From Eye to Insight

Leica
MICROSYSTEMS

Cybersecurity Manual

User Manual

10 747 996 version 04

Date of issue: 2024-12-03

CE

Thank you for purchasing a Leica surgical microscope.
In developing our systems, we have placed great emphasis on simple, self-explanatory operation. Nevertheless, we suggest studying this user manual in detail in order to utilize all the benefits of your new surgical microscope.
For valuable information about Leica Microsystems products and services, and the address of your nearest Leica representative, please visit our website:

www.leica-microsystems.com

Thank you for choosing our products. We hope that you will enjoy the quality and performance of your Leica Microsystems surgical microscope.

Leica Microsystems (Schweiz)AG
Max Schmidheiny-Strasse 201
CH-9435 Heerbrugg
Phone: +41 71 726 3333

Legal disclaimer
All specifications are subject to change without notice.
The information provided by this manual is directly related to the operation of the equipment. Medical decision remains the responsibility of the clinician.
Leica Microsystems has made every effort to provide a complete and clear user manual highlighting the key areas of product use. Should additional information regarding the use of the product be required, please contact your local Leica representative.
You should never use a medical product of Leica Microsystems without the full understanding of the use and the performance of the product.

Liability
For our liability, please see our standard sales terms and conditions. Nothing in this disclaimer will limit any of our liabilities in any way that is not permitted under applicable law, or exclude any of our liabilities that may not be excluded under applicable law.

Contents

1 Introduction 2
- 1.1 Purpose 2
- 1.2 Symbols in this user manual 2

2 ARveo 8/ARveo 8x – Purpose and Requirements of Networked Connections 2

3 Cybersecurity Controls 4

4 Advanced Feature Configuration and Use for IT Users 6
- 4.1 Authenticate as an IT User 6
- 4.2 Configuring ARveo 8/ARveo 8x Application Security Settings 7
- 4.3 Configuring and Verifying DICOM Settings 8
- 4.4 Running Audit Report 9
- 4.5 Elevating Windows Access 10
- 4.6 Resetting User Password 10
- 4.7 Configuring ARveo 8 /ARveo 8x Network Settings 10

5 Software Updates 12

6 Cybersecurity Incident Reporting 12

1 Introduction

1.1 Purpose

This manual is documenting the purpose of connecting ARveo 8 and ARveo 8x to network and other hospital equipment; define the set of cybersecurity controls used to secure the Leica Microsystems ARveo 8 and ARveo 8x and how a customer with elevated privileges (IT user role) may configure these controls.

1.2 Symbols in this user manual

The symbols used in this user manual have the following meaning:

Symbol	Warning word	Meaning
⚠	**Warning**	Indicates a potentially hazardous situation or improper use that could result in serious personal injuries or death.
⚠	**Caution**	Indicates a potentially hazardous situation or improper use which, if not avoided, may result in minor or moderate injury.
	Note	Indicates a potentially hazardous situation or improper use which, if not avoided, may result in appreciable material, financial and environmental damage.
!		Information about use that helps the user to employ the product in a technically correct and efficient way.
►		Action required; this symbol indicates that you need to perform a specific action or series of actions.

2 ARveo 8/ARveo 8x – Purpose and Requirements of Networked Connections

ARveo 8 and ARveo 8x are intended to be used within the operating room in a hospital. It may be stored in the same room as use or moved to storage space (room or hallway) within the secure facilities. Hospital IT, nurses, and surgeons will regularly have access to the system.

The system has the following data interfaces which have been considered when evaluating system cybersecurity:

- networked data transfer for storage
- data transfer to external storage media
- connection to Leica RemoteCare server to post service status of the microscope and connections to 3rd party equipment to support interconnectivity and visualization in the operating room

ARveo 8 and ARveo 8x provide the following networked data transfer for storage: ethernet connectivity to DICOM nodes. Data transfer to external storage media is supported through USB 3.0 connections on the microscope. Connections to 3rd party equipment are connected by DVI and SDI connections for video distribution and CAN for control communications.

⚠ **CAUTION**

Microscope Network Connection

Connecting the microscope to the hospital network exposes the microscope to additional risks of the network that could result in unidentified risks to patient, operator, or 3rd parties. Hospital organization responsible for the network should work with the microscope users to identify, analyze, evaluate and control these risks.

Networked data connections are supported by a wired 10Gbase-T (ARveo 8) or 2.5Gbase-T (ARveo 8x) ethernet connection for TCP/IP connections. This connection is used to transfer data after surgery is complete, there is no risk to microscope use due to network quality or bandwidth, reduced bandwidth will slow transfer of the data. The connection supports up to a 10 Gbit/s (ARveo 8) or 2.5 GBit/s (ARveo 8x) bandwidth connection; 100Mbps is enough for reasonable speed of data transfer (ARveo 8 does not support 100Mbps connections). The system supports the use of TLS 1.1. and 1.2 for encrypted communications over this connection when the hospital supports the use of TLS encryption. DICOM connectivity is a customer purchasable option that allows the user to obtain electronic patient information and push images and videos to network storage in accordance with DICOM standard DICOM PS3.1. The user can connect to a DICOM node that contains Modality Worklist schedule to obtain the patient information that the

microscope may use to associate acquired images (JPG) and videos (MP4) with the scheduled patient prior and create a DICOM standard file (DCM) to export to a DICOM node. The DICOM connection attempt to use encrypted communications by default, however many DICOM nodes in use do not support encrypted communications and in these cases ARveo 8 and ARveo 8x will use unencrypted communications. The use of encrypted communications presents a hazardous situation where patient information is being communicated unencrypted and may be detected in transit leading to potential disclosure of patient information. This risk is mitigated by the assumption that the institution is taking precautions to provide engineering controls and operational security that limits access to the network.

