workstation* just provides the standard access controls, implemented by the installed Microsoft Windows operating system. No special access controls are currently implemented for the imaging system, except for applications Steel Expert (SE) and Cleanliness Expert (CE) which implement a role-based access control.

3.1.1 Identity Provisioning

Provisioning of *Imaging Workstation* user accounts (provided and managed by the OS) includes the steps of account creation, maintenance, and suspension of the account when it is no longer needed. A user account is created for use by a specific individual. This user account is associated with access rights and is recorded in the operating system security audit logging. Identity provisioning establishes a link between a specific individual and a user account which can then be used during security audit reviews.

New user accounts can be set up either locally using an account with administrative rights or via a central identity and access management (IAM) system (e.g., Active Directory), which is implemented in the customer's network and is usually managed by the customer's local IT staff. We recommend connecting the PC to a central IAM to manage users centrally and increase security.

If Active Directory authentication is used, the default Windows user account can be used to join the customer’s Active Directory and then disable the account. New Windows user accounts can then be created in the customer’s Active Directory.

If local authentication is used, the customer will be required to change the default Windows user account password upon installation of the *Imaging system*. The customer should then create unique Windows user accounts and passwords for every active user.

Whether local authentication or Active Directory authentication is implemented at the customer’s site, the customer is responsible for all future management and maintenance of user accounts on the *Imaging Workstation*.

3.1.2 User Authentication

User authentication verifies that the user attempting to access the system is the user associated with the given account. Once a user has been authenticated by the Microsoft Windows authentication system, they have full access to the *Imaging Software* and any data stored in that account.

Microsoft Windows user authentication relies on the operating system’s built-in account policies. Adding more secure user authentication policies and requirements should be weighed by the customer against the risk of attack and ease of use for individuals accessing the system. Automatic log-off policy is disabled by default due to application requirements for long-term experiments. The customer may configure this policy depending on the setup.

If authentication is handled by a domain controller or other network-based mechanisms, it is recommended to create at least one user with elevated privileges such as “administrator”. Leica also recommends creating of a “local user” with administrative privileges for Leica Service Engineers (for on-site routine service and technical support).

3.1.3 Assigning Access Rights

Assigning access rights is the administrative process for connecting permissions with user accounts.

No administrative rights are required for normal use of the software. We therefore recommend that normal users are only in the Windows Users group and do not have administrative rights and only have access to the directories and services required for normal work.

Aside from typical access rights defined by the Microsoft Windows identity provisioning and authentication system, *Imaging Software* requires the following settings:

a) All users of the *Imaging Software* need proper access (Read/Write/Modify) to LAS X folders and the ‘Temp’ folder (usually C:\Temp or D:\Temp) - defined inside *LAS X Software* (under the configure tab, memory icon
b) For best performance of the *Imaging system*, it’s recommended to store files on the local drive. If the user’s desktop or other document folders are automatically redirected to a network drive, it is recommended to redirect/configure the user folders for *Imaging Workstation* (inside *LAS X Software*, go to Configure-->User) to a local folder.
c) If there are group policies defined, please make sure that all the folders/programs listed in section 11 are accessible (i.e. with full access permission) to all *Imaging system* users.

We also recommend regular access control reviews to maintain a secure and efficient system.

3.1.4 Privacy Consent Management

Privacy Consent Management is the process of supporting the customer’s ability to express their privacy requirements. This is distinct from other forms of consent such as the consent to treat.

The *Imaging system* does not create, transfer, or store any patient data; therefore, this capability has not been implemented.

In addition, depending on your Software Product Leica Microsystems may use the following optional services of:

1. “Remote Analytics” to analyze your use of the Software Product. For this purpose, “Remote Analytics” records and stores the Internet Protocol ("IP") address of your internet router or other electronic device when you use the Software Product. An IP address identifies the electronic device you employ to use the Software Product, which allows Leica Microsystems or its service providers to maintain communication with your computer or system to provide services. The Software Product implements a call-home system which collects and processes data, which includes statistical data related to the use of the *Imaging system*. This data may be used by Leica Microsystems or “Remote Analytics” and their suppliers and affiliated companies.
2. “Remote Care” to constantly check the functionality of your soft- and hardware so potential failures or problems can be rectified before data collection is interrupted or system performance is reduced. Therefore, technical machine data and software log files will be transferred to a server.

