Security

Elekta IntelliMax™ Security Information

Table of Contents

Elekta IntelliMax™ Security Information

1.0 Purpose and Scope

This document gives the security configuration and infrastructure setup for hospitals before IntelliMax™ Agent can be installed. It is intended to be used by Elekta personnel, hospital staff and IT departments as a guide to answer questions and concerns before IntelliMax Agent is introduced into the hospital environment.

This document includes information about IntelliMax Agent version 3.x (installed on an IntelliMax Agent computer) and Remote Access programs:

- IntelliMax Connect (installed on an Elekta product)
- Elekta Remote Service program 1.0 or above (installed on an Elekta product)

Earlier releases of the Elekta IntelliMax can use a different configuration than specified here and must be upgraded to the latest available release compatible with the necessary medical device.

Remote Services capabilities using Elekta IntelliMax™ and any associated uptime guarantees defined with the service agreement can only be provided where equipment is connected to an IntelliMax Agent.

2.0 Elekta IntelliMax™ Overview

Elekta has an obligation under international regulations to make sure that Elekta products connecting to a network can do so without compromising the integrity of the Elekta product, or the safety of patient or health information. These parts are included in the Remote Services infrastructure.

Remote Access to Elekta medical products for remote desktop sharing, text-based chat, and file transfer. Remote Access sessions connect two computers at the same time.

The users of these computers are referred to as:

- The hospital-based user is the user who operates the Elekta product in a hospital. This can be a Clinical User or a Service User.
- Elekta IntelliMax support user is an Elekta certified user who can give remote support for one or more Elekta products. This user is not at the hospital.

IntelliMax Agent is a software program that is installed on a dedicated computer in the hospital. IntelliMax Agent is the only access point for Remote Access sessions from supported Elekta products out of the hospital network. IntelliMax Agent collects machine data from supported Elekta products, which it sends to IntelliMax Enterprise using a secure Internet connection. IntelliMax Agent does not collect patient data.

IntelliMax Enterprise is used for the analysis of data collected by IntelliMax Agent. It is also used to administer the Remote Access sessions to connected Elekta products. Approved users can get access to IntelliMax Enterprise through a web-based interface.

The IntelliMax Enterprise is hosted by PTC in the USA and uses PTC technology. More information can be found at http://ptc.com. There will be no need for Elekta customers to contact PTC directly. All information or queries related to PTC or IntelliMax Enterprise will be made through the Elekta support organization.

Using the definition in NB-MED/2.2/Rec4 – Software and Elekta products (refer to http://www.team-nb.org), the IntelliMax Agent and IntelliMax Enterprise have each been categorized as non-medical products. For the latest Elekta IntelliMax compatibility with remote monitoring and remote access, refer to the IntelliMax Agent Configuration application on the IntelliMax Agent computer.

3.0 Security Overview

Communication between IntelliMax Agent and IntelliMax Enterprise is transported over Secure Socket Layer (SSL), using SHA256 encryption through TCP port 443. All data is encrypted and sent securely from IntelliMax Agent to IntelliMax Enterprise.

IntelliMax Enterprise uses an SSL certificate signed by DigiCert from 2017. IntelliMax Agent must first authenticate with IntelliMax Enterprise before communication can be established.

Remote Access sessions are routed through IntelliMax Agent and use the IntelliMax Agent Internet connection. All Remote Access sessions are recorded in the audit log including the Elekta IntelliMax support user and computer involved in the session.

The IntelliMax Enterprise has a web browser-based user interface and uses SHA 256-bit AES encryption for communication between the IntelliMax Enterprise server and web browser.

IntelliMax Agent starts all communication to the Elekta medical product and IntelliMax Enterprise. IntelliMax Agent polls IntelliMax Enterprise for any requests. If IntelliMax Agent is switched off, no communication is possible to the Elekta products or the IntelliMax Enterprise server.

3.1 FIPS Compliance

The Federal Information Processing Standard (FIPS) Publication 140-2, (FIPS PUB 140-2), is a U.S. government computer security standard used to approve cryptographic modules.

The IntelliMax Agent can be made FIPS Compliant at installation. Please contact your local Elekta Service Representative or Regional Elekta Care™ Support center if this is required.

4.0 Attended Remote Access Sessions

When you use a Remote Access program through an IntelliMax Agent to a medical device, Remote Access has to be started and permission granted from the hospital-based user of the Elekta medical product. It is only possible to start a session from the Elekta product in the medical facility.

