SITRANS IQ

Communication and software SITRANS serve IQ Getting Started

Getting Started

10/2021

A5E47612806-AD

Legal information

Warning notice system

This manual contains notices you have to observe in order to ensure your personal safety, as well as to prevent damage to property. The notices referring to your personal safety are highlighted in the manual by a safety alert symbol, notices referring only to property damage have no safety alert symbol. These notices shown below are graded according to the degree of danger.

⚠DANGER

indicates that death or severe personal injury **will** result if proper precautions are not taken.

⚠WARNING

indicates that death or severe personal injury **may** result if proper precautions are not taken.

⚠CAUTION

indicates that minor personal injury can result if proper precautions are not taken.

NOTICE

indicates that property damage can result if proper precautions are not taken.

If more than one degree of danger is present, the warning notice representing the highest degree of danger will be used. A notice warning of injury to persons with a safety alert symbol may also include a warning relating to property damage.

Qualified Personnel

The product/system described in this documentation may be operated only by **personnel qualified** for the specific task in accordance with the relevant documentation, in particular its warning notices and safety instructions. Qualified personnel are those who, based on their training and experience, are capable of identifying risks and avoiding potential hazards when working with these products/systems.

Proper use of Siemens products

Note the following:

⚠WARNING

Siemens products may only be used for the applications described in the catalog and in the relevant technical documentation. If products and components from other manufacturers are used, these must be recommended or approved by Siemens. Proper transport, storage, installation, assembly, commissioning, operation and maintenance are required to ensure that the products operate safely and without any problems. The permissible ambient conditions must be complied with. The information in the relevant documentation must be observed.

Trademarks

All names identified by ® are registered trademarks of Siemens AG. The remaining trademarks in this publication may be trademarks whose use by third parties for their own purposes could violate the rights of the owner.

Disclaimer of Liability

We have reviewed the contents of this publication to ensure consistency with the hardware and software described. Since variance cannot be precluded entirely, we cannot guarantee full consistency. However, the information in this publication is reviewed regularly and any necessary corrections are included in subsequent editions.

Siemens AG
Digital Industries
Postfach 48 48
90026 NÜRNBERG
GERMANY

Document order number: A5E47612806
Ⓟ 10/2021 Subject to change

Table of contents

About this Document 1

This document provides instructions to install:

- SITRANS serve IQ
- Additional software components like Docker and Keycloak
- Siemens Automation License Manager.

It includes:

- Instructions how to add and manage users
- Configuration of connections to IMAP and SCADA systems (via standard interface IEC 60870-5-104)
- Recommendation of security and firewall setting

Always check on the Siemens Industry Online Support (SIOS) for newest Information, including FAQ section: https://www.siemens.com/SIOS/sitransserveiq (https://www.siemens.com/SIOS/sitransserveiq)

We recommend that you align with your IT department prior to installation.

1.1 Introduction

Remote sensors in the field either feature their own wireless communication module and send their measurement and status data directly via the mobile network (e.g. MAG 8000 3G/4G) – or are connected to an RTU30xxc (preferably Modbus, alternatively 4..20 mA/HART), which then sends the data via the mobile network. In both cases, the process data, alarms and status indicators are included in csv-files which are being sent via email to a designated customer email-account.

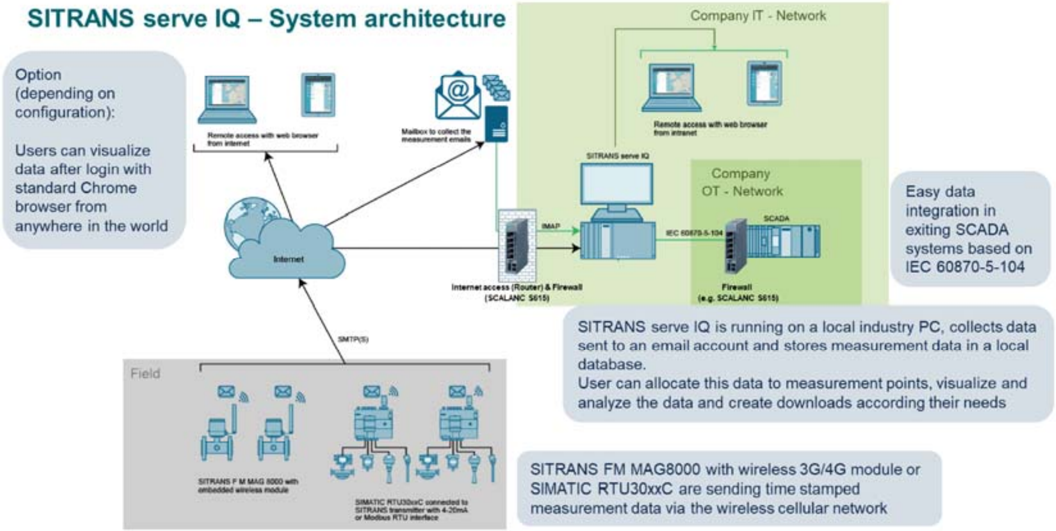
SITRANS serve IQ is an on-premises application which downloads the emails, extracts the information, and stores it locally.

The data can be visualized in trends and tables via web browser. In addition, warnings and alarms can be defined in SITRANS serve IQ to inform of threshold violations, based on the data received. Furthermore, data can be downloaded.

SITRANS serve IQ is available in English and German only.

Optionally,

- the measurement data can be sent to SCADA via IEC 60870-5-104 telemetry protocol commonly found in the water and power industries.
- the SITRANS serve IQ can be accessed from the Internet. Note: additional IT security measures are recommended. Due to licencing constraints, access to serve IQ must strictly be limited to the organization holding the licenses.



SITRANS serve IQ – System architecture

Option (depending on configuration):

Users can visualize data after login with standard Chrome browser from anywhere in the world

Easy data integration in exiting SCADA systems based on IEC 60870-5-104

SITRANS serve IQ is running on a local industry PC, collects data sent to an email account and stores measurement data in a local database.
User can allocate this data to measurement points, visualize and analyze the data and create downloads according their needs

SITRANS FM MAG8000 with wireless 3G/4G module or SIMATIC RTU30xxC are sending time stamped measurement data via the wireless cellular network

Company IT - Network
Remote access with web browser from internet
Mailbox to collect the measurement emails
Remote access with web browser from intranet
SITRANS serve IQ
Company OT - Network
SCADA
IMAP
IEC 60870-5-104
Internet
Internet access (Router) & Firewall (SCALANC S615)
Firewall (e.g. SCALANC S615)
SMTP(S)
Field
SITRANS F M MAG 8000 with embedded wireless module
SIMATIC RTU30xxC connected to SITRANS transmitter with 4-20mA or Modbus RTU interface

Figure 1-1 SITRANS serve IQ - System architecture

1.2 Software architecture and components

The solution consists of:

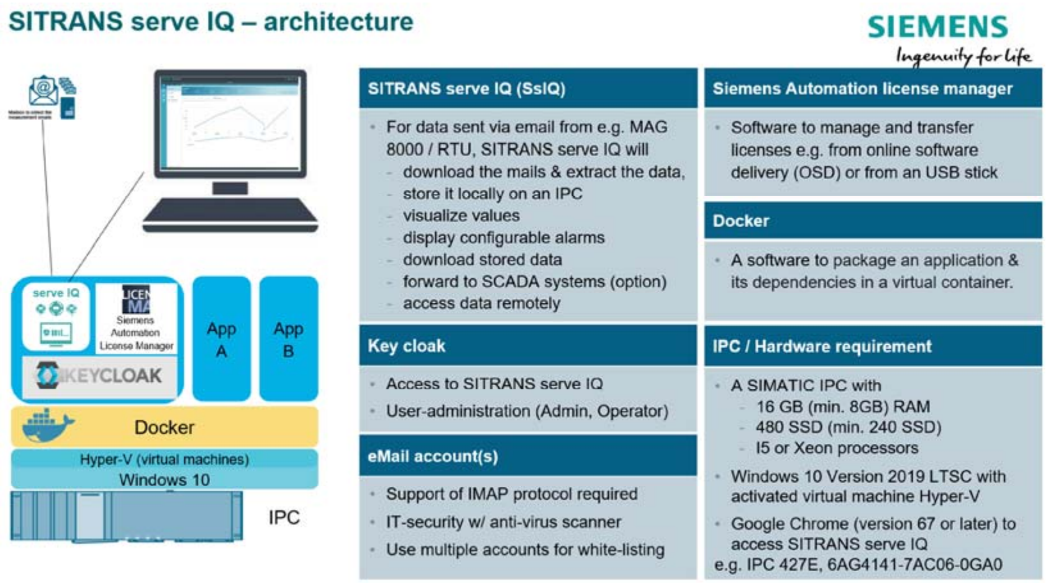
- The hardware and network:
  - The solution SITRANS serve IQ runs on a dedicated hardware. We recommend a Siemens industry pc IPC427E Microbox PC.
  - The IPC must be connected to the Internet and must be protected from the Internet with a dedicated firewall (e.g. SCALANCE S615)
  - In case that you fully utilize the system, including access from the Intranet and backend-connection to the Scada Systems:

    a) a fixed IP address or registered domain

    b) additional measures for ensuring proper IT security, see Configuration of firewall/Router settings (Page 32).

    c) further IT security measures to allow data communication to the specified SCADA system (e.g. additional firewall).
- The software
  - Underlying the software is is the operating system **Windows 10** IoT Enterprise 2019 LTSC (including its features Hyper-V and Container)
  - **Docke**r, which creates a runtime environment on the designated drives
  - An application **‘Keycloak’** to manage user rights and grant access rights to the software
  - The software **SITRANS serve IQ** {SsIQ). SsIQ is an application that always runs in the background.
  - The Automation License Manager **ALM** to transfer required licenses
  - A standard browser (recommended: Google Chrome) to access the software SITRANS serve IQ (SsIQ). Note: even if the user is on the very same IPC, access to SsIQ will be via the browser.

Also, to provide remote support, customers may choose to install a respective software like SINEMA Remote Connect.



SITRANS serve IQ – architecture

SIEMENS
Ingenuity for life

serve IQ
LICEN MA
Siemens Automation License Manager
KEYCLOAK
App A
App B
Docker
Hyper-V (virtual machines)
Windows 10
IPC

SITRANS serve IQ (SsIQ)

- For data sent via email from e.g. MAG 8000 / RTU, SITRANS serve IQ will
  - download the mails & extract the data,
  - store it locally on an IPC
  - visualize values
  - display configurable alarms
  - download stored data
  - forward to SCADA systems (option)
  - access data remotely

Siemens Automation license manager

- Software to manage and transfer licenses e.g. from online software delivery (OSD) or from an USB stick

Docker

- A software to package an application & its dependencies in a virtual container.

Key cloak

- Access to SITRANS serve IQ
- User-administration (Admin, Operator)

eMail account(s)

- Support of IMAP protocol required
- IT-security w/ anti-virus scanner
- Use multiple accounts for white-listing

IPC / Hardware requirement

- A SIMATIC IPC with
  - 16 GB (min. 8GB) RAM
  - 480 SSD (min. 240 SSD)
  - I5 or Xeon processors
- Windows 10 Version 2019 LTSC with activated virtual machine Hyper-V
- Google Chrome (version 67 or later) to access SITRANS serve IQ

e.g. IPC 427E, 6AG4141-7AC06-0GA0

Figure 1-2 SITRANS serve IQ - software architecture

A complete list of the used Open-Source-Software, you will find in the ‘OSS Readme for SITRANS serve IQ’ under https://www.siemens.com/SIOS/sitransserveiq (https://www.siemens.com/SIOS/sitransserveiq)

Prerequisites for installing SITRANS serve IQ 2

2.1 Data sources: SITRANS MAG 8000 and SIMATIC RTU

SITRANS serve IQ application is compatible with the following devices:

- SITRANS F M MAG8000 with a wireless communication module (WCM) for 3G/UMTS*
- SIMATIC RTU30xxC

*the 3G module is downward compatible with the 2G network. A 4G version is in preparation.

At the place of installation, a sufficient mobile phone coverage is required. Please refer to the respective manuals for further information and additionally required items like e.g. SIM Cards for data traffic. The WCM and the RTU can be programmed with different frequencies to a) capture a data point from the connected sensors and to b) send the captured data via the mobile phone network. We recommend:

- to capture at least once an hour a measurement value from the sensors. Customers often choose 5 to 15 min intervals of capturing data. A higher capture rate of measurements will influence battery life.
- to configure the devices (the WCM / the RTU) to send the emails with data - files to that email account, from which SITRANS serve IQ is downloading the data. We recommend sending data at least daily. In case of crucial and time critical measurement points, the interval of sending emails could be reduced to once an hour or even less. Please note, that alarms defined in SITRANS serve IQ will only react to data that has been received via email by SITRANS serve IQ. Increased sending of emails will influence battery life.

Note

Settings of a MAG 8000

- The prefix of the csv file name must be set to "MAG8000" (default value) in the wireless module, otherwise the csv files attached in the email can't be recognized by SITRANS serve IQ.
- The subject of the emails sent by the MAG 8000 must be set to: "MAG8000: 12345H789" (where the Serial Number of the device is 12345H789)
- The local time zone setting should be set to 0, i.e. UTC time in the wireless module. Current versions of the SITRANS serve IQ will assume the data-stamps to be in UTC and convert time-stamps to the time-zone settings in the IPC.

Please refer to the Operating Instructions of 3G/UMTS module for the setting details.

Note

Settings of an RTU

- The correct allocation of data in SITRANS serve IQ depends on the proper naming of the log-filenames (csv-files), sent by the RTU. **Only the first 3 digits** of the log filename of the attachment in the email from the RTU3000 are used to distinguish the data sources. Hence it is crucial, that you select these first 3 digits well and do not allocate the same to another RTU, that is sending its data to the same mailaccount.
- The local time zone setting should be set to 0, i.e. UTC time in the wireless module. Current versions of the SITRANS serve IQ will assume the data-stamps to be in UTC and convert time-stamps to the time-zone settings in the IPC.

Please refer to the Operating Instructions of the RTU for the setting details.

Ideally, before installing SITRANS serve IQ, some emails with data have been sent and are available in the Mailbox for proper testing of successful installation.

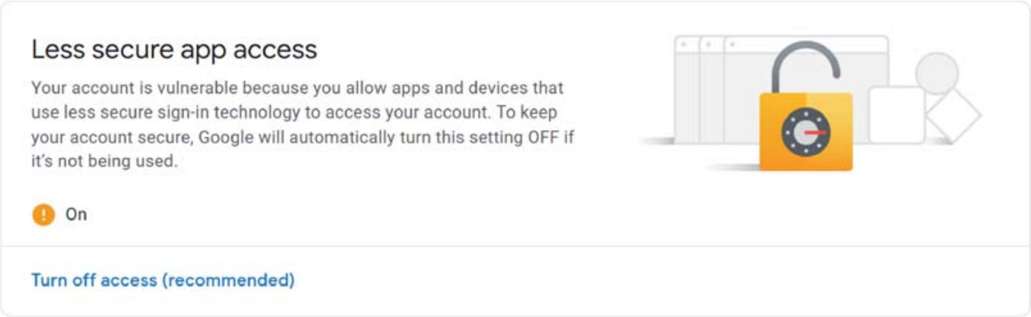
2.2 Email account used for receiving emails with data

SITRANS serve IQ can only be connected to an email account based on IMAP protocol. The credentials must be available during commissioning.

We recommend using a dedicated email account for each SITRAN serve IQ installation and using it only for data connection. The email account shall not contain any personal information.

It is advised to use proper mailboxes settings for receiving mails with data. Activate anti-virus mechanism & monitor the email traffic actively.

Provider of email services are increasingly using two-factor-authentification for granting access to the respective mailbox and are considering simple log-ins with username and password as 'less secure'. For SITRANS serve IQ to still be able to connect, you need to enable 'access by less secure apps'. See example below. Likewise, if SITRANS serve IQ was disconnected for some time from the mailbox (e.g. a week), you might need to re-activate the 'less secure access'.



Less secure app access

Your account is vulnerable because you allow apps and devices that use less secure sign-in technology to access your account. To keep your account secure, Google will automatically turn this setting OFF if it's not being used.

! On

Turn off access (recommended)

Note

Notes on data authentication

SITRANS serve IQ identifies emails with data only by the serial number (MAG) or first three digits (RTU) of the attachment, there is no mechanism to authenticate devices resp. email accounts sending data. Therefore, it is recommended to white-list known sending devices (some customers apply multiple mailboxes):

1. Mailbox 1 will receive all emails. In addition, it features a ‘white-list’ of all known sender-emails, that are entitled to send data to SITRANS serve IQ. Only emails coming from these senders are being forwarded to the 2nd Mailbox.
2. Mailbox 2 will only accept emails forwarded from the 1st Mailbox. SITRANS serve IQ will access and download only from this 2nd Mailbox.

2.3 Industry PC: hardware and software requirements

Hardware Requirements

We recommend installing SITRANS serve IQ on a standalone SIMATIC IPC (IPC 427E Microbox PC, MLFB 6AG4141-5AC05-0GA0 or 6AG4141-7AC06-0GA0).

We recommend 16 GB of RAM and 450 GB SSD, i5 processor or higher, minimal configuration is 8GB RAM and 250GB HDD.

Software Requirements

The software requirements for installing SITRANS serve IQ are:

- Microsoft Windows 10 IoT Enterprise 2019 LTSC with support for 'Hyper-V' and 'Containers' features
- Google Chrome™ web browser (version 67 or later)
- SITRANS serve IQ installation software with valid license(s)
- Internet access to OpenStreetMap server
- Access to an email account that supports IMAP protocol

SITRANS serve IQ is only tested on SIMATIC IPC. The proper functioning of SITRANS serve IQ will not be guaranteed if it is installed on PCs other than specified stand-alone SIMATIC IPC.

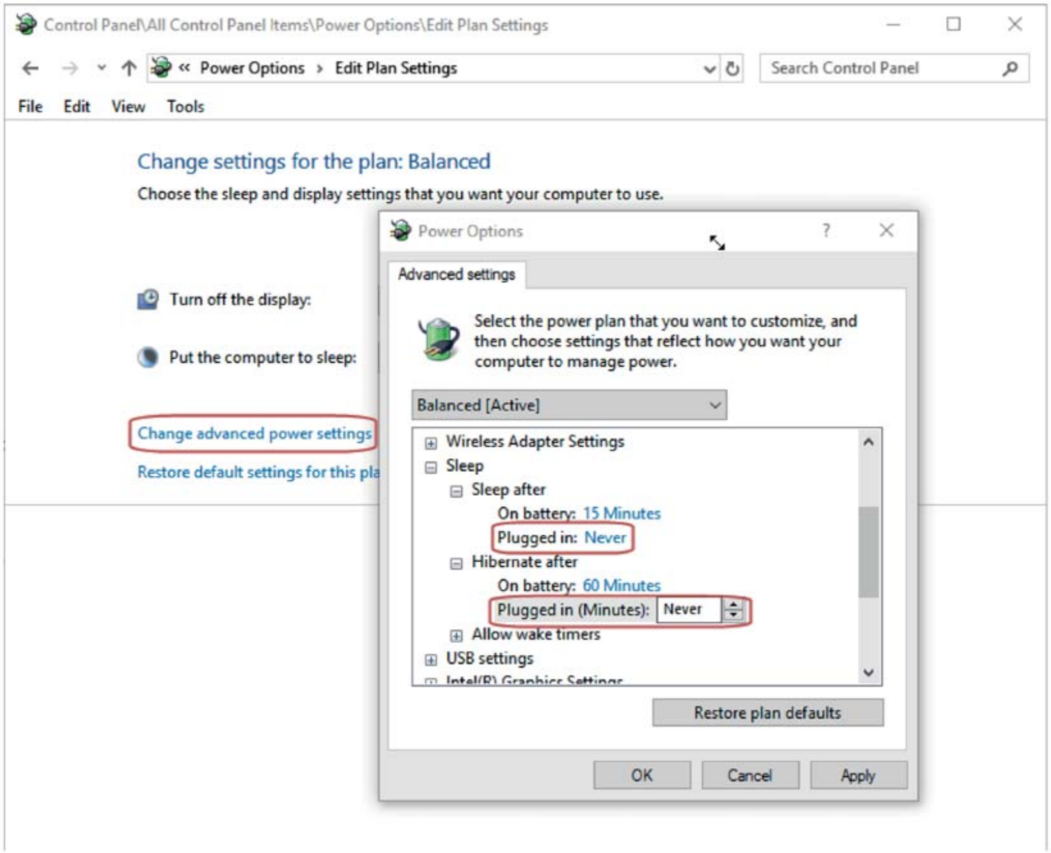
Note

Running SITRANS serve IQ on virtual machines

There are reports that SITRANS serve IQ is running successfully on virtual machines. As SIEMENS has not fully system tested this approach, we are unable to guarantee full functioning of SITRANS serve IQ system though.

2.4 Preparation of the hardware (IPC)

The PC should not go to sleep or hibernate while the SITRANS serve IQ is running, since putting Windows 10 to sleep could disturb the application in the docker container. Therefore, the value of "Sleep after" and "Hibernate after" in Power Options in Control Panel should be set to "Never".


Control Panel\All Control Panel Items\Power Options\Edit Plan Settings
« Power Options › Edit Plan Settings
Search Control Panel
File
Edit
View
Tools
Power Options
?
Restore plan defaults
OK
Cancel
Apply

Change settings for the plan: Balanced

Choose the sleep and display settings that you want your computer to use.

Turn off the display:

Put the computer to sleep:

Change advanced power settings

Restore default settings for this pla

Advanced settings

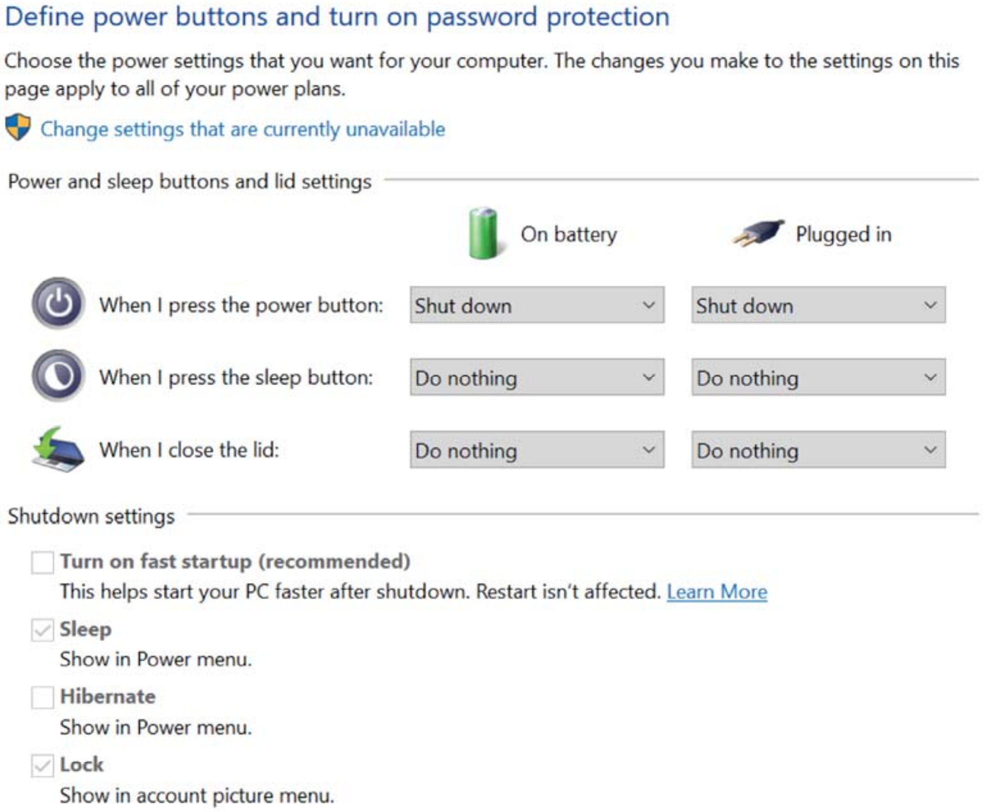
Select the power plan that you want to customize, and then choose settings that reflect how you want your computer to manage power.

Balanced [Active]

- Wireless Adapter Settings
- Sleep
  - Sleep after
    - On battery: 15 Minutes
    - Plugged in: Never
  - Hibernate after
    - On battery: 60 Minutes
    - Plugged in (Minutes): Never
  - Allow wake timers
- USB settings
- Intel(R) Graphics Settings

Fast Startup feature in Windows 10 should be disabled to guarantee the required resources is properly loaded during system reboot. Please uncheck the box "Turn on fast startup (recommended)" in Shutdown settings. Also, disable any option that might put the computer to sleep.

If you would like to power down the computer, first log out of SITRANS serve IQ. Then run the script "stop SITRANS serve IQ". After that, you may power down your computer. We recommend to always power it down entirely. Don't use hibernate or sleep mode and choose the respective settings accordingly (see picture below).



Define power buttons and turn on password protection

Choose the power settings that you want for your computer. The changes you make to the settings on this page apply to all of your power plans.

Change settings that are currently unavailable

Power and sleep buttons and lid settings

	On battery	Plugged in
When I press the power button:	Shut down	Shut down
When I press the sleep button:	Do nothing	Do nothing
When I close the lid:	Do nothing	Do nothing

Shutdown settings

□ **Turn on fast startup (recommended)**
This helps start your PC faster after shutdown. Restart isn't affected. Learn More

☑ **Sleep**
Show in Power menu.

□ **Hibernate**
Show in Power menu.

☑ **Lock**
Show in account picture menu.

2.5 Windows 10 settings: activation of Hyper-V and Container

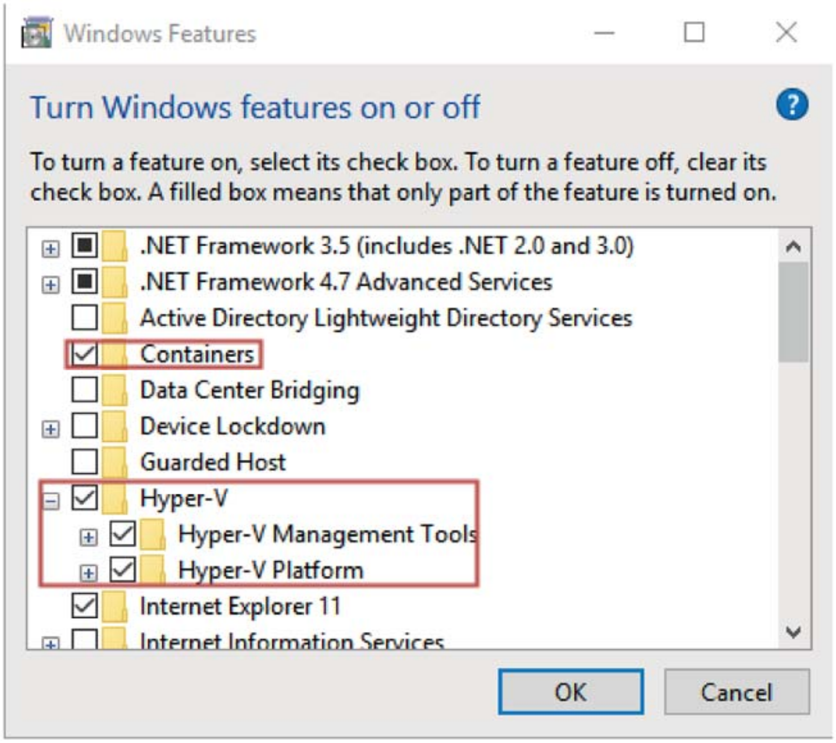
Hyper-V and Container features in Windows 10 are required to install SITRANS serve IQ.

Installation

Before you begin, ensure you have **administrator rights** on the PC/Server for installing SITRANS serve IQ, with a strong password. When installing, always execute ‘run as administrator’.

To launch Hyper-V service for virtual machine:

- Click the **Start** icon and type **Turn windows features on or off**.
- On the **Turn windows features on or off** screen, select all **Hyper-V** and **Container** check boxes.
- Click **OK**. The computer restarts.



Windows Features

Turn Windows features on or off

To turn a feature on, select its check box. To turn a feature off, clear its check box. A filled box means that only part of the feature is turned on.