Some of the data may be stored or processed in jurisdictions other than Germany whose data protection laws may differ; however, Leica Microsystems will take the security measures described in the Privacy Policy to keep your information secure (see also https://www.leica-microsystems.com/company/privacy-policy/)

3.1.5 Logfiles and Error Report

The components of the software generate several log files (text files) that are stored locally on the computer. With the tool "Create error report" all logfiles can be collected and saved in a zip archive. If the software crashes, the tool is triggered automatically. The zip archive can help Leica Microsystems find problems in the software or configuration and should be sent to Leica Microsystems in case of a problem.

The log files contain a lot of technical information, but also some user-related information such as: Windows username, timestamps, names of images, folders, and other names and text that appear in the user interface.

If you are unsure whether your log files contain private or sensitive data, please contact Leica Microsystems before sending the bug report to Leica Microsystems.

3.2 Data Privacy and EULA

You can find the latest End User License Agreement (EULA) here:

https://contenthub.leica-microsystems.com/cdn/5FPGj63/end-user-license-agreement-eula-leica-microsystems-cms-gmbh-english.pdf

Please find the Privacy Policy here:

https://www.leica-microsystems.com/company/privacy-policy/

3.3 Privacy and Security Audit Logging and Accountability Controls

Privacy and Security Audit Logging and Accountability Controls support security surveillance and privacy investigations and reporting.

The *Imaging Workstation* audit logging and accountability controls are handled by the Microsoft Windows Event logging. Customers are encouraged to follow Microsoft's audit policy recommendations, located at: https://docs.microsoft.com/en-us/windows-server/identity/ad-ds/plan/security-best-practices/audit-policy-recommendations

4.0 Information Protection

This section describes privacy and security operations and contains guidelines for the preparation of a secure environment for the *Imaging system*.

Security capabilities are best implemented as part of an overall "Defense in Depth" information assurance strategy and are used throughout an Information Technology system which addresses attack exposure from personnel, physical security, and technology. This layered approach of Defense in Depth limits the risk that the failure of a single security safeguard will allow compromise of the target system.

4.1 Network Security

Leica Microsystems strongly recommends that the *Imaging system* and other research data acquisition and analysis systems are operated in a secure network environment that is protected from unauthorized intrusion. There are many effective techniques for isolating and protecting research data acquisition and analysis systems, including implementing firewall protection, demilitarized zones (DMZs), Virtual Local Area Networks (VLANs), and network enclaves.

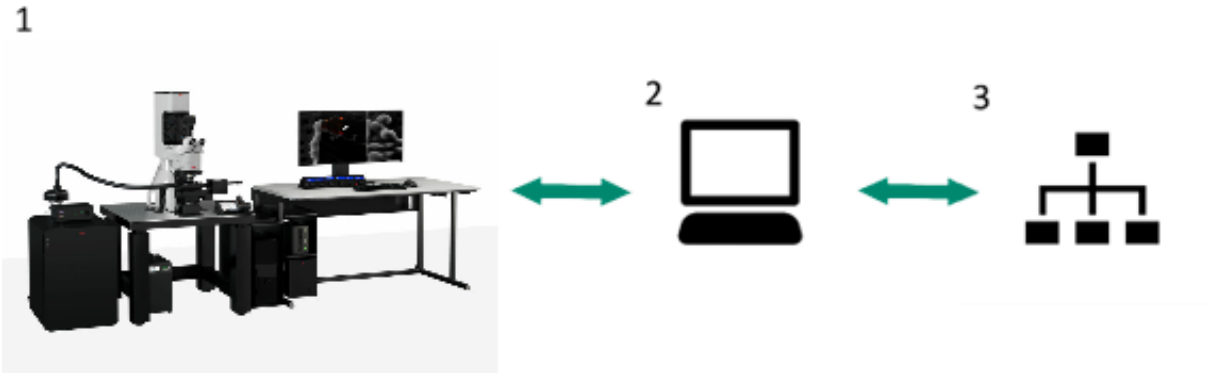
The *Imaging system* can be operated standalone, without any external network connection other than the private and direct ethernet connection between the Imaging Systems and the *Imaging Workstation*. The *Imaging Workstation* has an additional network interface port that can be optionally connected to a wired ethernet connection to also communicate with a customer's local network.

