SIEMENS

www.siemens.com/healthcare

syngo MR E11

Operator Manual – IT Configuration & Security Package

syngo MR E11

Operator Manual – IT Configuration & Security Package

Legend

	Indicates a hint Provides information on how to avoid operating errors or information emphasizing important details
»	Indicates the solution to a problem Provides troubleshooting information or answers to frequently asked questions
■	Indicates a list item
✓	Indicates a prerequisite A condition that has to be fulfilled before starting a particular operation
◆	Indicates a single-step operation
1 2 3	Indicates steps within operating sequences
Italic	Used for references and for table or figure titles
→	Used to identify a link to related information as well as previous or next steps
Bold	Used to identify window titles, menu items, function names, buttons, and keys, for example, the Save button
Blue	Used to emphasize **particularly** important sections of the text
Courier	Used for on-screen output of the system including code-related elements or commands
`Courier`	Identifies inputs you need to provide
Menu > Menu Item	Used for the navigation to a certain submenu entry
<variable>	Identifies variables or parameters, for example, within a string
⚠ CAUTION	CAUTION Used with the safety alert symbol, indicates a hazardous situation which, if not avoided, could result in minor or moderate injury or material damage. CAUTION consists of the following elements: ■ Information about the nature of a hazardous situation ■ Consequences of not avoiding a hazardous situation ■ Methods of avoiding a hazardous situation

WARNING

Indicates a hazardous situation which, if not avoided, could result in death or serious injury.

WARNING consists of the following elements:

- Information about the nature of a hazardous situation
- Consequences of not avoiding a hazardous situation
- Methods of avoiding a hazardous situation

WARNING

Legend

Table of contents

Table of contents

Table of contents

Table of contents

1 Introduction

In order to operate the MR system accurately and safely, the operating personnel must have the necessary expertise as well as knowledge of the complete operator manual. The operator manual must be read carefully prior to using the MR system.

1.1 Layout of the operator manual

Your complete operator manual is split up into several volumes to improve readability. Each of these individual operator manuals covers a specific topic:

- Hardware components (system, coils, etc.)
- Software (measurement, evaluation, etc.)

Another element of the complete operator manual is the information provided for the system owner of the MR system.

The extent of the respective operator manual depends on the system configuration used and may vary.

All components of the complete operator manual may include safety information that needs to be adhered to.

The operator manuals for hardware and software address the authorized user. Basic knowledge in operating PCs and software is a prerequisite.

1.2 The current operator manual

This manual may include descriptions covering standard as well as optional hardware and software. Contact your Siemens Sales Organization with respect to the hardware and software available for your system. The description of an option does not infer a legal requirement to provide it.

The graphics, figures, and medical images used in this operator manual are examples only. The actual display and design of these may be slightly different on your system.

Male and female patients are referred to as “the patient” for the sake of simplicity.

1.3 Intended use

Your MAGNETOM MR system is indicated for use as a magnetic resonance diagnostic device (MRDD) that produces transverse, sagittal, coronal and oblique cross sectional images, spectroscopic images and/or spectra, and that displays the internal structure and/or function of the head, body, or extremities. Other physical parameters derived from the images and/or spectra may also be produced. Depending on the region of interest, contrast agents may be used. These images and/or spectra and the physical parameters derived from the images and/or spectra when interpreted by a trained physician yield information that may assist in diagnosis.

Your MAGNETOM MR system may also be used for imaging during interventional procedures when performed with MR compatible devices such as in-room displays and MR Safe biopsy needles.

The MAGNETOM MR system is not a device with measuring function as defined in the Medical Device Directive (MDD). Quantitative measured values obtained are for informational purposes and cannot be used as the only basis for diagnosis.

For the USA only: Federal law restricts this device to sale, distribution and use by or on the order of a physician.

Your MR system is a medical device for human use only!

1.4 Authorized operating personnel

The MAGNETOM MR system must be operated according to the intended use and only by qualified persons with the necessary knowledge in accordance with country-specific regulations, e.g. physicians, trained radiological technicians or technologists, subsequent to the necessary user training.

This user training must include basics in MR technology as well as safe handling of MR systems. The user must be familiar with potential hazard and safety guidelines the same way the user is familiar with emergency and rescue scenarios. In addition, the user has to have read and understood the contents of the operator manual.

Please contact Siemens Service for more information on available training options and suggested duration and frequency of such training.

1.4.1 Definitions of different persons

Term used	Explanation
User/Operator/ Operating personnel	Person who operates the system or software, takes care of the patient or reads images Typically physicians, trained radiological technicians, or technologists
System owner	Person who is responsible for the MR environment. This includes legal requirements, emergency plans, employee information and qualifications, as well as maintenance/repair.
MR worker	Person who works within the controlled access area or MR environment User/Operator as well as further personnel (for example, cleaning staff, facility manager, service personnel)

Term used	Explanation
Siemens Service/service personnel	Group of specially trained persons who are authorized by Siemens to perform certain maintenance activities References to “Siemens Service” include service personnel authorized by Siemens.

2 Overview of the Security Package

Welcome to the *syngo* Security Package from Siemens. As a *syngo* Security Package user, you will have access to several security settings of clinical applications.

 Selected security features can only be configured if the security package is installed.

2.1 Authorized Users

The *syngo* Security Package must be used by persons with the necessary specialist knowledge according to country-specific regulations, for example, physicians, trained radiologists or trained technologists, after an appropriate application training.

2.2 Data and Function Security

Clinical decisions are made based on diagnostic images and patient medical reports. The patient medical data may contain sensitive information. In modern healthcare, it is necessary to protect all such sensitive information from unauthorized access.

The Health Insurance Portability and Accountability Act (HIPAA) is a legal requirement to ensure the privacy, integrity and consistency of patient data in healthcare.

In support for HIPAA and as may be required by country-specific regulatory *syngo* provides competent user management and highly configurable access control to implement privacy, integrity and consistency of patient data in healthcare.

- Access to functions as well as to data is only permitted to authenticated and authorized users. Each user is identifiable at all times.
- Logon and action on data such as creation, read, update and deletion are recorded in an audit trail. The audit trail can only be viewed by authorized users.
- *syngo* only accepts DICOM Query/Retrieve requests from trusted hosts. Requests from unknown hosts are rejected.
- Communication during secured remote service sessions is encrypted.
- If the computer is unused for a specific period of time, the screen is automatically locked.

Security has to be set up on every workstation. Satellite consoles inherit the security settings from the main console.

Furthermore, if the computer is connected to a hospital network, all partner workstations have to be set up for security; otherwise, a security gap will exist.

2.3 Scope

Security in *syngo* provides the infrastructure that is necessary to protect patient data from unauthorized access.

The security system consists of the following parts:

- Authentication of users who are working on the system
- Access protection to patient data with user specific permissions
- Protection for execution of application functionality with user-specific privileges
- Logging the access to patient data in an Audit Trail

2.4 Use Cases

The following use cases show you some benefits of the *syngo* user management and security system.

- To ensure high throughput of patients, two assistants work on one system at the same time. While one assistant prepares a patient for the next examination at the modality, the other assistant sends the images from the previous examination to the archive. The assistants can take over the system and log on without restarting the application or a significant delay being caused due to a patient data unload.
- A system can be shared between wards or hospitals. Patient data is visible only to the staff of the ward/hospital who has acquired the data.
- The presence of a VIP patient in the hospital is kept confidential. Data acquisition is carried out by the departmental head and one assistant. The acquired images and even the existence of the patient's records is hidden from all other users of the system.

2.5 Terms and Definitions in Security

The following table gives an overview about terms available in security settings:

Terms	Definitions
Access Rights	In *syngo* security, access to patient health information (data) is protected with group/user specific permissions.
Authentication	Authentication of users who are working with *syngo* is the underlying basis of all security measures. A user account is created for every person who will be working with *syngo*. To log on to the system, the user enters the user account and password. By this, a user is identifiable.

Terms	Definitions
Audit Trail	On a secure system, all actions on data are logged. *syngo* uses auditing to track the user account that was used to access files or other objects, number of logon attempts, system shutdowns or restarts, and such similar events. Only authorized users can track auditing activity by viewing the log files of the audit trail. The log files of the audit trail need to be archived on a regular schedule.
Authorization	■ Data Access: Only users who need access to certain patient data can view it. ■ Functional Privileges: Only users with the necessary authorization can modify the data.
Data Access and Groups	The data access security check is based on groups and users: ■ Users need to have access to patient data within their sphere of influence (for example, their ward). ■ Users are assigned to groups that correspond with their sphere of influence, these groups are allowed access to the corresponding patient data It is easier to manage permissions for groups than for individual users. Access to patient data is secured through the needed permissions. In order to reduce complexity, the following permission levels are implemented: ■ NO ACCESS ■ FULL CONTROL

Terms	Definitions
Domains	A domain represents a group of computers in a network that have a common file database. Managed by a domain administrator, the domain provides common security guidelines and regulates data access for the computers within the domain. Users and groups of a domain can be used to manage the access privilege within the domain. Because user management on a domain server is not limited to *syngo*, it is possible to integrate non-*syngo* groups and roles into *syngo* roles and groups. The use of domain group policies is not supported.

Terms	Definitions
Everyone (Group and Role)	*syngo* security makes use of the **Everyone** group and a **Everyone** role ■ The **Everyone** group is the default group for setting up access to data. If the "Everyone" group is configured to have access to all data within the hospital, all users will have access to all data (regardless of any group or individual settings). It is essential that the **Everyone** group is restricted to patient data that everyone must have access to (for example, emergency patients). ■ The **Everyone** role is the default level for granting privileges to users. If all privileges are assigned to **Everyone**, the configuration of other roles or individuals will not have any actual effect. It is essential to limit the privileges of the **Everyone** role to those that everyone must have. All users potentially have full access to data and functions because the default settings of the **Everyone** group and role allow full access. The effective privilege for a user depends on the configuration of this group and role. You can follow two different strategies for the **Everyone** setup: ■ Following the "Allow nothing" strategy, you would withdraw almost all privileges from the "Everyone" group and role and then set up the user groups and the roles. In this case, even common privileges would have to be assigned to every group and role. ■ Following the "Common rights" strategy, you would only withdraw critical privileges that are not needed by all users.

Terms	Definitions
Groups	Groups are assigned to users who are members of a team or a department. All members of a group receive the same data access privileges. Establishing groups helps to efficiently assign data access privileges to users and reduces the time needed for configuration
Patient Group	Patient data that is assigned to a patient group can only be accessed by users who have the privilege to access data of that group. It is possible to assign patient data to several patient groups at the same time. Authorized users are allowed to modify the patient group assignment.
Permissions	Data access rights. The right to create, read, update, delete or protect data is granted via permissions. The following permission levels are available: ■ NO ACCESS ■ FULL CONTROL
Privileges	The right to execute functions is granted via privileges. The functional security check is based on roles and users: ■ Users need to perform functions that correspond with their role in the hospital, for example, nurse, physician. ■ Privileges are managed by roles. It is easier to manage privileges for roles than for individual users. ■ Users are associated with roles and inherit the corresponding privileges.

Terms	Definitions
Roles	Users having the same tasks are assigned a role (for example, radiologists, administrators, or technicians). All users assigned to a certain role have the same privilege to execute functions, such as archiving data. Establishing roles helps to efficiently assign execution rights to users and reduces the time needed for configuration.
Trusted Hosts	Trusted hosts is a principle for a secure exchange of data between systems in a network. The trusted host functionality is switched on by default in the **Local Service Software**.

2.6 Security information for the operator

2.6.1 Protected health information (PHI)

Protected health information is any information about health status, provision of health care, or payment for health care that can be linked to a specific individual. This includes any part of a patient's medical record or payment history.

Handle PHI with care and avoid unauthorized access. Ask your administrator for details.

Be aware which parts of your work deal with PHI and need special attention:

- **Patient registration**: You enter patient information and therefore PHI.
- **Image acquisition and postprocessing**: Acquired image data are PHI, they contain patient sensitive information. Image postprocessing may create new PHI as new series. If you view images, PHI may be shown as image text.
- **Data transfer**: Whenever you transfer (send/receive) patient or image data, ensure to use secure communication. This also applies for sending data, for example, to a CD.

For installations with elevated security requirements, it is recommended to lock the operator room to make it inaccessible to patients and non-authorized persons.

Optional system components:

- The hospital network and all components outside the MR systems are assumed to be under control of the customer. Siemens makes no prescriptions about how to structure the network. However, there are some recommendations for secure networking. For details, contact you administrator.
- The MRWP (MR Workplace) is an optional workstation for image inspection and post-processing. It could even be located in a separate room. Information in the patient and image database located on the MRAWP is shared between the MRAWP and the MRWP, that is, sensitive information is transferred over the hospital network. For systems with elevated security requirements it is recommended to either not using the MRWP, or to make sure that the network communication between the MRAWP and the MRWP is secured.

2.6.2 Authorized access

The *syngo* user model ensures that every user is allowed to access only to the data the user is authorized to work with (data security) and to the functions the user is authorized to use (functional security).

For details, see: (➔ Page 91 *Information for Users*)

2.7 Security Settings

2.7.1 About Viewing the Security Settings

Based on diagnostic images and medical reports, decisions are made that affect the health of patients. Therefore, in modern health care, it is necessary to protect such sensitive documents from unauthorized access and to record all actions on the data.

syngo provides competent user management and highly configurable access control to implement privacy, integrity and consistency of patient data in health care which may be required by country specific regulatory.

