SIEMENS

SINUMERIK

MindSphere
Manage MyMachines /Remote - installation in existing control environments

Application examples

Valid for control:
SINUMERIK 840D pl/ 840D sl/840DE sl
HMI-Advanced V6.4/7.6
SINUMERIK Operate V2.7.3.10

Manage MyMachines /Remote V1.0.2.0

10/2018
A5E45211403B AB

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
Division Digital Factory
Postfach 48 48
90026 NÜRNBERG
GERMANY

A5E45211403B AB
℗ 12/2018 Subject to change

Table of contents

Fundamental safety instructions

1

1.1 General safety instructions

⚠ WARNING

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

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

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

⚠ WARNING

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

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

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

1.2 Warranty and liability for application examples

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

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

1.3 Industrial security

Note

Industrial security

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:

Industrial security (http://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 at:

Industrial security (http://www.siemens.com/industrialsecurity)

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, malware 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.
- Protect the drive against unauthorized changes by activating the "know-how protection" drive function.

Preface

2

SINUMERIK documentation

The SINUMERIK documentation is organized into the following categories:

- General documentation/catalogs
- User documentation
- Manufacturer/service documentation

Additional information

You can find information on the following topics at the following address (https://support.industry.siemens.com/cs/de/en/view/108464614):

- Ordering documentation/overview of documentation
- Additional links to download documents
- Using documentation online (find and search in manuals/information)

If you have any questions regarding the technical documentation (e.g. suggestions, corrections), please send an e-mail to the following address (mailto:docu.motioncontrol@siemens.com).

mySupport/Documentation

At the following address (https://support.industry.siemens.com/My/ww/en/documentation), you can find information on how to create your own individual documentation based on Siemens' content, and adapt it for your own machine documentation.

Training

At the following address (http://www.siemens.com/sitrain), you can find information about SITRAIN (Siemens training on products, systems and solutions for automation and drives).

FAQs

You can find Frequently Asked Questions in the Service&Support pages under Product Support (https://support.industry.siemens.com/cs/de/en/ps/faq).

SINUMERIK

You can find information about SINUMERIK at the following address (http://www.siemens.com/sinumerik).

Target group

This publication is intended for:

- Project engineers
- Technologists (from machine manufacturers)
- Commissioning engineers (systems/machines)
- Programmers
- Users

Benefits

The function manual describes the functions so that the target group knows them and can select them. It provides the target group with the information required to implement the functions.

Standard scope

This documentation describes the functionality of the standard scope. Extensions or changes made by the machine tool manufacturer are documented by the machine tool manufacturer.

Other functions not described in this documentation might be executable in the control. This does not, however, represent an obligation to supply such functions with a new control or when servicing.

Further, for the sake of simplicity, this documentation does not contain all detailed information about all types of the product and cannot cover every conceivable case of installation, operation or maintenance.

Note regarding the General Data Protection Regulation

Siemens respects the principles of data privacy, in particular the data minimization rules (privacy by design). For the "Manage MyMachines Remote" product, this means the following:

Information about the remote session duration and those participating.

The product processes/saves the following personal data:

This data does not involve data from the personal/private or intimate domain.

The data specified above is required to evaluate session information. The data saved is limited to the absolute minimum that is required to identify the sessions carried out and the associated participants. Further, it is information that is absolutely necessary to invoice costs between the service provider (OEM) and the end user.

The above specify data cannot be saved with anonymity as the purpose is to identify the associated operating personnel.

This session data can be deleted if necessary. To do this, contact customer support.

Technical Support

Country-specific telephone numbers for technical support are provided in the Internet at the following address (https://support.industry.siemens.com/sc/ww/en/sc/2090) in the "Contact" area.

Introduction 3

3.1 Overview

This document provides information about how to connect SINUMERIK Powerline controls with the HMI Advanced and SINUMERIK Operate operating software with the "Manage MyMachines /Remote" application.

The description below refers to the components listed in following Chapter: System requirements (Page 14).

3.2 System requirements

If you want to connect "Manage MyMachines /Remote" to an existing control environment, the following requirements must be met.

Requirement

To connect to MindSphere, you need a current version of the SINUMERIK Integrate client - and the service client for Manage MyMachines /Remote. Install and configure the client subsequently.

Note

Windows XP

Windows XP and older versions of Windows do not support the TLS1.2 encryption protocol for secure data transmission that is necessary for a connection to MindSphere.

Operating software and hardware

The following procedure is provided with the following components by way of example:

Table 3-1 SINUMERIK 840D pl

Operating software version	SINUMERIK Integrate Client software version	Hardware version	Operating system
HMI-Advanced V07.06.02.05	V4.12.0.21	PCU 50.3B	WinXP SP3
		PCU Base 8.6	
HMI-Advanced V07.06	V4.12.0.21	PCU 50.1	
		PCU 50.3B	
HMI-Advanced V06.04	V4.12.0.21	PCU 50.1	
		PCU 50.3B	
SINUMERIK Operate V2.7.3.10		PCU 50.3	WinXP as of V8.6 SP3
		PCU 50.5	WinXP as of V1.3

SIMATIC IoT2040

Component	Description
SIMATIC IoT2040	Hardware
SIMATIC IoT2000 SD card example image	Firmware for IoT2040
Apache HTTP server (http)	
Apache APR	Condition for Apache
Apache APR-util	Condition for Apache
PCRE	Condition for Apache

Component	Description
dd	Tool for image processing
Roadkil's disk image	Tool for image processing

Security instructions

NOTICE

Security standards for SINUMERIK controls connected to MindSphere

The connection of SINUMERIK controls to MindSphere via TLS 1.2 /https meets the highest security standards.

SINUMERIK versions that do not meet these standards are not part of the product. For these versions, additional security measures must be taken.

You are responsible for preventing unauthorized access to your plants, systems, machines, and networks. Systems, machines and components should only be connected to the company's network or the Internet if and to the extent necessary and with appropriate security measures (e.g. use of firewalls and network segmentation) in place.

NOTICE

Data misuse due to insecure Internet connection

An unrestricted Internet connection can lead to data misuse.

Before establishing a network connection, ensure that your PC is exclusively connected to the Internet via a secure connection. Pay attention to the information relevant to security.

You will find further information about communication security in the configuration manual: Industry Security (https://support.industry.siemens.com/cs/ww/de/view/108862708).

Note

Making the operator PC secure (service engineering side)

The necessary security measures (e.g. virus scanner, firewalls, OS patching, etc.) must be implemented on the PCs that are used for visualization and configuration of Manage MyMachines /Remote with the machine operator or end customer.

Further information about PCs in the industrial environment can be found in the Configuration Manual: Industry Security (https://support.industry.siemens.com/cs/ww/de/view/108862708).

Note

Making the SINUMERIK control secure (machine operator side)

The necessary security measures (e.g. virus scanner, firewalls, operating system patching, etc.) must be implemented on the SINUMERIK controls.

You will find further information about communication security in the Configuration Manual: Industry Security (https://support.industry.siemens.com/cs/ww/de/view/108862708).

NOTICE

Misuse of data

It is essential to use secure data storage for saving your data, particularly confidential data. Store this data encrypted, either locally or on the network. Make sure that this data cannot be accessed by unauthorized personnel.

This applies to the following data:

- Archive files
- Image files
- Project files
- Trace files
- Safety-related data

You will find further information about secure data storage in the Configuration Manual: Industry Security (https://support.industry.siemens.com/cs/ww/de/view/108862708).

NOTICE

Data manipulation possible

There is a risk that an attacker inside the network could gain access to the operator PC. There, the hacker can read or manipulate various system components (e.g. the content of databases). In this way, the attacker can change tool data, NC programs, machine archives, or the system structure itself, for example. Manage MyMachines /Remote cannot prevent this type of attack.

- As the person responsible for the machine network, take measures to ensure the industrial security of the production/machine network.

Siemens AG accepts no liability for this!

Note

Saving the acquired data

The "Manage MyMachines Remote" product was developed by Siemens, taking the "privacy by design" principle into account. This means that it is up to the service provider (OEM) to decide how long the acquired data, such as information about the time period and participation in remote sessions, will be stored.

Delivery form

The SINUMERIK Integrate client, the service client for Manage MyMachines /Remote as well as the latest updates and further information on the applications and products are stored on PridaNet and can be downloaded directly from there.

- OR -

You can contact your machine manufacturer.

- OR -

You can contact the Siemens Service&Support.

Additional references

- Further information on the "SINUMERIK Operate" operating software can be found in the following reference:
  SINUMERIK Operate Commissioning Manual (IM9)
- For further information on "SINUMERIK Integrate", please refer to:
  SINUMERIK Integrate MMP, MMT, AMC, AMP, AMM/E, AMD Commissioning Manual

Additional information regarding MindSphere applications is available at the following links:

MindSphere (https://support.industry.siemens.com/cs/de/en/view/109742256)

MindSphere documentation (https://documentation.mindsphere.io/index.html#/kiosk/de)

Additional information

When connecting SINUMERIK controls that are not of the current generation, special attention must be paid to security requirements.

The security requirements of MindSphere according to the state of the art must be considered for such controls and ensured with further measures and network components within the local IT environment.

- It must be ensured that the communication between the factory network and MindSphere meets the current security standards, e.g. TLS 1.2.
- It must be ensured that unauthorized access to the control in the company network / factory network environment and attacks on the firewall in front of the control are not possible.
- It must be ensured that communication inside the factory network environment cannot be attacked.

The guidelines of the customer's IT department must be followed.

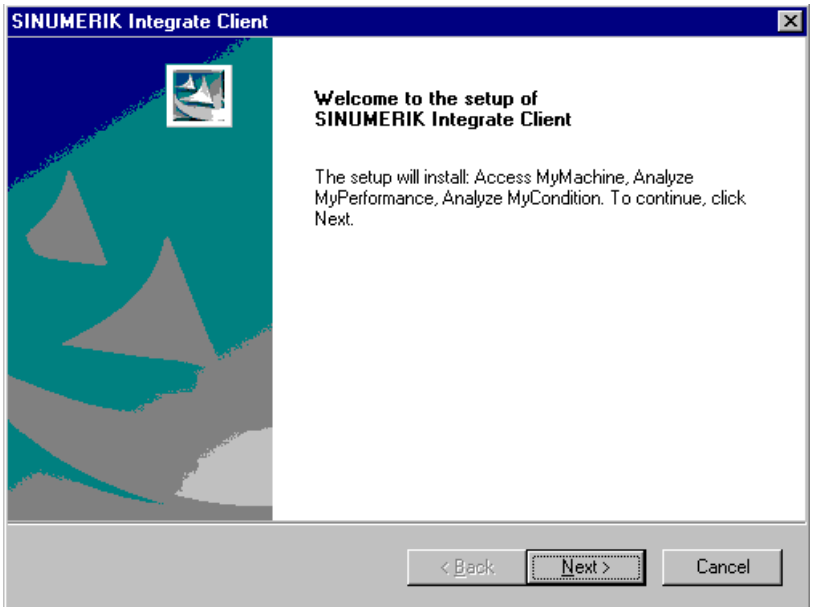
Installation/configuration

4

4.1 SINUMERIK control with HMI-Advanced - installing SINUMERIK Integrate

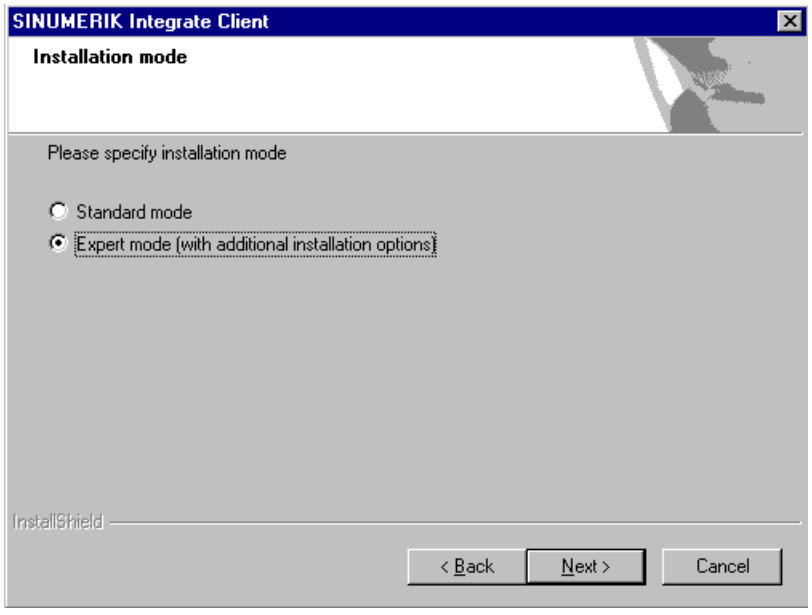
Procedure

1. Start the SINUMERIK control system in Windows service mode.
2. Open the installation directory.
3. Start the "setup.exe" setup file by double-clicking.
   - If you have not installed the appropriate Internet Explorer, a message will appear indicating this, for example, "The program requires Internet Explorer 6 or higher". Installation is canceled and you must install the appropriate Internet Explorer first. Then restart the client installation.
4. The welcome dialog box opens.
   The installation language is English.
   Click on the "Next >" button to prepare for the installation.

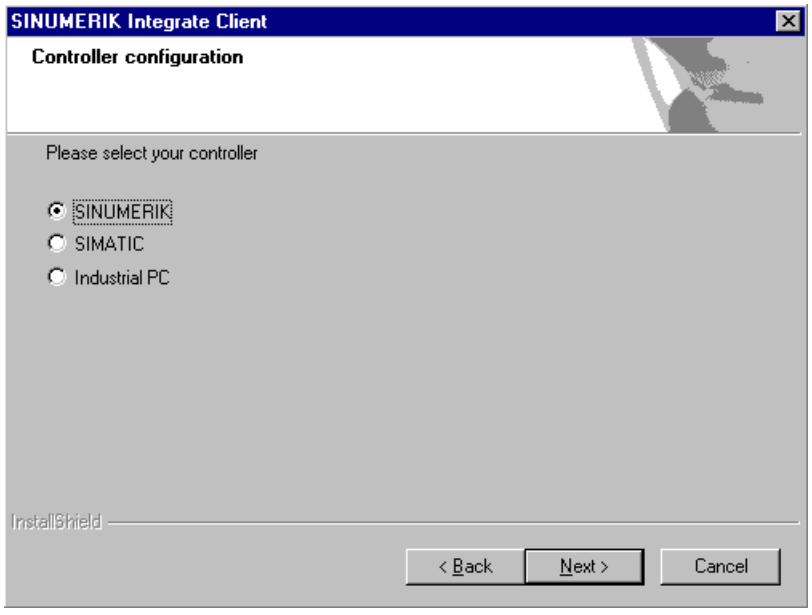


5. The "License Agreement" window opens.
   Read the license agreement.
   - Click "Print" if you want to print out the terms.
   - Then select the "I accept the terms of the license agreement" check box and click "Next >".
     - OR -
     Click "< Back" to return to the previous window.

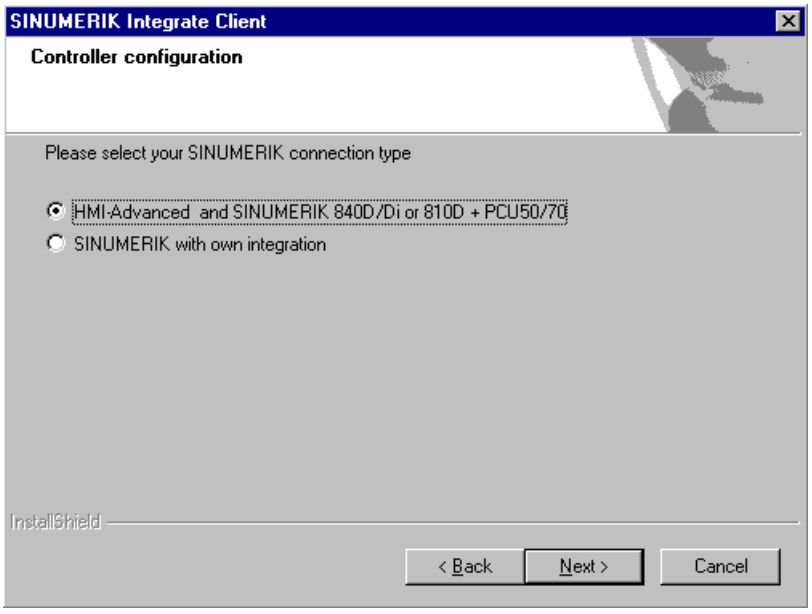
6. The "Installation mode" window opens.
   – Select the option button "Expert mode (with additional installation options)."
   – Click "Next >".



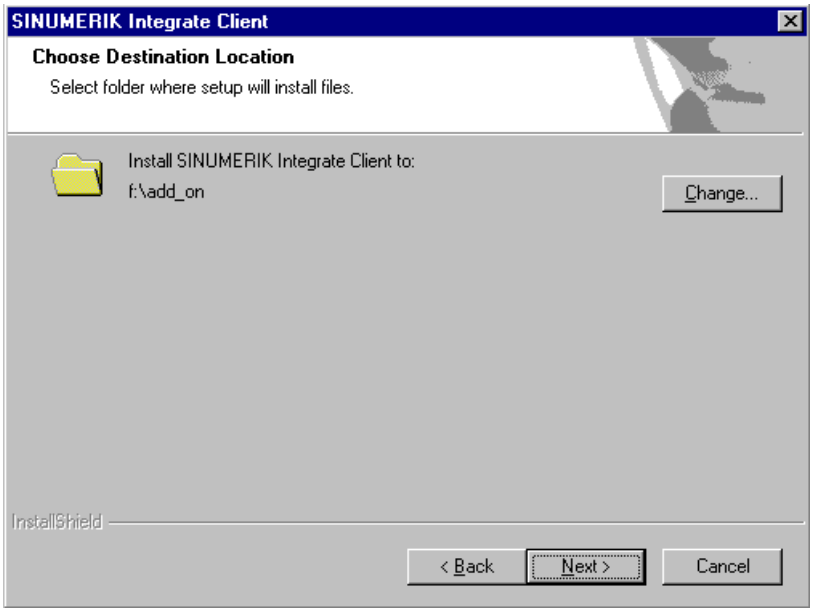
7. The "Controller configuration" window opens. Select your controller.
   – Select, for example, the "SINUMERIK" option button.
   – Click "Next >".



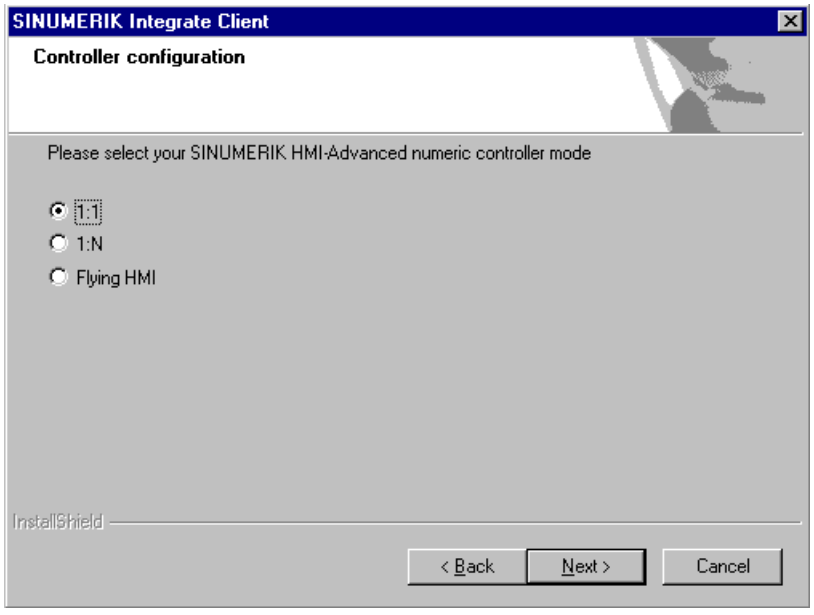
8. Now select the SINUMERIK connection type in the "Controller configuration" window.
   – Select the option button "HMI-Advanced and SINUMERIK 840D/Di or 810D + PCU50/70".
   – Click "Next >".



