

SIEMENS

Insights Hub

MindConnect Software Agent

System Manual

04/2024

Introduction

1

User Interface

2

User Roles and Scopes

3

Onboarding and Configuring
MindConnect Software Agent

4

Managing MindConnect Software
Agent

5

Configuring protocols

6

Appendix

7

Glossary

8

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.

Table of contents

1. Introduction	6
1.1. Overview of MindConnect Software Agent.....	6
2. User Interface	11
2.1. Insights Hub User interface of MindConnect Software Agent Plugin...	11
2.2. MindConnect Software Agent Web User Interface.....	14
3. User Roles and Scopes	16
3.1. User Roles and Scopes for MindConnect Software Agent.....	16
4. Onboarding and Configuring MindConnect Software Agent	17
4.1. Overview of Onboarding MindConnect Software Agent.....	17
4.2. Logging in to Insights Hub.....	18
4.3. Creating an asset for MindConnect Software Agent.....	19
4.4. Downloading the setup file for MindConnect Software Agent.....	20
4.5. Installing MindConnect Software Agent in Windows.....	22
4.6. Procedure to uninstall the MindConnect Software Agent.....	25
4.7. Installing MindConnect Software Agent in Docker.....	25
4.8. Onboarding the MindConnect Software Agent.....	29
4.9. Configuring data in Asset Manager for MindConnect Software Age...	32
4.10. Creating an aspect and variables for MindConnect Software Agent...	33
4.11. Creating a type in Asset Manager for MindConnect Software Agen...	33
4.12. Adding a data source for MindConnect Software Agent.....	33
4.13. Adding data points for MindConnect Software Agent.....	37
4.14. Mapping an aspect to a data source for MindConnect Software Ag...	40
4.15. Configuring Network settings.....	43
4.16. Configuring Dagnostic settings.....	45
4.17. Browsing datapoint of a data source for MindConnect Software A...	49
4.18. Importing data source configurations with datapoint mapping for...	52

4.19. Configuring MindConnect Software Agent using API.....	57
5. Managing MindConnect Software Agent.....	60
5.1. Diagnosing MindConnect Software Agent.....	60
5.2. Device Maintenance.....	63
5.3. Settings in MindConnect Software Agent.....	66
5.4. Firmware update in Asset Manager for MindConnect Software Age...	72
5.5. Automatic firmware update of MindConnect Software Agent.....	74
5.6. Remote restart for MindConnect Software Agent.....	75
5.7. Send commands for MindConnect Software Agent.....	75
5.8. Using MindConnect Software Agent's Hyper-V VM.....	79
5.9. Managing or maintaining the virtual machines or instances.....	80
5.10. Configuring MindConnect Software Agent in Docker.....	84
5.11. Troubleshooting.....	95
6. Configuring protocols.....	99
6.1. Overview of supported protocols for MindConnect Software Agent.....	99
6.2. Overview of S7 protocol for MindConnect Software Agent.....	100
6.3. Overview of OPC UA protocol for MindConnect Software Agent.....	106
6.4. Overview of Modbus TCP protocol for MindConnect Software Agent...	116
6.5. Overview of SYSTEM protocol for MindConnect Software Agent.....	122
6.6. Overview of Rockwell protocol for MindConnect Software Agent.....	136
6.7. Overview of S7+ protocol for MindConnect Software Agent.....	138
6.8. Overview of Fanuc Focas protocol for MindConnect Software Agent...	141
6.9. Overview of Sinumerik protocol for MindConnect Software Agent.....	144
6.10. Overview of IEC61850 protocol for MindConnect Software Agent.....	146
6.11. Overview of MTConnect protocol for MindConnect Software Agent...	148
6.12. Overview of BACnet protocol for MindConnect Software Agent.....	149
7. Appendix.....	157

7.1. Data center locations.....	157
7.2. Using quality code.....	157
7.3. Quality codes OPC UA and S7 protocol.....	158
7.4. Quality codes Modbus protocol.....	160
7.5. Quality codes SYSTEM protocol.....	161
7.6. Quality codes Rockwell protocol.....	162
7.7. Quality codes S7+, Fanuc Focas, Sinumerik, IEC61850 and MTConne...	163
7.8. Offline buffer.....	163
7.9. Firewall Settings.....	164
7.10. List of abbreviations.....	165
7.11. MindConnect EthernetIP - CIP Communication path (route param...	166
7.12. Case 1 – Accessing data inside an Allen- Bradley PLC.....	167
7.13. Case 2 – Accessing the Allen- Bradley PLC via integrated Ethernet ...	168
7.14. Case 3 – Accessing the Allen- Bradley PLC via the ControlNet interf...	168
7.15. MindConnect General Security Principles.....	169
7.16. Differentiating MCSA between Windows and Linux.....	171
7.17. DHCP Network settings.....	173
7.18. Samba Installation.....	173
7.19. MindConnect Software Agent in HyperV Host system.....	176
7.20. Known restrictions of MindConnect Software Agent.....	177
7.21. Default values for datasource Import and Export.....	179
8. Glossary.....	181
8.1. Glossary.....	181

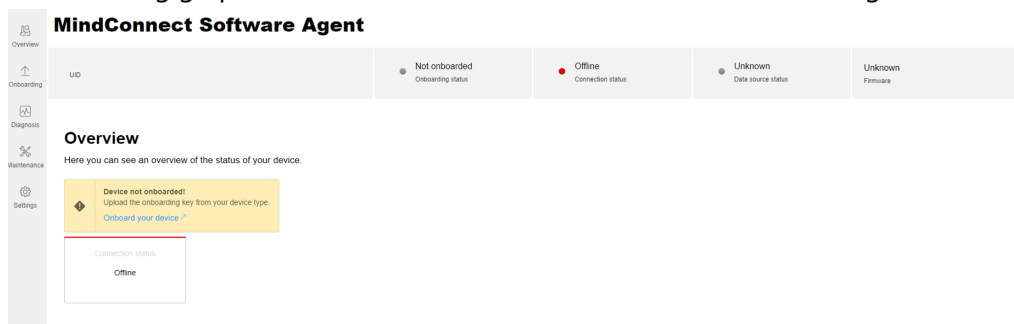
Introduction

1.1 Overview of MindConnect Software Agent

MindConnect Software Agent is a pure software solution to connect industrial data sources with Insights Hub. It allows connecting with Insights Hub, collect local data and send it encrypted to Insights Hub.

MindConnect Software Agent is a virtual representation of the MindConnect firmware which can be installed on Windows 10 system which supports Hyper-V and also can be installed on Linux systems which supports Docker.

The following graphic shows the overview of MindConnect Software Agent:



The online and offline firmware updates from V3.5 to V3.6 for MindConnect Software Agent are not supported. To update the firmware, you need to uninstall MindConnect Software Agent V3.5 current version and install MindConnect Software Agent V3.6 latest version manually using MindConnect Software Agent InstallShield setup.

