# Rubo Medical-Imaging DICOM Viewer 2.0 ...including DICOM Communication DICOM Anonymizer DICOM Parser DICOM Pyr Burner

OICOM DVD Burner
 Waveform viewer

• IVUS Longitudinal viewer

# Network/Floating License Installation Instructions for the USB Key license

Installation steps:

On the Windows computer that will act as License Manager (**SERVER**):

- 1. Install Gemalto/Sentinel Run-time environment, SERVER
- 2. Plug in the red USB hardware key, SERVER
- 3. Setup the Gemalto/Sentinel License Manager, SERVER

On the **CLIENT** computer:

- 1. Install the DICOM Viewer and Gemalto/Sentinel environment, CLIENT
- 2. Setup the Gemalto/Sentinel License Manager, CLIENT
- 3. Open port 1947 in the firewall(s)

General information:

- What to distribute to the client PC's
- Setup a different server IP address, CLIENT
- Registration / Activation window is displayed

See the next pages..

These instructions apply to DICOM Viewer 2.0, build 6553 or later. The latest versions of the Gemalto/ Sentinel/HASP Run-time environment and Drivers can be downloaded from our website: <u>www.rubomedical.com/download</u>.

# Install Gemalto/Sentinel Run-time environment, SERVER

You must have administrator privileges to install the Gemalto/Sentinel Run-time environment.

Download 'HASPUserSetup.exe' from our website: <u>www.rubomedical.com/sentinel</u>. Run it to install the Gemalto/Sentinel Run-time environment. Click through all the setup screens and wait for the 'successfully installed' message. See images below.

Sentinel Runtime Setup	– 🗆 X	🛃 Sentinel Runtime Setup	– 🗆 X
	Welcome to the Sentinel Runtime Installation Wizard	Updating System The features you selected are currently being installed.	gemalto <sup>×</sup>
cemalto	It is strongly recommended that you exit all Windows programs before running this setup program. Click Cancel to quit the setup program, then close any programs you have running. Click Next to continue the installation. WARNING: This program is protected by copyright law and international treaties. Unauthorized reproduction or distribution of this program, or any portion of it, may result in severe civil and criminal penalties, and will be prosecuted to the maximum extent possible under law.	Install drivers	
security to be free	< Back Next > Cancel	x	Cancel



Communication is routed through port 1947. Make sure that this port is not blocked.

# Plug in the red USB hardware key, SERVER

The red USB hardware key is programmed with the number of simultaneous users you have ordered. This key must be attached to the server PC at all times to enable clients to logon and use the DICOM Viewer.



After you have installed the Gemalto/Sentinel Run-time environment, plug in the USB hardware key in any USB port of your appointed server PC. The device driver software will now be installed.

The light in the USB key will switch on and wait for the message 'Your device is ready to use'. This will take a few minutes. See the images below.



Click on the driver installation tray icon to view the progress



#### Setup the Gemalto/Sentinel License Manager, SERVER

Open the internet browser to setup the Gemalto/Sentinel License Manager. In the address field type: '<u>http://localhost:1947</u>' and press enter. The Gemalto/Sentinel License Manager Admin Control Center' will show (*image 1*).

The menu on the left, under Options, shows 'Configuration'. Click it and next click on tab 'Access from Remote Clients' (*image 2*).

Make sure that 'Allow access from Remote Clients' is checked. In the 'Access Restrictions' box, enter the line 'allow=all' and click 'Submit' (*image 3*).

You now allow all client PCs to access the License Manager, asking permission to start the DICOM Viewer.

The settings are stored in a file called 'hasplm.ini', the exact location is shown below all the setting options. See *image 2* and 3.



