syngo.via WebViewer

Operator Manual – Administration

VA20B

siemens-healthineers.com

Table of contents

● 1 Introduction 5

1.1 Intended purpose 5

1.1.1 Intended use 5

1.1.2 Indications for use 6

1.1.3 Patient target group 6

1.2 Clinical benefits 6

1.3 User profiles 7

1.4 Legal notes 7

● 2 Safety advisory 9

2.1 Image processing and viewing 9

2.2 Connectivity 10

2.3 Administration and maintenance 10

2.4 Data protection and security 11

2.5 Hardware and software requirements 12

● 3 Server start and stop 13

3.1 Starting the syngo.via WebViewer server 13

3.2 Checking the syngo.via WebViewer availability 13

3.3 Starting, stopping, or restarting the syngo.via WebViewer services 14

● 4 syngo.via WebViewer client 15

4.1 Configuring syngo.via WebViewer access to syngo.via database 15

4.1.1 Adding a Node 15

4.1.2 Changing a Node 16

4.1.3 Deleting a Node 16

4.2 Client installation for web browsers 17

4.3 Client installation for mobile devices 17

4.3.1 Installing the application for mobile devices 17

4.3.2 Configuring the server information 17

4.3.3 Uninstalling the application for mobile devices 18

● 5 Maintenance 19

5.1 Backup and recovery 19

5.1.1 Configuring the backup settings 19

Table of contents

5.2 Administration Portal access 20
5.2.1 Accessing the Administration Portal logon screen 20
5.2.2 Entering the Administration Portal 20
5.2.3 Accessing the Online Help 21
5.3 System monitoring 21
5.3.1 Checking the condition of the syngo.via WebViewer services 21
5.3.2 Checking the render server and web server log files 22
5.3.3 Changing the granularity of the log files 22
5.3.4 Configuring the backup time of log files 22
5.3.5 Downloading a log file archive 23
5.4 Server configuration 23
5.4.1 Configuring the syngo.via database 23
5.4.2 Changing or renewing an SSL certificate 24
5.4.3 Changing the SSL ports 25
5.4.4 Configuring the Autologout period 25
5.4.5 Installing a new license 26
5.4.6 Configuring biometric login for mobile devices 27
5.5 Update 27
● 6 Data and system security 29
6.1 Communication ports 29
6.2 Siemens Remote Service 31

1 Introduction

syngo.via WebViewer provides access to rendered medical image data through web browsers and mobile devices. Image data includes 2D images as well as volumetric data.

syngo.via WebViewer is a client-server product. It supports secure web-enabled client devices with LAN or wireless connections. The web client is available for common web browsers without any installation procedure or the need for additional plugins. The mobile client for iOS mobile devices is an app which can easily be installed by using the official Apple App Store.

For *syngo*.via server M/L/XL grade *syngo*.via WebViewer can be installed on the same hardware. For M grade *syngo*.via servers, one client is allowed to run on a *syngo*.via server. For L/XL grade *syngo*.via servers, up to three WebViewer clients can run on a *syngo*.via server.

If more than three clients are required, *syngo*.via WebViewer server has to run on its own hardware, which is independent of *syngo*.via system components. In addition to the image data, *syngo*.via WebViewer server also relies on the user management of the *syngo*.via server. Therefore, the intended user group consists of internal clinical staff.

1.1 Intended purpose

1.1.1 Intended use

syngo.via WebViewer is a software-only device indicated for reviewing medical images from *syngo*. via. It supports interpretation and evaluation of examinations within healthcare institutions, for example, in Radiology, Nuclear Medicine and Cardiology environments (supported image types: CT, MR, CR, DR, DX, PET). It is not intended for storage or distribution of medical images.

syngo.via WebViewer is an option for the *syngo*.via system and cannot be run without it. It is client server architecture and the client is intended to run on web clients which are connected to the healthcare institution IT infrastructure where the customer will insure HIPAA compliance.

The communication of *syngo*.via WebViewer with connected medical IT systems will be done via standard interfaces such as but not limited to DICOM.