ARveo 8 and ARveo 8x support file transfer to external transportable media through USB 3.0. The system provides an export capability to copy images (JPG) and videos (MP4) to the external media. The external media is treated as a USB mass storage device class (MDC) and will support file transfer at up to 625 MB/s provided that the user is using an external media device that is USB 3.0 compatible. This connection is used to transfer data after surgery is complete, there is no risk to microscope use due to reduced bandwidth, this will simply slow transfer of the data. As such there are no hazardous situations that result from failure of the network to meet required bandwidth characteristics.

Leica RemoteCare Connection provides a direct connection for Leica service associates to receive microscope system information that will aid in providing highest levels of system up-time and mean time to repair. Each system is provisioned at the factory using a X.509 certificate configured to adhere to appropriate policies using Authentication, authorization, and accounting (AAA) framework. RemoteCare utilizes the hospital LAN connection of the microscope to establish a connection with the Leica data server. This server is responsible for collecting and distributing the following data to authorized service personnel, facilitating diagnostics and support:

- System Component Hardware Versions
- System Component Software Versions
- Status of installed Licenses
- Lamp Accumulated hours for lamp 1
- Lamp Accumulated hours for lamp 2
- Available hard drive space
- Service Log files

No personal data is collected or distributed via RemoteCare.

This data is accessible to service users with credentials that allow access to the AWS data through a web application that presents a dashboard of the system data. To achieve this capability, RemoteCare requires that the hospital provides incoming and outgoing internet access through firewalls on the Hospital network.

Microscope provides several connections to 3rd party equipment in the operating room. There are DVI- and 3G/12G- SDI video outputs that can be used to display the microscope video on additional monitors or to be connected to an external recording or distribution system. There is a DVI-I video input connection to allow endoscope video to be displayed on the microscope views. There is DVI-I video input to provide video from an Image Guided Surgery (IGS) System to display that information as part of the microscope displays. These input and output videos support standard high definition video formats supported by the DVI-I and 12G/3G/HD-SDI connections. System supports communication to the IGS system through a proprietary protocol that is defined by the IGS provider and supported by a CAN connection.

3 Cybersecurity Controls

Medical device security is a shared responsibility of all stakeholders: manufacturers, hospital employees, service providers and patients. Compromised cybersecurity can result in loss of data, system availability, system integrity or expose other connected devices or networks to security threats. The following lists the design controls that are in place to mitigate potential vulnerabilities and the associated threats.

Operating System Access
ARveo 8 and ARveo 8x users interact with the system configured with minimum permissions. Authenticated clinical users, Leica Sales users, and unauthenticated users cannot use any Windows OS functions and may only run the microscope application. Authenticated IT users and Leica Service users may use the system with elevated permissions and have access to Windows OS functions; this access is required for specific configuration actions.

Operating System Configuration
ARveo 8 and ARveo 8x run Windows 10 IoT Enterprise LTSC 2021 with all unnecessary services and port access disabled. Microscope application runs in a shell launched to run the system as a kiosk device.

Operating System Runtime Restrictions
ARveo 8 and ARveo 8x are configured with Windows Firewall and Windows AppLocker actively running to limit what software may execute. This includes disabling Autorun functionality of USB ports.

Real-time Threat Protection
ARveo 8 and ARveo 8x are configured with Windows Defender activated providing real time protection against viruses and malware.

Encryption Measures
All information stored on the hard disc of the ARveo 8 and ARveo 8x is encrypted with a strong encryption algorithm using the Windows BitLocker feature. This ensures that no information is stored as plain text on the hard disc, and theft of the computer or its hard discs will not compromise the sensitive information of the patients. In addition to hard drive encryption, all PHI and auditable events are encrypted prior to being stored in local databases.
The microscope application uses private cryptographic keys stored securely on a Trusted Platform Module (TPM). The TPM is a stand-alone device installed in the computing module, independent from the CPU. It can store the private keys securely and providing them to the application as needed. This ensures that the private keys are never stored on the system's working memory.
All personally identifiable information stored on ARveo 8 and ARveo 8x is encrypted prior to storage and decrypted for presentation to the user.

User Management
ARveo 8 and ARveo 8x have implemented three user types for user operations and two user roles for Leica Microsystems personnel.

Unauthenticated Users
Use of the microscope does not require any user authentication, an unauthenticated user may use microscope including recording videos and pictures. The sole limitation is the inability to access or enter patient information for export or association with recorded imagery.

Authenticated Clinical User
Access to stored patient information, patient information from a modality worklist, or entering patient information that will be stored on the system requires Clinical users to login with their personally identifiable username and password prior to accessing these system features.

Authenticated IT Users
These users have extensive rights to configure the security settings of the system. This includes resetting user passwords, creating new users, disabling users, configure security settings, configure connections, and generate audit reports. These users can exit the application and access the Operating System with elevated permissions to change Windows configuration and install software updates.

Leica Microsystems Accounts Limitation and Security
Leica Microsystems has two specialized accounts, Sales and Service, which allow Leica representatives system access to configure and troubleshoot the system. These accounts are only accessible by use of a hardware dongle that is managed by Leica Microsystems and is active for a predefined lifetime and are traceable to individual associates. These accounts do not have the ability to access patient information on the system.

User Authentication
Authenticated users require usernames and passwords to manually be entered through the software interface; authentication via credentials supplied over the network, using badge readers or biometrics is not possible. User names are expected to be unique to individuals to enable auditing to allow events to be traced to specific users.

