SIEMENS

SINUMERIK

Mcenter, Manage MyResources, Optimize MyProgramming /NX-Cam Editor, Analyze MyPerformance /OEE, Access MyData /Collector

Installation Manual

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

Software
Mcenter, version 5.2.1.0

10/2022
A5E44672080B AP

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

A5E44672080B AP
Ⓟ 10/2022 Subject to change

Copyright © Siemens AG 2018 - 2022.
All rights reserved

Table of contents

Introduction 1

1.1 About Mcenter

Overview of Manage MyResources /Tools

For CNC machines, the Manage MyResources /Tools product manages the complete tool circuit within a production operation.

Manage MyResources /Tools facilitates resource optimization and reduces machine downtimes by providing optimized master data, correction (offset) data and OEM tool data. It also supports tool management, component management and tool handling.

Further, Manage MyResources /Tools facilitates access to APIs. Solution partners as well as customers can integrate Manage MyResources /Tools into their processes and, based on the interfaces, develop their own applications.

1.2 About this documentation

Target group

This document addresses commissioning engineers and machine tool manufacturers. The document provides detailed information for commissioning engineers that they require to commission the software.

Scope of validity

This manual is valid for use with the following product versions:

- Mcenter, version 1.2.1.0
- Manage MyResources /Tools, version 1.2.1.0
- Manage MyResources /Programs, version 1.2.1.0
- Optimize MyProgramming /NX-Cam Editor, version 1.2.1.0
- Analyze MyPerformance /OEE, version 1.2.1.0
- Access MyData /Collector, version 1.0.0.0

Benefits

The operating manual allows the target group to get familiar with the software user interface. Based on the manual, the target group is capable of responding to problems and to take corrective action.

1.2.1 Standard scope

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

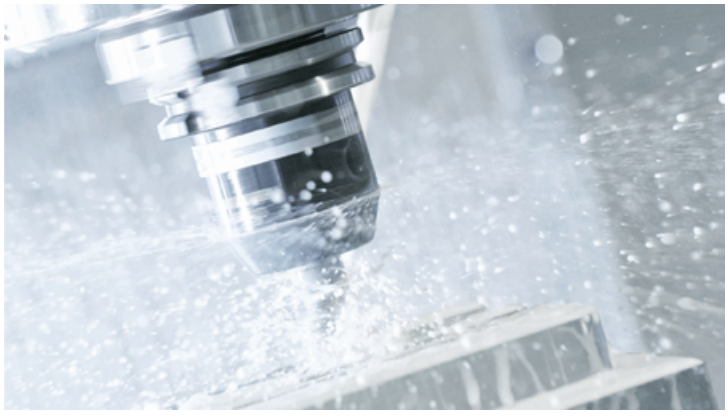
Comprehensive documentation about the functions provided in SINUMERIK ONE Version 6.13 and higher is provided in the Documentation overview SINUMERIK ONE (https://support.industry.siemens.com/cs/ww/en/view/109768483).

You can display documents or download them in PDF and HTML5 format.

The documentation is divided into the following categories:

- User: Operating
- User: Programming
- Manufacturer/Service: Functions
- Manufacturer/Service: Hardware
- Manufacturer/Service: Configuration/Setup
- Manufacturer/Service: Safety Integrated
- Information and training
- Manufacturer/Service: SINAMICS

Comprehensive documentation about the functions provided in SINUMERIK 840D sl Version 4.8 SP4 and higher is provided in the Documentation overview SINUMERIK 840D sl (https://support.industry.siemens.com/cs/ww/en/view/109766213).



You can display the documents or download them in PDF and HTML5 format.

The documentation is divided into the following categories:

- User: Operating
- User: Programming
- Manufacturer/Service: Functions
- Manufacturer/Service: Hardware
- Manufacturer/Service: Configuration/Setup
- Manufacturer/Service: Safety Integrated
- Manufacturer/Service: SINUMERIK Integrate/MindApp
- Information and training
- Manufacturer/Service: SINAMICS

Comprehensive documentation about the functions provided in SINUMERIK 828D Version 4.8 SP4 and higher is provided in the 828D documentation overview (https://support.industry.siemens.com/cs/ww/en/view/109766724).

You can display documents or download them in PDF and HTML5 format.

The documentation is divided into the following categories:

- User: Operating
- User: Programming
- Manufacturer/Service: Configuring
- Manufacturer/Service: Commissioning
- Manufacturer/Service: Functions
- Manufacturer/Service: Safety Integrated
- SINUMERIK Integrate/MindApp
- Info & Training

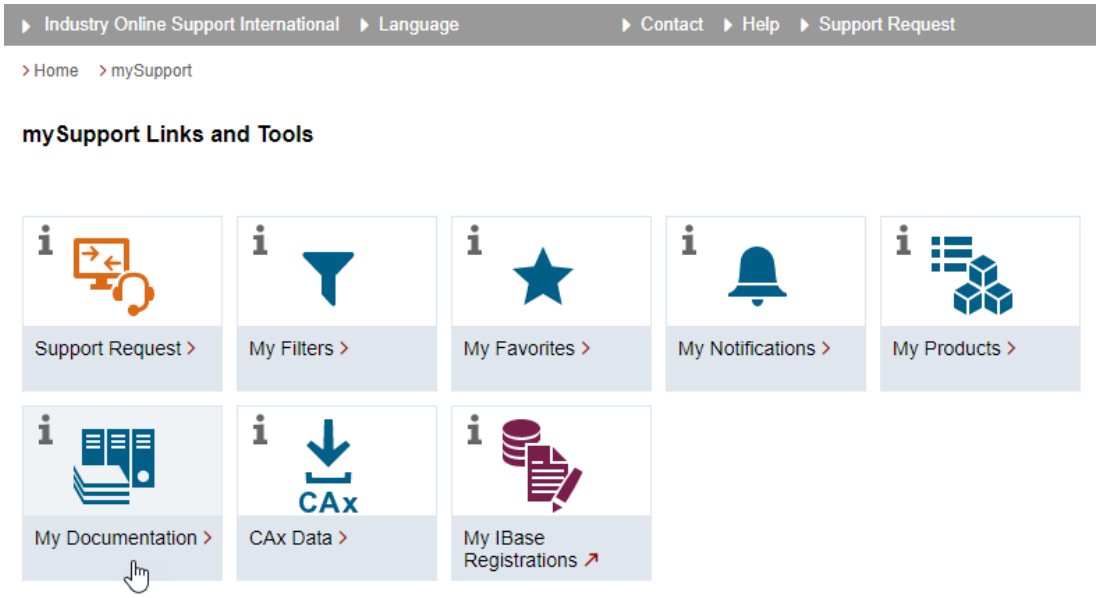
1.4 Feedback on the technical documentation

If you have any questions, suggestions or corrections regarding the technical documentation which is published in the Siemens Industry Online Support, use the link "Provide feedback" 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 homepage (https://support.industry.siemens.com/cs/my?lc=en-WW):



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

The following is provided at this address:

- Up-to-date product information (product announcements)
- FAQs
- 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 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.
SITRAIN offers training courses for automation and drives products, systems and solutions from Siemens.

Siemens support on the go

With the award-winning "Siemens 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 "Siemens Industry Online Support" app is available for Apple iOS and Android.

Data matrix code on the nameplate

The data matrix code on the nameplate contains the specific device data. This code can be read with a smartphone and technical information about the device displayed via the "Industry Online Support" mobile app.

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://cryptsoft.com/)

1.8 General Data Protection Regulation (GDPR)

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.

Fundamental safety instructions 2

2.1 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.

2.2 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.

2.3 Security information

Siemens provides products and solutions with industrial security 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 security 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 security measures that may be implemented, please visit
https://www.siemens.com/industrialsecurity (https://www.siemens.com/industrialsecurity).

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 Security RSS Feed under
https://www.siemens.com/cert (https://www.siemens.com/cert).

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 holistic, state-of-the-art industrial security concept for the installation or machine.
- Make sure that you include all installed products into the holistic industrial security concept.
- Protect files stored on exchangeable storage media from malicious software by with suitable protection measures, e.g. virus scanners.
- On completion of commissioning, check all security-related settings.

Overview 3

3.1 Checklist Mcenter

Before you install the Mcenter server, observe and check the following points:

Overview

- You require an administrator user on the Windows Server (can be a Domain User) who can perform installation on the virtual machine.
- On the SQL Server, you require authorization level user "Sysadmin" (can be Domain User).
  - OR -
  You have authorization level user "dbcreator" and "securityadmin".
- Database instance is available. A database, without a database instance, is not sufficient.
  - The database should either be available on the local computer or on a separate server. The database must accessible from the server.
- SQL Server and Mcenter server communicate via port 1433.
  - Check that this requirement is fulfilled on the application server using the following PowerShell command: `Test-NetConnection [SQL-IP] -port 1433`
  - Check the firewall settings.
    - OR -
    Check the group policy with your IT department.
- The application server (Mcenter server) is accessible via the port 8090 (HTTP).
  - Check that this requirement is fulfilled on the application server. Use the following PowerShell command from another computer:
    `Test-NetConnection [APPSRV-IP] -port 8090`
  - Check the firewall settings.
    - OR -
    Check the group policy with your IT department.
- The application server communicates with the license server via ports 28000 and 28001 (default)
  - The defined port should be enabled between the application server and license server. The default port is defined when installing the license server.
  - Check that this requirement is fulfilled on the application server using the following PowerShell command:
    `Test-NetConnection [LICSRV-IP] -port [LICSRV-PORT]`
- Maintenance task is not activated on the application server. Program maintenance checks various times, especially before running and during the installation.
  - The automatic Windows maintenance significantly slows down the setup process. Therefore, deactivate the maintenance function while you execute setup.
- IIS service runs

- The following preconditions are satisfied:
  - Microsoft OLE DB Driver for SQL Server (version 18, x64) (version 19 is not supported)
  - Microsoft Visual C++ 2015 Redistributable Update 3 (or later)
  - .NET Hosting Bundle for Windows (version 6.0.8 or higher)

  For AMP /OEE are more prerequisites needed:
  - Java Runtime Environment 8 x 64 Oracle or Zulu
  - Apache Tomcat version 9

  For more information, see Further installations (Page 68).
- Check the correct .Net version with this command line command: `dotnet --info`
- HTTPS communication
  - SSL certification is required for the settings.
  - After installation, see Setting up an encrypted connection after installation (Page 125).
- The difference between the operating system time of the Mcenter web server and the license server must not be more than 1 hour. Use the domain synchronization for the web servers to avoid potential problems.
- In case of running the database on a separate server:
  For the encrypted SQL communication, a certificate is needed on the DB server.
  It is important that the common name of the certificate must be the machine name.
  For more information, see Setting up the encrypted communication for SQL Server (Page 59).
- Mcenter uses the Microsoft Windows technology for the setup. During the Mcenter installation, Microsoft Windows saves the information and the files in the Windows Installer directory. This information is necessary to carry out an Mcenter update.
  Do not make any manual changes in the Windows Installer directory.

The connected machines must have the same time configured, as the Mcenter web server. If the machines have a different time, some Mcenter application might not work properly.

For further information about the configuration of Access MyData /Collector see the operation manual Access MyData /Collector.

3.2 System prerequisites

Prerequisites

- Install on a virtual system to allow better maintenance.
- Windows Server 2016 standard
- Windows Server 2019 standard
- SQL Server 2019 Standard (https://www.microsoft.com/en-us/sql-server/sql-server-2019)

- SQL Server 2016 SP2 (https://www.microsoft.com/en-us/sql-server/sql-server-2016)
  Complete installation of the SQL Server is required on the Mcenter Server on which the database instance is also installed.
  - OR -
  If a server system is used with a remote database, complete installation of the SQL Server is required on the DB machine
- Microsoft OLE DB Driver for SQL Server (version 18, x64) (https://go.microsoft.com/fwlink/?linkid=2206347), version 19 is not supported
- Microsoft Visual C++ 2015 Redistributable Update 3 (https://www.microsoft.com/en-us/download/details.aspx?id=53587)

Note

Microsoft Visual C++ 2015 Redistributable Update 3 installation

This is a prerequisite for the .NET Windows Hosting bundle. Install it before the hosting bundle.

- .NET Hosting bundle for Microsoft Windows (version 6.0.8 or higher) (https://download.visualstudio.microsoft.com/download/pr/c5e0609f-1db5-4741-add0-a37e8371a714/1ad9c59b8a92aeb5d09782e686264537/dotnet-hosting-6.0.8-win.exe)

Note

IIS activation

Activate IIS before installing the hosting bundle.

Server/PC/SINUMERIK control overview

Release	**Mcenter, version 5.2.1.0**				
Product	**Manage MyRessources**		**Optimize MyProgramming /NX-Cam Editor**	**Analyze MyPerformance /OEE**	**Access MyData /Collector**
	Tools	**Programs**			
Product version	1.2.1.0	1.2.1.0	1.2.1.0	1.2.1.0	1.0.0.0
Mcenter - local operation					
Integrate server					
Disk space (GB)	Web server: 150 GB[12)] Database Instance space: 500 GB[1)]	Web server: 150 GB[12)] Database Instance space: 5 GB[8)]	Web server: 150 GB[12)] Database Instance space: 5 GB	Web server: 150 GB[12)] Database Instance space: 300 GB	Web server: 150 GB[12)] Database Instance space: 5 GB[8)]
Operating systems	Windows Server 2016 (x64), Standard en-US Windows Server 2019 (x64) Standard en-US				
Databases[2)]	SQL Server 2016 SP2 Standard (en) SQL Server 2019 Standard (en)				

Release	**Mcenter, version 5.2.1.0**				
Product	**Manage MyRessources**		**Optimize MyProgramming /NX-Cam Editor**	**Analyze MyPerformance /OEE**	**Access MyData /Collector**
	Tools	**Programs**			
Prerequisites	Microsoft OLE DB Driver for SQL Server (version 18, x64) (version 19 is not supported) .NET Hosting Bundle for Windows (version 6.0.8 or higher) Visual C++ Redistributable 2015 x64 (update 3 or higher)				
	-	-	-	Apache Tomcat 9 Zulu Java JRE 8 x64 Or Oracle Java JRE 8 x64	-
Hardware constellation for amount of clients					
Processor	from Quadcore 2.6 GHz				
RAM	32 GB				
Maximal number of machine clients[7)]	350	180	20	50	50
Parallel use with all products	350				
Web browser for remote PC					
Google Chrome - recommended	Version 105, 64 bit for Windows				
Mozilla Firefox	Version 91 (ESR - Extended Support Release); 64 bit for Windows				

1) During operation, make sure that there is sufficient free storage space in your database, for example if you collect Tool statistics data from up to 150 machines for 2 years

7) The number of clients supported depends on additional parameters. For example: The more tool changes that take place, the fewer clients are supported

8) The amount of disk space needed depends on the number and size of the NC program files that are used

12) Make sure before the Mcenter installation or update that you have on system drive 2 GB and target drive 2 GB free space. In case of complete installation 4 GB free space is required on the system drive

Release	**Mcenter, version 5.2.1.0**				
Product	**Manage MyRessources**		**Optimize MyProgramming /NX-Cam Editor**	**Analyze MyPerformance /OEE**	**Access MyData /Collector**
	Tools	**Programs**			
Machine[4)]					
840D sl					

Release	**Mcenter, version 5.2.1.0**				
Product	**Manage MyRessources**		**Optimize MyProgramming /NX-Cam Editor**	**Analyze MyPerformance /OEE**	**Access MyData /Collector**
	Tools	**Programs**			
Operate versions[5)]	from 4.5 SP4 from 4.5 SP5 from 4.5 SP6 from 4.7 SP2 from 4.7 SP3[11)] from 4.7 SP4 from 4.7 SP5 from 4.7 SP6 from 4.7 SP7 from 4.8 SP2 from 4.8 SP3 from 4.8 SP4 from 4.8 SP5 from 4.8 SP6 from 4.8 SP7 from 4.93 from 4.94 from 4.95 from 4.95 SP1 from 4.95 SP2		from 4.7 SP3 from 4.7 SP4 from 4.7 SP5 from 4.7 SP6 from 4.7 SP7 from 4.8 SP2 from 4.8 SP3 from 4.8 SP4 from 4.8 SP5 from 4.8 SP6 from 4.8 SP7 from 4.95	from 4.5 SP4 from 4.5 SP5 from 4.5 SP6 from 4.7 SP2 from 4.7 SP3[11)] from 4.7 SP4 from 4.7 SP5 from 4.7 SP6 from 4.7 SP7 from 4.8 SP2 from 4.8 SP3 from 4.8 SP4 from 4.8 SP5 from 4.8 SP6 from 4.8 SP7 from 4.93 from 4.94 from 4.95 from 4.95 SP1 from 4.95 SP2	
SINUMERIK Integrate client for SINUMERIK Operate[6) 16)]	02.00.21.00.009 03.00.21.00.029 04.00.21.00.006		03.00.21.00.029 04.00.21.00.006	02.00.21.00.009 03.00.21.00.029 04.00.21.00.006	
Hardware	NCU 7x0.3 PN NCU7x0.3B PN PCU 50.5 XP/Win7 IPC Win7 / Win10		PCU 50.5 Win7 IPC Win7 / Win10	NCU 7x0.3 PN NCU7x0.3B PN PCU 50.5 XP/Win7 IPC Win7 / Win10	
HMI screen resolution for Operate	640 x 480 800 x 480 (16:9.6; TP900) 800 x 600 1024 x 768 1280 x 768 (Ergoline Panel) 1280 x 1024 1366 x 768 (16:9; WXGA (TV, SINUMERIK TOP 1500, SINUMERIK TOP 1900) 1280 x 800 (16:10; TP1200) 1920 x 1080 (SINUMERIK TOP 2200)		800 x 600 1024 x 768 1280 x 768 (Ergoline Panel) 1280 x 1024 1366 x 768 (16:9; WXGA (TV, SINUMERIK TOP 1500, SINUMERIK TOP 1900) 1280 x 800 (16:10; TP1200) 1920 x 1080 (SINUMERIK TOP 2200)	640 x 480 800 x 480 (16:9.6; TP900) 800 x 600 1024 x 768 1280 x 768 (Ergoline Panel) 1280 x 1024 1366 x 768 (16:9; WXGA (TV, SINUMERIK TOP 1500, SINUMERIK TOP 1900) 1280 x 800 (16:10; TP1200) 1920 x 1080 (SINUMERIK TOP 2200)	
SINUMERIK ONE[17)]					

Release	**Mcenter, version 5.2.1.0**				
Product	**Manage MyRessources**		**Optimize MyProgramming /NX-Cam Editor**	**Analyze MyPerformance /OEE**	**Access MyData /Collector**
	Tools	**Programs**			
Operate versions[5)]	from 6.14 from 6.15 from 6.15 SP1 from 6.15 SP2 from 6.20	from 6.14 from 6.15 from 6.15 SP1 from 6.15 SP2 from 6.20	from 6.15 from 6.15 SP1 from 6.15 SP2 from 6.20	from 6.14 from 6.15 from 6.15 SP1 from 6.15 SP2 from 6.20	
SINUMERIK Integrate client for SINUMERIK Operate[6)17)]	04.00.21.00.006	04.00.21.00.006	04.00.21.00.006	04.00.21.00.006	
Hardware	PPU 1740 NCU 1740 NCU 1750 NCU 1760	PPU 1740 NCU 1740 NCU 1750 NCU 1760	-	NCU 1750 NCU 1760	
840D pl					
HMI-Advanced	Version for NT 6.4.28.00[13)] Version for XP 6.4.28.00[13)] Version for XP SP3 7.6.2.12 HMI ADV Retrofit for Win10 from version 7.7.1.0[15)]		-	Version for NT 6.4.28.00[13)] Version for XP 6.4.28.00[13)] Version for XP SP3 7.6.2.12 HMI ADV Retrofit for Win10 from version 7.7.1.0[15)]	
Hardware	PCU 50.1 NT[9)] PCU 50.2 NT/XP PCU 50.3/ PCU 50.5 Windows XP SP3[9)] Retrofit IPC 427D[14)]		-	PCU 50.1 NT[9)] PCU 50.2 NT/XP PCU 50.3/ PCU 50.5 Windows XP SP3[9)] Retrofit IPC 427D[14)]	
SINUMERIK Integrate client for HMI-Advanced	4.15.0.13		-	4.15.0.13	
HMI screen resolutions for HMI Advanced	640 x 480 800 x 600 1024 x 768 1280 x 768 (Ergoline Panel) 1920 x 1080		-	640 x 480 800 x 600 1024 x 768 1280 x 768 (Ergoline Panel) 1920 x 1080	
828D[10)]					

Release	**Mcenter, version 5.2.1.0**				
Product	**Manage MyRessources**		**Optimize MyProgramming /NX-Cam Editor**	**Analyze MyPerformance /OEE**	**Access MyData /Collector**
	Tools	**Programs**			
Operate versions	from 4.5 SP4 from 4.5 SP5 from 4.5 SP6 from 4.7 SP2 from 4.7 SP3[11)] from 4.7 SP4 from 4.7 SP5 from 4.7 SP6 from 4.7 SP7 from 4.8 SP4 from 4.8 SP5 from 4.8 SP6 from 4.8 SP7 from 4.93 from 4.94 from 4.95 from 4.95 SP1 from 4.95 SP2		-	from 4.5 SP4 from 4.5 SP5 from 4.5 SP6 from 4.7 SP2 from 4.7 SP3[11)] from 4.7 SP4 from 4.7 SP5 from 4.7 SP6 from 4.7 SP7 from 4.8 SP4 from 4.8 SP5 from 4.8 SP6 from 4.8 SP7 from 4.93 from 4.94 from 4.95 from 4.95 SP1 from 4.95 SP2	
Third-party controller					
Machine Agent Core version		1.5.5		1.5.5	
Auxiliary hardware		IPC 127E or equivalent		IPC 127E or equivalent	
Auxiliary hardware OS		Windows 10 Enterprise LTSC version 1809 or newer		Windows 10 Enterprise LTSC version 1809 or newer	
FANUC [18)19)]					
FANUC SW Adapter		1.2.0		1.2.0	1.2.0
FANUC HW		0i 31i-B 30i-B		0i 31i-B 30i-B	0i 31i-B 30i-B
Heidenhain					
SW adapter				1.1.0	1.1.0
HW				iTNC530	iTNC530
Mitsubishi [20)]					
SW adapter				1.0.0	1.0.0
HW				Model Series 800M	Model Series 800M
OPC UA					
SW adapter				1.0.0	1.0.0

Release	**Mcenter, version 5.2.1.0**				
Product	**Manage MyRessources**		**Optimize MyProgramming /NX-Cam Editor**	**Analyze MyPerformance /OEE**	**Access MyData /Collector**
	Tools	**Programs**			
HW				any controller that supports opc ua	any controller that supports opc ua
MT Connect					
SW adapter				1.1.0	1.1.0
HW				any controller that supports mt connect protocol	any controller that supports mt connect protocol
Rest					
SW adapter					1.0.0
HW					any controller that supports http (rest server)
Server - client network connection					
min bandwidth (MBit/s)	100				
External systems					
NX	-	-	1899	-	-
NX CAM server	-	-	3.19.5	-	-
Third-party components					
SIEMENS PLM License Server	11.0.0				

2) Separate database is supported

4) No details regarding the processor and operating system, because these parameters are defined by the hardware components

5) SINUMERIK Operate Service Pack supports all hotfix versions

6) For compatibility with the integrated SINUMERIK Integrate client (in SINUMERIK Operate) and the newest versions, refer to the following table "Compatibility"

9) Encrypted connection is supported with a proxy solution

11) For the SINUMERIK Operate V4.7 SP3 it is recommended to update to the latest SINUMERIK Integrate client from the delivery.

13) The Application management is supported from PCU-Basesoftware WIN NT V06.02.01.00

14) Onboarding is possible with workaround, additional information is provided in chapter: Mcenter with HMI-Advanced on a Retrofit machine

15) Only power line is supported for HMI-Advanced version for Retrofit

16) The Timeout in the SINUMERIK Integrate client for SINUMERIK Operate should not be changed from 200s.

17) SINUMERIK ONE is supported, but without "Digital Twin".

18) Tested on the listed 0i and 31i-B FANUC versions (HSSB High Speed Serial Bus is not supported)

19) 0i and 30i-B FANUC version is not tested, FANUC adapter supports 30i-B version according to FANUC documentation.

20) Mitsubishi Adapter - additional components need to be purchased. Please get in touch with SIEMENS for further details.

Compatibility

SINUMERIK Integrate client 2.00						
SINU-MERIK Oper-ate	**02.00.00.00. 030**	**02.00.01.00. 028**	**02.00.04.00. 010**	**02.00.07.00. 06**	**02.00.12.00. 011** **02.00.14.00. 015** **02.00.15.00. 006** **02.00.16.00. 004** **02.00.17.00. 014** **02.00.18.0 0.003**	**02.00.19.0 0.009** **02.00.21.0 0.009**
4.5 SP4	X				X	X
4.5 SP5		X			X	X
4.5 SP6			X		X	X
4.5 SP6 from HF8				X	X	X

SINUMERIK Integrate client 3.00								
SINU-MERIK Oper-ate	**03.00.04.0 0.045**	**03.00.04.0 0.045**	**03.00.06.00 .022**	**03.00.10.00 .032**	**03.00.11.00 .024**	**03.00.12.00 .012**	**03.00.14.00 .018** **03.00.15.00 .006** **03.00.16.00 .005** **03.00.17.00 .025** **03.00.18.00 .003**	**03.00.19.00 .007** **0.3.00.21.0 0.029**
4.7 SP2	X						X	X
4.7 SP3		X					X	X
4.7 SP4			X				X	X
4.7 SP5				X			X	X
4.7 SP6					X		X	X
4.7 SP7						X	X	X
4.8 SP2					X		X	X
4.8 SP3						X	X	X
4.8 SP4						X	X	X
4.8 SP5						X	X	X
4.8 SP6							X	X
4.8 SP7								X

SINUMERIK Integrate client 4.00						
SINUMERIK Operate	**04.00.15.00.010**	**04.00.16.00.005**	**04.00.17.00.010**	**04.00.18.00.005**	**04.00.19.00.008**	**04.00.21.00.006**
4.93	X	X	X	X	X	X
4.94			X	X	X	X
4.95			X	X	X	X
4.95 SP1			X	X	X	X
SINUMERIK Operate SINUMERIK ONE						
6.14			X	X	X	X
6.15			X	X	X	X
6.15 SP1			X	X	X	X
6.20						X

Hardware

SINUMERIK OP HW NCU	**4.5 SP4** **4.5 SP5** **4.5 SP6** **4.7 SP3** **4.7 SP4** **4.7 SP5** **4.7 SP6** **4.7 SP7** **4.8 SP2** **4.8 SP3** **4.8 SP4** **4.8 SP5** **4.8 SP6** **4.93** **4.94** **4.95** **4.95 SP1**
NCU 710.3 PN PLC 317	X
NCU 720.3 PN PLC 317	X
NCU 730.3 PN PLC 317	X
NCU 710.3 (B) PN PLC 317	X

SINUMERIK OP HW NCU	**4.5 SP4** **4.5 SP5** **4.5 SP6** **4.7 SP3** **4.7 SP4** **4.7 SP5** **4.7 SP6** **4.7 SP7** **4.8 SP2** **4.8 SP3** **4.8 SP4** **4.8 SP5** **4.8 SP6** **4.93** **4.94** **4.95** **4.95 SP1**
NCU 720.3 (B) PN PLC 317	X
NCU 730.3 (B) PN PLC 317	X

SINUMERIK OP HW PCU	**4.5 SP4** **4.5 SP5** **4.5 SP6** **4.7 SP3** **4.7 SP4**	**4.7 SP5**	**4.7 SP6** **4.7 SP7** **4.8 SP2** **4.8 SP3** **4.8 SP4** **4.8 SP5** **4.8 SP6** **4.8 SP7**	**4.93** **4.94** **4.95** **4.95 SP1**
PCU 50.5 XP	X	X	X	
PCU 50.5 Win7	X	X	X	X
IPC 627D Win7		X	X	X
IPC 427D Win7		X	X	X
IPC 477D Win7		X	X	X
IPC 427E Win7		X	X	X
IPC 477E Win7			X	X
IPC 427E Win10			X	X
IPC 477E Win10			X	X

SINUMERIK 840D for HMI Advanced HW PCU	**6.4.28**	**7.6.2**
PCU 50.1 NT	X	
PCU 50.2 NT/XP	X	
PCU 50.3 XP	X	
PCU 50.3 XP SP3		X
PCU 50.5 XP SP3		X

SINUMERIK 840D for HMI Advanced Retrofit	**6.5.00**	**7.7.1.0**
IPC 427D		X

Firewall settings

On the Mcenter server enable as Inbound rules these ports:

- Port 8090 for unencrypted connection (HTTP) Inbound
- Port 443 for encrypted connection (HTTPS) Inbound

For installation on the following server system:

- Configuring the SQL Server 2016 with remote database

Set the following ports on the remote database server as Inbound:

- TCP 8080 and TCP 8443
- TCP 1433, UDP 1434
  SQL Server 2016 with remote database: SQL Server (Page 42)

You need the following ports on the license server to be enable as Inbound:

- 28000, 28001

For more information, see Set license server (Page 84).

On the Mcenter server enable as outbound rules these ports if they are on a separated installation:

Communication with machines and browsers:

- Port 8090 for unencrypted connection (HTTP)
- Port 443 for encrypted connection (HTTPS)

For installation on the following server system:

- Configuring the SQL Server with remote database

Set the following ports on the remote database server as outbound:

- TCP 1433, UDP 1434.

You need the following ports on the license server to be enable as outbound:

- 28000, 28001

Set the following ports if you use Analyze MyPerformance /OEE:

- TCP 8080
- TCP 8443

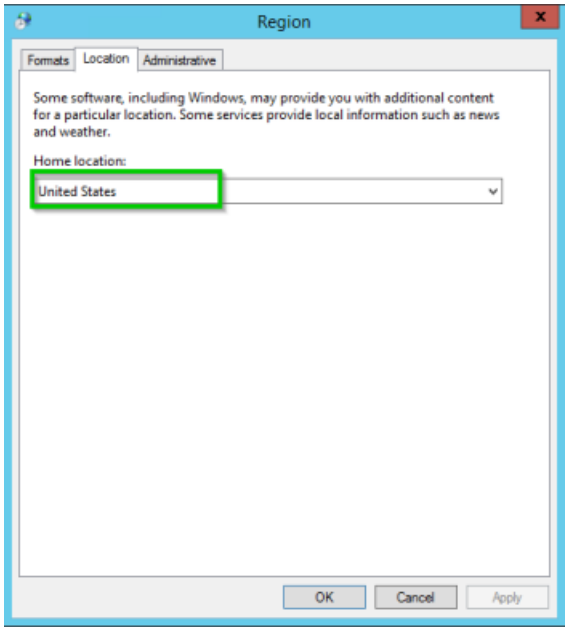
You need the following ports on Machine Agent machine and on the Fanuc controller as well for MMR Programs to work with Fanuc

- 8193

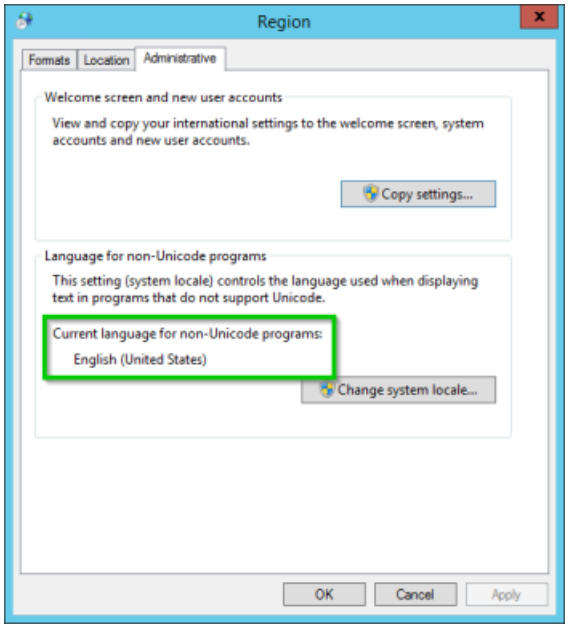
Operating system settings

Check the following settings of your operating system:

1. Select "Start" > "Control Panel" > "Region".
2. Open the "Location" tab (if applicable).
   The setting "United States" must be selected in the "Home location" drop-down list.



3. Open the "Administrative" tab.
   In the section "Current language for non-Unicode programs", the language "English (United States)" must be selected for programs that do not support Unicode.



3.3 Client version and required TLS/SSL

Overview

The following tables show which protocols are required to ensure the data exchange between a client and the server.

Client version	TLS 1.0	TLS 1.2	SSL Proxy
SINUMERIK Integrate Operate Client V02.00.06.49	X	X	-
SINUMERIK Integrate Operate Client V03.00.06.22	X	X	-
SINUMERIK Integrate Operate Client V02.00.06.48	X	-	X
SINUMERIK Integrate Operate Client V03.00.06.21	X	-	X
SINUMERIK Integrate HMI-Advanced client (Windows 7 SP1)	X	X	-
SINUMERIK Integrate HMI-Advanced client (Windows XP SP3)	X	-	X
SINUMERIK Integrate HMI-Advanced client (Windows XP SP2)	-	-	X
SINUMERIK Integrate HMI-Advanced client (Windows NT)	-	-	X

The SINUMERIK Integrate client should be updated to the latest version what is delivered in the software package if it is possible.

For more information, see System prerequisites (Page 18).

3.4 Machines and setting machine data

The following overview of the machines and the settings of the machine data are only valid to Manage MyResources /Tools.

Overview machines

The following machine tools are supported by Manage MyResources /Tools:

- Machines with milling technology, with active tool management and with the handling tool: **T**ool**M**anagement**Mag**azin (TMMG).
  For the D-number you can use absolute (1 : 32000) or relative (1 : 12) D-number.
- Machines with turning technology with active tool management and turret magazines.
  - The turret magazine must be displayed as a real magazine in the standard tool management.
  - The tools must have a T-number and an absolute (1 : 32000) or relative (1 : 12) D-number.
  - Use loading stations as magazine type for loading and unloading.

- Machines with turning technology without a configured magazine. In this case, Manage MyResources /Tools displays T-number instead of place.
- Machines with turning technology without active tool management a configured magazine. In this case, Manage MyResources /Tools displays the T-number instead of place, while the magazine name is shown as "NC Memory".
  For the D-number the following options are available:
  - When relative D-number is selected, then DNo = 1 : 12 is possible.
  - When absolute D-number is selected, then DNo = 1 : 32000 is possible.
  - When flat D-number is selected, then DNo = 1 is predefined. The tool management needs to be deactivated.

Additional information on tool management is available in: Function Manual SINUMERIK 840D sl, Tool management

Setting machine data

Activates and influences the program runtime measurement

At the SINUMERIK control system, using the SINUMERIK Operate operating system, set a machine data to activate capturing program run and tool usage times when acquiring the statistical data for each configured channel.

Set the following bits of the machine data to activate Tool statistics:

MD27860 $MC_PROCESSTIMER_MODE	Activates and influences the program runtime measurement
Bit 0 = 1	The measurement of the total runtime for all part programs is active ($AC_OPERATING_TIME)
Bit 1 = 1	Measuring of the current program runtime is active ($AC_CYCLE_TIME)
Bit 2 = 1	The measurement of the tool cutting time is active ($AC_CUTTING_TIME)

Before installation it is necessary to configure Tool statistics.

For more information, see Configuring Tool statistics (Page 170).

Mark tool data change for the SINUMERIK control system

SINUMERIK Operate display support.

This data enables individual data to be explicitly taken into account or not taken into account in the OPI variables (block C/S) toolCounter, toolCounterC, toolCounterM.

"Value changes to tool status" and "value changes to remaining tool count" are relative to the value changes which are caused by internal processes in the NC, as well as to value changes caused by writing the respective system variables.

Set the following bits of the machine data to mark tool data change:

MD17530 $MN_TOOL_DATA_CHANGE_COUNTER	Mark tool data change for HMI
Bit 0 = 1	Changes to the values of the tool status ($TC_TP8) are taken into account in toolCounterC
Bit 1 = 1	Changes to the values of the remaining number of tools ($TC_MOP4) are taken into account in toolCounterC

3.5 Exemplary system behavior of MMR /Tools

System Requirements

Mcenter application server:

Web server: 150 GB

Operating Systems

Windows Server 2016 (x64) Standard en-US 12GB RAM

Intel® Xeon® E5-2690 V4 Processor – 2.6GHz – 35MB Cache (4 processors)

Prerequisites:

Microsoft OLE DB Driver for SQL Server (version 18, x64), version 19 is not supported

NET Hosting Bundle for Microsoft Windows (version 6.0.8 or higher)

Visual C++ Redistributable 2015 x64 (Update 3 or later)

Mcenter database server:

Windows Server 2016 8GB RAM

Intel® Xeon® E5-2690 V4 Processor – 2.6GHz – 35MB Cache (4 processors)

Installation:

Microsoft SQL Server 2017 Standard (en)

Microsoft Visual C++ 2015-2019 Redistributable (x64)

.NET Framework 4.5.2

Overview

The above-mentioned system requirements ensure the functionality of our application.

System reaction time with a defined number of connected machines:

300 connected machines with a tool exchange every ~17 sec – load to spindle and load back to the magazine – statistical events are created for loading and unloading

30 Monitoring tools applications are open with different users. Every Monitoring tool refresh is performed within 10 sec. Thus, the tool state change is immediately shown on the machine. However, as to the server, it can take up to 10 sec for the state to be refreshed (6 sec to send the data to the server, 4 sec to update the data within the Server UI). As long as the tool is within the spindle, the tool state change is uploaded to the server, but this does not apply to the residual lifetime or residual work piece. These are updated when the tool is loaded back to the magazine.

Every new open instance of “Monitoring tool” slows the system down. You should therefore close applications you do not need.

The performance of the "Tool master data" application depends on the number of Master data values, and especially on the user-defined attributes, attached documents and used components. The more complex the data, the more resources are needed to show the data.

In our application, we can make sure that the data is shown within 6 seconds. This applies to Master data with 5000 Tool master data items, every item containing 50 customer-specific attributes.

The Tool stock performance depends on the number of tool instances used or created. This means Tool stock shows the data within 9 seconds, when the system contains 20.000 Tool instances, created from 10.000 Tool master data items with 50 customer-specific attributes.

You can improve the performance of Tool master data and Tool stock. When you open a Master data set or a Tool instance, you can right-click, and open the data with a new tab. Thus, you do not need to wait for the data to load when you open the next dataset.

Example for machine-client behavior with Operate 4.7.4 without any OEM applications.

MMR /Tools is supported on Operate machines from the versions 4.5 SP4 or 4.7 SP3 (see System Requirements).

Installing a MMR /Tools client on the Operate machine uses resources. The average response time for switching between the application is 2.5-3.5 seconds. The time average within the MMR /Tools application itself is 2-3 seconds. If the Operate machine is a combination of a NCU and a PCU/IPC, the response time is better, the average reaction time for switching between the application being ~3 seconds and with in MMR /Tools ~2 seconds.

A running CNC program slows the machine down and has an impact on the response time, especially if the CNC program has a lot of tool changes.

The machine operator company can also connect machines with HW version: Sinumerik 840D sl NCU 739.2PN MLFB: 6FC5373-0AA01-BAA2 with the Operate version 02.07.02 HF 02 without PCU under certain conditions.

The response time for this machine amounts to 2-3 seconds, when you switch between the applications. To connect old Operate machines, you have to deactivate statistics. This can be done via the configuration in mmrconfig.json, located at the machine.

Do not connect older Operate Client 840D sl.

MMR /Tools is supported on Advance client machines, like the version for NT 6.4.28.00 (see System Requirements). Do not connect older clients, because the installation is more time-consuming.

As a machine operator, you need to make sure the OEM software on the Sinumerik client is up to date. Ensure that additionally installed applications do not use too many resources, especially on old clients. Writing or reading on the hard disc, using services like SlCap or checking magazine data every few seconds, slows down the machine and affects its usability.

Note

Mcenter server and client machines in the same network

Mcenter server and the client machines connected to it should be in the same network (LAN). Tunneling (for example VPN) is not supported in any form (PPTP, L2TP, etc...).

Installing/configuring Windows services

4

4.1 Overview

Before installing the local server, you must set the Windows functions - and install the applications along with the SQL Server.

Prerequisite

Always use the original data storage medium when installing the Windows server!

Procedure

Proceed as follows:

1. Install and configure the Internet Information Services (IIS).
   For more information, see Setting up Internet Information Services (Page 35).
2. Install the SQL Server.
   For more information, see SQL Server (Page 42).
3. Install additional components.
   For more information, see Further installations (Page 68).
4. Take all of the necessary measures to harden the Internet Information Services (IIS).
   for more information, see TLS and Assets (Page 147).
   The measures are mandatory for secure operation!

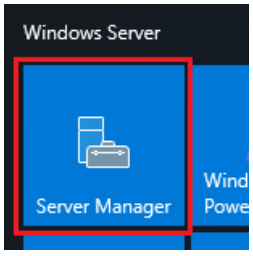
4.2 Setting up Internet Information Services

The following settings apply to the SQL servers 2016 and 2019.

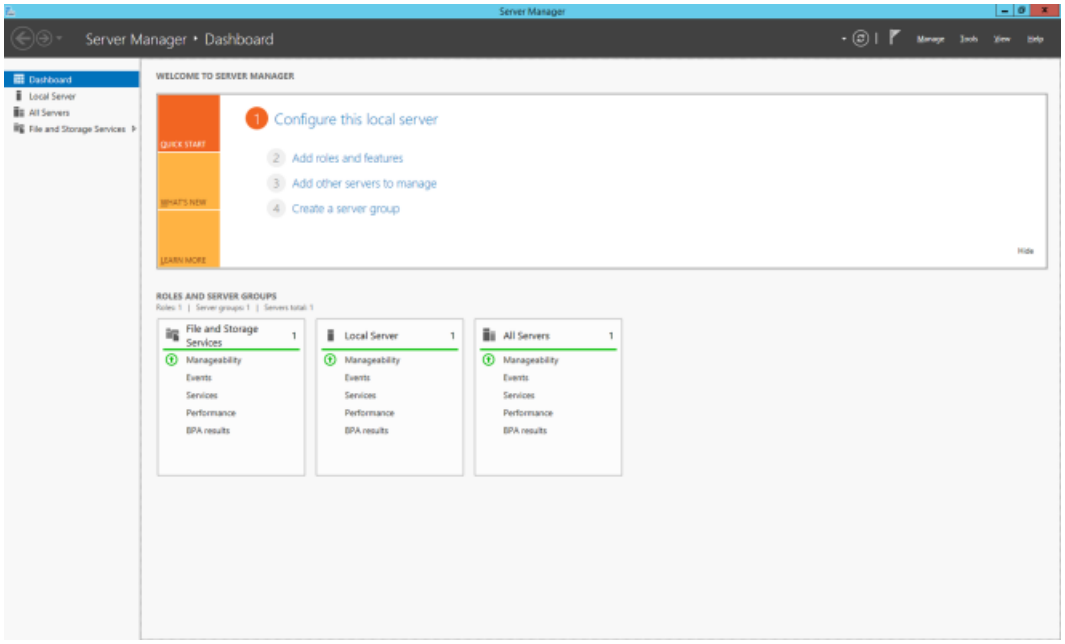
If there are any differences compared to the SQL Server 2016, they are written on that point.

Procedure

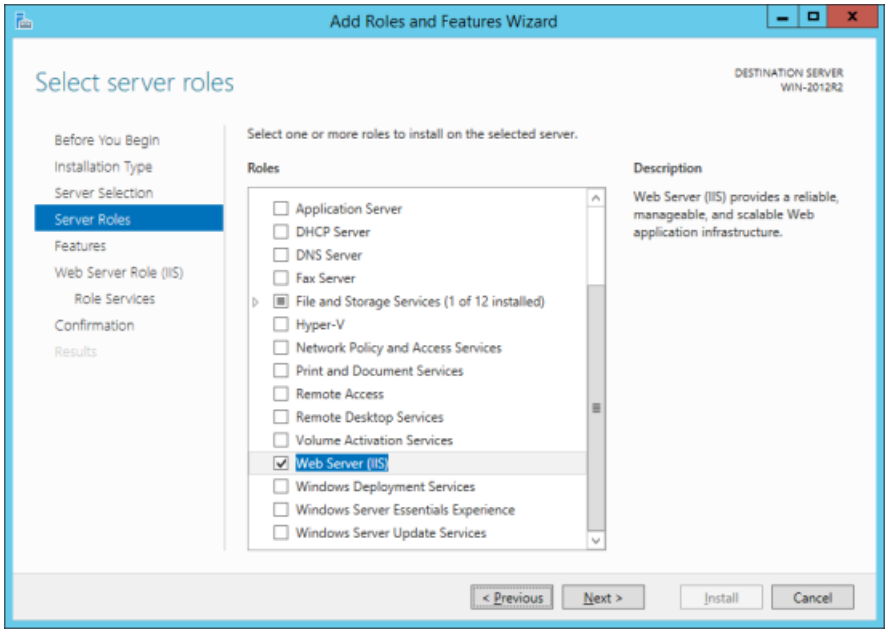
1. Insert the server installation CD/DVD into the CD drive.
2. Start the "Server Manager".



3. Select "Dashboard" and click "Add roles and features".

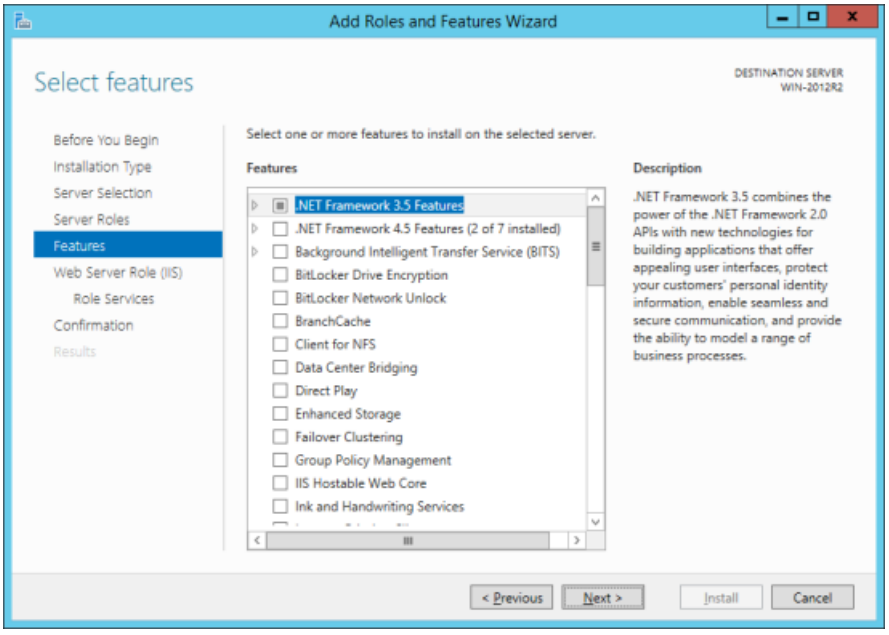


4. Select the "Server Roles" function in the "Add Roles and Features Wizard" window and activate the "Web Server (IIS)" checkbox.



5. Select the "Features" function and activate the following option box:
   – ".NET Framework 3.5 Features". This selection is required for SQL.

   Click "Next >".



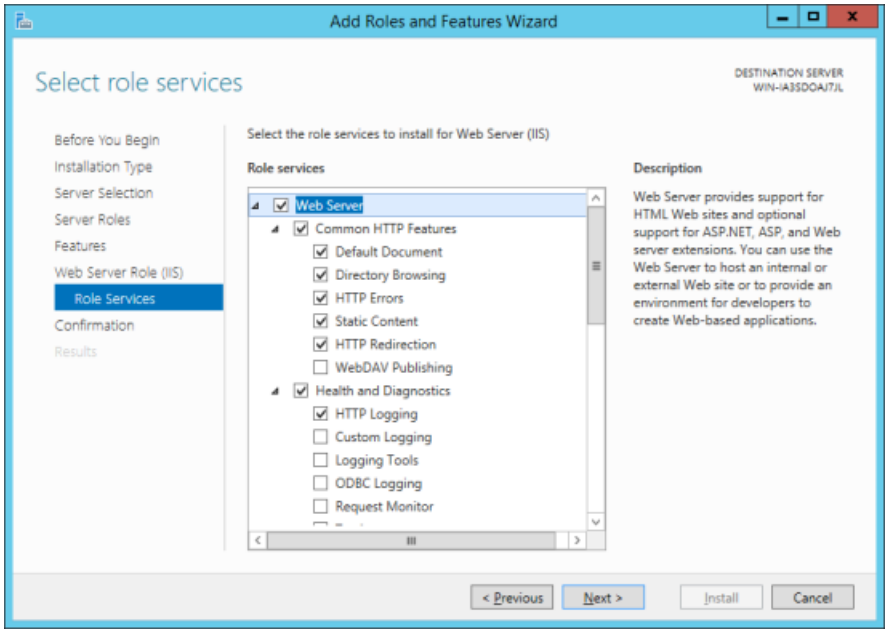
6. Select the "Role Services" function at "Web Server Role (IIS)".
   Activate the "Web Server" checkbox.
   Activate the "Common HTTP Features" checkbox and the following properties below:
   - Default Document
   - Directory Browsing
   - HTTP Errors
   - Static Content
   - HTTP Redirection

   Activate the "Health and Diagnostics" checkbox and the following property below:
   - HTTP Logging

Note

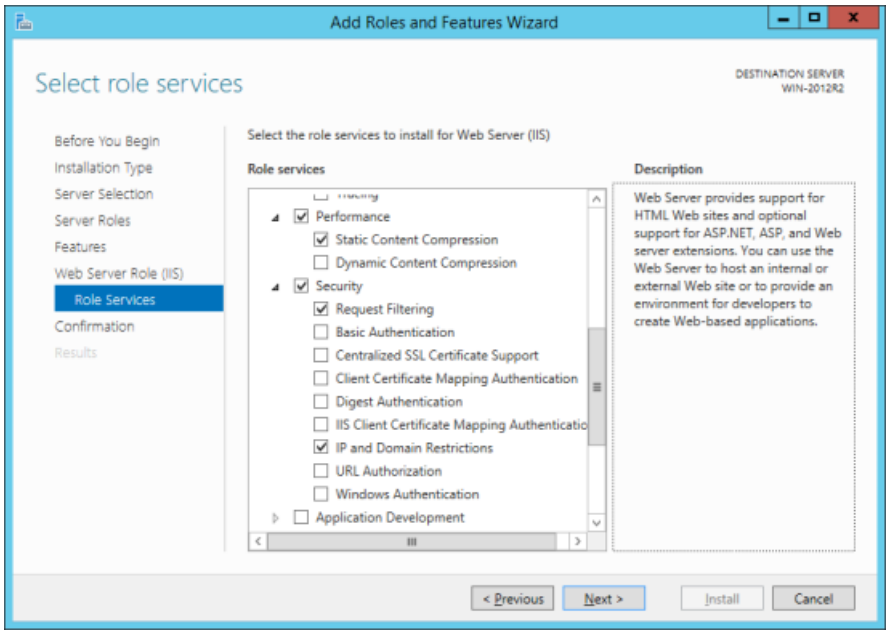
Role services

Do not enable the "WebDAV Publishing" feature!

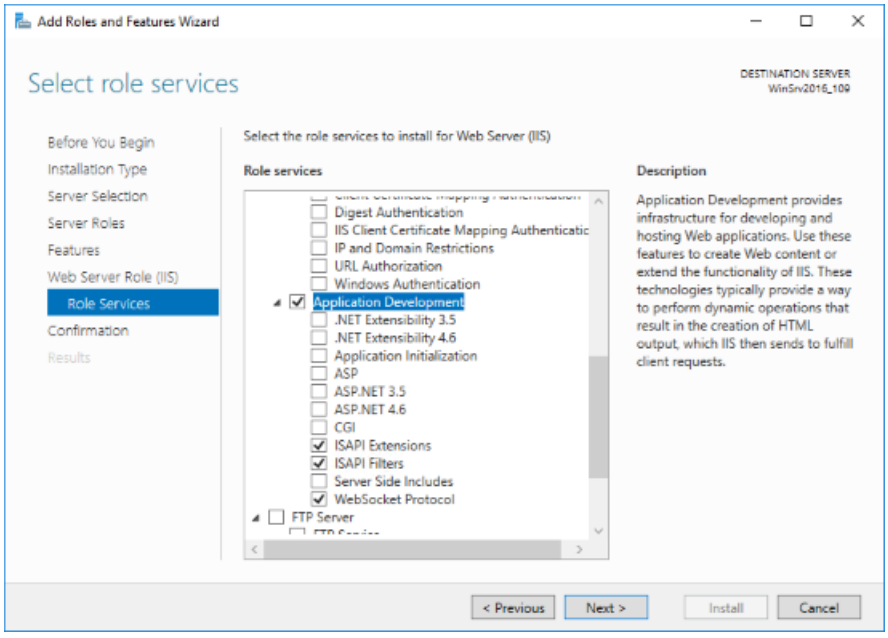


7. Activate the "Performance" checkbox and the following property below:
   – Static Content Compression

   Activate the "Security" checkbox and the following property below:
   – Request Filtering
   – IP and Domain Restrictions

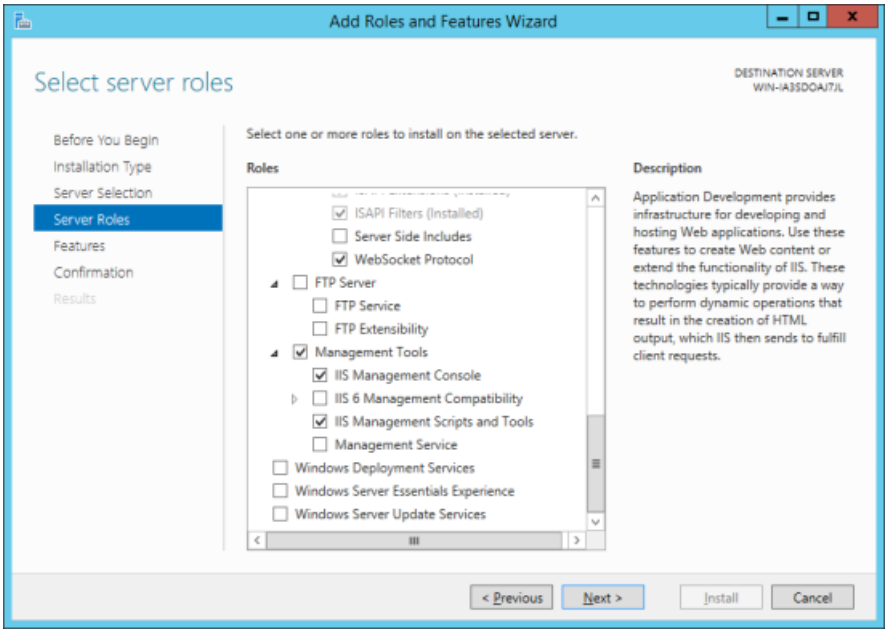


8. Set the following:
   Check the "Application Development" checkbox and below it the following properties**:**
   - ISAPI Extensions
   - ISAPI Filters
   - WebSocket Protocol

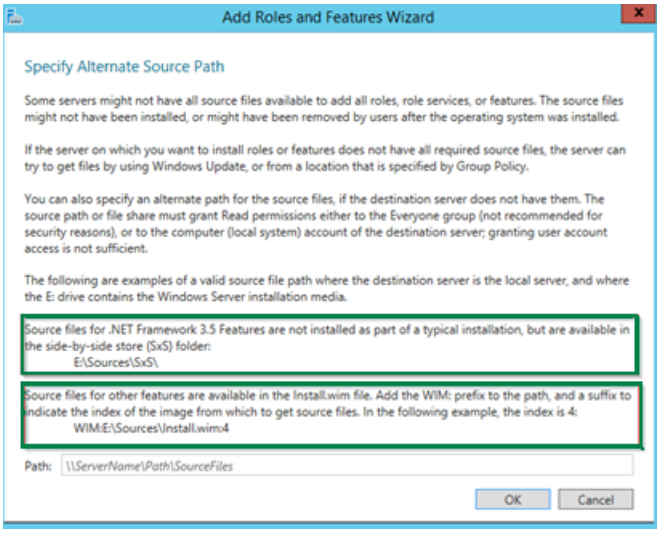


9. Activate the "Management Tools" checkbox with the following properties:
   - IIS Management Console
   - IIS Management Scripts and Tools

   Click "Next >".
   The settings are backed up.



10. Select the "Confirmation" function and click on "Specify Alternate Source Path".
    The "Specify Alternate Source Path" window opens.
    Enter the directory for the installed components in the “Path:" entry field. For example, in case of a mounted Windows image the directory is "D:\Sources\SxS".



4.3 SQL Server

4.3.1 Installing SQL Server

The following settings apply to the SQL servers 2016 and 2019.

If there are any differences compared to the SQL Server 2016, they are written on that point.

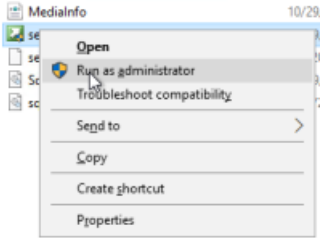
Prerequisite

You require administrator rights to install the SQL Server.

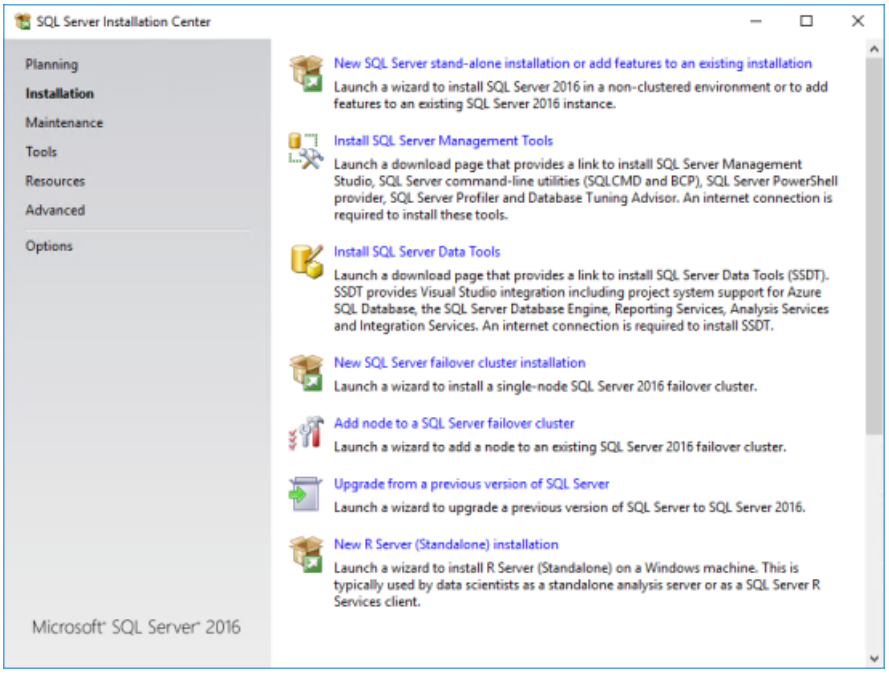
Always use the original data storage medium.

Procedure

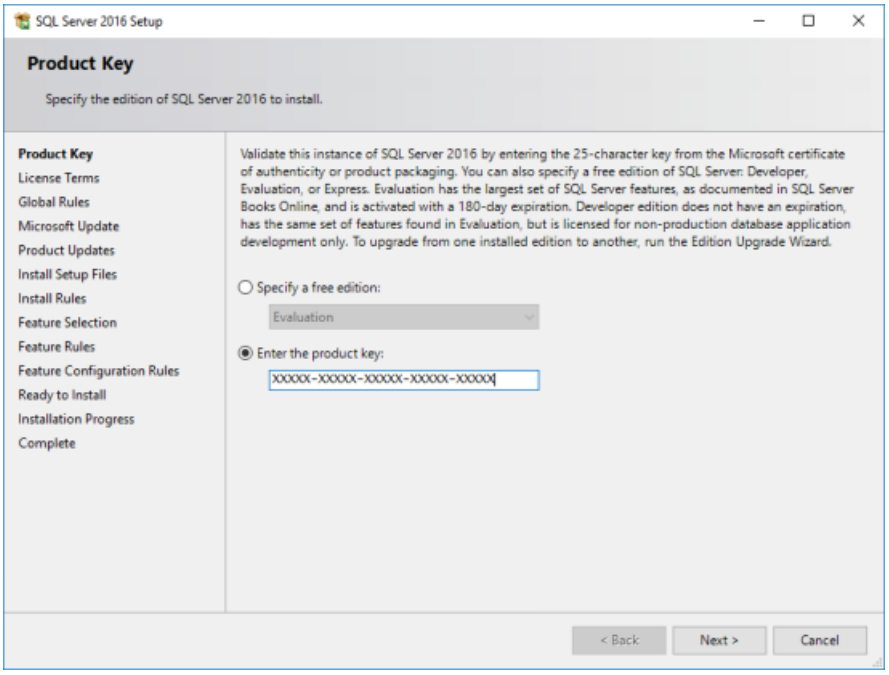
1. Select the setup application "SQL 2016 standard".
2. Right-click to open the "Setup" menu and start the installation with the "Run as administrator" menu command.



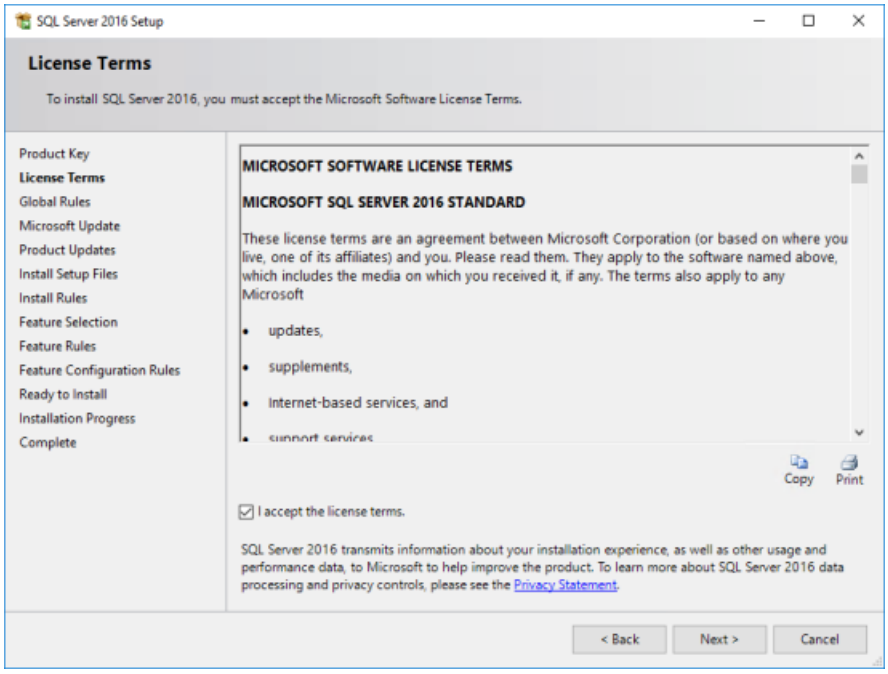
3. The "SQL Server Installation Center" window opens.
   Select the "Installation" function and click option "New SQL Server stand-alone installation or add features to an existing installation".



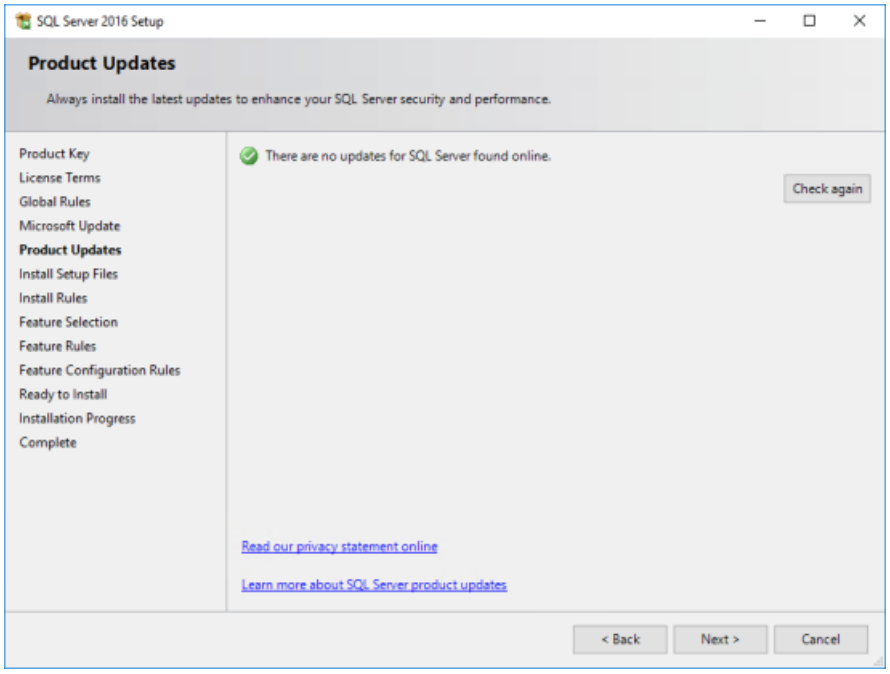
4. The "Product Key" window opens.
   Activate the "Enter the product key" option button
   Enter the key and click "Next >".



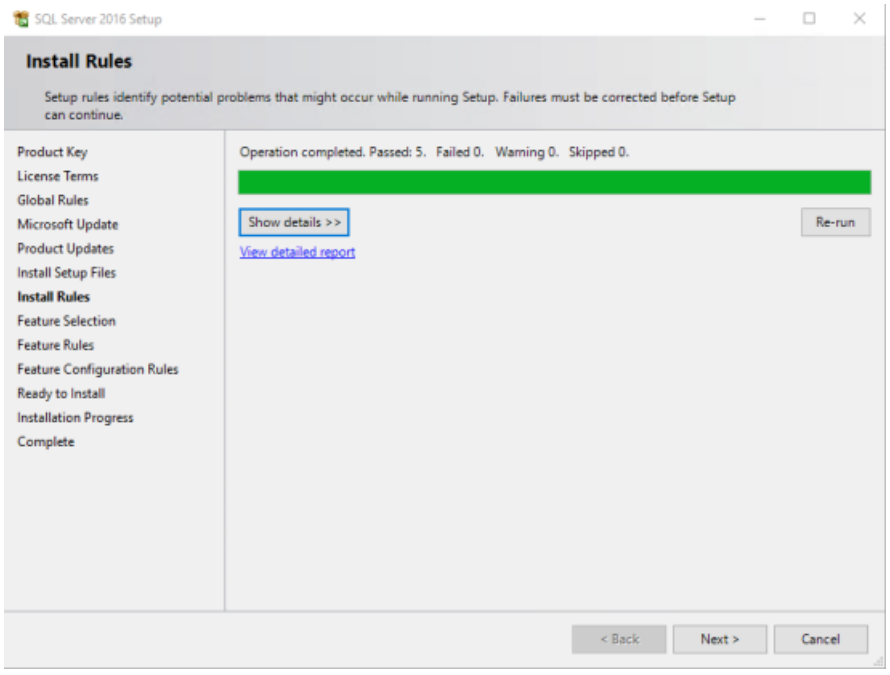
5. The "License Terms" window opens.
   Read the license agreement.
   - If you want to print the terms, click "Print".
   - If you want to copy the terms, click "Copy".
   - Then activate the "I accept the license terms" option button and click "Next >".