The system is not intended for the display of digital mammography images for diagnosis.

1.1.2 Indications for use

syngo.via WebViewer is indicated for reviewing medical images from *syngo*.via to support interpretation in the field of radiology, nuclear medicine and cardiology.

The system is **not** intended to be used as stand-alone device. It is intended to be an option for a *syngo*.via system only.

The system is **not** indicated for mammography images for diagnosis.

The system is **not** intended for storage or distribution of medical images from one medical device to another.

The application is **not** to be used as an archiving device for patients' image data.

The application is **not** to be used as a sole basis for clinical decisions.

1.1.3 Patient target group

syngo.via Web Viewer has neither limitations concerning the patient population (e.g. age, weight, health, condition) nor limitations concerning region of body or tissue type.

1.2 Clinical benefits

syngo.via WebViewer facilitates access with Apple mobile devices and WebBrowsers to images on *syngo*.via in diagnostic reading quality, including thin-slices and image reconstructions.

1.3 User profiles

Please note that the following profiles may vary in practice depending on (hospital) organization, qualification, and personal responsibilities, and can only be considered as a general guide.

The following user profiles have been identified for *syngo*.via WebViewer:

- **User**

  Mainly radiologists who review medical images from *syngo*.via and non radiologist physicians inside the hospital / facility of various specialities

- **Administrator**

  Executes updates/upgrades, is the first level in case of troubleshooting (according to call handling and incident management process)

1.4 Legal notes

This document is confidential, proprietary to Siemens Healthineers, protected by copyright laws, and licensed for use by customers only in strict accordance with the license agreement governing its use.

Any reports or other figures that appear in this document are merely illustrative and do not contain the names or data of real people.

Any similarity in names of people, living or dead, or in data is strictly coincidental and is expressly disclaimed.

Siemens Healthineers does not warrant that the material contained in its documentation is error-free.

Documentation supplied to Siemens Healthineers by third parties and included with this documentation is not warranted for accuracy or completeness. The information contained in this document is subject to change. Revisions and updates will be issued from time to time to document changes and/or additions.

1 Introduction

2 Safety advisory

Warnings indicate a potential hazard to the health or life of patients or personnel.

Cautions indicate conditions or consequences that you should pay particular attention to when working with *syngo*.via WebViewer, but no direct danger is involved.

If you encounter any serious problems during your work with *syngo*.via WebViewer, please let us know.

In addition, the competent authority of your country where the user and/or the patient is located, must be informed of such serious problems.

2.1 Image processing and viewing

⚠ CAUTION

Use of inappropriate devices (displays, printers) to review radiological images.

Incorrect review of images.

- Review of images require an optimum display of images. Only use suitable monitors and printers for review of images. Follow the maintenance and care instructions given in the manufacturer's documentation.

2.2 Connectivity

⚠ CAUTION

Firewall rules can block correct transfer of data.

Images or reports cannot be viewed.

- Check and verify transfer of all types of data before releasing the software for general use.

2.3 Administration and maintenance

⚠ CAUTION

Important settings are lost during update or modification of system.

System does not work as intended after an update/upgrade.

- Always perform a backup of the current installation before update or modification of the system.
- Always perform a backup of the current configuration (including role-specific settings, such as user profiles) before updating or modifying the system.

2.4 Data protection and security

⚠ **CAUTION**

Unauthorized access to the system.

Hazards up to and including loss of all patient data and non-operational system.

- The administrator is responsible for network security at the site. Set up firewalls and user account password protections. Do not allow users to change configuration files. Update virus protection software as required.

⚠ **CAUTION**

Unauthorized access to the system.

Hazards up to and including loss of all patient data and non-operational system.

- Check the log book periodically for failed login attempts and take appropriate measures to avoid unauthorized access to the system.

⚠ **CAUTION**

Use of an anti-virus software that is not provided by Siemens.

Malicious software can cause harms up to and including non-operational system and loss of all patient data.

- The administrator is responsible for the configuration of the anti-virus software. Configure and regularly update the anti-virus software.