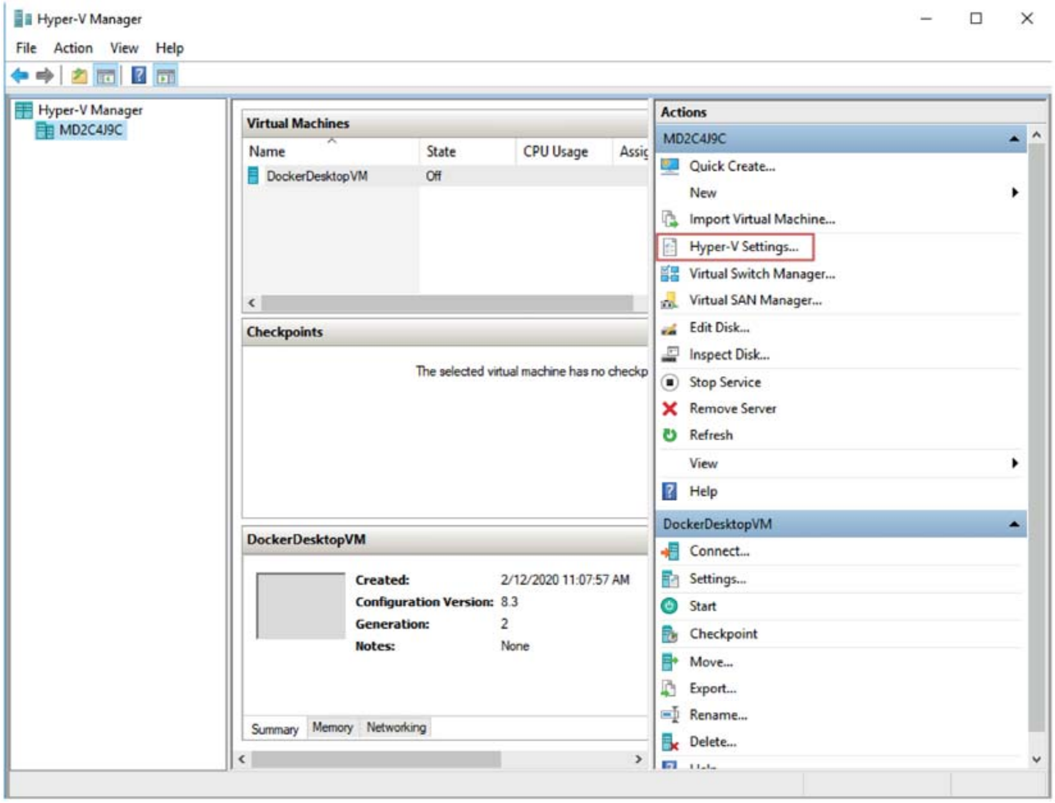
⊞ ■ .NET Framework 3.5 (includes .NET 2.0 and 3.0)
⊞ ■ .NET Framework 4.7 Advanced Services
□ Active Directory Lightweight Directory Services
☑ Containers
□ Data Center Bridging
⊞ □ Device Lockdown
□ Guarded Host
⊟ ☑ Hyper-V
⊞ ☑ Hyper-V Management Tools
⊞ ☑ Hyper-V Platform
☑ Internet Explorer 11
⊞ □ Internet Information Services

Change the Location of the Hyper-V Service

Virtual Machine Disks of Hyper-V must be installed on the same drive as the SITRANS serve IQ application. As the Windows operating system is normally installed on the C: drive, **it is recommended to install on drive C as well.**

To change the location of the Hyper-V service:

- Click the **Start** icon and type **Hyper-V**.
- Click **Hyper-V Manager** from the results to launch the console.

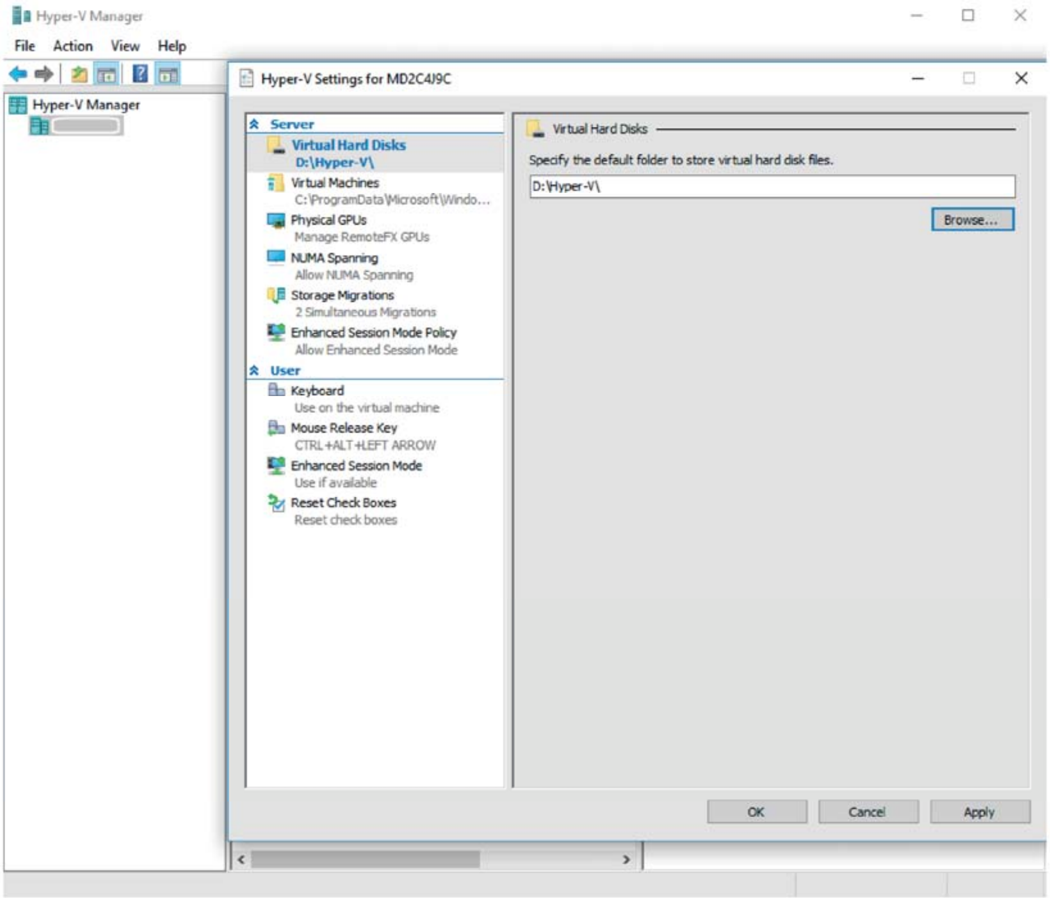


Name	State	CPU Usage	Assig
DockerDesktopVM	Off		

The selected virtual machine has no checkp

Created: 2/12/2020 11:07:57 AM
Configuration Version: 8.3
Generation: 2
Notes: None

- Click **Hyper-V Settings**, and a new window "**Hyper-V Settings**" will pop up. Check if the folder of **Virtual Hard Disks** is pointing to a specified folder on **drive C**: (for instance, C:Hyper-V), where SITRANS serve IQ will be or is installed, and click **OK.**



Hyper-V Settings for MD2C4J9C

Server

Virtual Hard Disks
D:\Hyper-V\

Virtual Machines
C:\ProgramData\Microsoft\Windo...

Physical GPUs
Manage RemoteFX GPUs

NUMA Spanning
Allow NUMA Spanning

Storage Migrations
2 Simultaneous Migrations

Enhanced Session Mode Policy
Allow Enhanced Session Mode

User

Keyboard
Use on the virtual machine

Mouse Release Key
CTRL+ALT+LEFT ARROW

Enhanced Session Mode
Use if available

Reset Check Boxes
Reset check boxes

Virtual Hard Disks

Specify the default folder to store virtual hard disk files.

D:\Hyper-V\

Installation of software including SITRANS serve IQ

3

3.1 Accessing the installer software

SITRANS serve IQ is available in two forms: on a USB stick or as OSD (Online software delivery).

- USB delivery: Connect the USB stick containing the SITRANS serve IQ installation package and licenses to the PC.
- OSD: Follow the instruction as received by email and download the media folder containing installation package from the website. You might do this with another pc and transfer the downloads to the IPC with a USB stick.

3.2 Starting the Installation

Note

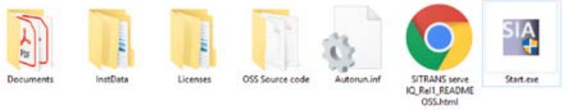
Ensure you have Internet access during SITRANS serve IQ installation.

The Installer will install the software on the IPC. Among other, the following software will be installed:

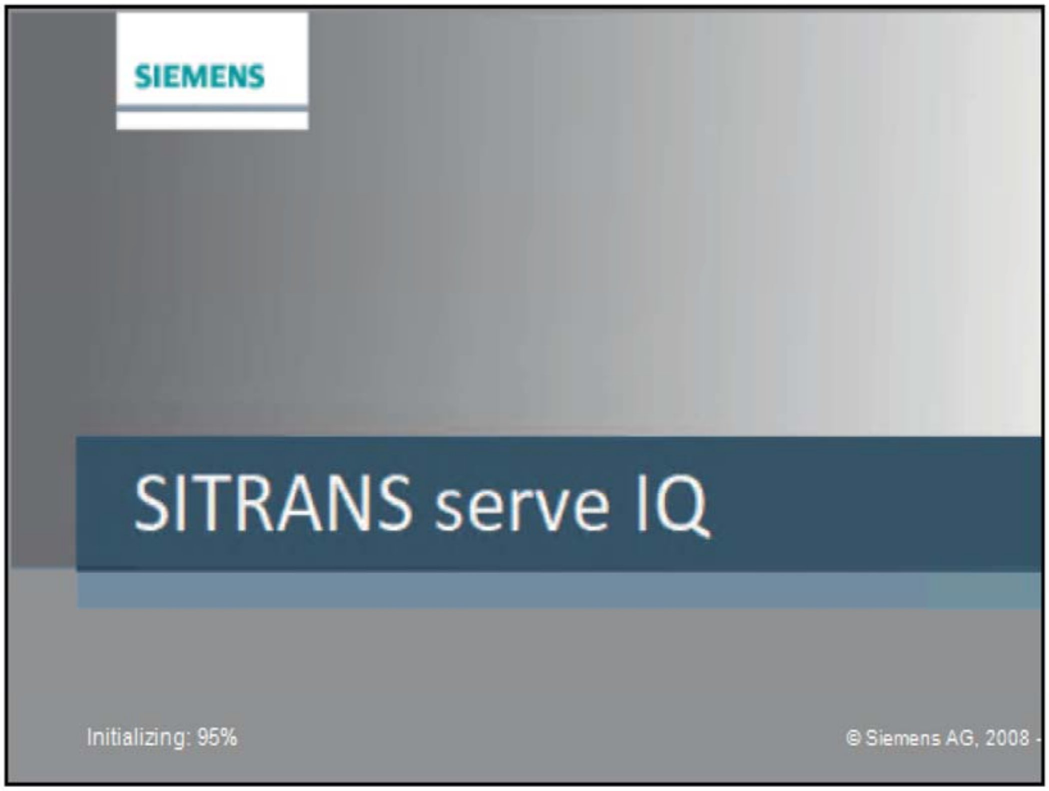
- SITRANS serve IQ
- Keycloak
- Siemens Automation License Manager
- Docker (dedicated version, which was system tested with SITRANS serve IQ)

You can install the SITRANS serve IQ application by executing the following steps:

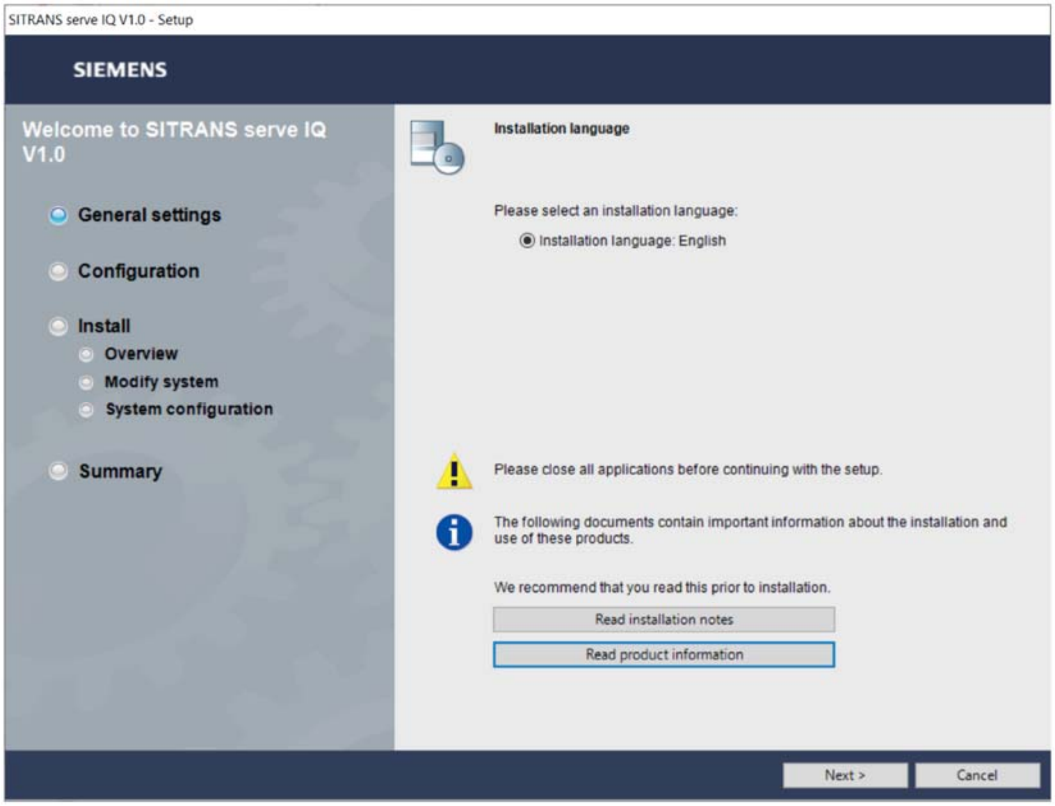
- From the installation media, search for the ‘Start.exe’. (depending on the version, you might have to navigate to SEBU-SITRANS-serve-IQ.)
- Right-click the Start.exe and select Run as Administrator to launch the installer.



- The installation wizard's Welcome screen appears.



- On the General settings screen:



SITRANS serve IQ V1.0 - Setup

Installation language

Please select an installation language:

● Installation language: English

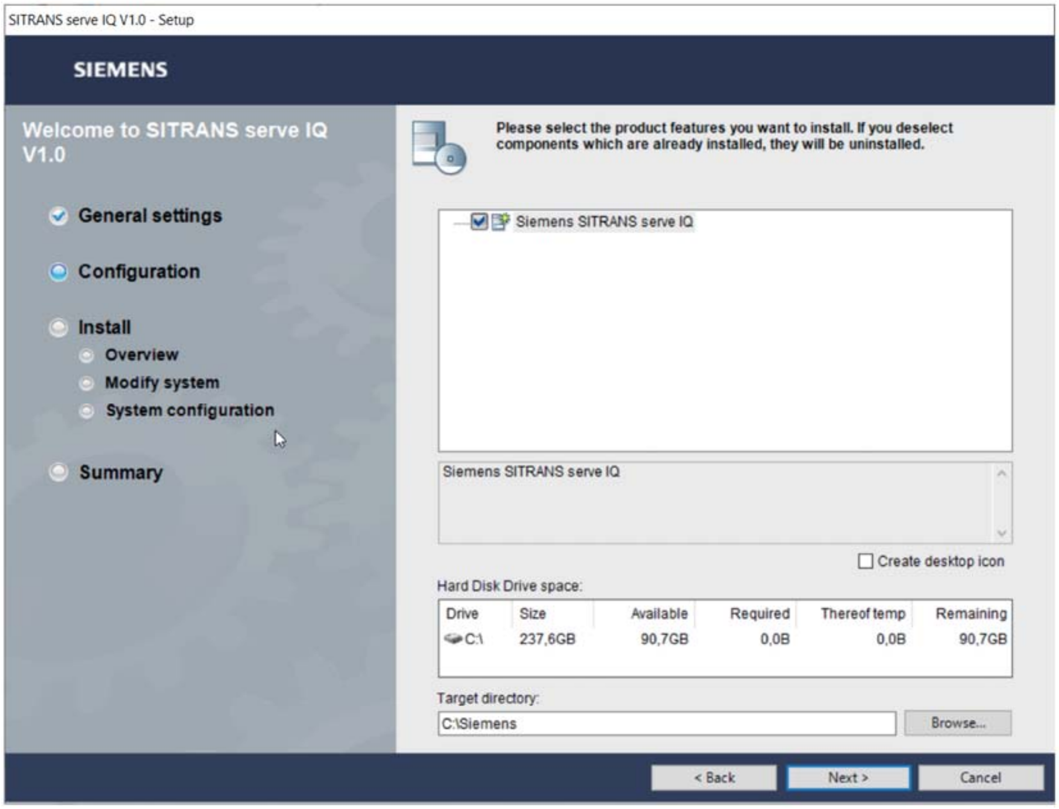
Please close all applications before continuing with the setup.

The following documents contain important information about the installation and use of these products.

We recommend that you read this prior to installation.

- Select Installation language: English. Click Next.

- On the Configuration screen:



Please select the product features you want to install. If you deselect components which are already installed, they will be uninstalled.

☑ Siemens SITRANS serve IQ

Siemens SITRANS serve IQ

□ Create desktop icon

Hard Disk Drive space:

Drive	Size	Available	Required	Thereof temp	Remaining
C:\	237,6GB	90,7GB	0,0B	0,0B	90,7GB

Target directory:

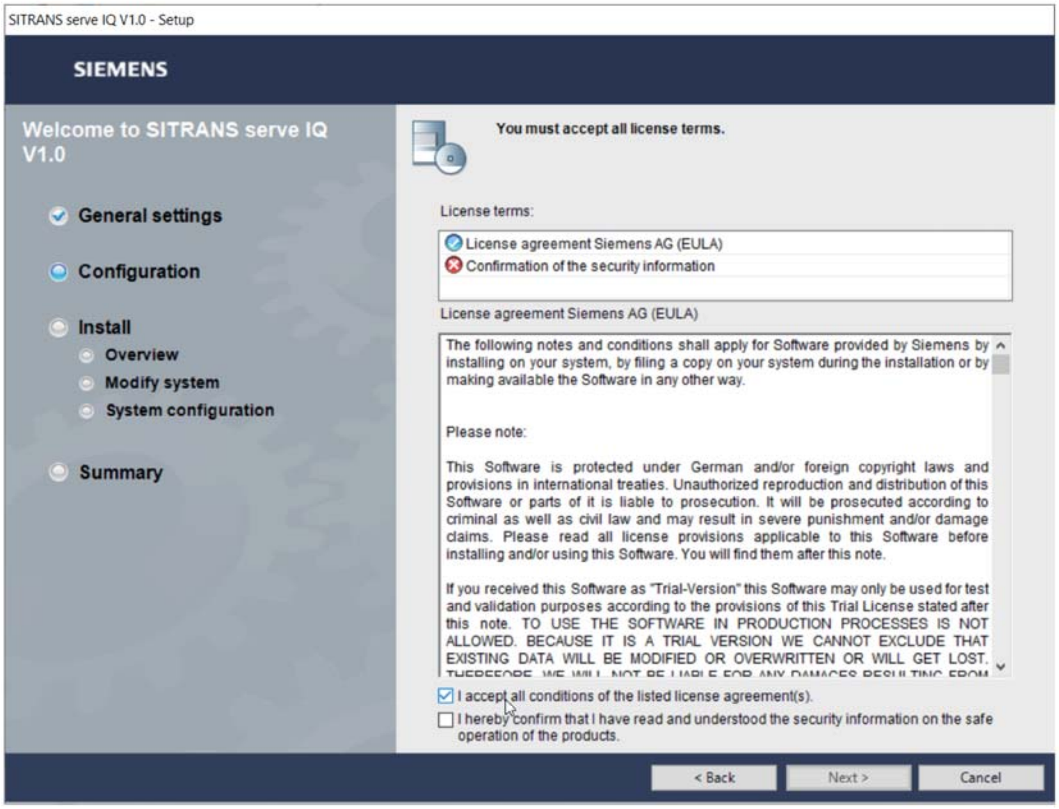
C:\Siemens

- Select Siemens SITRANS serve IQ.
- Ensure that the target directory is C (see picture above) and click Next.

Note

SITRANS serve IQ should be installed on the same drive as Hyper-V Virtual Hard Disks.

Read the license terms. Select I accept all conditions of the listed license agreement(s) and I hereby confirm that I have read and understand the security information on the safe operation of the products. Then click Next.



You must accept all license terms.

License terms:

✓ License agreement Siemens AG (EULA)

☒ Confirmation of the security information

License agreement Siemens AG (EULA)

The following notes and conditions shall apply for Software provided by Siemens by installing on your system, by filing a copy on your system during the installation or by making available the Software in any other way.

Please note:

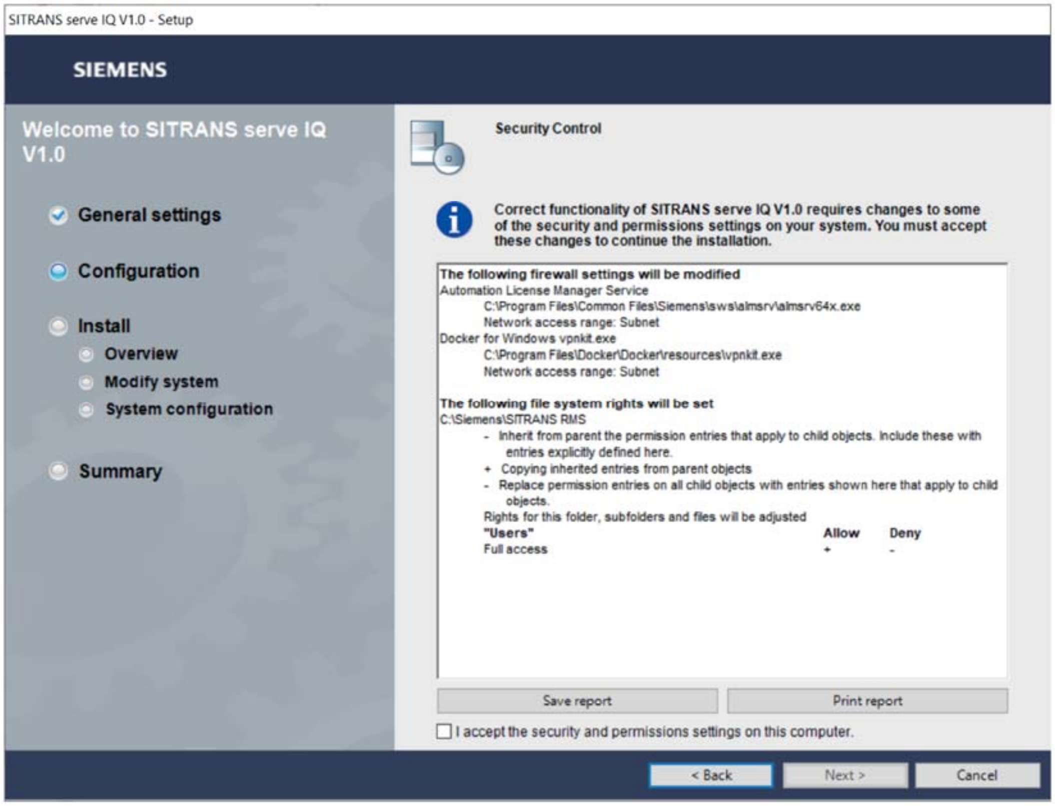
This Software is protected under German and/or foreign copyright laws and provisions in international treaties. Unauthorized reproduction and distribution of this Software or parts of it is liable to prosecution. It will be prosecuted according to criminal as well as civil law and may result in severe punishment and/or damage claims. Please read all license provisions applicable to this Software before installing and/or using this Software. You will find them after this note.

If you received this Software as "Trial-Version" this Software may only be used for test and validation purposes according to the provisions of this Trial License stated after this note. TO USE THE SOFTWARE IN PRODUCTION PROCESSES IS NOT ALLOWED. BECAUSE IT IS A TRIAL VERSION WE CANNOT EXCLUDE THAT EXISTING DATA WILL BE MODIFIED OR OVERWRITTEN OR WILL GET LOST. THEREFORE WE WILL NOT BE LIABLE FOR ANY DAMAGES RESULTING FROM

☑ I accept all conditions of the listed license agreement(s).

□ I hereby confirm that I have read and understood the security information on the safe operation of the products.

Read the terms and then select I accept the security and permissions settings on this computer.



Security Control

Correct functionality of SITRANS serve IQ V1.0 requires changes to some of the security and permissions settings on your system. You must accept these changes to continue the installation.

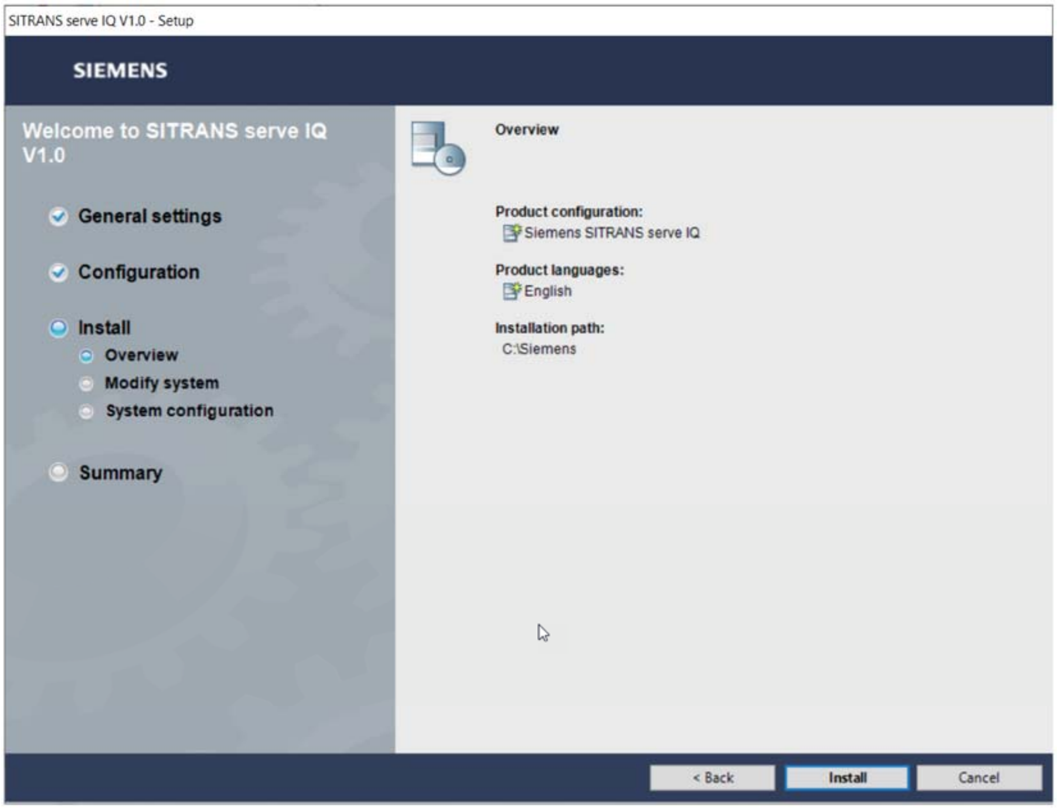
```
The following firewall settings will be modified
Automation License Manager Service
        C:\Program Files\Common Files\Siemens\sws\almsrv\almsrv64x.exe
        Network access range: Subnet
Docker for Windows vpnkit.exe
        C:\Program Files\Docker\Docker\resources\vpnkit.exe
        Network access range: Subnet

The following file system rights will be set
C:\Siemens\SITRANS RMS
        -  Inherit from parent the permission entries that apply to child objects. Include these with
             entries explicitly defined here.
        +  Copying inherited entries from parent objects
        -  Replace permission entries on all child objects with entries shown here that apply to child
             objects.
        Rights for this folder, subfolders and files will be adjusted
        "Users"                                                   Allow      Deny
        Full access                                               +          -
```

□ I accept the security and permissions settings on this computer.

- Optionally, select Save Report or Print Report to save or print the security report respectively.
- Click Next.

- On the Overview screen, verify the installation settings and click Install to begin the installation.

