

From Eye to Insight



PROVEO 8x

Cybersecurity Manual

10 735 164 version 02

Date of issue: 2026-08-04

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
9435 Heerbrugg, Switzerland

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	3
1.1	Purpose	3
1.2	Symbols in this user manual	3
2	PROVEO 8x – Purpose and requirements of networked connections	3
3	Cybersecurity controls	5
4	Advanced feature configuration and use for IT users	8
4.1	Authenticating as an IT user	8
4.2	Configuring PROVEO 8x application security settings	9
4.3	Configuring and verifying DICOM settings	10
4.4	Running audit report	11
4.5	Elevating Windows access	12
4.6	Update system date and time	12
4.7	Resetting user password	13
4.8	Generating license request and installing license updates	13
5	Software updates	17
6	Cybersecurity incident reporting	17

1 Introduction

1.1 Purpose

This user manual documents the purpose of connecting PROVEO 8x to network and other hospital equipment; define the set of cybersecurity controls used to secure the Leica Microsystems PROVEO 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 PROVEO 8x – Purpose and requirements of networked connections

PROVEO 8x is intended to be used within 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: it supports data transfer to DICOM nodes; 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. Connections to 3rd party equipment in the operating room are connected by ethernet connections for data communications using IEEE 11073 Service-oriented Device Connectivity (SDC) protocol.

Networked data connections are supported by a wired 1Gbase-T 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 1 Gbit/s bandwidth connection; 100Mbps is enough for reasonable speed of data transfer.

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, PNG) and videos (MP4) with the scheduled patient prior and create a DICOM standard file (DCM) to export to a DICOM node. DICOM connections are made using the networked connections described above. The system supports the use of TLS 1.1 and 1.2 for encrypted communications over this network when the hospital supports the use of TLS encryption.

The DICOM connection attempts to use encrypted communications by default; however, when using encrypted communications, it is up to the external (to the system) DICOM node to dictate whether TLS 1.1 or 1.2 will be used.

**CAUTION**

The use of unencrypted 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. The use of encrypted communications is strongly recommended. Furthermore, because TLS 1.1 has known security vulnerabilities, it is strongly recommended that the external (to the system) DICOM nodes to be configured to use TLS 1.2 instead of 1.1, which, as described above, will allow the system to communicate with the highest security possible.

PROVEO 8x provides an export capability to copy images (JPG, PNG) and videos (MP4) to the external media. The external media is treated as a USB mass storage device class (MDC). 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 PROVEO 8x 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 microscope data to authorized service personnel, facilitating diagnostics and support:

- System Component Hardware Versions
- System Component Software Versions
- Which brakes are enabled in selected brakes
- Accessories Enabled/Disabled (AutoReset, Keratoscope, OCT)
- System Errors reported in the Issue List
- Lamp Accumulated hours main
- Lamp Accumulated hours Red-reflex
- Empty hard drive space
- USB Device Connected

It is important to note that patient data will not be collected through this process.

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 provide incoming and outgoing internet access through firewalls on the Hospital network.

PROVEO 8x provides a connection to 3rd party equipment in the operating room using a 1Gbase-T ethernet connection. This connection is configured to use a static IP to enable a device to communicate. The 3rd party equipment is sending the PROVEO 8x parameter information (modes and level settings) to include in the display. The communication between the device uses IEEE 11073 Service-oriented Device Connectivity (SDC) protocol. The protocol relies on certificates generated and signed by a trusted root, and a private key used for encryption. Each PROVEO 8x microscope has a certificate and private key generated and signed by a trusted root during manufacturing. The trusted root needs to be identified as an accepted trusted root on the certificate store of the 3rd party device prior to connection. The SDC library uses TLS 1.1 for secure communications over Port 3702 UDP for discovery and 5555 UDP for data streaming.

NOTE

The use of TLS 1.1 in this environment, even with known vulnerabilities in the TLS 1.1 protocol, has acceptably low enough risk because the environment is limited to 1-to-1 connections within the scope of the operating room, and no sensitive or private data is communicated (as stated above, only parameter information - modes and level settings are communicated).

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:

PROVEO 8x users interact with the system configured with minimum permissions. Authenticated clinical users, Leica users, and unauthenticated users cannot use any Windows OS functions and may only run the PROVEO 8x 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:

PROVEO 8x runs Windows 10 LTSC with all unnecessary services and port access disabled. PROVEO 8x application runs in a shell launched to run the system as a kiosk device.

Operating System Runtime Restrictions:

PROVEO 8x is configured with Windows Firewall and Windows AppLocker actively running to limit what software may execute. This includes disabling Autorun functionality of USB ports; restricting the execution of unsigned software; restricting the location from which software may launch its execution.

Real-time Threat Protection:

PROVEO 8x is configured with Windows Defender activated providing real time protection against viruses and malware.

Encryption Measures:

All information stored on the hard disc of the PROVEO 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 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 PROVEO 8x application uses private cryptographic keys stored securely on a Trusted Platform Module (TPM). The TPM is a standalone 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 PROVEO 8x is encrypted prior to storage and decrypted for presentation to the user.

User Management:

PROVEO 8x has implemented three user types for user operations and one 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, retrieve 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:

