SIEMENS

SINUMERIK

Manage MyMachines /Remote

Function Manual

Introduction 1

Security instructions 2

System requirements 3

Setting up the SINUMERIK control system for Manage MyMachines /Remote 4

Integrating Insights Hub 5

Working with Manage MyMachines /Remote 6

Setting up Manage MyMachines /Remote Service Client 7

Using MyMachines / Remote Service Client 8

Disconnecting a SINUMERIK control from Insights Hub 9

Troubleshooting when onboarding 10

Appendix A

Valid for control:
SINUMERIK 840D sl/ 840DE sl/ 828D
SINUMERIK ONE

Software
Manage MyMachines /Remote, Version 01.06.04.00

11/2023
A5E44039359B AU

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

A5E44039359B AU
Ⓟ 11/2023 Subject to change

Copyright © Siemens AG 2018 - 2023.
All rights reserved

Table of contents

1 Introduction 7

1.1 About Manage MyMachines /Remote 7

1.2 About this documentation 7

1.3 Documentation on the internet 9

1.3.1 Documentation overview Manage MyMachines/Remote 9

1.4 Feedback on the technical documentation 9

1.5 mySupport documentation 9

1.6 Service and Support 10

1.7 OpenSSL 11

1.8 General Data Protection Regulation 11

2 Security instructions 13

2.1 Fundamental safety instructions 13

2.1.1 General safety instructions 13

2.1.2 Warranty and liability for application examples 13

2.1.3 Cybersecurity information 13

2.2 Security instructions in Insights Hub documentation 15

2.3 Data management, confidentiality and encryption 15

3 System requirements 17

4 Setting up the SINUMERIK control system for Manage MyMachines /Remote 25

4.1 Activating the data acquisition 25

4.2 Checking and updating the versions 27

4.2.1 Displaying version data 27

4.2.2 Installing a SINUMERIK 828D update 28

4.2.3 Client update under Windows 30

4.2.4 Client update under Linux 34

4.3 SINUMERIK Integrate 38

4.3.1 Activating the SINUMERIK Integrate client 38

4.3.2 Activating SINUMERIK Integrate use 39

4.4 SINUMERIK 840D sl 40

4.4.1 Configuring the URL and proxy 40

4.4.2 Install the registration key on a SINUMERIK control system 43

4.4.3 Create drive 46

4.5 SINUMERIK 828D 47

4.5.1 Configuring the URL and proxy 47

4.5.2 Install the registration key on a SINUMERIK control system 50

4.6 Adapting SINUMERIK Operate 52

4.6.1 Exchanging a certificate (optional) ... 52
4.6.2 Activating logs for troubleshooting ... 55
4.7 PCU retrofit ... 56
5 Integrating Insights Hub ... 61
5.1 Logging in to Insights Hub ... 61
5.2 Icons and buttons in Insights Hub ... 63
5.3 Managing users ... 66
5.4 Asset Manager ... 67
5.4.1 Overview ... 67
5.4.2 Opening the Asset Manager ... 68
5.4.3 Creating an asset type ... 69
5.4.4 Creating an Asset ... 71
5.5 Shopfloor Management Application ... 74
5.5.1 Overview ... 74
5.5.2 Billing model UTS (Usage Transparency Service) ... 75
5.5.2.1 Activating Manage MyMachines /Remote ... 75
5.5.3 Billing model PB (Package Builder) ... 81
5.5.3.1 Activating Manage MyMachines /Remote ... 81
5.5.4 Changing the billing model ... 83
5.5.5 Calling a machine configuration ... 84
5.6 Connecting SINUMERIK controls with Insights Hub ... 84
6 Working with Manage MyMachines /Remote ... 89
6.1 Open Manage MyMachines /Remote ... 89
6.2 Machine Configuration ... 91
6.3 Download remote service client ... 94
6.4 Download certificate ... 96
6.5 Remote sessions ... 98
6.5.1 Overview ... 98
6.5.2 Starting a remote session as a SE ... 99
6.5.3 Joining a remote session ... 103
6.5.4 Managing remote sessions ... 104
6.5.5 Configuring the session log settings ... 111
6.5.6 Evaluating and editing session information ... 112
6.5.7 Exporting session information ... 116
6.5.8 Remote sessions with Manage MyMachines ... 119
6.5.8.1 Start new remote session ... 120
6.5.8.2 Joining a remote session ... 122
6.6 Service Dashboard ... 125
6.7 Using the calendar function ... 128
7 Setting up Manage MyMachines /Remote Service Client ... 131
7.1 Setting up Manage MyMachines /Remote - Machine operators (MO) ... 131
7.1.1 Overview ... 131
7.1.2 Installing Manage MyMachines /Remote Service Client MO (IPC or PCU) ... 132

7.1.3 Entering the address of a proxy server ... 140
7.1.4 Integrating an OEMFrame application into HMI sl ... 141
7.1.5 Silent Installation ... 142

7.2 Setting up Manage MyMachines /Remote - service engineer (SE) ... 144
7.2.1 Installing Manage MyMachines /Remote Service Client SE ... 144
7.2.2 Entering the address of a proxy server ... 153

8 Using MyMachines /Remote Service Client ... 155

8.1 Overview of the functions ... 155

8.2 User roles and operator interface ... 156

8.3 Joining a remote session as MO (PCU/NCU) ... 157

8.4 Joining a remote session as MO (IPC) ... 160

8.5 Conducting a remote session via VPN (IPC) ... 163

8.6 Desktop sharing (SINUMERIK Integrate Client) ... 168

8.7 Desktop sharing (IPC / PCU) ... 170

8.8 Transferring files ... 173

8.9 Remote STEP 7 ... 183
8.9.1 Setting-up the Internet connection with SIMATIC Manager ... 183
8.9.2 Setting up a connection with the TIA Portal via the Internet ... 187

8.10 Transferring the conference leadership ... 192

8.11 Terminating the remote session ... 196

8.12 Additional functions ... 198
8.12.1 Network interruption ... 198
8.12.2 Setting the login data ... 198
8.12.3 Setting file transfer ... 199
8.12.4 Setting the language ... 201
8.12.5 Setting the log file ... 202

9 Disconnecting a SINUMERIK control from Insights Hub ... 205

9.1 Overview ... 205

9.2 Disconnecting a SINUMERIK control from Insights Hub ... 205

9.3 Deactivating use of SINUMERIK Integrate ... 207

10 Troubleshooting when onboarding ... 209

10.1 SINUMERIK controls ... 210
10.1.1 Preconditions ... 210
10.1.1.1 Checking the network configuration ... 210
10.1.1.2 Checking that SINUMERIK Integrate has been enabled ... 212
10.1.1.3 Checking that SINUMERIK Integrate has been activated ... 214
10.1.1.4 Checking proxy settings ... 215
10.1.1.5 Checking the SINUMERIK Integrate URL ... 219
10.1.1.6 Checking the network connection ... 222
10.1.1.7 Checking directory "boot_job" ... 222
10.1.1.8 Checking the asset type in Insights Hub ... 222
10.1.1.9 Checking the existence of onboard.key ... 222

10.1.2 Resolving known faults 222
10.1.2.1 Onboard key exists but onboarding does not start 222
10.1.2.2 Onboarding starts, cert.key is created; however, onboard.key does not disappear 223
10.1.2.3 No boot script available 224
10.1.3 More information 224

A Appendix 227

A.1 Preconditions for the Shopfloor Management Application 227

A.2 List of abbreviations 229

Index 231

Introduction 1

1.1 About Manage MyMachines /Remote

Insights Hub

Insights Hub is a cloud-based, open IoT operating system from Siemens that connects your machines and physical infrastructure with the digital world. This gives you a complete overview of your data at all times.

Several Insights Hub-based applications are available – the "Manage MyMachines for Industrial Operations X Cloud".

Manage MyMachines /Remote

With "Manage MyMachines /Remote", you can provide efficient and low-cost support for machine tools and production equipment via the Internet.

In the event of a fault, the service organization of the machine manufacturer has fast access to important control data and diagnostic functions. In that way, the machine manufacturer or maintenance department can immediately analyze the current condition of the machine tool in which a fault occurred.

Remote Sessions (remote access) helps you avoid time-consuming on-site service assignments and prepare them better. Machine manufacturers can reduce their warranty costs while providing more efficient service support.

1.2 About this documentation

Overview

This document describes the following:

How you connect Insights Hub to the SINUMERIK control system (machine tool).
More information can be found at: Setting up the SINUMERIK control system for Manage MyMachines /Remote (Page 25).

The functionality of Manage MyMachines for Industrial Operations X Cloud "Manage MyMachines /Remote"
More information can be found at: Working with Manage MyMachines /Remote (Page 89)

Insights Hub

Insights Hub is a cloud-based, open IoT operating system from Siemens that connects your machines and physical infrastructure with the digital world. This gives you a complete overview of your data at all times.

Several Insights Hub-based applications are available – the "Manage MyMachines for Industrial Operations X Cloud".

Target group

This publication is intended for:

- Project engineers
- Technology experts (from machine manufacturers)
- Commissioning engineers (systems/machines)
- Programmer-users

Benefits

The Function Manual describes the functions in such a way that the target group is aware of them and can select them. The manual provides the target group with the information required to implement the functions.

Standard scope

This documentation only describes the functionality of the standard version. This may differ from the scope of the functionality of the system that is actually supplied. Please refer to the ordering documentation only for the functionality of the supplied drive system.

It may be possible to execute other functions in the system which are not described in this documentation. This does not, however, represent an obligation to supply such functions with a new control or when servicing.

For reasons of clarity, this documentation cannot include all of the detailed information on all product types. Further, this documentation cannot take into consideration every conceivable type of installation, operation and service/maintenance.

The machine manufacturer must document any additions or modifications they make to the product themselves.

Websites of third-party companies

This document may contain hyperlinks to third-party websites. Siemens is not responsible for and shall not be liable for these websites and their content. Siemens has no control over the information which appears on these websites and is not responsible for the content and information provided there. The user bears the risk for their use.

1.3 Documentation on the internet

1.3.1 Documentation overview Manage MyMachines/Remote

More information about Manage MyMachines for Industrial Operations X Cloud is provided at: Documentation in Insights Hub (https://siemens.mindsphere.io/en/docs/Manage-MyMachines-Remote)

As well as the manuals, you will also find data sheets and FAQs at the following link: Insights Hub (https://plm.sw.siemens.com/en-US/insights-hub/).

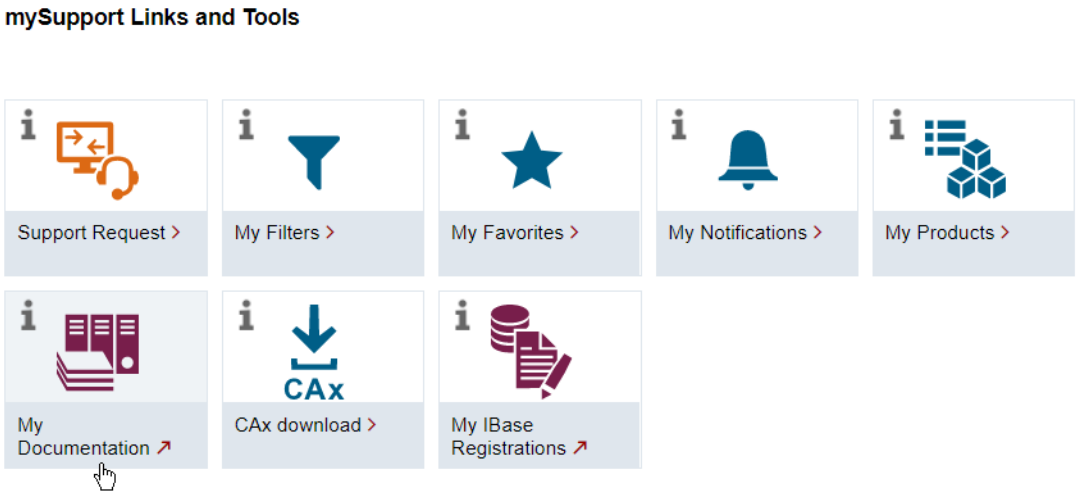
1.4 Feedback on the technical documentation

If you have any questions, suggestions, or corrections regarding the technical documentation published in the Siemens Industry Online Support, use the link "Give feedback" link which appears at the end of the entry.

1.5 mySupport documentation

With the "mySupport documentation" web-based system you can compile your own individual documentation based on Siemens content, and adapt it for your own machine documentation.

To start the application, click on the "My Documentation" tile on the "mySupport links and tools" (https://support.industry.siemens.com/cs/ww/en/my) portal page:



The configured manual can be exported in RTF, PDF or XML format.

Note

Siemens content that supports the mySupport documentation application can be identified by the presence of the "Configure" link.

1.6 Service and Support

Product support

You can find more information about products on the internet:

Product support (https://support.industry.siemens.com/cs/ww/en/)

The following is provided at this address:

- Up-to-date product information (product announcements)
- FAQs (frequently asked questions)
- Manuals
- Downloads
- Newsletters with the latest information about your products
- Global forum for information and best practice sharing between users and specialists
- Local contact persons via our Contacts at Siemens database (→ "Contact")
- Information about field services, repairs, spare parts, and much more (→ "Field Service")

Technical support

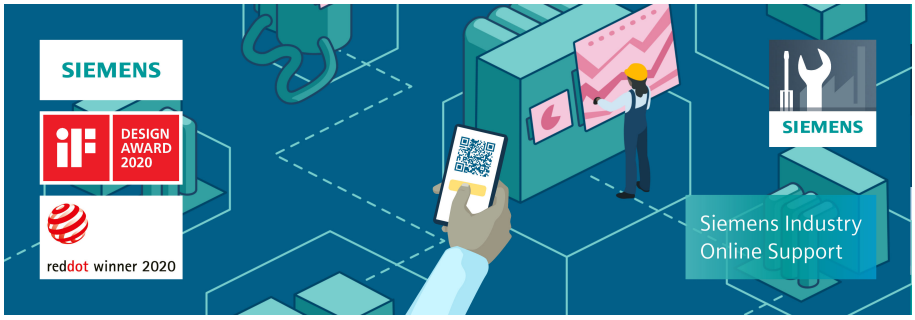
Country-specific telephone numbers for technical support are provided on the internet at address (https://support.industry.siemens.com/cs/ww/en/sc/4868) in the "Contact" area.

If you have any technical questions, please use the online form in the "Support Request" area.

Training

You can find information on SITRAIN at the following address (https://www.siemens.com/sitrain).
SITRAIN offers training courses for automation and drives products, systems and solutions from Siemens.

Siemens support on the go



With the award-winning "Industry Online Support" app, you can access more than 300,000 documents for Siemens Industry products – any time and from anywhere. The app can support you in areas including:

- Resolving problems when implementing a project
- Troubleshooting when faults develop
- Expanding a system or planning a new system

Furthermore, you have access to the Technical Forum and other articles from our experts:

- FAQs
- Application examples
- Manuals
- Certificates
- Product announcements and much more

The "Industry Online Support" app is available for Apple iOS and Android.

1.7 OpenSSL

This product can contain the following software:

- Software developed by the OpenSSL project for use in the OpenSSL toolkit
- Cryptographic software created by Eric Young.
- Software developed by Eric Young

You can find more information on the internet:

- OpenSSL (https://www.openssl.org)
- Cryptsoft (https://www.cryptsoft.com)

1.8 General Data Protection Regulation

Siemens observes standard data protection principles, in particular the data minimization rules (privacy by design).

For this product, this means:

The product does not process or store any personal data, only technical function data (e.g. time stamps). If the user links this data with other data (e.g. shift plans) or if he/she stores person-related data on the same data medium (e.g. hard disk), thus personalizing this data, he/she must ensure compliance with the applicable data protection stipulations.

Security instructions 2

2.1 Fundamental safety instructions

2.1.1 General safety instructions

⚠ WARNING

Danger to life if the safety instructions and residual risks are not observed

If the safety instructions and residual risks in the associated hardware documentation are not observed, accidents involving severe injuries or death can occur.

- Observe the safety instructions given in the hardware documentation.
- Consider the residual risks for the risk evaluation.

⚠ WARNING

Malfunctions of the machine as a result of incorrect or changed parameter settings

As a result of incorrect or changed parameterization, machines can malfunction, which in turn can lead to injuries or death.

- Protect the parameterization against unauthorized access.
- Handle possible malfunctions by taking suitable measures, e.g. emergency stop or emergency off.

2.1.2 Warranty and liability for application examples

Application examples are not binding and do not claim to be complete regarding configuration, equipment or any eventuality which may arise. Application examples do not represent specific customer solutions, but are only intended to provide support for typical tasks.

As the user you yourself are responsible for ensuring that the products described are operated correctly. Application examples do not relieve you of your responsibility for safe handling when using, installing, operating and maintaining the equipment.

2.1.3 Cybersecurity information

Siemens provides products and solutions with industrial cybersecurity functions that support the secure operation of plants, systems, machines and networks.

In order to protect plants, systems, machines and networks against cyber threats, it is necessary to implement – and continuously maintain – a holistic, state-of-the-art industrial cybersecurity concept. Siemens' products and solutions constitute one element of such a concept.

Customers are responsible for preventing unauthorized access to their plants, systems, machines and networks. Such systems, machines and components should only be connected to an enterprise network or the internet if and to the extent such a connection is necessary and only when appropriate security measures (e.g. firewalls and/or network segmentation) are in place.

For additional information on industrial cybersecurity measures that may be implemented, please visit
https://www.siemens.com/global/en/products/automation/topic-areas/industrial-cybersecurity.html.

Siemens' products and solutions undergo continuous development to make them more secure. Siemens strongly recommends that product updates are applied as soon as they are available and that the latest product versions are used. Use of product versions that are no longer supported, and failure to apply the latest updates may increase customer's exposure to cyber threats.

To stay informed about product updates, subscribe to the Siemens Industrial Cybersecurity RSS Feed under
https://new.siemens.com/global/en/products/services/cert.html.

Further information is provided on the Internet:

Industrial Security Configuration Manual (https://support.industry.siemens.com/cs/ww/en/view/108862708)

⚠ WARNING

Unsafe operating states resulting from software manipulation

Software manipulations, e.g. viruses, Trojans, or worms, can cause unsafe operating states in your system that may lead to death, serious injury, and property damage.

- Keep the software up to date.
- Incorporate the automation and drive components into a state-of-the-art, integrated industrial cybersecurity concept for the installation or machine.
- Make sure that you include all installed products in the integrated industrial cybersecurity concept.
- Protect files stored on exchangeable storage media from malicious software by with suitable protection measures, e.g. virus scanners.
- Carefully check all cybersecurity-related settings once commissioning has been completed.

2.2 Security instructions in Insights Hub documentation

Take into consideration the content of the following Insights Hub documentation:

- MindSphere security model (https://assets.new.siemens.com/siemens/assets/api/uuid:6b876b5e-5594-4da4-90e0-e9e0c6f1f1e1/siemens-plm-mindsphere-security-model-wp-75966-a7.pdf)
- MindSphere architecture (https://documentation.mindsphere.io/MindSphere/concepts/concept-architecture.html)
- Authentication & Authorization (https://documentation.mindsphere.io/MindSphere/concepts/concept-authentication.html)

Note

Applying the defense-in-depth concept

To protect industrial plants and systems comprehensively against cyber attacks, measures must be applied simultaneously
at all levels. From the operational level up to the field level – from
access control to copy protection. Therefore, apply the "Defense in depth" protection concept to avoid security risks in your environment before
setting up the OPC UA server.

Note in particular that the company network must not be connected to the Internet without suitable
protective measures.

More information on the defense-in-depth concept, protective measures and general Industrial Security can be found in the Industrial Security Configuration Manual (https://support.industry.siemens.com/cs/ww/de/view/108862708).

2.3 Data management, confidentiality and encryption

HTTPS with TLS 1.2 is used to establish all of the communications between the individual components.

Furthermore, when transferring data from your machine to Insights Hub, "Manage MyMachines /Remote" uses customer-specific OAUTH-2.0 tokens, which are provided by Insights Hub.

System requirements

3

Hardware and operating software

The connection is established via the "Manage MyMachines /Remote Service Client".

The SINUMERIK Integrate Client is required if you wish to use the integrated Manage MyMachines /Remote Client in the SINUMERIK Integrate Client. It may be necessary to upgrade this component.

SINUMERIK 840D sl

SINUMERIK Integrate client software version	Operating software SINUMERIK Operate version	Hardware version	Operating system
2.0.13 2.0.14	4.5 SP4, HF1, 2, 3, 4	NCU 7x0.3 (B) PN	Linux
2.0.16 2.0.19 2.0.22	4.5 SP5, HF1, 3, 5 4.5 SP6, HF2, 3, 5, 7, 8, 10, 11, 13 14, 15, 16, 17, 18, 19	PCU 50.5 IPC 427E IPC 477E	Windows 7 Windows 10
	4.5 SP4, HF1, 2, 3, 4 4.5 SP6, HF1, 3, 5, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18	NCU 7x0.3 (B) PN	Linux
3.0.13	4.7 SP1, HF1	NCU 7x0.3 (B) PN	Linux
3.0.14 3.0.16 3.0.19 3.0.22	4.7 SP2, HF1, 3, 4 4.7 SP3, HF1, 2, 3 4.7 SP4, HF1, 4, 5, 6 4.7 SP5, HF1 4.7 SP6, HF1, 3, 4, 5, 6, 7 4.7 SP7, HF14 4.8 SP1, HF1, 2, 3 4.8 SP2, HF1, 3 4.8 SP3, HF1 4.8 SP4, HF1, 3, 4, 6, 8 4.8 SP5, HF5, 6 4.8 SP6, HF1, 3, 4, 5 4.8 SP7	PCU 50.5 IPC 427E IPC 477E	Windows 7 Windows 10
4.0.16	4.92, HF3	NCU 7x0.3 (B) PN	Linux
4.0.19 4.0.20 4.0.22	4.93, HF1, 2, 3, 5, 6 4.94, HF3, 4 4.95 4.95, HF1 4.95 SP1, HF1 4.95 SP1, HF3	PCU 50.5 IPC 427E IPC 477E	Windows 7 Windows 10

SINUMERIK ONE

SINUMERIK Integrate client software version	Operating software SINUMERIK Operate version	Hardware version	Operating system
4.0.15	6.13, HF1, 4, 6	NCU 1750	Linux
4.0.16	6.14, HF3	NCU 1740	
4.0.18	6.15, HF1	NCU 1760	
4.0.19	6.15 SP1	IPC 427E	Windows 10
4.0.20	6.15 SP1, HF1		
4.0.22	6.15 SP1, HF3		

Client software version, SINUMERIK Integrate	Operating software version, SINUMERIK Operate	Hardware version	Operating system
4.0.22	1.15	MCU 1720	Windows 10 IoT Enterprise LTSB 2016, 64-bit

RS7 functionality is not supported for the MCU.

SINUMERIK 828D

SINUMERIK Integrate client software version	Operating software SINUMERIK Operate version	Hardware version	Operating system
2.0.13 2.0.14 2.0.16 2.0.19 2.0.22	4.5 SP4 4.5 SP5, HF1, 2 4.5 SP6, HF1, 2, 3, 4	PPU 281.3 PPU 261.3 PPU 241.3	Linux
3.0.13 3.0.19	4.7 SP2, HF1 4.7 SP3, HF2 4.7 SP4, HF1, 2 4.7 SP5 4.7 SP6, HF1		
3.0.13	4.8 SP4, HF1	PPU 271.4	
3.0.14 3.0.16 3.0.19 3.0.22	4.7 SP2, HF1 4.7 SP3, HF2 4.7 SP4, HF1, 2 4.7 SP5 4.7 SP6, HF1, 2 4.7 SP7, HF1, 3	PPU 290.3 PPU 28x.3 PPU 26x.3 PPU 24x.3	
3.0.14 3.0.19	4.8 SP4, HF1, 2, 3, 4, 5 4.8 SP7	PPU 27x.4 PPU 290.4	
4.0.17 4.0.18 4.0.19 4.0.22	4.94 4.95, HF1		

Retrofit

SINUMERIK Integrate Client Version	Operating software HMI Advanced Version	Hardware version	Operating system
4.15.0.13	7.7.1.0 7.7.1.1	IPC 427D	Windows 10

SINUMERIK control system

Screen resolution	800 x 600 1280 x 1024 1366 x 768 1440 x 900 1600 x 1200 1680 x 1050 1920 x 1200 1920 x 1080

Web browser

You can use the following web browsers:

- Chrome
  Version from 65.0.3325.18 (64 bit) up to the current version
- Firefox
  Version 59.0.2 (64 bit) up to the current version
- Microsoft Edge (Chromium based)
  Version from 85.0.564.51

Operator PC

Processor	1 GHz processor
RAM (GB)	4
Free hard disk capacity (GB)	1
Operating systems	Windows 7 SP1 (x64) Professional/Enterprise/Ultimate Windows 10 (x64) Pro/Enterprise
Screen resolution	At least 1980 x 1080

Industrial PC

Processor	1 GHz processor
RAM (GB)	4
Free hard disk capacity (GB)	1
Operating systems	Windows 7 SP1 (x64) Professional/Enterprise/Ultimate Windows 7 Standard Embedded Windows 10 (x64) Pro/Enterprise
Screen resolution	At least 1980 x 1080 pixels

Note

Only one VNC connection possible

Only one VNC viewer connection is permissible to the SINUMERIK control system.

Remote STEP 7

- SIMATIC Manager versions:
  - 5.4
  - 5.5
  - 5.6
- TIA Portal versions:
  - 15.0
  - 15.1
  - 16.0
  - 16.1
  - 17.0
- TCU and Remote STEP 7 support the following SINUMERIK Integrate client versions:
  - 2.0.13
  - 2.0.14
  - 3.0.13
  - 3.0.14
  - 3.0.19
  - 4.0.20
- SINUMERIK Operate runs under PCU or IPC with the following SINUMERIK Integrate client versions:
  - 2.0.16
  - 2.0.22
  - 3.0.16
  - 3.0.22
  - 4.0.16
  - 4.0.20
  - 4.0.22

Note

Function "Remote STEP 7"

Remote STEP 7 is available in the following configurations:

- SINUMERIK Operate under Linux (NCU)
- SINUMERIK Operate on PCU or IPC

Remote STEP 7 is **not** supported by SINUMERIK 828D.

Remote STEP 7 is supported by SINUMERIK ONE if SINUMERIK Integrate Client version 4.0.20 and Manage MyMachines /Remote Service Client version 2.0.0.6 are installed.

Note

SINUMERIK Integrate applications

Parallel operation with SINUMERIK Integrate applications is not possible.

More information

More information on how to connect remote control systems are provided in the following manual:

"Manage MyMachines /Remote - installation in existing control environments" and "SIMATIC IoT2040".

Type of delivery

The "Manage MyMachines /Remote Service Client" is available via the "Manage MyMachines / Remote" application.

The updates and more information on the applications and products are stored on PridaNet and can be downloaded directly from there.

- OR -

You can contact your machine manufacturer.

- OR -

You can contact the Siemens Service & Support.

Note

Trustworthy software from the Internet

If you download clients from the Internet, only install software that has been signed by Siemens.

DNS addresses

The remote client uses an encrypted TLS https connection over port 443 to the following DNS addresses.

For authentication (log-in):

- Link 1 (https://*.industrysoftware.automation.siemens.com)
- You only need the following links if you are not using link 1:
  - Link 2 (https://identity.industrysoftware.automation.siemens.com)
  - Link 3 (https://www2.industrysoftware.automation.siemens.com)
  - Link 4 (https://content.industrysoftware.automation.siemens.com)
  - Link 5 (https://identityapi.industrysoftware.automation.siemens.com)
  - Link 6 (https://ws-apip.industrysoftware.automation.siemens.com)
- Link 7 (https://cdn.auth0.com)

- Link 8 (https://diswlogin.siemens.com)
- Link 9 (https://static.mentor-cdn.com)
- Link 10 (https://*.eu1.mindsphere.io)
  You only need the following links if you are not using link 10:
  - Link 11 (https://<tenant-Name>.uiam.eu1.mindsphere.io)
  - Link 12 (https://mmmops.piam.eu1.mindsphere.io)
  - Link 13 (https://<tenant-Name>-mmmremote-mmmops.eu1.mindsphere.io))

For the active remote session:

- Link 14 (https://*.mmmr.siemens.cloud)
  - Link 15 (https://server11.mmmr.siemens.cloud)

You can also enable the following simplified DNS names instead of the addresses mentioned above. This reduces the number of URLs that need to be shared.

- Link 16 (https://*.siemens.com)
- Link 17 (https://*.mindsphere.io)
- Link 18 (https://*.siemens.cloud)
- Link 19 (https://cdn.auth0.com)
- Link 20 (https://static.mentor-cdn.com)

Note

Using the SINUMERIK ISW proxy (SSL proxy) in conjunction with HMI Advanced and IPC 127

Communication between the Manage MyMachines /Remote Service Client for Machine Operator IPC, Mozilla Firefox on PCU50, and the ISW proxy on the IPC127 takes place with an encrypted https connection. TLS 1.2 https encryption is established with the ISW proxy for the Insights Hub cloud connection. The web browser is only required to log in to Insights Hub and download the remote session token.
By default, Manage MyMachines /Remote uses proxy port 8433.

More information can be found at: ISW Proxy Manual.

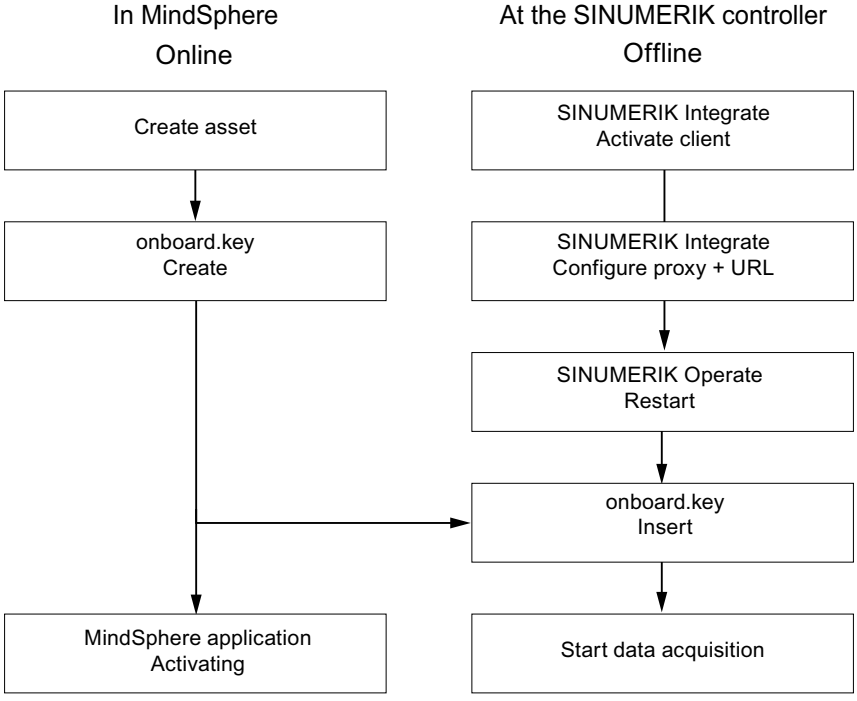
Setting up the SINUMERIK control system for Manage MyMachines /Remote

4

4.1 Activating the data acquisition

Overview

To use the Manage MyMachines for Industrial Operations X Cloud, you must carry out various steps in Insights Hub and on the SINUMERIK control itself.



Procedure

In Insights Hub:

1. Create the desired assets.
   More information can be found at: Asset Manager (Page 67)
   Detailed information can be found at: Insights Hub - Asset Manager System Manual
2. Create the "onboard.key".
   More information can be found at: Connecting SINUMERIK controls with Insights Hub (Page 84)

At the SINUMERIK control system:

1. Check the installed version.
   More information can be found at: Displaying version data (Page 27)
   – If an appropriate SINUMERIK Integrate version is not installed, then perform a client update.
   More information can be found at: Client update under Windows (Page 30)
2. Activate the SINUMERIK Integrate client.
   More information can be found at: Activating the SINUMERIK Integrate client (Page 38)
3. Enable the use of SINUMERIK Integrate.
   More information can be found at: Activating SINUMERIK Integrate use (Page 39)
4. Configure the URL and proxy.
   – On the SINUMERIK 840D sl control system:
   More information can be found at: Configuring the URL and proxy (Page 40)
   - OR -
   – On the SINUMERIK 828D control system:
   More information can be found at: Configuring the URL and proxy (Page 47)
   - OR -
   – On the SINUMERIK ONE control system:
   More information can be found at:Configuring the URL and proxy (Page 40)
5. Restart SINUMERIK Operate.
6. Insert "onboard.key".
   – On the SINUMERIK 840D sl control system:
   More information can be found at: Install the registration key on a SINUMERIK control system (Page 43)
   - OR -
   – On the SINUMERIK 828D
   More information can be found at: Install the registration key on a SINUMERIK control system (Page 50)
7. Start with editing the diagram.

Note

File "onboard.key"

The file "onboard.key" contains security-related information for the one-time connection setup of a SINUMERIK control with Insights Hub, and must therefore be stored securely - both on the end device, on which the file is stored temporarily, and on the target controller. This connection setup key is only no longer relevant when the connection between the SINUMERIK control system and Insights Hub has been completely established.

This file is then automatically deleted on the SINUMERIK control system.

Secure the terminals used for this accordingly, for example, using virus protection programs, firewalls, OS updates, etc.

4.2 Checking and updating the versions

4.2.1 Displaying version data

In the "Version data" window you can check whether you are using a suitable version.

Only use the versions specified in this document.
Additional information is provided in Chapter: System requirements (Page 17).

The following components with the associated version data are specified:

- CNC software
  Among other things, the SINUMERIK Operate version is displayed in the details.
- PLC basic program
- PLC user program
- System extensions
  Among other things, the SINUMERIK Integrate version is displayed in the details.
- OEM applications
- Hardware

Information is provided in the "Nominal version" column as to whether the versions of the components differ from the version supplied on the CompactFlash card.

Icon	Description
	The version displayed in the "Actual version" column matches the version of the CF card.
	The version displayed in the "Actual version" column does not match the version of the CF card.

Procedure

1. Start the SINUMERIK Operate operating software on the SINUMERIK control system.
2. Press the <MENU SELECT> key.
3. Select the "Diagnostics" operating area.



4. Press the "Version" softkey.
   The "Version data" window opens.
   The data of the available components is displayed.

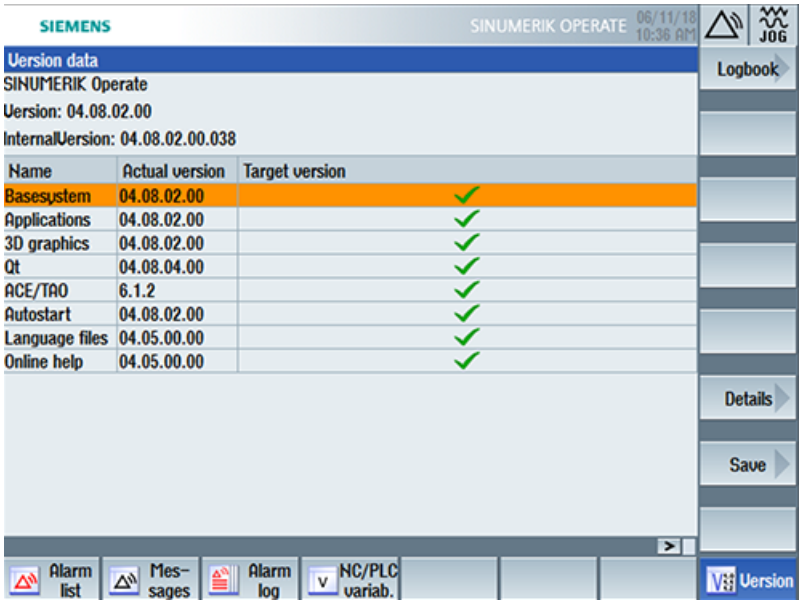


5. Select the component for which you would like more information.





6. Press the "Details >" softkey in order to obtain more detailed information on the components displayed.



Start a client update if you have the required SINUMERIK Integrate version on your SINUMERIK control system.

Information is provided in the following chapter as to how you perform a client update:

- Client update under Windows (Page 30)
  - OR -
- Client update under Linux (Page 34)

4.2.2 Installing a SINUMERIK 828D update

If you are not using a suitable software version on the SINUMERIK 828D control, you must install the required software update/backup.

Procedure

1. Switch the control on.
   The following is displayed during startup:



2. Press the <SELECT> key within three seconds.
   To call the "Startup menu", press the following keys in succession:
   Menu back key, **HSK2** (horizontal softkey 2), **VSK2** (vertical softkey 2)

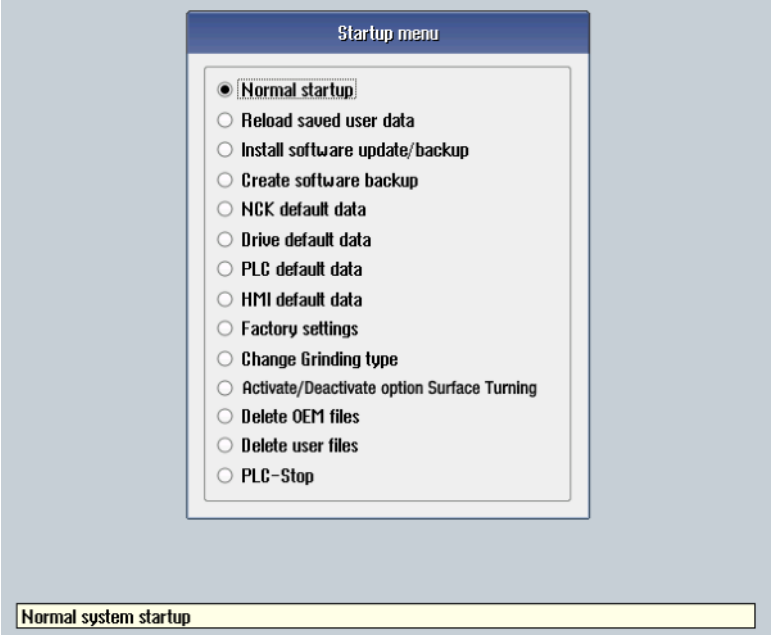


Note

PPU with touch operation

To call the "Startup menu" during startup, there is an additional shortcut key for all PPUs: **"8" → "2" → "8"**

3. The "Startup menu" is displayed, "Normal startup" is the default setting.



4. Select the "Install software update/backup" option to install an update on the system CompactFlash card from the user CompactFlash card or USB flash drive.

5. The following message is displayed:
   "Do you want to install the software update? Either CF card or USB stick must be plugged in".
6. Insert the USB flash drive into the USB interface on the front of the operator panel. Click on "Yes".
7. Make sure that only individual ".tgz" files are located on the USB flash drive. Press the <INPUT> key to install the required files.
8. The installation preparation and then the installation procedure are shown on the screen.
9. At the end, the following message is displayed: "Restoring complete. Switch off and remove data medium!"
   Switch off the control. Remove the storage medium.

Further information on commissioning SINUMERIK 828D can be found in the SINUMERIK 828D Commissioning Manual.

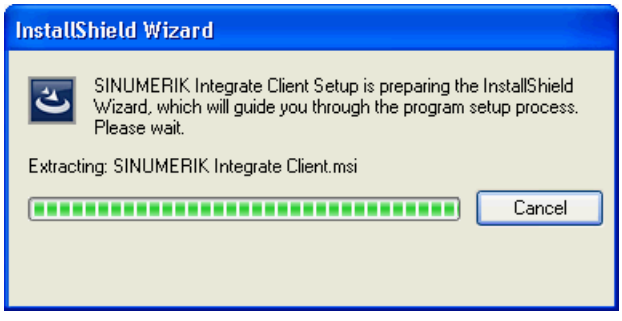
4.2.3 Client update under Windows

Requirement

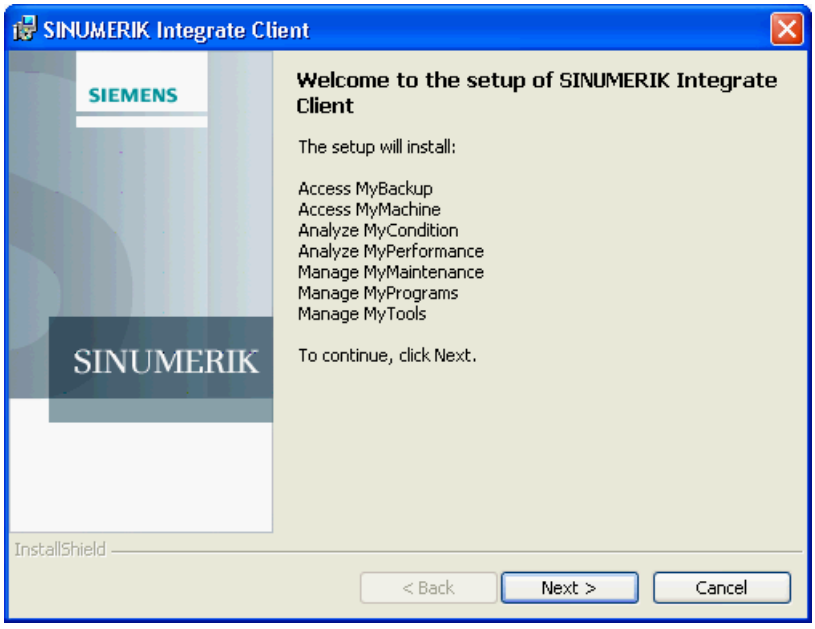
The SINUMERIK Integrate client update required "setup.exe" was transferred into the installation directory.

Procedure

1. Start the SINUMERIK control system in the Windows service mode.
2. Open the installation directory.
3. Start setup file "setup.exe" with a double-click.
   SINUMERIK Integrate Client - InstallShield Wizard opens.



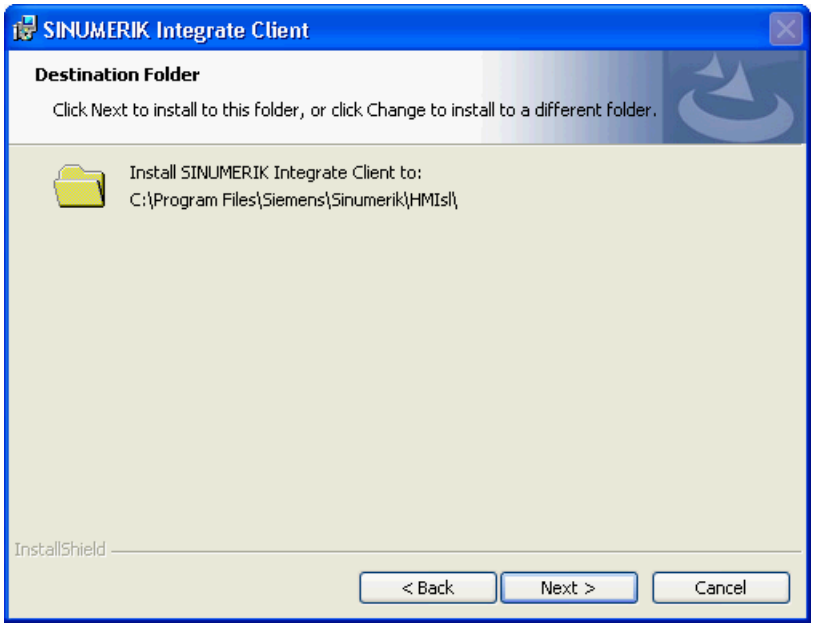
4. The welcome screen opens and shows the applications to which the update applies.
   Click "Next >" to start the installation preparation.



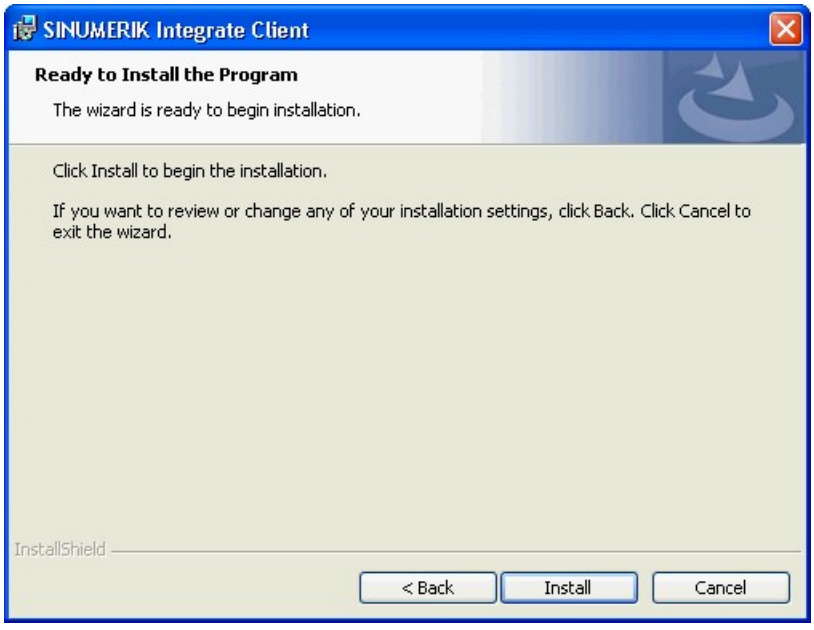
5. The "License Agreement" window opens.
   Read the license agreement.
   - If you want to print the terms, click "Print."
   - Then activate the "I accept the terms in the license agreement" checkbox and click "Next >".
     - OR -
     Click "< Back" to return to the previous window.



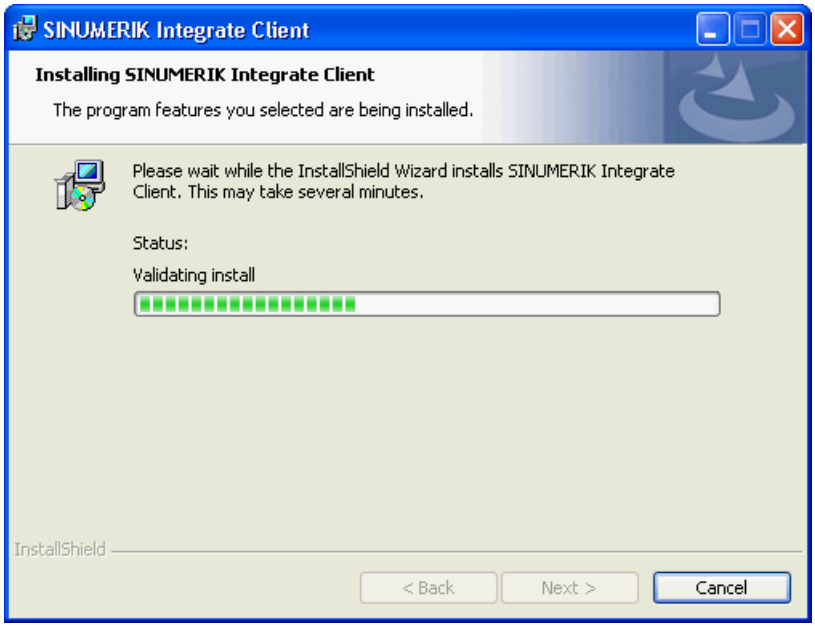
6. The next window displays the installation directory for the application.
   Click "Next >" to accept the directory suggested by the setup.



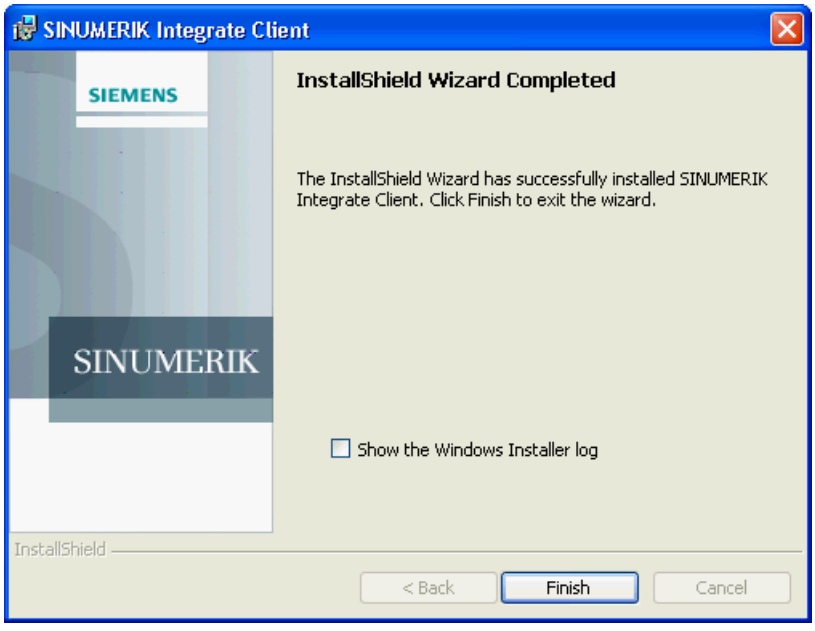
7. The Wizard is ready to start the installation.
   Click "Install" to start the installation.



8. The installation is started, and the progress is displayed with a progress bar.



9. Click "Finish" to complete the installation.



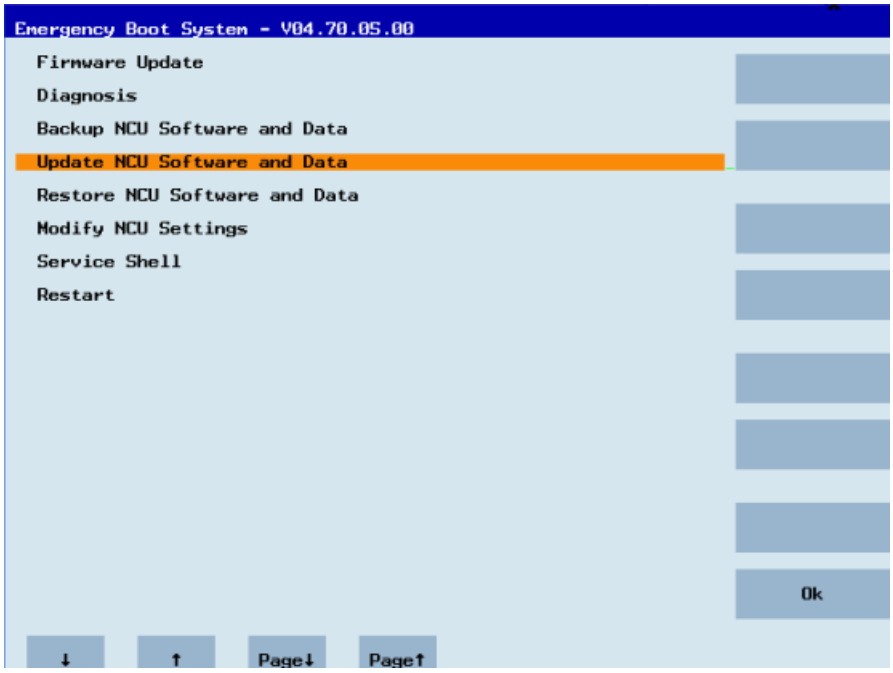
4.2.4 Client update under Linux

Precondition

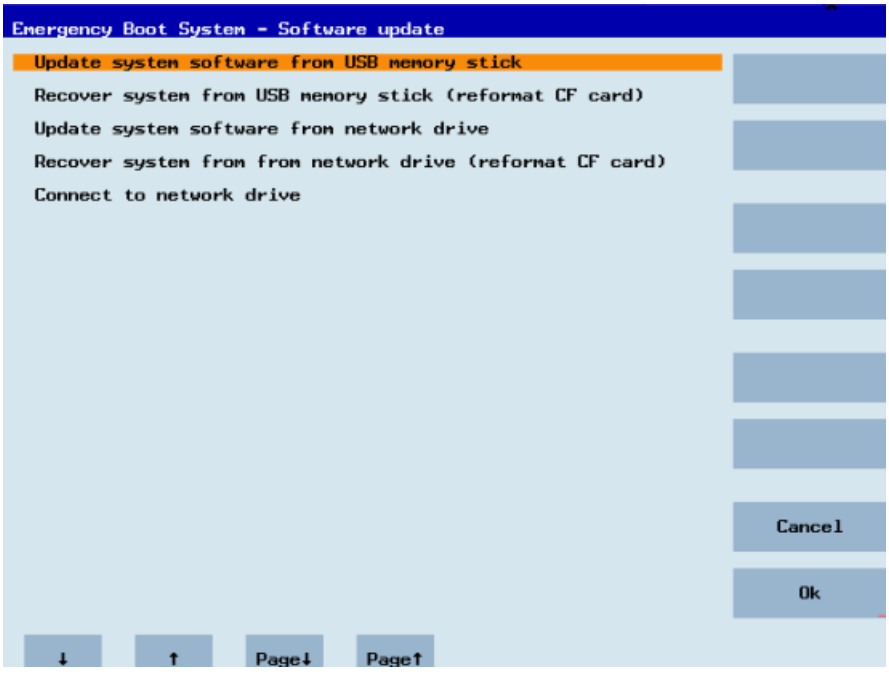
- Emergency Boot System V04.70.05.00
- SINUMERIK Operate 4.5 SP4
  - OR -
- SINUMERIK Operate 4.7 SP2
  - OR -
- SINUMERIK Operate 4.9x

Procedure

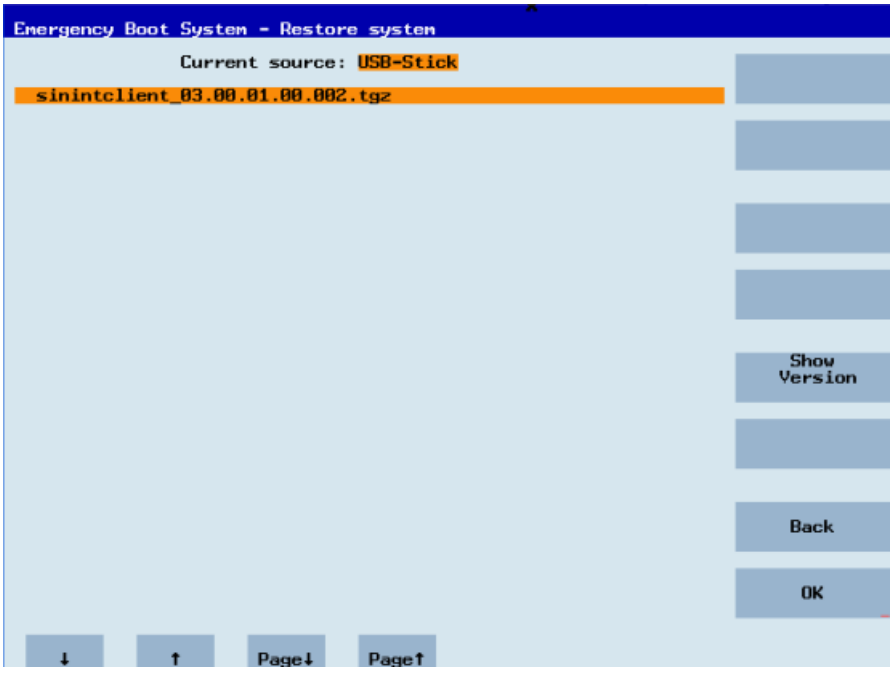
1. Copy the "sinintclient.tgz" file to the USB flash drive.
2. Insert the USB flash drive into the NCU.
3. Start the NCU.
4. In the menu, select "Update NCU Software and Data" with the cursor keys and press the "OK" softkey.



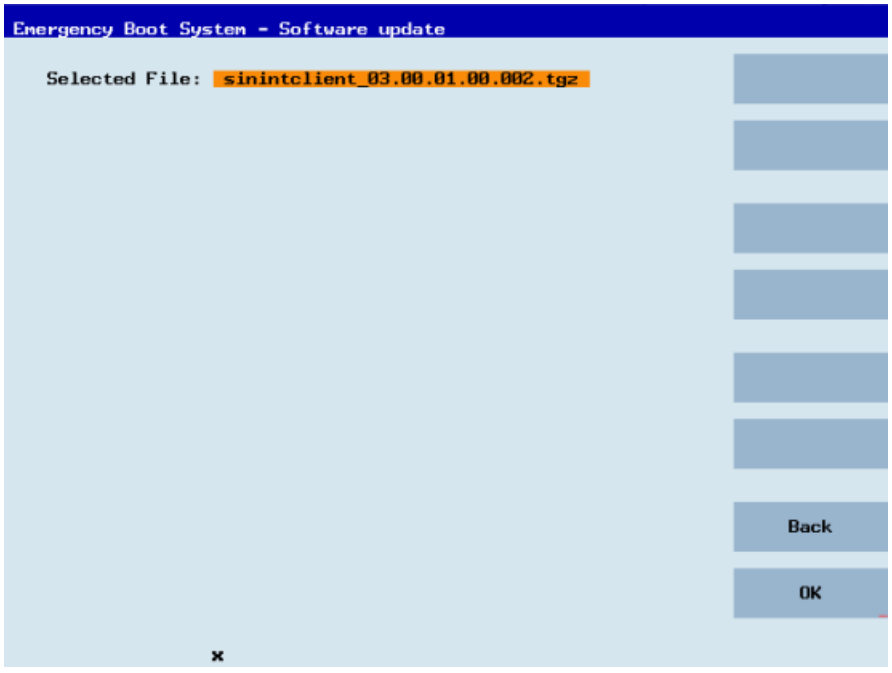
5. In the menu, select "Update system software from USB memory stick" with the cursor keys and press the "OK" softkey.