Storing large amounts of image data at runtime (during the acquisition) on network attached systems (servers, desktops, NAS etc.) might be negatively impacted by the existing network infrastructure, bandwidth and traffic, the implemented security concepts (Firewall, Antivirus Protection), and other factors. This impact can range from lags in performance/stability to a potential loss of data.
In such cases it might be useful to doublecheck and remove the Antivirus protection and monitoring of the target image folders on the network share or server.

To prevent this situation in general, it is recommended to first store data locally on the *Imaging Workstation* and move or copy the after the completion of the acquisition.

Component	Function
1	*Leica Imaging System* – private ethernet connection, USB connection etc.
2	*Imaging Workstation* – running *Imaging Software*, data storage for image data
3	LAN – Optional customer local area network

The image below shows a schematic representation of an *Imaging system* network connections.



4.2 Wireless Security

Due to the broadcast nature of wireless communication, wireless devices require special security considerations. There are effective techniques and tools for improving the security of wireless communication devices.

The *Imaging system* does not contain any wireless technology - therefore, this layer of security does not need to be considered.

4.3 Removable Media Security

The *Imaging Workstation* provides the possibility to use removable USB media, although this method is not recommended. If removable USB media is used, it is recommended that the media be encrypted using Microsoft's BitLocker technology. The storage media and the content on the storage media must be handled according to applicable customer site and security requirements.

Removable media can be used for storage of the following types of data:

- Image data and instrument meta data
- Configuration files
- System backups
- Backups of the service logs
- Backups of historical files

We also recommend:

- Disabling unnecessary USB ports and communication channels.
- Scan for malware and malicious threats on all removable media using a virus scanner.
- Deactivating the automatic start of applications from inserted removable media.

4.4 Data at Rest Security

Data at Rest Security methods protect data from unwanted access while it is stored on either local or external file systems. These methods most often employ some kind of data encryption.

The *Imaging system* does not currently utilize any Data at Rest Security methods, although tools like Microsoft BitLocker might be installed by the customer to provide this service through the Windows operating system. The installation of such tools or sub-systems might have a negative impact on the performance of the *Imaging system*.

4.5 Data integrity

The *Imaging system* creates image data and instrument metadata which is stored in files either of a proprietary Leica format (*.lif, *.xlef, *.lof) or optionally in common image file formats like TIFF, JPEG, BMP. The *Imaging system* does not provide any additional functionality to check data integrity of the stored files.

The *Imaging system* is not intended to be used as a medical device with access to patient data. It does not create, transfer, or store this kind of data and therefore does not support this capability.

4.6 Business Continuity

Business Continuity methods preserve data in the event of malicious attack or disaster recovery.

The *Imaging system* does not include any built in Business Continuity capabilities.

The *Imaging Workstation* stores configuration files, image data and instrument metadata. The customer is encouraged to create a disaster recovery plan which includes the configuration files and file system backup procedures.

5.0 System Protection

This section describes the guidelines for configuring and maintaining the product using methods that continuously protect privacy and security.

5.1 Protection from malicious software

The computing environment is increasingly hostile, and threats continue to grow from denial-of-service attacks and malicious software, including computer viruses, worms, Trojan horses, and other malware. Vigilant defense on many levels is required to keep the systems free from intrusion by malicious software.

To prevent unwanted software from running on the system, it is recommended to use an allowlisting procedure, such as Windows Defender Application Control. Windows Defender can be configured using the built-in tools provided by Microsoft to suit the organization's security needs.