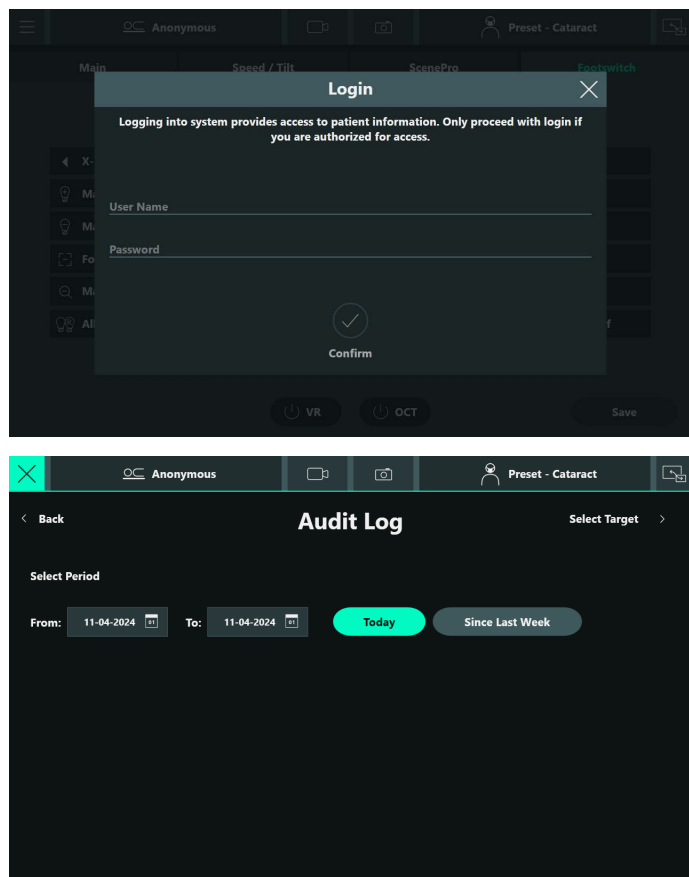
Leica Microsystems has two specialized accounts, Sales and Service, which allow Leica representatives system access to configure and troubleshoot the system. These accounts are only accessible by Leica Microsystems and are active for a predefined lifetime and are traceable to individual associates. These 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. Usernames are expected to be unique to individuals to enable auditing to allow events to be traced to specific users.

Access Notification:

PROVEO 8x notifies users when they would have access to patient information. The PROVEO 8x 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:**

PROVEO 8x is configured to use Transport Layer Security (TLS) for encrypting data that is exported over Ethernet. For DICOM communications, encrypted communications are selected by default. If the DICOM nodes that PROVEO 8x connects to accept only unencrypted data transport, the system may be configured to allow unencrypted DICOM syntaxes.

Secure Coding Practices:

PROVEO 8x 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 an 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. If the system detects that the digital signatures are either missing or incorrect, the application will not be launched. 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:

PROVEO 8x is configured prior to shipment to mitigate concerns of tampering during shipment from Leica Microsystems facilities. Tamper evident tape is used on the crate to ensure the microscope is not accessed during shipment without Leica Microsystems personnel being aware at installation.

Audit Logging:

PROVEO 8x provides facility customer 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 or network 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

- Auto delete option updated
- Deleting patient data file
- Initiating auto-delete
- 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
- System settings saving
- Firmware updates
- Factory and data reset
- Delete surgeon profiles
- Update user password

Secure by Default:

PROVEO 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:

- Require 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. Generic username and custom password.
- Require clinical user's passwords to meet 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.

Remote Access Restrictions:

To enhance security and prevent unauthorized access, remote access to the system will not be supported. This measure is implemented to mitigate the risk of remote attacks and unauthorized intrusion attempts.

EULA and Data Privacy Notice:

To access the application, users must first accept the End User License Agreement (EULA) and Data Privacy Notice. Acceptance of these agreements is mandatory to proceed and use the application's features. The EULA and Data Privacy Notice can be accessed at any time in the application.

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 to be authenticated as an IT user before proceeding with the instructions.



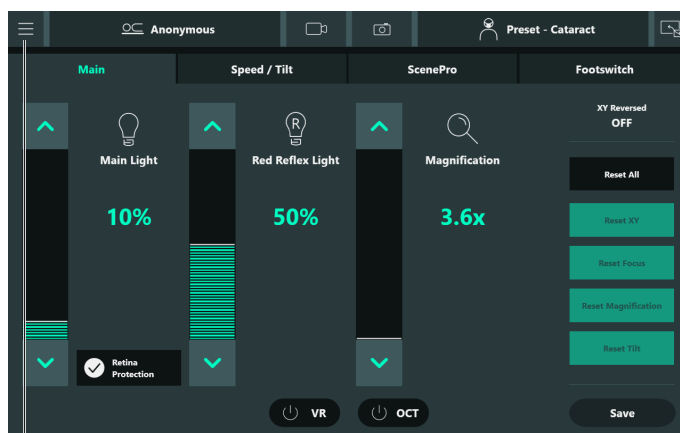
CAUTION

Risks Due to Changing Microscope Configuration

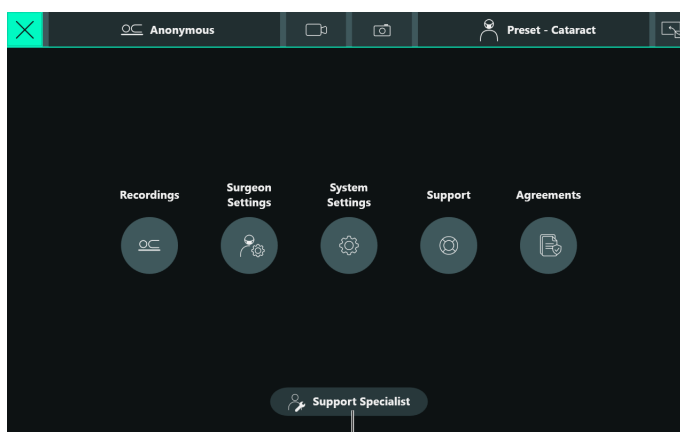
Once the configuration that control potential cybersecurity risks is established, take care not to change the configuration without assessing the potential risk impact. These changes would include but are not limited to network configuration changes, connection of additional items to the microscope,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

4.1 Authenticating as an IT user

► Select the Main Menu (1) and navigate to Options.



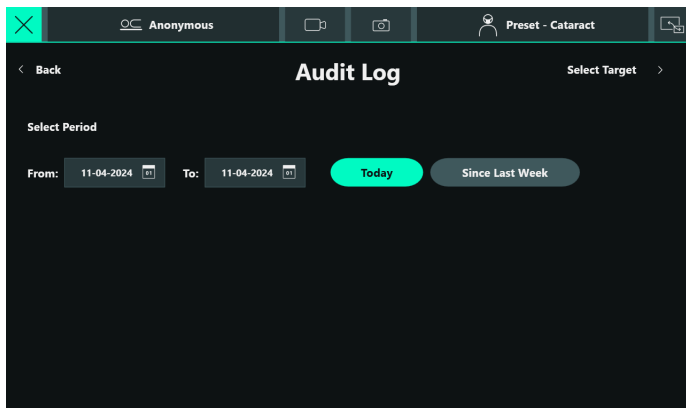
► Select Support Specialist (2).



► Select Hospital IT.