2.5 Hardware and software requirements

For installation of *syngo*.via WebViewer, your computer must meet specific requirements.

For integrated and virtual *syngo*.via WebViewer installation, refer to the *Data Sheet* of *syngo*.via, chapter "Hardware Specifications & Virtual Deployments".

For dedicated *syngo*.via WebViewer refer to the *Data Sheet* of *syngo*.via WebViewer.

3 Server start and stop

3.1 Starting the syngo.via WebViewer server

✓ The *syngo*.via server is running.

◆ Switch on the *syngo*.via WebViewer server.

syngo.via WebViewer server services are automatically started.

ℹ *syngo*.via WebViewer server consists of services only. Therefore, *syngo*.via WebViewer server will automatically be available after the startup of the operating system. Logging on as an administrative user is not necessary.

3.2 Checking the syngo.via WebViewer availability

1 In your web browser, enter the following URL:

https://<WebViewer_server>:4443

<WebViewer_Server> can be the IP address or the hostname (if configured) of the *syngo*.via WebViewer server. **4443** is the default SSL port.

2 Log on with a *syngo*.via user account.

3 Check if *syngo*.via WebViewer is operational.

3.3 Starting, stopping, or restarting the syngo.via WebViewer services

syngo.via WebViewer consists of five different services:

- *syngo*.via WebViewer License Manager
- *syngo*.via WebViewer Logfile Copy
- *syngo*.via WebViewer Nexus
- *syngo*.via WebViewer SSL Render Server
- *syngo*.via WebViewer Web Server

These services are automatically launched on system startup and monitored by the Windows Service Control Manager. To start, stop, or restart any of these services, proceed as follows:

1. Log on to the Windows operating system.
2. From the Windows **Start** menu, choose **Administrative Tools** > **Services**.
3. Right-click one of the services mentioned before.
4. Choose **Start** from the context menu.

   – or –

   Choose **Stop** from the context menu.

   – or –

   Choose **Restart** from the context menu.

4 syngo.via WebViewer client

ⓘ *syngo*.via WebViewer clients are medical devices in their own right. See the respective user documentation which can be accessed directly in the software.

4.1 Configuring syngo.via WebViewer access to syngo.via database

syngo.via WebViewer accesses the *syngo*.via database directly. In the *syngo*.via WebViewer Administration Portal, the database access parameters for a *syngo*.via server are configured as a node. The WebViewer can access an arbitrary number of *syngo*.via servers. In the *syngo*.via WebViewer Administration Portal, a separate node is established for each *syngo*.via server.

ⓘ You can configure only one node or one *syngo*.via server access at a time.

4.1.1 Adding a Node

To configure access to a *syngo*.via database, configure a node with the appropriate server access data on the **Administration Portal** > **syngo.via Database**.

1 Click **Add New Node**.

2 Enter a **Node Name for Users**.

Enter a friendly name to easily identify the node.

3 Enter the name of the desired *syngo*.via server.

You can enter an IP address or the hostname of this server.

4 Enter the *syngo*.via server port number.

The default port for *syngo*.via webservices is **`4510`**.

5 Click **Save** to confirm the new node.

A new database access is created.

To retrieve any images from the *syngo*.via database, the corresponding network share needs to be configured.

4.1.2 Changing a Node

To change an existing node, perform the following steps on the **Administration Portal** > **syngo.via Database**.

1 From the dropdown list select the node you want to change.

2 Enter the name of the *syngo*.via server.

You can enter an IP address or the hostname of this server.

3 Enter the *syngo*.via server port number.

The default port for *syngo*.via webservices is **`4510`**.

4 Click **Save** to confirm the new node.

The accessed database has been changed.

4.1.3 Deleting a Node

To delete a node, perform the following steps on the **Administration Portal** > **syngo.via Database**.

1 From the dropdown list select the node you want to delete.

2 Click **Delete this Node**.

A confirmation prompt will ask you, if you really want to delete this node.

3 Click **OK**.

The database access is removed.