6. The "Product Updates" window opens and shows whether updates are available. Click "Next >".



7. The "Install Rules" window opens and checks whether the installation can be started.



4.3.2 Configuring SQL Server

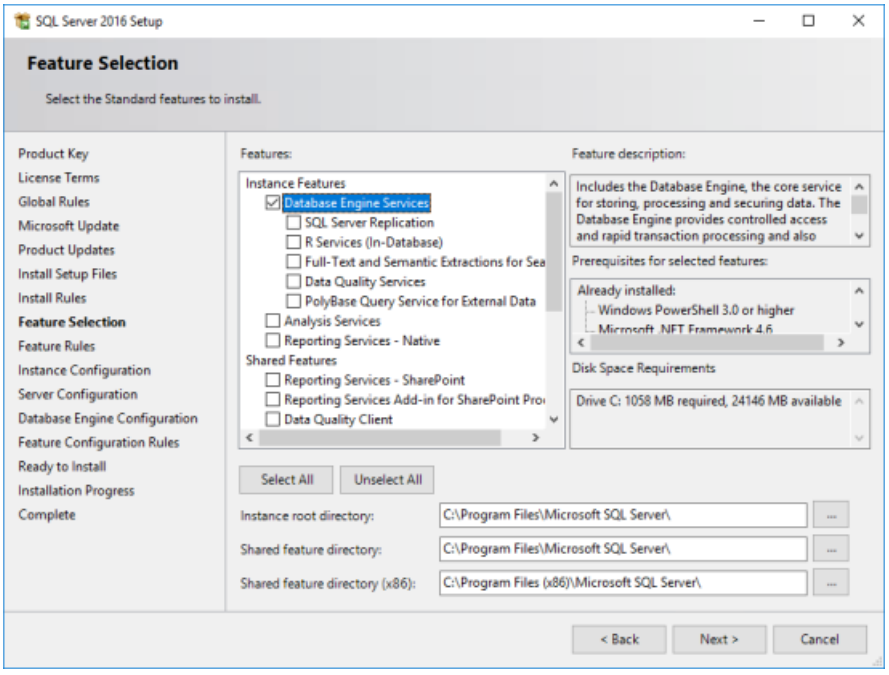
The following example is a description of the "SQL server" configuration.

Prerequisite

You require administrator rights in the database, for example authorization level user "Sysadmin" as "Domain/Local User" or as SQL user (sa).

Procedure

1. Select the "Feature Selection" function and activate the "Database Engine Services" checkbox.



Note

SQL Management Studio

The SQL Server installation does not contain an "SQL Management Studio" installation. If you need the "SQL Management Studio" you must install it separately.

2. Select the "Instance Configuration" function.

   – You can select the standard settings, activate the "Default instance" option button. A name is automatically created. The instance is already defined when installing the server.

   - OR -

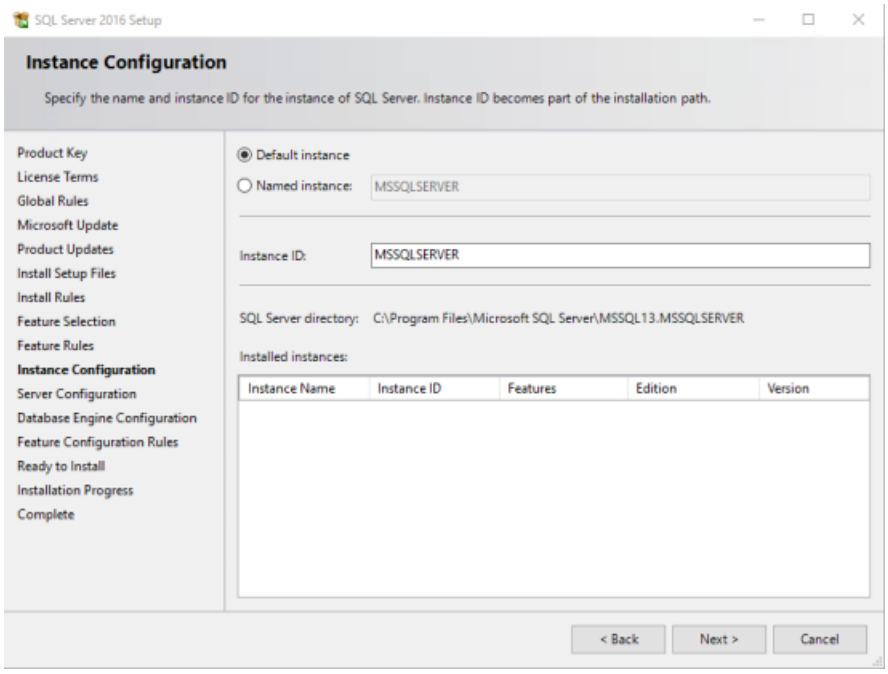
   – You can create your own "Instance Name".

   Both ways are supported by Mcenter.
   Click "Next >".

Note

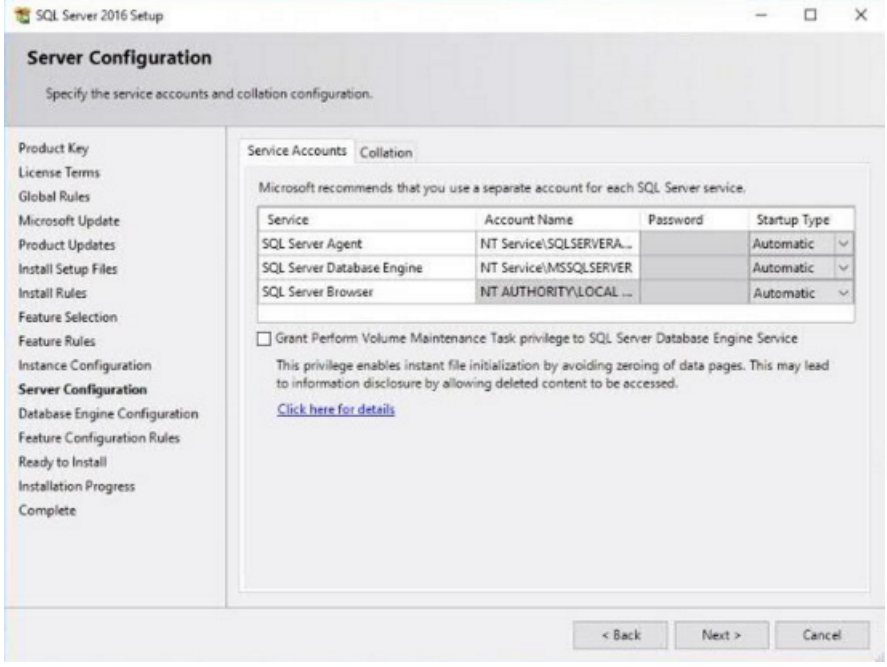
Configured instance

Instance names are limited to 16 characters. If you do not give a name to the instance, the machine name is the "Instance Name" which is limited to 16 characters. It is recommended to create a name for the instance, or change the machine name because it might cause problems during the installation.



3. Select the "Server Configuration" function.
   Open the "Service Accounts" tab and make the following settings:
   - SQL Server Agent: NT Service\SQLSERVER... and Automatic
   - Server Database Engine: NT Service\MSSQLSERVER and Automatic
   - SQL Server Browser: NT AUTHORITY\LOCAL SERVICE and Automatic

   Click "Next >" to continue with the configuration.



4. Select the "Database Engine Configuration" function.
   Open the "Server Configuration" tab and specify the following properties:
   - Authentication Mode: Activate the "Mixed Mode (SQL Server authentication and Windows authentication)" option button.
   - Enter a password: Enter a strong password for the login ID. You can delete this password after the installation. When installing the server, you use any SQL user with administrator rights.

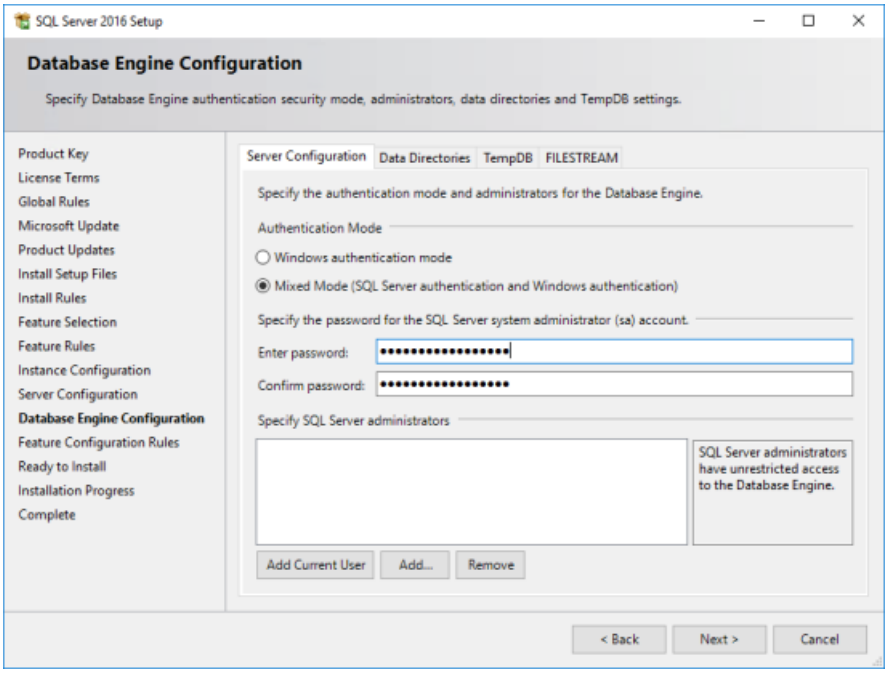
     Note

     Properties of a strong password

     - Use at least 14 characters.
     - Combine uppercase and lowercase letters, as well as special characters and numerals (?!%+...).
     - Make sure that the password is not listed in dictionaries.
     - Do not use any common variants and repetition or keyboard patterns, for example asdfgh - OR - 1234 abcd.
     - Do not simply append a simple password with numerals or common special characters such as $!?# to the end or beginning.
     - Do not use the same password for several user accounts.

   - Confirm password: Confirm the password by entering it again.
   - Specify the SQL Server administrators:
     Click "Add Current User" to enter the current user in the list of SQL Server administrators.
     Click "Add..." to add further users or user groups, such as the user group of Windows administrators, to the list of SQL Server administrators.

   Click "Next >" to continue with the configuration.



5. After completion of the installation, perform a restart.

4.3.3 Configuring the SQL Server with remote database

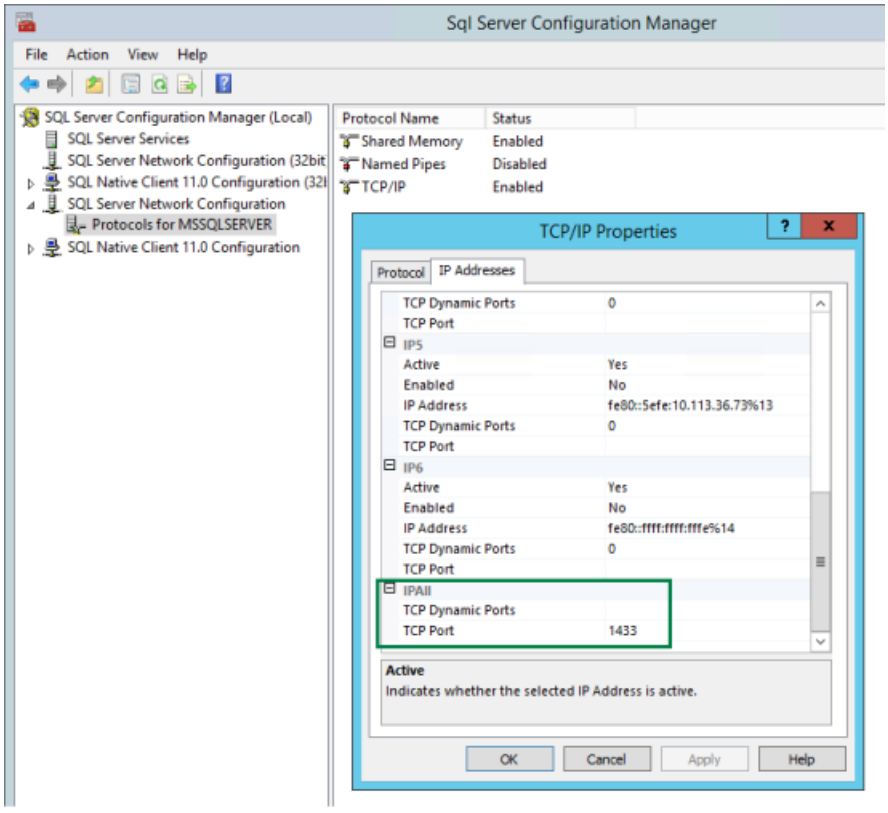
The following example is a description of the SQL server configuration with remote database.

Prerequisite

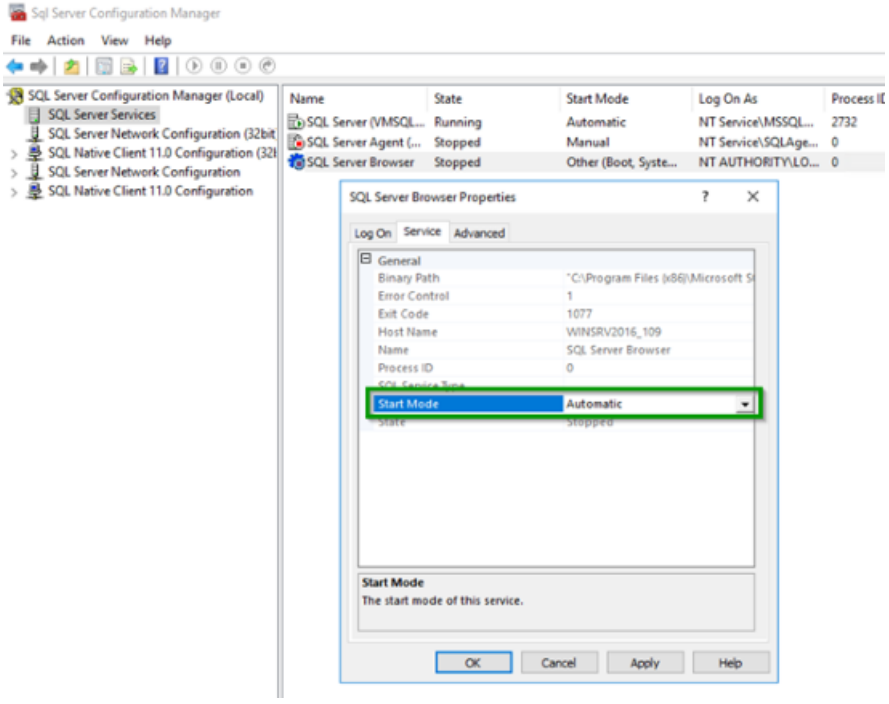
You require administrator rights in the database, e.g. authorization level user "Sysadmin" as "Domain/Local User" or as SQL user (sa).

Procedure

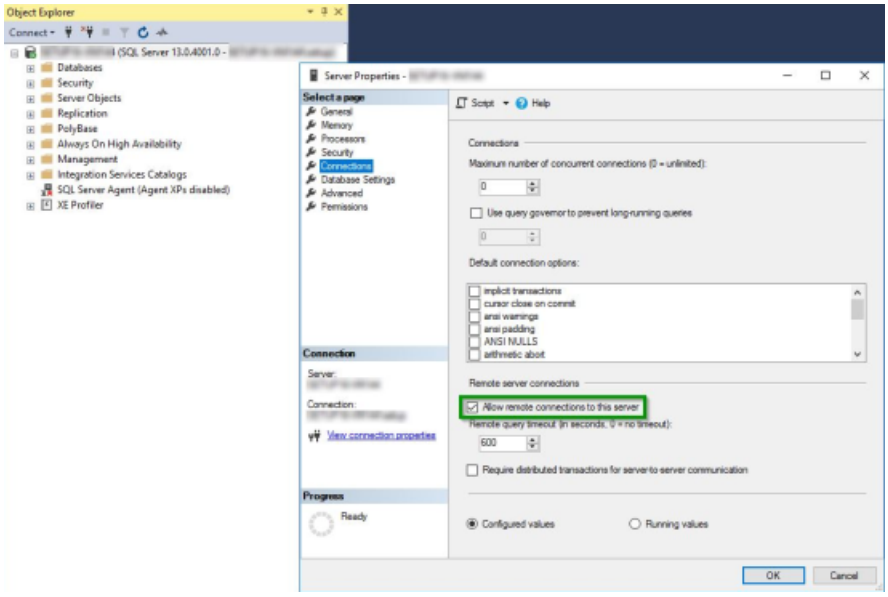
1. Open the "SQL Server Configuration Manager".
2. Open "SQL Server Network Configuration" and select "Protocols for <instance>".
   The status is shown in the right window area.
3. Open the properties for "TCP/IP", and check whether the Firewall is configured with following
   – TCP Dynamic Ports: without entry
   – TCP Port: 1433



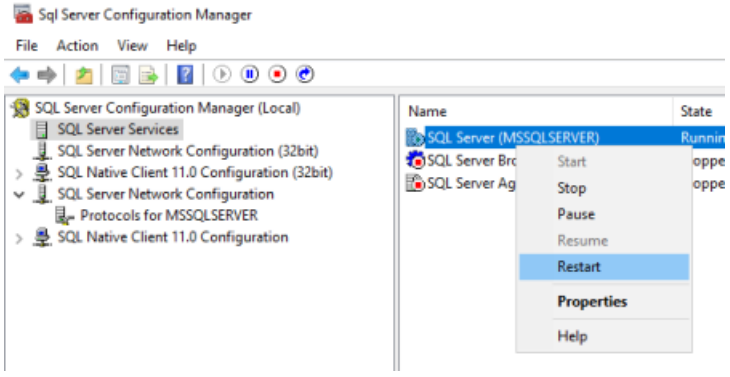
4. Check the SQL Server Services, the "SQL Server Browser" should be running. You might have to set "Start Mode" to "Automatic" before starting it: Right click > Properties
   Check that the Firewall is configured with the permitted communication UDP port 1434.



5. Open the "Microsoft SQL Server Management Studio".
   - Select the "Connections" page and check the "Allow remote connections to this server" checkbox.
   - To save the selection, click "OK".



6. Then carry out a restart.



4.3.4 Create databases and user in SQL Server

In order to use predefined databases/users during installation, the following databases and SQL login users have to be created before running the setup:

Note

Create databases and user

The databases are created during installation. If you do not want to use predefined databases, this step is not needed.

Note
Predefined databases

AMP /OEE currently does not support the use of predefined statbases.

Requirements

You require administrator rights in the SQL Database to create the users and databases.

Database structure

You need to create the following databases. Platform is mandatory, but you require the databases only for the application which you install.

- For Platform:
  - IdentityData
  - MachineData
  - MhCommData
  - PlantData
  - MachineModelData
  - AppData
  - GdaDtsConfigurationData
  - UserProfileData
  - CncOperationData
  - GdaDtsSystemMessageData
  - TaskData
  - MachineApiGatewayData
  - mabeDB
- For MMR /Tools:
  - OEMData
  - ToolInstanceData
  - ToolLocationData
  - ToolMasterData
  - MMRApplicationState
  - ToolPlan
  - AdditionalResourcesMasterData
  - AdditionalResourceInstancesData
  - ReservationData
  - ScheduleData

- For Toolstatistics:
  - ToolStatistics
- For MMR /Programs:
  - MMRProgramsData
- For AMD:
  - amdDB

SQL user

You need to create following users. Platform is mandatory, but you require the users only for the application which you install.

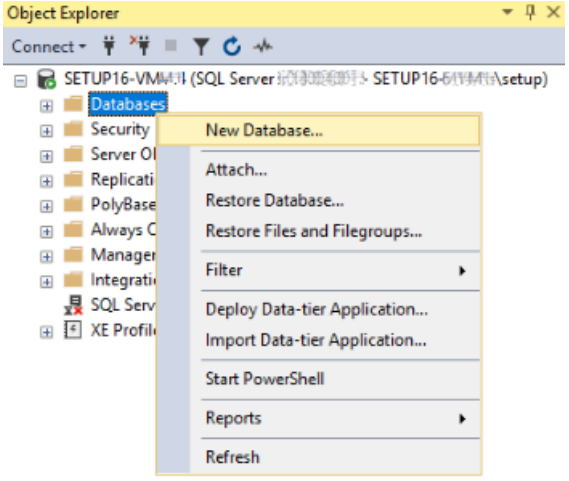
- For Platform:
  - identityUserName
  - machineUserName
  - mhcommUserName
  - plantUserName
  - machineModelUserName
  - appUserName
  - gdaDtsConfigurationUserName
  - userProfileUserName
  - cncOperationUserName
  - gdaDtsSystemMessageUserName
  - taskUserName
  - MachineApiGatewayUserName
  - mabeLogin
- For MMR /Tools:
  - oemDataUserName
  - toolInstanceUserName
  - toolLocationUserName
  - toolMasterDataUserName
  - MMRApplicationStateUserName
  - ToolPlanUserName
  - additionalResourcesMasterDataUserName
  - AdditionalResourceInstancesDataUserName
  - ReservationDataUserName
  - ScheduleDataUserName

- For Toolstatistics:
  - toolStatisticsUser
- For MMR /Programs:
  - mmrProgramsUserName
- For AMD:
  - amdLogin

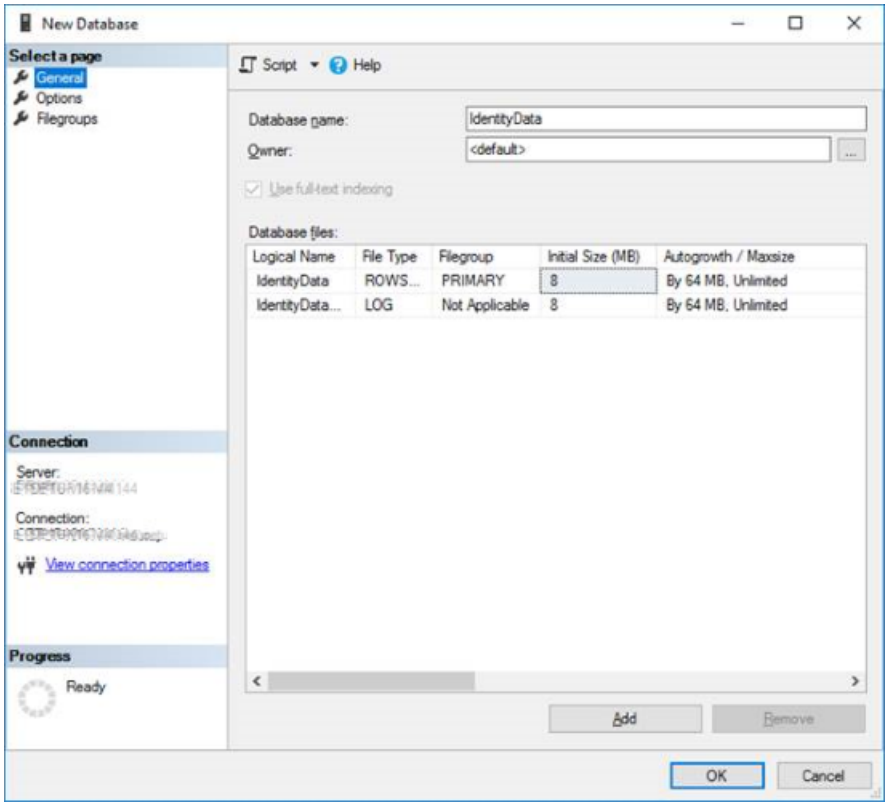
Procedure

Follow these steps to create the required databases and users.
"IdentityData" and "identityUserName" is used as an example on the screenshots.

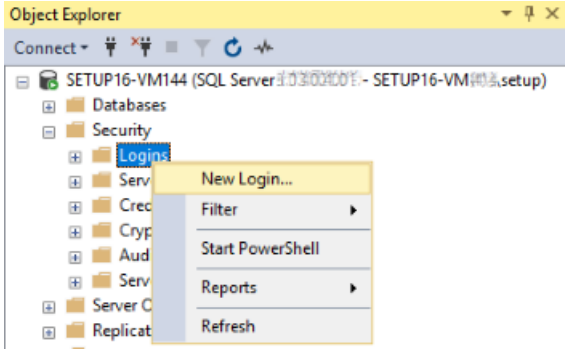
1. Log in to the "Microsoft SQL Server Management Studio" with administrator rights and select *<Windows Server name 2016>*.
2. Open the data directory of the machine involved.
3. Right-click on "Databases" and select "New Database...".



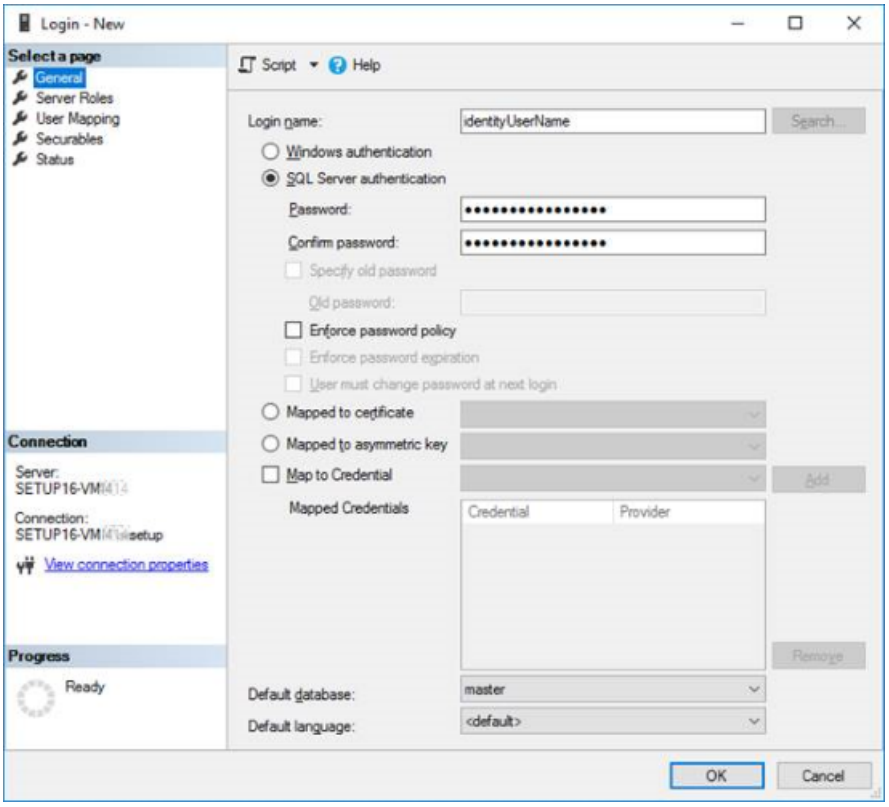
4. The "New Database" window opens.
   – Enter the database name in the "Database name" input field.
   – In the "Owner:" drop-down list, select the entry <database name>.



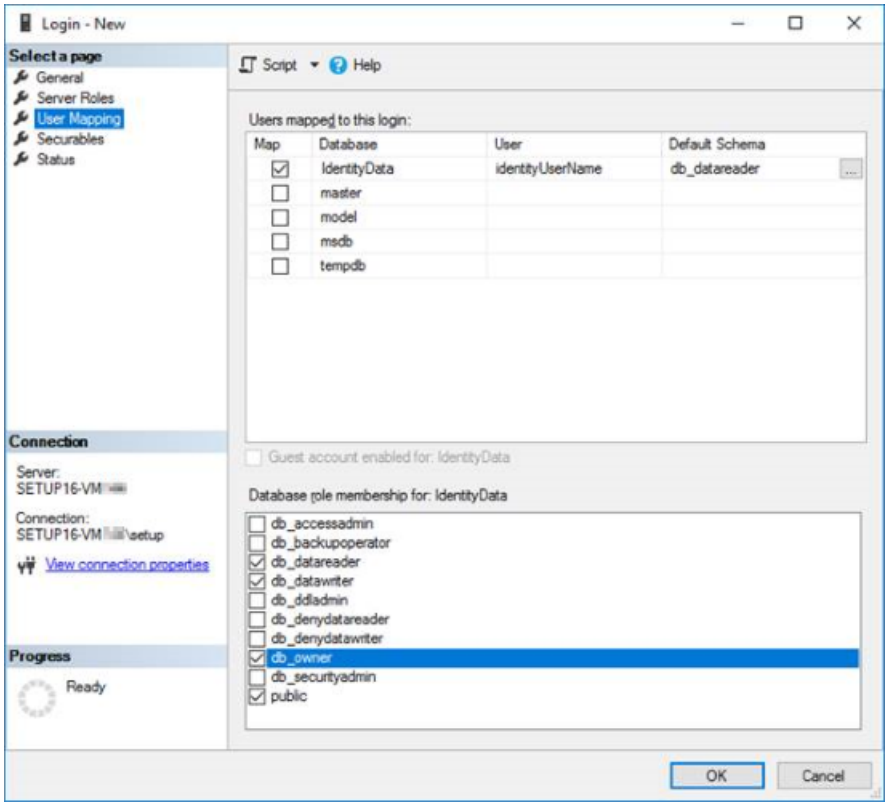
5. Open "Security".
   – Right click "Logins" and select "New Login...".



6. The "Login - New" window opens.
   Select the page "General".
   - Specify the "Login name".
   - Activate the "SQL Server authentication" checkbox.
   - Enter a password: Enter a strong password and make sure that the password meets the complexity requirements:
     Minimum 8 characters
     Must contain upper- and lowercase letter
     Number and special character. Only use these special characters: ! $ ( ) * + - . / ? @ [ ] _ { }
   - Confirm the password: Confirm the password by entering it again.



7. Select the page "User Mapping".
   Map the login user to the previously created database by adding the following roles to its database:
   - db_datareader
   - db_datawriter
   - db_owner
   - public (default)



4.4 Migration from the Server 2016 and SQL Server 2016 to 2019

You can update the Windows Server 2016 and the SQL Server 2016 to the 2019 version.

The update can be done in two different ways:

- Data migration
- Server update

Prerequisite

Mcenter system is running on Windows Server 2016 with remote SQL Server 2016. The databases are created as predefined.

Procedure - data migration

1. Install the same version of Mcenter on a Windows Server 2019.
2. Use a new separated SQL 2019 server. It is important to create the databases (predefined mode) with the same password which you have used with the SQL Server 2016.
3. Stop the IIS on the Windows Server 2016 with Mcenter.
4. Create a full backup of all Mcenter databases including also the logs for the databases.

5. Delete all databases on the SQL Server 2019.
6. Restore the databases on the SQL Server 2019 from the previously created backup.
7. Delete the assigned SQL users from the databases. These SQL user assignments can be found in the database, under security and users. These user assignments are also stored in the database backups. However, these are not the same as the ones from the existing users.
8. You have to do the SQL user mapping again.
   For more information, see Create databases and user in SQL Server (Page 52).
9. Restart the IIS on the Mcenter server.
10. Reconnect the machine to the new Windows Server 2019.
    Change only the server URL and perform an HMI restart.

Procedure - server update

1. Stop the IIS on the server on which Mcenter is installed on.
2. Update the Windows Server 2016 to 2019.
   Follow the steps recommended by Microsoft.
3. Update the SQL Server 2016 to 2019.
   Follow the steps recommended by Microsoft.
4. Restart the IIS on the server on which Mcenter is installed on.
5. The machine clients reconnect automatically.
6. After the server update, the Consul must be set again because it is deleted during the update process.

4.5 Setting up the encrypted communication for SQL Server

In case of running the database on a separate server, for the encrypted SQL communication a certificate is needed on the DB server.

Note

Local SQL server installation

In case of a local SQL server installation it does not affect the communication.

Prerequisite

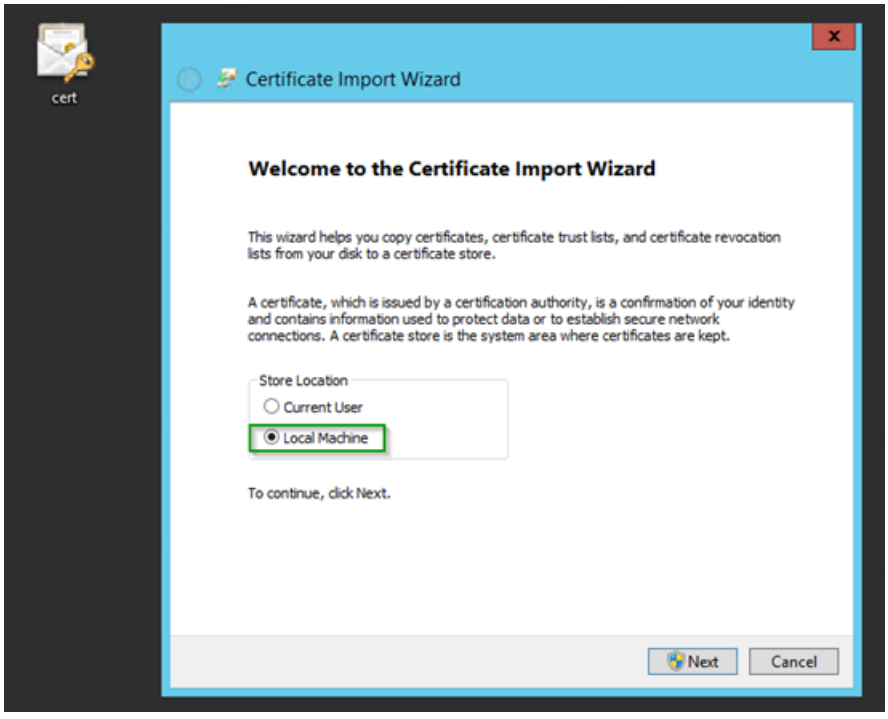
A certificate is needed on the DB server with the machine name or IP address as its subject. Make sure the first one is the machine name. (CN=Machine_name, CN=IP_address).

If the SQL Server Machine has a long DNS name also, the self-signed certificate must contain the long DNS machine name, for example "machine.networkname.net", to be accepted from the SQL Server.

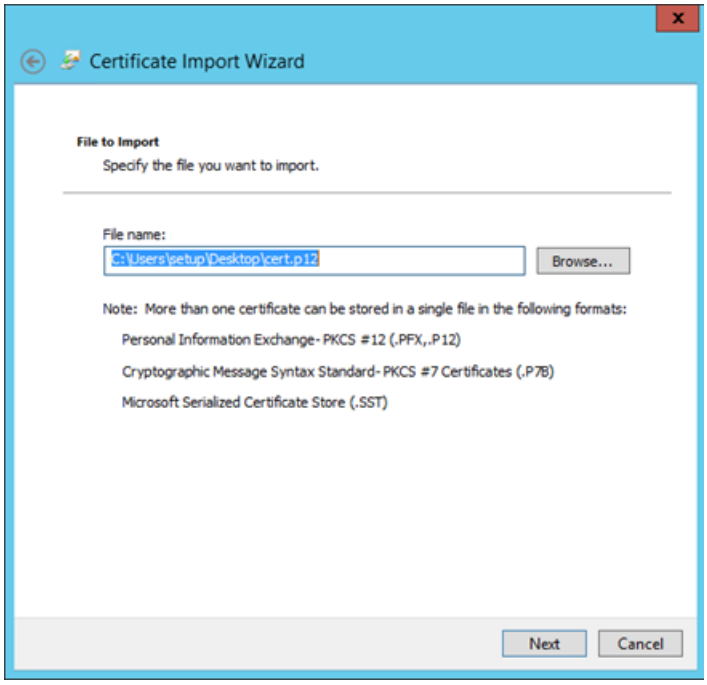
For more information, see Certificate Requirements (https://docs.microsoft.com/en-us/sql/database-engine/configure-windows/enable-encrypted-connections-to-the-database-engine?view=sql-server-ver15#certificate-requirements).

Procedure

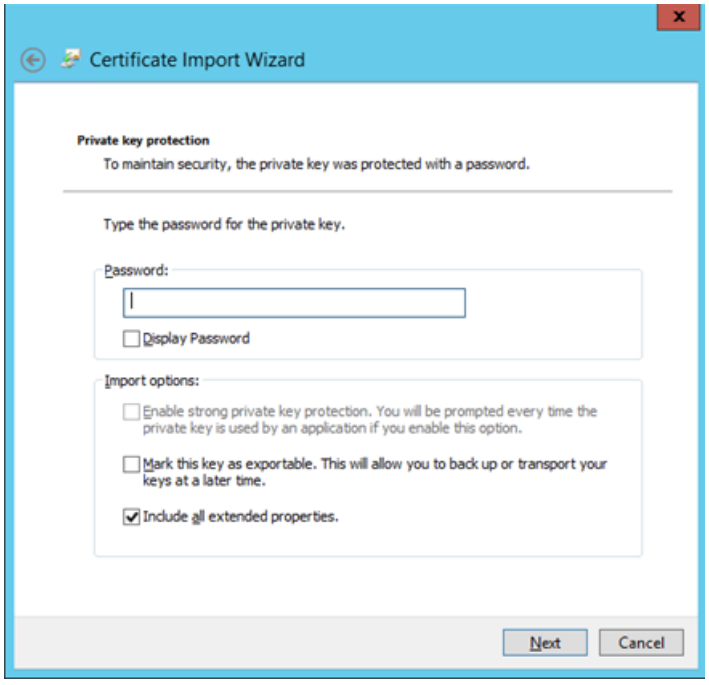
1. On the SQL database server double click on the certificate.
   Choose "Local Machine".



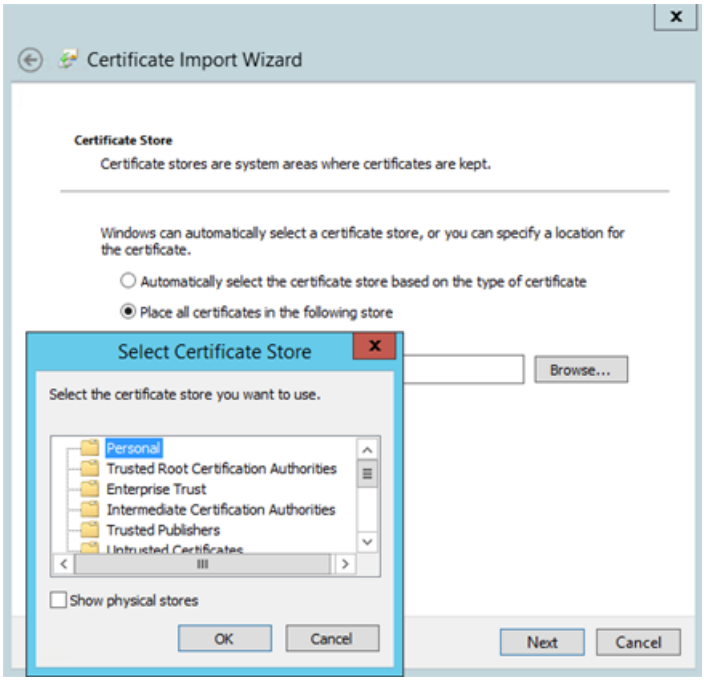
2. The certificate path will be opened automatically:



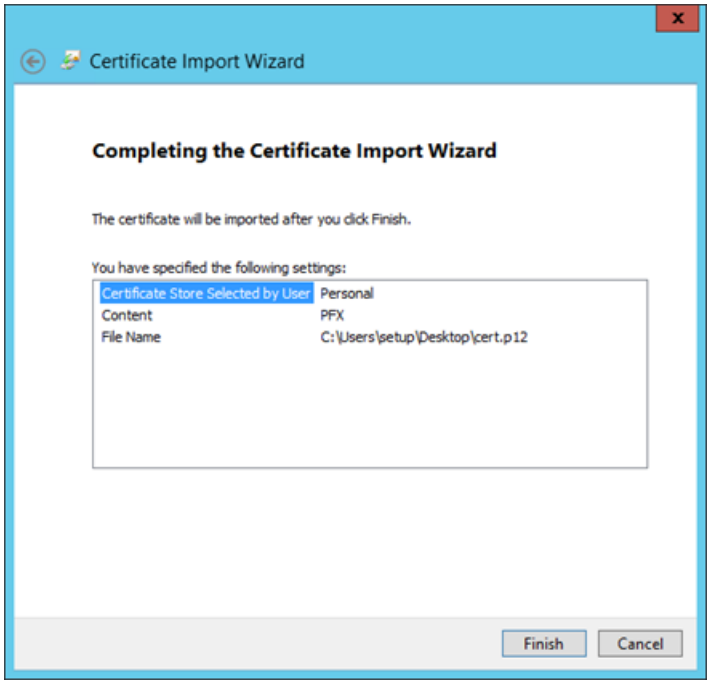
3. Input the password for the certificate.



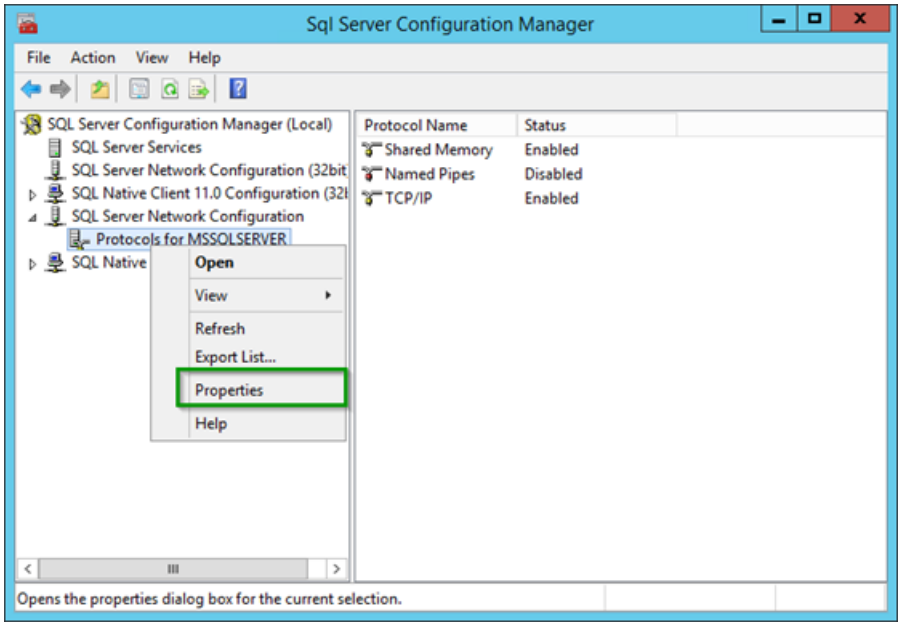
4. Import the certificate to the "Personal" folder.



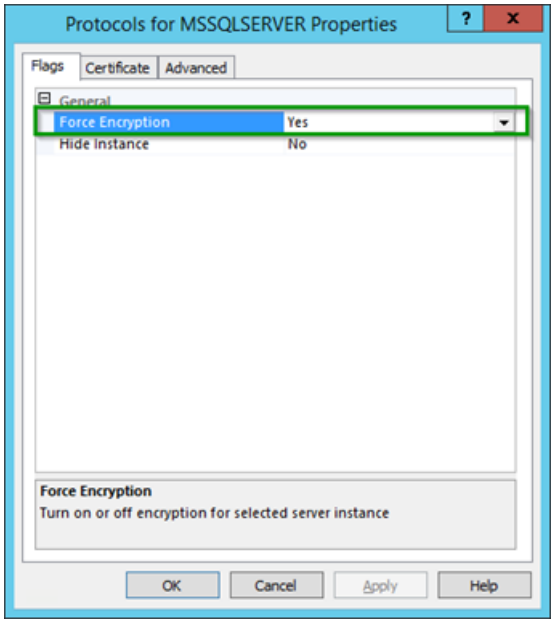
5. Click "Finish".



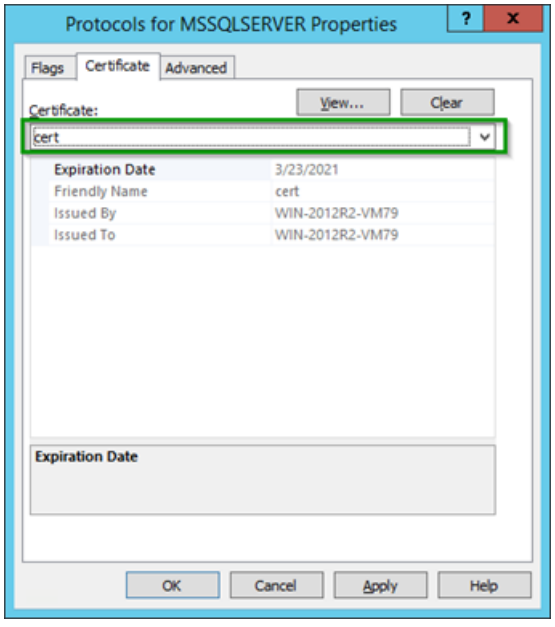
6. Go to the "SQL Server Configuration Manager" > "SQL Server Network Configuration". Right click on the Protocols for "Instance" > "Properties".



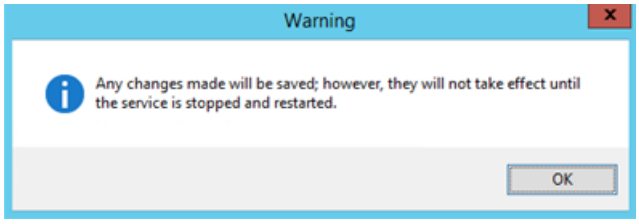
7. On the tab "Flags" set the "Force Encryption" to "Yes".



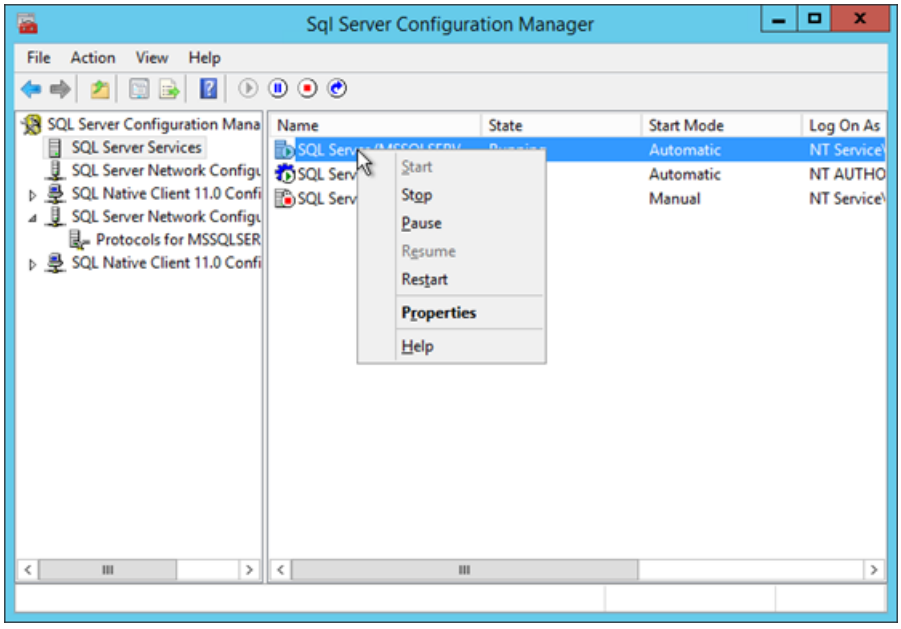
8. On the tab "Certificate" choose your certificate from the drop down list.



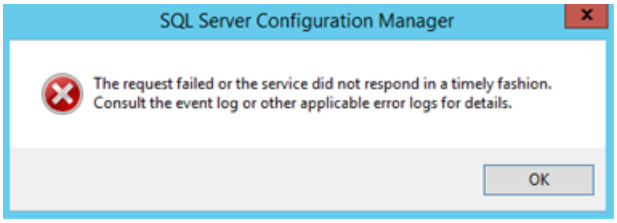
9. Click "OK". You get the warning message "Any changes made will be saved; however, they will not take effect until the service is stopped and restarted.".



10. You have to restart the service for the instance.
    Go to "SQL Server Services".

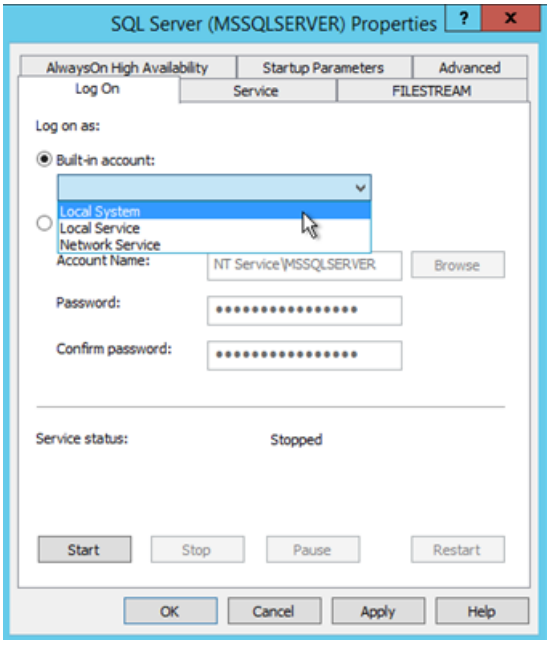


11. You will get an error message: "The request failed or the service did not respond in a timely fashion. Consult the event log or other applicable error logs for details.".



If the service cannot start, you have the following options:

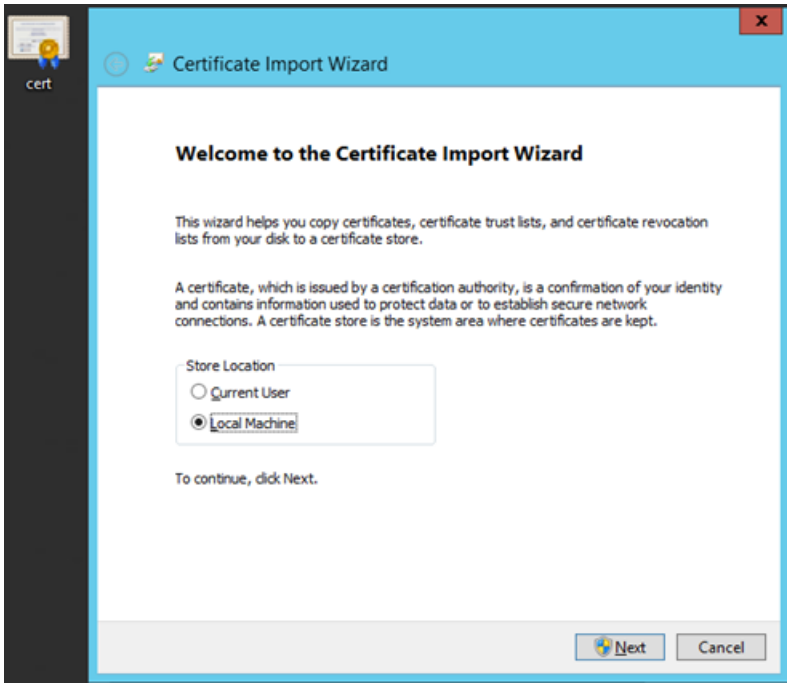
– Make sure, that it is running as a local admin (for example Local System)



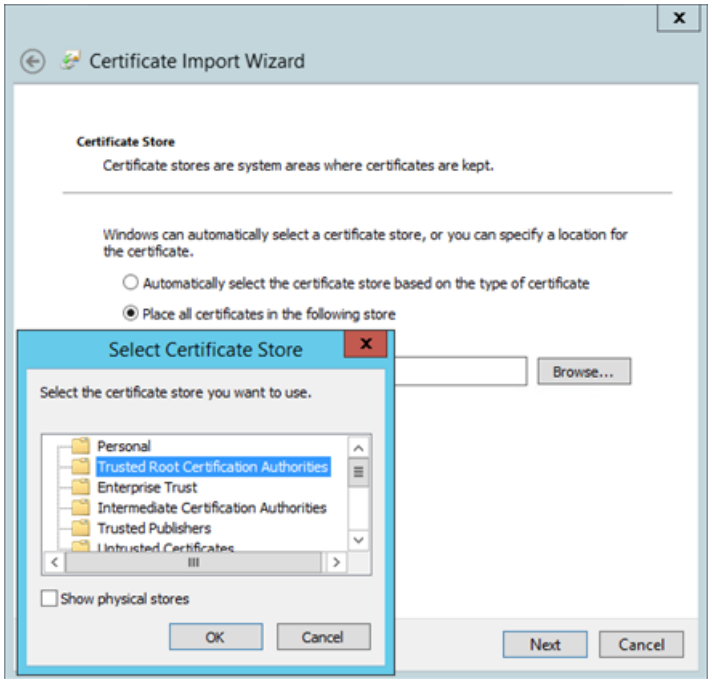
- OR -

– You can add the user to have access to these directories:
C:\Program Files\Microsoft SQL Server\MSSQL[version].[instance]\MSSQL\
C:\ProgramData\Microsoft\Crypto\RSA\MachineKeys
HKLM\System\CurrentControlSet\Services\WinSock2\Parameters

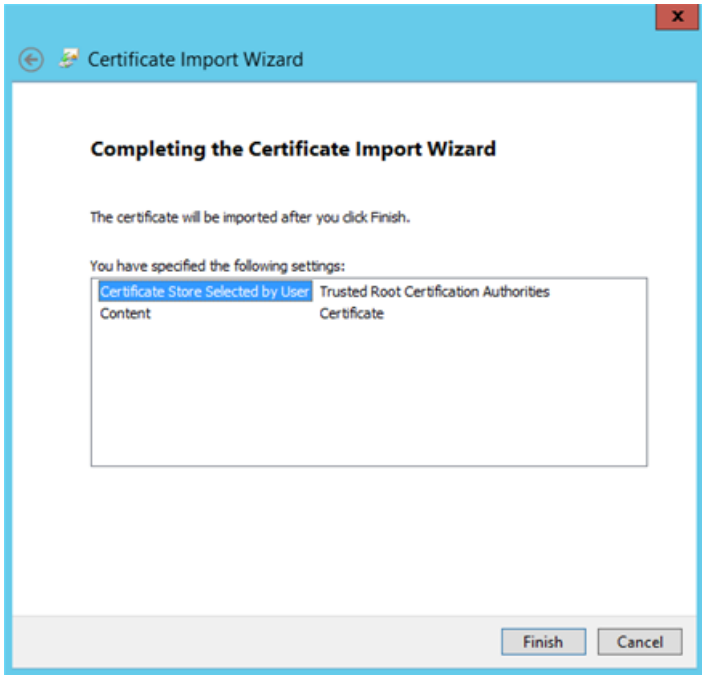
12. On the Mcenter server, double-click the certificate.
    Import the certificate for the "Local Machine".



13. Import the certificate in the “Trusted Root Certification Authorities” store.



14. Click "Finish".
    You can execute the Mcenter setup.

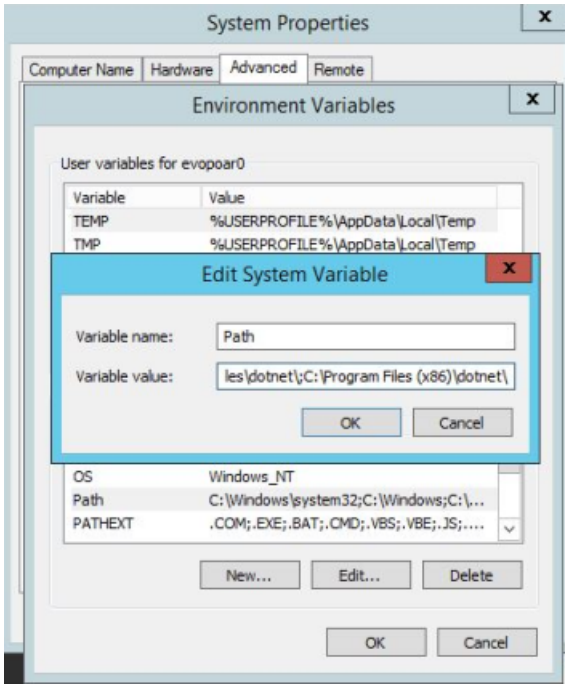


4.6 Further installations

Checking the "Path" variable

As the Mcenter server is only compatible with the x64 variant of the .NET runtime, check the order of the variable value of the variable "Path". Ensure that x64 still precedes x86 in the sequence.

1. Select "Advanced System Settings".
2. Open the "Advanced" tab.
   Open the "Environment Variables" window.
3. Click on the variable "Path".
   Open the "Edit System Variable" window.
4. Check the entries in the "Variable value:" field.
   The sequence must be as follows:
   C:\Program Files\dotnet\;C:\Program Files (x86)\dotnet\
5. To save the variable value, click "OK".



Note

Check the path variable

If on the application "Manage machines" it is impossible to create a machine you should check the path variable.

Analyze MyPerformance /OEE

Setting up and installation of "Java Runtime Environment (JRE) 8" and "Apache Tomcat 9.x" on the server:

1. Install "Java Runtime Environment 8" on the server.
   Download the desired Installer from the following links:
   - Zulu Java Runtime Environment 8 (https://www.azul.com/downloads/?version=java-8-lts&os=windows&architecture=x86-64-bit&package=jre)
     - OR -
   - Oracle Java Runtime Environment 8 (https://www.oracle.com/java/technologies/downloads/#jre8-windows)
2. Install Apache Tomcat 9.x on the server.
   Download the Installer from the following link:
   Apache Tomcat 9.x (https://tomcat.apache.org/download-90.cgi)
   Choose the Windows Service Installer.
3. Make sure that the "SQL Browser" service is running (can be checked in the Task Manager).

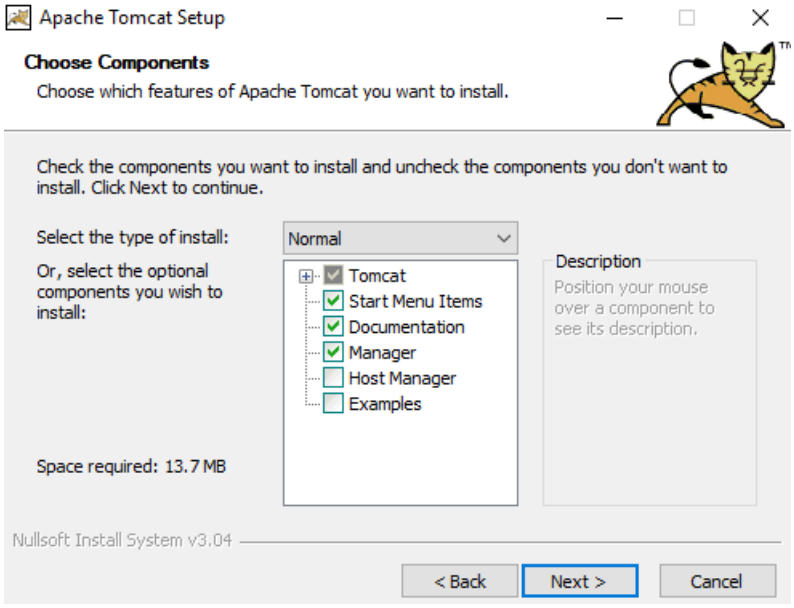
Settings from Apache Tomcat setup

Start the installation and follow the manufacturer's instructions.

To make all the functions of AMP /OEE available, make the following settings:

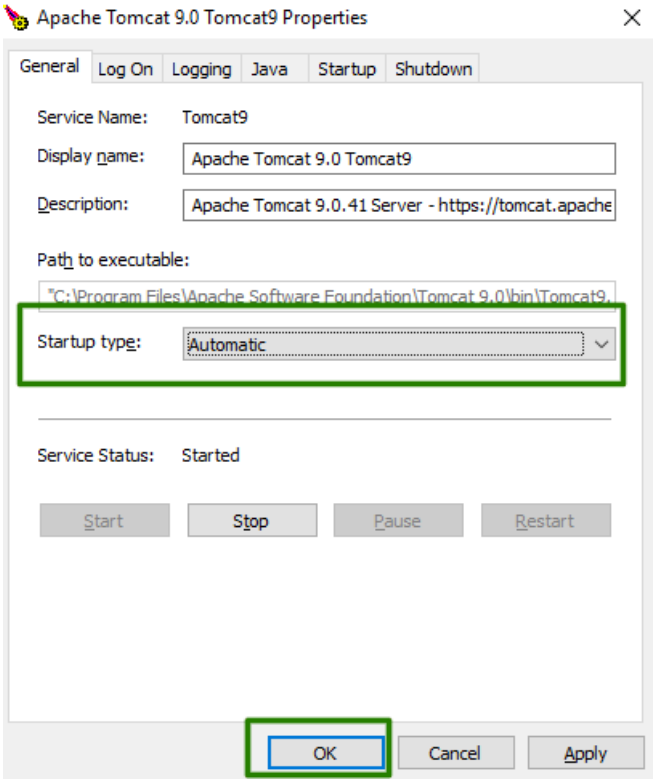
- In the "Choose Components" window, select the following optional components:
  - Start Menu Items
  - Documentation
  - Manager

  Click "Next >"



- Open the following folder: C:\Program Files\Apache Software Foundation\Tomcat 9.0\bin\
  - Open the "Tomcatxw.exe" > "Configure Tomcat".
  - Open the "General" tab and select the setting "Automatic" in the "Startup type" drop-down list.

  Click "OK".


Apache Tomcat 9.0 Tomcat9 Properties
General
Log On
Logging
Java
Startup
Shutdown
Service Name:
Tomcat9
Display name:
Apache Tomcat 9.0 Tomcat9
Description:
Apache Tomcat 9.0.41 Server - https://tomcat.apache
Path to executable:
"C:\Program Files\Apache Software Foundation\Tomcat 9.0\bin\Tomcat9.
Startup type:
Automatic
Service Status:
Started
Start
Stop
Pause
Restart
OK
Cancel
Apply

Setting up an encrypted connection before installation

5

5.1 Introduction

It is possible to set up an encrypted connection (HTTPS) on the server side before the installation.

This can also be done after the installation. However, it is recommended to do this before the installation, as it requires more steps afterwards.

5.2 Setting up an encrypted connection for IIS

For a secured communication (HTTPS) between a client and the server, you require a digital certificate that confirms the identity of the server.

Note

Certificate for the host name

In order to create a certificate for the host name instead of the IP address, enter the host name in the "IP address" input field.

An already created IIS website can be selected during the installation.

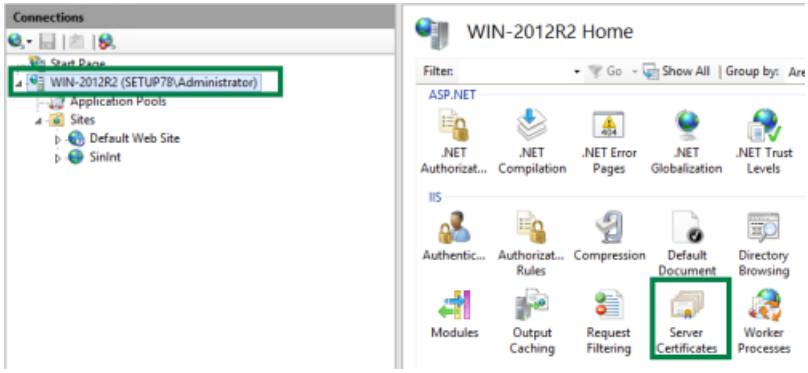
If this website is correctly configured for HTTPS communication there is no need to do additional settings regarding this matter after the installation.

Prerequisite

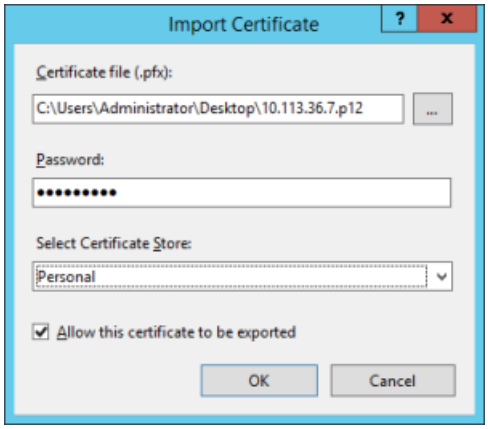
- You require a server certificate which meets these requirements:
  - The CN (Common Name) of the certificate corresponds to the address at which the server is to be reached.
  - The CN is also listed in the SAN (Subject Alternative Name) extension (depending on the type either as "DNS name" or as "IP address").
  - The certificate is created according to the “X509V3” standards, or has at least the "serverAuth" extended key usage property.

Procedure

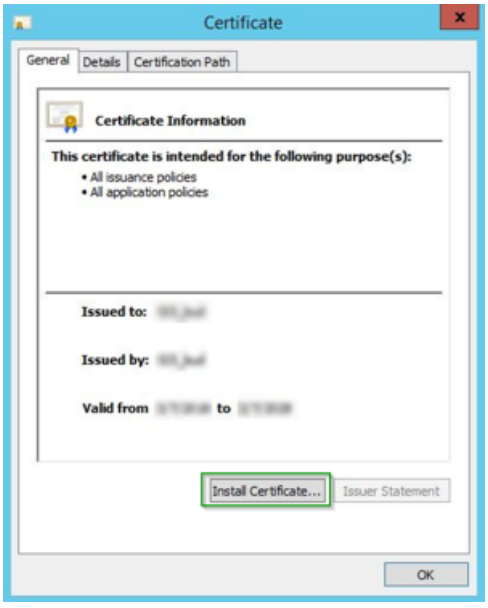
1. Import your server certificates according to IIS.
   - Start the Server Manager.
   - Select "Roles" in the "Web Server (IIS)" > "Internet Information Services (IIS) Manager" directory.
   - At "Connections", mark the server name and click "Server Certificates" in the "IIS" area.