- Enter username and password, then select Confirm

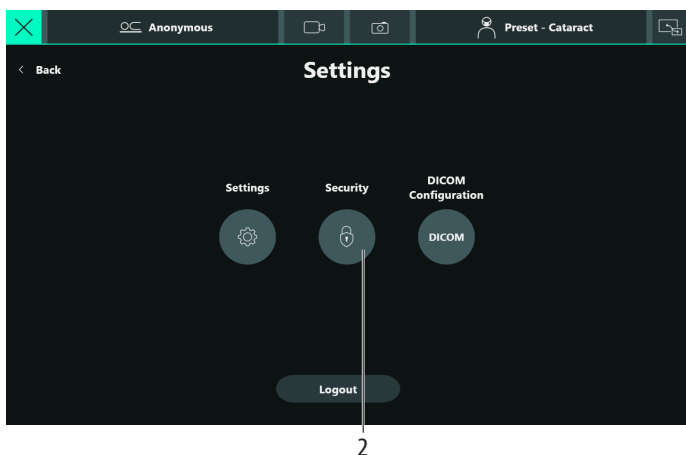


4.2 Configuring PROVEO 8x application security settings

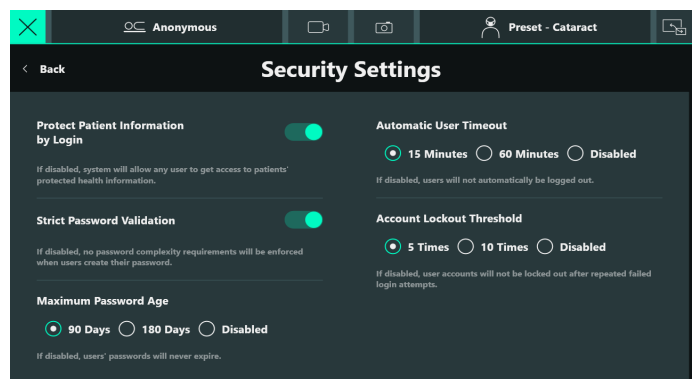
- Authenticate as an IT User
- Select Settings (1) from Hospital IT support page



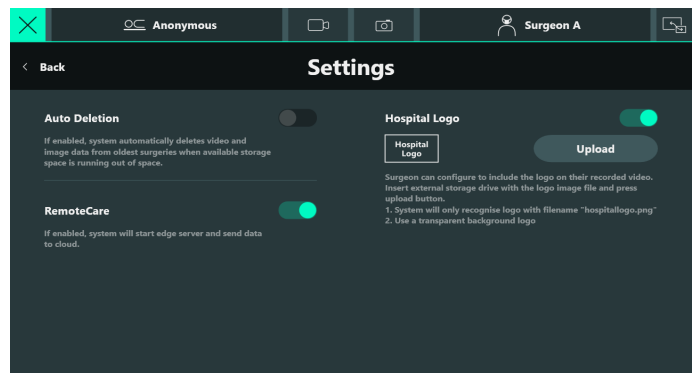
- Select Security (2) from Hospital IT – Settings Page



- Configure selections from this page, any changes made will automatically apply
- 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.
- Strict Password Validation: 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.
- 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.
- Account Lockout Threshold: Select specified number of invalid logins attempts before lockout or disable the feature.



- Select Settings from Hospital IT – Settings Page



- Auto Deletion: Choose to enable or disable function to automatically delete video and image data from the oldest surgeries when available storage space is running out of space. Be aware that this setting affects data from all patients performed by all surgeons for all future surgeries.
- RemoteCare: Choose to enable or disable function to send system information to Leica data server.
- Hospital Logo: Choose to enable or disable display of hospital logo on screen. This will overwrite surgeon profile – media settings to display hospital logo on screen and recording.

4.3 Configuring and verifying DICOM settings

PROVEO 8x DICOM functionality is a licensed feature that when purchased will be configured by Leica Microsystems 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. PROVEO 8x allows 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 PROVEO 8x will connect:

Friendly Name – Name that PROVEO 8x 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 PROVEO 8x should use for establishing connection.

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

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

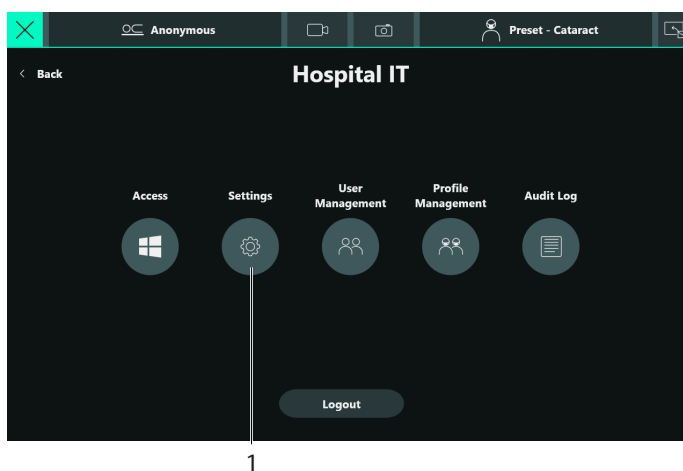
Connection Type – Setting to be configured depending on what the relationship between the DICOM node and PROVEO 8x is. "Storage" identifies the node as a location where PROVEO 8x should export data. "MWL" identifies the node as a location where PROVEO 8x should get a modality work list of which patients 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 DICOM conformance statement of the software that runs on the DICOM node.