Even with a secure configuration, the application still requires regular customer interaction to stay up-to-date and effective. Ongoing monitoring and maintenance are essential to ensure continued protection against emerging threats.

5.2 Antivirus Protection

An *Imaging system* is designed to be used in an environment where commercial antivirus software is used to detect the presence of malicious software (virus, Trojan horse, worm, etc.). The *Imaging Workstation* comes equipped with Microsoft Windows Defender configured, enabled and with up-to-date AV signatures at the time of manufacturing.

Beside this default setup, other Antivirus software packages can be installed and used on a *Imaging Workstation*. In case they have an impact on performance or stability of the *Imaging Software* or the connected imaging system, try to exclude the folders mentioned in section 11.0 or 12.0 from being monitored.

Switching off the anti-virus scan procedure on the specific "temp" drive of the Imaging Software ensures that performance issues won't occur.

5.3 Firewall Protection

The *Imaging Workstation* comes with the Microsoft Windows built-in Firewall configured and activated. See details for the LAS X Software in chapter 11.1.1 Firewall LAS X System and for LMD in chapter 12.1.1 Firewall LMD System.

5.4 Server and/or Workstation Security

The *Imaging system* can be operated standalone or as part of a customer's network. In standalone mode, the Windows security setup can be manually adjusted by the customer to fit individual requirements (i.e., inactivity timeout, screen lock, etc.). If the *Imaging Workstation* is added to an

Active Directory group, the Windows security can be managed by Microsoft's Group Policy or the customer's local IT team.

5.5 Third party software

Leica Microsystems cannot test the compatibility of *Imaging Software* with all available third-party software possibly installed by customers. Installation of any such third-party software (including updates and patches) is at the customer's own risk. It is recommended to contact the local IT department/network administrator before installing or configuring such software.

The *Imaging system* is guaranteed to perform to specifications only in the original state it was delivered and installed – this includes application software, device drivers and firmware. If additional third-party software (image analysis, antivirus, etc.) is installed by the customer, it cannot be guaranteed that the system will perform to specifications.

In case of unacceptable results after the installation of third-party software, it is recommended to remove of the third-party software or update/hotfix separately to restore functionality on the system.

5.6 System Change Management

The *Imaging Workstation* is delivered installed with the latest Microsoft Windows Operating System security updates available at the time the system was built. For information regarding which security patches have been installed on the system, click **Start** on the taskbar, and then select **Control Panel | Programs | Programs and Features | View installed updates**. Security setting verification needs to be performed by a user with an Administrator account.

The *Imaging Workstation* is configured with default security settings using the security configurations of the Microsoft Windows operating system. These security settings are configured in accordance with the Leica Microsystems privacy and security recommendations. The default settings can be changed by members of the Administrators user group.

Regarding Leica Microsystems privacy and security recommendations it is required to change the initial password as well as making sure to change password in a 90 day period.
The Password should fulfill the following requirements:

a) Passwords must be at least ten characters in length
b) Passwords must contain the following 4 requirements to meet complexity requirements. One upper case alpha character, one lower case alpha character, one numeric value and a special character (i.e. !, @, #, $, %, ^, &).
c) Passwords cannot be reused.

Leica Microsystems does not provide additional automatic *Imaging Software* updates after system delivery.

The customer is responsible for manually updating the system with Microsoft Windows operating system security and critical patches released periodically by Microsoft. These updates should be done by a user with administrative privileges. This activity most likely requires configuration of the *Imaging Workstation* to use the optional external network interface to connect to the customer's local network. Note that many Windows updates require a reboot of the system. To avoid impact on *Imaging system* performance, including potentially running experiments, install the updates only when the *Imaging system* is not in use.

For the installation of “Optional OS updates” or “Service Packs”, the LMS Support should be contacted to check whether the update is compatible with our *Imaging system*. Updating the operating system with service packs may reduce workstation and memory resources available for the application software.