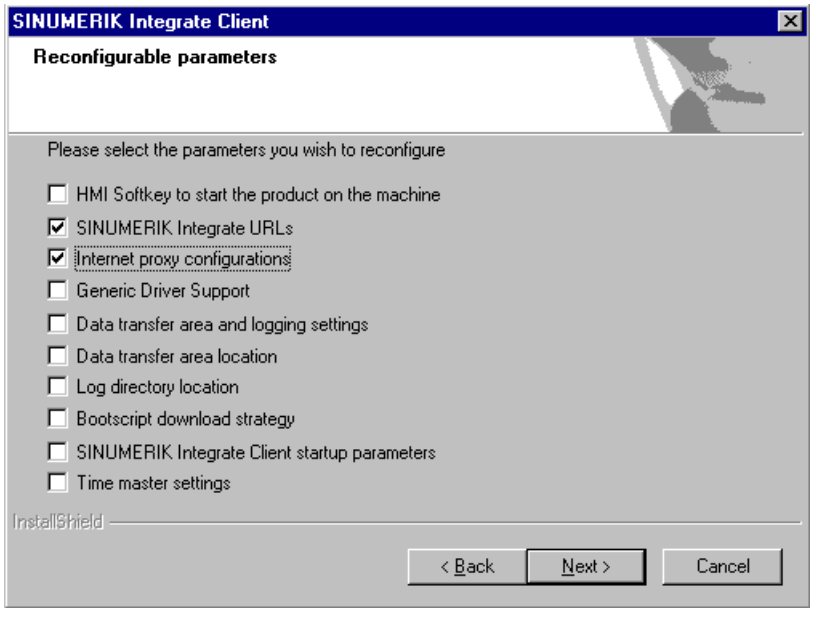
9. The "Choose Destination Location" window opens and the installation directory is displayed.
   – Click "Next >".
   - OR -
   Click "Change..." to change the directory.



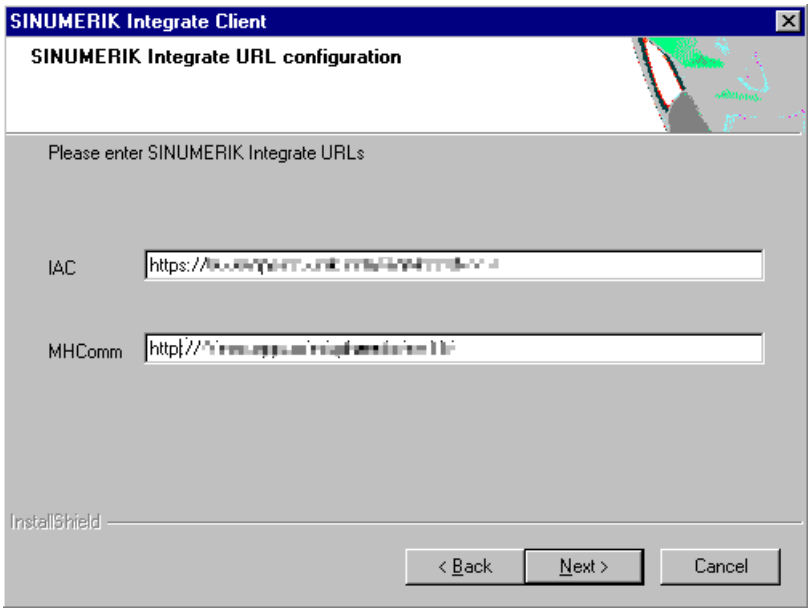
10. The "Controller configuration" window opens.
    - Select the option button for connection "1:1".
    - Then click "Next >".



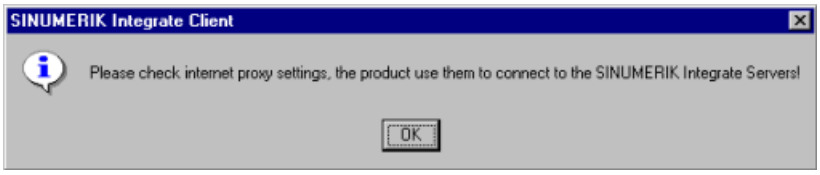
11. The "Reconfigurable parameters" window opens.
    - Select the "SINUMERIK Integrate URLs" and "Internet proxy configurations" check boxes.
    - Click "Next >".



12. The "SINUMERIK Integrate URL configuration" window opens.
    The proxy server is required to connect the control to MindSphere.
    - Enter the following WebService URL for the MindSphere V3 Livesystem in the "MHComm" text box:
      https://gateway.eu1.mindsphere.io/api/agentcom-mmmops/v3/ws11
    - Click "Next >".

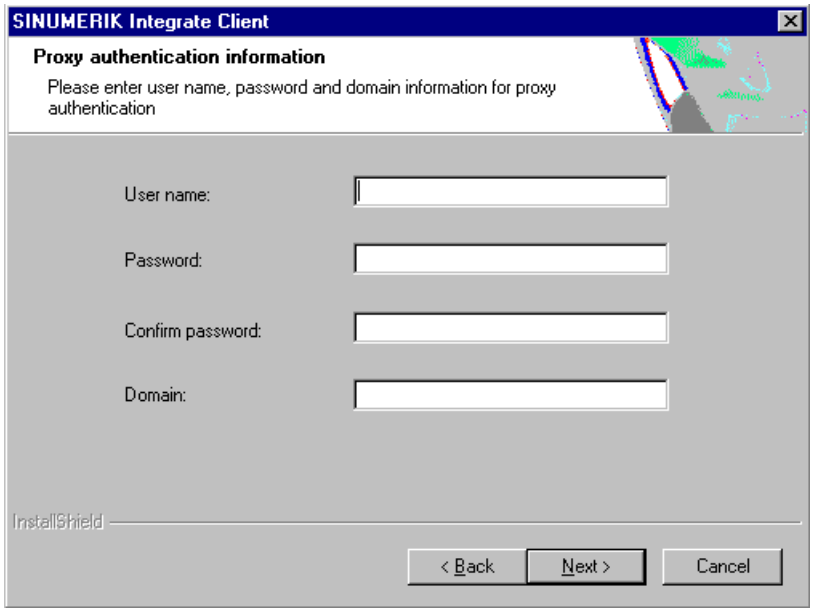


13. The following message is displayed: "Please check internet proxy settings, the product use them to connect to the SINUMERIK Integrate Servers!"
    - Click "OK" to adapt the proxy server.

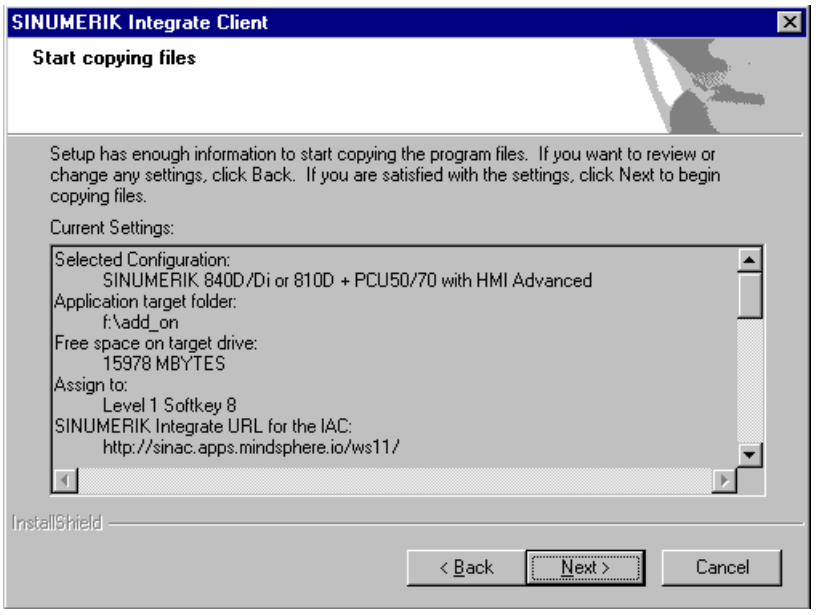


14. The "Question" window opens with the following question: "Do you need proxy authentication?"
    - If authentication is required for the proxy, click "Yes".

15. The "SINUMERIK authentication information" window opens.
    Enter the data in the text boxes:
    - User name:
    - Password:
    - Confirm password:
    - Domain:
    - Click "Next >".



16. The "Start copying files" window opens and the settings made are displayed.
    – Click "Next >" to copy the data to the SINUMERIK control.



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

4.2 SINUMERIK control with SINUMERIK Operate - Setting the proxy

The SINUMERIK Operate operating software is delivered together with the SINUMERIK Integrate Client software.

An update is not possible.

Note

Transferring SINUMERIK data on the MindSphere platform

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

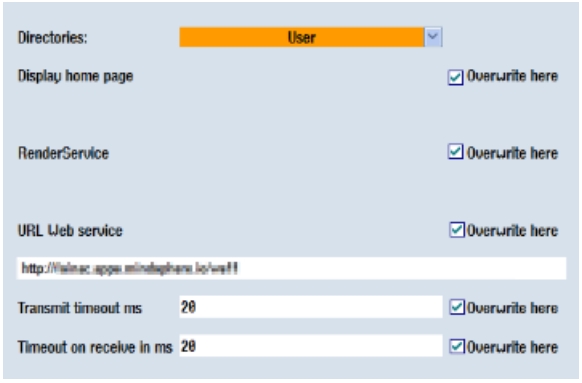
By performing the steps described below, Processes in which software scripts are loaded to the SINUMERIK control are performed automatically, especially by input and confirmation of the web service URL.

Requirement

SINUMERIK Integrate has been enabled for usage.

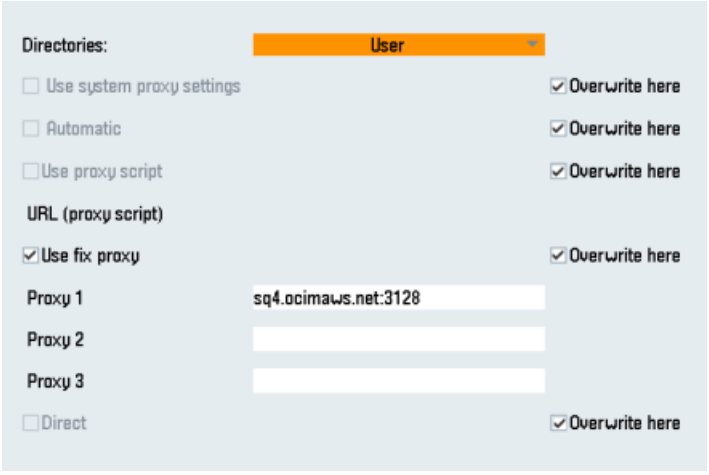
Procedure

1. The "Settings" window is open.
   Press the "URLs>" softkey.
2. Press the "Edit" softkey and select the following settings:
   - Directory: Select the "User" entry in the "Directory" drop-down list.
   - Display home page: Select the "Overwrite here" check box.
   - RenderService: Select the "Overwrite here" check box.
   - URL web service: Select the "Overwrite here" check box.
   - Enter the following WebService URL, for example, for the MindSphere V3 Livesystem:
     https://gateway.eu1.mindsphere.io/api/agentcom-mmmops/v3/ws11
   - Enter the required value in the "Transmit timeout ms" text box (default value is 200). For MindSphere, a value of "20" is recommended, and select the "Overwrite here" check box.
   - Enter the required value in the "Timeout on receive in ms" text box (default value is 200). For MindSphere, a value of "20" is recommended, and select the "Overwrite here" check box.

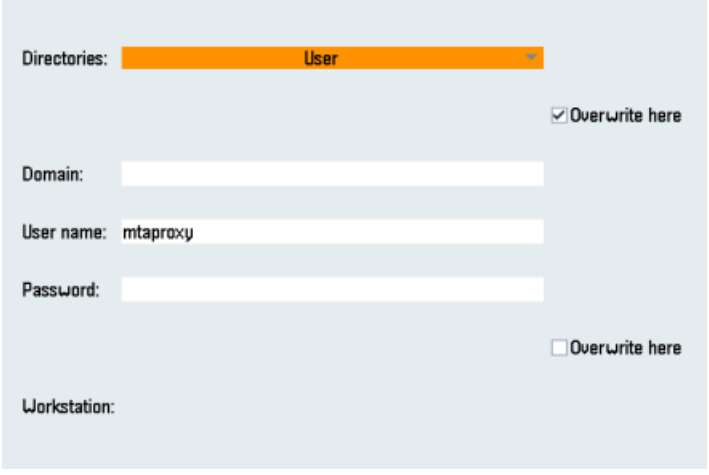


3. Press "OK".
   A syntax check is performed and the access data is saved.
4. To establish a connection from the customer network, you must adapt the proxy settings.
   - Press the "Proxys>" softkey.
     The stored settings are displayed.

5. Press the "Edit" softkey and select the following settings:
   - Select the "Use fix proxy" check box.
   - Enter your proxies in the "Proxy 1" to "Proxy 3" text boxes.
   - Select the "Overwrite here" check box even if you only enter one proxy, to apply the new entry.
   - Press the "OK" softkey to save the settings.



6. If an authentication is required for the proxy, press the "Authorization" softkey.
   - Select the "Overwrite here" check box to apply the new entry.
   - Enter the user data in the "Domain", "User name" and "Password" text boxes.
   - Press the "OK" softkey to save the settings.



7. Restart the control so that the access data can take effect.

4.3 Installing Service Client Manage MyMachines /Remote under Windows XP

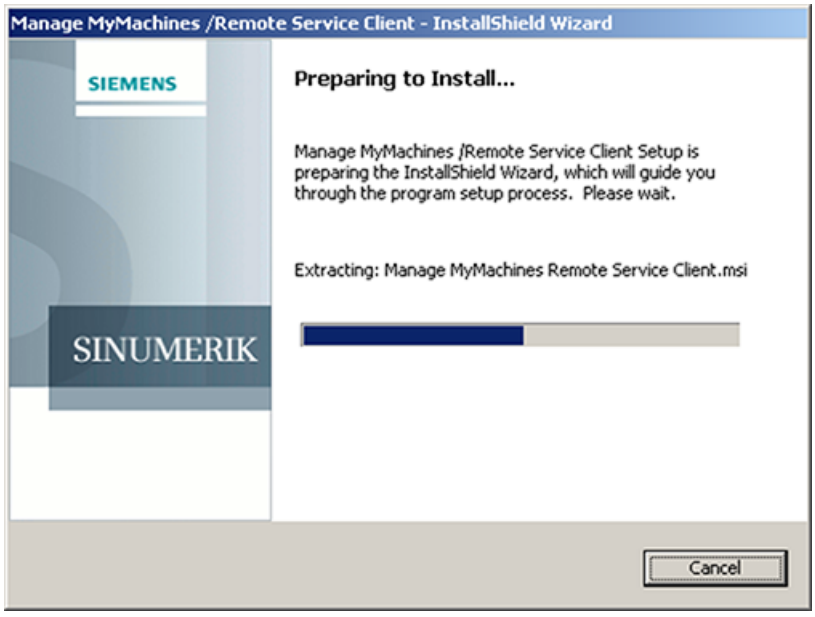
Requirement

You have downloaded the following software from "Manage MyMachines /Remote", e.g. to a USB flash drive.

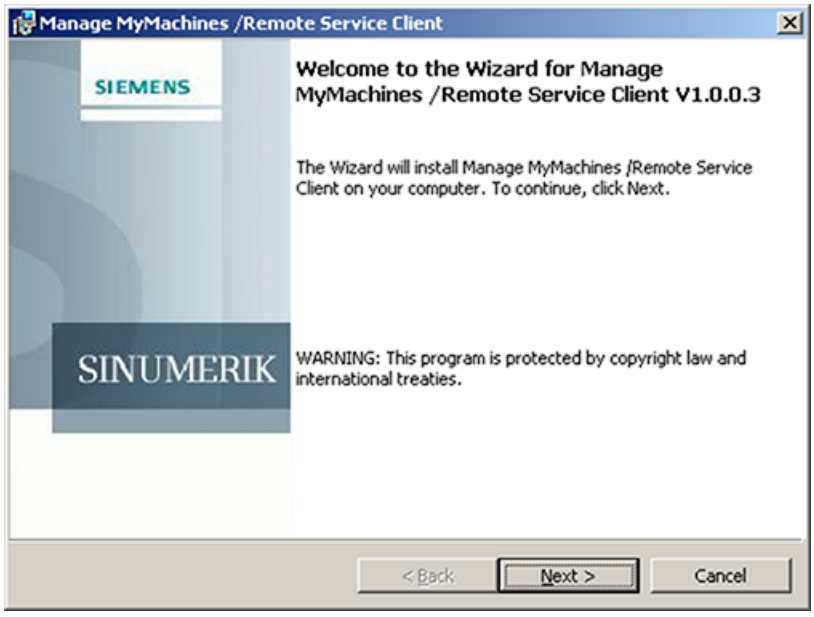
- Manage MyMachines /Remote Service Client for Machine Operators - PCU

Procedure

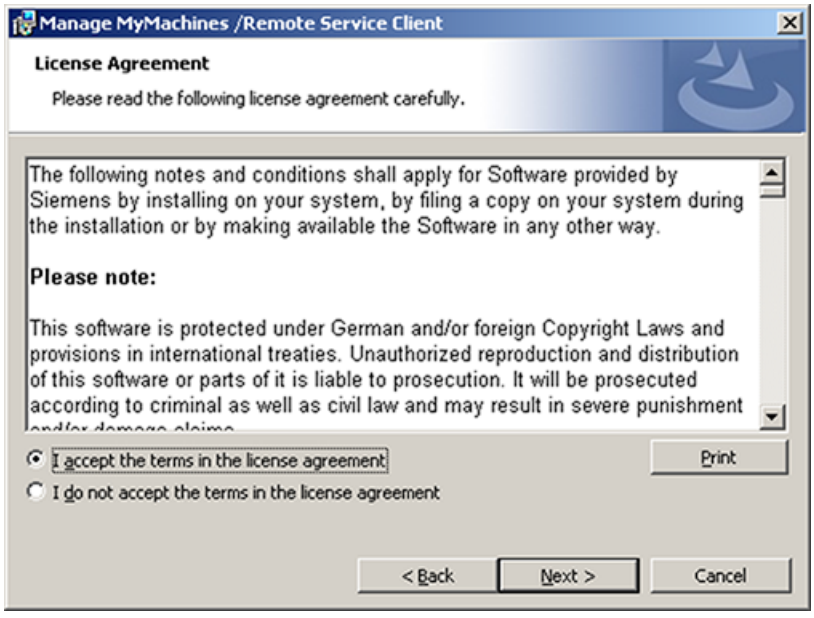
1. Place the software in the installation directory, e.g. under "F".
2. Start "setup.exe" with a double click.
   English is the installation language.
3. "Manage MyMachines /Remote Service Client - InstallShield Wizard" is opened.
   If you click "Cancel", then you return to the previous window.