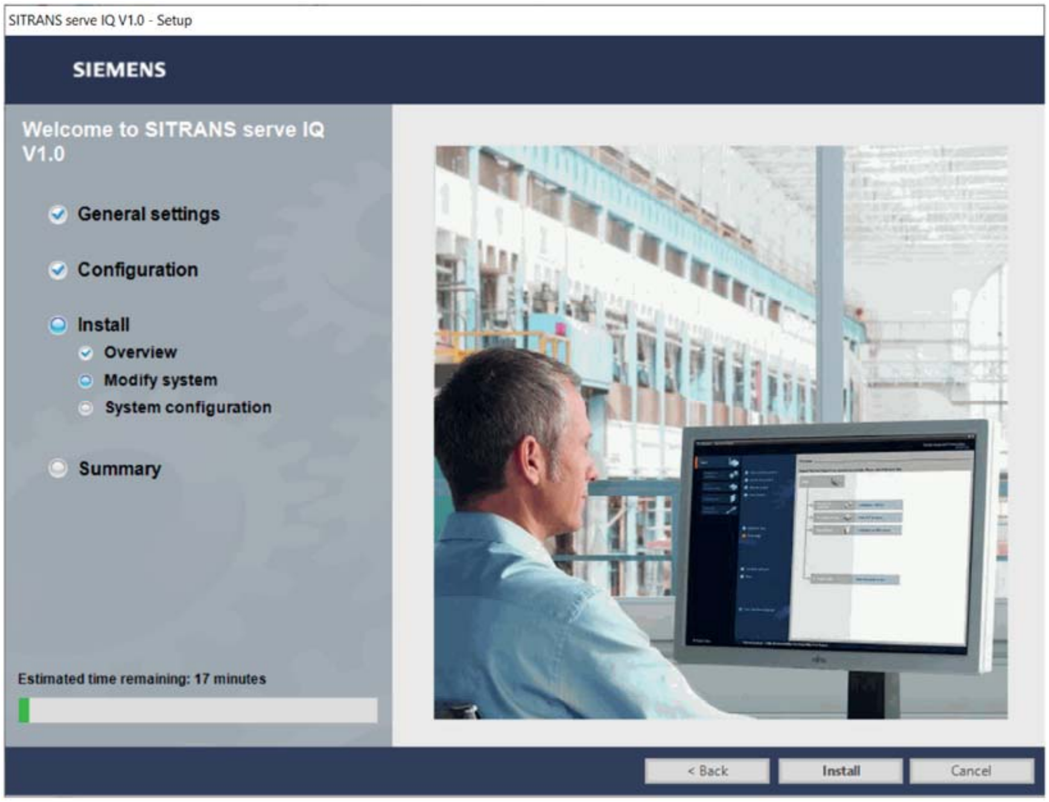


Product configuration:
Siemens SITRANS serve IQ

Product languages:
English

Installation path:
C:\Siemens

- The installation begins and progress is shown.



Estimated time remaining: 17 minutes

Note

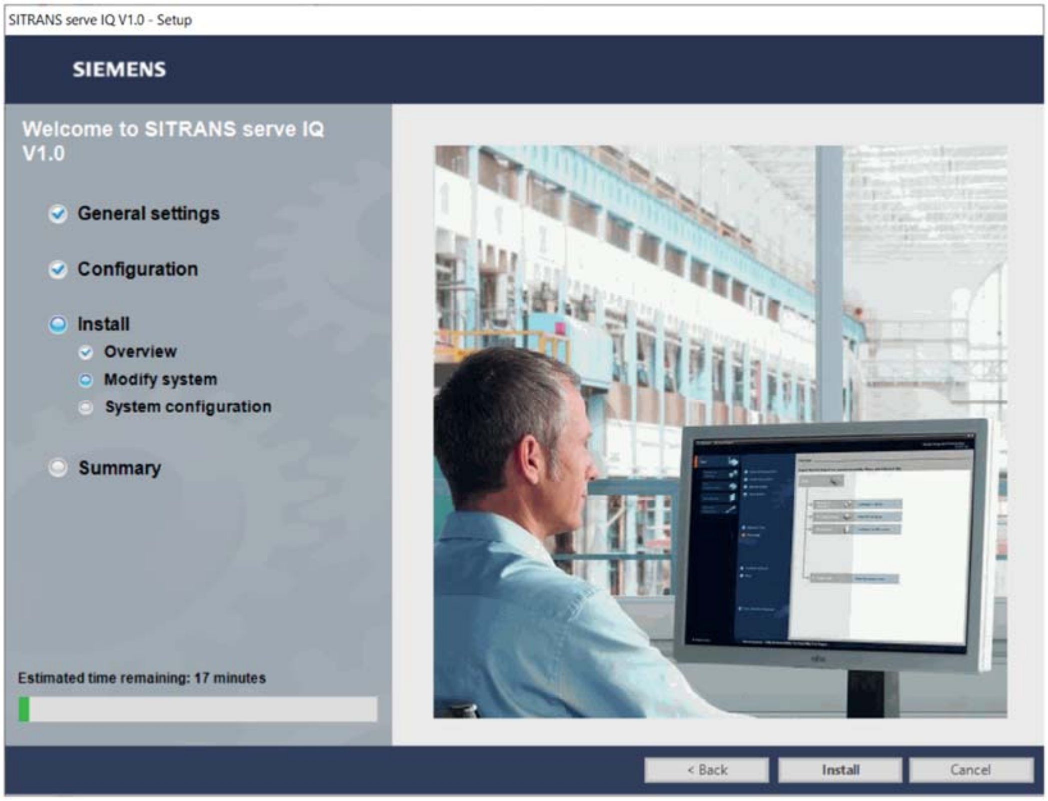
A Docker engine version will be installed with SITRANS serve IQ package. If you see a pop-up window ‘A new version of Docker is available’, select Skip this version. **Do not update to newer versions of Docker.**

Though we are continuously testing the newest available software versions and are providing these with the installation, there might be a time delay until we have performed all tests.

Please check on the Siemens Industry Online Support (SIOS) for newest Information (FAQ): https://www.siemens.com/SIOS/sitransserveiq (https://www.siemens.com/SIOS/sitransserveiq)

- Reboot the computer to resume the installation.

- The installation will resume automatically after reboot. Press any key to continue will pop up twice to resume the setup.

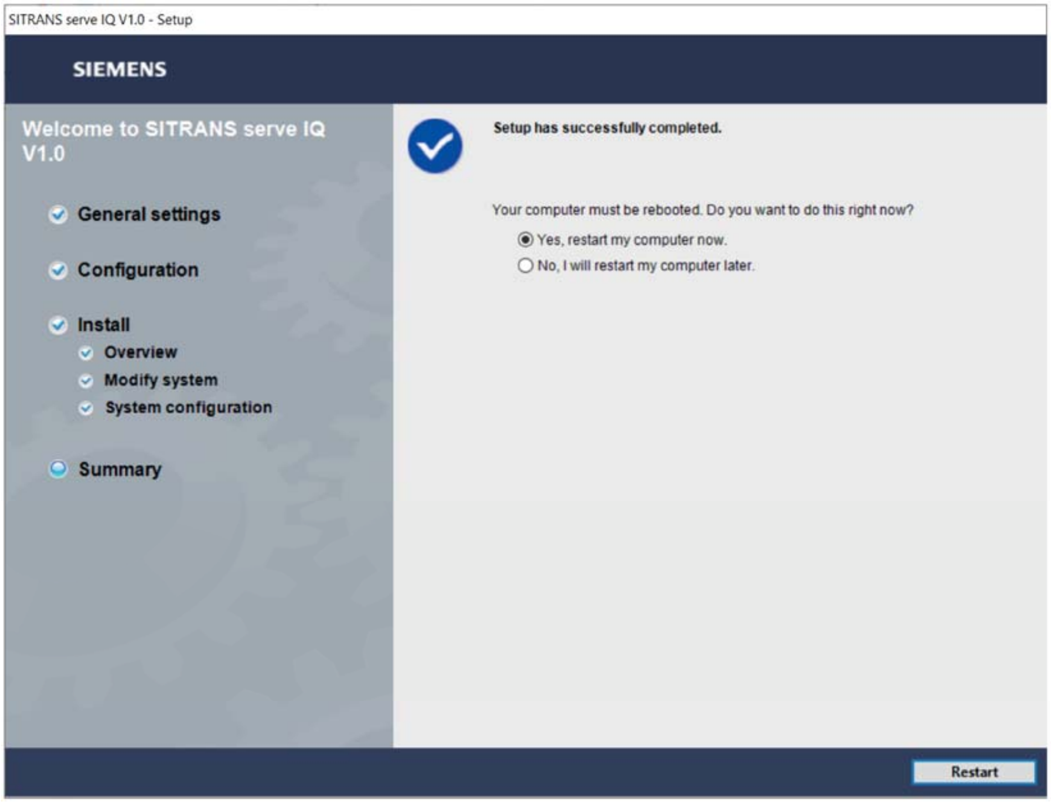


SITRANS serve IQ V1.0 - Setup

Welcome to SITRANS serve IQ V1.0

Estimated time remaining: 17 minutes

- On the Summary screen:



SITRANS serve IQ V1.0 - Setup

SIEMENS

Welcome to SITRANS serve IQ V1.0

- ✓ General settings
- ✓ Configuration
- ✓ Install
  - ✓ Overview
  - ✓ Modify system
  - ✓ System configuration
- ● Summary

Setup has successfully completed.

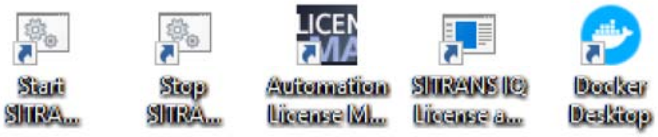
Your computer must be rebooted. Do you want to do this right now?

● Yes, restart my computer now.
○ No, I will restart my computer later.

The 2nd reboot is required after the setup is completed. Click Restart to reboot the computer.

On successful installation, five icons will appear on the desktop of the computer:

- Start SITRANS serve IQ,
- Stop SITRANS serve IQ,
- Automation License Manager (ALM)
- SITRANS IQ License activation
- Docker Desktop.



Note

Additional software is installed but has no separate icons (e.g. Keycloak)

3.3 Docker

Docker is the mandatory environment, in which the SITRANS serve IQ application is running.

Note

The actual screens might differ slightly. Please enter the information accordingly.

⚠ CAUTION

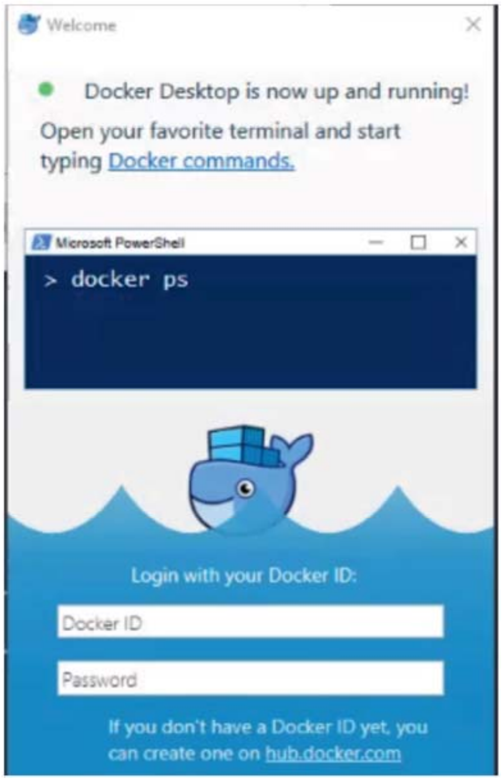
Attention: Do not update docker to a newer version.

Docker will ask you to upgrade to newer versions. These might differ in functionality and might require continuous updates to be activated. Therefore, do not update, but continue to use Docker with the software version as provided with the installation of SITRANS serve IQ.

3.3.1 Start docker application

Docker application must be started before running SITRANS serve IQ. To start the Docker application manually if it doesn't run automatically

- Double-click Docker desktop icon on the desktop to launch Docker. The startup of Docker desktop may take about 2-3 minutes, depending on the computer's performance. A message Docker Desktop is running will pop up to indicate docker is ready



● Docker Desktop is now up and running!

Open your favorite terminal and start typing Docker commands.

```
> docker ps
```

Login with your Docker ID:

If you don't have a Docker ID yet, you can create one on hub.docker.com

- A log-in with a Docker ID is not required. Please **ignore** the dialog box "Login with your Docker ID".
- For information (not required for installation): Typing "docker ps -a" in the command will list all active docker containers (ps = "process status")

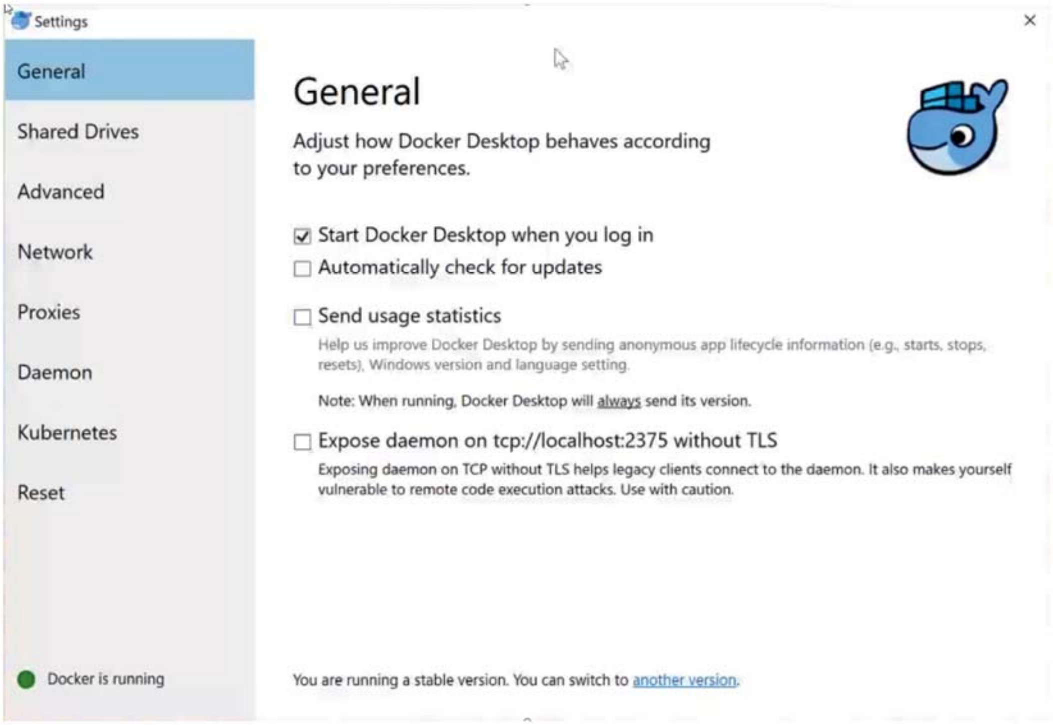
Note

A message may appear asking the user to manually enable the shared drive (in case it was not configured yet). Refer to Configure Docker Shared Drives (Page 28).

3.3.2 Configuration of docker

To configure the Docker:

- Navigate to the system tray, right-click the Docker icon and select Settings.
- On the Settings screen, select General. It is recommended to
  - turn on: Start Docker Desktop when you log in,
  - turn off: Automatically check for updates and Send usage statistics.



Settings

General

Adjust how Docker Desktop behaves according to your preferences.

☑ Start Docker Desktop when you log in

□ Automatically check for updates

□ Send usage statistics

Help us improve Docker Desktop by sending anonymous app lifecycle information (e.g., starts, stops, resets), Windows version and language setting.

Note: When running, Docker Desktop will always send its version.

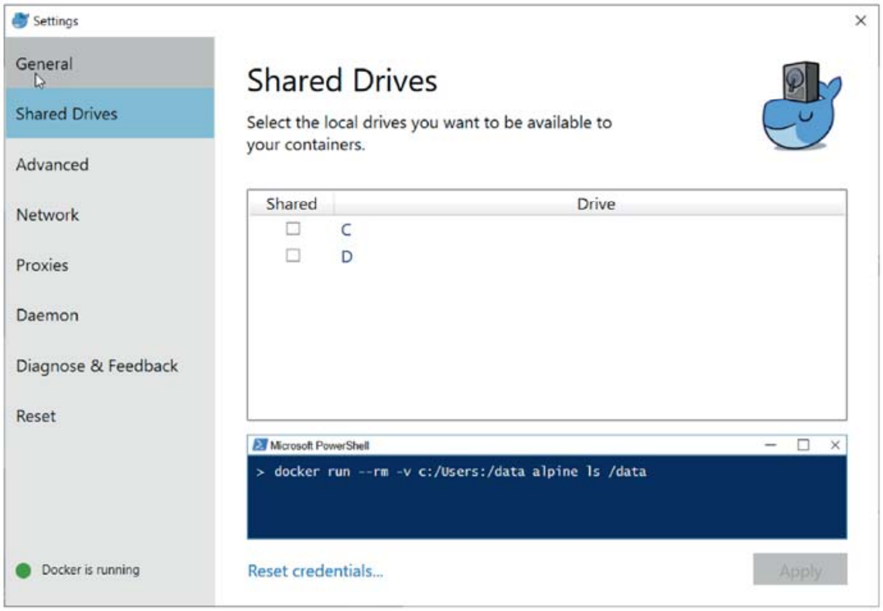
□ Expose daemon on tcp://localhost:2375 without TLS

Exposing daemon on TCP without TLS helps legacy clients connect to the daemon. It also makes yourself vulnerable to remote code execution attacks. Use with caution.

Docker is running

You are running a stable version. You can switch to another version.

- Select Shared Drives.
  Ensure that the same drive is selected correctly as above:
  - drive C is shared when SITRANS serve IQ is installed on drive C.



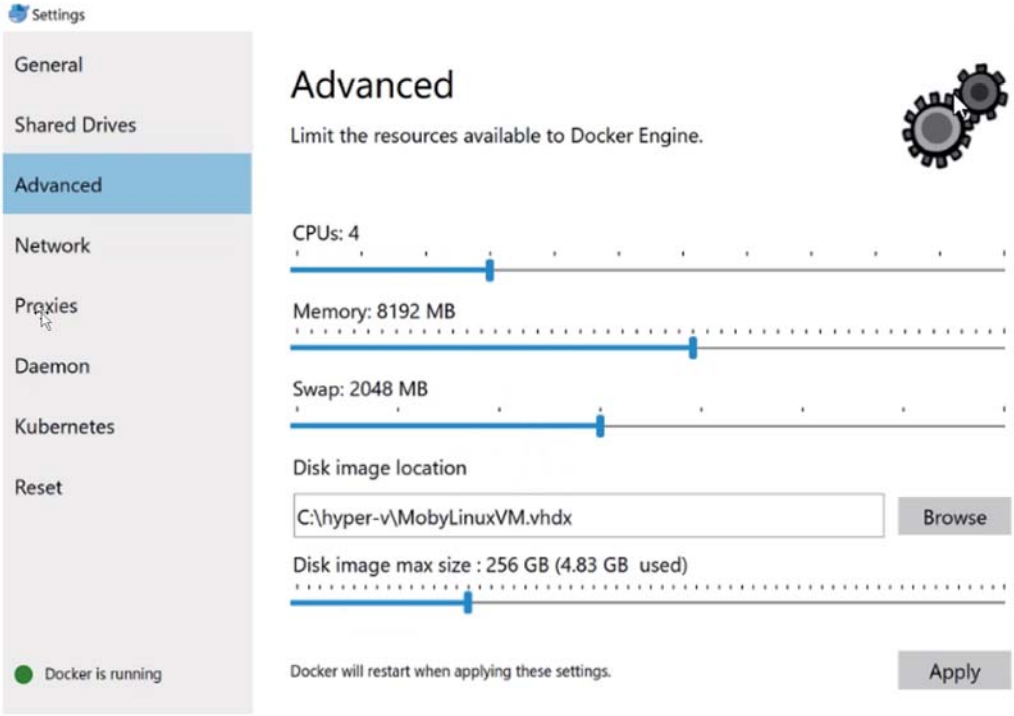
Shared Drives

Select the local drives you want to be available to your containers.

Shared	Drive
□	C
□	D

```
> docker run --rm -v c:/Users:/data alpine ls /data
```

- On the window "Docker needs to access your computer’s filesystem", login as Administrator with your Windows credentials and click Ok.
- On the **Advanced** screen, configure the **CPU**, **Memory**, **Swap**, **Disk image size**, and **Disk image location** values and then click **Apply**.



Advanced

Limit the resources available to Docker Engine.

CPUs: 4

Memory: 8192 MB

Swap: 2048 MB

Disk image location

C:\hyper-v\MobyLinuxVM.vhdx

Disk image max size : 256 GB (4.83 GB used)

Docker will restart when applying these settings.

The recommended values are shown below:

Parameter	Recommended minimum values
CPU	**Use all available CPU's**
Memory	16 GB (or min 8 GB)
Swap	2 GB of SWAP memory
Disk image size	At least 64 GB
Hard disk	250 GB up to 450 GB, **reserve** 5 to 10% of **disc capacity**

Note

IMPORTANT

Do not commit the entire available disc space but leave ca. 5-10% free disc capacity. There have been observations, that if the entire disc space has been committed and was entirely used up, archiving of data is a challenge.
With free disc capacity available, you could increase the reserved hard disk and perform the data archive. In case of questions, please raise a support request on SIOS https://www.siemens.com/SIOS/sitransserveiq (https://www.siemens.com/SIOS/sitransserveiq)

- Close the Settings window.

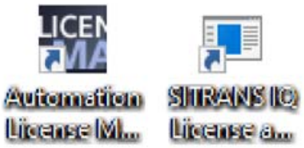
3.4 Installing licenses

The license keys are delivered with the SITRANS serve IQ installation package, either on an USB stick or online software delivery (OSD). The license keys can be transferred from the USB stick to the computer by drag-and-drop by using the Siemens Automation License Manager ALM. The license keys can also be installed via Web License Key Download in ALM.

Note

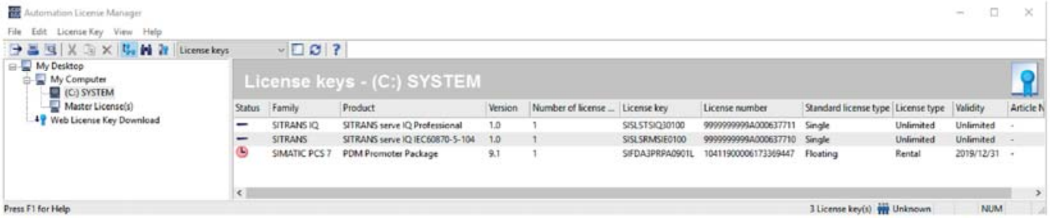
Licenses are hidden files and can only be identified and moved with the Siemens ALM.

Start ALM first and in a second step run the 'SITRANS License activation'



Add or move the required licenses to the drive where SITRANS serve IQ is installed.

- For the software SITRANS serve IQ itself
- For (additional) measurements to be added to SITRANS serve IQ
- For IEC Communication (if not included with the SITRANS serve IQ license)



License keys - (C:) SYSTEM

Status	Family	Product	Version	Number of license ...	License key	License number	Standard license type	License type	Validity	Article N
—	SITRANS IQ	SITRANS serve IQ Professional	1.0	1	SISLSTSIQ30100	9999999999A000637711	Single	Unlimited	Unlimited	-
—	SITRANS	SITRANS serve IQ IEC60870-5-104	1.0	1	SISLSRMSIE0100	9999999999A000637710	Single	Unlimited	Unlimited	-
◷	SIMATIC PCS 7	PDM Promoter Package	9.1	1	SIFDA3PRPA0901L	10411900006173369447	Floating	Rental	2019/12/31	-

Figure 3-1 View on Siemens ALM with multiple licenses

Also use ALM to verify, which licenses are currently allocated to your system (the drive which has been shared with docker).

For further details, please consult the SIMATIC Automation License Manager Programming and Operating Manual on Siemens Industry online Support https://support.industry.siemens.com/cs/start?lc=en-WW (https://support.industry.siemens.com/cs/start?lc=en-WW)

Note

Each sending unit is consuming one measurement license.

A sending unit could be either one (1) MAG 8000 3G/4G or one (1) RTU 30xxc. Even if there are multiple devices connected to a RTU, it still is counted as one sending unit. The same applies to a MAG 8000 3G/4G, that has a pressure transmitter connected to it - it still is counted as one sending unit.

Configuration of firewall/router settings 4

4.1 Introduction: firewall/router settings

Siemens recommends checking with your company's IT-governance and IT security regulations with your IT department.

Ensure that you consider any upcoming IT - threats as they become known

It is strongly recommended that you install and maintain firewalls

1. between the internet and the IPC
2. from the IPC to your SCADA system (in case you are using the IEC interface)

We recommend keeping the IPC separated from your OT-network to minimize any risk of intrusion.

This section describes the minimal settings to start using SITRANS serve IQ and gives an outlook on advanced secure approaches.

For further support, please follow the general publications and consult https://www.siemens.com/SIOS/sitransserveiq (https://www.siemens.com/SIOS/sitransserveiq)

4.2 Basic network and firewall configuration

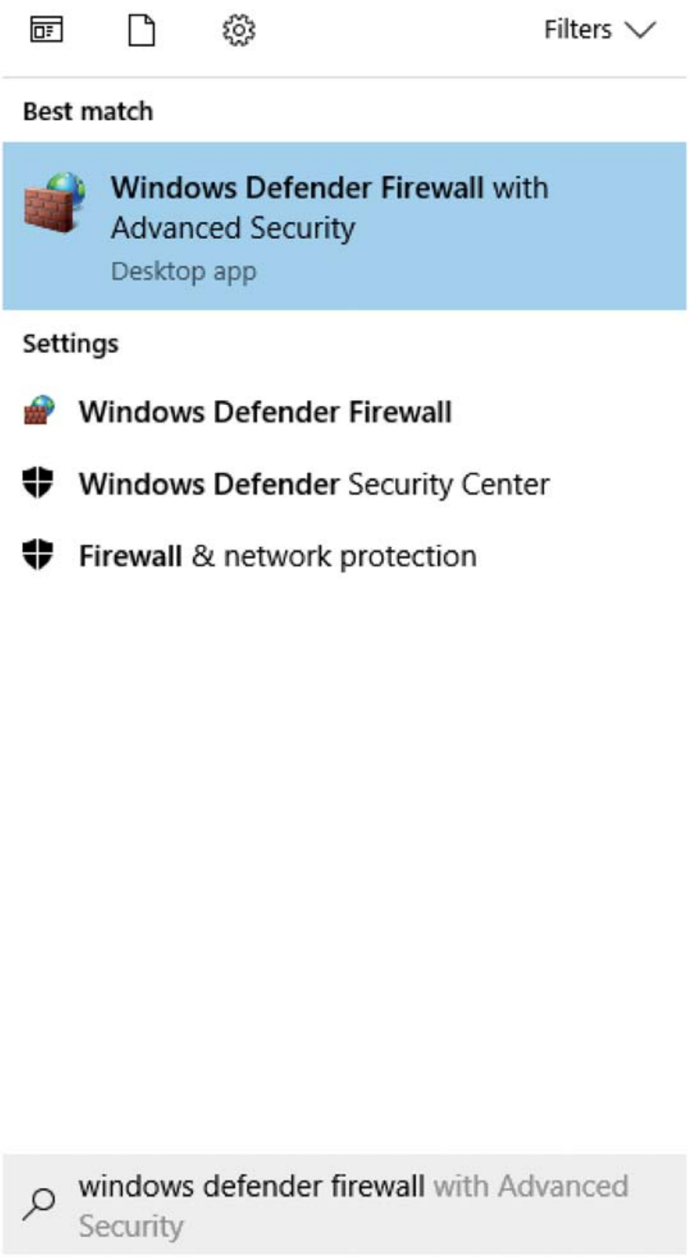
Basic configuration

In this configuration, you enable SITRANS serve IQ to access

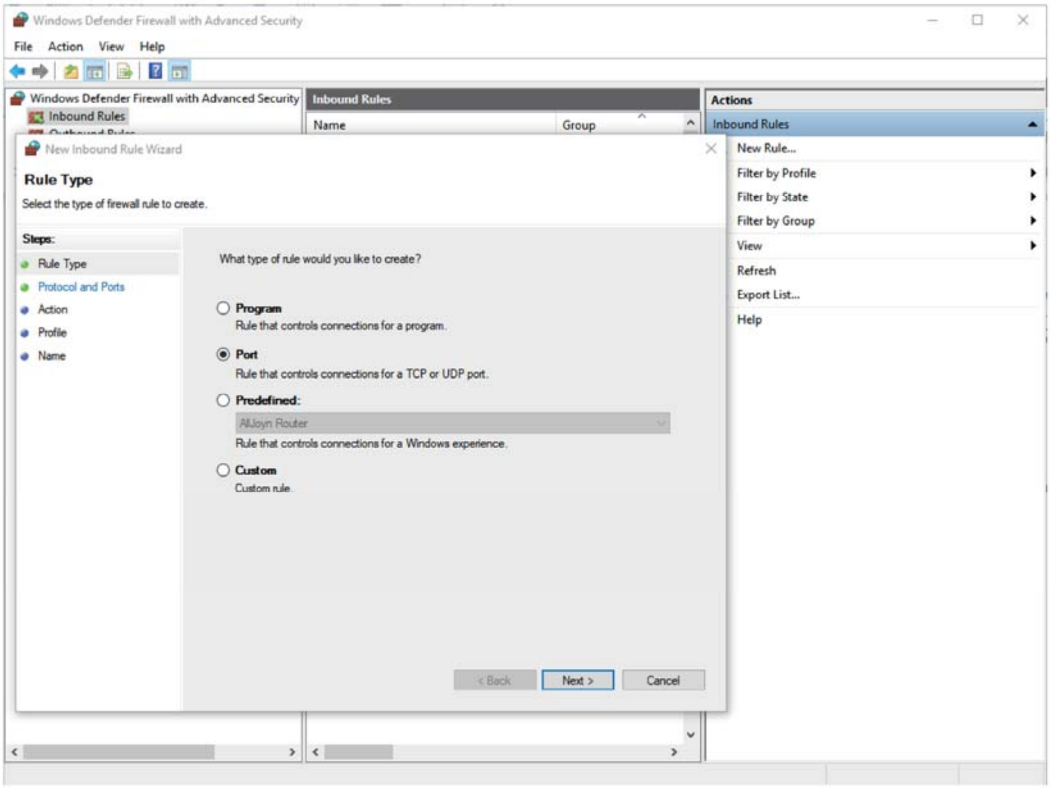
- the email server with IMAP protocol
- the Open-street-Map server

To configure Windows Defender firewall for SITRANS serve IQ to access the email server:

1. Click the Start icon and type Windows Defender firewall with Advanced Security. Click Windows Defender firewall with Advanced Security from the results to launch the console.