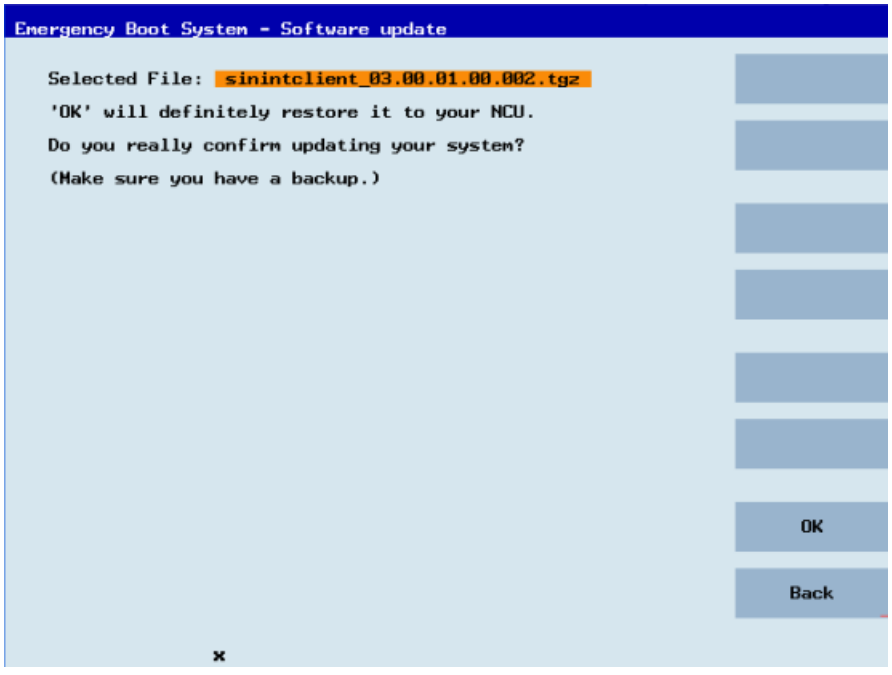
6. You receive a list with all tgz files.
   Select the current file.
   Press the "OK" softkey to confirm your selection.
   - OR -
   Press the shortcut key <Shift> + <F8> on the operator panel.



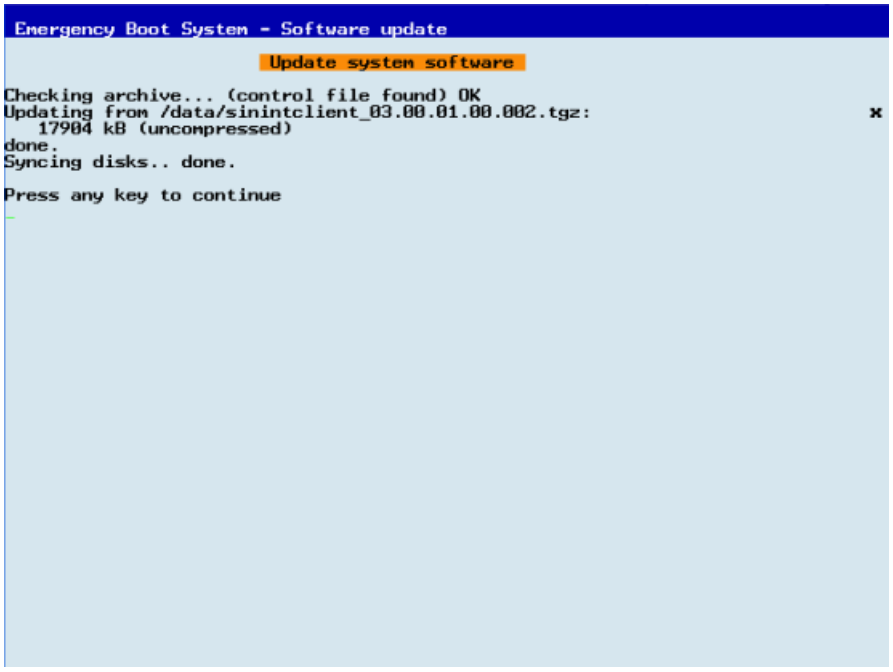
7. The selected file is displayed.
   Press the "OK" softkey to confirm your selection.
   - OR -
   Press the shortcut key <Shift> + <F8> on the operator panel.



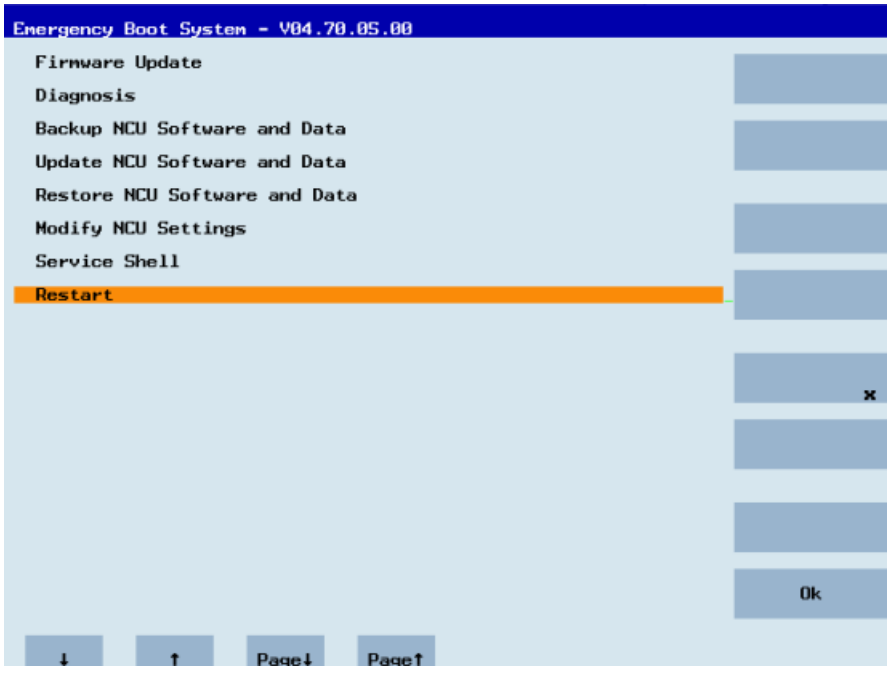
8. A confirmation prompt appears.
   Press the "OK" softkey to confirm the confirmation prompt.
   - OR -
   Press the shortcut key <Shift> + <F7> on the operator panel.



9. The installation is started.



10. When the installation has been completed, the following message appears. Remove the USB flash drive.
Select "Restart" from the menu and press the "OK" softkey.

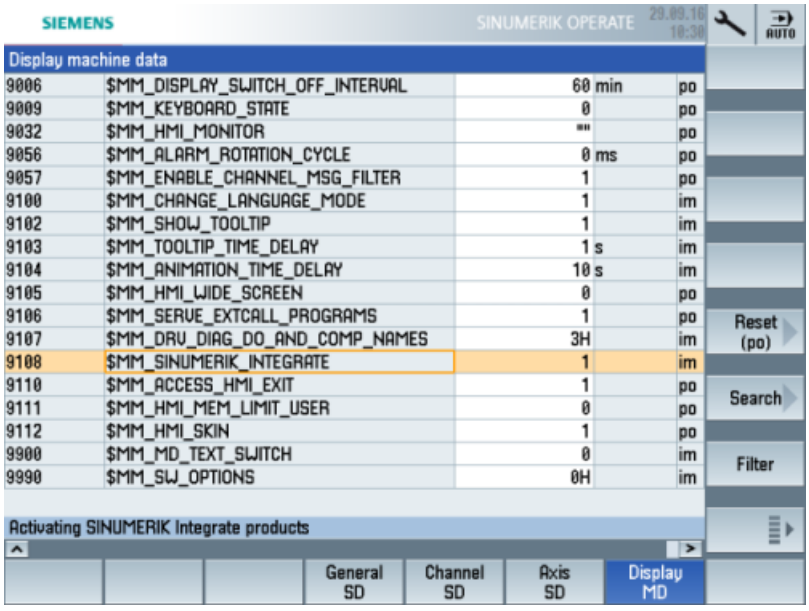


4.3 SINUMERIK Integrate

4.3.1 Activating the SINUMERIK Integrate client

Procedure

1. Start the SINUMERIK Operate operating software on the control.
2. Press the "Setup" and "Mach. data" softkeys.
3. Press the "Password" softkey.
4. The "Set password" window opens.
5. Enter the password for "Manufacture" and press the "OK" softkey.
6. Press the menu forward key and the "Display MD" softkey.
   – Set the machine data
   MD9108 $MM_SINUMERIK_INTEGRATE to "1".



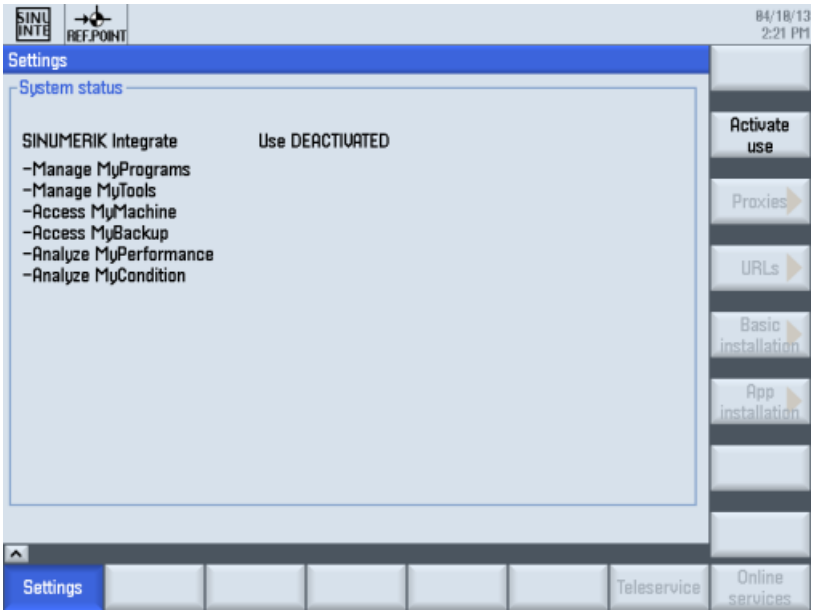
7. Press the <MENU SELECT> key followed by the menu forward key.
8. The "SINUMERIK Integrate" softkey is displayed on the extended horizontal softkey bar.



4.3.2 Activating SINUMERIK Integrate use

Procedure

1. Press the "SINUMERIK Integrate" softkey.
   The "SINUMERIK Integrate" welcome window opens.
2. Press the "Settings" softkey.
   The "Settings" window opens displaying the system status "Use DEACTIVATED".
   – Press the "Activate use" softkey.



3. The confirmation prompt "Do you want to activate the use of SINUMERIK Integrate applications?" is displayed.
   – Press the "OK" softkey to confirm the prompt.
   The use of SINUMERIK Integrate applications is enabled.

4.4 SINUMERIK 840D sl

4.4.1 Configuring the URL and proxy

Note

Transferring SINUMERIK data to the Insights Hub platform

The following steps allow you to transfer SINUMERIK data to the Insights Hub platform.

By performing the steps described below, in particular through input and confirmation of the Web service URL, processes are performed automatically in which software scripts are loaded to the SINUMERIK control.

Precondition

The use of SINUMERIK Integrate has been activated.

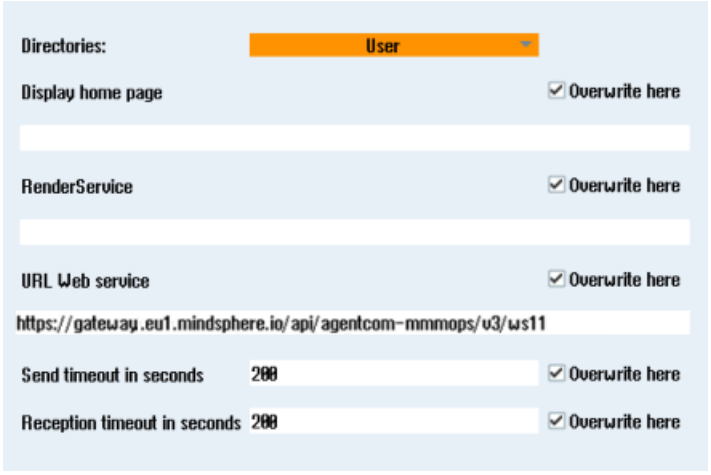
Check whether the Internet connection is available and activated:

- TCU:
  Press "Online Services". The "Login" window is opened.
  If this is not the case, check the connected Internet connection.
- PCU:
  Start the control in service mode, and call up an Internet page using the Web browser, for example, "www.siemens.com".

Procedure

The "Settings" window is open.

1. Press the "URLs >".
2. Press "Edit" and select the following settings:
   - Directory: Select the "User" entry in the "Directory" drop-down list.
   - Display home page: Select the "Overwrite here" check box.
   - RenderService: Select the "Overwrite here" check box.
   - Web service URL: Select the "Overwrite here" check box.
   - Enter the following web service URL depending on which Insights Hub system you are connected to:
     Insights Hub V3 Livesystem (https://gateway.eu1.mindsphere.io/api/agentcom-mmmops/v3/ws11)
     Insights Hub Alibaba (https://gateway.cn1.mindsphere-in.cn/api/agentcom-dimcopt/v3/ws11)
   - Enter the required value in the "Transmit timeout in seconds" input field. The default value is 200. Then select the "Overwrite here" check box.
   - Enter the required value in the "Receive timeout in seconds" input field (default value is 200), and select the "Overwrite here" check box.

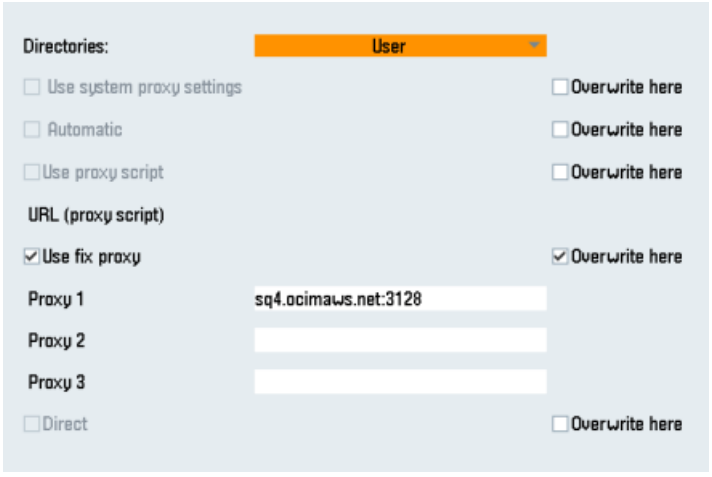


3. Press "OK".
   A syntax check is performed and the access data is saved.
   Usually, the settings are now complete. If further adaptations need be made within your company network, read the following paragraph:

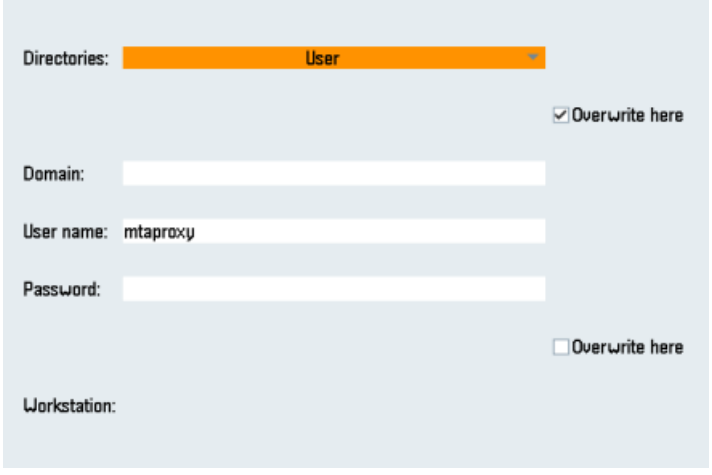
Proxy adaptations (optional)

1. Clarify with your network administrator whether the Proxy settings have to be adjusted for the connection to Cloud mode.
   If this is necessary, proceed as follows:
2. Press "Proxys >".
   The stored settings are displayed.

3. Press "Edit" and then select the following settings:
   - Select the "Use fix proxy" check box.
   - Enter your proxies in the "Proxy 1" to "Proxy 3" input fields.
   - Select the "Overwrite here" check box even if you only enter one proxy in order to accept the new entry.



4. Press "OK" to save the settings.
5. If authentication is required for the proxy, press "Authorization".
   - Select the "Overwrite here" check box to accept the new entry.
   - Enter the user data in the "Domain", "User name" and "Password" input fields.

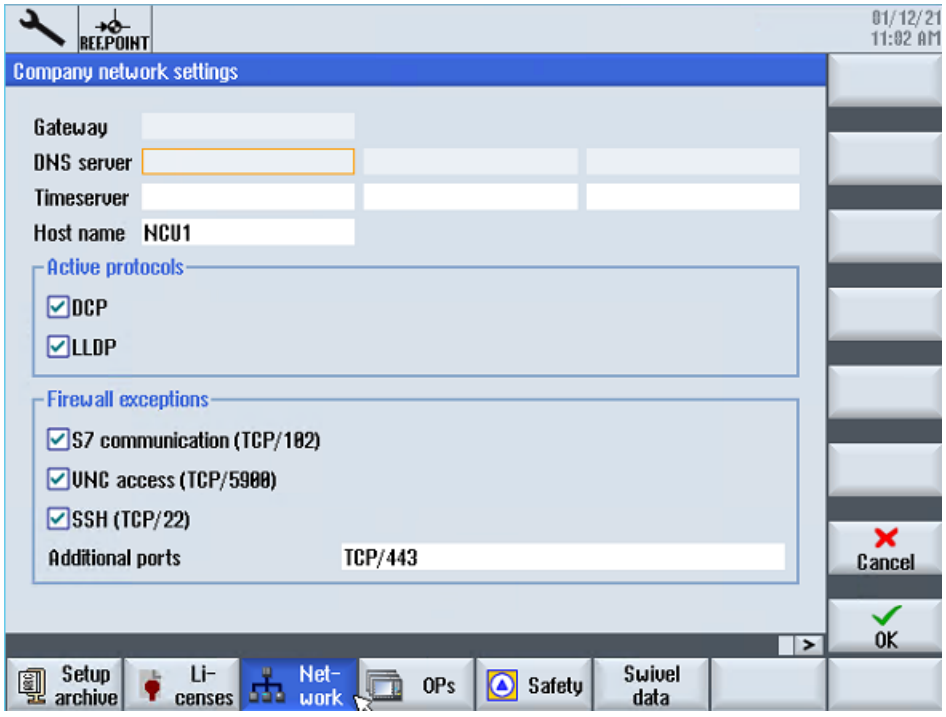


6. Press "OK" to save the settings.
7. Restart the control so that the access data can take effect.

Additional ports

Activate the port for HTTPS communication to ensure secure data transfer between the user server and the control.

1. Press softkey "Commissioning" >" Network" > "Company network".
   The "Company network settings" window opens.
2. Press "Change" to edit the settings.
3. In the "Firewall exceptions" area, add port "TCP/443" in the "Additional ports" input box.
4. Press "OK".



4.4.2 Install the registration key on a SINUMERIK control system

Activating SINUMERIK Integrate generates the setup of the URL/proxy and the restart in the directory of the "boot_job" folder.

- Operate (PCU): C:\temp\boot_job
- Operate (NCU): /var/tmp/boot_job (accessible on the CF card via WinSCP)

The boot_job folder is created automatically. If the folder was not set up, then check that the device has the correct network connection (e.g. proxy settings, permitted IP list for Insights Hub addresses, etc.).

There are 2 ways to copy the "onboard.key" to the SINUMERIK control system:

- Via the SINUMERIK Operate user interface
- With the aid of WinSCP

Precondition

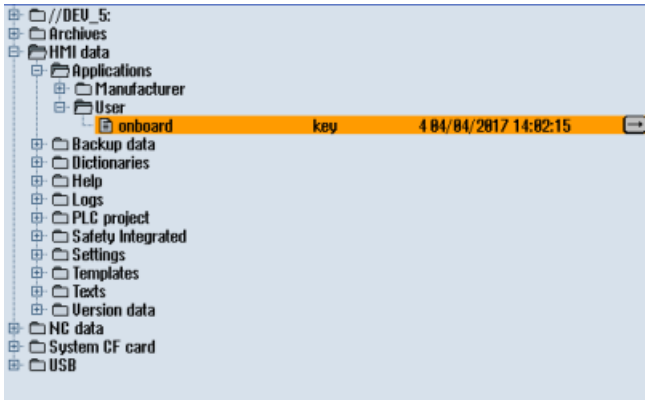
- The "onboard.key" has been generated.
- The "boot_job" folder is created on the SINUMERIK control system, e.g. at C:\temp
- The time and date on the control system has been synchronized with the current time and date.
- The Internet connection has been checked and is established.

Procedure with SINUMERIK Operate (PCU 50)

1. Insert the USB flash drive with the "onboard.key" file into the PCU.
   The USB flash drive is shown in the directory tree.
2. Copy the file "onboard.key" into the following directory: C:\temp\boot_job.
3. Check the PCU configuration.

Procedure with SINUMERIK Operate (NCU)

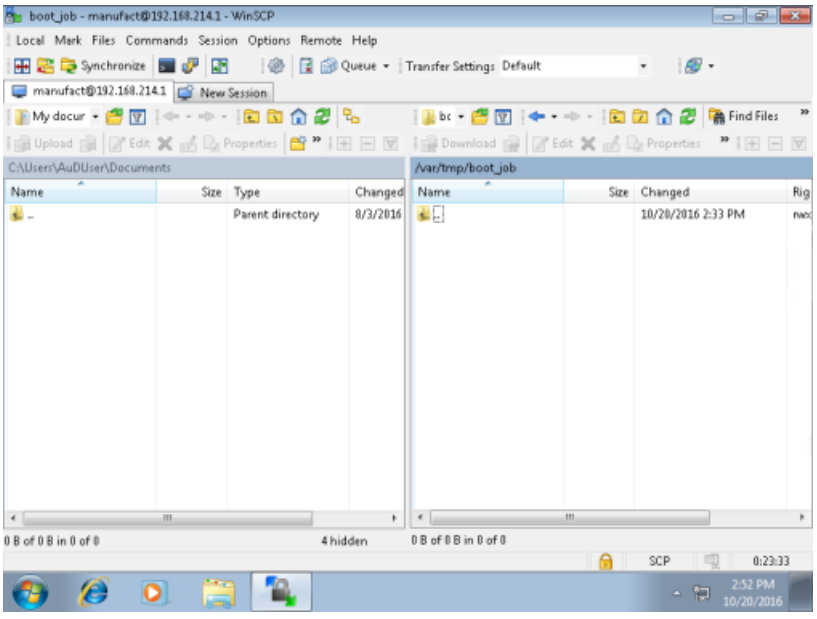
1. At the SINUMERIK control system, start the SINUMERIK Operate operating software.
2. Press "Setup".
3. Press "System data".
   The directory tree is displayed.
4. Insert the USB flash drive with the "onboard.key" file into the NCU.
   The USB flash drive is displayed in the directory tree.
   If the USB flash drive is not detected by SINUMERIK Operate, you must change to a different USB port or configure a logical drive.
   Further information is provided in Chapter: Create drive (Page 46)
5. Select the "onboard.key" and press "Copy".
6. Navigate in the following directory: HMI data\Applications\User and press "Paste".



7. Then restart.

Procedure with, e.g. WinSCP (NCU)

1. Copy the generated "onboard.key" file using a suitable tool, e.g. using WinSCP via the network to the control system.
2. Start the SINUMERIK control system and open the directory /var/tmp/boot_job.



3. Insert the "onboard.key" file in the "boot_job" directory.
   - If a "cert.key" file exists in the /var/tmp/boot_job folder, then the control system was already connected to Insights Hub.
     Delete the complete content of folder "boot_job" and empty the cache. Then insert the new "onboard.key" file.
   - Alternatively, you can also insert the "onboard.key" file into the following directory: /user/sinumerik/hmi/appl.
4. Then start the SINUMERIK Operate operating software.
   When the connection to the server is successful, the "cert.key" file is created.
5. The onboarding process is completed. The "onboard.key" is no longer displayed in the directory.

4.4.3 Create drive

Parameters

Entry		Meaning
Connection	Front	USB interface that is located at the front of the operator panel.
	X203/X204	USB interface X203/X204 that is located at the rear of the operator panel.
	X212/X213	TCU20.2/20.3
Symbolic		Symbolic name of the drive

Procedure

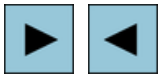


1. Select the "Start-up" operating area.





2. Press the "HMI" and "Log. drive" softkeys.
   The "Set up drives" window opens.



3. Select the softkey that you want to configure.



4. To configure softkeys 9 to 16 or softkeys 17 to 24, click the ">> Level" softkey.



5. To allow input fields to be edited, press the "Change" softkey.
6. Select the data for the appropriate drive or enter the required data.



7. Press the "Details" softkey if you want to enter additional parameters.
   Press the "Details" softkey to return to the "Set up drives" window.





8. Press the "OK" softkey.
   The entries are checked.
   A window with a prompt opens if the data is incomplete or incorrect. Acknowledge the prompt with the "OK" softkey.
   The drive, e.g. "usb-NEU" is shown in the directory tree.



4.5 SINUMERIK 828D

4.5.1 Configuring the URL and proxy

Note

Transferring SINUMERIK data to the Insights Hub platform

The following steps allow you to transfer SINUMERIK data to the Insights Hub platform.

By performing the steps described below, in particular through input and confirmation of the Web service URL, processes are performed automatically in which software scripts are loaded to the SINUMERIK control.

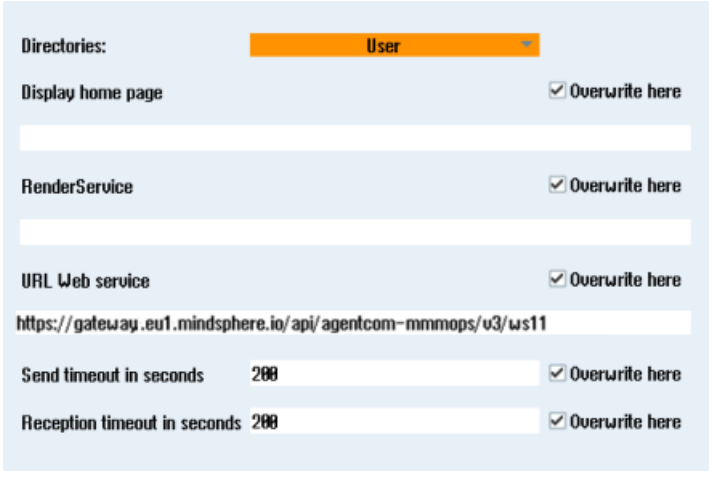
Precondition

The use of SINUMERIK Integrate has been activated.

Procedure

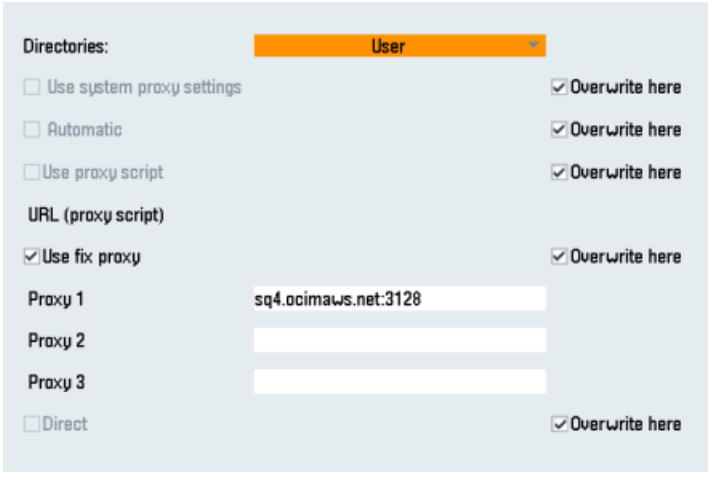
The "Settings" window is open.

1. Press the "URLs >".
2. Press "Edit" and then select the following settings:
   - Directory: Select the "User" entry in the "Directory" drop-down list.
   - Display home page: Select the "Overwrite here" check box.
   - RenderService: Select the "Overwrite here" check box.
   - Web service URL: Select the "Overwrite here" check box.
   - Enter the following web service URL depending on which Insights Hub system you are connected to:
     Insights Hub V3 Livesystem (https://gateway.eu1.mindsphere.io/api/agentcom-mmmops/v3/ws11)
     Insights Hub Alibaba (https://gateway.cn1.mindsphere-in.cn/api/agentcom-dimcopt/v3/ws11)
   - Enter the required value in the "Transmit timeout in seconds" input field. The default value is 200. Then select the "Overwrite here" check box.
   - Enter the required value in the "Receive timeout in seconds" input field (the default value is 200), and select the "Overwrite here" check box.

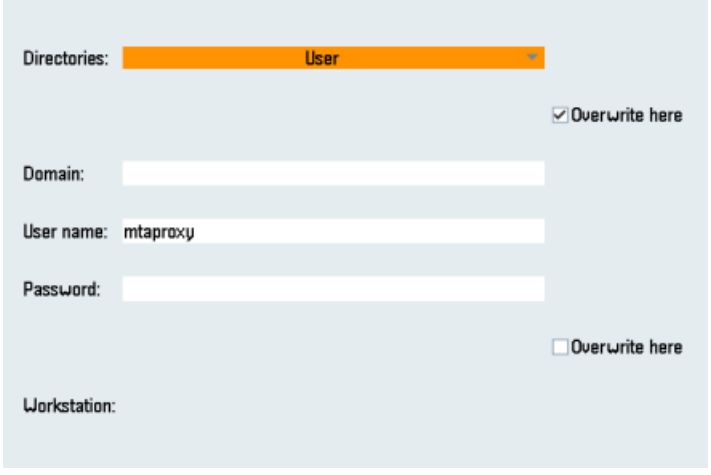


3. Press "OK".
   A syntax check is performed and the access data is saved.
4. In order to establish a connection from the customer network, you must adapt the proxy settings.
   Press "Proxys >".
   The stored settings are displayed.

5. Press "Edit" and then select the following settings:
   - Select the "Use fix proxy" check box.
   - Enter your proxies in the "Proxy 1" to "Proxy 3" input fields.
   - Select the "Overwrite here" check box even if you only enter one proxy in order to accept the new entry.



6. Press "OK" to save the settings.
7. If authentication is required for the proxy, press "Authorization".
   - Select the "Overwrite here" check box to accept the new entry.
   - Enter the user data in the "Domain", "User name" and "Password" input fields.

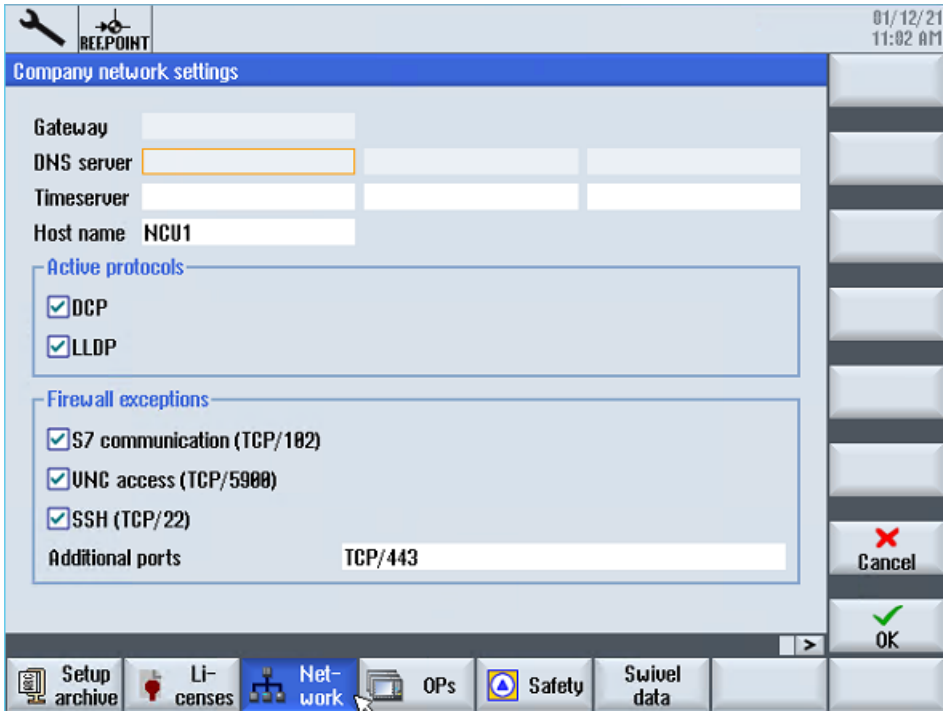


8. Press "OK" to save the settings.
9. Restart the control so that the access data can take effect.

Additional ports

Activate the port for HTTPS communication to ensure secure data transfer between the user server and the control.

1. Press "Commissioning" >" Network" > "Company network".
   The "Company network settings" window opens.
2. Press "Change" to edit the settings.
3. In the "Firewall exceptions" area, add port "TCP/443" in the "Additional ports" input box.
4. Press "OK".



4.5.2 Install the registration key on a SINUMERIK control system

The activation of SINUMERIK Integrate, the setting up of the URL/proxy and the restart creates the "boot_job" folder in the /var/tmp/ directory.

The boot_job folder is created automatically. If the folder was not set up, then check that the device has the correct network connection (e.g. proxy settings, permitted IP list for Insights Hub addresses, etc.).

Copy the "onboard.key" to the SINUMERIK control system, e.g. using WinSCP.

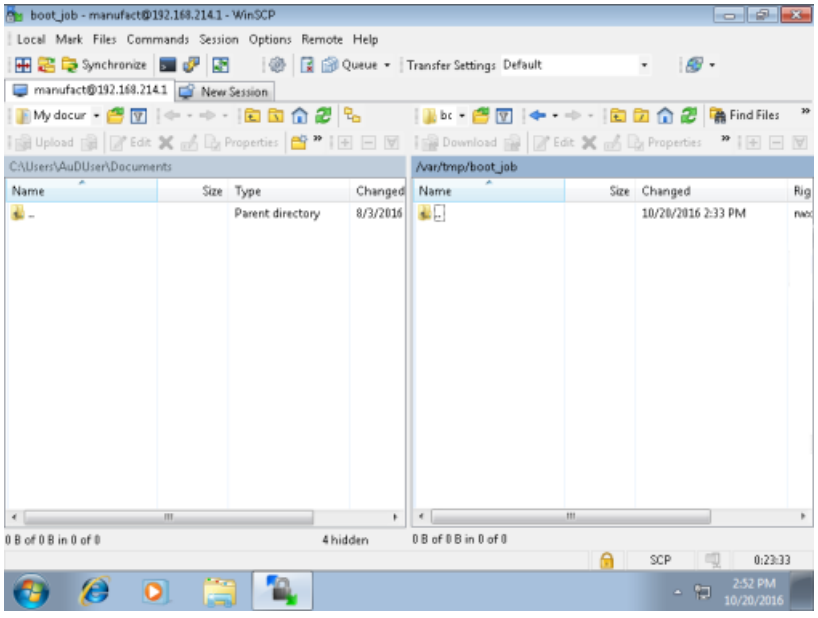
Precondition

- The "onboard.key" has been generated.
- The "boot_job" folder is created on the SINUMERIK control system, e.g. at C:\tmp

- The time and date on the control system has been synchronized with the current time and date.
- The Internet connection has been checked and is established.

Procedure

1. Copy the generated "onboard.key" file using WinSCP for example via the network to the SINUMERIK control system.
2. Start the SINUMERIK control system and open the directory, e.g. /var/tmp/boot_job.
   If the "boot_job" folder does not exist, then create the folder manually.



3. Open folder "boot_job" and insert file "onboard.key".
   – If a "cert.key" file exists in the /var/tmp/boot_job folder, then the control system was already connected to Insights Hub.
   Delete the complete content of folder "boot_job" and empty the cache. Then insert the new "onboard.key" file.
4. Then start the SINUMERIK Operate operating software.
   When the connection to the server has been successfully established, then the "cert.key" file is created.
5. The onboarding is completed and the "onboard.key" is no longer displayed in the directory.

4.6 Adapting SINUMERIK Operate

4.6.1 Exchanging a certificate (optional)

In order to achieve comprehensive security, it is necessary to update the certificate "cacert.pem". The following manual steps are required for this purpose.

Note

Manage MyMachines and Manage MyMachines /Remote

On SINUMERIK devices with Integrate Clients, versions exists with expired QuoVadis intermediate certificate signatures. This certificate expired on November 06, 2022. Checking the validity of this certificate leads to an immediate connection abort or failure of onboarding in the SINUMERIK Integrate Client. This prevents remote access sessions from occurring.

Due to the expiry of the QuoVadis Global SSL ICA G3 certificate, the connection to the machine is terminated if the following SINUMERIK Integrate Client versions are involved:

- 02.00.19 / 02.00.20 / 02.00.21
- 03.00.19 / 03.00.20 / 03.00.21
- 04.00.19 / 04.00.20 / 04.00.21

This only applies to the SINUMERIK ONE, SINUMERIK 840D sl, and SINUMERIK 828D Operate controls.

The SINUMERIK 840 D PL is not affected.

Note

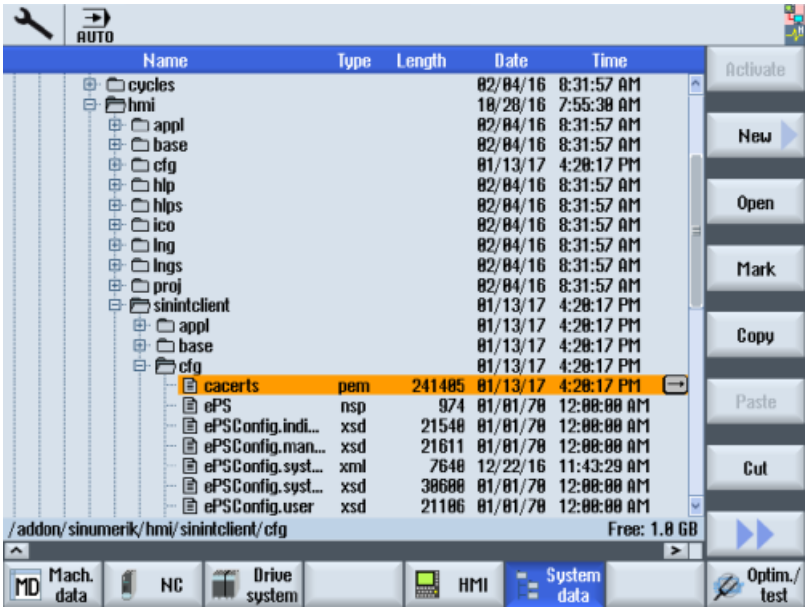
SINUMERIK Integrate clients: previous versions

For previous versions, the certificate in the cacerts.pem file is still valid.
No update is required for these clients.

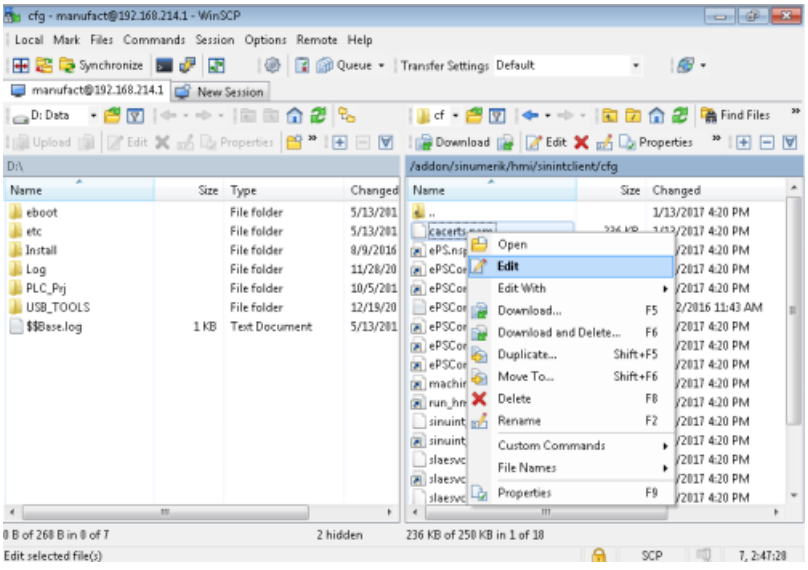
Please check the SINUMERIK Integrate Client version before performing a certificate update.

SINUMERIK Operate with SINUMERIK Integrate client under Linux

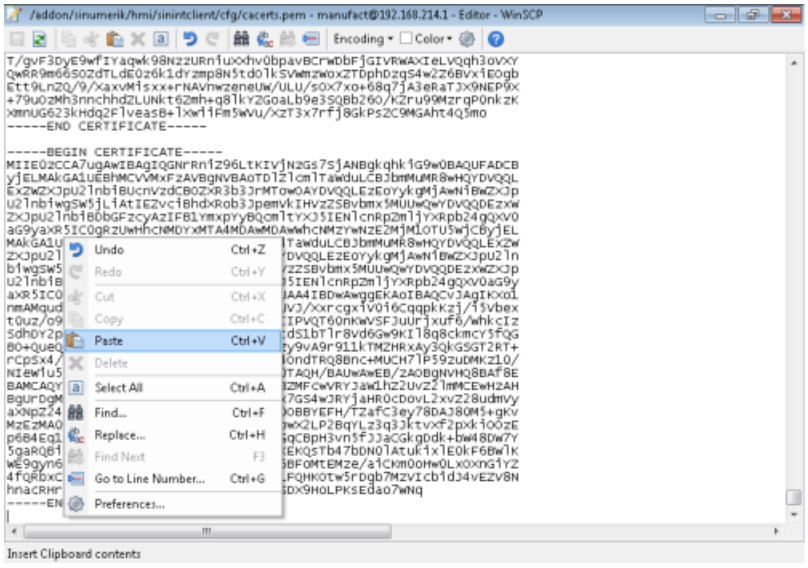
1. Open the directory: card/addon/sinumerik/hmi/sinintclient/cfg
2. Select "cacerts.pem".



3. Use WinSCP, for example, to open "cacerts.pem" in the editor.



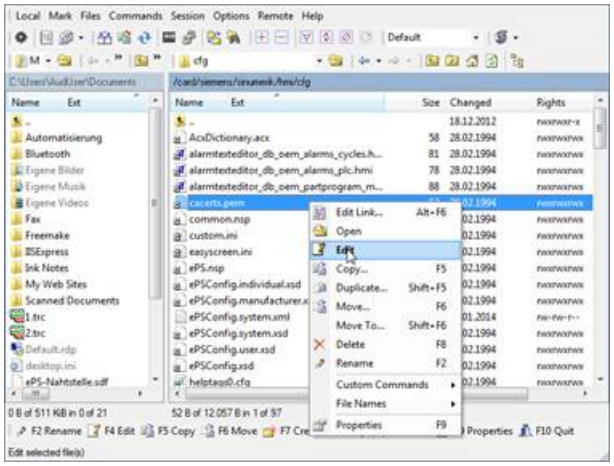
4. Insert the content of "Customer Root CA" at the end of "cacerts.pem".



5. Close the file to save the certificate.
6. Perform a restart.

SINUMERIK Operate under Windows

1. Open the "Customer Root CA" file in the editor and copy the entire content to the clipboard.
2. Use WinSCP, for example, to open "cacerts.pem" in the editor.
   C:\ProgramData\Siemens\MotionControl\addon\sinumerik\hmi\sinintclient\cfg\cacerts.pem



3. Insert the content of "Customer Root CA" at the end of "cacerts.pem".



4. Close the file to save the certificate.
5. Store the adapted file in the same directory again:
   C:\ProgramData\Siemens\MotionControl\addon\sinumerik\hmi\sinintclient\cfg
6. Perform a restart.

4.6.2 Activating logs for troubleshooting

At the SINUMERIK control system, activate the logs in the "ePSConfig.user.xml" file for troubleshooting.

Procedure

1. Press the "System data" softkey.
2. Navigate in the following directory: System CF card/user/sinumerik/hmi/cfg.
3. Open file "ePSConfig.user.xml".

Note

Path to the "ePSConfig.user.xml" file

The path to the "ePSConfig.user.xml" file can be found here: Path description "ePSConfig.user.xml" (https://documentation.mindsphere.io/resources/html/manage-my-machine-eu1/readme/en-US/113606291083.html)

4. Make the following setting:
```
<logging>
<separateScriptLog active="1">1</separateScriptLog>
<scriptLogPath active="1">/var/tmp/scriptLog</scriptLogPath>
<scriptLogSeverity active="1">8</scriptLogSeverity>
<uiScriptLogSeverity active="0">2</uiScriptLogSeverity>
<maxScriptLogSize active="1">10000</maxScriptLogSize>
<maxLogLifeTimeDays active="0">30</maxLogLifeTimeDays>
</logging>
```
5. Restart the SINUMERIK control system and have the log files sent to you.

4.7 PCU retrofit

Precondition

HMI-Advanced V7.7 is installed. More information about the installation is provided in the Commissioning Manual "SINUMERIK 840D PCU Retrofit".

Setting up SINUMERIK Integrate Client for PCU Retrofit

1. Install the current SINUMERIK Integrate Client. More information is provided in the Installation Manual "SINUMERIK Integrate 5, Manage MyResources, Optimize MyProgramming /NX-Cam Editor, Analyze MyPerformance /OEE".
2. Open the following file: F:\add_on\MH\settings.ini
   - Change the following entry:
     [APP]
     ACCESSTYPE ="DDE"
   - Save and close the file.
3. Open the following file: F:\add_on\regie.ini
   - Change the following entry:
     [StartupConfiguration]
     Startup42 = name := oemframe, cmdline := "cmd.exe /c F:\\add_on\\MH\ \MhDdeService.exe"
     Startup43 = name := oemframe, cmdline := "cmd.exe /c F:\\add_on\\MH\ \MachineHandler.exe"
   - Save and close the file.
4. Create and connect the machine with Insights Hub. More information is provided in Chapters:
   - Setting up the SINUMERIK control system for Manage MyMachines /Remote (Page 25)
   - Connecting SINUMERIK controls with Insights Hub (Page 84)

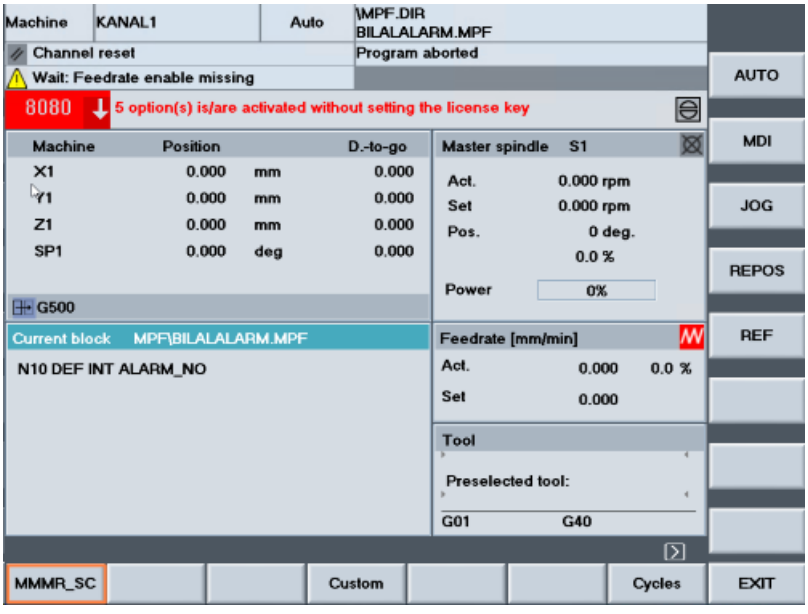
Setting up Manage MyMachines /Remote Service Client for PCU Retrofit

1. Install the "Manage MyMachines /Remote Service Client for Machine Operators - IPC" on the PCU retrofit machine. More information is provided in Chapters:
   - Download remote service client (Page 94)
   - Setting up Manage MyMachines /Remote Service Client (Page 131)
2. Open the following folder: F:\add_on\language
   - Insert the following line in "INI" file: HSK8="MMMR_SC"
     Name "MMMR_SC" can be selected as required.
   - The selected name appears as 8th softkey on the horizontal softkey bar.
     The digit can be selected as required. Ensure that you use the same digit for "Task" in file "regie.ini".
3. Open the following file: F:\add_on\regie.ini
   - Insert the following line in the file: Task8=name := Oemframe, cmdline := "C:\\Program Files (x86)\\Siemens\\MMMR SC\\ManageMyMachinesRemoteServiceClientMO.exe", Timeout :=30000, HeaderOnTop := False, Preload := False, WindowName:=" Manage MyMachines /Remote Service Client"

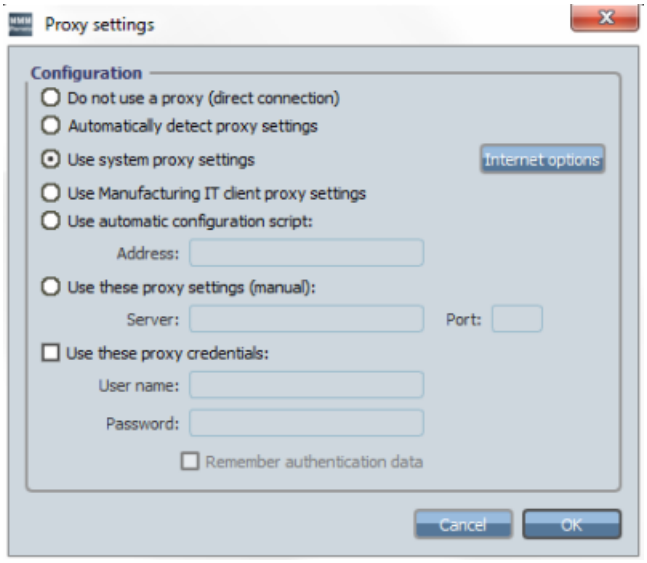
   Note

   Extensions of file "regie.ini"

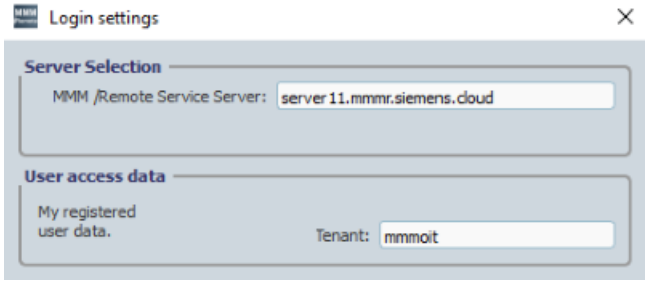
   The following extensions of file "regie.ini" may be required:
   - "Startup42 = name := oemframe, cmdline := "cmd.exe /c F:\\add_on\\MH\ \MhDdeService.exe", Timeout := 60000"
   - "Startup43 = name := oemframe, cmdline := "cmd.exe /c F:\\add_on\\MH\ \MachineHandler.exe", Timeout := 60000"
4. Start HMI-Advanced. The selected name appears as 8th softkey on the horizontal softkey bar. Press the softkey.



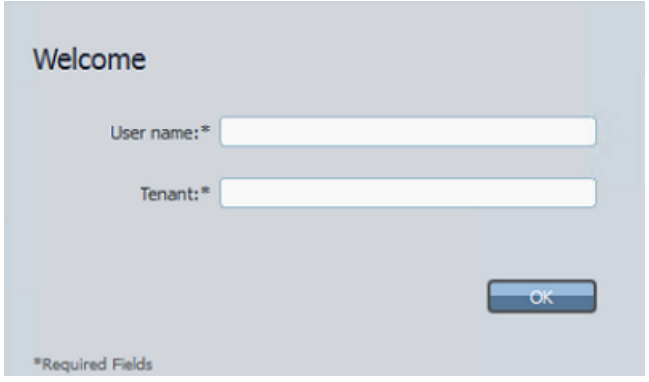
5. ManageMyMachinesRemoteServiceClientMO.exe opens. In the menu bar, call "Settings" > "Proxy...".
   Window "Proxy settings" opens. Check the settings.



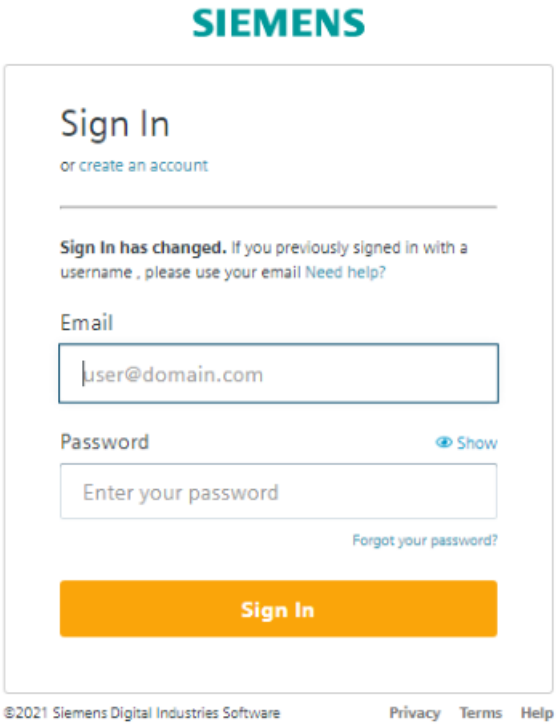
6. In the menu bar, call "Settings" > "Login...".
   Window "Login settings" opens. Check the settings.



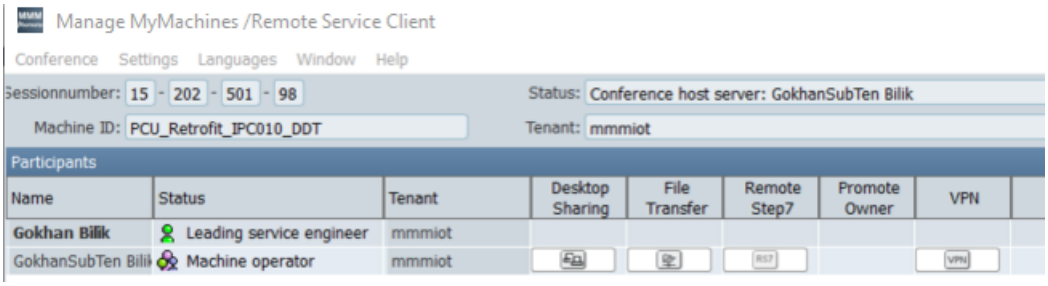
7. Enter your user name and your tenant and then click on "OK".



8. When using for the first time, a "Sign In" browser window will appear for authenticating your machine.
   - Enter your email address and your Insights Hub password.
   - Click on "Sign In".



9. Session window "Manage MyMachines /Remote Service Client" opens.
   The session is established and you see a list of the participants.



Note

Incorrect registration entries

If PCU Retrofit was started in the service mode, then HMI-Advanced must be started using administrator rights, as otherwise additional, incorrect registration entries will be generated for the SInInt client.

If incorrect registration entries were generated, each content that starts with "ePS Network" must be deleted.

Restrictions for active sessions:

If you work in HMI Advanced while a session is active, and you navigate back to the session window "Manage MyMachines /Remote Service Client" via the softkey that was created, in some cases, a gray window opens.

- If you see a gray window, click in the window at a location at which an element should be available. The window is then re-displayed.
- If you cannot use the mouse on the machine operator page, then press "F1" (Help).
- The problem does not occur if a remote access or file transfer operation was already executed.

Integrating Insights Hub

5

5.1 Logging in to Insights Hub

Precondition

You require a MindAccess user account in Insights Hub.

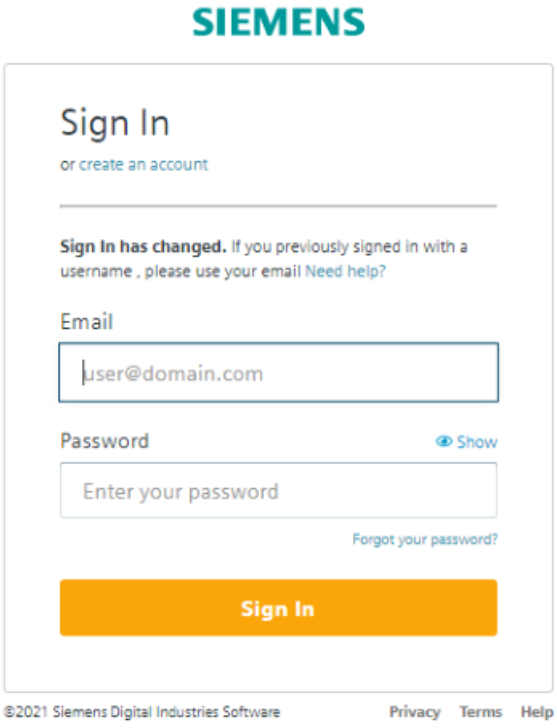
More information on creating an account can be found at:

- "Insights Hub - Settings System Manual"
- "Insights Hub - Asset Manager System Manual"

Procedure

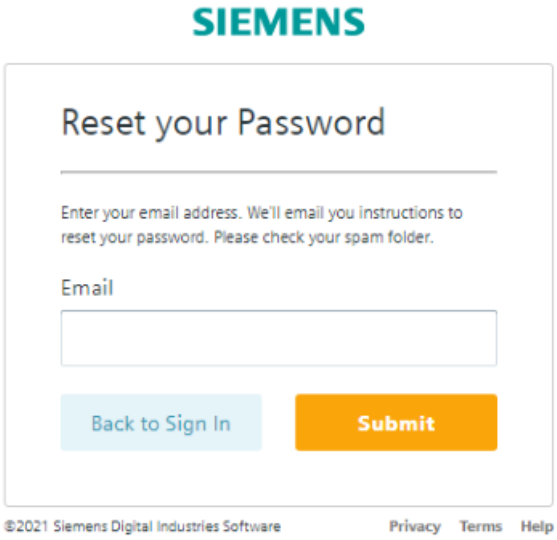
1. Click the link provided by email from Siemens AG.
   The website is displayed: https://<tenant-Name>.eu1.mindsphere.io
   The "Sign In" window opens.
2. Enter your e-mail address and your password.

3. Click on "Sign In".



- OR -
If you have forgotten your password, click "Forgot Password?".
The "Reset your Password" window opens.
Enter your e-mail address and click the "Submit" button.
Your password is reset and you are informed of this via e-mail.

4. Click on "Back to Sign In".



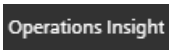
5. The launch pad opens. You can access the individual applications via this user interface.



