

BAUSCH + LOMB

Bausch + Lomb **Stellaris Elite™** vision enhancement system
with **eyeTELLIGENCE™**



BL11145, BL14455, and BL15455



Medical Device Cybersecurity Manual

Risk Tier: **Tier 1 “Higher Cybersecurity Risk”**
Document Version: 1
Rev. 2021-03
4151600



Bausch & Lomb Incorporated
1400 North Goodman Street
Rochester, NY 14609 USA

<https://www.bausch.com/ecp>

Bausch + Lomb Stellaris Elite vision enhancement system Medical Device Cyber Security Manual

®/TM are trademarks of Bausch & Lomb Incorporated or its affiliates.

© 2021 Bausch & Lomb Incorporated or its affiliates
This document may not be reproduced or distributed.

Table of Contents

Table of Contents	ii
List of Tables	ii
List of Figures	ii

1. Introduction.....	3
1.1. Purpose	3
1.2. Background	3
1.3. Document Organization	3
1.4. Acronyms	3
2. Device Overview.....	4
2.1. Device Specification	5
2.2. Intended Use	6
2.3. Device Security Functionality	6
2.4. Backup and Restore	6
2.5. Infrastructure Requirements	6
2.6. Configuration Settings	7
2.7. Device Ports and Interfaces	7
2.8. Roles and Services	8
2.8.1. Roles	8
2.8.2. Services	9
2.9. Identification Procedures	9
2.10. Device Security Response	9
2.11. Device Intrusion Detection/Evidence	9
2.12. Device Recovery	9
2.13. Device Component List [CBOM]	10
2.14. External Operating Environment Components	13
2.15. Deployment Instructions	13
2.16. Residual Risk Disclosure	13
2.17. Terms of Support	13
3. Secure Operation	14
3.1. Initialization	14
3.2. Maintenance Guidance	14
3.3. User Guidance	14

List of Tables

Table 1 - Acronym Definitions	3
Table 2 - Module Interface Mappings	8
Table 3 - Unauthenticated Services	9

List of Figures

Figure 1 - Physical Diagram	5
Figure 2 - Functional Block Diagram	5

1. Introduction

1.1. Purpose

This Cybersecurity Manual for the **Stellaris Elite™** vision enhancement system by Bausch + Lomb with **eyeTELLIGENCE™** describes how the device meets the security recommendations of the FDA Premarket Recommendations for cybersecurity, the MDCG cybersecurity guidance, and how to set up and operate the device in a secure fashion.

This document was prepared as part of the Tier 1 risk management process for the device.

1.2. Background

Content of Premarket Submissions for Management of Cybersecurity in Medical Devices Draft Guidance for Industry and Food and Drug Administration Staff details the FDA recommendations for medical devices with cyber risk. More information on the FDA cybersecurity guidance can be found on the FDA website:

<https://www.fda.gov/medical-devices/digital-health/cybersecurity>

Additional information is drawn from the MDCG 2019-16 Guidance on Cybersecurity for medical devices from the EU group that assists in compliance with the MDR and the GDPR. More information on this guidance can be found on the EU website:

https://ec.europa.eu/health/md_sector/new_regulations/guidance_en

Information specific to the **eyeTELLIGENCE™** subsystem is provided in a separate manual insert.

1.3. Document Organization

This Security Manual is part of the Bausch + Lomb **Stellaris Elite™** vision enhancement system.

The **Stellaris Elite™** vision enhancement system is also referred to in this document as the device, or the product. The **eyeTELLIGENCE™** feature on the **Stellaris Elite™** vision enhancement system allows wireless communication to the Bausch + Lomb cloud (refer to **eyeTELLIGENCE™** user manual insert for further information on this feature).

1.4. Acronyms

Table 1 - Acronym Definitions

Acronym	Definition
AES	Advanced Encryption Standard
APN	Access Point Name, a handle for connecting to a cellular provider
CBOM	Commercial Bill of Materials
CSIRT	Cyber Security Incident Response Team
DHCP	Dynamic Host Configuration Protocol
FDA	Food and Drug Administration
FIPS	Federal Information Protection Service
GDPR	General Data Privacy Regulation
HDO	Healthcare Delivery Organizations
MFA	Multi-Factor Authentication
SSL	Secure Socket Layer
TLS	Transport Layer Security
USB	Universal Serial Bus
VPN	Virtual Private Network

2. Device Overview

The **Stellaris Elite™** vision enhancement system is a comprehensive device for ophthalmologic surgeries. There are three (3) versions available.