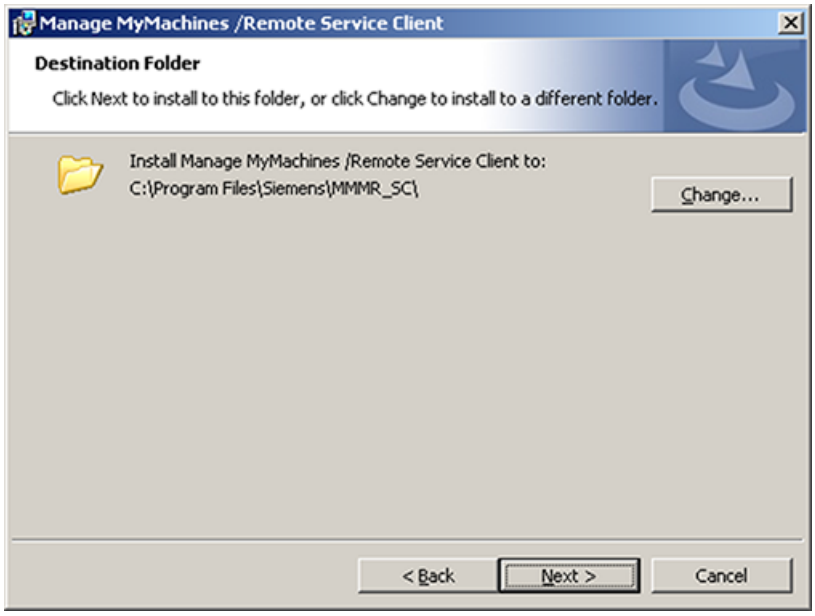
4. The welcome dialog box opens and shows the current version.
   Click "Next >" to prepare for installation.



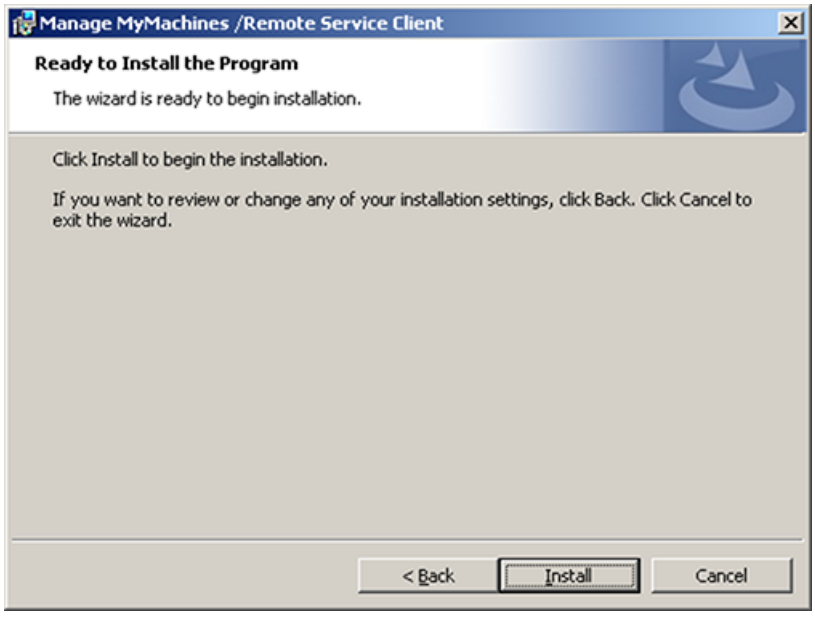
5. The "License Agreement" window opens.
   Read the license agreement.
   - Click "Print" if you want to print out the terms.
   - Then select the "I accept the terms in the license agreement" check box, and click "Next >".



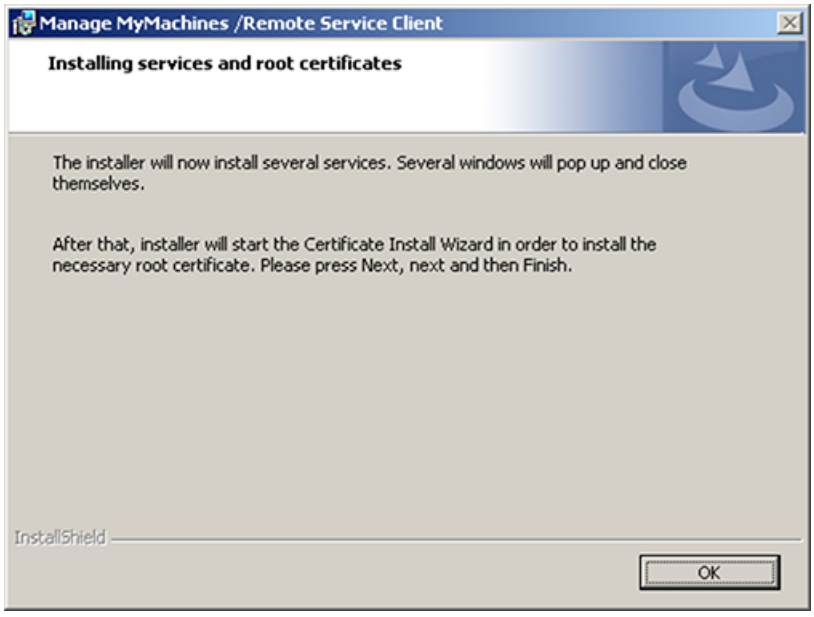
6. The "Destination Folder" window opens and the installation directory is displayed.
   Click "Next >".
   - OR -
   Click "Change..." to change the directory.



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

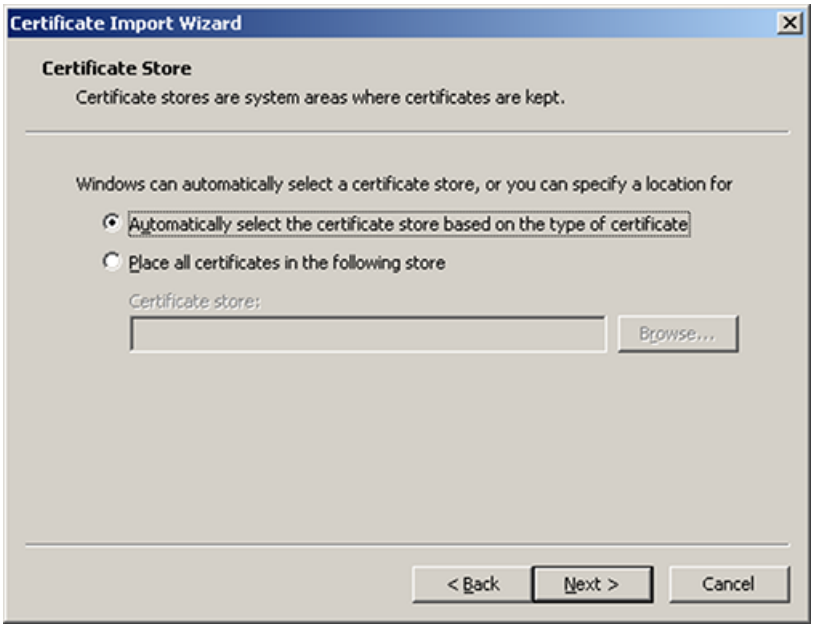


8. The "Installing services and root certificates" window opens.
   Click "OK" to continue with the installation.

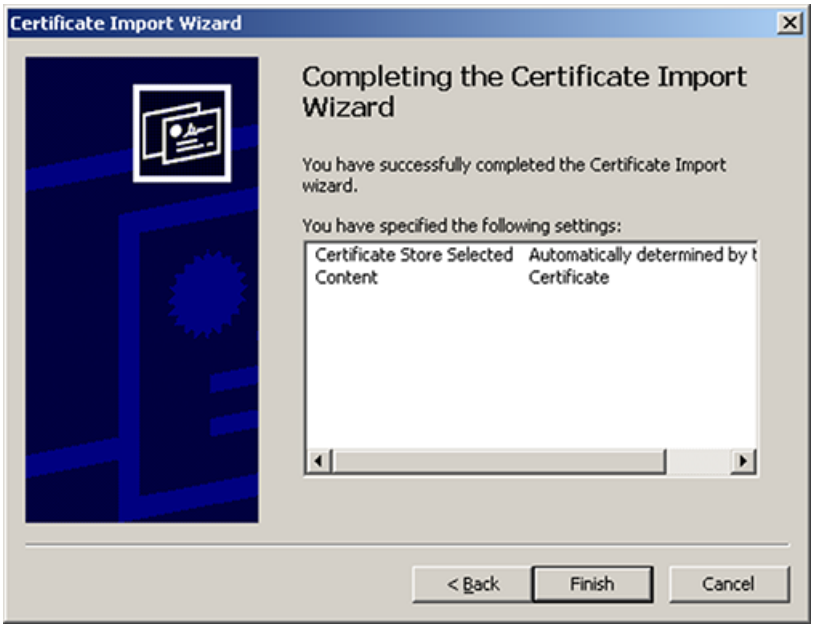


9. The "Welcome to the Certificate Export Wizard" window opens.
   Click "Next >" to start importing the certificates.
   - OR -
   If you click "< Back", you return to the previous window.

10. The "Certificate Store" window opens.
    - Select the check box "Automatically select the certificate store based on the type of certificate".
    - Click "Next >".



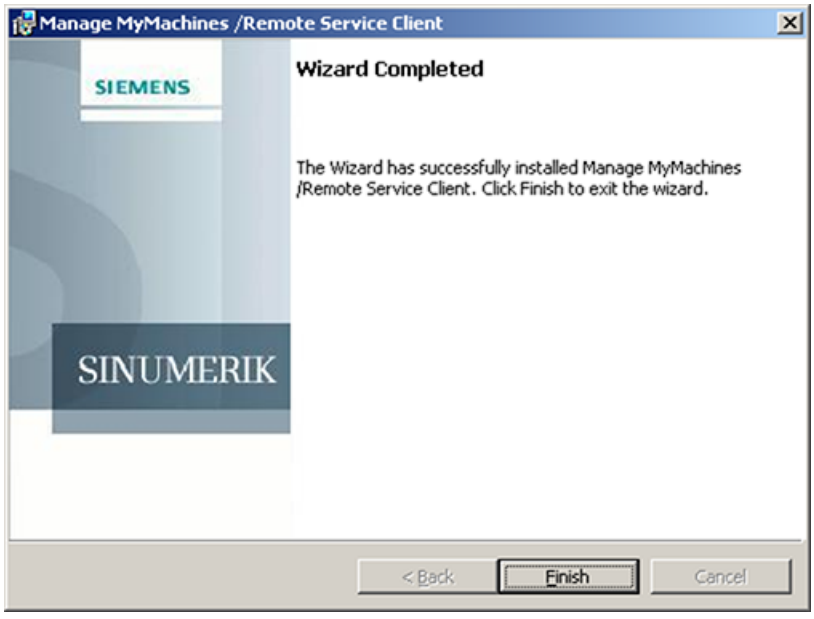
11. The "Completing the Certificate Import Wizard" window is opened.
    You see the selected settings.
    Click "Finish" to complete import of the certificates.



12. You receive a security warning.
    Click "Yes" to continue installing the certificates.

13. A message is displayed indicating that the certificate was successfully imported.
    Click "OK", to exit certificate import.

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



4.4 Connecting the SINUMERIK control system with MindSphere

The activation of SINUMERIK Integrate, the setting up of the URL/proxy and the restart creates the "boot_job" folder in the /var/tmp/ directory. If the directory is not set up, create it manually.

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

- Via the user interface of the operating software
- With the aid of WinSCP

Requirement

The onboard key has been generated

The "boot_job" folder is created on the control, e.g. under "C".

- Linux (SINUMERIK 840): /var/tmp/boot_job
- Win7 PCU 50: C:\temp\boot_job
- WinXP PCU 50: F:\tmp\boot_job

Procedure

1. Start the operating software on the control in service mode.
2. Insert the USB flash drive with the "onboard.key" file into the PCU.
   The USB flash drive is shown in the directory tree.
3. Copy the "onboard.key" file, for example, to the following directory: C:\temp\boot_job.
4. After connection, the "onboard.key" file is deleted and the "cert.key" file is created.
   In the Manage MyMachine Dashboard, the SINUMERIK control (machine) is shown online.

References

You will find further information in the following manual: Function Manual Manage MyMachines

4.5 SIMATIC IoT2040

Overview

This chapter provides information on how to use SIMATIC IoT2040 to install a proxy.

With IoT2040, you connect SINUMERIK controls with MindSphere that do not support TLS 1.2.

TLS 1.2 is required for the connection to IoT2040.

Hardware setup

SIMATIC IoT2040 (**6ES7647-0AA00-1YA2**) is used to setup this configuration.

Products (https://mall.industry.siemens.com/mall/de/WW/Catalog/Products/10321262)

To understand additional preconditions that are required, read the following Chapter: System requirements (Page 14), paragraph "SIMATIC IoT2040".

4.5.1 SIMATIC IoT2000 SD card example image on IoT2040

Procedure

Download the SIMATIC IoT2000 SD-Card example image from the following link:

SD card image (https://support.industry.siemens.com/cs/document/109741799/)

- OR -

From the .zip file:

Image Zip example (https://support.industry.siemens.com/cs/attachments/109741799/)

Roadkil's disk image

1. Use the "Roadkil's Disk Image" to install the image.
   Download the standalone version at the following link:
   Roadkil Disk Image (http://www.roadkil.net/program.php/P12/Disk%20Image)

   Note
   Erase all partitions

   To avoid malfunctions, erase all existing partitions on the SD card before you start.

2. Select the "Write Image" tab.
3. Select "Physical Disk" so that the image can be written to it.

   Note
   Selection of the physical disk

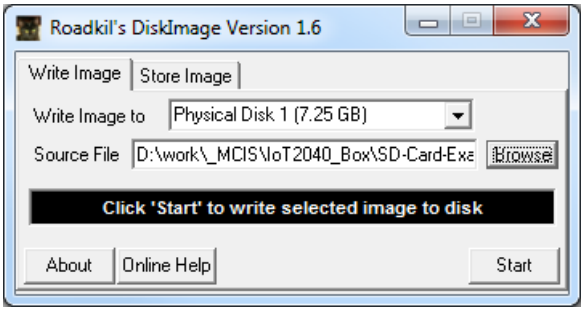
   Ensure that the SD card is selected.

4. Select the "example-V2.2.0.wic" image file.
5. Click "Start".

Note

Preparing the SD card

Erase all existing partitions on the SD card before you start.



dd

Parameter	Description
if	Input file
of	Output disk/partition
bs	Blocked space (10 MB is recommended)
--progress	Shows the progress

Procedure

1. Use "dd" to install the image.
   Download "dd" at the following link:
   dd (http://www.chrysocome.net/dd)
   - OR -
   From the zip. file:
   dd zip (http://www.chrysocome.net/downloads/dd-0.6beta3.zip)

   Note

   Erase all partitions

   To avoid malfunctions, erase all existing partitions on the SD card before you start.

2. Run, e.g. the following command:
   Note: Run the following lines as a command:

```
dd if=D:\temp\example-V2.2.0.wic of=\\?\Device
\Harddisk1\Partition0 bs=10M --progress
```

Windows computer

1. Open Windows "CMD" as administrator.
2. Open the directory in which "dd.exe" is stored.

3. Write "`dd --list`".
   A list of all mounted drives and partitions appears.
4. Search for the correct drive that you want to use. Observe the displayed warning.
5. Download the image file and the target drive to the "dd tool".
   The procedure takes approximately 3 - 5 minutes.
   The success is displayed.
6. Next step: Output

```
dd --list
rawwrite dd for windows version 0.6beta3.
Written by John Newbigin <jn@it.swin.edu.au>
This program is covered by terms of the GPL Version 2.
Win32 Available Volume Information
\\.\Volume{7994290d-4b77-11e2-b265-c01885b5e329}\
 link to \\?\Device\HarddiskVolume2
 fixed media
 Not mounted
\\.\Volume{afccbe56-4bb9-11e2-8a23-2cd444b4b548}\
 link to \\?\Device\HarddiskVolume1
 fixed media
 Mounted on \\.\c:
\\.\Volume{049b1544-4b77-11e2-a26b-806e6f6e6963}\
 link to\\?\Device\HarddiskVolume3
 fixed media
 Mounted on\\.\d:
\\.\Volume{66f507b7-c527-11e7-8975-005056c00008}\
 link to\\?\Device\HarddiskVolume7
 removeable media
 Mounted on \\.\f:
\\.\Volume{049b1547-4b77-11e2-a26b-806e6f6e6963}\
 link to\\?\Device\CdRom0
 CD-ROM
 Mounted on \\.\e:
NT Block Device Objects
 \\?\Device\CdRom0
  size is 2147483647 bytes
 \\?\Device\Harddisk0\Partition0
  link to \\?\Device\Harddisk0\DR0
  Fixed hard disk media. Block size = 512
  size is 500107862016 bytes
 \\?\Device\Harddisk0\Partition1
  link to \\?\Device\HarddiskVolume1
```

```
  \\?\Device\Harddisk0\Partition2
    link to \\?\Device\HarddiskVolume2
  \\?\Device\Harddisk0\Partition3
    link to \\?\Device\HarddiskVolume3
  \\?\Device\Harddisk1\Partition0
    link to \\?\Device\Harddisk1\DR4
    Removable media other than floppy. Block size = 512
    size is 7780433920 bytes
  \\?\Device\Harddisk1\Partition1
    link to \\?\Device\HarddiskVolume7
    Removable media other than floppy. Block size = 512
    size is 7780433920 bytes
Virtual input devices
    /dev/zero         (null data)
    /dev/random       (pseudo-random data)
    -                 (standard input)
Virtual output devices
    -                 (standard output)
    /dev/null         (discard the data)
```

- Next step: Command
  Note: Run the following lines as a command:
  `dd if=D:\temp\example-V2.2.0.wic of=\\?\Device \Harddisk1\Partition0 bs=10M --progress`

Error correction when the image is written to the SD card

If you expect problems when the image is written to the SD card:

- Disconnect the Internet connection.
- Stop the antivirus software.

A local security regulation can also hinder the execution of disk tools.

- Attempt to write the image to the SD card with a computer with less restrictive security settings.

4.5.2 Infrastructure

Overview

This chapter provides notes and tips for the configuration of the IoT2040 in your network. The Linux installation is largely identical. But some specific topics for the associated Yocto image must be observed.

Default network configuration

The configuration for installation of the "default image" is shown below.

The standard network configuration of IoT2000 is:

- X1 P1 LAN (eth0)
  - DHCP: no
  - IP: 192.168.200.1
  - Subnet mask: 255.255.255.0
- X2 P1 LAN (eth1)
  - DHCP: yes

The network configuration is stored at: **/etc/network/interfaces**

```
# /etc/network/interfaces -- configuration file for ifup(8),
ifdown(8)
 # The loopback interface
auto lo
iface lo inet loopback
# Wired interfaces
auto eth0
iface eth0 inet static
     address 192.168.200.1
     netmask 255.255.255.0
auto eth1
iface eth1 inet dhcp
```

First access to IoT240

Ensure the following when accessing IoT2040 for the first time:

- Port "X1 P1" is configured with the static IP address 192.168.200.1
  - For access from this port, set your IP address in the range 192.168.200.2 - 192.168.0.254
- Port "X2 P1" is configured as DHCP
  - For access from this port, interconnect to a network with DHCP server.
  - You must know the IP address of your IoT2040.