Principles of Security Settings

- **User Management**: Access to functions as well as to data is only permitted to authenticated and authorized users. Each user is identifiable at all times.
- **Groups and Roles** rule data access rights and functional privileges:
  - Groups are assigned to users who are members of a team or a department. All members of a group receive the same data access rights (permission, for example, to view or to process data).
  - Users having the same tasks are assigned a role (for example, radiologists, administrators, or technicians). Then all users with this role have the same rights to execute functions, such as archiving data.
- **Patient Groups**: Patient data that is assigned to a patient group can only be accessed by users who have the right to access data of that group.

Viewing your current settings

When the security system is switched on at a syngo system, a dialog box provides you with information (mentioned above) about your current access rights and functional privileges.

2.7.2 Opening the Security Settings dialog box

The **Security Settings** dialog box provides information about your current data access permissions and functional privileges.

How to Open the Security Settings

- On any task card, choose the **Options** > **Security** menu item.

  The **Security Settings** dialog box is displayed.

2.7.3 Viewing the Security Settings

The **Security Settings** dialog box provides you information about your current data access permissions and functional privileges.

How to View the Settings

1 Open the **Security Settings** dialog box.

2 Click the **Groups/Roles** tab to check your groups and roles membership.

- Groups are assigned to users who are members of a team or a department. All members of a group receive the same data access rights (permission, for example, to view or to process data).
- Users having the same tasks are assigned a role (for example, radiologists, administrators, or technicians). Then all users with this role have the same rights to execute functions, such as archiving data.

3 Click the **Privileges** tab to check which functional privileges are assigned to you.

Name and **Description** help you to identify which functions are available.

4 Click the **Patient Groups** tab to check which patient data is accessible for you.

The list gives you information about all data (stored in patient groups) you can access.

If in doubt about your settings, or if you cannot access data or execute functions, contact your security administrator immediately.

2 Overview of the Security Package

3 Information for Administrators

Once the security system has been installed, Administrators are responsible for establishing and maintaining competent user management, and for ensuring that the system remains secure. This includes the following main tasks:

- Creation and maintenance of user and group accounts and role definitions
- Definition of data access rights (permissions)
- Assignment of functional privileges
- Handling of the audit trail
- Regularly backing up the audit trail

User management has to be set up on every workstation. Satellite consoles inherit the security settings from the main console.

3.1 Overview diagrams

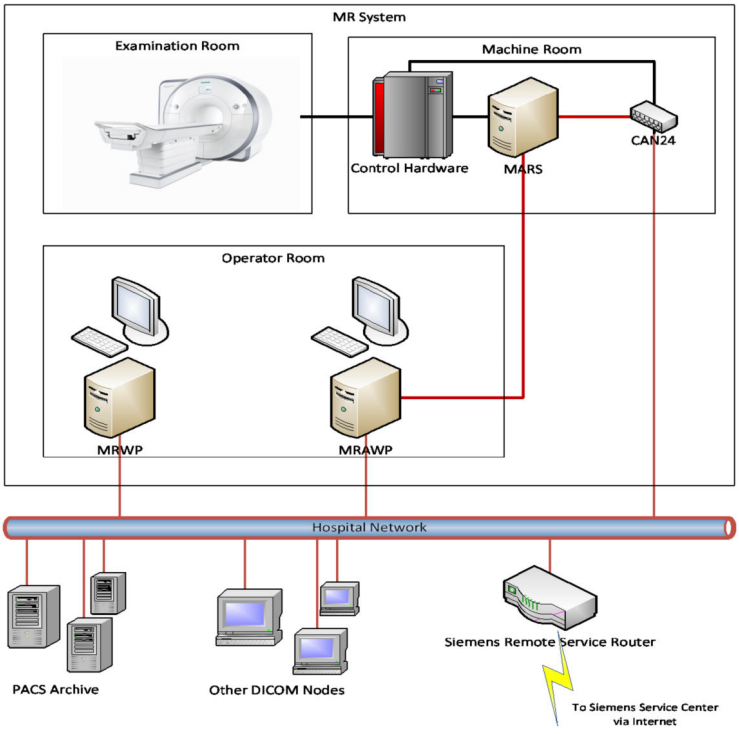
The following images show high-level system overview and high-level data flow diagrams, which show the most important data flows through the hardware and software components, and what kind of data is transferred so that the customer can prepare security appropriately.

Short definitions of terms used in the diagrams, as follows:	
Operator	Person who operates the system or software, takes care of the patient or reads images
Patient registration	Process of entering sensitive, personal patient demographics (PHI)

Short definitions of terms used in the diagrams, as follows:	
Patient/Image data-base	Central database for all patient and image related information. Object-oriented database (no SQL), with a proprietary interface
Image visualization	Function of viewing image data (incl. PHI); different applications (e.g., GSP)

3.1.1 Diagram of MR system components

The following image shows a high-level overview of the MR system and its integration into the hospital environment.



(CAN = Control Area Network, CAN24 = Controller of the CAN network)

The MR system is located in three different but adjacent rooms: The examination room, where the patient is examined, the operator room, where the medical operators work, and the machine room, where most of the control hardware is installed.

Communication lines shown in red are Ethernet connections (TCP and UDP). Communication lines shown in black use other internal protocols (CAN, PCIe, or proprietary protocols). Only the MRWP, MRAWP, and the CAN24 "red" Ethernet connections are connected to the hospital network. All other "red/black" network connections are internal and regarded as secure.

The internal Ethernet connections between the MRAWP (MR Acquisition Workplace) and the MARS (Measurement And Reconstruction System), and between the CAN24 and the MARS are not accessible from the hospital network.

It is strongly recommended that the machine room is locked and not accessible to patients or non-authorized personnel.

For the MRWP the same security settings, Roles/Groups/Audit trail etc. of the MRAWP apply!

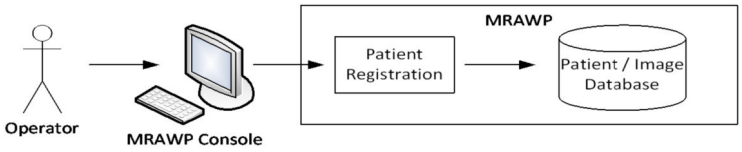
Optional components:

- Siemens remote service is an optional feature. Without remote service, the router to the Siemens service center is not needed.
- The network access security is part of the customer network security policy.
- The CAN24 box is used to monitor the magnet status by remote system, even if the other system parts are switched off. Without remote service, this cannot be done. The CAN24 is not optional, however, the connection to the hospital network can be omitted.

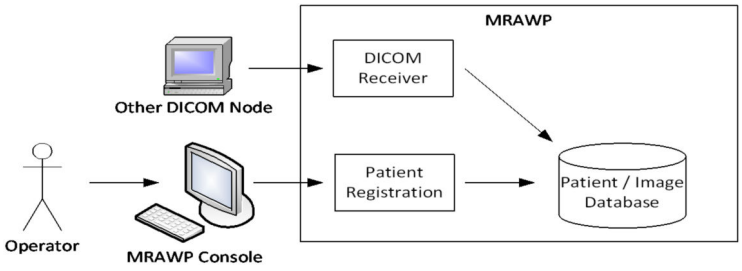
External network connection (for example, hospital network) is not mandatory to operate the MR systems and security is part of the customer network security policy.

3.1.2 Patient registration - data flow diagrams

During patient registration, the operator enters the relevant information into the patient / image database.

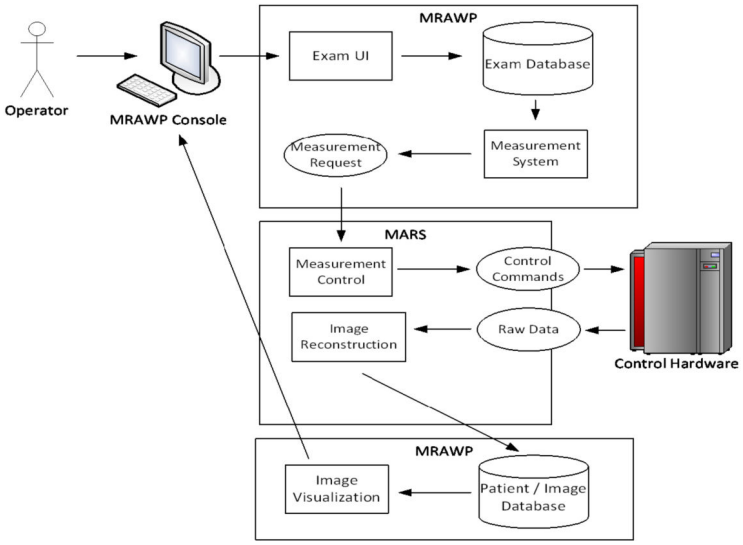


A possible variant of the patient registration is that the database is prefilled by a DICOM modality worklist. The operator still needs to enter/complete and confirm the information received from the RIS into the *syngo* scheduler.



3.1.3 Image acquisition - data flow diagram

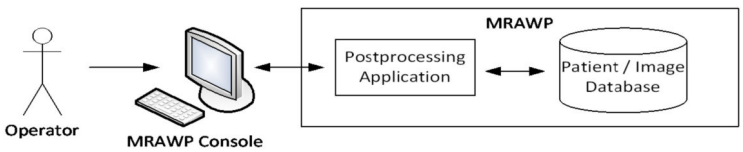
The measurement system creates a measurement request and sends this to the MARS. This system controls the hardware parts with the correct signals and receives the raw data from the receiver. The raw data is then reconstructed into the intended MR images, which are returned to the MRAWP and stored in the patient/image database as a series containing patient demographics and clinical images.



The examination database is based on SQLite. However, the database contains only examination protocols for running the examination with neither patient demographics nor images. Its interface is not directly exposed to any user interface or network port, and user input is carefully validated before stored into the database.

3.1.4 Image postprocessing - data flow diagram

Image postprocessing is needed if the acquired image needs further processing before it can be decided whether the image is suitable for diagnosis or not. Examples range from a simple subtraction from previously measured images up to dedicated cardiological or neurological evaluations.



All postprocessing applications are controlled by the operator and work on images already stored in the patient/image database. However, images in the database are never modified; instead, if new images are created, they are stored as new images.

3.1.5 Image archiving - data flow diagram

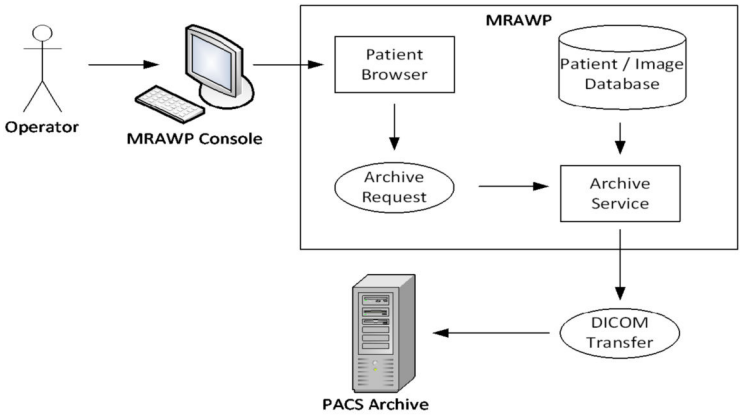
As the MR system is not intended to be used as an image archive, images should be transferred to the PACS archive as soon as possible. This also prevents potential image loss.

The patient information stays on the system until deleted.

There are two possibilities for starting image archiving:

- Automatic transfer to the archive, that is, whenever a new image is stored into the patient/image database, it is transferred to the dedicated archive. A filter can be set to exclude certain image types.
- Manual transfer to the archive, that is, the operator sends images actively to the archive using the archive command.

Archiving is done via DICOM transfer.



A PACS archive is not always needed. Some customers prefer to print the images onto a film sheet and archive them into a film based archive, and some customers prefer to burn the results on a CD or DVD and transfer them to the archive manually. From a security perspective, the latter has some advantage, because the archive does not need to have a connection to the hospital network.

Please ensure that data is handled according to your local data protection laws.

The use CDs or DVDs as a long-term storage is not recommended, because the lifetime of those media is not yet guaranteed.

3.2 Physical safeguards

The MRAWP and MRWP components contain personal protected information (for example, patient data and images). Those components are also high-performance personal computers and are therefore attractive for potential thieves.

In order to prevent theft, it is highly recommended to protect both the MRAWP and MRWP systems from theft.

The following possibilities should be considered:

- Restricting access to the operator room, so that no unauthorized person can enter it easily.
- Installing the MRAWP and the MRWP into a closed cabinet, so that it cannot be removed easily.
- Chaining the computers to a wall, using a chain or a steel cable and a padlock. Both the MRAWP and the MRWP have latches at the rear side, which are intended for this purpose.
- Or a combination of these measures, for additional security.

3.3 Encrypted harddisk - BitLocker

Your harddisk can be encrypted with the Microsoft BitLocker software to protect the computer from unauthorized access. Contact Siemens Service for the initial setup of the encryption.

At the end of the encryption process, you will get the decryption key information as *RecoveryKey.txt* file from Siemens Service.

If the BitLocker is installed, you can boot the computer system only if the correct USB stick with the corresponding decryption key is connected to the computer. For starting a computer locked by BitLocker, see: (→ Page 91 *Starting the computer locked by BitLocker*)

You can create duplicate USB sticks.

- Connect the original USB stick to a computer and use the cmd.exe to copy the complete information from the original to the new USB stick. For example, on a Windows 7 computer, use the following command :

  ```
  xcopy /h [Drive Letter of old usb device] [Drive Letter of new usb device]
  ```

Save the *RecoveryKey.txt* and store all USB sticks in a safe location! Advice all users about the rules to deposit the USB stick in this safe location.