The BL11145 is the basic version that includes all of the functions necessary for surgeries related to the anterior segment of the eye. Primarily this is the removal of cataracted lenses from patient eyes and implantation of replacement intraocular lens. Secondary functions provide ancillary support during the surgery. Ancillary support may include removal of vitreous material in case of capsular rupture and coagulation in case of operative site bleed. The device offers a wireless foot control for user control of surgical outputs. The device has 2 USB ports available for the user to back up and move surgeon settings profiles between machines and to save end of case data screenshots. The device has an ethernet port that is configured for UDP output to a video overlay system.

WARNING: Do not connect the ethernet port to the hospital network. It is only for use with the Bausch + Lomb DMS video overlay.

The BL14455 is the Posterior Combined version of the **Stellaris Elite™** vision enhancement system. It adds illumination, fluid/air exchange, and high speed vitrectomy to support surgeries in the posterior segment of the eye in addition to all of the functions of the BL11145 system.

The BL15455 system includes all of the functions of the other two and adds a 535nm green treatment laser for retinal coagulation and laser trabeculoplasty.

The **eyeTELLIGENCE™** feature for the **Stellaris Elite™** line adds a cellular gateway to the platform. The cellular gateway is equipped with a eSIM allowing the device to get a connection from almost any cellular provider with signal bands compatible with the radio. The device uses the cellular connection to enhance the experience for the users in various ways listed below. The cellular gateway is firewalled and permits access only to the addresses that are expected for interaction. All communications are initiated by the device, no incoming messages are accepted other than expected responses. All communications are REST exchanges over TLS using SSL1.2. Sensitive data within message packets is encrypted before being loaded for transmission. Finally, the connection between the cellular gateway and GUI PC is disconnected while surgical outputs are active to prevent potential harmful interactions during surgery.

Features enabled by the gateway include:

- Synchronization of the device's system clock to network time to prevent drift
- Reporting and monitoring of the device's location, configuration, and activity
- Online, dashboard help system
- Remote desktop support (at user's request and authorization)
- Optional pairing of the user's customized settings files to an email, allowing the files to be cloud-backed up and synchronized among all devices on which a user authenticates
- Ability to aggregate collected system data of the user and provide by email for study purposes (no protected health information is collected)

2.1. Device Specification

The device module is a Tier 1 surgical device with cellular connectivity to a cloud server and includes various accessories. See the following diagram for a physical layout.