Access Notification
ARveo 8 and ARveo 8x notify users when they would have access to patient information. The microscope software reminds Clinical users that accessing patient information should only be done by authorized personnel and not to continue with login if unauthorized.

Network Communications
ARveo 8 and ARveo 8x are configured to use Transport Layer

Security (TLS) for encrypting data that is exported over Ethernet. For DICOM communications, encrypted communications are selected by default but DICOM nodes that ARveo 8 and ARveo 8x connects may only accept unencrypted data transport. In this case the system may be configured to allow unencrypted DICOM syntaxes.

Secure Coding Practices

Microscope software application has been developed by Leica Microsystems in accordance with development standards and practices. This includes requiring developers to complete secure coding training; conducting system cyber security risk assessment; conducting vulnerability assessments; implementing design controls to mitigate risks and vulnerabilities to achieve and acceptable level; conducting static code analysis during software development and deployment; and conducting 3rd party penetration testing and gap mitigation.

Digital Signatures

All software applications from Leica Microsystems are digitally signed. This ensures that the application being used is trustworthy, reducing the risk of unauthorized applications compromising the sensitive information stored on the machine.

Shipping Integrity

ARveo 8 and ARveo 8x are configured prior to shipment to mitigate concerns of tampering during shipment from Leica Microsystems facilities.

Audit Logging

ARveo 8 and ARveo 8x provide IT users the ability to generate an audit log that reports all security events, identifies the user who initiated the event, and when the event occurred. Security events that are recorded include the following:

- DICOM Exporting images (start, error-finish, success-finish)
- Exporting images to file system (USB drive) (start, error-finish, success-finish)
- Export audit logs to file system (start, error-finish, success-finish)
- Export non-audit logs to the file system (start, error-finish, success-finish)
- Retrieving and viewing OS elevated access credentials
- Start/End/Continuation (after GUI restart) of surgery
- Initiating exports to file system
- Aborting exports to file system
- Viewing MWL queries (with patient names)
- Viewing recorded surgeries (with patient names)
- Retrieving and viewing OS elevated access credentials
- License dongle insertion
- Automatic user activated on dongle insertion
- License dongle removal
- Being denied access to a UI page that requires more authorization
- Logging in successfully using a password that has expired (or that was a default password)
- Logging in successfully (using a password that has not expired)
- Logging in successfully
- Login failures
- Login failures (exhausted login attempts)
- Default user activation
- New user created
- User updated
- User passwords reset
- Patient Information Protection Option updated (in multiple places)
- Auto delete option updated
- Unable to delete missing patient data file (in two places – regular and auto)
- Error deleting patient data file
- Deleting patient data file (in two places – regular and auto)
- No record limit received from database (in two places)
- Initiating auto-delete (with info about how much space to be freed)
- During auto-delete, removing complete surgery metadata, or updating surgery metadata
- During startup, removing orphaned surgeries (no recordings), or errors trying to remove orphaned surgeries
- During startup, removing orphaned patients (no metadata)
- Enabling/Disabling users from IT account
- Creating surgeon profiles
- Updating surgeon profiles
- Parameter saving (from GUI, all basic settings except Brightcare.)
- Firmware updates

Secure by Default

- ARveo 8 and ARveo 8x security features are enabled by default; there are some security features that may be disabled at the discretion of IT users. These decisions on security configuration are applied to all system users once applied; these features include:
- Requiring clinical users to authenticate with username and password prior to accessing or recording any patient health information.
- Require clinical users to have a unique, individualized username and password.
- Require clinical user passwords to meet minimum password requirements: one uppercase, one lowercase, one numeric, one special character and a minimum of 10 characters.
- Require clinical accounts to be changed when maximum password age is reached.
- Limit clinical user passwords from using repeated passwords from recent history.
- Automatic timeout of user account after inactivity.
- Automatically lockout users after specified number of invalid login attempts.

4 Advanced Feature Configuration and Use for IT Users

This section provides details for how IT users may change the system configuration. At the time of system installation, Leica Microsystems personnel will assist with initial setup of these functions. If no changes are required after installation, it is recommended to leave the system in the configuration established at installation. If the configuration must be changed, contacting Leica Microsystems Service teams to manage these changes is recommended. All the functions in the section require the user be authenticated as an IT user before proceeding with the instructions.