1. Admin Control Center

Gemalto Sentinel ACC:	Configura × +					-		×
< → ひ ⋒	Iocalhost:	1947/_int_/c	onfig_from.html			☆ ☆	0	
gemalto <sup>×</sup>				Senti	nel Admin Co	ontrol C	ente	r
Options	Configuration	for Sentin	el License Manager					
Sentinel Keys	Basic Settings	Users	Access to Remote License Managers	Access from Remote Clients	Detachable Licenses	Network	]	
Features Sessions Update/Attach Access Log Configuration Diagnostics Help About	Allow Access Re Access Re	ess from Remo astrictions eent Client Acces	E Clients     You may experience a delay       Image: Second secon	of a few minutes before your changes t der in which they are specified. As soon d of list	ake effect. as a match is found, evaluatio	n stops.		
Languages English Deutsch Español Français Haliano 日本語								

☆ 幸 🔍 …  $\leftarrow$   $\rightarrow$  O  $\widehat{m}$  O localhost:1947/\_int\_/config\_from.html gemalto Sentinel Admin Control Center Configuration for Sentinel License Manager Options 
 Basic Settings
 Users
 Access to Remote License Managers
 Access from Remote Clients
 Detachable Licenses
 Network
 Sentinel Keys Products Features Sessions Currently, a network-enabled Sentinel protection key is not connected to this License Manager Allow Access from Remote Clients Vou may experience a delay of a few minutes before your changes take effect. Update/Attach Access Restrictions allow=all Access Log Configuration Diagnostics Help About The entries are evaluated in the order in which they are specified. As soon as a match is found, evaluation stops, allow-all is implicitly added to end of list Submit [Cancel] [Set Defaults] Activate and save changes Show Recent Client Access Language English Deutsch Español Français Italiano igUrl('conf\_from.html')

3. Set the Access Restrictions

# Install the DICOM Viewer and Gemalto/Sentinel environment, CLIENT

The installation of the DICOM Viewer and the Gemalto/Sentinel Run-time environment is fully automated. The user only has to click through the setup screens.

The user must have administrator privileges to install.

It is important to pass the IP address of the server PC to the client installation process. At every startup of the DICOM Viewer, the viewer will search for the server/PC to which the USB key is attached. To speed up the search, the IP address of the server should be set in the run-time configuration file.

For each client, start the DICOM Viewer installation by passing the IP address to 'DicomViewerSetup32.exe' via the command line parameter '-IP:' as follows:

D:\>DicomViewerSetup32.exe -IP:192.168.2.101 Example IP address 192.168.2.101

Accept the end-user license agreement and click 'Next'. On the next pages, choose to install the offline help files and make sure that 'USB Hardware Key Drivers' is checked.

You can also choose to install the DICOM Viewer on the server and make it accessible to every client. However, it's then still necessary to install the Gemalto/Sentinel Run-time environment on each client PC. See 'Install Gemalto/Sentinel Run-time environment, SERVER' to install the environment and 'Setup the Gemalto/Sentinel License Manager, CLIENT' or 'Setup a different server IP address, CLIENT' to setup the servers IP on the client PC

The DICOM Viewer setup file is available here: <u>www.rubomedical.com/download</u>.

To set up or change the IP address manually *after* installation of the environment, see 'Setup the License Manager, CLIENT'.

#### Setup the Gemalto/Sentinel License Manager, CLIENT

**You can skip this** if the server PC is located on your local network. The default settings apply and a broadcast will be used to find the server.

**You can skip this** if the installation of the DICOM Viewer and Gemalto/Sentinel environment succeeded and the server IP address was set as command-line argument of the setup file. See 'Install the DICOM Viewer and Gemalto/Sentinel environment, CLIENT'.

Open a internet browser to setup the Gemalto/Sentinel License Manager. In the address field type: '<u>http://localhost:1947</u>' and press enter. The 'Gemalto/Sentinel Admin Control Center' will open.

The menu on the left, under Options, shows 'Configuration'. Click it and next click on tab 'Access to Remote License Managers'. Make sure that 'Allow Access to Remote Licenses' is checked (*image 2*).

If you do not know the IP address of the server PC with the License Manager -or- the server PC is located on your local network, check 'Broadcast Search for Remote Licenses' (*image 2*). These settings should be checked by default.

If you do know the IP address of the server PC and/or it is located outside your local network, please do the following: **UN**check 'Broadcast Search for Remote Licenses' and check 'Aggressive Search for Remote Licenses'. In the 'Remote License Search Parameters' list, enter the IP address of the server PC (*image 3*).

Press 'Submit' to save the changes. The changes are now stored but you may need to **restart** your PC (or restart the Gemalto/Sentinel service) for the changes to take effect.