4.2 Client installation for web browsers

syngo.via WebViewer only requires a supported web browser. No additional plugin is required.

The user is notified if the web browser that is used is not supported.

4.3 Client installation for mobile devices

4.3.1 Installing the application for mobile devices

◆ Download the *syngo*.via WebViewer application from the Apple App Store.

4.3.2 Configuring the server information

Upon the first startup of the *syngo*.via WebViewer application for mobile devices, certain information about the local *syngo*.via WebViewer server must be configured.

✓ The connection information has been provided by the IT administrator.

1 Start the *syngo*.via WebViewer application on the mobile device.

2 Tap inside the **Server** text field.

3 Tap **Add Server...**.

4 In the **Server Name** text field, enter an arbitrary name to identify the *syngo*.via WebViewer server.

5 In the **Address** text field, enter the IP of the *syngo*.via WebViewer server.

6 In the **SSL Port** text field, enter the mobile device SSL port as configured in the *syngo*.via WebViewer Administration Portal. Leave this text field empty to use the default SSL port.

7 In the **Comment** text field, enter a description to identify the server configuration.

8 Tap the **Save** button to save the configuration.

– or –

Tap the **Cancel** button to delete the configuration.

The default SSL port for mobile clients is 4475.

Afterwards the **Server** text field shows the name of the configured server.

4.3.3 Uninstalling the application for mobile devices

1. On the home screen of your mobile device, keep the *syngo*.via WebViewer icon pressed until the icons start to jiggle.
2. Tap the **X** icon on top of the *syngo*.via WebViewer icon.
3. Confirm the deletion message box.

5 Maintenance

5.1 Backup and recovery

syngo.via WebViewer does not host critical data whose loss could lead to system downtimes or disturbances of the clinical workflow.

syngo.via WebViewer relies on the Windows Server Backup for backup and recovery. Using Windows Server Backup, you can schedule periodic backups of the *syngo*.via WebViewer server.

For further information about the Windows Server Backup, use the Internet to find specific backup information of the system your are using.

5.1.1 Configuring the backup settings

✓ The **Windows Server Backup Features** are installed.

1. Log on to the operating system of the *syngo*.via WebViewer server.
2. From the Windows **Start** menu, choose **Administrative Tools** > **Windows Server Backup**.
3. In the **Actions** pane, click **Backup Schedule**.

   The **Backup Schedule Wizard** dialog box opens.
4. In the **Getting Started** dialog box, click **Next** to configure a new backup schedule.

   – or –

   Click **Modify backup** to change the configuration of a previously added backup schedule and click **Next**.
5. In the **Select Backup Configuration** dialog box, click **Full server (recommended)** and **Next**.
6. In the **Specify Backup Time** dialog box, click **Once a day**, select a time with less clinical routine work and click **Next**.
7. In the **Specify Destination Type** dialog box, select the backup destination type and click **Next**.

8 In the **Select Destination Disk** dialog box, choose the backup location, click **Next** and **Close**.

5.2 Administration Portal access

5.2.1 Accessing the Administration Portal logon screen

Use the **Administration Portal** to configure *syngo*.via WebViewer server. It consists of a web page which can be accessed by any supported web browser. To enter the Administration Portal, proceed as follows:

- In your web browser, enter the following URL:

  https://<WebViewer_server>:4443/Config.html

  <WebViewer_Server> can be the IP address or the hostname (if configured) of the *syngo*.via WebViewer server. **4443** is the default SSL port.

i The language of both the Administration Portal and the web client is controlled by the language setting of the web browser. If the browser is set to a language that is not supported by *syngo*.via WebViewer, English will be used as the default language.

5.2.2 Entering the Administration Portal

1 At the logon screen of the *syngo*.via WebViewer Administration Portal, enter a valid user name of a WebViewer administration account.

2 Click the upper **Login** button.

The **About** screen appears. The screen shows the **Client Version** as well as the **Server Version** of the *syngo*.via WebViewer.

i The web browser client can use a cookie to save the **User Name**. To use this feature, select the **Remember user name** checkbox.