Filters
Best match
Windows Defender Firewall with Advanced Security
Desktop app
Settings
Windows Defender Firewall
Windows Defender Security Center
Firewall & network protection
windows defender firewall with Advanced Security

2. Right-click **Inbound Rules** and select **New Rule.**



Rule Type

Select the type of firewall rule to create.

What type of rule would you like to create?

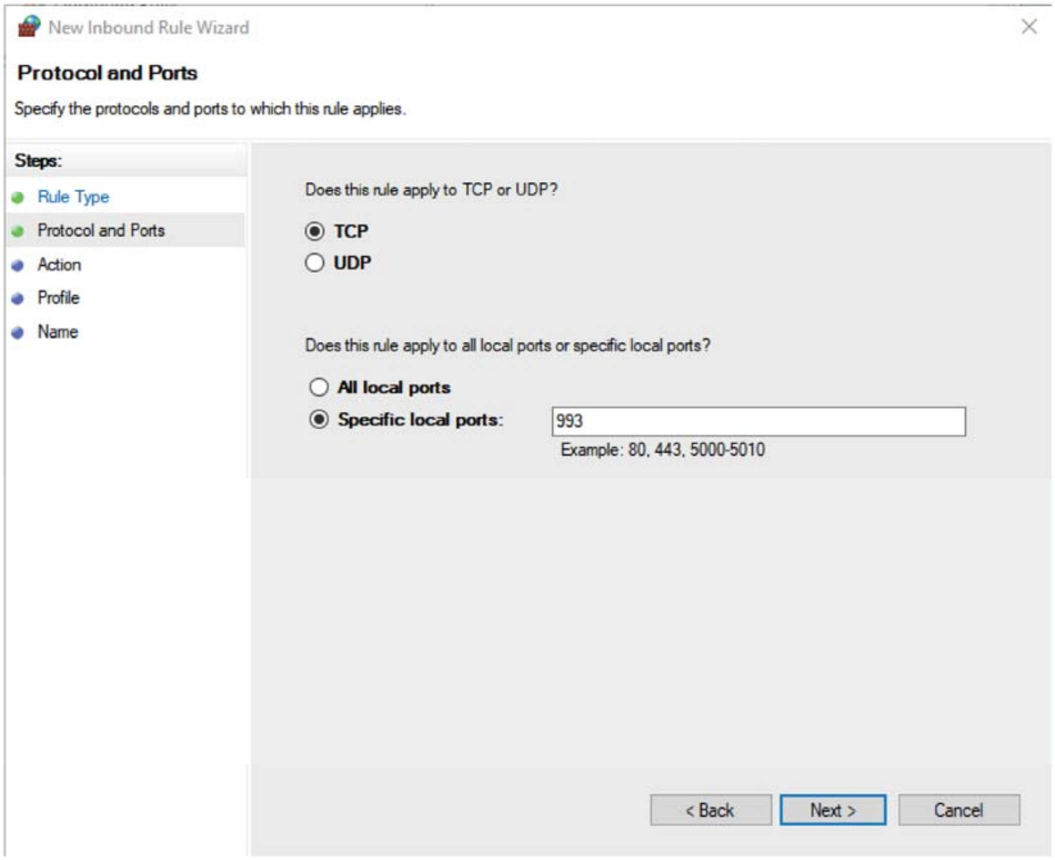
○ Program
Rule that controls connections for a program.

● Port
Rule that controls connections for a TCP or UDP port.

○ Predefined:
AllJoyn Router
Rule that controls connections for a Windows experience.

○ Custom
Custom rule.

3. On the New Inbound Rule Wizard screen, perform the following steps:
   - Under Rule Type, select Port and click Next.
   - Under Protocols and Ports, select TCP protocol and Specific local ports and type 993 in the input box. Click Next.



New Inbound Rule Wizard

Protocol and Ports

Specify the protocols and ports to which this rule applies.

Steps:
- Rule Type
- Protocol and Ports
- Action
- Profile
- Name

Does this rule apply to TCP or UDP?

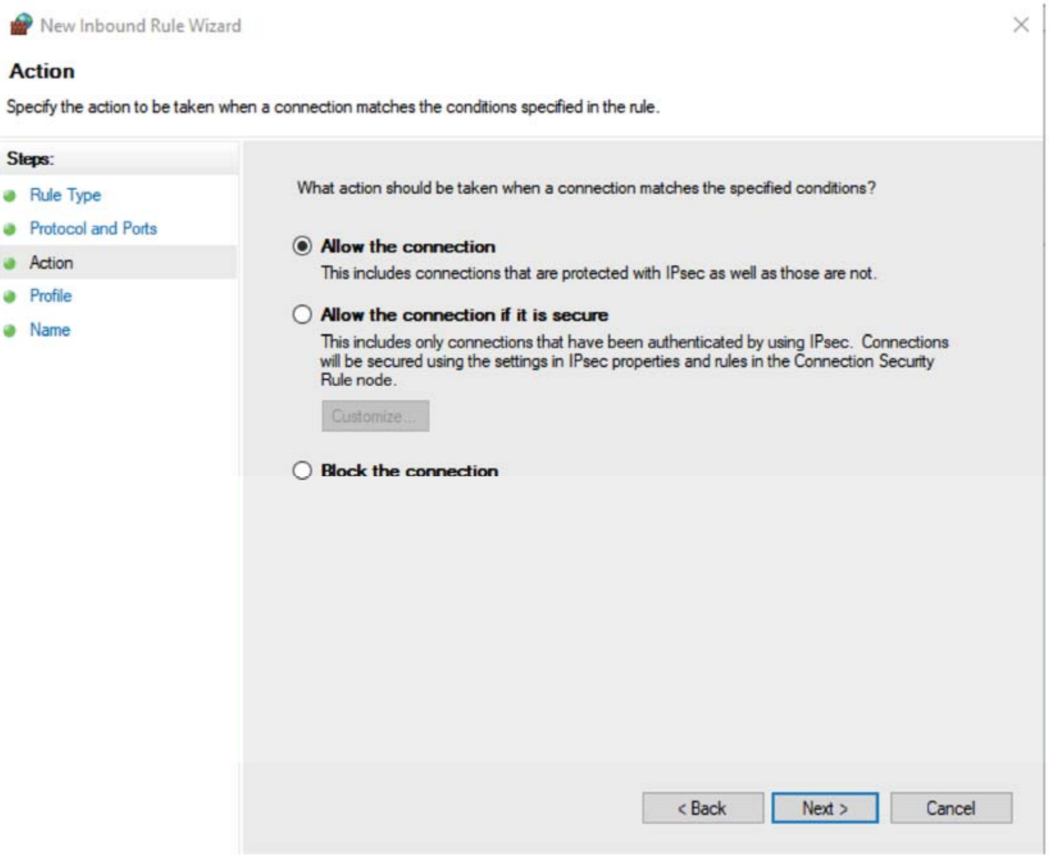
● TCP
○ UDP

Does this rule apply to all local ports or specific local ports?

○ All local ports
● Specific local ports: 993

Example: 80, 443, 5000-5010

– Under Action, select Allow the Connection and click Next.



New Inbound Rule Wizard

Action

Specify the action to be taken when a connection matches the conditions specified in the rule.

Steps:
- Rule Type
- Protocol and Ports
- Action
- Profile
- Name

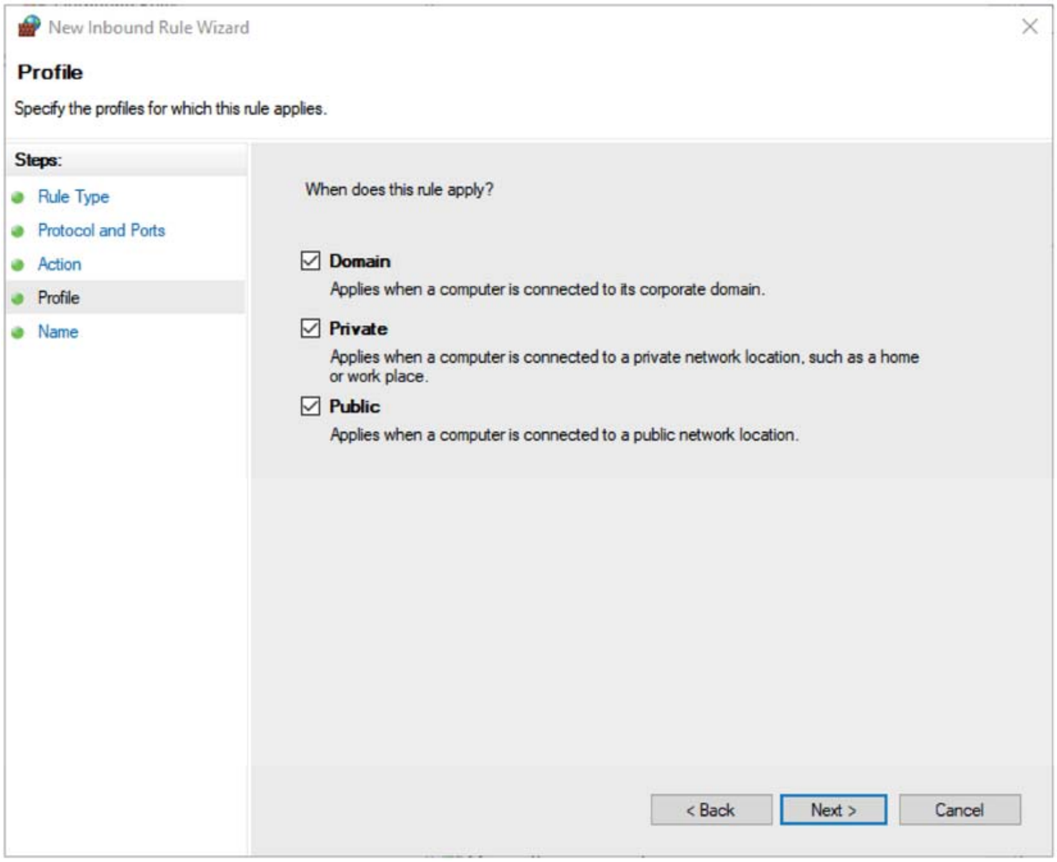
What action should be taken when a connection matches the specified conditions?

● **Allow the connection**
This includes connections that are protected with IPsec as well as those are not.

○ **Allow the connection if it is secure**
This includes only connections that have been authenticated by using IPsec. Connections will be secured using the settings in IPsec properties and rules in the Connection Security Rule node.

○ **Block the connection**

– Under Profile, ensure all the options are selected and click Next.



Profile

Specify the profiles for which this rule applies.

When does this rule apply?

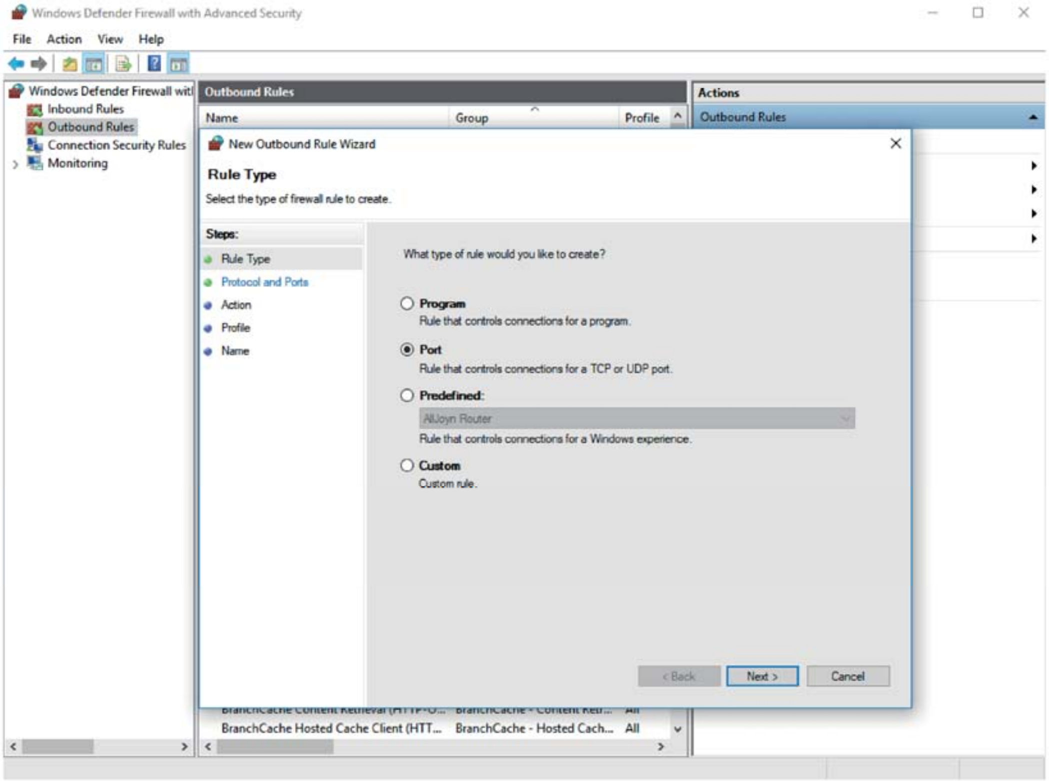
☑ **Domain**
Applies when a computer is connected to its corporate domain.

☑ **Private**
Applies when a computer is connected to a private network location, such as a home or work place.

☑ **Public**
Applies when a computer is connected to a public network location.

– Under Name, in the Name input box enter SITRANS IMAP Inbound Rule and click Finish.

4. Right-click **Outbound Rules** and select **New Rule**. Repeat the procedure in step 3 to create SITRANS IMAP Outbound Rule.



Windows Defender Firewall with Advanced Security
File
Action
View
Help
Windows Defender Firewall witl
Inbound Rules
Outbound Rules
Connection Security Rules
Monitoring
Outbound Rules
Name
Group
Profile
Actions
Outbound Rules
BranchCache Content Retrieval (HTTP-O...
BranchCache - Content Retr...
All
BranchCache Hosted Cache Client (HTT...
BranchCache - Hosted Cach...
All
New Outbound Rule Wizard
Steps:
Rule Type
Protocol and Ports
Action
Profile
Name
< Back
Next >
Cancel

Rule Type

Select the type of firewall rule to create.

What type of rule would you like to create?

○ **Program**
Rule that controls connections for a program.

● **Port**
Rule that controls connections for a TCP or UDP port.

○ **Predefined:**
AllJoyn Router
Rule that controls connections for a Windows experience.

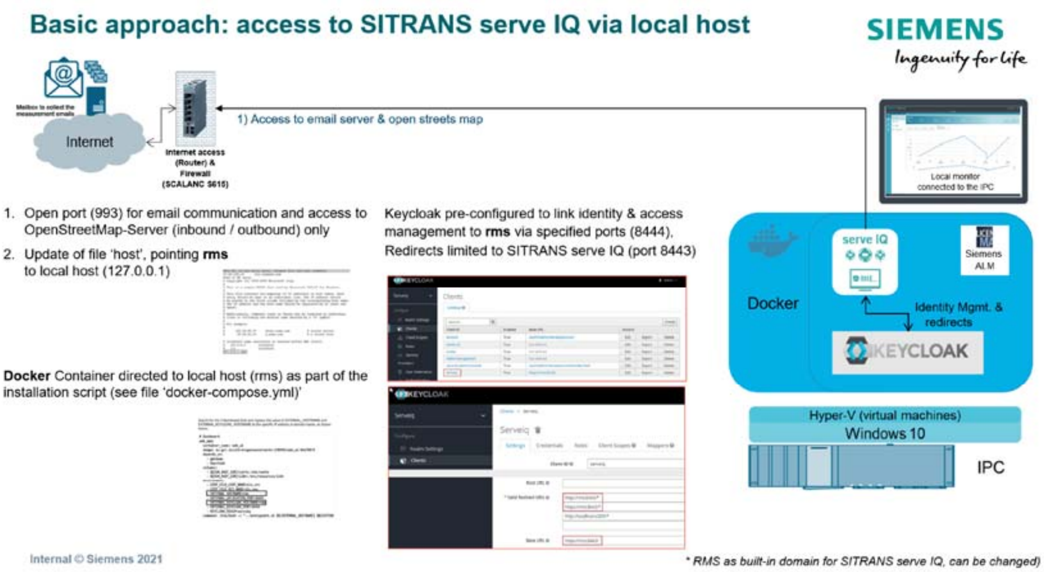
○ **Custom**
Custom rule.

4.3 Local access to SITRANS serve IQ

We recommend running SITRANS serve IQ first without remote access from the internet. This section describes the configuration to access, as a user, SITRANS serve IQ on the IPC itself.

Note

SITRANS serve IQ (SsIQ) is an web-application, which runs on the IPC. To access SsIQ, using a browser (Google Chrome), you need to edit the host file of your IPC.



Basic approach: access to SITRANS serve IQ via local host

1. Open port (993) for email communication and access to OpenStreetMap-Server (inbound / outbound) only
2. Update of file 'host', pointing **rms** to local host (127.0.0.1)

Docker Container directed to local host (rms) as part of the installation script (see file 'docker-compose.yml)'

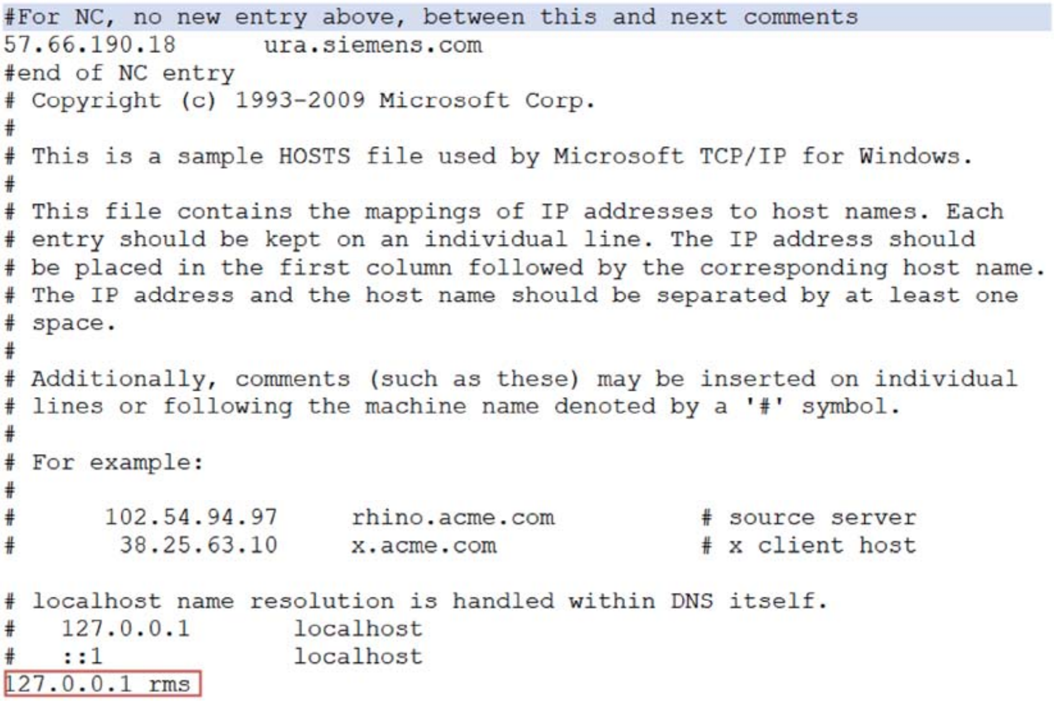
Keycloak pre-configured to link identity & access management to **rms** via specified ports (8444), Redirects limited to SITRANS serve IQ (port 8443)

SIEMENS
Ingenuity for life
Mailbox to collect the measurement emails
Internet
Internet access (Router) & Firewall (SCALANC S615)
1) Access to email server & open streets map
Local monitor connected to the IPC
serve IQ
Siemens ALM
Docker
Identity Mgmt. & redirects
KEYCLOAK
Hyper-V (virtual machines)
Windows 10
IPC
Internal © Siemens 2021
* RMS as built-in domain for SITRANS serve IQ, can be changed)

Figure 4-1 Local access to SITRANS serve IQ

To access SITRANS serve IQ, edit the hosts file on your windows computer as following:

- Click the Start button and type Notepad. Then Notepad Desktop App will be shown as best match.
- Right-click Notepad App and click Run as an Administrator (running as an Administrator is mandatory).
- Click File->Open in Notepad, and open file 'hosts' in the folder <Drive>: Windows/System32/drivers/etc. (If you are unable to see the file 'hosts', be sure that you did search for all files '*.*' .)
- If you are running SITRANS serve IQ on the same IPC, enter the IP address of the local host: 127.0.0.1, followed by the text string 'rms'.



```
#For NC, no new entry above, between this and next comments
57.66.190.18      ura.siemens.com
#end of NC entry
# Copyright (c) 1993-2009 Microsoft Corp.
#
# This is a sample HOSTS file used by Microsoft TCP/IP for Windows.
#
# This file contains the mappings of IP addresses to host names. Each
# entry should be kept on an individual line. The IP address should
# be placed in the first column followed by the corresponding host name.
# The IP address and the host name should be separated by at least one
# space.
#
# Additionally, comments (such as these) may be inserted on individual
# lines or following the machine name denoted by a '#' symbol.
#
# For example:
#
#      102.54.94.97     rhino.acme.com          # source server
#       38.25.63.10     x.acme.com              # x client host

# localhost name resolution is handled within DNS itself.
#   127.0.0.1       localhost
#   ::1             localhost
127.0.0.1 rms
```

- Save and close the host file.

Note

It is possible to run SITRANS serve without remote access from the internet and accessing the application from your local intranet or only on the IPC itself. While enabling access to the email account and internet access for accessing StreetMap-server (see also section 4.1), you could set your firewall(s) to block all other internet traffic.

4.4 Internet access to SITRANS serve IQ

Note

The sections below are for advanced users, which requires you to be familiar with network configuration, firewalls, Docker and Keycloak. For first time users of SITRANS serve IQ, that are accessing SsIQ on the local IPC only, please continue with Starting the SITRANS serve IQ application (Page 52)**.**

If you would like to access the SITRANS serve IQ from the Internet, you need to configure your network firewall(s) Docker and Keycloak accordingly. Some guidance is described in the sections below.

Note

Due to design constraints, you either can access SITRANS serve IQ locally or via the (external) IP address. It is not possible to have access in parallel.

⚠ **CAUTION**

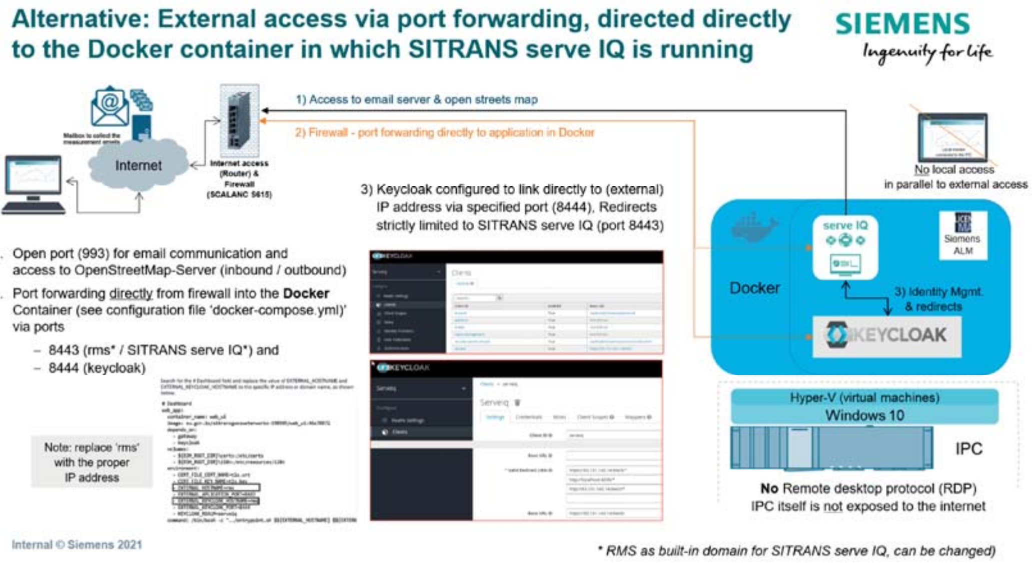
Attention

Before enabling any remote access, contact your IT department and align with your company's IT-governance and IT security regulations.

Ensure that you always consider potential threats from exposing access to SITRANS serve IQ from the internet and undertake respective measures.

4.4.1 Access with an IP-address

The Keycloak setting and the Docker setting must be revised depending on how you would like to access SITRANS serve IQ, i.e. accessing with a fixed IP address or domain name other than "rms".



Alternative: External access via port forwarding, directed directly to the Docker container in which SITRANS serve IQ is running

1. Open port (993) for email communication and access to OpenStreetMap-Server (inbound / outbound)
2. Port forwarding directly from firewall into the **Docker** Container (see configuration file 'docker-compose.yml)' via ports
   - 8443 (rms* / SITRANS serve IQ*) and
   - 8444 (keycloak)

3) Keycloak configured to link directly to (external) IP address via specified port (8444), Redirects strictly limited to SITRANS serve IQ (port 8443)

Note: replace 'rms' with the proper IP address

Internal © Siemens 2021

* RMS as built-in domain for SITRANS serve IQ, can be changed)

SIEMENS
Ingenuity for life
Mailbox to collect the measurement events
Internet
Internet access (Router) & Firewall (SCALANC S615)
1) Access to email server & open streets map
2) Firewall - port forwarding directly to application in Docker
No local access in parallel to external access
serve IQ
Siemens ALM
Docker
3) Identity Mgmt. & redirects
KEYCLOAK
Hyper-V (virtual machines)
Windows 10
IPC
No Remote desktop protocol (RDP)
IPC itself is not exposed to the internet

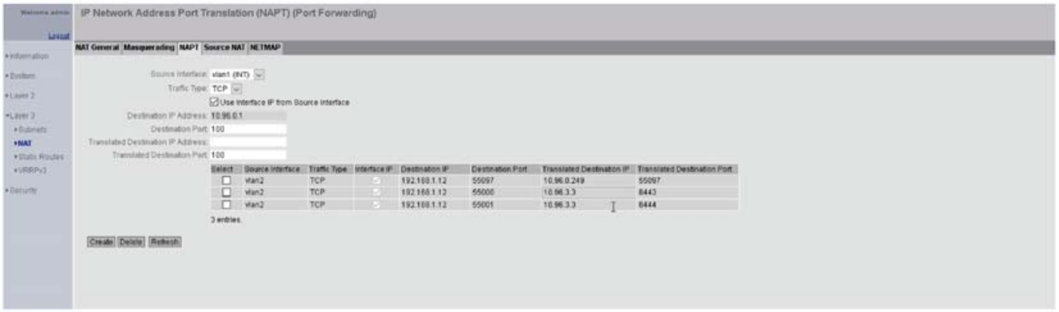
Figure 4-2 Firewall port access

4.4.1.1 Firewall settings (port forwarding)

Now SITRANS serve IQ can be remotely accessed by the specified IP address or by the specified domain name.