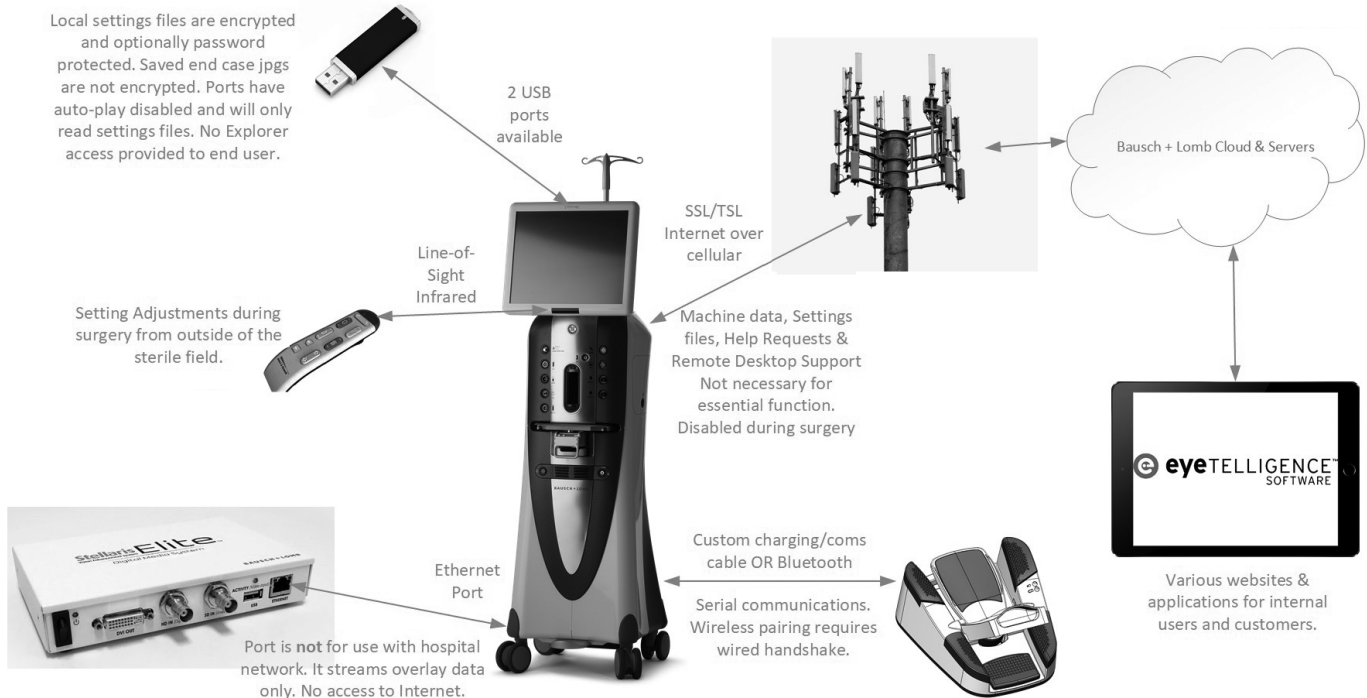


Figure 1 - Physical Diagram

The device has a Bluetooth host that is configured for communicating only to a custom foot control with a UART over Bluetooth protocol. Pairing a specific foot control to a device requires the units to be connected with the backup wired connection for exchange of serial numbers. The device has an Ethernet port that is configured to stream overlay data over UDP from and to fixed ips. The port will not accept ip assignment from a DHCP server and will not attempt to access a foreign network that is connected to it. The firewall in the router is configured to prevent access to the cellular connection from the externally accessible port.

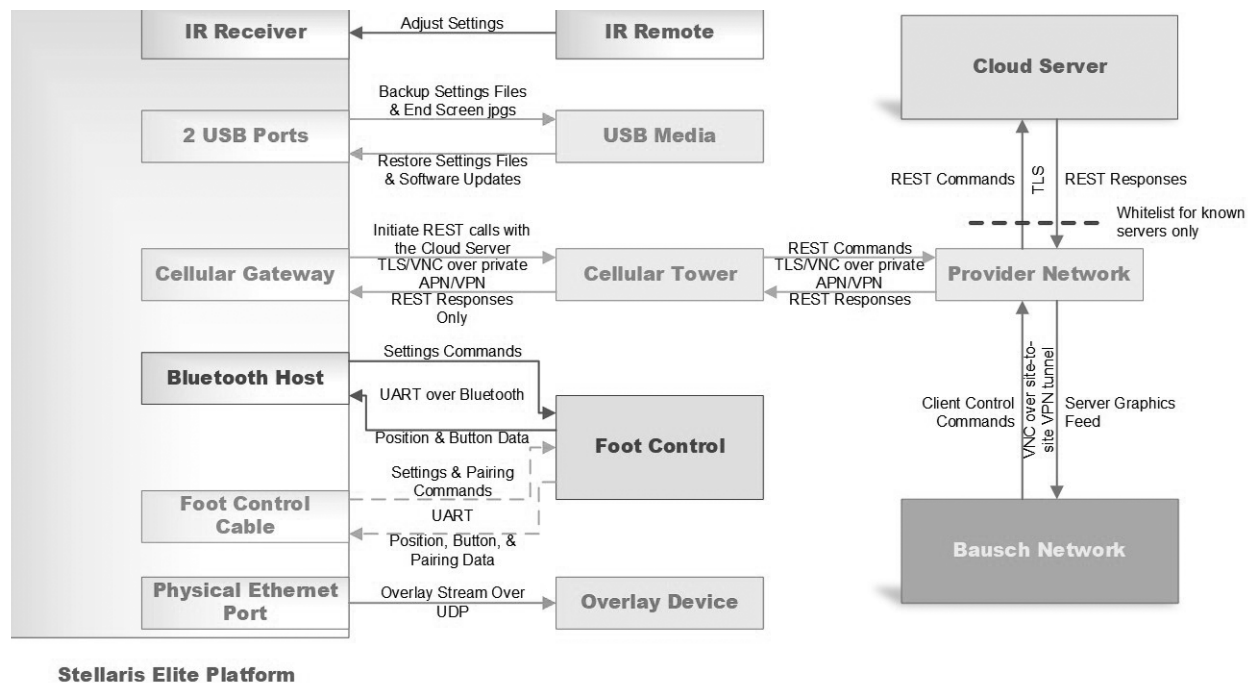


Figure 2 – Functional Block Diagram

2.2. Intended Use

The **Stellaris Elite™** vision enhancement system is intended for the emulsification and removal of cataracts, anterior and posterior segment vitrectomy. The system is designed for use in both anterior and posterior segment surgeries. It provides capabilities for phacoemulsification, coaxial and bimanual irrigation/aspiration, bipolar coagulation, vitrectomy, viscous fluid injection/removal, and air/fluid exchange operations.

The **Stellaris Elite™** vision enhancement system configured with the laser module is additionally intended for retinal photocoagulation and laser trabeculoplasty.

The cybersecurity of the device does not require any specific actions or infrastructure on the part of the customer beyond basic physical security. The device proved to be secure without a hacker being able to physically connect to the device. The device is not intended for connection to the hospital network, hence no customer firewall is required. End Users that create an **eyeTELLIGENCE™** account in the cloud are responsible for creating and maintaining sufficiently strong and secure passwords to keep their settings files safe. It is possible to damage the machine with destructive devices if physical access and security has been compromised. However, this is not considered part of normal use environment.