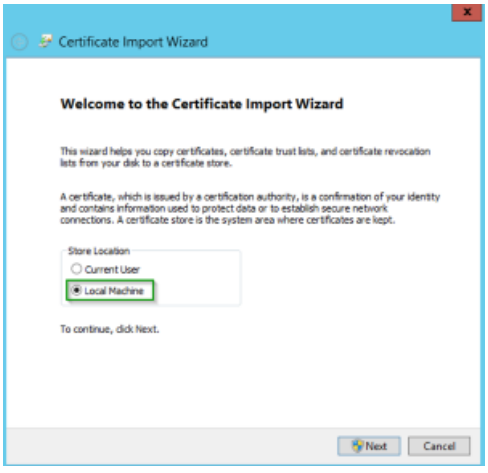
2. The "Server Certificates" window opens.
   Select "Import...".
3. The "Import Certificate" window opens.
   - In the "Certificate file (.pfx):" field, the directory is displayed.
   - Enter the password.
   - Select the desired Certificate Store from the "Select Certificate Store" drop-down list.
   - Activate the "Allow this certificate to be exported" checkbox.
   - Click "OK".



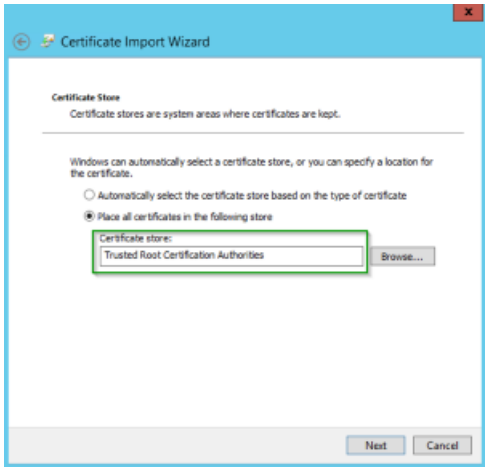
4. Add the Root certificate to "Trusted Root Certification Authorities store".
   - Double-click on the certificate, the Certificate information page will open.
   - Click on the "Install certificate" button.



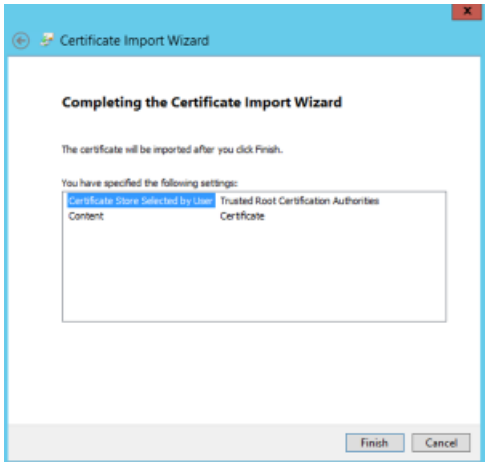
5. The "Welcome to the Certificate Import Wizard" window opens.
   Activate option field "Local Machine" and click "Next".



6. The "Certificate Store" window opens.
   - Activate option field "Place all certificates in the following store" .
   - Browse out "Trusted Root Certification Authorities".
   - Click "Next".



7. The "Completing the Certificate Import Wizard" window opens.
   - You see the specified settings.
   - Click "Finish".



8. Right-click on the required IIS page (default: SinInt) and select "Edit Bindings". If no suitable website is present, add a new website (right-click on "Sites" and select "Add Website..."). The "Site Bindings" window opens. The port settings are listed.
   Click "Add..."
   The "Add Site Binding" window opens.
   Make the required settings, e. g.:
   - Type: "https"
   - IP address: "<server ip address>" or "<host name>"
   - Port: 443
   - SSL certificate: Click "Select" to select the certificate.

Note

Application Pool

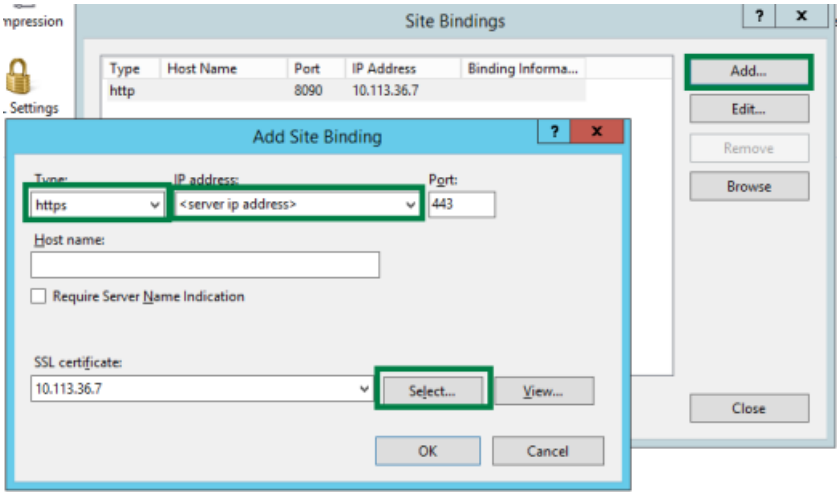
The Application Pool assigned to a new website must have "No Managed Code" set as ".NET CLR version".

Note

Require Server Name Indication

Do not activate the "Require Server Name Indication" checkbox. Otherwise communication problems may occur.

Click "OK".



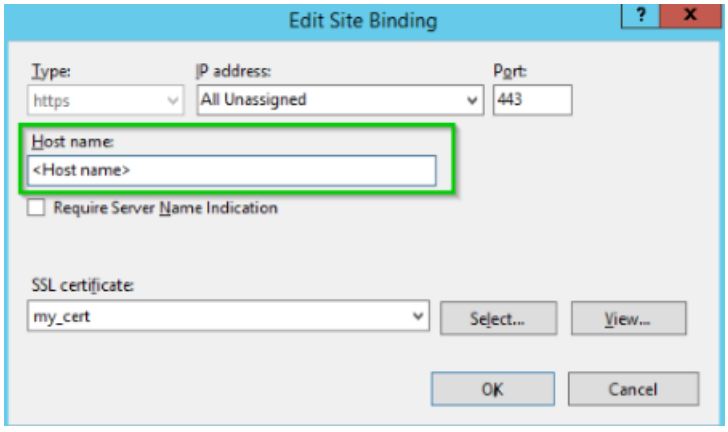
- OR-
If HTTPS is to be configured with the use of a DNS name (host name), open the "Site Bindings" window.

- Click "Edit...".
- The "Edit Site Binding" window opens
  Fill the "Host name" field in IIS.

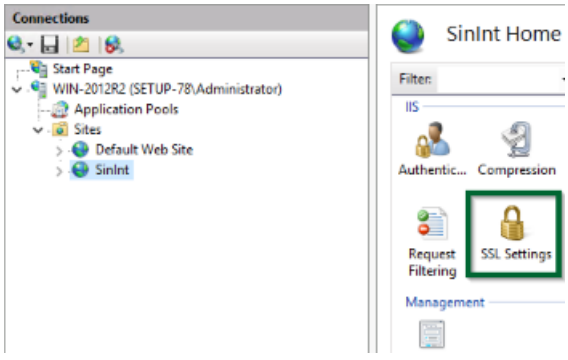
Note

Delete Type "HTTP"

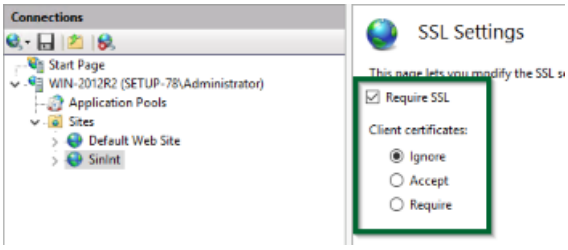
If you want to have just the HTTPS communication, you have to delete HTTP binding on the "Site Bindings" window.



9. Adapt the SSL settings for "SinInt" under the installed sites in IIS:
   – Select the application and click "SSL Settings".



   – The "SSL Settings" window opens:
   Activate the "Require SSL" checkbox.
   Click on "Apply" after it.
   Activate the "Ignore" option button at "Client certificates:".



10. Do an IIS reset.

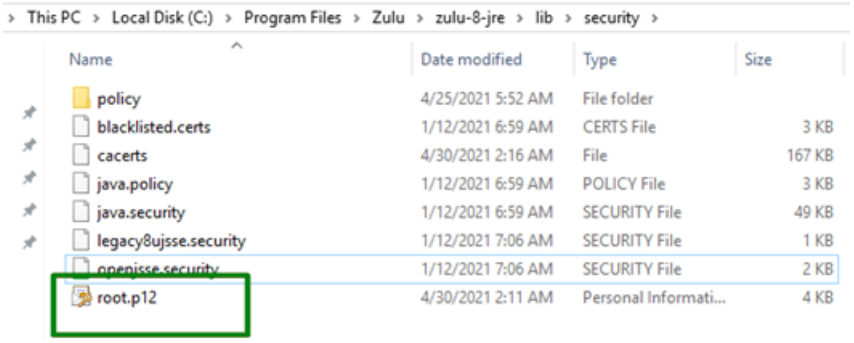
5.3 Setting up an encrypted connection for Tomcat

For a secured communication (HTTPS) between a client and the server, you require a digital certificate that confirms the identity of the server.

The AMP /OEE functionality uses Tomcat (not IIS) for web hosting. If you plan to install this functionality, you need to set up Tomcat for HTTPS.

Procedure

1. Copy your Root certificate to the following path: %JRE_PATH%\lib\security



2. Open “cmd”
   – Change directory to “%JRE_PATH%\lib\security”.

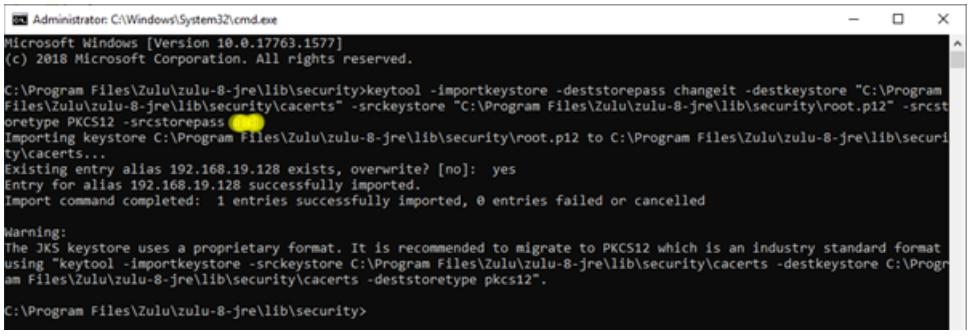
3. Run the following command:
   `keytool -importkeystore -deststorepass changeit -destkeystore "%JRE_PATH%\lib\security\cacerts" -srckeystore "%JRE_PATH%\lib\security\<rootCertificate.p12>" -srcstoretype PKCS12 -srcstorepass <rootCertificatePassword>`
   - Replace `%JRE_PATH%` with installed JRE folder path on your PC, that is `C:\Program Files\Zulu\zulu-8-jre`
   - Replace `<rootCertificate.p12>` with your root certificate name.
   - Replace `<rootCertificatePassword>` with your root certificate password.

Note

Default password

The default java keystore password is `changeit`.

If you set another password for keystore, please use it in above command instead of `changeit`.

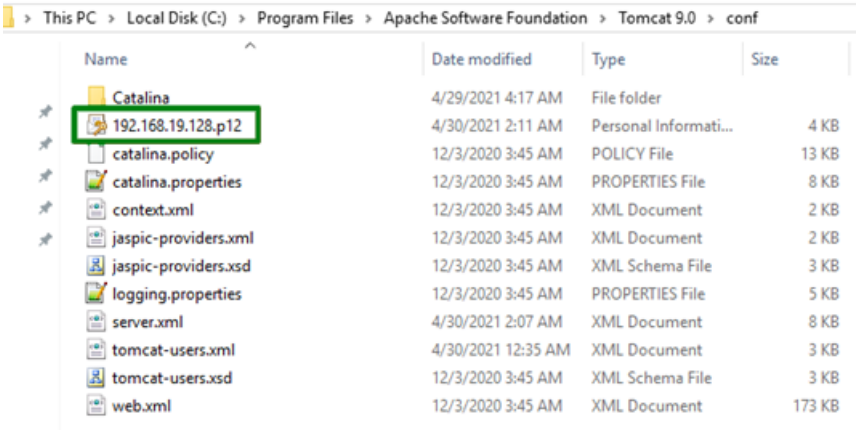


Note

Remote database

Steps 1 to 3 are only necessary if you use a remote database.

4. Copy your personal certificate to "C:\Program Files\Apache Software Foundation\Tomcat 9.0\conf".



Note

Personal certificate

The "personal certificate" is the certificate of the Mcenter server.

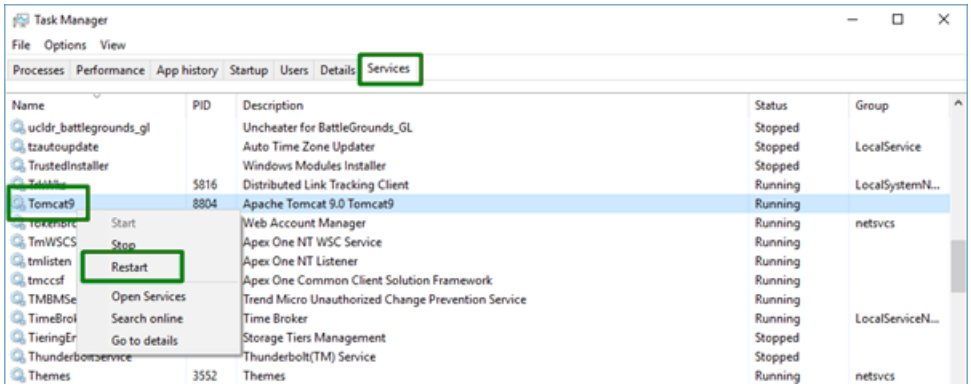
5. Add the connector in the below to server.xml under “C:\Program Files\Apache Software Foundation\Tomcat 9.0\conf” for HTTPS connection:

```
<Connector name="Secure" port="8443" scheme="https" secure="true"
SSLEnabled="true"
protocol="org.apache.coyote.http11.Http11NioProtocol"
maxHttpHeaderSize="65536">
  <SSLHostConfig sslProtocol="TLS">
  <Certificate certificateKeystoreFile="conf/
<yourCertificateName>.p12"
certificateKeystorePassword="<certificatePassword>" clientAuth="false"/>
  </SSLHostConfig>
  </Connector>
```

6. Remove the connector for HTTP in server.xml.

```
<Connector port="8080" protocol="HTTP/1.1" connectionTimeout="20000" redirectPort="8443" maxHttpHeaderSize="65536" />
```

7. Open the Task Manager.
   - Open the "Services" tab.
   - Restart the Tomcat9 server.



Installing/uninstalling/modifying the Mcenter server

6

6.1 Overview

Prerequisites

The following conditions must be fulfilled:

- The license server must be available and configured.
  For more information, see Set license server (Page 84).
- The additional Windows services are set. The SQL Server is installed.
  For more information, see Installing/configuring Windows services (Page 35).
- You require administrator rights (for Windows or SQL user) to perform the installation.
  - OR -
  You can use predefined SQL databases.
- Make sure that you have more than 4 GB free space on the system drive.
  - OR -
  In case of a custom installation you need more than 2 GB free space on system drive and 2 GB free space on the target drive.
- If you are operating and installing a virtual machine on a PC running the "Windows 10" operating system, then turn off "Airplane mode".
- Make sure that the SQL Database instance does not contain any Mcenter or SINUMERIK Integrate 5 data from a previous installation or a previous version. If there are databases or tables from previous installation, the setup might finish successfully, but the system does not work properly.
- Check the state of "Force Encryption" in "SQL Server Configuration Manager" for your SQL instance. Make sure that it is "disabled" if you have no certificate configured for your SQL instance.

Optimize MyProgramming /NX-Cam Editor

- The NX CAM server is installed and ready for operation.
  If you have any further questions, please contact NX CAM Support at: NX /CAM support (https://www.plm.automation.siemens.com/global/de/support/).

Analyze MyPerformance /OEE

- Java Runtime
- Tomcat

Procedure

Perform the following steps:

1. Launch the server setup.
2. Select the installation language.
3. Select the setup type:
   – Select "Complete", all applications are installed.
   - OR -
   – Select "Custom", choose which applications you want installed and where they are installed (Platform is mandatory).

   For more information, see Installing the server setup (Page 85).
4. Accept the license agreement.
5. Set the accessibility of the license server.
6. Set the accessibility of the database.
7. Setup the administrator password.
8. Start the installation.
9. Complete the installation. Copy the consul token to clipboard.

6.2 Set license server

Prerequisite

- Install the "Siemens PLM License Server" on a separate server.
- Ensure that the necessary ports in your firewall are open on the web server and the license server.

Note

Only for test purpose

For testing purpose it is possible to install the License Server on the same Server where the Mcenter Server.

Port settings

To ensure that the license server communicates with the Mcenter server, you need the following 2 port settings:

- Server Port (standard is 28000): You need this port to perform the setup.
  For more information, see Installing the server setup (Page 85).
- Vendor Port (standard is 28001): You can configure this port freely.
  Information on this can be found in the following directory: SI5\Third-party\Siemens PLM \Documentation\SPLMLicensing_user_guide.pdf and fnp_LicAdmin.pdf

Note

Web server

If you exchange license files on the web server, you must perform an IIS reset.

Additional information

The "SPLMLicenseServer-Setup" can be found in the software package at:
SI5\Third-party\Siemens PLM\SPLMLicenseServer_v11.0.0_win_setup.exe

A description of the installation can be found in the software package at:
SI5\Third-party\Siemens PLM\Documentation\SPLM_Licensing_Install.pdf

6.3 Installing the server setup

Prerequisite

- You need more than 4 GB free space on the system drive.
  - OR -
- In case of custom installation you need 2 GB free space on system drive and 2 GB free space on the target drive.
- The user <Admin> creates himself/herself a new user account and sets the roles "Administrator", "Key user".
  Additional information on managing users are available in the following manuals:
  - Operating Manual Manage MyResources
  - Operating Manual Optimize MyProgramming /NX-Cam Editor
  - Operating Manual Analyze MyPerformance /OEE

Procedure

Starting the installation

1. Open the "SI5\Server" installation directory.
2. Start the "Setup.exe" setup file with a double-click.

3. "Mcenter" opens.
   Select the installation language.
   This language selection is binding only for the installation.
   The following languages are listed:

   – German

   – English

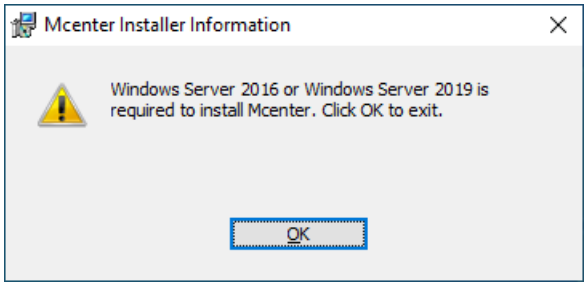
   Click "OK" to confirm the selection.

Note

Windows Server 2016 or 2019 required

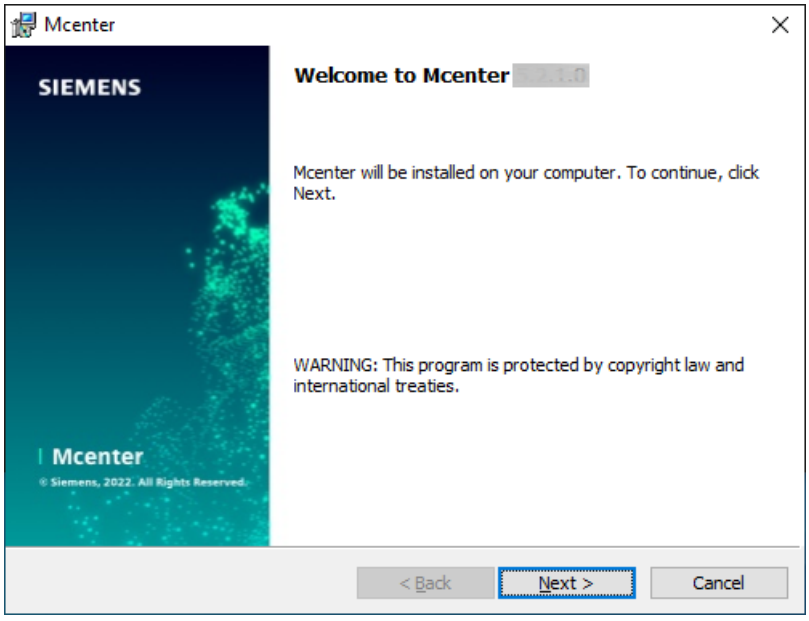
If you do not install the permitted server, you receive a note that the installation can only be performed on a Windows Server 2016 or 2019: "Windows Server 2016 or Windows Server 2019 is required to install Mcenter. Click OK to exit."

Confirm the note with "OK".
The setup is canceled.



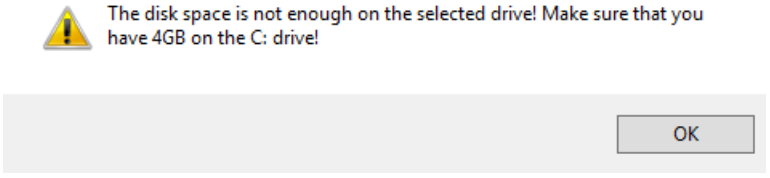
Install the required server version and restart the setup.

4. The "Welcome to Mcenter xx" window opens.
   Click "Next >" to start the installation preparation.



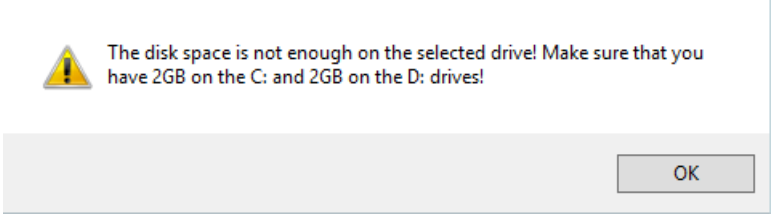
5. The "Setup Type" window opens.

   – Activate the "Complete" option button. Make sure that you have 4 GB free space on the selected drive.
   If there is not enough disk space on the system drive, you get the following error message: "The disk space is not enough on the selected drive! Make sure that you have 4GB on the C: drive!"

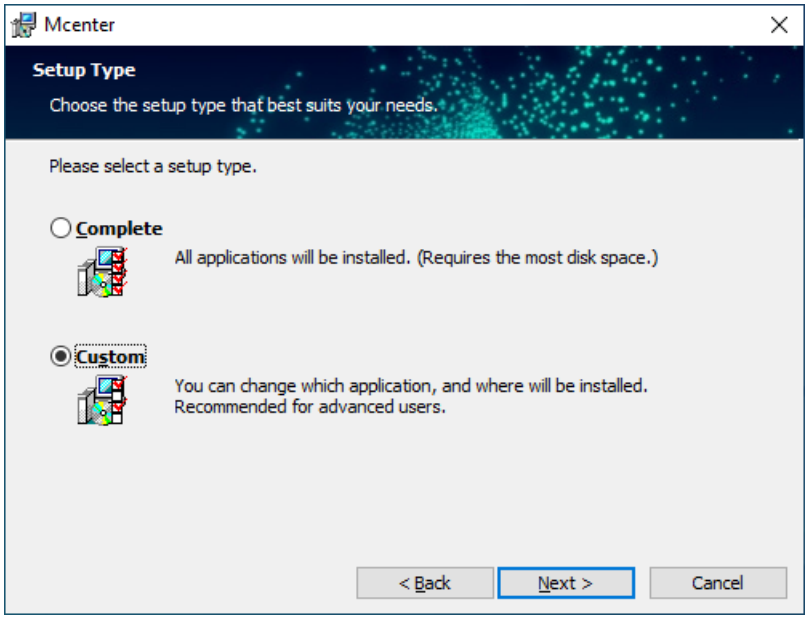


   - OR -

   – Activate the "Custom" option button. Make sure that you have 2 GB free space on the system drive and 2 GB free space on the target drive.
   If there is not enough disk space on the selected drive, you get the following error message: "The disk space is not enough on the selected drive! make sure that you have 2GB on the C: and 2GB on the D: drives!"

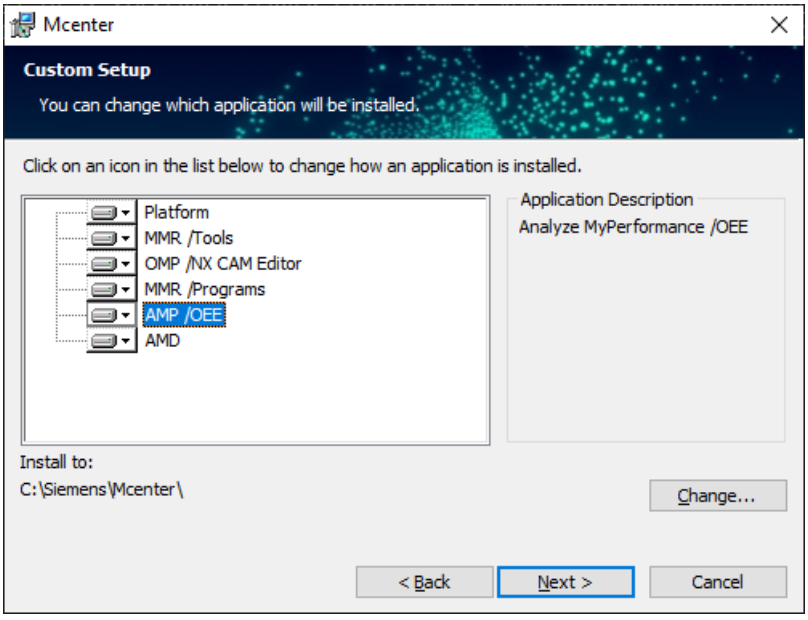


   Click "Next >".

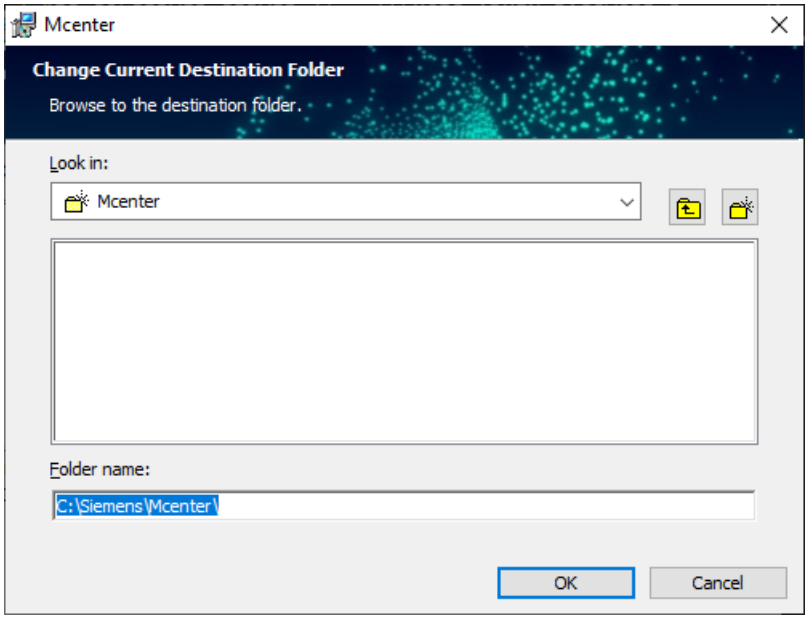

Mcenter
Setup Type
Choose the setup type that best suits your needs.
Please select a setup type.
Complete
All applications will be installed. (Requires the most disk space.)
Custom
You can change which application, and where will be installed.
Recommended for advanced users.
< Back
Next >
Cancel

Configuration

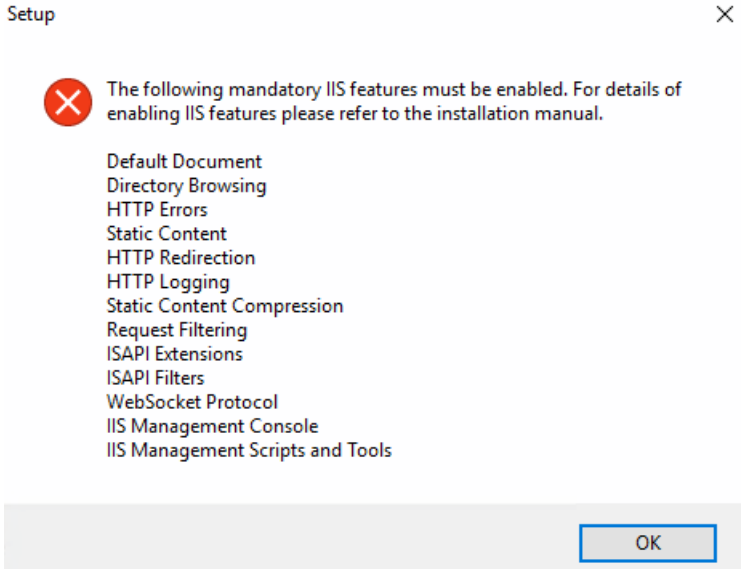
1. This step is only relevant for the "Custom Setup". The "Custom Setup" window opens. You can deselect the applications that should not be installed on your system:
   - Platform: No deselection possible, always installed.
   - Applications: Each can be deselected if not needed.
   - "Install to:"
     Shows the installation directory (for example: C:\Siemens\Mcenter\).
     If you want to specify a different directory, click "Change...".



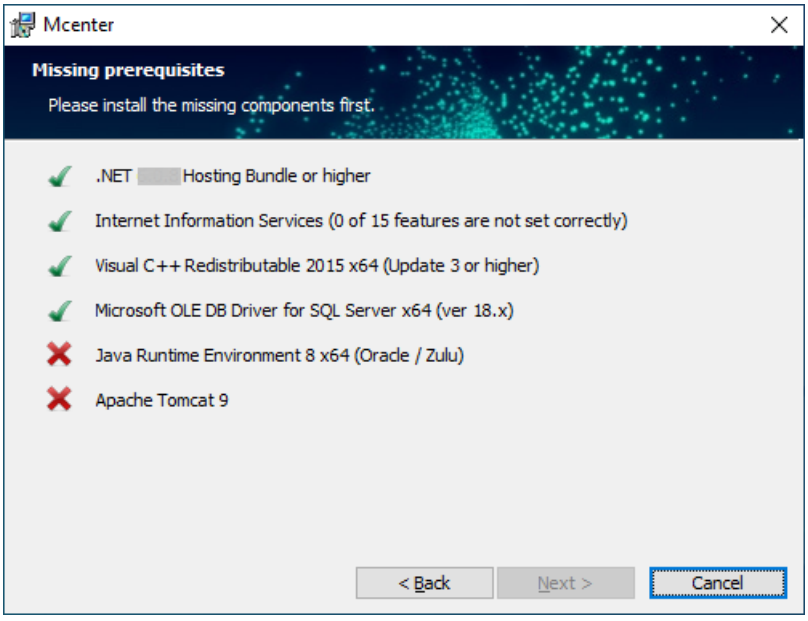
   - The "Change Current Destination Folder" window opens.
     Select the directory in the "Look in" selection box with the symbol.
     Enter a name in the "Folder name:" input field.
     To save the new folder, click "OK".
     - OR -
     To discard the input, click "Cancel".



2. Click "Next >" in the "Setup type" window.
   - OR -
   Following error messages are displayed about IIS feature:
   – An IIS feature is not activated
     - OR -
   – An IIS feature must be deactivated



   For more information, see Setting up Internet Information Services (Page 35).
   - OR -
   If you have not installed all of the Windows functions, the "Missing prerequisites" window opens. You are provided a view of the missing components.
   The grayed out prerequisites are not required for your current selected application that is installed.

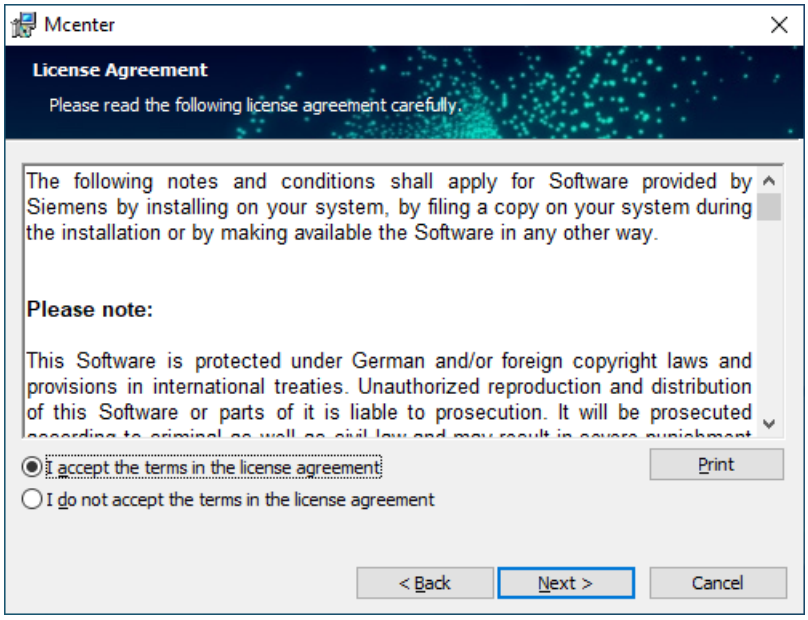


For a list of all required components, see System prerequisites (Page 18).

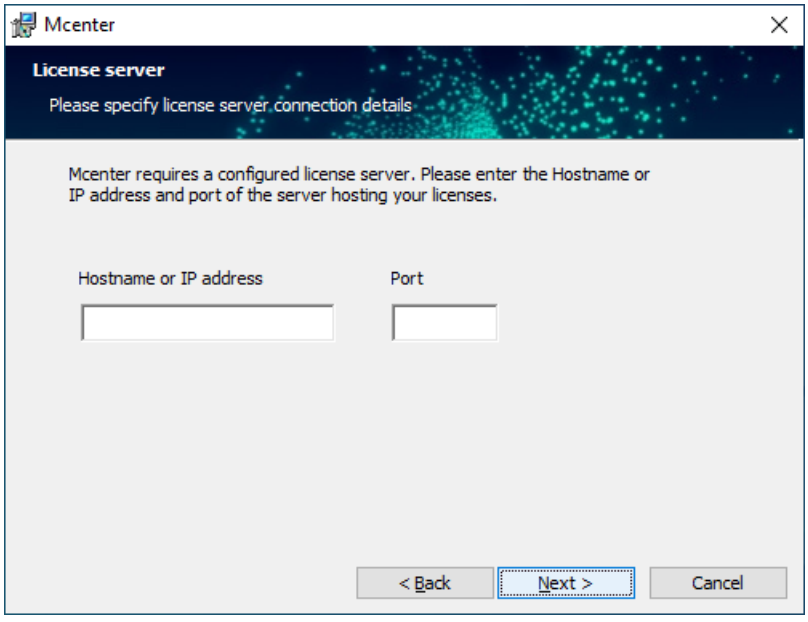
– Click "Cancel" to cancel the server setup.
  Install and configure any missing components.
  - OR -
  Click "< Back" to return to the previous window.
– Then start the server setup again.

3. If you have not set up all Windows functions, an error message is issued stating, for example, the functions which have to be activated.
   For the functions to be activated, see Setting up Internet Information Services (Page 35).
   Click "OK" to activate the function.

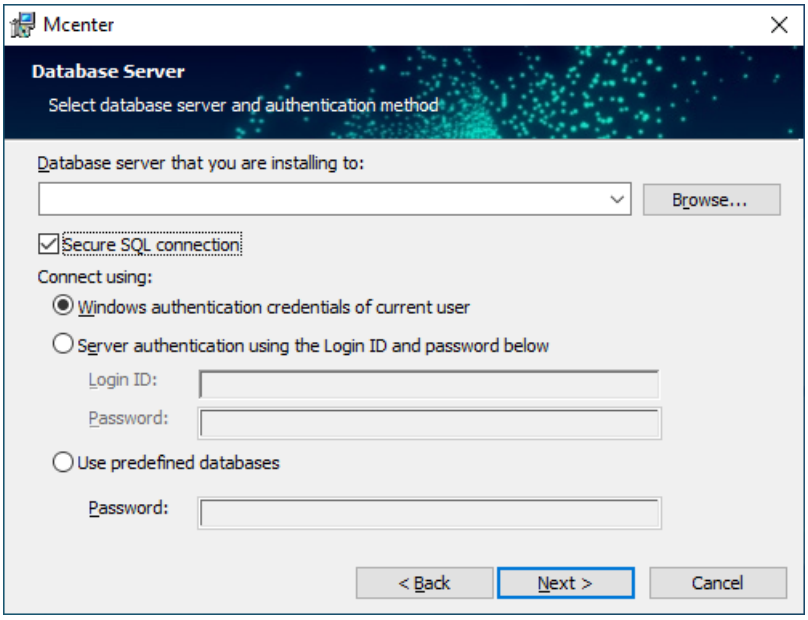
4. The "License Agreement" window opens.
   Read the license agreement.
   - If you want to print the terms, click "Print".
   - Then activate the "I accept the terms in the license agreement" option button and click "Next >".



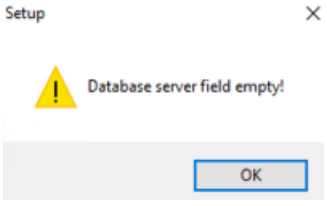
5. The "License server" window opens.
   Enter the data of the license server in the "Hostname or IP address" and "Port" input fields.
   Click "Next >".
   If you enter invalid addresses, you receive a corresponding error message.



6. The "Database Server" window opens.
   All data from Mcenter use a common database. Some tables of this database, for example the user administration and plant hierarchy tables, are used by all applications.
   The SQL database must be installed.



   – Database server that you are installing to:
     Select the SQL instance for installation.
     The value can be entered in the form of *<IP address/hostname>\<instance name>*
     - OR -
     Can be browsed.
     - OR -
     Selected from the drop-down list.
     Note:
     You get an error message if this field is empty: "Database server field empty".



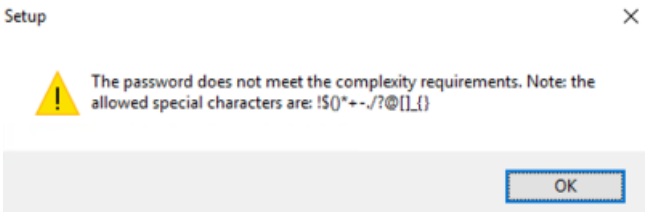
– Connect using via the following three options:
  Select the "Windows authentication of the current user" connection.
  - OR -
  Activate the "Server authentication using the login ID and password below" option button.
  Enter the login ID of any SQL user with system administrator rights.
  - OR -
  Select the "Use predefined databases" option button.
  With this option it is possible to use databases created manually prior installation. In this case the setup does not create additional databases.
  Make sure that all the required databases and login operator are created.
  For more information, see Create databases and user in SQL Server (Page 52).

Note

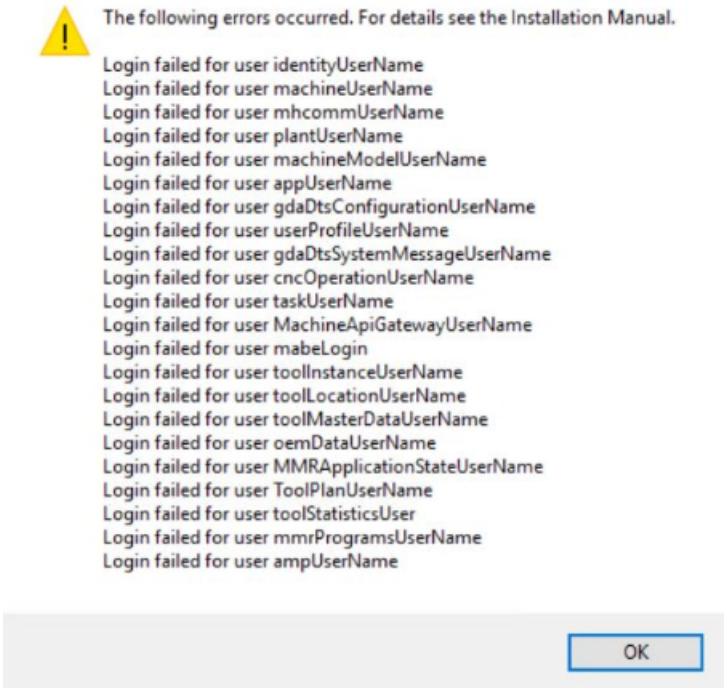
Complexity requirements for a password

Make sure that you use these special characters. Otherwise the setup does not accept the password.

- Minimum 8 characters
- Must contain upper- and lowercase letter
- Number and special character. Only use these special characters: ! $ ( ) * + - . / ? @ [ ] _ { }



– If a connection to predefined databases could not be established, an error message appears with a list of these databases.
Example:



– By clicking "Next", the setup verifies whether a connection can be established to the predefined databases with the provided password.
The checkbox for the "Secure SQL connection" allows the setup to set up an encrypted communication between the database server and the Mcenter server.

Note

"Secure SQL connection" checkbox

If you try to use "(local)\instance" with an activated "Secure SQL connection" checkbox as the SQL server path you get an error message.

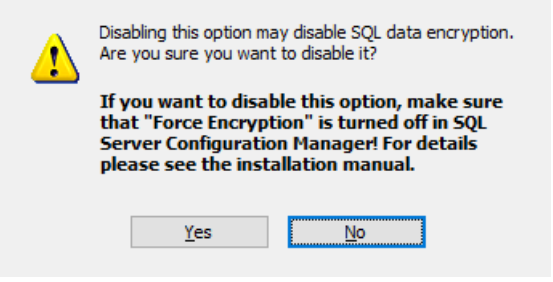
If the machine has a long DNS name also, the self-signed certificate must contain the long DNS machine name for example "machine.networkname.net". You must change the DB Server address to "machine.networkname.net\<instance>".

For more information, see Setting up the encrypted communication for SQL Server (Page 59).
If the checkbox "Secure SQL connection" is deactivated, a warning appears: "Disabling this option may disable SQL data encryption. Are you sure you want to disable it?"

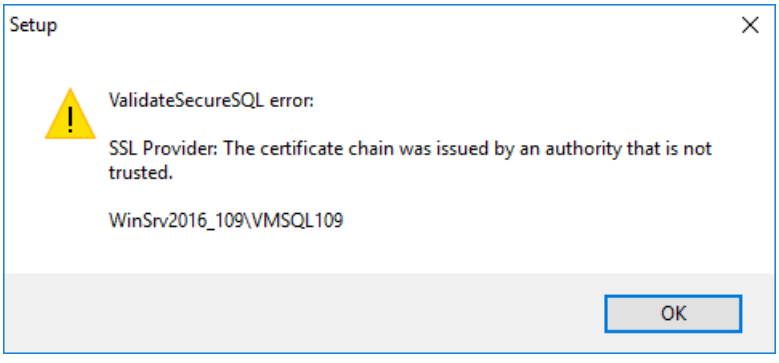
Note

Disable SQL data encryption

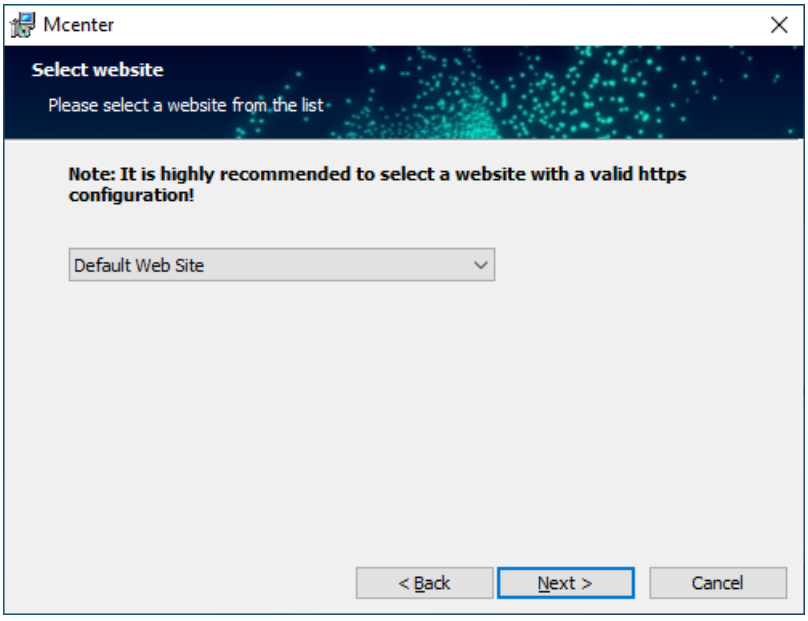
If "Force Encryption" is turned on in the SQL Configuration Manager without a valid certificate for the SQL instance, the installation fails.
You must turn off "Force Encryption" if you have not added a certificate to the SQL instance. You get a warning: "If you want to disable this option, make sure that "Force Encryption" is turned off in SQL Server Configuration Manager!"



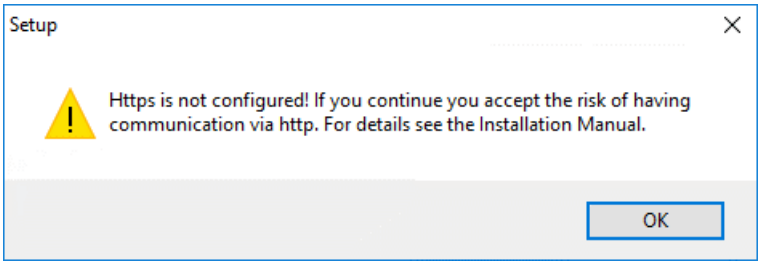
If the certificate is not imported correctly you get the following error message: "ValidateSecureSQL error: SSL Provider: The certificate chain was issued by an authority that is not trusted."



7. In the "Select website" window you can select the website that he wants to install the Mcenter Server websites
   - In the dropdown menu all of the existing Websites are listed from IIS for example: "Default Web Site".
   - If you choose one of these websites, the setup tries to install with https settings if it is configured previously.
     Note:
     It is recommended that you use a website which has https settings.
     For more information, see Setting up the encrypted communication for SQL Server (Page 59).



   - If https is not configured you get an error message: "Https is not configured! If you continue you accept the risk of having communication via http. For details see the Installation Manual."



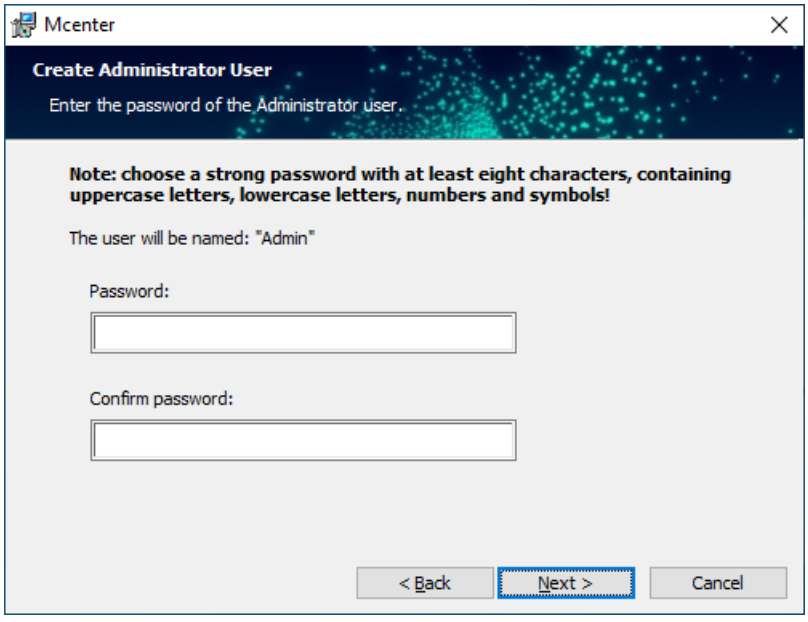
8. The "Create Administrator User" window opens. The username is "Admin".
   After the setup has successfully installed Mcenter, you are able to log in with this user.
   – Enter a strong password in the "Password:" input field.
   – Repeat the password in the "Confirm the password:" input field.

   Note

   Properties of a strong password

   - Use at least 8 characters.
   - Combine uppercase and lowercase letters and special characters and numbers, for example M?a!%+5).
   - Make sure that the password is not listed in dictionaries.
   - Do not use any common variants and repetition or keyboard patterns, for example asdfgh - OR - 1234 abcd.
   - Do not simply append a simple password with numerals or common special characters such as $!?# to the end or beginning.
   - Do not use the same password for several user accounts.

   – Click "Next >".

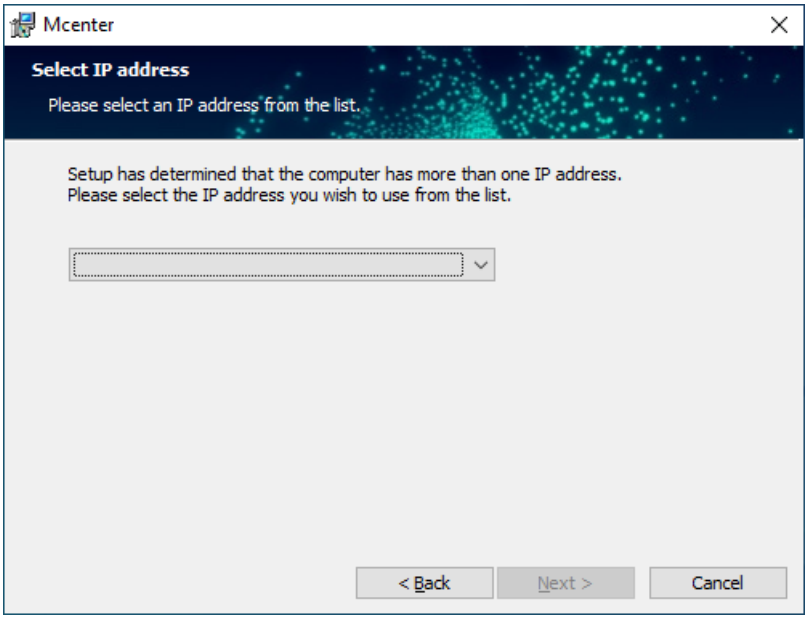


9. If several IP addresses are configured on your computer, the "Select IP address" window opens.
   Open the drop-down list and select the required IP address.

   Note

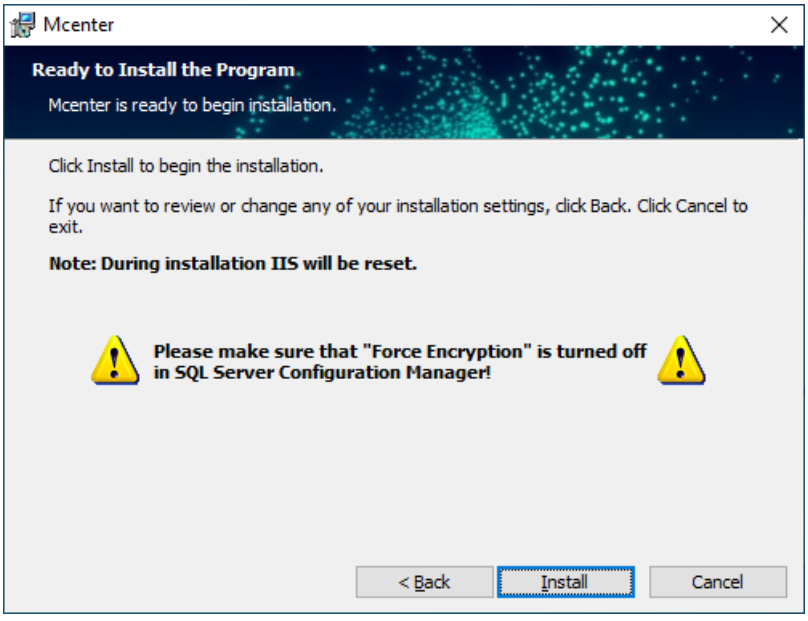
   Selecting the IP address

   The installation is only continued after you have selected the IP address.



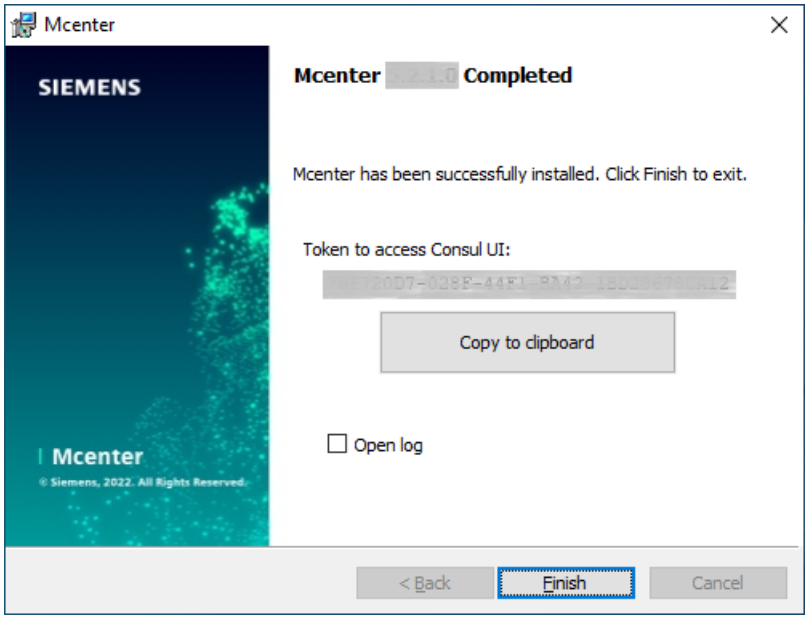
Complete installation

1. The "Ready to Install the Program" window opens.
   To cancel the installation after a prompt, click "Cancel".
   - OR -
   To start the installation, click "Install".



2. The installation is started. The progress is displayed on a progress bar.

3. The "Mcenter.x Completed" window opens.
   A message is displayed showing that the installation was successful.
   A token is generated during the installation for access to the "Consul" software.
   - Click on the "Copy to clipboard" button to copy the token directly to the clipboard.
     - OR -
     If you need the token at some later date, find the file in the following directory: "C:\Siemens\SINUMERIK_Integrate_5\Consul\encrypt.json".
     You require administrator rights to open the token.
   - Activate the "Open log" checkbox to open the log files.
   - Then click on "Finish" to complete the installation and to view the log files, if applicable.
     If the log file has been created in the installation directory, the file opens.
     If the log file was not created in the installation directory, the current log file MSI Log opens.
     For more information about log files, see Log files (Page 123).



4. After the installation has been completed, a restart is recommended.

After the installation, set up the encrypted connection.

For more information, see Certificate on the server (Page 125).

6.4 Installing the server update

Prerequisite

- You need more than 4 GB free space on the system drive.
  - OR -
  In case of custom installation you need 2 GB free space on the system drive and 2 GB free space on the target drive.
- Various errors can occur during an update, some of which cannot be undone and damage your database.
  In this case, restore the backed up data.

Note

Creating backup

Before starting the server update, generate a snapshot of your virtual machine, and then backup all data and configurations.

The backup must include all elements of Mcenter, such as

- Database
- IIS configuration
- License server
- Applications

Note

Reconnect is not necessary

After an Mcenter Server update, you do not have to reconnect the SINUMERIK controller.

Note

Machine model database is cleared

During server update the contents of machine model database is cleared. The machines upload their machine models again when they update their infrastructure scripts. Some features are not available until the machine models are available again (like assigning applications)

- Mcenter uses the Microsoft Windows technology for the setup. During the Mcenter installation, Microsoft Windows saves the information and the files in the Windows Installer directory. This information is necessary to carry out an Mcenter update.
  Do not make any manual changes in the Windows Installer directory.

Procedure

Preparation

1. Create a snapshot of the virtual machine.
2. Create a backup of the system.
3. Stop communication to the web server, for example
   – Open the command line and start the following command: `iisreset /stop`

4. When you install into predefined SQL databases, create the necessary databases with the corresponding users.

   Note

   Database structure and SQL user

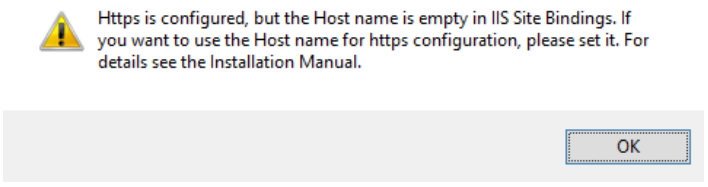
   - Use the database instance created on SQL server and the user in any instance.
     For more information, see Create databases and user in SQL Server (Page 52).
   - Set the appropriate password for each user.
     Also set the password for each database.
     Enter a "strong" password.
   - The setup verifies the settings during installation.
     Additional information is provided on the "Database Server" window below.

5. Consider a secure SQL connection:
   During the update you can activate the secure communication between the SQL server and the Mcenter server. For this secure communication you need a certificate on the SQL server. This change cannot be deactivated.
   For more information, see Setting up the encrypted communication for SQL Server (Page 59).
6. Check whether the latest version is installed.
   - SQL server: System prerequisites (Page 18)
   - .NET: Further installations (Page 68)
     If you reinstall .NET, stop communication with the web server following installation, see point 3. Then restart the operating system.
   - Check the IIS settings to see whether the "IIS Management Scripts and Tools" setting is activated: Setting up Internet Information Services (Page 35)
7. Check the state of "Force Encryption" in "SQL Server Configuration Manager" for your SQL instance. Make sure that it is "disabled" if you have no certificate configured for your SQL instance.
8. Open the "SI5\Server" installation directory.
9. Start the "Setup.exe" setup file with a double-click.
   Make sure that you have more than 4 GB free space on the system drive.
   - OR -
   In case of a custom installation, make sure that you have 2 GB on the system drive and 2 GB free space on the target drive.

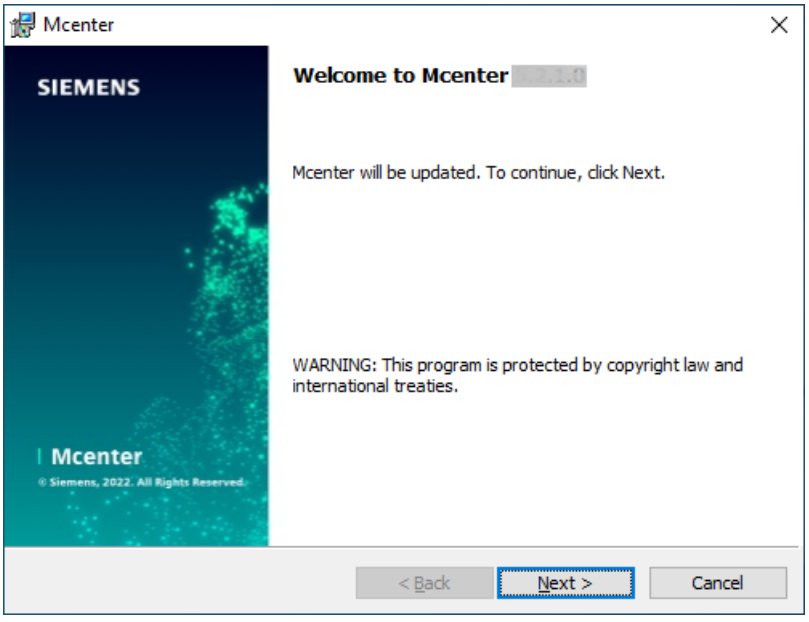
Starting the update

1. Mcenter installation starts.
   Select the installation language.
   This language selection is binding only for the installation.
   The following languages are listed:
   - German
   - English

   Click "OK" to confirm the selection.
2. After initiating an update, if HTTPS is enabled, but the host name is not entered in IIS, the following warning appears right after running the setup: "Https is configured, but the Host name is empty in IIS Site Bindings. If you want to use the Host name for https configuration, please set it."
   This warning can be disregarded and the update process can be continued if HTTPS needs to be configured with the IP address of the server.

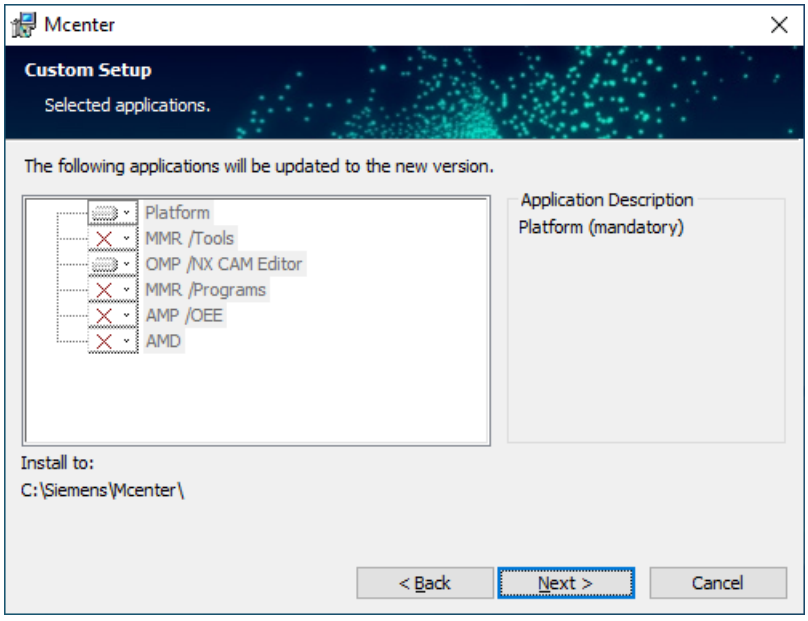


   For more information about the "Add Site Binding" window, see Certificate on the server (Page 125).
3. The welcome screen opens.
   Click "Next >" to start the installation preparation.

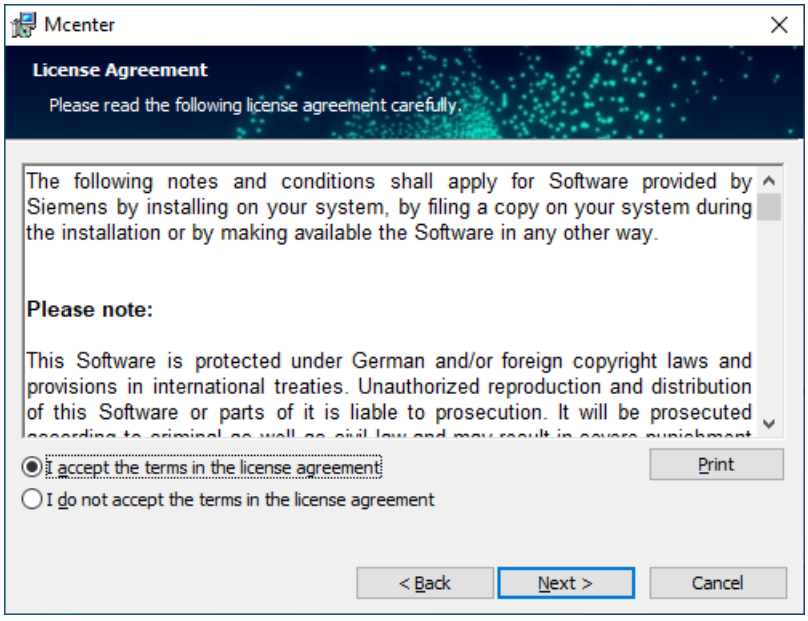


4. The "Custom Setup" window opens.
   No selection can be made, but you are shown the following information:
   - The functions which are updated. Only functions currently installed can be updated.
   - Shows the installation directory

   Click "Next >".



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" option button and click "Next >".

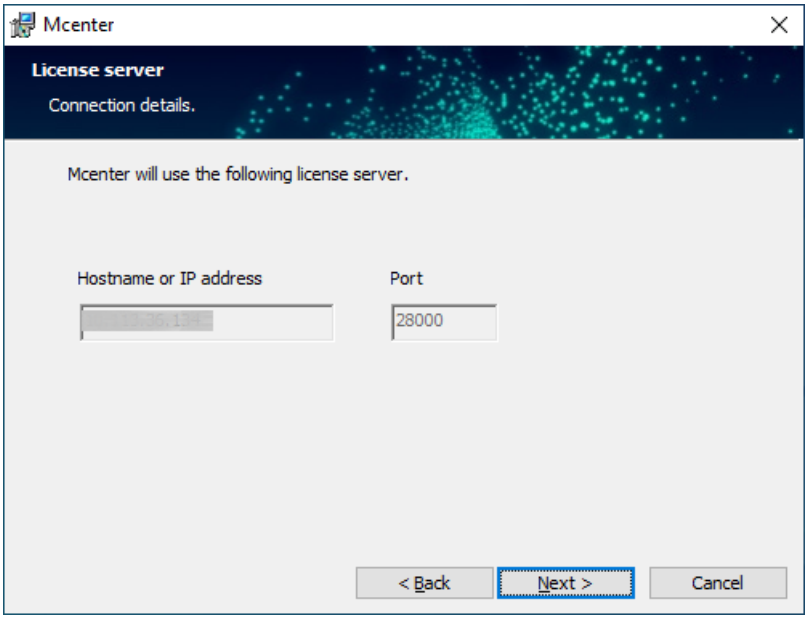


6. The "License server" window opens.
   The "Hostname or IP address" and the set "Port" of the license server are shown. You cannot change them in the dialog.
   Click "Next >".

Note

Changing IP address or port

If changing the values is mandatory before the update, please change it manually in the registry under HKLM\SOFTWARE\WOW6432Node\Siemens\MCIS\SINUMERIK_Integrate_5 - "License_IP" and "License_Port".



7. The "Database Server" window opens.
   You have the option to change the connection string during an update, but you cannot switch to another SQL database.

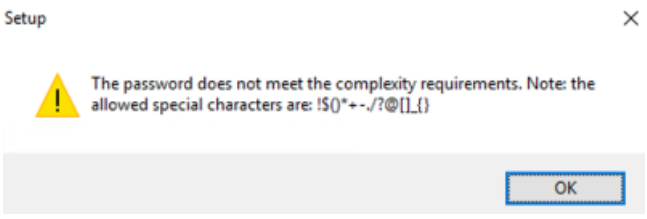
– Connect using via the following three options:
  Select the "Windows authentication of the current user" connection.
  - OR -
  Activate the "Server authentication using the login ID and password below" option button.
  Enter the login ID of any SQL user with system administrator rights.
  - OR -
  Select the "Use predefined databases" option button.
  With this option it is possible to use databases created manually prior installation. The setup does not create additional databases.
  Make sure that all the required databases and login users are created.
  For more information, see Create databases and user in SQL Server (Page 52).