5.2 Icons and buttons in Insights Hub

Icon	Description
	Switches to the launch pad.
Customer-specific tenant name, e.g. Siemens AG	Opens a menu and shows the following data: • Tenant name • Tenant type • Tenant location

Icon	Description
Manage MyMachines	Opens a menu with the following information: • Shows the version • Copyright Siemens AG Links to the product: • Function Manual • Readme • Application Note • Readme OSS • Insights Hub OSS • Support information • Release notes • Insights Hub status
Siemens Xcelerator	Opens a menu with the following information and links to the product: • Privacy – App Store – Platform status – Platform data • Information – Training Academy – Documentation – Support Center – Online Community – Company • Directive – Permissible use
	Logs out of Insights Hub after a confirmation prompt.
Asset Manager	
Asset Manager	Opens a menu with the following information: • Shows the version • Copyright Siemens AG Links to the product: • Third-party software • Documentation - System Manual Asset Manager
	Hides the list of assets.
	Shows the list of assets again.
Filter	Text box for free text search
	Opens the Asset search
	Switches to the hierarchical view of the assets

Icon	Description
	Edits an asset
	Adds a subordinate asset
	Opens a selection of "Asset Manager" functions, and provides the option of directly accessing the required view. • Share asset • Move asset • Files • Operations Insight • Delete asset
Operations Insight	
	"Operations Insight" is the successor of the "Fleet Manager" application. Opens a menu with the following information and links to the product: • Shows the version • Copyright Siemens AG Links to more information: • Third-party software: Frame Application • Third-party software: Frame Dashboards • Third-party software: KPIs • Third-party software: Work orders • Third-party software Web Components • Third-party software: Tour guide • Documentation - Operations Insight System Manual
Shopfloor Management App	
	Opens a menu with the following information: • Shows the version • Copyright Siemens AG Links to the product: • Function Manual • Readme • Application Note • Readme OSS • Insights Hub OSS • Support information • Release notes • Insights Hub status

Icon	Description
ManageMyMachines /Remote	
Manage MyMachines /Remote	Opens a menu with the following information: • Shows the version • Copyright Siemens AG Links to the product: • Function Manual • Readme • Application Note • Third-party software • Release notes • Insights Hub status

5.3 Managing users

You process/edit users, roles and rights in the Manage MyMachines for Industrial Operations X Cloud "Settings".

More information is provided at: Insights Hub (https://siemens.mindsphere.io/en/docs/mindaccess.html)

User groups and authorizations

For "Manage MyMachines /Remote", you create users with different rights.

The following users are available:

- Administrator:
  - mmmremote.admin

  Can access each Manage MyMachines /Remote function
- Standard user
  - mmmremote.user

  The following restrictions apply:
  "Machine Configuration" area
  - Read-only access
  - Cannot register or log off machines

  Area "Manage remote sessions":
  - Cannot change the status of a session
  - Cannot delete session information

- Subtenant user
  Can only access function:
  - "Download Client"
  - "Start new session"
  - "Manage remote sessions" (read access)

  For machine operators that only install or update the Remote Service Client
- Tenant Administrator
- Shopfloor Management Application administrator
  - shopfloormgmtapp.admin

Procedure

1. In the launch pad, click on the "Settings" application.

   The "Settings" window opens and offers you user administration for editing/processing.
2. Create or edit the users.
3. Assign the corresponding roles.

5.4 Asset Manager

5.4.1 Overview

Functions

"Asset Manager" is a Manage MyMachines for Industrial Operations X Cloud of the Industrial IoT platform from Siemens. In the "Asset Manager", using assets, you model the structure of an industrial process within Insights Hub.

The specific functions and configuration options for the "SINUMERIK" area are discussed in the following.

Using an asset type, you can define which aspects should be integrated into the template. Using asset types, you have the option of creating a template, e.g. for several devices, and linking this with your aspects. When creating a new asset, you can access the template or the type.

Aspects are combined, preconfigured data and form the context for evaluating industrial processes. An aspect can comprise several variables. Within an industrial process, assets

transfer the aspects into the Manage MyMachines for Industrial Operations X Cloud as time series data.

5.4.2 Opening the Asset Manager

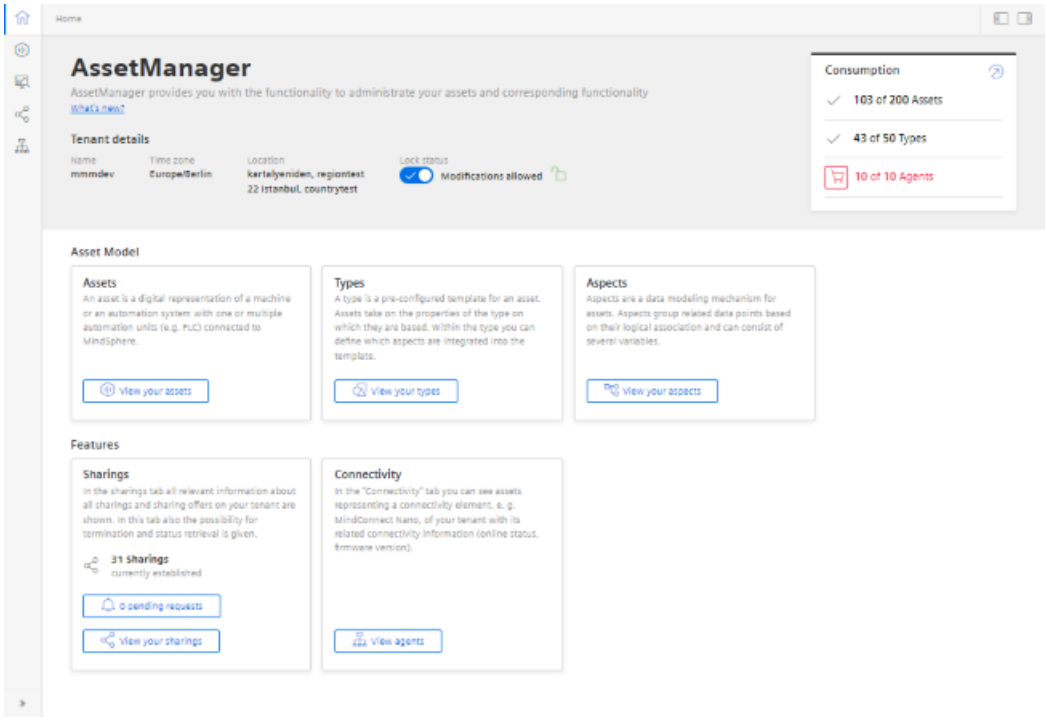
Procedure

1. In the launch pad, click on Manage MyMachines for Industrial Operations X Cloud "Asset Manager".



The "AssetManager" window opens and you have the following options:

- Edit assets
- Add subordinate assets
- Creating assets
  More information can be found in the following section: Creating an Asset (Page 71).
- Creating and editing types
  More information can be found in the following section: Creating an asset type (Page 69)
- Creating and editing aspects



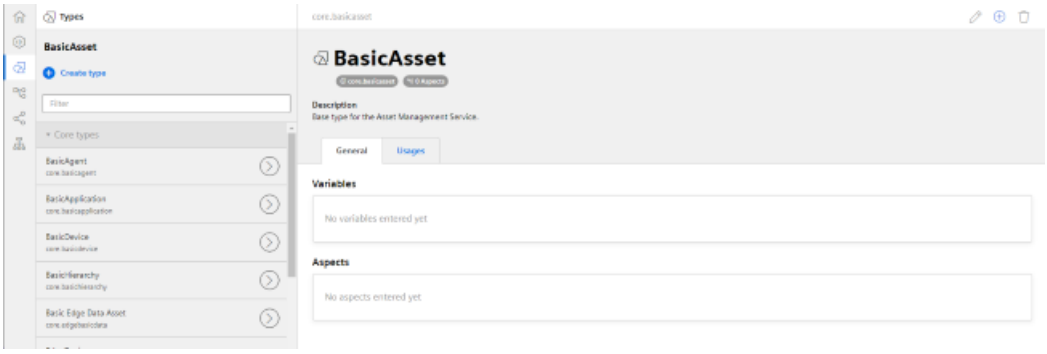
5.4.3 Creating an asset type

The following asset types are supported:

- BasicAsset
- BasicAsset > BasicDevice
- BasicAsset > BasicDevice > BasicSinumerikAsset
- BasicAsset > BasicAgent
- BasicAsset > BasicAgent > MindConnectIoT2040
- BasicAsset > BasicAgent > MindConnectLib
- BasicAsset > BasicAgent > MindConnectNano

Procedure

1. In the left window pane, click the "Library" > "Asset Types" button.
   The "BasicAsset" window opens.



2. Select "BasicDevice" and click on the small arrow (navigate to the child element).
   The "BasicDevice" window opens.

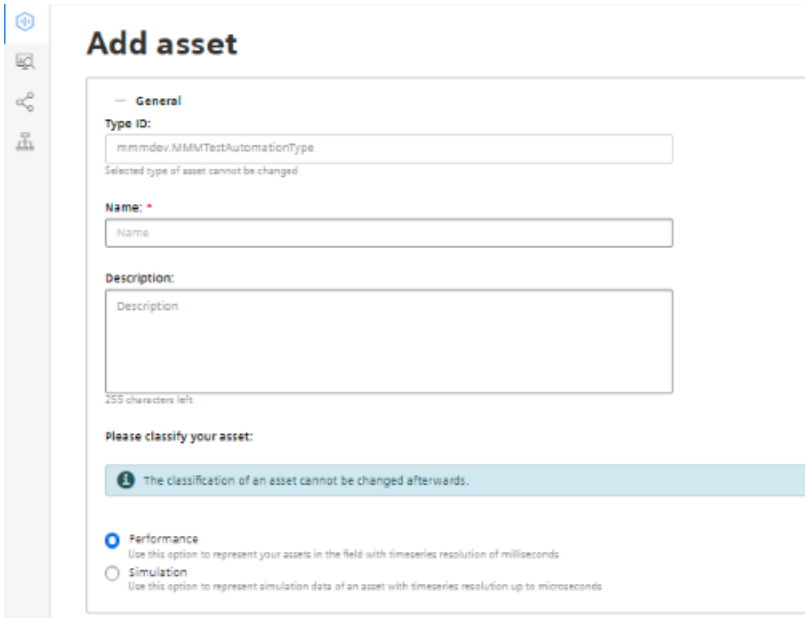
3. Select "BasicSinumerikAsset" and click on the small arrow (navigate to the child element).
   The "BasicSinumerikAsset" window opens.
4. Click on "+ Create type" to create a new asset type.
   The "Create type" window opens.
   - Enter a name for the new asset type.
     You must enter a name and this activates the "Save" button.
   - Enter a description of the new asset type.
   - Select an image with the maximum permitted size of 5 MB.

     Note

     Images in the working area

     Ensure that the name of the image in your working area is unique.

   - Add your chosen variables.
   - Add your chosen aspects.
   - Click "Save" to create the new type.



Filtering an asset type

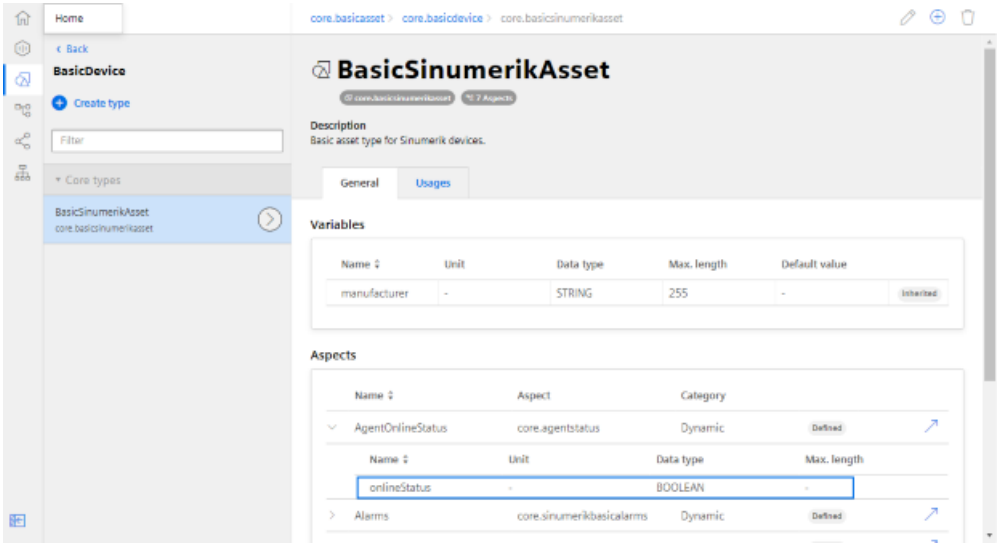
1. Open the "Types" window.
2. In the center window pane, select "BasicDevice" > "BasicSinumerikAsset".
3. In the input field "Filter", enter the name.
   The corresponding data is displayed in the right-hand window area.

5.4.4 Creating an Asset

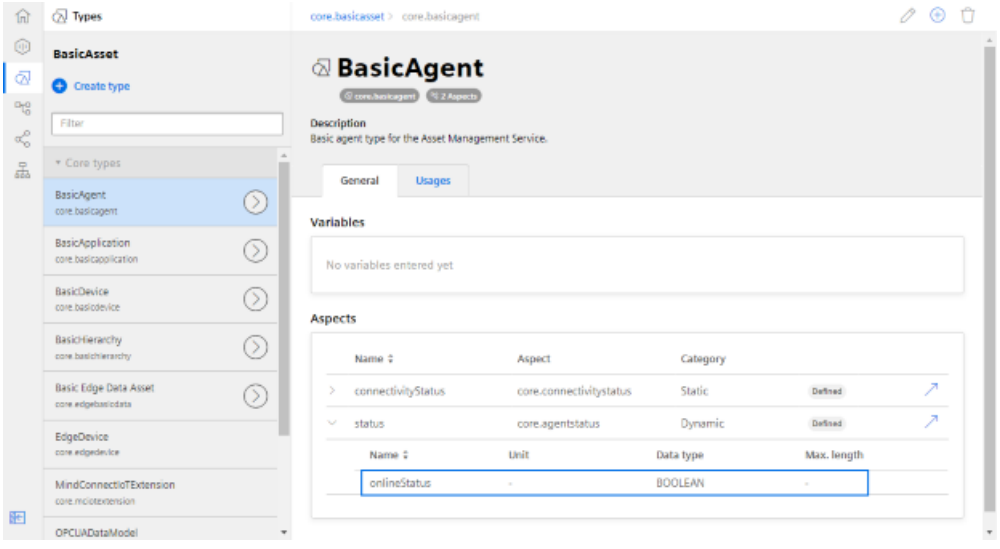
Online status

Manage MyMachines for Industrial Operations X Cloud can evaluate the status of an asset using variable "OnlineStatus". This variable is predefined in the aspects of the following asset types:

- BasicSinumerikAsset



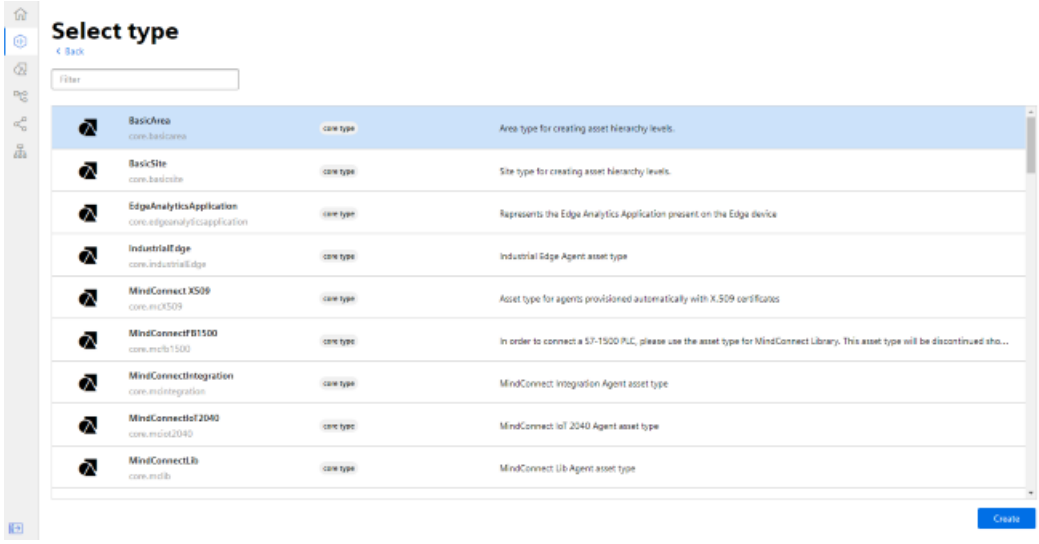
- BasicAgent



To monitor the online status, use an asset type that is based on these types.

Procedure

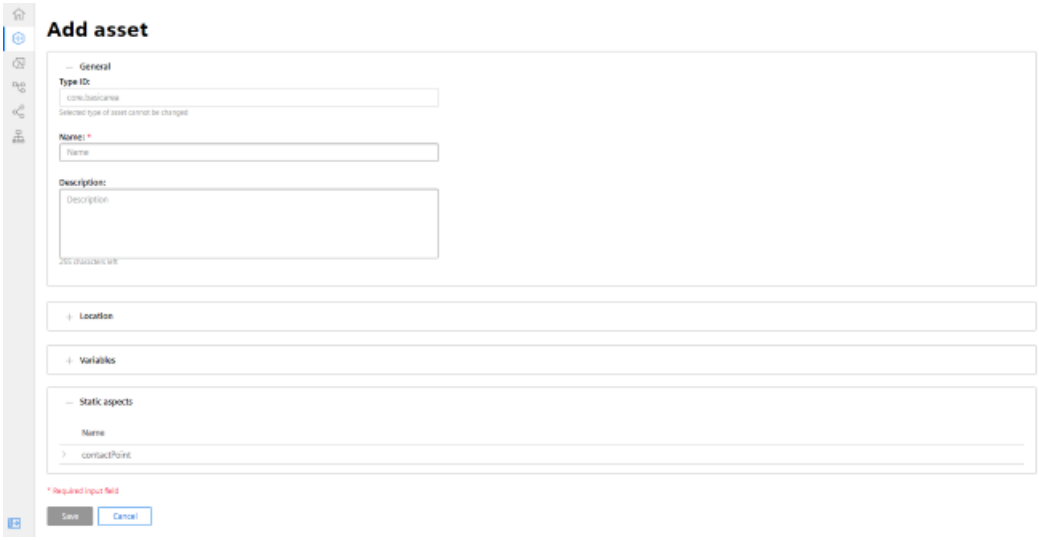
1. In the left window pane, click "Assets".
2. In the center window pane, click "+ Create asset".
   In the right window pane, you can see "Select type".
3. In the "Filter" field, enter the name of the required asset type or select the type that you have just generated from the list.
4. Click on "Create".



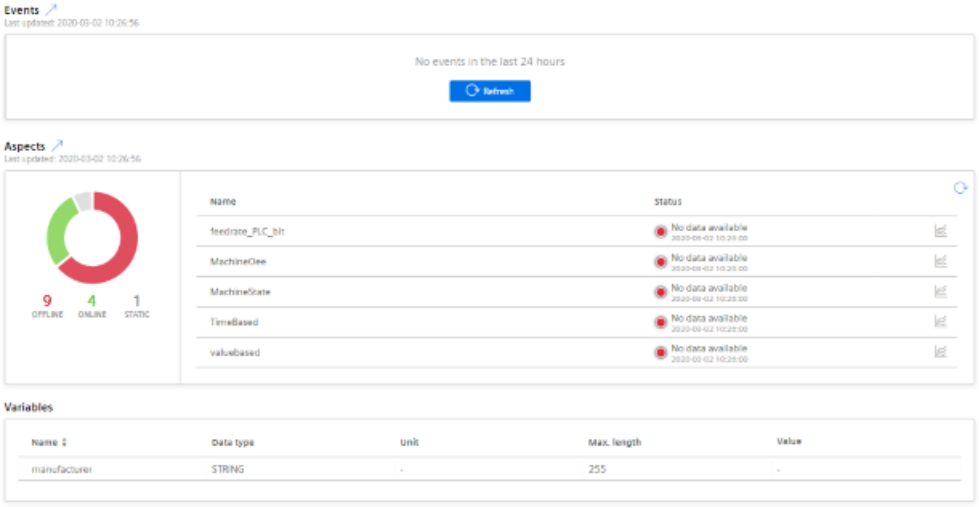
   The "Add asset" window opens.

5. In the "Name: *" input field, enter a name.
   This input field is a mandatory field.

6. Populate the input fields in the "General" and "Location" areas.
   The "Save" button is activated.
7. Click "Save" to save the new asset.



The new asset is displayed.



5.5 Shopfloor Management Application

5.5.1 Overview

Manage MyMachines for Industrial Operations X Cloud "Shopfloor Management Application" has buttons in the left-hand section of the window that allow you to do the following.

- Activation of assets for the application
- Configuring a variable
- Configuration of a gateway

Precondition

You require the following user role to use the Manage MyMachines for Industrial Operations X Cloud "Shopfloor Management Application":

- shopfloormgmtapp

More information is provided in Chapter: Managing users (Page 66).

Buttons

Button	Description
	Select an asset from "Shopfloor". In the "Application" tab, activate or deactivate access to the application "Manage MyMachines /Remote". More information can be found in the following chapters: Billing model UTS (Usage Transparency Service) (Page 75) Billing model PB (Package Builder) (Page 81)
	Under "Gateway", you integrate data from "SINUMERIK Integrate Analyze MyCondition" into Insights Hub. You will find more information in the "Manage MyMachines, Manage MyMachines / Spindle Monitor" Function Manual.
	Window "Machine overview" of the Manage MyMachines for Industrial Operations X Cloud is opened under "MMM". You will find more information in the "Manage MyMachines, Manage MyMachines / Spindle Monitor" Function Manual. Note: The relevant MMM role is a requirement.
	The "Overview" window of Manage MyMachines for Industrial Operations X Cloud "Analyze MyPerformance" is opened under "AMP". More information can be found in the "Analyze MyPerformance" Function Manual.
	Under "SSA" the "SINUMERIK Service Assistance" window opens. You will find more information in the "Manage MyMachines, Manage MyMachines / Spindle Monitor" Function Manual. A precondition is that you have purchased the "SSA" application.

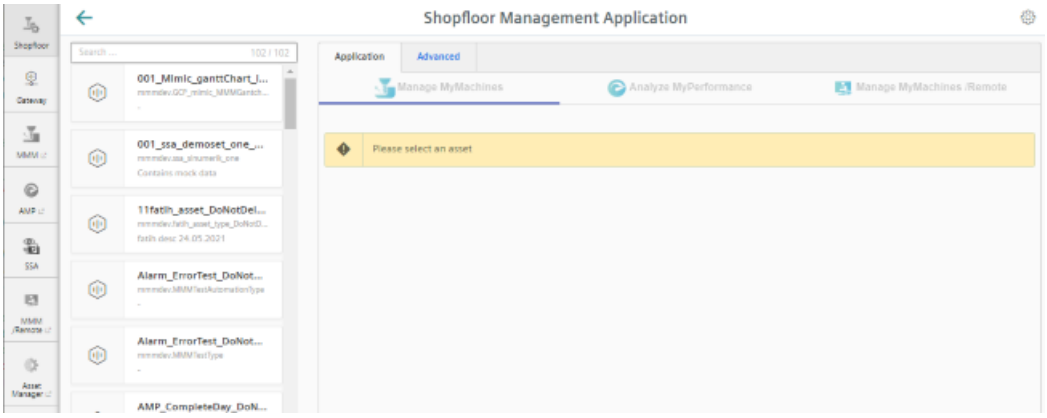
Button	Description
	Window "Navigation view" of the Manage MyMachines for Industrial Operations X Cloud is opened under "MMM /REMOTE". More information is provided in Chapter: Working with Manage MyMachines /Remote (Page 89)
	Manage MyMachines for Industrial Operations X Cloud "Asset Manager" is opened under "Asset Manager". You will find more information in the "Manage MyMachines, Manage MyMachines / Spindle Monitor" Function Manual.

Procedure

1. In the launch pad, open the Manage MyMachines for Industrial Operations X Cloud "Shopfloor Management App".



2. Window "Shopfloor Management Application" > "Shopfloor" opens.
Select the required asset in the center of the window area.



5.5.2 Billing model UTS (Usage Transparency Service)

5.5.2.1 Activating Manage MyMachines /Remote

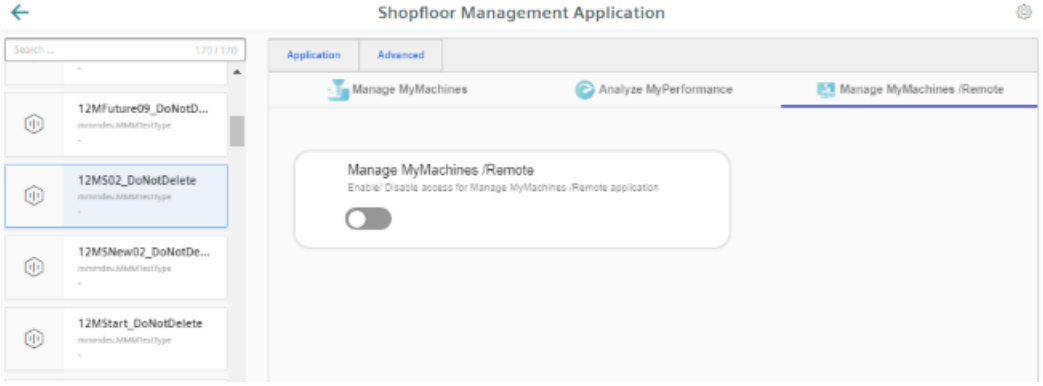
Precondition

- You have purchased Manage MyMachines for Industrial Operations X Cloud.
- You require the following user roles:
  - Tenant admin and shopfloormgmtapp.admin

  More information is provided in Chapter: Managing users (Page 66).

Procedure

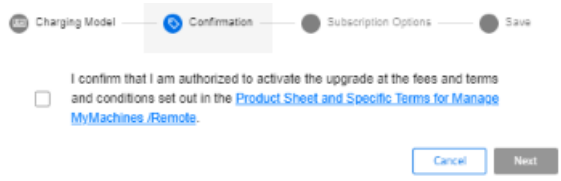
1. In the launch pad, click on Manage MyMachines for Industrial Operations X Cloud "Shopfloor Management App".
2. Window "Shopfloor Management Application" > "Shopfloor" > tab "Application" > "Manage MyMachines" opens.
   - Select the required asset on the left-hand side of the window.
     To filter the assets, enter a character string in the "Search ..." field.
   - Select the "Application" tab > Manage MyMachines /Remote in the upper right corner.
   - To activate the use of "Manage MyMachines /Remote" for this asset, set the slider to the right to activate access to "Manage MyMachines /Remote".



3. A pop-up "Charging model" opens.
   - Activate option button "1 month enablement (charged monthly in areas)"
     - OR
     Activate option button" 12 months enablement (charged annually upfront)"
   - To confirm the selection, click on "Next".
     - OR -
     If you do not wish to keep the selection, then click on "Cancel".



4. Click on link "Product Sheet and Specific Terms for Manage MyMachines/Remote". Carefully read the information.
   - Activate the "I confirm that I am authorized to activate the upgrade at the fees and terms and conditions set out in the Product Sheet and Specific Terms for Manage MyMachines/ Remote." check box.
   - Click on "Next".



5. Activate the "Start Now (Automatically renewed)" option button to start the runtime with the current date.



- OR -
Activate the "Custom Duration" option button to specify the runtime individually.

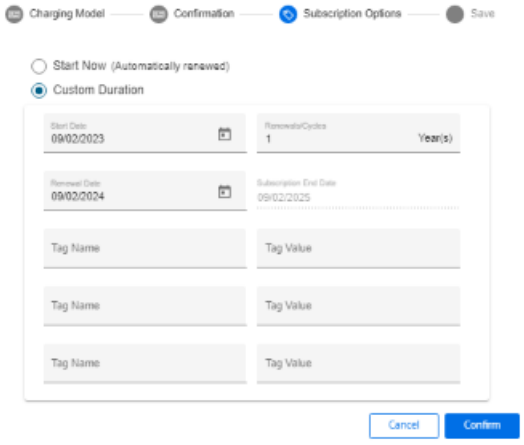
– In the "Start Date" text box, open the calendar to define the start date.
In the "Renewal Date" text box, open the calendar to set the start date.

– In the "Renewals/Cycles" input field, specify the renewal period in years.

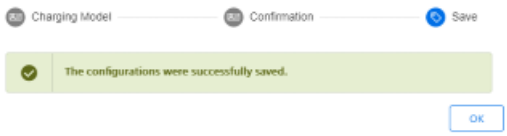
– The "Subscription End Date" field is automatically populated if you define the "Start Date", "Renewal Date" and "Renewals/Cycles" text boxes. The subscription end date obtained from the renewal period is displayed.

– Add the individual tag names in text box "Custom-Tag Name".
Add the individual tag values in text box "Custom-Tag Value".

– Click "Cancel" to exit the procedure.
- OR -
Click the "Confirm" button to confirm the time period.



6. You will receive a confirmation that the configuration has been saved successfully. Click the "OK" button to close the message.

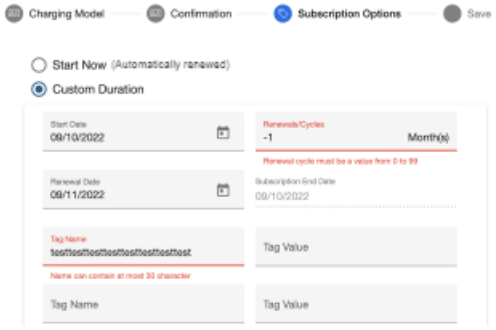


7. Data acquisition is initiated if the "Start Now" (Automatically renewed) option is enabled or the "Custom Duration" option is enabled and the start date is set to "Today".
If the "Custom Duration" option is enabled and the start date is not set to "Today", data acquisition will start at the date you specified.

Editing the billing period

When entering the data for the custom period, note the following:

- The renewal cycle for years/months must be between 0 and 99.
- The key of the custom tag and the value of the custom tag must not exceed 30 characters.



Manage MyMachines /Remote Product Sheet and Specific Terms

If you click on link "Product Sheet and Specific Terms for Manage MyMachines /Remote", window "Manage MyMachines /Remote Product Sheet and Specific Terms" opens.

You obtain information about the product:

- Preconditions
- A brief product description
- Cost model
- Special Terms & Conditions
- Export control regulations
- Safety information
- Explanation of terms

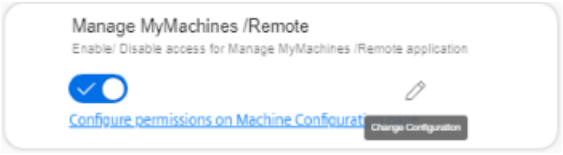
Changing the billing period

Note

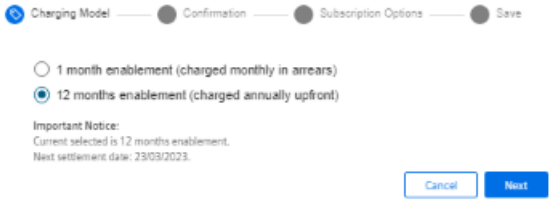
Multiple billing when changing the start date or subscription option

If you change the start date of an active billing period or the subscription option, then you receive a new billing, even if the new billing period already lies in the active billing period.

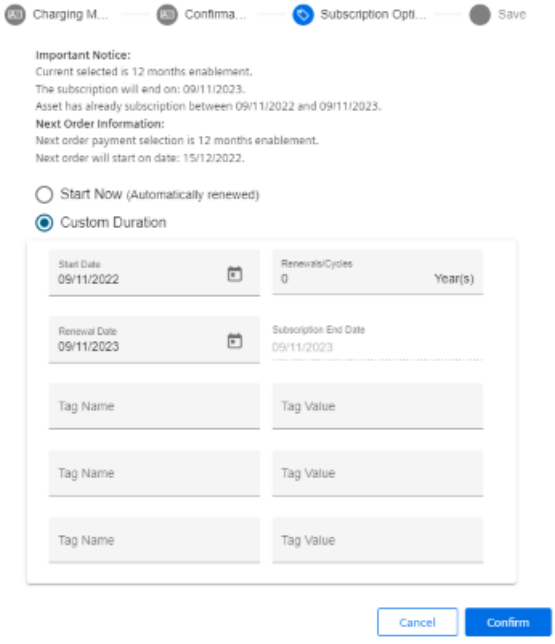
1. To change the billing period, click the "Change Configuration" icon.



2. A pop-up "Charging model" opens. You are notified of the next billing date.



3. The "Subscription Options" pop-up contains a note that the subscription for the asset is already active for a billing period.
   - If you change the "Renewal date" or the "Renewals/Cycles" of the billing period, the newly selected option will not take effect until the end of the currently active subscription option.
   - If you change the "Start date" of the billing period, the newly selected option becomes active at the defined start date.
     The billing occurs either on the same day or later.



4. If you set the billing period in the future, you will see the activation date and the slider will be displayed in yellow.

5.5.3 Billing model PB (Package Builder)

5.5.3.1 Activating Manage MyMachines /Remote

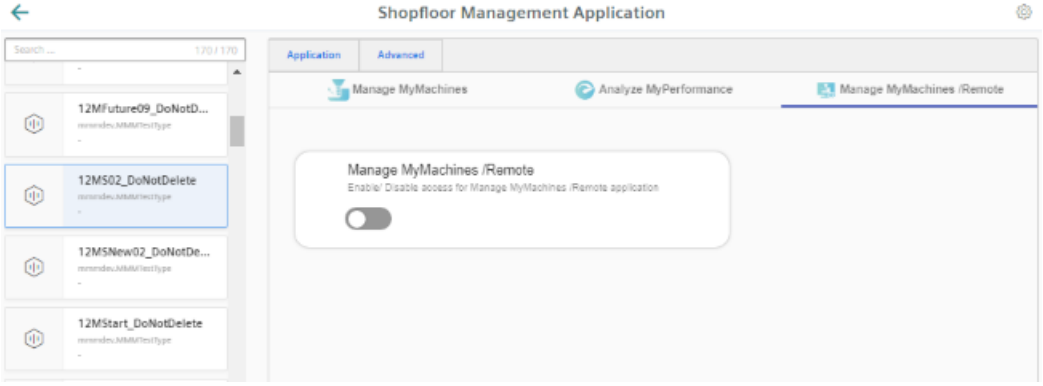
Precondition

- You have purchased Manage MyMachines for Industrial Operations X Cloud "Manage MyMachines /Remote" and you have a package quota to activate the use of "Manage MyMachines /Remote" for assets.
- You require the following user roles:
  - Tenant admin and shopfloormgmtapp.admin

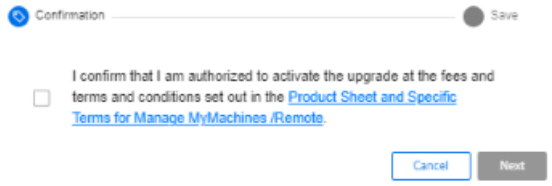
  More information is provided in Chapter: Managing users (Page 66).

Core statement

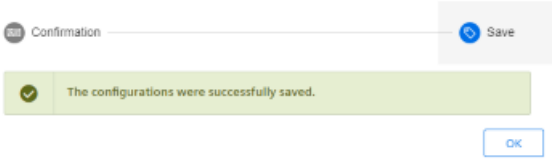
1. In the launch pad, click on Manage MyMachines for Industrial Operations X Cloud "Shopfloor Management App".
2. Window "Shopfloor Management Application" > "Shopfloor" > tab "Application" > "Manage MyMachines" opens.
   - Select the required asset on the left-hand side of the window.
     To filter the assets, enter a character string in the "Search ..." field.
   - Select the "Application" tab > Manage MyMachines /Remote in the upper right corner.
   - To activate the use of "Manage MyMachines /Remote" for this asset, set the slider to the right to activate access to "Manage MyMachines /Remote".



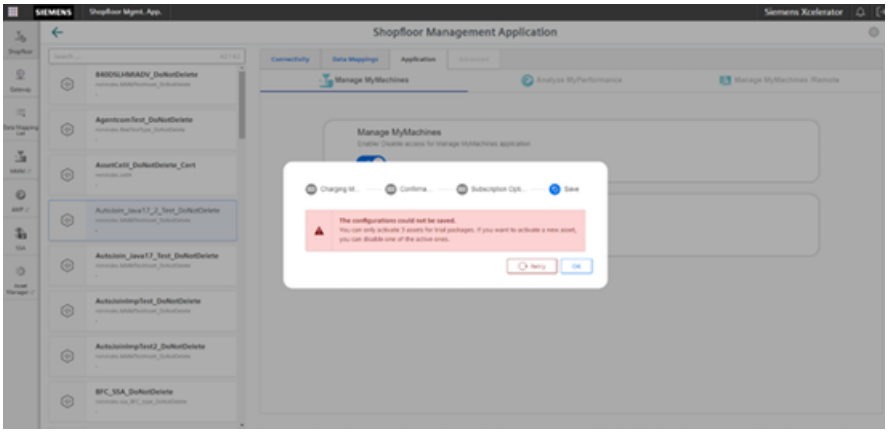
3. A "Charging model" pop-up opens.
   Click on link "Product Sheet and Specific Terms for Manage MyMachines/Remote". Carefully read the information.
   - Activate the "I confirm that I am authorized to activate the upgrade at the fees and terms and conditions set out in the Product Sheet and Specific Terms for Manage MyMachines/ Remote." check box.
   - Click on "Next".
     - OR -
     Click on "Cancel" to cancel the operation.



4. You will receive a confirmation that the configuration has been saved successfully.
   Click the "OK" button to close the message.



   - OR -
   You receive a message that the configuration was not able to be saved as the activated assets exceed the packages in your tenant.
   Update your package quota and click on "Repeat".



5.5.4 Changing the billing model

You have the option to migrate an application, for example "Manage MyMachines" from a UTS-based billing model to a PB-based billing model or vice versa.

When migrating from a UTS-based to a PB-based billing model, the assets activated for the application are kept. They are not deactivated. However, it is possible that the application will not function correctly.

When migrating from a PB-based to a UTS-based billing model, the application is deactivated for already activated assets.

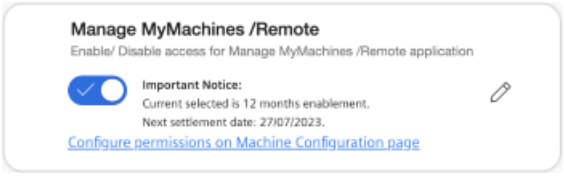
5.5.5 Calling a machine configuration

Precondition

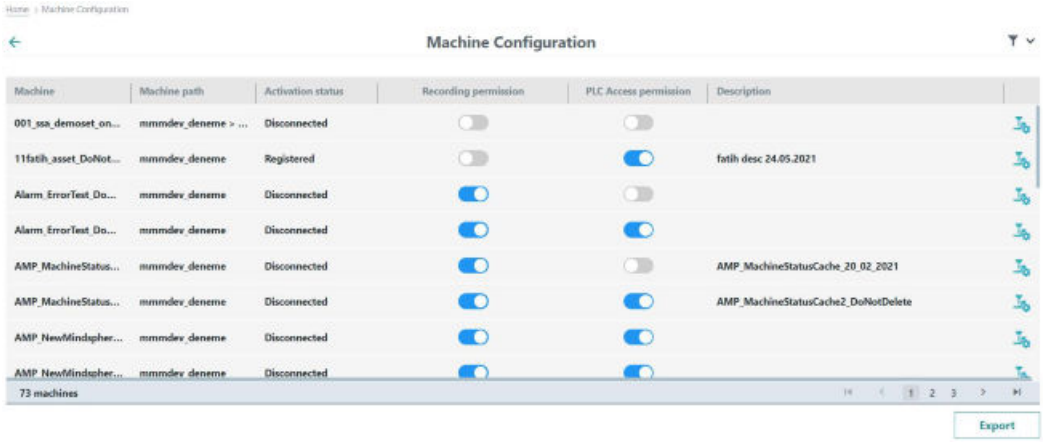
- You have activated Manage MyMachines for Industrial Operations X Cloud "Manage MyMachines /Remote".

Procedure

1. Click on the link "Configure permissions on Machine Configuration page".



2. Window "Machine configuration" opens.
Click on button to return to the "Shopfloor Management Application" window and the relevant asset.



5.6 Connecting SINUMERIK controls with Insights Hub

Connect SINUMERIK controls with Insights Hub using the Manage MyMachines for Industrial Operations X Cloud "Shopfloor Management App".

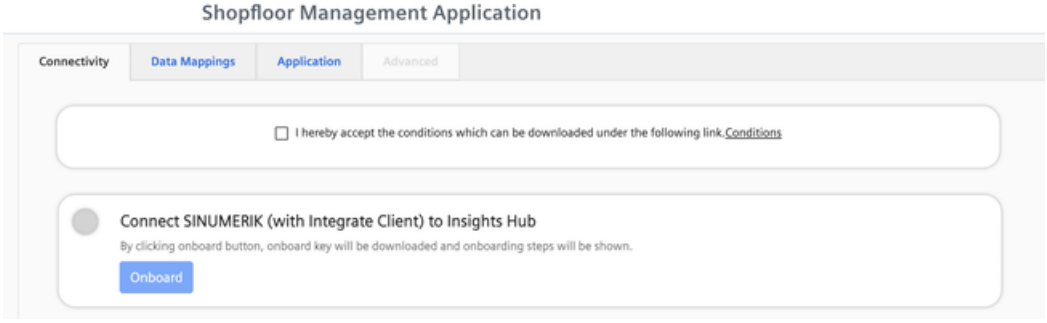
More information about roles within Insights Hub and on configuring assets is provided in: Documentation Insights Hub (https://siemens.mindsphere.io/en/docs/mindaccess.html)

Precondition

- Manage MyMachines for Industrial Operations X Cloud is activated.
- You require the "MindAccess User" role in Insights Hub to do this.
- The configuration must have been saved.

Procedure

1. Click on Manage MyMachines for Industrial Operations X Cloud "Shopfloor Management App".
2. Select the required asset in the left-hand side of the window.
3. Click in the "Connectivity" tab in the right-hand section of the window.
4. Select check box "I accept the conditions, which can be downloaded from the following link. Conditions".
   - Click on the "Conditions" link.
     The "Insights – Terms & Conditions" window opens.
   - Click on your region.
   - From the list, select the appropriate Terms & Conditions.
   - Read the Terms & Conditions.
     - OR -
     Download the Terms & Conditions.
     - OR -
     Print the Terms & Conditions.
   - Close the window.
     The "Connectivity" tab is displayed again.
5. Activate option button "Connect SINUMERIK (with Integrate Client) to Insights Hub" and click on "Onboard" to connect the asset with Insights Hub.

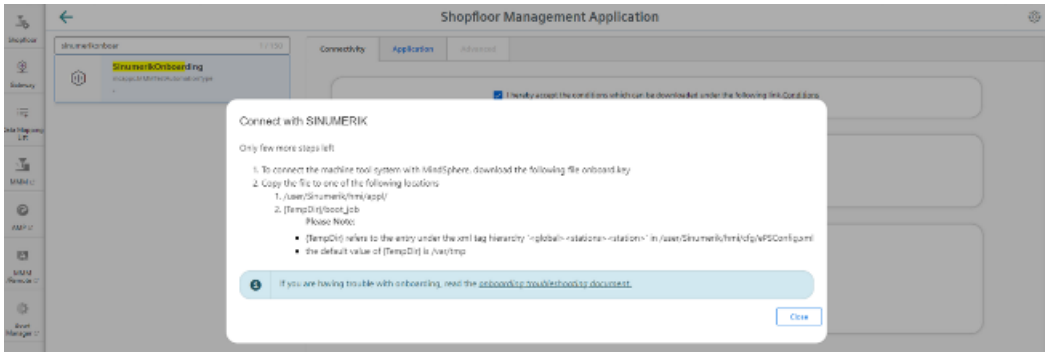


6. The "onboard.key" is generated. Window "Connect with SINUMERIK" opens.
   - Download file "onboard.key".
   - Copy the file to one of the specified storage locations in the controller.
     More information can be found in the following chapters:
     SINUMERIK 828D: Install the registration key on a SINUMERIK control system (Page 50)
     SINUMERIK 840D sl: Install the registration key on a SINUMERIK control system (Page 43)
   - Call the troubleshooting document if you have problems with onboarding.

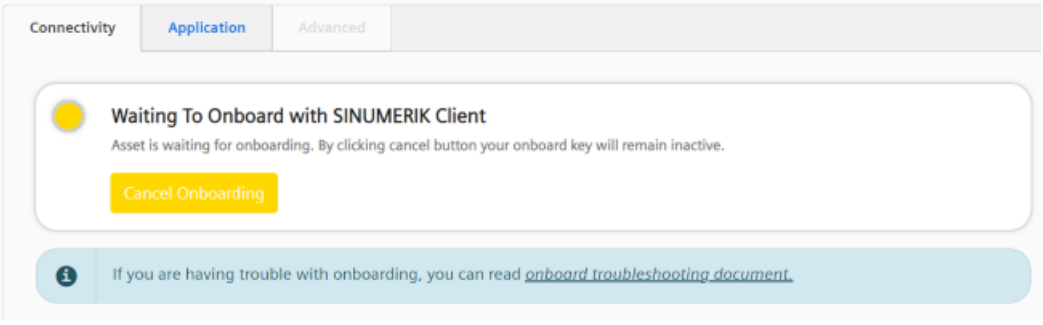
Note

Machines with IPC MO client

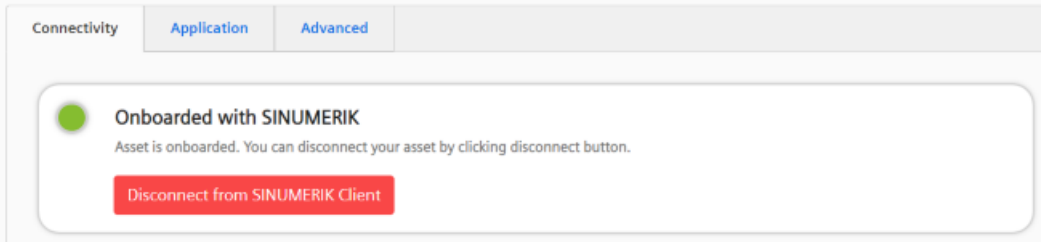
For machines with an IPC MO client, no "onboard.key" is required.



7. The status is displayed as "Waiting to Onboard with SINUMERIK Client".
   Here, you can also call the document for troubleshooting during the onboarding process: Troubleshooting when onboarding (Page 209)
   – Wait until the status changes to "Onboarded with SINUMERIK".
   - OR -
   – Click on button " Cancel Onboarding" to cancel the operation.
   The window with the two connection options re-opens.



8. The connection was successfully established, and the status is displayed as "Onboarded with SINUMERIK".



Working with Manage MyMachines /Remote

6

6.1 Open Manage MyMachines /Remote

Precondition

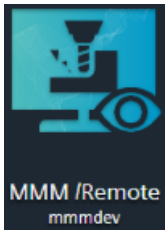
- The SINUMERIK control has been successfully connected with Insights Hub.
- The owner of the tenant, in which the Manage MyMachines /Remote application is operated, must use Multi Factor Authentication (MFA).

More information

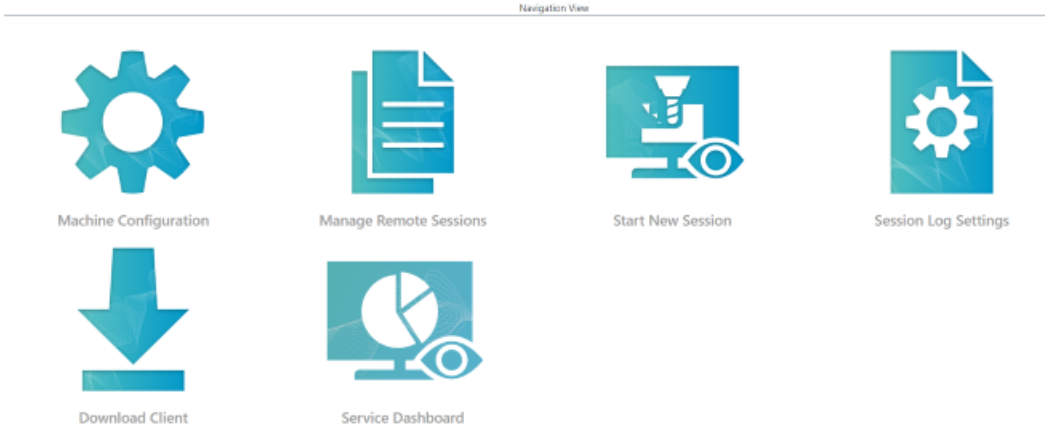
- Information on how to connect a SINUMERIK controller can be found in the chapter: Setting up the SINUMERIK control system for Manage MyMachines /Remote (Page 25).
- Information about the owners of the tenant is provided in the System Manual: User Management, in the chapter: "Administering users"
- If you have the authorization level of a subtenant, you have restricted access authorization and you **cannot** access the following functions:
  - Machine Configuration
  - Session Log Settings

Procedure

1. To open Manage MyMachines /Remote, click on the "MMM /Remote" symbol.



2. The "Navigation View" window opens and you have the following options:
   - Machine Configuration
     More information on this topic can be found in the chapter: Machine Configuration (Page 91)
   - Manage Remote Sessions
     More information on this topic can be found in the chapter: Using MyMachines /Remote Service Client (Page 155)
   - Start New Session
     More information on this topic can be found in the chapter: Starting a remote session as a SE (Page 99)
   - Session Log Settings
     More information on this topic can be found in the chapter: Configuring the session log settings (Page 111)
   - Download Client
     More information on this topic can be found in the chapter: Download remote service client (Page 94) and Download certificate (Page 96)
   - Service Dashboard
     More information on this topic can be found in the chapter: Service Dashboard (Page 125)



Navigation view for subtenant

If you open Manage MyMachines /Remote with the authorization of a Subtenant, you only have access to the following functions:

- Managing remote sessions - only read access
- Start New Session
- Download Client

6.2 Machine Configuration

You have the possibility of registering SINUMERIK control systems for Manage MyMachines / Remote and authorization to issue session recordings.

Precondition

You require the appropriate authorization levels.

More information can be found in Chapter: Managing users (Page 66).

You cannot use the function if you only have "Subtenant" authorization.

Parameters

Parameter/icon	Description
Machine	Displays the name of the SINUMERIK control system.
Machine path	Shows the path of the SINUMERIK control system.
	The "Released" icon indicates a released asset.
Activation status	Displays the state of the SINUMERIK control system: • Registered • Disconnected
Recording permission	Displays whether the authorization for recording the session is available or not: • Yes • No
PLC Access permission	Displays whether authorization to access the PLC is available or not: • Yes • No
Description	Shows an individual description.
	The "Manage MyMachines /Remote" start page opens.

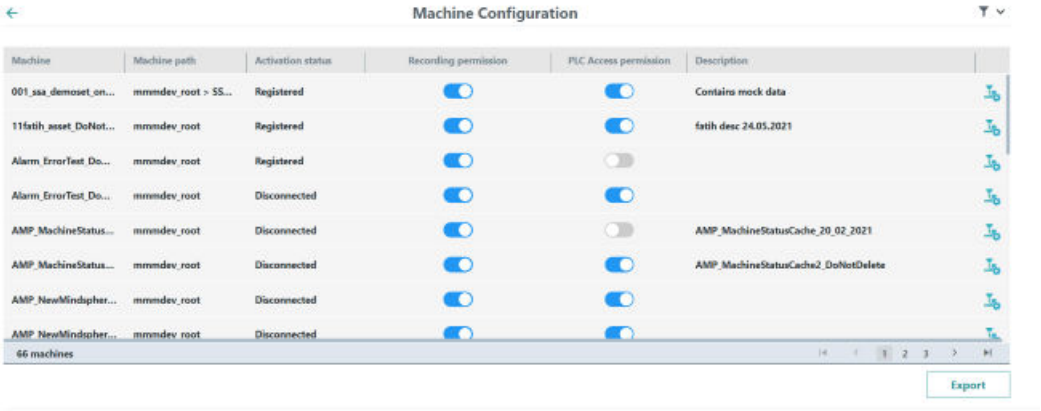
Parameter/icon	Description
	Opens window "My Filters" to filter the SINUMERIK control systems (machines) according to specific criteria. Attributes: • Machine path • Activation status • Recording permission • PLC Access permission
	In the "My Filters" window you add additional values for the search.
	Deletes a filter criterion in window "My Filters".
	Closes window "My filters".
	Indicates whether session recording or PLC access is allowed or not.
	The "Shopfloor Management application" icon opens the "Shopfloor Management application" window and calls the corresponding asset.
Export	Exports the displayed list in the CSV format.

Procedure

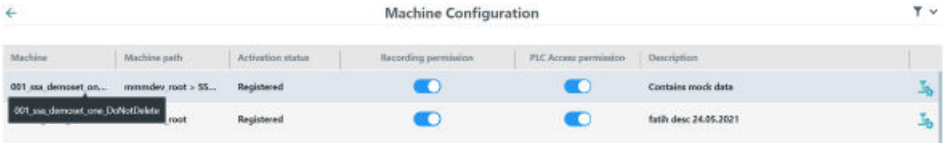
1. Click the "Machine Configuration" button.



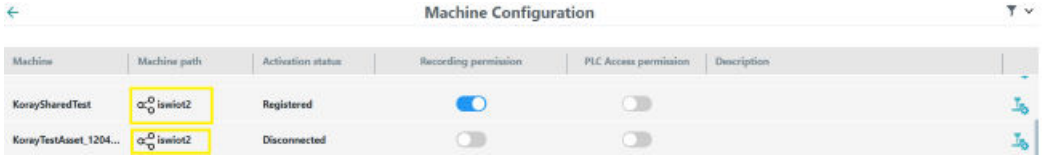
2. The "Machine Configuration" window opens and shows the overview of the SINUMERIK control systems (machines).
   - You can enlarge or reduce the individual columns in the overview.
   - In the status bar you can see the number of acquired machines in the left area and the number of window pages in the right area.



   - If the entry is too long, this is indicated by three dots.
     If you move the mouse pointer over the entry, the complete entry is displayed in a tooltip.



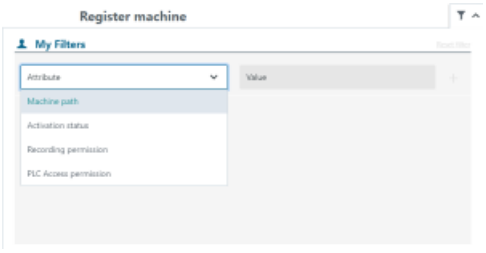
   - Distributed machines are shown to you in the "Machine path" column with an icon and the <name>.



3. Select a SINUMERIK control system (machine) and click on "Edit".

Filtering machines

1. Click on the "Filter" symbol.
   The "My Filters" window opens.
2. Select the required filter criterion from list "Attribute".



3. Select the required value from list "Value".
4. Add the filter criterion for the current filter using the "+" icon.
   Remove the corresponding filter criterion using the "Delete" symbol.
5. Click on "Reset Filters" to remove all filters.

Export overview

1. Filter the list if necessary.
2. Click on "Export".
   The displayed list is exported in the CSV format, and is saved in the download directory of the browser.
3. The file is displayed in the lower left-hand section of the window. You have the following options:
   - Open
   - Always open a file of this type
   - Display in folder:

6.3 Download remote service client

Precondition

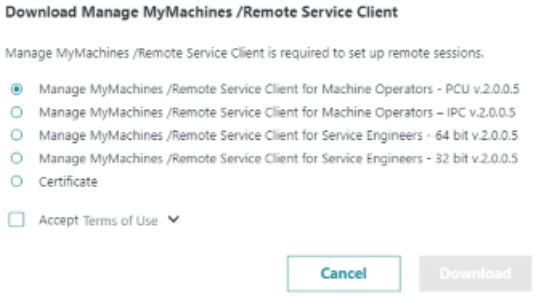
The SINUMERIK control has been successfully connected with Insights Hub.

Procedure

1. Click the "Download client" button.



2. The "Download Manage MyMachines Remote Service Client" opens and lists these options:
   - "Manage MyMachines /Remote Service Client for machine operators - PCU from Vx.x.x.x.": Client for installation on the SINUMERIK control system (PCU) with version data
   - "Manage MyMachines /Remote Service Client for machine operators - IPC from Vx.x.x.x": Client for installation on the IPC with version data
   - "Manage MyMachines /Remote Service Client for service engineers - 64 bit from Vx.x.x.x": Client for installation on an operating PC with a 64-bit operating system with version data
   - "Manage MyMachines /Remote Service Client for service engineers - 32 bit from Vx.x.x.x": Client for installation on an operating PC with a 32-bit operating system with version data



3. Behind "Accept", click on "Terms of Use" or the small arrow and read the associated information.
   Then activate option checkbox "Accept Terms of Use".
   If you wish to cancel the operation, then click "Cancel".
   - OR -
   To download the corresponding version, activate the check box and click "Download".
4. Then carry out the installation and configuration.

More information can be found in the following chapters:

Setting up Manage MyMachines /Remote - Machine operators (MO) (Page 131)

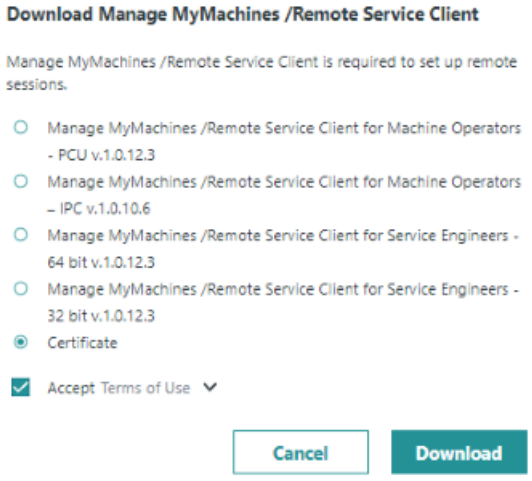
Setting up Manage MyMachines /Remote - service engineer (SE) (Page 144)

6.4 Download certificate

Procedure

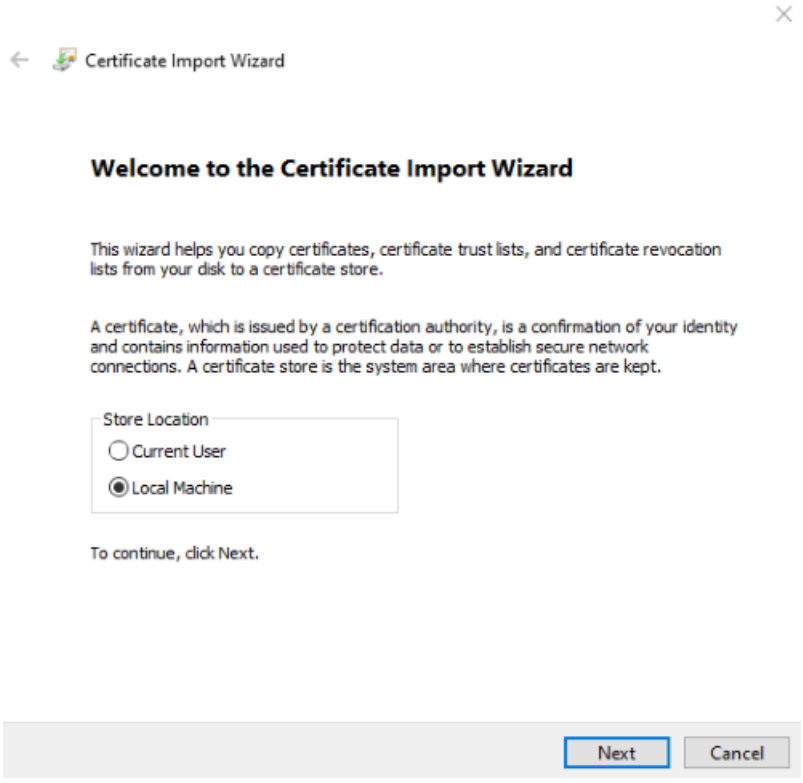
1. Click the "Download client" button.
2. Window "Download Manage MyMachines /Remote Service Client" opens.
   - Activate the "Certificate" option button.
   - Behind "Accept", click on "Terms of Use" or the small arrow and read the associated information.
     Then activate option checkbox "Accept Terms of Use".