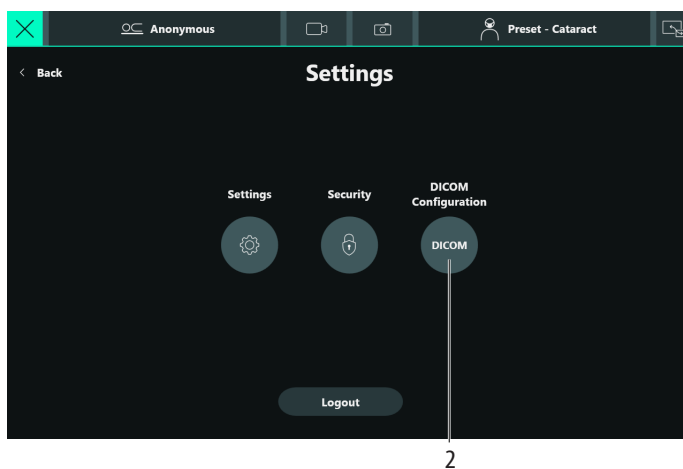
Preferred Image Compression – Select "Compressed" if it is known that the node supports compressed JPEG DICOM syntax and storing compressed files to minimize space is preferred to storage of uncompressed images; otherwise select "Uncompressed." This support should be defined in the DICOM conformance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

Video Storage – Select the default "Left & Right Channel" option which works on both 3D IVC and 2D IVC systems. 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 Settings (1)

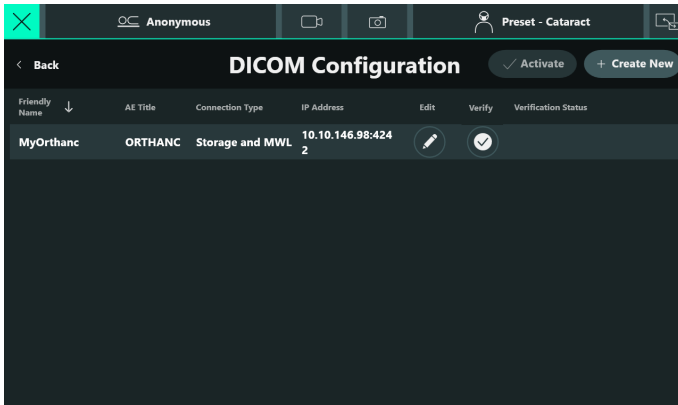


- ▶ Select DICOM Configuration (2) from Hospital IT – Settings page



4.3.1 Verify node status – verify that the PROVEO 8x can communicate with the node

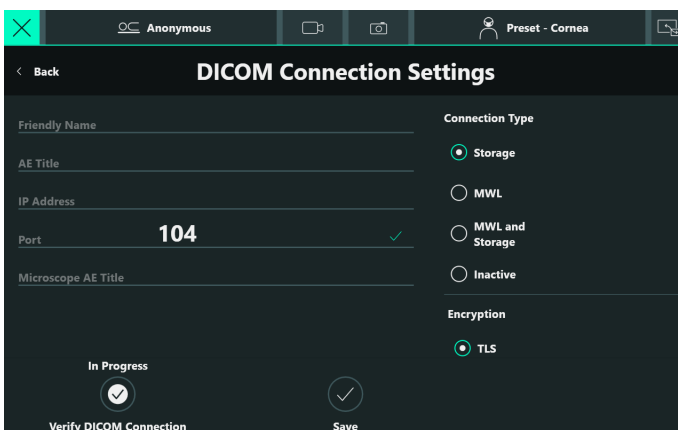
- ▶ Select checkmark icon under the Verify column in the row of the node to be tested



- ▶ Wait for Verification Status to populate with results. "Success" in the Verification Status column indicates the node is active and PROVEO 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 needs to be changed, page has additional option that may be selected by scrolling down
- ▶ When changes are complete, select "Verify DICOM Connection" to confirm that the information edited is correct and results in PROVEO 8x communicating with the node
- ▶ Select "Save" to save the changes for the node
- ▶ At any time, select "Back" to discard the changes

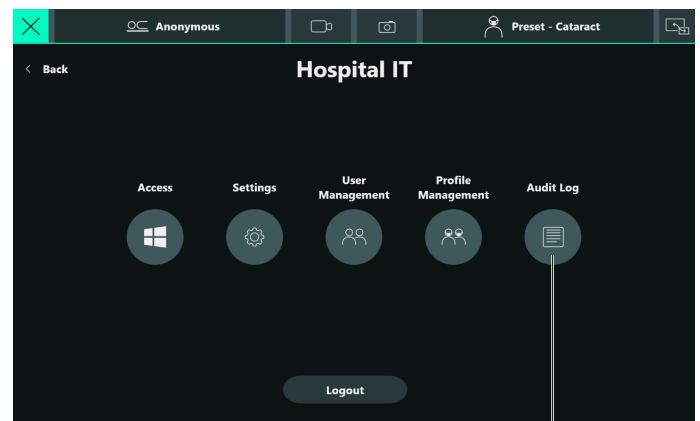


4.3.3 Create a new DICOM node

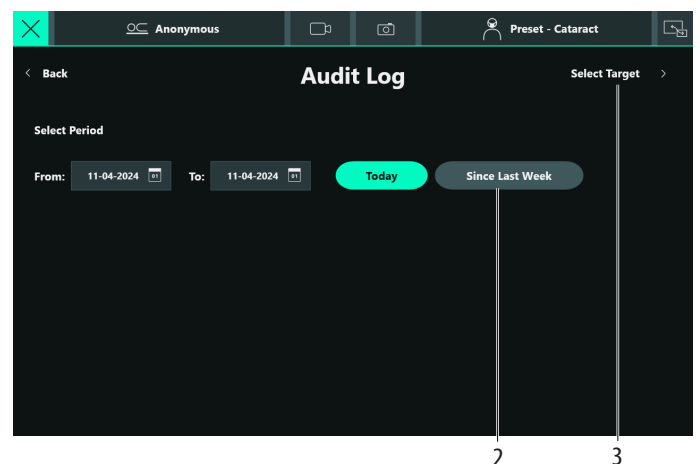
- ▶ Select "+ Create New" which launches same view as edit with all fields empty
- ▶ Modify the setting that needs to be changed, page has additional option that may be selected by scrolling down
- ▶ When changes are complete, select "Verify DICOM Connection" to confirm that the information edited is correct and results in PROVEO 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

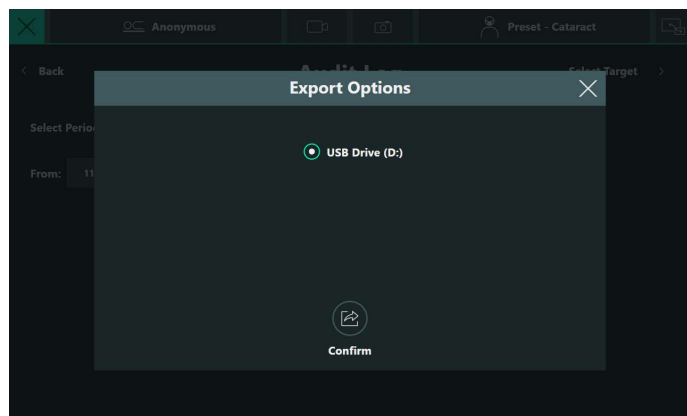
- ▶ Insert trusted USB into PROVEO 8x USB connector for use as a location to export the audit log
- ▶ Authenticate as an IT User
- ▶ Select Audit Log (1)