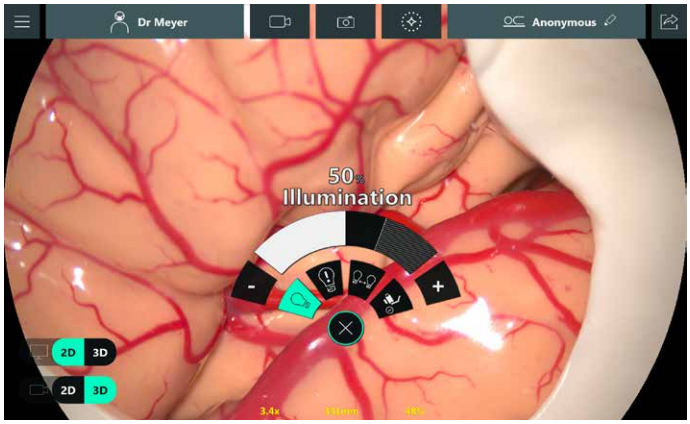
CAUTION

Risks Due to Changing Microscope Configuration

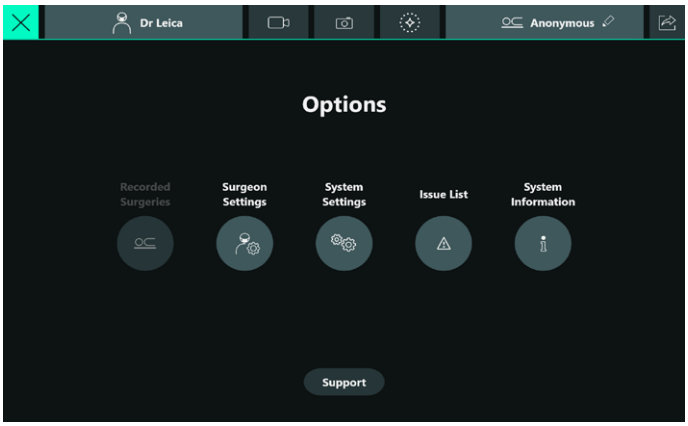
Once the configuration that control potential cyber security risks is established, take care not to change the configuration without assessing the potential risk impact. These changes would include but are not limited to network configuration changes, connection of additional items to the microscope, disconnection of items from the microscope, update of equipment.

4.1 Authenticate as an IT User

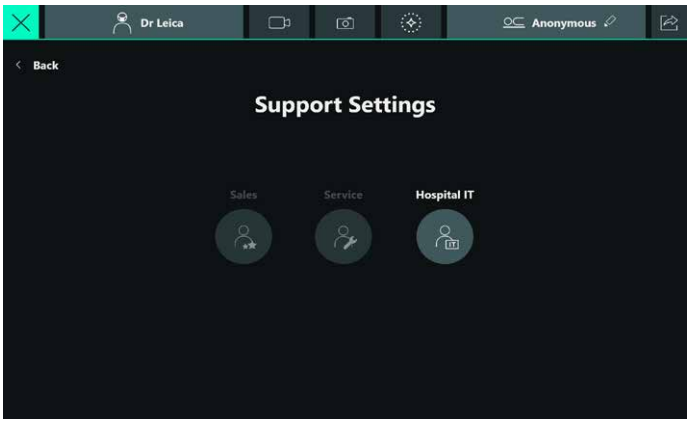
► Navigate to Options by selecting the Main Menu



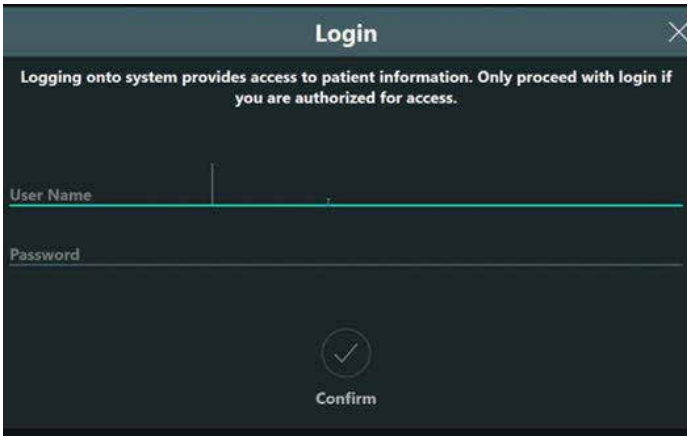
► Select Support



► Select Hospital IT

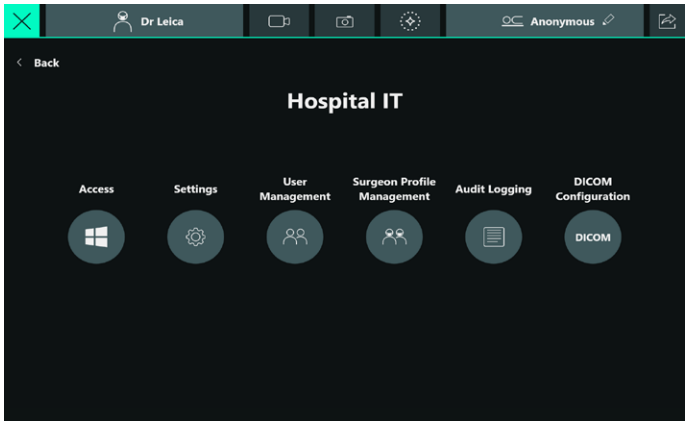


► Enter username and password, then select Confirm



4.2 Configuring ARveo 8/ARveo 8x Application Security Settings

► Authenticate as an IT User
► Select Settings from Hospital IT support page



► Configure selections from this page, any changes made will automatically apply

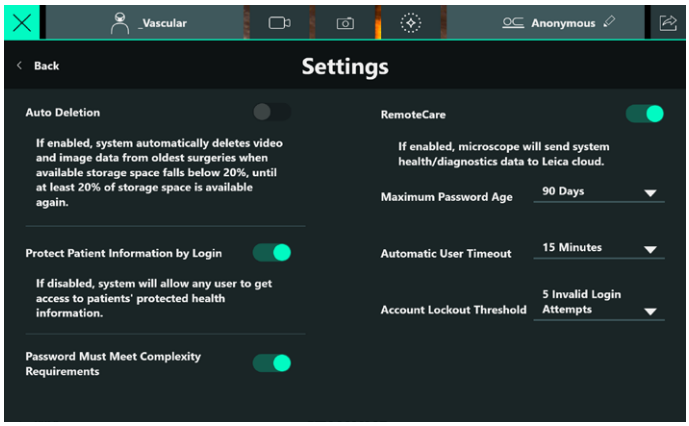
- Auto Deletion:
  Choose to enable or disable function to automatically delete oldest data from storage when available storage is less than critical percent of disk space.
- Protect Patient Information by Login:
  Choose to enable or disable function to require clinical users to authenticate with username and password prior to accessing or recording any patient health information.
- Password must meet complexity requirements:
  Choose to enable or disable function to require clinical user passwords to meet minimum password requirements: one uppercase, one lowercase, one numeric, one special character and a minimum of 10 characters.