Note

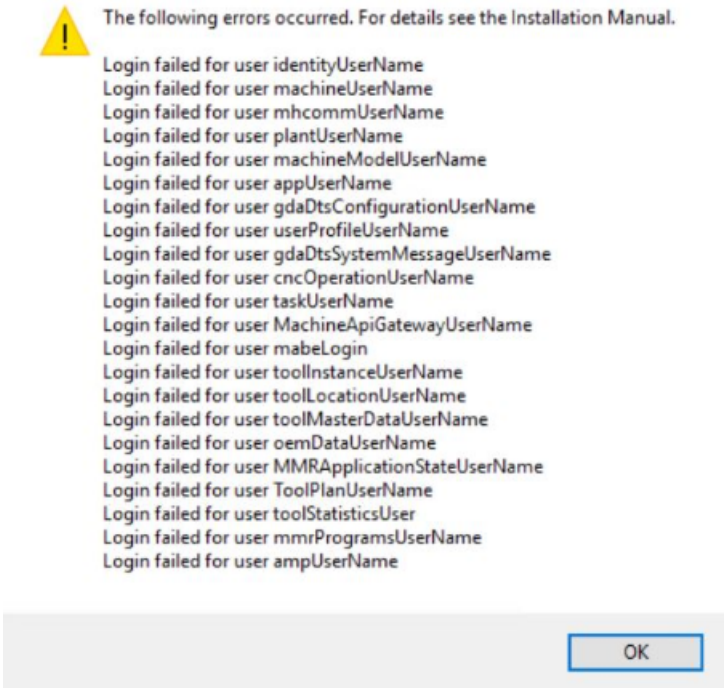
Complexity requirements for a password

Make sure that you use these special characters otherwise the setup does not accept the password!

- Minimum 8 characters
- Must contain upper- and lowercase letter
- Number and special character. Only use these special characters: ! $ ( ) * + - . / ? @ [ ] _ { }



– If a connection to predefined databases could not be established, an error message appears with a list of these databases.
Example:



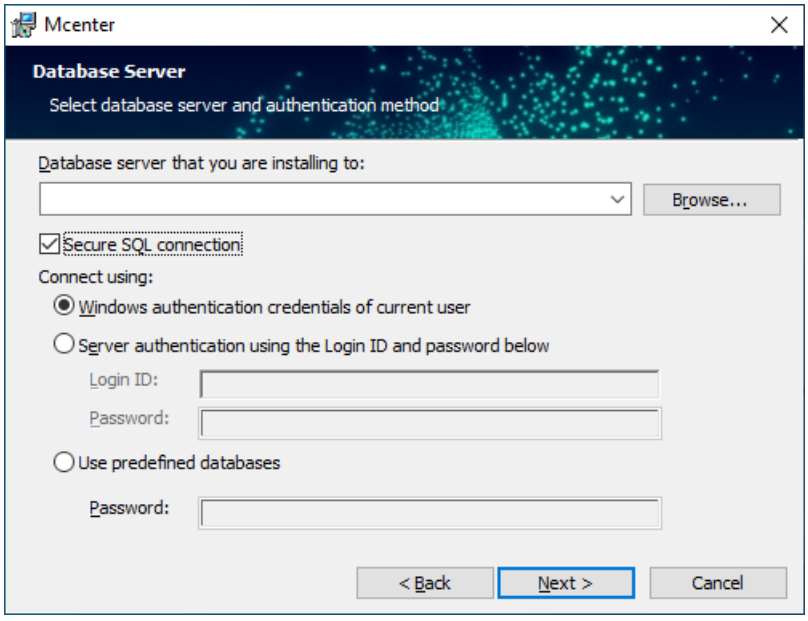
– By clicking "Next", the setup verifies whether a connection can be established to the predefined databases with the provided password.

Note

Secure SQL Connection

During the update it is possible to activate the secure communication between the SQL server and the Mcenter server. For this secure communication you need a certificate on the SQL server. This change cannot be deactivated.

For more information, see Setting up the encrypted communication for SQL Server (Page 59).


Mcenter
Database Server
Select database server and authentication method
Database server that you are installing to:
Browse...
Secure SQL connection
Connect using:
Windows authentication credentials of current user
Server authentication using the Login ID and password below
Login ID:
Password:
Use predefined databases
Password:
< Back
Next >
Cancel

Completing the update

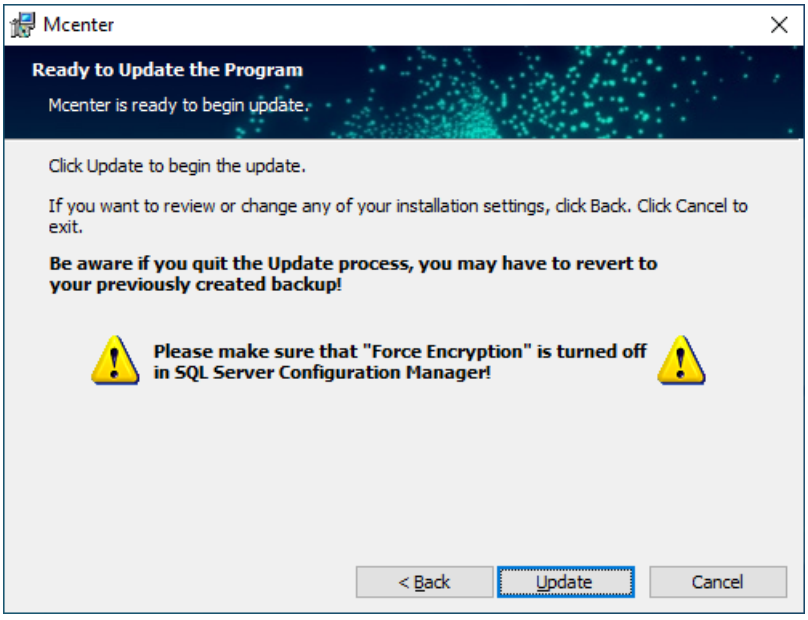
1. The "Ready to Update the Program" window opens.
   Click "Cancel" to cancel the update after prompt.

   Note

   Cancel update

   If you cancel an update, or the update fails due to an unexpected error, then revert to the previous server snapshot, since the setup cannot undo all the changes that were made during the setup.

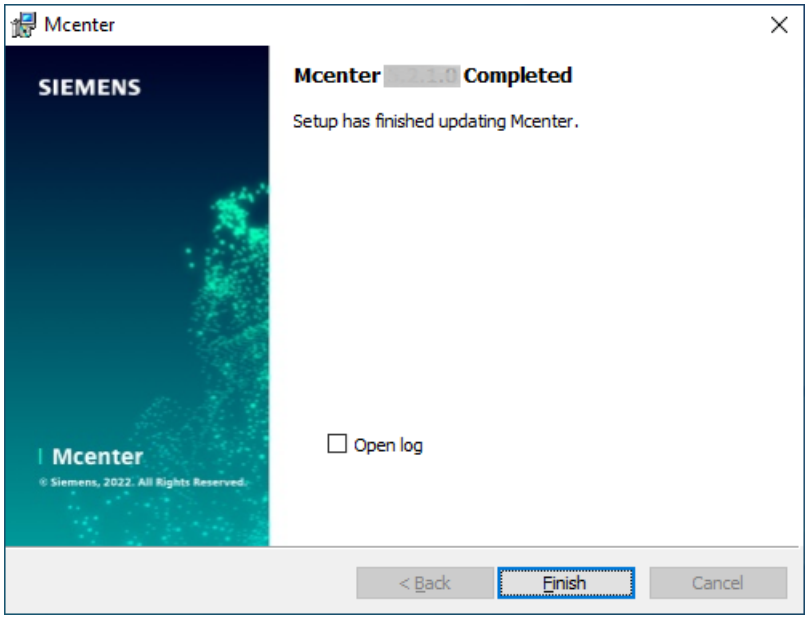
   - OR -
   Click "Update >" to start the update.



2. The update is started. The progress is displayed on a progress indicator.

3. The "Mcenter.x Completed" window opens.
   A message is displayed showing that the installation was successful.
   - Activate the "Open log" checkbox to open the log files.
   - Then click "Finish" to complete the installation and view the log files if required.
     If the log file is in the installation directory, it opens.
     If the log file was not created in the installation directory, the current log file MSI Log opens.

   For more information, see Log files (Page 123).



4. Perform a restart of the SINUMERIK control system and restart the client.

6.5 Modifying/repairing the server setup

You have two options for changing or repairing Mcenter.

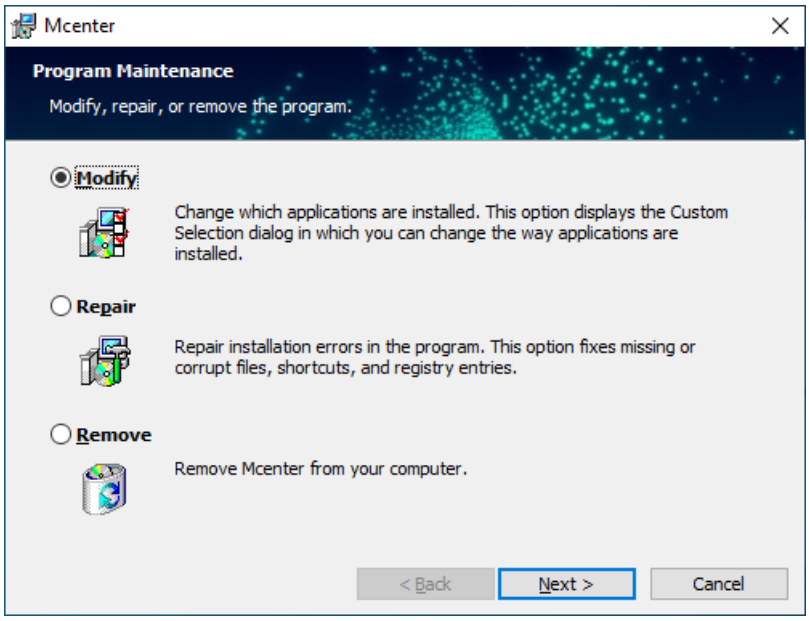
1. Procedure: Start menu "Start" > "Control Panel" > "Programs and Features".
   Select the Mcenter entry and click "Modify".
   - OR -
2. Procedure: "Setup.exe" file with "Modify" or "Repair".

Prerequisite

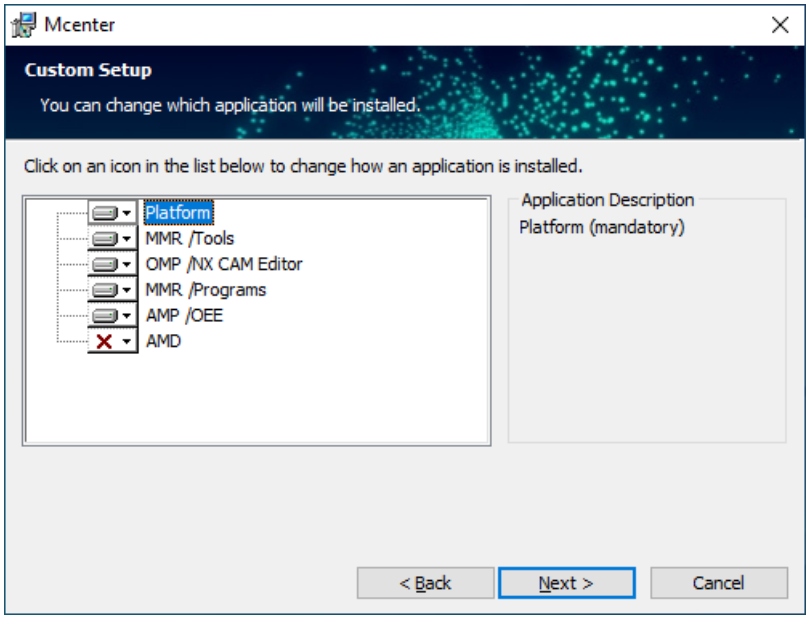
You require local administrator rights to modify or repair the server setup.

Modify Mcenter

1. Start the "setup.exe" file.
2. The "Program Maintenance" window opens.
   Activate option field "Modify" and click "Next >".

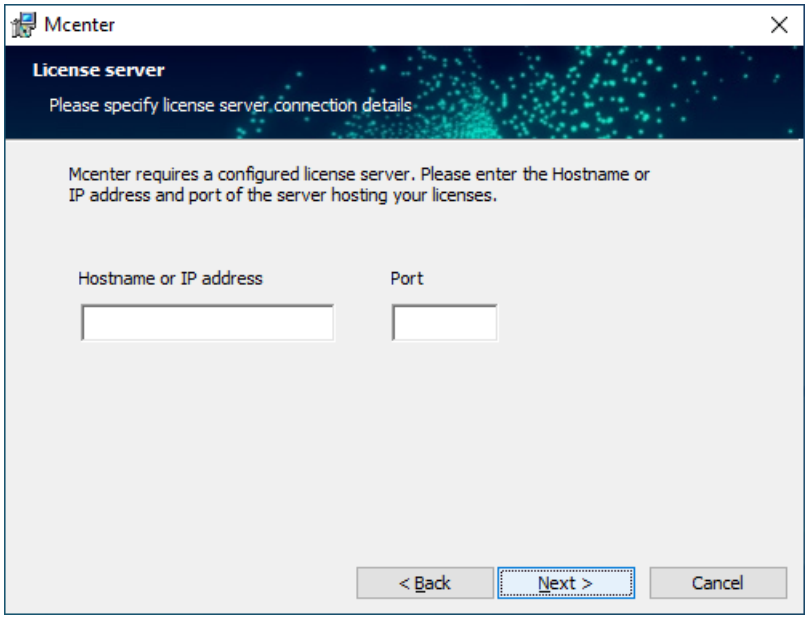


3. The "Custom Setup" window opens and you can select the applications that should be installed on your system:
   - Platform: No deselection possible, always installed.
   - Applications: Each can be selected (or deselected) to install (or remove) them.



4. The "License server" window opens.
   – Enter the server data in the "Hostname or IP address" and "Port" input fields.
   – Click "Next >".

   If you enter invalid addresses, you receive a corresponding error message.



5. The "Database Server" window opens.

   – Database server that you are installing to:
   You have the option to change the connection string during "Modify", but you cannot switch to another SQL Database.

   – Connect using via the following three options:
   Select the "Windows authentication of the current user" connection.
   - OR -
   Activate the "Server authentication using the login ID and password below" option button. Enter the login ID of any SQL user with system administrator rights.
   - OR -
   Select the "Use predefined databases" option button.
   With this option it is possible to use databases created manually prior installation. In this case the setup does not create additional databases.
   Make sure that all the required databases and login users are created.
   For more information, see SQL Server (Page 42).

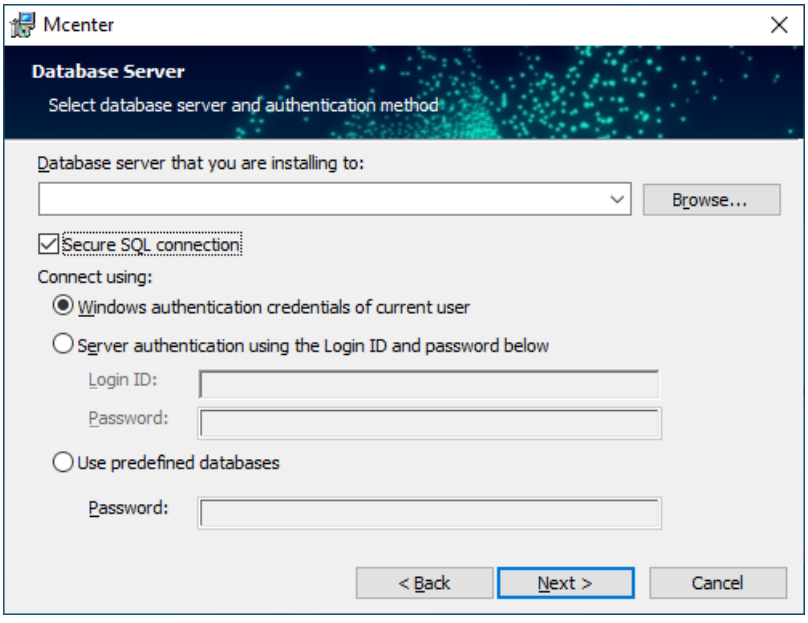
   By clicking "Next", the setup verifies whether a connection can be established to the predefined databases with the provided password.

Note

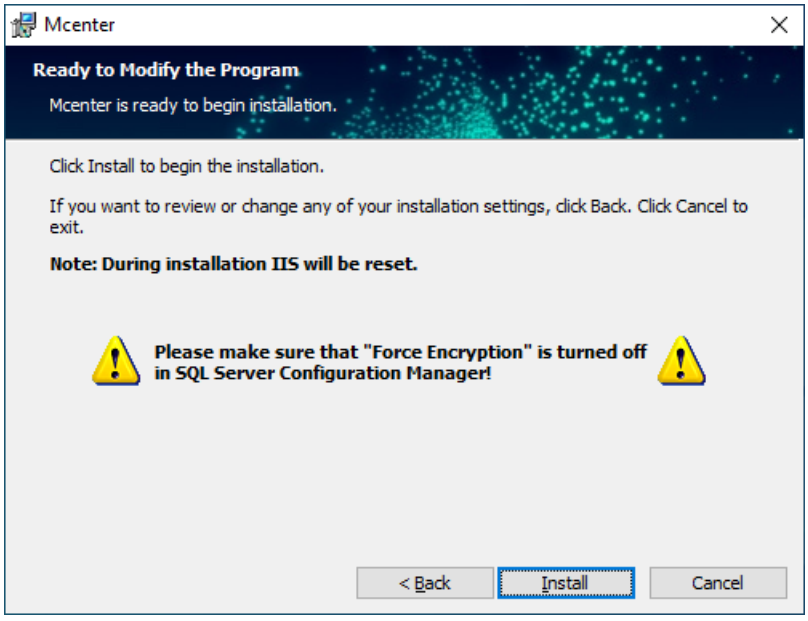
Secure SQL Connection

During the modify it is possible to activate the secure communication between the SQL server and the Mcenter server. For this secure communication you need a certificate on the SQL server. This change can not be deactivated.

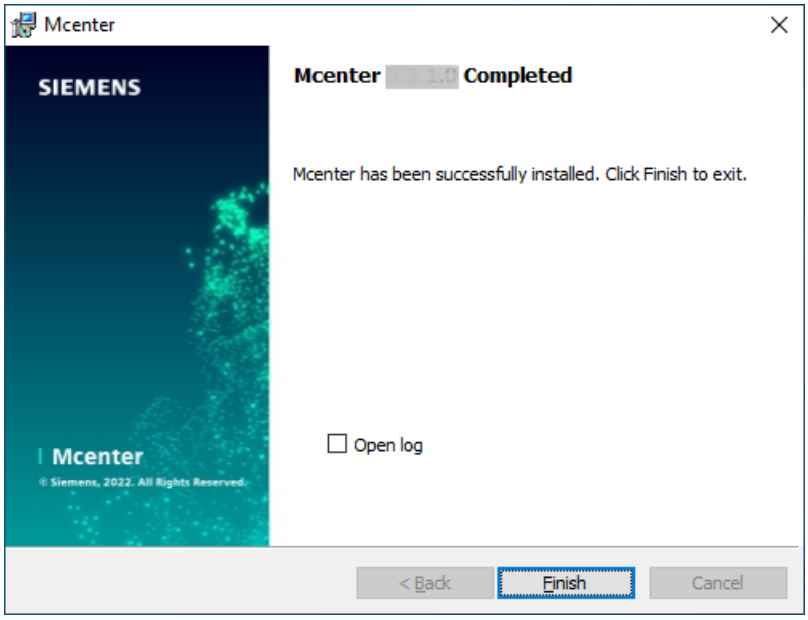
For more information, see Setting up the encrypted communication for SQL Server (Page 59).



6. The "Ready to Modify the Program" window opens.
   Click "Install".



7. The "Mcenter Completed" window opens.
   A message is displayed showing that the installation was successful.
   - Activate the "Open log" checkbox to open the log files.
   - Then click "Finish" to complete the installation and view the log files if required.
     If the log file is in the installation directory, it opens.
     If the log file was not created in the installation directory, the current log file MSI Log is opened.
     For more information, see Log files (Page 123).



Repairing Mcenter

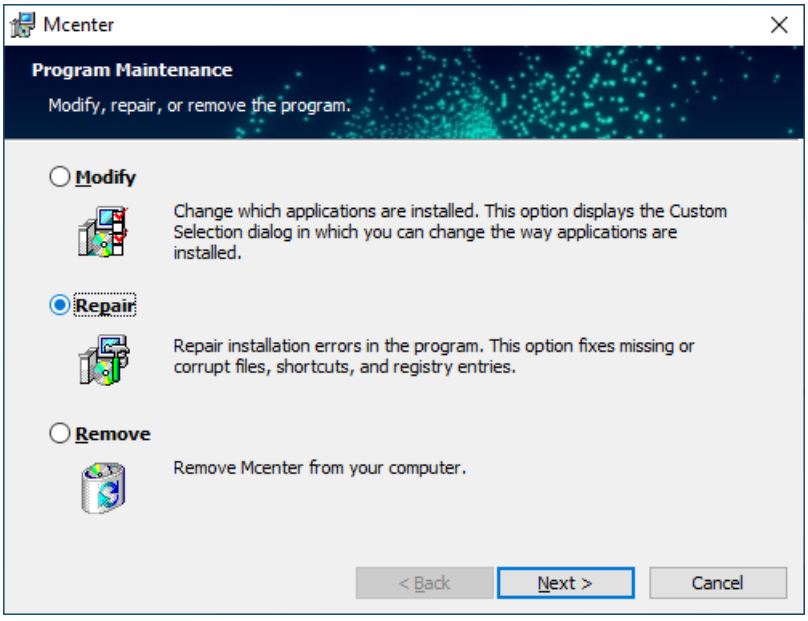
If the application does not work because of manual file changes, shortcuts and registry entries you made, you can use the "Repair" function. In certain cases, this program can repair the installation errors.

Note

"Repair"

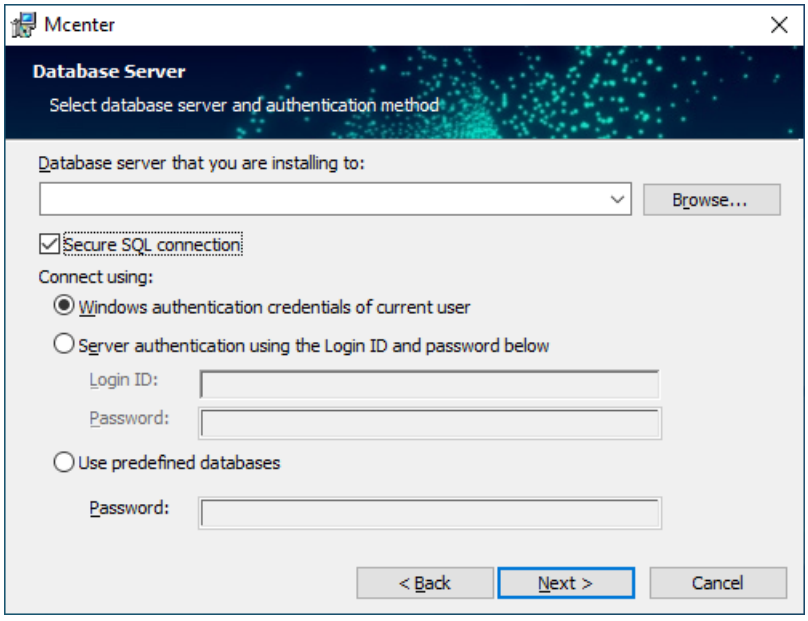
If "Repair" does not fix the errors, you must do a complete reinstallation.

1. Start the "setup.exe" file.
2. The "Program Maintenance" window opens
   Activate option field "Repair" and click "Next >".

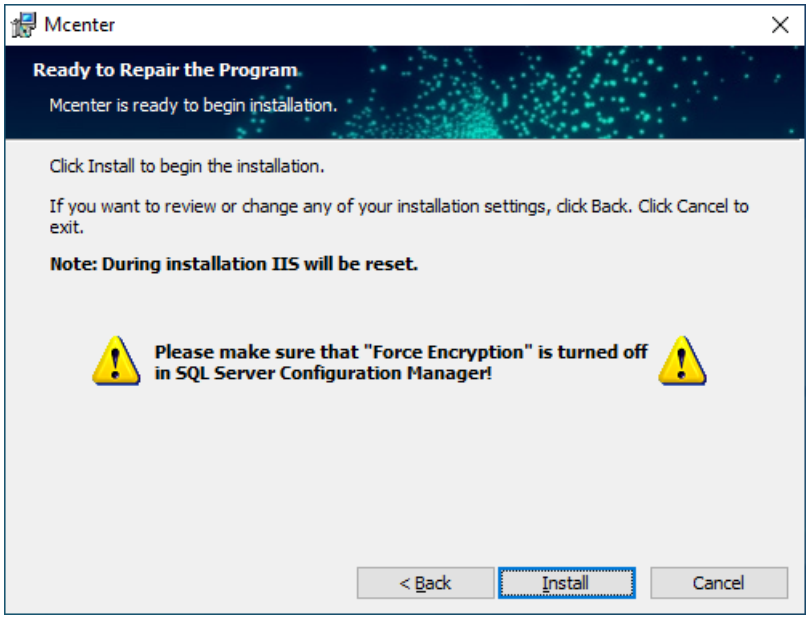


3. The "Database Server" window opens.
   - Database server that you are installing to:
     You have the option to change the connection string during "Repair" but you cannot switch to an other SQL Database.
   - Connect using:
     Select the authentication that you selected for the initial installation, for example "Windows authentication of current user".
     Use predefined databases: If the password has been changed manually for the Mcenter relevant SQL login users, the new password can be set for the applications by selecting "Use predefined databases" and entering the new password.

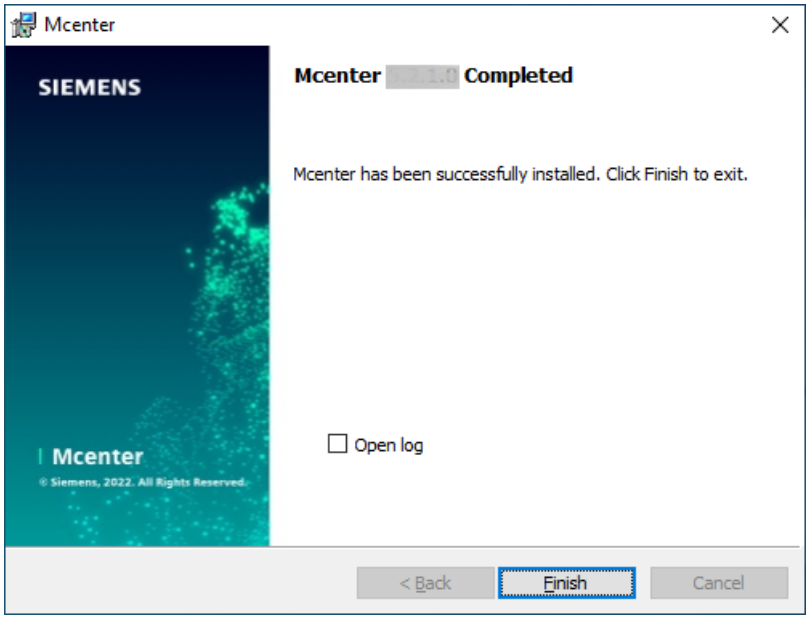
   By clicking "Next", the setup verifies whether a connection can be established to the predefined databases with the provided password.



4. The "Ready to Repair the Program" window opens.
   Click "Install".



5. The "Mcenter Completed" window opens.
   A message is displayed showing that the installation was successful.
   - Activate the "Open log" checkbox to view the log files.
   - Then click "Finish" to complete the installation and view the log files if required.
     If the log file is in the installation directory, it opens.
     If the log file was not created in the installation directory, the current log file "MSI Log" is opened.
     For more information, see Log files (Page 123).



6.6 Uninstalling the server setup

You have two options for uninstalling "Mcenter".

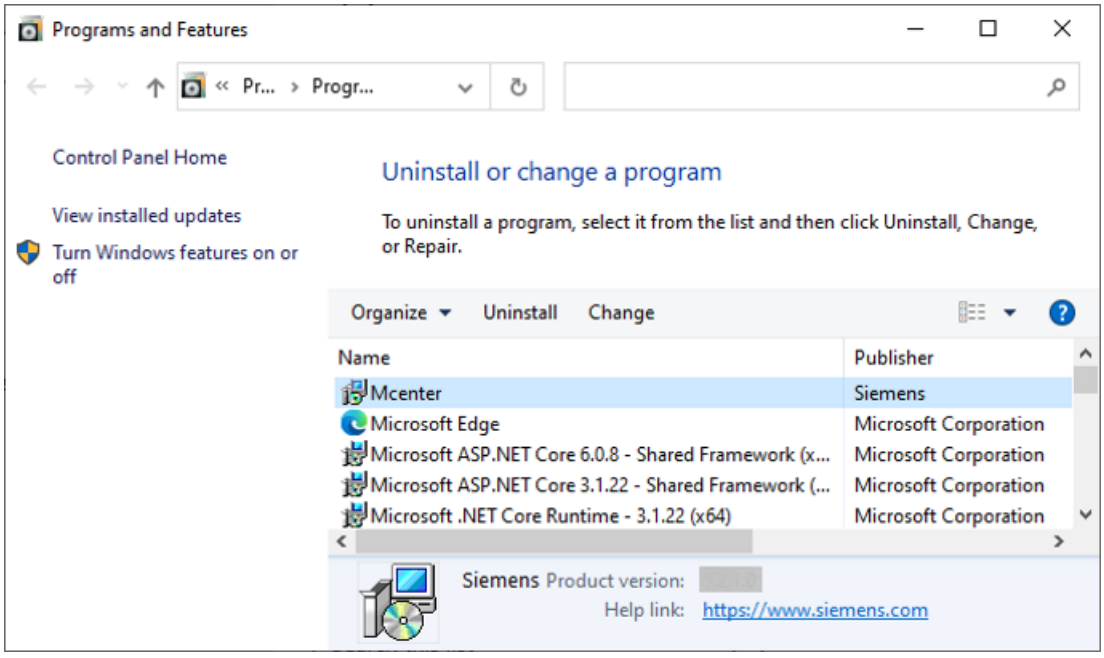
1. Procedure: Start menu "Start" > "Control Panel" > "Programs and Features".
   Select the Mcenter entry and click "Uninstall".
   - OR -
2. Procedure: "Setup.exe" file with "Remove".

Prerequisite

You require local administrator rights to uninstall the server setup.

1st procedure

1. Start menu "Start" > "Control Panel" > "Programs and Features".
2. Select "Mcenter" from the program list and click "Uninstall".
   Depending on the Windows settings a confirmation dialog may appear.

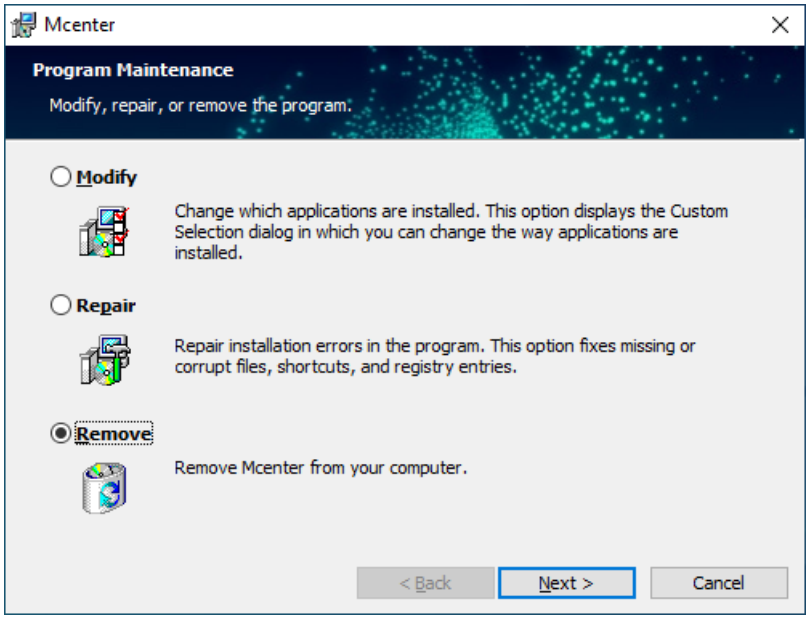


3. The uninstallation is started. The progress is displayed on a progress bar.

2nd procedure

1. Start the "setup.exe" file.
2. The "Program maintenance" window opens

3. Activate option field "Remove" and click "Next >".



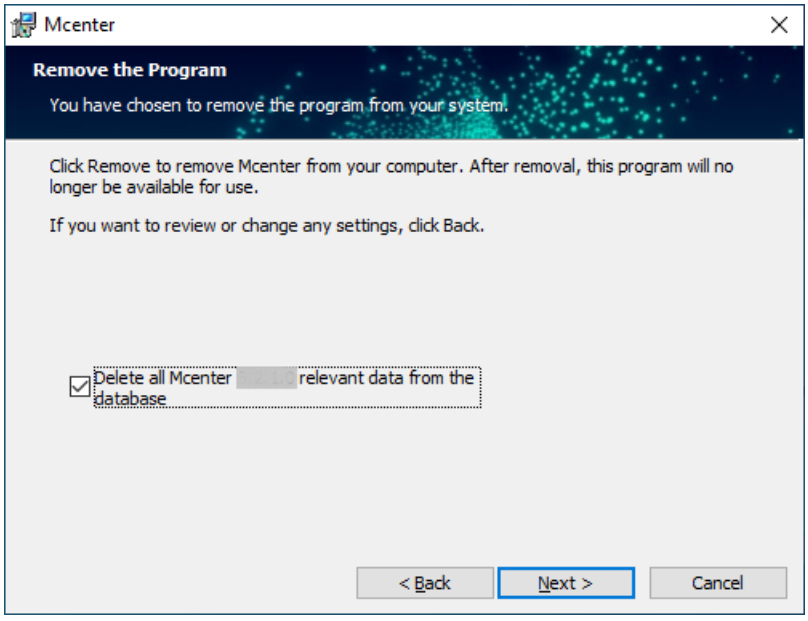
4. The "Remove the Program" window opens.
   – Check the "Delete all Mcenter relevant data from the database" checkbox if you want to delete all of the Mcenter-relevant data. You will be asked for SQL login credentials to perform the action!

     Note

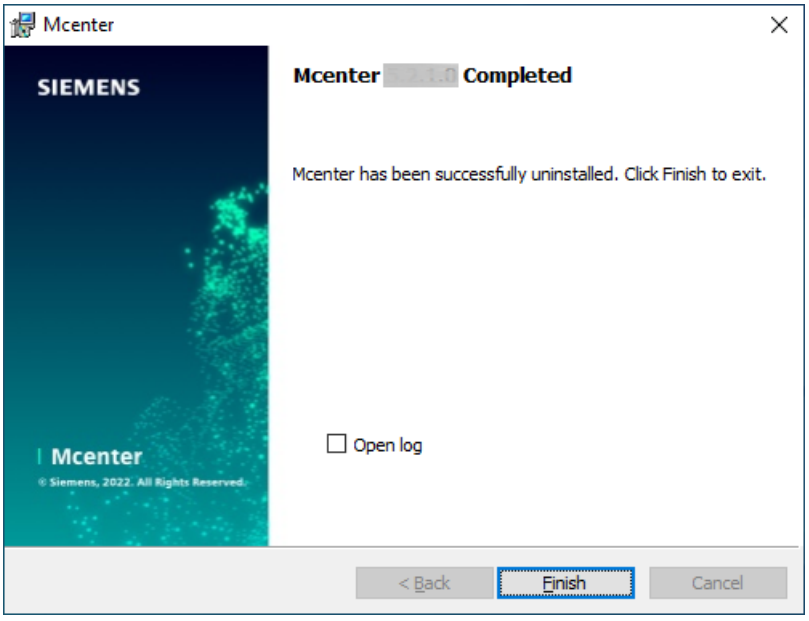
     Deleting the Mcenter relevant data

     By deleting the Mcenter relevant data such as Mcenter users, toolstatistics data, etc., all the data gathered are permanently deleted.

   – Click the "Next >" button.



5. The uninstallation is started. The progress is displayed on a progress bar.
6. The "Mcenter Completed" window is displayed.
   – Activate the "Open log" checkbox to view the log files.
   – Then click "Finish" to complete the installation and view the log files if required.
   As the uninstallation deletes the "log" directory, there is no log file, and the current log file MSI Log opens.
   For more information, see Log files (Page 123).



Note

Scope of the uninstallation

The following data is deleted:

- All files
- Registry entries
- Consul settings
- Configuration files

6.7 Silent Installation and log files

6.7.1 Silent Installation

You have the option of installing Mcenter using Silent Installation.

Parameters

You can use the following parameters in the command line:

`/s` Suppressing the initialization dialog and the language selection
`/v` Provision of additional parameters for "msiexec.exe".
(run msiexec.exe - a list of the generic Windows installation parameters can be seen)

You use the following parameters with `/v`

Parameters	Description
INSTALLDIR	Target folder for the installation
IS_SQLSERVER_SERVER	Instance (mandatory field for silent installation!)
IS_SQLSERVER_AUTHENTICATION	SQL Authentication type
	0: Windows authentication (default) 1: SQL authentication 2: Use predefined databases
PRE_CREATED_PW	Password of the predefined users in case "Use predefined databases" selected
IS_SQLSERVER_USERNAME	SQL user name for SQL authentication
IS_SQLSERVER_PASSWORD	SQL password for SQL authentication
ADMIN_PASSWORD	Password for "admin" user (mandatory field)
LICENSE_IP	IP address of the configured license server (mandatory field for the Silent Installation)
LICENSE_PORT	Port of the configured license server (mandatory field for the Silent Installation)
ADDLOCAL	Installation of the products: • All products are installed using switch "ALL". • Manage MyResources /Tools is installed using "Core,Platform,MMRtools". • Manage MyResources /Programs is installed using "Core,Platform,MMRprograms". • Optimize MyProgramming /NX-Cam Editor is installed using "Core,Platform,OMP". • Analyze MyPerformance /OEE is installed using "Core,Platform,AMP". • Access MyData /Collector is installed usind "Core,Platform,AMD"
SECURE_SQL	Secure SQL checkbox parameter, default value is on To turn off: "SECURE_SQL="""

The following commands are available:

Command	
/l*vx "log file"	Log installation (default setting is: %TEMP%\MSI****.log)
/qb	Silent mode – progress display only
/qn	Silent mode - no UI

Example

Complete silent installation:

```
setup.exe /s /v"IS_SQLSERVER_SERVER=(local)
ADMIN_PASSWORD=Password_1 LICENSE_IP=1.2.3.4 LICENSE_PORT=5 /qn"
```

Installation on C:\SI5, log the installation process to C:\temp\log.log:

```
setup.exe /v"INSTALLDIR=C:\SI5 /l*vx C:\temp\log.log"
```

Installation with deactivated "Secure SQL checkbox":

```
setup.exe /s /v"IS_SQLSERVER_SERVER=(local)
ADMIN_PASSWORD=Password_1 LICENSE_PORT=280000 LICENSE_IP=1.2.3.4
SECURE_SQL="""""" /qn"
```

6.7.2 Log files

If the installation process of an installation, repair or modification update is completed successfully, the system generates a .zip file containing all application-specific log files (*.log).

Overview

These log files are saved in the installation directory under "Logs". The log zip files will get a timestamp, to prevent overwriting.

The following zip files are generated:

Log files	Description
SI5_Install_Logs.zip	Contains the log files of the installation.
SI5_Administration_Logs.zip	Contains the log files of the repair and change installation.
SI5_Upgrade_Logs.zip	Contains the log files of a software update.
SI5_Rollback_Logs.zip	Contains the log files of a repeat process, e.g. if you interrupt the installation process or an error is displayed and the process is re-started. A precondition in this regard is that an actual process has been started and the "Logs" directory is available.

No log file is generated during the uninstall process as the "Logs" directory is removed.

If necessary, you can view the MSI log file. The .zip file contains the log files of the "Logs" directory and the current MSI log.

The application services also save the log files in the "Logs" directory in their own log files.

Setting up an encrypted connection after installation

7

7.1 Certificate on the server

For a secured communication (HTTPS) between a client and the server, you require a digital certificate that confirms the identity of the server.

Note

Certificate for the host name

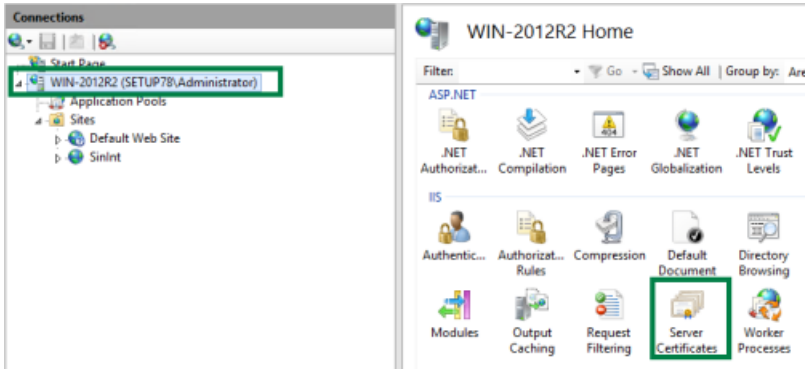
In order to create a certificate for the host name instead of the IP address, enter the host name in the "IP address" input field.

Prerequisite

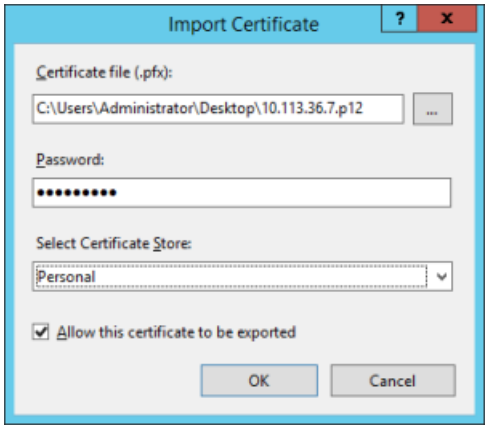
- You require a server certificate which meets these requirements:
  - The CN (Common Name) of the certificate corresponds to the address at which the server is to be reached.
  - The CN is also listed in the SAN (Subject Alternative Name) extension (depending on the type either as "DNS name" or as "IP address").
  - The certificate is created according to the “X509V3” standards, or has at least the "serverAuth" extended key usage property.
- The server has been installed.
  For more information, see Installing the server setup (Page 85).

Procedure

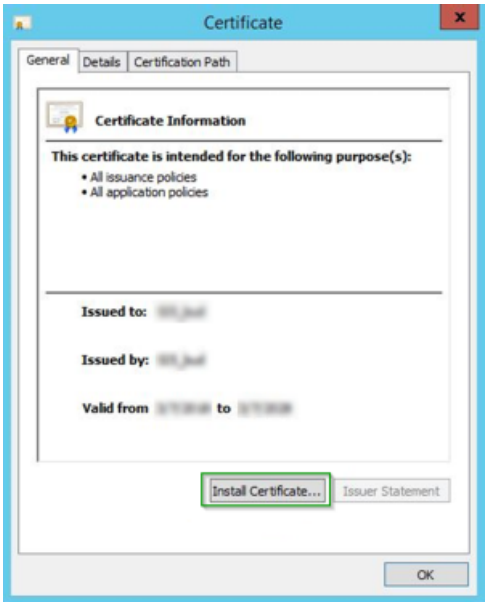
1. Import your server certificates according to IIS.
   - Start the Server Manager.
   - Select "Roles" in the "Web Server (IIS)" > "Internet Information Services (IIS) Manager" directory.
   - At "Connections", mark the server name and click "Server Certificates" in the "IIS" area.



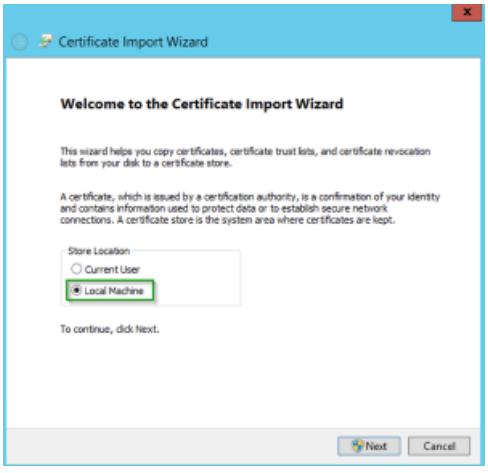
2. The "Server Certificates" window opens.
   Select "Import...".
3. The "Import Certificate" window opens.
   - In the "Certificate file (.pfx):" field, the directory is displayed.
   - Enter the password.
   - Select the desired Certificate Store from the "Select Certificate Store" drop-down list.
   - Activate the "Allow this certificate to be exported" checkbox.
   - Click "OK".



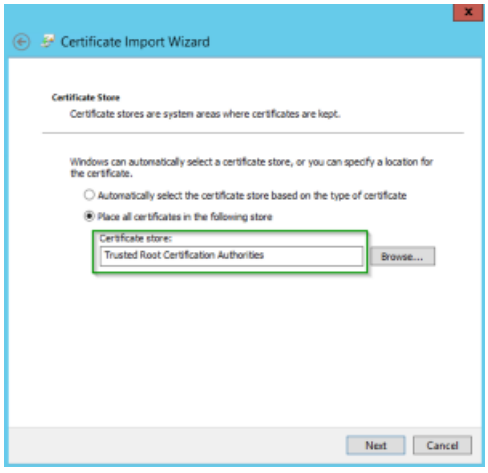
4. Add the Root certificate to "Trusted Root Certification Authorities store".
   - Double-click on the certificate, the Certificate information page will open.
   - Click on the "Install certificate" button.



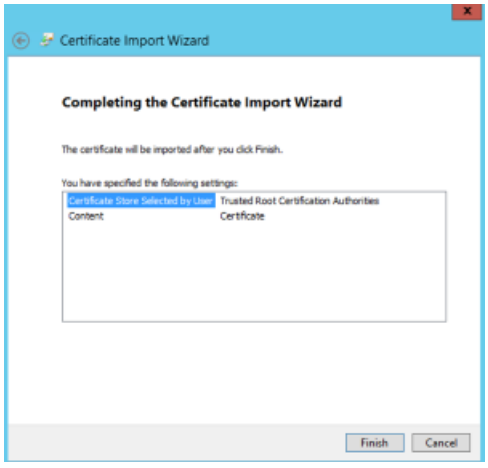
5. The "Welcome to the Certificate Import Wizard" window opens.
   Activate option field "Local Machine" and click "Next".



6. The "Certificate Store" window opens.
   - Activate option field "Place all certificates in the following store"
   - Browse out "Trusted Root Certification Authorities".
   - Click "Next".



7. The "Completing the Certificate Import Wizard" window opens.
   - You see the specified settings
   - Click "Finish".



8. Right-click on the required IIS page (default: SinInt) and select "Edit Bindings".
   The "Site Bindings" window opens. The port settings are listed.
   Click "Add..."
   The "Add Site Binding" window opens.
   Make the required settings, e. g.:

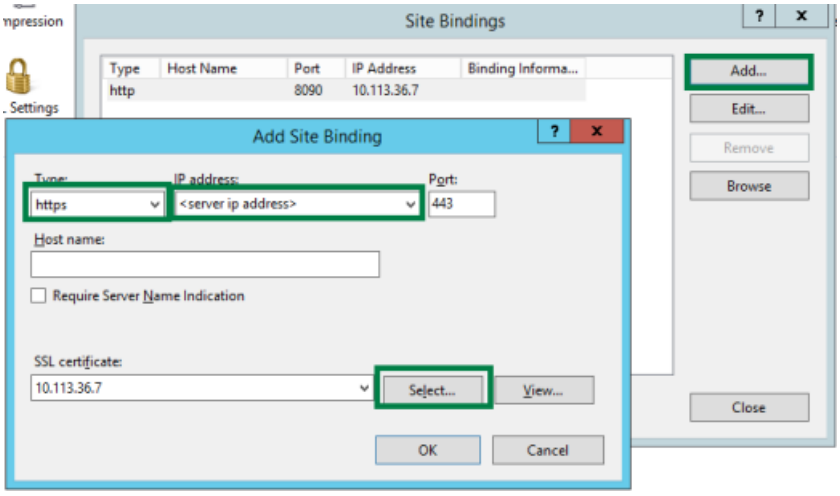
   – Type: "https"

   – IP address: "<server ip address>" or "<host name>"

   – Port: 443

   – SSL certificate: Click "Select" to select the certificate.

   Note:
   Do not activate the "Require Server Name Indication" checkbox. Otherwise communication problems may occur.
   Click "OK".



   - OR-
   If HTTPS is to be configured with the use of a DNS name (host name), open the "Site Bindings" window.

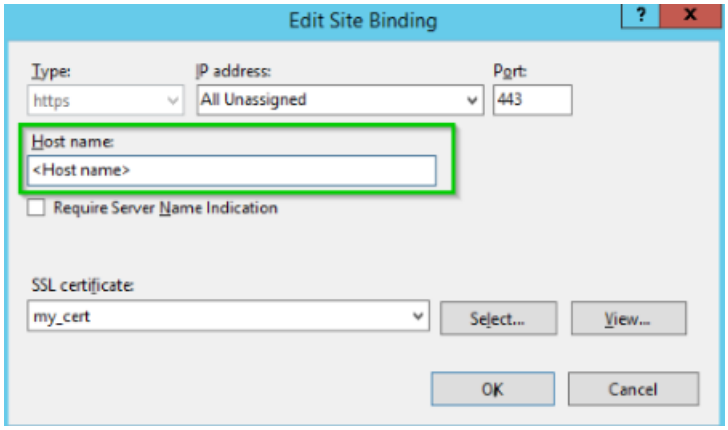
   – Click "Edit...".

   – The "Edit Site Binding" windows opens
     Fill the "Host name" field in IIS.

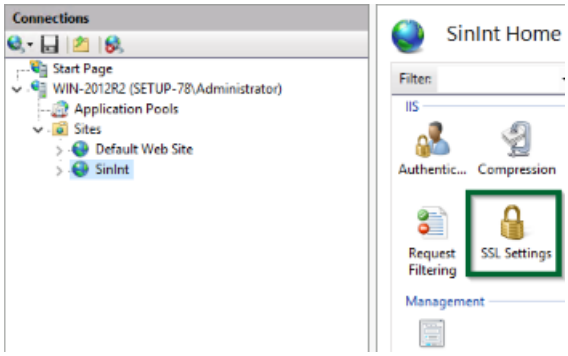
Note

Delete Type "HTTP"

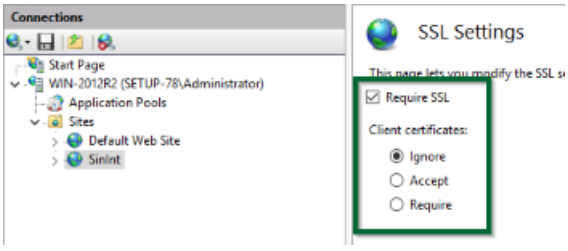
If you want to have just the HTTPS communication, you have to delete HTTP binding on the "Site Bindings" window.



9. Adapt the SSL settings for "SinInt" under the installed sites in IIS:
   – Select the application and click "SSL Settings".



   – The "SSL Settings" window opens:
   Activate the "Require SSL" checkbox.
   Click on "Apply" after it.
   Activate the "Ignore" option button at "Client certificates:".



10. Do an IIS reset.

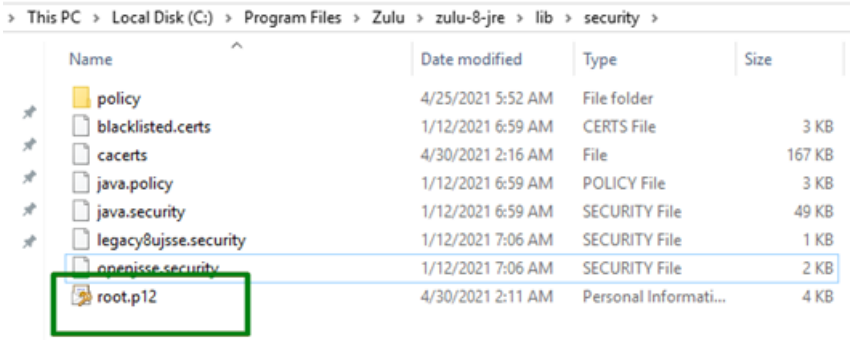
7.2 Certificate on the server using AMP /OEE

For a secured communication (HTTPS) between a client and the server, you require a digital certificate that confirms the identity of the server.

If you use AMP /OEE with an Apache Tomcat server, you need to make additional settings.

Procedure

1. Copy your Root certificate to the following path: %JRE_PATH%\lib\security



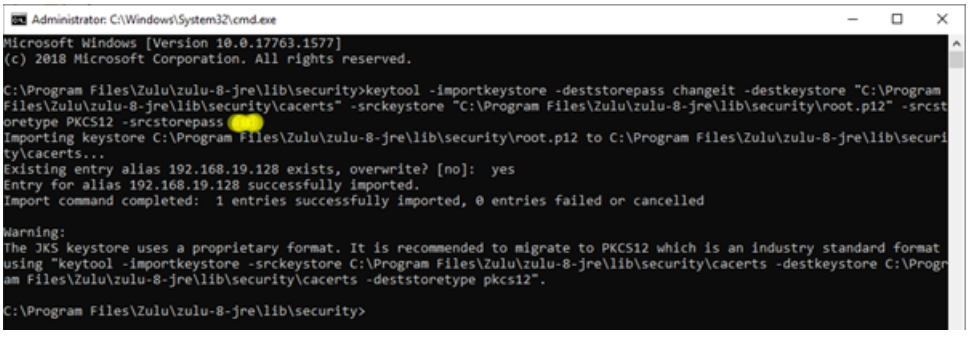
2. Open “cmd”
   - Change directory to “%JRE_PATH%\lib\security”.
3. Run the following command:
   `keytool -importkeystore -deststorepass changeit -destkeystore "%JRE_PATH%\lib\security\cacerts" -srckeystore "%JRE_PATH%\lib\security\<rootCertificate.p12>" -srcstoretype PKCS12 -srcstorepass <rootCertificatePassword>`
   - Replace `%JRE_PATH%` with installed JRE folder path on your pc, i.e. `C:\Program Files\Zulu\zulu-8-jre`
   - Replace `<rootCertificate.p12>` with your root certificate name.
   - Replace `<rootCertificatePassword>` with your root certificate password.

Note

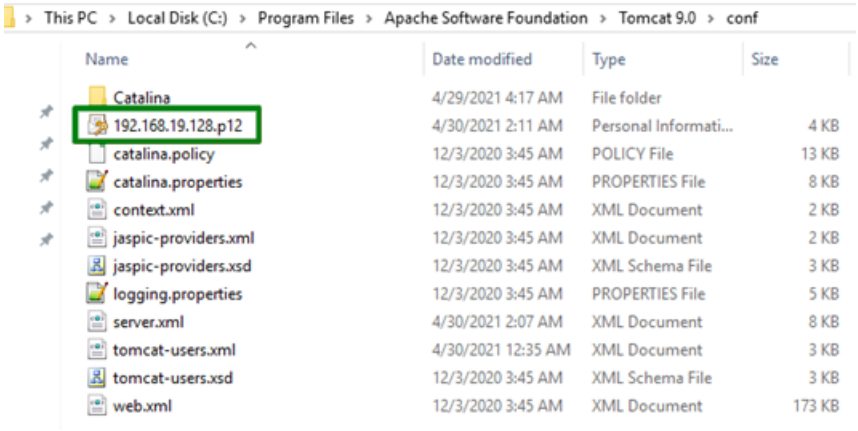
Default password

Default java keystore password is `changeit`.

If you set another password for keystore, please use it on above command instead of `changeit`.



4. Copy your personal certificate to "C:\Program Files\Apache Software Foundation\Tomcat 9.0\conf".



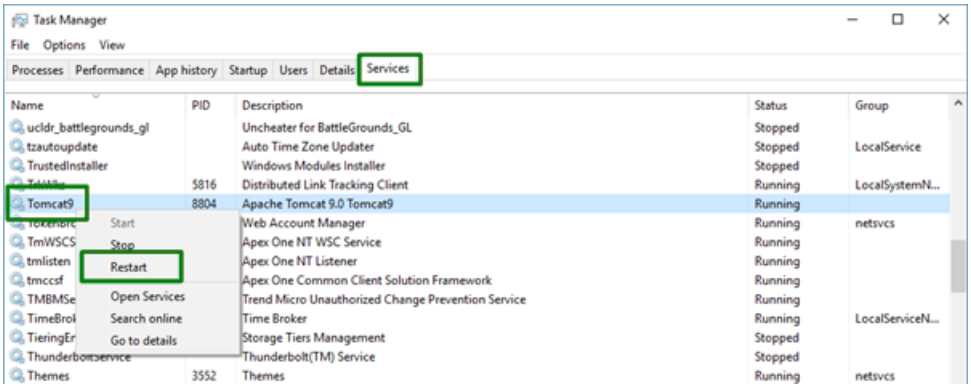
5. Add the connector in the below to server.xml under "C:\Program Files\Apache Software Foundation\Tomcat 9.0\conf" for HTTPS connection:

```
<Connector name="Secure" port="8443" scheme="https" secure="true"
SSLEnabled="true"
protocol="org.apache.coyote.http11.Http11NioProtocol"
maxHttpHeaderSize="65536">
  <SSLHostConfig sslProtocol="TLS">
  <Certificate certificateKeystoreFile="conf/
<yourCertificateName>.p12"
certificateKeystorePassword="<certificatePassword>" clientAuth="false"/>
  </SSLHostConfig>
  </Connector>
```

6. Remove the connector for HTTP in server.xml.

```
<Connector port="8080" protocol="HTTP/1.1" connectionTimeout="20000" redirectPort="8443" maxHttpHeaderSize="65536" />
```

7. Open the Task Manager.
   - Open the "Services" tab.
   - Restart the Tomcat9 server.



7.3 Adaptation in Consul

Make further adaptations, for example with the aid of "Consul".

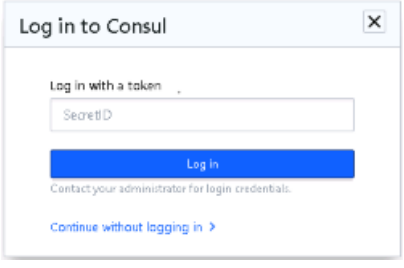
Note

"Consul" available

"Consul" is available to you after the installation from the Mcenter server.

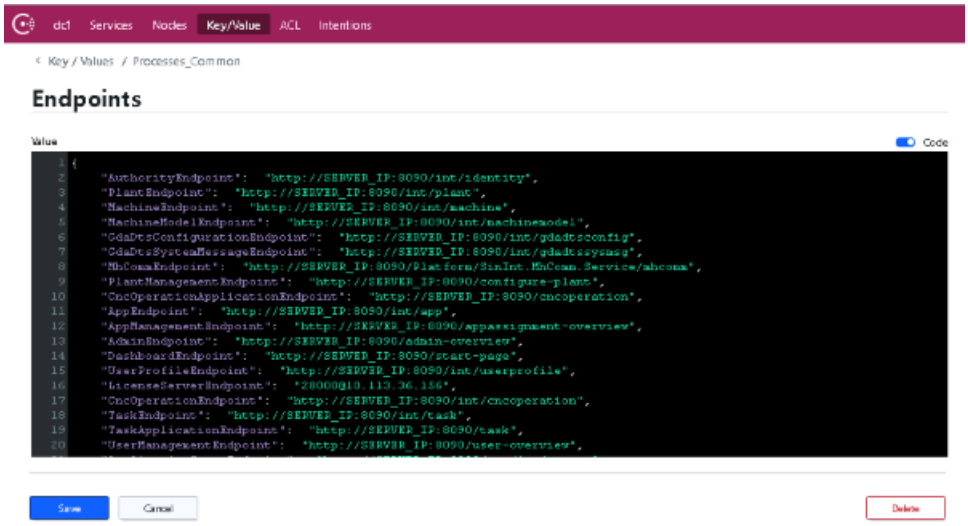
Procedure

1. Open the browser on the server and enter the following link: http://localhost:8500/ui.
2. The start page "Log in to Consul" opens.
   - A token was generated during the setup. Enter the token in the "Log in with a token" field.
   - Click "Log in".



3. The "Settings" window opens.

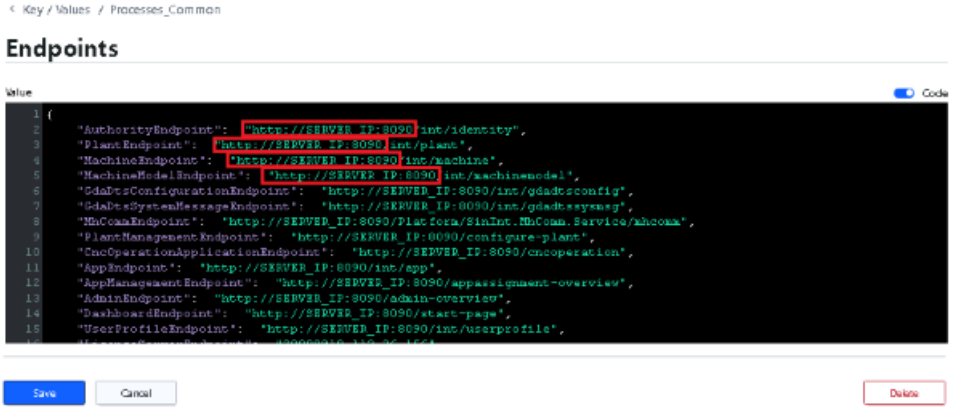
4. Click on the "Key/Value" button and open "Processes_Common" > "Endpoints".



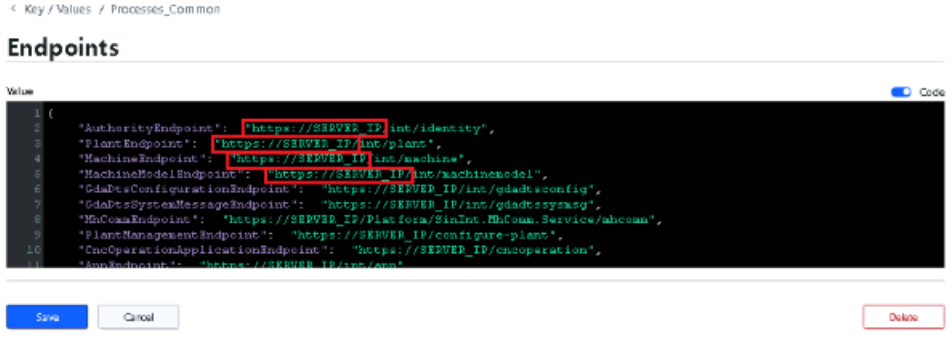
5. Overwrite all of the entries containing the IP address from `http://SERVER_IP:SERVER_PORT/...` to `https://SERVER_IP/...`.
   https://SERVER_IP is correct just when the created certificate is assigned to server IP.
   - OR -
   In the case when the certificate is assigned to server hostname, `https://SERVER_HOSTNAME` must be written into the consul and configuration files.
   For AMP related endpoints also add the port 8443.
   AMP related endpoints:
   - AMPPerformanceMonitoring
   - AMPUtilizationPlanning
   - AMPProductionQuality
   - AMPConfiguration
   - AMPOperator
   - AMPClientEndpoint

Note

The easiest way to execute this task is to copy the whole text into a text editor. Copy and replace the entries and copy them back to consul!



- To save the changes click the "Save" button.



6. Click the "Key/Value" button and open "Processes" > "SinInt.MhComm.Service" > "AppBackendOptions".
   – Overwrite all entries containing the IP address from `http://SERVER_IP:SERVER_PORT/...` to `https://SERVER_IP/...`.
   https://SERVER_IP is correct just when the created certificate is assigned to server IP.
   - OR -
   In the case when the certificate is assigned to server hostname, `https://SERVER_HOSTNAME` must be written into the consul and configuration files.

   For AMP related endpoints also add the port 8443.
   AMP related endpoints:

   – AMPPerformanceMonitoring
   – AMPUtilizationPlanning
   – AMPProductionQuality
   – AMPConfiguration
   – AMPOperator
   – AMPClientEndpoint

   – Click on the "Save" button to save the changes.


Key / Values / Processes / SinInt.MhComm.Service
AppBackendOptions
Value
Code
{
"AppBackEndUris": [
{
"ClientName": "directCommClient",
"AppBackEndUrl": "",
"DataHandlerInterface": "DirectComm"
},
{
"ClientName": "MhComm",
"AppBackEndUrl": "https://SERVER_IP/Platform/SinInt.MhComm.Service/mhcomm",
"DataHandlerInterface": "AppRestBackend"
},
{
"ClientName": "MMR7",
"AppBackEndUrl": "https://SERVER_IP/mar/int/marclient",
"DataHandlerInterface": "AppRestBackend"
},
{
"ClientName": "MMR",
"AppBackEndUrl": "https://SERVER_IP/mar/int/marclient",
"DataHandlerInterface": "AppBackend"
},
{
"ClientName": "ToolStat",
"AppBackEndUrl": "https://SERVER_IP/mar/int/toolstatisticsclient",
"DataHandlerInterface": "AppRestBackend"
},
Save
Cancel
Delete

7. Edit all the "clients.json" files under the folder "C:\Siemens\SINUMERIK_Integrate_5\Platform \SinInt.Identity.Service\identityserver\[app name].

   – Change the URL from `http://SERVER_IP:SERVER_PORT/...` to `https://SERVER_IP/...`

   For AMP related endpoints also add the port 8443.
   AMP related endpoints:

   – AMPPerformanceMonitoring

   – AMPUtilizationPlanning

   – AMPProductionQuality

   – AMPConfiguration

   – AMPOperator

   – AMPClientEndpoint

   For example:

```
{
   "Enabled": true,
   "ClientId: "sinint-dashboard",
   "ClientName": "Dashboard.Application",
   "ClientUri": null,
   "LogoUri": null,
   "BackChannelLogoutUri": "http://SERVER_IP:SERVER_PORT/start-
page/signout-oidc",
   "RedirectUris": [
      "http://localhost:5140/signin-oidc",
      "http://localhost/Dashboard/signin-oidc",
      "http://SERVER_IP:SERVER_PORT/start-page/signin-oidc"
   ],
   "PostLogoutRedirectUris": [
      "http://localhost:5140/signout-callback-oidc",
      "http://localhost/Dashboard/signout-callback-oidc",
      "http://SERVER_IP:SERVER_PORT/start-page/signout-callback-
oidc"
   ],
     "AllowedScopes": [
        "sinint-api",
        "sinint-tr"
   ]
}|
```

   – Save the "clients.json".

```
{
   "Enabled": true,
   "ClientId: "sinint-dashboard",
   "ClientName": "Dashboard.Application",
   "ClientUri": null,
   "LogoUri": null,
   "BackChannelLogoutUri": "https://SERVER_IP/start-page/signout-
oidc",
   "RedirectUris": [
```

```
            "http://localhost:5140/signin-oidc",
            "http://localhost/Dashboard/signin-oidc",
            "https://SERVER_IP/start-page/signin-oidc"
        ],
        "PostLogoutRedirectUris": [
            "http://localhost:5140/signout-callback-oidc",
            "http://localhost/Dashboard/signout-callback-oidc",
            "https://SERVER_IP/start-page/signout-callback-oidc"
        ],
          "AllowedScopes": [
             "sinint-api",
             "sinint-tr"
        ]
    }|
```

8. Do an IIS reset.
9. In case AMP /OEE is installed, change the protocol and port in the following files (depending on the installation folder, the actual path may differ):
   - C:\Siemens\SINUMERIK_Integrate_5\AMP\WEB-INF\classes\application.properties
   - C:\Siemens\SINUMERIK_Integrate_5\AMP\WEB-INF\classes\static\main.xxxxxxxxxx.js

```
5  #AMP - instance details
6  amp.server.context-path=amp
7  amp.server.host=localhost
8  amp.server.port=8080
9  amp.server.url=http://${amp.server.host}:${amp.server.port}/${amp.server.context-path}
10 amp.db.instance.path=localhost\\MSSQLSERVER
```

10. Perform a Tomcat restart.

7.4 Inserting the certificate at the client with SINUMERIK Operate

If you operate your SINUMERIK controller in local mode, insert the root certificate into the "cacerts.pem" file.