- ▶ Configure the date range for the audit log report to be exported
 - Adjust From and To fields to set range of dates
 - Select "Today" to get today's events
 - Select "Since Last Week" (2) to get events from last 7 days



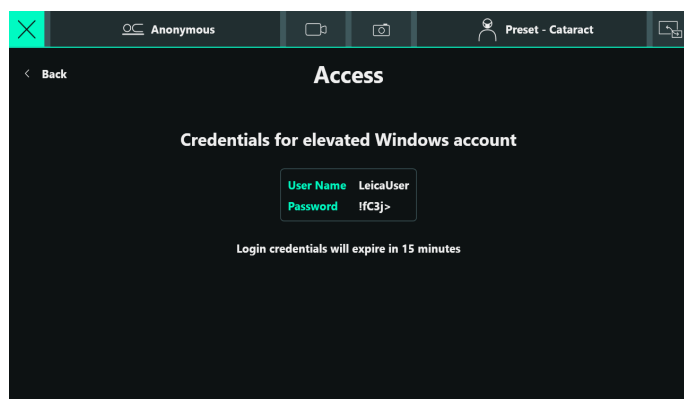
- ▶ Click "Select Target" (3) to choose where to send report
- ▶ In the pop-up window, click "Confirm" to export the log files



- ▶ Remove USB and review exported audit log on a secure computer

4.5 Elevating Windows access

- ▶ Authenticate as Hospital IT
- ▶ Select Access and record credentials for Windows login use



- ▶ Insert USB keyboard
- ▶ Enter CTRL + ALT + DEL on the keyboard, then press "Sign Out" on the screen
- ▶ 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, user must restart system and elevate access again as the credentials have been changed.

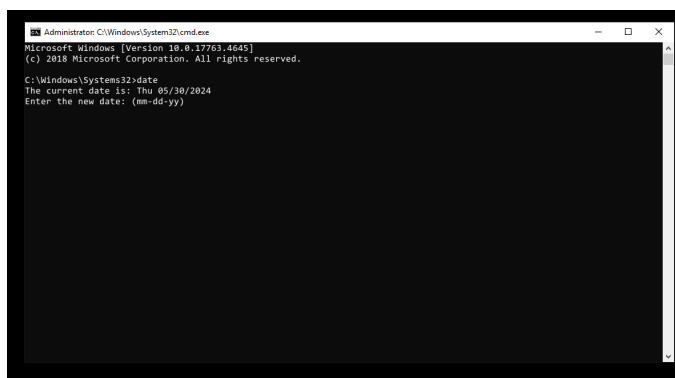
NOTE

After elevating Windows access and completing the necessary changes, user should power cycle the microscope to return to PRO-VEO 8x application.

4.6 Update system date and time

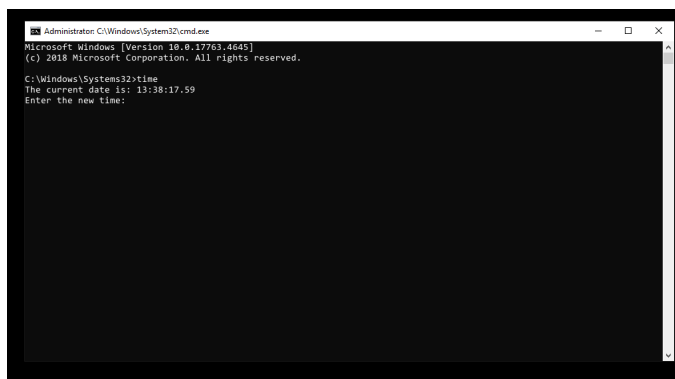
To update system date, in the command prompt type:

- a) date and press Enter
- b) type the date and press Enter (to change the date)



To update system time, in the command prompt type:

- a) time and press Enter
- b) type the time and press Enter (to change the date)



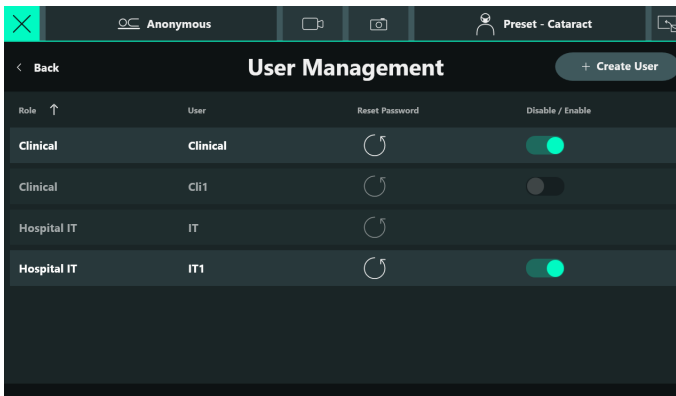
Power cycle the microscope to return to PROVEO 8x application.

4.7 Resetting user password

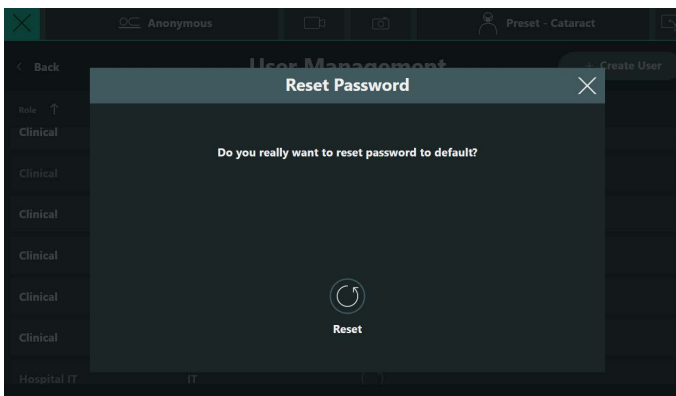
If a clinical or IT user forgets the password or the system has been disabled because incorrect passwords have been entered too many times, the Hospital IT user can reset this password.