2.3. Device Security Functionality

The device is largely secure by design. The device is inaccessible via the Internet, preventing remote delivery of any malware due to existing on a private APN/VPN of the cellular provider. The ip addresses of the gateways are not pingable from the general internet. Further, the cellular provider has implemented a whitelist preventing access to/from any ip address outside of the expected interactions.

The USB ports have auto-play disabled and are deactivated in normal usage except on the screens for backing up and restoring offline settings files, on the end case screen when they are write only, or in maintenance mode. They will not read any files except for the surgeon settings files. These are encrypted and integrity checked to prevent tampering. A tampered file will not be accepted or processed by the GUI. In case of some malware being delivered to machine somehow, the hard drive that stores the OS and GUI program is write protected and the machine actually operates from a RAM copy. A simple reboot of the machine will clear system memory and thus remove the malware.

Finally, to prevent interruption of core functionality during surgery, the GUI disables its Ethernet connection while the surgical outputs are active, specifically on the user hitting the Advance to Surgery button. The port is re-enabled as part of the End of Case activities. The entire **eyeTELLIGENCE™** suite of features can also be disabled via software if the customer is not interested or if no cellular signal is available at the user facility.

2.4. Backup and Restore

The device allows backup and restoration of off-line surgeon settings files via USB only. For online surgeon files, the cloud maintains the history of settings files. If a local copy is corrupted, the user can sign off and sign on again at the device and the cloud will restore the most recent file. As intentional changes are made to the file, the user must accept the changes on each machine that they are signed into. Rejection of the file at any paired device will cause the file to revert to the version that is local to the machine where the reject was pressed.

In the unlikely event that the Graphical User Interface software was corrupted, restoration has to be completed by Bausch + Lomb Surgical service personnel.

2.5. Infrastructure Requirements

Using the **eyeTELLIGENCE™** features requires only a cellular signal at 4G or 3G bandwidths. The radio and SIM support the AT&T, T-Mobile, and Verizon networks. If such a connection is not available and the facility does not want to install repeaters or cellular piconet, the **eyeTELLIGENCE™** suite can be disabled on the device to prevent nuisance errors (such as no cellular connection UIC28 code).

It is expected that the facility has implemented physical access control and will prevent potential bad actors from gaining access to their devices. It is recommended that the physical access controls of the facility are of the strength to provide non-reputability of changes made to the device.

As the Stellaris Elite system is not intended to be connected to hospital or facility networks, there are no IT requirements on the hospital or facility for proper, secure device operation.

2.6. Configuration Settings

There are only two configuration options available for specification by the customer. The **eyeTELLIGENCE™** feature can be optionally disabled and enabled by a Bausch + Lomb Surgical service representative later. A Bausch + Lomb representative can also program the SIM to use a specific carrier to make establishment of the cellular connection quicker.

Updates to software or firmware that are required have to be installed by a Bausch + Lomb representative so that the device essential performance can be ensured.

The system OS is configured to remove all non-essential services and programs to minimize the threat area. The device router and the device OS both enable appropriate firewalls. The device utilizes a write-protection scheme of its system and GUI as well as a supervisory program preventing the execution of unexpected or unapproved applications. The device is not configured with an active anti-virus or security scanning software to maximize performance. This is considered safe as there is no method to introduce undesirable software to the device.

Session time outs are implemented for the maintenance role (accessed by Bausch + Lomb personnel only) to protect the system from tampering while in a modifiable state and are implemented for the device in its connection to the Cloud via expiring session tokens. The device ensures it is communicating with the Cloud server and vice versa via a security certificate exchange when obtaining a unique session token with each connection. Session time outs are not implemented for regular users to maintain availability of essential surgical performance.

The communications to the server implements traffic filtering and segmentation protections against DDOS attacks and similar cyber events. That particular protection mechanism is monitored by a CSIRT.

The system is configured for all Windows logging, including logins, OS events and changes, and security detections. Additionally the system logs its hardware and software configuration and usage of all of the surgical functions in a per surgery and cumulative mode for purposes of system use monitoring. These log files are stored in a non-write protected partition and are uploaded to the cloud via separate APIs. These files are neither user readable nor retrievable at the machine.

To maintain the device integrity, do not attempt to connect any equipment to the device that is not approved by Bausch + Lomb for use with the **Stellaris Elite™** vision enhancement system with **eyeTELLIGENCE™**.