When deactivating the password complexity requirements, passwords can be a single character which can cause severe data security issues:
- Clinical user accounts become vulnerable to attackers, which might lead to a leak of patient information.
- Hospital IT accounts become vulnerable and respective settings can be accessed and altered.
- Windows can be accessed by any user, using the elevated Windows access (see chapter 4.5) which allows to alter configuration, gather sensitive data and more.

- RemoteCare (enabled by default):
  Choose to enable or disable the RemoteCare connection. When enabled and the system is connected to the internet, microscope will send system health/diagnostics data to the Leica cloud.
- Maximum Password age:
  Choose frequency when clinical accounts passwords need to be changed or disable the feature.
- Automatic user timeout of user account after inactivity.

Deactivating the automatic user timeout can cause severe data security issues:
- Patient information can become available to any user of the microscope.
- Hospital IT menu can be accessed by any user and respective settings can be altered.
- Windows can be accessed by any user, using the elevated Windows access (see chapter 4.5 "Elevating Windows Access", page 10) which allows to alter configuration, gather sensitive data and more.

- Account lockout threshold:
  Select specified number of invalid logins attempts before lockout or disable the feature.



4.3 Configuring and Verifying DICOM Settings

DICOM functionality is a licensed feature that when purchased will be configured by Leica Microsystems' personnel at time of installation or at a subsequent service visit. The following instructions are provided for any cases where changes must be made after installation with Leica Microsystems' personnel supporting remotely rather than being on site. ARveo 8 and ARveo 8x allow the user to configure multiple DICOM nodes that may be used simultaneously for obtaining modality work list for the microscope and for storage of acquired data. The following settings are configured for each DICOM node that the ARveo 8 and ARveo 8x will connect:

Friendly Name – Name that microscope application uses to identify the node during export and communication reporting.

AE Title ¬– Application Entity Title of the DICOM node the microscope will connect. It is locally unique identifier that the node uses within DICOM messages to identify itself.

IP Address ¬– This is the network address of the DICOM node that ARveo 8 and ARveo 8x should use for establishing connection.

Port – This is the port on the DICOM node that will accept DICOM communications from ARveo 8 and ARveo 8x.

Microscope AE Title - Application Entity Title that ARveo 8 and ARveo 8x use to identify itself while communicating with this node. It must be a unique identifier that the node only uses when communicating with the microscope.

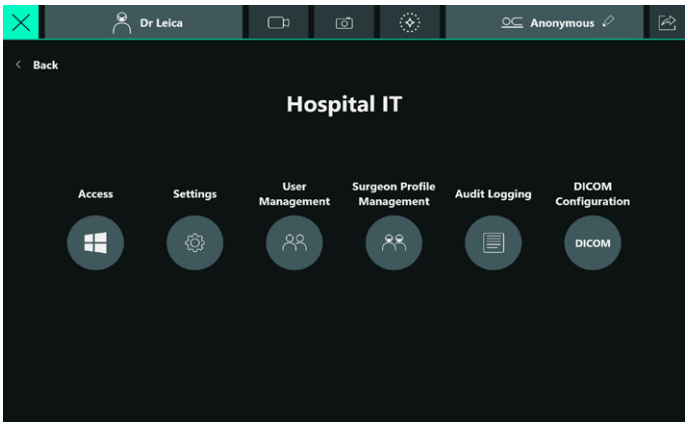
Connection Type – Setting to be configured depending on what the relationship between the DICOM node and ARveo 8 or ARveo 8x is. "Storage" identifies the node as a location where ARveo 8 and ARveo 8x should export data. "MWL" identifies the node as a location where ARveo 8 and ARveo 8x should get a modality work list of which patients are scheduled for the microscope. "MWL and Storage" identifies the node as being used for both purposes. "Inactive" means the node should not be used for DICOM communications.

Encryption – Select "TLS" if it is known that the node supports encrypted DICOM communications or if support is unknown. Select "Unencrypted" if encrypted DICOM communications are known to not be supported by the node. This support should be defined in the DCIOM conformance statement of the software that runs on the DICOM node.

Preferred Image Compression - Select "Compressed" if it is known that the node supports compressed JPEG DICOM syntax and storing compressed files to minimize space is preferred to storage of uncompressed images; otherwise select "Uncompressed." This support should be defined in the DCIOM conformance statement of the software that runs on the DICOM node.

Video Storage – Select which channel or channels of video should be exported when videos are selected for export: Left Channel; Right Channel or Left & Right Channel. Compressed MP4 is the only option for video export and must be supported by the DICOM node as defined in the conformance statement of the DICOM node.

- ▶ Authenticate as an IT User
- ▶ Select DICOM Configuration



4.3.1 Verify Node Status – verify that the ARveo 8 / ARveo 8x can communicate with the node

- ▶ Select Check mark icon under verify column in the row of the node to be tested



- ▶ Wait for Verification Status to populate with results. "Success" in the Verification Status column indicates the node is active and ARveo 8 and ARveo 8x can communicate with that node. Failure may require confirming network connection, adjusting DICOM node or adjusting network settings.