The **Service key** login text fields and the lower **Login** button are used by the Siemens UPTIME Service Center only.

5.2.3 Accessing the Online Help

◆ In the upper right corner of the screen, click the **Question Mark** icon.

The Online Help opens.

5.3 System monitoring

5.3.1 Checking the condition of the syngo.via WebViewer services

To ensure *syngo*.via WebViewer server is in operating condition, the administrator must regularly monitor the system status:

1 Choose **Administration Portal** > **Services Status**.

2 Check the availability of the following components:

- *syngo*.via WebViewer Web Server
- *syngo*.via WebViewer Logfile Copy
- *syngo*.via WebViewer SSL Render Server
- *syngo*.via WebViewer Nexus
- *syngo*.via WebViewer License Manager

The status of each service should be **running**. This depends on the type of installation: for integrated deployment, the service is disabled. For dedicated deployment, the service is enabled.

If one of the services is not running, click the **Update Services** button to refresh the status view. If this is not working, you can manually start a service, see (→ Page 14 *Starting, stopping, or restarting the syngo.via WebViewer services*).

5.3.2 Checking the render server and web server log files

Information from the log files may be required for troubleshooting. Log files are stored in the following folder of the *syngo*.via WebViewer server: **C:\ispace\log**.

The file names of the log files in this directory indicate the respective event source. The render server produces log files with the prefix “rs”. The web server produces log files with the prefix “ws”. To search for information inside the log files, proceed as follows:

◆ Open the log files in a text editor of your choice.

5.3.3 Changing the granularity of the log files

To configure the granularity (all, verbose, debug, info, warning, error) of the Web and Render Server log files, proceed as follows:

1. Choose **Administration Portal** > **Log Files**.
2. Select the desired **Webserver Log Level**.
3. Select the desired **Render Server Log Level**.

   The granularity of the two log files changes immediately.

Additionally, *syngo*.via WebViewer creates an audit log file in the log directory. It contains information on user logins, rendering rates, and image or volume open operations. The auditing information is written in the YAML format in a file named **ispace_audit.yaml**. You can use a standard editing tool, for example Notepad, to read the log file.

All log files in the log directory are limited in size. When a log file exceeds a certain size, it will be renamed and a new log file will be started.

5.3.4 Configuring the backup time of log files

A periodic job copies the logs from the log file directory to a configured remote share (only applicable for dedicated deployment). The remote share is located on the *syngo*.via server hosting the database. To change the time of the daily backup, proceed as follows.

✓ *syngo*.via WebViewer services are enabled due to dedicated deployment scenario.

1 Choose **Administration Portal** > **Log Files**.

2 Adjust the **Time of Daily Log Copy** text field.

3 Click the **Save** button.

5.3.5 Downloading a log file archive

To download an archive containing all log files in the **.zip** format, proceed as follows:

1 Choose **Administration Portal** > **Log Files**.

2 Click the **Download Logs** button.

5.4 Server configuration

syngo.via WebViewer is configured by Siemens during the installation. The configuration must be adapted in some situations, for example:

- Changed IP address or server name of the *syngo*.via server
- Changing or renewing an SSL certificate
- Configuring the Autologout period
- Installing a new license

i Official SSL certificates need to be renewed periodically. The time period depends on the period provided by the trust authority.

5.4.1 Configuring the syngo.via database

syngo.via WebViewer server directly accesses the database and images stored on *syngo*.via server. Therefore, the database and the network share containing the images must be configured properly. If changes are necessary, proceed as follows:

1 Choose **Administration Portal** > **syngo.via Database**.

2 In the **syngo.via server** text field, enter the hostname or IP address.

3 Click the **Save** button.

When changing the settings for *syngo*.via server, the *syngo*.via WebViewer server settings have to be adjusted appropriately.