To be able to access SITRANS serve IQ remotely from the internet, the IPC with SITRANS serve IQ needs to be accessible from the internet. Prerequisite is, that the router that is acting as internet access point has a fixed internet protocol address and create respective rules in your router / firewall enabling port forwarding (e.g. https://83.151.142.14:8443/).

In the example above, the remote call from the internet to the external IP-address 83.151.142.14 with the port extension 8443 would then be rerouted to the IPC. This port forwarding requires additional settings in your router / firewall, like the network address translation (NAT) section Port Forwarding to ports 8443 and 8444.



IP Network Address Port Translation (NAPT) (Port Forwarding)

Source Interface: vlan1 (INT)
Traffic Type: TCP
☑ Use Interface IP from Source Interface
Destination IP Address: 10.96.0.1
Destination Port: 100
Translated Destination IP Address:
Translated Destination Port: 100

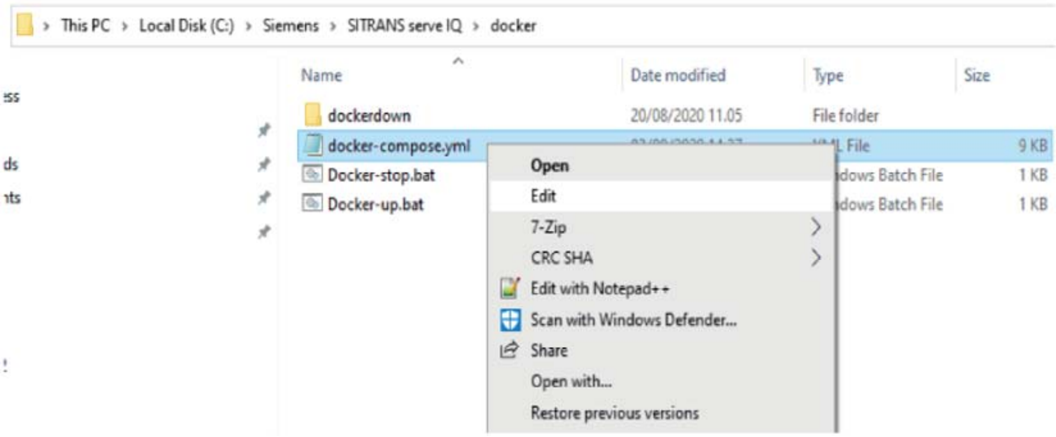
Select	Source Interface	Traffic Type	Interface IP	Destination IP	Destination Port	Translated Destination IP	Translated Destination Port
□	vlan2	TCP	✓	192.168.1.12	55097	10.96.0.249	55097
□	vlan2	TCP	✓	192.168.1.12	55000	10.96.3.3	8443
□	vlan2	TCP	✓	192.168.1.12	55001	10.96.3.3	8444

3 entries.

Please contact your IT department for support regarding the router / firewall settings in use within your company.

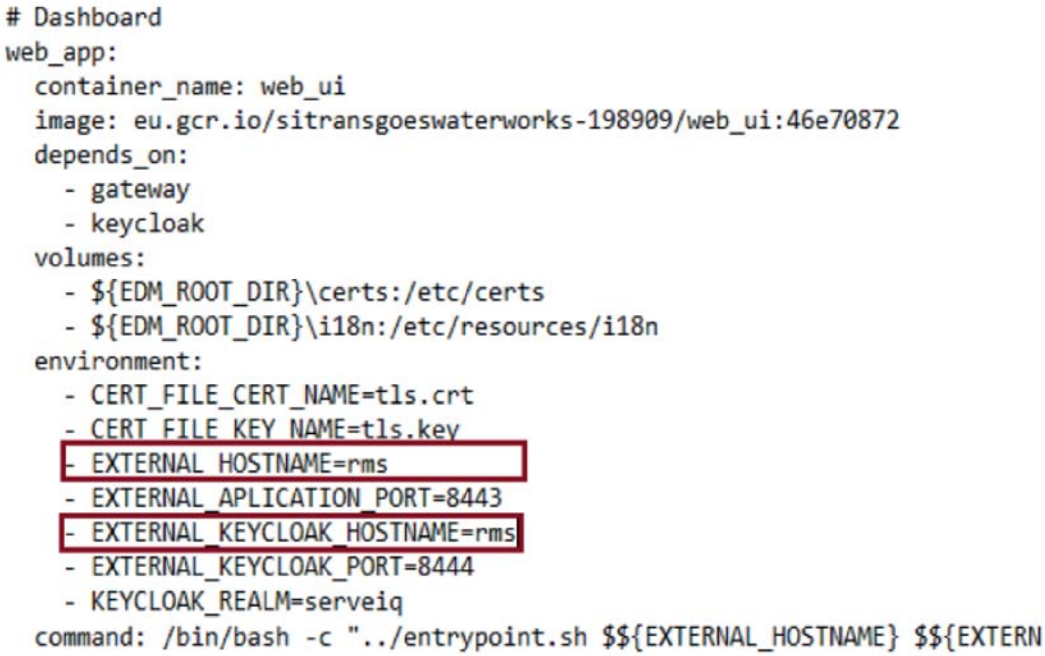
4.4.1.2 Settings in Docker

- Navigate to SITRANS serve IQ installation folder SITRANS serve IQ docker, right-click the docker-compose.yml file, and click Edit.


This PC › Local Disk (C:) › Siemens › SITRANS serve IQ › docker
ss
ds
nts
Open
Edit
7-Zip
CRC SHA
Edit with Notepad++
Scan with Windows Defender...
Share
Open with...
Restore previous versions

Name	Date modified	Type	Size
dockerdown	20/08/2020 11.05	File folder	
docker-compose.yml		L File	9 KB
Docker-stop.bat		dows Batch File	1 KB
Docker-up.bat		dows Batch File	1 KB

- Search for the # Dashboard field and replace the value of EXTERNAL_HOSTNAME and EXTERNAL_KEYCLOAK_HOSTNAME to the specific IP address or domain name, as shown below.



```
# Dashboard
web_app:
  container_name: web_ui
  image: eu.gcr.io/sitransgoeswaterworks-198909/web_ui:46e70872
  depends_on:
    - gateway
    - keycloak
  volumes:
    - ${EDM_ROOT_DIR}\certs:/etc/certs
    - ${EDM_ROOT_DIR}\i18n:/etc/resources/i18n
  environment:
    - CERT_FILE_CERT_NAME=tls.crt
    - CERT_FILE_KEY_NAME=tls.key
    - EXTERNAL_HOSTNAME=rms
    - EXTERNAL_APLICATION_PORT=8443
    - EXTERNAL_KEYCLOAK_HOSTNAME=rms
    - EXTERNAL_KEYCLOAK_PORT=8444
    - KEYCLOAK_REALM=serveiq
  command: /bin/bash -c "../entrypoint.sh $${EXTERNAL_HOSTNAME} $${EXTERN
```

For instance, if you would like to remotely access SITRANS serve IQ with the IP address 2.108.64.158 or the domain name serveiq.net, the following changes shall be made.

EXTERNAL_HOSTNAME=2.108.64.158

EXTERNAL_KEYCLOAK_HOSTNAME=2.108.64.158

or

EXTERNAL_HOSTNAME=serveiq.net

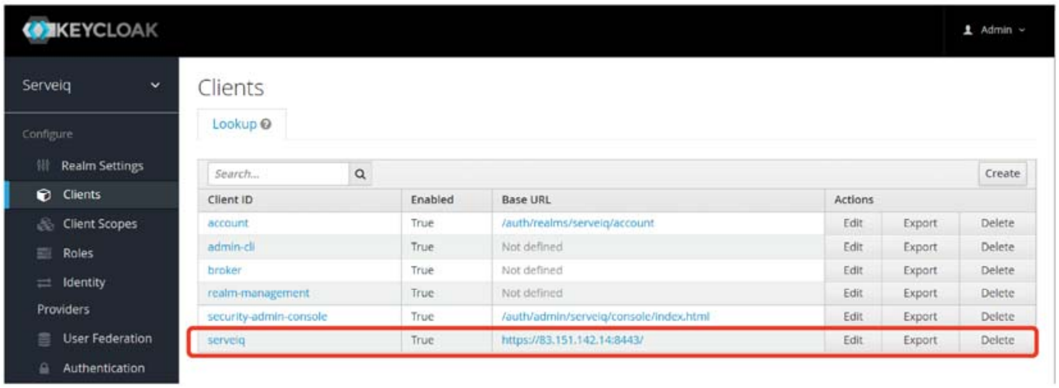
EXTERNAL_KEYCLOAK_HOSTNAME= serveiq.net

- Save the changes and close the docker-compose.yml file.
- Click the START SITRANS serve IQ icon to restart the SITRANS serve IQ program.

4.4.1.3 Settings in Keycloak

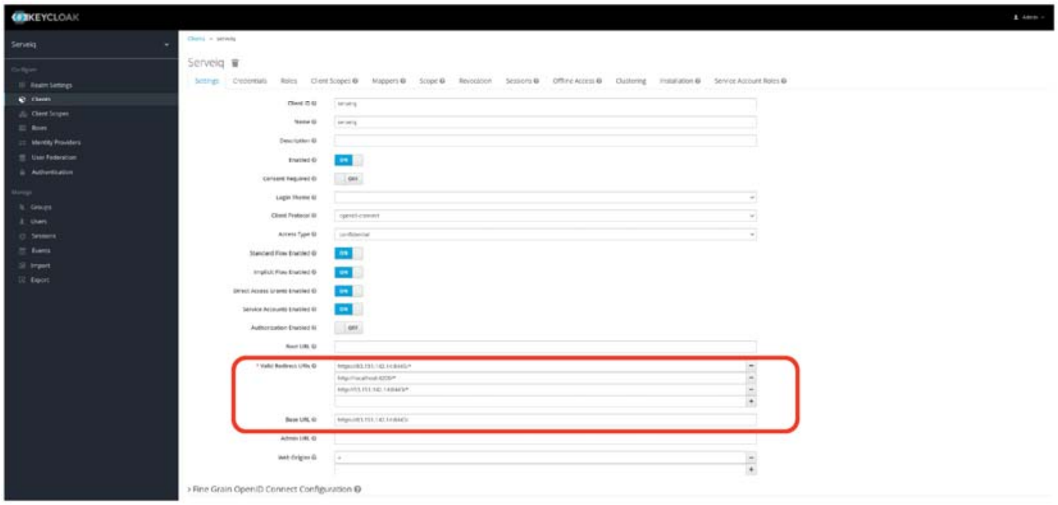
Perform the following steps to access SITRANS serve IQ remotely with a specific IP address or a customized domain name.

- Log in to Keycloak as admin.
- Under the Configure tab, select Clients and click serveiq.



Client ID	Enabled	Base URL	Actions		
account	True	/auth/realms/serveiq/account	Edit	Export	Delete
admin-cli	True	Not defined	Edit	Export	Delete
broker	True	Not defined	Edit	Export	Delete
realm-management	True	Not defined	Edit	Export	Delete
security-admin-console	True	/auth/admin/serveiq/console/index.html	Edit	Export	Delete
serveiq	True	https://83.151.142.14:8443/	Edit	Export	Delete

- Replace the text string "rms" in the Valid Redirect URIs and Base URL fields with the specific IP address or domain name assigned to SITRANS Serve IQ. In the example above, the entry "https://83.151.142.14:8443/*" indicates + an IP address 83.151.142.14 + the port number (for port forwarding) is 8443. For a domain, you would enter the domain name accordingly e.g. use "https://serveiq.net:8443/*"



- Click Save in the end of the menu. (Note: if instead of an IP address, you are using a local domain name e.g. 'rms', please enter 'https://rms:8443/*' or 'http://rms:8443/*'. When done, press 'Save' at the bottom of the page.

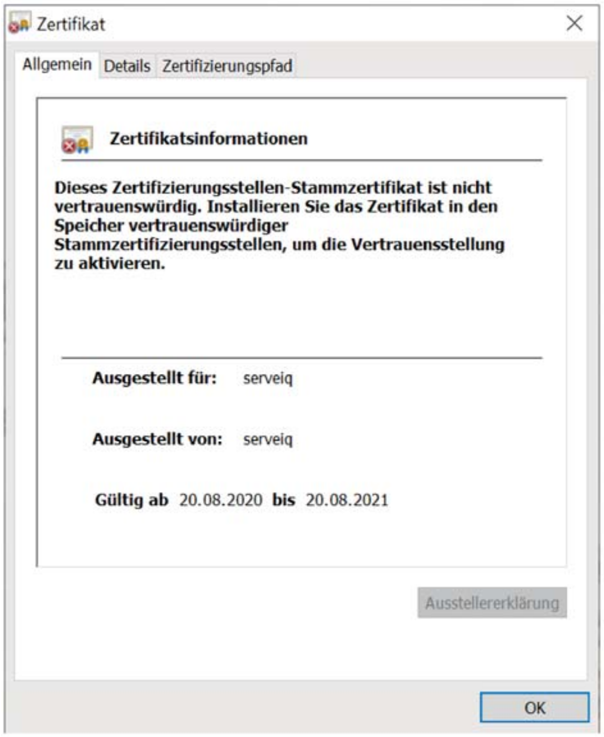
Note

If instead of an external IP address, you are using a local domain name for local access, for example, 'rms', please ensure that the entries are 'https://rms:8443/*' or 'http://rms:8443/*'.

- Click the Stop SITRANS serve IQ icon to stop the SITRANS serve IQ program.

4.4.1.4 Self-issued certificates for encrypted https-communication

- When accessing SITRANS serve IQ with an IP address or as a non-registered domain, it is advisable to create SSL-certificates yourself. This will enable you to use encrypted https -communication when accessing SITRANS serve IQ instead of the simple, not-encrypted http communication



Zertifikat

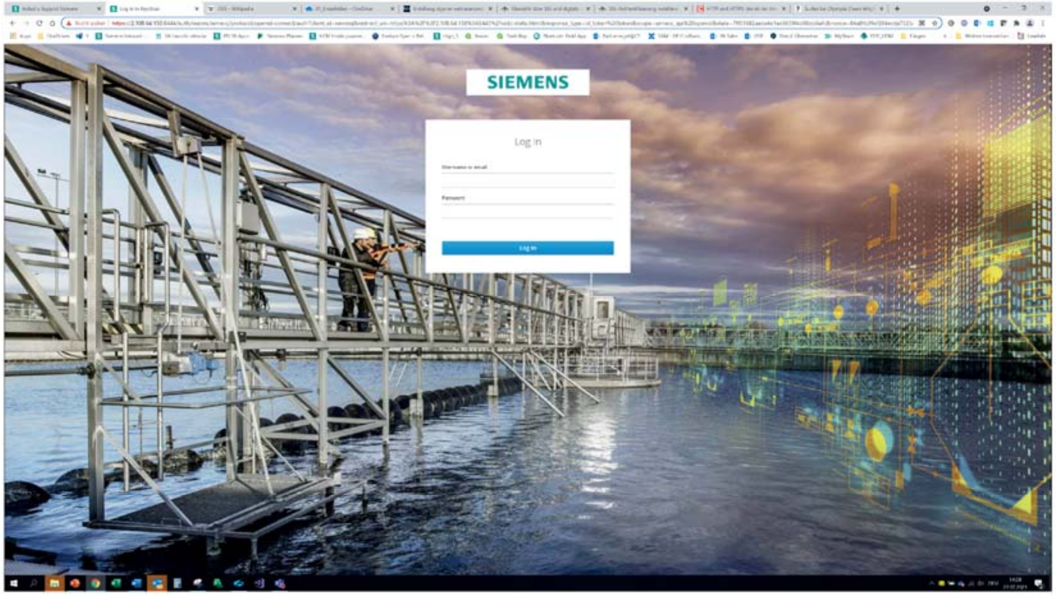
Zertifikatsinformationen

Dieses Zertifizierungsstellen-Stammzertifikat ist nicht vertrauenswürdig. Installieren Sie das Zertifikat in den Speicher vertrauenswürdiger Stammzertifizierungsstellen, um die Vertrauensstellung zu aktivieren.

Ausgestellt für: serveiq

Ausgestellt von: serveiq

Gültig ab 20.08.2020 **bis** 20.08.2021



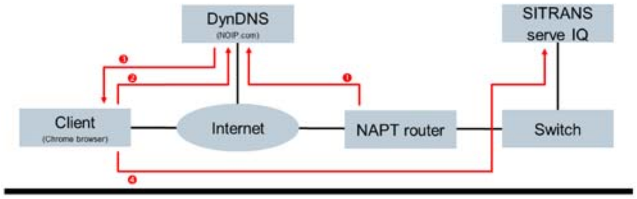
As the self-created SSL certificates by default are not registered with a certification authority, a warning message (connection unsecure) will remain.

Please contact your IT-department for support.

4.4.2 Internet access via domain

4.4.2.1 Overview

Alternatively, to a simple IP-address to access SITRANS serve IQ, you could create your specific domain (fictional example: https://sitransserveiq.customer.com:8443). To access computer’s IP-address via its domain, the principle applies:



1. The router must set his IP address in a DynDNS provider (e.g. www.noip.com) under his name (set e.g. IP=151.231.10.211 at NOIP.com, under www.MyDomainName.com) and update the IP address after a change invoked by the internet provider
2. The browser must seek the IP address of www.MyDomainName.com
3. The DynDNS provider (www.noip.com) delivers the IP address: e.g. 151.231.10.211
4. The browser uses this IP address automatically and reaches the router

Note

IP-Ports are noted after a ":" after the domain name, e.g. https://www.MyDomainName:8443. In this example the IP-Port is 8443.

4.4.2.2 Registration of domain and SSL from a Certification Authority

To avoid the warning (see 4.2.2), you need to register your domain, obtain a SSL certificate and add this to your local instance of SITRANS serve IQ.

The most common use of certificates is for HTTPS-based web sites. A web browser validates that an HTTPS web server is authentic, so that the user can feel secure that the interaction with the web site has no eavesdroppers and that the web site is who it claims to be. This security is important for sensitive data of a company. In practice, a web site administrator obtains a certificate by applying to a certificate authority (CA) with a certificate signing request (CSR). The certificate request is an electronic document that contains the web site name, company information and the public key. The certificate authority grants that certificate after certain investigations, thus producing a public certificate. The administrator must prove the ownership of the corresponding web site(s).

There are two protocols that provide secure communications over a computer network: Secure Sockets Layer (SSL) and Transport Layer security (TLS).

SSL is the term commonly used, and today usually refers to TLS. SSL/TLS provides data encryption, data integrity and authentication. This means a message encrypted with a public key can only be decrypted with the corresponding private key. The root certificate of the CA and end-entity certificate (e.g. for www.MyDomainName.com) can be considered as a chain of trust.

The root certificates from CA's like www.GlobalSign.com are normally stored in the browser (e.g. Chrome). SSL Certificates can be classified into three types:

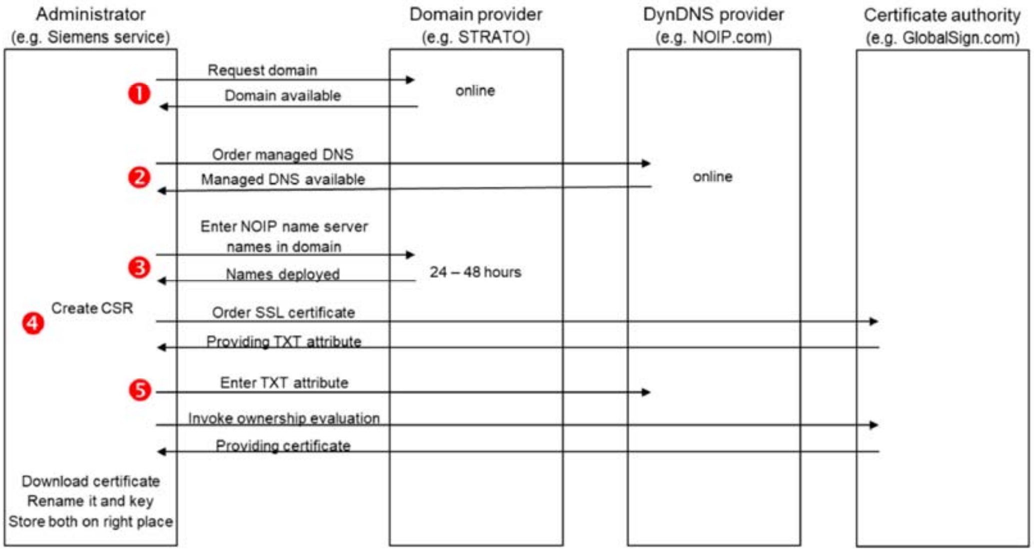
- Domain Validation SSL
- Organization Validation SSL
- Extended Validation SSL

In this manual, only domain validation certificates are considered, please align with your IT-organization about the possibilities for further validation.

Note

A Web site may also be configured with a self-signed certificate. The communication based on such a self-signed certificate is encrypted, however the authentication is not granted. In this case, clients will generally be unable to verify the certificate, and might terminate the connection unless certificate checking is disabled.

Steps to register a domain and obtain an SSL certificate



1. Request and order domain
   As mentioned above being owner of a domain is mandatory to get an SSL certificate. The best way to get a domain is to create an account at a registrar's site first. The registrar in the example is www.strato.de - but could be any registrar.
   Choose for a free domain name, which fits your requests on your naming scheme and order it, without hosting a web server, just managing the name. In this example let's expect, that the domain www.MyDomainName.com is available (not already used) and order it.
2. Order an account at a provider
   The best way to get a DynDNS service is to create an account at a provider first. The provider in this example here is www.noip.com - but could be any provider. After login, order for example a so-called Plus Managed DNS product (make sure that the feature with TXT attribute is supported).
   Enter your domain name, e.g. www.MyDomainName.com. Follow the instructions during

online purchase, and information you are going to receive via Email.
At the end of the process the DynDNS entry and the domain name build a tight relationship and allows the Certificate Authorization (CA) to check ownership and to grant a certificate

3. Enter name server names for your domain
   You will receive an Email from DynDNS www.noip.com with four Name-Server names which must be entered at the domain registrar's site accordingly. These names may look like: ns1.no-ip.com, ns2.no-ip.com, ns3.no-ip.com, ns4.no-ip.com
4. Order SSL certificates
   You can start with this step in parallel with the first three ones. But for evaluating ownership of your domain www.MyDomainName.com all first three steps must be fully conducted. Please follow this process for ordering SSL certificates:
   - Create a so-called Certificate Signing Request (CSR) There are several tools available, e.g. openssl
   - Create an account at www.globalsign.com or any other Certificate Authority (CA)
   - Order a certificate according to your request, e.g. DomainSSL, Single-Domain-Certificate, enter the complete content of your CSR, including 'Begin / End New Certificate Request'
   - The complete process is started. Follow instructions from Web site and/or Emails.
5. Make the SSL certificate available
   Copy the certificate as plain text in a file TLS.cer, which was created with notepad.exe and store it together with the key file (renamed to TLS.Key) in the appropriate directory.

Example:

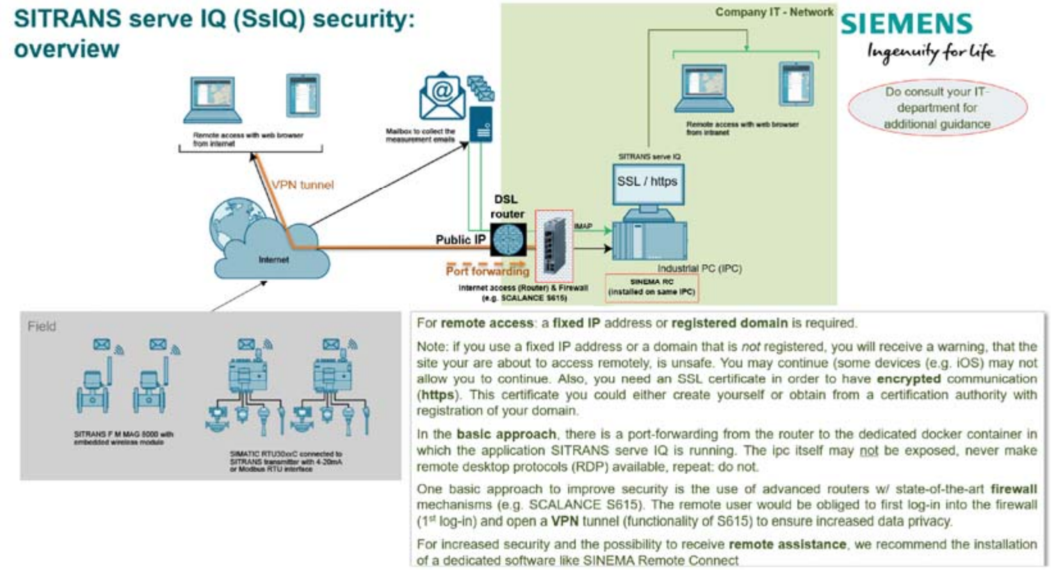
In an Email you will receive from www.GlobalSign.com you may find information like this.

- Upload an HTML or text file to the domain(s) under the "/.well-known/pki-validation" directory, with the random value "vQ0MHMfS+/xxxxxxxxxxxxxxxxx=" and then send us the link. This random value expires in 30 days. Please make sure that the random value as mentioned above is not part of the URL; or
- Upload the random value "vQ0MHMfS+/xxxxxxxxxxxxxxxxx=" as a publically viewable DNS TXT record and inform us when it is visible. This random value expires in 30 days or
- We can contact the domain registrants and confirm directly with them that your organization can request an SSL certificate for the domains. For this, we can use one of the following pre-approved email addresses: admin@domainname, administrator@domainname, postmaster@domainname, hostmaster@domainname, or webmaster@domainname → Choose the option #2: DNS TXT record
- Copy the random value for the DNS TXT record out of the Email from www.globalsign.com in your Plus Managed DNS www.MyDomainName.com in www.noip.com and click on the appropriate link in the Email to verify ownership.

If everything was done right, you will get an Email which contains your CA SSL certificate.

4.5 Additional firewall for enhanced security

A basic approach to increase security further is the use of advanced routers with state-of-the-art firewall mechanisms and VPN functionality (e.g. SCALANCE S615). The remote user would be obliged to first log-in into the firewall (1st log-in) and temporarily open the firewall for SITRANS serve IQ access (2nd log in). After completing the session, the remote user must activate the firewall again.


SITRANS serve IQ (SsIQ) security: overview
Company IT - Network
SIEMENS
Ingenuity for life
Do consult your IT-department for additional guidance
Remote access with web browser from internet
Mailbox to collect the measurement emails
Remote access with web browser from intranet
SITRANS serve IQ
SSL / https
VPN tunnel
DSL router
Public IP
IMAP
Internet
Port forwarding
Internet access (Router) & Firewall (e.g. SCALANCE S615)
Industrial PC (IPC)
SINEMA RC (installed on same IPC)
Field
SITRANS F M MAG 8000 with embedded wireless module
SIMATIC RTU30xxC connected to SITRANS transmitter with 4-20mA or Modbus RTU interface

For **remote access**: a **fixed IP** address or **registered domain** is required.

Note: if you use a fixed IP address or a domain that is *not* registered, you will receive a warning, that the site your are about to access remotely, is unsafe. You may continue (some devices (e.g. iOS) may not allow you to continue. Also, you need an SSL certificate in order to have **encrypted** communication (**https**). This certificate you could either create yourself or obtain from a certification authority with registration of your domain.

In the **basic approach**, there is a port-forwarding from the router to the dedicated docker container in which the application SITRANS serve IQ is running. The ipc itself may not be exposed, never make remote desktop protocols (RDP) available, repeat: do not.

One basic approach to improve security is the use of advanced routers w/ state-of-the-art **firewall** mechanisms (e.g. SCALANCE S615). The remote user would be obliged to first log-in into the firewall (1st log-in) and open a **VPN** tunnel (functionality of S615) to ensure increased data privacy.