6.0 Remote Service

The only remote service applications included with the *Imaging system* are the services provided by the Microsoft Windows operating system. These services are disabled by default at the factory. For troubleshooting purposes, Leica Support might request your permission to remotely connect to your computer. Usually, that is done via the BeyondTrust support portal, which can temporarily install a program for establishing this remote connection. As soon as the service session has ended, the program will be automatically uninstalled. BeyondTrust solutions are designed to work transparently through firewalls, enabling a connection with any computer with internet connectivity, anywhere in the world. However, with certain highly secured networks, some configuration may be necessary.

Please check with Leica service which ports needs to be open.

7.0 Personal Information Collected by the System

The *Imaging system* is not designed and intended to be used as a medical device with access to patient data or personal information. It does not create, transfer, or store this kind of data.

8.0 Additional Considerations

The *Imaging system* has been designed with Privacy and Security functionality integrated into the core design; however, residual Privacy and Security risks remain that must be mitigated once the system is integrated into the customer’s work environment. This section describes those risks that should be imported into the Risk Assessment of the deployment of the *Imaging system* for proper mitigation.

The *Imaging system* includes an operating system which contains private user accounts used by the *Imaging Software* to control the hardware of the Imaging System to acquire data. These accounts are also required by Leica Service personnel for onsite troubleshooting or maintenance procedures. If the *Imaging Workstation* is breached by an attacker, the Imaging System may also be vulnerable to attack through these accounts or flaws in the underlying operating system.

The Imaging system is not compliant with the Federal Information Processing Standard (FIPS) and therefore FIPS should be deactivated or at least be adapted.

It is advisable to disable all active power saving/management modes in Windows, which can potentially turn off USB devices, hard disks, graphic cards etc.

9.0 Up-to-date Information on Privacy and Security

Leica Microsystems is hosting a dedicated web site to inform customers on critical Privacy and Security findings and the corresponding solutions. This includes an e-mail service, customers can subscribe.

https://www.leica-microsystems.com/company/product-security/

Potential security vulnerabilities or privacy issues with a Leica Microsystems product should be reported via e-mail to: ProductSecurity(at)leica-microsystems(dot)com

Please refrain from including sensitive information (e.g., sample information, PHI, PII, etc.) as a part of any submissions to Leica Microsystems. Please provide the following information in your submission:

- Your contact information (e.g., name, address, phone number, and email)
- Date and method of discovery
- Description of potential vulnerability
- Product name
- Version number
- Configuration details
- Steps to reproduce
- Tools and methods
- Exploitation code
- Privileges required
- Results or impact

10.0 Latest news on software

Please read the Release Notes from the latest *Imaging Software* version for new features, improvements and bug fixes.