5.4.2 Changing or renewing an SSL certificate

SSL encrypts the connection between *syngo*.via WebViewer server and the clients. You can either use a signed SSL certificate from a vendor of your choice or a self-signed SSL certificate. During the installation of WebViewer, a self-signed certificate is generated automatically to ensure that only encrypted communication is used between WebViewer clients and the *syngo*.via server. However, a self-signed certificate will require each user to ignore a security warning message. It is recommended to use a signed certificate, when accessing WebViewer via internet. A SSL certificate comes with a private key. Both need to be available to encrypt the connection between server and clients.

To install a certificate, proceed as follows:

1 Open a text editor of your choice.

2 Open the SSL certificate and copy its content.

The content has to be in unencrypted PEM format.

3 Choose **Administration Portal** > **SSL Files**.

4 Paste the text into the **New Certificate** text field.

Please note the hints below.

5 Open the corresponding private key in the text editor and copy its content.

The private key has to be unencrypted.

6 Switch to the web browser window containing **Administration Portal** > **SSL Files**.

7 Paste the text into the **New Private Key** text field.

8 Click the **Save** button.

The **SSL Files** page also shows the public key of the current SSL certificate in the **Current Certificate** text field.

A signed certificate comes typically with a root certificate. There is no single certificate but a chain of certificates, which have to be installed in a particular order. In this case, all certificates, meaning the one for WebViewer, the intermediate ones and the root certificate, need to be copied into the textfield in descending order, starting with the WebViewer certificate.

If a new certificate is generated, the private key has to be exchanged as well.

5.4.3 Changing the SSL ports

Besides the default SSL ports, the *syngo*.via WebViewer server can be configured to use ports of your choice. This applies to the ports for web browsers as well as mobile devices. To change the SSL ports, proceed as follows:

1 Choose **Administration Portal** > **SSL Ports**.

2 In the **Webserver SSL port** field, enter a port.

3 In the **Mobile device SSL port** field, enter a port.

4 Click the **Save** button.

5.4.4 Configuring the Autologout period

After a configurable period of inactivity, *syngo*.via WebViewer logs off any user automatically. To change this period, proceed as follows:

1 Choose **Administration Portal** > **Autologout**.

2 Enter the desired number of minutes in the **Autologout Time** field.

3 Click the **Save** button.

Clients are warned one minute before the autologout will happen. Additionally, if the user tries to close the web browser window or tab showing *syngo*.via WebViewer, a closing notification with an option to cancel will appear.

Clients periodically contact the server when they are connected. If the connection is lost, the server will close down the connection and the client will be logged off.

The *syngo*.via WebViewer Administration Portal features an autologout function as well. The duration of this autologout period, however, is fixed to 5 minutes.

5.4.5 Installing a new license

The server requires a license for operation. This license is obtained as a file from Siemens. To install a new license file, proceed as follows:

1 Start a text editor of your choice.

2 Open the license file and copy its content.

3 Choose **Administration Portal** > **License**.

4 Paste the text into the **New License** text field.

5 Adjust the **MAC Address** text field only if the *syngo*.via WebViewer network card has been replaced.

6 Adjust the **FlexID** text field only if the VENDOR_DEFINED_HOSTID has been replaced.

7 Click the **Save** button.

The new license is uploaded and activated.

The license is not only required for the *syngo*.via WebViewer server itself. It also determines the maximum number of simultaneous clients.

i

Each client connection counts towards the maximum number of simultaneous client connections. The same user logged on using two different client platforms counts as two clients. If the maximum number of permitted clients is reached, no more client logins will be accepted.

5.4.6 Configuring biometric login for mobile devices

syngo.via WebViewer supports biometric login using FaceID and TouchID. In the **Administration Portal**, you can configure the permission to log on to mobile devices using biometric data.

If the client device supports biometric login and it is allowed by configuration, a dialog box will be displayed to the user offering an option to turn biometric login on.

If the client device supports biometric login, but it is not allowed by configuration, a dialog box will be displayed informing the user to contact the IT administrator.

5.5 Update

Updates of the *syngo*.via WebViewer server are installed by Siemens Healthineers. Read the provided update information for changes.

i

For the remote update service, it is necessary to open a Remote Desktop Connection from the *syngo*.via server to the *syngo*.via WebViewer server. Ensure that the Terminal Service is installed and port 3389 is open between both servers.

i

The initially installed version of the Nvidia GPU (CUDA) is verified by Siemens. A driver without verification may cause parts of *syngo*.via WebViewer server to stop working in the designated way.