Changing the network configuration

Edit the "# interfaces" section in "/etc/network/interfaces":

Configure DHCP at a port, e.g. X2 P1 LAN (eth1)

```
auto eth1
iface eth1 inet dhcp
```

Configure a static (invariable) IP at a port, e.g. X1 P1 LAN (eth0)

```
auto eth0
iface eth0 inet static
   address 192.168.200.1
   netmask 255.255.255.0
   gateway 192.168.200.252
```

The "gateway" parameter is optional.

Note

Problems with the network configuration

- Do not configure both network ports as DHCP!
- Do not set both network ports as "default" gateways!
- If there are any problems with the network configuration, try configuring both network ports as static IP addresses!
- If the network problems cannot be resolved, contact your local administrator.

Connecting IoT2040

You connect IoT2040 to X1 P1 either with static IP address or with DHCP.

X1 P1 with a static IP address

The default IP address at port "X1 P1" is "192.168.200.1".

- Connect the computer directly to this port using an Ethernet cable.
- Set your local IP address in the same subnet, e.g. "192.168.200.2".
- Connect IoT2000 with the default data.

Connecting X2 P1 with DHCP

Port "X2 P1" of the IoT2040 is configured for DHCP.

- Connect IoT2040 with a DHCP router that provides an IP address.
  This IP address must be known in order to connect Iot2040.
- Connect IoT2000 with the default data.

User name and password

User name and password are preset:

- User name: root
- Password: iot2000

Setting the proxy connection

If you require a proxy server for the Internet connection, proceed as described in the next sections. For example, the Internet connection is required to download the packages required for the following steps.

You have two options for adding a proxy connection:

- Temporary, the connection is valid until the next start
- Permanent, the connection is retained permanently

The following example is used in the following sections:

- Proxy: 123.124.125.126
- Proxy port: 4321

For the implementation in your network, use the current data for your company.

Note

Apache Webserver

- The Apache Webserver does not accept the settings.
- You must also add the proxy connection to the Apache configuration.

Temporary proxy connection

The proxy connection is temporary. The connection is valid until the next start or reboot.

The example data are used for the following commands. Adapt your entries to the company data.

- Proxy: 123.124.125.126
- Proxy port: 4321

For the implementation in your network, use the current data for your company.

Company proxy with user authentication

Run the following commands in PuTTY:

- `export http_proxy="http://123.124.125.126:4321"`
- `export https_proxy="https://123.124.125.126:4321"`

The following command lists all environment variables; they so allow you to check your settings:

- `export`

Ports for the proxy connection

Several ports for Apache 80xxx are specified in the current documentation.

Note

Using different ports

If specifications require that you use different ports, this is always possible.

Adapt the proxy port everywhere.

The following settings are valid:

- /usr/local/apache2/conf/httpd.conf
- /usr/local/apache2/conf/extra/httpd-vhosts.conf
- All settings that you configured, for example, with your SINUMERIK control.

Permanent proxy connection

The proxy connection is permanent and also remains after a warm restart or reboot.

The example data is used for the following commands; adapt your inputs with your company data.

1. Navigate to the "etc" directory.
2. Open the "profile" file.
3. Add the following lines:
   ```
   export http_proxy="http://123.124.125.126:4321"
   export https_proxy="https://123.124.125.126:4321"
   ```
4. Add the following line (as penultimate line) at the end of the file:
   ```
   "umask 022"
   ```

Company proxy with user authentication

If your company proxy requires user authentication, proceed as follows:

1. Navigate to the "etc" directory.
2. Open the "profile" file.
3. Add the following lines:
   ```
   export http_proxy="http://username:password@123.124.125.126:4321"
   export https_proxy="https://
   username:password@123.124.125.126:4321"
   ```
   Replace "username" with your user name, and "password" with your password.
4. Add the following line (as penultimate line) at the end of the file:
   ```
   "umask 022"
   ```

Company proxy error correction

If problems occur with your particular environment:

- Try to find a solution that works for Linux, in particular in the Yocto project.

Because every company network reacts differently, it is not possible to provide a solution for every situation.

4.5.3 Apache http

Operational sequences and downloads

You require the following operational sequences and download packages for setting up the Apache httpd.

Note
Installation security

Always use the current version for the installation.

1. Download the following data packages:
   - Apache HTTP Server (httpd) (http://httpd.apache.org)
   - Apache APR & APR-util (https://apr.apache.org/)
   - PCRE (https://www.pcre.org/)

   If your IoT2040 has an Internet connection, call "`wget`" and download the data packages directly.
   - OR -
   - Download the data packages manually.
   - Copy the data packages to the following directory: /usr/downloads.
2. Create the directory "/usr/downloads":
```
 /usr
mkdir downloads
cd downloads
```
3. To download all required packages, execute the following commands:
   Note: Run the following lines as a command:
```
wget http://mirror.netcologne.de/apache.org//httpd/
httpd-2.4.33.tar.gz wget http://mirror.23media.de/apache//apr/
apr-1.6.3.tar.gz wget http://mirror.23media.de/apache//apr/apr-
util-1.6.1.tar.gz
```
   Note: Run the following lines as a command:
```
wget ftp://ftp.csx.cam.ac.uk/pub/software/programming/pcre/
pcre-8.42.tar.gz
```

Opening packages

To open the packages, run the following commands in directory "/usr/downloads/":

```
tar zxf httpd-2.4.33.tar.gz

tar zxf apr-1.6.3.tar.gz

tar zxf apr-util-1.6.1.tar.gz

tar zxf pcre-8.42.tar.gz
```

Storing packages in the appropriate folders

To store the packages in the appropriate folders and to name them correctly, run the following commands in directory "/usr/downloads/":

```
mkdir --parents /usr/local
mv httpd-2.4.33 apache2
mv apache2 /usr/local/
mv apr-1.6.3 apr
mv apr /usr/local/apache2/srclib/
mv apr-util-1.6.1 apr-util
mv apr-util /usr/local/apache2/srclib/
mv pcre-8.42 pcre
mv pcre /usr/local/
```

Installing "opkg" and "pcre"

1. Download and install "opkg".
   `opkg install make`
2. Compile and install "pcre".
   Run the following commands in directory "/usr/local/pcre/":
   ```
   ./configure --prefix=/usr/local/pcre
   make
   make install
   ```

Apache APR - Compiling and installing

Note

Error in APR V1.6.3

Because of an error in APR V1.6.3, the compilation of APR causes an error. Edit the file manually to prevent this error.

Further details can be found at: APR (https://stackoverflow.com/questions/).

- Run the following instructions.
- Check whether the error is still present in future APR versions.

1. Run the following command:
   `cd /usr/local/apache2/srclib/apr/`
2. Create a copy of the original file before you begin editing.
   `cp configure configure.original`
3. Replace the
   `$RM "$cfgfile"` line
   with
   `$RM -f "$cfgfile"`

4. Save the change.
5. Open the directory: `cd /usr/local/apache2/srclib/apr/`
   Run the following commands:
   ```
   ./configure --prefix=/usr/local/apr/
   make
   make install
   /usr/local/apache2/srclib/apr/libtool --finish /usr/local/apr/lib/
   ```

Compiling and installing Apache APR-util

1. Switch to the folder: `cd /usr/local/apache2/srclib/apr-util/`
2. Run the following commands:
   ```
   ./configure --prefix=/usr/local/apr-util --with-apr=/usr/local/
   apr
   make
   make install
   ```

Compiling and installing Apache HTTP server (httpd)

1. Switch to the folder: `cd /usr/local/apache2/`
2. Run the following command:
   Note: Run the following lines as a command:
   ```
   ./configure --prefix=/usr/local/apache2 --with-apr=/usr/local/apr/
   bin --with-apr-util=/usr/local/apr-util/bin --with-pcre=/usr/
   local/pcre/bin/pcre-config
   ```

   Note
   Line breaks

   Retain the line breaks - The preceding lines form a command.

   ```
   make
   make install
   ```

Starting and stopping Apache Webserver (httpd)

- Manual start:
  `/usr/local/apache2/bin/apachectl start`
- Manual stop:
  `/usr/local/apache2/bin/apachectl -k stop`
- Manual restart:
  `/usr/local/apache2/bin/apachectl -k graceful`

Apache Webserver (httpd) - Configuring autostart

Creating the start file

1. Open the directory: /etc/init.d/
2. Create the "apache2" file.
3. Enter the following text in the file:

```
#!/bin/bash
#
# apache2     Startup script for the Apache HTTP server
#
 chkconfig:   3 85 15
#             Apache is a World Wide Web server.
description:  It is used to serve \
              HTML files and CGI.
/usr/local/apache2/bin/apachectl $@
```

Editing file properties

1. Enter:
   `chmod 755 /etc/init.d/apache2`
2. Run the following command:
   `update-rc.d -f apache2 defaults`

Further details can be found at: Apache Autostart (https://serverfault.com/questions/16839/)

4.5.4 Configuring Apache http

This chapter describes how you create the required certificates.

You require certificates for:

- Using the https connection
- Configuring the Apache http as proxy for older SINUMERIK controls
- Connection to the live system in older SINUMERIK controls

A minimum configuration that suffices for the connection is described below. Only the required modules are loaded. Only TLS 1.2 is permitted for the SSL connection. Only those ciphers that MindSphere requires for the function are enabled.

Creating a certificate for the SSL connection

1. Create the directory for the certificate:
   `mkdir /usr/local/apache2/ssl_cert`
2. Change to the certificate directory:
   `cd /usr/local/apache2/ssl_cert`

3. Create the certificate and the associated key file with the following command:
   Note: Run the following lines as a command:
   ```
   openssl req -newkey rsa:2048 -nodes -keyout key.pem -x509 -days
   365 -out certificate.pem
   ```

   Note

   Validity of the certificate

   The certificate is valid for one year (365 days).

   To extend the validity, add the parameter "-days 365".

4. Follow the instructions and enter the required information:
   ```
   Generating a 2048 bit RSA private key
   ..............+++
   ..................+++
   writing new private key to 'key.pem'
   -----
   You are about to be asked to enter information that will be
   incorporated
   into your certificate request.
   What you are about to enter is what is called a Distinguished Name
   or a DN.
   There are quite a few fields but you can leave some blank
   For some fields there will be a default value,
   If you enter '.', the field will be left blank.
   -----
   Country Name (2 letter code) [AU]:DE
   State or Province Name (full name) [Some-State]:Bavaria
   Locality Name (e.g., city) []:Nuremberg
   Organization Name (e.g., company) [Internet Widgits Pty
   Ltd]:Siemens
   Organizational Unit Name (e.g., section) []:MindSphere
   Common Name (e.g. server FQDN or YOUR name) []:IoT2040
   Email Address []:
   ```

Editing Apache http configuration files

In the following configuration, the proxy is configured for connecting to MindSphere V3 Livesystem.

- http://gateway.eu1.mindsphere.io/api/agentcom-mmmops/v3/ws11

The following options are available for editing the configuration files:

- Via the connection with WinSCP
- Via the connection with PuTTY or some other SSH client, and using the integrated Linux command line editor "nano" in the current image
- In any other desired manner

The following files are edited:

- /usr/local/apache2/conf/httpd.conf
- /usr/local/apache2/conf/extra/httpd-ssl.conf
- /usr/local/apache2/conf/extra/httpd-vhosts.conf

Editing httpd.conf

Enter the following lines:

```
Listen 8082
LoadModule socache_shmcb_module modules/mod_socache_shmcb.so
LoadModule proxy_module modules/mod_proxy.so
LoadModule proxy_connect_module modules/mod_proxy_connect.so
LoadModule proxy_http_module modules/mod_proxy_http.so
LoadModule ssl_module modules/mod_ssl.so
#LoadModule status_module modules/mod_status.so
#LoadModule autoindex_module modules/mod_autoindex.so
LoadModule vhost_alias_module modules/mod_vhost_alias.so
#LoadModule dir_module modules/mod_dir.so
#ServerAdmin you@example.com
ServerName localhost
Include conf/extra/httpd-vhosts.conf
Include conf/extra/httpd-ssl.conf
```

Inserting the supplement for the company proxy

If a company proxy is used in your company, you must insert an additional line in the configuration.

Example:

- Proxy: 123.124.125.126
- Proxy port: 4321

Add the following line at the end of the file:

- httpd.conf:
  ```
  ProxyRemote * http://123.124.125.126:4321
  ```

Note

Proxy authorization in the proxy remote

Proxy authorization is not supported in the remote proxy in the current Apache version. It could possibly be implemented by Apache in a future release.

If you require this function for your application, you will find one possible solution at the following link:

Proxy authorization (https://bz.apache.org/bugzilla/show_bug.cgi?id=37355)

Editing extra\httpd-ssl.conf

Enter the following lines:

```
#Listen 443

#SSLCipherSuite HIGH:MEDIUM:!MD5:!RC4:!3DES
#SSLProxyCipherSuite HIGH:MEDIUM:!MD5:!RC4:!3DES
```

Note: Run the following lines as a command:

```
SSLCipherSuite ECDHE-RSA-AES128-CBC-SHA256:ECDHE-RSA-AES128-GCM-
SHA256:ECDHE-RSA-AES256-GCM-SHA384:AES128-SHA256
```

Note: Run the following lines as a command:

```
SSLProxyCipherSuite ECDHE-RSA-AES128-CBC-SHA256:ECDHE-RSA-AES128-
GCM-SHA256:ECDHE-RSA-AES256-GCM-SHA384:AES128-SHA256

SSLProtocol -all +TLSv1.2
SSLProxyProtocol -all +TLSv1.2

#ServerName www.example.com:443
#ServerAdmin you@example.com

ServerName IoT2040:443

SSLCertificateFile "/usr/local/apache2/ssl_cert/certificate.pem"

SSLCertificateKeyFile "/usr/local/apache2/ssl_cert/key.pem"
```

Editing extra\httpd-vhosts.conf

Enter the following lines:

```
#<VirtualHost *:80>
#  ServerAdmin webmaster@dummy-host.example.com
# DocumentRoot "/usr/local/apache2/docs/dummy-host.example.com"
#  ServerName dummy-host.example.com

#  ServerAlias www.dummy-host.example.com
# ErrorLog "logs/dummy-host.example.com-error_log"
#  CustomLog "logs/dummy-host.example.com-access_log" common
#</VirtualHost>

#<VirtualHost *:80>
#  ServerAdmin webmaster@dummy-host2.example.com
#  DocumentRoot "/usr/local/apache2/docs/dummy-host2.example.com"
#  ServerName dummy-host2.example.com

#  ServerAlias www.dummy-host2.example.com
#  ErrorLog "logs/dummy-host2.example.com-error_log"
#  CustomLog "logs/dummy-host2.example.com-access_log" common
#</VirtualHost>
```

Note: Run the following lines as a command:

```
  ProxyPassReverse / https://sinumerikagentcom-
dev.apps.mindsphere.io/</VirtualHost>
```