2.7. Device Ports and Interfaces

The device's ports and interfaces that are supported when operating in the intended environment:

- Cellular connection via private APN/VPN for **eyeTELLIGENCE™** features.
- UDP Ethernet Port for video overlay. Will not function with connection to hospital network as it has a static ip address programmed and DHCP is disabled.
- 2 USB ports for media for offline settings files, backup and restoration, and for capturing screenshots of the end of case screen. For safety, these ports are disabled by the GUI on all screens except the settings file load/save screens. Additionally, autoplay is disabled to prevent malware from being read from a drive and when browsing the drive from the GUI, only settings files will be shown or read.
- Bluetooth and wired connection for the supplied foot control. The Bluetooth uses a secure pairing that requires an exchange of data over the wired cable. The cable can then be removed, presuming that the embedded battery contains sufficient charge for the surgery.
- The device does not support a keyboard, scanner, or any other user input device beyond the GUI screen and the supplied remote control.
- The display unit contains a resistive touchscreen for user interaction through a sterile drape. It presents an onscreen keyboard with a limited character set when appropriate.
- The machine has a standard power cable with the appropriate plug for the region to which it is shipped. For the US, it is a 110V standard.

All ports are configured in compliance with the concept of Deny by Default, being enabled only for the intended functionality. The following ports and interfaces are explicitly disabled when operating in surgical mode:

- The Ethernet port on the GUI computer is disabled to prevent communications while the surgical outputs are active.
- The USB ports are disabled while the surgical outputs are active. They are activated only on the settings file backup and restoration screen and on the end of case screen.

Table 2 shows the device's physical interfaces mapped to the logical interfaces.

Table 2 - Module Interface Mappings

Interface	Port/Protocol	Data Direction	Use
Cellular	[Port 443: HTTPS/] / TLS1.2	In (response only) / Out	Upload of log files, configuration and settings files. Upload of Help Requests and Remote Desktop Requests. Download of updated connected settings files and responses to requests.
Ethernet	9 / UDP and TCP	In only	Wake On LAN Discard
Ethernet	135 / UDP and TCP	In / Out	Communication with DMS
Ethernet	3390 / TCP	In / Out	VNC Communication
Ethernet	4010 / UDP	Out only	Data stream of foot pedal position and surgical mode for display on overlay.
Ethernet	4020 / UDP	In only	Compressed Video Stream
Ethernet	8085 / TCP	In / Out	Remote Desktop
Bluetooth	[No port] / UART over Bluetooth	In / Out	Will only pair with a Bausch + Lomb foot control. Reads foot pedal position and activation state of buttons. Writes region configuration and stop settings.
Custom Charging Interface	[No port] / UART	In / Out	Wired version of Bluetooth connection, also includes battery charging voltage.
USB	[No port] / File system	In / Out	Only settings files will be read. Settings files and screenshots will be written.
IR	[No port] / Patented unique company protocol on a 40 kHz carrier wave.	In only	Configuration adjustments can be made in room via the line-of-site IR remote.

2.8. Roles and Services

2.8.1. Roles

The device uses role/identity-based authentication and has roles: General User, Specific **eyeTELLIGENCE™** Surgeon, Maintenance User.

The General User role is for nurses, biotechs, and surgeons without an **eyeTELLIGENCE™** account. The device always boots to the General User GUI and is logged in with this role. The user is able to select the device mode (Anterior/Posterior/Combined), select a surgical settings file, and advance to surgery. The user can enter the setup menu to create, edit, remove local settings files. The user can use a USB device on the Backup/Restore screen to move a settings file to/from a media drive. Offline settings files can also be secured with a local password. Assuming **eyeTELLIGENCE™** is active, the user has access to the Get Me Help dashboard assistance function. The user can be directed while on the phone with a Bausch + Lomb representative to enable the Remote Desktop support option. Note that any user can log out an **eyeTELLIGENCE™** surgeon from a specific device which will remove the local files of the user. This does not require the password for the case of a surgeon having left a practice. This has no effect on the user's cloud record.

The Surgeons role is for surgeons who chose to use **eyeTELLIGENCE™** and have provided Bausch + Lomb with an email account and have created their own secure password. These users have all of the access of General Users but are also able to use the 'Connect To Cloud Account' button on the startup screen to authenticate themselves at a device. This causes the device to generate a pairing to the user and to synchronize the user's settings files to the device. The user is able to add or remove files from their cloud profile via the setup menus, though each change to the cloud record requires an additional authentication. The user can contact Bausch + Lomb for collections of their data from the cases performed with their settings files.

The Maintenance role is reserved for Bausch + Lomb Surgical's service representatives. It enables access to the OS and is for updating the device configuration or performing preventative maintenance.

2.8.2. Services

The following table lists the unauthenticated services executing on the **Stellaris Elite™** GUI Processor in addition to the OS and the GUI application itself. There are no authenticated services being executed.