The Elekta IntelliMax support user cannot start the session. A visual indication is displayed on the Elekta product screen to show when the IntelliMax Connect or Remote Service is on and that an attempt to connect is possible.

Should remote access to the desktop of the device be reasonably necessary, IntelliMax Connect allows for either attended (mandatory for treatment machines) or unattended (configurable during installation for software systems) access using secure, 256 bit encryption. Access via Elekta IntelliMax, and details of any files transferred are recorded in an audit log which is available on upon request for a period of 12 months after the transfer.

5.0 Audit Log

The audit log contains the information as follows:

- Time stamp with the start and end time of each remote session
- User and device logged on
- File transfer of pre-defined files, for example file name, size and location.

The audit log contains information about user and device activity. The audit log data is kept on IntelliMax Enterprise and cannot be removed from the system.

IntelliMax Enterprise users can only see the audit log for the Elekta products they are permitted to see.

If a user or Elekta product is removed from the system, all data about the user or Elekta product will continue to be kept in the audit log.

When you use a Remote Access program through the IntelliMax Enterprise, user interface activity is not recorded in the audit log.

For IntelliMax Connect only: an audit log is made for the file transfer function which includes the direction of the file transfer and the file name, size and location. To record the changes made to an Elekta product when you use a remote access, you must use the applicable procedures for the Elekta product.

All files collected by IntelliMax Agent from the Elekta product and sent to IntelliMax Enterprise are recorded in the audit log. All files downloaded by a user from IntelliMax Enterprise are also recorded in the audit log which is available on upon request for a period of 12 months after the transfer.

6.0 Access Control

Access control to IntelliMax Enterprise and connected Elekta products is based on membership of user groups. This enables hierarchies of users to be easily created and managed. User group membership is defined in IntelliMax Enterprise. Privileges for each user group are also defined in IntelliMax Enterprise. Only user administrators can assign and create the user and privilege groups. Access will only be given to certified Service Engineers and hospital based users.

7.0 Remote Monitoring and Data Collection

Depending on the needs for Remote Service for each product, the data types as follows can be monitored/ collected by by IntelliMax Agent from attached Elekta products:

- Realtime configuration and system data from Control Systems
- Microsoft® Windows® registry information for system status and Elekta product license options
- Microsoft Windows Application/System events
- Elekta software log files
- Device configuration, calibration and log files
- Operating system log files

The collected data can be used for but not limited to the functions as follows:

- Machine diagnostics and to monitor the device
- Reports (system performance and statistical)to give proactive/predictive service information and help
- Windows Service monitoring

No Protected Health Information (patient or person identifiable information) is sent to IntelliMax Enterprise.

8.0 Data Transfer

All data transmitted between IntelliMax Agent and IntelliMax Enterprise and Global Access Servers (GAS) is compressed and encrypted. The data is transported over SSL, using 128-bit AES encryption. When the data has arrived at IntelliMax Enterprise, it is decrypted and decompressed. The data is then processed in order to trigger notifications or alarms, before being discarded or stored in the database.

GAS is used to route screen sharing traffic from Remote Access sessions, separating the screen sharing traffic from the session setup and auditing. The GASs are located in Japan, the United Kingdom, Germany, China, USA and Australia. A specified GAS can be tied to Elekta products if it is necessary for data to go or not to go through a specified route. Tell the Elekta Technical Helpdesk if this is necessary.

When you use Remote Access, files can be transferred off the Elekta product to the computer of the Elekta IntelliMax support user or specified drive.

9.0 Security Requirements

9.1 Firewall Rules

9.1.1 IntelliMax Agent to IntelliMax Enterprise (out of the hospital)

Tell Elekta Care™ Support if all GAS are not available from the hospital. The nearest available Global Access Server will be used. If for any reason the nearest GAS is unavailable or at capacity the next nearest GAS will be used. Therefore access is required to multiple servers to ensure availability.

The software program on IntelliMax Agent that will try to access the Internet is found in C:\Program Files\Axeda\Gateway\xGate.exe on 32bit versions of Windows and C:\Program Files(x86)\Axeda\Gateway\xGate.exe on 64bit versions of Windows. In some software firewall products it may be necessary to exclude the program from being blocked.

From IntelliMax Agent to IntelliMax Enterprise (outbound on the Internet), access to the domain names and ports is as follows. Elekta advise use of domain names in firewall rule configuration as IP addresses may change without significant notice periods.