11.0 LAS X Software

11.1 LAS X Architecture Overview

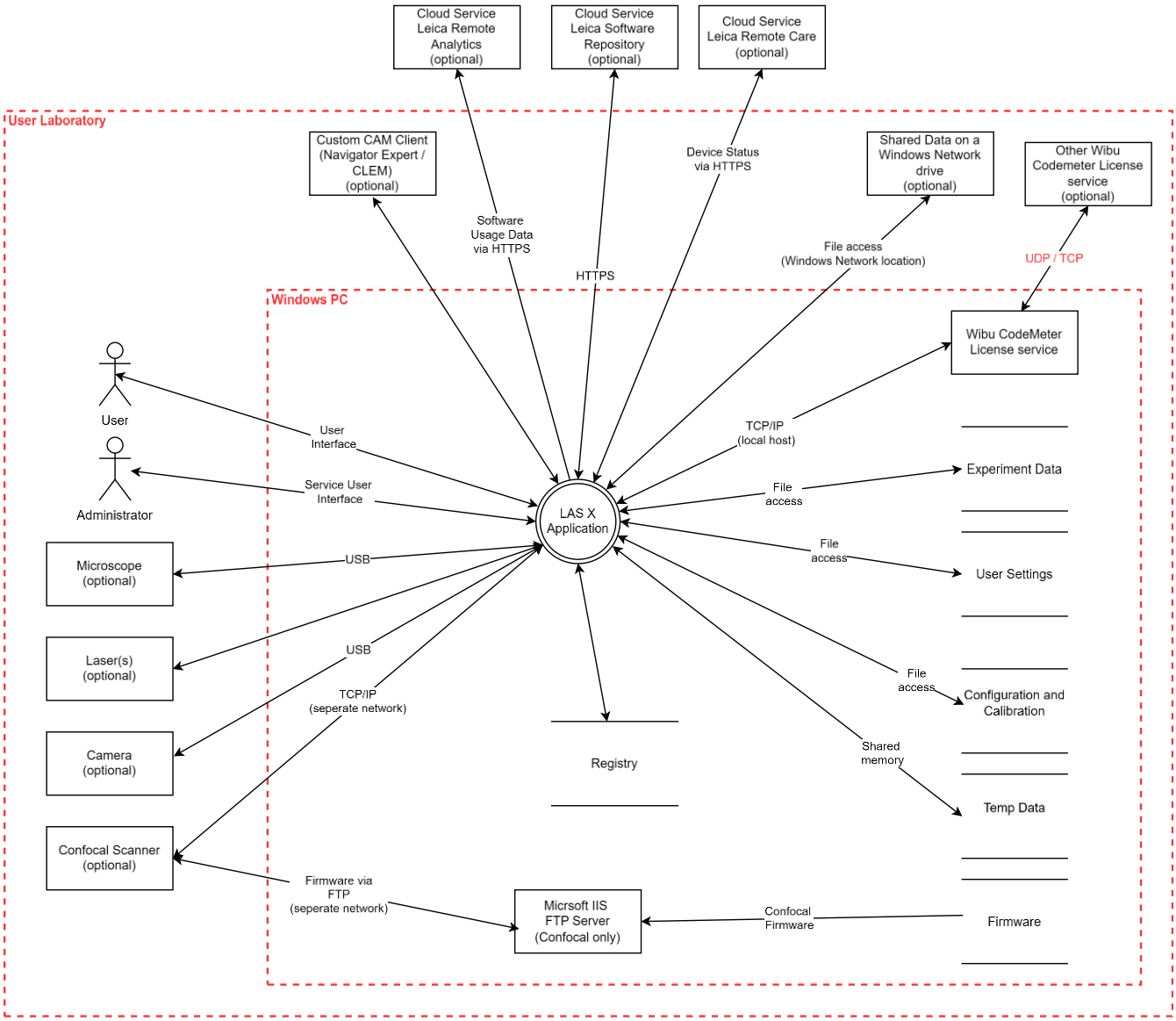
The *LAS X Software* is installed on Microsoft Windows PC workstations.

The microscope and other devices like cameras, confocal scan head, lasers etc., are connected to the PC. (USB, Ethernet, etc.)

Data can be stored on the local hard disc or on shared network drive

Third Party Software is used, like *WiBu CodeMeter* and *Nvidia* device drivers, to control third party hardware.

Main User Management is the Windows user management.



11.1.1 Firewall LAS X System

The following exceptions or rules were added to the firewall with the installation of the *Imaging Software*:

Connections (Most important)

Process	**Connections**
LMSDataContainerServerV2	Listens to port 8892. Accepts connections from localhost only
DyeDataBaseService.exe	Listens to port 8897. Accepts connections from localhost only
CodeMeter	(3rd Party License Software). Listen to TCP port 22350 and UDP 0.0.0.0:22350
CmWebAdmin	(3rd Party License Software). Listen to TCP port 22352
LMSApplication	Connection to LMSDataContainerServerV2 (8892) and CodeMeter (22350)