Table 3 - Unauthenticated Services

Service	Operator	Description	Input	Output	Critical Security Parameters
BLRemoteLock	Admin	Allows enabling/disabling of physical ports	ExecuteCommand (132) ExecuteCommand (133) ExecuteCommand (128) ExecuteCommand (129) ExecuteCommand (134) ExecuteCommand (135) ExecuteCommand (136) ExecuteCommand (137)	Enable Ethernet1 on UIC Disable Ethernet1 on UIC Enable Ethernet3 on MMC Disable Ethernet3 on MMC Disable USB1 on UIC Enable USB1 on UIC Disable USB2 on MMC Enable USB2 on MMC	
VNCAgent	Admin	Allows remote control of system over local TCP connection (used over the cellular connection for Remote Desktop support)	Connection VIEW Connection CONTROL	None	Service is inactive until user initiated at the system Password required for each connection type

2.9. Identification Procedures

Not applicable. No files are downloadable by the customer.

2.10. Device Security Response

Beyond announcement of password mismatch, no security messages are displayed.

2.11. Device Intrusion Detection/Evidence

Windows event logging is enabled and security events are uploaded to the cloud to be forwarded to Bausch + Lomb's CSIRT team. They will respond appropriately if an alert reaches them. The system also displays an undismisable alert box while the remote desktop feature is connected thus providing an indication to the user that the remote desktop feature is enabled.

2.12. Device Recovery

Device recovery/restoration procedures are covered in the Service Manual for Bausch + Lomb representatives only.

2.13. Device Component List [CBOM]

The following is a list of off-the-shelf software in the **Stellaris Elite™** hard drive image including the OS and its components.

Windows WES 2009 Extensions:

- Cumulative updates January 2008 – December 2008
 - Windows WES 2009 with SP3 Security Update 958644
 - Windows WES 2009 with SP3 Security Update 957097
 - Windows WES 2009 with SP3 Security Update 955069
 - Windows WES 2009 with SP3 Security Update 954459
 - Windows WES 2009 with SP3 Security Update 956802
 - Windows WES 2009 with SP3 Security Update 958215
 - Windows WES 2009 with SP3 Security Update 954600
 - Windows WES 2009 with SP3 Security Update 952069
 - Windows WES 2009 with SP3 Security Update 955839
- Cumulative updates January 2009 – December 2009
 - Windows WES 2009 with SP3 Security Update 969947
 - Windows WES 2009 with SP3 Security Update 976098
 - Windows WES 2009 with SP3 Security Update 974392
 - Windows WES 2009 with SP3 Security Update 974318
 - Windows WES 2009 with SP3 Security Update 976325
 - Windows WES 2009 with SP3 Security Update 973904
 - Windows WES 2009 with SP3 Security Update 955759
 - Windows WES 2009 with SP3 Security Update 970430
 - Windows WES 2009 with SP3 Security Update 971737
 - Windows WES 2009 with SP3 Security Update 968389
- Cumulative updates January 2010 – December 2010
 - Windows WES 2009 with SP3 Security Update 2296199
 - Windows WES 2009 with SP3 Security Update 2416400
 - Windows WES 2009 with SP3 Security Update 2423089
 - Windows WES 2009 with SP3 Security Update 2436673
 - Windows WES 2009 with SP3 Security Update 2440591
 - Windows WES 2009 with SP3 Security Update 2443105
 - Windows WES 2009 with SP3 Security Update 2443685

- Cumulative updates January 2011 – December 2011
 - Windows WES 2009 with SP3 Security Update 2443685
 - Windows WES 2009 with SP3 Security Update 2618444
 - Windows WES 2009 with SP3 Security Update 2618451
 - Windows WES 2009 with SP3 Security Update 2619339
 - Windows WES 2009 with SP3 Security Update 2620712
 - Windows WES 2009 with SP3 Security Update 2624667
 - Windows WES 2009 with SP3 Security Update 2633171
 - Windows WES 2009 with SP3 Security Update 2633952
 - Windows WES 2009 with SP3 Security Update 2639417
- Cumulative updates January 2012 – December 2012
 - Windows WES 2009 with SP3 Security Update 2727528
 - Windows WES 2009 with SP3 Security Update 2729449
 - Windows WES 2009 with SP3 Security Update 2737019
 - Windows WES 2009 with SP3 Security Update 2753842
 - Windows WES 2009 with SP3 Security Update 2758857
 - Windows WES 2009 with SP3 Security Update 2761465
 - Windows WES 2009 with SP3 Security Update 2770660
 - Windows WES 2009 with SP3 Security Update 2779030
 - Windows WES 2009 with SP3 Security Update 2661254
 - Windows WES 2009 with SP3 Security Update 2779562
- Cumulative updates January 2013 – December 2013
 - Windows WES 2009 with SP3 Security Update 2876331
 - Windows WES 2009 with SP3 Security Update 2868626
 - Windows WES 2009 with SP3 Security Update 2900986
 - Windows WES 2009 with SP3 Security Update 2862152
 - Windows WES 2009 with SP3 Security Update 954155
 - Windows WES 2009 with SP3 Security Update 2893984
 - Windows WES 2009 with SP3 Security Update 2898715
 - Windows WES 2009 with SP3 Security Update 2898785
 - Windows WES 2009 with SP3 Security Update 2893294
 - Windows WES 2009 with SP3 Security Update 2892075
 - Windows WES 2009 with SP3 Security Update 2904266