For increased security and the possibility to receive **remote assistance**, we recommend the installation of a dedicated software like SINEMA Remote Connect

Figure 4-3 SITRANS serve IQ security: with remote access (basic approach)

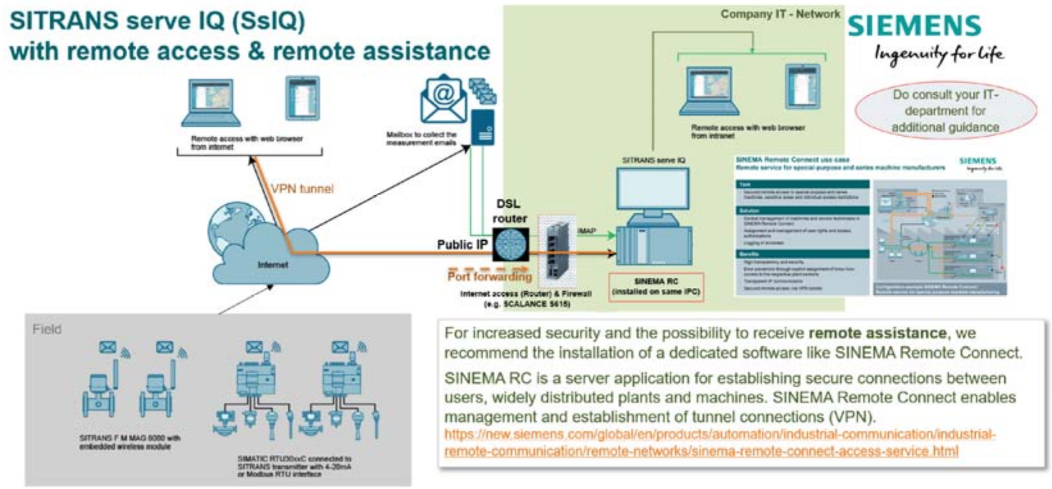
This is possible with simple IP addresses or with a registered domain.

For further information, please consult your IT department and/or Siemens via a support request on siemens.com/SIOS/sitransserveiq (https://www.siemens.com/SIOS/sitransserveiq)

4.6 Remote assistance

For increased security and the possibility to receive remote assistance, we recommend the installation of a dedicated software like SINEMA Remote Connect. SINEMA RC is a server application for establishing secure connections between users, widely distributed plants and machines. SINEMA Remote Connect enables management and establishment of tunnel connections (VPN).

https://new.siemens.com/global/en/products/automation/industrial-communication/industrial-remote-communication/remote-networks/sinema-remote-connect-access-service.html



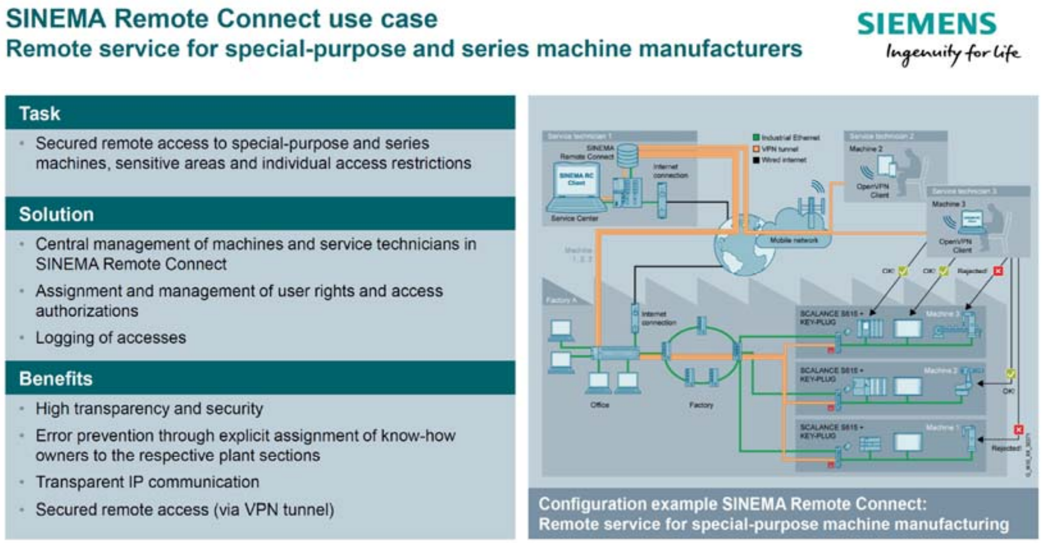
SITRANS serve IQ (SsIQ)
with remote access & remote assistance

For increased security and the possibility to receive **remote assistance**, we recommend the installation of a dedicated software like SINEMA Remote Connect.

SINEMA RC is a server application for establishing secure connections between users, widely distributed plants and machines. SINEMA Remote Connect enables management and establishment of tunnel connections (VPN).
https://new.siemens.com/global/en/products/automation/industrial-communication/industrial-remote-communication/remote-networks/sinema-remote-connect-access-service.html

Company IT - Network
SIEMENS
Ingenuity for life
Do consult your IT-department for additional guidance
Remote access with web browser from internet
Mailbox to collect the measurement emails
Remote access with web browser from intranet
VPN tunnel
Internet
DSL router
Public IP
Port forwarding
Internet access (Router) & Firewall (e.g. SCALANCE S615)
IMAP
SITRANS serve IQ
SINEMA RC (installed on same IPC)
Field
SITRANS F M MAG 8000 with embedded wireless module
SIMATIC RTU30xxC connected to SITRANS transmitter with 4-20mA or Modbus RTU interface

Figure 4-4 SITRANS serve IQ with remote access and remote assistance



SINEMA Remote Connect use case
Remote service for special-purpose and series machine manufacturers

Task

- Secured remote access to special-purpose and series machines, sensitive areas and individual access restrictions

Solution

- Central management of machines and service technicians in SINEMA Remote Connect
- Assignment and management of user rights and access authorizations
- Logging of accesses

Benefits

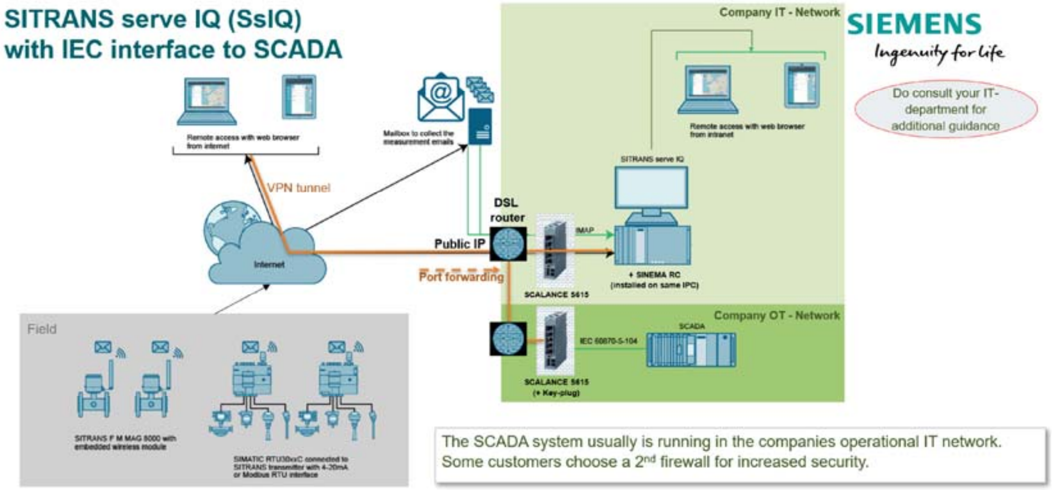
- High transparency and security
- Error prevention through explicit assignment of know-how owners to the respective plant sections
- Transparent IP communication
- Secured remote access (via VPN tunnel)

Configuration example SINEMA Remote Connect:
Remote service for special-purpose machine manufacturing

For further information, please consult your IT - department and /or Siemens via a support request on siemens.com/SIOS/sitransserveiq (https://www.siemens.com/SIOS/sitransserveiq)

4.7 Secure connection to SCADA

The SCADA system usually is running in the companies' operational IT network. In general and specifically when enabling access to SITRANS serve IQ from the internet, we recommend installing 2nd firewall for increased security of the SCADA .



SITRANS serve IQ (SsIQ)
with IEC interface to SCADA

The SCADA system usually is running in the companies operational IT network.
Some customers choose a 2nd firewall for increased security.

SIEMENS
Ingenuity for life
Do consult your IT-department for additional guidance
Remote access with web browser from internet
Mailbox to collect the measurement emails
VPN tunnel
Internet
DSL router
Public IP
Port forwarding
Company IT - Network
Remote access with web browser from intranet
SITRANS serve IQ
IMAP
+ SINEMA RC (installed on same IPC)
SCALANCE S615
Company OT - Network
SCADA
IEC 60870-5-104
SCALANCE S615 (+ Key-plug)
Field
SITRANS F M MAG 8000 with embedded wireless module
SIMATIC RTU30xxC connected to SITRANS transmitter with 4-20mA or Modbus RTU interface

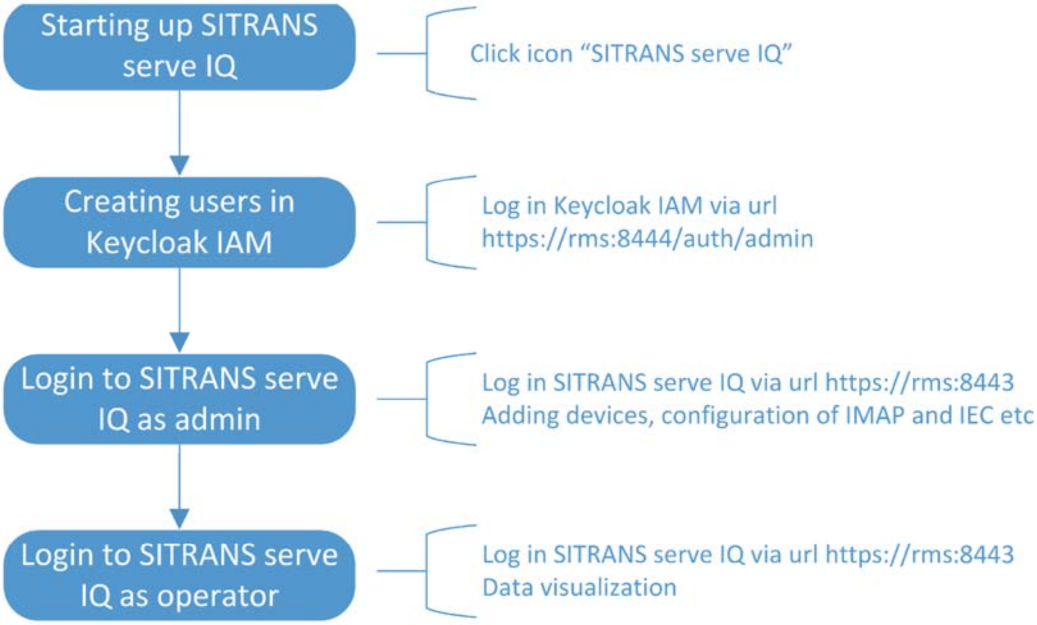
Figure 4-5 SITRANS serve IQ with IEC interface to SCADA

For further information, please consult your IT - department and /or Siemens via a support request on siemens.com/SIOS/sitransserveiq (https://www.siemens.com/SIOS/sitransserveiq)

5 Starting the SITRANS serve IQ application

Before starting SITRANS serve IQ, ensure that Docker containers are running. (see also Start Docker Application (Page 27)).

The subsequent steps are described as follows:



Starting up SITRANS serve IQ — Click icon “SITRANS serve IQ”

Creating users in Keycloak IAM — Log in Keycloak IAM via url https://rms:8444/auth/admin

Login to SITRANS serve IQ as admin — Log in SITRANS serve IQ via url https://rms:8443 Adding devices, configuration of IMAP and IEC etc

Login to SITRANS serve IQ as operator — Log in SITRANS serve IQ via url https://rms:8443 Data visualization

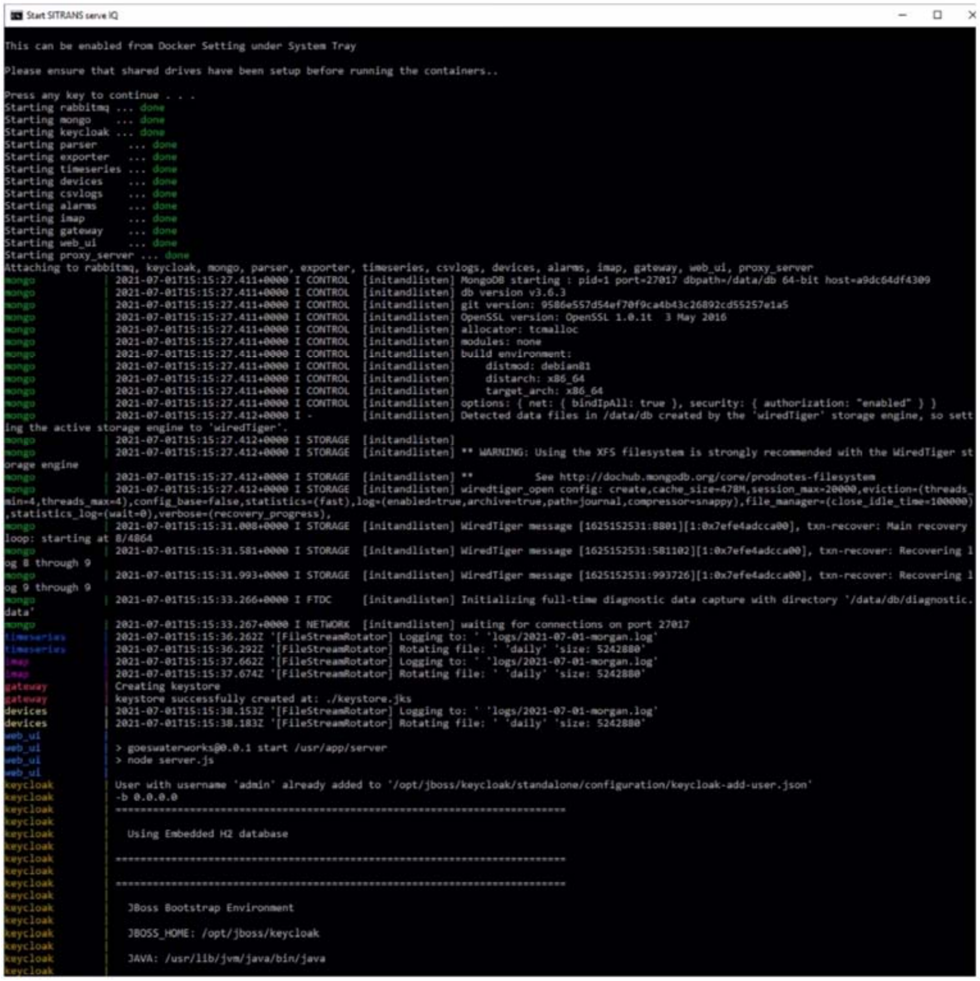
5.1 Starting SITRANS serve IQ

Click the icon "Start SITRANS serve IQ" on the desktop to start SITRANS serve IQ and required components like Keycloak and ALM.

Another window will open, asking you to ensure Docker is up and running, and that "shared drives have been set up before continuing" (see also Configuration of Docker (Page 28)).

If this is ok, press any key to continue.

The startup of SITRANS serve IQ will take about one minute, during which the window shows the software items starting.



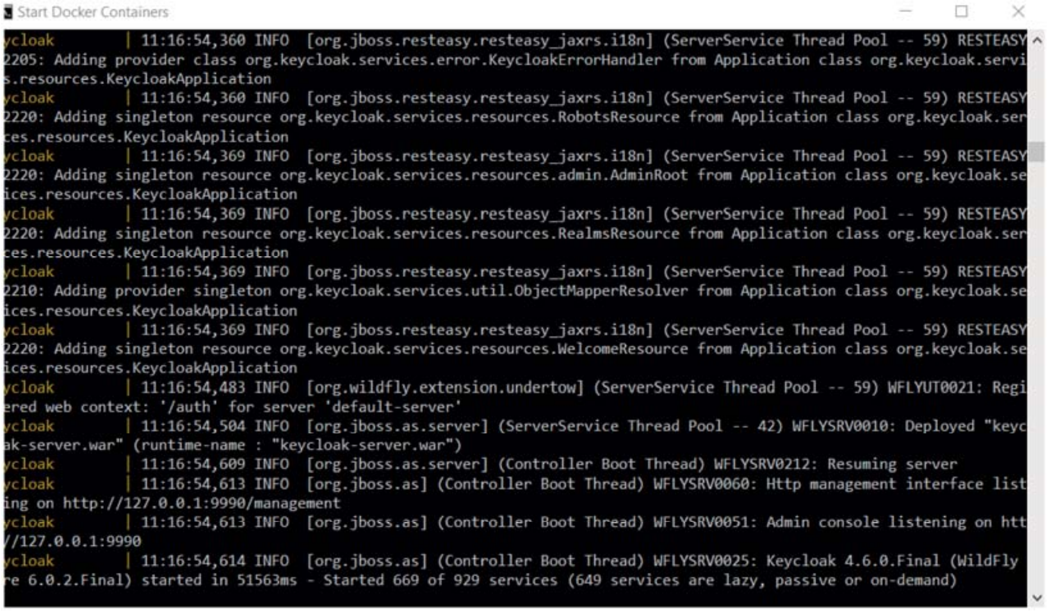
```
This can be enabled from Docker Setting under System Tray

Please ensure that shared drives have been setup before running the containers..

Press any key to continue . . .
Starting rabbitmq ... done
Starting mongo    ... done
Starting keycloak ... done
Starting parser     ... done
Starting exporter   ... done
Starting timeseries ... done
Starting devices    ... done
Starting csvlogs    ... done
Starting alarms     ... done
Starting imap       ... done
Starting gateway    ... done
Starting web_ui     ... done
Starting proxy_server ... done
Attaching to rabbitmq, keycloak, mongo, parser, exporter, timeseries, csvlogs, devices, alarms, imap, gateway, web_ui, proxy_server
mongo           | 2021-07-01T15:15:27.411+0000 I CONTROL  [initandlisten] MongoDB starting : pid=1 port=27017 dbpath=/data/db 64-bit host=a9dc64df4309
mongo           | 2021-07-01T15:15:27.411+0000 I CONTROL  [initandlisten] db version v3.6.3
mongo           | 2021-07-01T15:15:27.411+0000 I CONTROL  [initandlisten] git version: 9586e557d54ef70f9ca4b43c26892cd55257e1a5
mongo           | 2021-07-01T15:15:27.411+0000 I CONTROL  [initandlisten] OpenSSL version: OpenSSL 1.0.1t  3 May 2016
mongo           | 2021-07-01T15:15:27.411+0000 I CONTROL  [initandlisten] allocator: tcmalloc
mongo           | 2021-07-01T15:15:27.411+0000 I CONTROL  [initandlisten] modules: none
mongo           | 2021-07-01T15:15:27.411+0000 I CONTROL  [initandlisten] build environment:
mongo           | 2021-07-01T15:15:27.411+0000 I CONTROL  [initandlisten]     distmod: debian81
mongo           | 2021-07-01T15:15:27.411+0000 I CONTROL  [initandlisten]     distarch: x86_64
mongo           | 2021-07-01T15:15:27.411+0000 I CONTROL  [initandlisten]     target_arch: x86_64
mongo           | 2021-07-01T15:15:27.411+0000 I CONTROL  [initandlisten] options: { net: { bindIpAll: true }, security: { authorization: "enabled" } }
mongo           | 2021-07-01T15:15:27.412+0000 I -        [initandlisten] Detected data files in /data/db created by the 'wiredTiger' storage engine, so sett
ing the active storage engine to 'wiredTiger'.
mongo           | 2021-07-01T15:15:27.412+0000 I STORAGE  [initandlisten]
mongo           | 2021-07-01T15:15:27.412+0000 I STORAGE  [initandlisten] ** WARNING: Using the XFS filesystem is strongly recommended with the WiredTiger st
orage engine
mongo           | 2021-07-01T15:15:27.412+0000 I STORAGE  [initandlisten] **          See http://dochub.mongodb.org/core/prodnotes-filesystem
mongo           | 2021-07-01T15:15:27.412+0000 I STORAGE  [initandlisten] wiredtiger_open config: create,cache_size=478M,session_max=20000,eviction=(threads_
min=4,threads_max=4),config_base=false,statistics=(fast),log=(enabled=true,archive=true,path=journal,compressor=snappy),file_manager=(close_idle_time=100000)
,statistics_log=(wait=0),verbose=(recovery_progress),
mongo           | 2021-07-01T15:15:31.008+0000 I STORAGE  [initandlisten] WiredTiger message [1625152531:8801][1:0x7efe4adcca00], txn-recover: Main recovery
loop: starting at 8/4864
mongo           | 2021-07-01T15:15:31.581+0000 I STORAGE  [initandlisten] WiredTiger message [1625152531:581102][1:0x7efe4adcca00], txn-recover: Recovering l
og 8 through 9
mongo           | 2021-07-01T15:15:31.993+0000 I STORAGE  [initandlisten] WiredTiger message [1625152531:993726][1:0x7efe4adcca00], txn-recover: Recovering l
og 9 through 9
mongo           | 2021-07-01T15:15:33.266+0000 I FTDC     [initandlisten] Initializing full-time diagnostic data capture with directory '/data/db/diagnostic.
data'
mongo           | 2021-07-01T15:15:33.267+0000 I NETWORK  [initandlisten] waiting for connections on port 27017
timeseries      | 2021-07-01T15:15:36.262Z '[FileStreamRotator] Logging to: ' 'logs/2021-07-01-morgan.log'
timeseries      | 2021-07-01T15:15:36.292Z '[FileStreamRotator] Rotating file: ' 'daily' 'size: 5242880'
imap            | 2021-07-01T15:15:37.662Z '[FileStreamRotator] Logging to: ' 'logs/2021-07-01-morgan.log'
imap            | 2021-07-01T15:15:37.674Z '[FileStreamRotator] Rotating file: ' 'daily' 'size: 5242880'
gateway         | Creating keystore
gateway         | keystore successfully created at: ./keystore.jks
devices         | 2021-07-01T15:15:38.153Z '[FileStreamRotator] Logging to: ' 'logs/2021-07-01-morgan.log'
devices         | 2021-07-01T15:15:38.183Z '[FileStreamRotator] Rotating file: ' 'daily' 'size: 5242880'
web_ui          |
web_ui          | > goeswaterworks@0.0.1 start /usr/app/server
web_ui          | > node server.js
web_ui          |
keycloak        | User with username 'admin' already added to '/opt/jboss/keycloak/standalone/configuration/keycloak-add-user.json'
keycloak        | -b 0.0.0.0
keycloak        | =========================================================================
keycloak        |
keycloak        |   Using Embedded H2 database
keycloak        |
keycloak        | =========================================================================
keycloak        |
keycloak        | =========================================================================
keycloak        |
keycloak        |   JBoss Bootstrap Environment
keycloak        |
keycloak        |   JBOSS_HOME: /opt/jboss/keycloak
keycloak        |
keycloak        |   JAVA: /usr/lib/jvm/java/bin/java
keycloak        |
```

The startup of SITRANS serve IQ is completed successfully, once the following message is being displayed (the actual time in ms might vary though):

```
keycloak | 11:16:54,614 INFO [org.jboss.as] (Controller Boot Thread)
WFLYSRV0025: Keycloak 4.6.0.Final (WildFly Core 6.0.2.Final) started
in 51563ms - Started 669 of 929 services (649 services are lazy,
passive or on-demand)
```

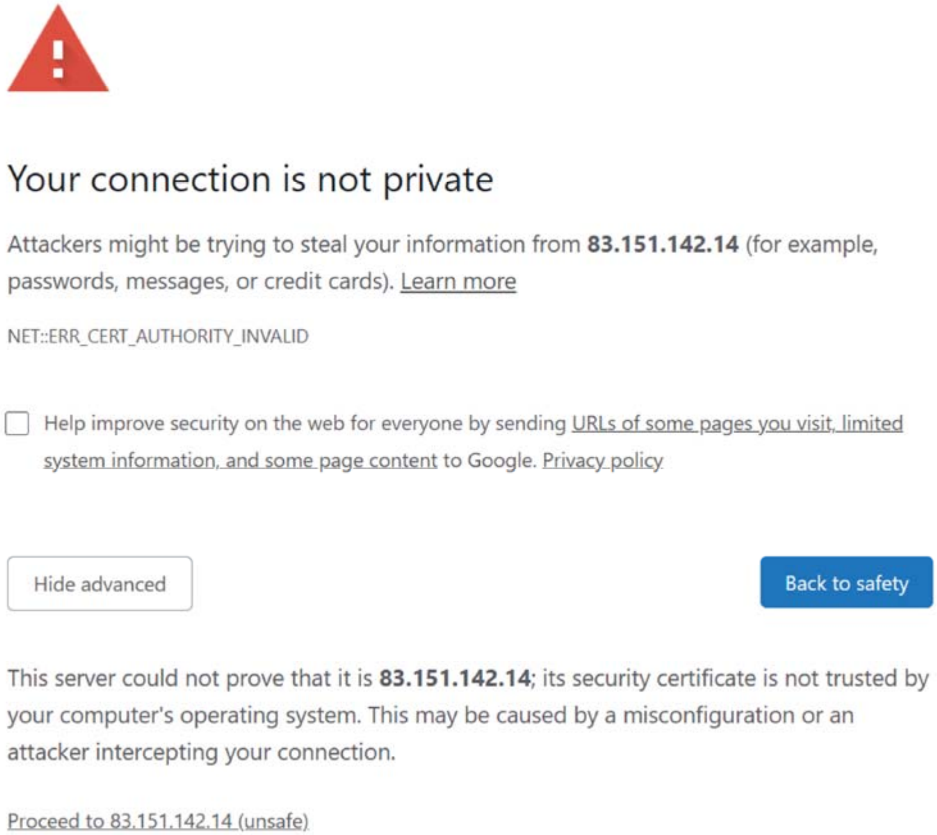


```
ycloak        | 11:16:54,360 INFO  [org.jboss.resteasy.resteasy_jaxrs.i18n] (ServerService Thread Pool -- 59) RESTEASY
2205: Adding provider class org.keycloak.services.error.KeycloakErrorHandler from Application class org.keycloak.servi
s.resources.KeycloakApplication
ycloak        | 11:16:54,360 INFO  [org.jboss.resteasy.resteasy_jaxrs.i18n] (ServerService Thread Pool -- 59) RESTEASY
2220: Adding singleton resource org.keycloak.services.resources.RobotsResource from Application class org.keycloak.ser
ces.resources.KeycloakApplication
ycloak        | 11:16:54,369 INFO  [org.jboss.resteasy.resteasy_jaxrs.i18n] (ServerService Thread Pool -- 59) RESTEASY
2220: Adding singleton resource org.keycloak.services.resources.admin.AdminRoot from Application class org.keycloak.se
ices.resources.KeycloakApplication
ycloak        | 11:16:54,369 INFO  [org.jboss.resteasy.resteasy_jaxrs.i18n] (ServerService Thread Pool -- 59) RESTEASY
2220: Adding singleton resource org.keycloak.services.resources.RealmsResource from Application class org.keycloak.ser
ces.resources.KeycloakApplication
ycloak        | 11:16:54,369 INFO  [org.jboss.resteasy.resteasy_jaxrs.i18n] (ServerService Thread Pool -- 59) RESTEASY
2210: Adding provider singleton org.keycloak.services.util.ObjectMapperResolver from Application class org.keycloak.se
ices.resources.KeycloakApplication
ycloak        | 11:16:54,369 INFO  [org.jboss.resteasy.resteasy_jaxrs.i18n] (ServerService Thread Pool -- 59) RESTEASY
2220: Adding singleton resource org.keycloak.services.resources.WelcomeResource from Application class org.keycloak.se
ices.resources.KeycloakApplication
ycloak        | 11:16:54,483 INFO  [org.wildfly.extension.undertow] (ServerService Thread Pool -- 59) WFLYUT0021: Regi
ered web context: '/auth' for server 'default-server'
ycloak        | 11:16:54,504 INFO  [org.jboss.as.server] (ServerService Thread Pool -- 42) WFLYSRV0010: Deployed "keyc
ak-server.war" (runtime-name : "keycloak-server.war")
ycloak        | 11:16:54,609 INFO  [org.jboss.as.server] (Controller Boot Thread) WFLYSRV0212: Resuming server
ycloak        | 11:16:54,613 INFO  [org.jboss.as] (Controller Boot Thread) WFLYSRV0060: Http management interface list
ing on http://127.0.0.1:9990/management
ycloak        | 11:16:54,613 INFO  [org.jboss.as] (Controller Boot Thread) WFLYSRV0051: Admin console listening on htt
//127.0.0.1:9990
ycloak        | 11:16:54,614 INFO  [org.jboss.as] (Controller Boot Thread) WFLYSRV0025: Keycloak 4.6.0.Final (WildFly
re 6.0.2.Final) started in 51563ms - Started 669 of 929 services (649 services are lazy, passive or on-demand)
```

5.2 Warning messages

When accessing SITRANS serve IQ with the IP address or as a non-registered domain, you might receive a warning, that this site is "not secure".