Directory

Depending on which operating system you are using, you will find the "cacerts.pem" file in the following directories:

Operating system	Directory of the client with SINUMERIK Operate
Windows XP	Windows XP F:\hmisl\user\sinumerik\hmi\cfg
Windows 7 (32 bit)	Windows 7 (32 bit) C:\Program Files\Siemens\MotionControl\user\sinumerik\hmi\cfg
Windows 7 (64 bit)	Windows 7 (64 bit) C:\Program Files (x86)\Siemens\MotionControl\user\sinumerik\hmi\cfg
Windows 10 (64 bit)	Windows 10 (64 bit) C:\Program Files (x86)\Siemens\MotionControl\user\sinumerik\hmi\cfg
Linux	Linux card/user/sinumerik/hmi/cfg

Procedure

1. Copy the content of the root certificate.
2. Navigate to the corresponding directory.
3. Check whether there is a file named "cacerts.pem".
   – If the file exists, open the file with the text editor.
   Append the content of the root certificate to the end of the file.

   - OR -

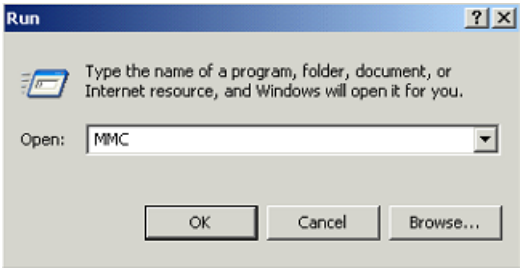
   – If the file is not present, copy the root certificate.
   Insert the copy into the relevant directory and rename the file to "cacerts.pem".

7.5 Inserting the certificate at the client with HMI-Advanced

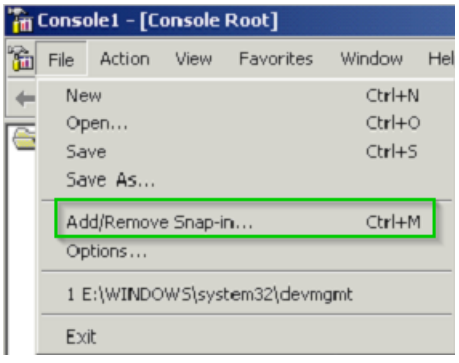
If you operate your SINUMERIK controller in local mode, insert the root certificate into the "cert.crt" file.

Procedure

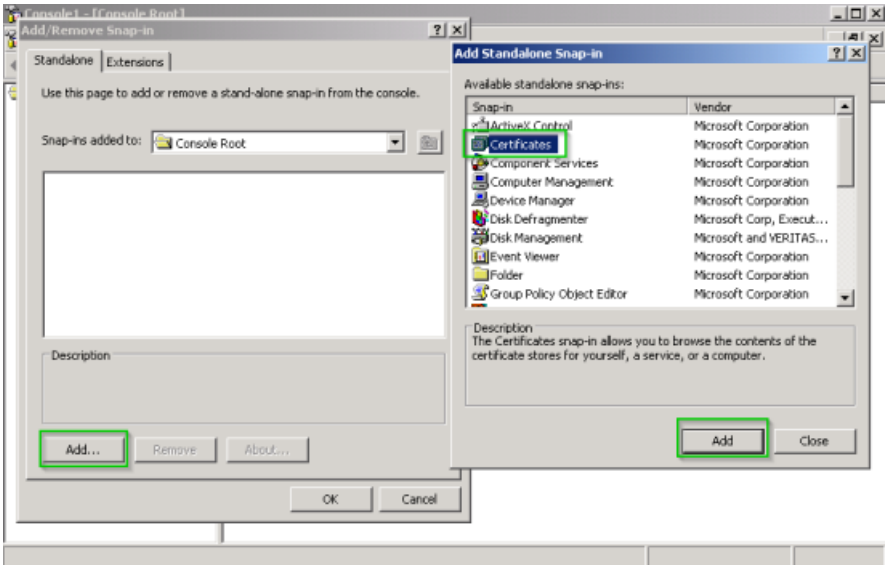
1. Open the Start menu > Run and open "MMC" (Microsoft Management Console).



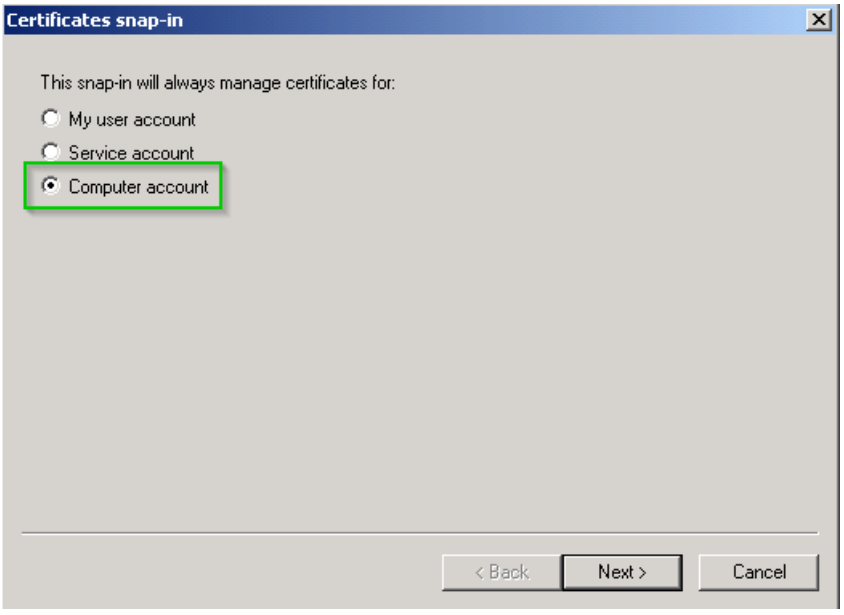
2. The "Console1 - [Console Root]" window opens.
   – Open the "File" menu.
   – Click on the "Add/Remove Snap-in..." function.



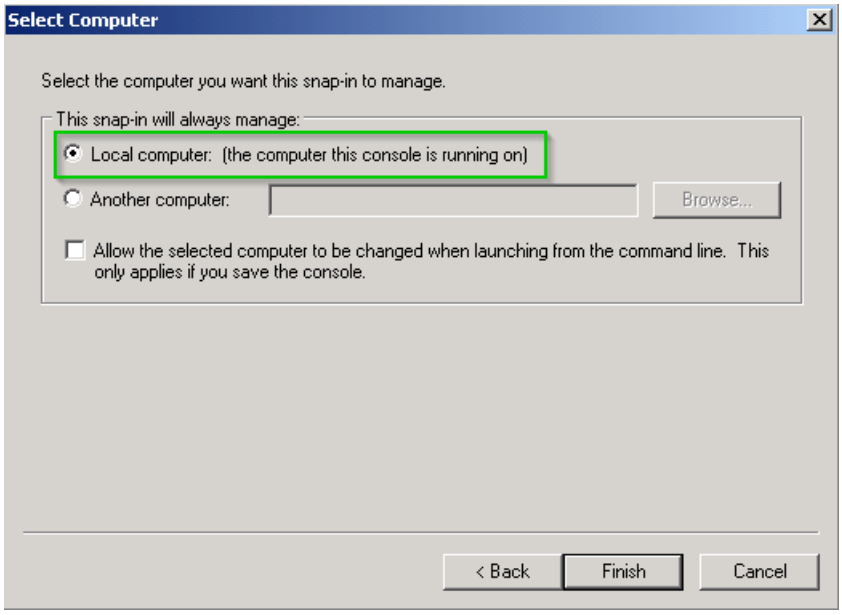
3. The "Add/Remove Snap-in" window opens.
   - Click the "Add..." button.
   - Select the Snap-in "Certificates" in the "Add Standalone Snap-in" window.
   - Click the "Add..." button.



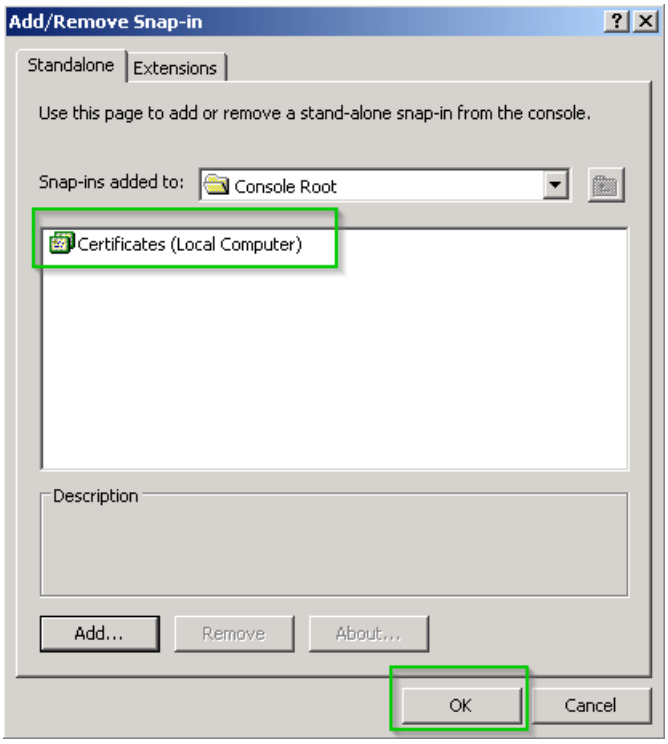
4. The "Certificates snap-in" window opens.
   - Select the "Computer account" option button
   - Click "Next >".



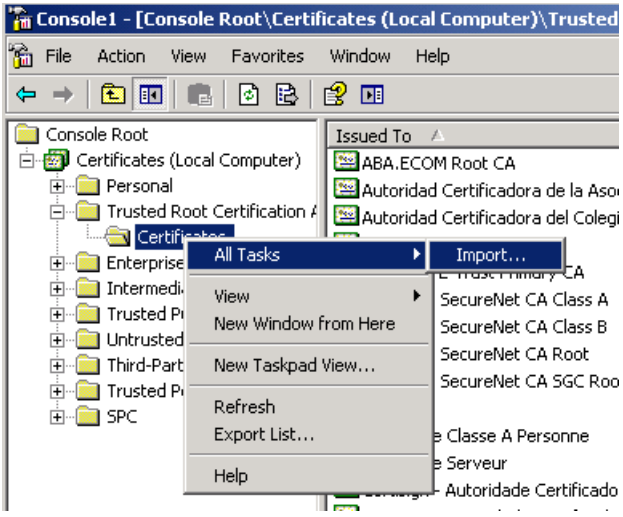
5. The "Select Computer" window opens.
   – Select the "Local computer: (the computer this console is running on)" option button.
   – Click "Finish".



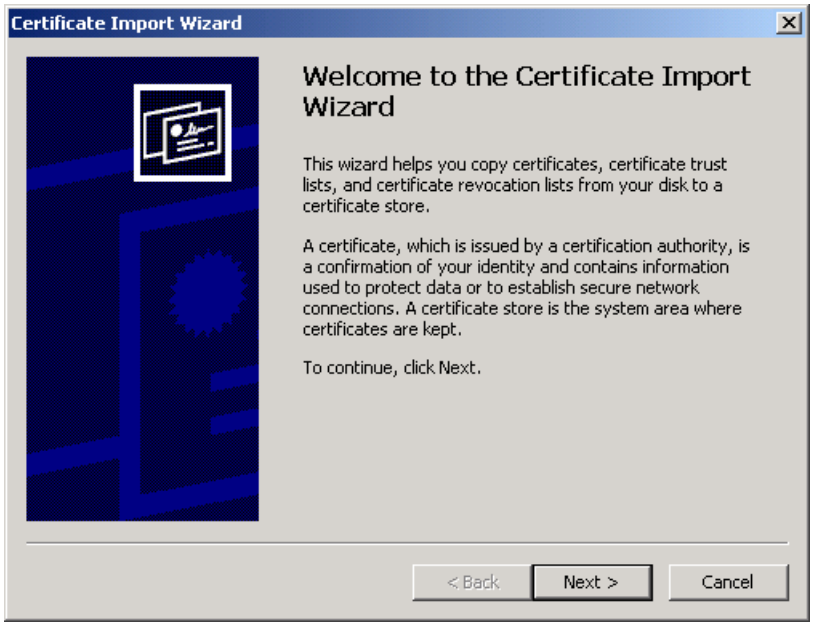
6. The "Add/Remove Snap-in" window opens.
   - Choose the "Console Root" directory in the "Snap-ins added to:" field.
   - Select "Certificates (Local Computer)".
   - Click "OK".



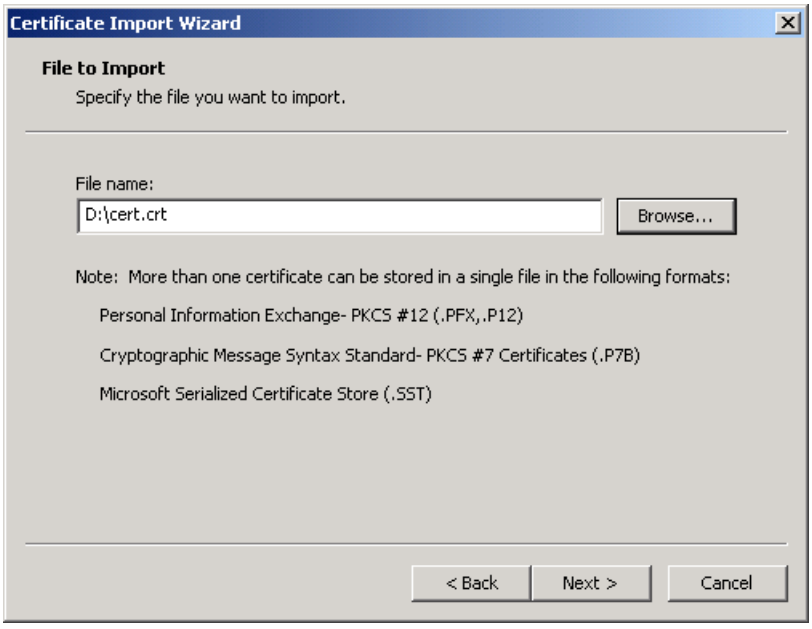
7. The window "Console1 - ..." opens.
   - Open the following directory: "Console Root" > "Certificates (Local Computer)" > "Trusted Root Certification ...".
   - Select "Certificates" and right-click to open the menu.
   - Select "All Tasks" and click the "Import..." function.



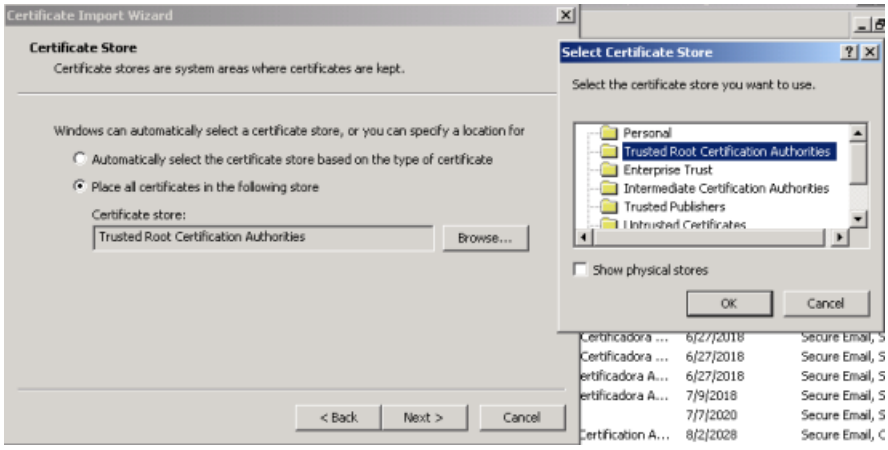
8. The "Welcome to the Certificate Import Wizard" window opens.
   - Click "Next >" to start importing.



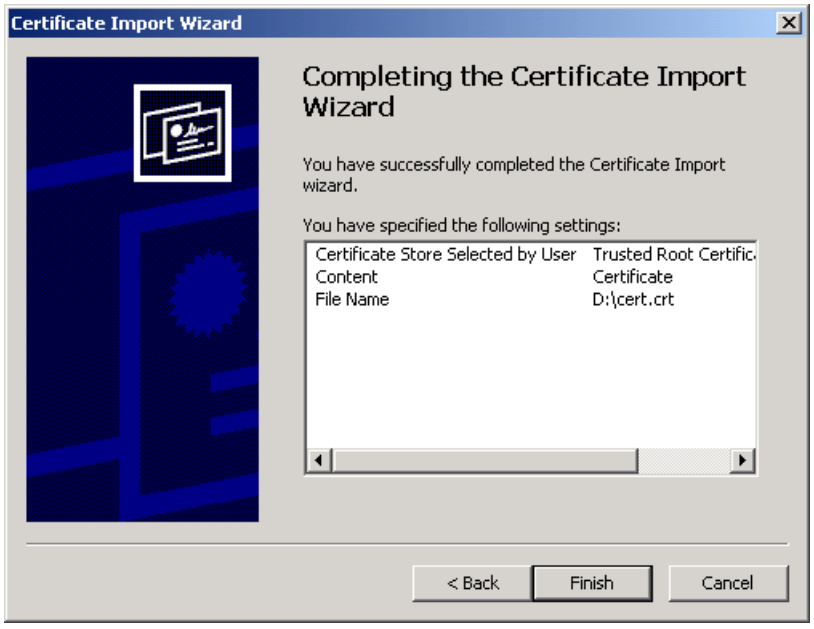
9. The "File to Import" window opens.
   – Click the "Browse..." button and select the desired directory.
   – Click "Next >".



10. The "Certificate Store" window opens.
    - Select the "Place all certificates in the following store" option button.
    - Click the "Browse..." button and select "Trusted Root Certification Authorities".
    - Click "Next >".



11. The "Completing the Certificate Import Wizard" window opens.
    - A success message and an overview of the settings are displayed.
    - Click the "Finish" button to complete the import.



7.6 Setting up encrypted communication

7.6.1 Introduction

The following chapters provide important information that has to be observed when installing the server.

Prerequisite

The server has already been installed.

7.6.2 TLS and Assets

Introduction

This chapter provides guidance to you as an end user on what to do in order to make your systems more secure against possible cyber attacks in addition to applying state-of-the-art technologies instead of the outdated solutions and to meeting the local regulatory requirements.

This section covers two main topics: system hardening and encrypted channels. Although the encryption of channels is part of the system hardening, it is emphasized because of its importance.

System hardening

In order to protect your assets or production unit, you must have the appropriate knowledge, and the installed system must be hardened. System hardening should be done based on the appropriate Microsoft and other hardening guidelines. For example, experts can find guidance in CIS (Center for Internet Security) manuals or, if accessible, in company-wide available documents, or they can choose the source which fits best for them.

Installation and maintenance engineers need to continuously improve their IT security knowledge because the information security threats are increasing day-by-day. The system security risk is increasingly growing, and as Siemens customer you need to prepare yourself accordingly.

You can reuse already hardened system configurations. These configurations, however, should also be regularly reviewed, and new rules must be applied.

Example

Carefully ensure that firewalls are "activated", and only open ports that are actually used and are absolutely necessary for operation. No other ports may be left open, because they could also provide a further attack surface.

When a remote desktop connection is deployed, the highest possible security configuration must be ensured to avoid a possible MITM (man-in-the-middle) attack.

Prepare yourself against DoS (Denial of Service) attacks, for example, by setting up appropriate firewall rules, implementing an IPS (Intrusion Prevention System) and/or a WAF (Web Application Firewall).

Protect your system against code injection by applying state-of-the-art technologies and the appropriate knowledge.

Store certificates securely so they cannot be exported by unauthorized entities. In such cases, you must follow the hardening guidelines when setting up.

Servers have to run in a secure, restricted, server zone/server room, where just only authorized personnel could access to it.

Servers' storage or the data on it are encrypted in order to prevent attacks against the system if the system was compromised physically.

Make backup copies on a regular basis of your system in order to protect your data.

License server is only deployed/available locally.

These are just a few examples of how you can make your system more secure. It is your task and you are responsible for configuring the hardened system.

TLS implementation

The system is prepared for use of the TLS 1.2 protocol. All modules and services must communicate via encrypted channels that meet the current security requirements. Consequently, the system is prepared to use the TLS 1.2 protocol. The server requires a digital certificate that confirms the identity of the server. You can purchase these items from CAs (Certificate Authorities). The certificate must be digitally signed. The clients must trust these certificates. If you use your own generated self-signed certificate, then the root certificates must be deployed on the controls on both Linux and Windows machines - and they must also be deployed on SSL proxies if they are being used. You are completely responsible for correctly implementing and checking your system.

If you are using an obsolete client (such as a Windows NT machine) that does not support the required TLS protocols, then you should use a hardware proxy to resolve this problem. Such hardware can provide an additional encryption layer for the communication channel.

You must also ensure that the hardware proxy is appropriate and correctly encrypted. The hardware proxy is not part of the product.

Finally, you must also have the knowledge and the experience to configure the IIS server. You must always be prepared to address the actual hardening requirements. You are responsible for making the correct system security settings in the client environment.

Configuring the settings

8

8.1 Configuring using the "Consul" software

8.1.1 Overview

Prerequisite

To make settings in Consul, you need a token. This token is generated at the end of the setup.

For more information, see Installing the server setup (Page 85).

Note

Restart IIS after change

Restart IIS after each change in Consul so that the changes can take effect.

Note

ConsulCheck

Under the "Process_Common" section there must be the key "ConsulCheck". This key is required by the application to check whether options are able to be read from Consul.

Do not change or delete it because it can cause the application to be inoperable.

Overview

In the local service mode, you set the basis function and configure the server.

The following configurations are described, e.g. using the "Consul" software.

Configuring password policies (Page 150)

Configuring blocking rules for users (Page 152)

Configuring the expiration time of applications (Page 153)

Configuring the Identity Service Signing certificate (Page 154)

Configuring logging for applications (Page 155)

Activating the debug level for logging (Page 156)

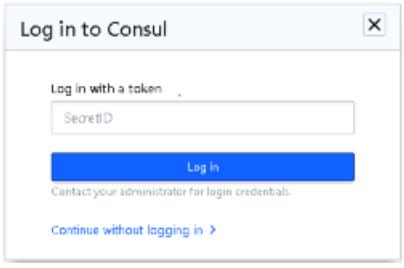
Configuring connection state in Manage machines (Page 158)

Configuring tool lifecycle distribution (Page 159)

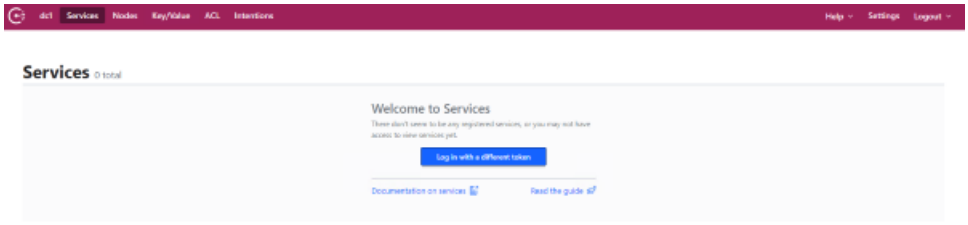
8.1.2 Open the "Consul" software

Procedure

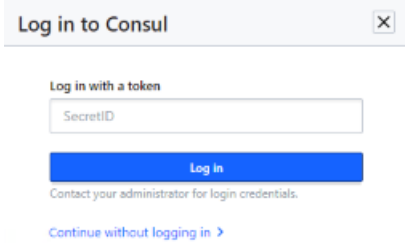
1. Open the browser on the server and enter the following link: http://localhost:8500/ui.
2. The start page "Log in to Consul" opens.
   – Enter the token that was generated during the setup in the "Log in with a token" field.
   – Click "Log in".



- OR -
The "Welcome to Services" window opens.
Click the "Log in with a different token" button.



3. The "Log in to Consul" window opens.
   – Enter the token that was generated during the setup in the "Log in with a token" field.
   – Click "Log in".



8.1.3 Configuring password policies

In the local service mode, you set the basis function and configure the server.

The configuration is described below, e.g. using the "Consul" software.

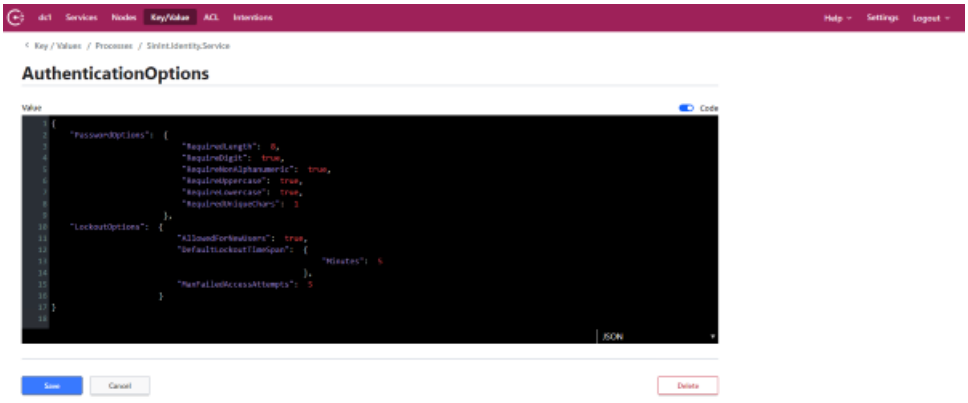
Parameter

You can configure the following password guideline, for example:

Parameter / Description	Settings	
	Type:	Default value:
`RequiredLength` Defines the minimum password length	`Integer`	`8`
`RequireDigit` If you activate this setting, then the password must include at least one character.	`Boolean`	`true`
`RequireNonAlphanumeric` If you activate this setting, then as a minimum, the password must include a special character, for example #, &, @, etc.	`Boolean`	`true`
`RequireUppercase` If you activate this setting, then the password must include at least one uppercase letter.	`Boolean`	`true`
`RequireLowercase` If you activate this setting, then the password must include at least one lowercase letter.	`Boolean`	`true`
`RequiredUniqueChars` Defines the number of special characters that the password must include.	`Integer`	`1`

Procedure

1. Click on the "Key/Value" button.
2. Select the "AuthenticationOptions" option at "Processes / SinInt.Identity.Service".
3. Scroll in the window area to "`PasswordOptions`".
   - Set the properties for the password.
   - Click on the "Save" button to save the changes.



4. Perform a restart so that the settings are accepted.

8.1.4 Configuring blocking rules for users

In the local service mode, you set the basis function and configure the server.

The configuration is described below, e.g. using the "Consul" software.

Parameter

Here, you can define the following settings, for example:

Parameter / Description	Settings
`AllowedForNewUsers` Defines whether new users can be locked out.	Example: `true` New users can be locked out.

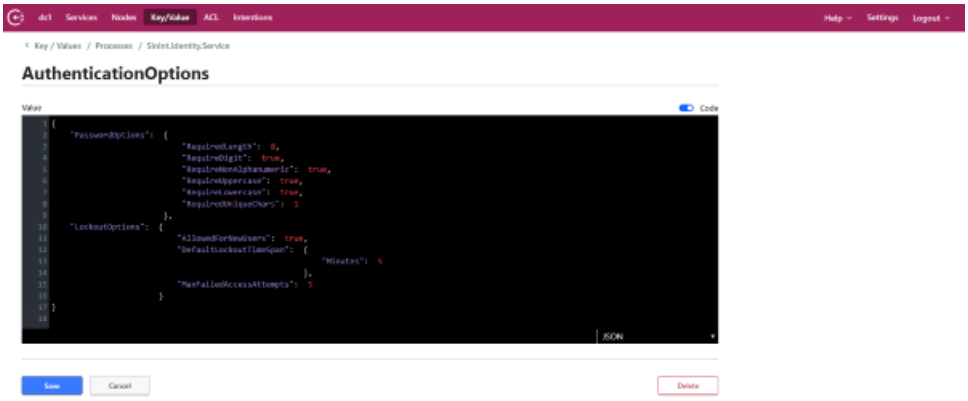
`DefaultLockoutTimeSpan`
Defines the time interval for which a user is locked out, for example: after an incorrect login attempt.
	Example:
	In minutes:
	`"DefaultLockoutTimeSpan": {`
	`"Minutes": 5`
	`},`
	
	In hours, minutes and seconds:
	`"DefaultLockoutTimeSpan": {`
	`"Hours": 0,`
	`"Minutes": 5,`
	`"Seconds": 30`
	`},`

`MaxFailedAccessAttempts` Defines the number of unsuccessful attempts before a user is locked out.	Example: `5`

Procedure

1. Click on the "Key/Value" button.
2. Select the "AuthenticationOptions" option at "Processes / SinInt.Identity.Service".

3. Scroll in the window area to "LockoutOptions".
   – Set the properties for the lockout.
   – Click on the "Save" button to save the changes.



4. Perform a restart so that the settings are accepted.

8.1.5 Configuring the expiration time of applications

In the local service mode, you set the basis function and configure the server.

The configuration is described below, for example using the "Consul" software.

Parameter/Description

You can set the expiration time for every application.

The expiration and automatic logout of Mcenter web applications can be configured in the consul. Each application is configured individually.

You can set the time-out to a different value for each application, but take the following into account:
When the expiration time of the Identity Service is longer than the expiration time of an application, you do not notice any difference. You can use the application until the Identity Service token expires, because the application token is automatically refreshed while you have a valid Identity authentication.

When the expiration time of the Identity Service is shorter than the expiration time of an application, you can access the application until the application token expires, even after the Identity Service token has expired.

If you want all applications to show the same behavior, you have to configure the same settings for all applications with the “Session” Key/Value parameter in consul.

The Mcenter start page and identity service is also an individual application, which has to be configured the same way in consul.

Parameter /Description	Settings
`CookieExpirationTime` Specifies the expiration time in seconds for the session cookie, which the particular application uses. If the time has expired, then the login page is opened and the user must log in again.	Example: `600`
`CookieSlidingExpiration` If the cookie is set to "true", then the session time is extended for each interaction with the application after half of the expiration time has expired. This prevents the session from being interrupted while it is active.	Example: `true`

Procedure

1. Click on the "Key/Value" button.
2. Select the "Session" option at "Processes / SinInt.Identity.Service".
3. Scroll in the window area to "CookieExpirationTime".
   - Set the tool life (in seconds).
   - Click on the "Save" button to save the changes.

4. Perform an IIS reset so that the settings are accepted.

8.1.6 Configuring the Identity Service Signing certificate

In the local service mode, you set the basis function and configure the server.

The configuration is described below, for example using the "Consul" software.

Overview

You can define which certificate of the identity service is used for signing the token.

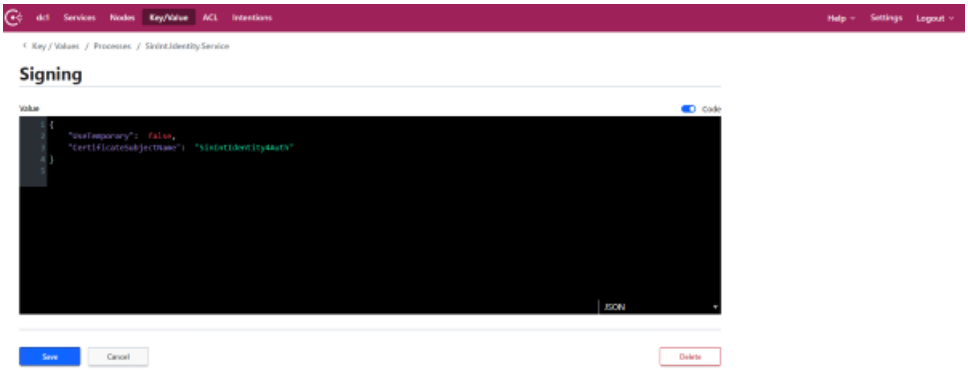
As default setting, Mcenter is installed with a certificate, which is configured for this purpose.

If you change the standard certificate, note the following:

- The certificate requires a "private key" and a "public key".
- The certificate must support 2048-bit encryption.
- The certificate must be installed at "Local Machine".
- Read access must be configured for the "IIS_IUSER" user.
- Using "Consul" you can change the name.

Procedure

1. Click on the "Key/Value" button.
2. Select the "Signing" option at "Processes / SinInt.Identity.Service".
3. Scroll in the window area to "`CertificateSubjectName`":
   – Enter the new name.
   – Click on the "Save" button to save the changes.



4. Perform an IIS reset so that the settings are accepted.

8.1.7 Configuring logging for applications

In the local service mode, you set the basis function and configure the server.

The configuration is described below, e. g. using the "Consul" software.

Procedure

1. Click on the "Key/Value" button.
2. Select option "Processes_Common".

3. Mark the required process in the window area.

4. Select the "Serilog" option.
   - On the right-hand side, scroll to entry "`pathFormat`".
   - Change entry "`%TEMP%`".
     Change the target directory in which the log files are stored, e.g. "`C:/log`".
   - Click on the "UPDATE" button to save the changes.

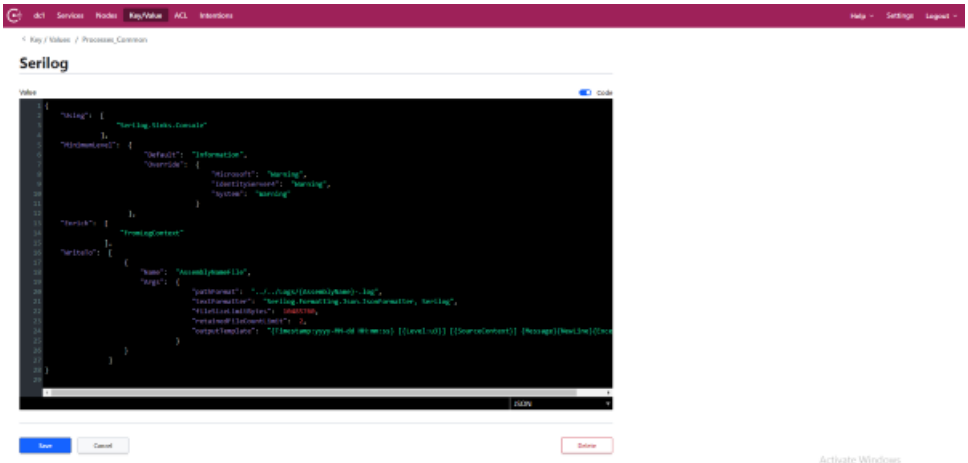
8.1.8 Activating the debug level for logging

In the local service mode, you set the basis function and configure the server.

The configuration is described below, e.g. using the "Consul" software.

Procedure

1. Activate "Debug Level" for logging:
   - Under "Key/Value", select option "Processes_Common" > "Serilog".
   - Enter the following setting:
     Change the entry `"MinimumLevel"` from `"Information"` to `"Verbose"`.
   - Click on the "Save" button to save the changes.



2. Enter the following setting:

```
{
  "Using":  [
            "Serilog.Sinks.Literate"
        ],
  "MinimumLevel": {
            "Default": "Verbose",
            "Override":  {
                    "SinInt":  "Verbose"
 }
        },
  "WriteTo":  [
           {
             "Name":  "LiterateConsole"
            },
            {
             "Name":  "RollingFile",
             "Args":  {
                 "pathFormat":  "***REQUIRED LOG FILE LOCATION***/
SMESmeClient_Service_log_{Date}.txt"
                 }
      }
    ],
  "Enrich":  [
        "FromLogContext"
    ]
}
```

3. Perform an IIS reset so that the settings are accepted.

8.1.9 Configuring connection state in Manage machines

You can configure parameters that affect values of the connection state column in Manage machines.

For onboarded machines, the connection state column displays if the machine is currently connected to the server or not.

Parameter

Here, you can define the following settings, for example:

Parameter / Description	Settings
`OnlineStatusInterval` Connection state is calculated based on communication between Mcenter and onboarded machine. The `OnlineStatusInterval` defines the time it takes for the machine to be offline. For example, setting the `OnlineStatusInterval` to the default value of `600` seconds, the status of the machine is offline if the machine does not send any data to Mcenter during the 10 minutes. Otherwise, the status of the machine is online.	Example: `600` seconds
`LastSeenCacheExpiration` A `LastSeenCache` in MhComm service is available to prevent overloading the database with a large amount of requests and to save LastSeen time. `LastSeenCacheExpiration` defines the time in seconds to prevent saving new LastSeen time to the database, which is equal to time of keeping entry from the cache.	Example: `60` seconds

Note

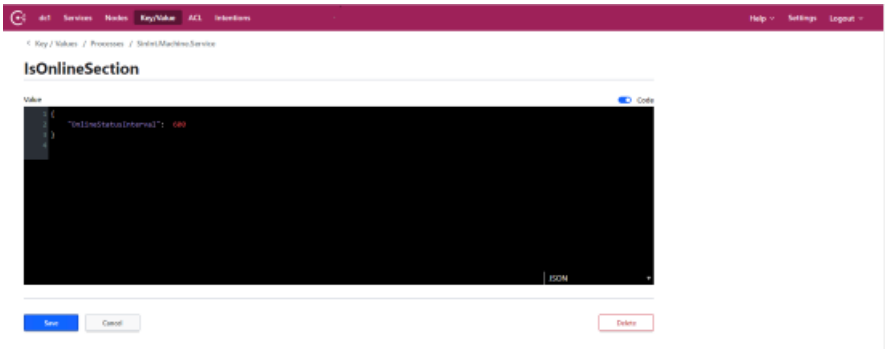
Proper value

In order to provide correct functionality `OnlineStatusInterval` value must be higher than `LastSeenCacheExpiration`.

Procedure

1. Click on the "Key/Value" button.
2. Select the "`IsOnlineSection`" option at "Processes / SinInt.Machine.Service".

3. Scroll to "`OnlineStatusInterval`".
   – Set the interval time (in seconds).
   – Click on the "Save" button to save the changes.



4. Select the "LastSeenCacheSection" option at "Processes / SinInt.MhComm.Service".
5. Scroll to "`LastSeenCacheExpiration`".
   – Set the expiration time (in seconds).
   – Click on the "Save" button to save the changes.

6. Perform an IIS reset to save the settings.
   - OR -
   Restart the IIS to save the settings.

8.1.10 Configuring tool lifecycle distribution

Data gathering/aggregation for tool lifecycle distribution is disabled by default. You can enable the aggregation if the system is capable of handling this additional periodical load.

In the local service mode, you set the basis function and configure the server.

The configuration is described below, e.g. using the "Consul" software.

Procedure

1. Click on the "Key/Value" button.
2. Select "SinInt.ToolStatistics.Service" at "Processes".
   If the part is missing, create it by clicking the "Create" button.
   The value must contain `{ "StatisticsAggregation": "Enabled" }`.
3. Perform an IIS reset.
4. Click on the "Key/Value" button again.
5. Select "ToolStatisticEvents" at "Process_Common".
   The value must contain `{ "Disabled": "false" }`.
6. Perform an IIS reset.

8.2 Configuring the external authentication provider

8.2.1 Types of authentication

There are different types of authentication.

Types of authentication

- Internal authentication
  The users are managed by the Mcenter server. You assign the roles in the "Manage users" application.
- External Authentication
  You can use the external authentication provider to log onto the Mcenter server. You create external users in the User management application.
  Both internal and external users can log onto the Mcenter server. The roles are assigned in the User management application.
- External user management
  Only the external authentication provider can be used for logging onto the Mcenter server. Users are managed by the external authentication provider. The external user roles are determined by the external authentication provider. You cannot assign roles to users which are managed by the Mcenter server.

NOTICE
External user management You need to configure the external authentication to enable the external user management.

8.2.2 Changing between authentication modes

You can change between authentication modes.

Authentication modes

- Internal Authentication is used when ExternalProvider:Authority is not set.
- External Authentication is used when ExternalProvider:Authority is set and a valid URL.
- External User Management is used when ExternalProvider:Authority is set and a valid URL, and ExternalProvider:UseExternalUserManagement is set to true.

8.2.3 Configuring the external authentication

8.2.3.1 Configuring without a secret

Identity Service supports using an external authentication provider via OIDC (OpenID Connect) protocol.

If this option is enabled, the external authentication provider is used by default.

Signing in at the default Mcenter login page is still possible, but you must navigate to the login page manually.
Open the following URL on the server: `https://<Mcenter ip address>/int/identity/account/login`

Prerequisite

The Mcenter server has already been installed.

You require administrator rights on the server.

Parameter

Parameter / Description	Settings	
	Type	Value
ClientId ClientId of the Mcenter Identity Service, same value as the ClientId of the "appsettings.production.json"	string	`<clientId>`
Redirection URLs After the users successfully authenticate themselves, the authorization server redirects the users back to the application with either an authorization code or access token in the URL.	string	`<SI5 server ip address>:<port>/int/identity/signin-oidc`
Post Logout Redirect URLs After a user successfully logged out from an application, the authorization server redirects the user back to this URL.	string	`<SI5 server ip address>:<port>/int/identity/signout-callback-oidc`
Scopes Scopes are used by an application during authentication to authorize access to user details. User data is not stored.	string	`profile, openid`

Parameter / Description	Settings	
	Type	**Value**
Grant Types Represents a user's permission for the client to access their data.	string	`Authorization Code`
Properties set in "appsettings.production.json"		
ResponseType	The response type that is used when authenticating with the external provider. Possible values: • code • code id_token • code id_token token • code token • id_token • id_token token • none • token	
ResponseMode	The response mode that is used when authenticating with the external provider. Possible values: • query • form_post • fragment	
IsSecure	Optional value. If it is set to "true", all cookies are marked "Secure" with "SameSite=None". Use this only with HTTPS. The default value is "false".	

Note

Scopes

- openid: mandatory scope and returns a sub claim, which represents a unique identifier for the authenticated user.
- profile: request access to the End-User's default profile claims

Configuring the Mcenter Identity Service

1. Open the following directory: <Installation directory>\SinInt.Identity.Service\
2. Open the file "appsettings.production.json".

3. Enter the following data:
   - ClientId: The ID of the Mcenter Identity Service client
   - Authority: The URL of the external identity server
     When adding the "Authority" endpoint, do not include the "/.well-known/openid-configuration" part of the URL.

```
"ExternalProvider": {
"ClientID": "<clientID>",
"Authority": "<external identity server ip address>:<port>",
}
```

Note

"Authority" endpoint

Check that the previously added "Authority" can be reached via a browser from the Mcenter server. In this case, the "/.well-known/openid-configuration" ending is necessary.

4. Save the "appsettings.production.json".
5. Restart the IIS.

8.2.3.2 Configuring with a secret

Identity Service supports using an external authentication provider via OIDC (OpenID Connect) protocol.

If this option is enabled, then the external authentication provider is used by default.

Signing in at the default Mcenter login page is still possible, but the user must navigate to the login page manually.
Open the following URL on the server: `https://<Mcenter server ip address>/int/identity/account/login`

Prerequisite

The Mcenter server has already been installed.

You require administrator rights on the server.

Parameter

Parameter / Description	Settings	
	Type	**Value**
ClientId ClientId of the Mcenter Identity Service, same value as the ClientId of the "appsettings.production.json"	string	`<clientId>`
Redirection URLs After a user successfully authenticates itself, the authorization server redirects the user back to the application with either an authorization code or access token in the URL.	string	`<Mcenter server ip address>:<port>/int/identity/signin-oidc`
Post Logout Redirect URIs After a user successfully logged out from an application, the authorization server redirects the user back to this URL.	string	`<Mcenter server ip address>:<port>/int/identity/signout-callback-oidc`
Scopes Scopes are used by an application during authentication to authorize access to a user's details. User data is not stored.	string	`profile, openid`
Grant Types Represents a user's permission for the client to access their data.	string	`Authorization Code`
Token Endpoint Authentication Method Include clientId and client secret in the request body.	string	`client_secret_post`
Client Secret This secret is used by the OAuth Client to authenticate itself to the authorization server.	string	`<secret>`
Properties set in "appsettings.production.json"		
ResponseType	The response type that is used when authenticating with the external provider. Possible values: • code • code id_token • code id_token token • code token • id_token • id_token token • none • token	

Parameter / Description	Settings	
	Type	Value
ResponseMode	The response mode that is used when authenticating with the external provider. Possible values: • query • form_post • fragment	
IsSecure	Optional value. If it is set to "true", all cookies are marked "Secure" with "SameSite=None". Use this only with HTTPS. The default value is "false".	

Note

Scopes

- openid: mandatory scope and returns a sub claim, which represents a unique identifier for the authenticated user.
- profile: request access to the End-User's default profile claims

Configuring Mcenter Identity Service

1. Open the following directory: <Installation directory>\SinInt.Identity.Service\
2. Open the file "appsettings.production.json".
3. Enter the following data:
   - ClientId: The ID of the Mcenter Identity Service client
   - Authority: The URI of the external identity server
     When adding the "Authority" endpoint, do not include the "/.well-known/openid-configuration" part of the URL.
   - ClientSecret: The secret of the client

```
"ExternalProvider": {
"ClientID": "<clientID>",
"Authority": "<external identity server ip address>:<port>",
"ClientSecret": "<optional>"
}
```

Note

"Authority" endpoint

Check that the previously added "Authority" can be reached via a browser from the Mcenter server. In this case, the "/.well-known/openid-configuration" ending is necessary.

4. Save the "appsettings.production.json".
5. Restart the IIS.

8.2.4 Configuring the external user management

8.2.4.1 Configuring the external user management

You can configure the external user management.

Prerequisite

The server must be configured for external authentication.

Procedure

1. Open the following directory: <Installation directory>\SinInt.Identity.Service\
2. Open the file "appsettings.production.json".
3. Enter the following data:
   - ClientId: The ID of the SI5 Identity Service client
   - Authority: The URI of the external Identity Server
     When you add the "Authority" endpoint, do not include the "/.well-known/openid-configuration" part of the URL.
   - ClientSecret: The secret of the client
   - UseExternalUserManagement: When set to true, the external user management is used instead of external authentication
   - ExternalRoleSource: Defines where the external roles are retrieved from
   - RoleMappingClaimType: The name of the claims used for determining the internal user roles
   - ExtendedScopeList: Additional scopes that are requested during authentication

```
"ExternalProvider": {
  "ClientID": "<clientID>",
  "Authority": "<external identity server ip address>:<port>",
  "ClientSecret": "<optional>",
  "UseExternalUserManagement": true,
  "ExternalRoleSource":"<type of external role source>",
  "RoleMappingClaimType": "<name of the claim type used for role
mapping>,
  "RoleMappings": [
    {
      "externalRoles": [
          <list of external roles>
    ]
      "internalRoles":
          <list of internal roles>
      ]
    }
  ],

"ExternalUserDataRetentionPeriodInDays":<numberofdaysafterinactive
externaluser'sprofiledataisdeleted>
"ExternalUserExpirationCheckPeriodInHours":
<thefrequencyexpiredusersarecheckedfordataretention>,
  "ExtendedScopeList": [<list of scopes>]
}
```

NOTICE
External user management: When you use the external user management, note the following points: • The login page at the identity service is not usable. • The user management application is not usable. • The "Manage users" tile is not shown in the dashboard application.

8.2.4.2 User data retention

User data retention

When using the external user management, you cannot delete users via the Mcenter "Manage users" application.
When the user has not logged in to the Mcenter server for a certain amount of time, the external user profile data is automatically deleted.

8.2.4.3 External role source

The external role source describes where the external roles are retrieved from.

Possible values are:

- IdToken:
  The external roles are retrieved from the identity token.
- AccessToken:
  The external roles are retrieved from the access token
- UserInfo:
  The external roles are retrieved from the UserInfo Endpoint of the external authentication provider

8.2.4.4 Role mapping rules

When you log on to the Mcenter server via the external authentication provider, the user roles are determined by

- the external roles
- the role mapping rules configured for the Identity Service

The claims with the RoleMappingClaimType type are used as external roles.

Role mapping rules

A role mapping rule consists of a list of external roles and a list of internal roles.
If you have all of the external roles listed in the mapping rule, the rule is applied. You receive the listed internal roles of the mapping rule.
All mapping rules are checked. Multiple rules can apply to the user.

Following roles and the internal names exist. Fore more information about the detailed rights, see "Operating Manual, Manage MyResources".

Displayed name	Platform role
Administrator	admin
Key user	service_technician
Manufacturing engineer	manufacturing_engineer
Technologist	technologist
NC Programmer	nc-programmer
Production planner	production_planner
Tool presetting operator	tool_presetter
Logistician	logistics
NC Programmer expert	nc-program_expert
Machine operator	machine_operator
Maintenance engineer	maintenance_engineer

Examples

1. If you have the external_admin role at the external authentication provider, you are assigned the admin role on the Mcenter server.
```
{
    "externalRoles": [
        "external_admin"
    ],
    "internalRoles": [
        "admin"
    ]
}
```
2. If you have the engineer role at the external authentication provider, you are assigned the manufacturing_engineer and the maintenance_engineer roles on the Mcenter server.
```
{
    "externalRoles": [
        "engineer"
    ],
    "internalRoles": [
        "manufacturing_engineer", "maintenance_engineer"
    ]
}
```

8.3 Configuring Tool statistics

Before starting the application Manage MyResources /Tools installation, it may be necessary to configure the Tool statistics.

Parameters

- Location of the configuration file:
  \SINUMERIK_Integrate_5\MMR\SinInt.MMRClient.Service\Configurations\
- Name of the configuration file
  dts.json

The most important parts of the configuration file are as follows:

Parameter	Description
`name`	Read only The name of the configuration must be `channel_toolstat`.
buffer	
`firstLevelMaxFiles`	The maximum number of events that can be buffered on the machine. It should be between 10 and 5000.
`bufferSizeInMb`	The size of the buffer in MB. It cannot be less than 1 MB.

Example of a dts.json file

1. Open the configuration file:

```
{
    "channels": [
        {
            "name": "channel_toolstat",
            "processInExtendedOverload": true,
            "collector": {
                "persistCollection": true,
                "collectorDurationInSeconds": null
            },
            "buffer": {
                "firstLevelMaxFiles": 5000,
                "bufferSizeInMb": 10
            }
        }
    ]
}
```

2. Perform an IIS reset after the adjustment.

Note

Functionalities of the Tool statistics

If other parts of the configuration are changed, or if the values of the changes are not supported, the functionalities of the Tool statistics might not be working.

8.4 Deactivating Tool statistics

Tool statistics is activated by default. To deactivate Tool statistics, modify the configuration file "mmrConfig.json"

Parameters

Property	Usage	Description
`toolStatisticsEnabled`	optional	Specifies if Tool statistics data collection is activated. Possible values: • `true`: The Tool statistics data collection is activated (default). • `false`: The Tool statistics data collection is deactivated

Procedure

1. Open or create the file "mmrConfig.json" on SINUMERIK as specified, see 1:1-Exchange (Page 241).
   To locate the directory for the configuration file “mmrConfig.json” , see Directory for configuring file "mmrConfig.json" (Page 248).
2. Extend the content of the file with a section `toolStatisticsEnabled` as described above.
   Example:
```
{
   ...
 },
"toolStatisticsEnabled": false
 }
}
```
3. Restart the HMI for the new settings to take effect.

8.5 Increasing system responsiveness

To increase the system responsiveness, reduce the processing time of the changes in MMR / Tools. Use the following internal settings in the configuration file "mmrConfig.json".

These internal settings only apply to SINUMERIK Operate machines.

The internal settings are ignored, if Tool statistics is deactivated. For more information see Deactivating Tool statistics (Page 171).

Parameters

Property	Usage	Description
changesProcessing	optional	Specifies parameters for processing changes in MMR /Tools.
bulkSize	mandatory if `changesProcessing` is specified	Specifies the number of processed changes at a particular time. It has to be chosen such that both MMR /Tools actual information updates are carried out at an adequate rate and no unprocessed changes occur. This applies to • the client and server UI • the server database

Procedure

1. Create the file "mmrConfig.json" or open it if it already exists.
   For more information, see
   – 1:1-Exchange (Page 241)
   – Directory for configuring file "mmrConfig.json" (Page 248)
2. Extend the file content with a "`changesProcessing`" section.
   Example:

```
{
  ...
 },
 "changesProcessing": {
 "bulkSize": 50
 }
}
```

3. Restart the HMI for the new settings to take effect.

Note

Loss of unprocessed changes

If MMR /Tools detects a loss of unprocessed changes, it logs a corresponding error in the MMR script log file.
Example: Error

```
RingBufferStrategy.getChanges() Detected losses in RingBuffer
changes! Try to increase changesProcessing.bulkSize parameter in
mmrConfig.json
```

In this case, increase the `bulkSize` parameter in the mmrConfig.json file.

8.6 Switch off the info on external view

You can switch off the info on external view that there are more then 100 tools available on the Server. The information window that more then 100 tools are available on the server for the machine in the hierarchy path can be switched of with an entry within mmrconfig.json.

Parameters

Property	Usage	Description
incompleteListInfoIntervalIn-Hours	optional	This is not a mandatory entry. If it is not with in the mmrconfig the default value is 8. That means the external Tools info Message is shown once after new restart of HMI after that this info is disabled for the next eight hours. The user can use a different number. It is set in hours.

Procedure

1. Create the file "mmrConfig.json" or open it if it already exists.
2. Extend the file content with a " incompleteListInfoIntervalInHours " section.

Example:

```
{
...
},
"incompleteListInfoIntervalInHours": 1
}
```

1. Restart the HMI for the new settings to take effect.

8.7 Synchron double spindle machines

The toolstatistics now support machines which have a synchronous double spindle configuration. In these machines, the ToolChange and ToolCutEnd events will be duplicated for each of the spindles. The ToolCutEnd events have the same cutting and idle time for each of the spindles. The tool specific parameters are however different for each spindle. The typical design of the spindles is that both are located in one channel on the machine.

Parameters

Property	Usage	Description
simultaneousSpindlesEnabled	optional	This property is needed for collecting the events

Procedure

1. Create the file "mmrConfig.json" or open it if it already exists.
2. Extend the file content with a " incompleteListInfoIntervalInHours " section.

Example:

```
{
...
},
"simultaneousSpindlesEnabled": true,
}
```

Installing SINUMERIK Integrate client

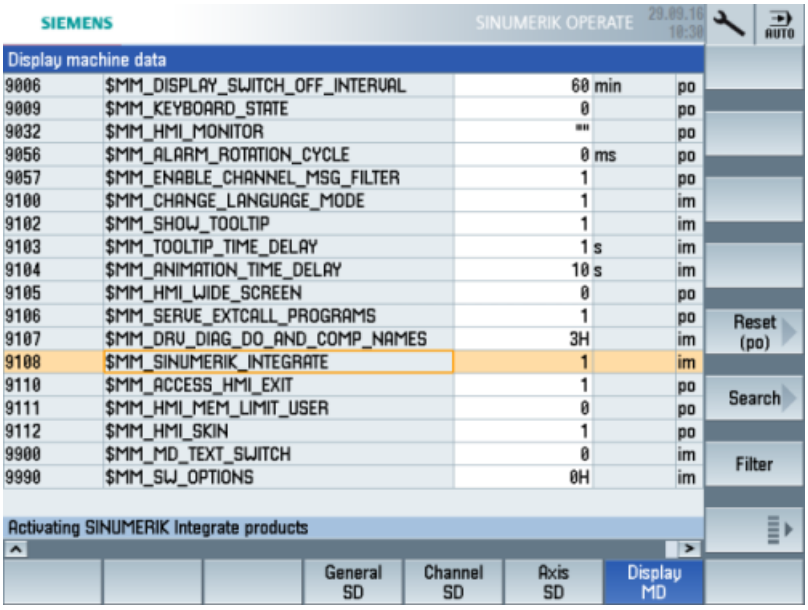
9

9.1 Mcenter with SINUMERIK Operate

9.1.1 Activating Mcenter products

Procedure

1. Start the SINUMERIK Operate operating software on the control.
2. Press the "Setup" and "Mach. data" softkeys.
3. Press the menu forward key and the "Display MD" softkey.
4. Set the machine data
   MD9108 $MM_SINUMERIK_INTEGRATE to "1".



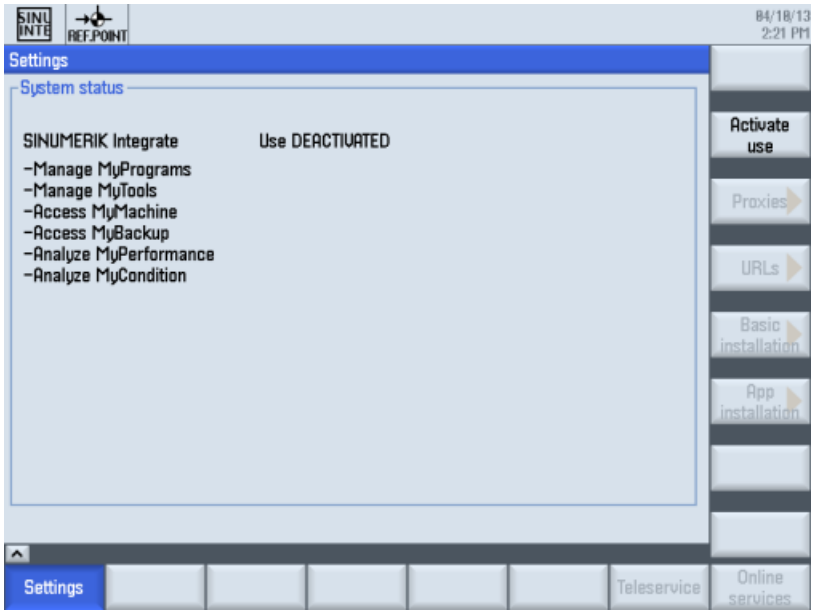
5. The "SINUMERIK Integrate" softkey is displayed on the extended horizontal softkey bar.

9.1.2 Enabling use

Procedure

To activate utilization of the products, proceed as follows:

1. Press the "SINUMERIK Integrate" softkey.
   The "Welcome" window opens.
2. Press the "Settings" softkey.
   The "Settings" window opens displaying the system status "Use DEACTIVATED".



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

9.1.3 Configuring the URL and proxy

Note

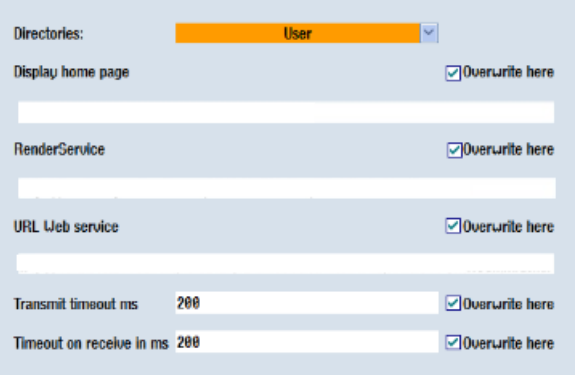
Transferring SINUMERIK data to the Mcenter platform

The following steps allow you to transfer the SINUMERIK data to the Mcenter 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.

Procedure

1. The "Settings" window is open.
   Press the "URLs >" softkey.
2. Press the "Edit" softkey and select the following settings:
   - Directories: Select the "User" entry in the "Directories" drop-down list.
   - Display home page: You do not have to enter any URL or you can leave the default setting.
   - RenderService: You do not have to enter any URL or you can leave the default setting.
   - URL Web service: Activate the "Overwrite here" checkbox.
   - Enter the following URL web service:
     Server port (http://<ipaddress>:SERVERPORT/Platform/SinInt.MhComm.Service/MHComm/MHComm.asmx)
     - OR -
     Platform (https://<hostname.domain>/Platform/SinInt.MhComm.Service/MHComm/MHComm.asmx)



3. Press the "OK" softkey.
   A syntax check is performed. The access data is saved.
4. Restart the control system.

9.1.4 Installing the Client update

An update from the SINUMERIK Integrate Client is only supported as of SINUMERIK Operate version 4.5.4.

If you upgrade SINUMERIK Operate from version 4.5.3 (or older) to version 4.5.4 (or later), you must delete the existing service entries from the configuration file "systemconfiguration.ini" manually.

The configuration file can be found in the following directories:

- Windows XP: F:\hmisl\user\sinumerik\hmi\cfg
- Windows 7: C:\Program Files (x86)\Siemens\MotionControl\user\sinumerik\hmi\cfg
- Linux: card/user/sinumerik/hmi/cfg

Procedure

1. Open the "systemconfiguration.ini" file.
2. Delete the following lines:
   - SVC013 ...
   - SVC014 ...
   - SVC015 ...
   - SVC017 ...
3. Save and close the file.
4. Delete the following files, if applicable:
   - systemconfiguration.ini.453
   - systemconfiguration.xml

9.1.5 Client update

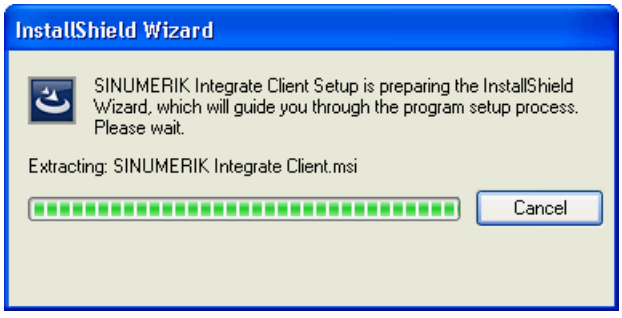
9.1.5.1 Client update under Windows

Requirement

If not installed, install the PCU Base Software from 01.04.00.00 before starting the SINUMERIK Integrate client update.

Procedure

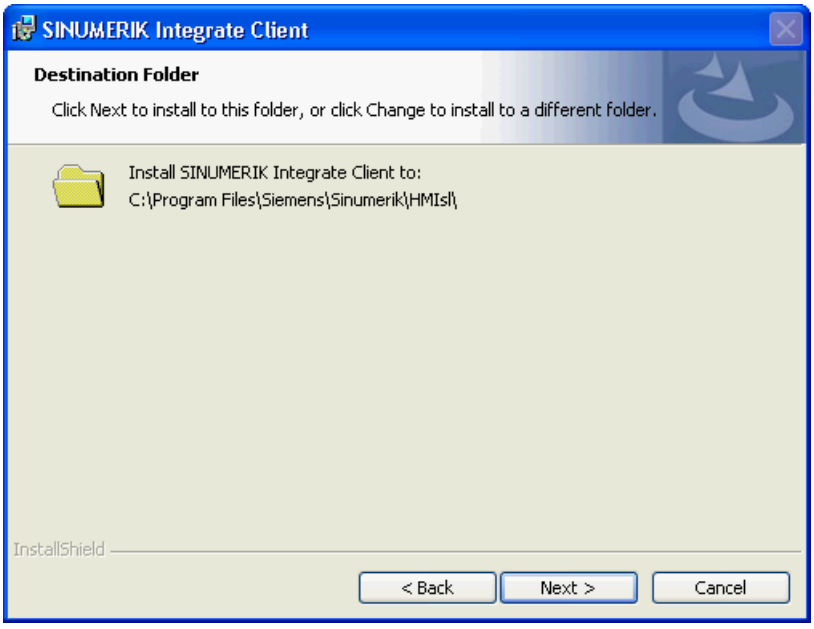
1. Start the PCU in the Windows service mode.
2. Open the installation directory on the PCU.
3. Start setup file "setup.exe" with a double-click.
   SINUMERIK Integrate Client - InstallShield Wizard opens.



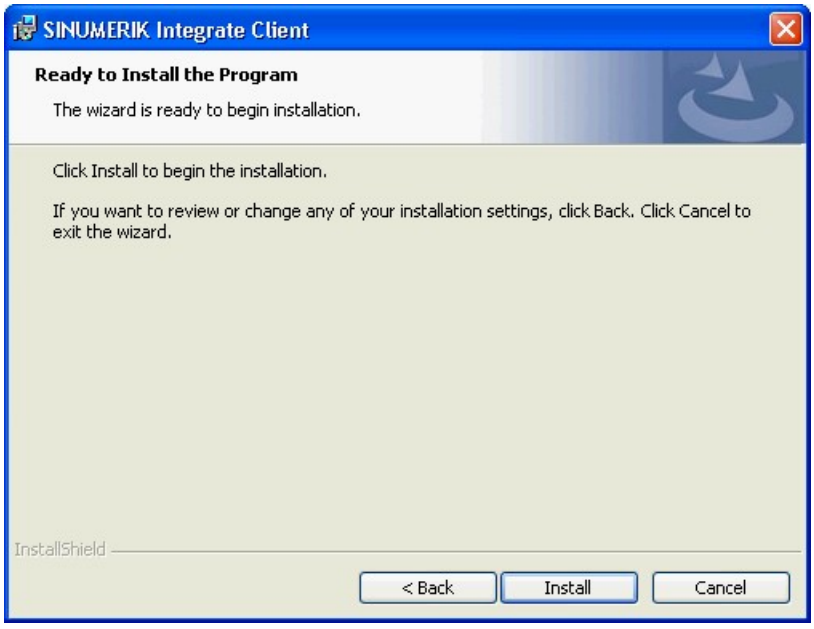
4. The welcome dialog opens and the current version number is displayed.
   The installation language is English.
   Click "Next >" to prepare for the installation.

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.