Prerequisites

The following prerequisites apply to install MindConnect Software Agent on a Windows PC or IPC and Docker in Linux (supports 64-bit only):

Parameter	MCSA Hyper-V	MCSA Linux	MCSA Aarch64
Supported Architecture		Intel 64 (amd64)	ARM 64 (amd64)

Parameter	MCSA Hyper-V	MCSA Linux	MCSA Aarch64
Supported OS Versions	Windows 10 with Hyper-V support (e.g. Windows 10 Professional or Enterprise)	MCSA-Docker supports only 64-bit Architecture with following Linux distributions. - Debian GNU/Linux 10.13 (buster) - Ubuntu 20.04.5 LTS - CentOS Linux release 7.9.2009 (Core) - Oracle Linux Server 7.9 (Maipo) - SUSE Linux Enterprise Server 15 SP4	MCSA-Docker supports only 64-bit Architecture with following Linux distributions. - Debian GNU/Linux 10.13 (buster) - Ubuntu 20.04.5 LTS - CentOS Linux release 7.9.2009 (Core) - Oracle Linux Server 7.9 (Maipo) - SUSE Linux Enterprise Server 15 SP4
Supported devices			SIEMENS SIMATIC IOT2050 Advanced-PG2 with installed Industrial OS 3.2.2 or 3.2.3.
Necessary applications		- dialog - docker - docker-compose - xz	- dialog - docker - docker-compose - xz
Time synchronization		Automatic time synchronization of the host should be switched off so that the MCSA Docker container can synchronize the system time with Insights Hub server time.	Automatic time synchronization of the host should be switched off so that the MCSA Docker container can synchronize the system time with Insights Hub server time.
RAM	4GB	4GB	4GB
CPU cores	2	2	2
Disk space	15GB	2GB	2GB

Features

The following features are supported with MindConnect Software Agent:







Windows	Linux
- Install Shield based setup	- Shell script based Linux installer
- MindConnect Nano core functionality, except USB stick support	- Dialog based configuration script for managing MCSA Docker containers - MindConnect Edge Analytics

Other features supported with MindConnect Software Agent for Local web UI (Windows & Linux) are:



















































- Onboarding support
- Shows current device status and information
- Diagnosis support includes download of diagnosis, log, and system files
- Manual firmware update
- Factory reset
- Log file upload control
- Change system time support
- Localization in English and German

General Features Overview

Protocols	Windows	Docker (INTEL64)	Docker (AARCH64)
Basics			
Onboarding via USB Stick	✘	✘	✘
Onboarding via WebServer	✔	✔	✔
Diagnostics via USB-Stick	✘	✘	✘
Diagnostics via Webserver	✔	✔	✔
Local Firmware Update (Webserver)	✔	✔	✔
Local Firmware Update (USB)	✘	✘	✘
Remote Firmware Update	✔	✔	✔
Remote Restart	✔	✔	✔
Additional Options			
Datapoint Browsing (see also data source details)	✔	✔	✔
File Transfer (File Storage or Integrated Data Lake)	✔	✔	✔

Protocols	Windows	Docker (INTEL64)	Docker (AARCH64)
Remote Service gateway (RS)			
Network routing			
Performance			
Read performance (datapoints/sec)	Depends on used hardware	Depends on used hardware	Depends on used hardware
Maximum number of connections (data sources)	Depends on used hardware	Depends on used hardware	Depends on used hardware
Maximum number of datapoints	1050	1050	1050

Protocols Feature Overview

Protocols	Minimum read cycle	Windows	Docker (INTEL64)	Docker (AARCH64)	Bi-Directional communication	Browsing
Basics						
S7	1 sec					
OPC UA	1 sec					
Modbus TCP IP	1 sec					
Modbus RTU	1 sec					
Rockwell	1 sec					
Simatic I/O Shield	1 sec					
System	1 sec					
Advanced Drivers						
S7+	50 ms					
Sinumerik	50 ms					
IEC61850	50 ms					

Protocols	Minimum read cycle	Windows	Docker (INTEL64)	Docker (AARCH64)	Bi-Directional communication	Browsing
MT Connect	50 ms	✓	✓	✓	✓	✓
Fanuc Focas	50 ms	✓	✓	✗	✗	●
BACNet	50 ms	✗	✗	✓	✓	✓



- ✓ = supported
- ✗ = not supported
- ● = in development

User Interface

2

2.1 Insights Hub User interface of MindConnect Software Agent Plugin

Manage the MindConnect Software Agent Plugin UI from the asset manger. The below image displays the user interface of MindConnect Software Agent Plugin.



① Navigation icons to navigate between the different tabs are mentioned below:

- Homescreen
- Assets
- Library
- Sharings
- Connectivity

② Select view for MindConnect Software Agent plugin interface

③ Displays the device onboarding status

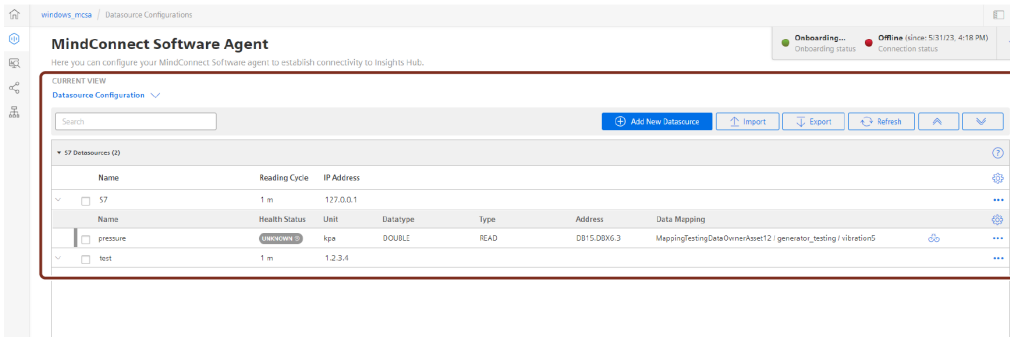
④ Displays the connection status to Insights Hub

The new UI is re-organized for all functionalities in 4 views i.e. "Datasource Configuration", "Agent Settings", "Advanced Mappings" and "Firmware Update". Based on the functionality, user can select the following view.