This follows the standard internet practice: for a domain to be considered safe, it must be registered and provide an SSL certificate, which has been issued by a certificate authority (CA). When setting up your own IPC and making it accessible to the internet, by default, the IP-address will not be registered and hence will be considered ‘unsafe’.



Your connection is not private

Attackers might be trying to steal your information from **83.151.142.14** (for example, passwords, messages, or credit cards). Learn more

NET::ERR_CERT_AUTHORITY_INVALID

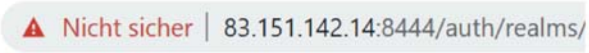
□ Help improve security on the web for everyone by sending URLs of some pages you visit, limited system information, and some page content to Google. Privacy policy

This server could not prove that it is **83.151.142.14**; its security certificate is not trusted by your computer's operating system. This may be caused by a misconfiguration or an attacker intercepting your connection.

Proceed to 83.151.142.14 (unsafe)

By continuing to ‘further information’, you have the possibility to proceed: ‘continue to <IP-address> (not recommended)’. (Note: some iOS devices might prohibit you from proceeding).

As you enter the site, you will continue to see also the comment ‘not secure’ in the address line of the browser.



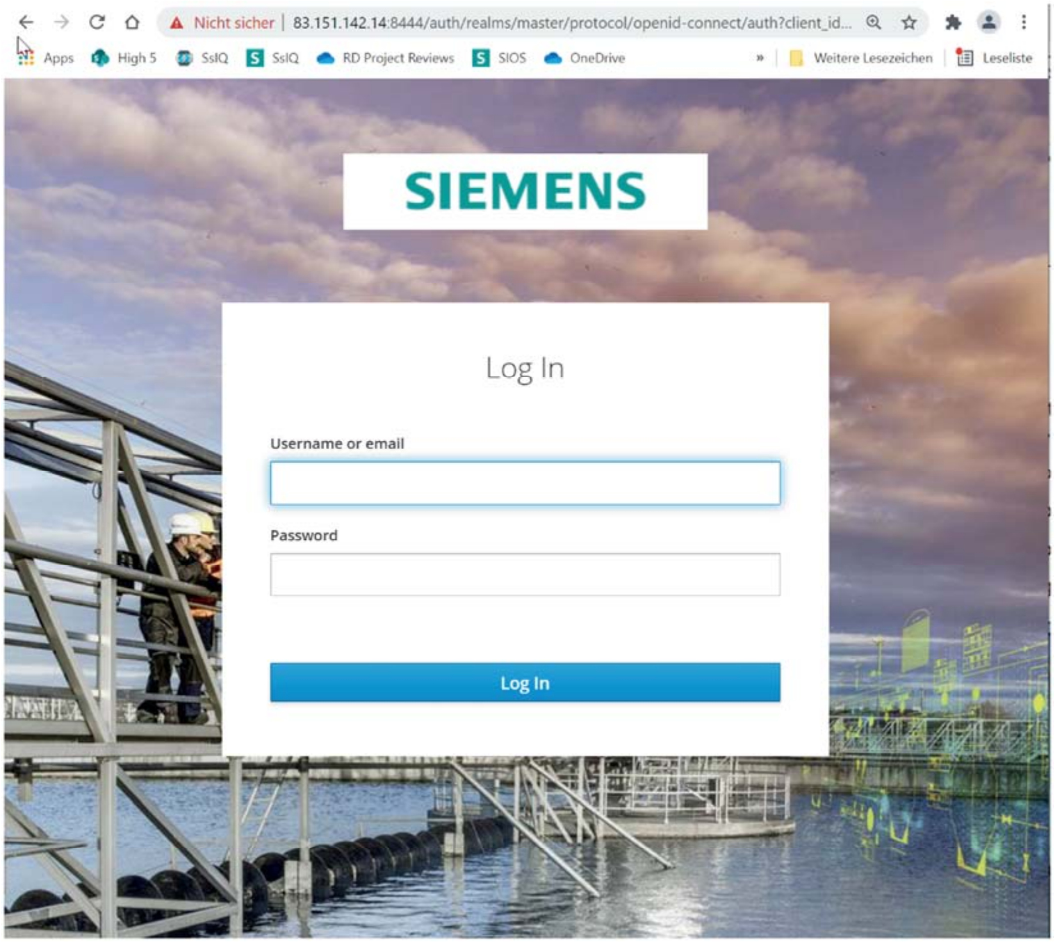
▲ Nicht sicher | 83.151.142.14:8444/auth/realms/

5.3 Access to Keycloak as admin

To start up Keycloak Identity and Access Management (IAM) to create users, type in the web browser (use Google Chrome) address box (depending on the previously described sections and possible further firewalls):

- https://rms:8444/auth/admin or
- https://<IP-address>:8444/auth/admin or
- https://<your domain>:8444/auth/admin

The login page appears.



Note

The Log – in page for Keycloak and for the application SITRANS serve IQ itself is identical. Only the port number determines whether you log into keycloak (port: 8444) or SITRANS serve IQ (port: 8443)

To Log In, enter the login credentials

Login: admin

Password: admin (which is the initial password) / < your updated password >

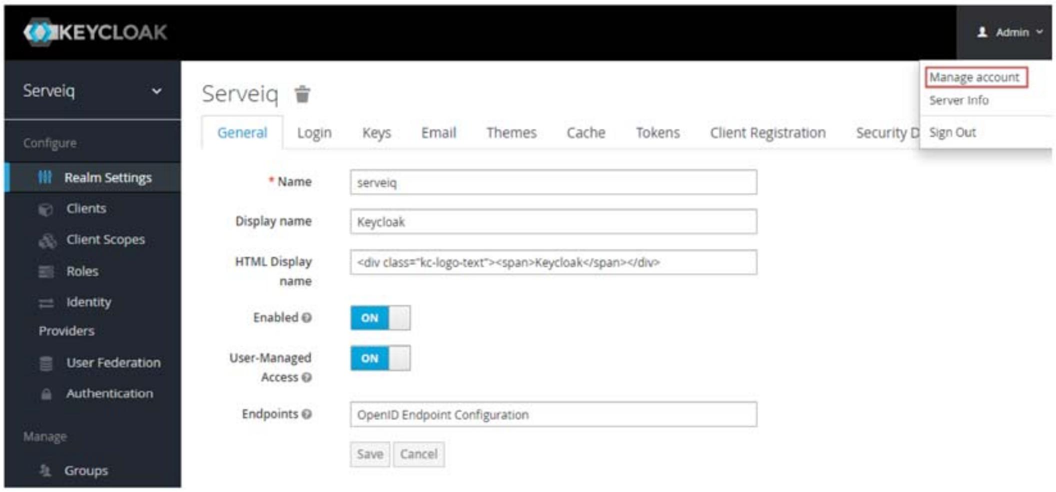
and press 'Log in'. You will be directed to Keycloak application.

The administrator-task in keycloak is exclusively to create users in SITRANS serve IQ.

It is highly recommended to change the initial password for Keycloak login.

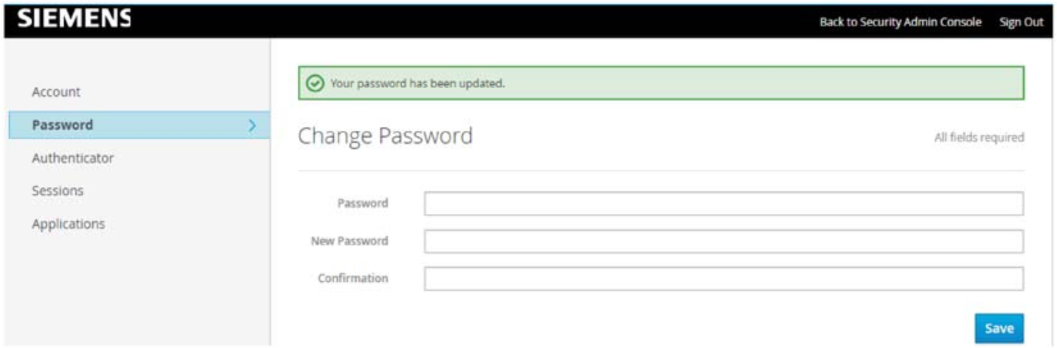
To change the password of the Administrator of Keycloak:

- click Admin on the upper right corner and select Manage account



* Name: serveiq
Display name: Keycloak
HTML Display name: <div class="kc-logo-text"><span>Keycloak</span></div>
Enabled: ON
User-Managed Access: ON
Endpoints: OpenID Endpoint Configuration

- under Configure tab on the left panel, click **Password**.



Your password has been updated.

- Please put the current password in Password box and put the new password to New Password and Confirmation boxes.
- Use secure passwords that include:
  - A maximum of 32 characters
  - A minimum of 8 characters
  - At least one upper case letter
  - At least one number
  - At least one special character
  - Click Save to update the password.

Note

If you click on Account by accident when changing password, please leave all fields in Account blank. Do not include personal name or email.

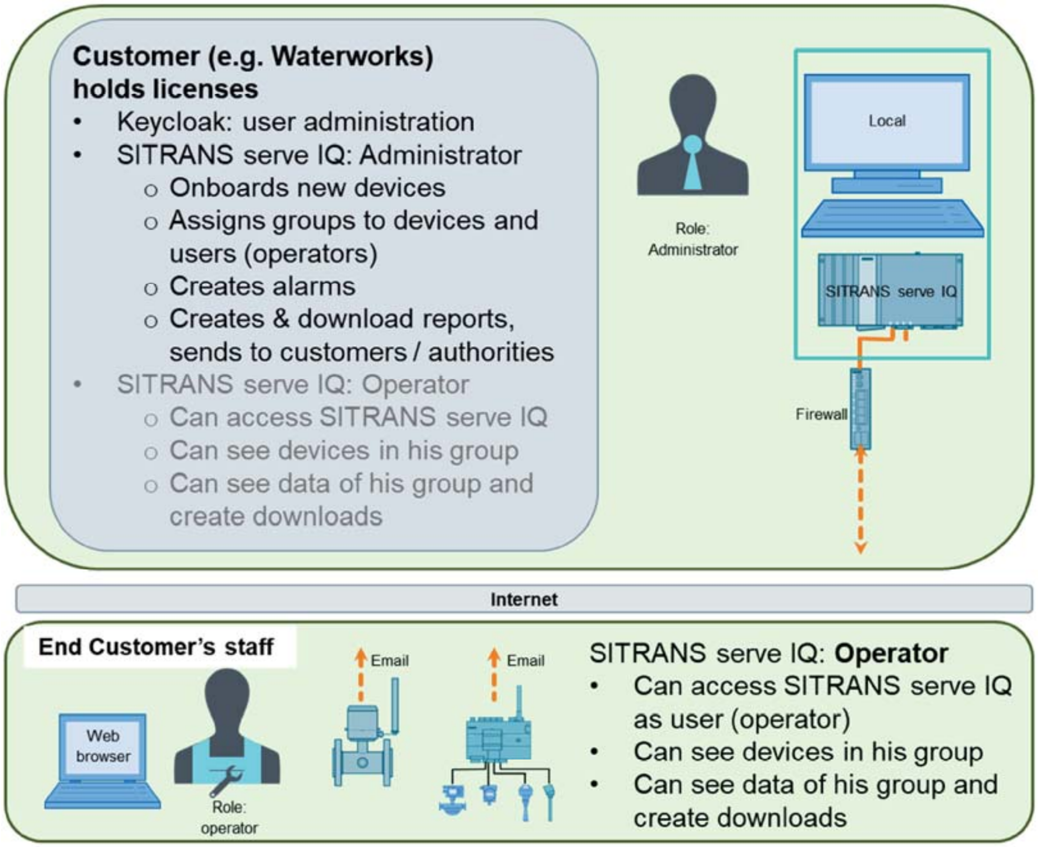
5.4 Keycloak: user administration for SITRANS serve IQ

5.4.1 Overview of user roles

The user accounts for SITRANS serve IQ must be created in Keycloak IAM before a user is able to access and operating SITRANS serve IQ.

Before continuing, please be advised about the three available user roles:

- administrator in Keycloak (Page 55)
- administrator of SITRANS serve IQ (Page 60) and
- operator of SITRANS serve IQ (Page 60)



Customer (e.g. Waterworks) holds licenses

- Keycloak: user administration
- SITRANS serve IQ: Administrator
  - o Onboards new devices
  - o Assigns groups to devices and users (operators)
  - o Creates alarms
  - o Creates & download reports, sends to customers / authorities
- SITRANS serve IQ: Operator
  - o Can access SITRANS serve IQ
  - o Can see devices in his group
  - o Can see data of his group and create downloads

End Customer's staff

SITRANS serve IQ: **Operator**

- Can access SITRANS serve IQ as user (operator)
- Can see devices in his group
- Can see data of his group and create downloads

The **administrator in Keycloak** can

- Add/remove administrators and operators of SITRANS serve IQ

We suggest keeping these administration rights of Keycloak strictly limited.

The **administrator of SITRANS serve IQ** can

- Set up and configure SITRANS serve IQ
- Add/edit/dis-able and enable/delete any/all devices
- Add/edit/delete templates.

- Add/edit/delete groups
- Allocate/remove access rights of operators to groups
- Add/edit/delete and acknowledge alarms

We suggest keeping these rights limited to responsible key personnel. An administrator in SITRANS serve IQ can delete devices, along with their data. Also, sensitive access information to e.g. the mailbox is visible to the administrators of SITRANS serve IQ.

The **operator of SITRANS serve IQ** can

- Access only the devices and alarms tabs in the assigned group
- View devices/groups that are assigned to the operator.
- View/acknowledge alarms from the assigned devices.

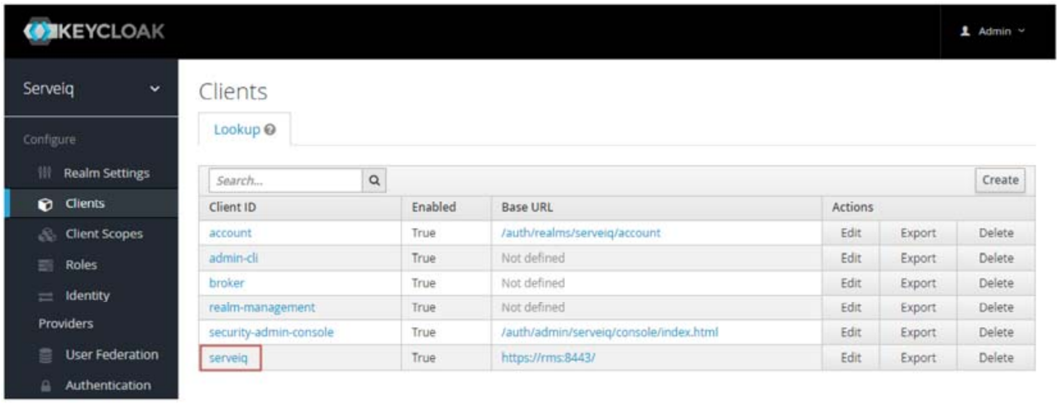
An operator in SITRANS serve IQ cannot harm or disable SITRANS serve IQ and is hence suitable for less trained colleagues.

Note

Due to legal constraints of licenses, only employees of the organization that is holding the licenses may be granted any access to SITRANS serve IQ. Though technically possible, it would be violation of license agreements and must be avoided.

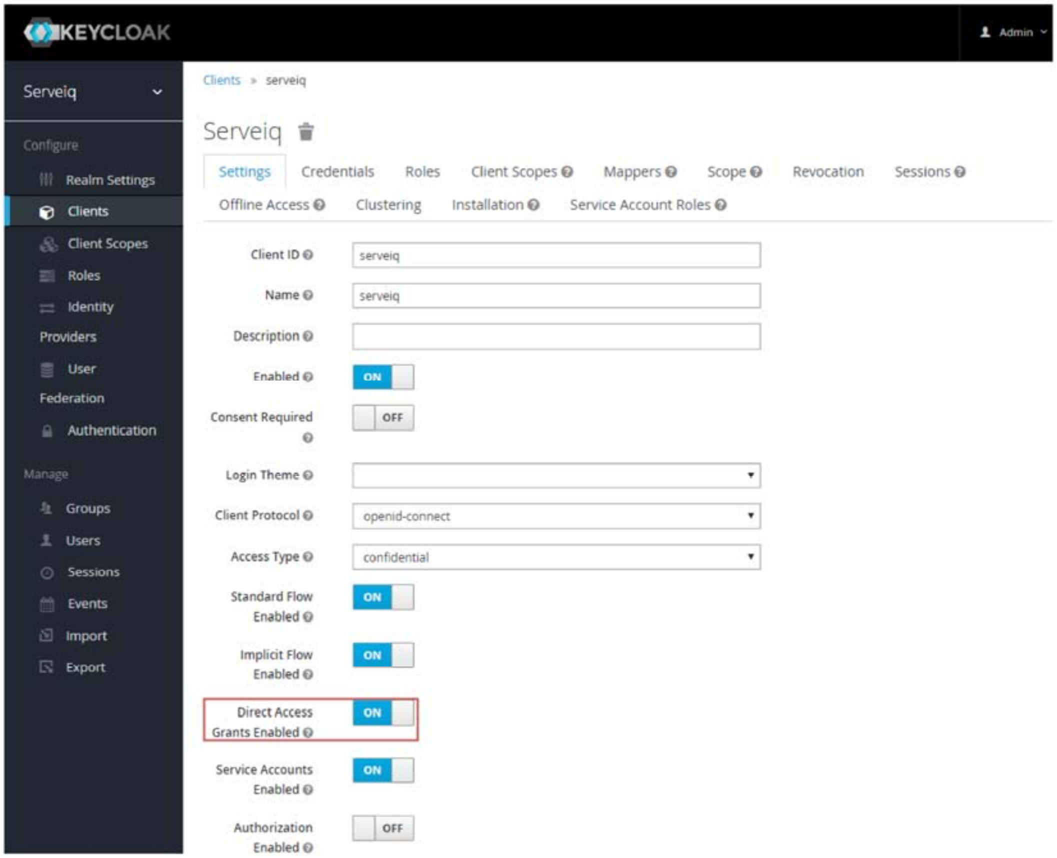
5.4.2 Creation of users

1. Under the **Configure** tab (left hand side), select **Clients** and click **serveiq**.



Client ID	Enabled	Base URL	Actions		
account	True	/auth/realms/serveiq/account	Edit	Export	Delete
admin-cli	True	Not defined	Edit	Export	Delete
broker	True	Not defined	Edit	Export	Delete
realm-management	True	Not defined	Edit	Export	Delete
security-admin-console	True	/auth/admin/serveiq/console/index.html	Edit	Export	Delete
serveiq	True	https://rms:8443/	Edit	Export	Delete

2. On the **serveiq** screen, select **Settings**.
   Switch the **Direct Access Grants Enabled** button **ON** and, click **Save**



Client ID: serveiq

Name: serveiq

Description:

Enabled: ON

Consent Required: OFF

Login Theme:

Client Protocol: openid-connect

Access Type: confidential

Standard Flow Enabled: ON

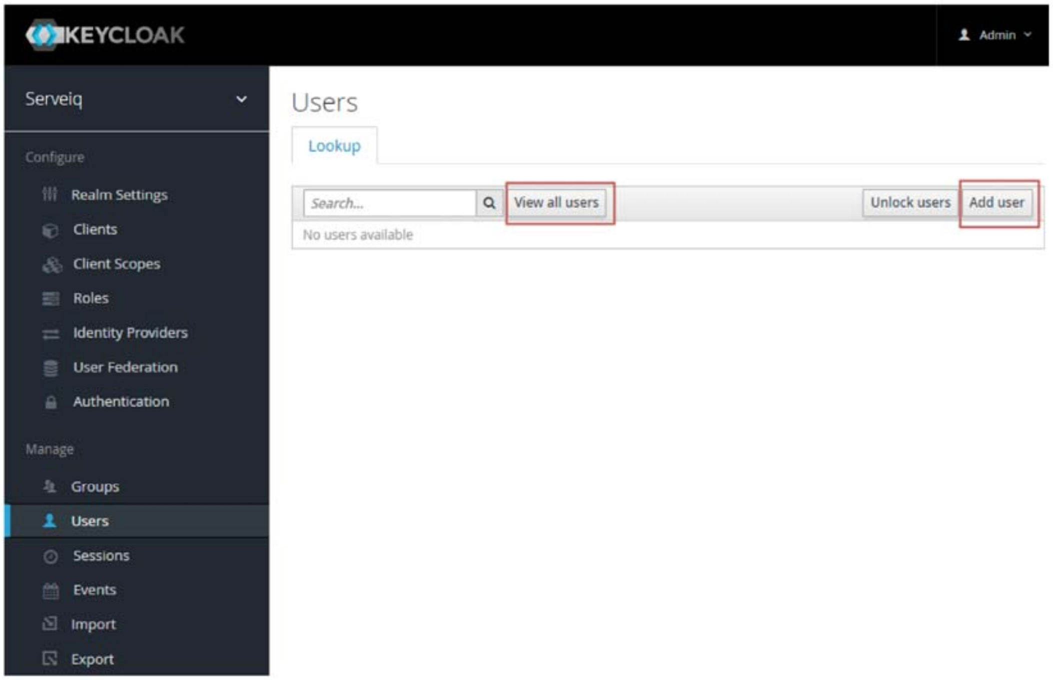
Implicit Flow Enabled: ON

Direct Access Grants Enabled: ON

Service Accounts Enabled: ON

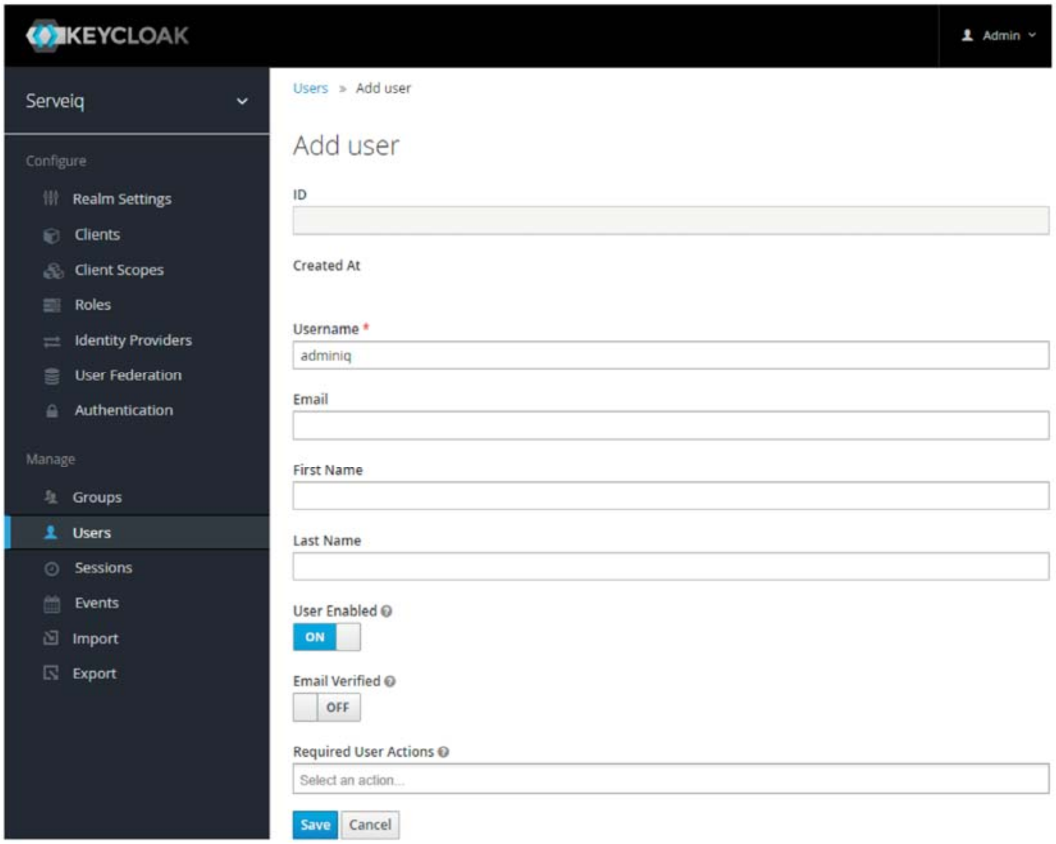
Authorization Enabled: OFF

3. Under the **Manage** tab (left hand side), select **Users**.



4. You can click View all users to show all the users created.
   To create a new user, you need to perform the following steps
   - Add the user (step 5)
   - Define a password (step 6)
   - Define level of user for SITRANS serve IQ (step 7)

5. Click Add user (on the right pane) to create new users. Provide the following information:
   - Please put the new username to tab Username
   - Set User Enabled to ON.
   - Required User Actions is optional. If Update Password is selected from the pull-down list of Required User Actions, the user is required to enter a new password at the first login to SITRANS serve IQ.
   - Click Save. The new username is created, and the menu is switched to the new user menu.



Add user

ID

Created At

Username *: adminiq

Email

First Name

Last Name

User Enabled: ON

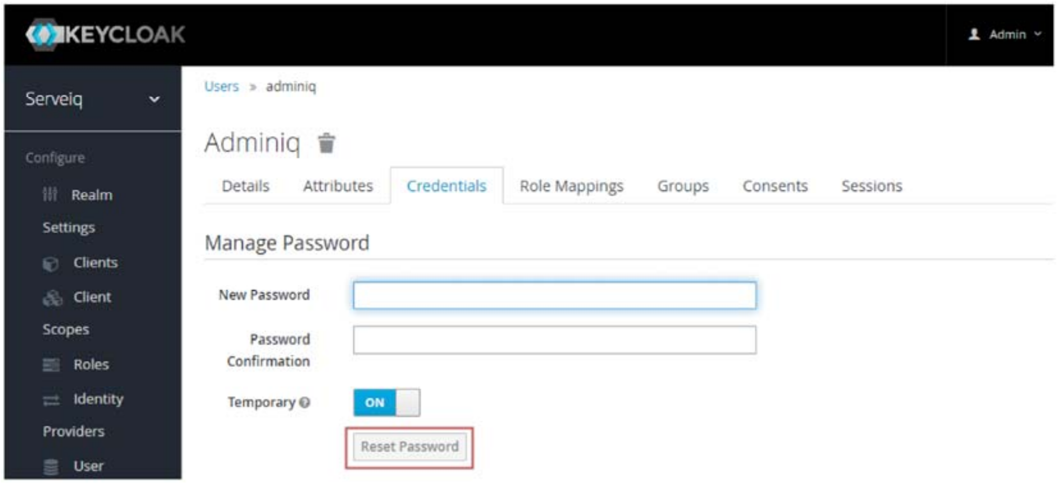
Email Verified: OFF

Required User Actions: Select an action...

Note

It is recommended to use impersonal user-names only. Also, do not enter any personal information (e.g. names) in order to ensure data privacy.

6. To define a password, click to Credentials the new user screen, create the new password and re-enter it.



Provide the following information:

- New Password
- Password Confirmation
- Temporary (If the Temporary switch is on, the new password can only be used once and the user will be asked to change the password after they have logged in.)

Click Reset Password and confirm Change password. The new password is created.

7. A role must be assigned to the new user. In SITRANS serve IQ, there are two roles:

- administrator of SITRANS serve IQ or
- operator in SITRANS serve IQ.