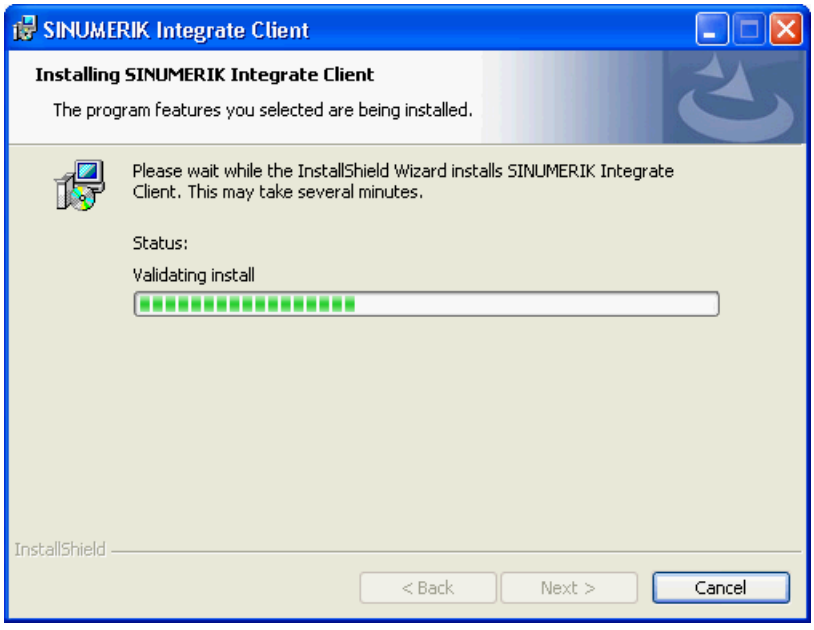
6. The next window displays the installation directory for the application.
   Click "Next >" to accept the directory suggested by the setup.



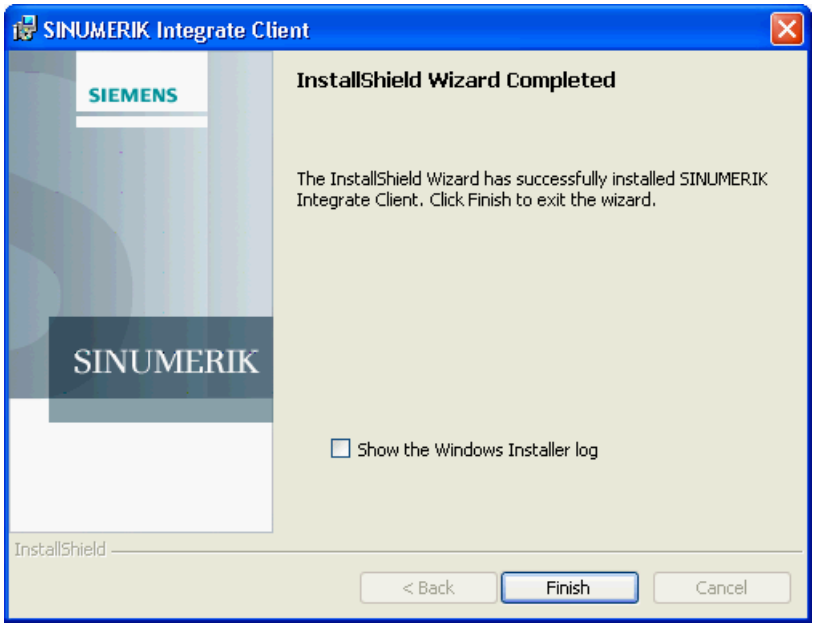
7. The Wizard is ready to start the installation.
   Click "Install" to start the installation.



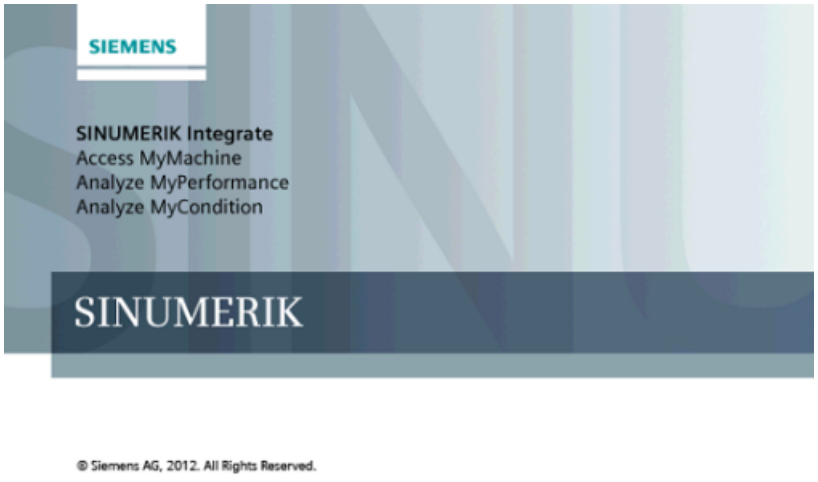
8. The installation is started, and the progress is displayed with a progress bar.



9. Click "Finish" to complete the installation.



10. Finally, an overview of the applications that the client can use is shown.



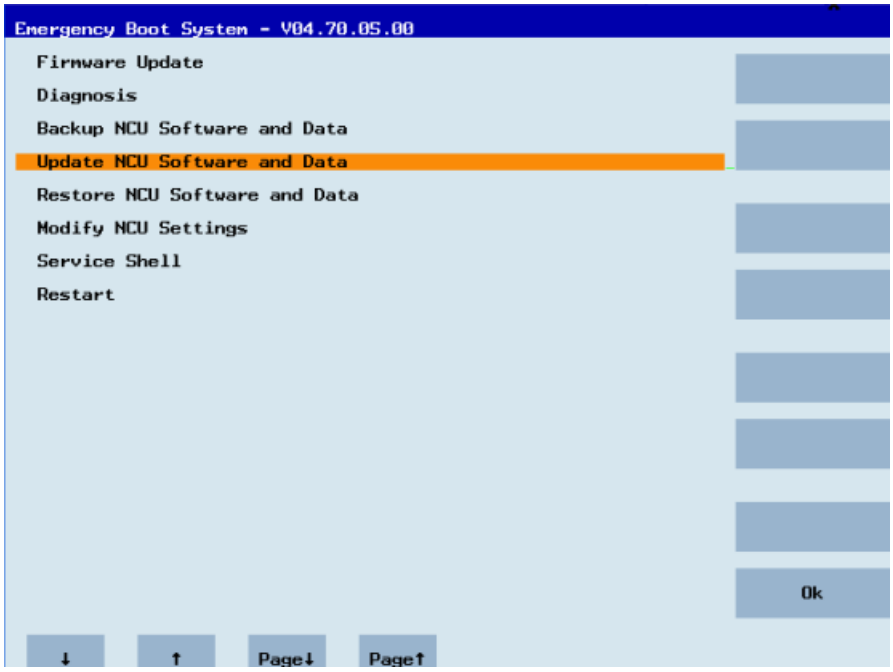
9.1.5.2 Client update under Linux

Prerequisite

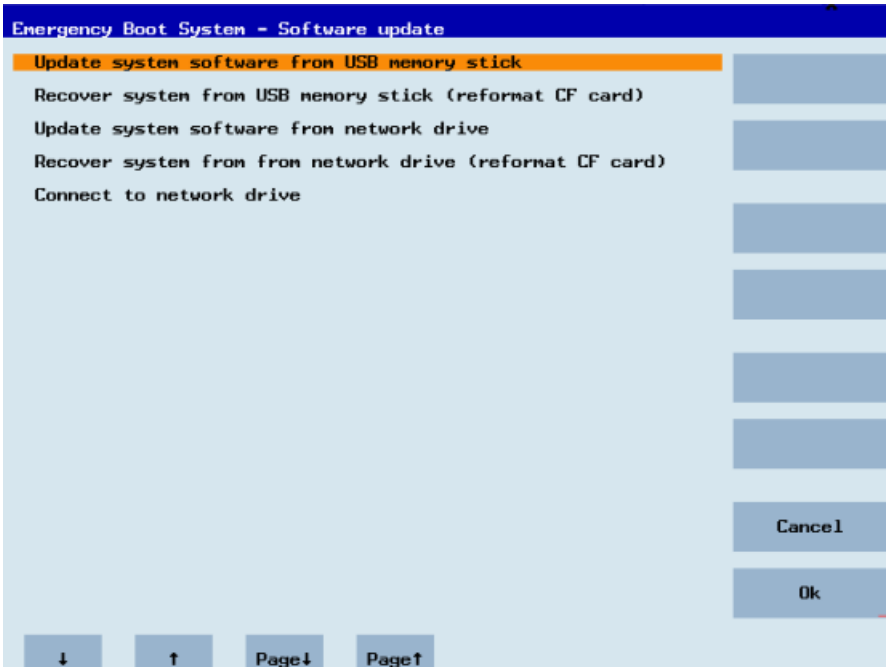
- Emergency Boot System as of Version 04.70.05.00
- SINUMERIK Operate as of Version 4.5 SP4
  - OR -
- SINUMERIK Operate as of Version 4.7 SP2

Procedure

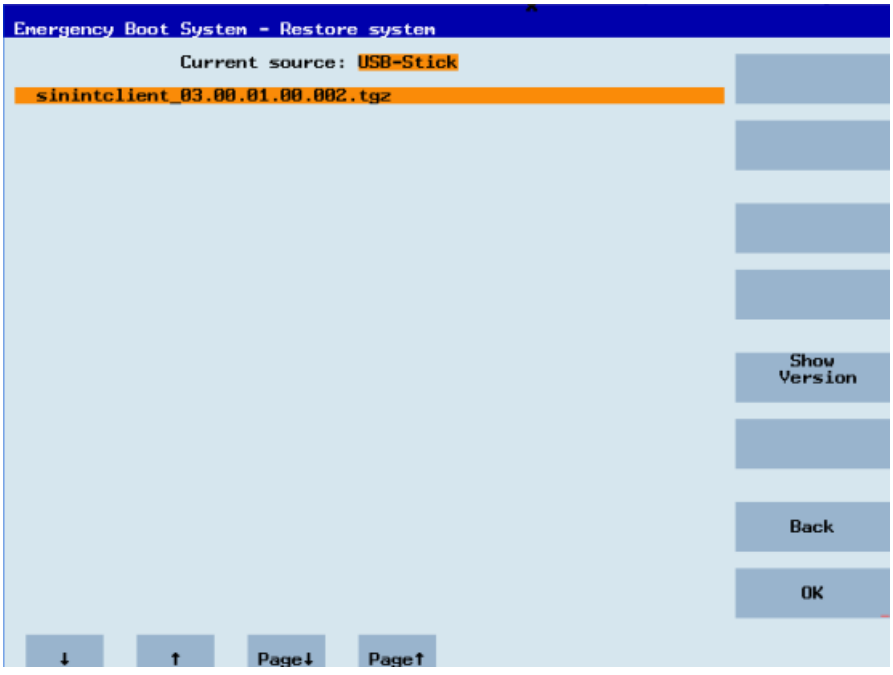
1. Copy the "sinintclient.tgz" file to the USB flash drive.
2. Insert the USB flash drive into the NCU.
3. Start the NCU.
4. In the menu, select "Update NCU Software and Data" with the cursor keys and press the "OK" softkey.



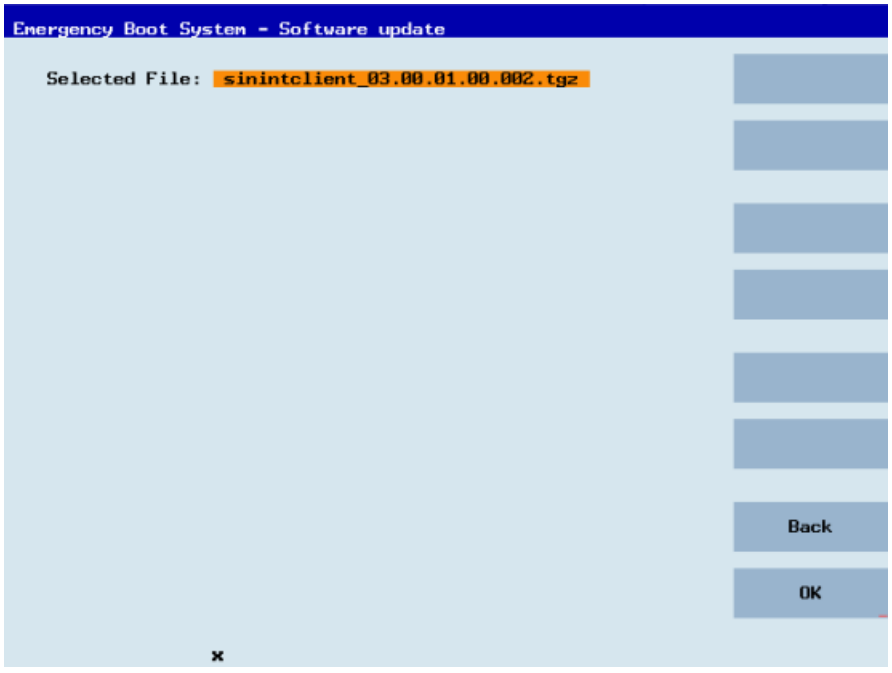
5. In the menu, select "Update system software from USB memory stick" with the cursor keys and press the "OK" softkey.



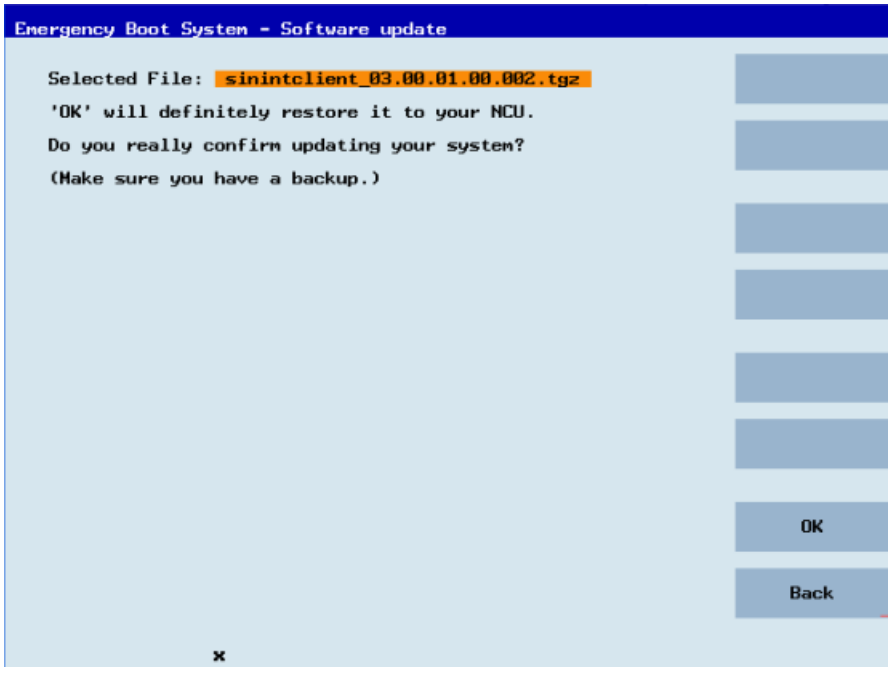
6. You receive a list with all tgz files.
   Select the current file.
   Press the "OK" softkey to confirm your selection.
   - OR -
   Press the shortcut key <Shift> + <F8> on the operator panel.



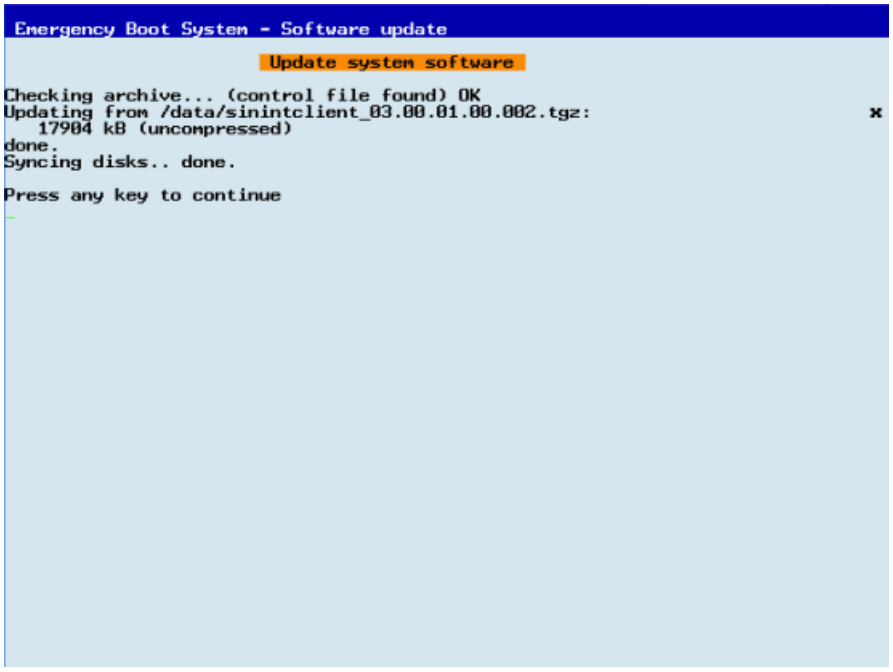
7. The selected file is displayed.
   Press the "OK" softkey to confirm your selection.
   - OR -
   Press the shortcut key <Shift> + <F8> on the operator panel.



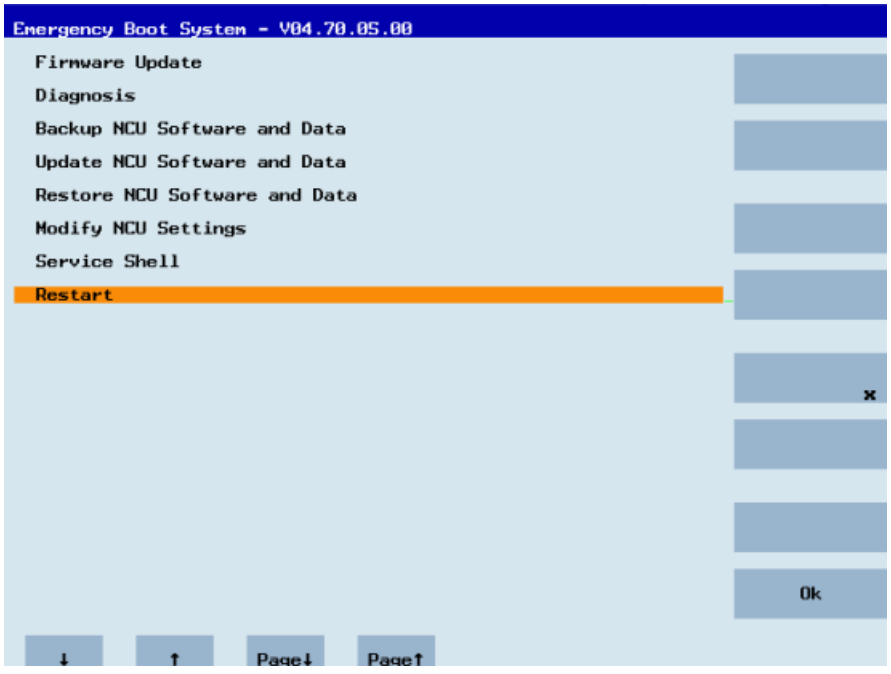
8. A confirmation prompt appears.
   Press the "OK" softkey to confirm the confirmation prompt.
   - OR -
   Press the shortcut key <Shift> + <F7> on the operator panel.



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.



9.1.6 Connecting to different Mcenter server

You have the option of connecting an already connected controller to another Mcenter server.

Procedure

1. Uninstall the currently assigned application to your controller, if you have any.
2. Delete the already connected controller from the Mcenter server.
   You must delete manually data for:
   - Sinumerik Operate on Linux:
     File: card/user/sinumerik/hmi/cfg/machineConfig.xml
     - AND -
     The following folder: /var/tmp/Si5
   - Sinumerik Operate on windows:
     The file <Install path>\Siemens\MotionControl\user\sinumerik\hmi\cfg
     \machineConfig.xml
     - AND -
     The following folder: C:/temp/Si5
     - OR -
     F:/tmp/Si5
3. For more information, see Connecting applications with the SINUMERIK control system (Page 225).

9.2 Mcenter with HMI-Advanced

9.2.1 Installing SINUMERIK Integrate client

If the SINUMERIK Integrate Client has already been installed, this must first be uninstalled.

The procedure for installation for the first time is explained below.

Prerequisite

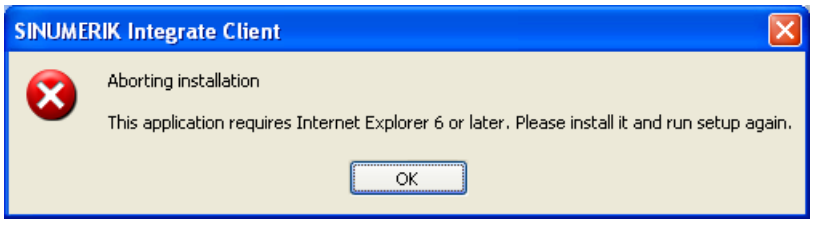
You installed Internet Explorer 6 or higher.

Procedure

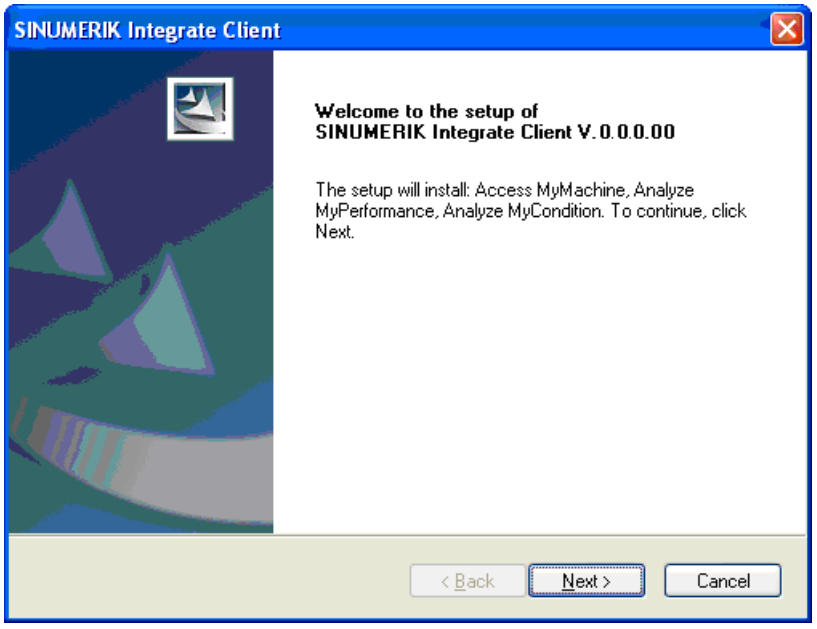
Start installation

1. Start the PCU in the Windows service mode.
   OR
   You have to have administrator rights.
2. Open the following directory: SI5\Clients\SinIntClient\HMI Advanced.
3. Copy the "eps_client_AT.exe" setup file into the installation directory on the PCU.

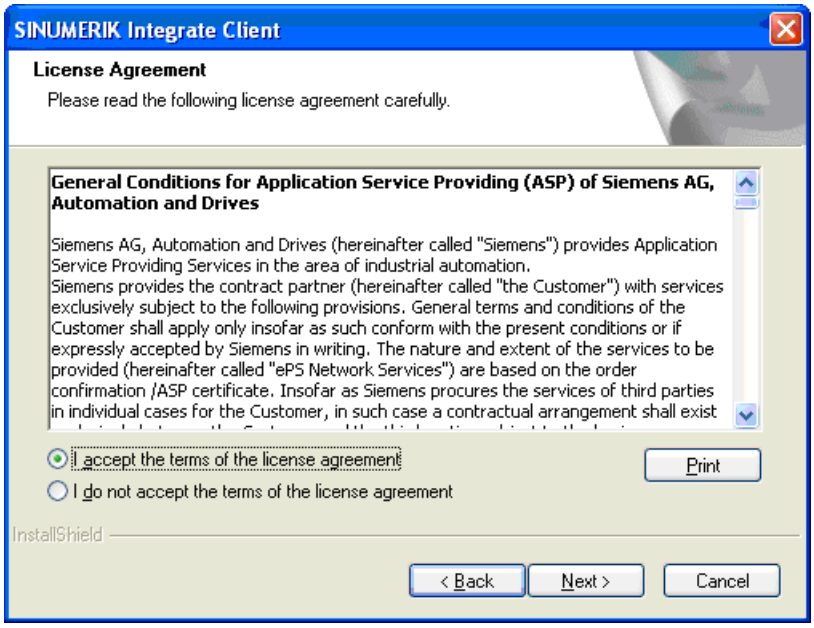
4. Start the "eps_client_AT.exe" setup file by double-clicking.
   If you have not installed the appropriate Internet Explorer, a corresponding message is displayed. For example, the program requires Internet Explorer 6 or higher.
   The installation is aborted and you must first install the appropriate Internet Explorer.
   Then restart the client installation.



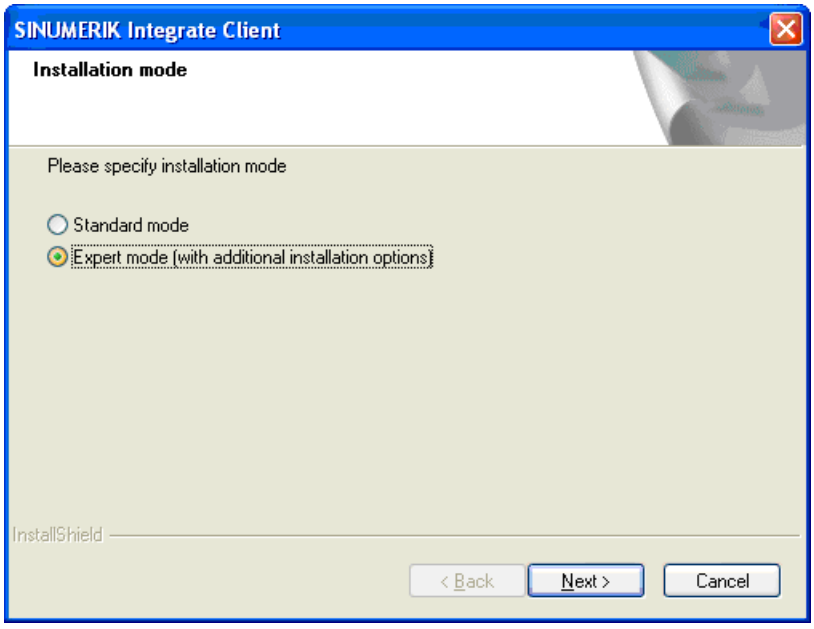
5. The welcome screen opens and displays the current version number (in place of "V.0.0.0.00", the current version number is displayed on the control system).
   The installation language is English.
   Click "Next >" to prepare for installation.



6. The "License Agreement" window opens.
   Read the license agreement.
   – Click "Print" if you want to print out the conditions.
   – Then activate the "I accept the terms of the license agreement" checkbox and click "Next >".
     - OR -
     Click "< Back" to return to the previous window.

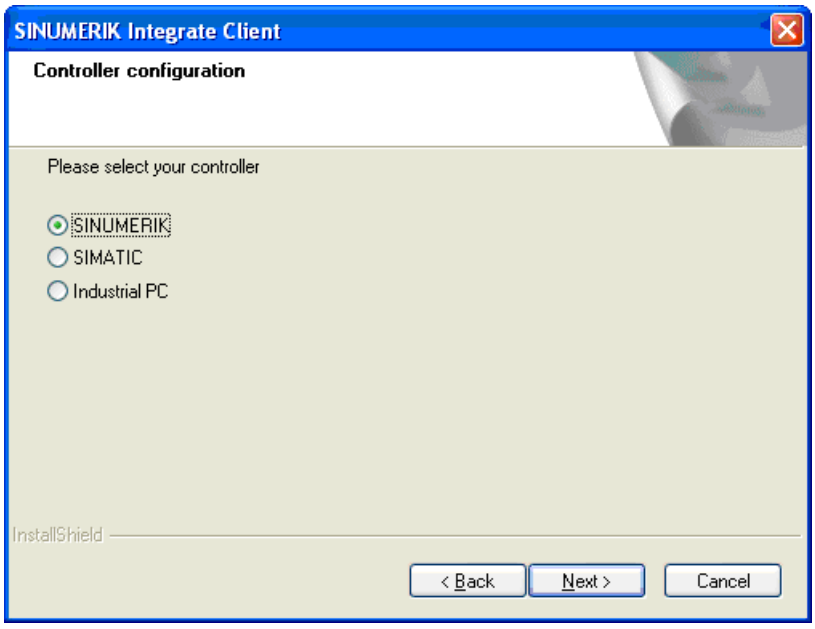


7. The "Installation mode" window opens.
   To change the preconfigured settings individually, select "Expert mode (with additional installation options)".
   Click "Next >".

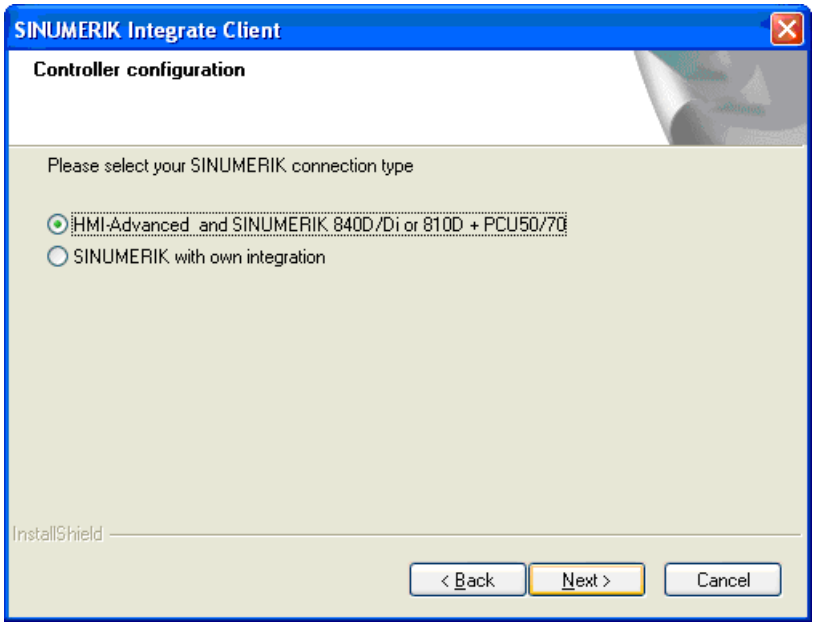


Configuration

1. The "Controller Configuration" window opens.
   Select "SINUMERIK".
   Click "Next >".

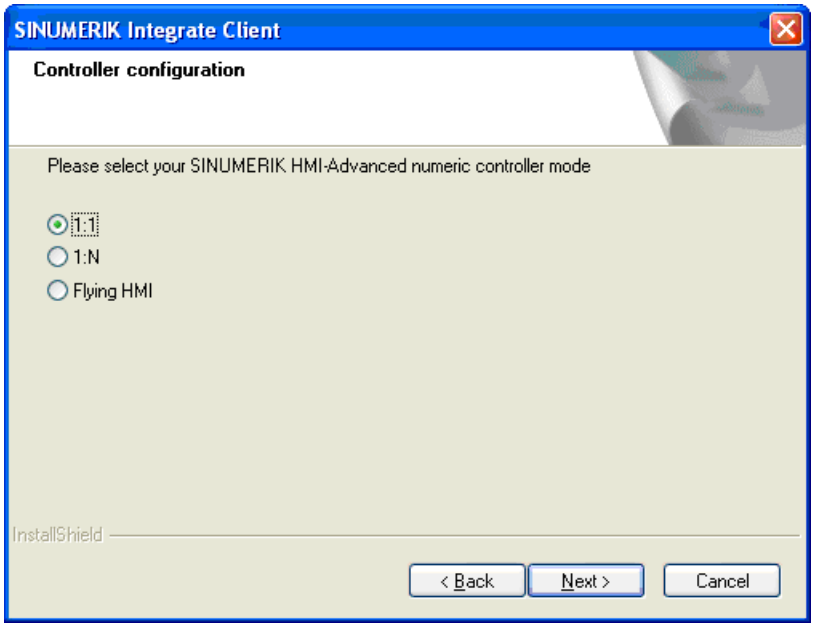


2. The SINUMERIK connection types are displayed in the "Controller Configuration" window.
   If you are working in a networked environment, select "HMI-Advanced and SINUMERIK 840D/Di or 810D + PCU50/70".
   - OR -
   If separately integrated, for example via HMI Pro, then select "SINUMERIK with own integration".

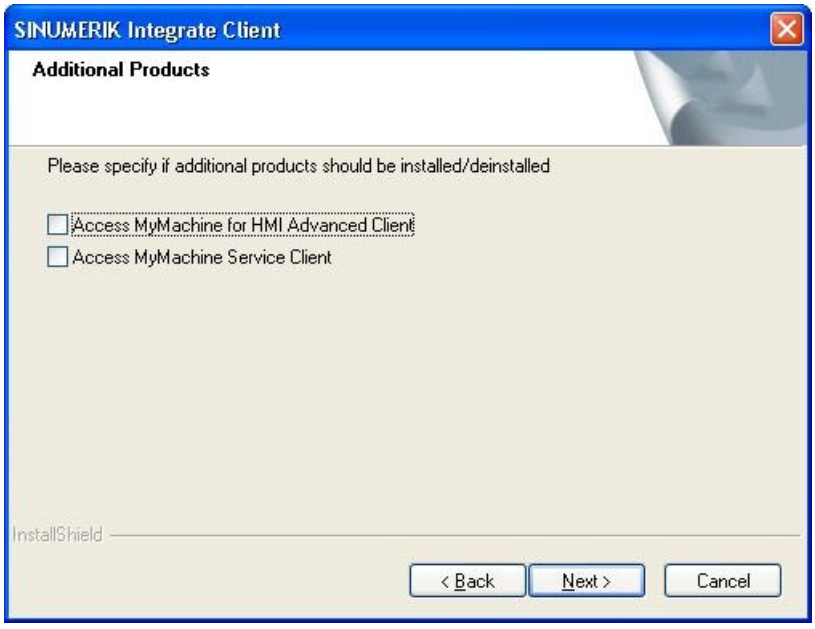


3. Select the connection type in the next window:
   - "1:1"
     The function allows a direct connection to a SINUMERIK controller.
   - "1:N"
     The function allows a connection in a group to several SINUMERIK controllers.
   - "Flying HMI"
     The function allows the use of Mcenter on a SINUMERIK controller on which a client cannot be installed because the operating software does not support this client. In this case, Mcenter is installed and configured on a workplace PC or machine PC (IPC). PC/IPC and SINUMERIK controller communicate via a (W)LAN connection.

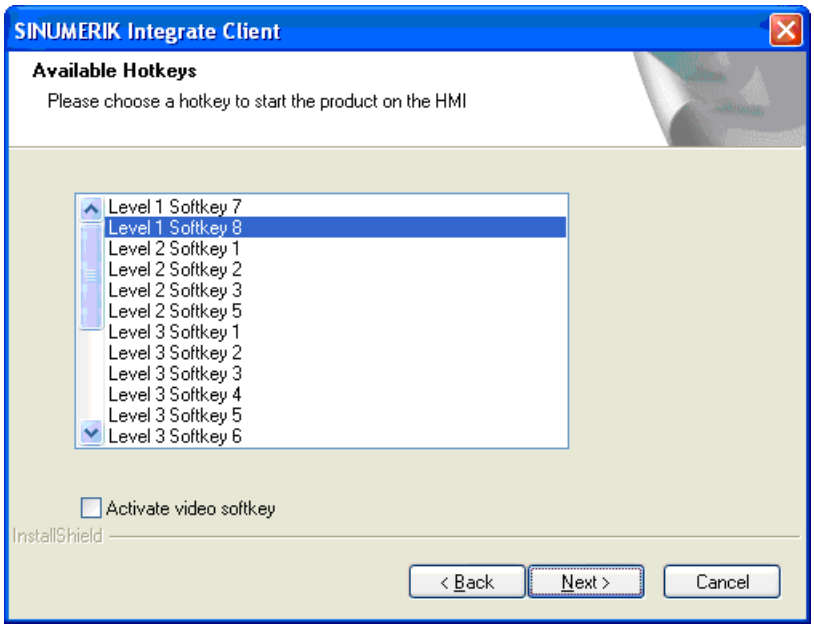
   Select connection type 1:1.
   Click "Next >".



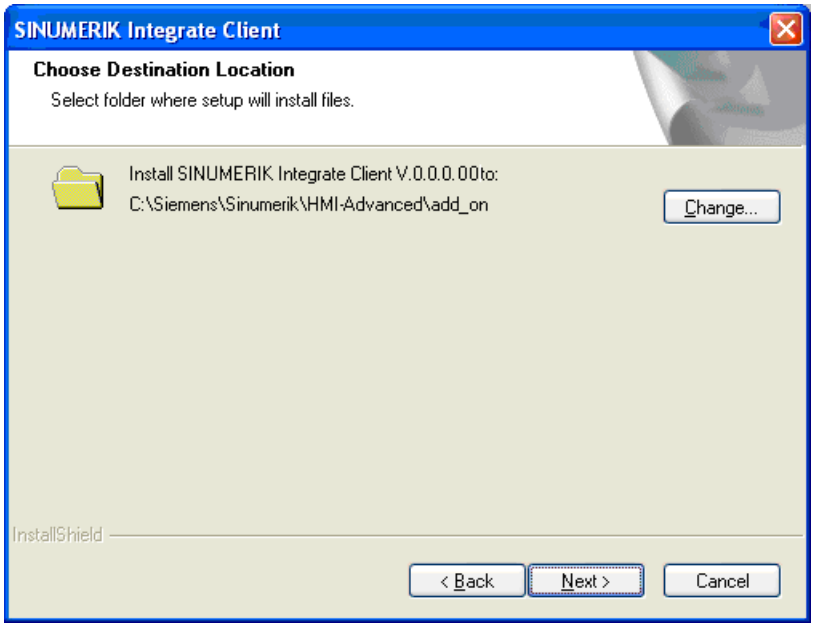
4. The "Additional Products" window opens.
   Do not check **any** of the checkboxes and click on "Next >".



5. If you select "HMI softkey to start the product on the machine", the "Available Hotkeys" window opens.
   From the drop-down list, select the position of the softkey with which you want to start the application on the user interface.
   Click "Next >".

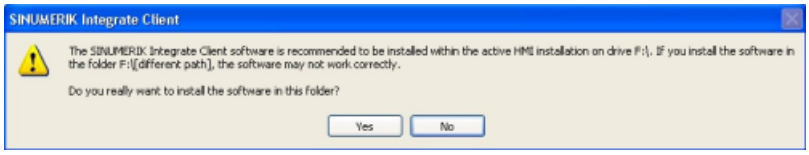


- OR -
If you selected "Expert mode" installation type, the "Choose Destination Location" window opens.
The installation directory is displayed.
If you want to use a different directory, click "Change..." and enter the required directory.

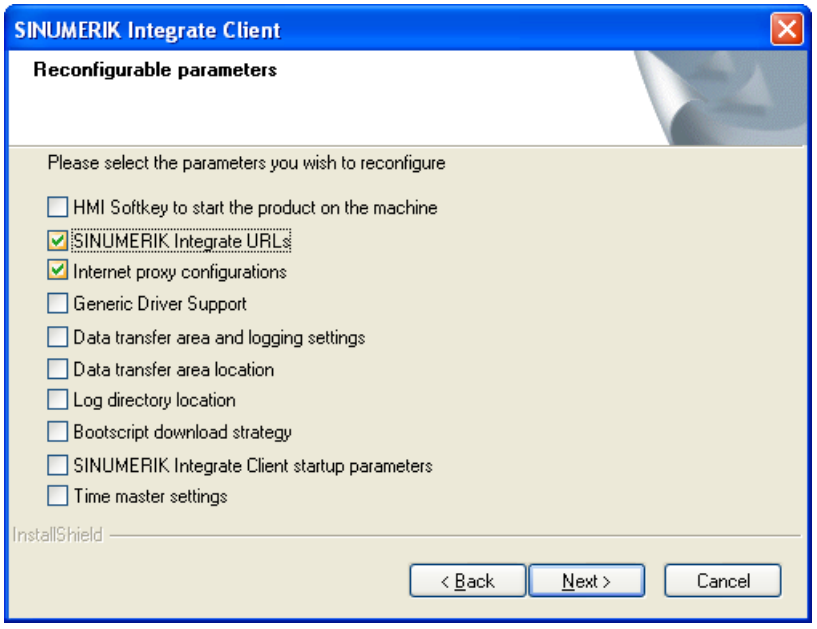


If you want to change the default directory, the following confirmation warning is displayed:

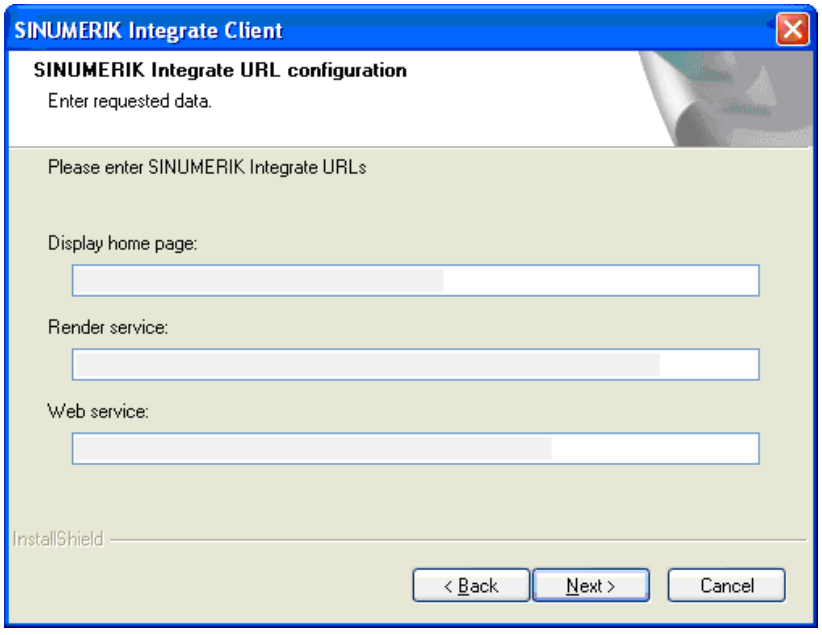
– Click "Yes" to change the path.
  - OR -
– Click "No" to cancel any changes.



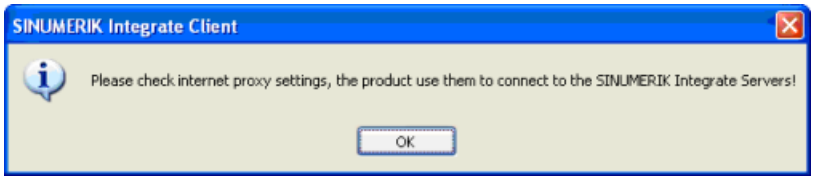
6. The "Reconfigurable parameters" window opens.
Check the "SINUMERIK Integrate URLs" checkbox.
- AND -
Check the "Internet proxy configurations" checkbox.



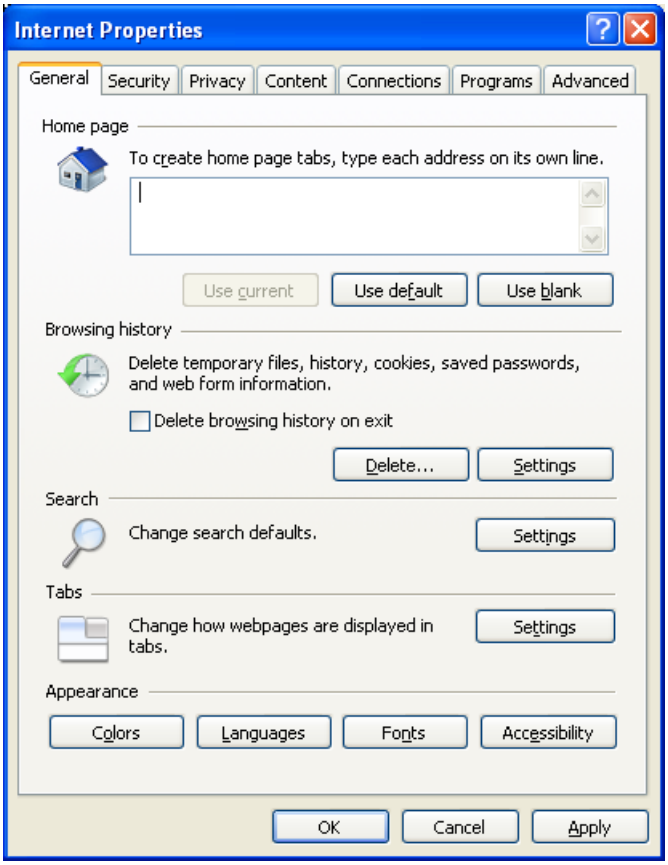
7. The "SINUMERIK Integrate URL configuration" window opens.
   Enter the following web service:
   - In case of http communication: http://<ipaddress>:SERVERPORT/Platform/SinInt.MhComm.Service/MHComm/MHComm.asmx
     - OR -
   - In case of https communication: https://<ipaddress>/Platform/SinInt.MhComm.Service/MHComm/MHComm.asmx



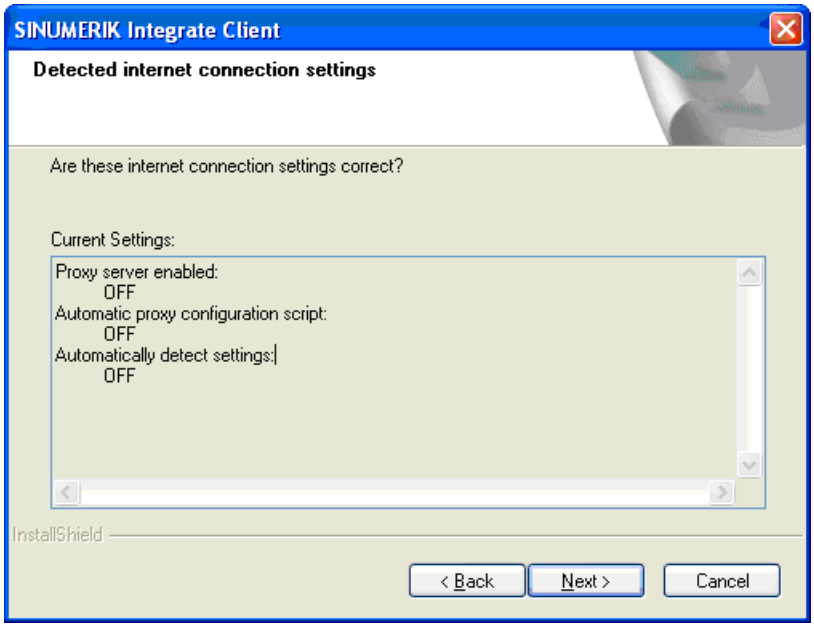
In the following prompt, you are requested to check the address settings.
Confirm the prompt to check the Internet settings with "OK".



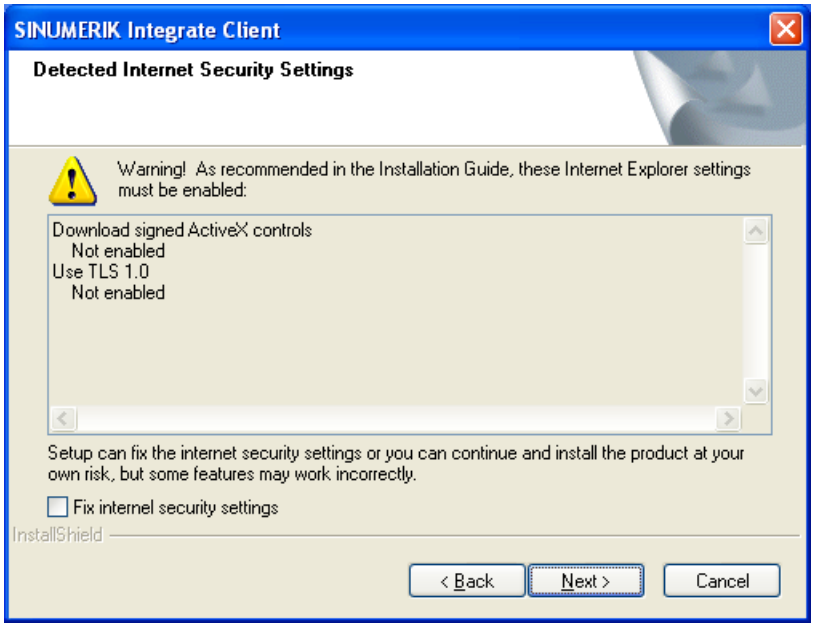
8. The "Internet Properties" window opens.
   The address is specified under the "General" tab in order to create the start page tabs.
   Click the "Connections" tab to set up the Internet connection and to configure the LAN settings.
   Use the connection in your company network that has already been set up.
   Click "OK".



9. The "Detected Internet Connection Settings" window opens and shows the actual settings.
   Click "< Back" to correct the settings.
   Click "Next >" to continue.

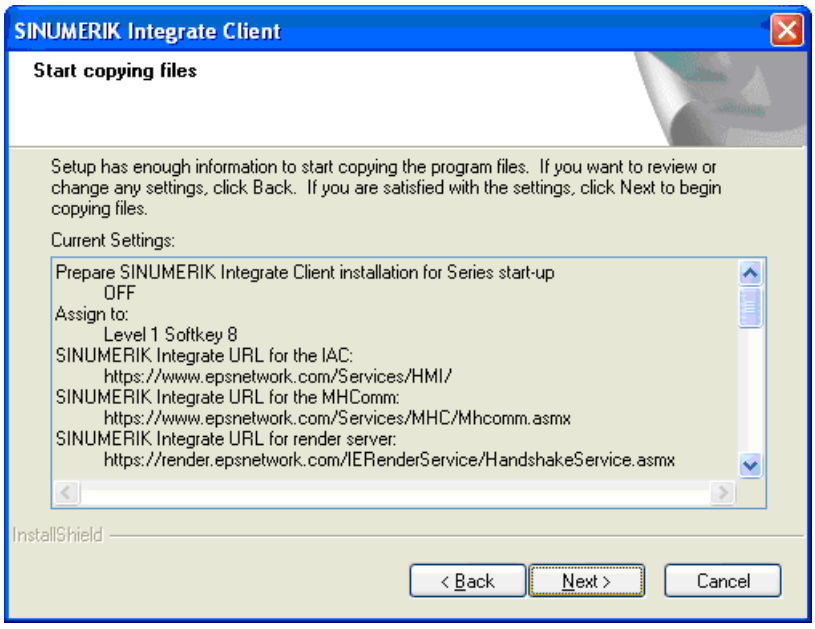


10. The settings are subject to an additional check, and an appropriate message is displayed in the "Detected Internet Security Settings" window.
    Click "< Back" to change the settings in the Internet Explorer.
    - OR -
    Activate the checkbox "Fix internet security settings" to permit the displayed settings.
    Click "Next >" to continue.

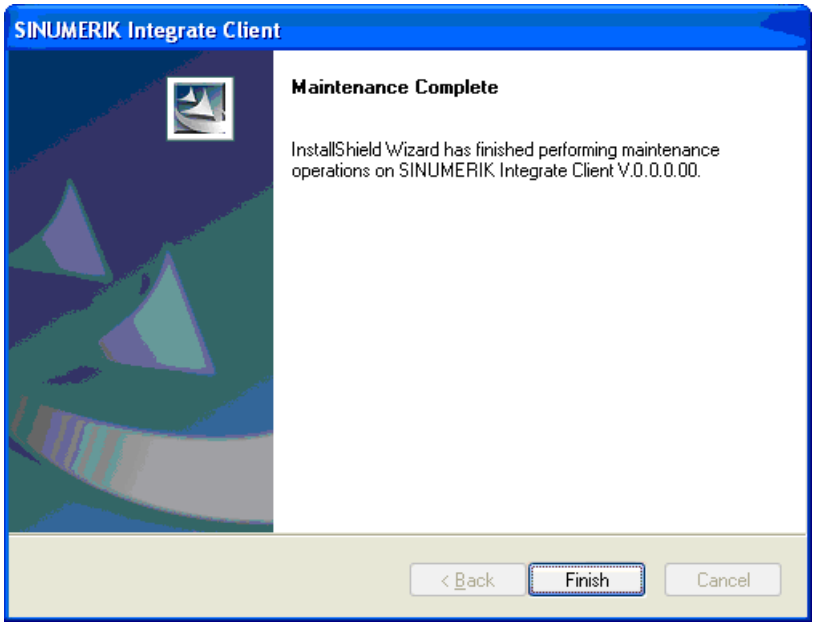


Completing the installation

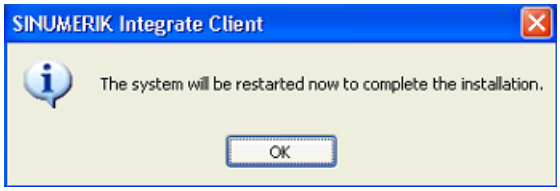
1. The "Start Copying Files" window opens and shows an overview of the settings that you have made.
   Click "Next >" to start the installation.



2. The "Maintenance Complete" window opens.
   Click "Finish" to complete the installation.



3. You are prompted to restart the system after the installation has been completed.
   To do this, click "OK".



9.2.2 Integrating the client setup as external applications

Introduction

You have the option of calling the client setup from other applications, e.g. via TRANSLINE 2000 HMI PRO CS.

The call is configured via the TRANSLINE user interface.

Setup client with HMI-Advanced

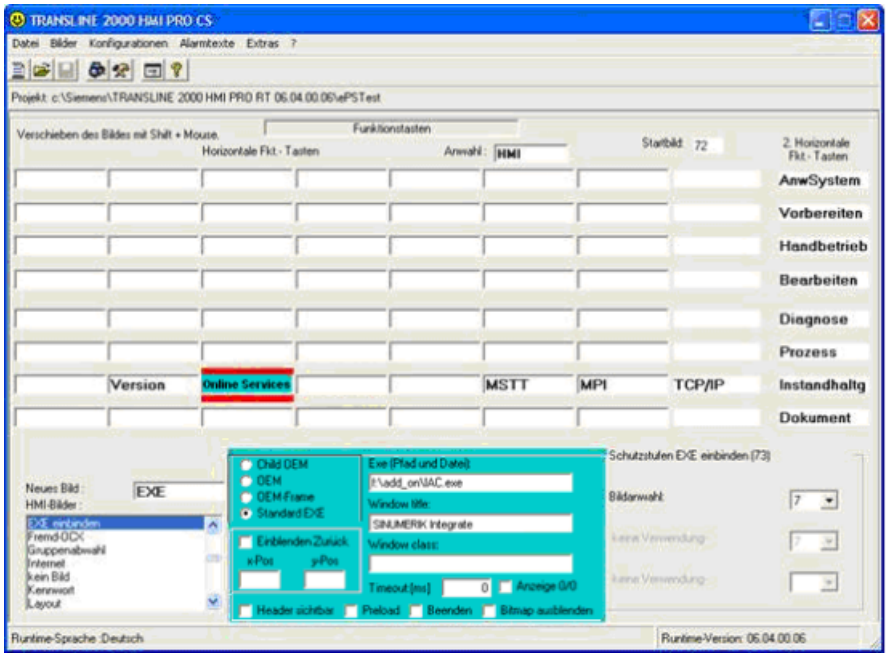
Within the external application, a softkey must be configured, which starts the "iac.exe" file.

Setup client without HMI-Advanced

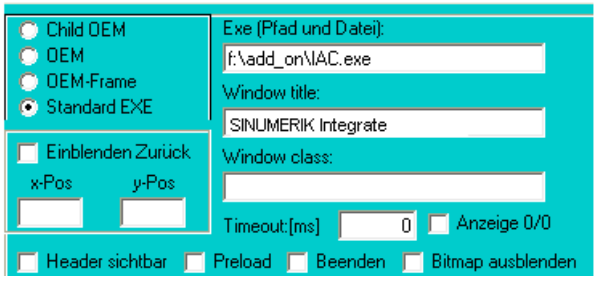
Within the external application, the "MhCtrlr.exe" file must be configured as a background process with the name "MhController".

Example: Setup client with HMI-Advanced

1. Select the menu "Configuration" and "Function keys".
   The following window is opened.
   - Under "New image", enter the softkey name, e.g. "EXE".
   - Define the softkey position using the <Shift> key + right mouse click.
   - In the selection list "HMI images", select the function "Integrate EXE.".



2. Make the other settings as follows:
   - In the option field, select "Standard EXE".
   - In the text field "Exe (path and file):" enter the following directory: "f:\add_on\IAC.exe"
   - In the text field "Windows title:" enter the title: "SINUMERIK Integrate"



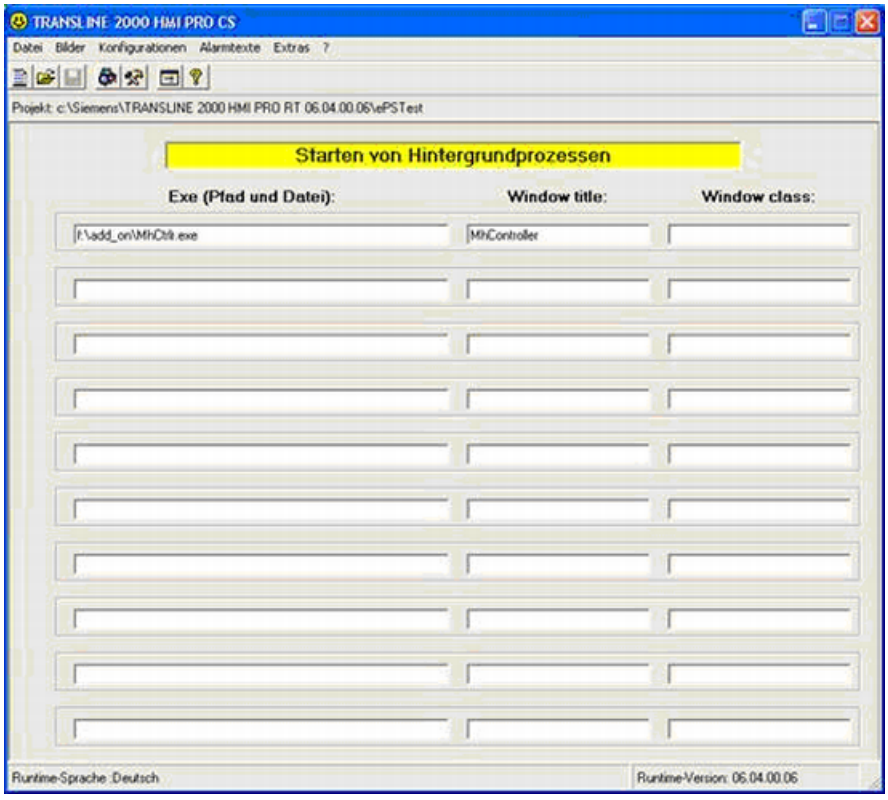
Example: Setup client without HMI-Advanced

1. Select the menu "Configuration" and "Start background processes".
   The following window is opened.
   - In the text field "Exe (path and file):" enter the following directory: "f:\add_on\MhCtrlr.exe".
   - In the text field "Windows title" enter the following title: "MhController"

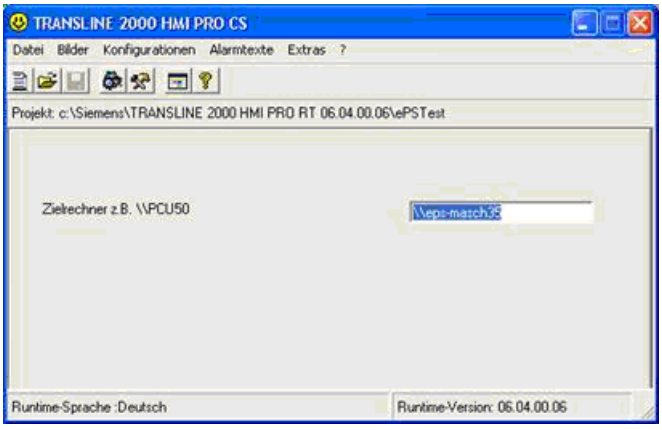
Note

If it is not allowed to start "MhCtrlr.exe" as a background process, it is started as a background task by the Regie (administrator) (e.g., Task88).

While installing in the control, ensure that the following connection type is not selected: "HMI-Advanced and SINUMERIK 840D/Di or 810D + PCU50/70".



2. Select the menu "File" and "Setting target computer", to configure the transfer of the project to the target computer, e.g. to the PCU.



- Select the menu "File" and "Installation of the system on PCU". The TRANSLINE system is transferred to the selected PCU and installed on the PCU with the HMI PRO setup.
- Select the menu "File" and "Installation of the project on PCU". The TRANSLINE project is transferred to the selected PCU and installed on the PCU with the HMI PRO setup.

9.2.3 Changing, repairing and uninstalling programs

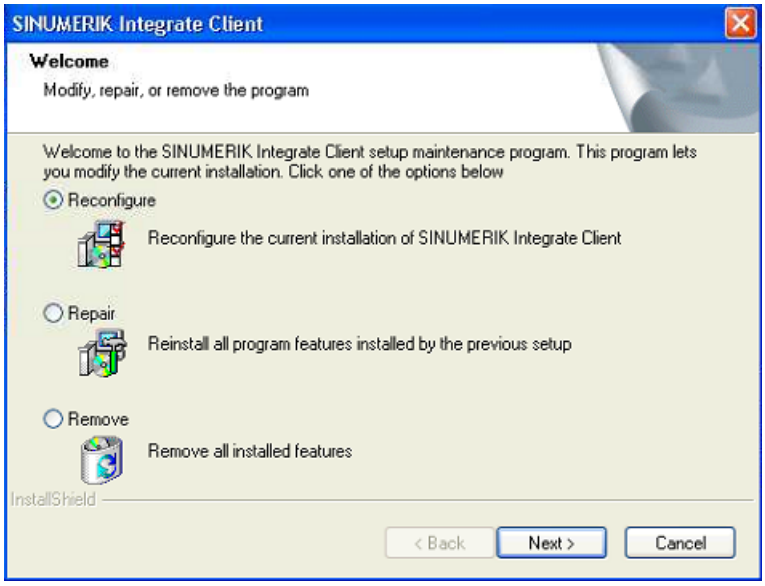
In an existing client setup, you have the option of changing, repairing or uninstalling installations.

Procedure

1. Start the PCU in the Windows service mode.
2. Open the installation directory.
3. Start the "eps_client_AT.exe" setup file by double-clicking.
4. The "Welcome" window opens and offers you the following options:
   - Changing the client setup
   - Repairing the client setup
   - Removing the client setup

Changing the client setup

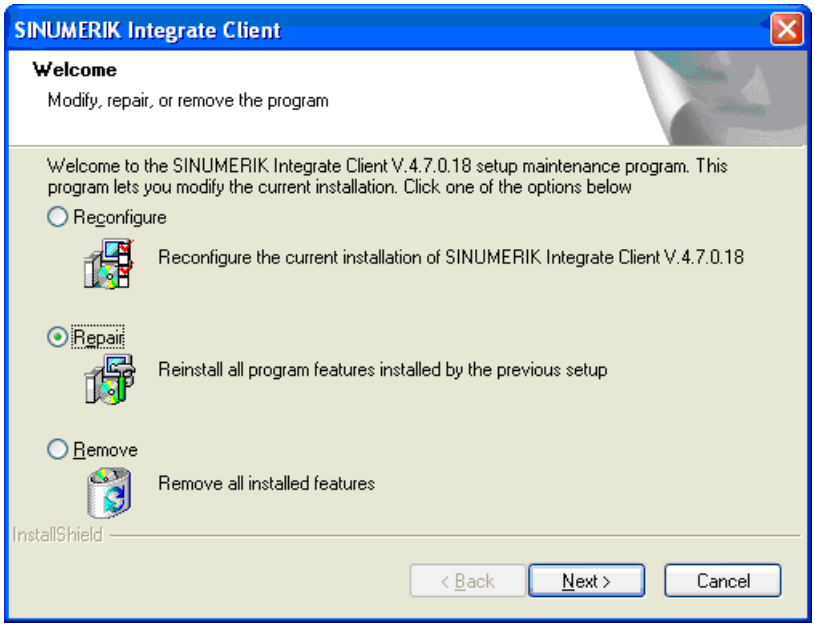
1. In the "Welcome" window, select the "Reconfigure" function if you want to change the client version.



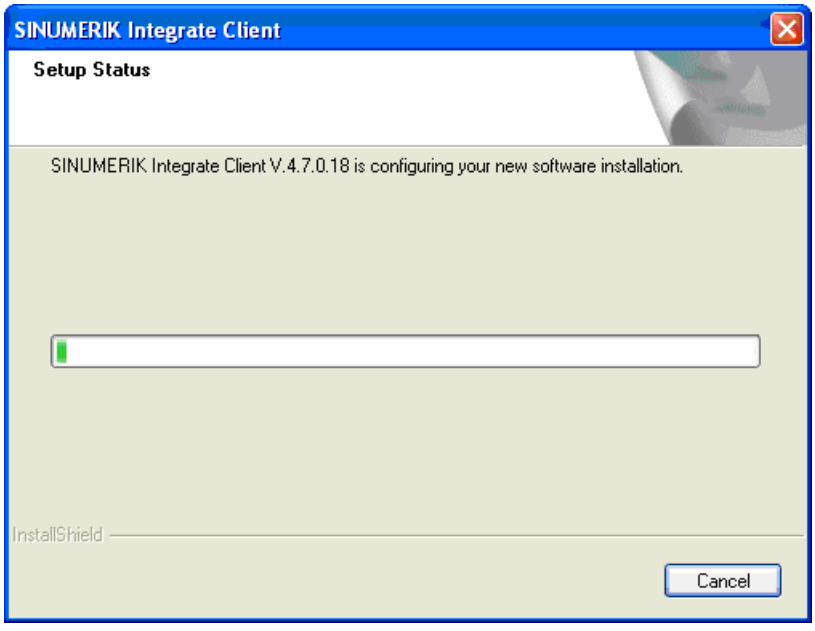
2. For the next steps, see Installing SINUMERIK Integrate client (Page 186).

Repairing the client setup

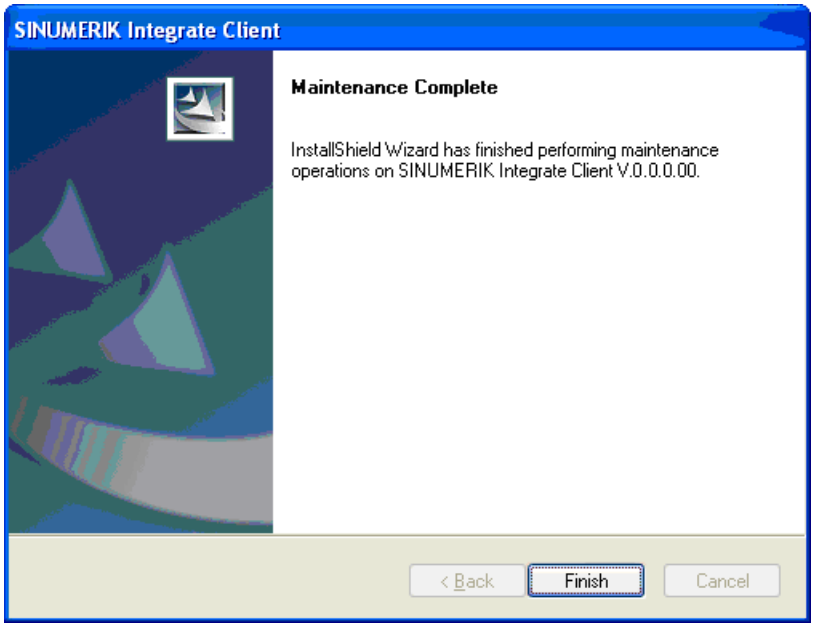
1. In the "Welcome" window, select the "Repair" function if applications are damaged and you want to restore the initial state.
   Click "Next >".