Datasource Configuration view

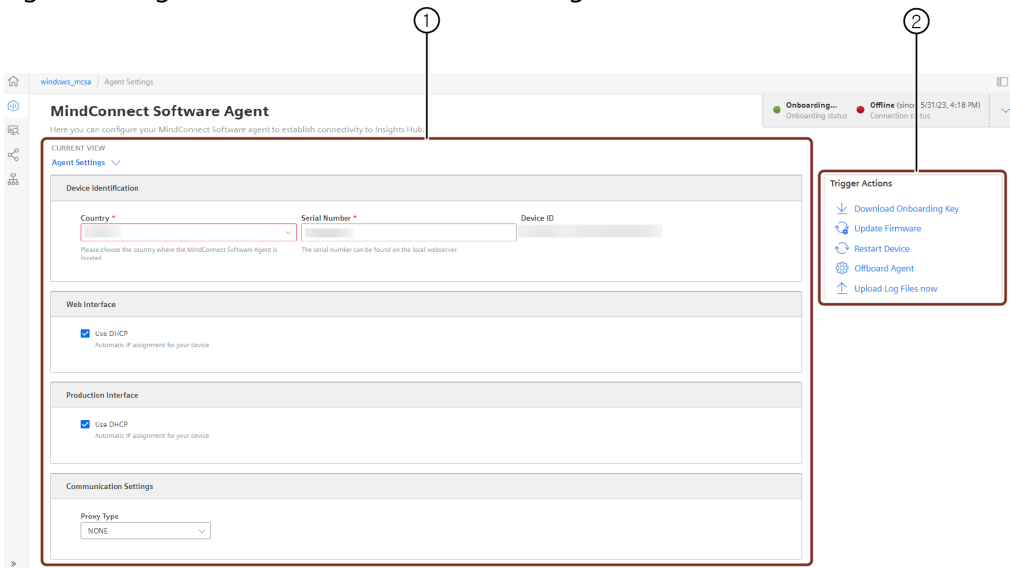
Datasource Configuration view enables the user to configure the datasources, datapoints and also to map the datapoints. The user can use the "Refresh" option to discard the changes made.

2.1 Insights Hub User interface of MindConnect Software Agent Plugin



Agent Settings view

In the "Agent Settings" view, user can find all the settings for MindConnect device including the related network and configuration information which enables the user to configure the agent. Agent settings view is shown in the below image.



- ① Agent Settings - Agents are configured or modified in this window.
- ② Trigger Actions - Following are the options available in Trigger actions window:
 - Download Onboarding Key: Downloads the Onboarding key to the local folder.
 - Update Firmware: Update to the latest firmware.
 - Restart Device: Restarts the device.
 - Offboard Agent: Offboards the Agent from the device.
 - Upload Log Files now: Uploads all the generated logs to Insights Hub.

Advanced Mappings

In Advanced Mappings view, user can map the datapoint of a datasource to a variable.

Datasources is now mapped directly, click the mapping field and select the asset to connect.

5. For more information, refer [Datamapping](#).

The import of datapoints (including Browsing) is now integrated in a wizard style workflow.

6. For more information, refer to [Importing datasource](#)

7. Grouping of datasources is available based on protocol.

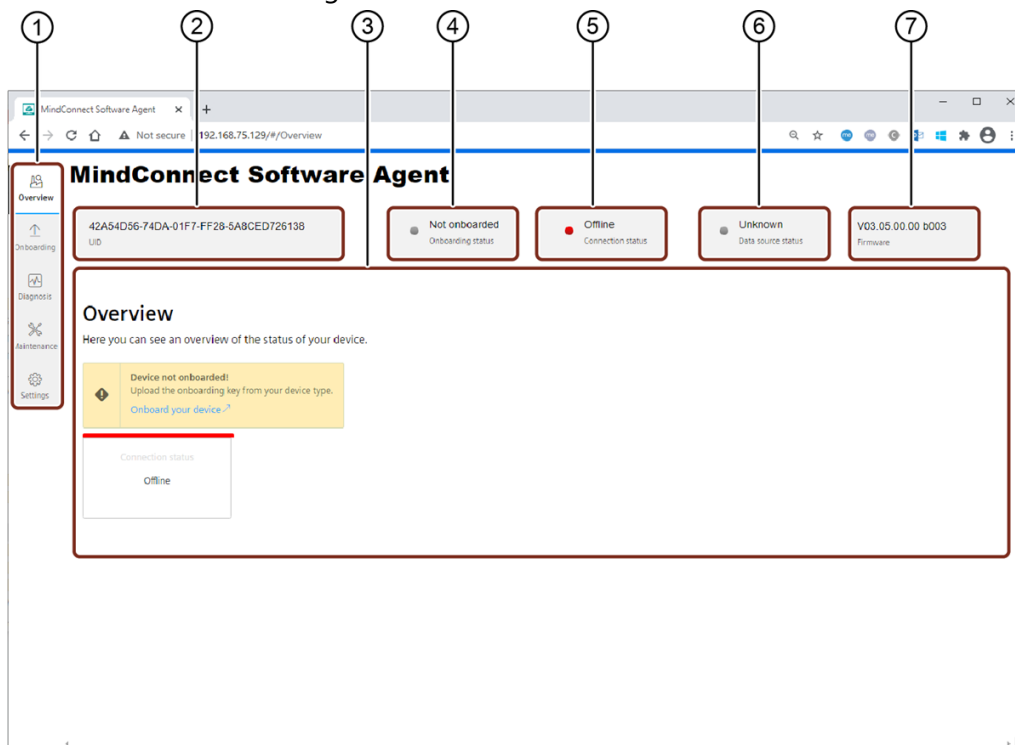
Delete all datasources functionality is discontinued. Multi-select and delete operation on

8. datasources is now supported.

9. Log column is discontinued in New UI.

2.2 MindConnect Software Agent Web User Interface

You manage the MindConnect Software Agent using the main navigation menu of the "MindConnect Software Agent" web UI.



- ① Navigation menu
- ② Serial number of the device
- ③ MindConnect Software Agent overview area
- ④ Onboarding status
- ⑤ Network status
- ⑥ Data source connection status after a data source configuration has been applied in the asset manager and downloaded to the device
- ⑦ Current firmware version



Onboarding, network, and data connection statuses shows the current status of the device like they are shown by the LED states of MindConnect Nano device (This information is not same as shown in Asset Manager).

Navigation menu

On the left side of the UI, there is a menu to navigate between the different tabs:

- Overview
- Onboarding
- Diagnosis
- Maintenance
- Settings

Overview area

The overview area provides following information:

- Onboarding status pane with direct link to onboarding area (only visible if device is not onboarded).
- Current network status pane.

Supported browser languages

MindConnect Software Agent's web UI supports following browser languages:

- English (default)

User Roles and Scopes

3

3.1 User Roles and Scopes for MindConnect Software Agent

There are multiple roles that are available for MindConnect device controlling. A device can be configured and can send the command to the device by an "Admin" user. If you want to ensure that a user cannot configure but can send a command, then you can use "DeviceCommander" role. If you want to ensure that a user can configure but cannot send a command, then you can use "DeviceConfigurator" role.