3.4 Protected personal information and pseudonymization

The MR system produces MR images as DICOM data (images, series and studies). DICOM data can contain all kinds of personal information, which is protected by law in many countries.

Contact your local security administrator for your institution's regulatory requirements.

In addition to the export of DICOM data, MR systems can also import DICOM data from other sources. If this happens, the system may even store more information than described above; some may also be considered being personal protected information.

First and foremost, **protected personal information** is all that can be used to identify the patient: Name, birthday, personal or social security number, etc. In addition, protected personal information is also everything that identifies operators or doctors. In some countries, even the hospital name is considered personal information.

The MR system has a feature called “Anonymization”, applicable to export of images and similar data. In case patient series shall be used, for example, for training or presentation purpose the PHI information can be removed by using the anonymization/pseudonymization functionality. If data protection is a critical issue (e.g. VIP patients), even pseudonymized images should not be distributed generously.

During pseudonymization, the following information is either removed or concealed (by replacing it with an arbitrary string).

Attribute	DICOM tag
Instance Creator UID	(0008,0014)
SOP Instance UID	(0008,0018)
Accession Number	(0008,0050)
Institution Name	(0008,0080)
Institution Address	(0008,0081)
Referring Physician’s Name	(0008,0090)
Referring Physician’s Address	(0008,0092)
Referring Physician’s Telephone Numbers	(0008,0094)
Station Name	(0008,1010)
Study Description	(0008,1030)
Series Description	(0008,103E)
Institutional Department Name	(0008,1040)
Physician(s) of Record	(0008,1048)
Performing Physicians’ Name	(0008,1050)
Name of Physician(s) Reading Study	(0008,1060)
Operators’ Name	(0008,1070)
Admitting Diagnoses Description	(0008,1080)

Attribute	DICOM tag
Referenced SOP Instance UID	(0008,1155)
Derivation Description	(0008,2111)
Patient's Name	(0010,0010)
Patient ID	(0010, 0020)
Patient's Birth Date	(0010,0030)
Patient's Birth Time	(0010,0032)
Patient's Sex	(0010,0040)
Other Patient Ids	(0010,1000)
Other Patient Names	(0010,1001)
Patient's Age	(0010,1010)
Patient's Size	(0010,1020)
Patient's Weight	(0010,1030)
Medical Record Locator	(0010,1090)
Ethnic Group	(0010,2160)
Occupation	(0010,2180)
Additional Patient's History	(0010,21B0)
Patient Comments	(0010,4000)
Device Serial Number	(0018,1000)
Protocol Name	(0018,1000)
Study Instance UID	(0020,000D)
Series Instance UID	(0020,000E)
Study ID	(0020,0010)

Attribute	DICOM tag
Frame of Reference UID	(0020,0052)
Synchronization Frame of Reference UID	(0020,0200)
Image Comments	(0020,4000)
Request Attributes Sequence	(0040,0275)
UID	(0040,A124)
Content Sequence	(0040,A730)
Storage Media Fileset UID	(0088,0140)
Referenced Frame of Reference UID	(3006,0024)
Related Frame of Reference UID	(3006,00C2)

It is also possible that personal information can be found in unexpected places, for example, in descriptive texts in the image itself, or in other free-text fields. It might also be possible to identify patients by physical properties present in the images (for example, by reconstructing the face). Using the pseudonymization does not disburden the responsible clinician from making sure that no protected information is contained in the images!

PHI can occur in several objects like the image text, free text, secondary capture images, and so on.

3.4.1 Protected personal information in log files

If the system behaves unexpectedly, or if an obvious defect shows up, the operator has the possibility to create a so-called "savelog". This is a collection of information about the current state of the system that helps Siemens service and development in finding a potential defect.

The savelog may contain protected personal information under the following circumstances.

- A savelog may optionally contain a screenshot, which may contain information about, for example, the current patient. While a screenshot can be helpful in diagnosing the defect, the operator may need to choose to not including the screenshot into the savelog. It is also possible to tell the service technician to disable the screenshot feature for savelogs altogether.
- The following patient information is kept for log file analysis. Other patient information is anonymized.
  - Patient's sex, height and weight as registered,
  - Patient's age, limited to full years for patients above 2 and below 90 years; limited to 0.1 years for patients below 2 years, and "90" for patients above 90 years.

3.5 Secure networking

Since a high number of cyber attacks are conducted over the network, the MR system should be operated in a secure network environment. This also prevents a possible spread of malware, in case it has infiltrated the network.

The MR system offers safeguard measures against known network attacks (of today), but nevertheless it is recommended to observe the following hints:

- Use **subnetting**. Operate the MR system and its associated DICOM nodes in a physical subnet or a VLAN. Keep this network as small as possible, and open only necessary ports to the outside (for example, DICOM port 104). Usually it makes sense to spread the subnet over some associated devices, such as a radiology department.
- Do not make network ports accessible to the outside. Network ports in corridors, waiting areas, or other publicly accessible places are easily abused by hackers.
- Do not use wireless LAN!
- Put the MRAWP and the MRWP into the same logical subnet.

It is recommend to consult a network security specialist for installations with high security requirements.

3.6 Network communication ports

In a single-console installation (only MRAWP), the following ports can be open to the hospital network.

Port/protocol	Explanation
80/tcp	Remote service (unencrypted) Not recommended; encrypted communication should be preferred.
104/tcp	DICOM communication (unencrypted)
443/tcp	Remote service (encrypted)
2762/tcp	DICOM communication (encrypted)
5900/tcp	Expert-i remote access

If a secondary workplace (MRWP) is present, the following ports are open in addition to the ones above.

Port/protocol	Explanation
137/udp	Windows folder sharing
138/udp	Windows folder sharing
139/tcp	Windows folder sharing
445/tcp	Windows folder sharing
5688/udp	Internal interprocess communication (MRAWP and MRWP)
5109/tcp	Versant Database access

Port/protocol	Explanation
> 1024/tcp	Several dynamically assigned ports for inter-process communication

It is recommended that open ports are kept in a protected subnet (for example, VLAN) unless communication outside the subnet is actually needed. For example, port 104 should only be opened in a router if there are DICOM nodes outside the protected subnet.

3.7 Security scanning

During development, the MR system is scanned using a number of state-of-the-art security scan tools, for example, Nessus. This applies both to anonymous scans (no authentication information available) and to qualified scans (using, for example, an administrator account and password).

However, since IT security findings and exploits are made public frequently, it cannot be guaranteed that the system resists scans or penetration tests in the future.

It is recommended that MR systems should not be scanned during patient examinations. Siemens will provide updates on a regular basis in order to close found vulnerabilities.

3.8 Operating system services

The MRAWP and the MRWP will run the following Windows services (also known as "demons").

Service name	Description
AppHostSvc	IIS application host helper (Windows internal)
AppInfo	as part of User Account Control (UAC) (Windows internal)

Service name	Description
Works AssetMgr	Manages a database of the installed hardware and software components (*syngo* MR specific)
AudioEndpointBuilder	Manages audio devices (Windows internal)
AudioSrv	Manages audio and audio devices (Windows internal)
AutoReport	Sends autoreport files to Siemens remote service (*syngo* MR specific)
BFE	Base filtering engine for firewalls and antivirus (Windows internal)
BuRe	Background burning of CD/DVD (*syngo* MR specific)
CryptSvc	Cryptographic services provider (Windows internal)
CsaCompMgrInit	Runs the Siemens component manager (*syngo* MR specific)
CsaKeyboardFilter	Handles special keyboard keys (*syngo* MR specific)
CscService	Manages the "offline files" cache (Windows internal)
DcomLaunch	Responds to COM/DCOM object activation requests (Windows internal)
Dhcp	DHCP client (Windows internal)
Dnscache	DNS client (Windows internal)
DPS	Diagnostic policy service (Windows internal)

Service name	Description
EventLog	Manages events and event logs (Windows internal)
EventSystem	Supports the system event notification service (Windows internal)
FontCache	Caches commonly used font data (Windows internal)
ftpsvc	Enables the FTP server (Windows internal)
gpsvc	Group policy client (Windows internal)
hasplms	Sentinel license service (*syngo* MR specific)
IISADMIN	Internet information services (Windows internal)
IKEEXT	Manages Internet key exchange (IKE) and AuthIP, needed for the IPsec protocol (Windows internal)
iphlpsvc	Provides tunnel connectivity using IPv6 transition technologies (6to4, ISATAP, Port Proxy, and Teredo) (Windows internal)
LanmanServer	Supports file, print, and named-pipe sharing over the network (Windows internal)
lmhosts	Supports NETBIOS over TCP/IP service and name resolution (Windows internal)
MpsSvc	Windows firewall (Windows internal)
MrBootpS	DHCP service, needed for MARS boot (*syngo* MR specific)

Service name	Description
netprofm	Network list service (Windows internal)
Netman	Manages objects in the “Network and Dial-Up Connections” folder (Windows internal)
Nlasvc	Collects and stores information about the network environment (Windows internal)
PcaSvc	Program compatibility assistant (Windows internal)
PlugPlay	Detection of newly connected hardware (Windows internal)
PolicyAgent	IPsec policy agent (Windows internal)
Power	Manages power policy and Audio output (Windows internal)
ProfSvc	User profile service (Windows internal)
RpcEptMapper	RPC endpoint mapper (Windows internal)
RpcSs	Remote procedure call service (Windows internal)
SAM	Security accounts manager (Windows internal)
SamSs	Security accounts manager (Windows internal)
scsrvc	McAfee Embedded Control solidifier (*syngo* MR specific)
SD_SERVER	Image viewing server (*syngo* MR specific)

Service name	Description
SENS	System event notification service (Windows internal)
Spooler	Printer spooler (Windows internal)
SysMain	Maintains system performance (Windows internal)
Themes	User experience theme management (Windows internal)
tftpd	TFTP server, needed for MARS boot (*syngo* MR specific)
TRANSFERMGR	Handles DICOM transfer (syngo MR specific)
UIODetect	Handles user notification for interactive services (Windows internal)
UxSms	Desktop window manager (Windows internal)
VERSANTD	Versant database engine (*syngo* MR specific)
W32Time	NTP client (Windows internal)
W3SVC	Web publishing service (Windows internal)
WAS	Provides process activation and resource management services for message-activated applications (Windows internal)
WdiServiceHost	Manages diagnostics in local service context (Windows internal)
Winmgmt	Provides an object model for Windows management information (Windows internal)

Service name	Description
wscsvc	Monitors and reports security health settings (Windows internal)

3.9 Denial-of-Service (DoS) attacks

✓ IT administrator is logged in

Although Siemens has made considerable effort to protect the system from network attacks like Denial-Of-Service, there is still a risk that a hacker detects a new way to disturb the system. The typical effect is that the user interface gradually slows down, probably leaving the system virtually unusable. If already under attack, try to perform the following steps.

1 Open the Windows task manager.

2 Select the **Networking** tab card.

If the external (hospital) network is extremely busy (80% or more), a denial-of-service attack is possible.

3 Disable remote service (if enabled), in case the attack is via port 80 or 443.

4 Disable Expert-I (if enabled), in case the attack is via port 5900.

5 Go to system control and shut down the Archnet task, in case the attack is via port 104 or 2762.

Note that if you do so, the operator will not be able to archive, print, or burn to DVD any more.

6 If all else fails, disconnect the Ethernet cable to the hospital network.

This can be done even during operation.

Make sure to not disconnecting the MARS Ethernet connection, because in this case running measurements will be aborted, and further measurements will not be possible any more.

3.10 Cryptographic algorithms

The MRAWP and the MRWP systems are based on Windows 7 as an operating system. Windows has built-in functions for encryption, authentication and message hashing. A complete list of the algorithms used can be obtained from Microsoft TechNet. All algorithms are FIPS-140 compliant. Those algorithms are used for encryption, authentication and message signing visible to the operator and to the hospital network.

For internal purposes, for example, the communication between the MRAWP and the MARS, and on the Linux system, additional algorithms are in place. Most of them are standard Linux implementations.

Cyphers:

- AES
- Blowfish
- Camellia
- SEED
- CAST-128
- DES
- IDEA
- RC2
- RC4
- RC5
- Triple DES
- GOST 28147-89[5]

Cryptographic hash functions:

- MD5
- MD2
- SHA-1
- SHA-2 (all variants)
- HMAC (RFC 2104)

- RIPEMD-160
- MDC-2
- GOST R 34.11-94[5]

Public-key cryptography:

- RSA
- DSA
- Diffie–Hellman key exchange
- Elliptic curve
- GOST R 34.10-2001[5]

Those internal implementations are assumed to be identical to the standard implementations, but not necessarily FIPS-140 certified.

3.11 Configuration of the Security System

3.11.1 Principles of the *syngo* User Management

Patient data is sensitive information that must be protected from unauthorized access, modification, transfer or deletion.

3.11.2 User Authentication

A user account must be created for every person who will be working with *syngo*. To log on to the system, the user enters the user account and password.

3.11.3 User Authorization

The *syngo* user management and security system provides a highly configurable access control and ensures that users obtain access only to application functions and patient data for which they have authorized access.

- The right to execute functions is granted via privileges.
- The right to create, read, update, delete or protect data is granted via permissions.

Permissions can be set on at the patient or at the study level. Series and instances inherit their permissions from the study they belong to.

3.12 Grouping of Users: Roles and Groups

Setting up the access rights for each user individually would take a long time and would inevitably lead to inconsistent rights for similar users.

Scenario: All radiologists shall be allowed to modify a patient's work status, but nurses shall not be allowed to do this.

Users can be grouped under certain aspects:

- According to user profession or duties, they may have assigned one or several roles, such as radiologist, nurse, or administrator.