- Cumulative updates January 2014 – December 2014
 - Windows WES 2009 with SP3 Security Update 3002885
 - Windows WES 2009 with SP3 Security Update 2992611
 - Windows WES 2009 with SP3 Security Update 2993958
 - Windows WES 2009 with SP3 Security Update 2978125
 - Windows WES 2009 with SP3 Security Update 2989935
 - Windows WES 2009 with SP3 Security Update 3006226
 - Windows WES 2009 with SP3 Security Update 3011780
 - Windows WES 2009 with SP3 Security Update 3013126
 - Windows WES 2009 with SP3 Security Update 3008923
 - Windows WES 2009 with SP3 Security Update 3012172
 - Windows WES 2009 with SP3 Security Update 3013410
- Cumulative updates January 2015
 - Windows WES 2009 with SP3 Security Update 3021674
 - Windows WES 2009 with SP3 Security Update 3019215
- Cumulative updates February 2015
 - Windows WES 2009 with SP3 Security Update 3019215
 - Windows WES 2009 with SP3 Security Update 3021674
 - Windows WES 2009 with SP3 Security Update 3029944
 - Windows WES 2009 with SP3 Security Update 3021952
 - Windows WES 2009 with SP3 Security Update 3013455
 - Windows WES 2009 with SP3 Security Update 3004361
 - Windows WES 2009 with SP3 Security Update 3020338
 - Windows WES 2009 with SP3 Security Update 3023562
- Cumulative updates March 2015
 - Windows WES 2009 with SP3 Security Update 3046049
 - Windows WES 2009 with SP3 Security Update 3030398
 - Windows WES 2009 with SP3 Security Update 3039066
 - Windows WES 2009 with SP3 Security Update 3035132
 - Windows WES 2009 with SP3 Security Update 3033889
 - Windows WES 2009 with SP3 Security Update 3032323
 - Windows WES 2009 with SP3 Security Update 3033395
 - Windows WES 2009 with SP3 Security Update 3034344
- Cumulative updates April 2015
 - Windows WES 2009 with SP3 Security Update 3032323
 - Windows WES 2009 with SP3 Security Update 3033395
 - Windows WES 2009 with SP3 Security Update 3049874
 - Windows WES 2009 with SP3 Security Update 3038314
 - Windows WES 2009 with SP3 Security Update 3046482
 - Windows WES 2009 with SP3 Security Update 3046306
 - Windows WES 2009 with SP3 Security Update 3037578

OS Components:

- Enhanced Write Filter (EWF)
- System Cloning (Unique System ID)
- Windows Firewall
- Time Zone (Default to Central Time)

Disabled OS Components:

- Index Service
- Screen Saver
- NWLink
- Print Spooler
- Internet Explorer

3rd Party Components:

- Bausch + Lomb Shell
- Softing and Ixxat CAN Buses
- Realtek AC'97 Version A4.06 (Advantech 4461 SOM)
- Realtek High Definition Audio Version 5.10.06493 (Kontron T40R SOM)
- Touch-Base Universal Pointing Device Driver (UPDD) Version 6.00.386.6279
- Intel 4 Series Chipset Device Software Version: 9.0.0.1008 (Advantech 4461 SOM)
- AMD G-T40R Series Chipset Device Software Version: 5.1.2600 (Kontron T40R SOM)
- GME940/945/960/965 Version 14.32 (Advantech 4461 SOM)
- AMD Radeon HD 6250 Version 8.950.0.0 (Kontron T40R SOM)
- Realtek PCIe FE Family Controller, Version 5.770.909.2010 (Advantech 4461 SOM)
- Broadcom NetLink(TM) Gigabit Ethernet Version 14.6.0 (Kontron T40R SOM)
- Microsoft Corporation Windows XP NULL device driver, File Version 5.1.2600.0

2.14. External Operating Environment Components

Data that is backed up from the device is stored in the Bausch + Lomb Cloud on IBM's Public Cloud Infrastructure. The data that contains personal information (physician and/or facility identification) is deidentified and encrypted before upload and is stored in an encrypted state. The system does not collect patient identifiable information. The non-personal data is not transmitted in an encrypted state but is stored encrypted with the standard method of the database. Data generated in the US is stored in the IBM Dallas environment.