Configuration files - Export

httpd.conf

```
#
# This is the main Apache HTTP server configuration file. It
contains the
# configuration directives that give the server its instructions.
# See <URL:http://httpd.apache.org/docs/2.4/> for detailed
information.
# In particular, see  # <URL:http://httpd.apache.org/docs/2.4/mod/
directives.html>
# for a discussion of each configuration directive.
#
# Do NOT simply read the instructions here without understanding
# what they do. They are shown only as hints or reminders. If you are
unsure,
# consult the online docs. You have been warned.
#
# Configuration and log file names: If the file names you specify for
many
# of the server control files begin with "/" (or "drive:/" for
Win32), the
# server will use that explicit path. If the file names do *not*
begin
# with "/", the value of ServerRoot is prefixed -- so "logs/
access_log"
# with ServerRoot set to "/usr/local/apache2" will be interpreted by
the
# server as "/usr/local/apache2/logs/access_log", whereas "/logs/
access_log"
# will be interpreted as '/logs/access_log'.
```

```
#
# ServerRoot: The top of the directory tree below which the server
# configuration, error and log files are kept.
#
# Do not add a slash at the end of the directory path. If you point
# ServerRoot at a non-local disk, be sure to specify a local disk on
the
# Mutex directive, if file-based mutexes are used. If you wish to
share the
# same ServerRoot for multiple httpd daemons, you will need to change
at
# least PidFile.
#
ServerRoot "/usr/local/apache2"
#
# Mutex: Allows you to set the mutex mechanism and mutex file
directory
# for individual mutexes, or change the global defaults
#
# Uncomment and change the directory if mutexes are file-based and
the default
# mutex file directory is not on a local disk or is not appropriate
for some
# other reason.
#
# Mutex default:logs
#
# Listen: Allows you to bind Apache to specific IP addresses and/or
# ports, instead of the default. See also the <VirtualHost>
# directive.
#
# Change this to Listen on specific IP addresses as shown below to
# prevent Apache from glomming onto all bound IP addresses.
#
#Listen 12.34.56.78:82
Lists 8082
```

```
#
# Dynamic Shared Object (DSO) support
#
# To be able to use the functionality of a module that was built as a
DSO, you
# must place corresponding 'LoadModule' lines at this location so
the
# directives contained in it are actually available _before_ they are
used.
# Statically compiled modules (those listed by 'httpd -l') do not
need
# to be loaded here.
#
# Example:
# LoadModule foo_module modules/mod_foo.so
#
```

```
LoadModule authn_file_module modules/mod_authn_file.so
#LoadModule authn_dbm_module modules/mod_authn_dbm.so
#LoadModule authn_anon_module modules/mod_authn_anon.so
#LoadModule authn_dbd_module modules/mod_authn_dbd.so
#LoadModule authn_socache_module modules/
#mod_authn_socache.so
LoadModule authn_core_module modules/mod_authn_core.so
LoadModule authz_host_module modules/mod_authz_host.so
LoadModule authz_groupfile_module modules/
mod_authz_groupfile.so
LoadModule authz_user_module modules/mod_authz_user.so
#LoadModule authz_dbm_module modules/mod_authz_dbm.so
#LoadModule authz_owner_module modules/
#mod_authz_owner.so
#LoadModule authz_dbd_module modules/mod_authz_dbd.so
LoadModule authz_core_module modules/mod_authz_core.so
LoadModule access_compat_module modules/
mod_access_compat.so
LoadModule auth_basic_module modules/mod_auth_basic.so
#LoadModule auth_form_module modules/mod_auth_form.so
#LoadModule auth_digest_module modules/
#mod_auth_digest.so
#LoadModule allowmethods_module modules/
#mod_allowmethods.so
#LoadModule file_cache_module modules/mod_file_cache.so
#LoadModule cache_module modules/mod_cache.so
#LoadModule cache_disk_module modules/mod_cache_disk.so
#LoadModule cache_socache_module modules/
#mod_cache_socache.so
LoadModule socache_shmcb_module modules/
#mod_socache_shmcb.so
#LoadModule socache_dbm_module modules/
#mod_socache_dbm.so
#LoadModule socache_memcache_module modules/
#mod_socache_memcache.so
#LoadModule watchdog_module modules/mod_watchdog.so
LoadModule macro_module modules/mod_macro.so
#LoadModule dbd_module modules/mod_dbd.so
#LoadModule dumpio_module modules/mod_dumpio.so
#LoadModule buffer_module modules/mod_buffer.so
#LoadModule ratelimit_module modules/mod_ratelimit.so
LoadModule reqtimeout_module modules/mod_reqtimeout.so
#LoadModule ext_filter_module modules/mod_ext_filter.so
#LoadModule request_module modules/mod_request.so
```

```
#LoadModule include_module modules/mod_include.so
LoadModule filter_module modules/mod_filter.so
#LoadModule substitute_module modules/mod_substitute.so
#LoadModule sed_module modules/mod_sed.so
#LoadModule deflate_module modules/mod_deflate.so
LoadModule mime_module modules/mod_mime.so
LoadModule log_config_module modules/mod_log_config.so
#LoadModule log_debug_module modules/mod_log_debug.so
#LoadModule logio_module modules/mod_logio.so
LoadModule env_module modules/mod_env.so
#LoadModule expires_module modules/mod_expires.so
LoadModule headers_module modules/mod_headers.so
#LoadModule unique_id_module modules/mod_unique_id.so
LoadModule setenvif_module modules/mod_setenvif.so
LoadModule version_module modules/mod_version.so
#LoadModule remoteip_module modules/mod_remoteip.so
LoadModule proxy_module modules/mod_proxy.so
LoadModule proxy_connect_module modules/
mod_proxy_connect.so
#LoadModule proxy_ftp_module modules/mod_proxy_ftp.so
LoadModule proxy_http_module modules/mod_proxy_http.so
#LoadModule proxy_fcgi_module modules/mod_proxy_fcgi.so
#LoadModule proxy_scgi_module modules/mod_proxy_scgi.so
#LoadModule proxy_uwsgi_module modules/
#mod_proxy_uwsgi.so
#LoadModule proxy_fdpass_module modules/
#mod_proxy_fdpass.so
#LoadModule proxy_wstunnel_module modules/
#mod_proxy_wstunnel.so
#LoadModule proxy_ajp_module modules/mod_proxy_ajp.so
#LoadModule proxy_balancer_module modules/
#mod_proxy_balancer.so
#LoadModule proxy_express_module modules/
#mod_proxy_express.so
#LoadModule proxy_hcheck_module modules/
#mod_proxy_hcheck.so
#LoadModule session_module modules/mod_session.so
#LoadModule session_cookie_module modules/
#mod_session_cookie.so
#LoadModule session_dbd_module modules/
#mod_session_dbd.so
#LoadModule slotmem_shm_module modules/
#mod_slotmem_shm.so
#LoadModule sed_module modules/mod_sed.so
```

```
#LoadModule lbmethod_byrequests_module modules/
#mod_lbmethod_byrequests.so
#LoadModule lbmethod_bytraffic_module modules/
#mod_lbmethod_bytraffic.so
#LoadModule lbmethod_bybusyness_module modules/
#mod_lbmethod_bybusyness.so
#LoadModule lbmethod_heartbeat_module modules/
#mod_lbmethod_heartbeat.so
LoadModule unixd_module modules/mod_unixd.so
#LoadModule dav_module modules/mod_dav.so
#LoadModule status_module modules/mod_status.so
#LoadModule autoindex_module modules/mod_autoindex.so
#LoadModule info_module modules/mod_info.so
#LoadModule cgid_module modules/mod_cgid.so
#LoadModule dav_fs_module modules/mod_dav_fs.so
LoadModule vhost_alias_module modules/
mod_vhost_alias.so
#LoadModule negotiation_module modules/
#mod_negotiation.so
#LoadModule dir_module modules/mod_dir.so
#LoadModule actions_module modules/mod_actions.so
#LoadModule speling_module modules/mod_speling.so
#LoadModule userdir_module modules/mod_userdir.so
LoadModule alias_module modules/mod_alias.so
#LoadModule rewrite_module modules/mod_rewrite.so


<IfModule unixd_module>
#
# If you wish httpd to run as a different user or group, you must run
# httpd as root initially and it will switch.
#
# User/Group: The name (or #number) of the user/group to run httpd
as.
# It is usually good practice to create a dedicated user and group
for
# running httpd, as with most system services.
#
User daemon
Group daemon
</IfModule>
```

```
# 'Main' server configuration
#
# The directives in this section set up the values used by the
'main'
# server, which responds to any requests that are not handled by a
# <VirtualHost> definition. These values also provide defaults for
# any <VirtualHost> containers defined later in the file.
#
# All of these directives may appear inside <VirtualHost>
containers,
# in which case these default settings will be overridden for the
# virtual host being defined.
#
#
# ServerAdmin: The address where problems with the server should be
# e-mailed. This address appears on some server-generated pages,
such
# as error documents. e.g. admin@your-domain.com
#
#ServerAdmin you@example.com
#
# ServerName gives the name and port that the server uses to identify
itself.
# This can often be determined automatically, but we recommend you
specify
# it explicitly to prevent problems during startup.
#
# If your host does not have a registered DNS name, enter its IP
address here.
#
#ServerName www.example.com:80
ServerName localhost
#
# Deny access to the entirety of your server filesystem. You must
# explicitly permit access to Web content directories in other
#
<Directory />
   AllowOverride none
   Require all denied
</Directory>
```

```
#
# Note starting at this point, you must specifically allow
# particular features to be enabled - so if something is not working
as
# expected, make sure that you have specifically enabled it
# below.
#
#
# DocumentRoot: The directory from which you access your
# documents. By default, all requests are taken from this directory,
but
# symbolic links and aliases can be used to point to other
locations.
#
DocumentRoot "/usr/local/apache2/htdocs"
<Directory "/usr/local/apache2/htdocs">
   #
   # Possible values for the Options directive are "None", "All",
   # or any combination of them:
   # Indexes Includes FollowSymLinks SymLinksifOwnerMatch ExecCGI
   MultiViews
   #
   # Note that "MultiViews" must be named *explicitly* --- "Options
   All"
   # does not suffice.
   #
   # The Options directive is both complicated and important. Please
   see
   # http://httpd.apache.org/docs/2.4/mod/core.html
   #options
   # for more information.
   #  Options Indexes FollowSymLinks
   #
   # AllowOverride controls which directives may be placed
   in .htaccess files.
   # They can be "All", "None" or any combination of the keywords:
   # AllowOverride FileInfo AuthConfig Limit
   #  AllowOverride None
   #
   # Controls who that can get data from this server.
   #
   Require all granted
</Directory>
```

```
#
# DirectoryIndex: sets the file that Apache accesses if a directory
# is requested.
#
<IfModule dir_module>
   DirectoryIndex index.html
</IfModule>
#
# The following lines prevent .htaccess and .htpasswd files from
being
# viewed by Web clients.
#
<Files ".ht*">
   Require all denied
</Files>
#
# ErrorLog: The location of the error log file.
# If you do not specify an ErrorLog directive within a <VirtualHost>
# container, error messages relating to that virtual host will be
# logged here. If you *do* define an error log file for a
<VirtualHost>
# container, that host errors will be logged there and not here.
#
ErrorLog "logs/error_log"
#
# LogLevel: Control the number of messages logged to the error_log.
# Possible values include: debug, info, notice, warn, error, crit,
# alert, emerg.
#
LogLevel warn
<IfModule log_config_module>
   #
   # The following directives define some format nicknames for use
   with
   # a CustomLog directive (see below).
   #
   LogFormat "%h %l %u %t \"%r\" %>s %b \"%{Referer}i\" \
   "%{User-Agent}i\"" combined
   LogFormat "%h %l %u %t \"%r\" %>s %b" common
   <IfModule logio_module>
    # You need to enable mod_logio.c to use %I and %O
    LogFormat "%h %l %u %t \"%r\" %>s %b \"%{Referer}i\" \
    "%{User-Agent}i\" %I %O"
```

```
combinedio
   </IfModule>
   #
   # The location and format of the access log file (Common Logfile
   Format).
   # If you do not define any access log files within a <VirtualHost>
   # container, they will be logged here. If, however, you *do*
   # define per-<VirtualHost> access log files, transactions will be
   # logged therein and *not* in this file.
   #
   CustomLog "logs/access_log" common
   #
   # If you prefer a log file with access, agent and referrer
   information
   # (Combined Logfile Format) you can use the following directive.
   #
   #CustomLog "logs/access_log" combined
</IfModule>
<IfModule alias_module>
   #
   # Redirect: Allows you to tell clients about documents that used
   to
   # exist in your server namespace, but not anymore. The client
   # will make a new request for the document at its new location.
   # Example:
   # Redirect permanent /foo http://www.example.com/bar
   #
   # Alias: Maps Web paths to filesystem paths and is used to
   # access content not present at DocumentRoot.
   # Example:
   # Alias /webpath /full/filesystem/path
   #
   # If you include a trailing / on /webpath, the server
   # requires it to be present in the URL. You will also likely
   # need to provide a <Directory> section to allow access to
   # the filesystem path.
```

```
    #
    # ScriptAlias: This controls which directories contain server
    scripts.
    # ScriptAliases are essentially the same as Aliases, except that
    # documents in the target directory are treated as applications
    and
    # run by the server when requested rather than as documents sent to
    the
    # client. The same rules about trailing "/" apply to ScriptAlias
    # directives as to Alias.
    #
    ScriptAlias /cgi-bin/ "/usr/local/apache2/cgi-bin/"
</IfModule>
<IfModule cgid_module>
    #
    # ScriptSock: On threaded servers, designate the path to the UNIX
    # socket used to communicate with the CGI daemon of mod_cgid.
    #
    #Scriptsock cgisock
</IfModule>
#
# "/usr/local/apache2/cgi-bin" should be changed to whatever your
ScriptAliased
# CGI directory exists, if it has been configured.
#
<Directory "/usr/local/apache2/cgi-bin">
    AllowOverride None
    Options None
    Require all granted
</Directory>
<IfModule headers_module>
    # Avoid passing HTTP_PROXY environment to CGIs on this or any
    proxied
    # backend servers that have lingering "httpoxy" defects.
    # 'Proxy' request header is undefined by the IETF, not listed by
    IANA
    #
    RequestHeader unset Proxy early
</IfModule>
<IfModule mime_module>
```

```
#
# TypesConfig points to the file containing the list of mappings
from
# file name extension to MIME type.
#
TypesConfig conf/mime.types
#
# AddType allows you to add to or override the MIME configuration
# file specified in TypesConfig for specific file types.
#
#AddType application/x-gzip .tgz
#
# AddEncoding allows certain browsers to uncompress
# information on the fly. Note: Not all browsers support this.
#
#AddEncoding x-compress .Z
#AddEncoding x-gzip .gz .tgz
#
# If the AddEncoding directives above are commented-out, then you
# probably should define those extensions to indicate media
types:
#
AddType application/x-compress .Z
AddType application/x-gzip .gz .tgz
#
# AddHandler allows you to map certain file extensions to
"handlers":
# actions unrelated to file type. They can be either built into the
server
# or added with the Action directive (see below)
#
# To use CGI scripts outside of ScriptAliased directories:
# (You will also need to add "ExecCGI" to the "Options"
directive.)
#
#AddHandler cgi-script .cgi
# For type maps (negotiated resources):
#AddHandler type-map var
```

```
    #
    # Filters allow you to process content before it is sent to the
    client.
    #
    # To parse .shtml files for server-side includes (SSI):
    # (You will also need to add "Includes" to the "Options"
    directive.)
    #
    #AddType text/html .shtml
    #AddOutputFilter INCLUDES .shtml
</IfModule>
#
# The mod_mime_magic module allows the server to use various hints
from the
# contents of the file itself to determine its type. The
MIMEMagicFile
# directive tells the module where the hint definitions are located.
#
#MIMEMagicFile conf/magic
#
# Customizable error responses come in three flavors:
# 1) plain text 2) local redirects 3) external redirects
#
# Some examples:
#ErrorDocument 500 "The server made a boo boo."
#ErrorDocument 404 /missing.html
#ErrorDocument 404 "/cgi-bin/missing_handler.pl"
#ErrorDocument 402 http://www.example.com/subscription_info.html
#
#
# MaxRanges: Maximum number of Ranges in a request before
# returning the entire resource, or one of the special
# values 'default', 'none' or 'unlimited'.
# Default setting is to accept 200 Ranges.
#MaxRanges unlimited
```

```
#
# EnableMMAP and EnableSendfile: On systems that support it,
# memory-mapping or the sendfile syscall can be used to deliver
# files. This usually improves server performance, but must
# be turned off when serving from networked-mounted
# filesystems or if support for these functions is otherwise
# broken on your system.
# Defaults: EnableMMAP On, EnableSendfile Off
#
#EnableMMAP off
#EnableSendfile on
# Supplemental configuration
#
# The configuration files in the conf/extra/ directory can be
# included to add extra features or to modify the default
configuration of
# the server, or you may simply copy their contents here and change
as
# necessary.
# Server-pool management (MPM-specific)
#Include conf/extra/httpd-mpm.conf
# Multi-language error messages
#Include conf/extra/httpd-multilang-errordoc.conf
# Fancy directory listings
#Include conf/extra/httpd-autoindex.conf
# Language settings
#Include conf/extra/httpd-languages.conf
# User home directories
#Include conf/extra/httpd-userdir.conf
# Real-time info on requests and configuration
#Include conf/extra/httpd-info.conf
# Virtual hosts
Include conf/extra/httpd-vhosts.conf
# Local access to the Apache HTTP Server Manual
#Include conf/extra/httpd-manual.conf
# Distributed authoring and versioning (WebDAV)
#Include conf/extra/httpd-dav.conf
# Various default settings
#Include conf/extra/httpd-default.conf
```

```
# Configure mod_proxy_html to understand HTML4/XHTML1
<IfModule proxy_html_module>
Include conf/extra/proxy-html.conf
</IfModule>
# Secure (SSL/TLS) connections
Include conf/extra/httpd-ssl.conf
#
# Note: The following must be present to support
# starting without SSL on platforms with no/dev/random equivalent
# but a statically compiled-in mod_ssl.
#
 <IfModule ssl_module>
SSLRandomSeed startup builtin
SSLRandomSeed connect builtin
</IfModule>
#ProxyRemote * http://123.124.125.126:4321
```

extra\httpd-ssl.conf

```
#
# This is the Apache server configuration file providing SSL
support.
# It contains the configuration directives to instruct the server how
to
# access pages over an https connection. For detailed information
about these
# directives, see <URL:http://httpd.apache.org/docs/2.4/mod/
mod_ssl.html>
#
# Do NOT simply read the instructions here without understanding
# what they do. They are shown only as hints or reminders. If you are
unsure,
# consult the online docs. You have been warned.
#
# Required modules: mod_log_config, mod_setenvif, mod_ssl,
# socache_shmcb_module (for default value of SSLSessionCache)
#
# Pseudo Random Number Generator (PRNG):
# Configure one or more sources to seed the PRNG of the SSL library.
# The seed data should be of good random quality.
# WARNING! On some platforms /dev/random blocks if insufficient
entropy
# is available. This means you then cannot use the /dev/random
device
# because it would lead to very long connection times (as long as
# it requires to make more entropy available). But usually those
# platforms additionally provide a /dev/urandom device that does not
# block. So, if available, use this one instead. Read the mod_ssl
User
# Manual for more details.
#
#SSLRandomSeed startup file:/dev/random 512
#SSLRandomSeed startup file:/dev/urandom 512
#SSLRandomSeed connect file:/dev/random 512
#SSLRandomSeed connect file:/dev/urandom 512
#
# When we also provide SSL, we must listen to the
# standard HTTP port (see above) and to the HTTPS port
#
#Listen 443
```

```
##
## SSL Global Context
##
## All SSL configurations in this context apply to
## the main server and all SSL-enabled virtual hosts.
##
# SSL Cipher Suite:
# List the ciphers that the client is permitted to negotiate,
# and that httpd will negotiate as the client of a proxied server.
# See the OpenSSL documentation for a complete list of ciphers, and
# ensure they follow appropriate best practices for this deployment.
# httpd 2.2.30, 2.4.13 and later force-disable aNULL, eNULL and EXP
ciphers,
# while OpenSSL disabled these by default in 0.9.8zf/1.0.0r/1.0.1m/
1.0.2a.
#SSLCipherSuite HIGH:MEDIUM:!MD5:!RC4:!3DES
#SSLProxyCipherSuite HIGH:MEDIUM:!MD5:!RC4:!3DES
```

Note: Run the following lines as a command:

```
SSLCipherSuite ECDHE-RSA-AES128-CBC-SHA256:ECDHE-RSA-AES128-GCM-
SHA256:ECDHE-RSA-AES256-GCM-SHA384:AES128-SHA256
```