Exception: Users who have been deactivated cannot have their password reset.

- ▶ Tap the reset password icon of the respective user



- ▶ Tap the reset icon



- ▶ The password reset is confirmed

NOTE

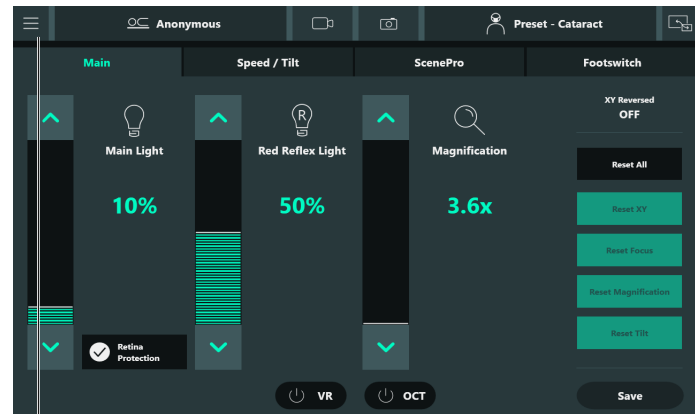
It is recommended to designate a secondary IT user as a backup in the event that the primary IT user forgets the password.

4.8 Generating license request and installing license updates

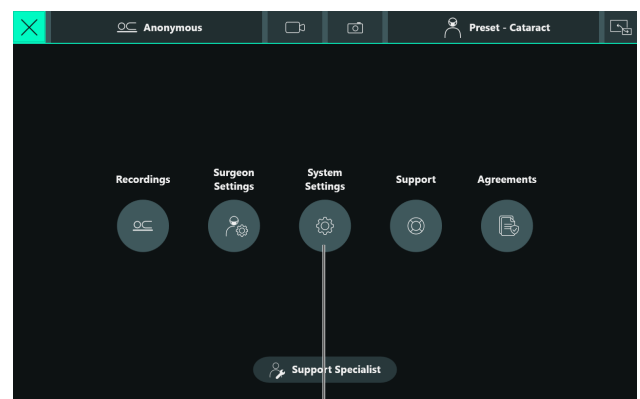
PROVEO 8x is configured with purchased licenses by Leica Microsystems at time of installation or at a subsequent service visit.

4.8.1 Installing license

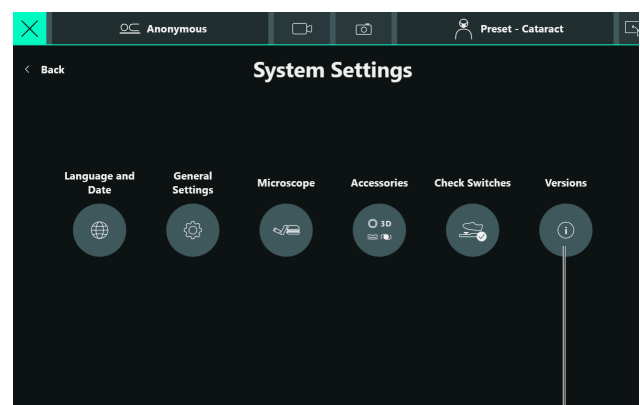
- ▶ Connect USB drive with the license to the PROVEO 8x USB port
- ▶ Click Menu (1)



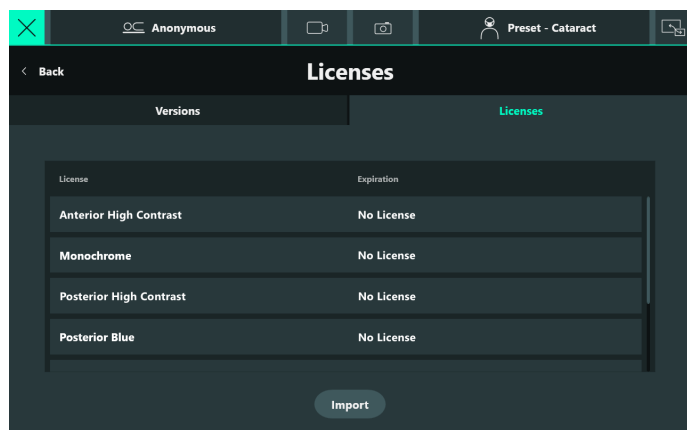
- ▶ Click "System Settings" (2)



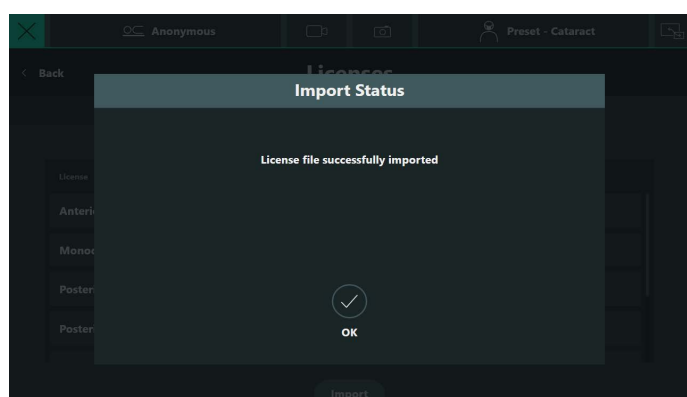
- ▶ Click "Versions" (3)



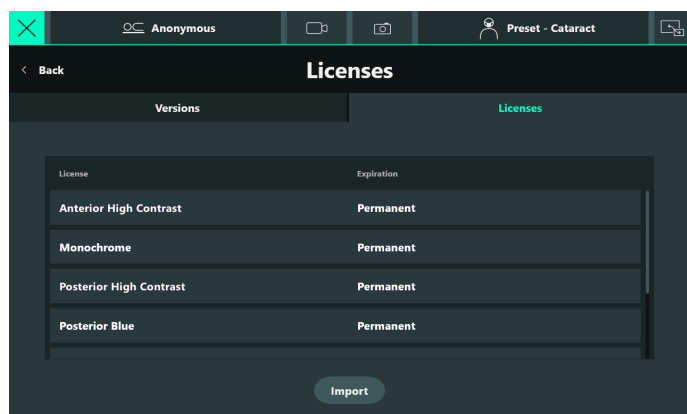
- Select "Licenses" tab and click "Import"