  Roles can be assigned certain function execution rights (privileges), such as sending data, correcting data or setting a work status. These rights extend to all users who assume a certain role (or several roles).

- According to the department a user belongs to, a user may also be assigned to one or several groups, such as the radiology department or a ward.

  For groups, you can configure data access rights (permissions), which are granted to all group members.

- You can also set up permissions and privileges for each user individually.

Typically, a user belongs to at least one group and has at least one role. A user can also be assigned to more than one group or role.

3.12.1 Recovering Deleted Group Members

If you need to recover patients that have been deleted via deleting a group they were in, you can do that in the **syngo Security Configuration**: In **Security Management -> Data Access Permissions -> Patient Groups**, you will find the **Patient Group** called 'LOST&FOUND'.

3.13 Internal Users

Internal user accounts are essential for the system. They consist of built-in users of the Windows operating system and *syngo* internal users.

 The symbol user with exclamation mark indicates internal users.

Although it is possible to change the password of these internal accounts using the **Reset Password**, we strongly recommend not to modify passwords for any of the internal users by using windows user interface.

See (→ Page 123 *Assign new password for internal users*)

The Standard Operating system account:

MedGuest: Built-in Windows account, not to be deleted. For *syngo*, this account is renamed and disabled.

sysadmin: Built-in Windows account, not to be deleted. For *syngo*, this account is renamed and disabled.

The user can change the administrator name from the service page.

The internal user accounts are:

- BRAdmin: Account for backing up and restoring files on the computer, regardless of any permissions that protect these files.
- DICOM_USER: Account for processes using DICOM services.
- LocalServiceUser: Account for the service technician.
- mars2: Account for accessing the MRAWP system from the MARS computer system.
- meduser: Account created by *syngo* to keep system services running.
- PPP: Account created by *syngo* to enable point-to-point communication used for remote service logon via modem.

- RemoteServiceUser: Account used for the remote service session.
- ReplAccUser: Used for replicating user permissions and privileges in an MRAWP + MRWP scenario.
- syadmin: System administrator account.
- viauser: Used for *syngo*.via integration with *syngo* MR.
- Auditors group: Special group created with permission to open the Application, Security System, and Event Log.

If the Security Package is active, the following changes apply:

- The meduser account receives a random password and cannot be used interactively any more.
- For every operational user, a Windows user account is generated, which has interactive rights.

3.14 DICOM Nodes

In security system, DICOM network nodes are treated as virtual user accounts. They are not intended for local logon, they are required for proper networking (transfer of data).

 The network symbol indicates virtual DICOM users.

For each DICOM service (AET) that is configured in the **Local Service Software**, automatically a corresponding entry is created in the special **DICOM Nodes** folder of the user management.

To set up the access rights for data being transferred from and to the network workstation, you should put each DICOM node into a user group and assign a role (this effectively assigns the workstation a user group and role). The relationship between user groups and patient groups define the permissions on the data as well as the default patient group, the roles define the functional privileges of the DICOM nodes.

The transfer of images to remote node will happen in secure or unsecure way based on the service page configuration for the DICOM network nodes.

For example: You may want to configure the system so that the workstation AET_HOP01 may query for data of VIP patients, but the workstation AET_WARD12 has no access. The Patient Groups configuration in the Data Access Permissions section is the place to configure this.

The network communication supports “Trusted DICOM Nodes”. That means data packages are encrypted and signed.

3.14.1 Tracking of user activities

In *syngo*, the activities of a user are recorded in the audit trail including the user’s identity. According to national regulations, it is not allowed to share user accounts.

Recommend the users to use the **Log In Different User** function to switch the user quickly at the workstation.

3.15 Multistage Security Setup

Security in *syngo* has a multistage security concept:

- The user management is the essential basis of all other security building blocks. It makes user logon mandatory and ensures user authentication.
- The audit trail records all actions involving patient data.
- The function execution check ensures that only authorized users perform actions.
- The data access check defines the rights to access patient data (assembled in patient groups).

Despite the mandatory user management, the following combinations of the options mentioned above are possible:

- User management for PACS or network
- User management and function execution check
- User management, audit trail and function execution check

3 Information for Administrators

- User management, function execution check and data access
- All items for full security management

4 Information for Service Technicians

4.1 Changing the BIOS password

By default, the systems are provided with standard BIOS passwords.

For additional security, it is recommended to change the BIOS passwords on the MRAWP and MRWP (but not on the MARS).

✓ Service technician is logged in

1 Press the BIOS hotkey on boot (system dependent, usually F2 or F10).

2 Go into the BIOS by using the default password.

3 Change the password in the appropriate menu.

Make sure to take a note of the new password (preferably on paper), and give it to the customer if he or she wants it.

4 Store the password in a safe place, since resetting a lost BIOS password is very difficult.

You will need the BIOS password for some (rare) service cases. For example, the system will not boot from USB or DVD by default, because the BIOS forbids it, but this can be changed if the system needs to be reinstalled on-site.

4.2 Disabling unused hardware interfaces

By default, the BIOS setting regarding the use of devices is as follows:

- all USB ports enabled
- one serial port enabled

- all Ethernet ports enabled
- other devices (for example, IEE1394, also known as FireWire) disabled

This is in most cases the setting the customer wants and needs. Some customers, however, want to have the USB ports at the front of the system disabled. Whether this is possible depends on the BIOS of the system; most systems allow it.

Do not disable the USB ports on the rear, since they are used for keyboard, mouse and license dongle.

Do also not disable internal USB ports, if present.

If the USB ports cannot be disabled selectively, consider using USB port locks (available, for example, from Kensington or Lindy). This is also an option, if the customer does not want to have the USB ports locked permanently, for example, if occasionally export to an external drive should be possible.

4.3 Time synchronization with the network

The system allows time synchronization via NTP. This setting is typically done on request by the customer. See also (→ Page 106 *Time synchronization*). As a service technician, you need to ask the customer for the name or IP address of the hospital's NTP server.

A public (Internet) NTP server is not recommended, since for security reasons the system should not have a direct Internet connection.

In addition, you need the current time zone of the installation, and whether automatic daylight time (summer time) switch should occur (if the specific time zone supports it).

The NTP settings are done in the configuration menu (section LocalHost / SiteInfo), please refer to the configuration manual for details.

4.4 Decomissioning or hardware change

When an MR system is decommissioned, or one of the computer systems (MRAWP, MRWP, MARS) needs to be replaced, it must always be assumed that all hard disks contain sensitive and personal information. This information must not leave the hospital uncontrolled.

✓ Service technician is logged in

◆ Remove the hard disks and give them to the customer. Make sure to tell the customer that the disks may contain sensitive data and should not be reused without deletion.

– or –

Use a disk erasure tool, for example, the blancco disk erasure software as described in the service manual, for deletion of the hard disk. Tell the customer that the disks have been deleted securely, and no information is left.

Be sure that not only the MRAWP disks have been treated that way, but also the disks in the MRWP and the MARS.

4 Information for Service Technicians

5 Safety

5.1 Activation of the *syngo* Security Package

Once the *syngo* Security Package has been enabled, access to the computer is possible only after the user has logged on and has been authorized.

By activating the *syngo* Security Package, the customer service technician turns your system into a system with high data protection level.

To secure your system, you will have to instruct a service technician as to which security options you want to be enabled.

⚠ CAUTION

Limited access to system.

After activating the security system, access is limited to only the defined users.

- Make sure that you have read and completed all preparatory steps.
- Back up your complete system as done after installation before activating the security system.

5.2 Configuration of the *syngo* Security Package

After activation, the *syngo* Security Package has to be configured immediately.

Based on your outline of the intended user management you can create user accounts, configure data access rights, and function execution privileges.

CAUTION

Behavior of secured systems

The hospital's security policy also affects the behavior of the *syngo* system in certain cases (for example, password strength requirements, enabled empty passwords, or locking of an account after a specific number of failed logins).

- Establish a user model for your hospital and verify it before the security system is activated.
- Establish a proper procedure for emergency access.
- You may enable the service page configuration, by which emergency login without password is possible provided the entered user name belongs to "Emergency access" group
- Always back up your system before enabling the security system and before any major changes.
- Inform all users about any changes and settings. They should contact you or any other administrator immediately in case of problems.

  It is recommended not to remove the predefined privileges of the administrative accounts because otherwise the administrator may not be able to solve system problems like disk is full (Bypass and archiving audit trail needed) or no license available (Bypass and change password for remote service needed). At least user management privilege should be granted. (Remark: system privileges assigned to build-in groups will not be removed without explicit user confirmation.)

5.3 Emergency Login

For every user who will work with the system, create a user account and assign a password.

The security policy influences the behavior in emergency cases. Depending on the security configuration, you can log on under the general emergency account in case of an emergency.

CAUTION

Inaccessible system

User access may be prevented due to forgotten or unknown accounts or passwords, or wrong setup (for example, in case of an emergency). Do not forget to define a general user account for emergency access and assign it to a group and a role both called “Emergency Access”. Define a local user account for emergency. The password for this account should never expire. Do not allow any user to change the password for this account.

- The users shall contact you immediately in case of problems.
- **Recommendations:**
  - Set the following attributes for emergency accounts: password never expires and user is not allowed to set password.
  - Define local accounts for emergency.
  - With VH22A, all user accounts (including emergency user account) is also subject to the lockout policy. Further, the default lockout duration in COEM is set to 0 which means that only user with administrator privilege can unlock the account. There is a service page configuration provided which when enabled, allows emergency user to login without password, provided the entered user name belongs to the "Emergency Access" group.

5.4 User Account Management

Authorized users (such as administrators) can set up the data protections.

As an administrator, you can add user(s) to group(s) for readjusting the data protections.

CAUTION

Protection of data is changed.

The access to the data is no longer possible.

- If too few protections for data are available, the person responsible for user management in hospital should add user(s) to the group(s) until access is possible.

5.5 Administration of the Audit Trail

Authorized users (such as administrators) can set up the Audit Trail and view, archive, and delete archived Audit Trail log files.

As an administrator, you can select for every application which audit events shall result in Audit Trail entries.

CAUTION

The system blocks when the audit trail is filled (too many records, or too much drive space covered).

In this case, it is not possible to work with the system. Emergency access is also not possible.

- To prevent system blockage, someone must archive the log files and remove them from the audit trail on a regular basis.
- When the audit trail blocks the system, user with the **SecuritySystem** > **BypassBlockedSystem** and the **Audit Trail** > **Archive** privileges can login to the system and delete/archive the log files.

5.6 PKI login

At interactive user level **PKI Login** is supported in *syngo*.

There will be a potential data loss of unsaved changes and switch user, when user is switched using PKI card.

Do not switch users during MR acquisitions, neither by pulling out the PKI card nor by logging off - especially not during contrast agent examinations. Otherwise, the running measurement will be stopped and the current patient will be closed.

If the PKI card is pulled out during acquisition, the screen gets locked once acquisition is over.

CAUTION

PKI card is pulled out during running acquisition leading to automatic screen lock.

Scan may need to be repeated.

- Please do not insert/replace a PKI card during running acquisition. Removing/Replacing the PKI card during acquisition will keep the current identity active until the acquisition is complete. Once acquisition is complete, the screen will be locked automatically.

5 Safety

6 Activation of the *syngo* Security Package

The following table gives an overview about available security settings:

Security properties	■ **User management**: Activates user management that is the basis for all other security options ■ **Data access check**: Access to data is always provided in accordance with the current permissions ■ **Functional check**: Access to functions is provided in accordance with the privileges granted to a user role ■ **Auditing**: Access to the system and configured actions are recorded in the **Audit Trail** ■ **Security status**: Status of the security is **inactive** before setting the **Security Properties**. After you save the newly configured properties in this dialog box, the **Security status** is displayed as **active**
DICOM access	**Enable trusted host functionality**: Access to the trusted host is enabled by default.
Remote service access	**SSL encryption**: Access to the remote service is granted. This configuration item is not linked to a license.
Emergency User	**Enable Emergency User**: Emergency user is able to login with a blank password.

6 Activation of the *syngo* Security Package

6.1 Preparatory steps for activating the *syngo* Security Package

The preconditions for *syngo* Security Package activation are given below.

Outline the intended user and security management before activating the *syngo* Security Package.

Document all settings after configuration of the *syngo* Security Package.

Develop a matrix that describes your needs concerning to following actions:

- Creation of user accounts
- Configuration of data access rights
- Function execution privileges for groups, roles
- Creation of special user accounts

Apart from the system administrator it may be useful to create one user account assigned to the **Administrators** group with the right to create other user accounts. Only users which are allowed to create new users can unlock blocked accounts, for example, if a user entered a wrong password three times.

Verify the developing matrix before activating the *syngo* Security Package.

The service technician should take the backup of your system before activating the *syngo* Security Package.

6.2 Enabling Security options

As a service technician, you have to perform the following steps to enable security options:

1 Login to an administrator service account and from main menu select **Options** > **Service** > **Local Service**.

Siemens Med Service Software window is displayed.

2 Enter your login information and wait for the systems authentication.

The **Siemens Med Service Software** main window is displayed.

Click **Configuration**.

3 From the **Configuration** navigation bar select **Security** > **Settings**.

The details of the settings that you can select are given below.

If you do not select **Data access check**, the data access rights cannot be restricted.

If you do not select **Functional check**, users that you create will have access to all functions irrespective of the roles and privileges assigned to them.

4 Click **Save** in the status bar of the dialog box.

Security was set. The administrator account will now be enabled. Please make sure to create a *syngo* user before disabling the administrator account. A message box is displayed.

5 Click **OK**.

Security was activated. Please enter an administrator password. For details about password rules, see: (→ Page 123 *Password Complexity*)

A message box is displayed.