Note: Run the following lines as a command:

```
SSLProxyCipherSuite ECDHE-RSA-AES128-CBC-SHA256:ECDHE-RSA-AES128-
GCM-SHA256:ECDHE-RSA-AES256-GCM-SHA384:AES128-SHAhttps://
defthw99wvesrv.ad001.siemens.net:4003/Themes/CustomControls/
Viewlets/CloseBtn.gif256
# By the end of 2016, only TLSv1.2 ciphers should remain in use.
# Older ciphers should be disallowed as soon as possible, while the
# kRSA ciphers do not offer forward secrecy. These changes inhibit
# older clients (such as IE6 SP2 or IE8 on Windows XP, or other
legacy
# non-browser tooling) from successfully connecting.
#
# To restrict mod_ssl to use only TLSv1.2 ciphers, and disable
# those protocols that do not support forward secrecy, replace
# the SSLCipherSuite and SSLProxyCipherSuite directives above with
# the following two directives, as soon as practicable.
# SSLCipherSuite HIGH:MEDIUM:!SSLv3:!kRSA
# SSLProxyCipherSuite HIGH:MEDIUM:!SSLv3:!kRSA
```

```
# User agents such as Web browsers are not configured for the user's
# own preference of either security or performance, therefore this
# must be the prerogative of the Web server administrator who
manages
# CPU load versus confidentiality, so enforce the server's cipher
order.
SSLHonorCipherOrder on
# SSL Protocol support:
# List the protocol versions that clients are allowed to connect with.
# Disable SSLv3 by default (cf. RFC 7525 3.1.1). TLSv1 (1.0) should
be
# disabled as quickly as practicable. By the end of 2016, only the
TLSv1.2
# protocol or later should remain in use.  #SSLProtocol all -SSLv3
#SSLProxyProtocol all -SSLv3
SSLProtocol -all +TLSv1.2
SSLProxyProtocol -all +TLSv1.2
```

```
# Pass Phrase Dialog:
# Configure the pass phrase gathering process.
# The filtering dialog program ('builtin' is an internal
# terminal dialog) must provide the pass phrase on stdout.
SSLPassPhraseDialog builtin
# Inter-Process Session Cache:
# Configure the SSL Session Cache: First the mechanism
# to use and second the expiring timeout (in seconds).
#SSLSessionCache "dbm:/usr/local/apache2/logs/ssl_scache"
SSLSessionCache "shmcb:/usr/local/apache2/logs/ssl_scache(512000)"
SSLSessionCacheTimeout 300
# OCSP Stapling (requires OpenSSL as of 0.9.8h)
#
# This feature is disabled by default and requires at least
# the two directives SSLUseStapling and SSLStaplingCache.
# Refer to the documentation on OCSP Stapling in the SSL/TLS
# How-To for more information.
#
# Enable stapling for all SSL-enabled servers:
#SSLUseStapling On
# Define a relatively small cache for OCSP Stapling using
# the same mechanism that is used for the SSL session cache
# above. If stapling is used with more than a few certificates,
# the size may need to be increased. (AH01929 will be logged.)
#SSLStaplingCache "shmcb:/usr/local/apache2/logs/
ssl_stapling(32768)"
# Seconds before valid OCSP responses are expired from the cache
#SSLStaplingStandardCacheTimeout 3600
# Seconds before invalid OCSP responses are expired from the cache
#SSLStaplingErrorCacheTimeout 600
##
## SSL Virtual Host Context
##
<VirtualHost _default_:443>
```

```
# General setup for the virtual host  DocumentRoot "/usr/local/
apache2/htdocs"
#ServerName www.example.com:443
#ServerAdmin you@example.com  ServerName IoT2040:443
ErrorLog "/usr/local/apache2/logs/error_log"
TransferLog "/usr/local/apache2/logs/access_log"
# SSL Engine Switch:
# Enable/Disable SSL for this virtual host.
SSLEngine on
# Server Certificate:
# Point SSLCertificateFile at a PEM-encoded certificate. If
# the certificate is encrypted, then you will be prompted for a
# pass phrase. Note that a kill -HUP will prompt again. Keep
# in mind that if you have both an RSA and a DSA certificate, you
# can configure both in parallel (to also allow the use of DSA
# ciphers, etc.)
# Some ECC cipher suites (http://www.ietf.org/rfc/rfc4492.txt)
# require an ECC certificate that can also be configured in
# parallel.
SSLCertificateFile "/usr/local/apache2/ssl_cert/certificate.pem"
SSLCertificateFile "/usr/local/apache2/ssl_cert/certificate.pem"
#SSLCertificateFile "/usr/local/apache2/conf/server-ecc.crt"
# Server Private Key:
# If the key is not combined with the certificate, use this
# directive to point at the key file. Keep in mind that if
# you have both a RSA and a DSA private key, you can configure
# both in parallel (to also allow the use of DSA ciphers, etc.)
# ECC keys, when in use, can also be configured in parallel
SSLCertificateKeyFile "/usr/local/apache2/ssl_cert/key.pem"
#SSLCertificateKeyFile "/usr/local/apache2/conf/server-dsa.key"
#SSLCertificateKeyFile "/usr/local/apache2/conf/server-ecc.key"
# Server Certificate Chain:
# Point SSLCertificateChainFile at a file containing the
# concatenation of PEM-encoded CA certificates that form the
# certificate chain for the server certificate. Alternatively
# the referenced file can be the same as SSLCertificateFile
# when the CA certificates are directly appended to the server
# certificate for convenience.
#SSLCertificateChainFile "/usr/local/apache2/conf/server-ca.crt"
```

```
# Certificate Authority (CA):
# Set the CA certificate verification path where to find CA
# certificates for client authentication or alternatively one
# huge file containing all of them (file must be PEM-encoded)
# Note: Inside SSLCACertificatePath you need hash symlinks
# to point to the certificate files. Use the provided
# Make file to update the hash symlinks after changes.
#SSLCACertificatePath "/usr/local/apache2/conf/ssl.crt"
#SSLCACertificateFile "/usr/local/apache2/conf/ssl.crt/ca-
bundle.crt"
# Certificate Revocation Lists (CRL):
# Set the CA revocation path where to find CA CRLs for client
# authentication or alternatively one huge file containing all
# of them (file must be PEM-encoded).
# The CRL checking mode needs to be configured explicitly
# through SSLCARevocationCheck (defaults to "none" otherwise).
# Note: Inside SSLCACertificatePath you need hash symlinks
# to point to the certificate files. Use the provided
# Make file to update the hash symlinks after changes.
#SSLCARevocationPath "/usr/local/apache2/conf/ssl.crl"
#SSLCARevocationFile "/usr/local/apache2/conf/ssl.crl/ca-bundle.crl"
#SSLCARevocationCheck chain
# Client Authentication (Type):
# Client certificate verification type and depth. Types are
# none, optional, require and optional_no_ca. Depth is a
# number that specifies how deeply to verify the certificate
# issuer chain before deciding the certificate is not valid.
#SSLVerifyClient require
#SSLVerifyDepth 10
# TLS-SRP mutual authentication:
# Enable TLS-SRP and set the path to the OpenSSL SRP verifier
# file (containing login information for SRP user accounts).
# Requires OpenSSL 1.0.1 or newer. See the mod_ssl FAQ for
# detailed instructions for creating this file. Example:
# "openssl srp -srpvfile /usr/local/apache2/conf/passwd.srpv -add
username"
#SSLSRPVerifierFile "/usr/local/apache2/conf/passwd.srpv
```

```
# Access Control:
# With SSLRequire you can do per-directory access control based
# on arbitrary complex Boolean expressions containing server
# variable checks and other lookup directives. The syntax is a
# mixture between C and Perl. See the mod_ssl documentation
# for more details.
#<Location />

#SSLRequire (%{SSL_CIPHER} !~ m/^(EXP|NULL)/ \
#            and %{SSL_CLIENT_S_DN_O} eq "Snake Oil, Ltd." \
#            and %{SSL_CLIENT_S_DN_OU} in {"Staff", "CA", "Dev"} \
#            and %{TIME_WDAY} >= 1
#            and %{TIME_WDAY} <= 5 \
#            and %{TIME_HOUR} >= 8
#            and %{TIME_HOUR} <= 20 ) \
#            or %{REMOTE_ADDR} =~ m/^192\.76\.162\.[0-9]+$/
#</Location>


# SSL Engine Options:
# Set various options for the SSL engine.

#  o  FakeBasicAuth:
#     Translate the client X.509 into a Basic Authorization. This
#     means that
#     the standard Auth/DBMAuth methods can be used for access
#     control. The
#     user name is the 'one line' version of the client's X.509
#     certificate.
      Note that no password is obtained from the user. Every entry in
      the user
      file needs this password: 'xxj31ZMTZzkVA'.
#  o  ExportCertData:
#     This exports two additional environment variables:
#     SSL_CLIENT_CERT and
#     SSL_SERVER_CERT. These contain the PEM-encoded certificates of
#     the
#     server (always existent) and the client (only existent when
#     client
      authentication is used). This can be used to import the
      certificates
      into CGI scripts.
```

```
#  o  StdEnvVars:
#     This exports the standard SSL/TLS related 'SSL_*' environment
#     variables.
#     By default, this export is switched off for performance
#     reasons,
      because the extraction step is an expensive operation and is
      usually
      useless for serving static content. So one usually enables the
      export for CGI and SSI requests only.
#  o  StrictRequire:
#     This denies access when "SSLRequireSSL" or "SSLRequire"
#     applied even
#     for a "Satisfy any" situation, i.e. when it applies, access is
      denied
      and no other module can change it.
#  o  OptRenegotiate:
#     This enables optimized SSL connection renegotiation handling
#     when SSL
      directives are used in per-directory context.
#SSLOptions +FakeBasicAuth +ExportCertData +StrictRequire
<FilesMatch "\.(cgi|shtml|phtml|php)$">
   SSLOptions +StdEnvVars
</FilesMatch>
<Directory "/usr/local/apache2/cgi-bin">
   SSLOptions +StdEnvVars
</Directory>
# SSL Protocol Adjustments:
# The safe and default, but still SSL/TLS standard compliant
shutdown
# approach, is that mod_ssl sends the close notify alert but does not
wait for
# the close notify alert from client. When you need a different
shutdown
# approach, you can use one of the following variables:
#  o  ssl-unclean-shutdown:
#     This forces an unclean shutdown when the connection is closed,
#     i.e. no
#     SSL close notify alert is sent or allowed to be received. This
#     violates
#     the SSL/TLS standard, but is needed for some brain-dead
      browsers. Use
      this when you receive I/O errors because of the standard
      approach where
      mod_ssl sends the close notify alert.
```

```
#  o  ssl-accurate-shutdown:
#     This forces an accurate shutdown when the connection is closed,
#     i.e. a
#     SSL close notify alert is sent and mod_ssl waits for the close
#     notify
#     alert of the client. This is 100% SSL/TLS standard compliant,
#     but in
#     practice often causes hanging connections with brain-dead
      browsers. Use
      this only for browsers where you know that their SSL
      implementation
      works correctly.
# Notice: Most problems of broken clients are also related to the
HTTP
# keep-alive facility, so you usually additionally want to disable
# keep-alive for those clients, too. Use variable "nokeepalive" for
this.
# Similarly, one has to force some clients to use HTTP/1.0 to
workaround
# their broken HTTP/1.1 implementation. Use variables
"downgrade-1.0" and
# "force-response-1.0" for this.
BrowserMatch "MSIE [2-5]" \
      nokeepalive ssl-unclean-shutdown \
      downgrade-1.0 force-response-1.0
# Per-server logging:
# The home of a custom SSL log file. Use this when you want a
# compact non-error SSL log file on a virtual host basis.
CustomLog "/usr/local/apache2/logs/ssl_request_log" \
      "%t %h %{SSL_PROTOCOL}x %{SSL_CIPHER}x \"%r\" %b"
</VirtualHost>
```

extra\httpd-vhosts.conf

```
# Virtual Hosts
#
# Required modules: mod_log_config
# If you want to maintain multiple domains/hostnames on your
# machine you can setup VirtualHost containers for them. Most
configurations
# use only name-based virtual hosts so the server doesn't need to
worry about
# IP addresses. This is indicated by the asterisks in the directives
below.
#
# Please see the documentation at
# <URL:http://httpd.apache.org/docs/2.4/vhosts/>
# for further details before you try to setup virtual hosts.
#
# You may use the command line option '-S' to verify your virtual
host
# configuration.
#
# VirtualHost example:
# Almost any Apache directive may go into a VirtualHost container.
# The first VirtualHost section is used for all requests that do not
# match a ServerName or ServerAlias in any <VirtualHost> block.
#
#<VirtualHost *:80>
#  ServerAdmin webmaster@dummy-host.example.com
#  DocumentRoot "/usr/local/apache2/docs/dummy-host.example.com"
#  ServerName dummy-host.example.com
#  ServerAlias www.dummy-host.example.com
#  ErrorLog "logs/dummy-host.example.com-error_log"
#  CustomLog "logs/dummy-host.example.com-access_log" common
#</VirtualHost>
#
#<VirtualHost *:80>
#  ServerAdmin webmaster@dummy-host2.example.com
#  DocumentRoot "/usr/local/apache2/docs/dummy-host2.example.com"
#  ServerName dummy-host2.example.com
#  ErrorLog "logs/dummy-host2.example.com-error_log"
#  CustomLog "logs/dummy-host2.example.com-access_log" common
#</VirtualHost>
```

```
<VirtualHost *:8082>
      ServerName gateway.eu1.mindsphere.io/
      SSLProxyEngine On RequestHeader set Front-End-Https "On"
      ProxyPass / http://gateway.eu1.mindsphere.io/
      ProxyPassReverse / http://gateway.eu1.mindsphere.io/
</VirtualHost>
```

4.5.5 Configuring SINUMERIK controls

4.5.5.1 Overview

Introduction

This chapter describes configuring the following SINUMERIK control for use of an Apache proxy on the IoT2040.

- SINUMERIK control with HMI-Advanced - Setting the proxy (Page 76)
- SINUMERIK control with SINUMERIK Operate - Setting the proxy (Page 85)

The following port is configured for MindSphere V3 Livesystem:

- Port 8082

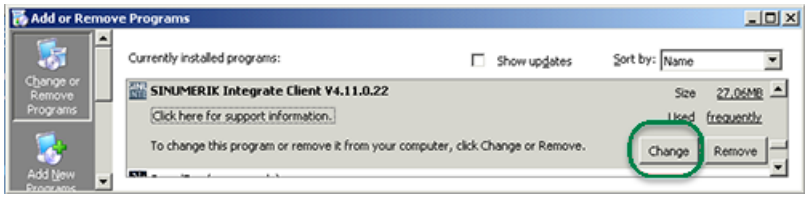
Configure the URL for connection to MindSphere with **http** - not with **https.**

- http://gateway.eu1.mindsphere.io/api/agentcom-mmmops/v3/ws11

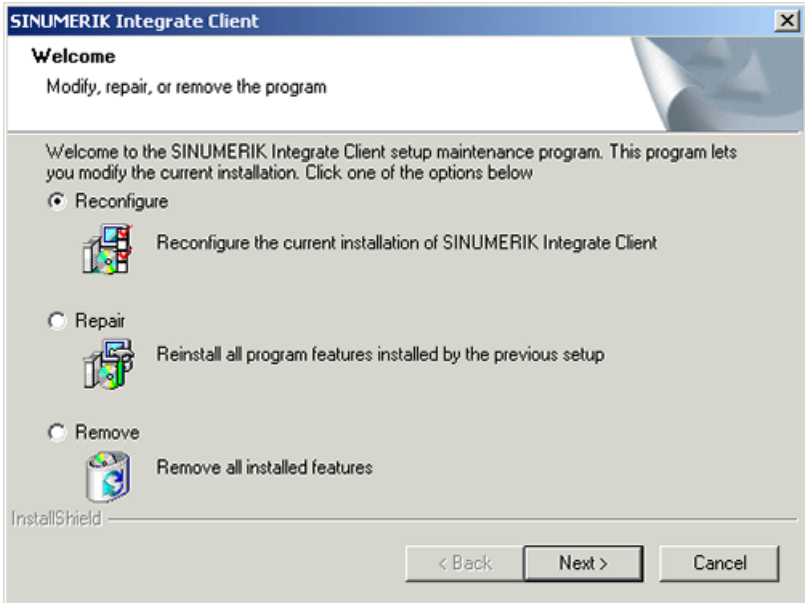
4.5.5.2 SINUMERIK control with HMI-Advanced - Setting the proxy

Procedure

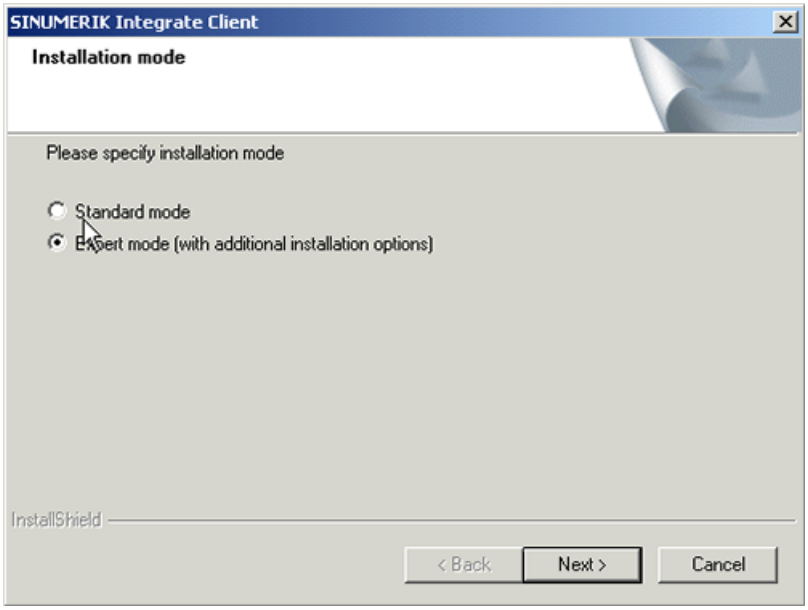
1. Start the PCU in service mode.
2. Open "Add or Remove Programs" in Windows and select "SINUMERIK Integrate Client". Click "Change".



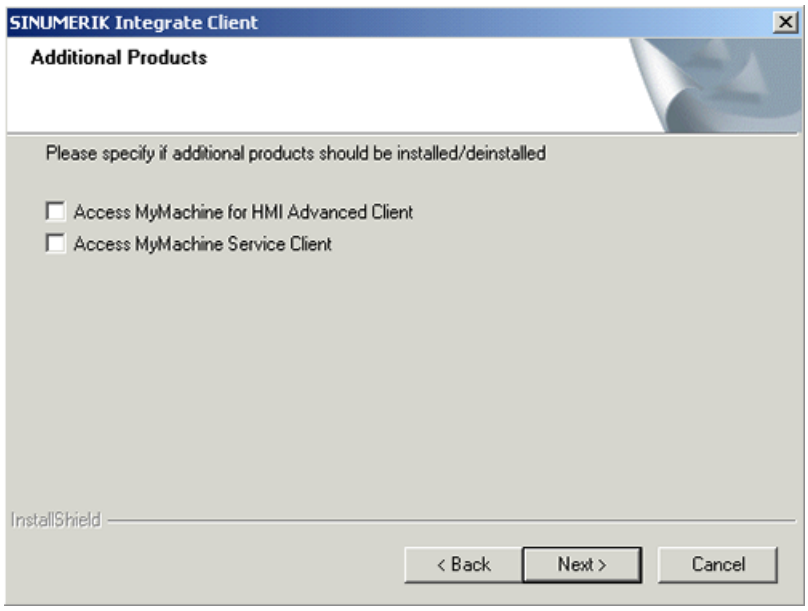
3. The "Welcome" window opens.
   - To edit the configuration, select the "Reconfigure" option button.
   - To perform the setup of the "SINUMERIK Integrate Client", click "Next >".



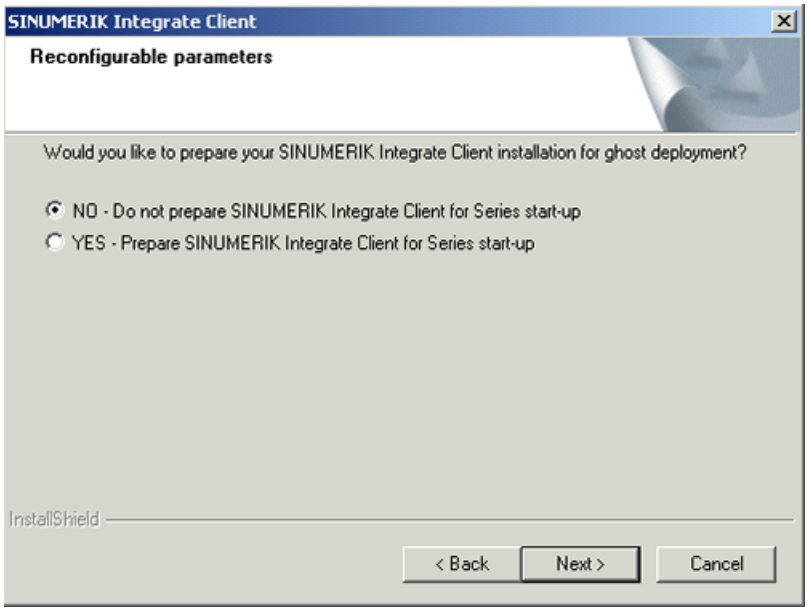
4. The "Installation mode" window opens.
   - Select the option button "Expert mode (with additional installation options)."
   - Click "Next >".