- Click "OK"



- Check the expected licenses are activated accordingly

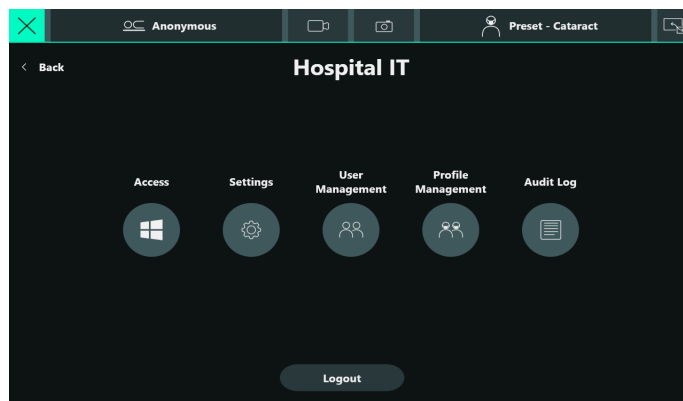


User Management

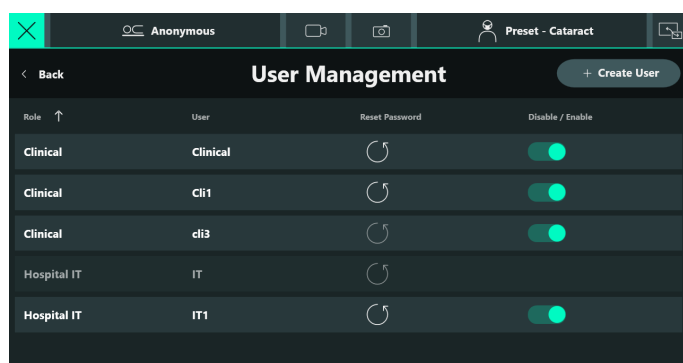
If a user forgets the password or the system has been disabled because incorrect passwords have been entered too many times, the "Hospital IT" user can reset this password. Hospital IT user can also enable/disable accounts and create accounts as needed (also see user manual of Leica surgical microscope).

Exception: Users who have been disabled cannot have their password reset until enabled.

- Authenticate as an IT User and enter Hospital IT Support
- Select "User Management"



- IT user may reset password, enable/disable users or create users

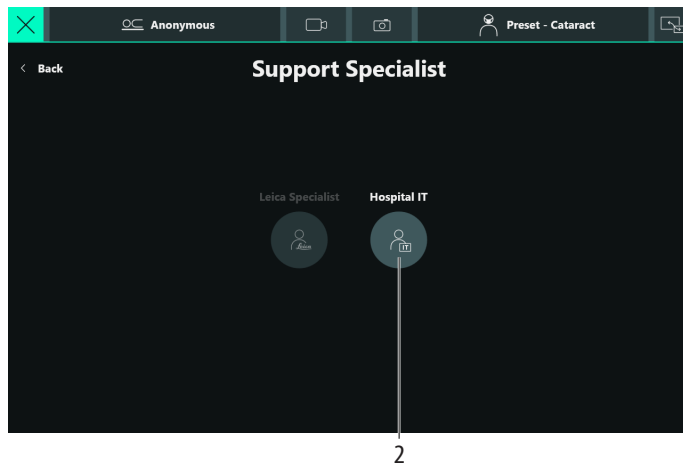
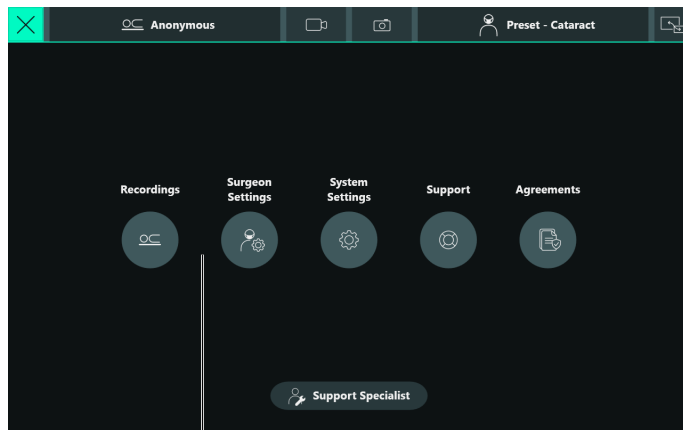


Account Creation

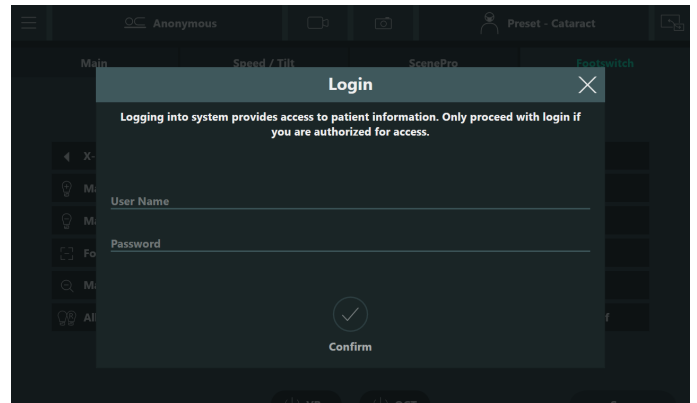
First time logging onto system default accounts

PROVEO 8x is delivered with a single use, default clinical user and hospital IT user account. Your Leica support specialist will provide you with the initial password for each account (Clinical and IT). After entering the default password you will be asked to change the password for the default account and to create a personalized account to proceed with accessing those features (also see user manual of Leica surgical microscope).