You are allowed to install updates/upgrades if you install them in the same driver branch.

⚠ CAUTION

Important settings are lost during update or modification of system.

System does not work as intended after an update/upgrade.

- Always perform a backup of the current installation before update or modification of the system.
- Always perform a backup of the current configuration (including role-specific settings, such as user profiles) before updating or modifying the system.

6 Data and system security

The same security strategy is valid for syngo.via WebViewer server and the syngo.via server. See (→ *syngo.via Administrator Online Help*).

See also (→ *syngo.via Administration Manual, chapter "Data and system security"*).

6.1 Communication ports

Specific TCP/IP ports must be opened in the router or network firewall to enable communication between *syngo*.via WebViewer clients and the *syngo*.via WebViewer server.

⚠ CAUTION

Firewall rules can block correct transfer of data.

Images or reports cannot be viewed.

◆ Check and verify transfer of all types of data before releasing the software for general use.

The Windows Firewall of the *syngo*.via WebViewer server is preconfigured after installation. Ensure that the ports mentioned below are opened at network firewalls and at routers between the communicating devices.

Service/Function	Necessary Ports	Description
Render Server	4475 4443	The port 4475 has to be opened in the firewall between WebViewer and the network, which contains the mobile client devices. The port 4443 needs to be opened towards the Web-Clients.
microsoft-ds (for CIFS)	445	The port 445 has to be opened between WebViewer and *syngo*.via server.
syngo.via Web-Services	4510	The port 4510 has to be opened between WebViewer and *syngo*.via server.

⚠ **CAUTION**

Unauthorized access to the system.

Hazards up to and including loss of all patient data and non-operational system.

- The administrator is responsible for network security at the site. Set up firewalls and user account password protections. Do not allow users to change configuration files. Update virus protection software as required.

⚠ CAUTION

Unauthorized access to the system.

Hazards up to and including loss of all patient data and non-operational system.

- Check the log book periodically for failed login attempts and take appropriate measures to avoid unauthorized access to the system.

⚠ CAUTION

Use of an anti-virus software that is not provided by Siemens.

Malicious software can cause harms up to and including non-operational system and loss of all patient data.

- The administrator is responsible for the configuration of the anti-virus software. Configure and regularly update the anti-virus software.

6.2 Siemens Remote Service

The Siemens UPTIME Service Center has no direct access to the *syngo*.via WebViewer server. Remote service is only possible using the service infrastructure of the *syngo*.via server. A Remote Desktop Connection is opened at the *syngo*.via server to connect to the *syngo*.via WebViewer server.

Service/Function	Necessary Ports
Remote Desktop Protocol	3389

This page has been intentionally left blank.

This page has been intentionally left blank.

This page has been intentionally left blank.

CE
0123

MD

Manufacturer's note:

All product designations and company names are trademarks or registered trademarks of the corresponding companies.

Siemens Healthineers reserves the right to modify the design and specifications contained herein without prior notice. Some of the specifications described herein may not be currently available in all countries. Please contact your local Siemens Healthineers Sales representative for the most current information.

Caution: US federal law restricts the herein described devices to sale by or on the order of a physician.

This medical device bears a CE Mark in conformity with Regulation (EU) 2017/745 of the European Parliament and of the council of 5 April 2017 on medical devices.

The original language of this document is English.

Made in Germany

Legal Manufacturer
Siemens Healthcare GmbH
Henkestr. 127
91052 Erlangen
Germany

Siemens Healthineers
Headquarters
Siemens Healthcare GmbH
Henkestr. 127
91052 Erlangen
Germany
Phone: +49 9131 84-0
siemens-healthineers.com

Published by Siemens Healthcare GmbH / Print No. P02-040.621.36.01.24 / © Siemens Healthcare GmbH, 2011 – 2020
Date of first issue: 2020-07