2. The "Setup Status" window opens and the operation is displayed on a progress indicator.

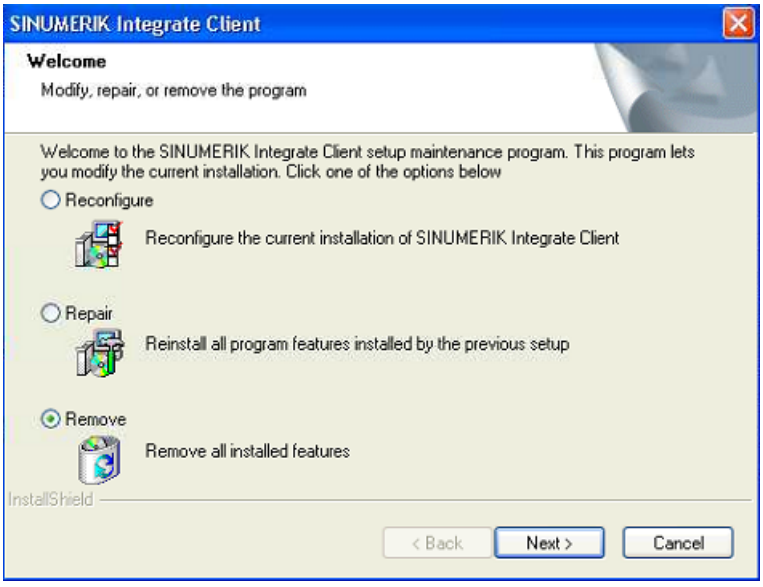


3. Click "Finish" to complete the installation.

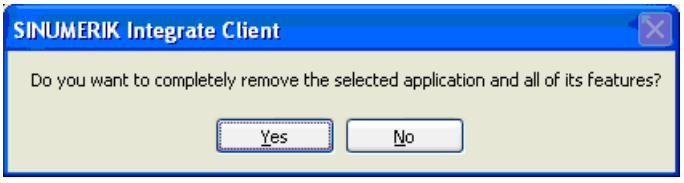

SINUMERIK Integrate Client
Maintenance Complete
InstallShield Wizard has finished performing maintenance operations on SINUMERIK Integrate Client V.0.0.0.00.
< Back
Finish
Cancel

Removing the client setup

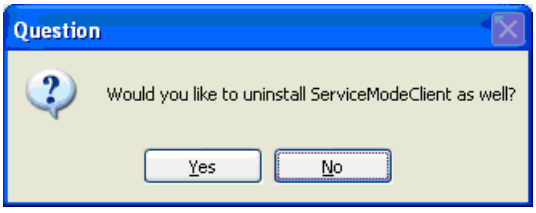
1. In the "Welcome" window, select the "Remove" function if you want to remove the client setup.
   Click "Next >".



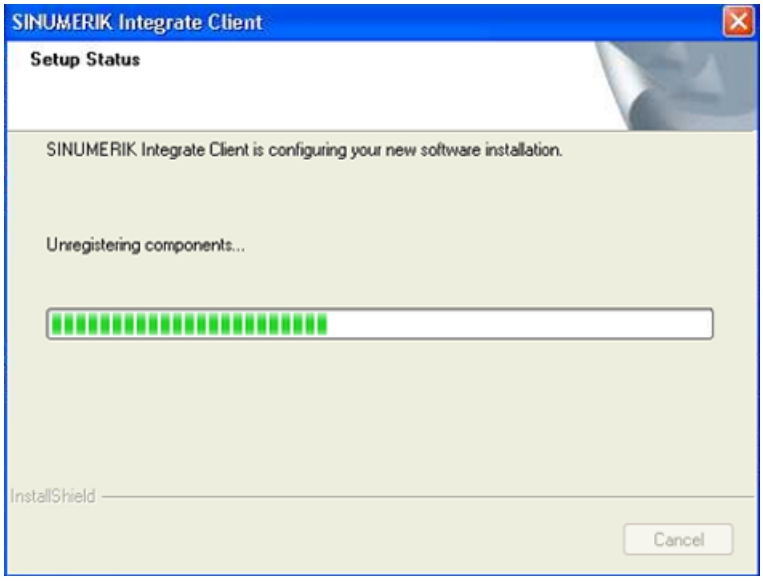
2. A prompt appears.
   Confirm this message with "Yes" if an additional application is installed and you want to uninstall this application.



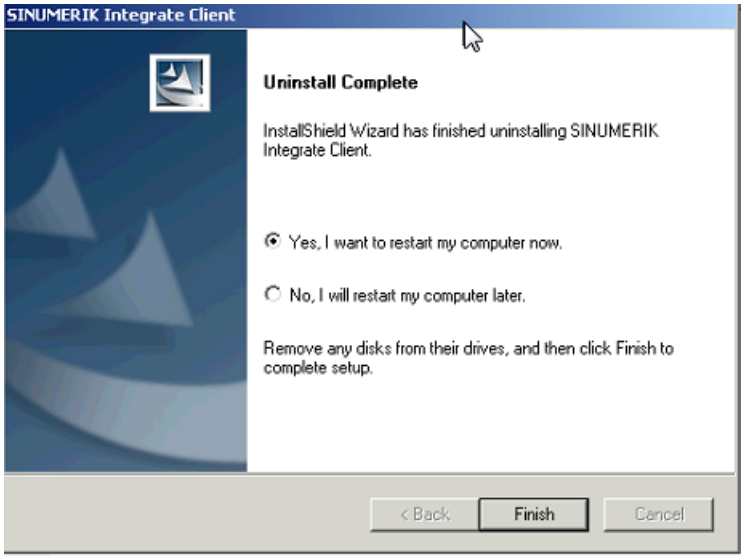
3. You may be shown an additional confirmation prompt asking, for example, whether you wish to uninstall the Service Mode Client application.
   Click "Yes" to start this operation.



4. The uninstallation is started and the procedure is displayed on a progress indicator.



5. Click "Finish" to complete uninstalling.



9.2.4 Connecting to different Mcenter server

You have the option of connecting an already connected controller to another Mcenter server.

Procedure

1. Uninstall the currently assigned application from your controller, if you have any.
2. Delete the already connected controller from the Mcenter server.
3. Delete the Si5 folder from f:\tmp.

4. Delete scripts/jobs under f:\add-on\mh\OOH.
5. Open the registry and delete MachineModel entry in registry:
   HKEY_LOCAL_MACHINE\SOFTWARE\ePS Network – Electronic Production Services GmbH \ePS Network – Services V4.13.0\Configuration\MH\
6. Uninstall the SINUMERIK Integrate client from your SINUMERIK controller with HMI-Advanced.
7. For more information, see Connecting applications with the SINUMERIK control system (Page 225).

9.3 Mcenter with HMI-Advanced on a Retrofit machine

The installation of the SINUMERIK Integrate client on the Windows 10 Retrofit machine is the same as Installing SINUMERIK Integrate client (Page 186).

Installing SINUMERIK Integrate client, but after the installation there must be some manual changes be made.

Prerequisite

Always start HMI-Advanced with administrator rights:

- Right click on "Run with Administrator".

Procedure

After you install SINUMERIK Integrate client, change the following:

1. Open the following file: F:\add_on\MH\settings.ini
   - Change the following entry:
     ```
     [APP]
     ACCESSTYPE ="DDE"
     ```
   - Save and close the file.
2. 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
3. Start HMI-Advanced and connect the machine.
   For more information, see Creating the SINUMERIK controller on the server (Page 227).

HMI-Advanced is stopped and two processes not ended

If the Retrofit Machine is started in Service Mode and you start the HMI-Advanced with the SINUMERIK Integrate client and you close the HMI Advanced, it is possible that the two processes will not be ended after HMI-Advanced is stopped!

End the two processes:

1. Go to Task Manager.
2. Click on "Details" tab.
3. Right-click "End Task" the following two tasks:
   - MachineHandler.exe
   - MhDdeService.exe

Installing the Machine Agent client 10

10.1 Overview

The Machine Agent is a new client side software that provides connectivity to third party controllers like FANUC, Heidenhain and others. It can be created and managed like regular SINUMERIK Integrate clients in the "Manage machines" application on the Mcenter server. Additional information is available in the following manual:

- Operating Manual Mcenter, Manage MyResources

Note

Client support

The Machine Agent client supports the Analyze MyPerformance /OEE, Manage MyResources / Programs and Access MyData /Collector applications.

Properties of the Machine Agent client

The Machine Agent client is registered in Windows as a service that is automatically started when the operating system is booted up, even if no users have signed into the system. This service is called "MachineAgentLauncher".

The Machine Agent client uses the following folders:

- The client's binaries can be found in the following directory: C:\Siemens\SINUMERIK Machine Agent
- Logs can be found in the following directory: C:\Temp\Log
- Configuration and data generated by the Core can be found in the following directory: C:\Windows\Temp\MachineAgent

10.2 Installing the Machine Agent client

Prerequisites

Hardware requirements

- The Machine Agent can be installed on any piece of hardware that complies with the respective part of the system requirements.
- You require administrator rights to install the Machine Agent client.

Machine Agent installer

- The Machine Agent installer can be requested from the Mcenter server in the "Manage machines" application. Additional information is available in the following manual:
  - Operating Manual Mcenter, Manage MyResources

  - OR -
- The Machine Agent installer can be acquired from the setup package.

Onboarding commands

- The Machine Agent client installer can immediately onboard the clients if the onboarding commands are provided along with the installer. This means the onboarding commands must be put in the same folder where the "setup.exe" file is located.
- Onboarding commands can be acquired from the Mcenter server in the "Manage machines" application. Additional information is available in the following manual:
  - Operating Manual Mcenter, Manage MyResources

Note

Name of onboarding commands

The onboarding commands can only be found by the installer if they are named as the MAC address of the machine you are trying to onboard.

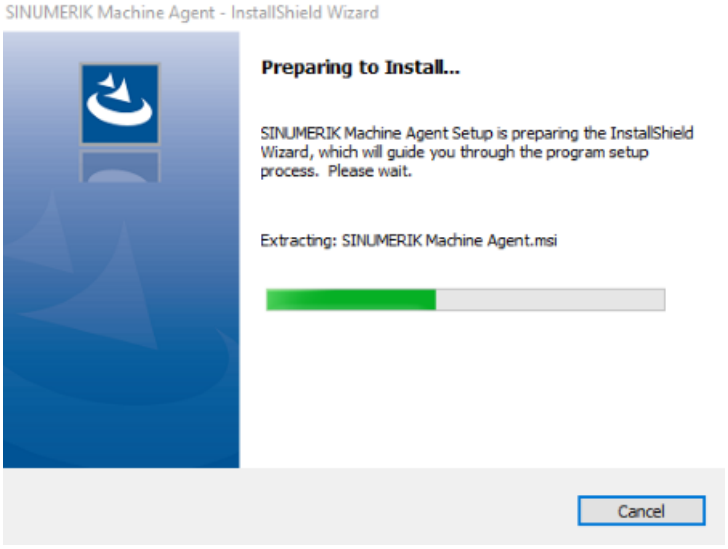
The MAC address must not contain any separators in the name of the command.

The command must have the extension "*.command".

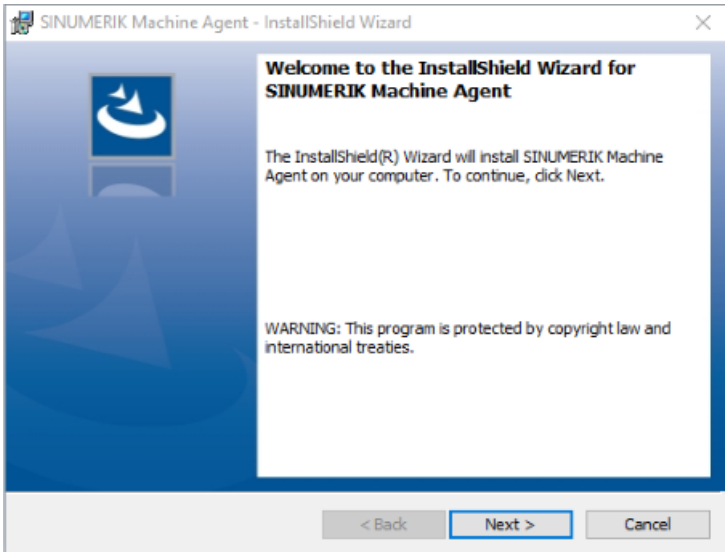
Procedure

1. Copy the installer, and if already present the onboarding command(s), onto a USB stick into the same folder.
2. Insert the USB stick into the machine and start the "setup.exe" file with a double-click.

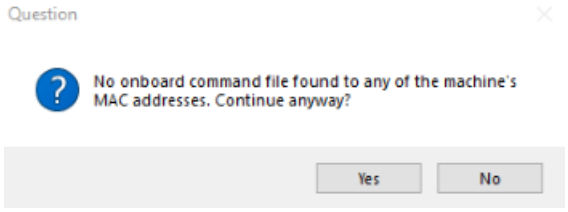
3. The "Preparing to Install" page appears and the installation is automatically prepared.



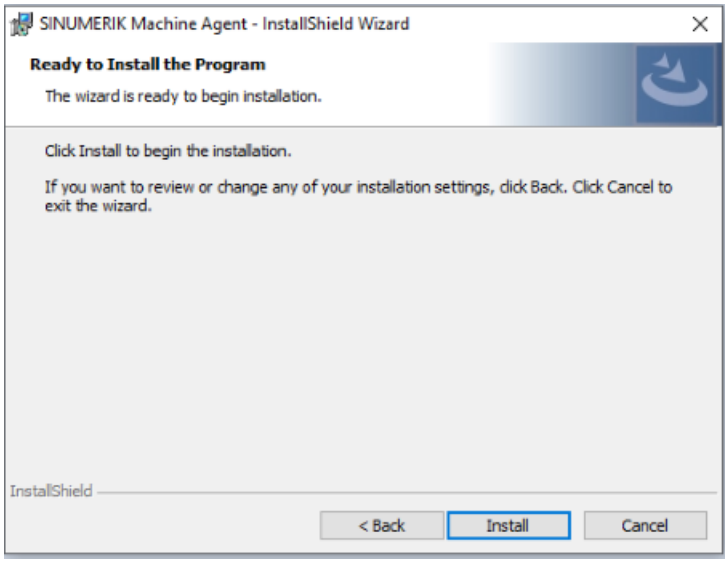
4. The "Welcome" page appears.
   Click "Next >".



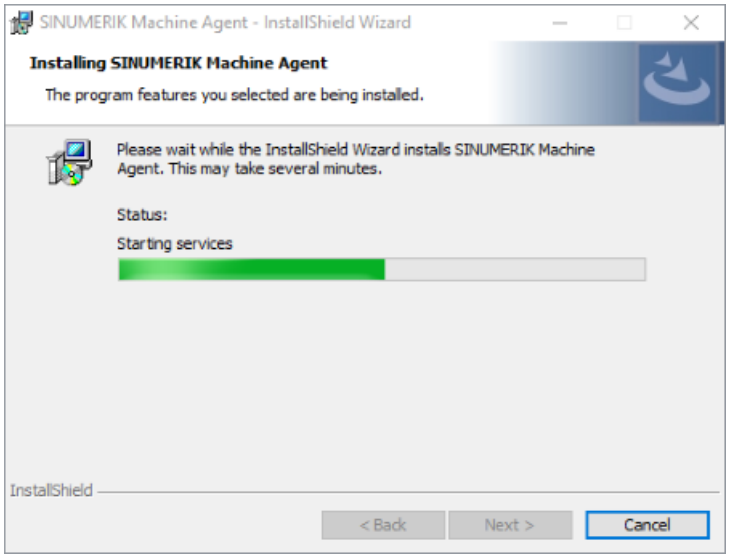
5. If no onboarding commands can be found in the same directory as the "setup.exe" file is located in, or neither are named as the MAC address of the machine you are installing the Machine Agent client to, a modal dialog appears.
   Click "Yes" to continue the installation. The Machine Agent is not onboarded and must be configured manually. For more information, see Configuring the Machine Agent client manually (Page 222).
   - OR -
   Click "No" to cancel the installation.



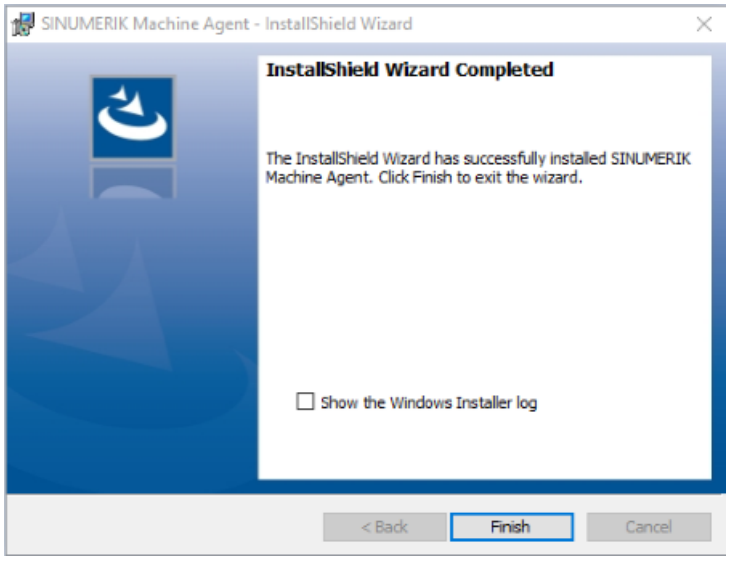
6. Click "Install" to start the installation.



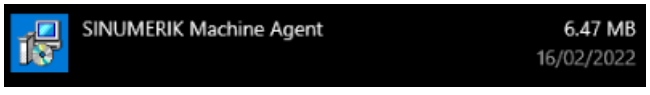
7. The installation is started. The progress is displayed with a progress bar.



8. Click "Finish" to complete the installation.
   Tick the "Show the Windows Installer log" checkbox to see further information about the installation.



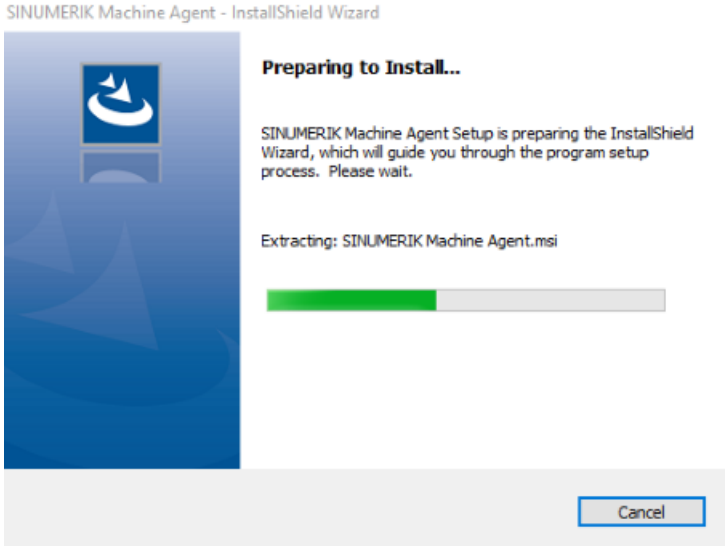
9. The Machine Agent client is now installed in the following directory: C:\Siemens\Machine Agent
   The Machine Agent is also visible in the "Apps and features" Windows setting.



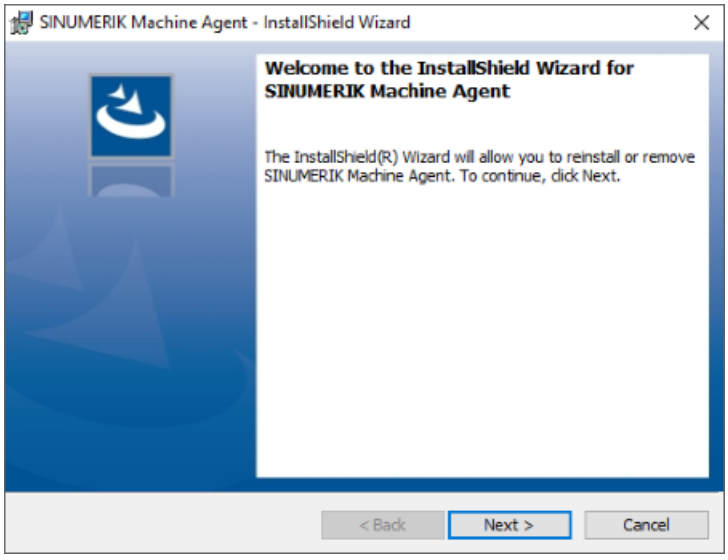
10.3 Modifying the installation

Procedure

1. Start the "setup.exe" file again with a double-click.
2. Wait until the "Preparing to Install" page disappears.



3. The "Welcome" page appears.
   Click "Next >".



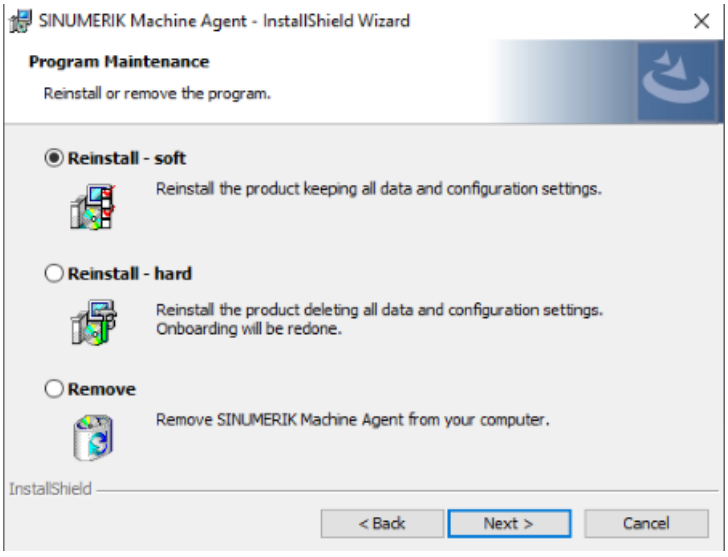
4. Activate the "Reinstall - soft" option button and click "Next >".

Note

"Reinstall - soft" action

All binaries associated with the Machine Agent client will be replaced, but all data and configuration will be kept.

The client will be able to resume normal operation after the "Reinstall - soft" action.



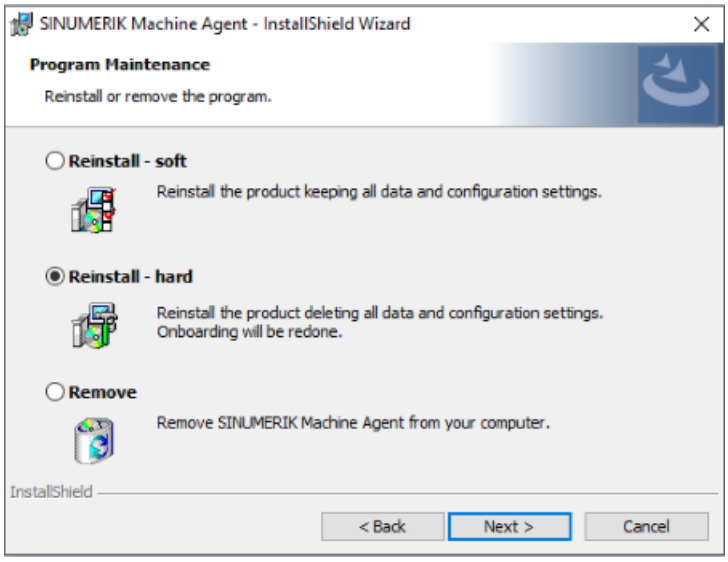
- OR -
Activate the "Reinstall - hard" option button and click "Next >".

Note

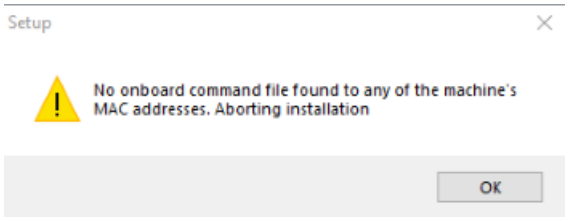
"Reinstall - hard" action

All binaries associated with the Machine Agent client will be replaced and all data and configuration will be deleted.

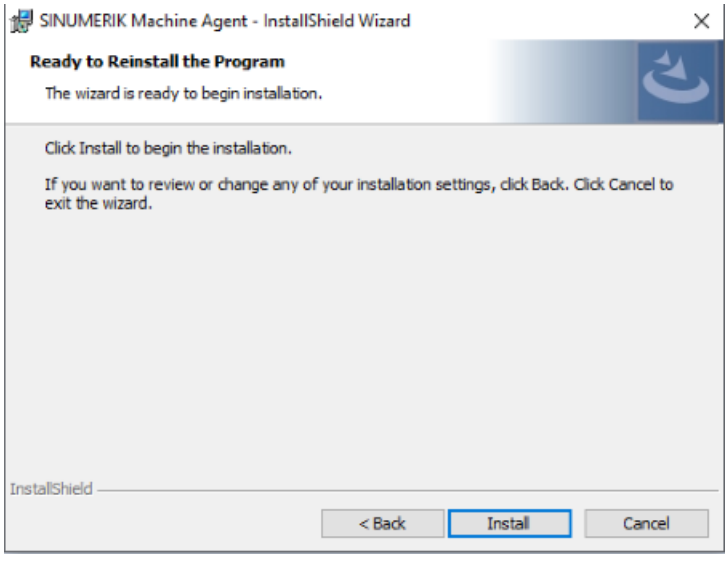
The client must be onboarded and configured again after the "Reinstall - hard" action!



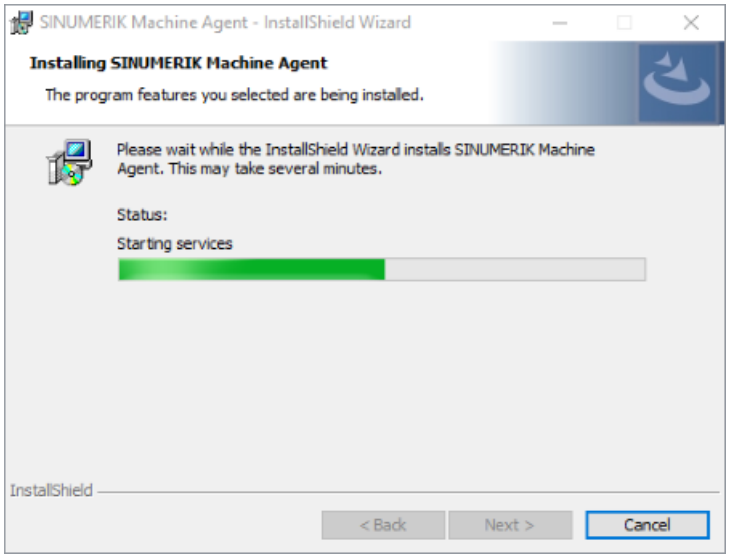
If there is no onboarding command in the same folder where the "setup.exe" file is located, an error message appears and reinstallation will be aborted.



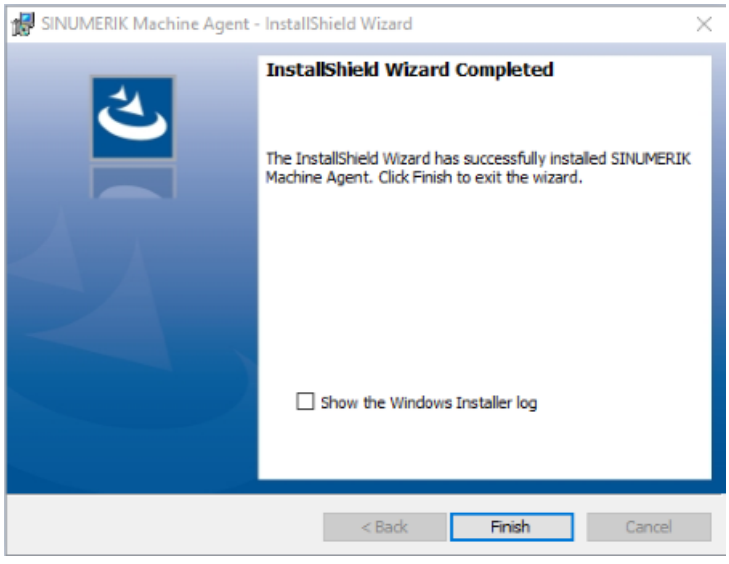
5. Click "Install" to start the installation.



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



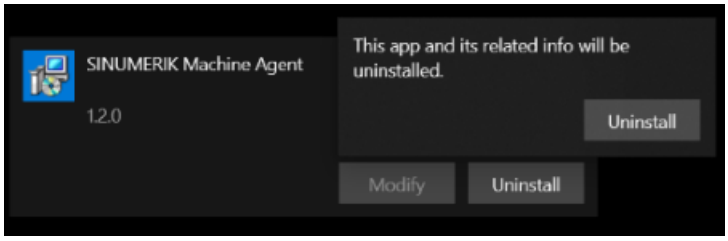
7. Click "Finish" to complete the installation.
   Tick the "Show the Windows Installer log" checkbox to see further information about the installation.



10.4 Uninstalling the Machine Agent client

Procedure

1. Go to the "Apps and features" Windows setting and select the "SINUMERIK Machine Agent". Click "Uninstall".



2. The Installer will be prepared and the Machine Agent client will be uninstalled.

Note

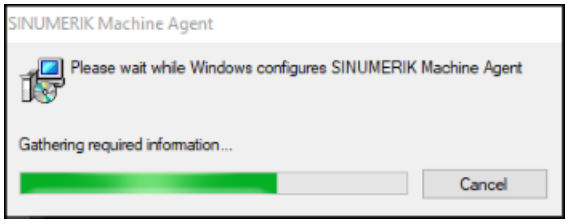
VCRedist installation

This action will not uninstall the VCRedist that has been installed during the installation process!

Note

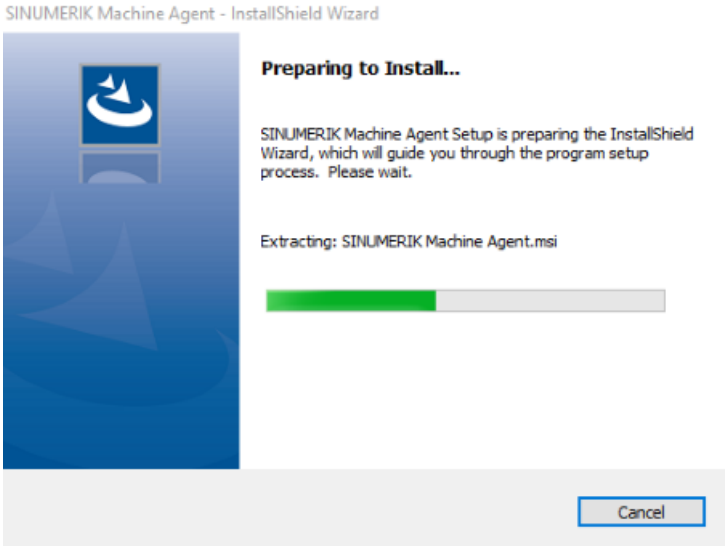
Data and configurations removal

Uninstalling the Machine Agent client will remove all data and configurations associated with it and cannot be undone!

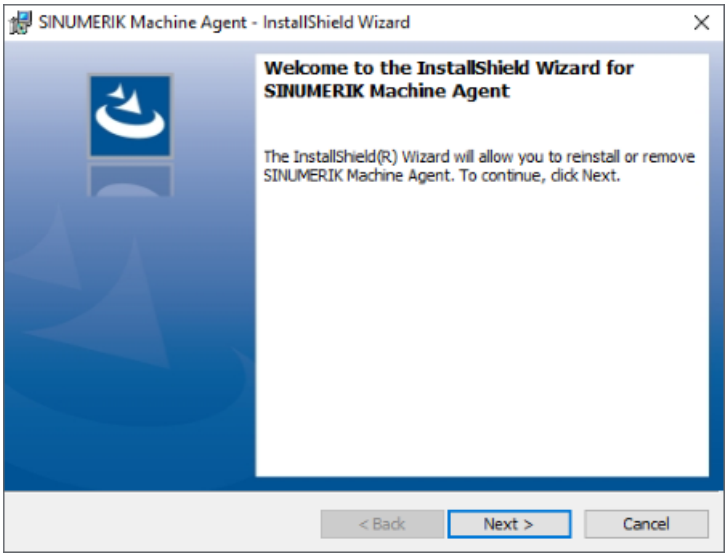


- OR -

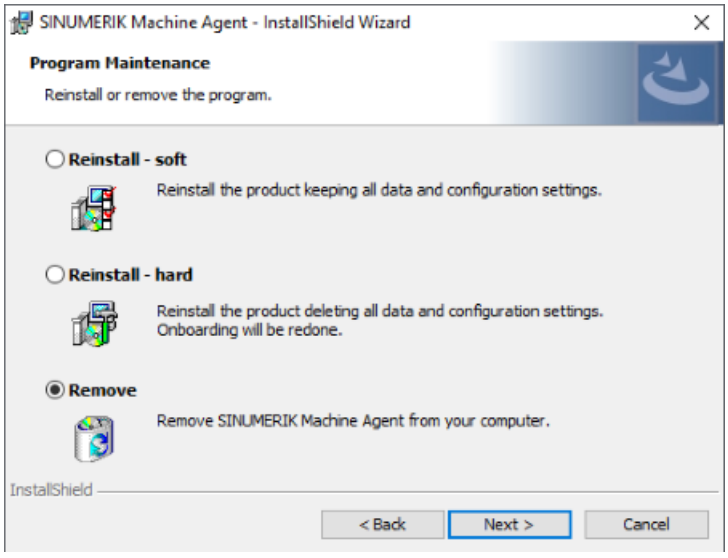
1. Start the "setup.exe" file again with a double-click.
2. Wait until the "Preparing to Install" page disappears.



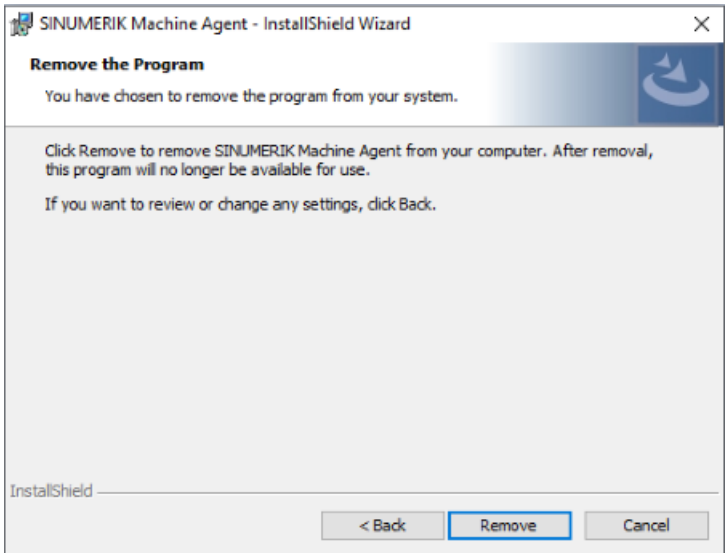
3. The "Welcome" page appears.
   Click "Next >".



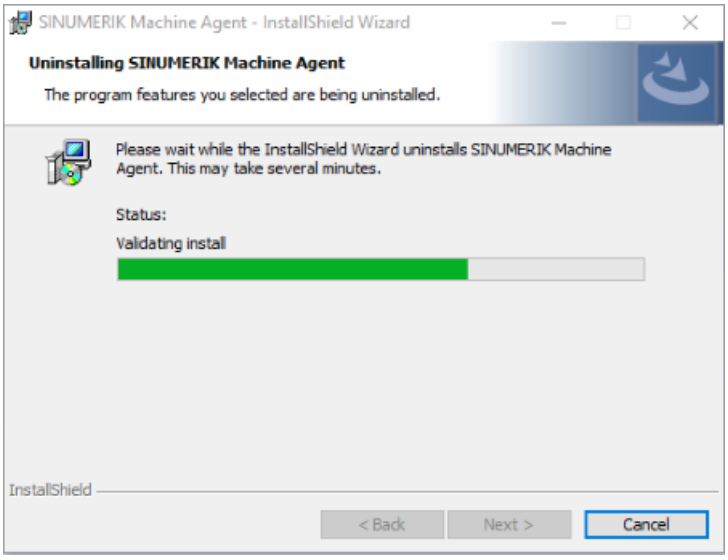
4. Activate the "Remove" option button and click "Next >".



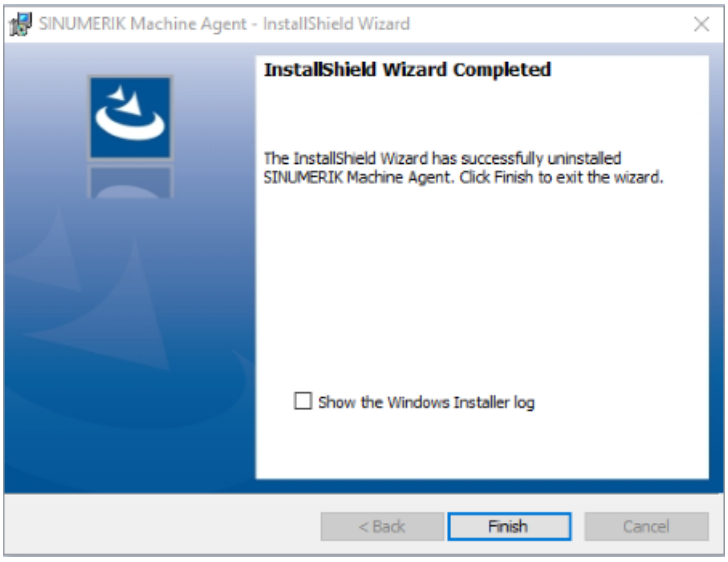
5. The "Remove the Program" page appears.
Click "Remove".



6. The Machine Agent client will be uninstalled.



7. Click "Finish" to complete the uninstallation.
   Tick the "Show the Windows Installer log" checkbox to see further information about the uninstallation.



10.5 Configuring the Machine Agent client manually

Onboarding without the installer

If during the installation the onboarding has not been successful for any reason, you can manually onboard the Machine Agent client:

1. Request a valid onboarding command for the machine from the server.
2. Copy the received onboarding command file to a USB stick.
3. Insert the USB stick into the machine and copy the onboarding command into the "C:\commands" folder.

   Note

   "C:\commands" folder

   If the "C:\commands" folder does not exist, it must be created manually.

4. Wait until a file with the same name as the onboarding command, but with the extension "*.result", appears.
5. Check the result file for "cmd_done_ok".

   Note

   "cmd_done_error" or "cmd_in_progress"

   If the result file contains "cmd_done_error", contact customer support for further assistance.

   If the result file contains "cmd_in_progress", wait until it either contains "cmd_done_ok" or "cmd_done_error".

Setting the logger configuration

The logger configuration of the Machine Agent client can be found in the following directory: C:\Windows\Temp\MachineAgent\data\system\cfg

1. Open the "log.cfg" file in any text editor to set the logger configuration.
2. To set the log level, find the keys "default_severity" and set them to one of the following values:
   - error
   - warn
   - info
   - debug

Starting and stopping the Machine Agent client

Stopping the Machine Agent client

1. Press Windows+R and type "services.msc".
2. Right click on the service called "MachineAgentLauncher" and press "Stop".
3. Wait until Windows finished the operation.

Starting the Machine Agent client

1. Press Windows+R and type "services.msc".
2. Right click on the service called "MachineAgentLauncher" and press "Start".
3. Wait until Windows finished the operation.

Connecting applications with the SINUMERIK control system

11

11.1 Overview

Prerequisite

The following components are already installed on the SINUMERIK controller:

- Mcenter (is available with the "SINUMERIK Operate" operating software)
- Secure communication is set up.
  For more information, see Certificate on the server (Page 125).
- The basic functions are configured.
  For more information, see Overview (Page 149).
- Manage MyResources is installed on the SINUMERIK controller.
  For more information, see Installing new applications (Page 229).
- Mcenter machine server connection with HTTP/HTTPS mixed mode
  Normally a server configured for HTTPS will always redirect all pure HTTP requests to HTTPS.For testing purposes we allow machines to be connected via pure HTTP. In order to allow such connections the following configuration has to be set:
  - In consul, navigate to /Processes/SinInt.MhComm.Service/NetworkProtocolOptions/AllowTestingWithoutHttpsRedirect under key value settings. Enter "true" in the value field.
  - In IIS remove the "Requires SSL" checkbox from the SinInt.MHComm.Service application under SSL Settings.

NOTICE
Settings in production environment Siemens strictly recommends not to use this setting in production environment! This setting poses a security risk for the whole system.

Procedure with SINUMERIK Operate

To establish a connection from the SINUMERIK controller to the server, perform the following steps:

1. Start the "SINUMERIK Operate" operating software.
   Enable the "SINUMERIK Integrate" softkey on the user interface to start Mcenter
   For more information, see Activating Mcenter products (Page 175)
2. Enable the use of Mcenter
   For more information, see Enabling use (Page 176).
3. Configure the proxy and URL addresses
   For more information, see Configuring the URL and proxy (Page 176).

4. To install a current version of Mcenter, proceed as follows:
   – Install a client update.
   For more information, see Installing the Client update (Page 177).
   Windows: For more information, see Client update under Windows (Page 178).
   - OR -
   Linux: For more information, see Client update under Linux (Page 181).
5. Restart the SINUMERIK controller.

Procedure with HMI-Advanced

To establish a connection from the SINUMERIK controller to the server, perform the following steps:

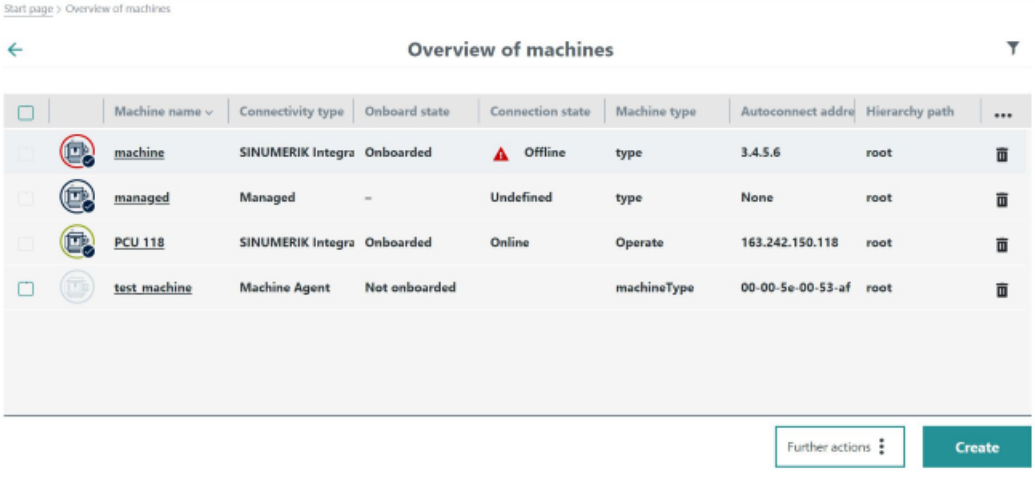
1. Install and configure Mcenter.
   For more information, see Mcenter with HMI-Advanced (Page 186).
2. Restart the SINUMERIK controller.

11.2 SINUMERIK controller is ONBOARDED

This chapter describes how to check if a machine is "ONBOARDED" in the Mcenter.

Procedure

1. On the start page of Mcenter, click on "Manage machines".
2. The "Overview of machines" window opens.
3. The machine is displayed with the onboard state "Onboarded" and the connection state "Online" in the overview.



11.3 Creating the SINUMERIK controller on the server

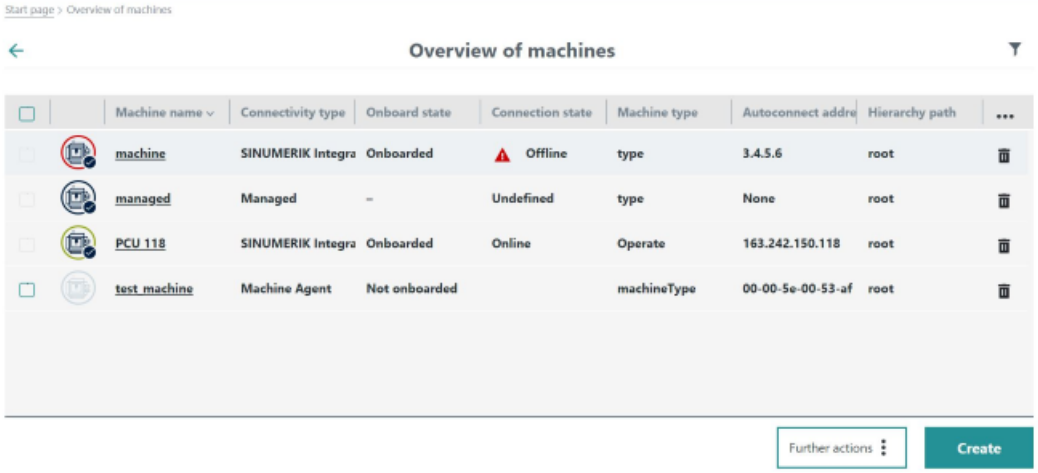
Prerequisite

- The URL must be configured on SINUMERIK controller.
- For HMI-Advanced machines, you must have administrator rights to onboard the machine.
- Determine the following:
  - IP address/MAC address of the SINUMERIK controller
  - Suitable machine designation

Procedure

1. On the start page of Mcenter, click on "Manage machines".

   - OR -
   Open the following URL on the server:
   - In case of http communication: Manage machines (http://<{Server_IP}>:<{Server_port}>/configure-plant)
   - In case of https communication: Manage machines (https://<{Server_IP}>/configure-plant)
2. Click the "Create" button.
3. Create a new machine. Enter the IP/MAC address that has been determined, the suitable machine designation (name), and appropriate machine type.
4. Reload the window.
5. The newly created machine is shown in the overview without a connection state and with the onboard state "Not onboarded".



Manage applications on machines 12

12.1 Installing new applications

New application clients (software packages) can be loaded to SINUMERIK controller via the user interface on the server.
Examples:

- Manage MyResources /Tools, including Manage MyResources /Tools Statistics
- Manage MyResources /Programs
- Optimize MyProgramming /NX-CAM Editor
- Analyze MyPerformance /OEE

Prerequisite

The application clients are provided.

NOTICE
SINUMERIK Operate updated If you updated your SINUMERIK Operate to version 4.95 or higher, and you already had installed Mcenter applications on this SINUMERIK controller, they do not work anymore after the SINUMERIK Operate update. Use the application management functionality of Mcenter, to first uninstall the applications and then install them again. After the installation, the applications work properly again.

Procedure

1. On the start page of Mcenter click "Manage applications on machines".

- OR -
Open the following URL: Manage application on machines ((https://{ServerIP}/appassignment-overview))

Additional information

Additional information on manage applications on machines is available in the following manuals:

- Operating Manual Manage MyResources
- Operating Manual Optimize MyProgramming /NX-Cam Editor
- Operating Manual Analyze MyPerformance /OEE

12.2 Installing and configuring applications on HMI-Advanced

12.2.1 On a Retrofit machine (Windows 10 with HMI-Advanced Retrofit)

To use the application management functionality of SINUMERIK Integrate 5 some configurations are needed before applications are assigned to the HMI-Advanced machines.

See these configurations in the subsections of this section. Some configurations are needed before applications are assigned to the controller with the operating software HMI-Advanced.

Prerequisite

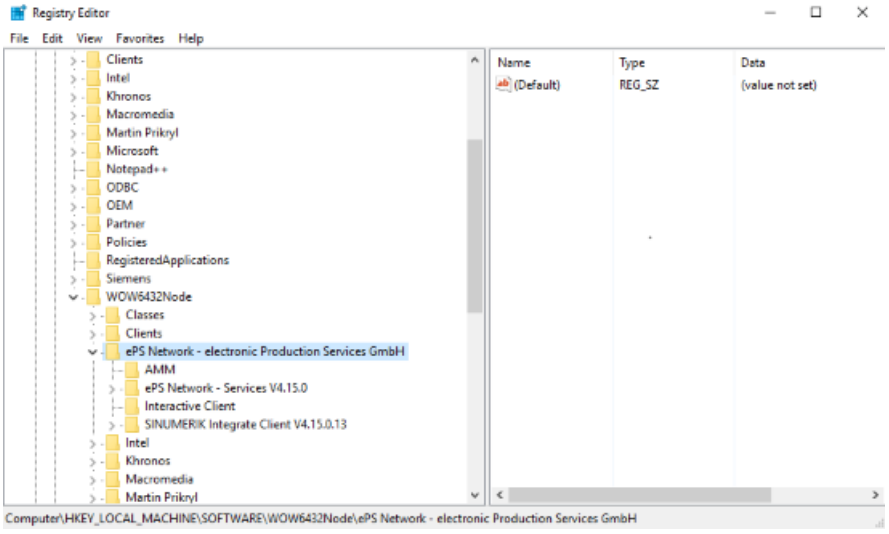
You require administrator rights on the machine.

Installing

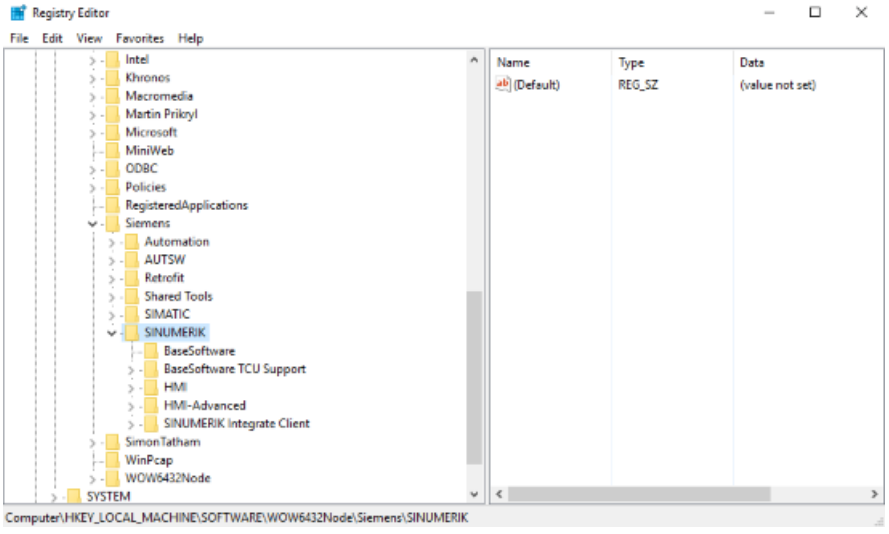
Enable installation for users that do not have admin rights.

1. Login to the controller with the operating software HMI-Advanced Retrofit.
2. Right-click on "Entry" > "Permissions > allow "full control" for the user.

3. Give user rights for the following registry entries:
   `HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\ePS Network - electronic Production Services GmbH`



4. Give user rights for the following registry entries:
   `HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Siemens\SINUMERIK`



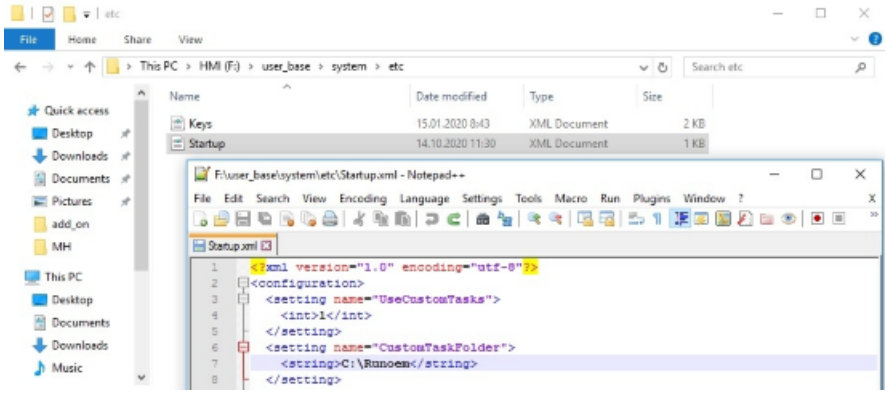
Configuring

Automatic execution is turned off on these machines by default.

You have to change this.

1. Open the following file:
   F:\user_base\system\etc\Startup.xml file
2. Add the following settings:

```
<setting name="UseCustomTasks">
   <int>1</int>
 </setting>
 <setting name="CustomTaskFolder">
   <string>C:\Runoem</string>
 </setting>
```



12.2.2 On a Retrofit machine without admin rights

You can set up users without administrator rights on a retrofit machine with HMI-Advanced.

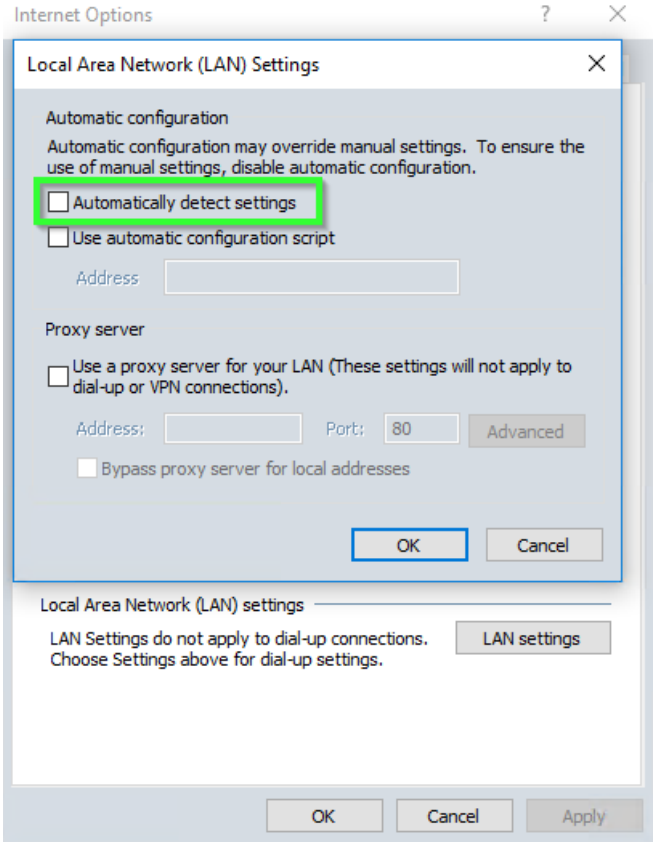
Prerequisite

You have administrator rights on the machine.

Procedure

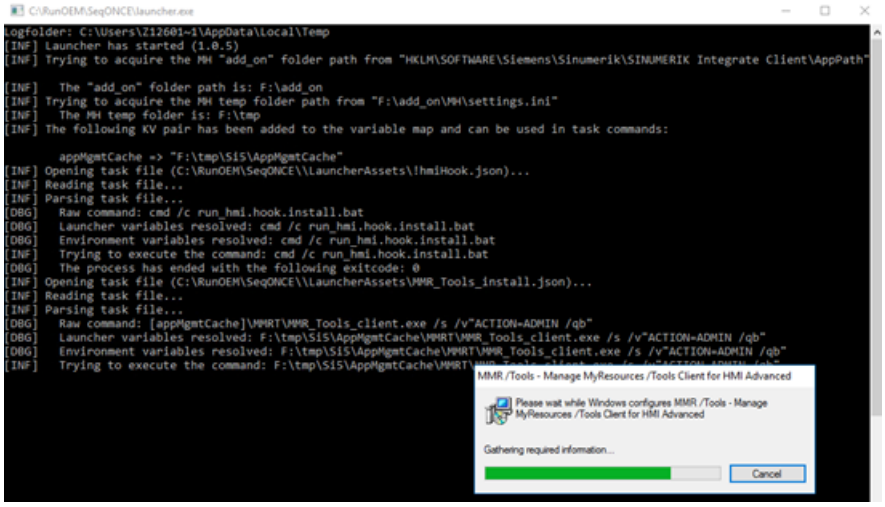
1. Login to the controller with the operating software HMI-Advanced Retrofit.
2. Install the SINUMERIK Integrate client.
3. Give user rights for the following registry entries:
   - `[HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\ePS Network - electronic Production Services GmbH`
   - `[HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Siemens\SINUMERIK`

4. Open the "Internet Options" > "Local Area Network (LAN) Settings" and check that the "Automatically detect settings" option is not enabled.
   Check the option for each user individually!



5. Start HMI-Advanced and connect to the Mcenter server.
6. Add the application to the machine.

7. Start the installation.
   - If the alarm appears on the HMI-Advanced, turn off the HMI-Advanced.
   - Run with file explorer in directory `C:\RunOEM\SeqONCE\launcher.exe`



8. When the process is finished, open the following directory: C:\RunOEM\SeqONCE, and delete the "LauncherAssets".
9. The installation process is finished. Start HMI-Advanced.

Note

First start with administrator rights

When you start the MMR /Tools client for the first time after an installation/update, you must perform as an administrator user. Otherwise you get an error message.

12.2.3 On Windows NT/XP

Prerequisite

You require administrator rights on the machine.

If you are working on your SINUMERIK controller with the NT operating system, also install "Windows Installer 2.0".

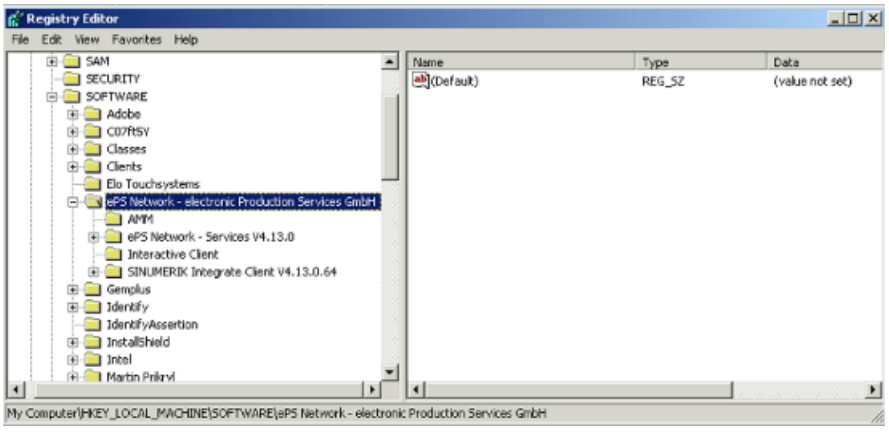
Open the following folder: "SI5\Clients\Appliction_Clients\MMR\HMI advanced\instmsiw.exe".

The MMR /Tools HMI Advanced Client requires the SINUMERIK Integrate Client for HMI Advanced. You find the "ePS_Clinet_AT.exe" installation file under: "SI5\Clients\SinIntclient\HMI Advanced".

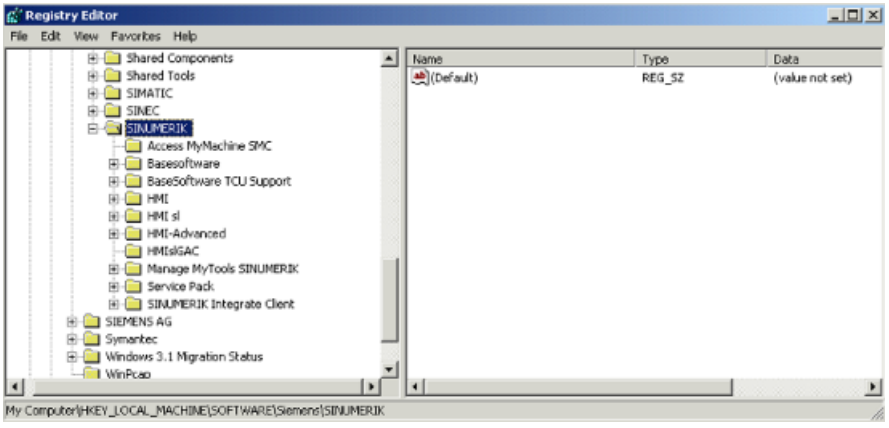
Installing

Enable installation for users that do not have admin rights.

1. Login to the controller with the operating software HMI-Advanced.
2. Right click on "Entry" > "Permissions > allow "full control" for the user.
3. Give user rights for the following registry entries:
   `HKEY_LOCAL_MACHINE\SOFTWARE\ePS Network - electronic Production Services GmbH`



4. Give user rights for the following registry entries:
   `HKEY_LOCAL_MACHINE -> SOFTWARE -> Siemens -> SINUMERIK`



Configuring automatic execution

- On Windows NT this feature is available only from PCU Base Software V06.02.01.00.
- On the supported NT and XP versions the execution in RunOem is turned on by default. No configuration is needed.

Configuring applications 13

13.1 Manage MyResources /Tools

13.1.1 PLC connection for unloading, loading and 1:1-Exchange

13.1.1.1 Overview

Overview

To unload, load or replace tools, MMR /Tools uses the PLC interface between the standard tool management and the PLC.

The machine manufacturer must ensure that when the process is initiated and control is transferred from the SINUMERIK control to the PLC, the machine moves to the home position, if possible, and supports the user with other steps required for loading/unloading/exchanging tools by displaying appropriate information, such as:

- "Loading station move to basic position"
- "Close loading door"
- "Loading in automatic mode not possible"

13.1.1.2 Unloading process

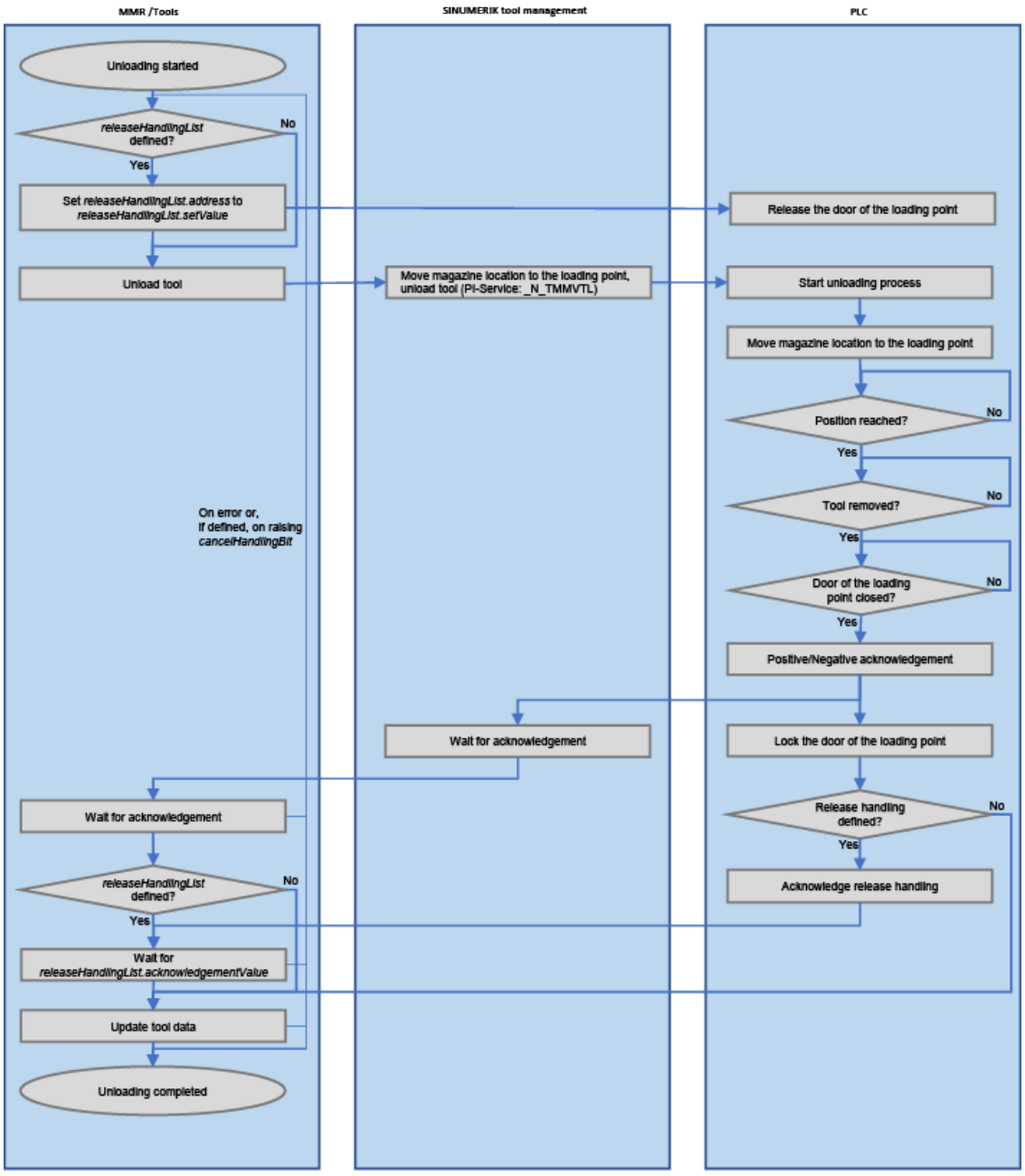
Overview

The PLC is informed about the unloading process. The tool data and the defined loading point are written to the corresponding PLC addresses. Thus the unloading process can be started by the PLC. After the PLC has finished all steps of the unloading process, it must acknowledge the unloading positively with a corresponding signal. In case of an error, the unloading is acknowledged negatively and the corresponding error message is displayed by the PLC. The error code can be returned to MMR /Tools via the PLC interface for processing.

Note

Negative PLC acknowledgement

MMR /Tools also supports negative PLC acknowledgement. If PLC acknowledges successful tool load and unload negatively, `negativeAcknowledgement` parameter should be set to `true` for MMR /Tools to handle it properly.