6 Click **OK**.

7 The **Users Settings** page of the **Siemens Med Service Software** window is displayed.

You can also open the **Users Settings** page by selecting **Local Host > Users** in the **Configuration** navigation bar.

The default account is **meduser**, but can be changed.

8 Enter and confirm the password in the **Random Password** fields of the administrator account.

Use the **Account for Administrator** only the first time after the *syngo* Security Package was activated to create new user accounts.

9 If **Enable Autologin** is checked, *syngo* application starts without asking for username/password of meduser.

10 Click **Save** and then **Finish** on the status bar of the dialog box to confirm your settings.

11 Click **Home** in the main menu.

Reboot the system to apply the changes.

12 Click **OK** to start shutdown or select **Cancel**.

A message box is displayed.

13 Click **OK**.

An automatic restart is performed.

After a restart of the system, only authenticated and authorized persons can use the workstation.

14 Use the **Account for Administrator** to log on to the system and set up the security configuration.

Security options are enabled to secure your system.

During configuring the *syngo* Security Package, create a separate user account for each administrator and assign these accounts to both **Administrators** and **SecurityAdmins** groups.

After having configured the *syngo* Security Package, ask the service technician to back up the system to avoid loss of configuration data.

It is recommended to test the settings after configuration of the *syngo* Security Package.

6.3 Starting the *syngo* Security Configuration

After activation the *syngo* Security Package must be configured immediately.

Based on your outline of the intended user management system you will create user accounts, configure data access rights and function execution privileges with the User and **Security Management** features in the **syngo Security Configuration** window.

1 Log on to **Account for Administrator** to set up the user management.

2 From the main menu select **Options** > **Security** > **Configure...**.

The **syngo Security Configuration** window is displayed.

3 By clicking an item in the tree view on the left-hand side, displays the various pages for set-up.

Use the **Show/Hide Console Tree** icon if the tree view does not appear after start-up.

4 **User Management** for managing user, groups and roles with the following sub-folders:

- **Users** for creating and setting up user accounts
- **Internal Users** for checking built-in and internal system accounts
- **DICOM Nodes** for checking those accounts that are automatically created for all configured network partners
- **Groups** for managing the user groups and the group members
- **Roles** for managing the roles and their owners

5 **Security Management** with following sub-folders:

- **Data Access Permissions** for defining the access rights to any data
- **Functional Privileges** for defining the function execution rights based on the users/roles view

On the right-hand side, you see the settings page that has been selected on the left-hand side.

6 Activation of the *syngo* Security Package

7 Groups and Roles

7.1 Configuration of Groups and Roles

7.1.1 About groups and roles

The *syngo* security system makes use of users, groups, and roles.

- Groups are used to configure the same data access rights for a group of people (for example, everyone who works in a particular ward).

  We recommend to create a user group for every team or department of user model. And assign the user accounts to that group.

- Roles are used to configure the same function execution privileges for people with similar tasks (for example, physicians, nurses, or assistants).

Assign user accounts to a role.

7.1.2 Built-in groups and roles

By default, some general groups and roles are automatically created when you install the Windows operating system and *syngo*. The default groups and roles are named identically.

List of groups and roles names:

- EmergencyAccess
- SecurityAdmins
- RoleDoctor
- RoleMTA

7.1.3 No group hierarchies

You cannot create sub-groups (groups-in-groups), such as "Hospital" for hospital-wide permissions and "Neurology" for defining permissions for people working in the neurology department of the hospital.

7.1.4 Configuration levels

The security configuration provides you with two different ways to assign group members and owners of roles.

- Starting at the **Users** level easily provides a good overview about the current memberships of the user and lets you easily pick the desired groups or roles for this user.
- Starting at **Groups** or **Roles** level gives you a good overview of which users have already been assigned to the group or role under configuration.

7.1.5 Filtering Groups and Roles

If a large number of groups and roles are defined, you can use filters to limit the number of displayed items.

7.1.6 Using domains

Groups and roles can also be managed within domains on a network. These groups and roles are administered by the domain administrator. To use them, you must integrate these groups and roles into the *syngo* security system.

7.2 Creating a new Group

Depending on individual requirements, you can define user groups to configure the same data access rights for a group of users.

1. From the main menu task card, select **Options** > **Security** > **Configure...**.

   The **syngo Security Configuration** window is displayed.
2. In the navigation bar, open the **User Management** folder.
3. Select the **Groups** folder.
4. From the context menu select **New** > **Group**.

   The **Group** tab card is displayed.
5. In the **Group** tab card, enter a name and description.

- You cannot create sub-groups.
- You can create multiple groups.
- Each group name must be unique. The recommended group name minimum of at least 20 characters.
- Special characters e.g., " / \ [ ] : ; | = , + * ? < > are not allowed.

6 Open the **Members** tab card and apply the desired changes.

You can add members to groups or remove them by multi-selecting them in the **Available Users** list by clicking **Add** or **Remove**.

7 Click **Apply** to save the settings.

– or –

Click **OK** to save the settings and close the **Group** tab card.

8 Click  **Replicate now** to activate the new group immediately and to refresh the window.

The created group contains all the assigned members.

7.3 Creating a new Role

Depending on individual requirements, you can define roles to configure privileges for users. Privileges help users to perform specific functions within the system.

1 From the main menu task card, select **Options** > **Security** > **Configure...**.

The **syngo Security Configuration** window is displayed.

2 In the navigation bar, open the **User Management** folder.

3 Select the **Roles** folder.

4 From the context menu, select **New** > **Role**.

The **Role** tab card is displayed.

5 In the **Role** tab card, enter a name and description.

- You cannot create sub-roles.
- You can create multiple roles.
- Each role name must be unique. The recommended role name minimum of at least 20 characters.
- Special characters e.g., " / \ [ ] : ; | = , + * ? < > are not allowed.

If the group and role are identical then a message is displayed that all the changes made to the group or role is applicable for both.

6 Open the **Owners** tab card and apply the desired changes.

You can add owners to groups or remove them by multi-selecting them in the **Available Users** list by clicking **Add** or **Remove**.

7 Click **Apply** to save the settings.

– or –

Click **OK** to save the settings and close the **Role** tab card.

8 Click  **Replicate now** to activate the new role immediately and to refresh the window.

The created role contains all the assigned owners.

7.4 Creating a new Patient Group

Patient groups are the basis for the definition of data access checks.

Users belonging to a particular patient group have the same rights to access patient data during *syngo* Security Package configuration. You can assign one or more user groups to a patient group.

1 From the main menu task card, select **Options** > **Security** > **Configure...**.

The **syngo Security Configuration** window is displayed.

2 In the navigation bar, open the **Data Access Permissions** folder.

3 Select the **Patient Groups** folder.

4 From the context menu, select **New** > **Patient Group**.

5 In the window enter full name and descriptions in the **Full name** and **Description** fields.

- You cannot create sub-groups.
- You can create multiple patient groups.
- Each patient group name must be unique. The recommended role name minimum of at least 20 characters.
- Special characters e.g., " / \ [ ] : ; | = , + * ? < > are not allowed.

6 Select the **Grant Read Access for syngoServiceUsers in service sessions** check box to allow a service technician access to any patient data protected by this patient group.

7 Click **Apply** to save the settings.

– or –

Click **OK** to save the settings and close the **Patient Group** card.

8 Click  **Replicate now** to activate the new patient group immediately and to refresh the window.

The created patient group can access patient data.

By default, *syngo* delivers the built in **STANDARD** patient group for data protection. It serves as a fall-back protection for patient groups. Otherwise the patient group will be unprotected data and cannot be deleted. **STANDARD** is used if there is no other patient group assigned to a new patient.

7.5 Filtering Users, Roles or Groups

With the filter option you can filter the **Roles** or **Groups** in the **syngo Security Configuration** window.

1 Select the **User Management** folder in the **syngo Security Configuration** window.

2 From the drop-down list select the desired filter content.

3 Enter a filter criterion in the list to the right, or select an already existing options from the drop-down list.

4 Press **Enter** to apply the filter.

By using the filter option, you can reduce the number of displayed users, roles, or groups according to several filter criteria in the **syngo Security Configuration** window.

Only the users, roles, or patient groups that match the specified options are displayed. The filter criteria are retained unless it is retained.

7.6 Managing Groups, Roles or Patient Groups

You can manage groups, roles or patient groups by renaming or deleting.

7.6.1 Replacing an outdated Group, Role or Patient Group

1 Create a group, role or patient group with a new name instead of renaming.

2 Delete the outdated group, role or patient group.

Because of system integrity it is not possible to rename a group, role or patient group.

Because of system integrity it is not possible to delete the built-in user groups, roles or patient groups.

7.6.2 Deleting a Group, Role or Patient Group

1 Click the appropriate **Group**, **Role** or **Patient Group** folder in the navigation bar of the **syngo Security Configuration** window.

2 From the main menu, select the **Group**, **Role** or **Patient Group** and select **Action > Delete**.

3 Confirm the displayed message box by clicking **Yes**.

The desired group or role account, or patient group is deleted.

4 Click  **Replicate now** to activate the settings immediately and to refresh the window.

Groups or roles or patient groups are deleted from the **syngo Security Configuration** window.

Through deleting a group, a role or a patient group, all its members lose the corresponding privileges, rights, and data security.

To recover patients from a deleted group, your system administrator may help.

7.7 Integrating a Group from a Network Domain

Domains on network can provide defined user accounts, groups, and the assignments of users to groups. The domain administrator specifies the rights for the groups. If you want to use groups of a network domain (non-*syngo* groups), you have to integrate them into *syngo*.

1 Right-click **Groups** in the tree and choose the **Show all Groups** option from the context menu.

All groups including non-*syngo* groups will be displayed from the network domain.

2 Select the domain that provides the desired group from the list in the menu bar.

The groups that belong to the domain are displayed on the right-hand side of the window.

3 Right-click desired group in the **Name** column and select the **Integrate into syngo** menu item from the context menu.

4 Double-click the desired group to edit it.

7 Groups and Roles

Group is integrated into network domain.

8 Setup of Access Control

Access control in *syngo* security system consist of permissions (users and user groups who are allowed to access a certain data set) and functional privileges (user or roles who are allowed to execute a certain program module or function).

The different security levels applied to application functions and patient data in the context of the clinical workflow are normally defined in the hospital's security policy.

8.1 Privileges

A privilege is the right to use a specific *syngo* function, such as sending data or invoking the Patient Registration.

8.2 Patient Group Permissions

Patient group permissions regulate the access to data:

- You can define a list of patient groups according to the data security policy of your hospital. For example, create a patient group "Radiology" for data that should only be visible to members of the radiology department, or "VIP" for patient data that should only be visible to very few persons, such as the head physician.
- For each patient group, you can grant users and groups the permission to access data that is assigned to this group.

  You can set permissions for the following types of access:

  - **No Access**: The user will have absolutely no access to the data of this patient group.
  - **Full Control**: The user has access to the data, and can work with it according to the role. In general, the user can:
    - create data objects, like studies or series
    - read data, for example, load it into the Viewer
    - update or modify data. For example, draw annotations on images or correct the patient's name
    - delete data
    - execute changes to the security levels applying to certain data, for example, to hide the data of VIP patients from some doctors on the ward

  Permissions can be set at the patient or study level. Series and images inherit their permissions from the study to which they belong.

- A newly created patient entry or study is automatically assigned a patient group. Basically, this is the one that is assigned as default to the user (or to the group to which the user belongs).
  - If a user registers a new patient, this patient is first assigned to the default patient group.
  - If a user registers a new study of a known patient, the previously assigned patient groups are taken over.
  - If your system receives studies from a DICOM node and the patient is not known at your system, the default patient group of the DICOM node is assigned.
  - If your system receives studies of a known patient, the previously assigned patient groups are taken over.
- During **Patient Registration** and in the **Patient Browser**, you can modify the assignment of patient groups.

To reduce your configuration efforts, define permissions on group level and privileges on role level whenever possible.

8.3 Inheritance of Permissions and Privileges

The security system follows an inheritance strategy: Any right granted on group or role level is inherited by all members.

Typically, a user belongs to at least one group and one role. But you can also assign a user to more than one group or role.

The **Everyone** group is the top level of inheritance. The permissions set for the **Everyone** group are transferred to all groups of your security system. The same rule applies to the **Everyone** role.

In the configuration user interface, this effect is indicated by the display of **Effective** rights.

- It is not possible to deny rights that the user inherited from a group or role.
- It is possible to grant additional permissions and privileges for single users. This way you expand the permissions and privileges that have been defined for the group or role.
- Because of the heredity rules, it is very important to check and restrict the rights of the **Everyone** group and role.

The final decision as to whether a user will be granted an execution privilege or a permission depends on the inheritance hierarchy of roles and groups to which the user belongs.

8.4 Managing Patient Groups for data protection

(→ Page 82 *Data protection*)

(→ Page 83 *Special configuration issues*)

8.4.1 Data protection

The permissions (data access rights) are configured on the basis of patient groups. All data assigned to the same patient group has the same protection attribute.

You can create patient groups as desired according to your security concept and workflow, but *syngo* delivers some patient groups for data protection by default:

- The **STANDARD** patient group is a built-in group. It cannot be deleted, because it is used as a fall-back protection for otherwise unprotected data. The patient group is internally assigned to any data object that has not been explicitly assigned a protection (for example, a user without default protection created a new patient entry). Also any data that "loses" its patient group is also assigned to this group.

  Any user concerned with the import of data from archive or storage disks should have **Full Control** access to the STANDARD patient group.
- The **Emergency** patient group can be used to protect data from emergency acquisition.