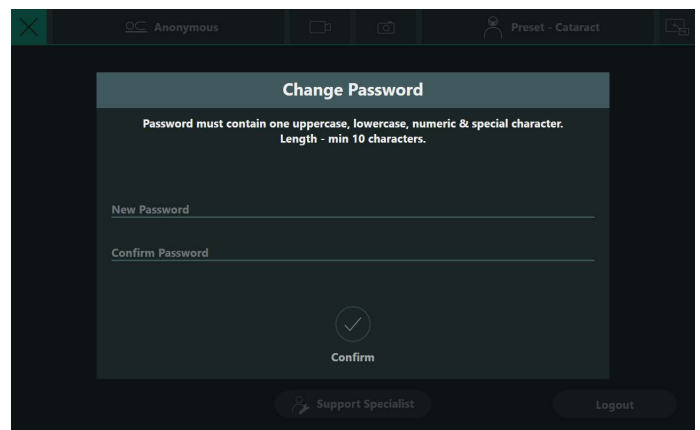
- Attempt to access material restricted to basic user; for clinical selected recording (1) or select Hospital IT (2) under Support Specialist for Hospital IT



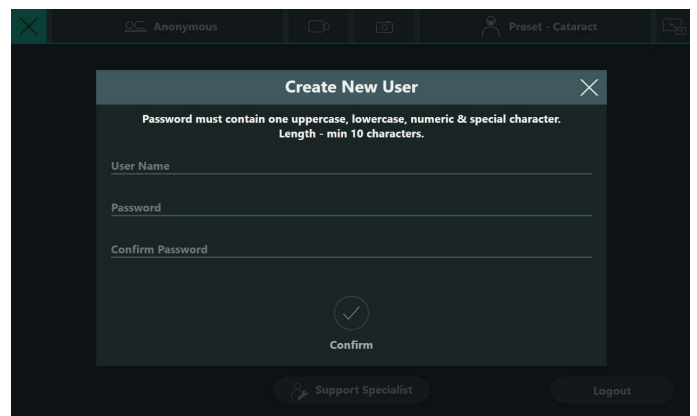
- Enter default username and password, then select Confirm



- Enter new password for default account (this password becomes the local password for this default account)



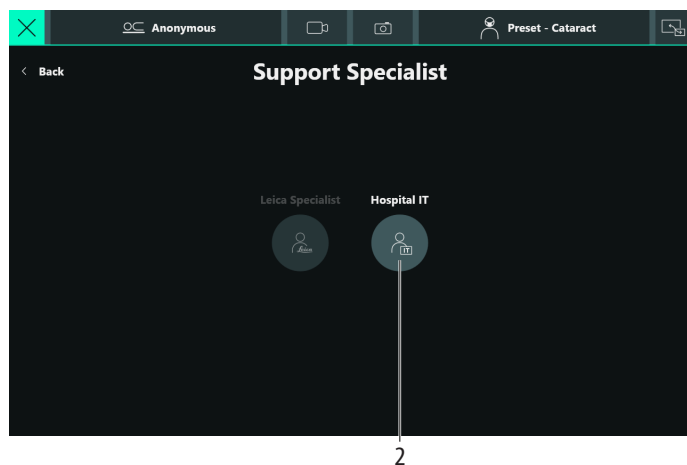
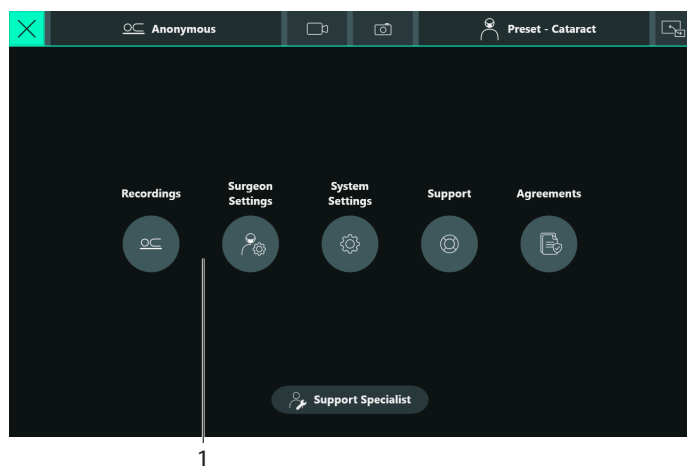
- Enter a personalized username and password. This is the username and password that you should use when personally working with the system. Do not share this username or password



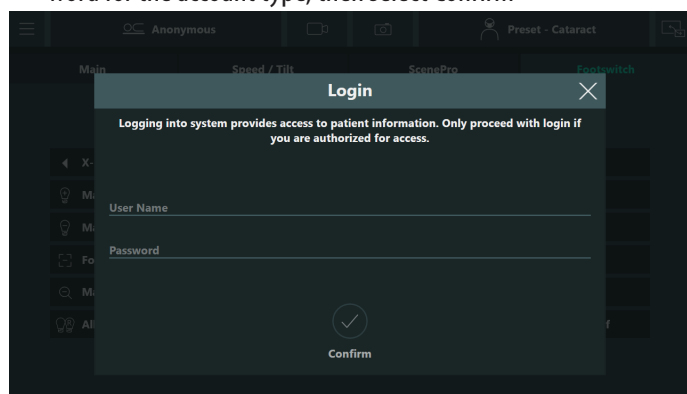
Account Creation After Initial Change of Default Account

Once the default password for the default user account has been changed, using the default account with the locally specified password will provide a means for generating new accounts of that class (clinical or hospital IT) (also see user manual of Leica surgical microscope).

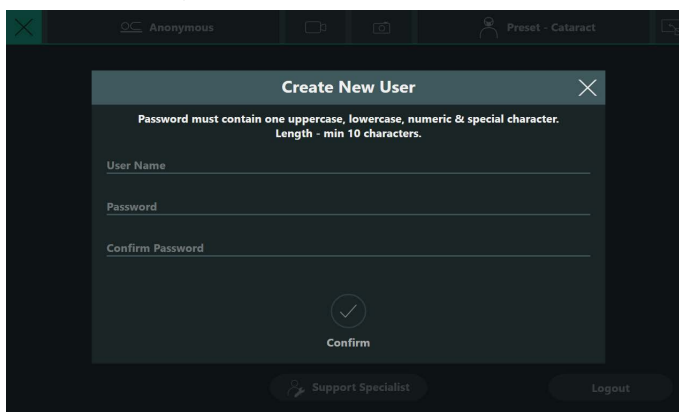
- Attempt to access material restricted to basic user; for clinical selected recording (1) or select Hospital IT (2) under Support Specialist for Hospital IT



- Enter default username (clinical or IT) and local account password for the account type, then select Confirm



- Enter a personalized username and password. This is the username and password that you should use when personally working with the system. Do not share this username or password



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 PROVEO 8x 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 findings with the impacted customers.



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

www.leica-microsystems.com

CONNECT
WITH US!