The following table shows the list of MindConnect device roles and scopes:

User role	Functionality or Scope
StandardUser (uipluginassetmanagemcnano:user)	This role grants the permission to visualize the MindConnect device plugin, but cannot change the device configuration and cannot send commands to the device.
DeviceConfigurator (plugins:deviceconfigurator)	This role grants the permission to visualize the MindConnect device plugins and update the device configuration, but cannot send commands to the device.
DeviceCommander (plugins:devicecommander)	This role grants the permission to visualize the MindConnect device plugins and can send the commands to the device, but cannot update the device configuration.
Admin (uipluginassetmanagemcnano:admin)	This role grants the permission to configure and command the MindConnect device.

By default, these roles are not enabled on the environment. To enable these roles you need to navigate to the "Settings" app.

In "Settings" app, click on "Roles" tab and click  to enable the new roles. For more information about roles, see ["Roles"](#) chapter in "Settings" documentation.



In case of role change, you need to log out and log in. It might take up to 15 minutes for the current configuration to be effective depending on the system.

Onboarding and Configuring MindConnect Software Agent

4

4.1 Overview of Onboarding MindConnect Software Agent

This chapter describes the initial configuration of an asset and MindConnect Software Agent in order to onboard MindConnect Software Agent to Insights Hub. Onboarding is the process of attaching a MindConnect Element to Insights Hub. And also, it describes the process of connecting industrial data sources to Insights Hub using MindConnect Software Agent. To establish the initial connection between MindConnect Software Agent and Insights Hub (onboarding), you have to configure the essential asset and MindConnect Software Agent data. For onboarding the full configuration is not required, although you can accomplish all steps using Asset Manager. The respective data to be configured for onboarding is described in the following procedure.

Prerequisites

- MindConnect Element is connected to the Internet and powered on.
- The connection cable for the Internet is correctly plugged into the Ethernet port for the Internet (Insights Hub).
- MindConnect Element is connected to asset or plant network.
- You have received the link to the Insights Hub UI with credentials (user and password data).
- A customer account is created.
- You have the role "mdsp:core:TenantAdmin". The user roles are set in Settings.
- MindConnect Software Agent is installed on Windows 10 system which supports Hyper-V and also can be installed on Linux systems which supports Docker.



Prepare MindConnect Element

To prepare your MindConnect Element for V3, you have to update the firmware for boxes that were already connected to V2 (SAP). For devices connecting to Insights Hub region China 1, the MindConnect Software Agent firmware should be V3.3.0.4 or higher.

Onboarding Procedure

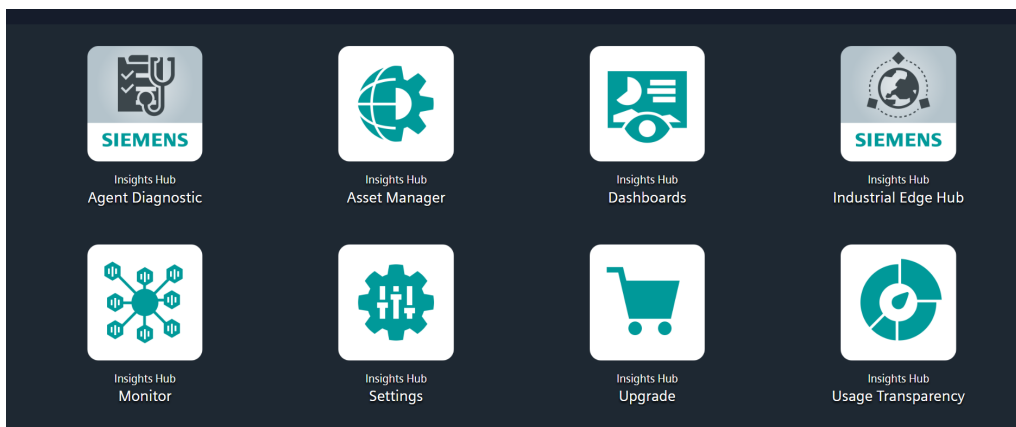
To onboard MindConnect Software Agent, follow these steps:

1. [Log in to Insights Hub](#)
2. [Creating an asset for MindConnect Software Agent](#)
3. [Downloading setup file of MindConnect Software Agent](#)
4. Installing MindConnect Software Agent
 - [Installing MindConnect Software Agent in Windows](#)
 - [Installing MindConnect Software Agent in Docker](#)
5. [Onboarding MindConnect Software Agent](#)
6. [Configuring data in Asset Manager](#)

4.2 Logging in to Insights Hub

To log in to Insights Hub, proceed as follows:

1. Click the link provided via mail by the Siemens AG.
 - The Insights Hub landing page for login will appear.
2. Log in to Insights Hub using the configured Authentication Provider (WebKey by default).
 - You will be redirected to your personal Insights Hub Launchpad.
 - Depending on your offering the Launchpad Icons will be displayed.



Insights Hub supports English, German and Chinese languages. Therefore, it is recommended to set the browser default to English, if you use a different language.

4.3 Creating an asset for MindConnect Software Agent

MindConnect Software Agent device is required to onboard using Asset Manager. For more information, see [Asset Manager](#) document.


To connect your MindConnect Software Agent in Asset Manager, you need to create an asset.

This process is the same for different types of MindConnect Elements that includes the Physical Asset type and the Virtual Asset type.

For information on creating a Virtual Asset type, refer "[Creating a type in Asset Manager for MindConnect Software Agent](#)".

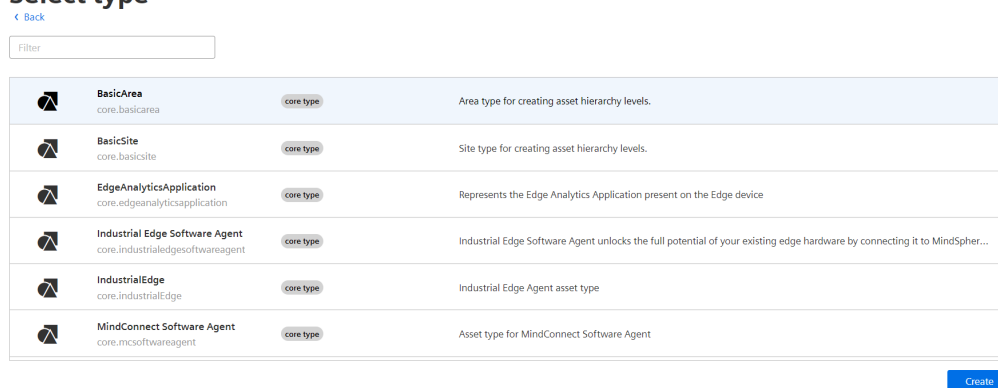
Procedure

To create an asset, follow these steps:

1. Select Asset Manager from the Launchpad.
2. Click "Assets" in the navigation area.
3. To create a new asset click .

The asset type overview window is opened.