IntelliMax Enterprise	elekta.axeda.com	port 443
GAS Japan	ghjap1.axeda.com	port 443
GAS Japan	ghjap2.axeda.com	port 443
GAS USA	ghsj1.axeda.com	port 443
GAS USA	ghsom1.axeda.com	port 443
GAS USA	gas-bo6.axeda.com	port 443
GAS UK	ghuk2.axeda.com	port 443
GAS UK	ghuk3.axeda.com	port 443
GAS Germany	gas-de2.axeda.com	port 443
GAS Germany	gas-de3.axeda.com	port 443
GAS Australia	gas-aus2.axeda.com	port 443
GAS Australia	gas-aus3.axeda.com	port 443

9.1.2 IntelliMax Agent to Elekta products (inside the hospital)

Between IntelliMax Agent and Elekta product, the ports as follows are used.
They will be opened automatically on the Elekta product firewall during installation:

Elekta Product	Function	Ports
Integrity™	Remote Monitoring & Access	**Com IP[1]:** TCP port 23 Microsoft File & Print sharing2: UDP ports from 135 through 139 TCP ports from 135 through 139 UDP port 445, TCP port 445 **IntelliMax Connect:** TCP ports 5920, 8330 and 8331
Leksell Gamma Knife®	Remote Monitoring	**File Transfer:** TCP port 22, 443, 8001 **Elekta Remote Service Program:** TCP ports 5900, 5920, 8330 and 8331
Leksell GammaPlan	Remote Monitoring Remove & Access	**File Transfer**: TCP port 22, 443, 8001 **Network Time Synchronization:** UPD port 123
XVI, iViewGT	Remote Monitoring & Access	**Microsoft File & Print sharing[2]:** UDP ports from 135 through 139 TCP ports from 135 through 139 UDP port 445, TCP port **IntelliMax Connect:** TCP ports 5920, 8330 and 8331
iViewC, iGuide and NSS (network Security Solution)	Remote Access Only	**IntelliMax Connect:** TCP ports 5920, 8330 and 8331
MOSAIQ and Monaco	Remote Monitoring & Access	**IntelliMax Connect:** TCP ports 5920, 8330 and 8331 **Messaging Service:** TCP ports 9011 and 9012

[1]COM/IP® is used on the Linac control system by the IntelliMax Agent to collect Item Part Values. The COM/IP® COM Port Redirector creates virtual COM ports and software modems for modem applications to use TCP/IP networks (including the Internet) instead of modem hardware and telephone connections.

[2]The IntelliMax Agent uses Windows® File and Print sharing to access the registry and to upload files from Elekta

9.2 Virus & Malware Protection & Microsoft® Hotfixes and Patches

The computer must be dedicated for the purpose of Elekta IntelliMax and not used for any other purpose, in order to maintain the integrity of IntelliMax Agent software and its functions, and to reduce the likelihood of any additional threat to the machine introduced by misuse, including web surfing.

Because of the unidirectional upload of files and data from the Elekta products to IntelliMax Enterprise, there is a minimum risk of virus & malware infection on the Elekta products connected to IntelliMax Agent. Only the explicit ports necessary for communication are opened on the inbuilt firewalls.

At the time of writing this document, no Elekta products have been infected by viruses as a result of having IntelliMax Agent connected.

Elekta shall in no event be responsible for viruses or malware or any other computer code, files, programs designed to interrupt, restrict, destroy, limit the functionality of or compromise the integrity of any computer software or hardware or telecommunications equipment and shall have no liability for any damage caused by such virus, malware or other intrusion.

IntelliMax Agent 3.x has been tested with Microsoft® Windows® 7 Professional and Windows 10 Professional and all communication in and out of the NSS (Network Security Solution) for Elekta Linear Accelerators, or IntelliMax Agent PC for Leksell Gamma Knife is virus scanned.

If a PC or Virtual Machine is used to host IntelliMax Agent (other than NSS/IntelliMax Agent PC for Leksell Gamma Knife), it is the responsibility of the hospital to make sure that virus and malware protection is installed and up-to-date on the IntelliMax Agent computer.

Elekta recommends that virus and malware protection is present and running before IntelliMax Agent software is installed. The installed anti-virus and anti-malware software must let the program access to the Internet as defined in the Firewall Rules section of this document.

Elekta recommends that all Microsoft security hotfixes are applied to the operating system where the computer is owned by the hospital. If necessary, Microsoft automatic update can be left on and updates applied daily.