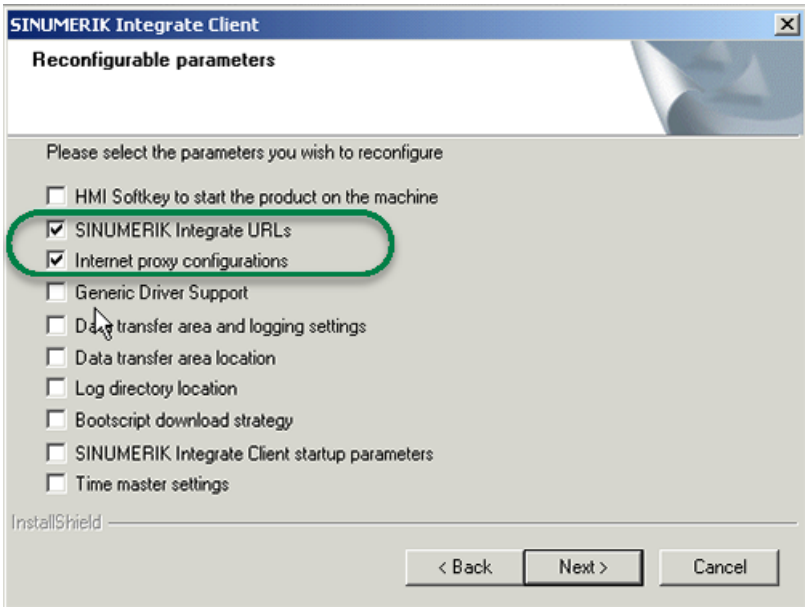
5. The "Additional Products" window opens.
   – Click "Next >".



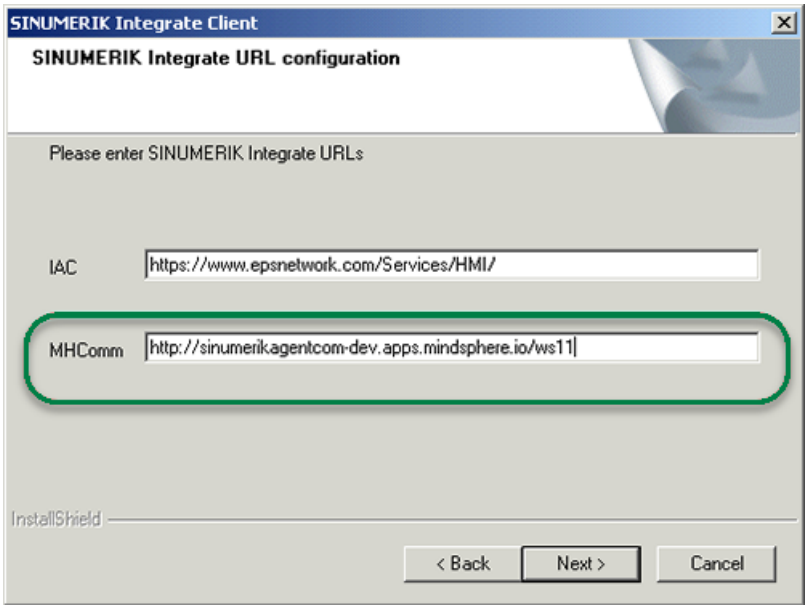
6. The "Reconfigurable parameters" window opens.
   – Select the "NO - Do not prepare SINUMERIK Integrate client for series start-up" option button.
   – Click "Next >".



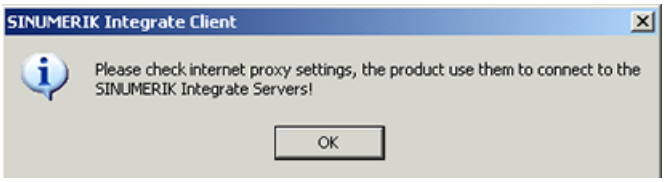
7. Select the following check boxes:
   - "SINUMERIK Integrate URLs"
   - "Internet proxy configurations"
   - Click "Next >".



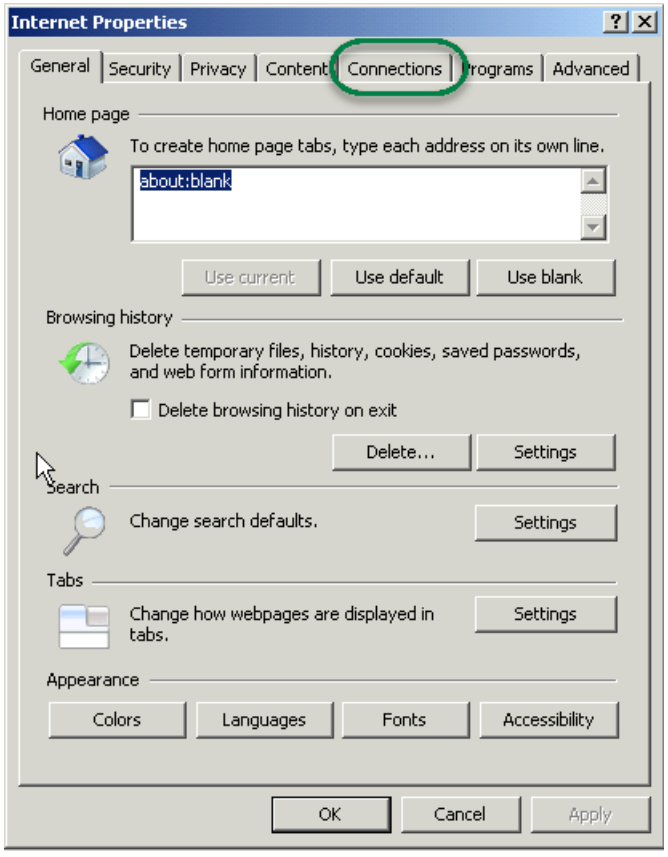
8. The "SINUMERIK Integrate URL configuration" window opens.
   - Configure the URL for connection to MindSphere with **http**, rather than with **https**. Enter the following web service URL for MindSphere V3 Livesystem in the "MHComm" text box:
     http://gateway.eu1.mindsphere.io/api/agentcom-mmmops/v3/ws11
   - Click "Next >".



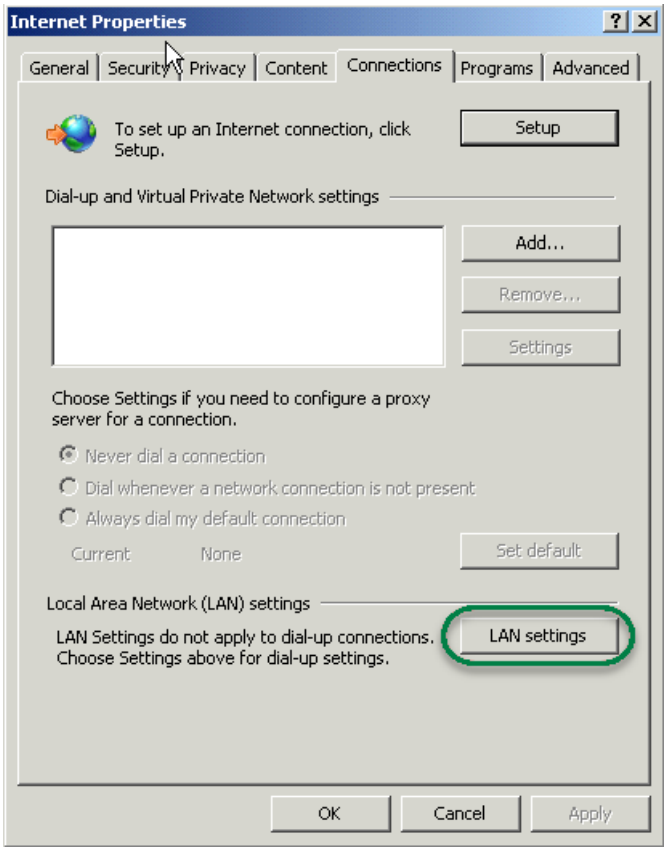
9. The following prompt is displayed: "Please check internet proxy setting, the product use them to connect to the SINUMERIK Integrate Servers!".
   – Click "OK".



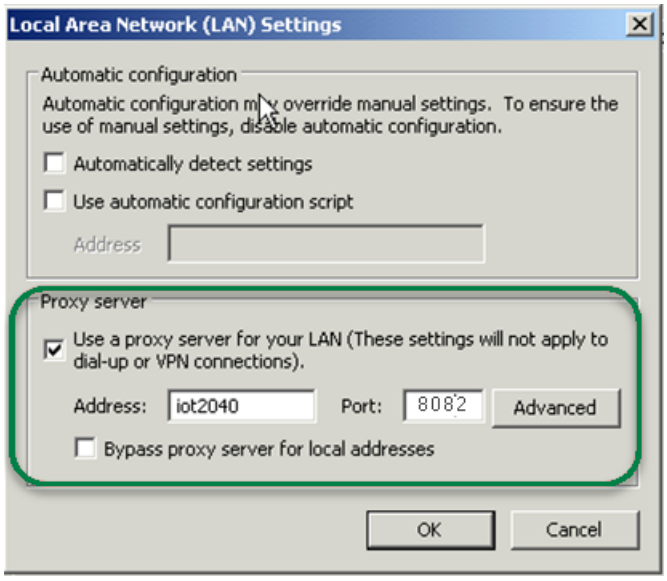
10. The "Internet Properties" > "General" window opens.
   – Open the "Connections" tab.



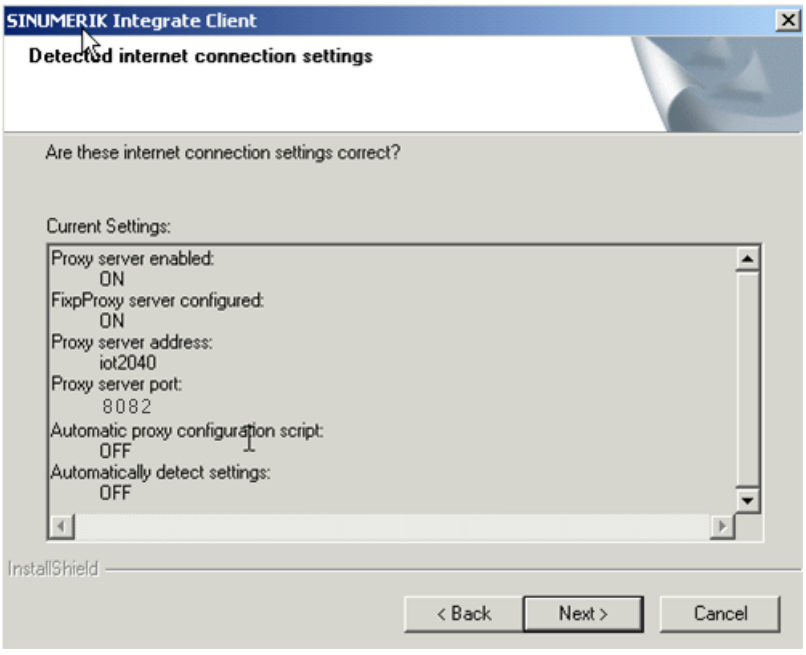
11. The "Connections" window opens.
   – In the "Local Area Network (LAN) settings" group box, click the "LAN settings" button.



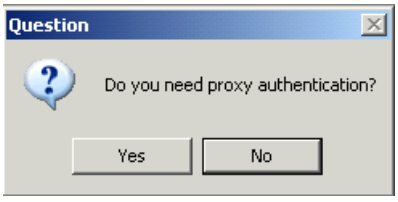
12. The "Local Area Network (LAN) settings" window opens.
    Enter the proxy settings:
    - Clear the "Automatically detect settings" check box.
    - Clear the "Use automatic configuration script" check box.
    - In the "Proxy server" group box, select the "Use a proxy server for your LAN …." check box.
    - Address: iot2040
    - Port (as configured in Apache), e.g.: MindSphere V3 Livesystem: 8082
    - Clear the "Bypass proxy server for local addresses" check box.
    - Click "OK".



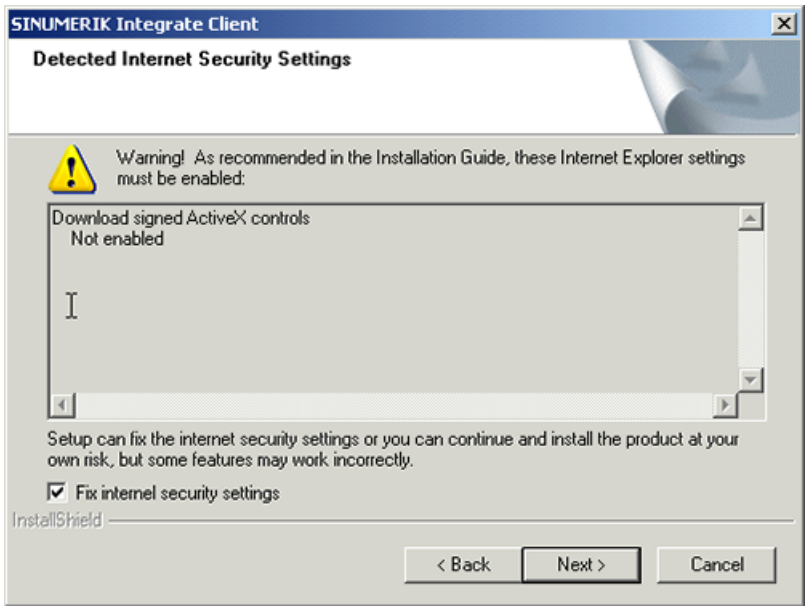
13. The "Detected internet connection settings" window opens.
    The defined proxy settings are shown for checking.
    – Click "Next >".



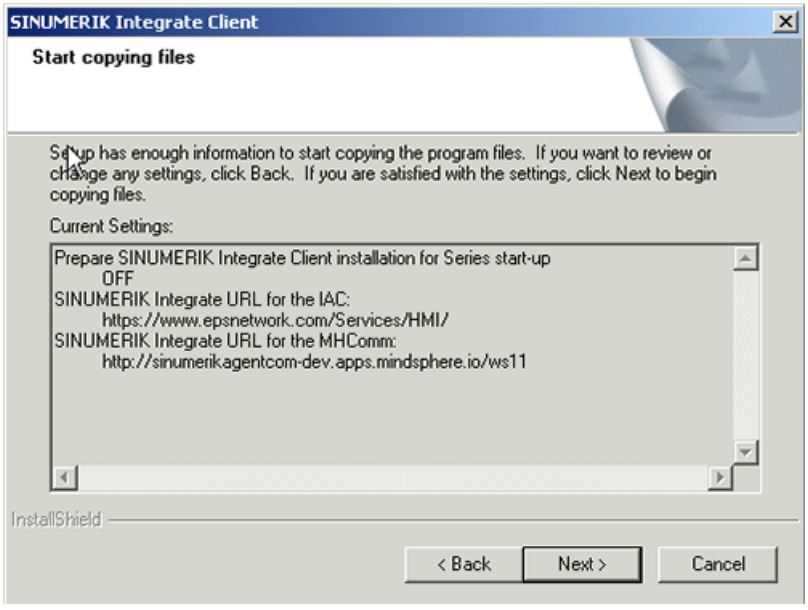
14. The following question is displayed: "Do you need proxy autentication?"
    – Click the "No" button.



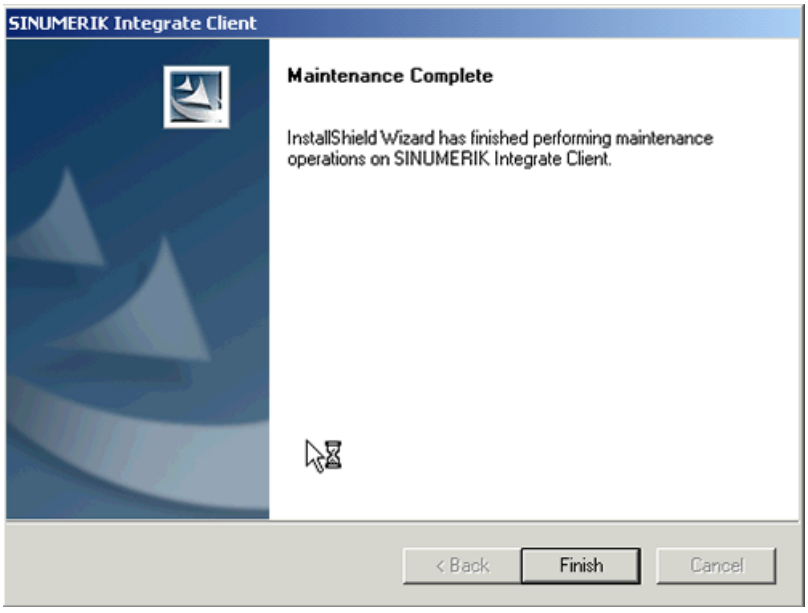
15. Select the "Fix internal security settings" check box.
    – Click "Next >".



16. The "Start copying files" window opens.
    The specified proxy settings are displayed for validation.
    – Click "Next >".



17. The "Maintenance Complete" window opens.
    – Click "Finish>" to complete the installation.

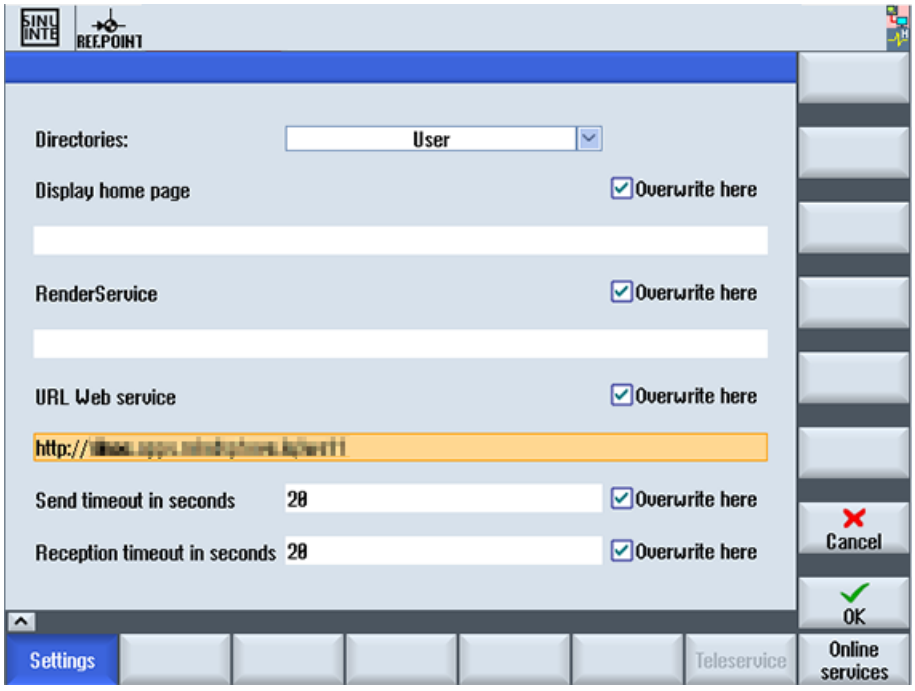


4.5.5.3 SINUMERIK control with SINUMERIK Operate - Setting the proxy

This chapter describes configuring the SINUMERIK Integrate Client for SINUMERIK Operate.

Procedure

1. The "Settings" window is open.
   Press the "URLs>" softkey.
2. Press the "Settings" softkey and select the following settings:
   - Directory: Select the "User" entry in the "Directories" drop-down list.
   - Display home page: Select the "Overwrite here" check box.
   - RenderService: Select the "Overwrite here" check box.
   - URL web service: Select the "Overwrite here" check box.
   - Configure the URL for connection to MindSphere with **http**, rather than with **https**.
     Enter the following "URL Web service":
     http://gateway.eu1.mindsphere.io/api/agentcom-mmmops/v3/ws11
   - Enter the required value in the "Send timeout in seconds" text box (default value is 200).
     For MindSphere, a value of "20" is recommended, and select the "Overwrite here" check box.
   - Enter the required value in the "Receptions timeout in seconds" text box (default value is 200).
     For MindSphere, a value of "20" is recommended, and select the "Overwrite here" check box.