Select type

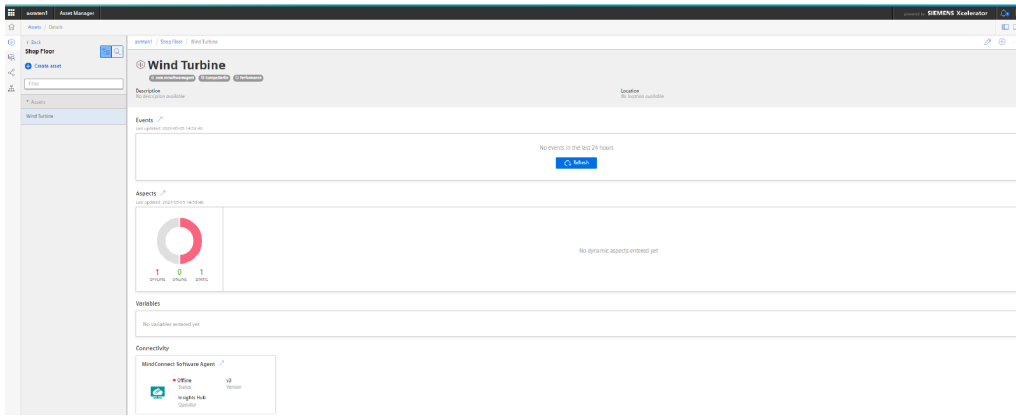


4. Select the respective asset type for your MindConnect Element, e. g. MindConnect Software Agent.
5. Enter a name and the data for the asset, e. g. "Wind turbine"
6. Confirm the entries with "Save".

Result

The new asset is available at the asset list.

The following graphic shows the created asset:



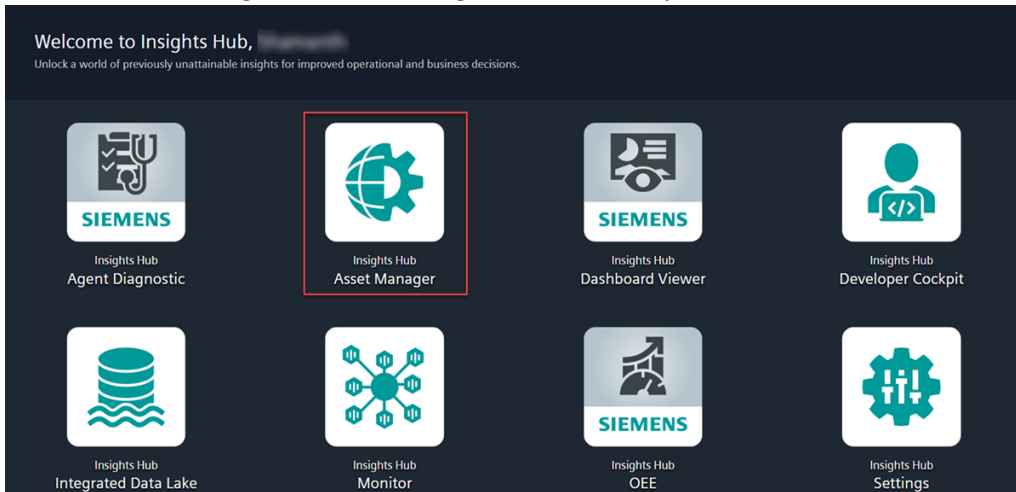
4.4 Downloading the setup file for MindConnect Software Agent

MindConnect Software Agent device is required to onboard using Asset Manager. For more information, see [Asset Manager](#) document.

Procedure to download setup file

To onboard the device, you need to create an asset in the Asset Manager. To create an asset for your in Asset Manager, see [Create Asset](#). Once the asset is created, open the UI plugin in Asset Manager to follow these steps:

1. Click "Asset Manger" from the Insights Hub Launchpad.



In Asset Manager, select the asset and click MindConnect Software Agent plugin as shown 2. in the image.

MCSA_AGENT
core.mcsoftwareagent EuropeBerlin Performance

Description
No description available

Location
No location available

Events ↗
Last updated: 2021-01-11 10:01:47
No events in the last 24 hours
Refresh

Aspects ↗
Last updated: 2021-01-11 10:01:47
No dynamic aspects entered yet

Variables
No variables entered yet

Connectivity

MindConnect Software Agent ↗	
● Offline Status	v3 Version
MindSphere Operator	

①

① Connect and onboard the MindConnect Software Agent

In MindConnect Software Agent plugin, choose the Country and enter the Serial number 3. (serial number can be found in the local web server) to identify the Asset.

Create Agent

MindConnect Software Agent

Here you can configure your MindConnect Software agent to establish connectivity to Insights Hub.

Device Identification ⓘ

Country *
Serial Number *

Please choose the country where the MindConnect Software Agent is located.
The serial number can be found on the local webserver.

After the Asset identification, "Download Setup and Installation" window is displayed as shown in the below image.

MindConnect Software Agent
Here you can configure your MindConnect Software agent to establish connectivity to Insights Hub.

Device Identification

Country * Serial Number *

Please choose the country where the MindConnect Software Agent is located. The serial number can be found on the local webserver.

Download Setup and Installation

First download the setup for the Mindconnect Software agent. Afterwards please install it on your Linux or windows 10 PC.

Firmware	Mindconnect Software Agent
Windows version	V03.06.00.20 b001
Linux version	V03.06.02.07 b001
Aarch64 version	V03.06.20.01 b001

I have read and accepted the [Terms and Conditions](#) for this firmware version.

[Download for Windows](#) [Download for Linux](#) [Download for Aarch64](#)

Accept the terms and Conditions for this firmware version and download the setup file based on the operating system.

- For Windows : Click "Download for Windows"
- For Linux : Click "Download for Linux"
- For Aarch64 : Click "Download for Aarch64"

To install MindConnect Software Agent for Windows and Docker, refer to the following sections.

- [Installing MCSA for Windows](#)
- [Installing MCSA for Docker](#)

4.5 Installing MindConnect Software Agent in Windows

MindConnect Software Agent can be installed on Windows system and IPCs running a Windows 10 version that supports Hyper-V feature.