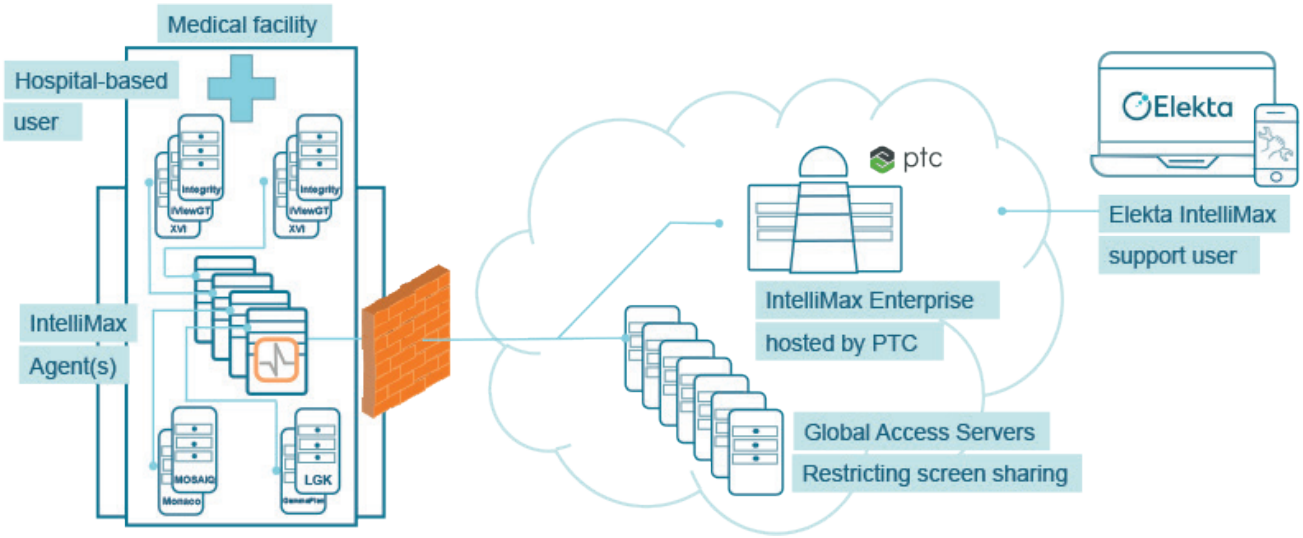
If the hospital IT do their own updates, Elekta recommends only Microsoft updates and anti-virus/anti-malware updates are applied.

PRT133 and LSR99001 as both contain the same information regarding the computer specification and Operating system software requirements for IntelliMax Agent and is available from http://elektamarketing.info or from your local Elekta Service representative.

10.0 Network Overview

Remote monitoring of machine data and all Remote Access communication from the hospital is routed out of the hospital through the IntelliMax Agent computer to https://elekta.axeda.com using 256 bit SSL connection.

Remote Access communication is sent from the hospital through the IntelliMax Agent computer to https://elekta.axeda.com. When the session is set up, screen sharing traffic is sent through one of the Global Access Servers during a Remote Access session on port 443.