4.3.2 Edit Existing Node

- Select pencil icon under “Edit” column in the row of the node to be edited



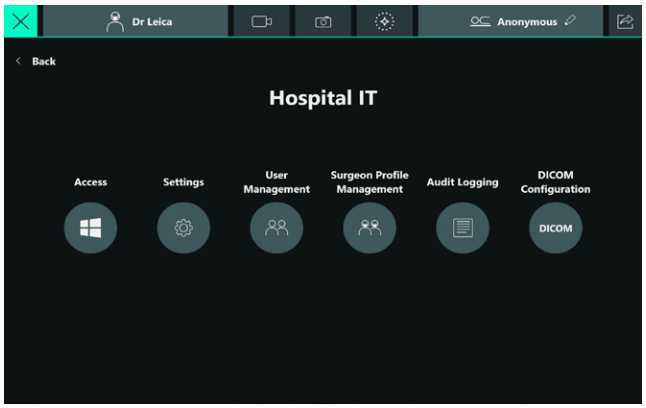
- Modify the setting that need to be changed.
- When changes are complete, select “Verify DICOM Connection” to confirm that the information edited is correct and results in ARveo 8 or ARveo 8x communicating with the node
- Select “Save” to save the changes for the node
- At any time, select “Back” to discard the changes

4.3.3 Create a New DICOM Node

- Select “+ Create New” which launches same view as edit with all fields empty
- Modify the setting that need to be changed.
- When changes are complete, select “Verify DICOM Connection” to confirm that the information edited is correct and results in ARveo 8 or ARveo 8x communicating with the node
- Select “Save” to save the changes for the node
- At any time, select “Back” to discard the changes

4.4 Running Audit Report

- Insert trusted USB into ARveo 8 or ARveo 8x USB connector for use as a location to export the audit log
- Authenticate as an IT User
- Select Audit Logging



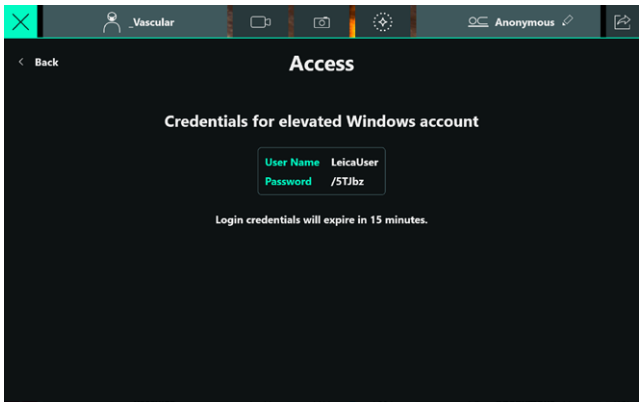
- Configure extent of dates that the report will report auditable events
  - Adjust From and To fields to set range of dates
  - Select “Today” to get today’s events
  - Select “Since Last Week” to get events from last 7 days



- Choose “Select Target” to choose where to send report
- Remove USB and review exported audit log on a secure computer

4.5 Elevating Windows Access

- ► Authenticate as an IT User
- ► Select Access and record credentials for Windows login use



- ► Insert USB keyboard, Enter Control + Alt +Delete, Select switch user
- ► Select LeicaUser as User and enter credentials recorded in prior step
- ► Windows launches with Command Shell viewable

NOTE

Elevated credentials are only valid for 15 minutes. After that duration the system must be restarted for elevate access again as the credentials have been changed.

NOTE

After elevating Windows access and completing the necessary changes, user should cycle power to the microscope to return to microscope application

4.6 Resetting User Password

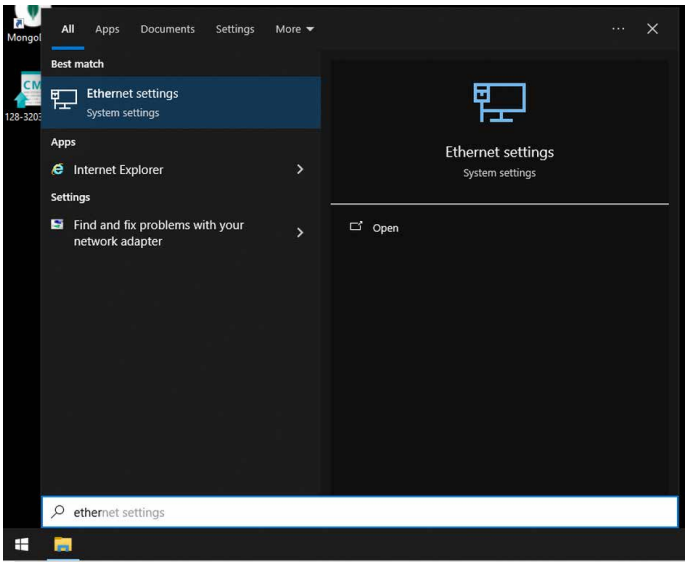
If an IT user needs their password reset, a secondary IT user or Leica Microsystems Service Associate may login and reset the password of the IT user who needs a password reset. The following procedure documents how to do reset the password of IT users.