   If you wish to cancel the operation, then click on "Cancel".
   - OR -
   To download the certificate, click on "Download".



3. The certificate is located in the lower left-hand section of the window.
4. Open the file.
   You can obtain information about the certificate.

5. Click on "Install certificate...".
   The certificate import wizard opens.
   – Activate the "Local computer" option button, and click the "Next" button.



6. The certificate store window opens.
   – Activate the "Place all certificates in the following store" option button.
   – Click on "Browse..." and select the "Trusted Root Certification Authorities".
   – Click on "Next".
7. Window "Completing the wizard" opens and lists the settings.
   Click on the "Finish" button.
8. Then install and configure the MyMachines /Remote service client.

More information can be found in the following chapters:

Installing Manage MyMachines /Remote Service Client MO (IPC or PCU) (Page 132)

Installing Manage MyMachines /Remote Service Client SE (Page 144)

6.5 Remote sessions

6.5.1 Overview

Precondition

The necessary client software has already been installed on the SINUMERIK control or the operator PC and has been configured.
More information can be found in the following chapters:

Setting up Manage MyMachines /Remote - service engineer (SE) (Page 144)

Setting up Manage MyMachines /Remote - Machine operators (MO) (Page 131)

Example

The following description is an example scenario.

1. The machine operator contacts the service engineer with a problem.
2. The service engineer starts a session in the Manage MyMachines for Industrial Operations X Cloud "Manage MyMachines /Remote" and opens the Manage MyMachines / Remote Service Client.
   More information on this topic can be found in Chapter: Starting a remote session as a SE (Page 99)
3. The service engineer informs the machine operator that a session has been initiated.
4. The machine operator at the SINUMERIK control system opens the Manage MyMachines / Remote Service Client and logs on for the session.
   More information can be found in the following chapters:
   - Joining a remote session as MO (PCU/NCU) (Page 157),
   - Joining a remote session as MO (IPC) (Page 160)
5. All of the functions are available as soon as both participants have entered the session:
   - Desktop sharing, including remote control
   - File transfer
6. Additional or monitoring participants can enter a session.
   More information on this topic is provided in Chapter: Joining a remote session (Page 103)
7. The data from a session is recorded and can be viewed in an overview in the MindSphere application Manage MyMachines for Industrial Operations X Cloud "Manage MyMachines / Remote".
   The data is thus still available at a later point in time.
   More information is provided in Chapter: Managing remote sessions (Page 104)

8. You can review a session in more detail - and you have the opportunity of changing and exporting log files.
   More information is provided in Chapters: Evaluating and editing session information (Page 112) and Exporting session information (Page 116)
9. The service engineer can provide a new certificate.
   More information is provided in Chapter: Download certificate (Page 96)

6.5.2 Starting a remote session as a SE

Only a service engineer can start a remote session.

Note

If you click the "Start new session" button and select an asset that is not online in Insights Hub or is not connected with the "Manage MyMachines" application, then the following warning message is displayed:
"The following action may not be possible due to a connection problem. Please confirm that the machine has an online connection."

You can still continue the process.

Note

Restrictions for simultaneous sessions

Do not start parallel sessions for the same asset with different users at the same time in different browsers. This results in undesirable behavior, such as two separate sessions for a single asset. The machine operator participates in the session that was started first.

Note

Note for machine operators

Do not press the "MMM /R" softkey until the service engineer has opened a new remote access session. Otherwise the connection may not be established.

Procedure

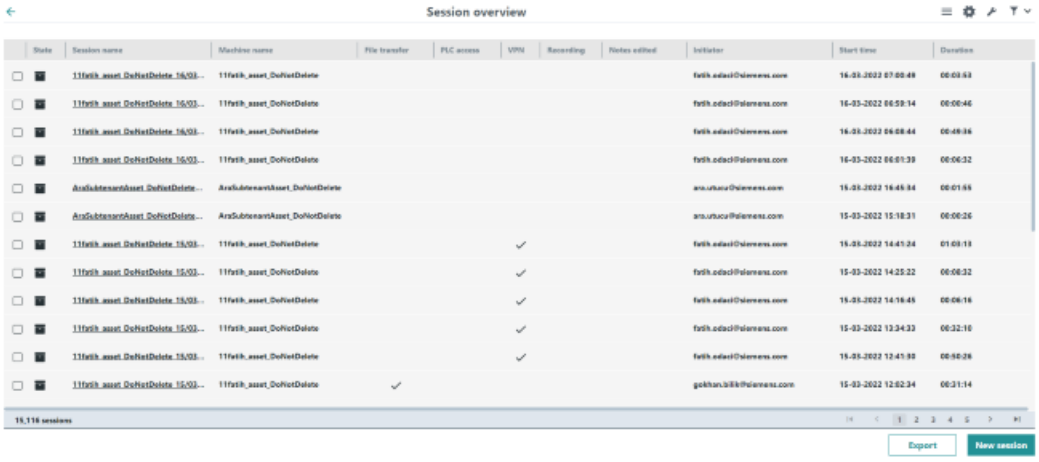
1. Click on "New session".



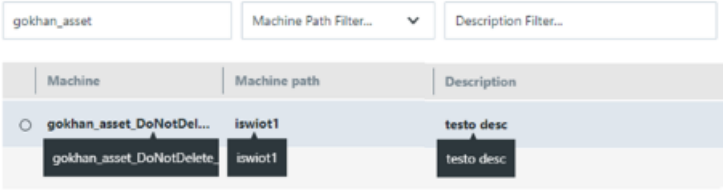
- OR -
Click on the "Manage remote sessions" button.



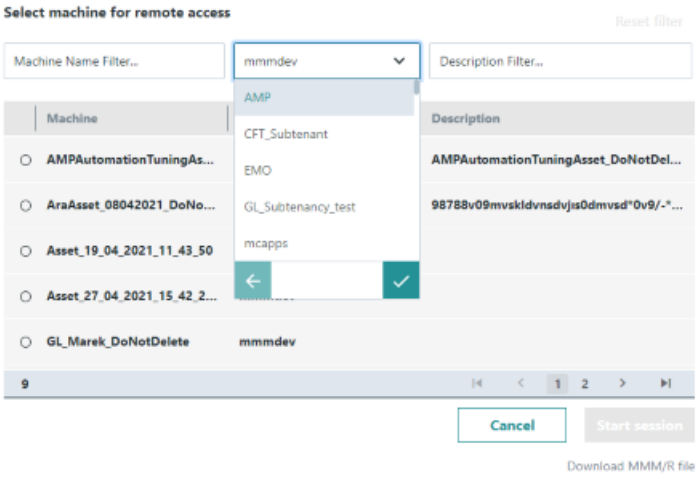
The "Session overview" window opens and displays an overview of all sessions.
Click on "New session".



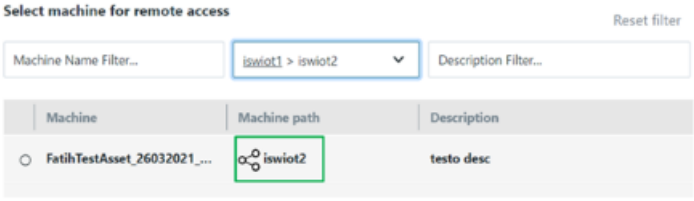
2. The "Select machine for remote access" window opens.
   - You can enlarge or reduce the individual columns in the overview.
   - If the entry is too long, this is indicated by three dots.
     If you move the mouse pointer over the entry, the complete entry is displayed in a tooltip.



– Select a machine directly from the list.
- OR -
Set a filter for the machine name, machine path or description.

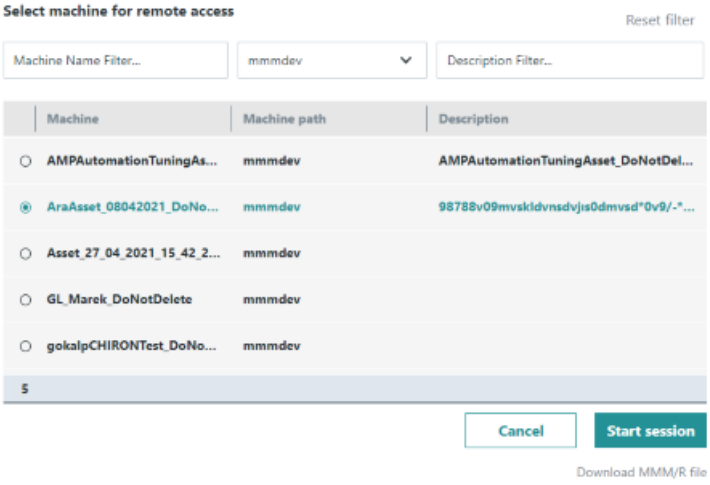


3. Afterwards mark the desired machine.
Released machines are shown to you in the "Machine path" column with an icon and the <name>.



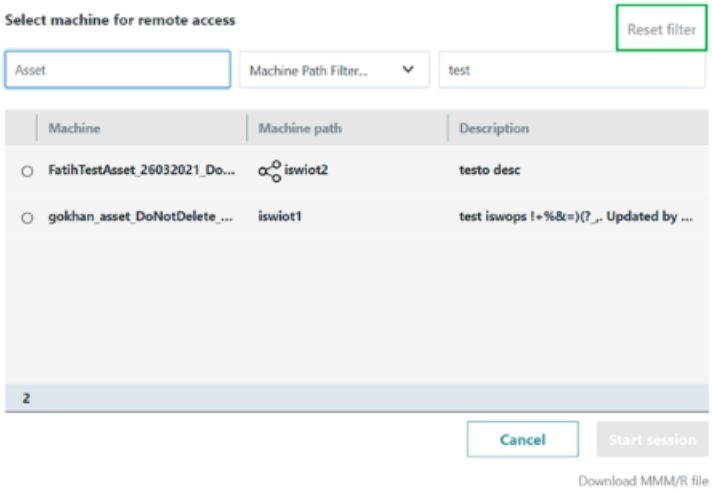
– To start the session, click on "Start session".
- OR -

– Click on "Download MMM /R File".



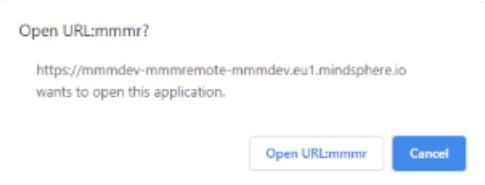
Resetting the filters

If you have set a filter, click the "Reset Filter" button to remove the filter selection.



Start session using the button

1. Click on "Start session".
2. Window "URL: mmmr open?" opens.
   - To start the session, click on button "URL: open mmmr".
   - To cancel the operation, click on "Cancel".



3. The "Manage MyMachines /Remote Service Client" application is started.
   The user is the head service engineer.

Download "MMM /R File"

1. Download "MMM /R File"
2. File "client_mmmr" is downloaded and is displayed in the lower left-hand section of the window.

3. Click on file.
   Window "Open client.mmmr" opens.
   – Activate check box "Open with" and from the drop-down list, select entry "Manage MyMachines /Remote Service Client".
   – Click "OK" to open the client.
4. The "Manage MyMachines /Remote Service Client" application is started.
   The user is the head service engineer.

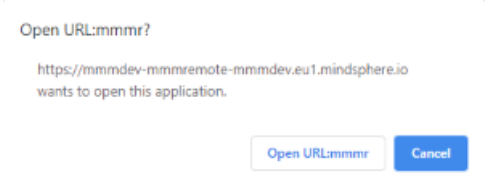
6.5.3 Joining a remote session

Precondition

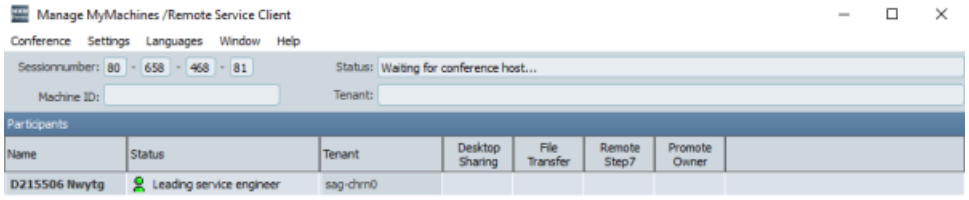
- The session is active.
- The machine operator has already joined the session.

Procedure

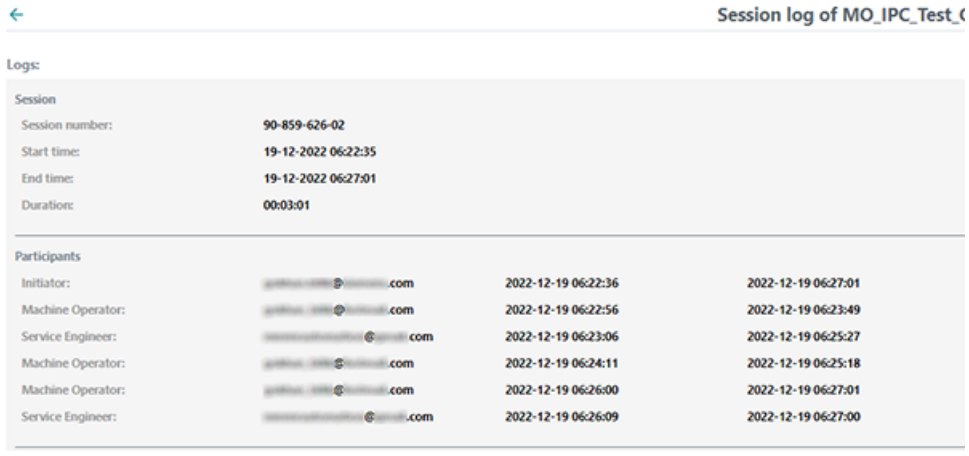
1. The "Session overview" window is open.
   Click in the overview on the underscored name of the required session. Active sessions are color-coded.
2. The "Session log of .." opens.
   Click on "Join".
3. Window "URL: mmmr open?" opens.
   To start the session, click on button "URL: open mmmr".
   To cancel the operation, click on "Cancel".



4. The "Manage MyMachines /Remote Service Client" window opens, and you are automatically dialed into the session.



5. Each time a service engineer or machine operator participates in a session, then this is saved in the session information.



6.5.4 Managing remote sessions

In the "Session Overview" page, you can see all of the sessions and you can do the following:

- View and edit the state of a session (save/do not save)
- View basic information of a session
- Delete a session
- Export a log file.
  For more information, refer to Chapter: Exporting session information (Page 116)
- Start a new session as service engineer.
  For more information, see Chapter: Starting a remote session as a SE (Page 99)

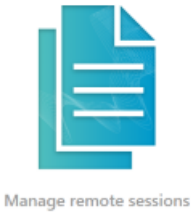
Parameters

Parameter/icon	Description
State   	Shows the following states: • Shows a closed session. • Indicates that a session was saved. • Shows a running session.
Session name	Indicates the session name.
Machine name	Shows the name of the machine.
File transfer 	Indicates whether a file was transferred.
PLC access 	Indicates whether the PLC was accessed.
VPN 	Indicates whether a VPN connection exists.
Desktop Share 	Indicates whether a desktop has been shared.
Recording 	Indicates whether the session was recorded.
Notes edited 	Indicates whether the session includes notes.
Initiator	Shows the e-mail address of the service engineer.
Start time	Shows the session date in the following format: DD-MM-YYYY hh:min:sec
Duration	Indicates the duration of the session in the following format: hh:min:sec
	Window "Navigation view" opens.
	"Displayed columns" icon: Opens a window in which you set columns to be displayed or hidden.
	Opens the "Session Log Settings" window.
	Opens a window in which you configure when session information is deleted. You cannot make any changes if you open this window as subtenant. You can only view the time periods.

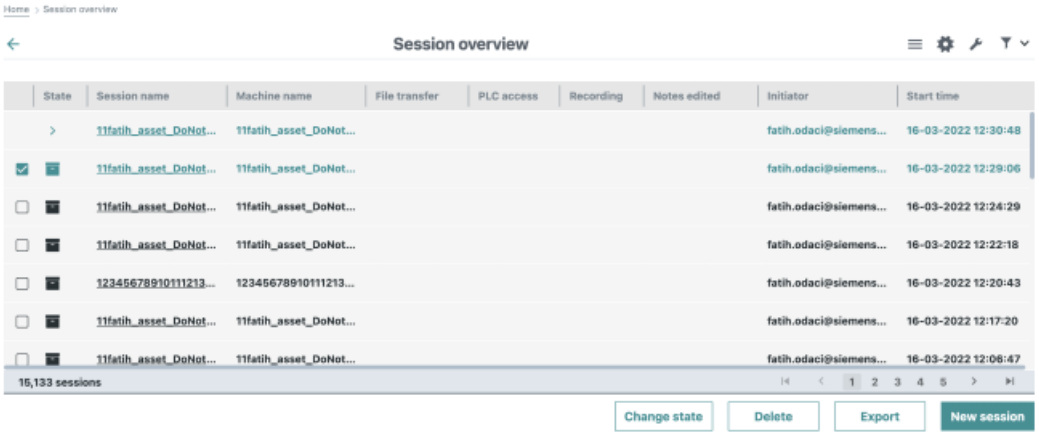
Parameter/icon	Description
	Opens window "My filters" and you can then filter the sessions according to the following criteria: • Name of the initiator • Session name • Machine name • File transfer • PLC access • VPN • Desktop Share • Recording • Notes edited • Start time • Duration The following operators are taken into account when filtering "Duration": – greater than – less than – between
	Creates an additional filter criterion in window "My filters".
	Deletes a filter criterion in window "My Filters".
	Closes window "My filters".
"Session log of <session name>" window	
Close Session	Click the "Close session" button to close the session on the UI. This is necessary if • the session is not closed when the service engineer exits the session. • the active session for the machine appears on the UI and is shown as open, but has already been closed on the client side.
Export CSV	Click on "Export CSV" to save the displayed information in the download directory in CSV format.
Export PDF	Click on "Export PDF" to create and export a PDF. Configure the print settings and click on "Save".
Join	Click on "Join" to join an active remote session.
Edit notes	Click on "Edit notes" to edit notes. You cannot change log data. For more information, see: Evaluating and editing session information (Page 112) Note: This field is available for all users as long as the session is not active. If you are not the session initiator, the button appears grayed out during the active session. Only the session initiator can edit notes during the active session.

Procedure

1. Click on the "Manage remote sessions" button.



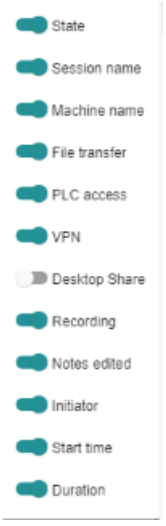
2. The "Session overview" window opens and displays an overview of all sessions. An active session is shown in color.



Displaying/hiding columns

You have the option of displaying or hiding columns.

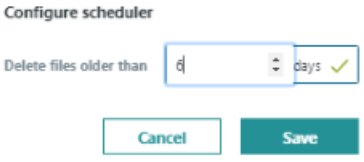
1. Click on the "Displayed columns" icon in the upper right-hand section of the window.
2. A window with all of the available columns opens.
   - Set the slider to the required column to the right to display the columns in the overview.
   - Set the slider to the required column to the left to hide the columns in the overview.



Configuring schedules

You have the option of defining when session information is deleted.

1. Click on the "Wrench" icon in the upper right-hand section of the window.
2. Window "Configure scheduler" opens.
   From the spin box, select the number of days after which session information should be deleted.



Note

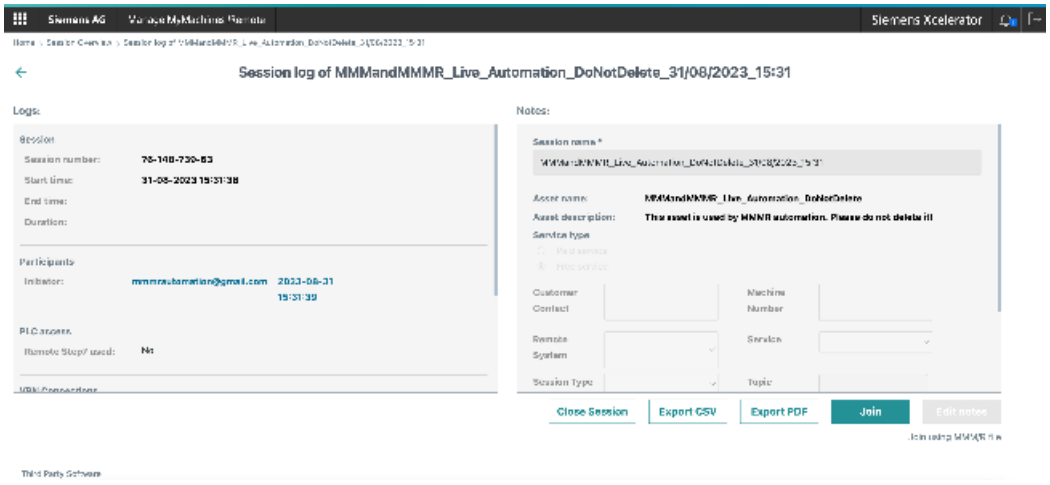
Subtenant only has read access

You can only view the time period, but you cannot make any changes if you open this window as subtenant.

Displaying session information

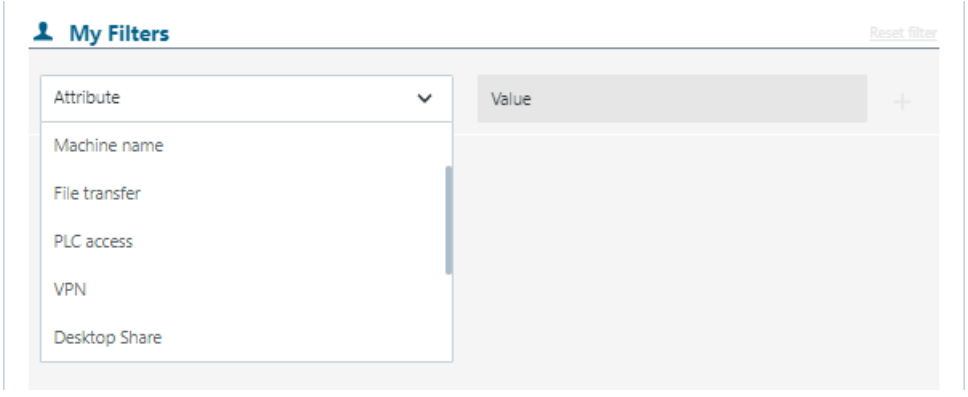
You have the option to view information about a past or active session.

1. Select a session from the overview and click on the underlined session name.
   Active sessions are highlighted in color.
2. The "Session log of <session name>" window opens.



Filtering session overview

1. Click on the "Filter" icon.
   The "My Filters" window opens.
2. From the drop-down list, select an attribute for filtering and enter the associated value.
   - Using the "+" symbol, define additional criteria to further restrict the search.
   - You delete individual filter criteria using the "Recycle bin" icon.
   - Click on "Reset Filter" to display all session information.



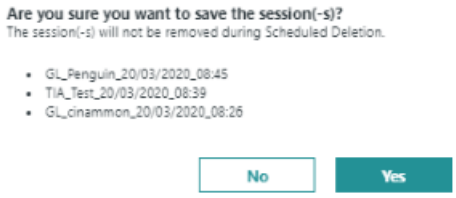
Changing a state

Note

Authorization required

As subtenant, you cannot change the state (save/do not save information).

1. Select one or more sessions.
2. Click the "Change state" button.
   The "Are you sure you want to save the session(s)?" window opens.
3. Click on "Yes" to save session information.
   - OR -
   Click on "No" to cancel the operation.



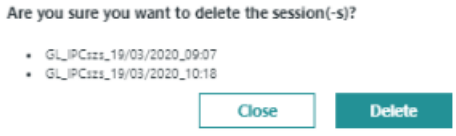
Delete sessions information

Note

Restrictions

- You cannot delete any active session!
- As subtenant, you cannot delete any sessions.

1. Select one or more sessions.
2. Click on "Delete".
   A confirmation prompt is displayed.
3. Click on "Delete" to delete session information.
   - OR -
   Click on "Close" to cancel the operation.



Exporting session information

1. Click the "Export" button.
2. The displayed list is exported in the CSV format, and is saved in the download directory of the browser.

Note

Export duration

For more than 30,000 remote access sessions in the remote access session management, the export of session information can take more than one minute.

6.5.5 Configuring the session log settings

You have the option of adding additional text fields to the session log.

Precondition

You require the appropriate authorization levels.

More information can be found in Chapter: Managing users (Page 66).

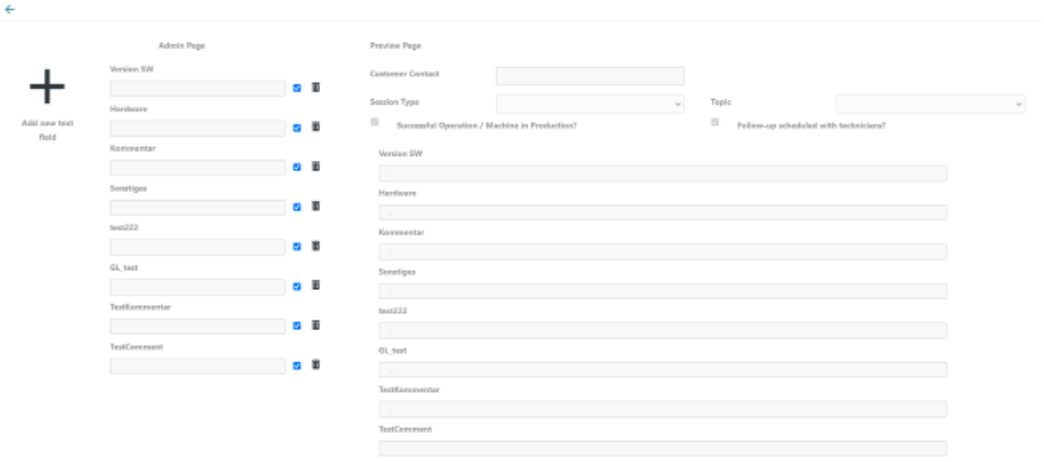
You cannot use the function if you only have "Subtenant" authorization.

Procedure

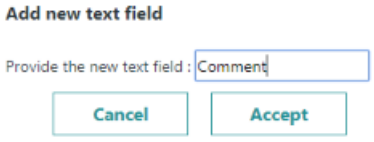
1. Click the "Session Log Settings" button.



2. The "Session Log Settings" window opens and displays the self-defined text boxes on the administrative page and a preview page for the session log.



3. Click the "Add new text field" button.
4. Enter the required labeling for the text box. Click on the "Accept" button.



5. The new text field is displayed on the administrative page and on the preview page. The text field is also created in the session log of the next remote access session.

6.5.6 Evaluating and editing session information

When a session is finished, you can still edit or add session data. You have the option of exporting this data into a CSV file and/or in the PDF format.

If you need additional text fields in the session log, you can use the Configuring the session log settings (Page 111). The additional text fields will then be available to you for future sessions.

Precondition

You require the appropriate authorization levels.

More information is provided in Chapter: Managing users (Page 66).

Parameters

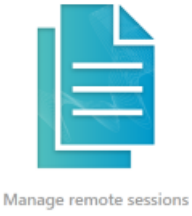
Parameters	Description	
Logs:	Shows the following session data:	
Session		
	Session name	Shows the session names.
	Start time End time	Shows the start and end time in the following format: Year-month-day (YYYY-MM-DD) Hour:Minute:Second (hh:mm:ss)
	Duration	Displays the total duration of the session in the following format: Hour:Minute:Second (hh:mm:ss) The session is still active if the data is shown in color.
Participants		
	Initiator Machine operator Service engineer	Shows the e-mail addresses of the service engineer. Shows the machine operator. Shows the email address of the additional service engineer if this engineer participated in the session.
PLC access		
	Remote STEP 7 used	Shows whether PLC access is via Remote STEP 7: • Yes • No
Recording		
	Start time	Shows the start time in the following format: Year-month-day (YYYY-MM-DD) Hour: Minute: Second (hh:mm:ss)
	Duration	Displays the total duration of the session in the following format: Hour:Minute:Second (hh:mm:ss)
	Traces that have been completed	Contains a list of the traces that have been completed.
File transfer		
	File transfers that have been completed	Contains a list of the file transfers that have been completed.
Notes		

Parameters	Description	
	Session name *	Shows the session names.
	Asset Name	Displays the machine names
	Asset description	Shows the description of the asset
	Service type	Shows the following: • Paid service • Free service
	Customer contact	Add the customer's contact data.
	Session type	You can select the session type from the drop-down list.
	Topic	You can select the topic of the session from the drop-down list.
	Successful Operation / Machine in Production?	You can appropriately activate/deactivate the option box.
	Follow-up scheduled with technicians?	You can appropriately activate/deactivate the option box.
	Comments	You can enter comments in the text boxes provided.

* Is a mandatory field and must be filled out

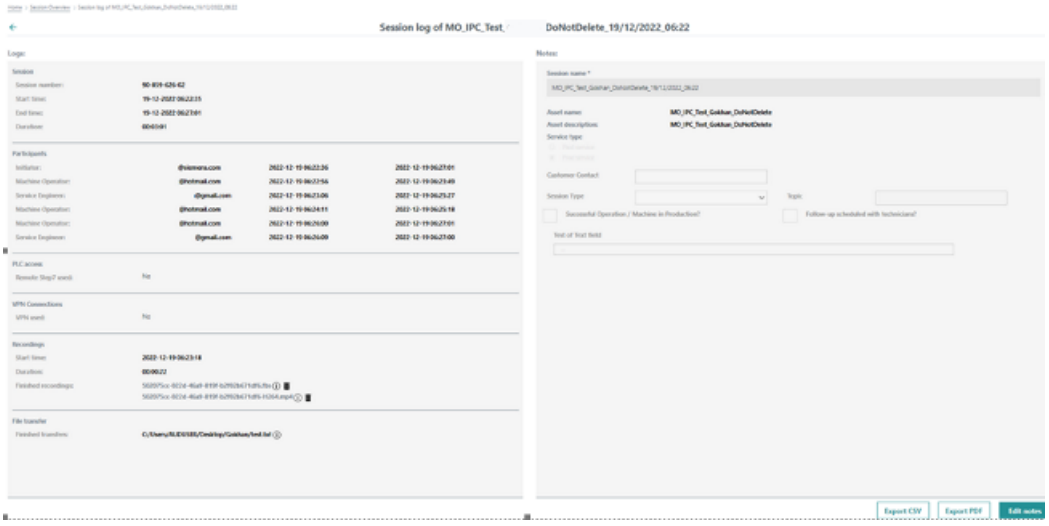
Procedure

1. Click on the "Manage remote sessions" button.



2. Window "Session information" opens.

3. In the overview, select a session and click on the session name that is underlined.
   The "Session log of <session name>" window opens.



4. Click on the "Edit notes" button.
   The right window area is released for changes and additions.
   Note: You cannot change log data!
5. Edit the required entries.
   - Enter the name of the customer contact
   - Select the session type and session topic from the appropriate lists.
   - Fill-out the customer-specific text boxes.
6. Click on "Save" to save the changes.
   - OR -
   Click "Cancel" to discard the entries.

More information is provided in Chapter: Exporting session information (Page 116).

Asset deleted

When an asset has been deleted in Insights Hub, you will get the message in the upper right area as well as in the right area above the asset name.

- The icon for deleting records of deleted assets is disabled.
- Recordings cannot be downloaded.



6.5.7 Exporting session information

You have the option of exporting session information for the displayed sessions in the following formats:

- Log file in the CSV format
- PDF

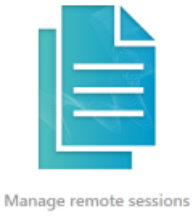
Precondition

You must have the appropriate authorization levels to view all session information.

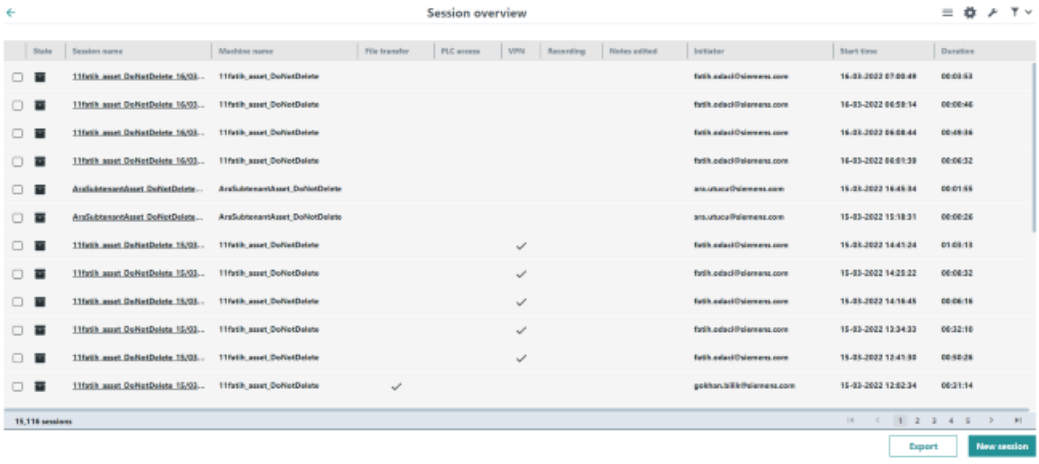
More information can be found in Chapter: Managing users (Page 66).

Procedure

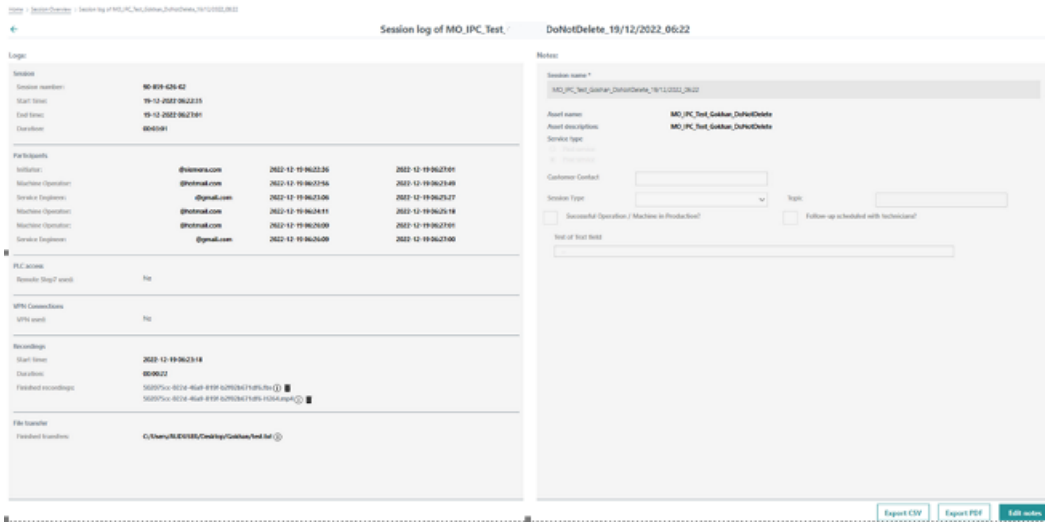
1. Click on "Manage remote sessions".



2. The "Session overview" window opens and displays an overview of all sessions. Filter the displayed sessions if necessary.

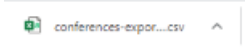


3. In the overview, select a session and click on the session name that is underlined.
   Window "Session information of <Name_date_time>" opens.

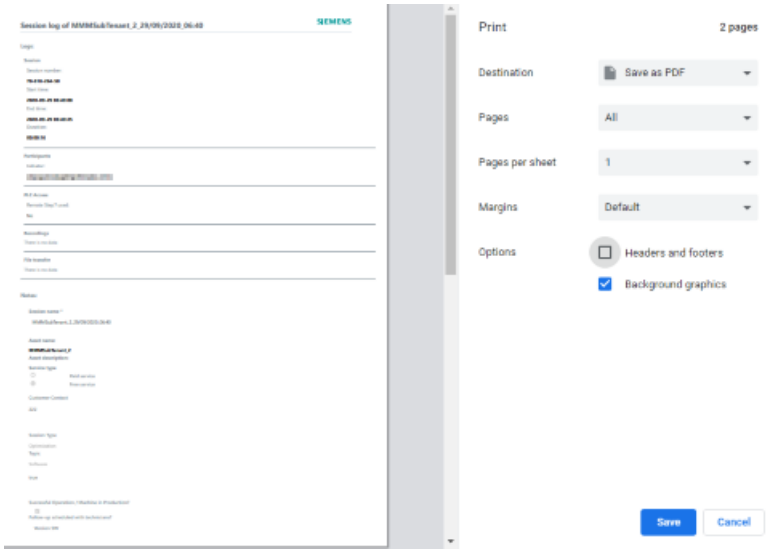


4. Click on "Export CSV".
   The displayed information is saved in the download directory in the CSV format.
   The file is displayed in the lower left section of the window.
   When clicking on the arrow icon you have the following options:

   – Open - opens the file
   – Always open files of this type - automatically opens the file
   – Show in folder - exports the file to the selected folder



   - AND / OR -
   Click on "Export PDF".
   An additional window opens in which you can define the print settings.
   Click on "Save" to start printing the PDF.



6.5.8 Remote sessions with Manage MyMachines

You can also start or enter remote sessions via Manage MyMachines.

Precondition

- You have purchased Manage MyMachines and Manage MyMachines /Remote for the particular tenant.
- You are logged in as user and have Manage MyMachines and Manage MyMachines /Remote rights.
- Access to Manage MyMachines and Manage MyMachines /Remote for the required asset is activated.
  More information can be found in Chapter: Activating Manage MyMachines /Remote (Page 75).

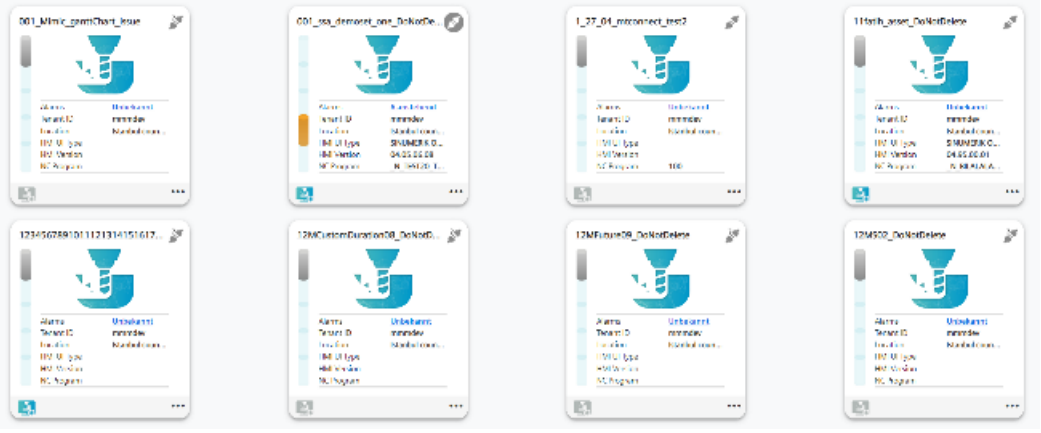
Parameters

Icon	Description
	• You have no rights to start the remote session. – The rights for Manage MyMachines /Remote were not assigned to the user or were removed. – Manage MyMachines /Remote was not purchased for the tenant - OR - • Manage MyMachines /Remote is not activated. – The subscription is not activated or has expired.
	You can start a new remote session.
	You can join an existing remote session.

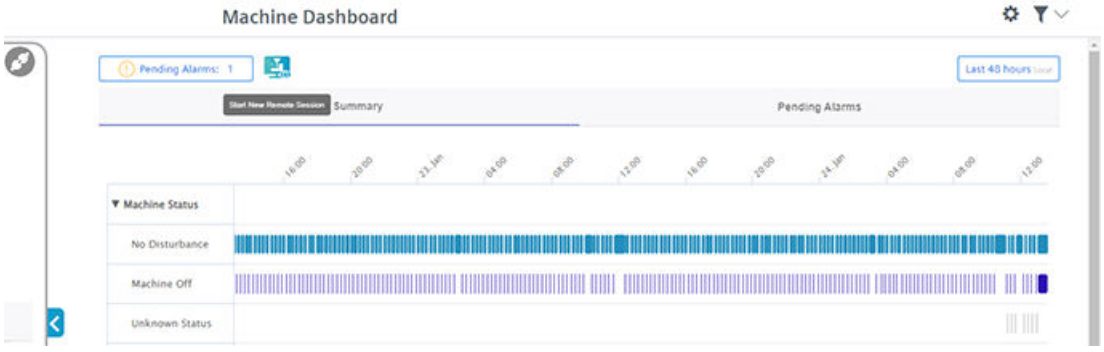
6.5.8.1 Start new remote session

Procedure

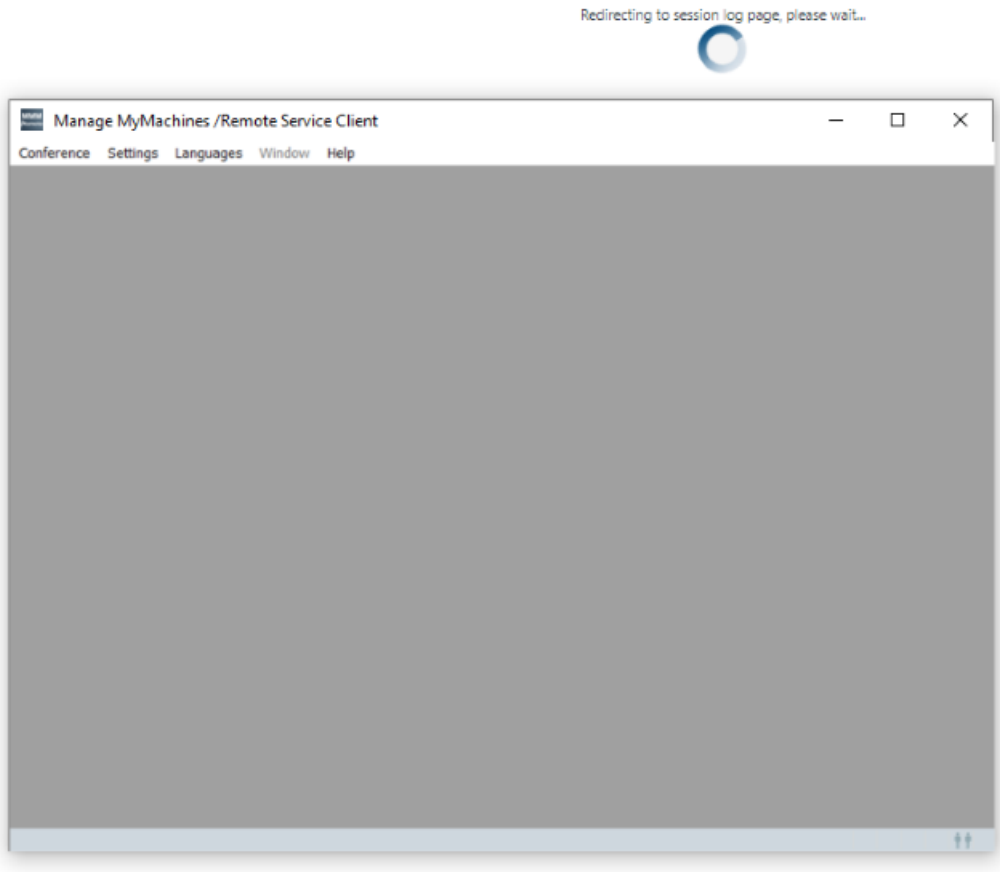
1. In the launch pad, click on the "Manage MyMachines for Industrial Operations X Cloud" icon.
2. The "Machine Overview" window opens and the available machines are displayed.



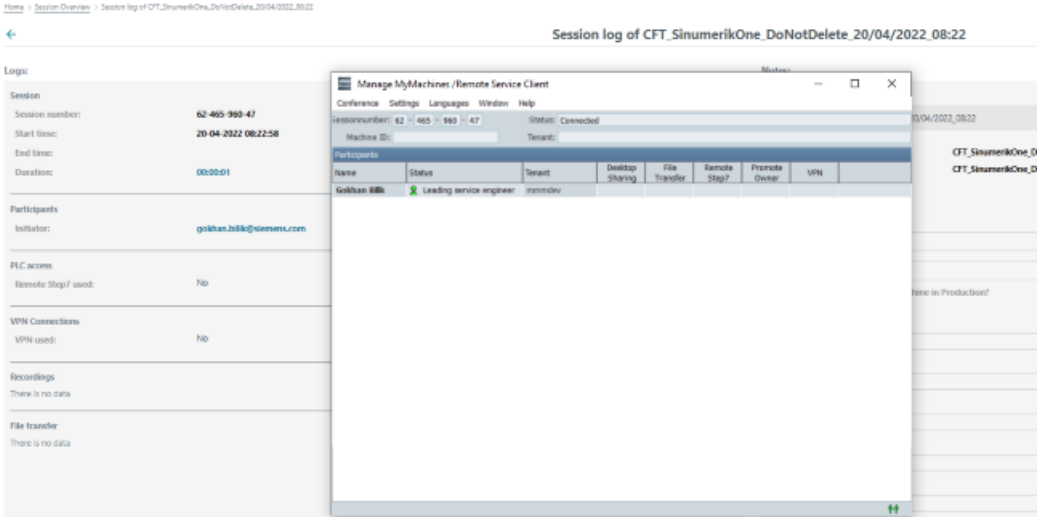
3. Click on the blue "MMM /R" icon "Start new remote session" of the required asset.
   - OR -
   Click on the underscored name of the required machine.
   The "Machine Dashboard" window opens.
   Click on the blue "MMM /R" icon next to the "Pending Alarms" display.
   - OR -
   Click on the ••• icon of the required machine and click on "Dashboard".
   The "Machine Dashboard" window opens.
   Click on the blue "MMM /R" icon next to the "Pending Alarms" display.



4. The "Manage MyMachines /Remote Service Client" session window opens.



5. A new remote session is started and the log details for the selected asset are displayed.



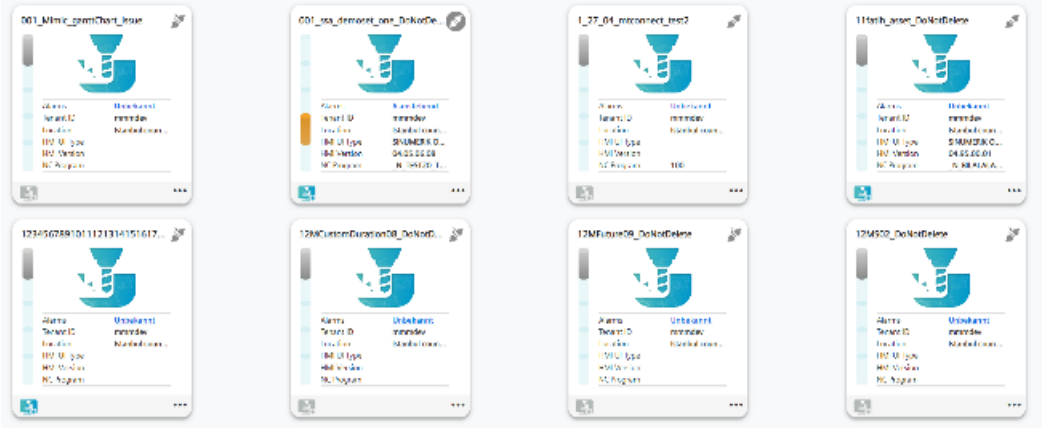
6.5.8.2 Joining a remote session

Precondition

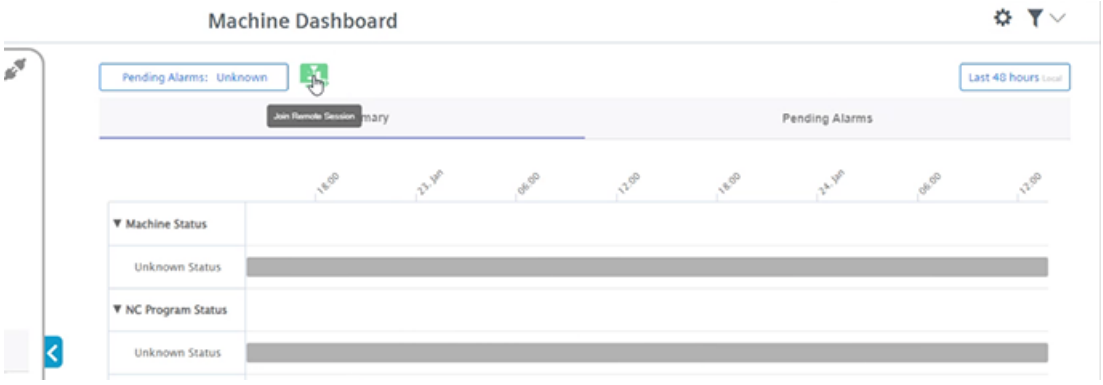
- The session is active.
- The service engineer and machine operator have already joined the session.
  The following warning message is output if there are no active owners in the session:
  "Terminated: There is no owner SE or MO yet".
- It is not permissible that a desktop is continually shared and/or files transferred.
  The following warning message is output if the desktop is shared and/or files transferred.
  "Aborted: Joining is not allowed during ongoing desktop sharing or file transfer".

Procedure

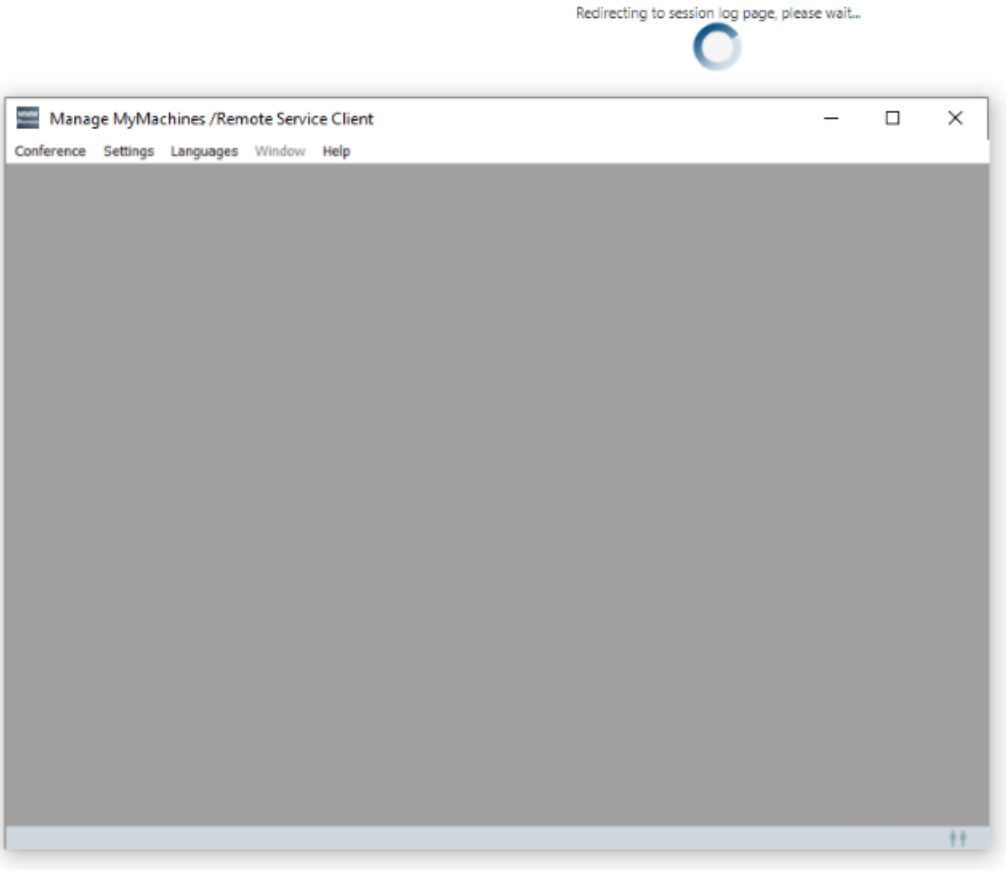
1. In the launch pad, click on the "Manage MyMachines for Industrial Operations X Cloud" icon.
2. The "Machine Overview" window opens and the available machines are displayed.



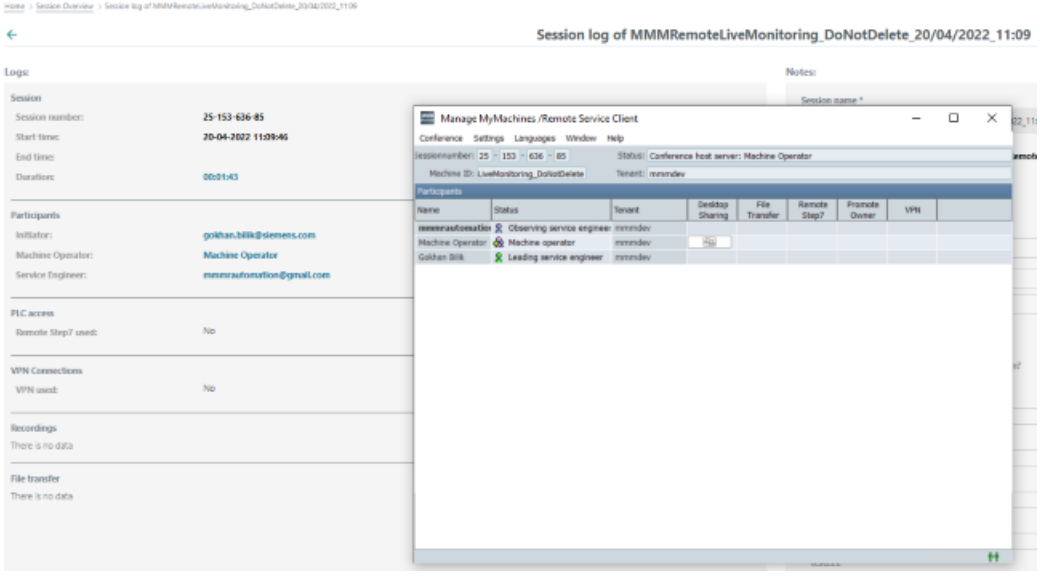
3. Click on the blue "MMM /R" icon "Join remote session" of the required asset.
   - OR -
   Click on the underscored name of the required machine.
   The "Machine Dashboard" window opens.
   Click on the green "MMM /R" icon next to the "Pending Alarms" display.
   - OR -
   Click on the ••• icon of the required machine and click on "Dashboard".
   The "Machine Dashboard" window opens.
   Click on the green "MMM /R" icon next to the "Pending Alarms" display.



4. The "Manage MyMachines /Remote Service Client" session window opens.



5. You join the remote session and the log details for the selected asset are displayed.

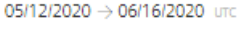


6.6 Service Dashboard

Precondition

You require admin rights to use the "Service Dashboard" function.

Parameters

Parameter/icon	Description
	Opens the "Manage MyMachines /Remote" start page.
	Displays the time range and the time zone used. By default, the time range is set to "Last 7 days". Opens the calendar function. More information can be found in Chapter: Using the calendar function (Page 128).
Export PDF	Exports the "Service Dashboard" data in the time range used to a PDF file.

Procedure

1. Click on the "Service Dashboard" button.



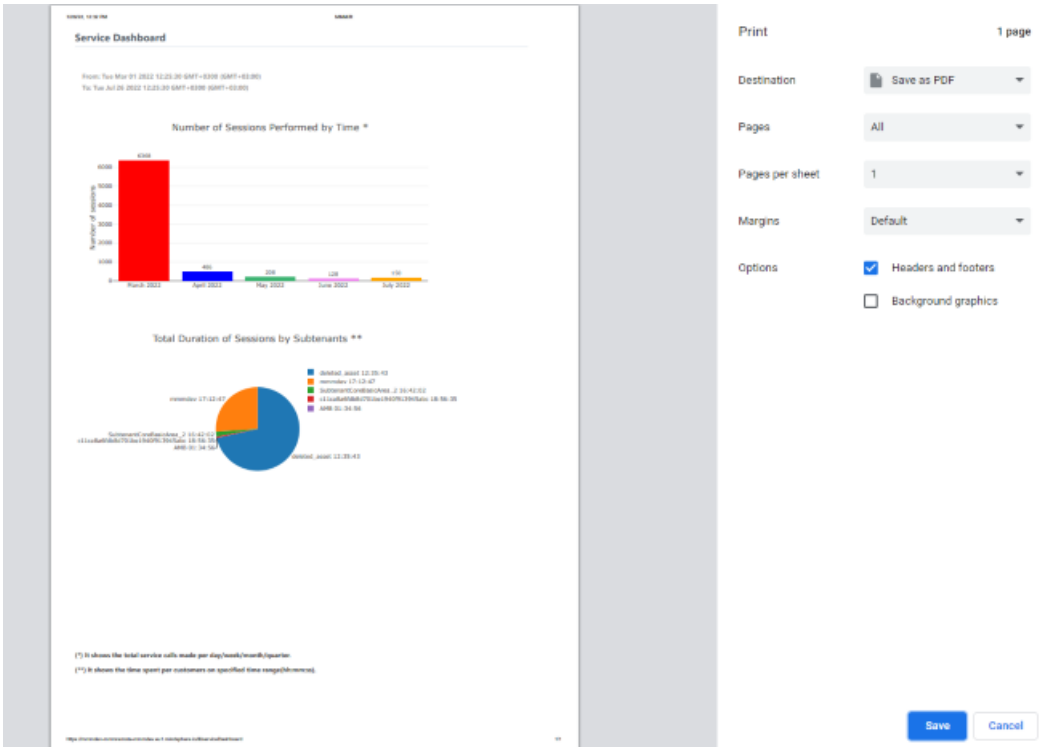
2. The "Service Dashboard" window opens.
   - The "Number of sessions performed by time" bar chart shows you the total number of service calls per day/week/month/quarter.
   - The "Total duration of sessions by subtenants" pie chart shows you the time spent per customer in a certain period of time (hh:mm:ss).
   - The "Number of sessions by subtenants" pie chart shows you the number of service calls per customer.