- The **Service** patient group is used to prohibit common access to the internal service patient.
- The **LOST&FOUND** patient group collects all studies that had been assigned to unknown or to undefined patient groups. Using this patient group, you can configure permission on this type of data. At least one user must have **Full Control** access.
- The **ALL_ACCESS** patient group gives all users complete access to all functions and data: The **Everyone** group has **Full Control** access.

Whenever a user registers a new study, a default data security level is applied to that data. You can configure the default data security level either for groups or for individual users.

Different views on the **Data Access Permissions** are available (based on the same configuration data):

- The **by User/Group View** allows selecting a single user or group and setting the rights on the various patient groups.
- The **by Patient Groups View** allows selecting a single patient group and setting the various user or group access rights.

8.4.2 Special configuration issues

Before modifying any security settings, it is important to take some special configurations into consideration:

- Follow a strategy regarding the **Everyone** group . Check the effective permissions. These are inherited from the various groups, including the top level **Everyone** group, see (→ Page 19 *Terms and Definitions in Security*).
- We recommend to allow the administrator group **Full Control** to the **Lost&Found** patient group.
- We recommend to allow the **Everyone** group **Full Control** to the **STANDARD** patient group.
- Please ensure that at least one administrator or user with administrative rights has access to each patient group.
- Do not configure **No Access** for all patient groups.

8 Setup of Access Control

9 Permissions and Privileges

9.1 Configuring Permissions in the User's View

Permissions give the user the right to create, read, update, delete or protect data. Depending on individual requirements, you can determine access rights to any data.

You can set up the data access permissions in the view of users/groups or in the view of patient groups.

- Switch between both views to identify all dependencies and set up the permissions accordingly.

9.1.1 Setting up Permissions in the User's View

1. From the navigation bar, click **Security Management** > **Data Access Permission** > **By User / Group**.
2. Select any one of the level options from **Everyone**, **Groups** or **Users** for whom you want to set up the permission.
3. Select an item from the drop-down list on the top left-hand corner of the dialog box.

   The drop-down list displays the names of the configured groups or users.

Do not select the **List only objects with permissions assigned**. If you select the check box, the list of the patient groups containing **Full Control** permission (**Eff. Permission** column) are displayed.

The drop-down list is disabled if the **Everyone** level is selected.

4 For each **Patient Group** select the desired access right from the drop-down list in the **Permission** column.

5 Click **Apply** to save the protection.

– or –

Click **OK** to save and close the dialog box.

6 Click  **Replicate now** to activate the new settings immediately and to refresh the window.

Permission are set in **User's view** to all the assigned groups and users.

The *syngo* Security Package follows an inheritance strategy. The **Everyone** group represents the top-level inheritance.

Any right granted on group level is inherited by all members. This is displayed in the **Effective Permissions** column.

Inherited rights cannot be denied to a user/group. However, additional the desired access rights can be assigned to the user/group.

9.2 Setting up the default Patient Group

You can configure the default protection for groups and users.

1 For each **Patient Group** for whom you want to configure default protections select the check box in the **Default** column.

2 Click **Apply** to save the protection.

– or –

Click **OK** to save and close the dialog box.

3 Click  **Replicate now** to activate the new settings immediately and to refresh the window.

The deviation between default settings (**Default** column) and effective default settings (**Eff. Default Patient Group** column) of patient group may originate from different configurations in the user items **Everyone**, **Groups** and **Users**, or from a membership in different user groups.

Whenever you create a user or a group, it is assigned to the **Patient Groups** configured here.

9.3 Setting up Permissions in the Patient Group View

For each patient group, you can grant permissions to groups or users. Full control or no access to data permissions is marked with that patient group.

1 From the navigation bar, click **Security Management** > **Data Access Permission** > **By Patient Group**.

The **Patient Group** dialog box is displayed.

2 Select any one of the level options from **Everyone**, **Groups** or **Users** for whom you want to set up the permission.

3 Select an item from the drop-down list **Patient Groups**.

The drop-down list displays the names of the configured patient group.

Do not select the **List only objects with permissions assigned**. If you select the check box, the list of the patient groups containing **Full Control** permission (**Eff. Permission** column) are displayed.

4 For each **User Group** select the desired access right from the drop-down list in the **Permission** column.

Permission are set in patient group view to all the assigned groups and users.

The deviation between permission settings (**Permission** column) and effective permission settings (**Eff. Default Patient Group** column) of user/group may originate from different configurations in the user items **Everyone**, **Groups** and **Users**, or from a membership in different user groups.

9.3.1 Setting up the default data protection

You can configure the default protections for patient groups.

1 For each **User/Group** for whom you want to configure default protection select the check box in the **Default** column.

2 Click **Apply** to save the protection.

– or –

Click **OK** to save and close the dialog box.

3 Click  **Replicate now** to activate the new settings immediately and to refresh the window.

The deviation between default settings (**Default** column) and effective default settings (**Eff. Default Patient Group** column) of patient group may originate from different configurations in the user items **Everyone**, **Groups** and **Users**, or from a membership in different user groups.

Whenever you create a user or a group, it is assigned to the **Patient Groups** configured here.

Changes to security settings are effective only when no images are loaded to an application.

Data access permissions are not valid until the data is unloaded from all applications.

9.4 Setting up Privileges

The privileges give the user the right to execute *syngo* functions, such as sending data, correcting data or setting a work status.

1 From the navigation bar, click **Security Management** > **Functional Privileges** > **By User / Role**.

The **Privileges of** dialog box is displayed.

The side tabs correspond to the various *syngo* modules installed at your system.

2 Select any one of the level options from **Everyone**, **Roles** or **Users** for whom you want to set up the privileges.

3 Select an item from the drop-down list **Privileges of**.

The drop-down list displays the names of the configured roles/ users.

4 Select the level of objects you want to configure at the top of the dialog box.

The drop-down list is disabled if the **Everyone** level is selected.

5 Select the desired access right from the left hand list of role/user.

6 Select the **Grant** column check box to enable the desired privilege.

7 Click **Apply** to save the protection.

– or –

Click **OK** to save and close the dialog box.

8 Click  **Replicate now** to activate the new settings immediately and to refresh the window.

The side tabs correspond to various *syngo* modules installed at your system.

An asterisk "*" at the beginning of the function name or privilege name indicates unsaved data.

Note that certain **Privilege** settings lead to serious malfunctions, e.g., if **Everyone** does not have the privilege interactive login, no one is able to log on to the system.

10 Information for Users

For security reasons, only authorized persons have access to sensitive data, such as diagnostic images, results, or reports.

syngo allows you to work only with the data and functions that you have been authorized to use. All other patient data is not visible to you and the prohibited functions are not available.

Contact and discuss with your administrator, in case your privileges seem insufficient to complete your task.

The audit trail logs all activities you perform on sensitive data in an audit trail. This also includes your identity.

Except for emergency access, you are only allowed to work with a *syngo* workstation if you are logged into your personal user account.

The system administrator will notify you about your user account and password.

10.1 Starting the computer locked by BitLocker

If the BitLocker is installed, you can boot the computer system only if the correct USB stick with the corresponding encryption key is connected to the computer.

✓ The correct USB stick is at hand.

1 Connect the correct USB stick to the computer before you switch on the computer.

The USB stick with the encryption key is needed only for booting. Once the software is running, you can remove the stick.

» **If you start the computer without the correct USB stick connected, the following message appears: Windows BitLocker Drive Encryption key needed**

- Insert the correct USB stick and press **ESC**, to restart the computer system.

2 If you do not need the USB stick anymore, reposit the stick in a secure location, for example, in a safe.

For more information, contact your administrator.

10.2 User Management and Access Control

10.2.1 User Accounts, Permissions and Privileges

The *syngo* user model ensures that every user is allowed to access only to the data the user is authorized to work with (data security) and to the functions the user is authorized to use (functional security).

10.2.2 How are you integrated in the *syngo* user model?

- The administrator created a user account for user. To work with *syngo*, user has to log on using logon credentials (password protected).
- Depending on user profession and duties, user is assigned one or several **Roles**, for example, nurse or doctor. **Privileges** that are associated with your roles give you the right to access specific *syngo* functions.
- Depending on the departments and/or teams user work in, user is assigned to one or several **Groups**. The rights on data are granted to all members of a group by **Permissions**.

- Members of the same group have access permissions to the same data. Users with the same roles have the same privileges for executing functions. The administrator can also set up privileges and permissions for every user individually.

  It is also possible to extend the data rights for someone beyond a group, for example for a doctor who wants a second opinion from a colleague on another ward.

- Depending on user permissions, administrator can manually grant access to data that you have created to members of a group who would otherwise not be able to access this data.

The user configuration depends on the security regulations of your hospital. For questions about your rights, ask the system administrator.

If you are asked to work temporarily in another department, for example to take over from a sick colleague, the administrator can temporarily assign you to this group.

10.3 Logging on and off

To log on to a workstation, enter your user name and password. After the system has authenticated you, you get access to the *syngo* application.

Logging off or locking a workstation does not interrupt or abort running or queued background jobs, such as filming images. Every background job is protocoled under the identity of the user who initiated it.

To log off, click **Log off**.

If you have finished your work, you can log off. This ends your session at the computer. All patient data is closed. At a new log on, *syngo* appears in a neutral state.

To ensure high throughput of patients, two assistants share modality consoles. While one assistant prepares a patient for the examination, the other assistant sends the images from the previous examination to the archive. Both assistants have the same privileges and permissions.

The switch user function allows them to efficiently work together at the same console. In this way, they can alternately use the consoles without suffering delays or losing the work of the other user.

To switch the user at your workstation, click **Log in Different User**.

If you share the workstation with other users, you can hand over the workstation quickly by using the switch user function.

The current user is logged off. The workstation can only be used by the new user after logging on.

If the new user has the same (or sufficient) access rights, the current images are not unloaded.

If the new user does not have the appropriate access rights, all patient data is unloaded and the currently active application function is terminated. Unsaved data will be lost.

Do not switch users during MR acquisitions, neither by pulling out the PKI card nor by logging off - especially not during contrast agent examinations. Otherwise, the running measurement will be stopped and the current patient will be closed.

As long as a measurement is running on your system, logging off is not possible. After stopping or finishing the measurement, you can log off again. Running background jobs, for example, image reconstructions will be completed.

10.4 Lock computer

1 From main menu, click **Options** > **End Session** menu item or press **CTRL**+**ALT**+**DEL** click **Lock Computer** to lock your computer.

The computer is locked.

If you have to leave your workstation unattended for a longer period without quitting your session, you should lock the workstation with this function.

2 Press **CTRL**+**ALT**+**DEL** and log on to unlock the computer.

If you are the person who locked the workstation, you will find your session as you left it.

If another user unlocks your computer and does not have the appropriate access rights, a warning appears. Only after explicit confirmation, any patient data is unloaded (without saving) and the currently active application function is terminated.

If a screen saver has been enabled on your workstation, it is automatically activated whenever there has been no mouse or keyboard activity for a certain period. The screen saver has the same effect as Lock Computer.

10.5 Change password

1 Press **CTRL**+**ALT**+**DEL** and click **Change Password**

2 Enter the password and confirm password.

The password is case sensitive. Its complexity depends on the settings in the **Password Complexity** tab. See (→ Page 123 *Password Complexity*)

The password is changed.

10.6 Failed log on

You cannot change your account name, but you can change your own password. Only administrators are allowed to change user accounts names.

If you have been denied access to your workstation because you have forgotten your user name or password proceed as follows:

- Ask your administrator for your current account name. The account name is not case sensitive.
- Make sure that the **Caps Lock** key is not accidentally set.

  Passwords are case sensitive.
- If this does not lead to success, ask your administrator to give you a new password.

10.7 Use of the Screen Saver

Screen Saver

You can configure a *syngo* screen saver. The screen saver locks the workstation if there has been no mouse or keyboard activity within a certain period.

Please note that for safety reasons the screen saver will not appear automatically during measurements. The screen saver could hide safety relevant popup windows, for example, that the patient needs attendance. However, it is possible to evoke the screen saver manually by pressing Ctrl-Alt-Del.

To unlock the workstation, the user must enter the account name and the password in the **Computer locked** dialog box.

The screen saver has the same effect as the **Lock Computer** function. If a user logs on to a workstation again, the user finds the workstation exactly as the user had left it. If another user logs on, depending on the permissions, pervious users data is closed and the unsaved changes are lost.

Configuration

The screen saver is automatically enabled during system installation.

In the **syngo Configuration Panel** use the **Screen Saver** to configure the inactivity period (time-out) before activation.

11 User Accounts

11.1 Configuration of User Accounts

User Accounts

For every user who will work with the system, create a user account and assign a password.

A user account that is no longer required can be disabled or deleted.

Always work in the **syngo Security Configuration**, never use the Microsoft Management Console (MMC) to create or to manage user accounts. *syngo* expands the Windows-related security system by data security management and distinguishes between groups and roles.

Note that the *syngo* security system only makes use of some fundamental levels of security granted to users by the Windows operating system. Moreover, the *syngo* security system has its own security concept.

Domains

Users can be members of domains provided by a network (RIS/HIS). Domains are used to manage groups of computers or users with common security privileges and are managed by domain administrators. Typically, only these administrators have the right to configure domains which typically involve in adding or defining user access rights. The *syngo* security system allows to select users from domains. Users, who are managed by a computer's operating system (and not the *syngo* security system) can be easily integrated into *syngo*. Creating new user accounts is only possible on your local system or has to be done by the domain controller within the network. Per default, the local users are displayed.