11.0 Remote Access Overview

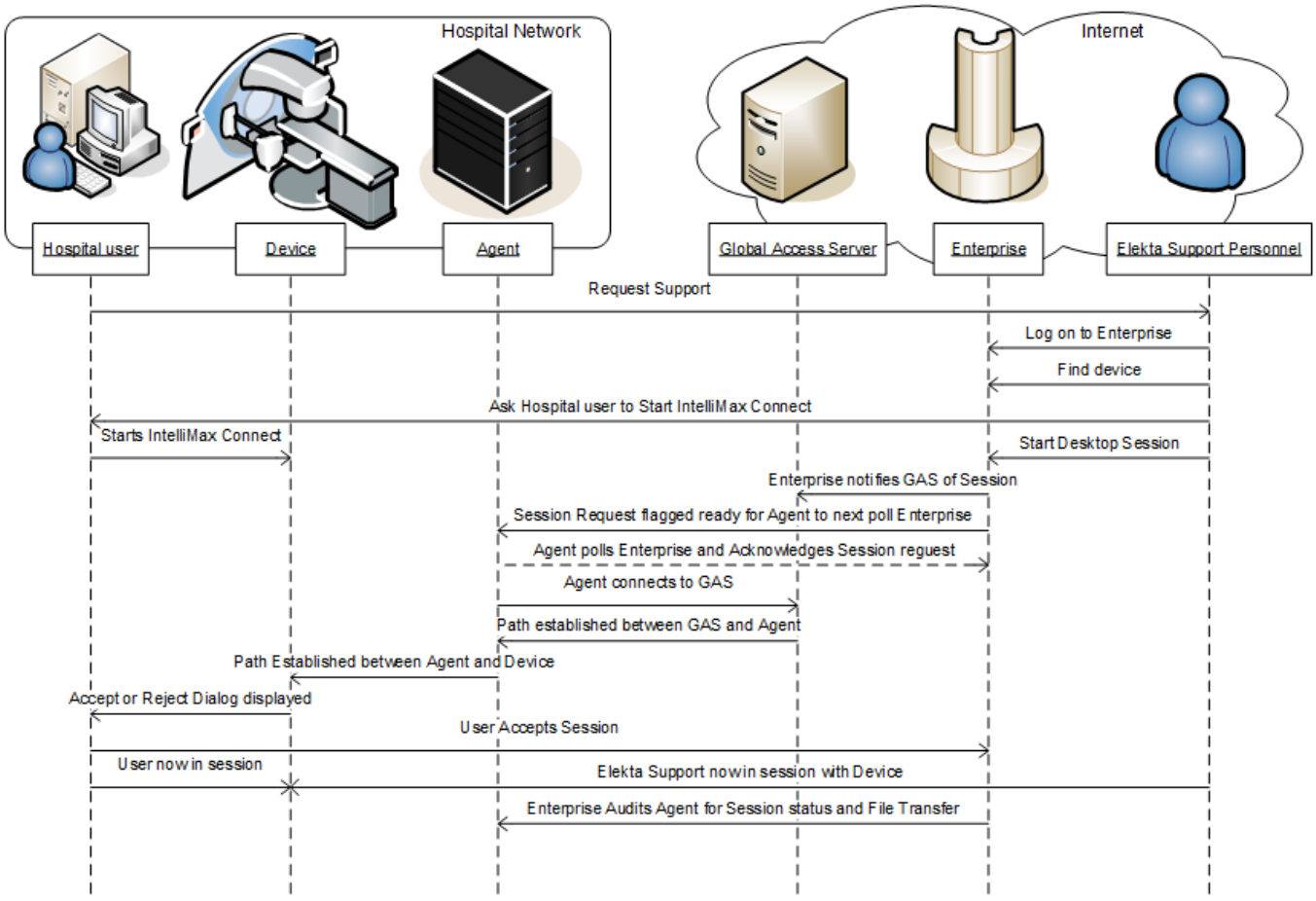
On Elekta Medical devices, only attended Remote Access sessions are permitted. For all attended sessions a user has to be present at the Elekta medical device.

An audit log is created each time a Remote Access session is attempted. The audit log also contains information about which Elekta product a user is trying to access, successful or failed attempts, and any file transfers that occur during the session.

To start a Remote Access session, the applicable program (IntelliMax Connect etc.) must be started by the hospital based user. See the Firewall Rules for details of the ports used for each program.

The Elekta IntelliMax™ support user will attempt a Remote Access session to an Elekta product, using the IntelliMax Enterprise web page. A connection from IntelliMax Enterprise is proxied by IntelliMax Agent to the Elekta product it is attached to.

Elekta processes and user documentation specify that the session must be stopped from the Elekta product. This is to make sure that the hospital-based user is sure the session is completed and that no more Remote Access connections can be made.



11.1 User Authentication

1. The user goes to http://elekta.axeda.com (or http://intellimax.elekta.com which will redirect the user to IntelliMax Enterprise).
2. The site certificate is checked by the web browser to make sure that it is valid.
3. IntelliMax Enterprise server shows an authentication page.
4. The user types their username and password and sends the information.
5. IntelliMax Enterprise Server confirms that the user is authorized:
   - If the user is authorized, IntelliMax Enterprise creates a session and the home page of the user is shown. The information visible is dependent on the rights of the user and the association groups.
   - If the user is not authorized, a failure message is returned and the user has to try to log on again.