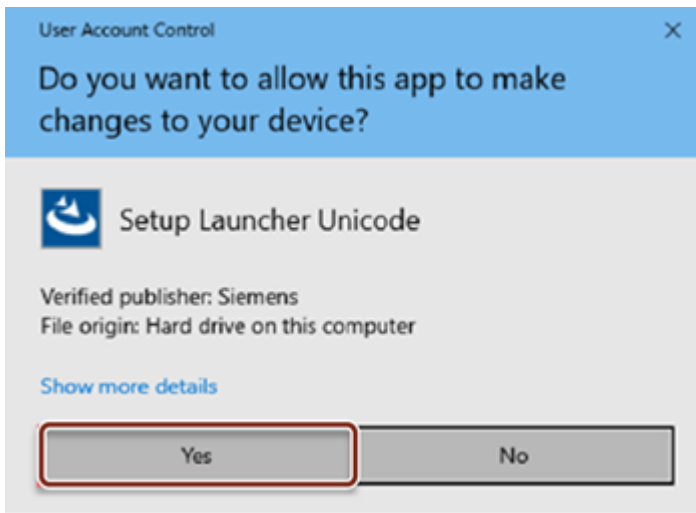


HyperV has to be activated on the local host PC.

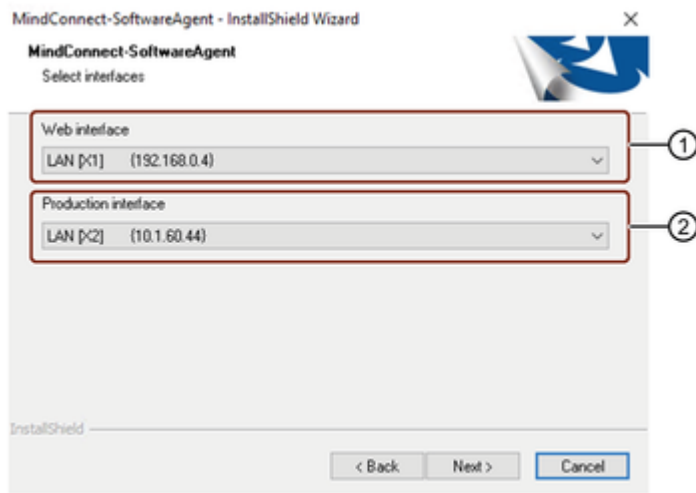
Procedure to install MindConnect Software Agent

To install MindConnect Software Agent, follow these steps:


1. Double click the downloaded setup file i.e. ".exe file".
2. Click "Yes" and click "Next".



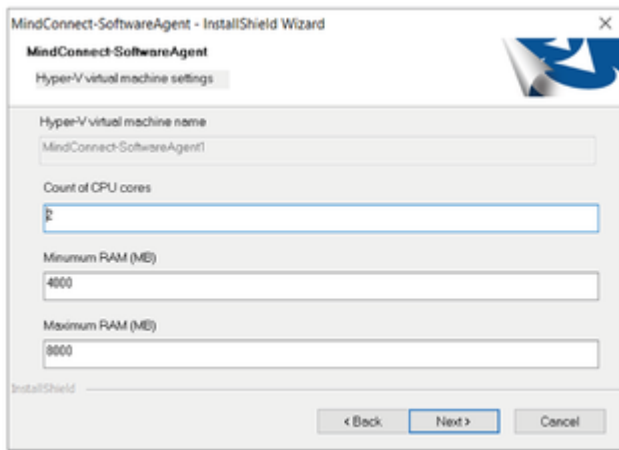
3. Select the network interfaces for MindConnect Software Agent.



- ① Connects to Insights Hub
- ② Connects to the field devices like PLCs

 Ensure to use the correct adapter for each connection.

4. Select "Custom" setup type to install(recommended) and click "Next".
5. Configure the virtual machine settings and click "Next".



Maximum RAM must be higher than the minimum RAM specification.
Recommended is 8GB as maximum RAM and 4GB as minimum RAM.

6. Change "Destination Folder" if required and click "Next".
7. Review the settings and click "Next".
8. Click "Install".

Procedure after installing the firmware

After installing MindConnect Software Agent firmware, follow these steps:

1. Restart your PC.
 2. Open Hyper-V Manager.
 3. Click on virtual machine (MindConnect Software Agent) and click "Connect".
- In VM console, information will be displayed (IP Address and Serial Number).

```
Network interface      IP address      Subnet mask
X1 P1 - Web interface: 192.168.75.129 255.255.255.0
X2 P1 - Production interface: 192.168.220.128 255.255.255.0

Serial number: 42A54D56-74DA-01F7-FF2B-5A8CED726138
```

In this sample, MindConnect Software Agent's web server URL is <http://192.168.75.129/>.

For more information using Hyper-V Manager, see [Using MindConnect Software Agent's Hyper-V VM](#).



- Currently, http protocol is supported.
- At least one of the connected networks must provide DHCP support, so that the system will receive an IP address that can be used to open the local web UI in a browser.
- If a connected network does not provide DHCP support, the values for IP address and subnet mask will be empty and the device has to be onboarded first.

4.6 Procedure to uninstall the MindConnect Software Agent

MindConnect Software Agent can be uninstalled either by executing MindConnect Software Agent's setup.exe file again, or via Windows Control Panel.



To uninstall MindConnect Software Agent using Windows Control Panel is available from the version MCSA V03.05.00.01 b004.

4.7 Installing MindConnect Software Agent in Docker

Starting from MCSA in Docker V03.06.02.07 b001 and V03.06.20.01 b001, extract the files from the Linux installer package to a given output folder only

```
./mcsa-installer.sh -x yes -o /opt/siemens/mindconnect/mcsa
```



Extract the file directly on a Linux system so that the file permissions will remain for the file mcsa-installer.sh extracted.



- mcsa-installer.sh needs to be executed with root permissions.
- mcsa-installer.sh also support -h option to show available options.

After extracting Linux installer package, open the Linux terminal window as root and navigate to the folder where the mcsa-installer.sh file had been extracted.



It is mandatory to execute the MCSA installation with root privileges - either directly as root or by getting root rights using su command, or by executing it with sudo command.

If the installer is not being started as root, a message will be shown that it has to be started as root and the script will terminate.

Prerequisites

Before installing MCSA Linux installer, check these components are installed on the target system. Following additional components are currently required to install, configure and run MCSA on Linux:

- dialog
- docker
- docker-compose
- xz

Furthermore, check if the Docker engine is already running.

If one of these components is not installed or the Docker engine is not running, the installer will display a message about missing components and provides the option to exit the installation:

- To install the required components manually, or
- To continue the installation and to install the missing components later

In the latter case, the MCSA components will be extracted to the installation folder, so that the MCSA installation can be started manually after installing the required components.



Installation of required components

- dialog belongs to ncurses and can be installed by using the Linux package manager (e.g. apt).
- docker should be installed by following the steps described on the [Docker installation](#).
- docker-compose installation is also described in the [Docker documentation](#).
- xz can be installed by installing xz-utils using the Linux package manager (e.g. apt).

Procedure to Install MCSA Linux installer

To install "MCSA Linux installer", follow these steps:

1. Open "Linux terminal" window as root.
2. Navigate to the folder where the "mcsa-installer.sh" file had been extracted.