   Hover the mouse over the diagrams to display the underlying data in detail.

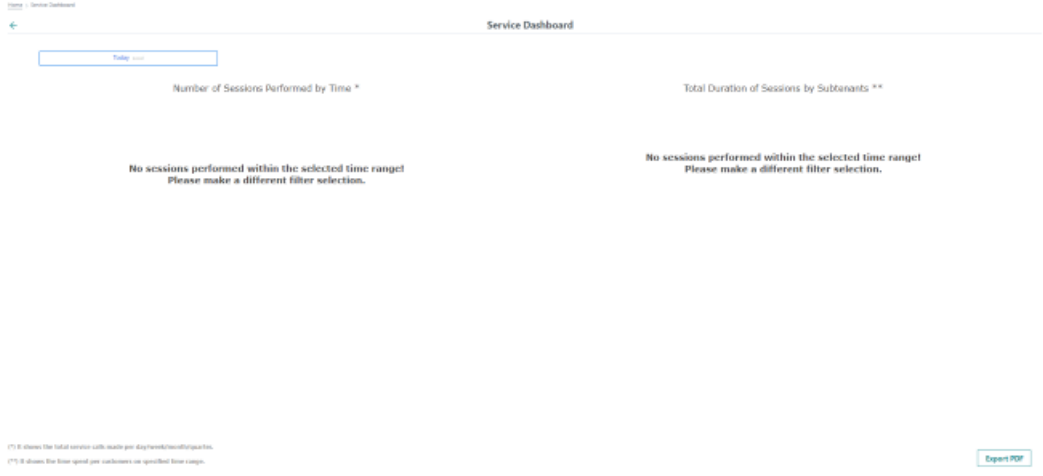


3. To make time range settings in the time range, click in the upper left of the time range window.

4. Click "Export PDF" to export the displayed data of the window to a PDF file.
   The "Print" window opens.
   To save the PDF file, click "Save"
   - OR -
   To cancel the operation, click "Cancel".



5. If no session was held in the selected time range, the following message is displayed:
   "No sessions performed within the selected time range! Please make a different filter selection."



6.7 Using the calendar function

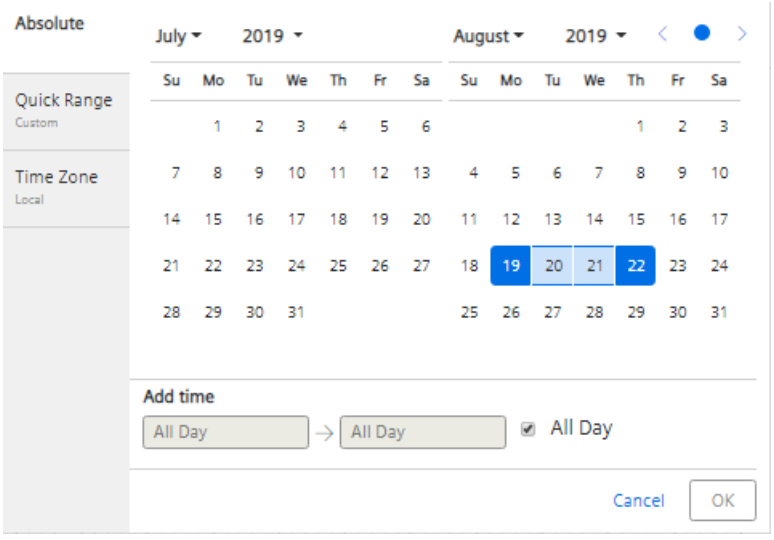
You have the option of selecting the time range and time zone using the calendar function.

Button / parameter

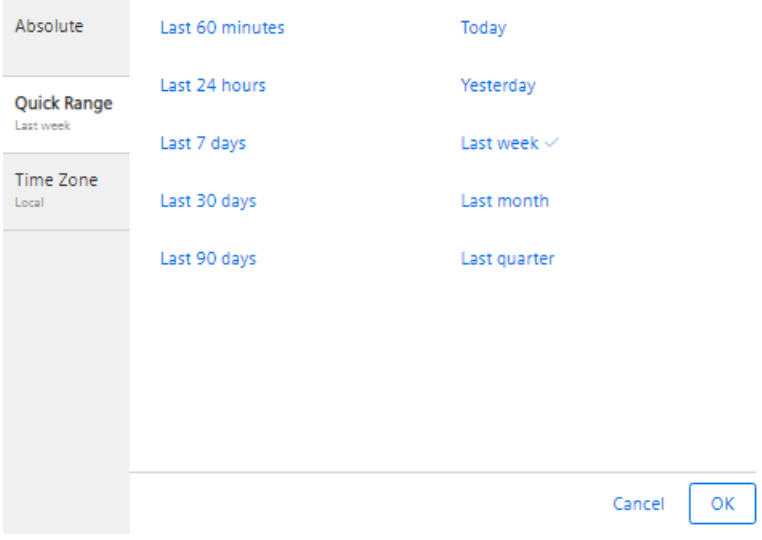
Button/parameter	Description
	Displays the time range and the time zone used. Opens the calendar function.
Absolute	Manually entering a fixed time range
Relative	Selecting a relative time range: • Last 60 minutes • Last 24 hours • Last 7 days • Last 30 days • Last 90 days • Today • Yesterday • Last week • Last month • Last quarter
Time zone	Selecting the time zone used • Local: Local time at the machine location • UTC: World time

Procedure

1. Click on the time range display.
   The calendar window opens.
2. To use a fixed time range:
   - Open the "Absolute" tab.
   - Click on the required start date.
   - Click on the required end date.
   - Enter a precise time in format hh:mm:ss.
     - OR -
     Activate the checkbox "All Day".



3. To use a relative time range:
   - Open the "Quick Range" tab.
   - Click on the required time range.



4. Open the "Time zone" tab, and select the required time zone.
5. Click on "OK".
   The calendar window is closed. The new time range and the time zone used are displayed on the button.

Setting up Manage MyMachines /Remote Service Client

7

7.1 Setting up Manage MyMachines /Remote - Machine operators (MO)

7.1.1 Overview

As the machine operator, you have various options for accessing the functions of Manage MyMachines /Remote:

1. **SINUMERIK Operate runs on the NCU.**
   In this scenario, you connect to Manage MyMachines /Remote with the aid of the SINUMERIK Integrate Client.
   You can find further information on the installation and configuration of the SINUMERIK Integrate Client in the following chapters:
   - Checking and updating the versions (Page 27)
   - SINUMERIK Integrate (Page 38)
   - Configuring the URL and proxy (Page 40)

   You can find further information on the installation of the SINUMERIK Integrate Client from a remote computer in the
   Application example Manage MyMachines /Remote - Installation in existing control environments
2. **SINUMERIK Operate runs on a PCU or IPC.**
   In this scenario, you install the Manage MyMachines /Remote Service Client.
   You can find further information on the installation and configuration of the Remote Service Client in the following chapters:
   - Download remote service client (Page 94)
     Ensure that you select the correct client. The clients for PCU or IPC use different processes for establishing a connection and authentication.
   - Installing Manage MyMachines /Remote Service Client MO (IPC or PCU) (Page 132)
   - Entering the address of a proxy server (Page 140)
   - You have the option of integrating the Remote Service Client into the SINUMERIK Operate as an OEMFrame application:
     Integrating an OEMFrame application into HMI sl (Page 141)

7.1.2 Installing Manage MyMachines /Remote Service Client MO (IPC or PCU)

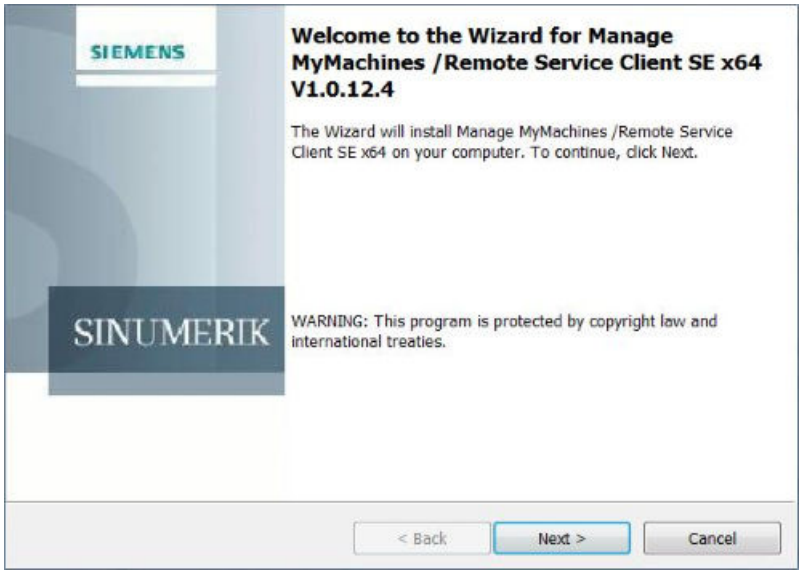
Precondition

You have downloaded the client setup, e.g. to a USB flash drive.

You will find information on this in Chapter Download remote service client (Page 94).

Procedure

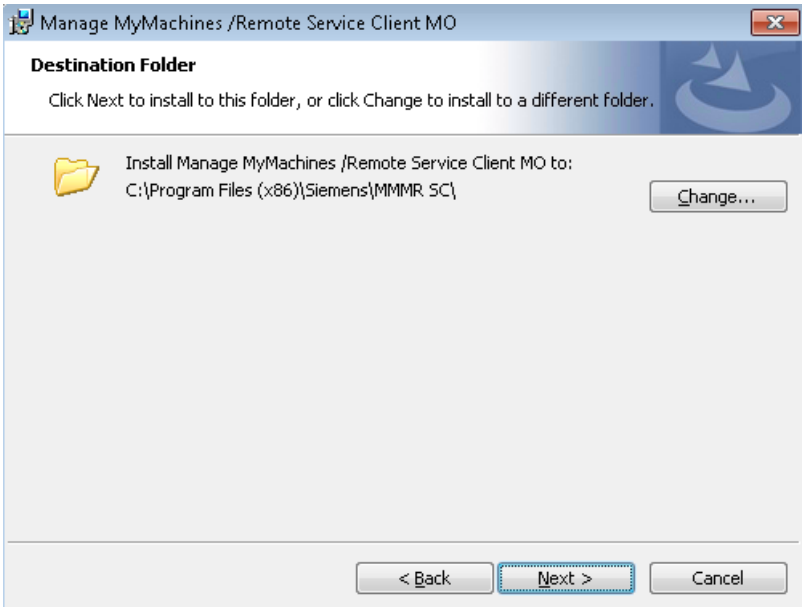
1. Copy the client setup, e.g. from the USB flash drive to the SINUMERIK control or the IPC.
2. Open the installation directory into which the client setup was copied.
3. Double-click to start the "MMMR_SC_MO_setup.exe" setup file, e.g. from "Manage MyMachines /Remote service client for machine operators - PCU from Vx.x.x.x.".
   The welcome dialog "Welcome to the Wizard for Manage MyMachines /Remote Service Client MO Vx.x.xx.x" opens.
   Click "Next >" to prepare the installation.



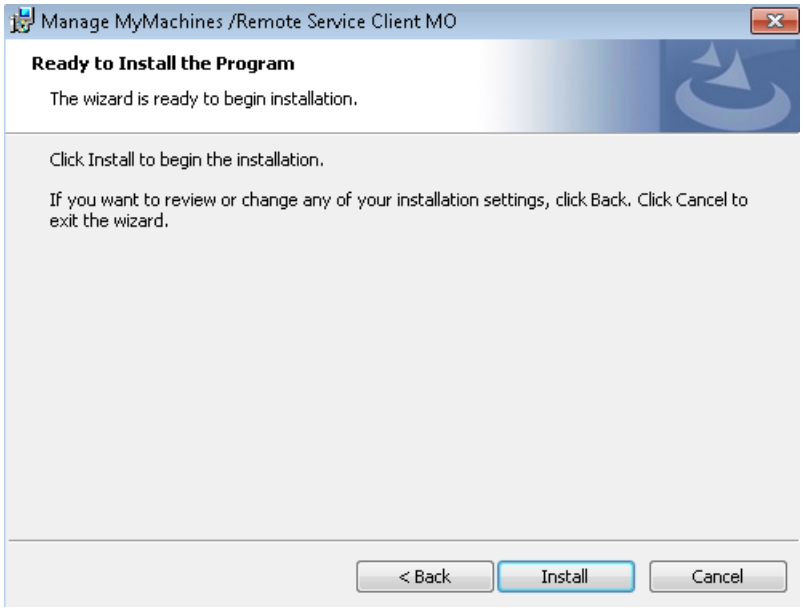
4. The "License Agreement" window opens.
   Read the license agreement.
   - Click "Print" if you want to print out the conditions.
   - Then select the "I accept the terms in the license agreement" option button and click "Next >".
     - OR -
     Click "< Back" to return to the previous window.



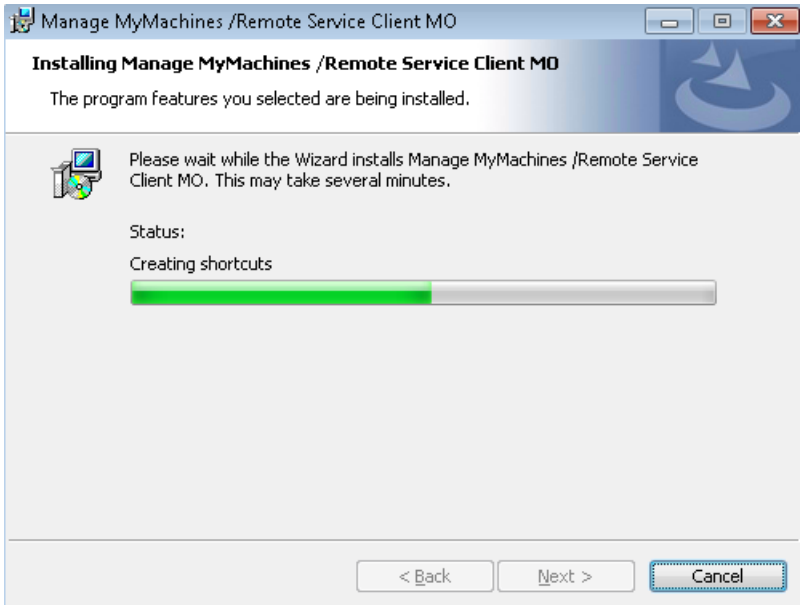
5. The "Destination Folder" window opens.
   Click "Next >" to accept the directory suggested by setup.
   - OR -
   Click "Change..." to change the installation directory.



6. The "Ready to Install the Program" window is opened.
   Click the "Install" button to start the installation.



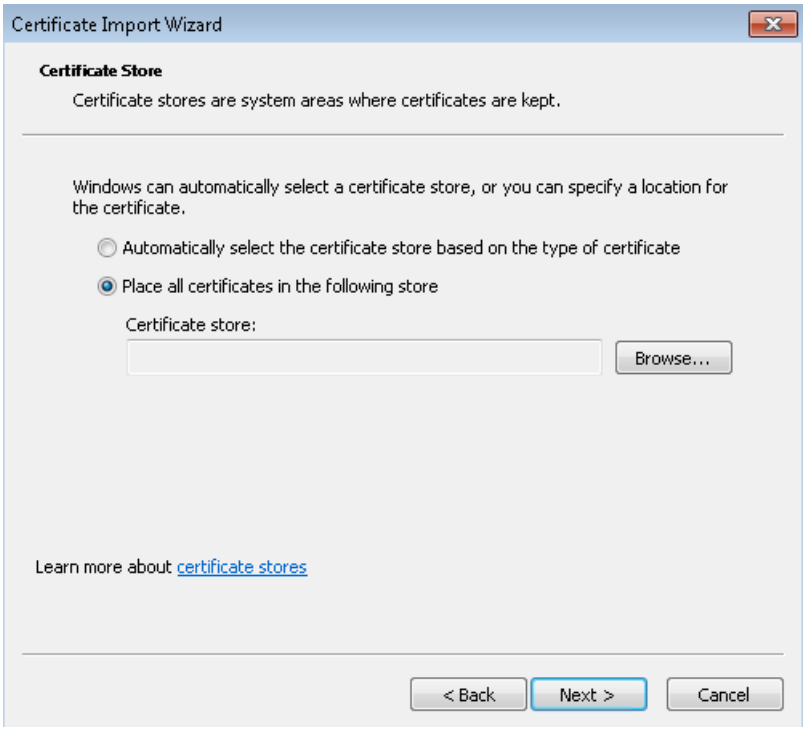
7. The "Installing Manage MyMachine /Remote Service Client MO" window is opened.
   The installation is started.



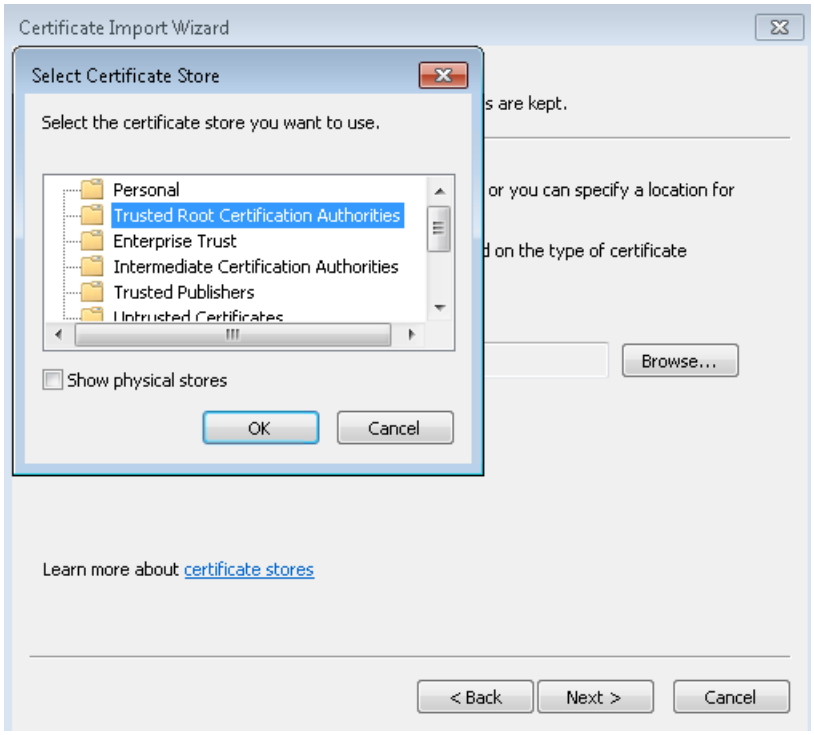
8. The "Welcome to the Certificate Import Wizard" window opens.
   Click on "Next >".



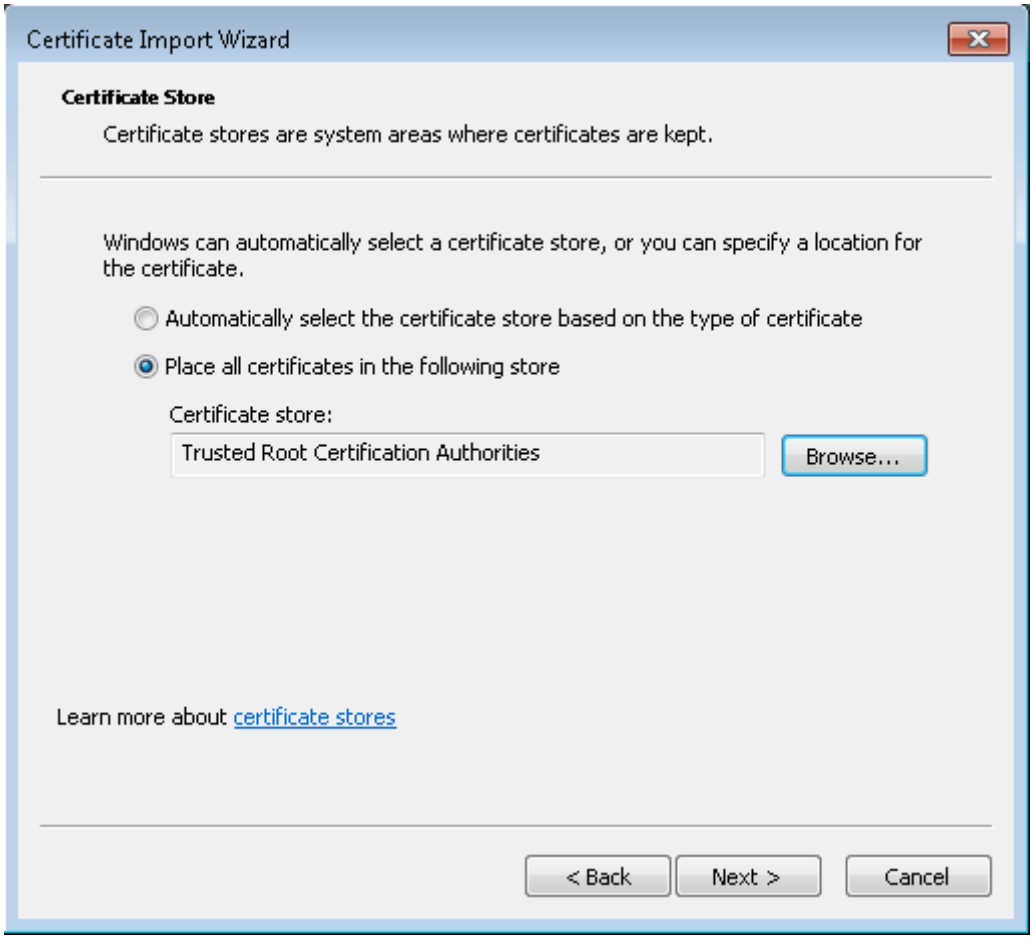
9. Window "Certificate Store" opens.
   Activate the "Place all certificates in the following store" option button.
   Click on "Browse...".



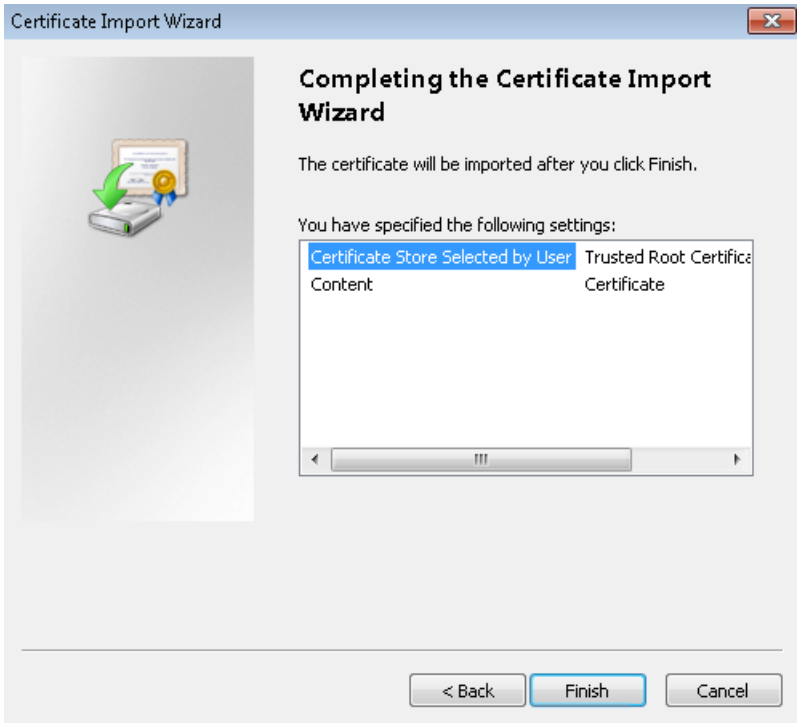
10. Window "Select Certificate Store" opens.
    Select "Trusted Root Certification Authorities" and click on "OK".



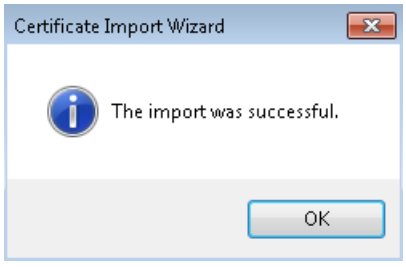
11. Window "Certificate Store" is redisplayed, and you see the entry below "Certification store:" Click on "Next >".



12. The "Completing the Certificate Import Wizard" window opens and shows you the settings. Click on the "Finish" button. The certificate is imported.



13. You receive a message that the certificate was successfully imported. Click "OK".

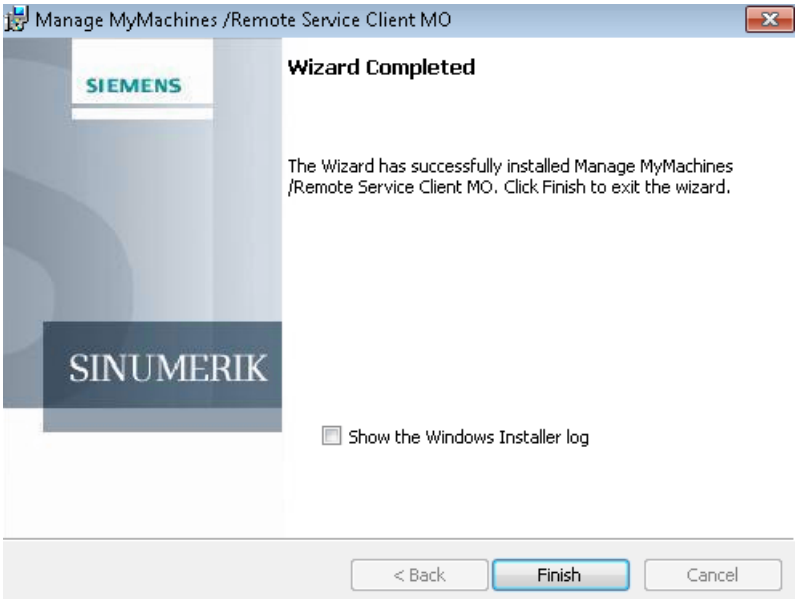


Note

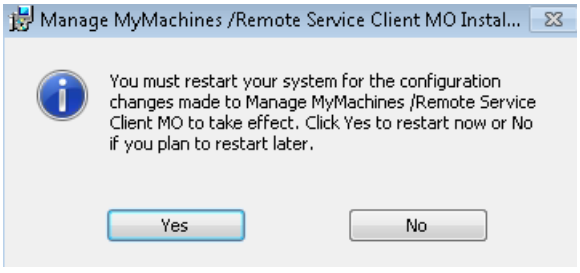
New request by the wizard

It is possible that the certificate import wizard again prompts you to import another certificate. Repeat steps as described under 8. to 13.

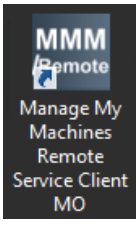
14. The "Wizard Completed " window opens.
    Click "Finish" to complete the installation.



15. Once installation has been completed, you will be prompted to restart your SINUMERIK control or the IPC.
    Click on "Yes".



16. The following symbol is displayed on the desktop for you to start Manage MyMachines / Remote:



7.1.3 Entering the address of a proxy server

Overview

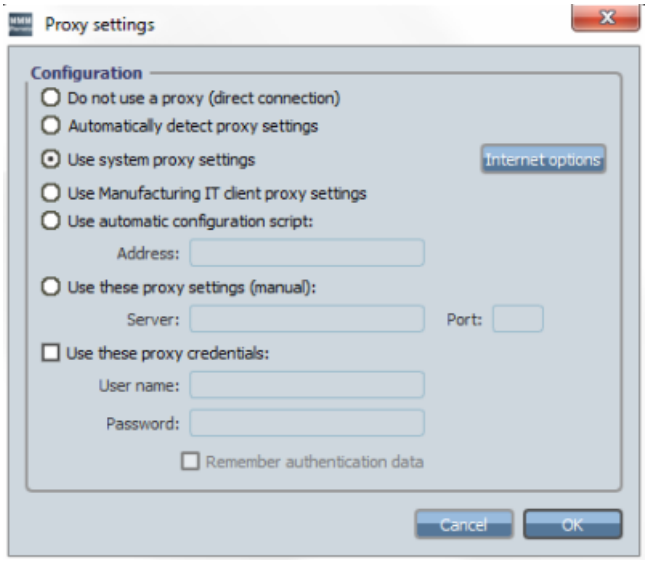
If access to the Internet is done via a proxy server, define the desired method via the proxy settings.

Settings	Description
Do not use a proxy (direct connection)	Establishes a direct connection to the Internet.
Automatic proxy detection	Automatically determines the address of a proxy server to access the Internet.
Use system proxy settings	The suggested setting: Uses the setting saved in Internet Explorer to go into the Internet. Click "Internet options" to open the Internet options of the system in order to check or change the proxy settings.
Use Manufacturing IT client proxy settings	Uses the settings of the Manufacturing IT client to gain access to the Internet.
Use automatic configuration script:	
Address	Address input of the proxy server from which the proxy script is downloaded.
Use these proxy settings (manual):	
Server	Address input (address and port) to specify a specific proxy server.
Port	
Use these proxy credentials:	
User name	Input of the access data if the proxy server requires a login.
Password	
Remember authentication data	The access data is stored retentively in the system. The password is stored in encoded form.

Procedure

1. Open "Manage MyMachines /Remote Service Client".
2. Call "Settings" > "Proxy..." in the menu bar.
   The "Proxy settings" window opens.

3. Select the desired proxy setting.
4. Click "OK" to save the settings.
   - OR -
   Click "Cancel" to reject the settings.



Using your own proxy logon data

If you are using your own proxy logon data, select the "Use these proxy settings (manual):" check box.

1. Then select the check box "Use these proxy credentials:" and enter your user name and password.
2. Select the "Remember authentication data" checkbox if you want to save your login data permanently.
3. Click the "OK" button to save the settings.

7.1.4 Integrating an OEMFrame application into HMI sl

Integrating an OEM Frame application

The Windows OEMFrame applications are used to generate and use softkeys. The required settings are described in this chapter based on an example.

You will have to modify or create the following files:

- Configuration file "systemconfiguration.ini"
- Configuring the start softkey
  In order to start an OEMFrame application from the operating software, configure a softkey on the expansion bar of the operating area.

Example configuration file "systemconfiguration.ini"

In file "systemconfiguration.ini", save the call for Manage MyMachines /Remote Service Client accordingly. Depending on the access protection level assigned to you, you extend the "systemconfiguration.ini" file contained in the relevant directory.

<HMIInstallDir>\\hmi\oem\sinumerik\hmi\cfg

<HMIInstallDir>\\hmi\addon\sinumerik\hmi\cfg

<HMIInstallDir>\\hmi\ \user\sinumerik\hmi\oem\

Extensions

Add the following line to the [areas] section:

```
AREA500=name:=MMMR, process:=ProcessOEM
```

Add the following line to the [processes] section:

```
PROC500=process:=ProcessOEM, cmdline:="C:\\Program Files (x86)\
\Siemens\\MMMR SC\\ManageMyMachinesRemoteServiceClientMO.exe",
oemframe:=true, deferred:=true, classname:="QWidget"
```

Adjust the indexes of the relevant entries (PROC500, AREA500) in accordance with your HMI configuration.

The path for the executable file of the service mode client can differ from the path stated above, depending on the version installed (32 bit/64 bit) and the path selected during installation.

Further information

You can find further information about the options for integrating OEMFrame applications in the SINUMERIK Operate Commissioning Manual.

7.1.5 Silent Installation

You have the option of using Silent Installation to install "MyMachines /Remote Service Clients".

This installation type allows you to install Manage MyMachines /Remote Service clients without any user interaction at all. The steps to install the certificate are part of the newly implemented Silent Installation.

The actions that would have had to be performed using the wizards to import the certificate are now performed in the background. While doing this, the correct certificates are placed at the storage location of the Trusted Root Certification Authorities.

Precondition

You require administration rights to perform a Silent Installation.

Parameters

Use the following parameters in the command line:

`/s` > for Silent Installation

`/x` > to delete

`setup.exe /s /v"/qn"` > for Silent Installation with default settings

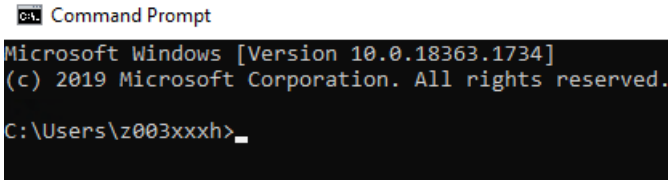
`REBOOT=ReallySuppress` > to suppress a forced restart (e.g. `MMMR_SC_SE_x64.exe /s /v"/qn REBOOT=ReallySuppress`)

Procedure

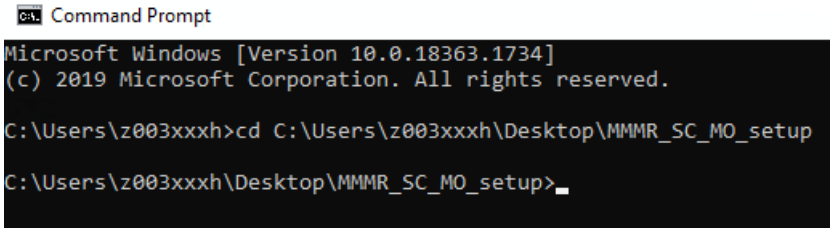
The subsequent example is applicable for machine operators.

You install other service clients using the same procedure running in the background.

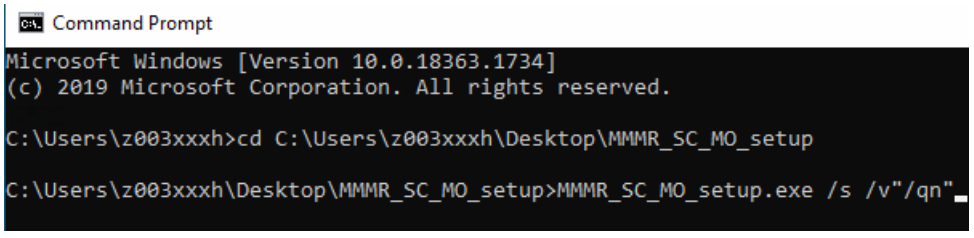
1. Open "Command Prompt".



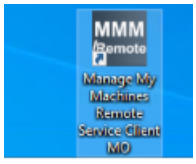
2. Enter the directory in which the "setup.exe" file is located.

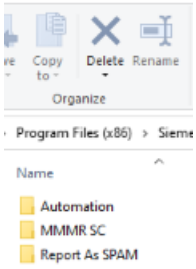


3. Execute the following Silent Installation command to install the client in the default directory. e.g. `MMMR_SC_MO_setup.exe /s /v"/qn"`



4. You do not have to make any other entries during the installation procedure.
   – The clients are installed in the standard directory C:\Programs (x86)\Siemens\MMMR SC.
   – The certificates are placed in the Trusted Root Certification Authorities.





5. To install function "OpenVPN", insert parameter `OPENVPN_OPTION=1` at the end of the command:
   `MMMR_SC_IPC_MO_setup.exe /s /v"/qn OPENVPN_OPTION=1`
   – The VPN button is added to the SE client user interface. VPN is only supported for MO / IPC clients.
6. If you want to completely remove the service clients, execute the following command:
   `MMMR_SC_MO_setup.exe /x /s /v"/qn"`

7.2 Setting up Manage MyMachines /Remote - service engineer (SE)

7.2.1 Installing Manage MyMachines /Remote Service Client SE

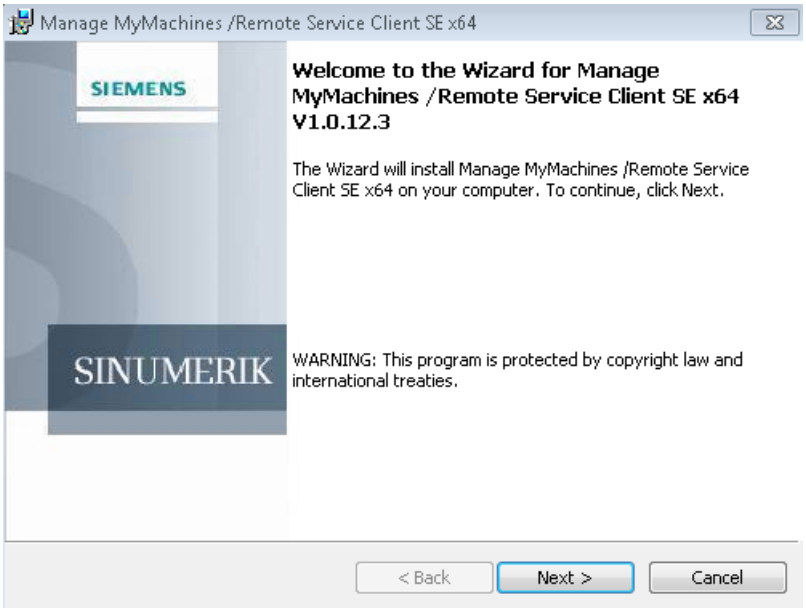
Precondition

You have downloaded the client setup.

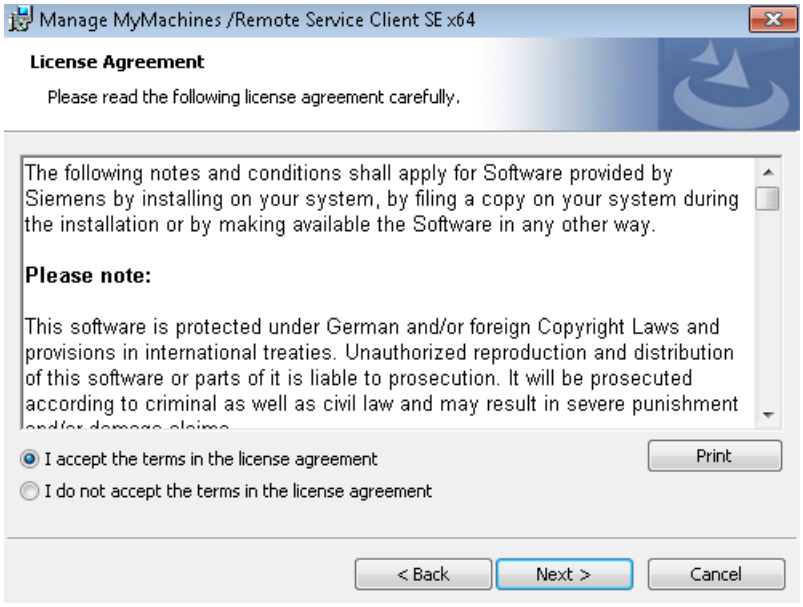
More information can be found in Chapter: Download remote service client (Page 94).

Procedure

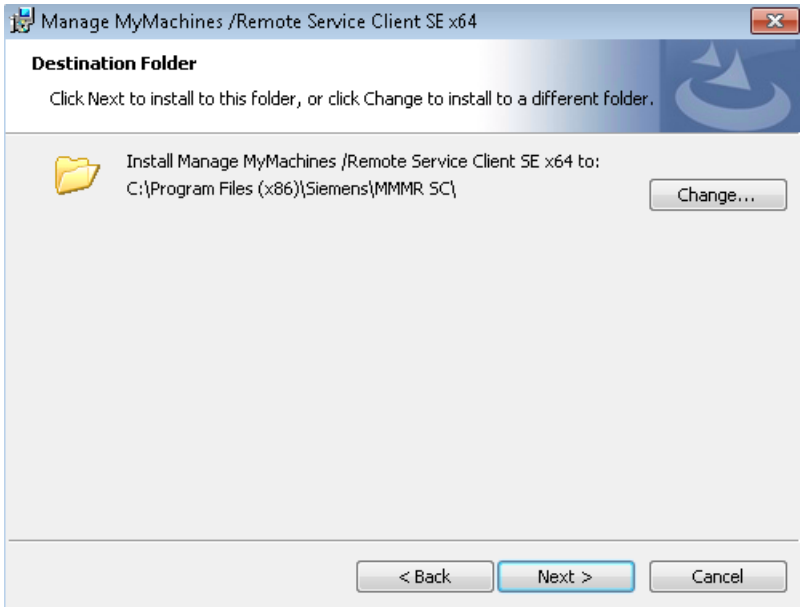
1. Open the installation directory on the operator PC.
2. Double-click to start the "MMMR_SC_MO_x64_setup.exe" setup file, e.g. from "Manage MyMachines /Remote Service Client for service engineers - 64 bit from Vx.x.x.x.".
   The welcome dialog "Welcome to the Wizard for Manage MyMachines / Remote Service Client SE x64 Vx.x.xx.x" opens.
   Click "Next >" to prepare the installation.



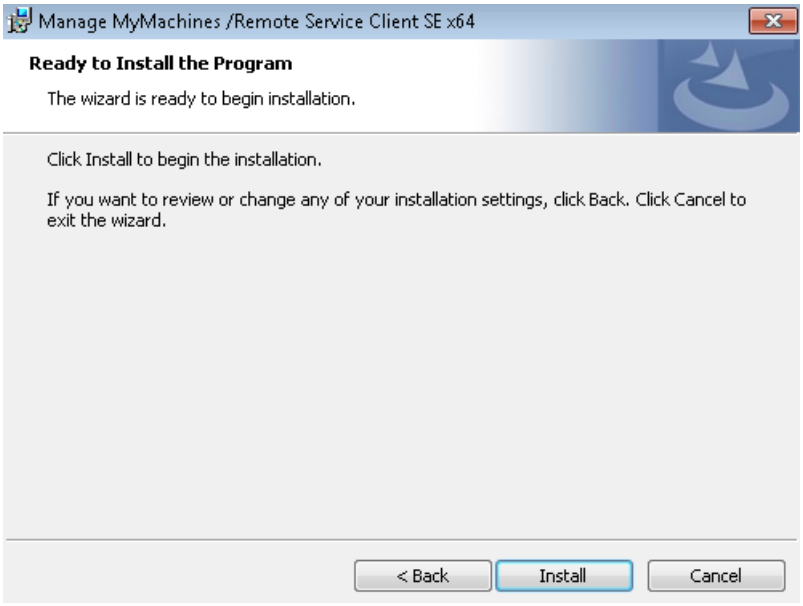
3. The "License Agreement" window opens.
   Read the license agreement.
   – Click "Print" if you want to print out the conditions.
   – Then select the "I accept the terms in the license agreement" option button and click "Next >".
     - OR -
     Click "< Back" to return to the previous window.



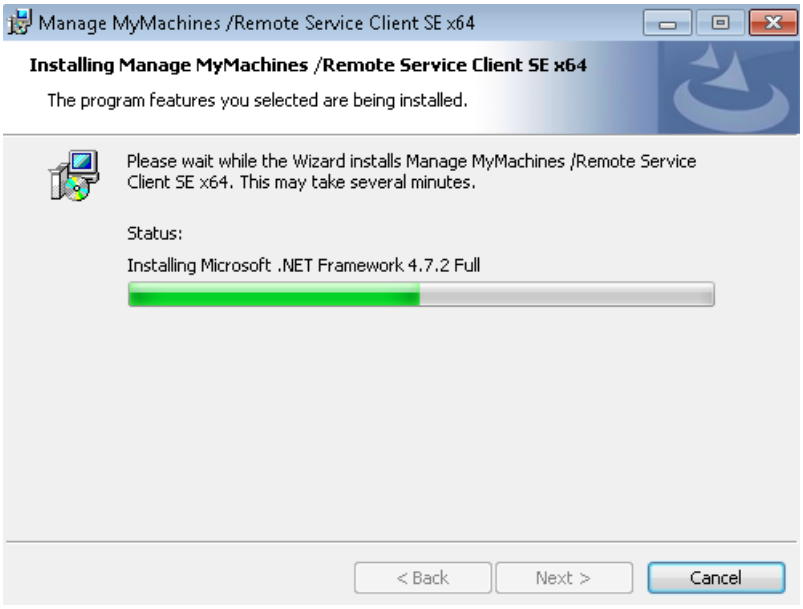
4. The "Destination Folder" window opens.
   Click "Next >" to accept the directory suggested by setup.
   - OR -
   Click "Change..." to change the installation directory.



5. The "Ready to Install the Program" window is opened.
   Click the "Install" button to start the installation.



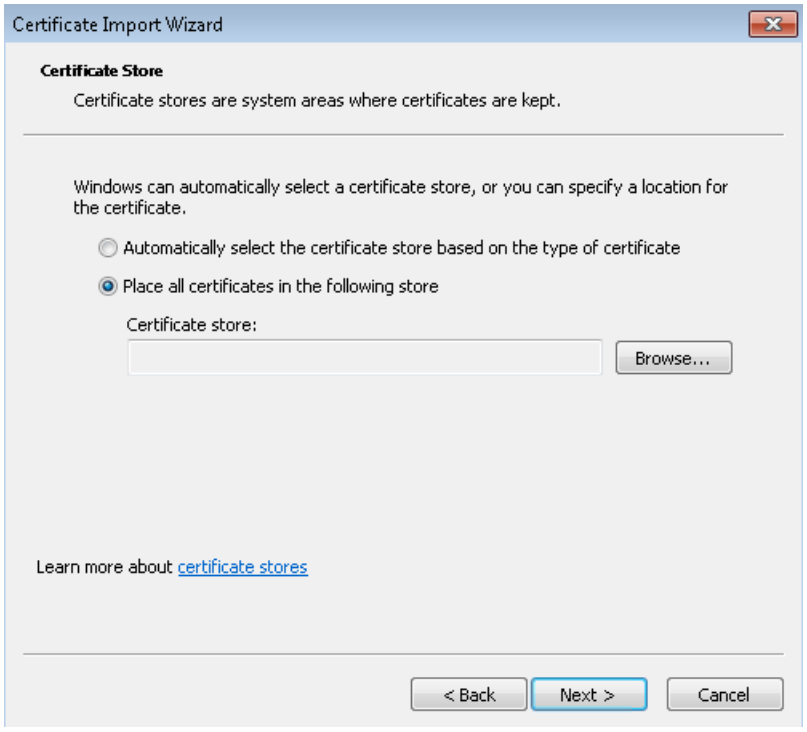
6. The "Installing Manage MyMachine /Remote Service Client SE x64" window is opened.
   The installation is started.



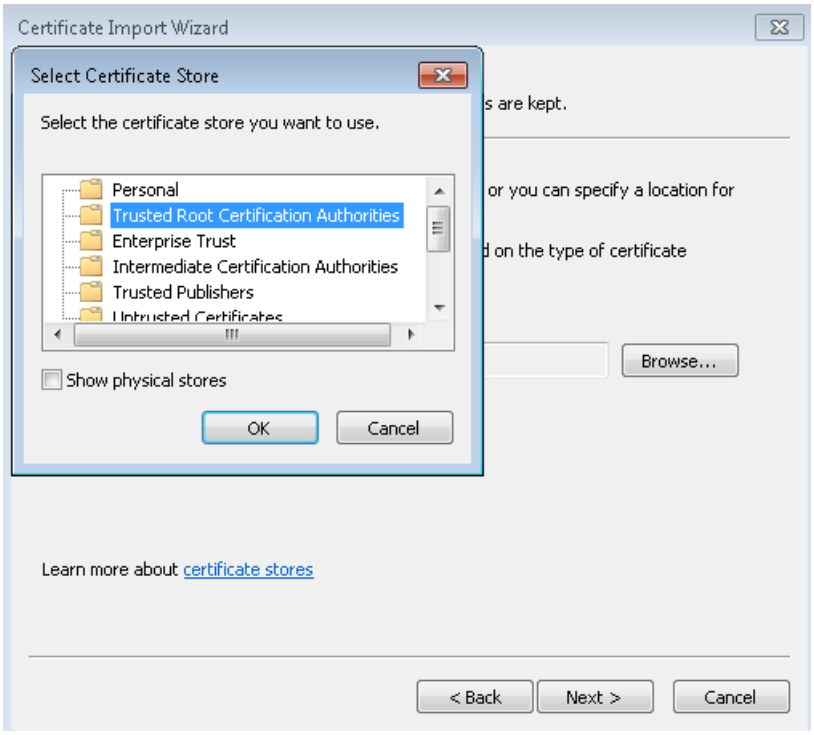
7. The "Welcome to the Certificate Import Wizard" window is opened.
   Click on "Next >".



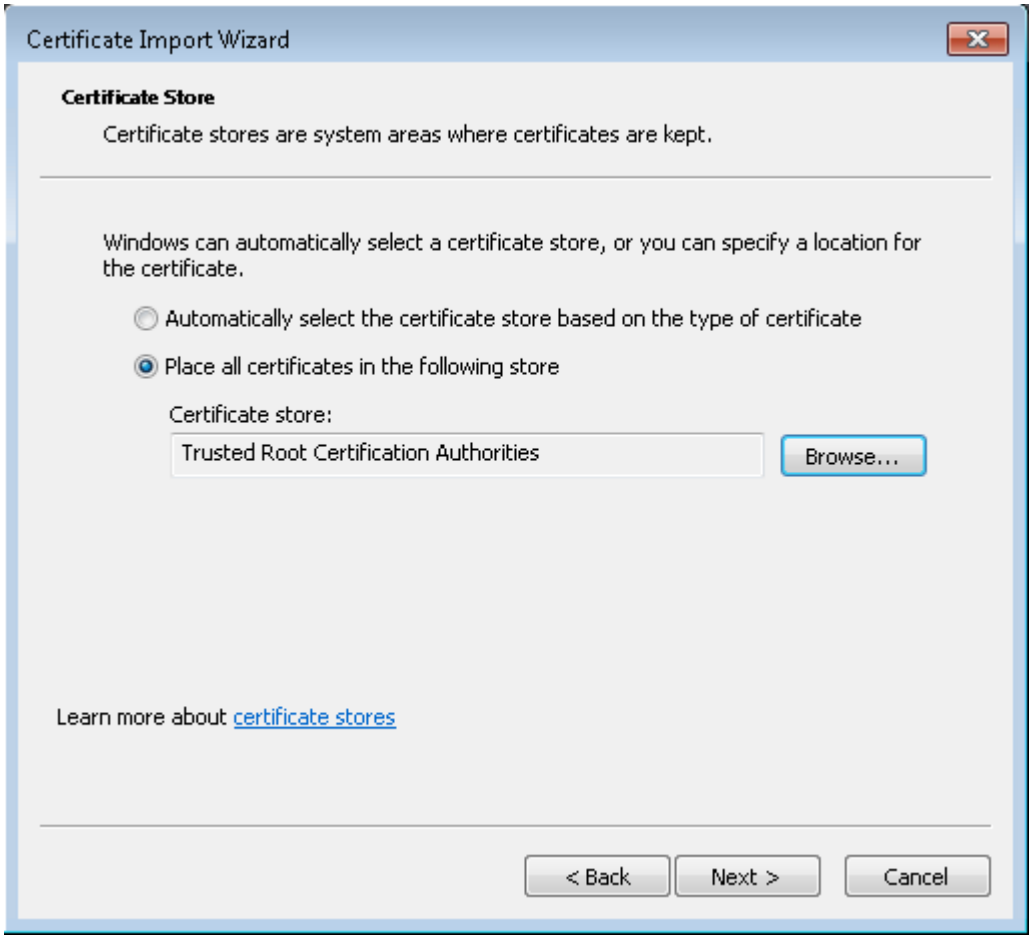
8. Window "Certificate Store" opens.
   Activate the "Place all certificates in the following store" option button.
   Click on "Browse...".



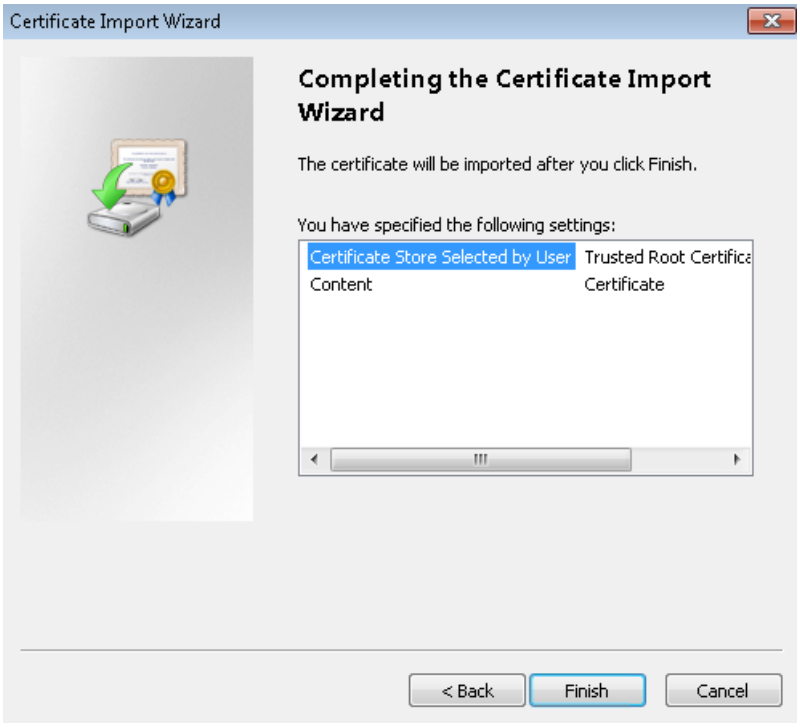
9. Window "Select Certificate Store" opens.
   Select "Trusted Root Certification Authorities" and click on "OK".



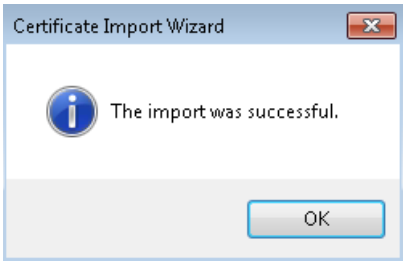
10. Window "Certificate Store" is redisplayed, and you see the entry below "Certification store:" Click on "Next >".



11. The "Completing the Certificate Import Wizard" window opens and shows you the settings. Click on the "Finish" button. The certificate is imported.



12. You receive a message that the certificate was successfully imported. Click "OK".

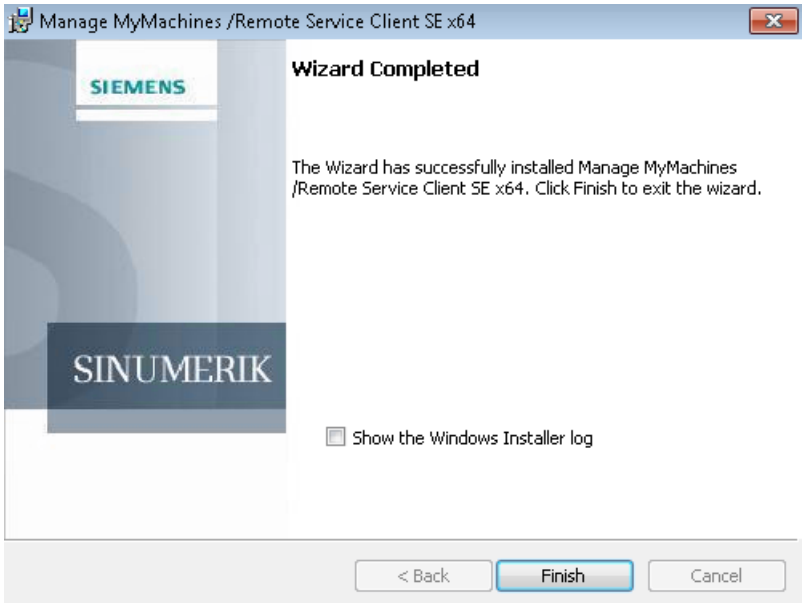


Note

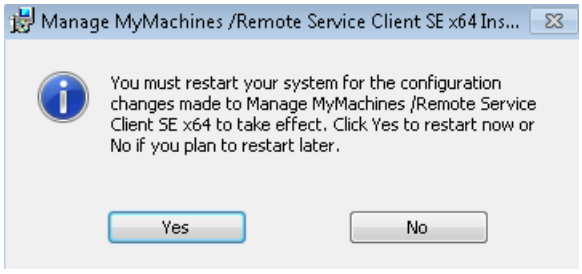
New request by the wizard

It is possible that the certificate import wizard again prompts you to import another certificate. Repeat steps as described under 7. to 12.

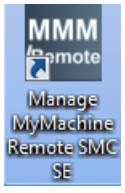
13. The "Wizard Completed " window opens.
    Click "Finish" to complete the installation.



14. Once installation has been completed, you will be prompted to restart your PC.
    Click on "Yes".



15. The following symbol is displayed on the desktop for you to start Manage MyMachines / Remote:



7.2.2 Entering the address of a proxy server

Overview

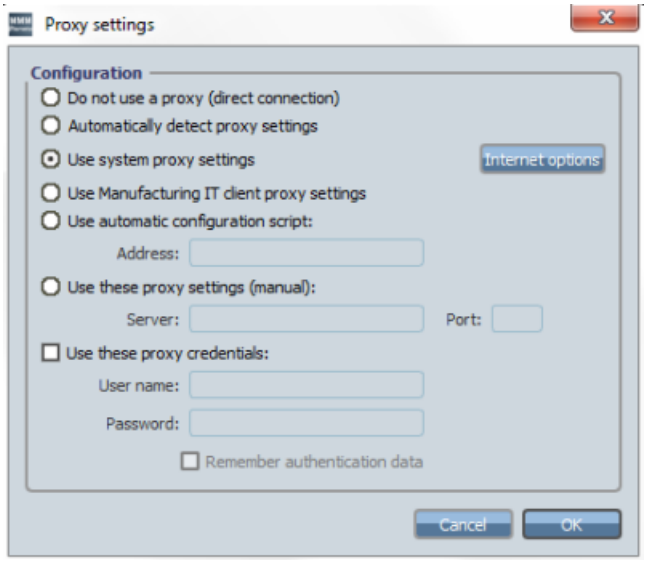
If access to the Internet is done via a proxy server, define the desired method via the proxy settings.