- ► Follow procedure to authenticate as an IT User
- ► Connect USB keyboard with trackpad to the ARveo 8 or ARveo 8x USB ports
- ► Follow procedure to Elevate Windows Access
- ► Select the Command Shell, confirm that shell is open to directory C:\Program Files\LMSMedical\ARveo8 by looking at the prompt
- ► If the shell is not open in the directory enter cd "C:\Program Files\LMSMedical\ARveo8"
- ► Enter Run "UserAccountReset.exe".
- ► Follow the software prompt and enter the user account that is being reset.
- ► Cycle power on the microscope

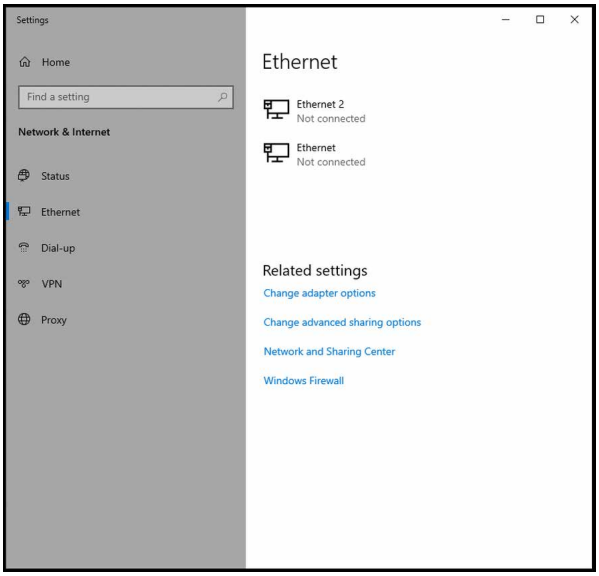
4.7 Configuring ARveo 8 /ARveo 8x Network Settings

ARveo 8 and ARveo 8x Ethernet settings are configured by default to obtain the TCP/IP settings automatically. It is preferred that any changes to connections that are needed are made on the network hardware (switch/router); the following instructions are provided for any cases where that is not possible and network configuration changes must be made on the microscope.

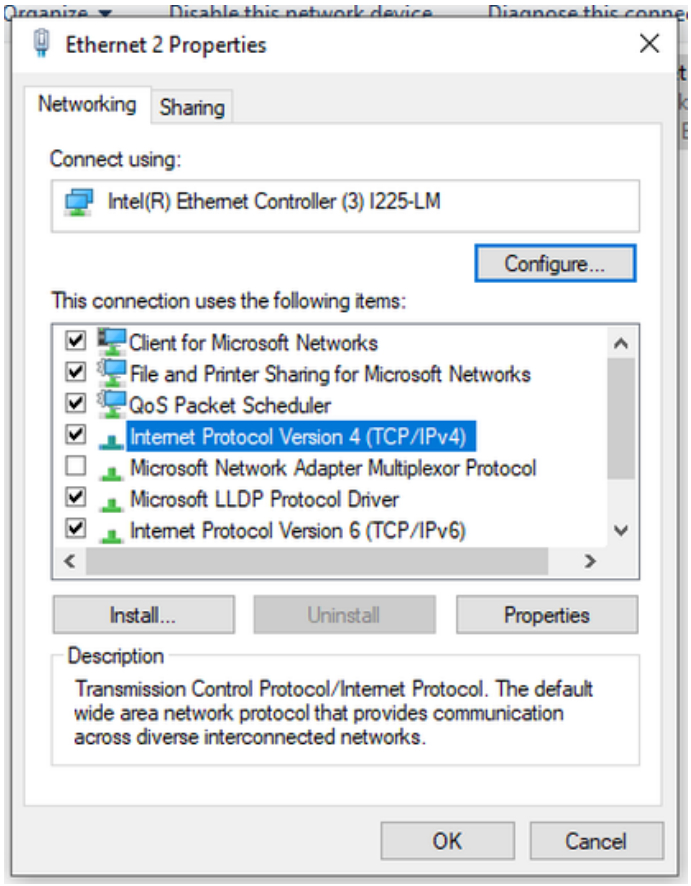
- ► Follow procedure to authenticate as an IT User
- ► Connect USB keyboard with trackpad to an ARveo 8 or ARveo 8x USB port
- ► Follow procedure to Elevate Windows Access
- ► Select the Command Shell and enter "C:"
- ► Enter "Explorer.exe". This will open standard Windows 10 operating system access.
- ► Enter Windows + S buttons to launch search then type Ethernet and select "Ethernet Settings"



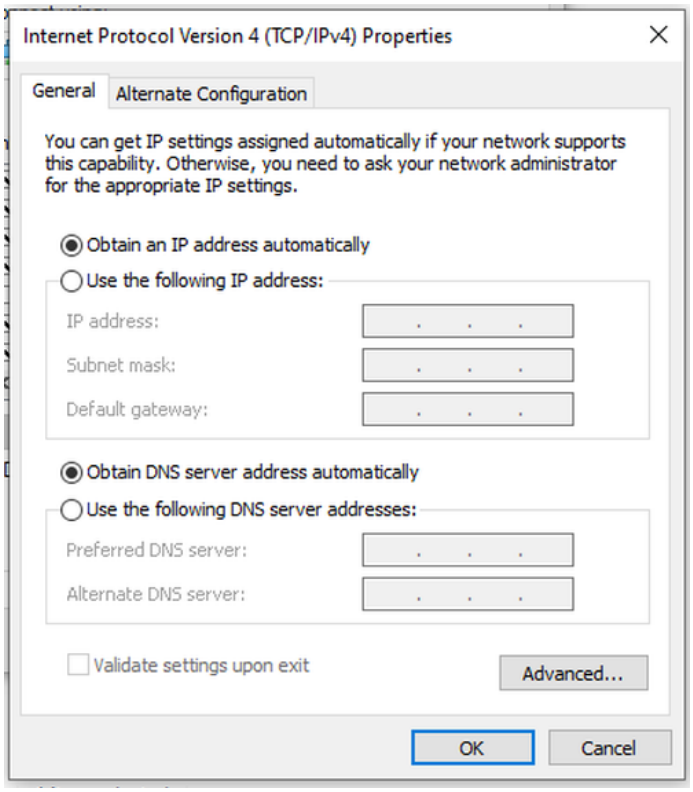
- ► Select "Change adapter options"