The settings are stored in file 'hasplm.ini', the exact location is shown below all the setting options. You can distribute this file to all client PC's to prevent you from configuring each client individually.

Gemalto Sentinel ACC	CHelp x + -		
$\leftarrow \rightarrow \circ$	🔉 💿 localhost 1947/_int_/ACC_help_index.html 🙀 🗲	0	
gemalto <sup>×</sup>	Sentinel Admin Control Cer	nter	
Options	Admin Control Center Help		1
Sentinel Keys Products	Admin Control Center Help		
Features Sessions	Welcome to the Admin Control Center. This application enables you to manage access to software licenses and Features, to control detachable licenses, to control sessions, and to diagnose problems.		
Update/Attach	Note: You can select the language in which Admin Control Center is displayed from the bottom of the Options pane.		
	The Admin Control Center enables you to monitor the following:		
Access Log Configuration Diagnostics	<ul> <li>All the Sentinel protection keys that are currently available on the network server, including their identity, type, and location</li> <li>The number of users currently logged into a protection key, and the maximum number of users allowed to be simultaneously logged into that specific key</li> <li>The Features to which each protection key allows access, and any restrictions that apply to the Feature</li> <li>The users who are currently logged into a specific protection key, including detailed login information</li> </ul>		
Help About	Note: SL UserMode keys are only displayed for the local (Windows) machine. SL UserMode keys are not displayed when the <u>configuration</u> parameter Do Not Load hasplmv.exe is selected.		
	You can perform actions, such as:		
	Detaching a license from the network and attaching it to your machine or a different recipient machine     Cancelling a detachable license prematurely     Installing an update to a license on a key that is visible in Admin Control Center		
	You can make basic configuration changes, including:		
Languages	<ul> <li>Setting the display refresh time</li> <li>Configuring access permissions from a client machine to a remote server, and configuring a server to allow it to be remotely accessed</li> <li>Defining values for Products with detachable licenses</li> </ul>		
English	The Diagnostics page enables you to view system information related to the current Sentinel License Manager, and to generate reports.		
Deutsch	Related Topics		
Español	Security Considerations		
Français	Serieura Reys Products		
Italiano	Features		
日本語	3-trashulis Update/Attach		



Completo Sontinel ACC						
$\rightarrow$ () (	O localhost:1947/ int	/config to html			~ <u>~</u>	•
		soning_tontin				_
gemalto			Senti	inel Admin Co	ontrol C	ente
Options	Configuration for Senti	nel License Manager				
Sentinel Keys	Basic Settings Users	Access to Remote License Managers	Access from Remote Clients	Detachable Licenses	Network	1
eatures	Allow Access to Remot	e Licenses 🔽 You may e	xperience a delay of a few minutes before	vour changes take effect.		
Sessions	Broadcast Search for F	temote Licenses		,		
Indate/Attach	Aggressive Search for	Remote Licenses				
opulaterAttach	Remote License Searc	h Parameters				
Access Log						
Configuration						
Diagnosics						
Help						
About						
		Submit Cance	Set Defaults			
Languages						
Languages						
English						
Deutsch Español						
Francais						
Italiano						
日本語						

2. Set the access parameters for local search

Gemalto Sentinel ACC:	Configura × +				1 <u></u> 1	o ×
<  →  ପ  ଲ	localhost:1947/_int	/config_to.html			☆ ≱	
gemalto <sup>×</sup>			Senti	nel Admin Co	ontrol Ce	nter
Options	Configuration for Sent	inel License Manager				
Sentinel Keys	Basic Settings Users	Access to Remote License Managers	Access from Remote Clients	Detachable Licenses	Network	
Products Features Sessions	Allow Access to Remo Broadcast Search for	te Licenses Vou may ex	perience a delay of a few minutes before	your changes take effect.		
Lindate/Attach	Aggressive Search for	Remote Licenses 🗹				
Access Log Configuration Diagnostics Help About	Remote License Sear	h Parameters 192.168.2.101 Submit Cancel	Set Defaults			
Languages English Deutsch Español Français		C:\Program Files (x86)/C	ommon Files Aladdin Shared HASP (haspim i	ni		
Italiano 日本語						-

3. Set the access parameters, search outside your local network

## Open port 1947 in the firewall(s), XP and Vista

The communication between the client PCs and server is routed through port 1947. Your Windows Firewall should be open to port 1947, TCP and UDP.