Filter

If the number of displayed users, groups or roles is large, it is possible to limit the displayed items by using signs or keywords as filter criterion. Only the items matching the criterion are displayed.

Special User Accounts

The security system comes with some default and some internal user accounts, and automatically generates DICOM Node user accounts.

All **internal users** are essential for the system and indicated as such. We strongly recommend not changing the passwords of these users!

- Default users are delivered with the software and contain, for example, the Administrator, the LocalServiceUser and the RemoteServiceUser.
- DICOM nodes are required for remote network functions. They are created as soon as you configure the DICOM services (AET). You can only change the password and the group assignment of these users.

Handling of Passwords

The password of a user in *syngo* may expire, and users may be allowed to change their passwords on their own (depending on the hospital's security policy).

You can assign a user a new password at any time.

Account lockout

If a wrong password was entered three times or if the password has expired, the account is locked. Only users which are allowed to create new accounts can re-activate a locked account.

The default setting for the account lockout duration is set to "0". If you keep the default duration value, the account is permanently locked out!

11.2 Creating a new User Account

Every person working with *syngo* needs a user account.

1 From the navigation bar, click **User Management** > **Users**.

2 From the context menu, select **New** > **User**.

The **User** tab card is displayed.

3 Enter the following details to create the user account:

- User name and the complete name
- Additional information about the user in the description
- Password and confirm password

The name in the **Name** field must be unique within the system and should consist of alphanumeric characters only.

Special characters e.g., " / \ [ ] : ; | = , + * ? < > are not allowed.

The recommended user name minimum of at least 20 characters.

Passwords are case-sensitive. It must be a combination of upper case, lower case, numbers, and non alpha numeric characters are allowed.

The **Password never expires** check box is selected by default. When selected, the password of a user in *syngo* never expires, but the user can change the preliminary password when logging on to the system.

If the **Password never expires** check box is not selected, the password expires based on the system configuration.

The user can change the password only if the **User cannot change password** check box is not selected during account creation.

4 Select the **User cannot change password** check box if you do not want to enable the users to modify the login password at subsequent logins.

It is recommended to use this option for **Emergency Accounts** only.

In order to facilitate rapid access to the system in case of an emergency, create at least one special user account for general emergencies.

5 Click the **Members of** tab to add/remove members to/from the group.

- See (→ Page 100 *Adding a member to Assigned Groups*)
- See (→ Page 101 *Removing a member from Assigned Groups*)

6 Click the **Owner of** tab to add/remove members to/from the role.

- See (→ Page 101 *Adding an owner to Assigned Roles*)
- See (→ Page 102 *Removing an owner from Assigned Roles*)

7 Click **Apply** to save the new user account.

– or –

Click **OK** to save the new account and to close the **User** tab card.

8 Click  **Replicate now** to activate the new settings immediately and to refresh the window.

The created user account contains all assigned members and owners.

Create at least one user account that is intended to stand in as both an administrator and security administrator.

11.2.1 Adding a member to Assigned Groups

1 Open the **Member of** tab card.

The **Assigned Groups** list displays user groups to which the user belongs.

2 From the **Assigned Groups** list, select the desired group to which you want to assign a user and click **Add**.

3 Click **Apply** to save the assignment.

– or –

Click **OK** to save the settings and close the dialog.

4 Click  **Replicate now** to activate the new settings immediately and to refresh the window.

11.2.2 Removing a member from Assigned Groups

1 Open the **Member of** tab card.

The **Assigned Groups** list displays user groups to which the user belongs.

2 From the **Assigned Groups** list, select the desired group from which you want to remove a user and click **Remove**.

3 Click **Apply** to save the removal.

– or –

Click **OK** to save the settings and close the dialog.

4 Click  **Replicate now** to activate the new settings immediately and to refresh the window.

11.2.3 Adding an owner to Assigned Roles

1 Open the **Owner of** tab card.

The **Assigned Roles** list displays the roles to which the user group belongs.

2 To add role to the **Assigned Roles** list, select the required roles from the **Available Roles** list, and click **Add**.

3 From the **Assigned Roles** list, select the desired role to which you want to assign a user and click **Add**.

4 Click **Apply** to save the assignment.

– or –

Click **OK** to save the settings and close the dialog.

5 Click  **Replicate now** to activate the new settings immediately and to refresh the window.

11.2.4 Removing an owner from Assigned Roles

1 Open the **Owner of** tab card.

The **Assigned Roles** list displays the roles to which the user group belongs.

2 From the **Assigned Roles** list, select the desired role from which you want to remove a user and click **Remove**.

3 Click **Apply** to save the removal.

– or –

Click **OK** to save the settings and close the dialog.

4 Click  **Replicate now** to activate the new settings immediately and to refresh the window.

11.2.5 Disabling a User Account

You can modify the properties of a user account, and enable or disable an account.

1 From the navigation bar, select the **User Management folder** > **Users**.

A list with all available user accounts is displayed.

2 Double-click the desired user account.

The **User** tab card is displayed with the properties for the selected user account.

3 Make the required modifications. See (→ Page 98 *Creating a new User Account*) for more information on the modification options.

4 Click **Apply** to save the new settings.

5 Click  **Replicate now** to activate the new settings immediately and to refresh the window.

It is not possible to rename a user account. You have to delete it and create a new one.

11.2.6 Deleting a User Account

1 From the navigation bar, select the **User Management folder** > **Users**.

A list with all available user accounts is displayed.

2 Select the user account and select **Delete** from the context menu.

A message box appears asking for the confirmation.

3 Click **Yes** to confirm.

4 Click  **Replicate now** to activate the new settings immediately and to refresh the window.

Due to system integrity, you cannot delete the built-in user accounts, and special accounts for example DICOM nodes.

11 User Accounts

12 Audit Trail

12.1 Audit Trail and Log Files

The *syngo* security system has an audit trail for recording the following actions:

- All user activities on sensitive data
- All logins (and unsuccessful login attempts)
- System shutdowns, system restarts and similar events

By reviewing the audit trail, all security relevant transactions can be reconstructed.

The audit trail consists of several log files, where only one log file is open at any one time. A new log file is created whenever the current log file is closed. This occurs, at *syngo* startup. A new log file is also created at system restart after a power failure.

As soon as a log file reaches a certain size, it is closed. Closing the file automatically creates a new one.

12.1.1 Naming of Log Files

To keep the files in the correct order, a number is appended to the file name, which is incremented with each new file:

file name = <host name>_<date of creation>_<Time of creation>_<incremented number>

example: "csant42_2002-04-14_10-47-28_1.xml"

12.1.2 Administration

Authorized users (such as administrators) can set up the audit trail and view, archive and delete archived audit trail log files. The files are protected against manual manipulation.

The audit trail log files are encrypted by default. These files are decrypted while displaying the same through audit trail Viewer.

12.1.3 Configuration

To configure the audit trail, you need to define general security parameters, such as the trail's location and size, and any transactions that are to be recorded.

The setup of the audit trail consists of two different parts (and two different configuration dialog boxes):

- Parameters for location, size and warning level as well as archiving parameters are set up in the **Audit Trail Settings** dialog box.
- Events to be recorded in the audit trail are specified in the **Audit Trail Management** console.

Because the size of the audit trail increases by time, *syngo* provides the **Audit Trail Archiving** dialog box to archive log files and to delete them subsequently.

You have to archive the audit trail at regular intervals. Failure to do this will cause the audit trail to fill up the disk partition, causing the system to block until the audit trail has been archived and removed.

Please ensure that archived audit files are kept according to national and local regulations.

In case of audit trail failure event logs are created and an auto report is sent to configured recipient.

12.1.4 Time synchronization

Timestamps for log file entries must be consistent within all log files in the audit trail. Therefore, it is important that all system components are synchronized with respect to time.

If you use a network of *syngo* systems, you can establish a special NTP (Network Time Protocol) that ensures a synchronized time all over the network system. Ask the service technician to connect *syngo* to the network.

You carry the responsibility for maintaining the time server. Ensure that you set the correct time, otherwise your service license may become outdated. This is because the license manager only accepts a jitter of 24 hours. When the service license becomes invalid, the system must be completely reinstalled.

12.2 Configuration of Audit Trail Settings

The *syngo* Security Package has an **Audit Trail** for recording all user activities in the system.

12.2.1 Setting up the Audit Trail

1 Log in as an administrator.

2 From the main menu, select **Options** > **Configuration...**.

The **syngo Configuration Panel** is displayed.

3 Double-click the **Audit Trail** icon.

4 Select the auditing mode.

- **Local file system**
- **Central syslog server**

5 Click **Next** to continue the following settings.

- Setting up the **Local file system** parameters see (→ Page 110 *Selecting the archive target for Audit Trail*)
- Setting up the **Central syslog server** parameters see (→ Page 110 *Setting up the Central syslog server parameters*)

6 Click **Setup** to start the configuration.

When the configuration is completed, the **Audit Trail Settings** dialog box is displayed.

By clicking the **Back** button in the dialog box, you can return to the previous dialog box without saving the settings you made to the existing dialog box. Click **Next** to move forward for completing the configuration.

The Audit Trail has to be enabled by the service technician.

12.2.2 Setting up the Local file system parameters

1. From the main menu, select **Local file system** and click **Next**.
2. Select the **Audit Trail directory**.

   A browser opens where you can navigate to select the folder of your choice.
3. Select the maximum size of the Audit Trail in the **Max. size [kBytes]** field.
4. Select the **Zipped** check box to compress the Audit Trail log file.
5. To determine the percentage of the storage capacity of the warning limit, use the up and down arrows to select the values in the **Warning level [%]** field.

A warning level of 80-85% is suggested.

6. To determine the percentage of the storage capacity of the warning limit, use the up and down arrows to select the values in the **Quota level [%]** field.

A quota limit of 90-95% is suggested.

7. Click **Next** to continue setting up the common parameters of the Audit Trail.

The local file systems parameters are configured for auditing.

The default drive for storing the Audit Trail must be located in %windir%\system32\winevt\logs\Auditing.

Always make sure that there is enough space on the drive for storing the Audit Trail. Otherwise the system will not get out of the blocked system state until enough space is available and a reboot is made.

As soon as a log file reaches this predefined size, it is closed, and a new log file is created.

Note that due to encryption of log files the physical storage requires 3 times the size of normal log file configured. For example, if the configured file size is 2 KB, then log files need 6 KB storage space on the physical storage.

As soon as the predefined percentage of the storage capacity of the hard disk is reached, a yellow warning icon is displayed in the status bar. A message box opens and informs you about the situation and how to proceed. Storing should be started immediately, otherwise the system blocks.

A message box opens and informs you about the situation and how to proceed.

As soon as this predefined percentage of the storage capacity of the hard disk is reached, a red warning icon is displayed in the status bar.

If the quota limit is filled the system is blocked and the administrator has to log on to the system again.

CD-R/USB is an exchange media and not suitable for long-term storage.

12.2.3 Setting up the Central syslog server parameters

1 Select the **Central syslog server** option from the Audit Trail settings and click **Next**.

The **Central auditing settings** dialog box is displayed.

2 Enter the host name and port number into the appropriate fields.

3 Select the protocol and the encoding type from the drop-down lists.

4 Click **Test** to verify the connection to the host.

5 Click **Finish** to save the configuration and to return to the **Audit Trail Settings** dialog box.

6 Click **OK** to exit the configuration.

The **Central syslog server** parameters are configured for auditing.

12.2.4 Audit Trail Storage

(→ Page 110 *Selecting the archive target for Audit Trail*)

(→ Page 111 *Storing the Audit Trail on CD-R*)

(→ Page 111 *Storing the Audit Trail on Network share*)

(→ Page 112 *Storing the Audit Trail on USB*)

Selecting the archive target for Audit Trail

1 Select the desired archive target in the **Audit Trail Settings** dialog box.

- Storing on CD-R

  See (→ Page 111 *Storing the Audit Trail on CD-R*).

- Storing on the Network share

  See (→ Page 111 *Storing the Audit Trail on Network share*).

- Storing on USB

  See (→ Page 112 *Storing the Audit Trail on USB*).

2 Click **Next** to continue setting up the common parameters of the Audit Trail.

Storing the Audit Trail on CD-R

✓ When storing on CD-R, insert an appropriate medium.

1 Select the **CD-R** archive target from the **Audit Trail Settings** dialog box and click **Next**.

2 Select the desired session type:

- If you select the **Single session** option, the **Finalize** check box is disabled.
- If you select the **Multi session** option it would allow you to store log files in multiple session. For multi-sessions, you may select the **Finalize** check box, it will finalize the session and the CD cannot be used for further storage.

3 Select the **Drive letter** from the drop-down list.

4 Select the **Burning speed** from the drop-down list.

5 Click **Finish** to save the configuration and to return to the **Audit Trail Settings** dialog box.

6 Click **OK** to exit the configuration.

Storing the Audit Trail on Network share

✓ For storing on network shares, the connection must be established.

1 Select the network share archive target in the **Audit Trail Settings** dialog box and click **Next**.

2 Enter the user name, domain, password and path of the network share into the network share fields.

3 Click **Test** to verify the path of the network folder.

If you do not click **Test** and have entered an incorrect network path, the Audit Trail details would not be saved. It is recommended to test the network path before saving the configurations.

4 Click **Finish** to save the configuration and to return to the overview **Audit Trail Settings** dialog box.

5 Click **OK** to exit the configuration.

If wrong data were entered in the fields for a network share, no error message is displayed after storing and during operation. It is important to check the data with the **Test** button.

The syntax for a share name is: **`\\servername\sharename\[folder]`** example: **`\\deeparchive\archaudit\at2002`**

Storing the Audit Trail on USB

✓ When storing on USB an appropriate device should be inserted.