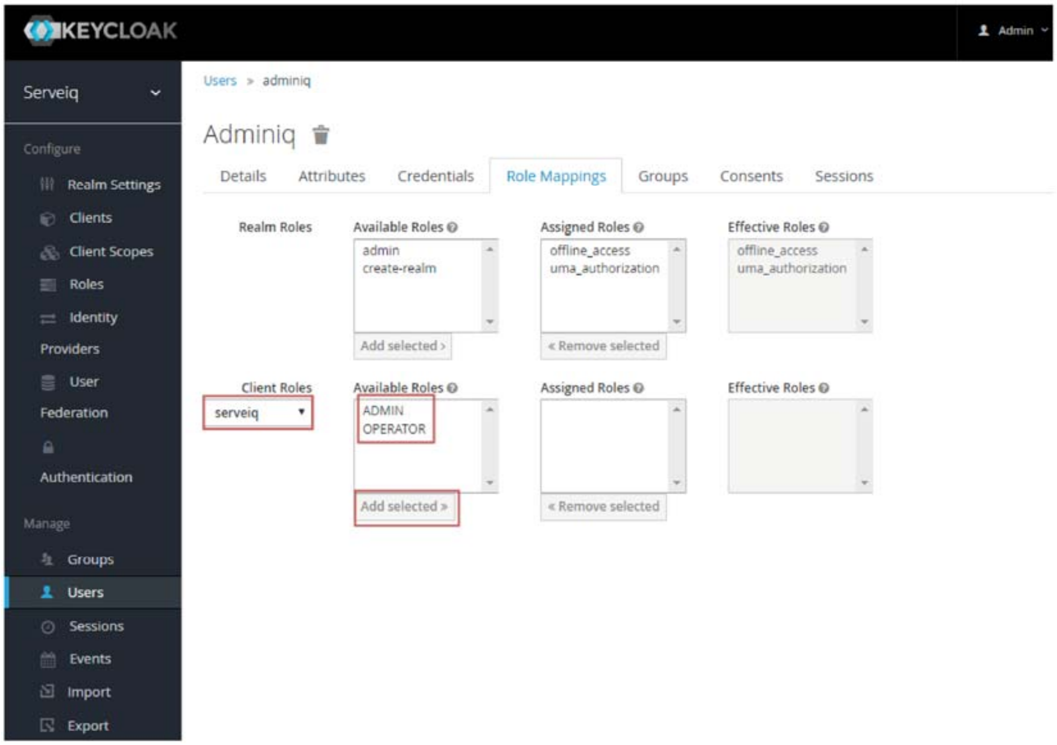
Note

You must add only one role for each user. Adding multiple roles will cause errors to occur.

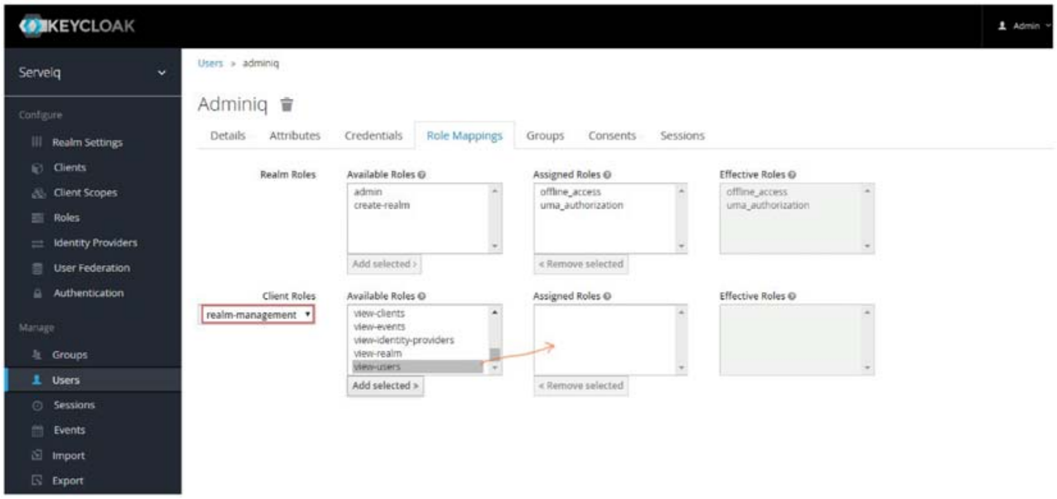
The roles are described in section below.

To specify a role for the new user:

- On the new user screen, click **Role Mappings**.
- From the **Client Roles** drop-down list, select **serveiq**. From the **Available Roles** list, select one proper role (**ADMIN** or **OPERATOR**) for the user. Click **Add selected** to assign the role to the user.

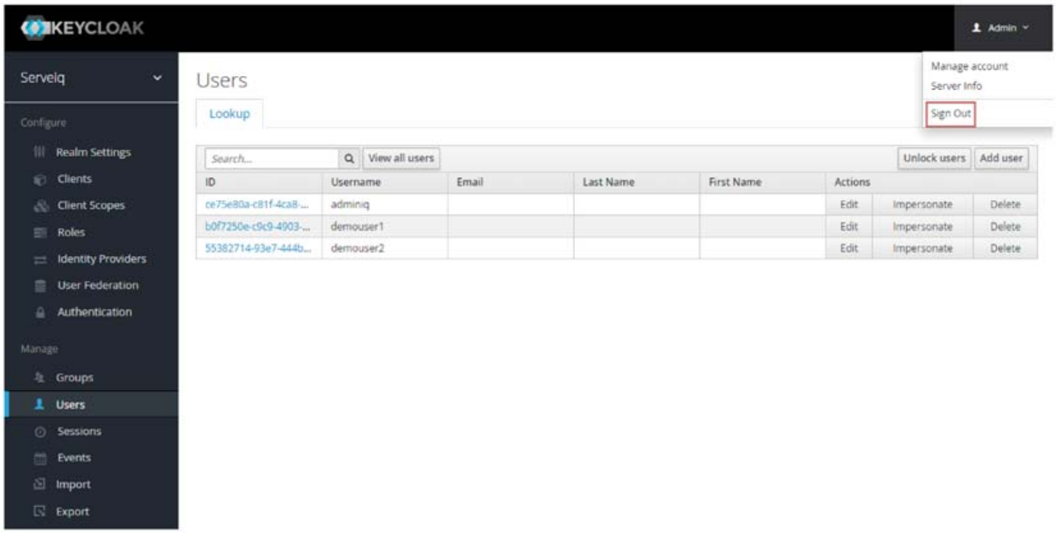


– From the **Client Roles** drop-down list, select **Realm-management**. From the available roles list, select **View-users** (applies to both admin and operator roles). Click **Add selected** to assign the role to the user. The View-user role should be assigned to all the users created for SITRANS serve IQ.



Repeat this procedure to add more users.

After all users have been added, sign out of Keycloak by clicking **Sign Out** on the top right corner.



ID	Username	Email	Last Name	First Name	Actions		
ce75e80a-c81f-4ca8-...	adminiq				Edit	Impersonate	Delete
b0f7250e-c9c9-4903-...	demouser1				Edit	Impersonate	Delete
55382714-93e7-444b...	demouser2				Edit	Impersonate	Delete

Note

To test, log-in to SITRANS serve IQ with the new user credentials:

- Start SITRANS serve IQ by typing in the web browser address box: https://rms:8443 or https://<IP-adress>:8443
- Enter the login credentials you created and click **Log In**.
  If you forgot the password, please reset the credentials in Keycloak as described above.

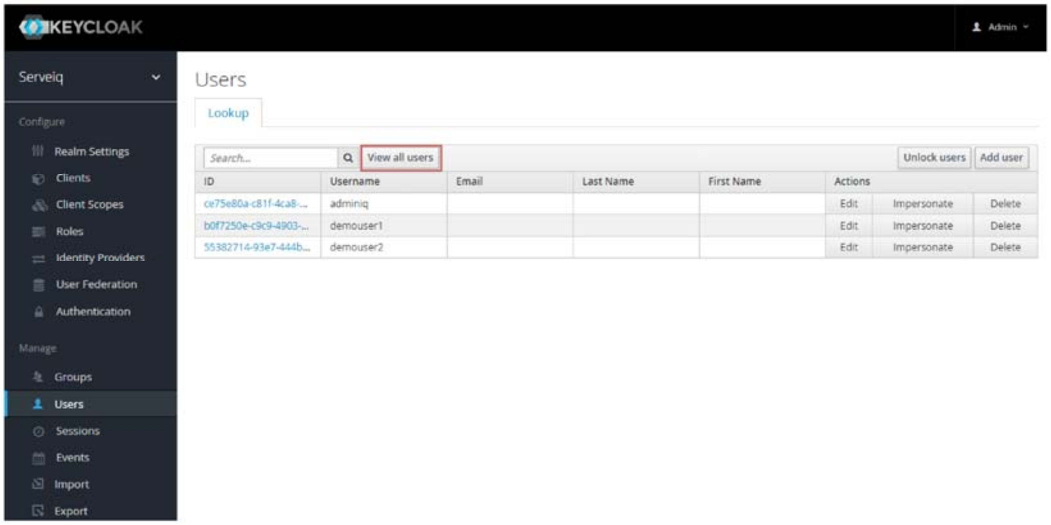
5.4.3 Search users

To manage a specific user:

- Click Manage and select Users.
- Click View all users to list every user in the system.

or

In the Search box type in a full or partial user name you want to search for in the user database.

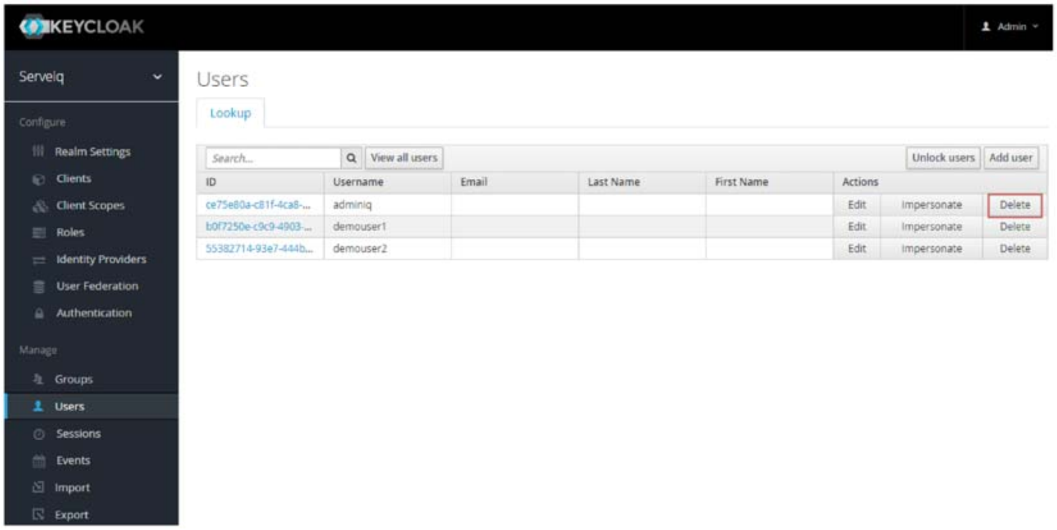


ID	Username	Email	Last Name	First Name	Actions		
ce75e80a-c81f-4ca8-...	adminiq				Edit	Impersonate	Delete
b0f7250e-c9c9-4903-...	demouser1				Edit	Impersonate	Delete
55382714-93e7-444b...	demouser2				Edit	Impersonate	Delete

5.4.4 Delete users

To delete a user:

- Click Manage and select Users.
- From the list of users displayed, select the user you intend to delete.
- Click Delete.
- Acknowledge the confirmation message.



ID	Username	Email	Last Name	First Name	Actions		
ce75e80a-c81f-4ca8-...	adminiq				Edit	Impersonate	Delete
b0f7250e-c9c9-4903-...	demouser1				Edit	Impersonate	Delete
55382714-93e7-444b...	demouser2				Edit	Impersonate	Delete

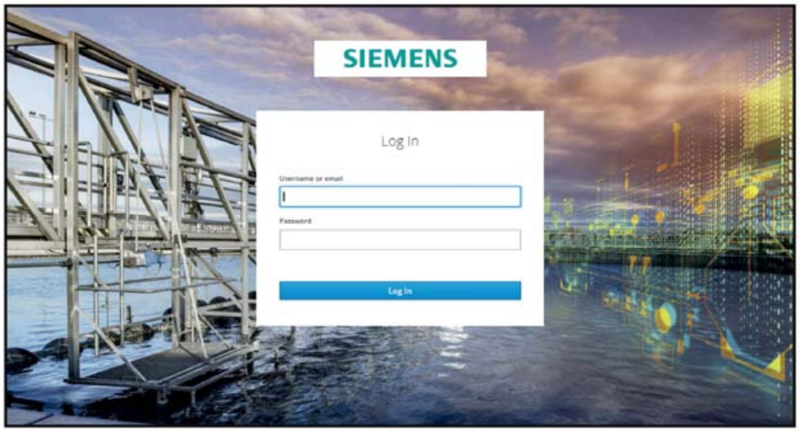
5.5 Logging into SITRANS serve IQ application

Before logging into SITRANS serve IQ, you need to start the application (see section 5.1 (Page 52)).

To log into SITRANS serve IQ, type in the web browser (Google Chrome) address box (depending on the previously described sections):

- https://rms:8443 or
- https://<IP-address>:8443 or
- https://<your domain>:8443

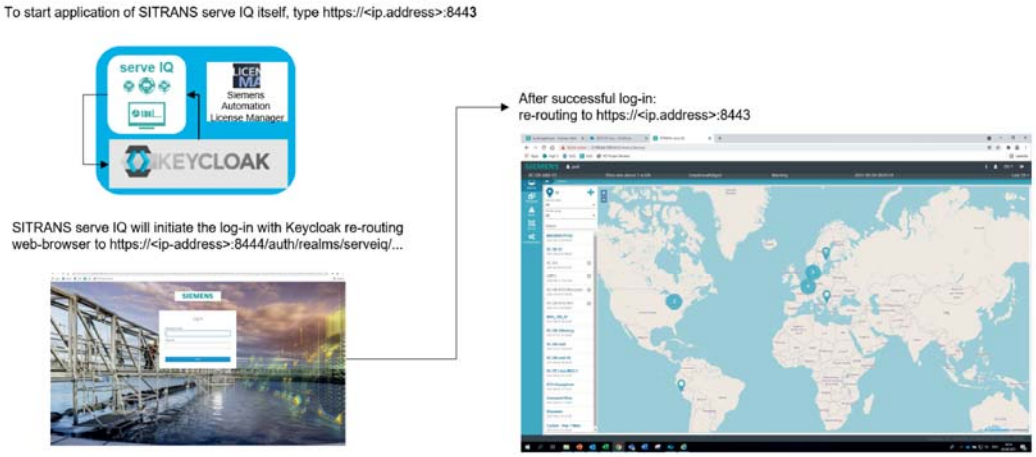
  The login page appears.



To log in, enter the login credentials of a user you have created in Keycloak and click Log In.

Note

To log into SITRANS serve IQ, ensure that you use the port 844**3** (note that the last digit is a three). The login itself will be handled in Keycloak, which results in changing port numbers as depicted below.


To start application of SITRANS serve IQ itself, type https://<ip.address>:8443

SITRANS serve IQ will initiate the log-in with Keycloak re-routing web-browser to https://<ip-address>:8444/auth/realms/serveiq/...

After successful log-in:
re-routing to https://<ip.address>:8443

Depending on the previously allocated user rights, you either are an operator or an administrator in SITRANS serve IQ.

For guidance on how to use SITRANS serve IQ, please continue with the handbook of SITRANS serve IQ https://www.siemens.com/SIOS/sitransserveiq (https://www.siemens.com/SIOS/sitransserveiq)

Before logging into SITRANS serve IQ, you need to start the application (see section 5.1).

Configuring connections 6

To configure the connections, you must have the role of administrator in SITRANS serve IQ.

6.1 Connection to an email account (IMAP)

The IMAP configuration allows to configure the mailbox to which the measurement data from individual devices are sent.

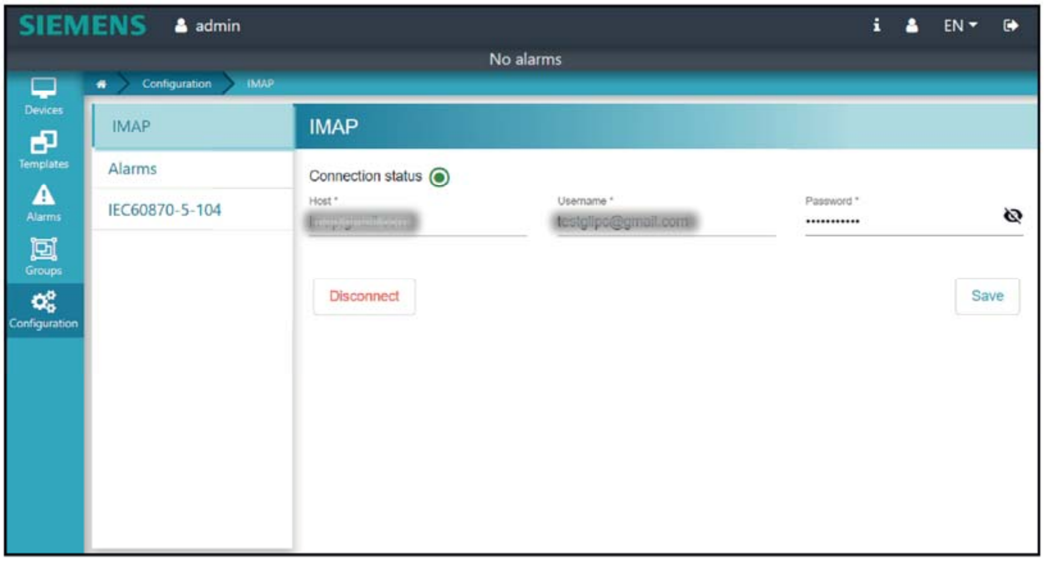
Note

The mailbox to collect measurement data must support IMAP protocol.

Perform the following steps to configure IMAP:

- On the main screen, select the **Configuration** tab.
- Click **IMAP**.

The IMAP configuration screen appears.



Connection status ●

Host * [redacted]

Username * [redacted]

Password * •••••••••••

- Specify the following configuration parameters:

Parameter	Description
Host (required) Password (required)	Enter the IMAP server address.
Username (required)	Enter the email address to which the measurement data is to be sent.
Password (required)	Enter the password of the email account.

- Click **Save**.
- Click **Connect**.
- The Connection status indicates the status of connection with IMAP system.
  - Green: Active connection
  - Red: Inactive connection

Note

An email address that is supported and managed by your company is recommended.

Free email services have been tested with SITRANS serve IQ. There may be other settings in the email service required for SITRANS serve IQ.

For example, some email provider require you to allow : "Let less secure apps access your account." Please consult with the email service provider if SITRANS serve IQ is unable to connect to account.

6.2 IEC 60870-5-104 configuration

The IEC 60870-5-104 configuration allows you to connect to a maximum of two redundant IEC 60870-5-104 systems.

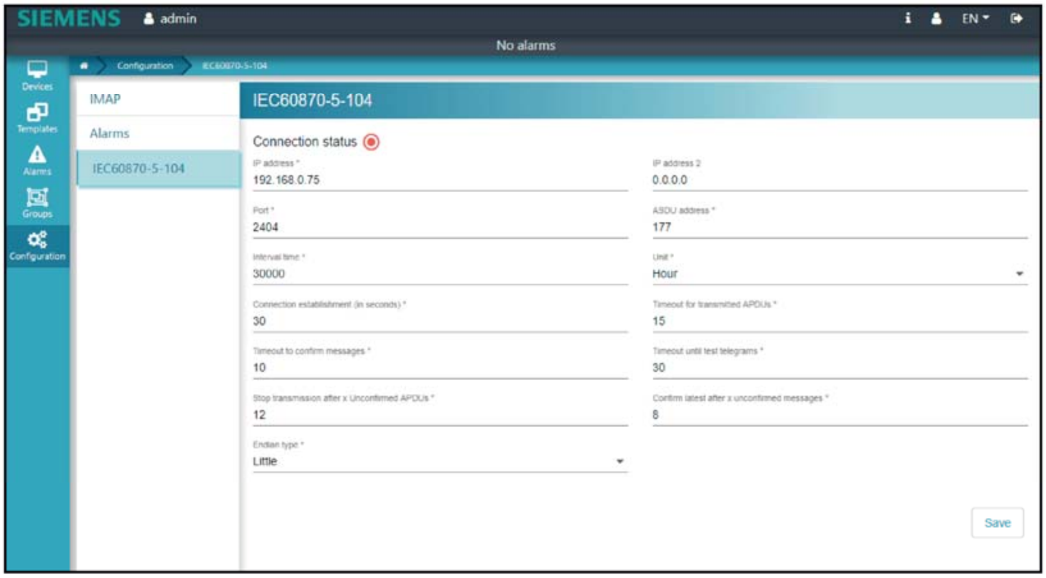
Note

- The IEC 60870-5-104 interface in SITRANS serve IQ is tested with Siemens SIMATIC WinCC. The compatibility with other SCADA system remains untested.
- SITRANS serve IQ will synchronize time with SCADA. The recommended synchronization interval is once a day.

Settings in SITRANS serve IQ

Perform the following steps to configure the IEC 60870-5-104 system:

- On the main screen, select theConfigurationtab.
- ClickIEC 60870-5-104.The IEC 60870-5-104 configuration screen appears.



IEC60870-5-104

Connection status

IP address * 192.168.0.75	IP address 2 0.0.0.0
Port * 2404	ASDU address * 177
Interval time * 30000	Unit * Hour
Connection establishment (in seconds) * 30	Timeout for transmitted APDUs * 15
Timeout to confirm messages * 10	Timeout until test telegrams * 30
Stop transmission after x Unconfirmed APDUs * 12	Confirm latest after x unconfirmed messages * 8
Endian type * Little	

- Specify the following configuration parameters:

Parameter	Description
IP address (required)	Enter the IP address of the first IEC 60870-5-104 server.
IP address 2	Optionally, enter the IP address of the second IEC 60870-5-104 server.
Port (required)	Enter the connection port value. The default connection port is 2404.
ASDU address (required)	Enter the ASDU address value.
Interval time (required)	Enter the interval time between the data sent to IEC 60870-5-104 system.
Unit (required)	Select a unit for the time interval: • Second • Minute • Hour
Connection establishment (in seconds) (required)	Enter the connection establishment time with the IEC 60870-5-104 system in seconds.
Timeout for transmitted APDUs (required)	Enter a timeout value for the transmitted APDUs.
Timeout to confirm messages (required)	Enter a timeout value to confirm messages.
Timeout until test telegrams (required)	Enter a timeout value untill test telegrams.
Stop transmission after x unconfirmed APDUs (required)	Enter a value for the number of unconfirmed APDUs after which the transmission is stopped.
Confirm latest after x unconfirmed messages (required)	Enter a value for the number of unconfirmed messages
Endian type (required)	Select one of the endian type: • Little • Big

- Click **Save**.
- The Connection status indicates the status of connection with IEC 60870-5-104 system.

  Green: Active connection

  Red: Inactive connection

Firewall configuration for communication with IEC 60870-5-104

To configure firewall for communication with IEC 60870-5-104:

- Click the **Start** icon and type Windows Defender firewall with Advanced Security. Click **Windows Defender firewall with Advanced Security** from the results to launch the console.
- Right-click **Inbound Rules** and select **New Rule**.

- On the **New Inbound Rule Wizard screen**, perform the following steps:
  - Under **Rule Type**, select **Port** and click **Next**.
  - Under **Protocols and Ports**, select **TCP protocol and Specific local ports** and type **2404** in the input box. Click **Next**.
  - Under **Action**, select **Allow the Connection** and click **Next**.
  - Under **Profile**, ensure all the options are selected and click **Next**.
  - Under **Name**, in the Name input box enter **SCADA** and click **Finish**.

  Right-click **Outbound Rules** and select **New Rule**.
- On the **New Outbound Rule Wizard** screen, perform the following steps:
  - Under **Rule Type**, select **Port** and click **Next**.
  - Under **Protocols and Ports**, select **TCP protocol and Specific local ports** and type **2404** in the input box. Click **Next**.
  - Under **Action**, select **Allow the Connection** and click **Next**.
  - Under **Profile**, ensure all options are selected and click **Next**.
  - Under **Name**, in the Name input box enter **SCADA** and click **Finish**.

  Close Windows Defender firewall with Advanced Security window.

Note

Please consult your local IT – department on how to configure the firewalls and rules. We recommend additional IT Security risk & threat analysis, e.g. in case the Windows Defender functionality was taken over by a third party firewall software.

Product documentation and support 7

7.1 Product documentation

Process instrumentation product documentation is available in the following formats:

- Certificates (http://www.siemens.com/processinstrumentation/certificates)
- Downloads (firmware, EDDs, software) (http://www.siemens.com/processinstrumentation/downloads)
- Catalog and catalog sheets (http://www.siemens.com/processinstrumentation/catalogs)
- Manuals (http://www.siemens.com/processinstrumentation/documentation)

  You have the option to show, open, save, or configure the manual.

  - "Display": Open the manual in HTML5 format
  - "Configure": Register and configure the documentation specific to your plant
  - "Download": Open or save the manual in PDF format
  - "Download as html5, only PC": Open or save the manual in the HTML5 view on your PC

You can also find manuals with the Mobile app at Industry Online Support (https://support.industry.siemens.com/cs/ww/en/sc/2067). Download the app to your mobile device and scan the device QR code.

Product documentation by serial number

Using the PIA Life Cycle Portal, you can access the serial number-specific product information including technical specifications, spare parts, calibration data, or factory certificates.

Entering a serial number

1. Open the PIA Life Cycle Portal (https://www.pia-portal.automation.siemens.com).
2. Select the desired language.
3. Enter the serial number of your device. The product documentation relevant for your device is displayed and can be downloaded.

To display factory certificates, if available, log in to the PIA Life Cycle Portal using your login or register.

Scanning a QR code

1. Scan the QR code on your device with a mobile device.
2. Click "PIA Portal".

To display factory certificates, if available, log in to the PIA Life Cycle Portal using your login or register.

7.2 Technical support

Technical support

If this documentation does not completely answer your technical questions, you can enter a Support Request (http://www.siemens.com/automation/support-request).

For help creating a support request, view this video here (www.siemens.com/opensr).

Additional information on our technical support can be found at Technical Support (http://www.siemens.com/automation/csi/service).

Service & support on the Internet

In addition to our technical support, Siemens offers comprehensive online services at Service & Support (http://www.siemens.com/automation/serviceandsupport).

Contact

If you have further questions about the device, contact your local Siemens representative at Personal Contact (http://www.automation.siemens.com/partner).

To find the contact for your product, go to "all products and branches" and select "Products & Services > Industrial automation > Process instrumentation".

Contact address for business unit:
Siemens AG
Digital Industries
Process Automation
Östliche Rheinbrückenstr. 50
76187 Karlsruhe, Germany

Appendix 8

8.1 Uninstall SITRANS serve IQ

To remove the software use the Windows Uninstall or change a program feature:

1. Click **Start > Control Panel > Programs > Programs and Features**.
2. Right-click **SITRANS serve IQ** and select **Uninstall** to remove all the SITRANS serve IQ components.

Note

The serve IQ uninstallation doesn't remove Docker and ALM programs. You can uninstall them manually. However, other programs requiring Docker or ALM will be affected if Docker or ALM is uninstalled.

8.2 List of Abbreviations

Abbreviation/Symbol	Description
ALM	Application Lifecycle Management
APDU	Application Protocol Data Unit
CA	Certificate Authority
CSV	Comma Separated Values (pseudo file format used to store tabular data in plain text form)
HDD	Hard Disk Drive
HTTPS	Hypertext Transfer Protocol Secure
IAM	Identity and Access Management
IEC	International Electrotechnical Commission
IMAP	Internet Message Access Protocol
IP	Internet Protocol
MAG	Magnetic-inductive flow meters
RAM	Random Access Memory
RMS	Remote Mail Server
RTU	Remote Terminal Units
SCADA	Supervisory Control And Data Acquisition
SMTP	Simple Mail Transfer Protocol
URL	Uniform Resource Locator
WCM	Wireless Communication Module

Glossary

IEC

The International Electrotechnical Commission is an international standards organization that prepares and publishes International Standards for all electrical, electronic and related technologies

IEC 60870-5-104

IEC 60870 part 5 is one of the IEC 60870 set of standards which define systems used for telecontrol (supervisory control and data acquisition) in electrical engineering and power system automation applications. Part 5 provides a communication profile for sending basic telecontrol messages between two systems, which uses permanent directly connected data circuits between the systems.

IEC 60870-5-104 (IEC 104) protocol is an extension of IEC 101 protocol with the changes in transport, network, link & physical layer services to suit the complete network access

IMAP

(Internet Message Access Protocol) is a standard email protocol that stores email messages on a mail server, but allows the end user to view and manipulate the messages as though they were stored locally on the end user's computing device(s).

Keycloak IAM

Keycloak is an Open Source Identity and Access Management (IAM) solution for advanced applications and services.

MAG8000 with WCM

Battery driven flow meter with integral Wireless Communication Module (WCM)

RTU30xxC

RTU30xxC series are energy-self-sufficient low-power remote terminal units (RTUs).

SIMATIC RTU30xxC and sensors

Remote terminal units (RTUs) and sensors responsible for collection and transmission of level, flow rate, filling height, temperature and, pressure without mains power.

Index