To open port 1947, TCP and UDP, do the following:

Windows XP:

- 1. Go to the Control Panel
- 2. Click 'Security Center'
- 3. Click 'Windows Firewall'
- 4. Go to the tab 'Exceptions'

Windows Vista:

- 1. Go to the Control Panel
- 2. Click 'Windows Firewall'
- 3. Click 'Change Settings'
- 4. Go to the tab 'Exceptions'

Press 'Add port...' and add TCP port number 1947, as shown below, and press 'OK'. Do the same for UDP port 1947.

Windows Firewall Settings	🦋 Windows Firewall Settings
General Exceptions Advanced	General Exceptions Advanced
Exceptions control how programs communicate through Windows Firewall. Add a program or port exception to allow communications through the firewall.	Exceptions control how programs communicate through Windows Firewall. Add a program or port exception to allow communications through the firewall.
Add a Port	Windows Firewall is currently using settings for the private network location. What are the risks of unblocking a program?
Use these settings to open a port through Windows Firewall. To find the port number and protocol, consult the documentation for the program or	Io enable an exception, select its check box:
service you want to use.	Program or port
	Microsoft Office OneNote
Part 1047 TCD	Microsoft Office Outlook
Name: Port 1947 TCP	Netlogon Service
10/7	✓ Network Discovery
Port number: 1947	✓ octoshape.exe
Particula o	Performance Logs and Alerts
Protocol: OICP	Port 1947 TCP
OUDP	Port 1947 UDP
0	Remote Administration
What are the ricks of energing a port?	Remote Assistance
	Remote Desktop
Change scope OK Cancel	Remote Event Log Management
	Remote Scheduled Tasks Management
Add program Add port Properties Delete	Add program Add port Properties Delete
Notify me when Windows Firewall blocks a new program	▼ Notify me when Windows Firewall <u>b</u> locks a new program
OK Cancel Apply	OK Cancel Apply

Add port 1947, UDP and TCP

Exceptions added to the list

This is your Windows software firewall. If you are connected to a router, refer to the documentation of your router how to open port 1947, UDP and TCP.

### Open port 1947 in the firewall(s), Windows 7 and up

Do the following to open port 1947 when using Windows 7 and up:

- 1. Go to the Control Panel, System and Security section
- 2. Open 'Windows Firewall'
- 3. Click 'Advanced Settings'
- 4. Go to 'Inbound Rules' and click 'New Rule...'
- 5. Choose 'Port' as the new rule type
- 6. Select 'TCP' as protocol
- 7. Enter 1947 as specific local port
- 8. Click 'Next' a few times to enter a name for the inbound rule
- 9. Press Finish
- 10. Now add the same rule for the 'UDP' protocol

Windows Firewall with Adv	vanced Security					X
<u>File Action View H</u> elp						
🗢 🔿 🖄 📰 🗟 🚺						
🔗 Windows Firewall with A	Inbound Rules				Actions	
🗱 Inbound Rules	Name	Group	Profile	Enable 🔦	Inbound Rules	•
Connection Security P	Microsoft Office Outlook		Private	Yes	Rule	
Monitoring	Port 1947 TCP		All	Yes	V Filter by Drofile	<b>`</b>
Monitoring	Opril 1947 UDP		All	Yes	Pilter by Profile	•
	BranchCache Content Retrieval (	BranchCache - Conten	All	No	Filter by State	•
	BranchCache Hosted Cache Serv	BranchCache - Hosted	All	No	Filter by Group	•
	BranchCache Peer Discovery (WS	BranchCache - Peer Di	All	No	View	•
	Connect to a Network Projector (	Connect to a Network	Private	No	a Refresh	
	Connect to a Network Projector (	Connect to a Network	Domain	No		
	Connect to a Network Projector (	Connect to a Network	Domain	NO	Export List	
	Connect to a Network Projector (	Connect to a Network	Private	NO	🛿 Help	
	Connect to a Network Projector (	Connect to a Network	Domain	No	Port 1947 TCP	
	Connect to a Network Projector (	Connect to a Network		No	Disable Rule	
	© Core Networking - Destination U	Core Networking	All	Yes		
	© Core Networking - Destination U	Core Networking	All	Yes	a Cut	
	Core Networking - Dynamic Hos	Core Networking	All	Yes	🛍 Сору	
	Core Networking - Dynamic Hos	Core Networking	All	Yes	🗙 Delete	
	Ocore Networking - Internet Grou	Core Networking	All	Yes	Properties	
	Core Networking - IPHTTPS (TCP	Core Networking	All	Yes		
	Ocore Networking - IPv6 (IPv6-In)	Core Networking	All	Yes		
	Ocore Networking - Multicast List	Core Networking	All	Yes		
	Ocore Networking - Multicast List	Core Networking	All	Yes		
	Ocore Networking - Multicast List	Core Networking	All	Yes		
	Ocore Networking - Multicast List	Core Networking	All	Yes 🖕		
<ul> <li>↓</li> </ul>	· · · · · · · · · · · · · · · · · · ·			•		