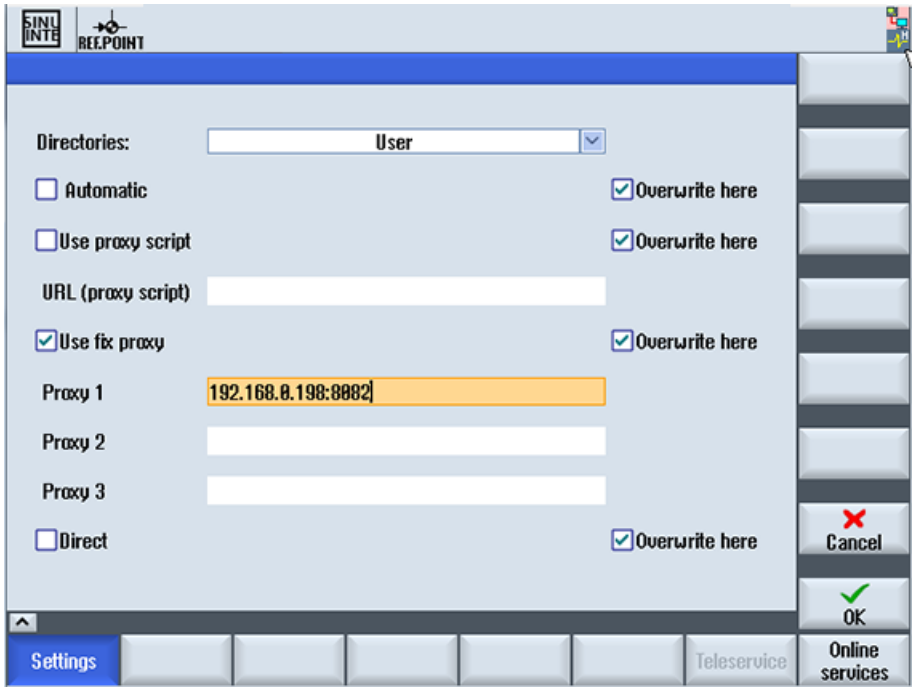


3. Configure the fixed proxy in SINUMERIK in the following format:
   <ip-address>:<port>
   <ip-address>: IP address of the IoT2040
   <port>: Port used by Apache: Port 8082 is configured for the MindSphere V3 Livesystem
   - Press "OK".

Example

The IP address of IoT2040 is 192.168.0.198.
This results in the following configuration:

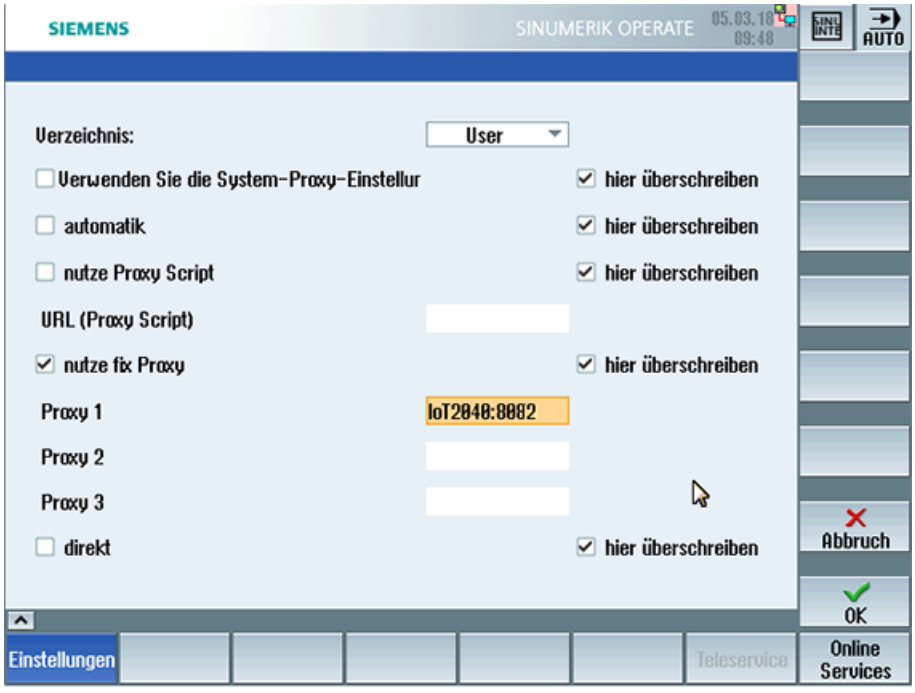
- MindSphere V3 Livesystem: 192.168.0.198:8082



Error correction in the proxy connection

The certificate is generated with the general name IoT2040. Rather than the IP address, it may be necessary to use FQDN: IoT2040 to access the proxy.
If the IoT2040 is accessed with the DNS, no further action is required.

1. If no DNS is used, extend the host files with the IP and the name of the IoT2040.
   In the PCU 50, the file is stored in the following directory:
   C:\Windows\System32\drivers\etc\hosts
2. In the following example, add the following file to the "Host":
   `192.168.0.198 IoT2040`
3. Enter the desired setting in the text box "Proxy 1", for example: "IoT2040:8082".


SIEMENS
SINUMERIK OPERATE
05.03.18
09:48
AUTO
Verzeichnis:
User
Verwenden Sie die System-Proxy-Einstellur
hier überschreiben
automatik
hier überschreiben
nutze Proxy Script
hier überschreiben
URL (Proxy Script)
nutze fix Proxy
hier überschreiben
Proxy 1
IoT2040:8082
Proxy 2
Proxy 3
direkt
hier überschreiben
Abbruch
OK
Einstellungen
Teleservice
Online Services

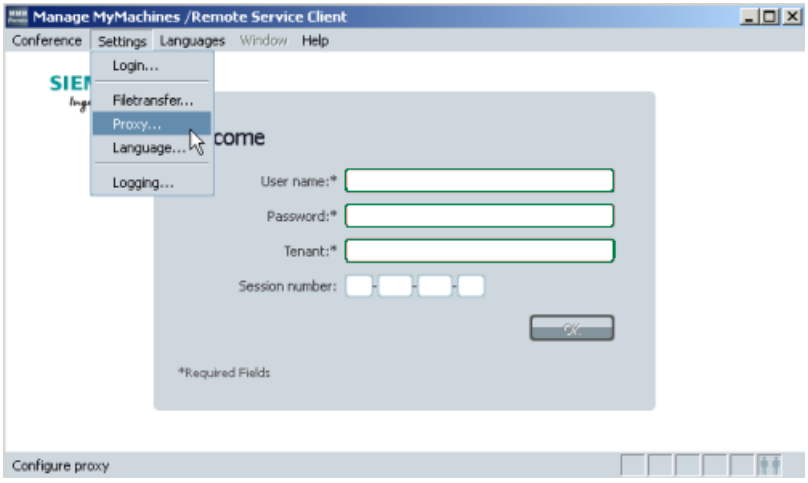
4.5.5.4 Configuring MMM /R SC MO

Procedure

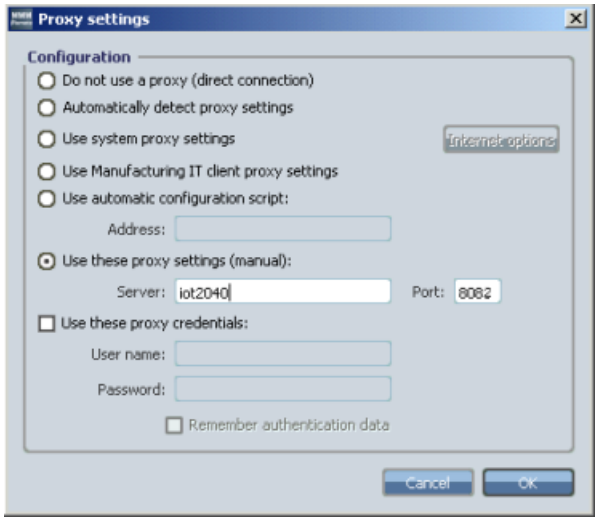
1. Click on icon "MMM /R

2. In the menu bar, call "Settings" > "Proxy...".
   The "Welcome" window opens.
   Enter your login data:
   - User name
   - Password
   - Tenant

   Click "OK".



3. The "Proxy settings" window opens.
   - Select the "Use this proxy settings (manual):" option button.
   - Enter the following server in the "Server:" text box: "iot2040".
   - In the text box "Port:", enter, for example, the following port: "8082".
   - Click "OK" to save the settings.
     - OR -
     Click "Cancel" to reject the settings.



4.5.6 Backup the root access to the IoT2040 Box - optional

Although this step is optional, we recommend that this configuration is performed for security reasons.

4.5.6.1 Setting a password for the root user.

No password is set for the root user.

For security reasons, it is recommended that you set the root password soon.

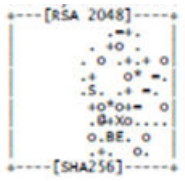
Procedure

1. Open a remote session with PuTTY and enter the following command:
   `passwd`
2. You are requested to enter a new password:
   Enter the new password as specified:
   ```
   Changing password for root
   Enter the new password (minimum of 5 characters)
   Please use a combination of upper and lower case letters and
   numbers.
   New password:
   ```
3. Repeat the password:
   `Re-enter new password:`
4. The following is then displayed:
   ```
   passwd: password changed.
   root@iot2000:~#
   ```
   The password is set.

4.5.6.2 Generating SSH key pairs

Procedure

1. Create the directory in which the keys are stored:
   `mkdir -p ~/.ssh`
2. Create the key pairs:
   `ssh-keygen -t rsa`
   - Generate the key pair "public/private rsa".
   - Enter the storage location of the key, e.g. /home/root/.ssh/id_rsa.
   - Enter the password.
     If you do not want to use a password, leave the input empty.
   - Repeat the password.
     Your identification is stored in the following directory: /home/root/.ssh/id_rsa.
     Your public key is stored in the following directory: /home/root/.ssh/id_rsa.pub.
     The fingerprint of the key is shown as follows:
     SHA256:vN0y+nIMQ0Nb5UOBkZ8upyVa4wwf/8Z1lDg7TJcMvrg root@iot2000
     The Randomart Image of the key is:



3. Copy the public key with the command "`ssh-copy-id`" to the authorization files of the new SINUMERIK control.
4. Ensure that the example name and the IP address have been replaced:
   `cat ~/.ssh/id_rsa.pub | ssh root@192.168.0.198 "mkdir -p ~/.ssh && cat >> ~/.ssh/authorized_keys`
   - The following is then displayed:
     ```
     The authenticity of host '192.168.0.198 (192.168.0.198)' can't
     be established.
     ECDSA key fingerprint is
     SHA256:KwhYZhX1APiu1K0WXUkTmzF35S9VDhqv0YcFo5/KSWg.
     Are you sure you want to continue connecting (yes/no)? yes
     Warning: Permanently added '192.168.0.198' (ECDSA) to the list
     of known hosts.
     DISPLAY "(null)" invalid; disabling X11 forwarding
     ```

Further details can be found at the following link:

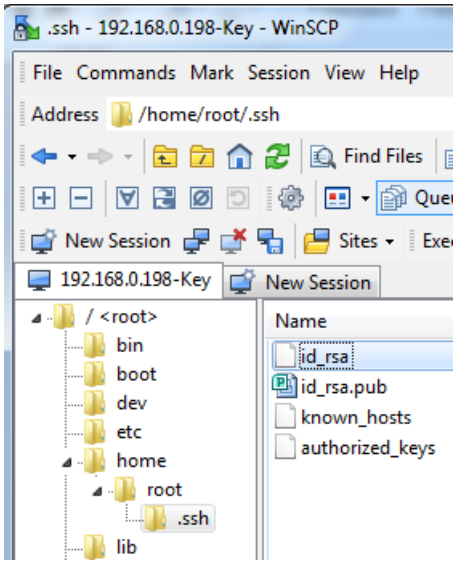
ssh key (https://www.yoctobe.com/servers/setting-up-ssh-keys/)

4.5.6.3 Generating the private key in PuTTY format

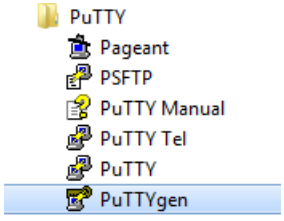
PuTTY SSH and the WinSCP client for Microsoft Windows do not use the same key format as the OpenSSH client. For this reason, a new SSH public and private key must be created with the PuTTYgen tool or an existing OpenSSH private key converted.

Procedure

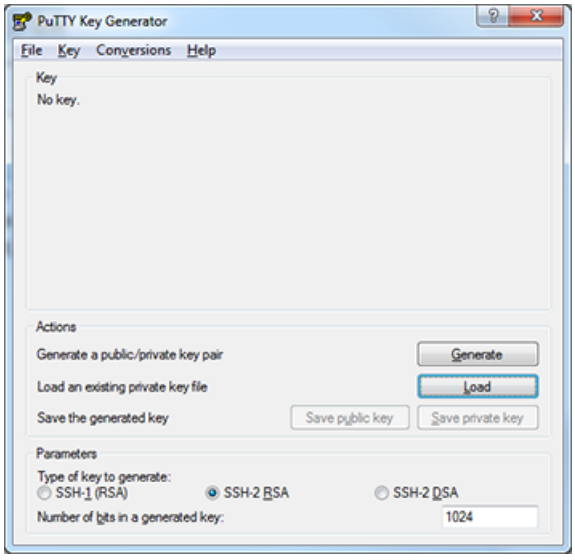
1. Download the generated private key from the IoT2040 into the local SINUMERIK control, into the following directory: /home/root/.ssh/id_rsa.



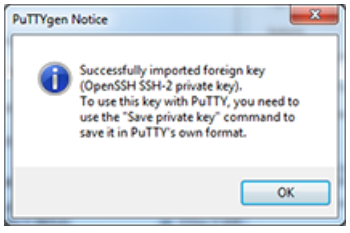
2. Start the PuTTY Key Generator by double-clicking "PuTTYgen".



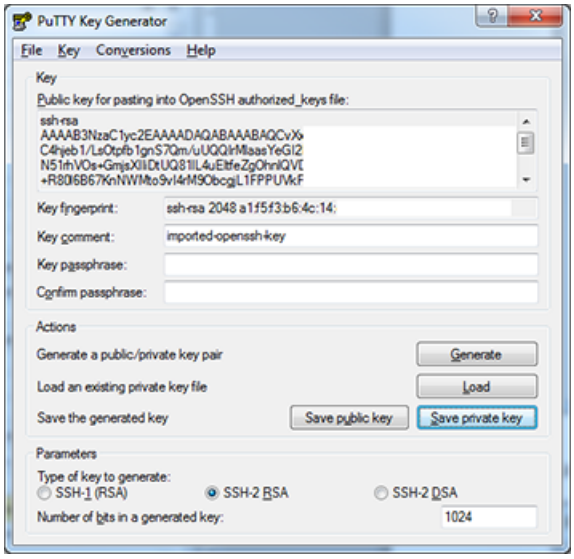
3. The "PuTTY Key Generator" window opens.
   There is still no key.
   – Click "Load" in the "Actions" area.
     Load the file with private key "id_rsa".



4. The "PuTTYgen Notice" window opens and a message indicates the success of the operation.
   Click "OK".



5. The "PuTTY Key Generator" window opens.
   The key is displayed.
   – In the "Actions" area, click "Save private key".



6. The new file, e.g. "id_rsa_PUTTY.ppk", is now created.

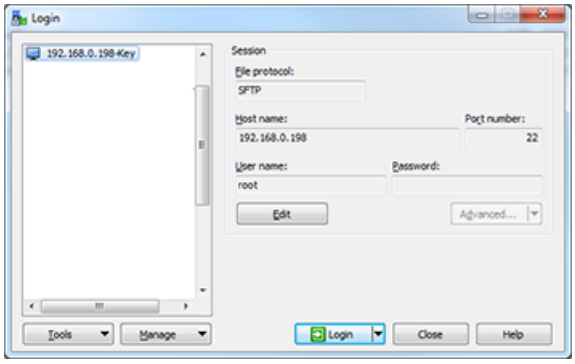
4.5.6.4 Connect to the IoT2040 using the private key

Requirement

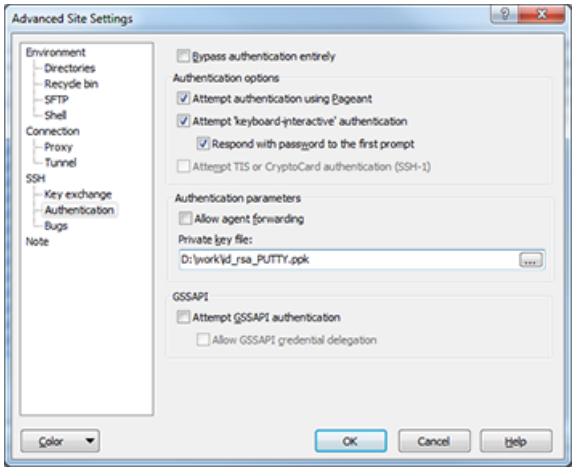
Create the connection to the IoT2040 either with WinSCP or with PuTTY once you have installed the private key, e.g. "id_rsa_PUTTY.ppk".
You will find further information in the following chapter: Generating the private key in PuTTY format (Page 91).

Procedure

1. Login to WinSCP.



2. Select Edit > Advanced > SSH > Authentication > Authentication parameters > Private key file.



3. Deactivate the login with user name and password.

Note

Ensure login

Perform this step only when you are sure that you can login with the created private key! Otherwise, you can no longer login to the IoT2040 and must reinstall the firmware.

- Create a backup before you perform the next steps.
- Open the file "/etc/ssh/sshd_config".
- Change the parameter: `PermitRootLogin without-password`.
- Change the parameter: `PermitEmptyPasswords no`.
- Remove any superfluous packages from the Yokto image (optional).
  For security reasons, we recommend that the superfluous packages and binaries made available in the default image of the IoT2040 are deleted.
- `opkg remove gdbserver --force-removal-of-dependent-packages`
- `opkg remove gdb-dev`

- `opkg remove gdb`

Appendix

A

A.1 List of abbreviations

Admin	Administrator (user role)
AMM /C	Analyze MyMachine /Condition
CNC	Computerized Numerical Control:
COM	Communication
DIR	Directory:
FAQ	Frequently Asked Questions
h	Hour
HTTP	Hypertext Transfer Protocol
HTTPS	HyperText Transfer Protocol Secure,
IB	Commissioning engineer (user role)
ID	Identification number
IE	Internet Explorer
IFC	Interface Client
IoT	Internet of Things
IPC	Industrial PC
MB	Megabyte
MLFB	Machine-Readable Product Code
MMM	Manage MyMachines
MMM /R	Manage MyMachines /Remote
MO	Machine operator
MSTT	Machine control panel
NC	Numerical Control: Numerical control
NCU	Numerical Control Unit: NC hardware unit
OEM	Original Equipment Manufacturer
OP	Operation Panel: Operating equipment
PC	Personal Computer
PCU	PC Unit: Computer unit
PLC	Programmable Logic Control: PLC
SE	Service engineer
SI	SINUMERIK Integrate
SK	Softkey
SW	Software
URL	Uniform Resource Locator, Uniform Resource Locator
UTC	Universal Time Coordinated

Index

R

S

U

X