1 Select the **USB** archive target from the **Audit Trail Settings** dialog box and click **Next**.

2 Select the drive from the drop-down list.

3 Click **Finish** to save the configuration and to return to the **Audit Trail Settings** dialog box.

4 Click **OK** to exit the configuration.

12.2.5 Configuration of Audit Trail Content

Event recording and the Audit Trail viewer are configured in the **Syngo - Audit Trail Management** window.

To access the **Syngo - Audit Trail Management** do the following:

1 From the main menu, select **Options** > **Audit Trail** > **View**.

2 The **Syngo - Audit Trail Management** window is displayed.

You need the **AuditTrail > SetFilter** privilege to configure the **syngo - Audit Trail Management** window.

Defining events to be recorded in the Audit Trail

1 From the navigation bar, select **Syngo** > **Audit Filter** window.

The **Audit Trail Filter Configuration** tab is displayed.

2 Click the desired application folder in the **Audited Component** list on the right-hand side of the window.

The audit events pertaining to that application are displayed.

3 Select the **Audit Event** check box to record the desired actions.

4 Click **Save** to save the settings.

Audit Trail event recording is defined.

The **Reset** button is used to clear your changes.

The default setting for auditing is to record all user actions on the *syngo* system.

Detailed recording can slow down system performance.

12.2.6 Managing Log Files

After defining the options for auditing, you can view, filter, store, and delete the log files.

(→ Page 113 *Viewing Log Files*)

(→ Page 114 *Filtering Log Files for Viewing*)

(→ Page 114 *Storing Log Files*)

(→ Page 116 *Deleting Log Files*)

Viewing Log Files

1 From the navigation bar, click **Syngo** > **Audit Viewer**.

The **File to view** window is displayed.

2 Select the desired folder in the **Files to view** field.

- If **Log Files** are selected then the all .xml and .xml.z log files are displayed.
- If **Auditing** is selected list of log files .xml.z with time stamp is displayed.

3 Double-click the log file in the **Total** list to view it.

4 Click **New Audit Trail** to view the current log file.

The current log file will be closed and added to the list in the **Total** field.

Back up the Audit Trail regularly.

Before doing new installations on the system, the current Audit Trail should be archived. Otherwise the data on drive C:\ will be overwritten.

You need the **AuditTrail > View** privilege to view **Audit Trail** log files.

Filtering Log Files for Viewing

To inspect a log file further, you can apply different filters or apply certain filter criteria.

1 Select the desired filters from the selection lists above the content area.

– or –

Copy a parameter from the log file and initiate an exact match search in the **Argument Filter criteria** field.

2 Click **Refresh**.

The content area shows only the data records that meet the filter criteria.

To reset a filter, select **All...** in the corresponding filter list and click **Refresh**.

Storing Log Files

1 From the main menu, select **Options** > **Audit Trail** > **Archive**.

The **Audit Trail Archiving** dialog box is displayed.

The available log files are listed.

Archiving status is displayed by the corresponding icon:

	Log file is not stored.
	Log file is stored.
	Log file is not stored but contain important information about data manipulation (for example, deletions).
	Log file is stored and contains important information about data manipulation (for example, deletions). The stored files must be kept according to national and local regulations (for example, 6 years).

2 Select the desired log files for storing in the **Audit Trail Archiving** dialog box.

3 Click **Archive** to store the selected log files to the predefined **archive target**.

The selected log files are stored and a message is displayed.

You need **AuditTrail** > **Archive** privilege to store or delete log files of the Audit Trail.

The current log file has to be closed before storing it.

When storing the Audit Trail on CD-R, existing export jobs are suspended.

Restart suspended jobs manually after the Audit Trail is stored.

Deleting Log Files

1 From the main menu, select **Options** > **Audit Trail** > **Archive**.

The **Audit Trail Archiving** dialog box is displayed.

You have to store log files before you can delete them.

2 Select the desired log files for deleting in the **Audit Trail Archiving** dialog box.

3 Click **Delete** to delete the selected log files.

The selected log files are deleted and a message is displayed.

13 Assigning Patients or Studies during Operation

In the **Patient Browser**, you can modify the assignment of patient groups or studies.

1 Log in as an administrator.

2 From the main menu, select **Patient** > **Browser**.

– or –

Press the  **Browser** key on the numeric keyboard.

– or –

Press the **.Del** key on the numeric keyboard.

The **Patient Browser** window is displayed.

3 Select the patient or study in the local database.

4 From the main menu, select **Edit** > **Modify Patient Groups**.

The **Modify Patient Groups** dialog box is displayed.

5 Confirm your selection with **OK**.

The selected patient groups or studies are modified.

You need the privilege **Patient Browser > Modify Patient Groups...** to assign patients or studies to patient groups.

To work with the **Browser** key on the symbol keypad, the **syngo Security Configuration dialog** box has to be closed.

13.1 Secure Transfer of Data

During the site-specific configuration of the local system, a service technician sets up the connection to network nodes, central archives, DICOM service providers and DICOM service users.

To establish a secure system, all these network partners and services must be reliable.

One policy is to establish a trusted sites zone. A trusted zone contains network nodes you trust--nodes that you believe you can receive data from or send data to without worrying about the security of computer or data.

To establish a trusted zone, you must assign nodes to this zone. Then the *syngo* security features let the system:

- Transfer and receive data, knowing that the computer and confidential patient information are safe.
- Only accept DICOM Query/Retrieve requests from trusted hosts or applications. Requests from unknown workstations or applications are rejected.

13.1.1 Security of Protocols

For security reasons, *syngo* follows a restrictive policy concerning ports and IP addresses. Data traffic through all unnecessary ports and addresses is blocked. Data exchange is restricted to defined paths only.

- After installation, all ports and addresses are blocked except for a few basic services, such as ports for the DICOM services.
- By configuring DICOM network nodes in the **Local Service Software**, the IP addresses become valid and the necessary ports are unlocked.
- If you need additional IP addresses for other reasons, you should define them as network nodes in the **Local Service Software** to enable them.

13.2 Service Access

In order to allow service activities, users with the appropriate privilege must grant the service technician access to the computer. The procedure differs for the local and remote service access.

Local access

Usually, a user account with restricted rights is created for the service technician for carrying out local service activities.

To allow local service activities you need to generate a temporary password for the general **LocalServiceUser** account. This password expires after a predefined number of days. Using this password, a service technician can log on to the computer under the **LocalServiceUser** user account.

Usually the **LocalServiceUser** account is member of the **syngoServiceUser** group and role. This way, the service technician obtains permissions and privileges as determined by the system administrator.

Remote access

Remote service access lets a service technician carry out maintenance activities from a remote workstation.

You can start a remote service session and wait for the response from the remote workstation. Depending on the required service activities, you can then grant the technician full or limited access to your workstation.

- Full Access
- Limited Access
- Access to Patient Data
- Remote Application Support
- No Access

Unexpected closing can cause inconsistent or inoperable system!

If you close a remote service session while the service technician is still working, all currently running service programs will be terminated. This may result in an inconsistent or inoperable system.

The service technician will only be notified that the session is going to be closed by you.

It is recommended that you seek permission from the service technician before you close the session.

13.3 Generating a Service Password for Local Access

To allow local service works for the service technician, the system will generate a temporary service password for the general **LocalServiceUser** account.

Using this password, a service technician can log on to the computer under the **LocalServiceUser** account.

13.3.1 Generating a temporary Password

1 From the main menu, select **Options** > **Service** > **Service Account**.

The **Set Password for the account LocalServiceUser** dialog box is displayed.

2 Enter the reason for a service access and the name of the service technician.

3 Enter the account expiration period in days.

4 Confirm with **Apply** to generate the password.

The generated password is displayed next to **Assigned password**.

5 Note down the password.

6 Click **Close** to end.

7 Keep the password confidential and pass it only to the service technician.

You need the privilege **EnableServiceAccount** to use the **Service User** menu item.

You can change the password with a double-click the **LocalServiceUser** account in the **syngo Security Configuration** dialog box.

13 Assigning Patients or Studies during Operation

14 Additional Information

14.1 Assign new password for internal users

1 Log in as an administrator.

2 From the main menu, select **Options** > **Configuration...**.

The **syngo Configuration Panel** is displayed.

3 Double-click the **Reset Password** icon.

4 Select the **Reset Password** tab.

5 Check on the users from the user list to reset the password.

6 Click the **Reset Password** button.

A message box is displayed asking for the confirmation to rest the password and to restart the machine.

7 Click **OK**.

A message box is displayed with list of selected users whose password should be reset.

8 Click **OK**.

The system is restarted.

Password is reset for all the selected users.

14.2 Password Complexity

Automatically generated passwords consist of the following characters: 4 upper case letters, 4 lower case letters, 4 special characters, and 4 digits.

Customized passwords must contain at least one from each of these 4 groups.

1 Log in as an administrator.

2 From the main menu, select **Options** > **Configuration...**.

The **syngo Configuration Panel** is displayed.

3 Double-click the **Reset Password** icon.

4 Select the **Password Complexity** tab.

5 Select the value from the list for minimum no. of uppercase, minimum no. of lowercase, minimum no. of numbers, minimum no. of non alpha numeric, and minimum password length.

Maximum total value of password complexity is 20 characters.

If the value of minimum password length do not match the configured value of the password a warning message is displayed.

6 Click **OK**.

A message box is displayed asking for the confirmation to restart the machine.

7 Click **OK**.

A message box is displayed asking for changing the password of the administrator and the front end users after the system has restarted.

8 Click **OK**.

The system is restarted.

All the user listed in **Reset Password** tab would get a new password with defined complexity. All the other system users would get the defined complexity.

14.3 Setting up the Certificate Handler

1 Log on as an administrator.

2 From the main menu, select **Options** > **Configuration...**.

The **syngo Configuration Panel** is displayed.

3 Double-click the **Certificate Handler** icon.

The **syngo Certificate Handling** dialog box is displayed.

4 Select one of the check boxes from **syngo Certificate Handling** dialog box.

- **Import intermediate/root certificates (PKI, SSL) with Windows Certificate Wizard**
- **Import certificate for secure connection to syngo service portal**
- **Import certificate for DICOM secure connection**
- **Reset to self signed certificate (machine and service portal)**

5 Click **Next** to make the required configuration as per the selected check box.

- Import intermediate/root certificates (PKI, SSL) with windows certificate wizard parameters see (→ Page 125 *Setting up Import Intermediate/Root Certificates*)
- Import certificate for secure connection to *syngo* service portal parameters see (→ Page 126 *Setting up Import certificate for secure connection to syngo service portal*)
- Import certificate for DICOM secure connection parameters see (→ Page 126 *Setting up Import certificate for DICOM secure connection*)
- Reset to self-signed certificate (machine and service portal) parameters see (→ Page 126 *Setting up Reset to self-signed certificate*)

The certificate is imported for the secure connection or reset to self-signed certificate in the system.

14.3.1 Setting up Import Intermediate/Root Certificates

1 Select **Import intermediate/root certificates (PKI, SSL) with Windows Certificate Wizard** from **syngo Certificate Handling** dialog box and click **Next**.

The **Certificates** dialog box is displayed.

2 Select any one intermediate or root certificate from the **Personal** tab and click **Import**.

The intermediate or root certificate is imported into the system.

14.3.2 Setting up Import certificate for secure connection to *syngo* service portal

1 Select **Import certificate for secure connection to syngo service portal** from **syngo Certificate Handling** dialog box and click **Next**.

The **syngo Certificate Handling** dialog box is displayed.

2 Select USB, CD/DVD drive, or default(c:\syngo\config\service \certificates) from **Select any Certificate Location**.

3 Select the certificate from the drop-down list.

4 Select the private key file (pfx) from the drop-down list.

5 Enter the password in **Provide Password** filed.

6 Click **Import**.

The certificate is imported for the secure connection into the system.

14.3.3 Setting up Import certificate for DICOM secure connection

1 Select **Import certificate for DICOM secure connection** from **syngo Certificate Handling** dialog box and click **Next**.

syngo Certificate Handling for DICOM Communication dialog box is displayed.

2 Select USB, CD/DVD drive, or default(c:\syngo\config\service \certificates) from **Select any Certificate Location**.

3 Select the certificate from the drop-down list.

4 Select the private key file (pfx) from the drop-down list.

5 Enter the password in **Provide Password** filed.

6 Click **Import**.

Certificate is imported for DICOM secure connection into the system.

14.3.4 Setting up Reset to self-signed certificate

1 Select **Reset to self signed certificate (machine and service portal)** from **syngo Certificate Handling** dialog box and click **Next**.

The **syngo Certificate Handling** dialog box is displayed.

2 Click on any one of the following options to reset the self-signed certificate.

- **Rest to built-in self signed certificate**
- **Rest to built-in self signed certificate for DICOM communication**
- **Export certificate for DICOM communication**

The certificate is reset to self-signed certificate or user can export the certificate.

14 Additional Information

Index

T

U

V

CE 0123

Manufacturer's note:

This device bears a CE mark in accordance with the provisions of Council Directive 93/42/EEC of June 14, 1993 concerning medical devices and the Council Directive 2011/65/EU of June 08, 2011 on the restriction of the use of certain hazardous substances in electrical and electronic equipment.

The CE marking applies only to medical devices which have been put on the market according to the above-mentioned EC Directives. Unauthorized changes to this product are not covered by the CE mark and the related Declaration of Conformity.

Legal Manufacturer
Siemens AG
Wittelsbacherplatz 2
DE-80333 Muenchen
Germany

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

Print No. MR-05024.640.02.02.24 |

www.siemens.com/healthcare