Process	Connections
LMSServiceControl	Connection to LMSDataContainerServerV2 (8892)
LCS	Listen to localhost TCP port 2081 Connection to LMSDataContainerServerV2 (8892) and CodeMeter (22350) Connection to Remote Care client (LMSIoTCoreService): 50000 (if Remote Care is activated)
LMSRemoteAnalytics	(if Remote Analytics is activated) Connection to LMSDataContainerServerV2 (8892) Calls Revulytics Server (67.227.186.229) on port 80
LMSUserDataService	Connection to LMSDataContainerServerV2 (8892)
LMSUserManager	Connection to LMSDataContainerServerV2 (8892)
LMSInformationService	Connection to LMSDataContainerServerV2 (8892)
LMSIOManager	Connection to LMSDataContainerServerV2 (8892)
LMSGPUComputeService	Connection to LMSDataContainerServerV2 (8892)
HWConfigurator	Connection to LCS (2081)
CAMServer	Listen to Port 8895 and accepts outside calls (off by default) Connection to LMSDataContainerServerV2 (8892) and CodeMeter (22350)
DyeDatabase	Connection to LMSDataContainerServerV2 (8892) and CodeMeter (22350)
Process	Connection to LMSDataContainerServerV2 (8892) and CodeMeter (22350)
LMSIoTCoreService	(Remote Care only) Listen to localhost port 50000. Accepts connections from localhost only Connection to LMSIoTConnector (4999)
LMSIoTConnector	(Remote Care only) Listen to localhost port 4999. Connection to Leica Remote Care hosted on Amazon Cloud (AWS)
Updater.exe	(If Leica Software Updater is used) Opens connection to update.leica-microsystems.com
CLEM.exe	Listen to Port 8896 and accepts outside calls (off by default) Connection to LMSDataContainerServerV2 (8892) and CodeMeter (22350)
NavigatorExpert.exe	Listen to Port 8896 and accepts outside calls (off by default) Connection to LMSDataContainerServerV2 (8892) and CodeMeter (22350)

11.1.2 Major LAS X Software Folders and Subfolders

- C:\Program Files\Leica Microsystems CMS GmbH
- C:\Program Files\CodeMeter
- C:\Program Files (x86)\Leica Microsystems CMS GmbH
- C:\Program Files (x86)\CodeMeter
- C:\ProgramData\Leica Microsystems
- C:\ProgramData\CodeMeter
- C:\Users\{user name}\AppData\Roaming\Leica Microsystems
- C:\Users\{user name}\AppData\Local\Leica_Microsystems
- C:\Users\{user name}\AppData\Local\Leica_Microsystems_CMS_Gm
- USB Hardware Dongle
- Temporary data container location: usually **C\Temp**: or **D:\Temp** (confirm configuration inside LAS X software)

12.0 LMD Software

The *LMD* is not designed and intended to be used as a medical device with access to patient data or personal information. It does not create, transfer, or store this kind of data.