MMR /Tools
SINUMERIK tool management
PLC
Unloading started
releaseHandlingList defined?
No
Yes
Set releaseHandlingList.address to releaseHandlingList.setValue
Unload tool
Move magazine location to the loading point, unload tool (PI-Service: _N_TMMVTL)
Release the door of the loading point
Start unloading process
Move magazine location to the loading point
Position reached?
No
Yes
Tool removed?
No
Yes
Door of the loading point closed?
No
Yes
Positive/Negative acknowledgement
Lock the door of the loading point
Release handling defined?
No
Yes
Acknowledge release handling
On error or, if defined, on raising cancelHandlingBit
Wait for acknowledgement
Wait for acknowledgement
releaseHandlingList defined?
No
Yes
Wait for releaseHandlingList.acknowledgementValue
Update tool data
Unloading completed

Additional Information

- The unloading of an internal tool is triggered by control elements on the SINUMERIK control.
  Additional information on using Manage MyResources /Tools at a SINUMERIK control system is available in following manual:
  Operating Manual Manage MyResources
- Information is exchanged between the SINUMERIK tool management and the PLC via the PLC interface.
  Additional information for documentation on the signal description of the PLC interface is available in following manual:
  SINUMERIK 840D sl tool management.

13.1.1.3 Loading process

Overview

The Loading of an external tool is similar to the unloading of an internal tool. The loading of the external tool is triggered by control elements on the SINUMERIK control.

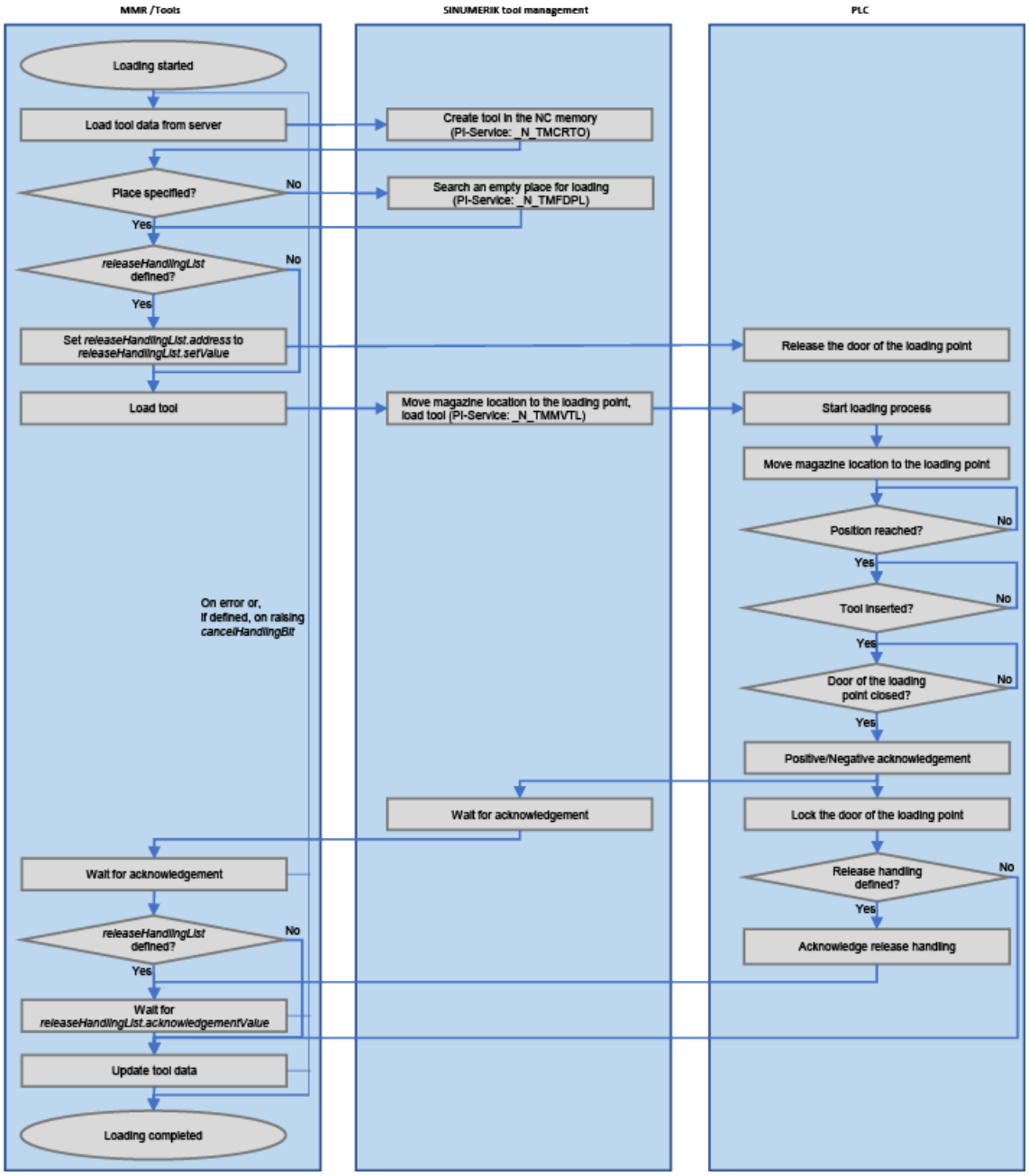
First, the PLC is informed about the loading process. The tool data, the target location in the magazine and the defined loading point are written to the corresponding PLC addresses. Thus the loading process can be started by the PLC. After the PLC has finished all steps of the loading process, it must acknowledge the loading positively with a corresponding signal.

In case of an error, the loading is acknowledged negatively and the corresponding error message is displayed by the PLC. The error code can be returned to MMR /Tools via the PLC interface for processing.

Note

Negative PLC acknowledgement

MMR /Tools also supports negative PLC acknowledgement. If PLC acknowledges successful tool load and unload negatively, `negativeAcknowledgement` parameter should be set to `true` for MMR /Tools to handle it properly.



13.1.1.4 Exchange / Check process

Overview

When checking or exchanging tools, the behavior of the PLC is similar to the unloading and loading processes.

Each process must be acknowledged individually by the PLC.

13.1.1.5 1:1-Exchange

With 1:1-Exchange, a tool is exchanged with a sister tool. First, a tool is unloaded. Then a sister tool is loaded.

Two modes are supported by the MMR /Tools to perform 1:1-Exchange:

- "Direct" mode
- "Quick" mode

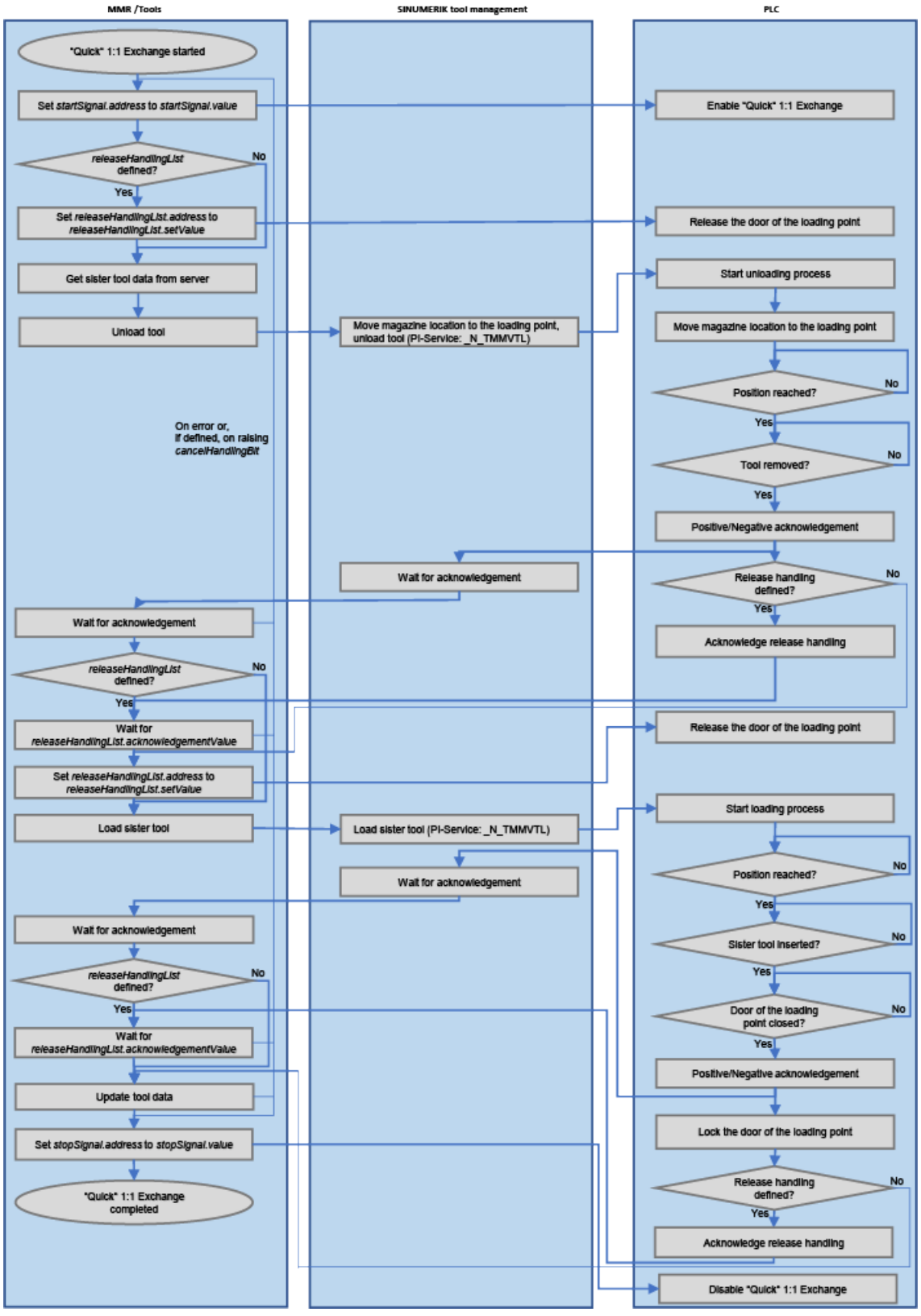
"Direct" mode

In this mode, the machine operator must confirm both the unloading and loading operations by closing a loading door after the tool is unloaded and after the sister tool is loaded.

"Quick" mode

In this mode, the machine operator must confirm both operations at once by closing a loading door after the sister tool is loaded.

The machine operator does not need to close the loading door after the tool is unloaded before loading the sister tool. The “Quick” mode is the preferred mode to perform the 1:1-Exchange, if the machine manufacturer supports it.


MMR /Tools
SINUMERIK tool management
PLC
"Quick" 1:1 Exchange started
Set startSignal.address to startSignal.value
releaseHandlingList defined?
No
Yes
Set releaseHandlingList.address to releaseHandlingList.setValue
Get sister tool data from server
Unload tool
Move magazine location to the loading point, unload tool (PI-Service: _N_TMMVTL)
On error or, if defined, on raising cancelHandlingBit
Wait for acknowledgement
releaseHandlingList defined?
No
Yes
Wait for releaseHandlingList.acknowledgementValue
Set releaseHandlingList.address to releaseHandlingList.setValue
Load sister tool
Load sister tool (PI-Service: _N_TMMVTL)
Wait for acknowledgement
Wait for acknowledgement
releaseHandlingList defined?
No
Yes
Wait for releaseHandlingList.acknowledgementValue
Update tool data
Set stopSignal.address to stopSignal.value
"Quick" 1:1 Exchange completed
Enable "Quick" 1:1 Exchange
Release the door of the loading point
Start unloading process
Move magazine location to the loading point
Position reached?
No
Yes
Tool removed?
No
Yes
Positive/Negative acknowledgement
Release handling defined?
No
Yes
Acknowledge release handling
Release the door of the loading point
Start loading process
Position reached?
No
Yes
Sister tool inserted?
No
Yes
Door of the loading point closed?
No
Yes
Positive/Negative acknowledgement
Lock the door of the loading point
Release handling defined?
No
Yes
Acknowledge release handling
Disable "Quick" 1:1 Exchange

Parameter

Below is the description of properties to be specified in the “mmrConfig.json” file. If any of the mandatory properties is missing, an error is logged in the script log file, and the “Standard” mode is used for 1:1-Exchange.

Property	Usage	Description
`__type`	mandatory	Value must be "`SinInt.MMR.LocalConfiguration`"
`oneToOneExchange`	optional	If missing, "Standard" mode is used for 1:1-Exchange.
`mode`	mandatory if parent `oneToOneExchange` is specified	1:1-Exchange mode. Possible values: • "Standard" • "Quick"
`directConfigurationList`	mandatory if parent mode "Quick" is specified	Specifies a list of configuration setting blocks for a "Quick" 1:1 Exchange.
`toa`	mandatory if parent `directConfigurationList` or `releaseHandlingList` are specified	Specifies for which TOA the settings within the block applies.
`loadingPoint`	mandatory if parent `directConfigurationList` or `releaseHandlingList` are specified	Specifies for which loading point the setting within the block applies.
`startSignal`	mandatory if parent `directConfigurationList` is specified	Specifies the PLC address and value that are written to the address by the MMR /Tools, when 1:1-Exchange is started. These PLC address and value must be obtained from the machine manufacturer.
`stopSignal`	mandatory if parent `directConfigurationList` is specified	Specifies the PLC address and value that are written to the address by the MMR /Tools, when 1:1-Exchange is finished or when an error occurs during 1:1-Exchange. The PLC address and value must be obtained from the machine manufacturer.
`address`	mandatory if parent `startSignal`, `stopSignal` or `releaseHandlingList` are specified	The PLC address is specified in one of the following formats: • For writing byte data: `/plc/datablock/byte[c<Area>,<Byte>]` • For writing bit data: `/plc/datablock/bit[c<Area>,<Byte>.<Bit>]` No validation of the PLC address is done by MMR /Tools.

Property	Usage	Description
`value`	mandatory if parent `startSignal` or `stopSignal` is specified	The PLC value is specified as a string. It is written by MMR /Tools to the given `address` without any validation of the address data type or range.
`releaseHandlingList`	optional	Specifies a list of configuration setting blocks for release handling. Only needed if the machine uses PLC addresses for enabling and acknowledging loading or unloading. The PLC `address`, `setValue`, `acknowledgementValue` must be obtained from the machine manufacturer.
`setValue`	mandatory if parent `releaseHandlingList` is specified	The PLC value is specified as a string. It is written by MMR /Tools to the given address in the block without any validation of the address data type or range. Writing the PLC value to the PLC address in the block enables loading or unloading.
`acknowledgementValue`	mandatory if parent `releaseHandlingList` is specified	The PLC value is specified as a string. MMR /Tools waits for the value to be written by the PLC to the given address in the block to finish loading or unloading.
`cancelHandlingBit`	optional	The machine operator can interrupt loading or unloading by pushing the cancel button. This triggers the PLC to set the cancelation PLC address bit to "1". MMR /Tools then cancels the process on the bit change from "0" to "1". The cancelation PLC address bit has to be obtained from the machine manufacturer. The cancelation PLC address bit is specified in the following format: `/plc/datablock/bit[c<Area>,<Byte>.<Bit>]` No validation of the cancellation PLC address bit is done by MMR /Tools.
`negativeAcknowledgement`	optional	Specifies if the PLC acknowledges tool loading and unloading negatively. Possible values: • `true`: PLC acknowledges tool loading and unloading negatively. MMR /Tools periodically checks whether the tool has actually been loaded to or unloaded from a magazine. The check stops when successful. You can also cancel the operation by pressing the "Cancel" softkey. • `false`: PLC acknowledges tool loading and unloading positively (default).

Property	Usage	Description
`unloadAfterCheckEnabled`	optional	Specifies if moving the original tool to the Assembly option is enabled after checking. Possible values: • `true`: After checking, moving the original tool to the Assembly option is activated. • `false`: After checking, moving the original tool to the Assembly option is deactivated (default).
`toolReservationEnabled`	optional	Specifies if the tool reservation information for the tools is displayed. Possible values: • `true`: The tool reservation, i.e. the tools reservation column, is displayed (default). • `false`: The tool reservation for the tools is not displayed.
`productionOrderFilterEnabled`	optional	Specifies if Production order filtering for tools is allowed. Possible values: • `true`: The Production order filters for tools are displayed (default). • `false`: The Production order filters for tools are not displayed.
`deleteCheckedTool`	optional	Specifies if a tool is deleted from the internal tool list from the PLC during the check and change process. • `true`: If you want to keep the original tool that is deleted from the list, MMR /Tools must load this tool data from the container "AtMachine" to the machine. • `false`: The tool is not deleted (default).

Example: File "mmrConfig.json"

The content of the file “mmrConfig.json” must be in the following format:

```
{
   "__type": "SinInt.MMR.LocalConfiguration",
   "oneToOneExchange": {
     "mode": "Quick",
     "directConfigurationList": [
      {
       "toa": 1,
       "loadingPoint": 3,
       "startSignal": {
          "address": "/plc/datablock/byte[c3502,100]",
          "value": "5"
      },
       "stopSignal": {
```

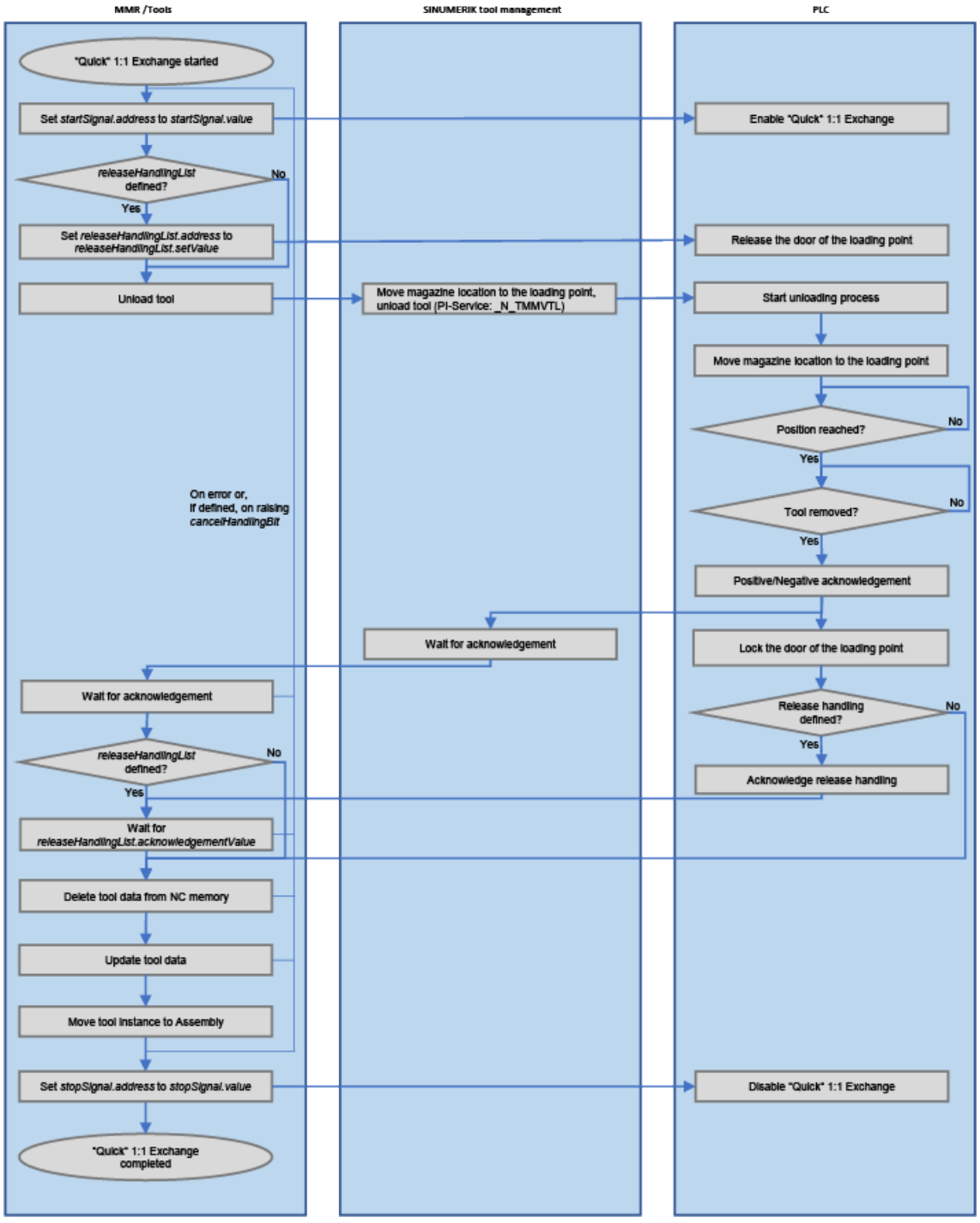
```
            "address": "/plc/datablock/byte[c3502,100]",
            "value": "0"
          }
        },
        {
           "toa": 2,
           "loadingPoint": 5,
           "startSignal": {
             "address": "/plc/datablock/bit[c79,300.1]",
             "value": "1"
           },
           "stopSignal": {
              "address": "/plc/datablock/bit[c79,300.1]",
              "value": "0"
           }
        }
      ]
    },
"releaseHandlingList": [
      {
        "toa": 1,
        "loadingPoint": 1,
        "address": "/plc/datablock/bit[c79,300.6]",
        "setValue": "1",
        "acknowledgementValue": "0"
      }

      {
        "toa": 1,
        "loadingPoint": 2,
        "address": "/plc/datablock/byte[c79,280]",
        "setValue": "0",
        "acknowledgementValue": "15"
      }
    ]
    "cancelHandlingBit": "/plc/datablock/bit[c21,7.7]"
}
```

Exchange / Check process with unloading a tool to Assembly

In addition to the "Keep" and "Exchange" options in MMR /Tools, the additional option "Assembly" allows you to unload the original tool to Assembly.

You can also use this option to check and unload a tool to Assembly without replacing it.


MMR /Tools
SINUMERIK tool management
PLC
"Quick" 1:1 Exchange started
Set startSignal.address to startSignal.value
releaseHandlingList defined?
No
Yes
Set releaseHandlingList.address to releaseHandlingList.setValue
Unload tool
Move magazine location to the loading point, unload tool (PI-Service: _N_TMMVTL)
Enable "Quick" 1:1 Exchange
Release the door of the loading point
Start unloading process
Move magazine location to the loading point
Position reached?
No
Yes
Tool removed?
No
Yes
Positive/Negative acknowledgement
Lock the door of the loading point
Release handling defined?
No
Yes
Acknowledge release handling
On error or, if defined, on raising cancelHandlingBit
Wait for acknowledgement
Wait for acknowledgement
releaseHandlingList defined?
No
Yes
Wait for releaseHandlingList.acknowledgementValue
Delete tool data from NC memory
Update tool data
Move tool instance to Assembly
Set stopSignal.address to stopSignal.value
Disable "Quick" 1:1 Exchange
"Quick" 1:1 Exchange completed

Procedure

To program MMR /Tools to use an option to check and unload a tool to Assembly, a file "mmrConfig.json" has to be created on SINUMERIK.

1. Open or create the file "mmrConfig.json" on SINUMERIK as specified.
   To locate the directory from the configuration file, see Directory for configuring file "mmrConfig.json" (Page 248).
2. Extend the content of the file with a new section `unloadAfterCheckEnabled` as described above.
   Example:
```
{
  ...
 },
 unloadAfterCheckEnabled: true
 }
}
```
3. Restart the HMI for the new settings to take effect.

Additional information

Additional information on supported operating modes on machines is available in following manual:

- Operating Manual Mcenter, Manage MyResources

13.1.2 Directory for configuring file "mmrConfig.json"

Overview

You can find the configuration file in the following directories

- **SINUMERIK Operate with PCU, other than Windows XP:**
  C:\Program Files (x86)\Siemens\MotionControl\user\sinumerik\hmi\cfg\mmrConfig.json
- **SINUMERIK Operate with PCU, Windows XP**:
  F:\hmisl\user\sinumerik\hmi\cfg\mmrConfig.json
- **SINUMERIK Operate with NCU**:
  /card/user/sinumerik/hmi/cfg/mmrConfig.json
- **SINUMERIK HMI-Advanced 7.6 and 6.4**:
  F:\add_on\mmrConfig.json

13.1.3 Code scanner

13.1.3.1 PLC code scanner

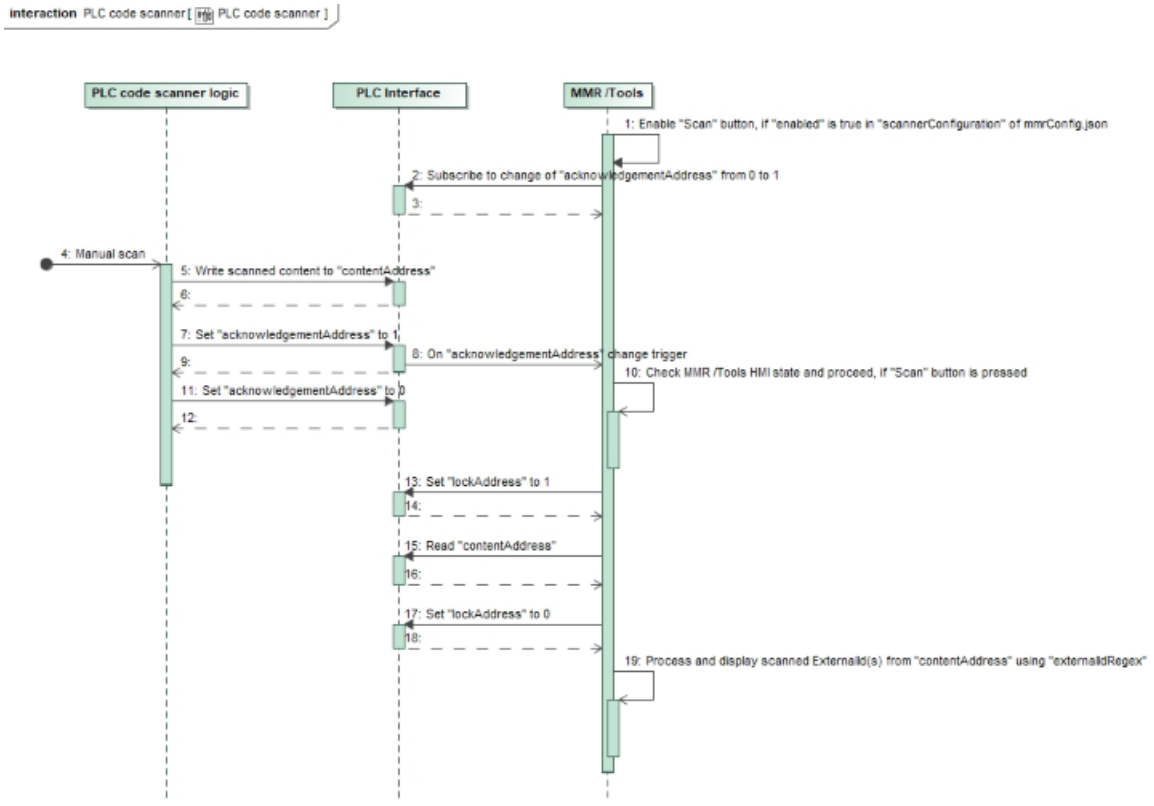
You can scan a tool instance identifier with a hand scanner, for example Balluff-RFID Chip, which is connected to the PLC. You have to program MMR /Tools to use the PLC code scanner by modifying the “mmrConfig.json” file.

Precondition

The code scanner feature is currently only available with MMR /Tools for the SINUMERIK Operate client

Overview

In the flowchart you can see the properties as they are used in the "mmrConfig.json" file.



Parameter

Property	Usage	Description
`scannerConfiguration`	optional	If missing, no PLC code scanner is supported.
`enabled`	mandatory if parent `scannerConfiguration` is specified	Specifies if code scanning via the PLC is enabled. Possible values: • `true`: The “Scan” softkey in MMR /Tools is enabled. • `false`: The “Scan” softkey in MMR /Tools is disabled.
`toggleMode`	optional	Specifies if "Scan" softkeys in "Tools to load" and "Sister tools for 1:1 Exchange" windows of MMR /Tools operate in a toggle mode. Possible values: • `true`: When you press the "Scan" softkey, it remains highlighted and the scan is performed continuously until you press the softkey again. This is how the "Scan" function works in the "Transfer list - loading list" window. • `false`: When you press the "Scan" softkey, a window opens prompting you to scan only once (default).
`externalIdRegex`	optional	If specified, it describes the location of tool instance IDs (externalIds) in the `contentAddress` in the form of capture groups in a regular expression. If there are multiple tool instance IDs in the `contentAddress`, only the first one is shown in the "Tools to load" and "Sister tools for 1:1 Exchange" window of MMR /Tools. However, all IDs of tool instances in `contentAddress` are considered for addition to the "Transfer list - loading list" window." **Examples:** • `"^(.*)$"` – the whole `contentAddress` specifies a tool instance ID. This is the same as when `externalIdRegex` is missing. • `"<extId>(.*?)</extId>"` – the IDs of tool instances are between `extId` tags in the `contentAddress`.
`contentAddress`	mandatory if enabled=`true` is specified	Specifies the PLC address range where IDs of scanned tool instances are stored as a null-terminated string. The PLC address range is specified in the following format: `/plc/datablock/byte[c<Area>,<StartingByte>,<EndingByte>]` MMR /Tools does not validate the PLC address.

Property	Usage	Description
`acknowledgementAddress`	mandatory if enabled= `true` is specified	Specifies the PLC address of the trigger bit. It is set by the code scanner to indicate that new content has been scanned and successfully written to the PLC (see `contentAddress`). MMR /Tools triggers the reading of content on the bit change from "`0`" to "`1`". The PLC address bit is specified in the following format: `/plc/datablock/bit[c<Area>,<Byte>.<Bit>]` MMR /Tools does not validate the PLC address.
`lockAddress`	optional	If specified, it describes the PLC address bit that MMR /Tools sets to "1" before reading the content from `contentAddress`. After reading the content from `contentAddress`, it is reset to "0". When the value in the `lockAddress` is "`1`", the code scanner must not write the ID to `contentAddress`. The PLC address bit is specified in the following format: `/plc/datablock/bit[c<Area>,<Byte>.<Bit>]` MMR /Tools does not validate the PLC address.

Procedure

To program MMR /Tools for the use of the PLC code scanner, you have to create a file "mmrConfig.json" on SINUMERIK.

1. Open or create the file "mmrConfig.json" on SINUMERIK as specified
   To find the configuration file directory, see Directory for configuring file "mmrConfig.json" (Page 248).
2. Extend the content of the file with a new section `scannerConfiguration` as described above.
   Example:

```
{
   ...
 },  "scannerConfiguration": {
    "enabled": true,
    "toggle mode": true",
    "externalIdRegex": "<extId>(.*?)</extId>",
    "contentAddress": "/plc/datablock/byte[c81,10,20]",
    "acknowledgementAddress": "/plc/datablock/bit[c82,2.1]",
    "lockAddress": "/plc/datablock/bit[c82,2.2]"
 }
}
```

13.1.3.2 USB code scanner

Overview

USB code scanners can also be used with MMR /Tools. A USB code scanner, when connected to SINUMERIK via USB, acts as a secondary keyboard and the scanned values appear in MMR /Tools as if being typed in with a regular keyboard.

USB code scanner scans an ID of a tool instance, which is set in the “Identification” field of the “Tools to load” window. The scanned value appears in the field and the tool list is updated with the external tool from the server. If only the "Identification" field has to be considered during the update, the "Production order" field should be kept empty."

13.1.4 Regional and language options

To enter decimal values without error message on the client, set the decimal separator in the operating system.

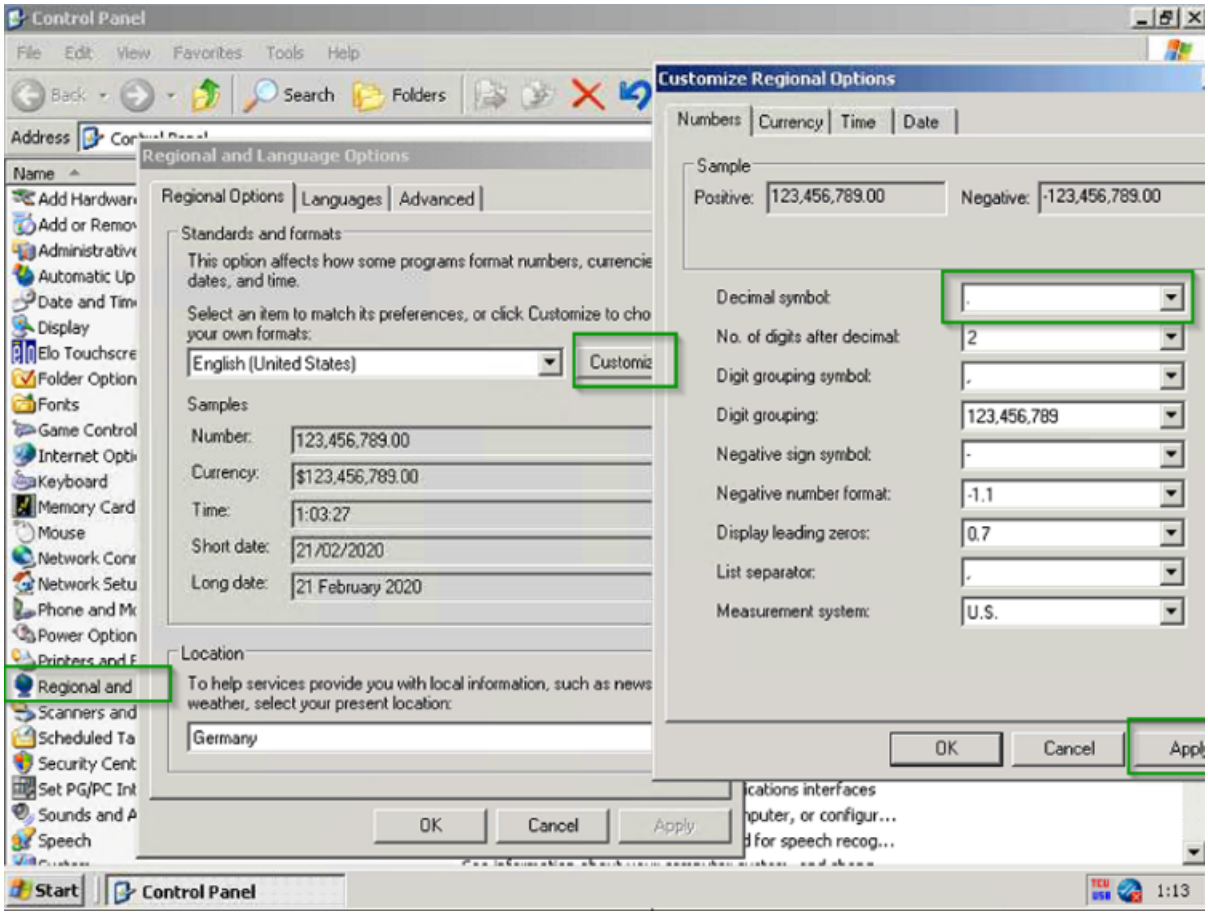
Prerequisite

PCU with HMI-Advanced

- Windows NT
- Windows XP

Procedure

1. Select: Windows > Control Panel > Regional and Language Options > Regional Options.
2. Select the desired language from the drop-down list, e. g. English (United States).
3. Click on the "Customize ..." button.
4. The "Customize Regional Options" windows > tab "Numbers" opens.
5. From the "Decimal symbol" drop-down list, select the entry ".".
6. Click "Apply".



13.1.5 Regie.ini file

When installing MMR /Tools on a SINUMERIK control where there is a previously installed application which has a softkey and entries in the "regie.ini" file and in control language files, you can comment with ";" installed application entries in the files to prevent MMR /Tools installation to overwrite those entries.

Prerequisite

PCU with HMI-Advanced

- Windows NT
- Windows XP

Procedure

1. You can find the files in following directory:
   – F:\add_on\
     - AND -
   – F:\add_on\language directory
2. Open the "regie.ini" and/or "language" file .
3. To prevent the new installation of MMR /Programs from overwriting the existing entries, comment the entries with ";".

13.1.6 Uninstall of Manage MyResources /Tools client on HMI-Advanced

If you cannot uninstall the client Manage MyResources /Tools, you must perform the following steps.

Procedure

1. Stop HMI-Advanced.
2. Start the PCU in service mode.
3. Run `CMD` with admin rights.
4. Goto F:\tmp\Si5\AppMgmtCache\Install\MMRT and run the exe with following parameters:
   `MMR_Tools_client.exe /v"ACTION=ADMIN UNINSTALL=1"`

13.2 Manage MyResources /Programs

13.2.1 Regie.ini file

When installing MMR /Programs on a SINUMERIK control where there is a previously installed application which has a softkey and entries in the "regie.ini" file and in control language files, you can comment with ";" installed application entries in the files to prevent MMR /Programs installation to overwrite those entries.

Prerequisite

PCU with HMI-Advanced

- Windows NT
- Windows XP

Procedure

1. You can find the files in the following directory:
   - F:\add_on\
     - AND -
   - F:\add_on\language directory
2. Open the "regie.ini" file and/or the "language" file.
3. To not overwrite the existing entries, comment these entries with ";".

13.2.2 Uninstall of Manage MyResources /Programs client on HMI-Advanced

If you cannot uninstall the client Manage MyResources /Programs, you must perform the following steps.

Procedure

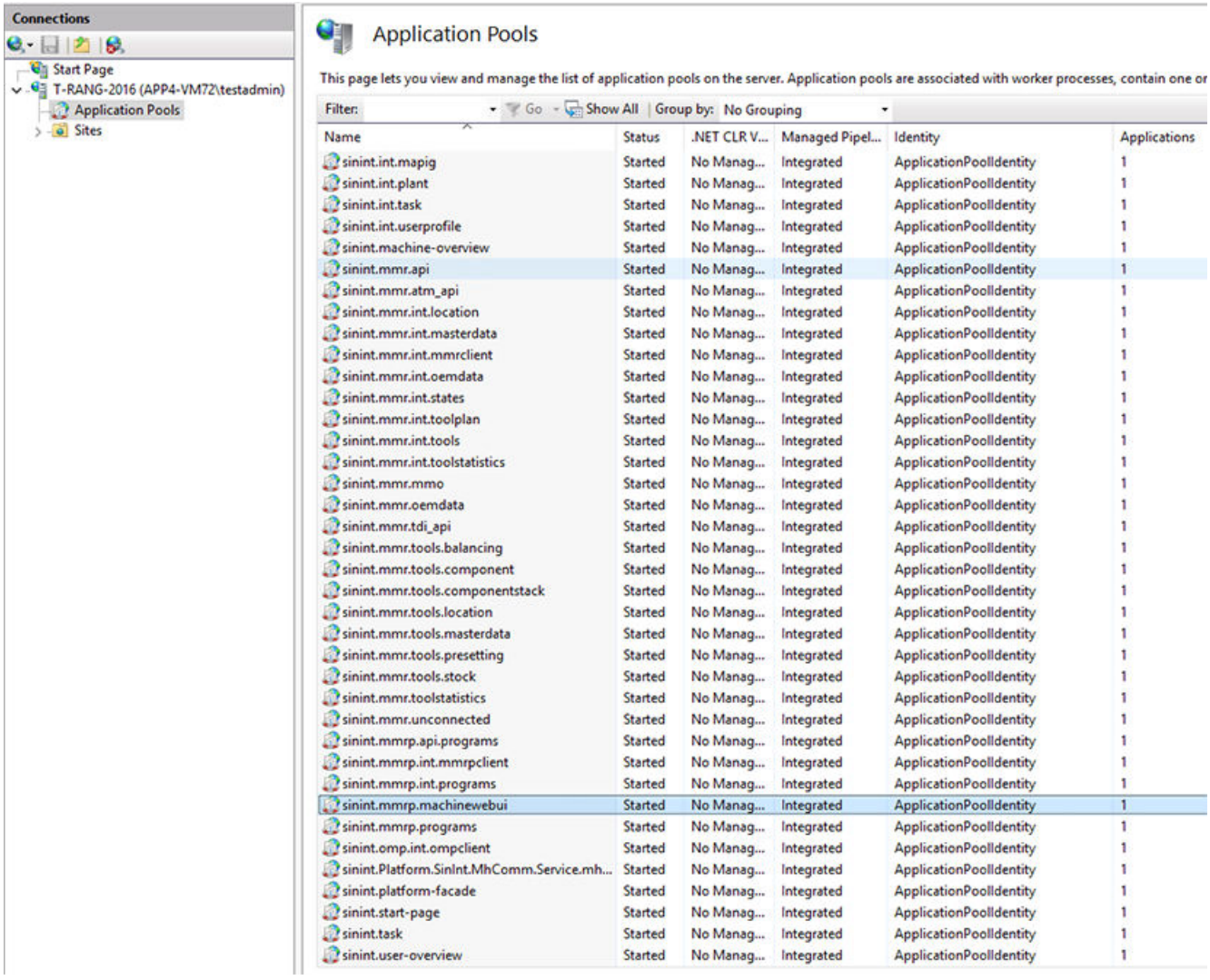
1. Stop HMI-Advanced.
2. Start the PCU in service mode.
3. Run `CMD` with admin rights.
4. Go to F:\tmp\Si5\AppMgmtCache\Install\MMRP and run the exe with following parameters:
   `MMR_Programs_client.exe /v"ACTION=ADMIN UNINSTALL=1"`

13.2.3 Programs for Managed Machines - Accessing remote file shares

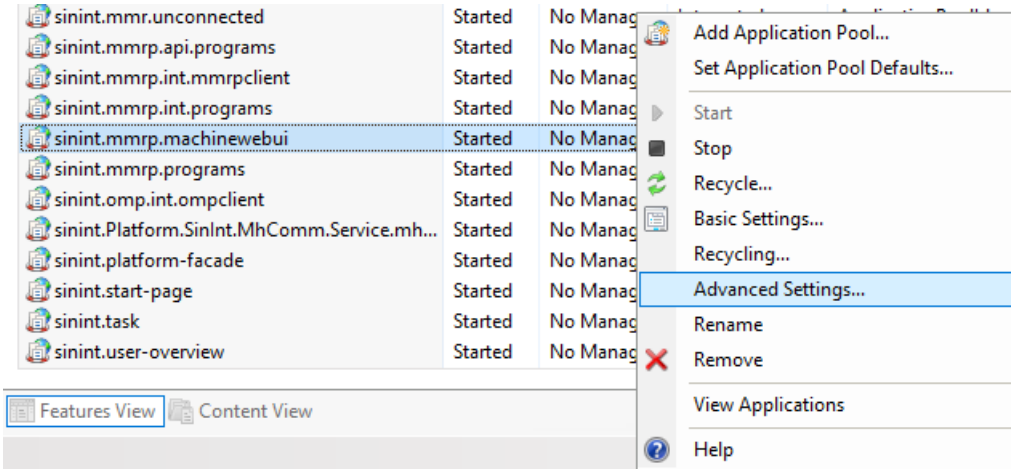
If you want to transfer files from the application to remote share locations, you have to configure some things manually.

Procedure

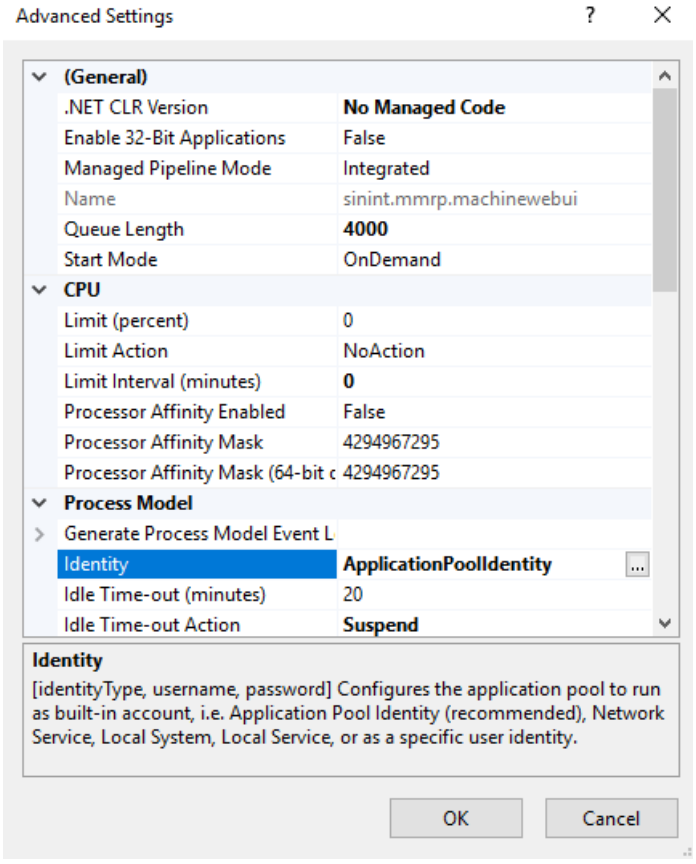
1. Open Internet Information Services (IIS) Manager.
   Under Application pools, find the "sinint.mmrp.machinewebui" application pool.



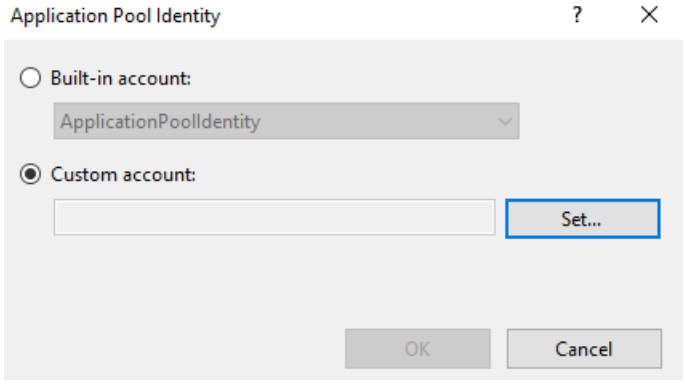
2. Click right and select "Advanced Settings..."



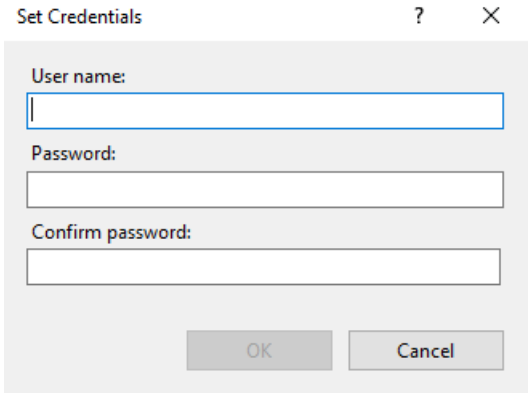
3. Select the Identity row in the popup window. The value by default is "ApplicationPoolIdentity". Click the three dots at the end of the row to configure.



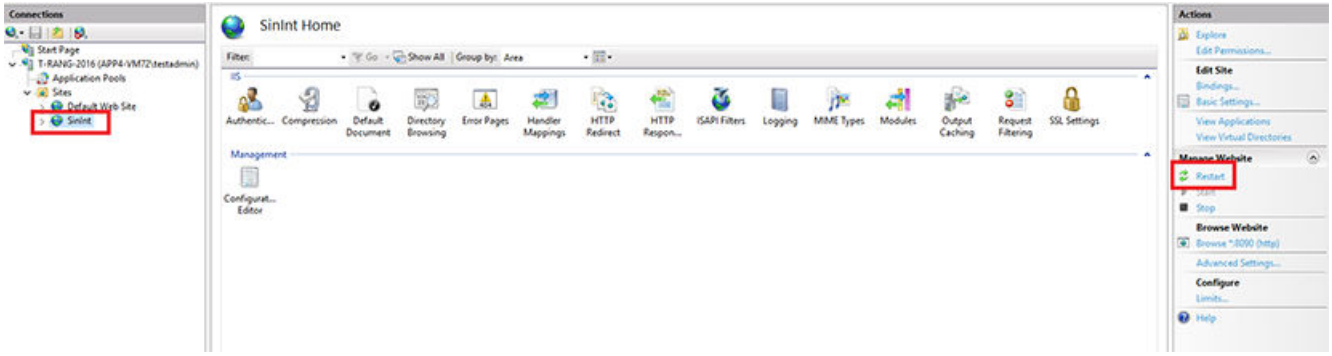
4. Select "Custom account".[Screenshots/13_2_3_accessing_remote_file_shares_4.png]



5. Click "Set...".
   Enter the user name and password that you would like to use. It is important to set a user that is allowed to access the desired locations. Otherwise the file transfer fails. The user must have read/write access to the file shares.
   After changing these settings, the "Programs on Managed Machine" application is running in the name of the selected user. It does all operations authenticated as that user.



6. Click "OK" on all windows.
7. Go to the "SinInt" site.
   Restart it for the new settings to take effect.



13.3 Optimize MyProgramming /NX-Cam Editor

13.3.1 Setting up a connection to the CAM server

You must make the following adaptations to set up a connection to the CAM server.

Prerequisite

- You need administrator rights.
- A user must already be created in the NX CAM server.

Procedure

1. Open the file in the following directory:
   <Installation directory>\SME\SinInt.SMEClient.Service\appsettings.production.json
2. Open entry "NxCamServer".
   Supplement the corresponding data, such as
   - end point and access data
   - User name and password, e.g.:

```
{
 "NxCamServer":{
 "Endpoint":"https://***NXCAMSERVERURL***",
 "Username":"***user***",
 "Password":"***pw***",
 "Scope":"SME"
 },
  "ConsulEncryptFile":"<Installation directory>\\Consul\
\encrypt.json"
}
```

Additional information

The following description explains how you install and configure the NX CAM server:

- NX CAM server documentation

For configuring secure connection between NX CAM server and Optimize MyProgramming /NX-Cam Editor see the following How-To (https://tomcat.apache.org/tomcat-8.5-doc/ssl-howto.html)

13.3.2 Running on HMI operate 4.95 and 6.15

If you are using OMP on an HMI Operate version 4.95 (or higher) or 6.15(or higher), the 3D model of the workpiece is not displayed, only the CAM operations. The core functionality of OMP is available, only the 3D model and toolpaths are not displayed.

In order to get the 3D model working again, you need to copy a binary file to the sinintclient folder.

On Windows HMI Operate systems:

- Navigate to the location: <HMIInstallDir>\Siemens\sinumerik\hmi\appl
- Locate the file: "slnxviewer.dll"
- Copy the file to the location:<HMIInstallDir>\addon\sinumerik\hmi\sinintclient\base \uiplugins
- Restart the HMI

On Linux embededd HMI Operate systems:

- Navigate to the location: /card/siemens/sinumerik/hmi/appl
- Locate the file: "libslnxviewer.so"
- Copy the file to the location: /card/addon/sinumerik/hmi/sinintclient/base/uiplugins
- Restart the HMI

13.4 Analyze MyPerformance /OEE

To use Analyze MyPerformance /OEE, no further configurations are required.

Troubleshooting

14

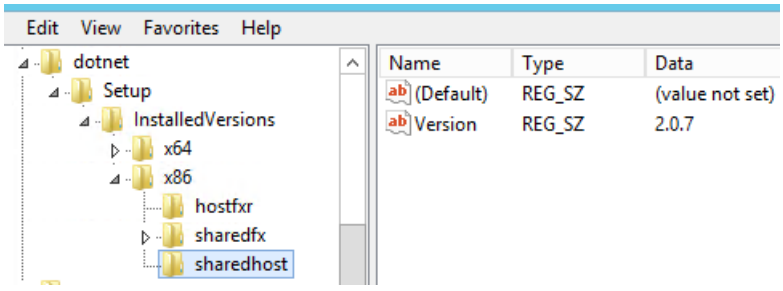
During the installation and configuration, various errors can occur.

The following is a list of error messages and their possible solution.

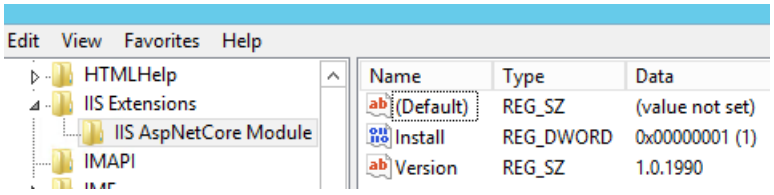
Installing a new version of ".NET".

If a ".NET" is already present, and you are installing the latest version, proceed as follows:

1. Delete the following entries from the registry:
   - HKLM\SOFTWARE\dotnet\Setup\InstalledVersions\x64\sharedhost
   - HKLM\SOFTWARE\dotnet\Setup\InstalledVersions\x86\sharedhost



   - HKLM\SOFTWARE\Wow6432Node \Microsoft\IIS Extensions\IIS AspNetCore Module \Install=1
   - HKLM\SOFTWARE\Wow6432Node \Microsoft\IIS Extensions\IIS AspNetCore Module \Version=x.x.xxxx

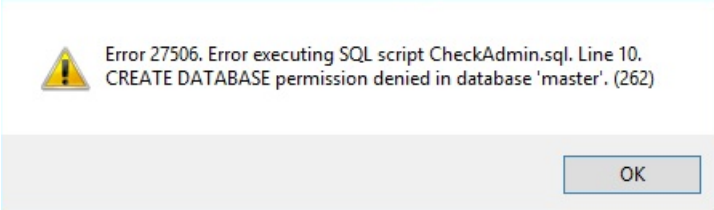


2. Uninstall every component of ".NET".
3. Now install the latest version of ".NET".

Message for the Mcenter installation

After selecting the desired SQL instance, you receive the following error message in the "Database Server" window:

"Error 27506. Error executing SQL script CheckAdmin.sql. Line 10. CREATE DATABASE permission denied in database 'master'. (262)".

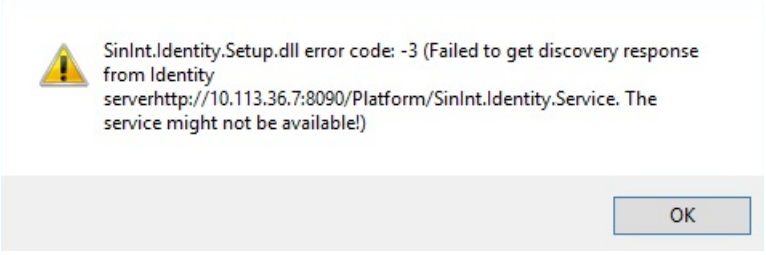


Error correction:

- Activate the "Mixed Mode (SQL Server authentication and Windows authentication)" option in the SQL configuration.
- Check whether the user has sufficient authorizations (admin rights) to save and manage tables and databases.

Message for the Mcenter installation

The Admin user creation may fail because of different settings. You receive an error message, for example "SinInt.Identity.Setup.dll error code: - 3 (Failed to get discovery response from Identity"



Error correction

Collect the log files from the log directories, and put the files in the installation directory.

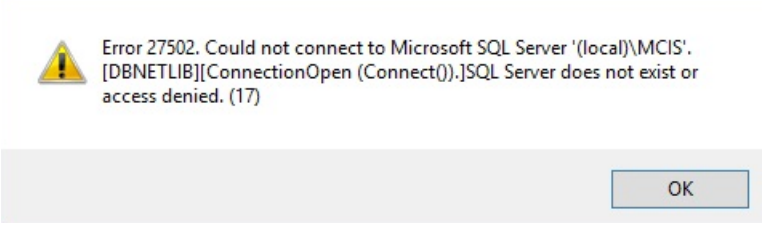
The default directory is, e.g.: C:\Siemens\SINUMERIK_Integrate_5\Logs.

Then contact the hotline.

Message for the Mcenter installation

In the case of a separate database installation, no connection to the SQL server can be established. During the server setup, the following error message is displayed:

"Error 27502. Could not connect to Microsoft SQL Server '(local)\MCIS'. [DBNETLIB] [ConnectionOpen (Connect(),]SQL Server does not exist or access denied"



Error correction:

Check and correct the following network configuration:

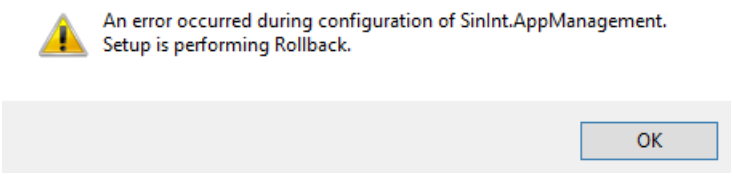
Instead of the SQL server name (`host name\instance`), enter the IP address (`ip address \instance`) of the SQL server instance.

- OR -

Check under "Advanced sharing settings" whether the "Network discovery" function is set to "ON".

Mcenter installation/update

You receive the following error message if a service could not be successfully installed or updated: "An error occurred during configuration of SinInt.AppManagement. Setup is performing Rollback." In this case, the installation/update is repeated.



Error correction:

1. Save all log files.
2. Contact the hotline.

Blank window after login

If different keys are found in the "applicationhost.config" file, a white or blank window is displayed after the login.

Error correction:

1. Open the following directory: C:\Windows\System32\Inetsrv\Config\
2. Open the configuration file "ApplicationHost.config"
3. Search for the following entry: `<httpProtocol>/<customHeaders>`
4. Delete the following keys from the list:

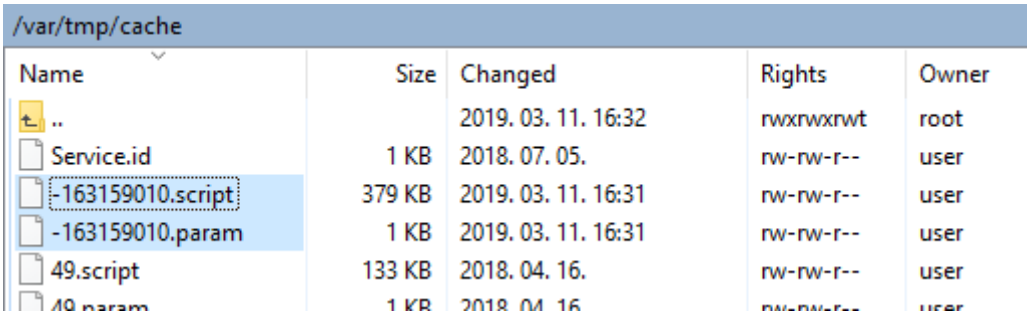
```
<add name="Content-Security-Policy" value="default-src 'none';
script-src 'self'; connect-src 'self'; img-src 'self'; style-src
'self';" />
<add name="Content-Security-Policy-Report-Only" value="script-src
'self' www.google-analytics.com ajax.googleapis.com; connect-src
'self'; img-src 'self'; style-src 'self';" />
```

The SINUMERIK controller does not connect to the Mcenter server

If the SINUMERIK control system was connected to the SINUMERIK Integrate 4.1 server or with another SINUMERIK Integrate 5.x server, no connection to the Mcenter server can be established. The reason for this are hidden scripts in the default directory of the SINUMERIK controller.

Error correction:

1. Delete the contents of the "cache" folder, except for the Service.id file and files that begin with "-", in the following default directories:
   - SINUMERIK Operate under Windows:
     C:\temp\cache

   - SINUMERIK Operate under Linux Embedded:
     /var/tmp/cache
2. Delete the "machineconfig.xml" file in the following standard directories:
   - SINUMERIK Operate under Windows:
     C:\Program Files (x86)\Siemens\MotionControl\user\sinumerik\hmi\cfg
   - SINUMERIK Operate under Linux Embedded:
     /card/user/sinumerik/hmi/cfg
3. Perform a restart.

Reading the details of "SinInt.Identity.Setup.dll" is not possible

The ".dll" file and its contents are hidden files and can only be read and executed by someone with administrator rights.

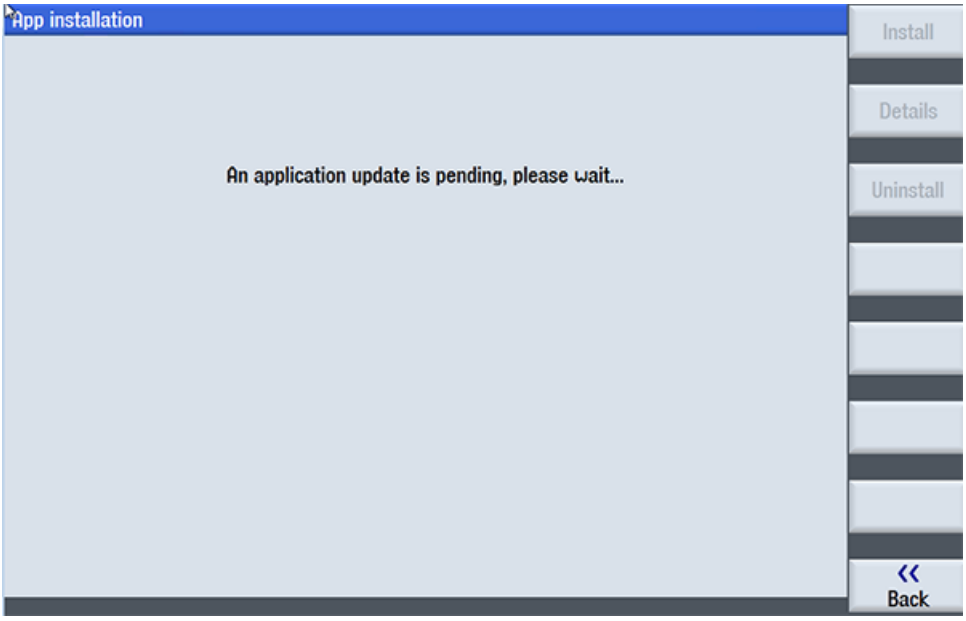
If you want to have the details displayed, execute the following command from the Administrator PowerShell:

```
Get-Command ("C:\Siemens\SINUMERIK_Integrate_5\Platform
\SinInt.Identity.Service\SinInt.Identity.Setup.dll") | Format-List
```

The list of applications is not updated following an update of the script client

If you performed an update with the new client which is not supported, the following message is displayed: "An application update is pending, please wait..."

The list under "Sinumerik_integrate" > "Settings" > "App Installation" is not updated.



Error correction

1. Open the following directories:
   - /addon/sinumerik/hmi/appl/uiscript
   - C:\ProgramData\Siemens\Motioncontrol\addon\sinumerik\hmi\appl\uiscript

   You see 2 directories with identical application names:
   - <Application name>
   - <Application name>_Update
2. Delete the "<Application name>_Update" directory.
3. Restart the HMI.
4. Check to see whether the directory has been deleted.

In case the softkey does not appear on HMI-Advanced

If there are custom softkeys configured it might happen that the softkey does not appear or is on the wrong place.

Control the file "regie.ini" and language settings in the folder:

- F:\Add_on
- F:\OEM
- F:\MMC2

You can modify the softkey place of the MMR /T HMI-Advanced client in file.

- F:\Add_on\regie.ini
  `Taskxx=name := MMRCnt, Timeout := 60000, PreLoad := true`

- AND -

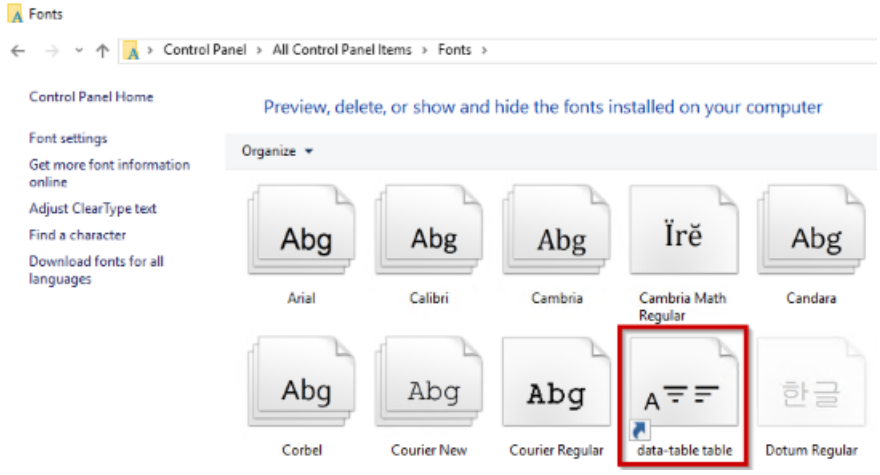
- F:\Add_on\language\RE_xx.INI
  `HSKxx="MMR /Tools"`

In case of a Rollback during an update folders are not deleted

During an update an error occurs and the setup has to rollback, it is possible that few folders are not deleted, for example:

- Logs
- MMR
- MMR-Programs
- Platform

To be able to delete these folders, you must delete from "Fonts" this “data-table table” font. After a system restart you can delete the folders.



HMI Advanced MMR /Tools application does not start

After clicking MMR /Tools HSK, the application does not start. MMR /Tools client application is not able to read certain NCK variables and thus cannot continue initiating process. In such a circumstance, the line below is printed into the file MmrHMIAdvancedScript_MMRT.MmrHMIAdvancedScript_x.log under F:\add_on\MH\log in Info log level:

Job: Script Info 15c8 lib.ncState.checkIsNcReady() - cannot access variables - Exception: Read_Fault

Error correction

The OPC server of the HMI-Advanced must be set to an operational state again. Advanced Windows expertise is required for these steps. Execute the following steps as administrator:

1. Check whether the file "MCVar.dll" exists in the directory "F:\mmc2". If the file is missing, reinstall HMI-Advanced using the "Repair" functionality in the Windows program list.
2. Use the "Regedit" tool to check whether the OPC server is registered in the Windows registry (name: "OPC.Sinumerik.Machineswitch"). If this entry is missing, execute the following command in the Windows command line to register the OPC server: "F:\mmc2\opc\dataaccess\SOPC_MachineSwitch /RegServer"
3. Restart the HMI-Advanced after the changes.

List of abbreviations

A

A.1 List of abbreviations

Admin	Administrator (user role)
API	Application Programming Interface: Programming interface or extension interface for connection and interaction between software systems
CNC	Computerized Numerical Control
COM	Communication
DIR	Directory, directory
FAQ	Frequently Asked Questions
h	Hour
HTTP	Hyper Text Transfer Protocol, hypertext transfer protocol
HTTPS	Hyper Text Transfer Protocol Secure, secure hypertext transfer protocol
IB	Commissioning engineer (user role)
ID	Identification number
IE	Internet Explorer
IFC	Interface Client
IIS	Internet Information Services
IoT	Internet of Things
MB	Megabyte
MLFB	Machine-Readable Product Code
MMR /Tools	Manage MyResources /Tools management
MMR /Programs	Manage MyResources /Programs management
MSTT	Machine control panel
NC	Numerical Control: Numerical control
NCU	Numerical Control Unit: NC hardware unit
OEE	Overall Equipment Effectiveness
OEM	Original Equipment Manufacturer
OP	Operation Panel: Operating equipment
OMP /NX-Cam Editor	Optimize MyProgramming /NX-Cam Editor
PC	Personal Computer
PCU	PC Unit: Computer unit
PLC	Programmable Logic Control
SI	SINUMERIK Integrate
SK	Softkey
SSL	Secure Sockets Layer, cryptographic protocol to encrypt data transferred between server and client
SW	Software
TLS	Transport Layer Security, cryptographic protocol to encrypt data transferred between server and client

TMD	Tool Master Data
TMD-ID	Unique identification of Tool Master Data
TOA	Tool Offset Active, identifier (file type) for tool offset
URL	Uniform Resource Locator
UTC	Universal Time Coordinated

Index

S

T

U

W