Both TCP and UDP inbound rules are added

This is your Windows software firewall. If you are connected to a router, refer to the documentation of your router how to open port 1947, UDP and TCP.

#### What to distribute to the client PC's

Scenario 1: each client installs the DICOM Viewer on their own PC. Distribute the file 'DicomViewerSetup32.exe' to each client including a created batch file with the servers IP address as a command-line argument.

Download the installation file of the DICOM Viewer here: <u>www.rubomedical.com/download</u>

See 'Install the DICOM Viewer and Gemalto/Sentinel environment, CLIENT'.

Scenario 2: each client has access to the DICOM Viewer which is installed on the server PC only.
Distribute the file 'HASPUserSetup.exe' to each client. Download the Gemalto/Sentinel driver installation file here:

www.rubomedical.com/sentinel

See 'Setup the Gemalto/Sentinel License Manager, CLIENT' for manual installation of the server IP address.

\_or\_\_

See 'Setup a different server IP address, CLIENT' for automatic installation.

# Setup a different server IP address, CLIENT

When the IP address of the server PC has changed, all client PCs have to be setup again. There are several ways of doing this:

- 1. Add the IP address as described in 'Setup the Gemalto/Sentinel License Manager, CLIENT' on a single client PC. Submit the changes and copy the new configuration file 'hasplm.ini' to every other client PC. The location of the configuration file is displayed just below the 'Submit' button.
- 2. Reinstall the DICOM Viewer on all clients as described in 'Install the DICOM Viewer and Gemalto/Sentinel environment, CLIENT'.

# **Registration / Activation window is displayed**

When the Registration / Activation window is displayed at start-up, the DICOM Viewer could not find a USB hardware key on the network or on the local PC. The software has now switched to software key (Activation Key) licensing.

Force the DICOM Viewer on the client PC to check for the USB hardware key license by either:

- 1. Plugging in *any* USB device in the client PC when the Registration / Activation window is displayed. Within a few seconds, the software will try to find the USB hardware key. If successful, a pop-up window will ask if this license must be used. Choose 'Yes' and a restart of the DICOM Viewer is required.
- Start the DICOM Viewer with argument '-hkey'. This will force a USB hardware key check at start-up just once. If not found, the software will again switch to software key (Activation Key) licensing. Repeat this step to force the USB hardware key check.
   Example: 'DICOMViewer.exe -hkey'.

After a successful USB hardware key license check and start of the DICOM Viewer,

the next start will automatically check for the USB key.

The USB hardware key may not be found when:

- 1. The USB hardware key drivers (<u>www.rubomedical.com/download</u>) are not installed. Download the drivers and install them or run the DICOM Viewer setup application and make sure that 'USB Hardware Key Drivers' is checked on the 'Set Additional Tasks' page of the installation process.
- 2. The USB hardware key is not plugged in to the local PC or network server.
- The client PC cannot find the USB hardware key on the network. On the client side, check the configuration settings as described in section 'Setup the Gemalto/Sentinel License Manager, CLIENT' of this document. On the server side, check installation of the USB hardware key drivers, check port 1947 is open and that the USB key is plugged in.