2.15. Deployment Instructions

Not Applicable.

2.16. Residual Risk Disclosure

The device underwent white hat penetration testing as part of the development process. This revealed very low risk of remote cybersecurity attacks due to the architecture. Being a Windows-based device, it was vulnerable to local attacks when the hacker was physically present with the device. It is recommended that the users make sure to follow good physical security practices at their facility as the device is vulnerable to attack vectors from an attacker who has physical access to the device.

2.17. Terms of Support

It is known that the device, the OS, and the version of the .NET framework that support the GUI are out of support by Microsoft. Both packages have been fully patched to the last support release. Bausch + Lomb has determined that the residual risk associated with these issues is manageable with the other controls in place and enforced. Bausch + Lomb is also monitoring for new exploits that could be a risk to fielded systems and will notify users of additional steps required to maintain secure systems.

3. Secure Operation

Secure operation of the device is a shared responsibility of good design and maintenance of the device and the overall system on the part of the manufacturer and good security practices and hygiene on the part of the owners and operators.

3.1 Initialization

Due to the nature of the connectivity of the device being wireless cellular, there are no special requirements or configuration required on the facility network or infrastructure. The embedded SIM ships in an off state. The connectivity features will be disabled until the SIM is reactivated. This can be done remotely by the Bausch + Lomb sales or service team representatives. The SIM will support multiple carriers. For the best experience, let your Bausch + Lomb representative know what cellular carrier has the best coverage inside of your facility. If your facility does not have cellular coverage and you'd still like to use the connectivity features, your service representative can assist in identifying a picocellular transmitter or a cellular repeater for you to install. If neither of these are possible or desired, let your representative know. The connectivity features can also be fully deactivated in software to disable messages about the connection not being present.

3.2 Maintenance Guidance

The configuration of the device does not allow the users to perform any maintenance on the software. When software updates including security patches are required, your local service representative will schedule a visit to install it. Software updates are authenticated via digital signature and an embedded cryptographic check.

The device is protected from malware by the access control built into it. It is designed with additional reinforcements of write protection of the device program drive and a supervisory program that only allows expected executables to run. If you have reason to believe that your device has been infected with some malware, a reboot of the device will most likely clear it up. If it does not, please call the Bausch + Lomb technical support line to report it and a service representative will visit as quickly as possible to address the potential security event. A functional verification of all surgical outputs is included as part of any service event. This ensures the device is ready for use after service events.

Bausch + Lomb recommends a yearly Preventative Maintenance service for optimal performance.

In the event of a data corruption of a corrupted surgeon settings file, contact service support. The files are backed up in the cloud and can be restored by Bausch + Lomb personnel to the last functional version.

No explicit override mode is provided as the essential surgical functionality does not depend on the connectivity in any way. The connectivity is disabled while the surgical functions are active.

3.3 User Guidance

The operating facility is expected to provide good physical security to prevent unauthorized physical access to the device. It is highly recommended that the facility be configured to use Access Control Measures such as smart ID cards to ensure only authenticated and authorized personnel are allowed access to the device. Given the nature of the device and its use in surgical settings, some level of physical access control can likely be assumed. Users taking advantage of the **eyeTELLIGENCE™** features should be trained in making sufficiently complex passwords and on general good security practices. Our corporate policy on passwords is enforced on the password creation tool on the website. Passwords should be difficult to guess and be:

- A minimum of 12 characters long
- Contain at least 1 number [0-9], 1 capitalized letter [A-Z], 1 lowercase letter [a-z], and 1 special character [~`!@#\$%^&*()-_+={}|\\;:'">,./?]

A good practice is to perform character substitution on a favorite phrase of a poem or song.

Multifactor authentication (MFA) is not enabled at this time.

In general, users should take care to never share their passwords with anyone else or to follow links in unexpected emails. The device tracks its own configuration and records and reports all changes to it. Combined with that record, the access list to the device can provide a non-reputable record of who made a destructive change.

It is recommended that facilities using the equipment provide Security Awareness Training to all users of the equipment consisting of the above and standard IT practices.

Do not attempt to use the device for anything beyond its intended uses.

Relevant to user privacy, the device itself is GDPR compliant. No data that contains patient identifiable information is captured at all. Case data by surgeon is only captured when the specific user has signed up for the program via the website and granted consent. The signed up user's data is limited to basic contact information and is kept in a GDPR compliant environment with FIPS compliant encryption. The user's guaranteed rights under the GDPR are all exercisable via the website. For non-signed up users, all case data is fully anonymized before uploading.