It is mandatory to execute the MCSA installation with root privileges

- Either, directly as root, or
- By getting root rights using "su" command.
- "mcsa-installer.sh" can be started using "sudo" command to execute it with root rights. If the installer is not started as root, a message will be shown to start as root and the script will be terminated.

3. Enter the file path /opt/siemens/mindsphere/mcsa and click "Enter".

```
+ Install MindConnect Software Agent 03.06.01.00 0602 for Linux +
-----
Check prerequisites ...
System: Linux version 4.19.0-14-amd64 (debian-kernel@lists.debian.org) (gcc version 8.3.0 (Debian 8.3.0-6)) #1 SMP Debian 4.19.171-2 (2021-01-30)
version: 1.3-2B190211
docker version 20.10.8, build 396767d
docker - Active: active (running) since Fri 2022-03-25 05:37:32 CET; 2h 36min ago
docker compose version 1.29.2, build 5becea4c
xz (XZ Utils) 5.2.4
liblzma 5.2.4
All prerequisites are fulfilled to install MindConnect Software Agent
-----
Enter MCSA installation directory [e.g. /opt/siemens/mindsphere/mcsa/]
|
```



By default, MCSA installer offers the possibility to install MCSA components in following folder:

- /opt/siemens/mindconnect/mcsa This folder will be used, if "enter" is pressed without entering a file path. In case old installation is at the file path /opt/siemens/mindsphere/mcsa this can be ignored. For new installation, artifacts at the file path /opt/siemens/mindconnect/mcsa can be updated.
- After entering the file path click "enter", then the installer checks if the folder already exists. If the folder is already existing, it will offer the possibility to select another folder or to delete the folder, so that the new MCSA components can be installed there.
- It is also possible to exit the installer at this point to manually remove the already existing MCSA installation folder, and to start the installer later again.

```

+ Install MindConnect Software Agent 03.06.01.00_b002 for Linux +
-----
Check prerequisites ...
System: Linux version 4.19.0-14-amd64 (debian-kernel@lists.debian.org) (gcc version 8.3.0 (Debian 8.3.0-6)) #1 SMP Debian 4.19.171-2 (2021-01-30)
version: 1.3-20190211
Docker version 20.10.8, build 3967b7d
Docker - Active: active (running) since Fri 2022-03-25 05:37:32 CET; 2h 36min ago
docker-compose version 1.29.2, build 5becea4c
xz (XZ Utils) 5.2.4
liblzma 5.2.4
All prerequisites are fulfilled to install MindConnect Software Agent
-----
Enter MCSA installation directory [e.g. /opt/siemens/mindsphere/mcsa/]
MCSA installation directory /opt/siemens/mindsphere/mcsa/ already exists
Remove existing directory [Y/n]? - or exit [x/q]

```

4. Extract the "mcsa-installer.sh" file to the selected installation folder for MCSA components.



While installing, the Docker engine should not be running, or docker, docker-compose, or xz should not be installed on the target system, the MCSA installer will end after extracting MCSA components. After the required components are installed, the "mcsa-install.sh" can be called manually to load the MCSA Docker image afterwards.

5. Load the Docker image into the local Docker repository.

```

Enter MCSA installation directory [e.g. /opt/siemens/mindsphere/mcsa/]
MCSA installation directory /opt/siemens/mindsphere/mcsa/ already exists
Remove existing directory [Y/n]? - or exit [x/q]
y
Remove existing directory ...
Installation directory: /opt/siemens/mindsphere/mcsa/
-----
Create MCSA installation directory ...
-----
Extract MCSA components ...
-----
Install MCSA components ...
Docker version 20.10.8, build 3967b7d
docker-compose version 1.29.2, build 5becea4c
Docker - Active: active (running) since Fri 2022-03-25 05:37:32 CET; 2h 40min ago
xz (XZ Utils) 5.2.4
liblzma 5.2.4
MCSA Docker image mcsa:03.06.01.00_b002 has already been loaded.
Remove already loaded MCSA Docker image? [N/y]
y
Remove MCSA Docker image mcsa:03.06.01.00_b002 ...
Image mcsa:03.06.01.00_b002 removed
Load MCSA Docker image mcsa:03.06.01.00_b002 ...

```

- If docker and/or docker-compose had to be installed manually, "mcsa-install.sh" script should be executed manually with root privileges - either directly as root, or by getting root rights using "su" command. "mcsa-install.sh" can be started using "sudo" command to execute it with root rights.
- If the installer is not started as root, a message will be shown to start as root and the script will be terminated.
- It is also necessary to start "mcsa-install.sh" script directly in the MCSA installation folder to make sure that the internally used files will be available during script execution.
- If the MCSA Docker image is already loaded, the installer will offer the option to load it again or to skip this step.
- In case that the MCSA Docker image is required to load again, installer will check for the MCSA Docker containers exist and offer the possibility to automatically delete the existing containers or they will remain, but the Docker image will be untagged.

- After removing the previously loaded image, the MCSA Docker image will be loaded again.

```

docker-compose version 1.29.2, build 5bece4c
xz (XZ Utils) 5.2.4
liblzma 5.2.4
All prerequisites are fulfilled to install MindConnect Software Agent
Enter MCSA installation directory (e.g. /opt/siemens/mindsphere/mcsa/)
MCSA installation directory /opt/siemens/mindsphere/mcsa/ already exists
Remove existing directory [Y/n]? - or exit [X/q]
y
Remove existing directory ...
Installation directory: /opt/siemens/mindsphere/mcsa/
-----
Create MCSA installation directory ...
-----
Extract MCSA components ...
-----
Install MCSA components ...
Docker version 20.10.8, build 3067b7d
docker-compose version 1.29.2, build 5bece4c
Docker Active: active (running) since Fri 2022-03-25 05:37:32 CET; 2h 40min ago
xz (XZ Utils) 5.2.4
liblzma 5.2.4
MCSA Docker image mcsa:03.06.01.00 b062 has already been loaded.
Remove already loaded MCSA Docker image? [N/y]

```

6. Add a first MCSA Docker container.



- After loading the MCSA Docker image, the MCSA configuration (Page 109) will be started automatically to add a first MCSA Docker container.
- If application dialog is not available for the target system, the installer will end after loading the MCSA Docker image. After it has been installed, “mcsa-config.sh” can be called manually to load the MCSA Docker image later.

Result

After MCSA installation is finished, the MCSA configuration dialog exits.

```

MCSA configuration finished.
You can start /opt/siemens/mindsphere/mcsa/mcsa-config.sh
again to add further MCSA Docker containers, and start/stop,
or delete MCSA Docker containers.
-----
+ MindConnect Software Agent for Linux installation finished +
-----
root@debian10:/home/debian/Downloads#

```

After the installation, a message is displayed that “mcsa-config.sh” can be called later again to create new or maintain existing MCSA Docker containers.