Settings	Description
Do not use a proxy (direct connection)	Establishes a direct connection to the Internet.
Automatic proxy detection	Automatically determines the address of a proxy server to access the Internet.
Use system proxy settings	The suggested setting: Uses the setting saved in Internet Explorer to go into the Internet. Click "Internet options" to open the Internet options of the system in order to check or change the proxy settings.
Use Manufacturing IT client proxy settings	Uses the settings of the Manufacturing IT client to gain access to the Internet.
Use automatic configuration script:	
Address	Address input of the proxy server from which the proxy script is downloaded.
Use these proxy settings (manual):	
Server	Address input (address and port) to specify a specific proxy server.
Port	
Use these proxy credentials:	
User name	Input of the access data if the proxy server requires a login.
Password	
Remember authentication data	The access data is stored retentively in the system. The password is stored in encoded form.

Procedure

1. Open "Manage MyMachines /Remote Service Client".
2. Call "Settings" > "Proxy..." in the menu bar.
   The "Proxy settings" window opens.

3. Select the desired proxy setting.
4. Click "OK" to save the settings.
   - OR -
   Click "Cancel" to reject the settings.



Using your own proxy logon data

If you are using your own proxy logon data, select the "Use these proxy settings (manual):" check box.

1. Then select the check box "Use these proxy credentials:" and enter your user name and password.
2. Select the "Remember authentication data" checkbox if you want to save your login data permanently.
3. Click the "OK" button to save the settings.

Using MyMachines /Remote Service Client 8

8.1 Overview of the functions

The following functions enable diagnostics to be performed and faults to be corrected via the control. It is up to the service engineer to execute the functions for all problems via remote access on a PC with a mouse and keyboard.

To be able to use these actions you must activate the functions in Manage MyMachines / Remote.

Functions

Function	Description
Desktop sharing	Permits the display and remote operation of a control. For safety reasons, however, it is not possible to initiate machine movements or to start NC programs. Additional information is provided in Chapter: Desktop sharing (SINUMERIK Integrate Client) (Page 168)
File transfer	Enables the transfer of one or more files or directories. Transfer can be from the workplace PC to the control or vice versa. This allows, for example, patches to be imported for the error correction. The control can also be updated quickly. Even complex NC programs are transferred to the service engineer for offline testing or for modification via file transfer. Additional information is provided in Chapter: Transferring files (Page 173)
Remote STEP 7	With STEP 7, the control tasks can be implemented based on the SIMATIC S7 automation systems. Additional information is provided in Chapter: Setting-up the Internet connection with SIMATIC Manager (Page 183)
Conference call	Allows several service engineers to participate in a conference. You either participate with an observing role or as leader of the conference. Additional information is provided in Chapter: Transferring the conference leadership (Page 192)
Automatic recording of the meeting	Enables the session to be recorded and archives to the server as session information.

8.2 User roles and operator interface

User roles

You can participate in a session with the following roles:

1. Session leader
2. Machine operator
3. Observing service engineer

These user roles can have different states and are defined on the user interface with different icons:

Icon	No.	Role	Status
	1	Session leader	The session leader actively participates in the session.
	2.	Session leader	The session leader is active and hosts the session (desktop sharing).
	3	Machine operator	The machine operator participates actively in the session.
	4	Machine operator	The machine operator hosts the session. The session leader does not control the remote desktop.
	5	Machine operator/service engineer	Transfer control
	6	Machine operator	The machine operator was present in the session, but is currently not present.
	7	Observing service engineer	The observing service engineer participates actively in the session.
	8	Observing service engineer	The observing service engineer was in the session, but is currently not present.

Information

It is possible to participate as an observing service engineer as follows:

- A service engineer at the operating PC leads the session
- A machine operator at the SINUMERIK control system participates in the session

User interface

	Description
Conference data	
Machine ID	Shows the ID of the machine.
Session ID	Shows the session ID.
Status	Displays current information for the session.
Tenant	Shows the organization of the connected machine.
Participants	
Name	Shows the names of the participants.
Status	Shows the current role of the participant.

		Description
Tenant		Shows the organization of the current user.
Remote access		Shows a remote access. Is only displayed for the head service engineer.
		Shows a terminated participant access.
		Shows that the function to end remote access is not available because desktop sharing has not been started. In this state, you cannot perform any function via the button.
File transfer		Shows the data transfer. Is only displayed for the head service engineer.
Transfer of leadership		Shows the transfer of leadership. Is only displayed for the head service engineer.

Symbols on the status bar

Icon	Description
	Shows a session recording.
	Shows no participation in the conference.
	Participation in a conference has been performed.
	The conference has been interrupted because of a network error.

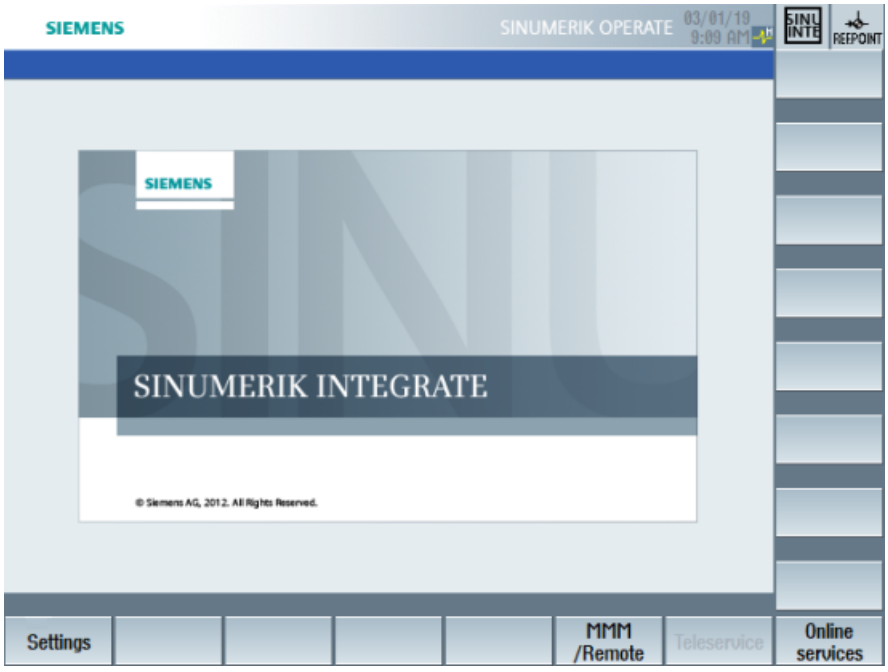
8.3 Joining a remote session as MO (PCU/NCU)

Precondition

- The SINUMERIK Operate operating software is started.
- The SINUMERIK control has been successfully connected with Insights Hub.
  More information is provided in Chapter: Install the registration key on a SINUMERIK control system (Page 43)
- As machine operator, the service engineer has informed you that he has started a remote session.

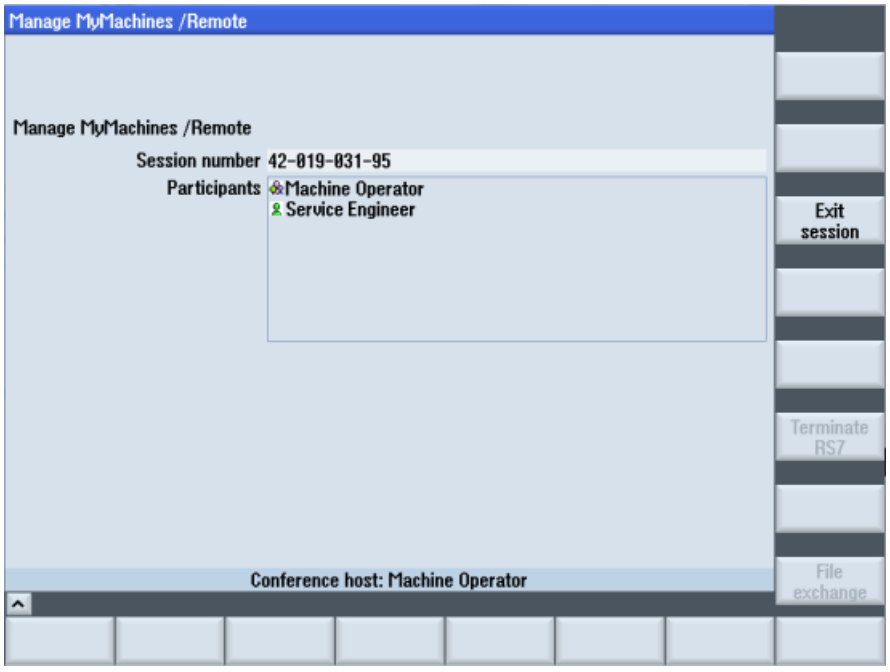
Procedure

1. Press the menu forward key and press softkey "SINUMERIK Integrate".
2. The "SINUMERIK INTEGRATE" window opens.
   For information
   The "MMM /Remote" softkey is available and activated if you have integrated "Manage MyMachines /Remote" as an OEMFrame application.
   Additional information on this topic is provided in Chapter. Integrating an OEMFrame application into HMI sl (Page 141).
   Press the "MMM Remote" softkey.

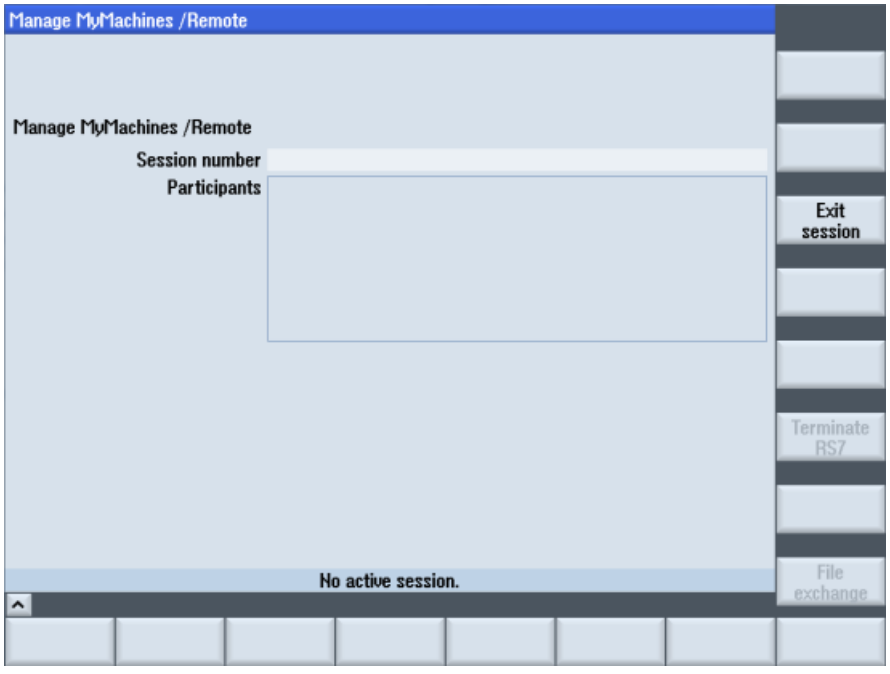


3. You can join the session as machine operator once the service engineer has started the session.

4. The "Manage MyMachines /Remote" session window opens. You see the session number and the participants.



- OR -
You see an appropriate message in the status bar if the service engineer has still not started a session.
Press the "Exit session" softkey if you wish to close the window.



5. The participants are displayed in the SE application once the participants have been registered at the SINUMERIK control system.
   As SE, you can use the following functions at the PC:
   - File transfer
   - Share screen
   - Remote STEP 7 is available for SINUMERIK Operate with Linux or Windows
     You can implement the control functions based on SIMATIC S7 using Remote STEP 7.
     You can find additional information at: Setting-up the Internet connection with SIMATIC Manager (Page 183)

   Additional information on the required versions of SINUMERIK Operate and SIMATIC Manager can be found at: "Supplementary Conditions".
6. To exit the session, press the "Exit session" softkey.

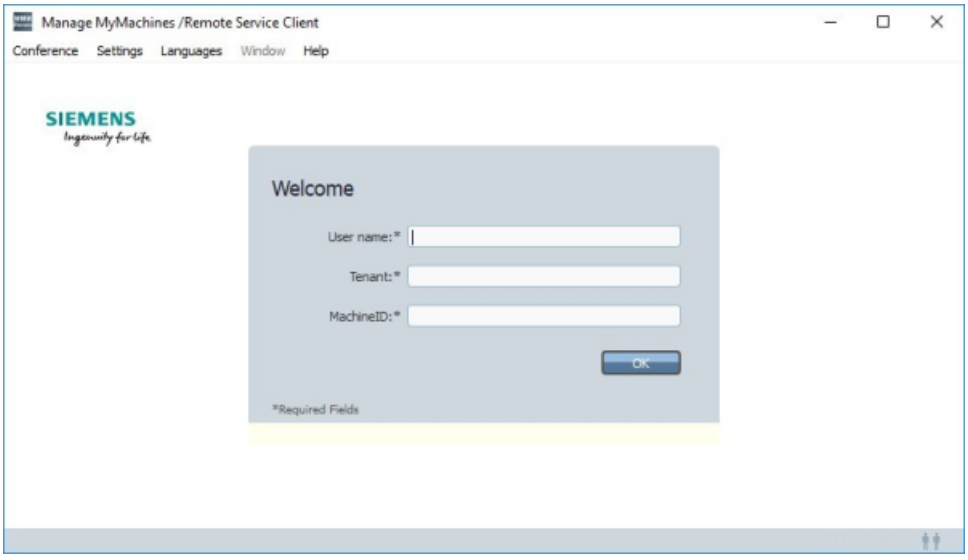
8.4 Joining a remote session as MO (IPC)

Precondition

- The "Manage MyMachines /Remote Service Client for machine operators - IPC" is installed.
  You can find additional information on this topic in the following chapter: Download remote service client (Page 94).
- As machine operator, the service engineer has informed you that he has initiated a remote session.
- The service engineer has started the session.

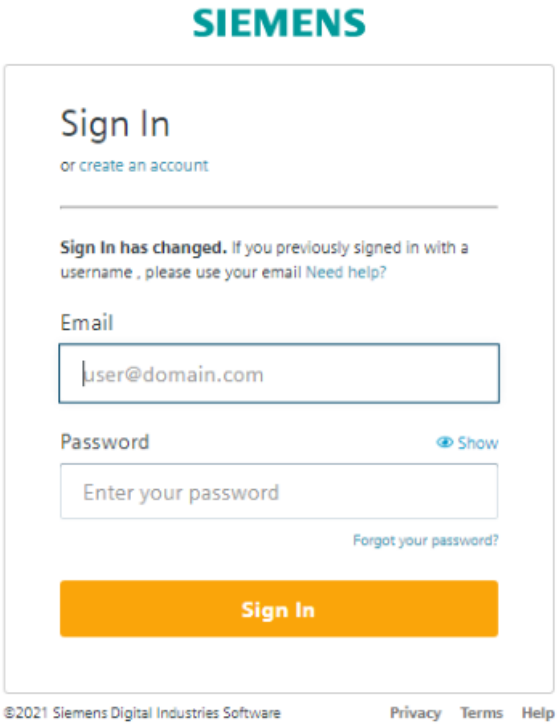
Procedure

1. Open the Manage MyMachines /Remote Service Client for machine operators - IPC.
   The "Welcome" window opens.

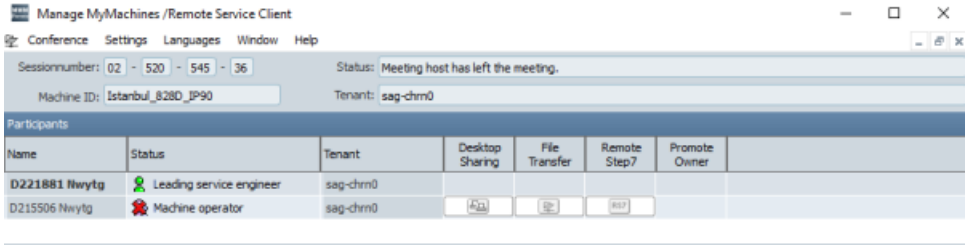


2. Enter your user name and your tenant.
3. When using the system for the first time, enter the machine ID.
   The machine ID is assigned when registering the machine for Manage MyMachines /Remote.
   If you select a registered machine in the Asset Manager or in Manage MyMachines, then the machine ID is displayed in the URL.
   Example of a machine ID: `a6cdxxxb8dca41d69456c6c6b7e5604e`
4. Click "OK".

5. When using for the first time, a "Sign In" browser window will appear for authenticating your machine.
   - Enter your email address and your Insights Hub password.
   - Click on "Sign In".



6. The "Manage MyMachines /Remote Service Client" session window opens.
   The session is established and you can see the list of participants.



Note

Opened session

You can participate as often as you want in a session that has been opened.
Only the session leader can finally close that session.

8.5 Conducting a remote session via VPN (IPC)

Virtual Private Networks (VPNs) allow users to send or receive data over a distributed or public network as if their computers were connected directly over a private network.

- The service engineer sends an invitation to the VPN conference.
- The machine operator agrees to the VPN connection.

Note

Service engineer PC

- It is not permissible that the service engineer has any administrator rights on the service engineer PC.
- The administrator of the service engineers PC must define the permissible applications, which communicate via the virtual VPN adapter, by configuring the firewall settings of the operating system.

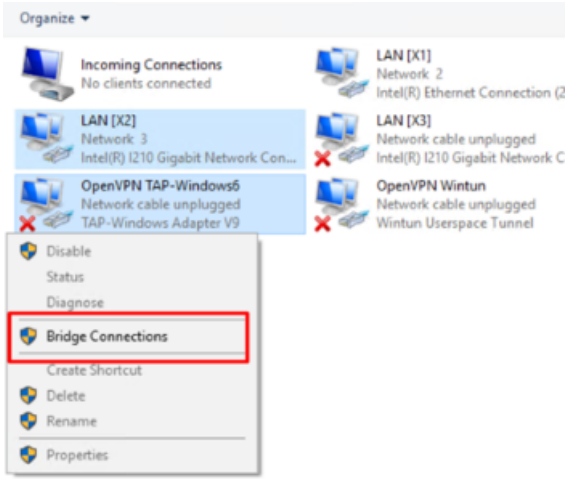
Precondition

- The connection between the service engineer at the PC and the machine operator at the SINUMERIK control system has been established.
  More information is provided in Chapter: Joining a remote session as MO (IPC) (Page 160).
- OpenVPN has been installed for both the service engineer and the machine operator, e.g. using Silent Installation.
  More information is provided in Chapter: Silent Installation (Page 142).
- A "Network Bridge" is set up for OpenVPN TAP and LAN [X2] (only has to be done once after a new installation):

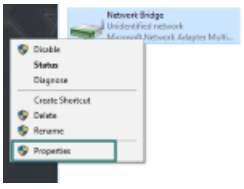
  Note

  The Windows English user interface is shown in the following diagrams.

  – Under "Network connections", select OpenVPN TAP and LAN [X2] and open the menu with a right-click
    Click on "Bridge Connections".



  – The "Network Bridge" network is created. Open the Network Bridge menu with a right-click and click on "Properties".



– Activate checkbox "Internet protocol version 4 (TCP/IPv4)" and click on button "Properties". Enter an IP address and then click on "OK".

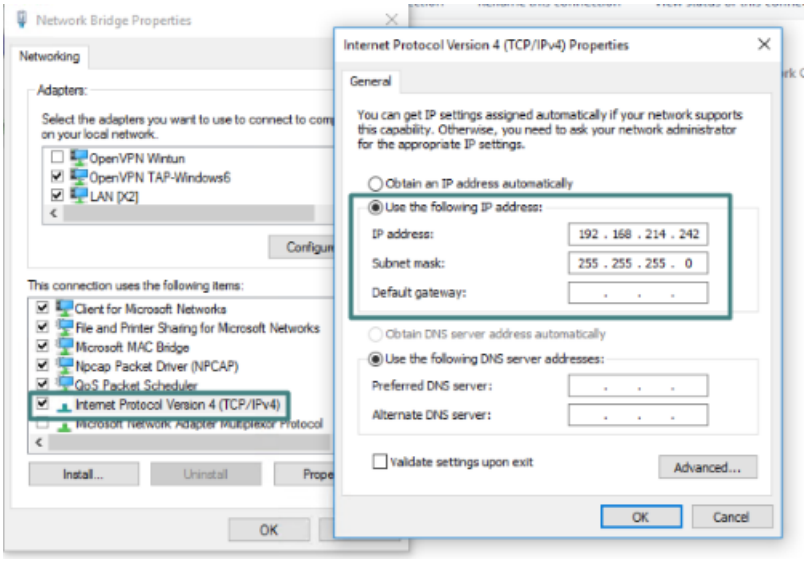
Note

Network Bridge settings

For the network bridge, the same network settings and restrictions apply that were defined for IPC LAN [X2].

The assigned IP for the network bridge must be one of the inactive IPs in the same machine network.

The OpenVPN-IP address assigned for the service engineer client as a default is 192.168.214.6. If this IP address is already being used, then it must be updated to an inactive IP in file "mmmr_se.ovpn" under "C:\Program Files (x86)\Siemens\MMMR SC".



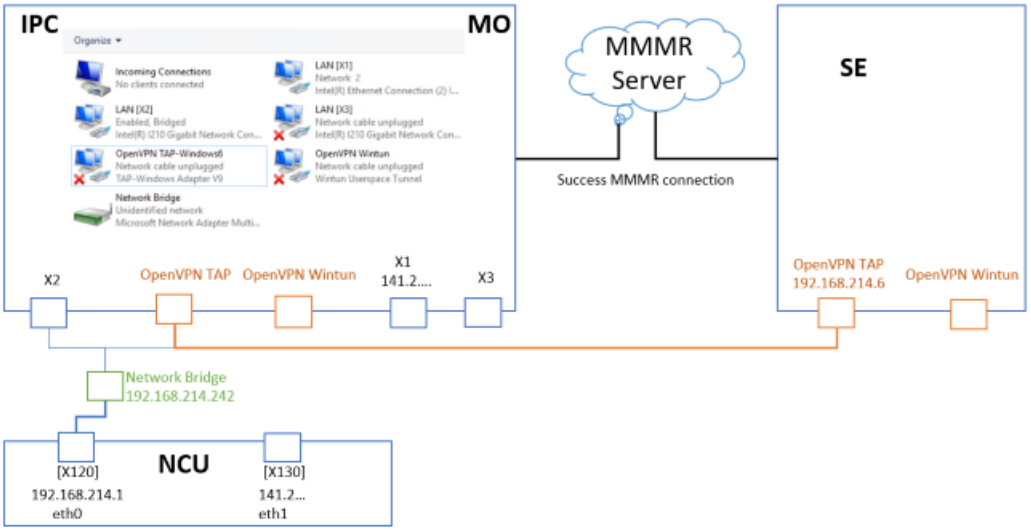
– Within the simulation environment, IPC [X2] had a direct connection to NCU [X120].

Note

Using the VPN connection, you can access devices in the machine network.

Any other procedure requires additional security measures.

After establishing the network bridge, a direct connection to the PLC on the NCU via SINUMERIK Operate is not supported.

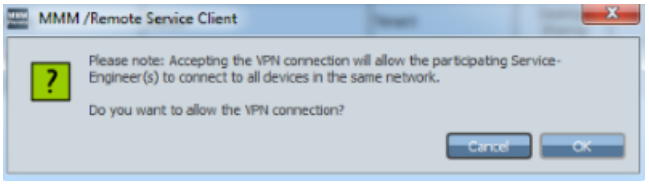


Procedure

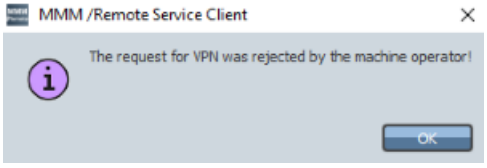
1. With a connection established, the service engineer clicks on the "VPN" icon in the "Manage MyMachines Service Client" to send an access request.



2. The machine operator receives a message in the "Manage MyMachines /Remote Service Client" session window indicating that the service engineer wants to establish a VPN connection allowing him to access all devices in the same network.

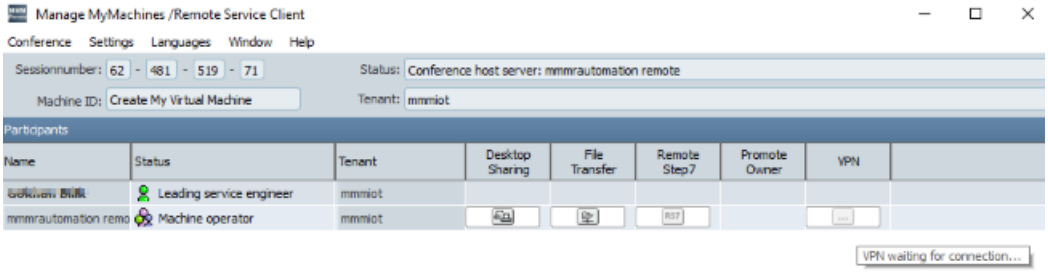


   – The machine operator clicks on "Cancel" if he does not wish to establish a connection. The service engineer receives an appropriate notification.

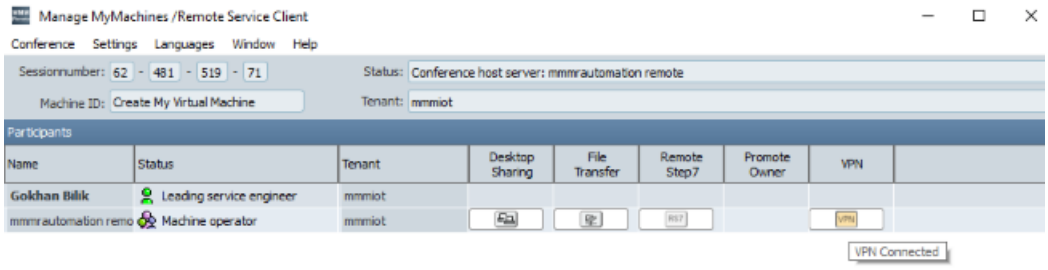


   – The machine operator clicks on "OK" if he agrees to establish a connection.

3. While the VPN connection is being established, the service engineer can see the tooltip "VPN waiting for connection..." when the mouse pointer is hovered over the VPN button.



4. After successful establishment of the VPN connection, the following window is started on both sides:
   - "OpenVPN Connection (mmmr_se)" is started on the service engineer's PC.
   - "OpenVPN Connection (mmmr_mo)" is started on the machine operator's control.
   - On both sides, the color of the "OpenVPN Connection (mmmr_se)" and "OpenVPN Connection (mmmr_mo)" icon in the taskbar changes from yellow to green.
5. The color of the "VPN" icon changes in column "VPN".
   Message "VPN connected" is displayed in the tooltip if the mouse pointer is positioned above the icon.



8.6 Desktop sharing (SINUMERIK Integrate Client)

Desktop sharing enables the display and remote operation of a control. For safety reasons, however, it is not possible to initiate machine movements or to start NC programs.

- The owner of the conference requests desktop sharing.
- The machine operator consents to desktop sharing.

Precondition

- The connection between the service engineer at the PC and the machine operator at the SINUMERIK control system has been established.
- Using the SINUMERIK Operate operating software, the rights for remote access was set under "Diagnostics" > "Remote diagnostics" > "Right for remote diagnostics".
- The "Desktop sharing" function is activated.

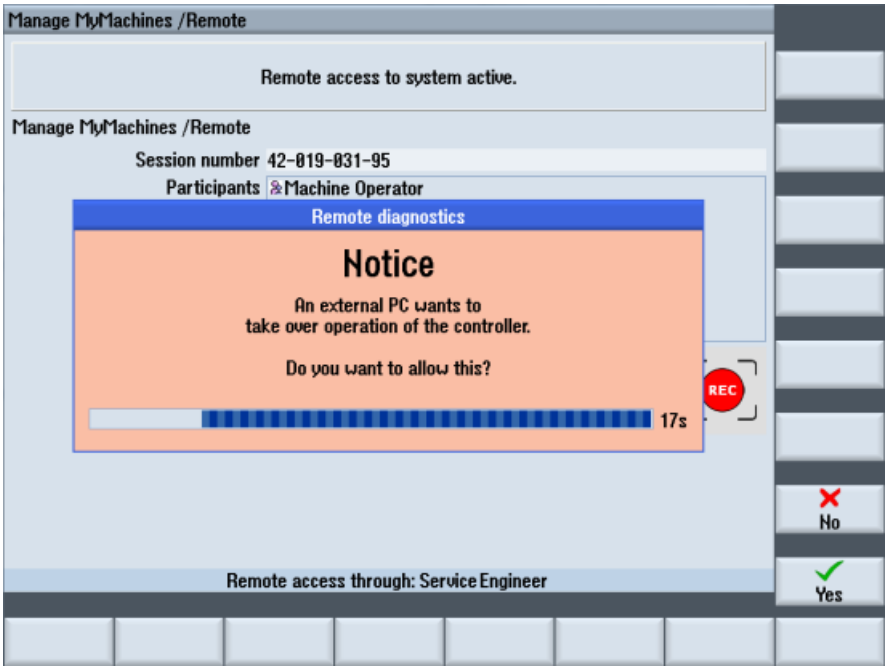
NOTICE
Allowing remote access to the SINUMERIK control system Only allow a remote access session if you know the following: • Have you been notified of a remote access session? • Do you know and trust the person who is conducting the session?

Procedure

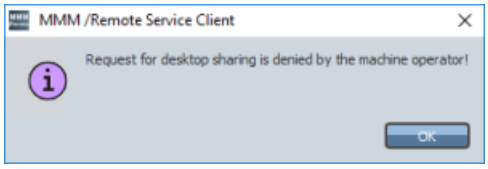
1. The owner of the conference clicks the "Desktop sharing" icon to access the SINUMERIK control.



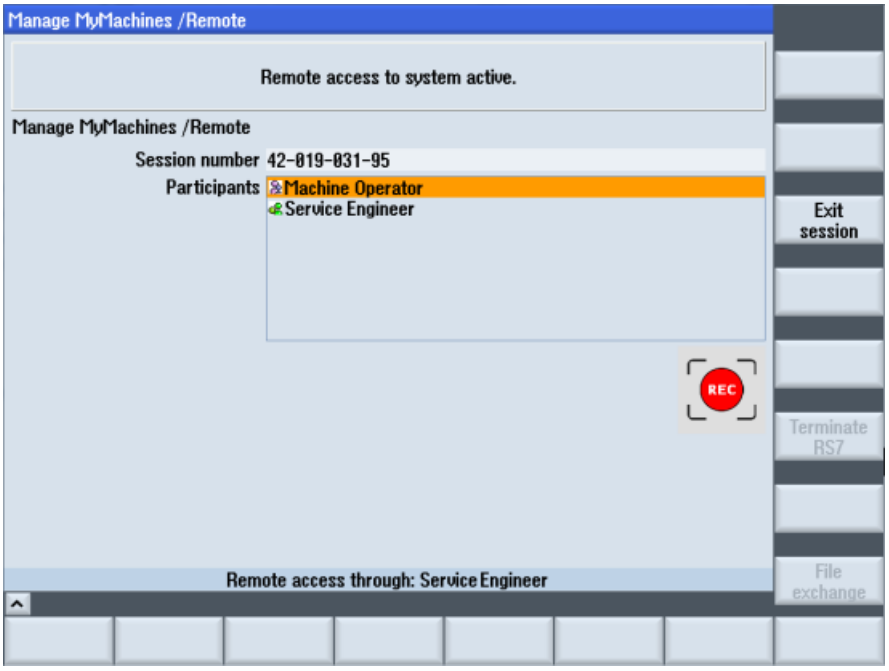
2. The machine operator at the SINUMERIK control system receives a message that an external PC wishes to access the control system.
   The machine operator can either authorize or deny access.



   – The machine operator clicks "No" to deny access.
     The service engineer cannot control the SINUMERIK control system of the machine operator until access permission is issued by the machine operator.
     The service engineer sees the following message:



– The machine operator clicks "Yes" to authorize access.
The user interface of the SINUMERIK control system is then displayed at the operator PC.
The service engineer can now access the SINUMERIK control system.
The "REC" icon indicates the access.



Note

Only one desktop can be shared

If remote control is already active, a second desktop cannot be shared on the same SINUMERIK control within the existing session.

Note

Scaling the screen

If you change the screen size at the PC, then the size of the user interface is also scaled.

When access is terminated, the position and size of the screen is saved. If you reopen the same session, then the same screen size is displayed.

8.7 Desktop sharing (IPC / PCU)

Desktop sharing enables the display and remote operation of a control. For safety reasons, however, it is not possible to initiate machine movements or to start NC programs.

- The owner of the conference requests desktop sharing.
- The machine operator consents to desktop sharing.

Precondition

- The connection between the service engineer at the PC and the machine operator at the SINUMERIK control system has been established.
- The "Desktop sharing" function is activated.

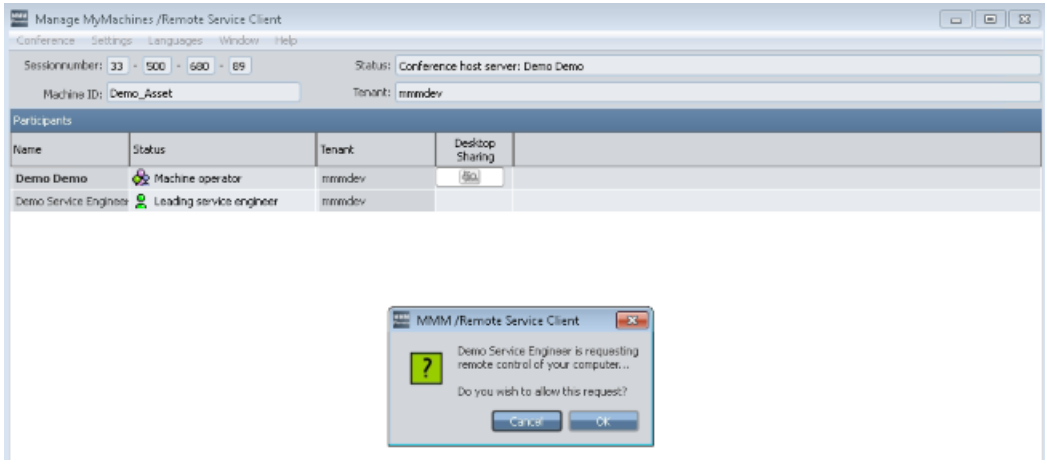
NOTICE
Allowing remote access to the SINUMERIK control system Only allow a remote access session if you know the following: • Have you been notified of a remote access session? • Do you know and trust the person who is conducting the session?

Procedure

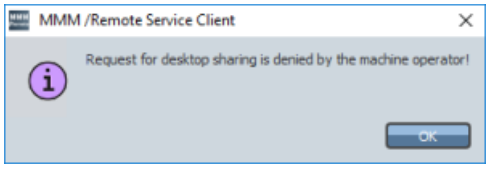
1. The session leader clicks on the "Desktop sharing" icon to access the machine operator's PC.



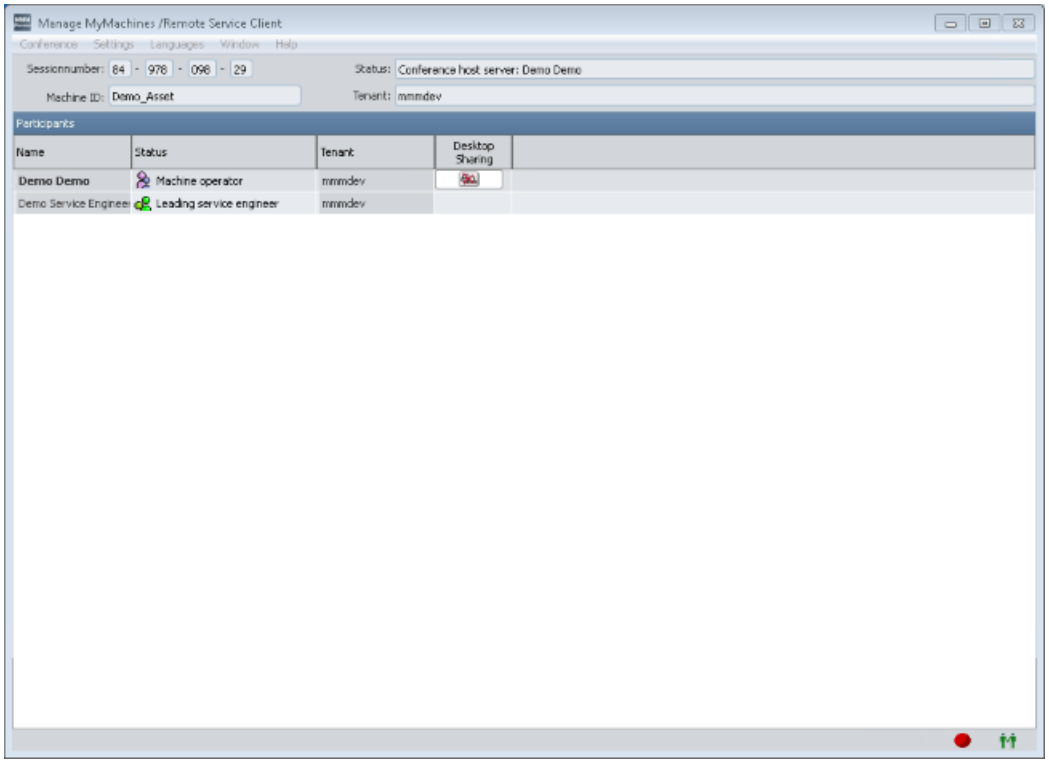
2. The machine operator in the MMM /Remote application receives a notification that an external PC would like to access the control system.
   The machine operator can either authorize or deny access.



   – The machine operator presses "Cancel" if he denies access.
     The service engineer cannot control the machine operator's PC until the machine operator issues access permission.
     The service engineer sees the following message:



– The service engineer clicks on "OK" if the machine operator authorizes access.
The user interface of the machine operator's PC is then displayed on the service engineer's PC.
The service engineer can now access the machine operator's PC.
The red dot in the status bar indicates access.



8.8 Transferring files

It is possible to transfer single or multiple files or directories between the service engineer's PC and the operating PC of the machine operator - and vice versa. This allows, for example, patches to be imported for error correction.

Precondition

- The connection between the service engineer and the machine operator has been established.
- The "File Transfer" function is current.

Important icons

Icon	Description
	Opens the higher level in the directory tree.
	Updates the view of the directory tree. The directory list is only updated automatically when other actions, such as navigation, copying, renaming or deleting, have been performed. If the machine operator makes changes to the directory tree outside of the remote session, the owner of the conference must update the view.
	Creates a new subdirectory in the selected directory level.

Displaying file properties

In the "Filetransfer" window, the following file properties are displayed in the file system in the column view:

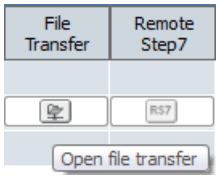
- File name
- File size
- Date of the last change
- Attributes

When you close the window, the window size and position are saved. When the function is opened again, the window is restored with the same dimensions.

You can set the column width and position. However, the settings are not saved.

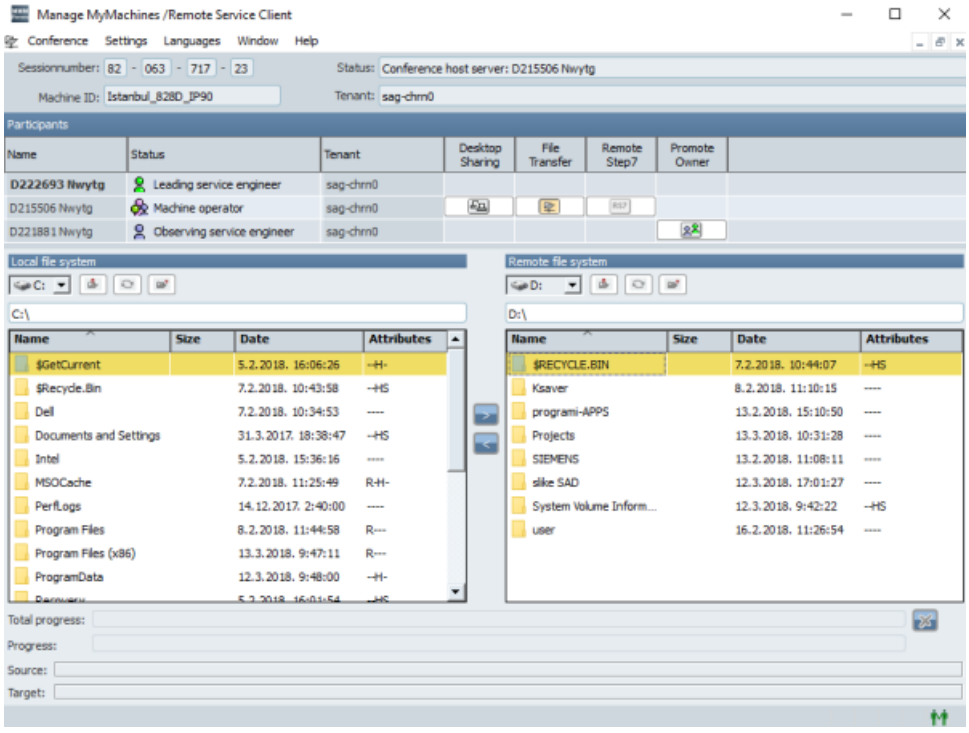
Start transmission

1. Click the "Open file transfer" icon to start the file transfer.



2. The "Filetransfer" window is displayed once the function has been established.
   You can now transfer files between your PC (local file system) and another PC (remote file system).
3. Use the cursor to navigate to the required files.
4. Some directories and files are protected. If you do not have sufficient access rights, the message "Access denied" is displayed.

5. Select the files or directories that you want to transfer, either at the PC (local file system) and/or at the remote file system.



6. The machine operator must grant permission for the file transfer.

Note

Issuing permission for all functions of a session

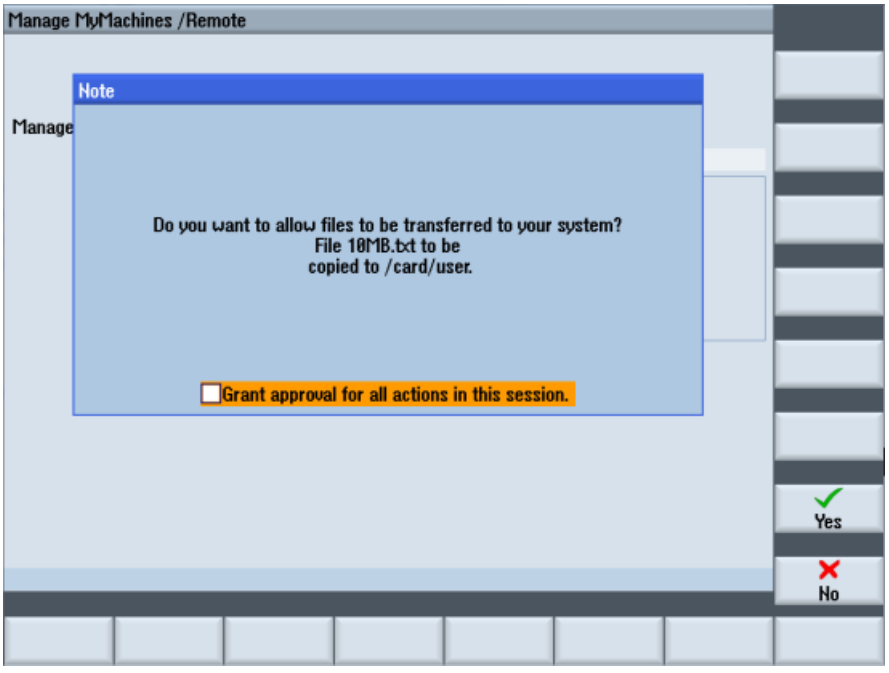
If the machine operator activates option checkbox "Grant approval for all actions in this session" then approval is also issued for the following functions of the session:

- Desktop sharing
- File transfer
- STEP 7 via Internet
- Automatic session recording

If the machine operator uses the SINUMERIK control:

– Transfer is started if the machine operator presses the "Yes" softkey.

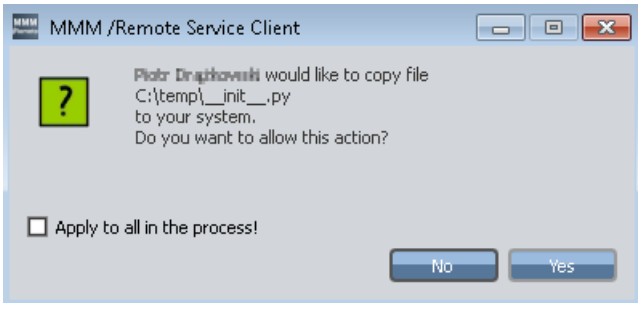
– Transfer is denied if the machine operator presses the "No" softkey.



If the machine operator uses the application MMM /Remote PCU/IPC:

– Transfer is started if the machine operator clicks on "Yes".

– Transfer is rejected if the machine operator clicks on "No".



7. Copy the selection into the appropriate directory using symbols ">" / "<".
   No other actions can be performed during the copying procedure.

Note

The file transfer can be canceled by the machine operator. In this case, the message "Filetransfer canceled!" appears

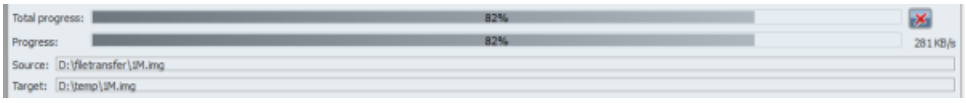
Note

If a directory or a file already exists in the target system, the following prompt is displayed: "Path already exists on the remote file system. Overwrite?" The source and target directories are also displayed.

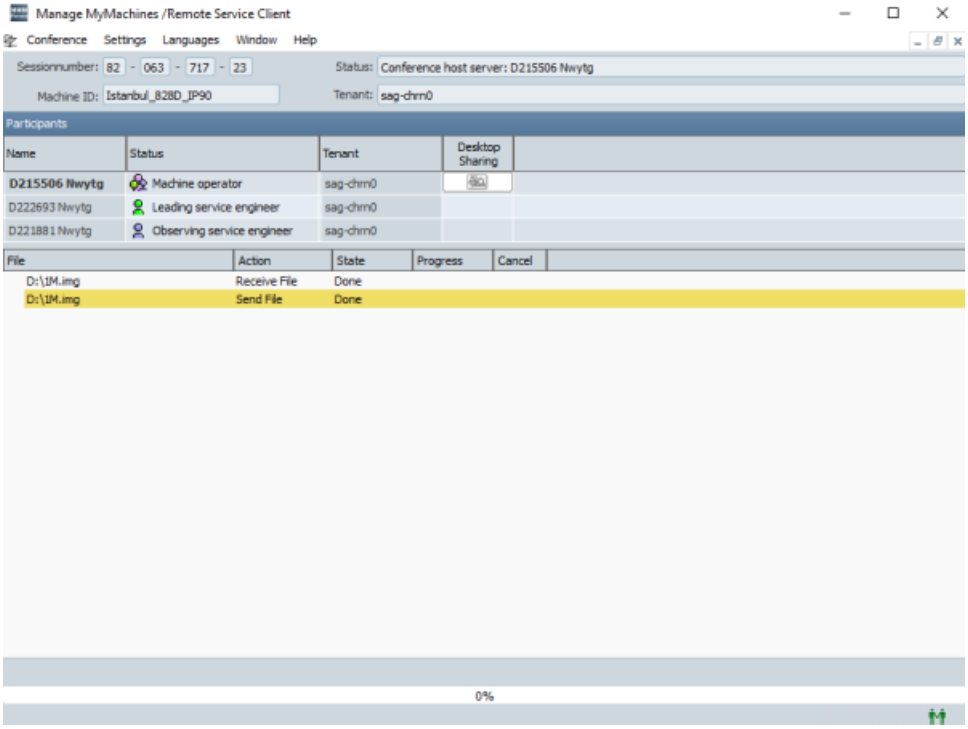
Confirm this message with "OK".

If you no longer want to receive such messages, activate the "Apply to all in the process!" checkbox before confirming.

The operation is displayed on a progress indicator.

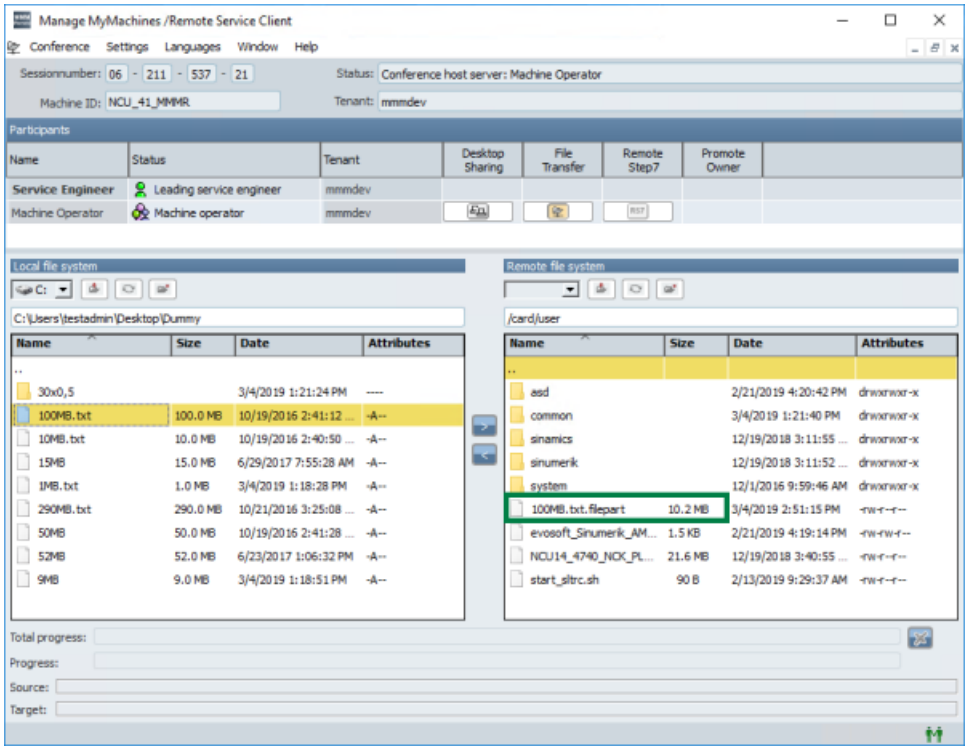


8. You see the result at the end of the data transfer.



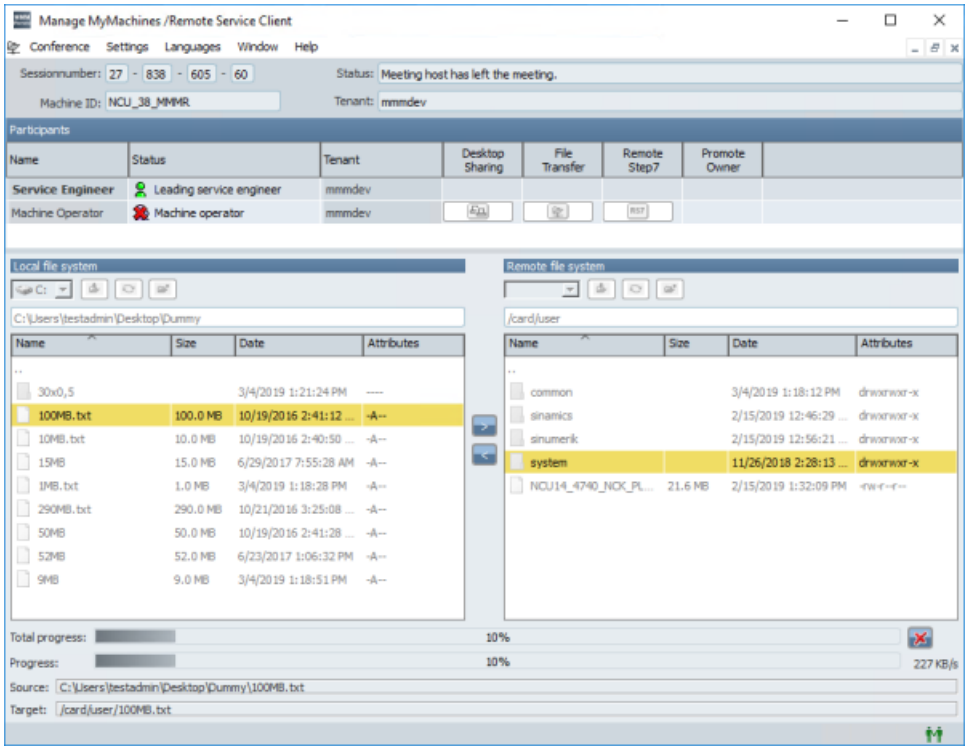
Resuming the file transfer

If a file transfer is interrupted by a temporary network fault, the copy procedure is resumed automatically when the connection is established again. During network failure, the corresponding window is deactivated. As soon as the network fault has been corrected, file transfer is automatically resumed starting from the last byte transferred successfully.



If the connection cannot be re-established during the current session, then the transfer can be continued manually in a later, separate session.

The service engineer must start the copying procedure to the same target directory again. If the system finds the incomplete file from the previous unsuccessful transfer in this directory, then the operation is continued from precisely this position.



Note

Check the source and target files

To ensure that the source and target files are identical, the checksums are compared first. This calculation can take several minutes for large files (above approx. 100 MB). During this interval, the message "Waiting for confirmation!" is displayed in the status bar.

Creating a new directory

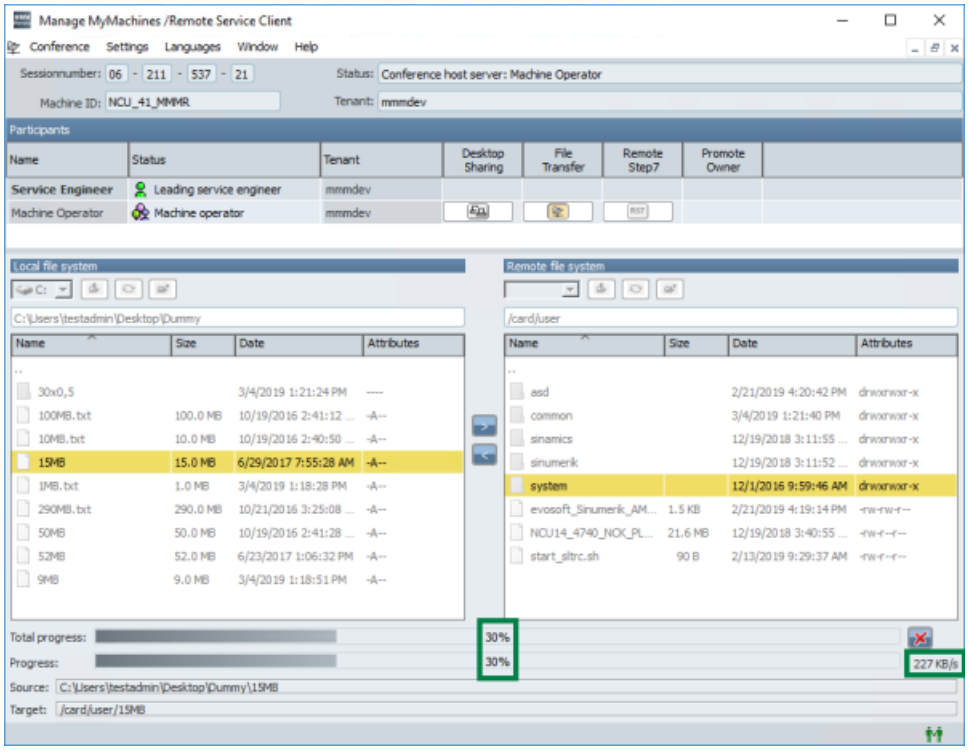
You can create new directories on your operator PC or on the SINUMERIK control in the same way.

1. Navigate to the required directory level.
2. Click the icon to create a new directory.
3. Assign a name to the new directory.
4. The machine operator must authorize creation of the directory.

Performance optimization of the file transfer

The "speed" of file transfer depends on the specific network configuration and the network load. The file transfer rate can also fluctuate substantially during transfer.

In addition to the progress bar, the current percentage and transfer rate (KB/s) can be observed.



Display of the file transfer in the protocol

The actions performed by the service engineer are shown in the dialog below the list of participants in the protocol. The protocol is only available for the machine operator.

Protocol window of the file transfer	
File	The protocol window of the file transfer opens automatically when the service engineer performs an action. The window can also be shown or hidden via the "Conference" > "File transfer protocol" window. The directory and the file name to which the actions performed by the service engineer refer, are displayed in the window. The protocol settings can be made using window "Settings" > "File transfer".
Action	Shows the type of action.
Status	Shows the current status of the action.
Sequence	Shows the progress as a percentage and as a progress bar. A progress bar and percentage is also shown in the lower part of the window.
	The machine operator can cancel the action via the icon.

The machine operator automatically sees the protocol when the service engineer starts the file transfer. Irrespective of this, the machine operator can open and close the protocol window manually:

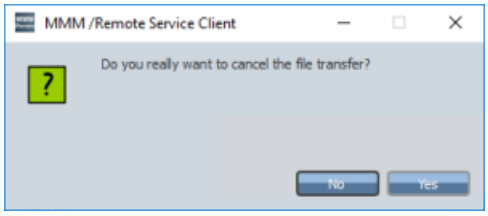
1. Call the "Conference" > "File transfer protocol" menu.
   You will see the log in the lower window with the current status.
2. During the file transfer, in addition to the name of the current file, you will see the action performed, the status, a progress bar and an icon to cancel the file transfer in the protocol window.

Note

In the "Settings" menu, you specify whether the file functions performed during a session are to be written to a protocol file.

Canceling file transfer

1. Click on icon  to cancel an ongoing file transfer.
2. A confirmation prompt is displayed.
   Click on "Yes" to irrevocably cancel the file transfer.



Deleting files

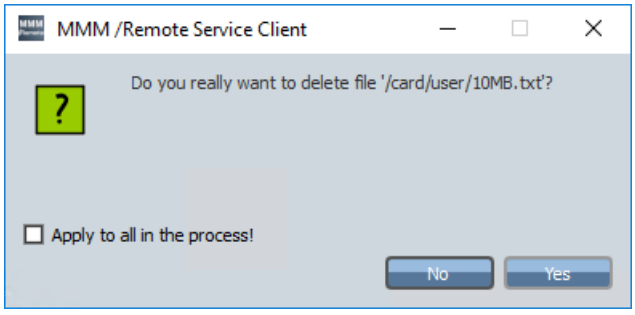
1. Select the directories or files to be deleted.
2. Right-click to call the "Delete file" menu command.