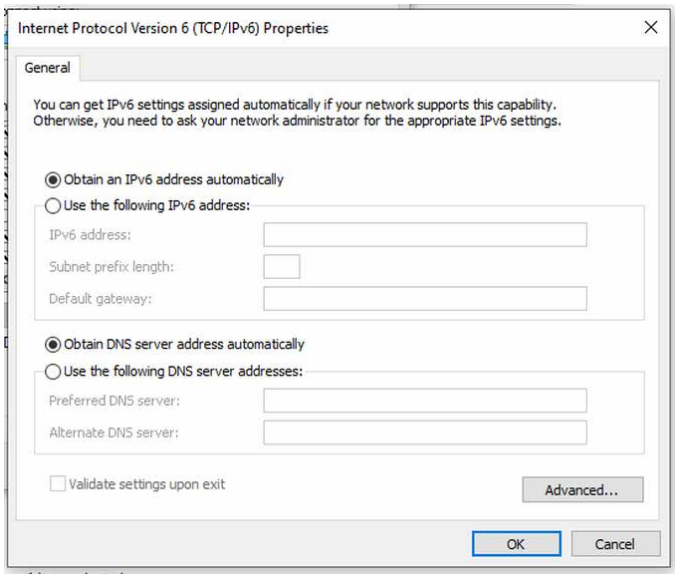


- ► Highlight the Internet protocol version that is being used and select properties

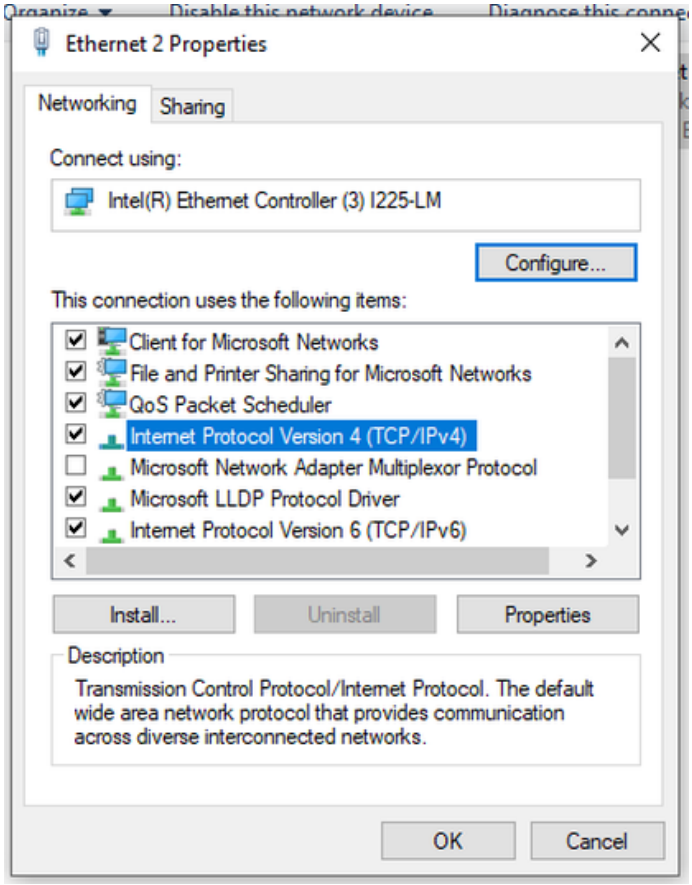


► Make needed changes to IP, DNS, and subnet settings as required by institution.





► Before exiting the Ethernet Properties window, confirm that the protocol version has a check mark and then select “OK”



► Cycle power on the microscope

5 Software Updates

At Leica Microsystems, we develop products that help our customers to gain new insights. Insights that help to advance science, patient outcome, and gain insights for key questions concerning research, development, and engineering. To achieve this, we uphold core values that define our responsibility to those we serve. Among them are an unwavering commitment to the safety and security of our instruments and services. In response to potential threats to cybersecurity, Leica Microsystems is continually assessing vulnerabilities and determining responses. As part of the response, it is expected that microscope application software, operating system, antivirus definition files, and additional on product software will be regularly updated. For critical security vulnerabilities, Leica Microsystems will contact our customers and communicate the vulnerability, available short-term mitigations and when available provide the security update for installation. For non-critical security vulnerabilities, Leica will accumulate these changes into our patch release cycle and make them available at next scheduled service visit or upon customer request. In order to notify customers of these updates, it is important that we have accurate contact information for your institution. If the contact of record from your institution departs, please contact Leica Microsystem so we may update your contact information.

6 Cybersecurity Incident Reporting

Potential security vulnerabilities or privacy issues with a Leica Microsystems product should be reported to local Leica Microsystems customer service representatives. We ask that you please refrain from including sensitive information (e.g., PHI, PII, etc.) as a part of any submissions to Leica Microsystems. Please provide the following information in your submission:

- 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
- Results or impact

This incident report will be handled through Leica Microsystems Complaint Handling process. This includes investigating the incident or concern and determining corrective and preventative actions where needed and communicating those finding with the impacted customers.

10 747 996 –04–en · © 2024 by Leica Microsystems (Schweiz) AG
Subject to modifications. LEICA and the Leica logo are registered trademarks of Leica Microsystems IR GmbH.

Leica Microsystems (Schweiz) AG · Max-Schmidheiny-Strasse 201 · CH-9435 Heerbrugg
T +41 71 726 3333

www.leica-microsystems.com

CONNECT
WITH US!