12.0 Frequently Asked Questions

12.1 File Transfer out of the Hospital

What data is transferred?	See section 8 Data Transfer
Why is the data transferred?	See section 8 Data Transfer
Where does the transfer occur?	Machine data is transferred from the Elekta product to the IntelliMax Agent computer for interpretation or temporary storage. The data is then transferred to IntelliMax Enterprise as collected or on a schedule depending on the intended use of the data.
Where is the data kept and for how long?	IntelliMax Enterprise servers are hosted securely by Elekta. All machine data is kept for a maximum of 30 days on the IntelliMax Enterprise but can be transferred internally to Elekta Business Intelligence data warehouse for more analysis.
How is data transfer done?	All communication between IntelliMax Agent and IntelliMax Enterprise is encrypted HTTPS using SSL 256 bit encryption, using port 443.
What elements of personal data (Person Identifiable Information) are included in the file or data transfer?	No patient or personal data is transferred from the hospital with IntelliMax Agent. IntelliMax Agent only collects data from the Elekta products in relation to operation and status of the machine, not the patient in treatment. Remote Access clients give remote access to the graphical user interface of the medical product therefore the remote engineer can be exposed to personally identifiable information. But, this is no different to when the Engineer is in front of the machine and sees the same data during a service visit to the hospital. The Elekta IntelliMax™ support user can also transfer files off the Elekta product (depending on the remote access client) used on specified locations through IntelliMax Enterprise. All users with access to IntelliMax Enterprise or to use the file transfer functions in Remote Access must obey local laws and applicable employee governance to ensure correct data handling, storage and removal. Failure to comply will result in removal of access to Elekta IntelliMax systems and could result in dismissal and other legal action.

12.1 File Transfer out of the Hospital (continued...)

Are there externally imposed limits on the purpose for which personal data can be collected?	The visibility of personal data by Elekta IntelliMax™ support user will only be necessary when the diagnosis of a fault requires the Clinical User to step through the clinical program. The hospital has complete control of access limit. Elekta is prohibited from further using or disclosing individually identifiable health information for any purpose other than the purpose stated in the Purchasing & Licensing Agreement as part of the original purchase of the Elekta product.
Are there likely to be onward transfers of personal information to other jurisdiction?	All Elekta Employees and contractors must obey the Elekta Privacy and Security Policy which states: Elekta must use applicable administrative, technical and physical safeguards to prevent uses and disclosures of protected patient personal data/health information not permitted by applicable directives and laws. All users with access to IntelliMax Enterprise or to use the file transfer functions in Remote Access must obey local laws and applicable employee governance to ensure correct data handling, storage and removal. Failure to comply will result in removal of access to Elekta IntelliMax systems and could result in dismissal and other legal action.

12.2 Security

What requirements are there for applicable security measures to prevent personal data loss, and against unauthorized access, use, modification, disclosure or destruction? How are they conveyed to employees?	All Elekta Employees and contractors must obey the Elekta Privacy and Security Policy which states: Elekta must use applicable administrative, technical and physical safeguards to prevent uses and disclosures of protected patient personal data/health information not permitted by applicable directives and laws. All users with access to the IntelliMax Enterprise or to use the file transfer functions in Remote Access must obey local laws and applicable employee governance to ensure correct data handling, storage and removal. Failure to comply will result in removal of access to the Elekta IntelliMax™ systems and could result in dismissal and other legal action.
What, if any, specified security procedures are necessary or followed—for example, access control, encryption, and audit trails?	IntelliMax Enterprise requires each user to have a unique user name ID and password to access the system. Each user must change their password every 90 days as a further security measure. The password complexity is high, requiring the users to use eight or more characters, and a combination of mixed case alphanumeric digits. IntelliMax Enterprise automatically logs off inactive users to prevent unauthorized use of authorized access. Audit trails of all remote sessions and file transfers can be viewed from IntelliMax Enterprise and printed out if necessary.
What Security and Privacy requirements are covered by the use of IntelliMax Agent?	IntelliMax Agent has satisfied most major Security and Privacy requirements through a VeriSign Audit undertaken by our 3rd Party supplier: Axeda. This audit is based on: ISO 17799 Security Standard, Sarbanes Oxley Section 404, Gramm-Leach-Bliley Act, HIPAA Security Standard, NERC Urgent Action Standard 1200, CA Notice of Security Breach, 21 CFR Part 11, Information Security Forum Standard of Good Practice, IT Control Standards for Sarbanes Oxley (ITGI/ISACA), and Payment Card Industry (PCI) Data Security Standards.