Note

If you delete a directory or a file with write protection, the following prompt is displayed: "File is write-protected, do you still want to delete it?"

- Click "OK" to delete the message.
- If you no longer want to receive such messages, select the "Apply to all in the process!" check box before confirming.

3. The machine operator must authorize the deletion of the files.



Note

Delete operation

You cannot perform any other actions during deletion.

Renaming a file

As a remote user, you can change the name of transferred files or directories:

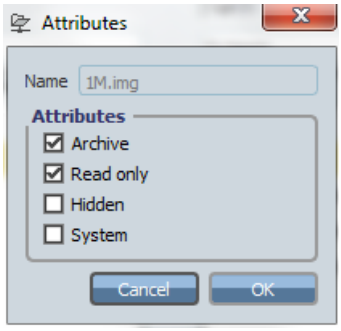
1. Select the appropriate file or directory.
2. Right-click to call the "Rename" menu command.
3. Enter the required name.
4. Click "OK".
5. The machine operator must authorize the name change.

Assigning attributes

As a remote user, you can change the attributes of transferred files or directories:

1. Select the appropriate file or directory.
2. Right-click to call the "Attributes" menu command.
   The setting dialog opens for the attributes of the selected element (file or directory).
3. Set the required attributes via the check boxes.

4. Click "OK" to confirm the settings.



5. The machine operator must authorize the attribute change.

Ending file transfer

You end file transfer in the same way:

- Owner of the conference: You close file transfer using icon "X" in the upper right-hand section of the window.
- Owner of the conference: You close file transfer and end the conference.
  File transfer and any operations still in progress are terminated.
- Machine operator: You leave the conference.
  The message "File transfer canceled!" is displayed for the service engineer.

8.9 Remote STEP 7

8.9.1 Setting-up the Internet connection with SIMATIC Manager

Using the "Remote STEP 7" function, as a remote user, you can execute all of the functions in SIMATIC Manager.

Prerequisites

- The SIMATIC Manager must be installed on the local PC.
  Versions 5.4 and 5.5 are supported.
- The Service Engineer Client must then be installed.
- The client on the machine operator side must support Remote STEP 7.
- The network interface of the SIMATIC Manager on the PC must be adapted.
- The "Step 7 via Internet" function is updated.

- The "Commissioning engineer" or "Service engineer" role must be assigned.
- The operator at the SINUMERIK control system must have adequate access rights.
  - Machine manufacturer (password)
  - Service (password)
  - User (password)

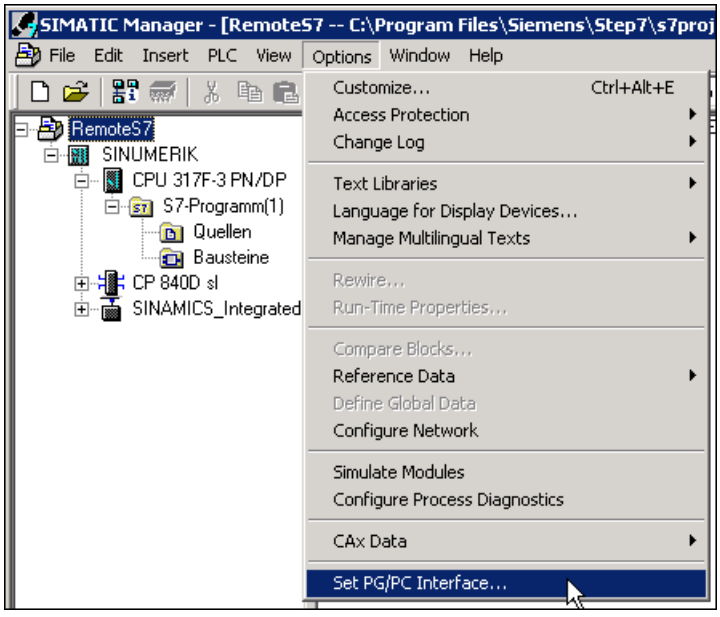
Further information can be found at: Installation Manual "SINUMERIK Integrate MMP, MMT, AMC, AMP, AMM/E, AMD".

NOTICE
Allowing remote access to the SINUMERIK control system Only allow a remote access session if you know the following: • Have you been notified of a remote access session? • Do you know and trust the person who is conducting the session?

Changing the network interface of the SIMATIC Manager

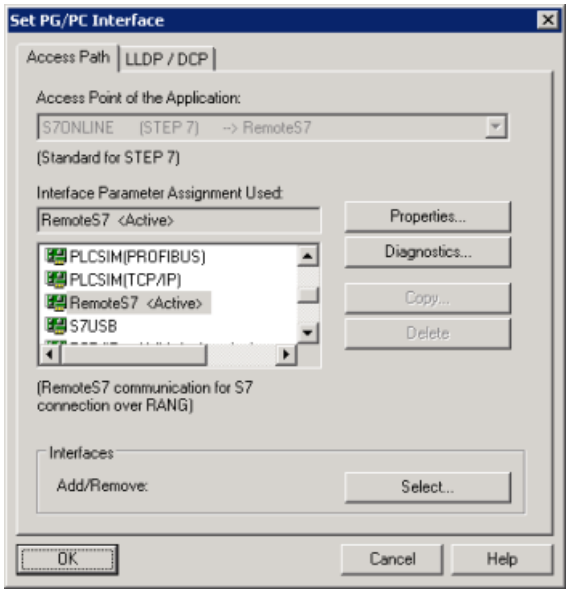
To be able to use the "RemoteS7" function, the network interface of SIMATIC Manager must first be changed.

1. Open the menu "Tools" > "Set PG/PC interface..." in SIMATIC Manager.

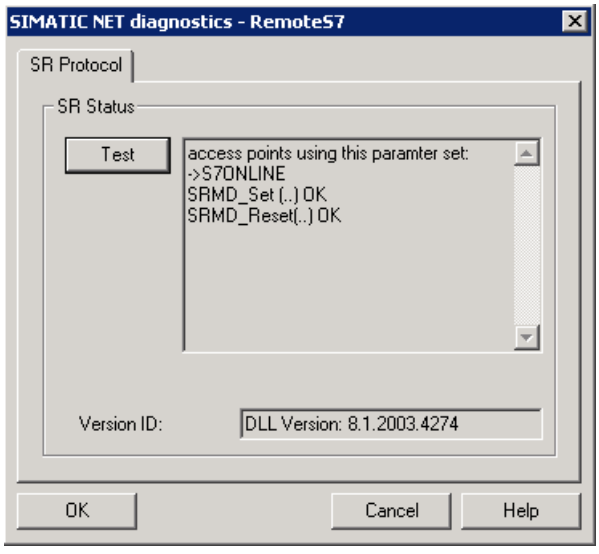


2. The "Set PG/PC Interface" dialog opens.
3. Click the "Access Path" tab.
   In the "Interface Parameter Assignment Used" list, navigate to the "RemoteS7" interface parameter assignment and select the appropriate entry.

4. Click on "Diagnostics..." if you wish to test the interface parameterization.

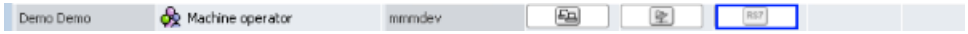


5. The Diagnostics dialog then opens.
   Click "Test". The result is displayed in the Diagnostics dialog.
   Click "OK" in both dialogs.

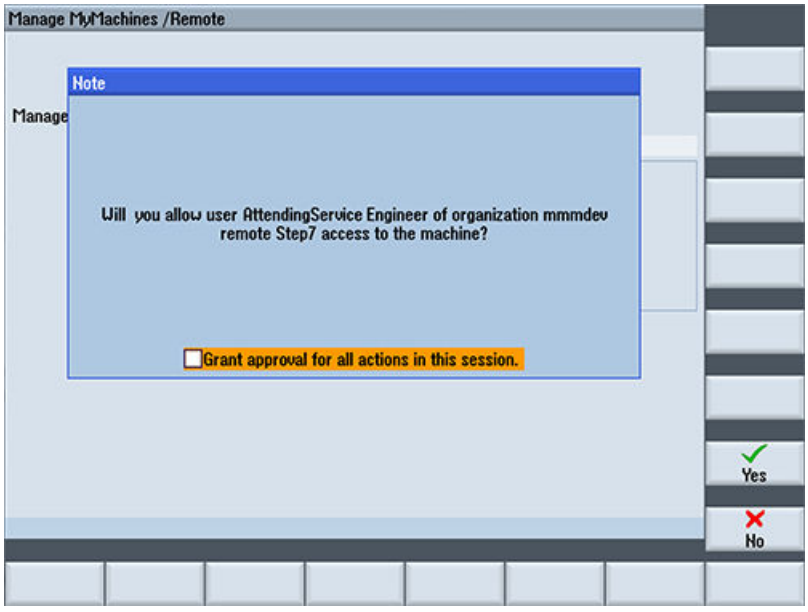


Start Remote STEP 7 on the SINUMERIK control system

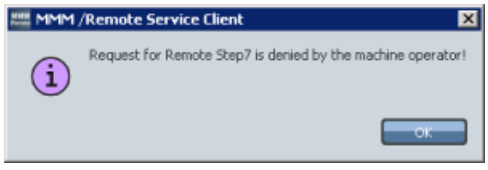
1. Click on the "RS7" icon to remotely access the SINUMERIK control system.



2. The function start depends on the default setting:
   - Remote STEP 7 is active after a short time when the "Always request permission" function is selected.
   - If the "Always request permission" function is not selected, the machine operator must permit access.
     If the machine operator presses the "Yes" softkey, access is permitted.



3. If the machine operator presses the "No" softkey, access is denied for the remote user.
   The remote user receives the following message:



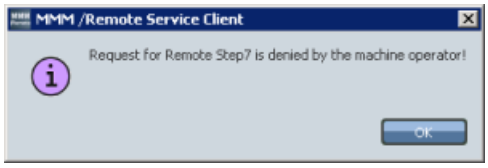
Access rights at the SINUMERIK control system

The following access rights are required at the SINUMERIK control system to start Remote STEP 7:

- Access level 1 = machine manufacturer (password)
- Access level 2 = service (password)
- Access level 3 = user (password)

Inadequate access rights

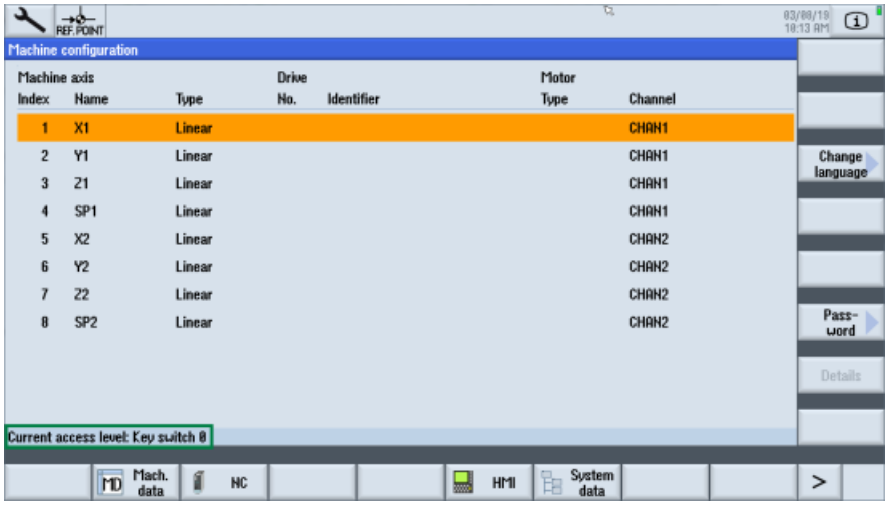
The message is also displayed if the access rights are inadequate:



Inadequate access rights are:

- Access level 4 = keyswitch 3
- Access level 5 = keyswitch 2
- Access level 6 = keyswitch 1
- Access level 7 = keyswitch 0

The current access level is displayed in the lower section of the window.



Closing Remote STEP 7

1. Check that no operations are active in the SIMATIC Manager.
2. Click the "RS7" icon again to end the remote access.
3. Confirm the prompt with "Yes" if you really want to terminate the function.

8.9.2 Setting up a connection with the TIA Portal via the Internet

Using the "Remote STEP 7" function, as a remote user, you can execute all of the functions in SIMATIC Manager.

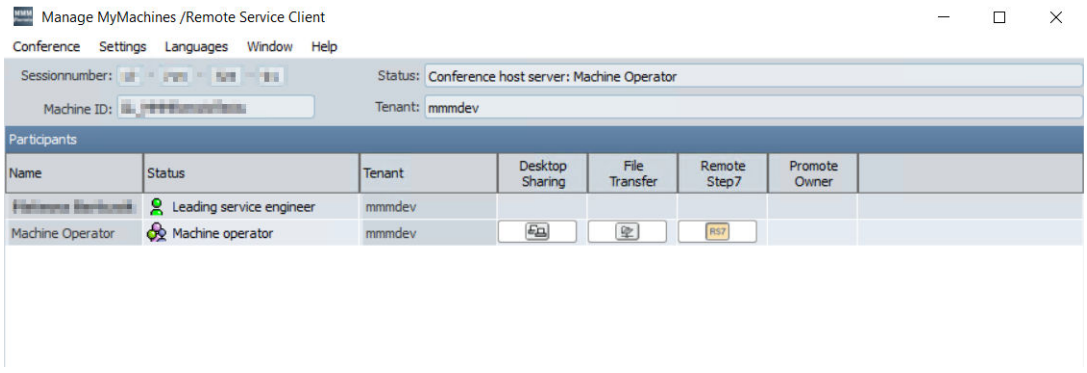
Prerequisites

- The TIA Portal must be installed on the local PC.
  Versions 15.0, 15.1, 16.0, 16.1, and 17 are supported.
- If PLCs use the "Remote STEP 7" function with the TIA Portal, then OMS+ must be activated.

- The Service Engineer Client must be installed on the local PC.
- The client on the machine operator side must support "Remote STEP 7".
- The device must be registered and online in the network.
- The remote session must have been set up.

Start Remote STEP 7 on the SINUMERIK control system

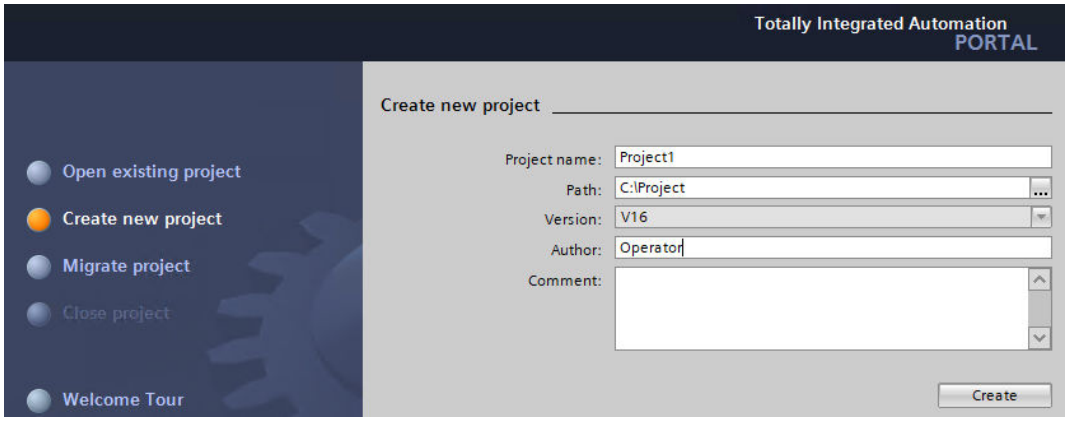
1. To activate function "Remote STEP 7" click on the icon RS7.



2. Wait for the machine operator's response. The machine operator must issue permission for the remote access.
   Remote STEP 7 access is activated.

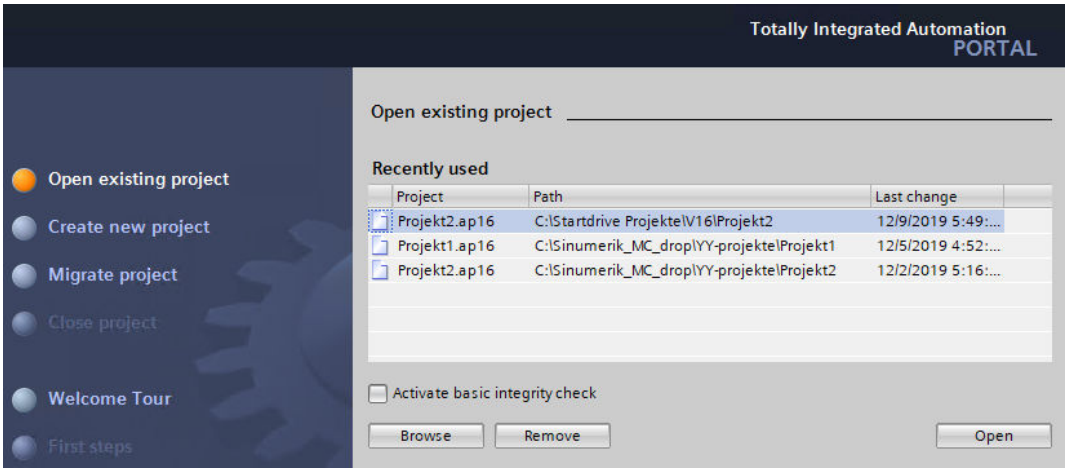
Connecting the device with the TIA Portal

1. Start the TIA Portal.
   The TIA Portal opens and the portal view is displayed. You can now create a new project or open an existing project.
2. To create a new project, in the portal view click on entry "Create new project". Enter the basic project data at the right in the work cell.



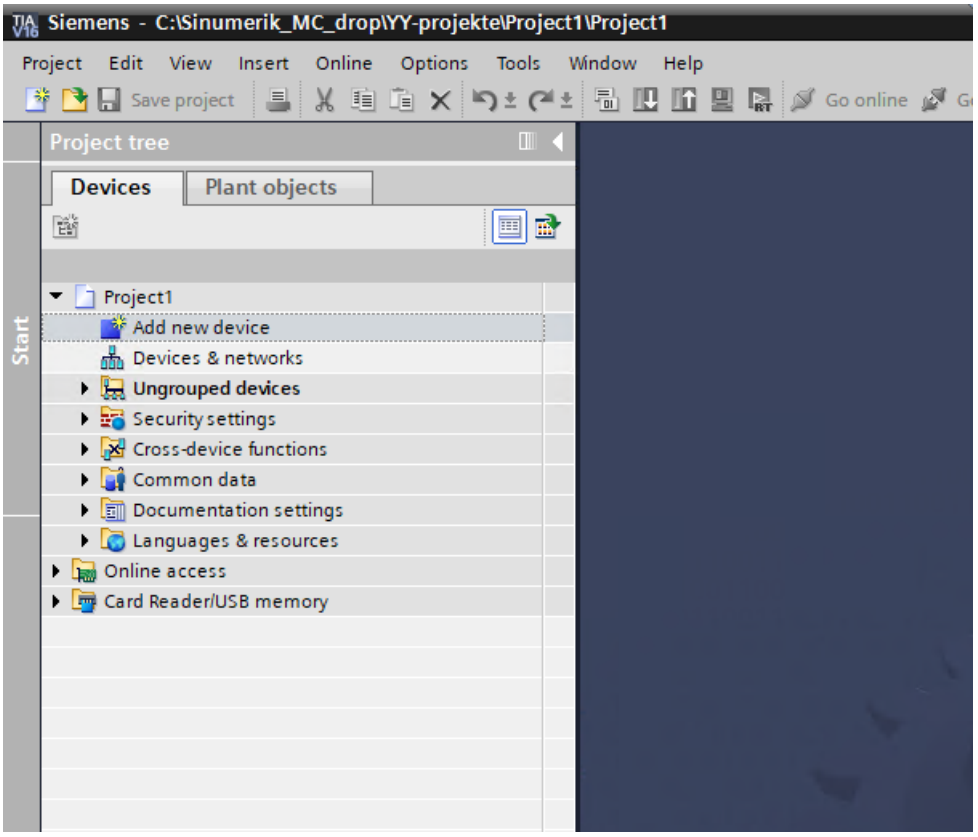
- OR -

3. To open an existing project, click on entry "Open existing project" in the portal view.



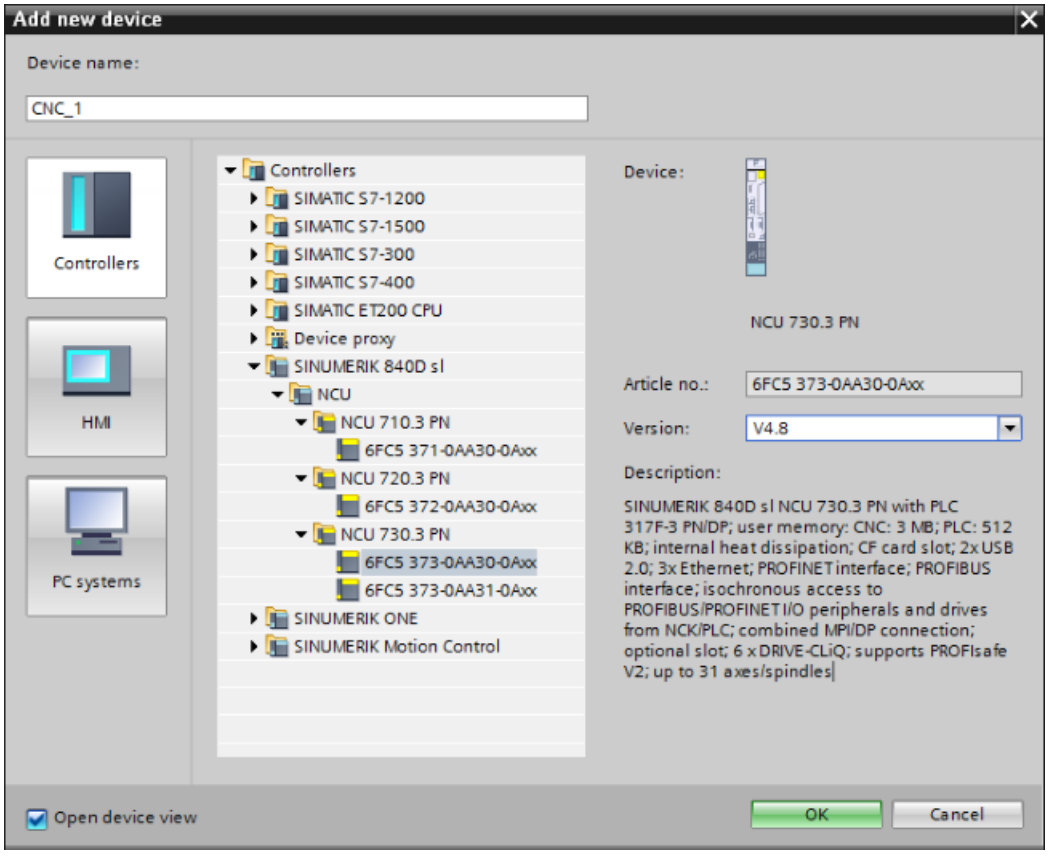
The last project used is displayed to the right in the work cell.
Here, select a project and click on "Open". Alternatively, using "Browse", you can open the directory structure of the PC, from where you can select a project.

4. In the TIA Portal, switch from the portal view to the project view.



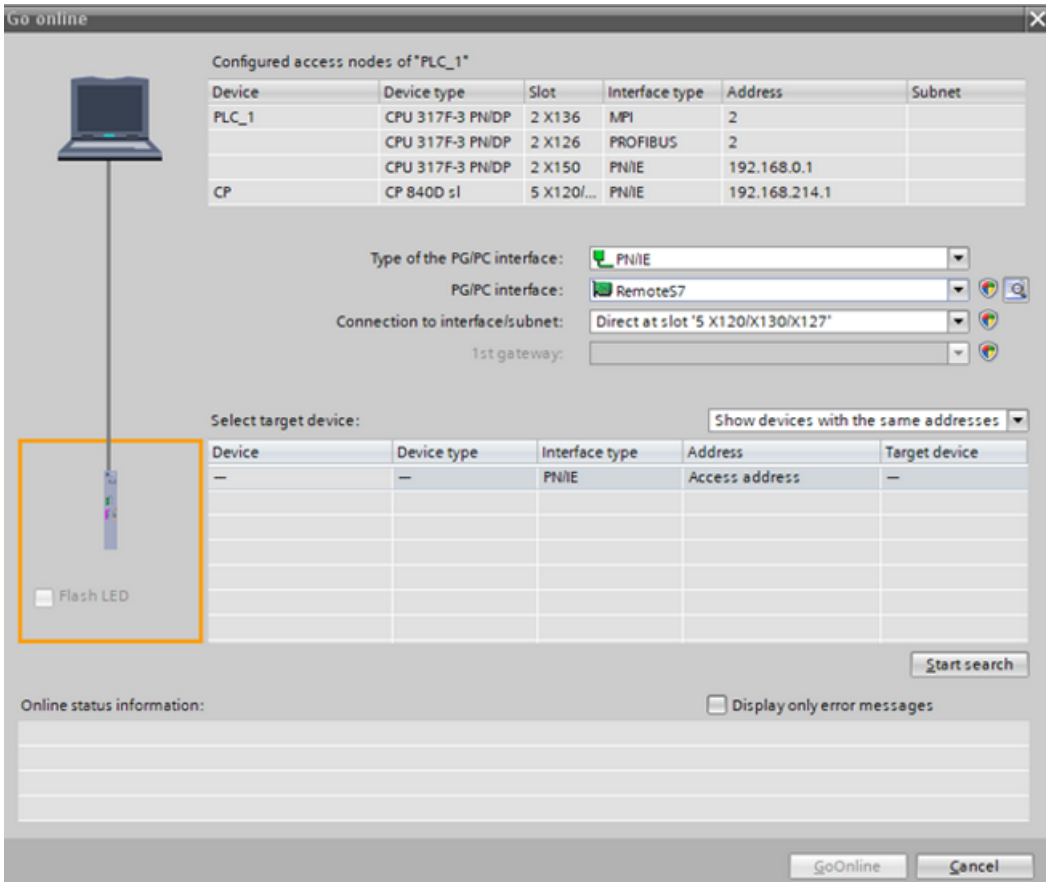
5. Double-click on entry "Add new device" in the project navigation.
A dialog with the same name opens.

6. Click the "Controller" button.



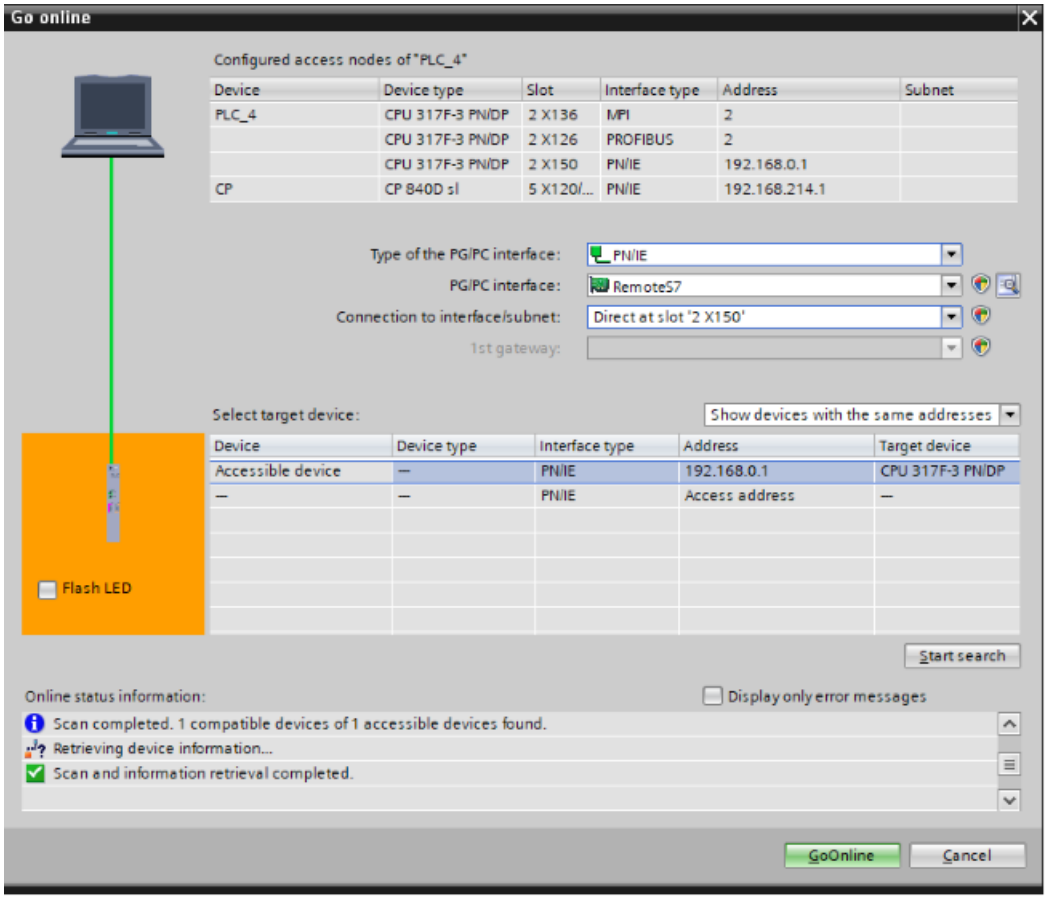
7. In the folder structure under "Controller", expand the corresponding SINUMERIK device family and then select the required device and confirm your selection with "OK".
The selected device is created in the project navigation.

8. Select the device in the project navigation and call menu path "Go online / Extended online". The "Go online" dialog opens.



9. Here, make the following connection settings:
   - Select "PN/IE" in the "PG/PC interface type" field.
   - Select the entry "RemoteS7" in the "PG/PC interface" field.
   - Select the entry "Direct at slot '2 X150'" in the "Connection to interface/subnet" field.
10. In the "Select target device" field, select option "Show devices with the same addresses".

11. In the dialog, click on "Start search".
    The search starts. The results are listed in the results list once the search has been completed.



12. Select the device you require from the list, and click on "Go online".
    If your device was successfully connected with your PC, then this is displayed in the status information using this icon ✅.
    The project work cell is marked using an orange bar on the right-hand side.

Disconnecting the device from the TIA Portal

Click in the icon bar of the TIA Portal on icon "Disconnect online connection".

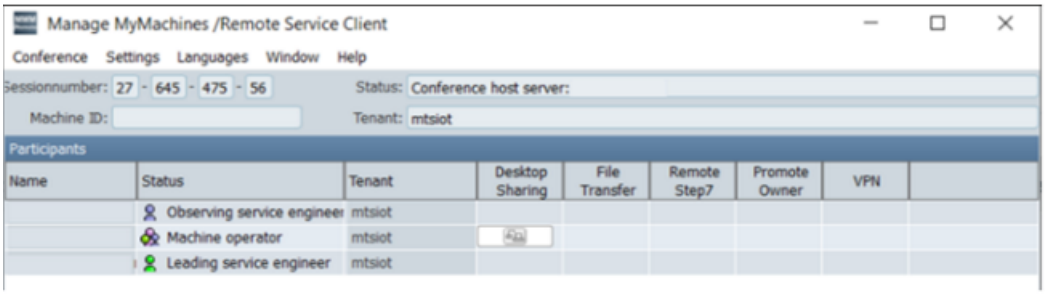
The connection is disconnected.

8.10 Transferring the conference leadership

As conference owner, you can transfer the conference leadership to another, observing service engineer. The owner role therefore switches to another operator.

Precondition

- The remote session must be set up.
  More information can be found at: Download remote service client (Page 94)
- At least one head service engineer and a monitoring service engineer must actively participate in a session.

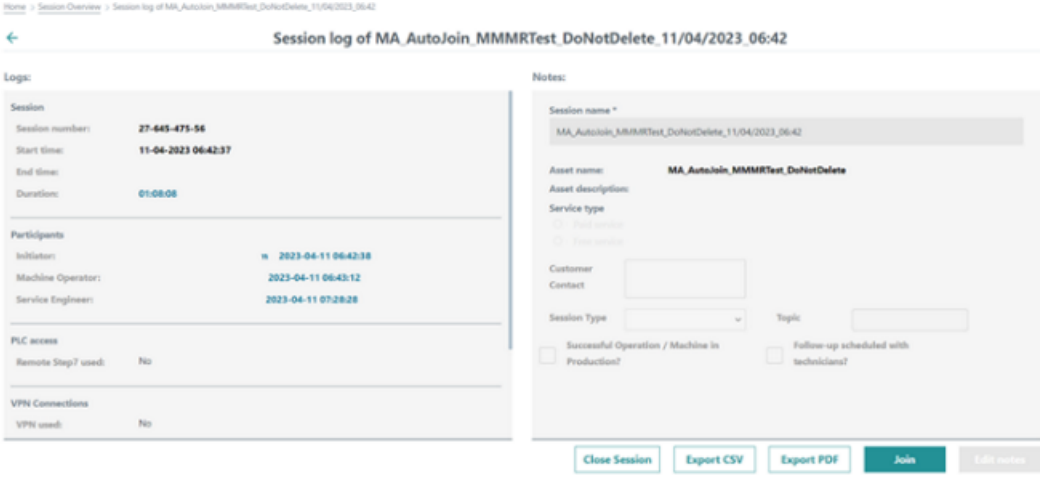


Procedure

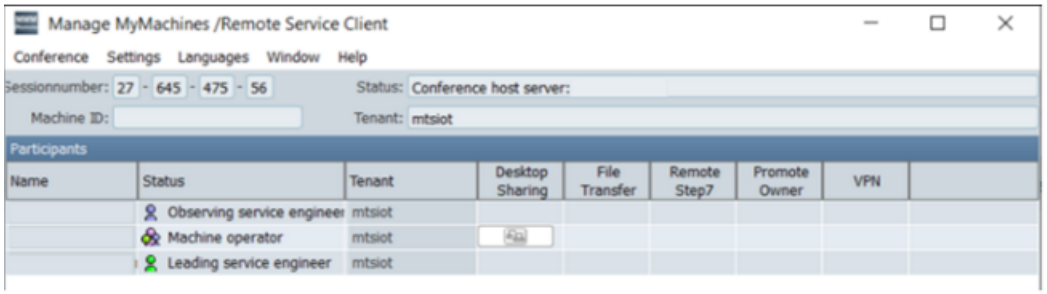
1. Log into MDSP in the presence of the monitoring service engineer.
   Open the session log of the active session.



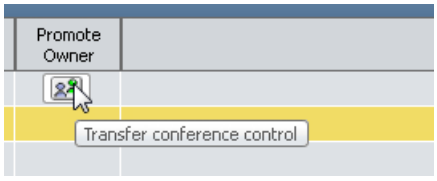
2. The monitoring service engineer clicks the "Join" button to join the active session.
   In the session log, the monitoring service engineer appears in the left window area as "Service Engineer".



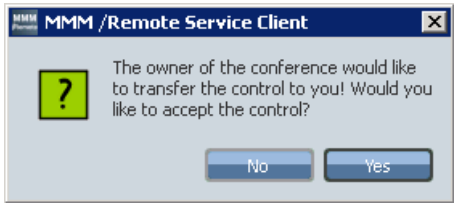
3. After starting MMM /R SC SE, the name of the monitoring service engineer appears in the "Status" field.



4. As conference head, click on icon "Transfer conference control" in the line of the service engineer to whom you want to transfer conference leadership.



The message that the system is waiting for confirmation by the future conference owner is displayed on your PC.
The following query appears on the PC of the selected service engineer:



5. The observing service engineer must click the "Yes" button to take over the conference leadership.

Note

If the observing service engineer rejects the transfer of leadership with the "No" button, an appropriate message appears on the PC.

6. If the "Always request permission" function is not active, the machine operator must confirm the transfer of leadership.
The message "Waiting for confirmation from the machine operator!" appears on your PC and on the PC of the next conference leader.
7. The machine operator agrees to the transfer of leadership.
The conference leadership is then transferred to the desired observing service engineer. The changed user roles are updated accordingly in the list of participants.

Note

Rejecting the transfer

If the machine operator rejects the transfer, you and the observing service engineer receive the following message: "The transfer of leadership has been rejected by the machine operator!"

8.11 Terminating the remote session

For the various participants, a session is terminated in various ways

- The service engineer terminates the session:
  - The machine operator at the control system sees the following message: "Session ended".
  - The other participants see the following message: "The session has been terminated by the owner"
- An observing participant terminates the session:
  - The window is closed, however the session remains active.
  - The observing participant can join the active session again at any time.
- The machine operator at the control system exits the session:
  - The session remains active for all of the other participants.
  - The remote access function is deactivated.

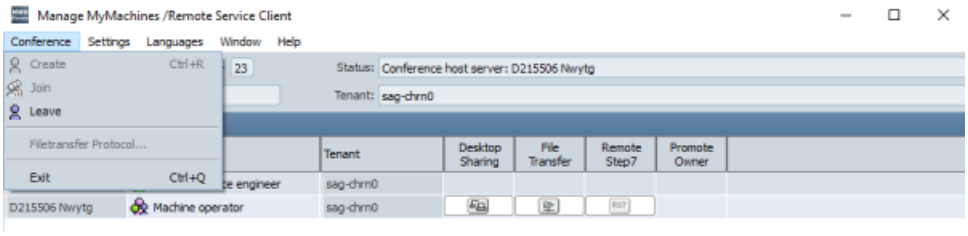
Note

Closing a session

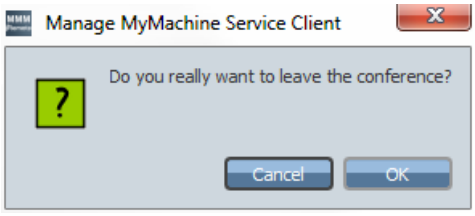
Only a service engineer at the PC can close a session.

Procedure

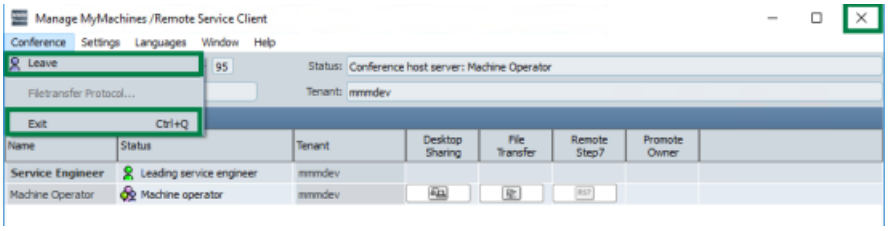
1. Select the "Conference" > "Exit" menu.



2. If actions of the service engineer are still active when you leave the session, relevant messages are displayed.
3. Click on "Yes" to exit the session.
   The functions or applications in progress are cancelled.
   - OR -
   Click "No" if you do not yet want to exit the remote session.



   - OR -
   In the "Conference" menu, select the "Exit" function to terminate the conference.
   In the upper right-hand section of the window, click on the "X" to close the window.



Note

Exiting the remote access session

It is recommended to end the session using the second option "Conference -> Exit".

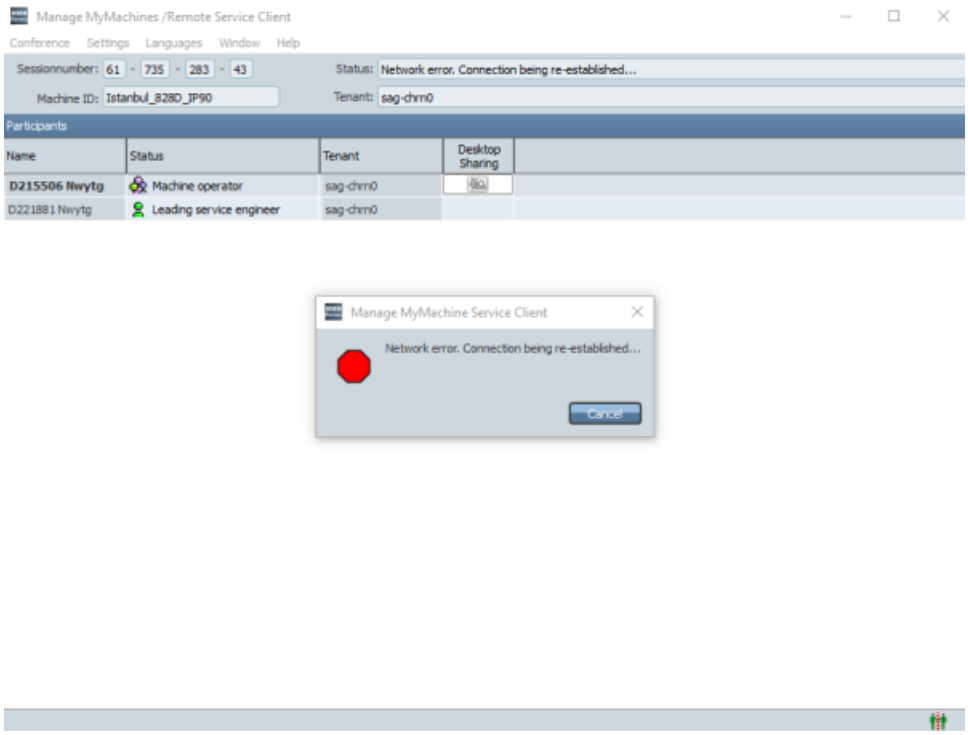
8.12 Additional functions

8.12.1 Network interruption

The following error message is displayed if the network is interrupted during an active session.

All internally active functions are terminated and "Manage MyMachines /Remote Service Client" cyclically attempts to participate in the session again.

Click the "Cancel" button to terminate the connection process.



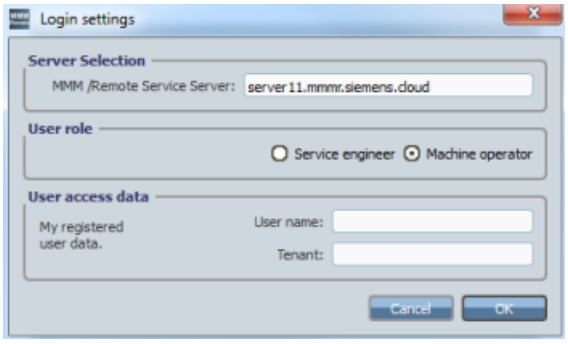
8.12.2 Setting the login data

You can save your login data. Your data is then automatically set when logging in.

Settings	Description
Server selection	
MMM /Remote Service Server	Address of the Manage MyMachines /Remote Server
User role	
Service engineer	Activate the appropriate role.
Machine operator	
Login data - my registered user data.	
User name	Enter the registered Insights Hub user data to log in
Tenant	

Procedure

1. Call "Settings" > "Login..." in the menu bar.
   The "Login settings" window opens.
2. Enter the necessary data.
   Click "OK" to save the settings.
   - OR -
   Click "Cancel" to reject the settings.



8.12.3 Setting file transfer

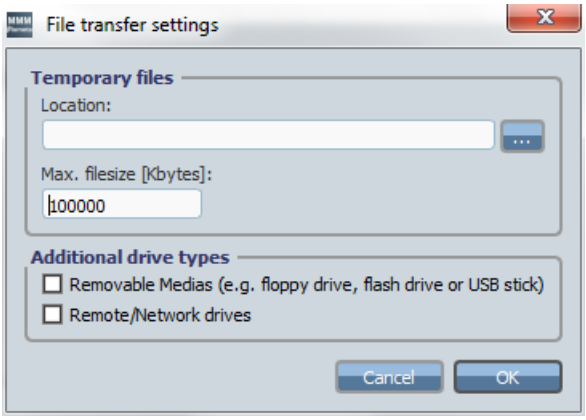
You can log the actions in a file during a remote session. You specify the settings of the log file in the "File Transfer Settings" window.

Settings	Description
Temporary files	
Location:	Specify the log directory or create a new directory in which the log files will be stored. The directory selection is made in the "Find directory" window.
Max. filesize [Kbytes]:	Defining the maximum number of log files. If "0" is entered, no log files are written. When the maximum number of files is reached, the oldest log file is deleted.
Additional drive types	
Removable drives	The machine operator specifies which drive types the service engineer may access. If no drive type is selected, the service engineer may only access the available hard drives.
Remote/network drives	

Procedure

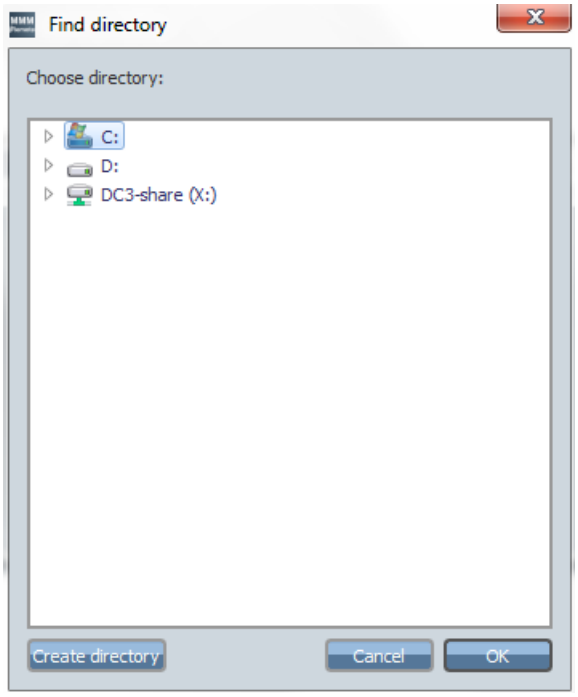
1. In the menu bar, call "Settings" > "File transfer...".
   Window "File transfer settings" opens.
2. A standard directory is specified for the logs.
   If you want to use another directory as the log directory, you can specify that here. Additional information at: "Find directory / Create new directory".
3. Specify the maximum number of log files that can be saved in the log directory.

4. Then define which drive types are supported for the file transfer.
   Select the corresponding check box for each drive type that is to be supported.
5. Click "OK" to save the settings.
   - OR -
   Click "Cancel" to reject the settings.



Find directory / Create new directory

1. Click "..." behind "Location:" if you want to set a different directory than that specified.
   The "Find Directory" window opens.
2. Select the required directory in the directory tree.
   - OR -
   Click "Create new directory" to create a new directory.
3. Click "OK" to specify the directory.



8.12.4 Setting the language

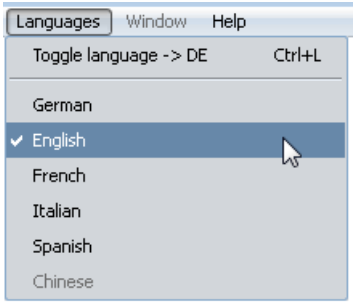
You can make the following language setting:

- Set the language you want the display to appear in
- Define 2 favorites to speed up setting the language.
- Use language toggling.

Changing the language in the "Languages" menu

You can change the currently displayed language on two ways.

1. Open the "Languages" menu.
   All the available languages are displayed. The current language has a check mark.
2. Select the required language.
   The user interface is changed and displays the texts in the corresponding language.



Toggling the language

You must have first defined 2 favorite languages if you wish to quickly set the language.

1. Call "Settings" > "Language..." in the menu bar.
2. The "Toggle language" window opens.
   Select the favorite languages.

3. Click "OK" to save the selection.
   - OR -
   Click "Cancel" to reject the selection.



4. Enter the key combination <Ctrl> and <L>.
   The language changes.

8.12.5 Setting the log file

A log file is frequently required for diagnostic purposes.

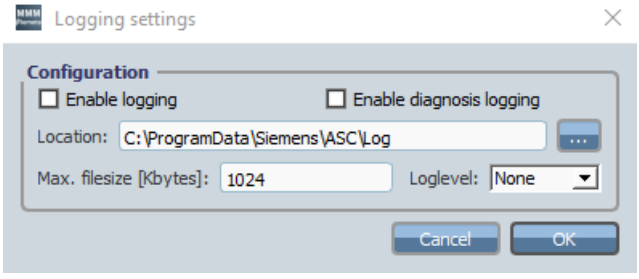
You can activate the creation of a log file and make further settings.

Parameter

Setting		Description
Configuration		
Enable logging		Switches the log functionality on/off.
Enable diagnosis logging		Performs the logging with an increased log level and a greater maximum file size. More data is therefore available for diagnostic purposes. In this mode, no maximum file size and no log level must be specified. These values are specified by "Manage MyMachines /Remote".
Location:		Defines or creates a directory in which the log files are stored. The directory is created in the "Find Directory" window.
Max. filesize [Kbytes]		Specification of the maximum file size in KB. "Manage MyMachines /Remote" creates a maximum of 2 log files. As soon as the first file reaches the maximum size, a new log file is created. If an older file already exists, then it is overwritten.
Log level		Specifies whether and which data is to be logged.
	None	Do not log any data.
	Fatal	Critical errors that prevent further program execution.
	Error	Simpler errors that occur during the program execution, but that do not prevent further execution.
	Warning	Warnings that indicate problems.
	Info	Information that indicates irregularities in the execution.
	DebugN	Logging of the program execution. "N" specifies the level of detail.

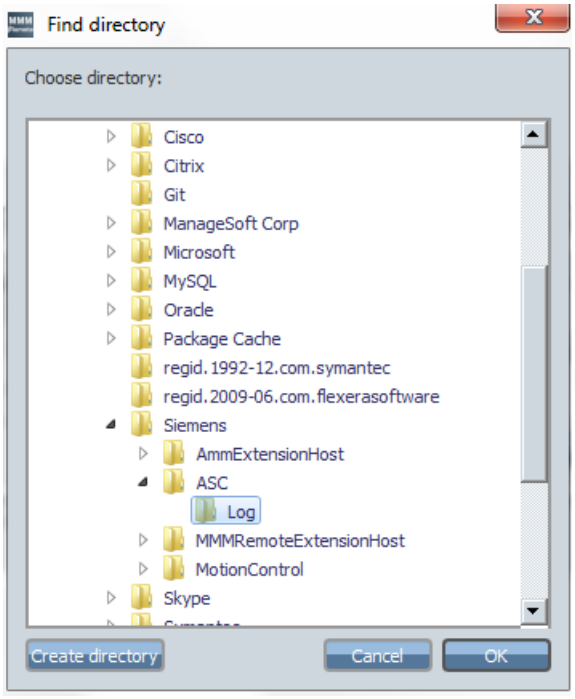
Procedure

1. In the menu bar, call "Settings" > "Logging ...".
   Window "Logging settings" opens.
2. Activate option box "Enable logging".
   This activates creating a log file. You create log files with the default settings displayed in the dialog. If required, you make fine settings for the logging.
3. A standard directory is specified for the log files.
   If you want to use another directory as the log file directory, specify that directory; you will find more information under: "Find/create directory"
4. Activate option checkbox "Activate diagnostics logging" if you wish to have an extended log file.
   However, you can then no longer manually define the maximum file size and the log level.
5. Click "OK" to save the settings.
   - OR -
   Click "Cancel" to reject the settings.



Search/create directory

1. Click "..." behind "Location:" if you want to set a different directory than that specified.
   The "Find Directory" window opens.
2. Select the required directory in the directory tree.
   - OR -
   Click "Create new directory" to create a new directory.
3. Click "OK" to specify the directory.



Disconnecting a SINUMERIK control from Insights Hub

9

9.1 Overview

Introduction

If you no longer wish to use the Manage MyMachines for Industrial Operations X Cloud on your SINUMERIK control, proceed as follows:

1. Lock SINUMERIK Integrate: Deactivating use of SINUMERIK Integrate (Page 207)
2. In the "Shopfloor Management App", disconnect the machine tool system from Insights Hub: Disconnecting a SINUMERIK control from Insights Hub (Page 205)

9.2 Disconnecting a SINUMERIK control from Insights Hub

Disconnect SINUMERIK controls or other controls from Insights Hub using the Manage MyMachines for Industrial Operations X Cloud "Shopfloor Management App".

More information about roles within Insights Hub and on configuring assets is provided in: Documentation Insights Hub (https://siemens.mindsphere https://documentation.mindsphere.io/MindSphere/index.htmlhttps://documentation.mindsphere.io/MindSphere/index.html.io/en/docs/mindaccess.html)

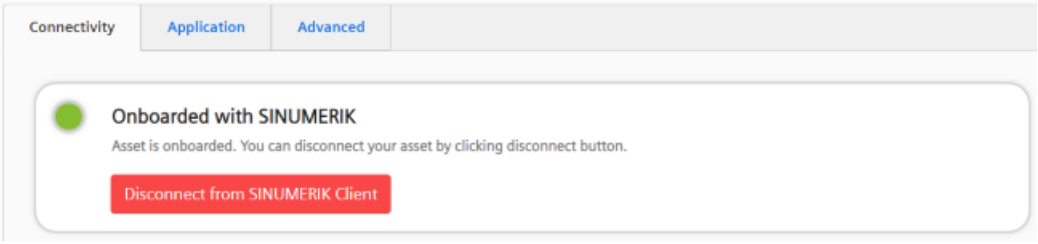
Precondition

In Insights Hub, you require the role "shopfloormgmtapp" as standard user or administrator.

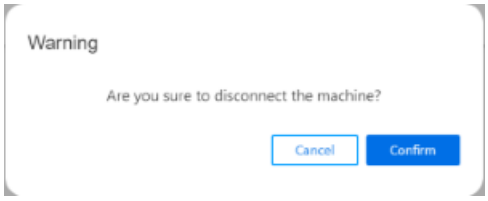
Procedure

1. In the launch pad, open the Manage MyMachines for Industrial Operations X Cloud "Shopfloor Management App".
2. Select the required asset in the left-hand side of the window.
3. Open the "Connectivity" tab in the right-hand section of the window.

4. Under the "Connectivity" tab, you can see the connection status, e.g. "Onboarded with SINUMERIK".
   – Click the "Disconnect from SINUMERIK client" button to disconnect the asset from Insights Hub.



5. You receive a confirmation prompt: "Are you sure to disconnect the machine?".
   – Click on the "Confirm" button to disconnect the connection.
   -OR -
   – Click "Cancel" to abort the operation.



Note

After Insights Hub and the machine tool have been disconnected, we recommend deleting the following files from your SINUMERIK control:

- All files in the "boot_job" folder
- All files in the "cache" folder
- All files in the "service_job" folder

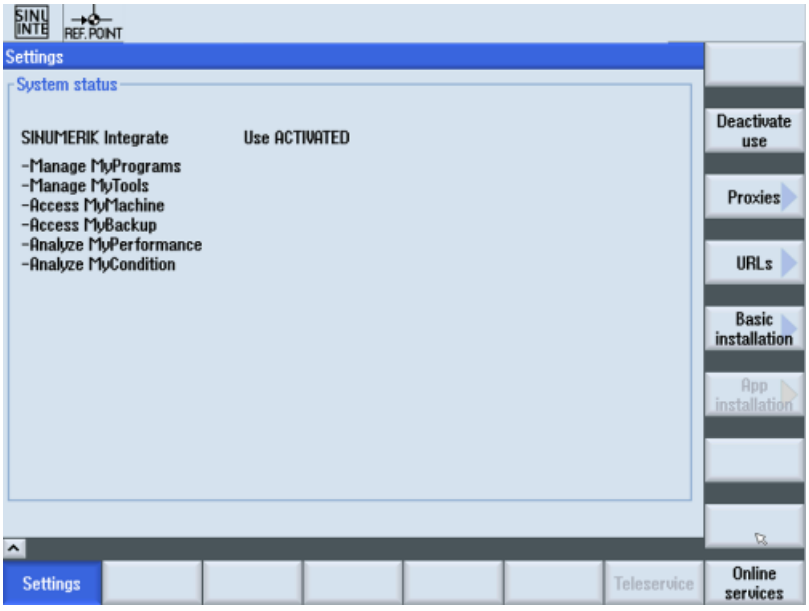
You will find the files:

- If you use PCU/IPC under: C:\temp
- If you use NCU under: /var/tmp

9.3 Deactivating use of SINUMERIK Integrate

Procedure

1. Press the "SINUMERIK Integrate" softkey.
   The "SINUMERIK Integrate" welcome window opens.
2. Press the "Settings" softkey.
   The "Settings" window opens displaying the system status "Use ACTIVATED".
   – Press the "Deactivate use" softkey.



3. You obtain the confirmation prompt "Do you really want to deactivate the use of the SINUMERIK Integrate applications?".
   – Press the "OK" softkey to confirm the prompt.
   The use of SINUMERIK Integrate applications is deactivated.

Troubleshooting when onboarding

10

These troubleshooting instructions help you to find and resolve faults when onboarding. Ensure that all preconditions are satisfied before you start onboarding.