12.1 LMD System Context

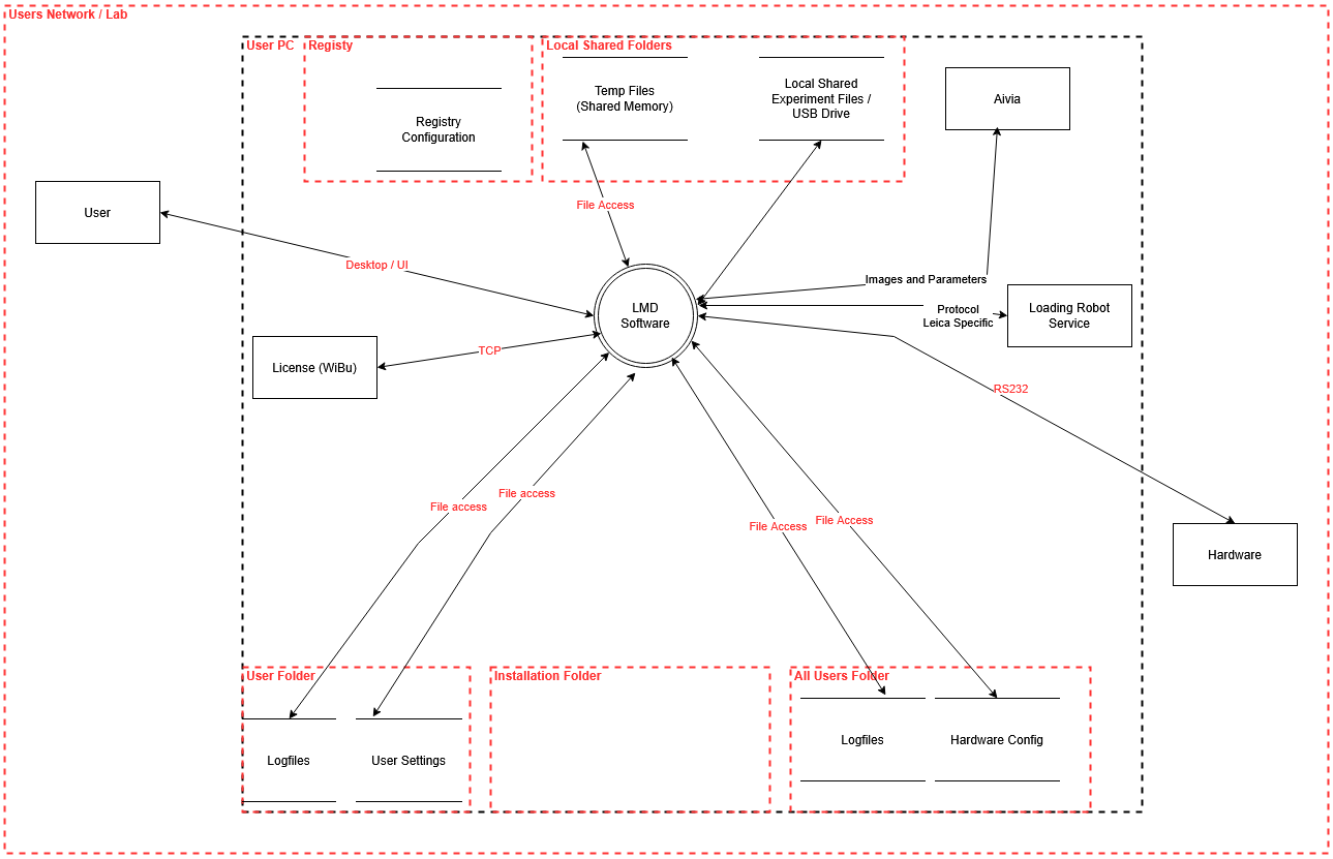
The *LMD Software* is installed on Microsoft Windows PC workstations.

The microscope and other devices like cameras, lasers etc., are connected to the PC.
(USB, Ethernet, RS-232, etc.)

Data can be stored on the local hard disc or on shared network drive

Third Party Software is used, like *WiBu CodeMeter* drivers, to control third party hardware.

Main User Management is the Windows user management.



12.1.1 Firewall LMD Systems

The following exceptions or rules were added to the firewall with the installation of the *Imaging Software*:

Connections (Most important)

Process	**Connections**
LMSDataContainerServerV2	Listens to port 8892. Accepts connections from localhost only
CodeMeter	(3rd Party License Software). Listen to TCP port 22350 and UDP 0.0.0.0:22350
CmWebAdmin	(3rd Party License Software). Listen to TCP port 22352
LMD	Connection to LMSDataContainerServerV2 (8892) and CodeMeter (22350) Optional: Listen to predefined port (must be set and activated in settings).
LMD Lif Browser	Connection to LMSDataContainerServerV2 (8892)
External program	Optional: Connection to LMD via predefined port (must be set and activated in settings)

12.1.2 Major LMD Software Folders and Subfolders

- C:\Program Files\Leica Microsystems CMS GmbH
- C:\Program Files\LeicaLMD
- C:\Program Files\CodeMeter

- C:\Program Files\Leica Microsystems\DataContainer

- C:\ProgramData\Leica Microsystems
- C:\ProgramData\CodeMeter
- C:\Users\{user name}\AppData\Roaming\Leica Microsystems
- C:\Users\{user name}\AppData\Local\Leica_Microsystems
- C:\Users\{user name}\AppData\Local\Leica_Microsystems_CMS_Gm
- USB Hardware Dongle
- Temporary data container location: usually C\Temp: or D:\Temp (confirm configuration inside LMD software)