12.3 Virtual Private Networks

Why does Elekta IntelliMax not support VPN connections?
1. We do not support VPN access for Elekta IntelliMax, but do put the control in the hands of the hospital at all times.
2. Given the way the information is encrypted when sent from IntelliMax Agent, you cannot monitor the outbound packets. • However, the Agent is in the hospitals control, and all data sent is visible on both the Agent and on the IntelliMax Enterprise. • Elekta allows customers' access to their own devices on the IntelliMax Enterprise This allows them to see the data that is collected from their device(s) • It is against our policies to automatically upload any patient data (which is sensitive personal data) to IntelliMax Enterprise. Elekta will not allow or facilitate any such up load and will take active steps to enforce this policy in the event of a breach. The use of uncontrolled Screen sharing (IntelliMax Connect or others) could result in the disclosure of patient to the person viewing the screen. Elekta employees are aware and regularly educated on their duties when dealing with patient data.
3. VPN solutions are not as controlled or auditable as IntelliMax Connect.
4. VPN solutions require extensive validation for each customer.
5. They do not offer the full range of remote capabilities Elekta can provide via Elekta IntelliMax (automated data, notifications etc.).
6. VPN solutions are subject to security vulnerabilities.
7. They do not easily support automatic software downloads and updates.
8. With Elekta IntelliMax: • The hospital can install one IntelliMax Agent PC. They then have control over access (i.e. turn it off to stop it) • All communication is outbound only, is secure and does not let Elekta on their network without explicit permission each and every time. • All connections are audit logged. • It scales for Elekta as we do not need to maintain VPN access and authenticate to each of our 6000 customers.
9. You don't need an Elekta linac to install an IntelliMax Agent PC to get remote access onto the Treatment Network

12.4 Technical Safeguards

Can software not authorized by Elekta be installed on the Elekta product?	No. IntelliMax Agent must be dedicated for the use of Elekta IntelliMax. It is the It is the responsibility of the hospital to keep the integrity of the IntelliMax Agent computer. The IntelliMax Agent software is designed to be run on a dedicated computer and is not tested with any other software.
Can the operating system security patches or other software be installed?	See section 9.2 Virus & Malware Protection & Microsoft hotfixes and patches
Can the IntelliMax Agent be serviced by remote?	Yes, IntelliMax Connect is installed on the IntelliMax Agent to allow for remote access if it is necessary.
Does the IntelliMax Agent computer support user specific ID and password?	The IntelliMax Agent computer must have an administrator account.
What are the IntelliMax Enterprise user password complexity requirements?	The password is a minimum of eight characters long. The password contains characters from a minimum of three of the five categories as follows: • English uppercase characters (A – Z) • English lowercase characters (a – z) • Base 10-digits (0 – 9) • Non-alphanumeric (for example: !, $, #, or %) • Unicode characters. Users must change their password at intervals of 90-day intervals.
Are access sessions terminated after a predetermined length of inactivity?	Sessions to IntelliMax Enterprise are automatically terminated after a period of inactivity. Remote Access sessions will time-out because of inactivity if less than 4096 bytes are transmitted in a session for 15 minutes. For Treatment Planning Systems, the hospital-based user selects the quantity of time the session will stay active.
What state must the IntelliMax Agent computer be left in?	The IntelliMax Agent computer must stay on 24 hours a day in order to collect and upload the machine data and log files over night. It is not necessary for the hospital personnel to log on to the IntelliMax Agent computer for it to operate correctly.
Is it necessary to do maintenance on the computer?	See section 9.2 Virus & Malware Protection & Microsoft hotfixes and patches

12.5 Network

Can the IntelliMax Agent computer be integrated into the existing IP address numbering plan?	Yes, if IntelliMax Agent can communicate with the Treatment Network.
What other systems are necessary for IntelliMax Agent connection?	The Internet and any supported Elekta product in the hospital network that will be monitored by IntelliMax Agent or used for Remote Access. A compatibility matrix which shows the latest supported products is available from your local Elekta service representative and also displayed on the IntelliMax Agent configuration utility.
What are the network port and firewall requirements?	See section 9.1 Firewall Rules above.

12.6 Program Maintenance

Can the system installed in the hospital be integrated into the site backup systems?	No, as IntelliMax Agent only operates as a Gateway to temporarily keep and forward information, it is not critical to the operation of the attached machines or the hospital. If IntelliMax Agent does not operate correctly, it can be installed again.
What is the average frequency of upgrades to IntelliMax Agent?	IntelliMax Agent upgrades are released when new functionality or maintenance releases are necessary.
How are the upgrades done?	Once the hospital provides permission, IntelliMax Agent is upgraded remotely. The upgrades are designed to require no intervention at the hospital and occur out of clinical hours unless an Engineer is present. (For the function of Elekta IntelliMax, clinical hours are between 06:00 to 20:00 local time). Elekta Field Change Order process is currently used to give Notification to a named person(s) at the hospital before an upgrade occurs and if necessary, notification on the success of the upgrade can also be given.