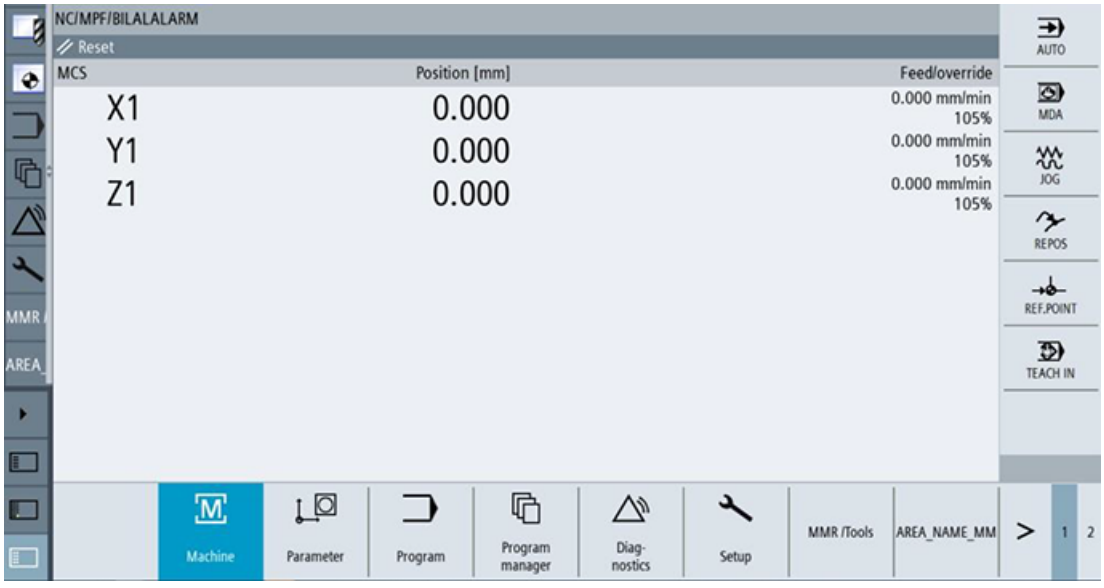
10.1 SINUMERIK controls

10.1.1 Preconditions

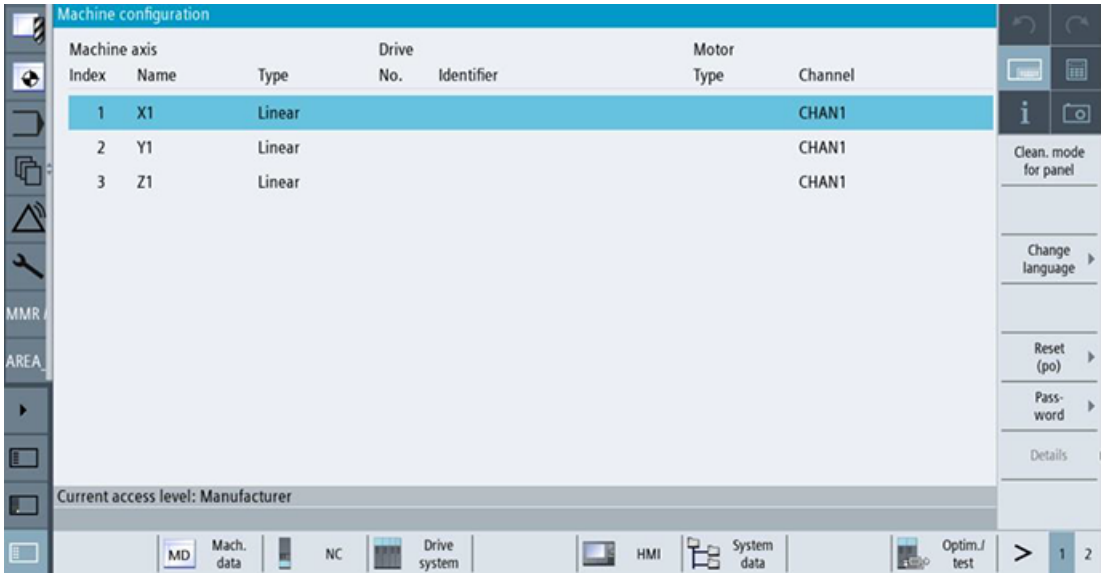
10.1.1.1 Checking the network configuration

Procedure

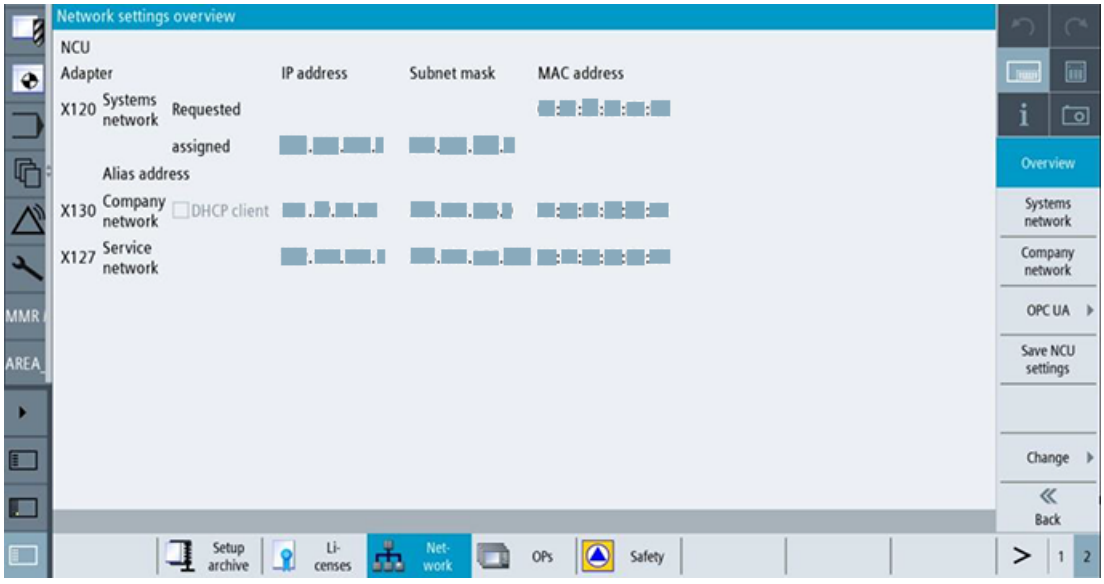
1. Press "F10" on the HMI operator panel.



2. Select "Setup".



3. Select the right-hand arrow.
4. Select "Network".

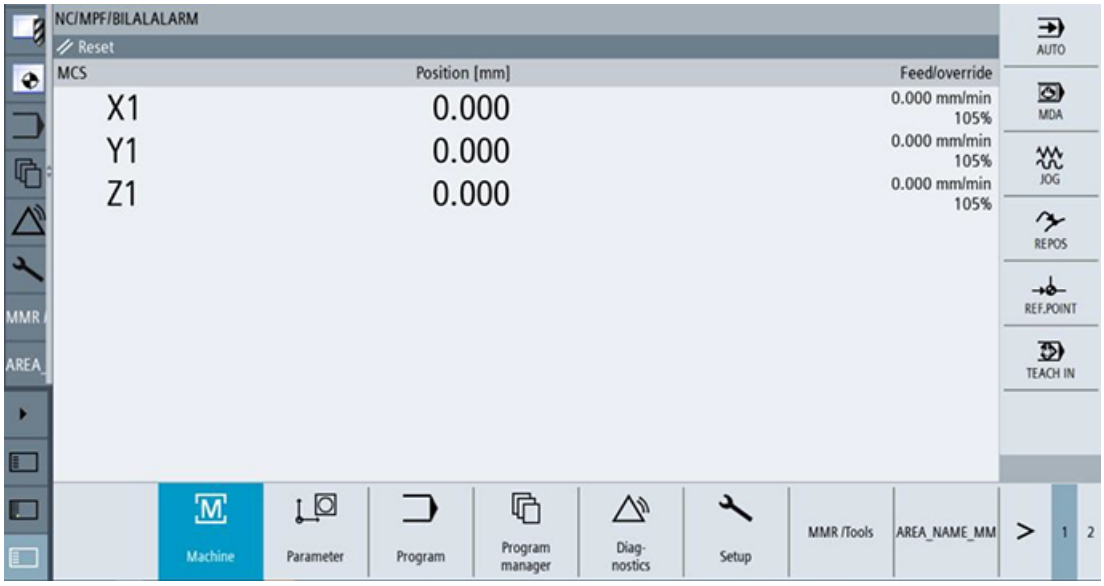


5. Check that the correct IP has been entered for x130.

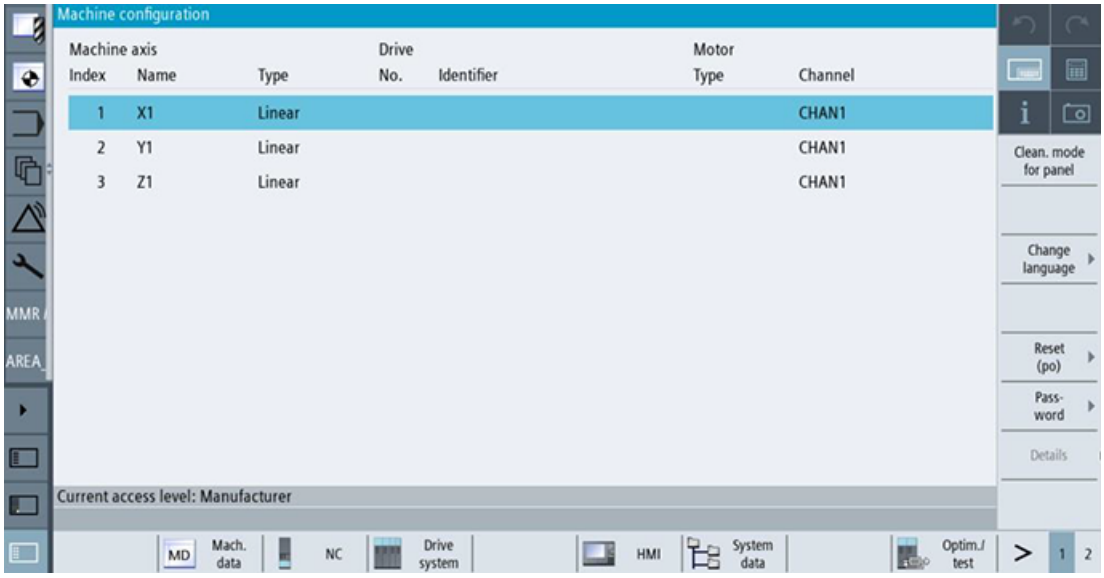
10.1.1.2 Checking that SINUMERIK Integrate has been enabled

Procedure

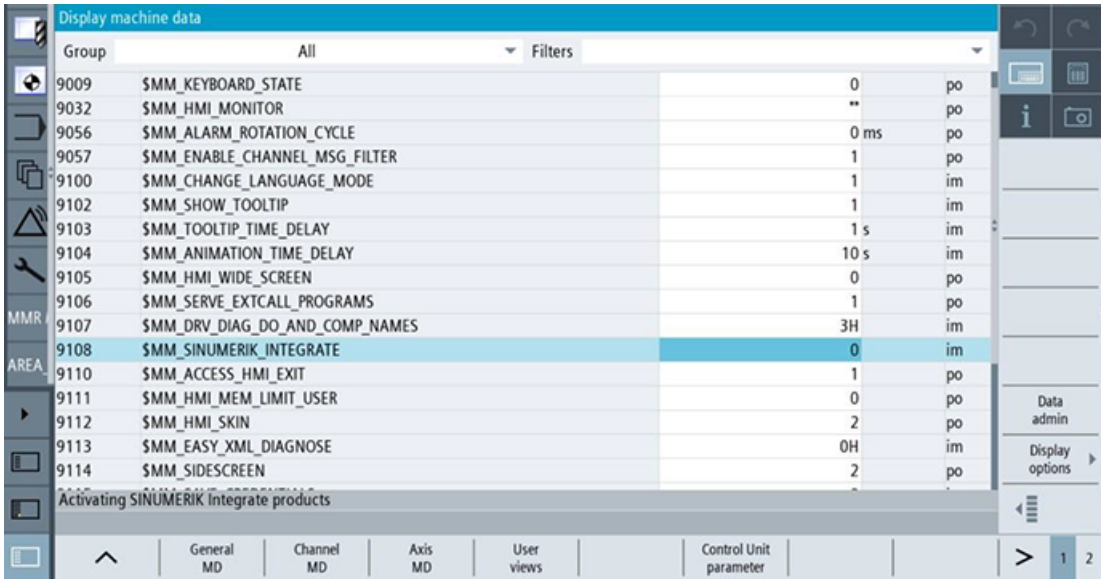
1. Press "F10" on the HMI operator panel.



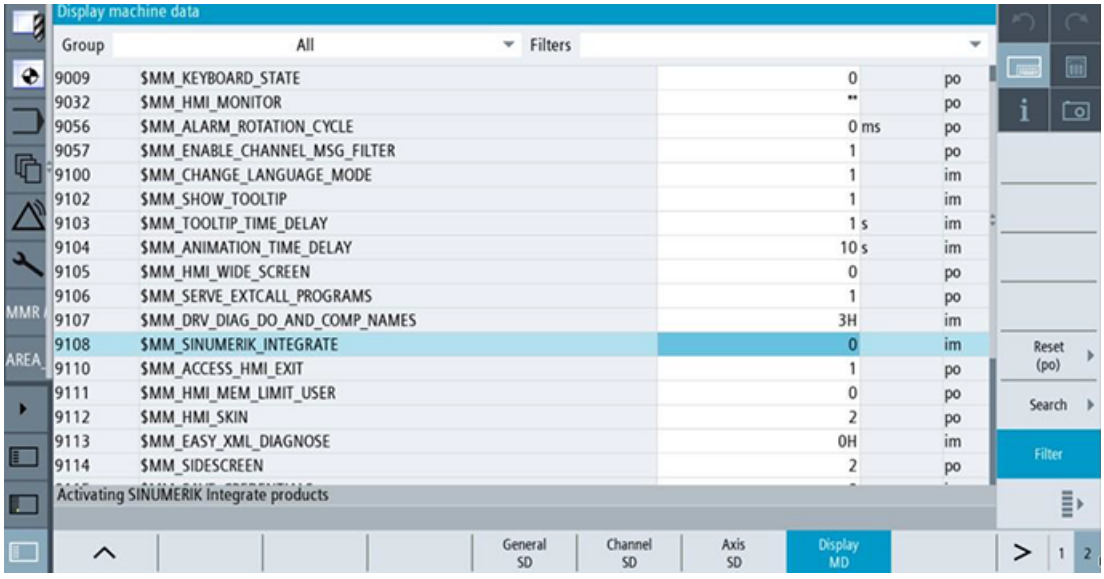
2. Select "Setup".



3. Select "Machine data".



4. Select the right-hand arrow.
5. Select "Display MD".

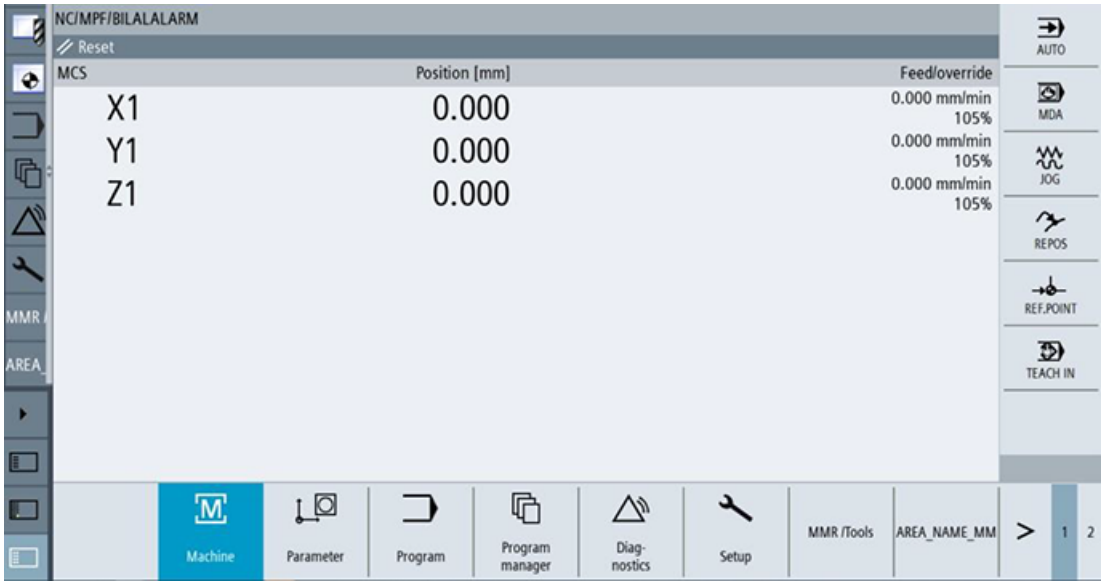


6. Check whether "9108 MM_SINUMERIK_INTEGRATE" is equal to "1".
7. If "9108 MM_SINUMERIK_INTEGRATE" is not equal to "1":
   Then set "9108 MM_SINUMERIK_INTEGRATE" equal to "1".

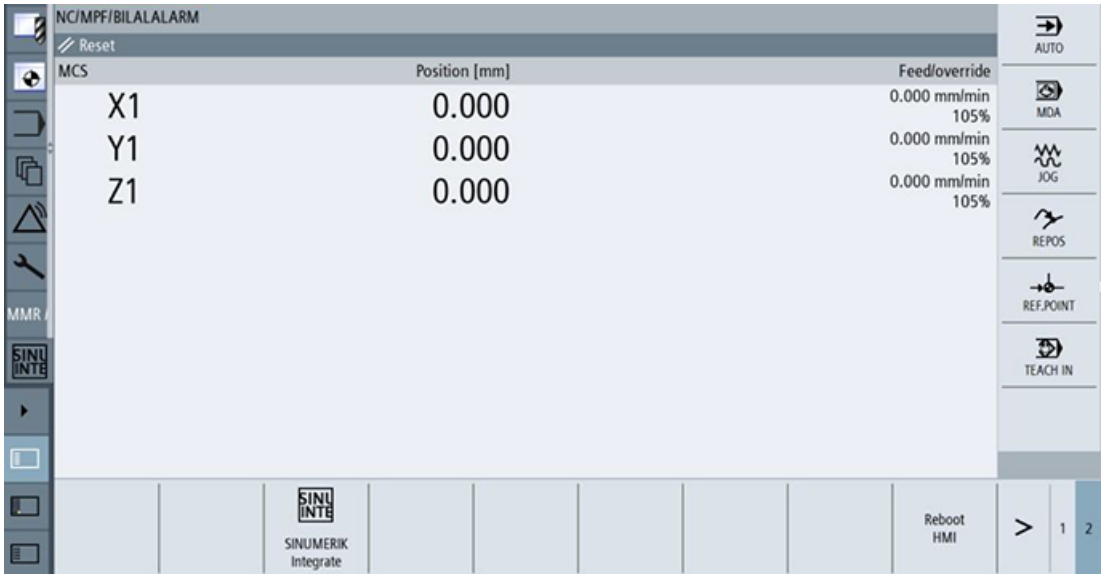
10.1.1.3 Checking that SINUMERIK Integrate has been activated

Procedure

1. Press "F10" on the HMI operator panel.



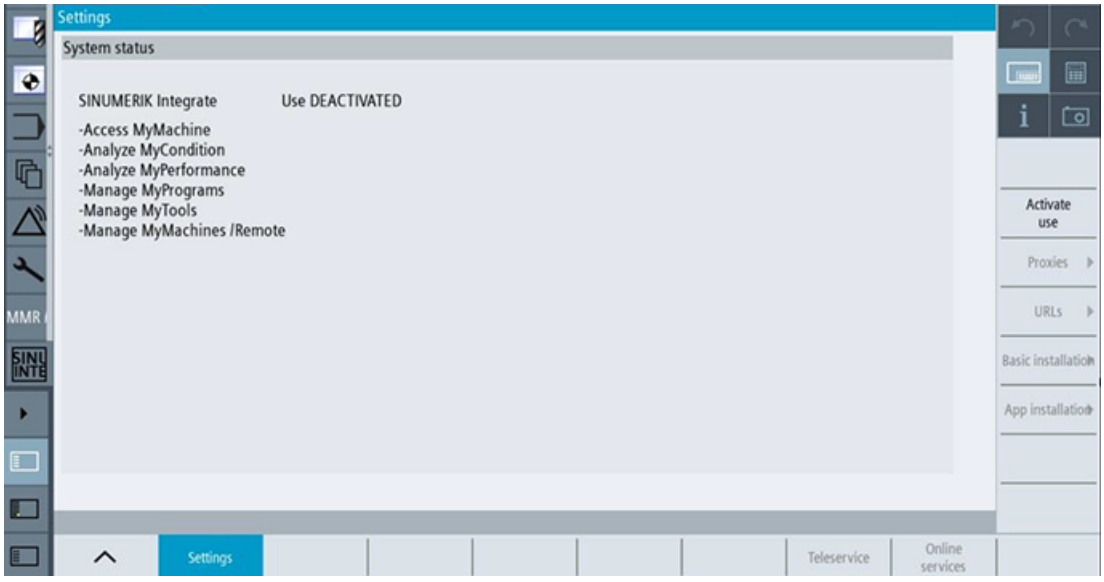
2. Select the right-hand arrow.



3. Select "SINUMERIK Integrate".



4. Select "Settings".



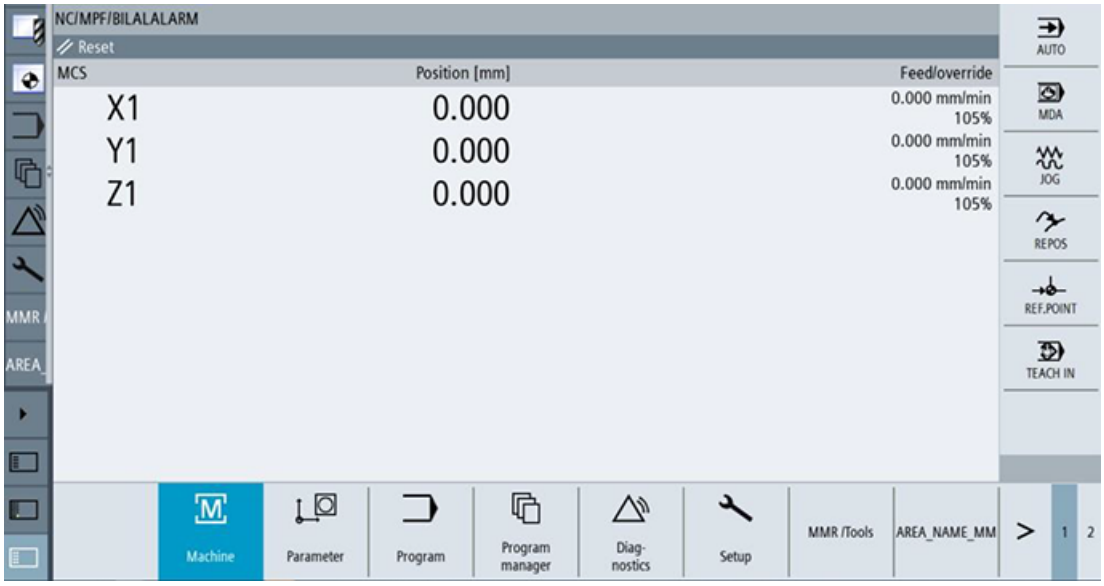
5. Check whether "SINUMERIK Integrate" is enabled.
6. If SINUMERIK Integrate is locked
   - Select "Activate use".
   - Confirm the activation

10.1.1.4 Checking proxy settings

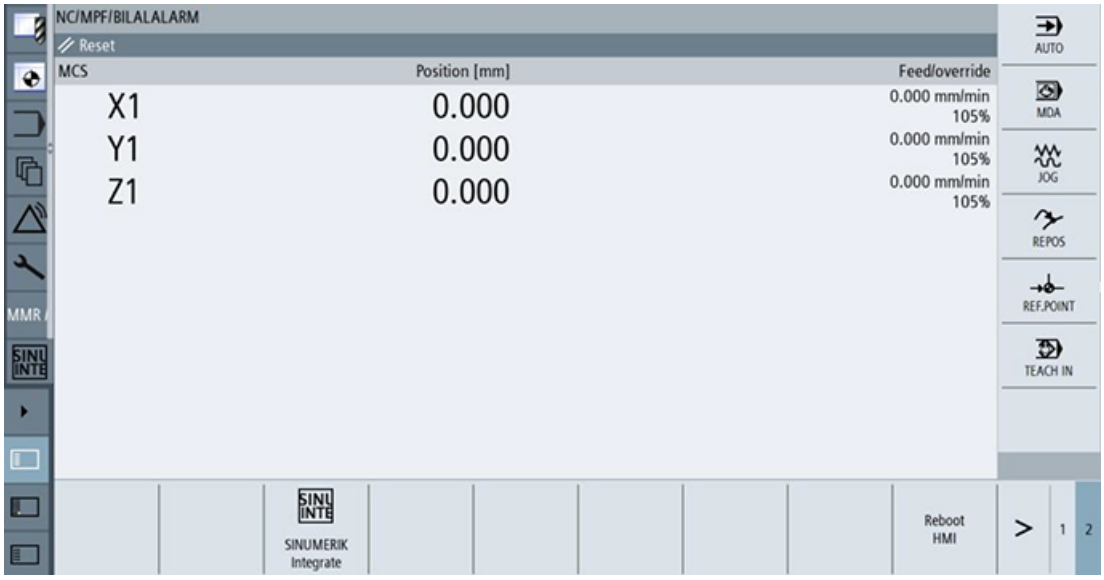
Check that the proxy settings are correct if the machine accesses a network via a proxy.

Procedure

1. Press "F10" on the HMI operator panel.



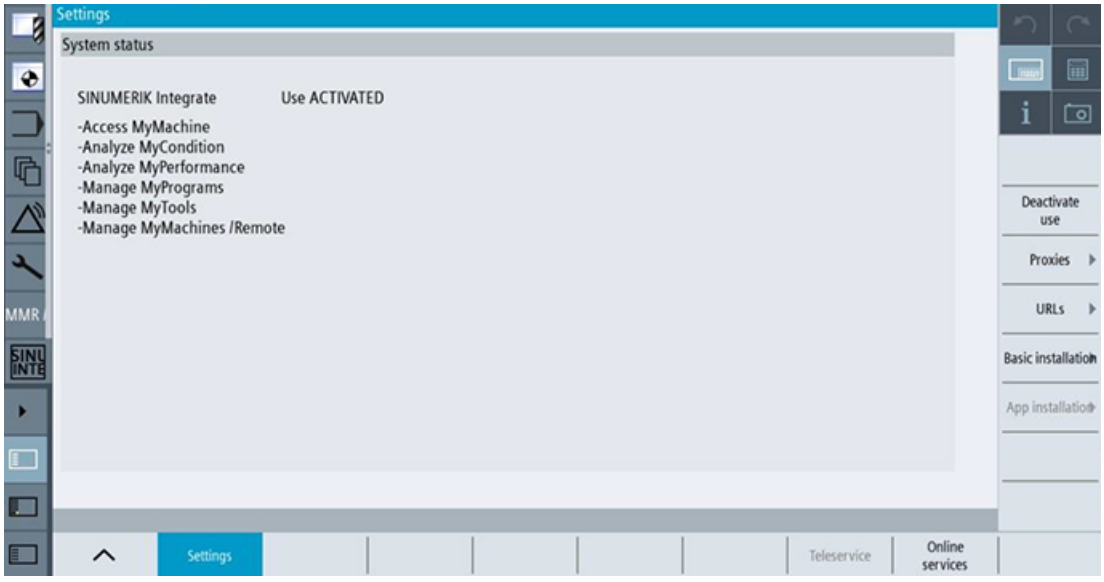
2. Select the right-hand arrow.



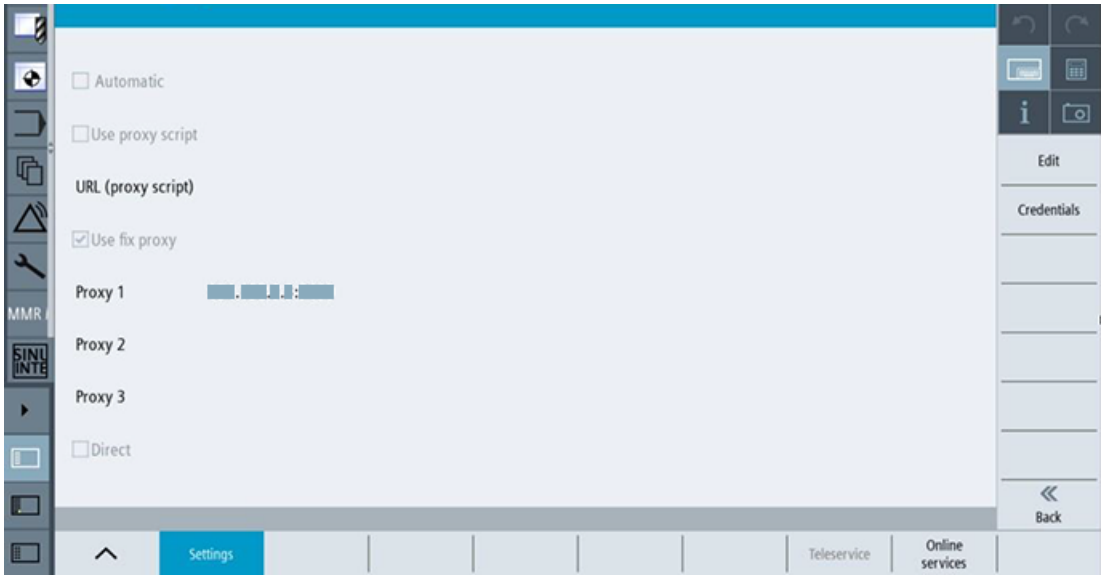
3. Select "SINUMERIK Integrate".



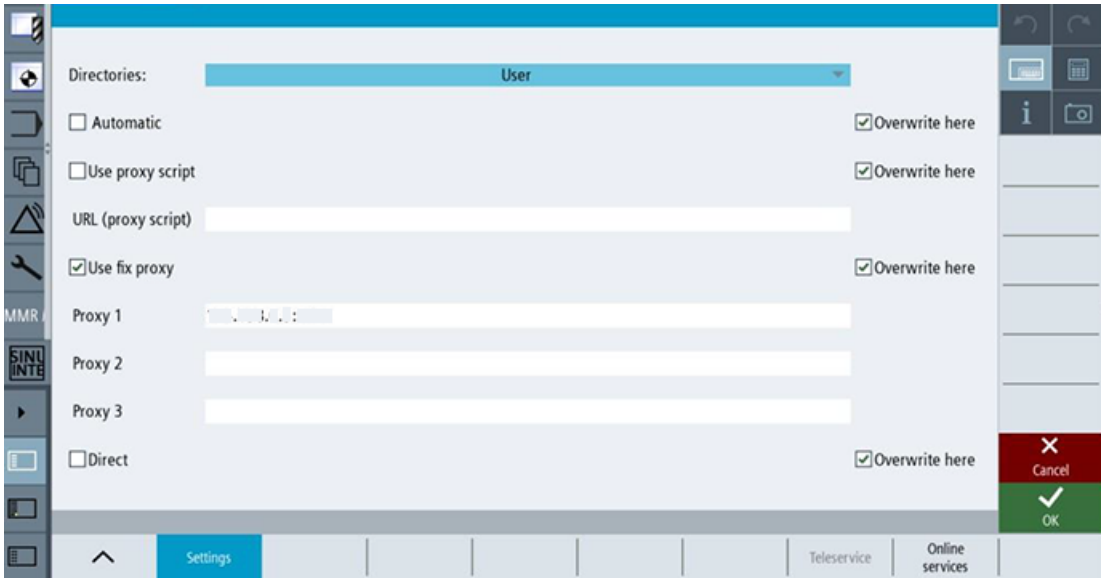
4. Select "Settings".



5. Select "Proxies".



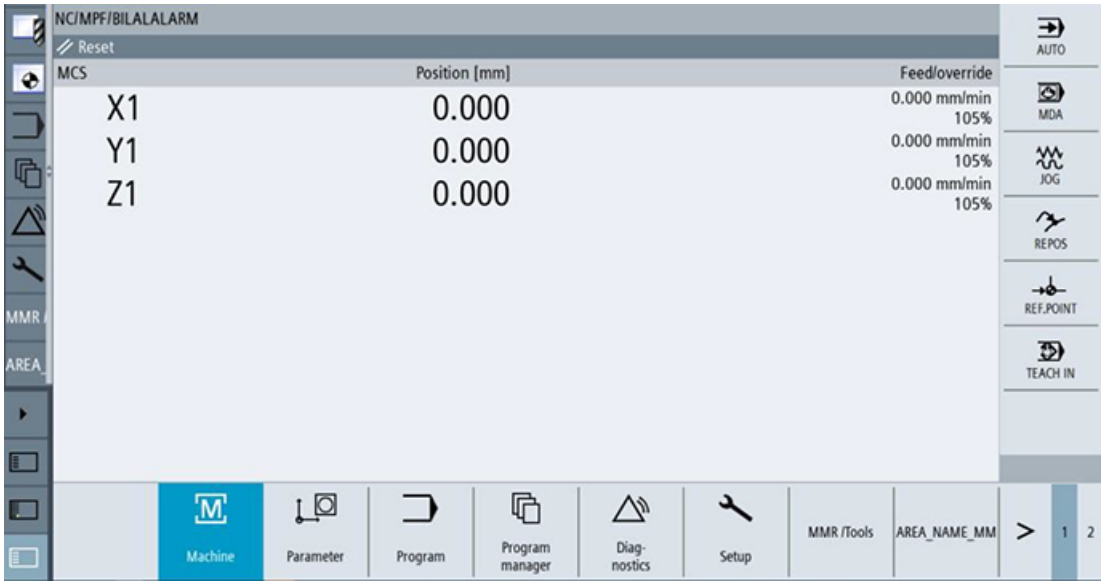
6. Check the proxy information.
7. If the proxy settings are not correct
   - Select "Edit".
   - For the proxy settings, select "Overwrite here"
   - Enter the correct settings
   - Select "OK"
   - Restart the machine.



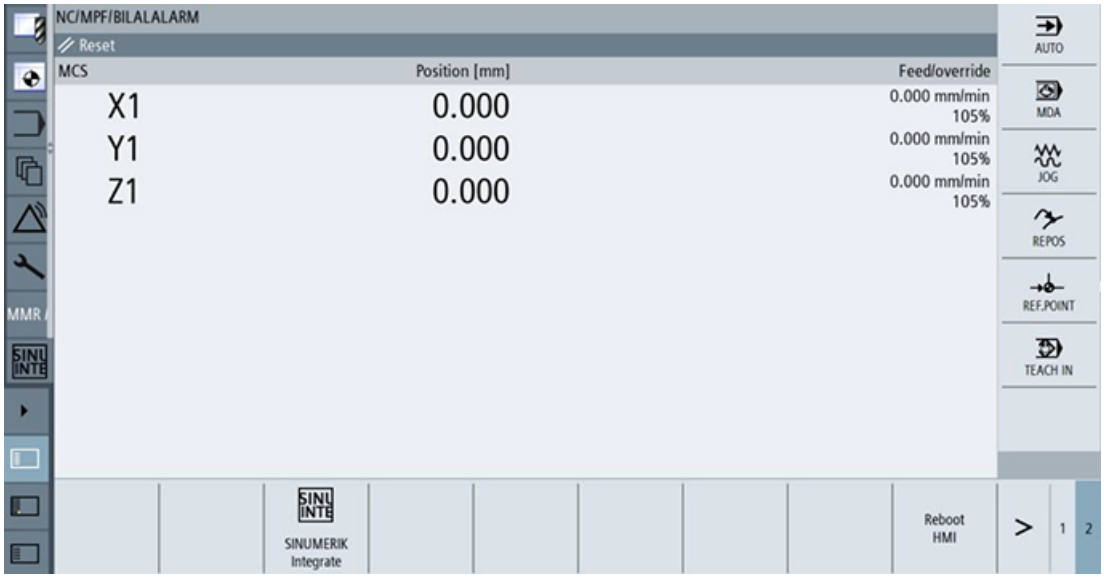
10.1.1.5 Checking the SINUMERIK Integrate URL

Procedure

1. Press "F10" on the HMI operator panel.



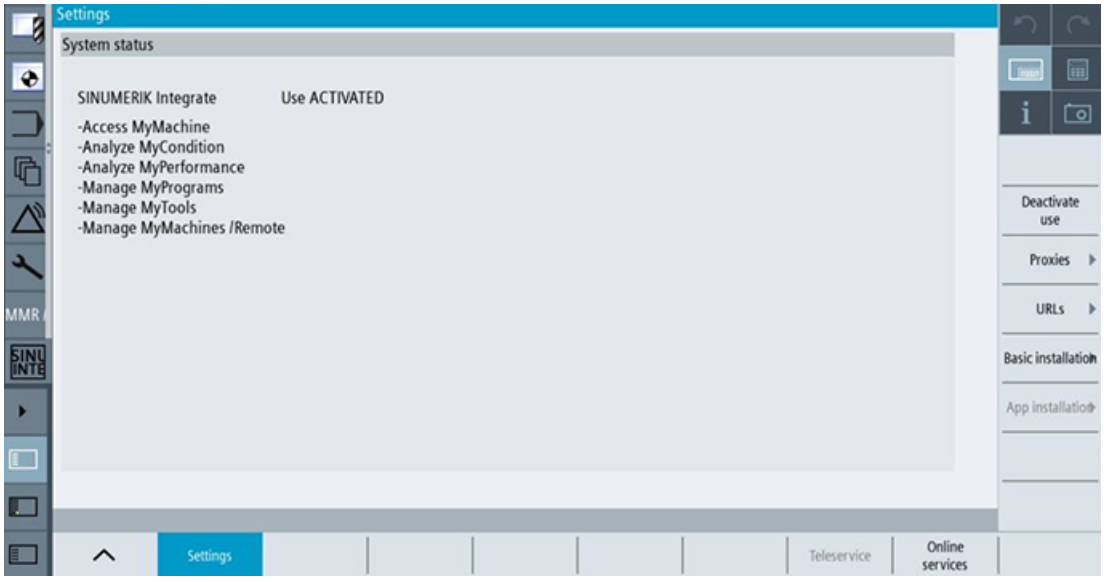
2. Select the right-hand arrow.



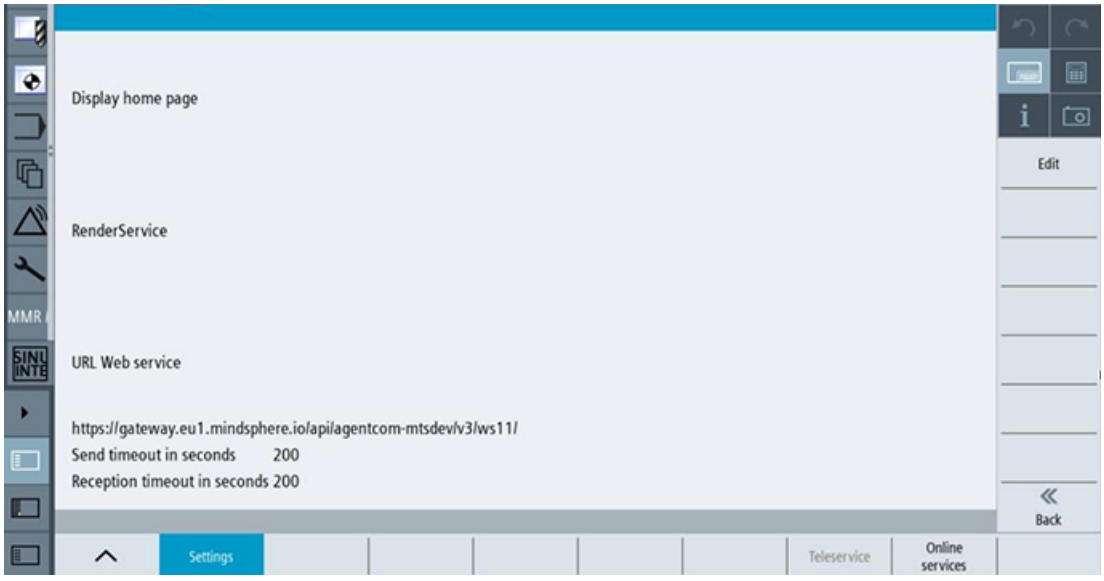
3. Select "SINUMERIK Integrate".



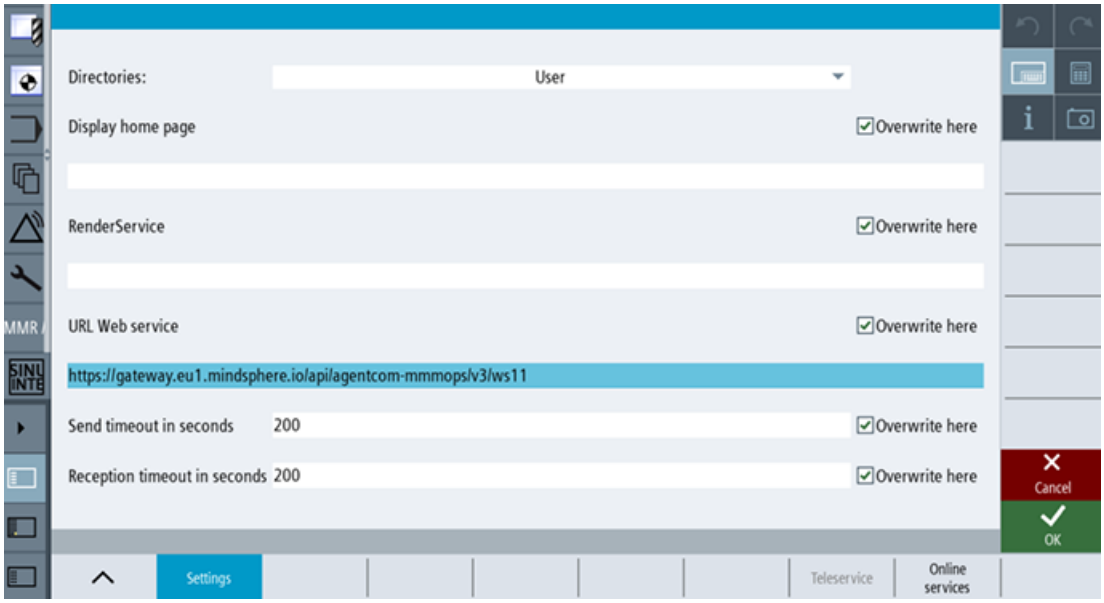
4. Select "Settings".



5. Select "URLs".



6. Check whether the specified URL information is correct.
7. If the URL is not correct
   - Select "Edit".
   - For the web service, select "Overwrite here"
   - Enter the correct URL.
   - Select "OK".
   - Perform an "sc reboot".



10.1.1.6 Checking the network connection

Procedure

Check whether there is an Internet connection at the machine. Onboarding does not start correctly if there is no Internet connection.

10.1.1.7 Checking directory "boot_job"

Procedure

1. Check whether the following folders exist:
   - On the PCU: C.\Temp\boot_job
   - On the NCU: var/tmp/boot_job
2. If the folders do not exist, even though the previous preconditions have been satisfied, check the network connection.

10.1.1.8 Checking the asset type in Insights Hub

Procedure

Assets must be created as asset type under "BasicSinumericAsset".

1. Select: "BasicDevice > BasicSinumerikAsset > YourAssetType"
2. Create a new asset if the asset type does not exist there.

10.1.1.9 Checking the existence of onboard.key

Procedure

File onboard.key must exist in directory "boot_job".

Onboarding does not start if onboard.key does not exist.

10.1.2 Resolving known faults

10.1.2.1 Onboard key exists but onboarding does not start

- "onboard key" exists in directory "boot_job".
- Onboarding does not start.

Cause

- There are problems with the network connection.
- The date or time set at the HMI is incorrect.

Remedy

- Check the network connection.
- Check whether the date and time settings are correct.
- If the date or time is incorrect
  - Select "Settings > HMI > DateTime".
  - Enter the correct date and time.
  - Select "OK".
  - Restart the HMI.

10.1.2.2 Onboarding starts, cert.key is created; however, onboard.key does not disappear

- Onboarding starts.
- "cert.key" exists.
- "onboard.key" does not disappear.



Cause

The SINUMERIK Integrate URL is incorrect.

Remedy

- Check whether the SINUMERIK Integrate URL has been correctly specified.
- Check whether "onboard.key" has expired. The expiration time is 30 minutes.
  - Clean all the files in the "boot_job" folder.
  - Create a new onboard.key and save it.
  - Perform an "sc reboot". It is not sufficient to just restart the HMI.

10.1.2.3 No boot script available

An error message indicating that a boot script is not available is displayed at the HMI.



Cause

- Problems with the network connection have occurred.
- There is a problem with the date or time setting.
- The SINUMERIK Integrate URL is incorrect.

Remedy

- Check the network connection to the machine. Also check the proxy settings.
- Check whether the date and time settings at the HMI are correct.
- Check whether the SINUMERIK Integrate URL is correct.

10.1.3 More information

Running "sc reboot"

You can use WinSCP.

1. Open WinSCP.
2. Log on with the user name and password of the device.
3. Open the console using "Open Terminal".
4. Enter "sc reboot".
5. Click on "Execute".

Executing an HMI reboot

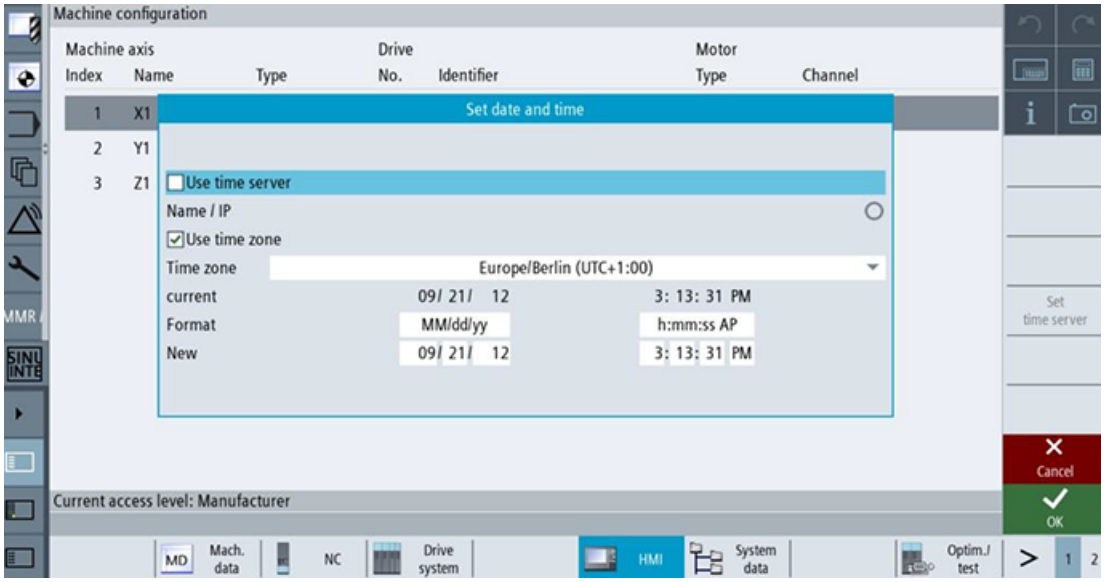
1. Press "F10" on the HMI panel.
2. Select the right-hand arrow.
3. Select "HMI reboot".

Updating SINUMERIK Operate causes problems relating to date and time

If HMI date and time are not current, the directories have the following creation dates and times.



Check whether the HMI date and time are current.



Onboarding duration

If you have saved onboard.key, then onboarding is completed within between 2 and 3 minutes. The duration depends on the SINUMERIK device that is used for onboarding.

Directory {TempDir}/boot_job

The value of {TempDir} refers to the following entry from file "/user/Sinumerik/hmi/cfg/ePSConfig.xml":

```
<global><stations><station name="NCU840D"><tempDir>
```

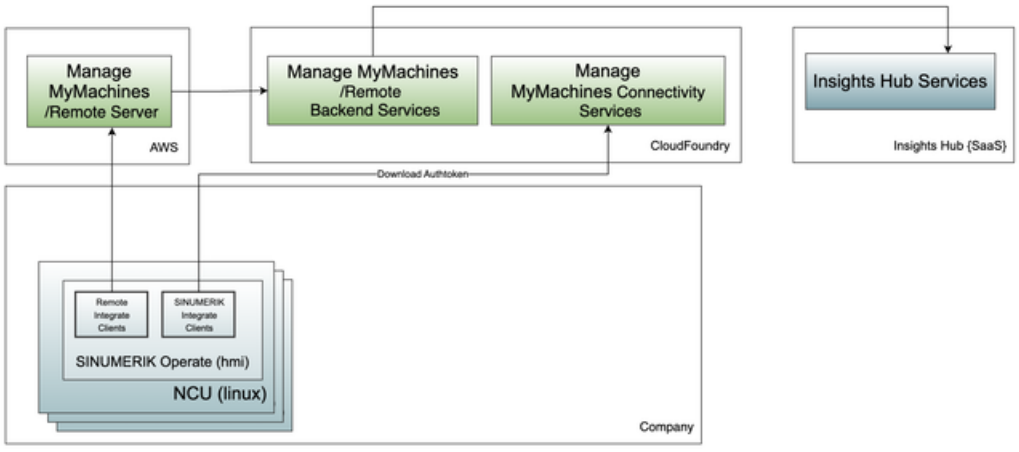
The default value of {TempDir} is "/var/tmp".

Appendix

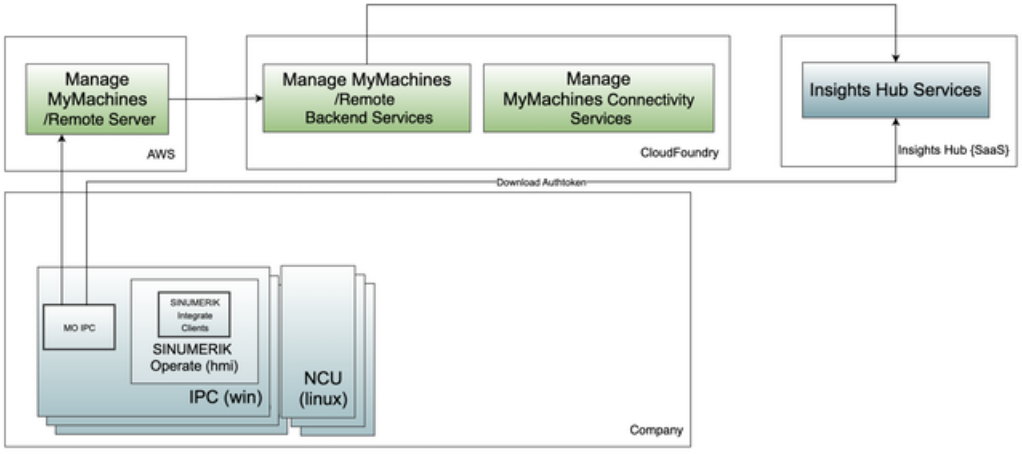
A

A.1 Preconditions for the Shopfloor Management Application

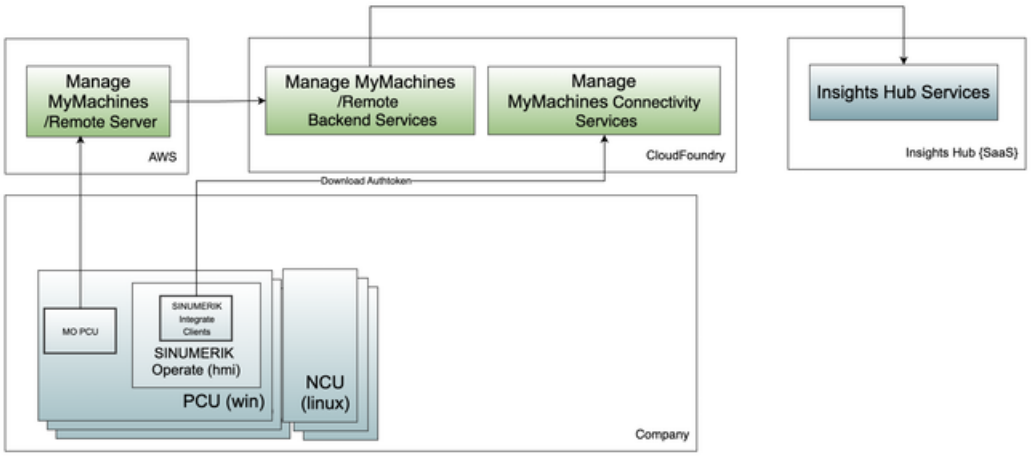
NCU



IPC



PCU



Precondition

The system on which "SINUMERIK Integrate" or "HMI Advanced" is installed has access to the internal network and to the Internet.

Connections required

Connections with SINUMERIK Integrate

The SINUMERIK Integrate client is installed and activated in SINUMERIK Operate or HMI Advanced.

Configure the MMM Machine Communication URL in the SINUMERIK Integrate client.
If a proxy is installed in the network, configure the proxy in the SINUMERIK Integrate client.
You can find more information in the "Configuring URL and proxy" chapters for

- SINUMERIK 840D sl (Page 40)
- SINUMERIK 828D (Page 47)

The SINUMERIK Integrate client is connected with the Internet and has access to the address Gateway client based (https://gateway.eu1.mindsphere.io/api/agentcom-mmmops/v3/ws11).

Internal links required

For machines to access the "MMM Machine Communication" URL, access to the following pages is allowed within the firewall of the internal network:

- *.siemens.com (https://siemens.com)
- cdn.auth0.com (https://cdn.auth0.com)
- static.mentor-cdn.com (https://static.mentor-cdn.com)
- *.mindsphere.io (https://mindsphere.io)
- *.siemens.cloud (https://siemens.cloud)

To register machines in the MMM connection:

- Call the following page:
  Asset Manager (https://yourtenant-assetmanager.eu1.mindsphere.io/entity/yourtenantid/plugin/mtaassetconfig?selected=yourassetid)
- Download the "onboard.key".

Summary

Devices in the factory have access via the internet to

- *.siemens.com (https://siemens.com)
- cdn.auth0.com (https://cdn.auth0.com)
- static.mentor-cdn.com (https://static.mentor-cdn.com)
- *.mindsphere.io (https://mindsphere.io)
- *.siemens.cloud (https://siemens.cloud)

The proxy and MAC address configuration for the machine agents is correct. If the internet connection is interrupted, then data are backed up encrypted and locally in the buffer of the client/agent.

The registry key for MMM /Remote Session is stored encrypted on the hard disk.

A.2 List of abbreviations

Admin	Administrator (user role)
AMM /C	Analyze MyMachine /Condition
AST	Auto Servo Tuning: Automatic servo tuning
CNC	Computerized Numerical Control:
COM	Communication
DIR	Directory:
FAQ	Frequently Asked Questions
h	Hour
HTTP	Hypertext Transfer Protocol
HTTPS	HyperText Transfer Protocol Secure,
IB	Commissioning engineer (user role)
ID	Identification number
IE	Internet Explorer
IFC	Interface Client
IoT	Internet of Things
IPC	Industrial PC
MB	Megabyte
MFA	Multi Factor Authentication
MLFB	Machine-Readable Product Code
MMM	Manage MyMachines
MMM /R	Manage MyMachines /Remote

MO	Machine operator
MQTT	Message Queuing Telemetry Transport
MSTT	Machine control panel
NC	Numerical Control: Numerical control
NCU	Numerical Control Unit: NC hardware unit
OEM	Original Equipment Manufacturer
OP	Operation Panel: Operating equipment
Open API	Open Application Programming Interface: open programming interface
PB	Package Builder
PC	Personal Computer
PCU	PC Unit: Computing unit
PLC	Programmable Logic Control: Programmable Logic Controller
REST API	Representational State Transfer Application Programming Interface
SE	Service engineer
SI	SINUMERIK Integrate
SK	Softkey
SW	Software
TPM	Trusted Plattform Module: Chips for safety functions
URL	Uniform Resource Locator
UTC	Universal Time Coordinated, coordinated global time
UTS	Usage Transparency Service
VNC	Virtual Network Computing
VPN	Virtual Private Network

Index

A

Access levels for STEP 7, 186
Activating
  Data acquisition, 25
  SINUMERIK Integrate client, 38
  Using SINUMERIK Integrate, 39
Asset
  Asset type, 69
  Create, 72
  Online status, 71
Asset Manager
  Functions, 67
  Open, 68
Authorizations, 66

C

Calendar function, 128
Certificate
  Download, 96
  Import for machine operator (MO), 135
  Import for service engineer (SE), 148
Charging model, 76
Commissioning overview, 25
Conference call, 155
Configuring the proxy
  SINUMERIK 828D, 47
  SINUMERIK 840D sl, 40
Configuring the URL
  SINUMERIK 828D, 47
  SINUMERIK 840D sl, 40
Create drive
  SINUMERIK 840D sl, 46

D

Data acquisition
  Activating, 25
Desktop sharing, 169, 172
Displaying version data, 27

E

ePSConfig.user.xml, 55
Exchanging a certificate
  Linux, 53
  Windows, 54

F

File transfer, 155
  Assigning attributes, 182
  Cancel, 181
  Deleting files, 182
  Execution, 173
  Exit, 183
  Performance optimization, 179
  Protocol, 180
  Restart, 178
  Settings, 199
  Start, 174

I

Insights Hub
  Connecting the SINUMERIK open-loop control, 85
  Disconnecting the SINUMERIK control system, 205
  Login, 61
Installation
  Manage MyMachines /Remote Service Client MO, 132
  Manage MyMachines /Remote Service Client SE, 145
  SINUMERIK 828D software update, 29

L

Language
  Change, 201
Logging settings, 203
  Create folder, 204
  Find directory, 204
Login settings, 199

M

Machines
  Exporting data, 94
  Filtering, 94
  Registering, 93

Manage MyMachines
Activating, 76
Manage MyMachines /Remote
Open, 90
Product information, 7
Managing remote sessions, 117

N

Network interruption, 198

O

OEMFrame application
Integrating, 141
onboard.key
SINUMERIK 828D - WinSCP (NCU), 51
SINUMERIK 840D sl - NCU, 44
SINUMERIK 840D sl - PCU 50, 44
SINUMERIK 840D sl - WinSCP (NCU), 45
Online status, 71

P

Proxy settings, 140, 153
Configuration, 140, 153
Own logon data, 141, 154

R

Recording the session, 155
Remote access
Changing the conference leadership, 195
Changing the network interface of the SIMATIC Manager, 184
Remote STEP 7, 186
Remote Service Client
Download, 94
Remote session
Exit, 197
Join, 104
Overview, 100
Remote sessions
Overview, 107
Remote STEP 7
Close, 187
Start, 186

S

Screen
Sharing, 155, 169, 172
Service Client
Logging settings, 203
Login data, 199
Proxy server, 140, 153
Setting file transfer, 199
Session log
Editing, 114
Export PDF, 118
Exporting CSV, 118
Settings, 112
Setting the login data, 199
Settings
File transfer settings, 199
Logging, 203
Login, 199
Proxy settings, 140, 153
Shopfloor Management Application, 76
Open, 75
Silent Installation, 142
SINUMERIK 828D
Configuring the URL and proxy, 47
Installing a software update, 29
SINUMERIK 840D sl
Configuring the URL and proxy, 40
Create drive, 46
SINUMERIK Integrate
Activating client, 38
Activating use, 39
Lock use, 207
SINUMERIK Integrate Client update
For SINUMERIK Operate under Linux, 34
For SINUMERIK Operate under Windows, 30
Installing, 30
Step 7 via the Internet, 155
Symbols
Functions, 157

T

TIA Portal
Connecting the device, 188
Disconnecting the connection, 192
Time range
setting, 128

U

Update - SINUMERIK Integrate
SINUMERIK Operate under Linux, 34
SINUMERIK Operate under Windows, 30
User groups, 66
User interface, 156
User roles, 156