12.7 Remedies

What formal mechanism is there for individuals to complain about breaches and to get redress?	The Clinical User must understand the limitations imposed by local hospital privacy policies before using the Remote Access program. But if a complaint occurs, Elekta has an established Customer Feedback Reporting (CFR) process to make sure that all complaints are addressed.
What do we do if support is necessary for IntelliMax Agent?	Contact your local Elekta support representative or the Regional Elekta Care Support center.

Appendix A – Hospital Prerequisites

This form contains the information that the hospital must give the engineer who will install Elekta IntelliMax, before the installation starts.

- IntelliMax Agent MUST be dedicated for the function of Elekta IntelliMax and not used for other functions—for example web access
- IntelliMax Agent MUST NOT be installed on a clinical Elekta product

It is the responsibility of the hospital to install and do the maintenance of the anti-virus and anti-malware software, firewalls and Microsoft hotfixes

The engineer who does the installation must have the following information before the installation begins:

Anti-virus/Anti-malware software pre-installed?

☐ **Yes** ☐ **No**

A1

Desired Hostname of the Agent computer:_____ Static IP Address:_____

Subnet Mask:_____ Default Gateway:_____

Primary DNS:_____ Workgroup (or Domain if required):_____

(Internet access)

A2

If an HTTP or SOCKS Proxy Server is used for access to the Internet, the Proxy address must be given.

_____

A3

If an authentication is necessary for the proxy, record these credentials at the time of installation.

Username (if available):_____ Password (if available):_____

A4

Do you need to know the MAC address of the IntelliMax Agent computer (for configuration of the hospital firewall)?

☐ **Yes** ☐ **No**

A5

Access out of the hospital network must be given to:

IntelliMax Enterprise	elekta.axeda.com	port 443
GAS Japan	ghjap1.axeda.com	port 443
GAS Japan	ghjap2.axeda.com	port 443
GAS USA	All ghsj1.axeda.com	port 443
GAS USA	ghsom1.axeda.com	port 443
GAS USA	gas-bo6.axeda.com	port 443
GAS UK	ghuk1.axeda.com	port 443
GAS Germany	gas-de2.axeda.com	port 443
GAS Germany	gas-de3.axeda.com	port 443
GAS Australia	gas-aus2.axeda.com	port 443
GAS Australia	gas-aus3.axeda.com	port 443

A6

If the connected devices are on a separate subnet (not directly connected to the hospital network) a second IP Address will need to be assigned to the IntelliMax Agent computer for access to device network:

Static IP Address:_____ Subnet Mask:_____
(Device access)

A7

Is (temporary) Internet access for the service engineer laptop available? (This will help the Installation procedure.)

☐ **Yes** ☐ **No**

A8

If Yes, do you need to know the MAC address of the service engineer's laptop (for configuration of the hospital firewall)?

☐ **Yes** ☐ **No**

Appendix B – Feedback

If you have identified a reason why IntelliMax Agent cannot be installed—funding, IT security, infrastructure, etc.—please return to **support@elekta.com**. This will allow Elekta to address the reasons given and improve the service provided.

Does the hospital already have remote access or monitoring from any other equipment provider:

☐ **Siemens** ☐ **Varian** ☐ **Philips** ☐ **Other** _____

Hospital:_____

Country:_____

Hospital contact:_____

Elekta contact:_____

We are healthcare technology innovators, specializing in radiotherapy treatments for cancer and brain disorders.

We help clinicians to improve patients' lives through our forward-thinking treatment solutions and oncology informatics, creating focus where it matters to achieve better outcomes.

Elekta

Elekta Offices

Elekta AB
Box 7593
SE–103 93
Stockholm, Sweden
T +46 8 587 254 00
F +46 8 587 255 00

Europe, Middle East, Africa
T +46 8 587 254 00
F +46 8 587 255 00

North America
T +1 770 300 9725
F +1 770 448 6338

Latin America, South America
T +55 11 5054 4550
F +55 11 5054 4568

Asia Pacific
T +852 2891 2208
F +852 2575 7133

Japan
T +81 3 6722 3800
F +81 3 6436 4231

China
T +86 10 5669 2800
F +86 10 5669 2900


elekta.com


/elekta


@elekta


/company/ elekta

Art. No.4513 371 0831 V8