4.8 Onboarding the MindConnect Software Agent

Procedure to access the web server URL and onboard the device


4.8 Onboarding the MindConnect Software Agent

To access the web server URL and onboard the device, follow these steps:

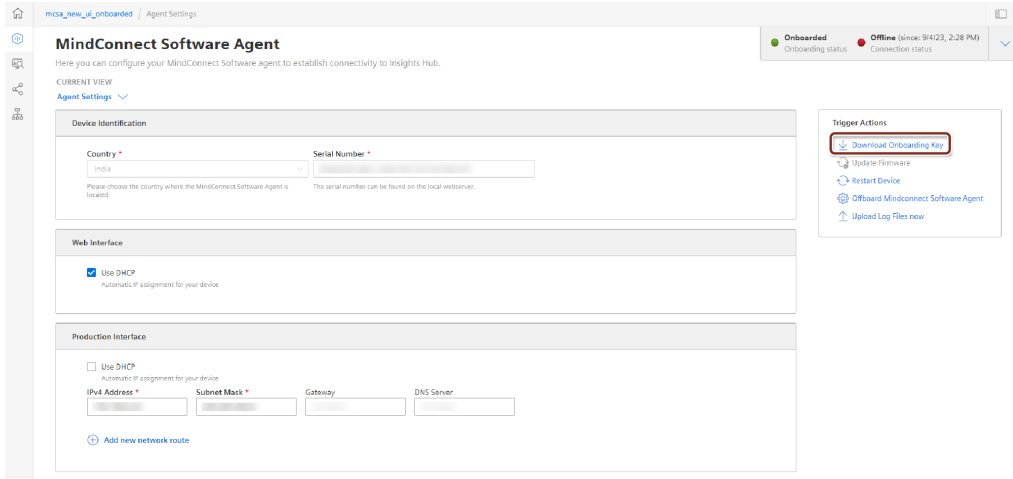
1. In browser, open new tab and enter web server URL.

2. In MindConnect Software Agent overview page, copy the "Serial Number (UID)".

In MindConnect Software Agent plugin page, paste the "Serial Number" and click "Save" and

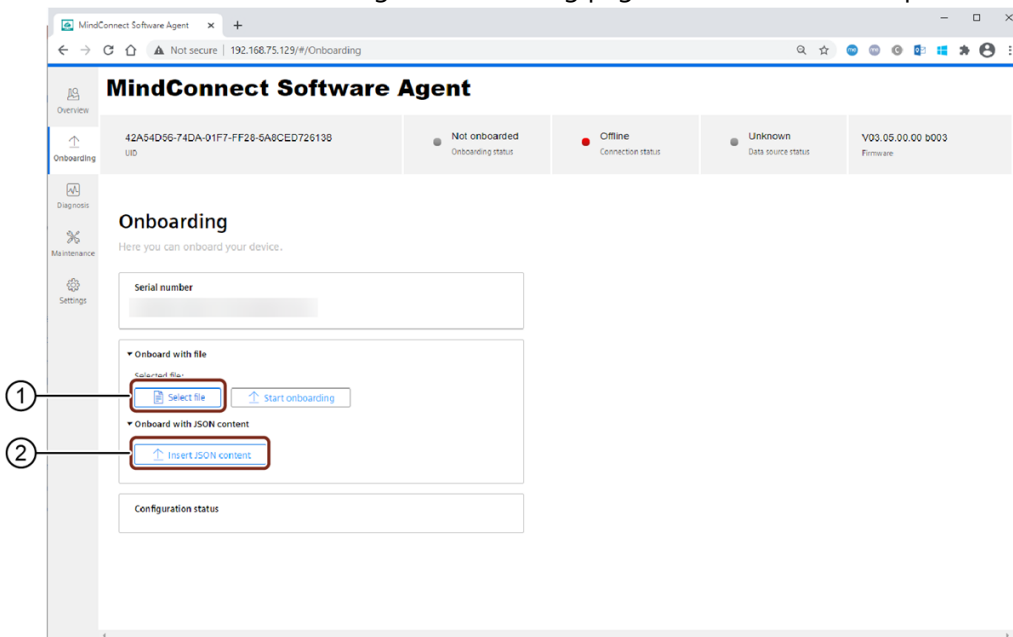
3. then click  to initiate the onboarding process.

4. In the Agent settings view, check the settings and download the onboarding key file.



5. In MindConnect Software Agent's overview page, click "Onboard your device".

6. In MindConnect Software Agent onboarding page, follow the either step:



① Uploads the downloaded onboarding key file

② Inserts the JSON content from the onboarding key file

- Click "Select file" to upload the downloaded onboarding key file with the filename constructed form of serial number.

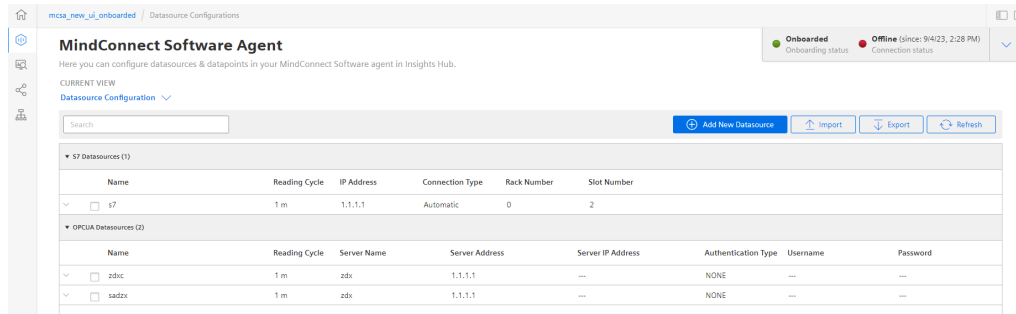
or

- Copy the text from the onboarding key file and click "Insert JSON content" to paste.

7. Click "Start onboarding".
8. In Edit MindConnect page, click "Save" after the device is onboarded.

After the device is successfully onboarded, you can add data sources and data point

9. mapping.



For more information on adding a data source and data points, see [Adding a data source for MindConnect Software Agent](#).

To manage and maintain multiple virtual machines (VM's) in MindConnect Software Agent, see [Managing or maintaining the virtual machines or instances in MindConnect Software Agent](#).

Serial number

The serial number section provides the serial number to copy and paste it to the serial number field during the asset configuration in asset manager.

Onboard with file


In "Onboarding" page, the exported configuration file from asset manager can be selected and click "Start onboarding" to start onboarding.

Onboard with JSON content

It is also possible provide the configuration data directly as JSON input by clicking "Insert JSON input" and paste the JSON configuration data into the opened dialog. Thereafter, start the onboarding by clicking the "Start onboarding".

Configuration status

The status of the onboarding/configuration process is shown in the "Configuration status" section.

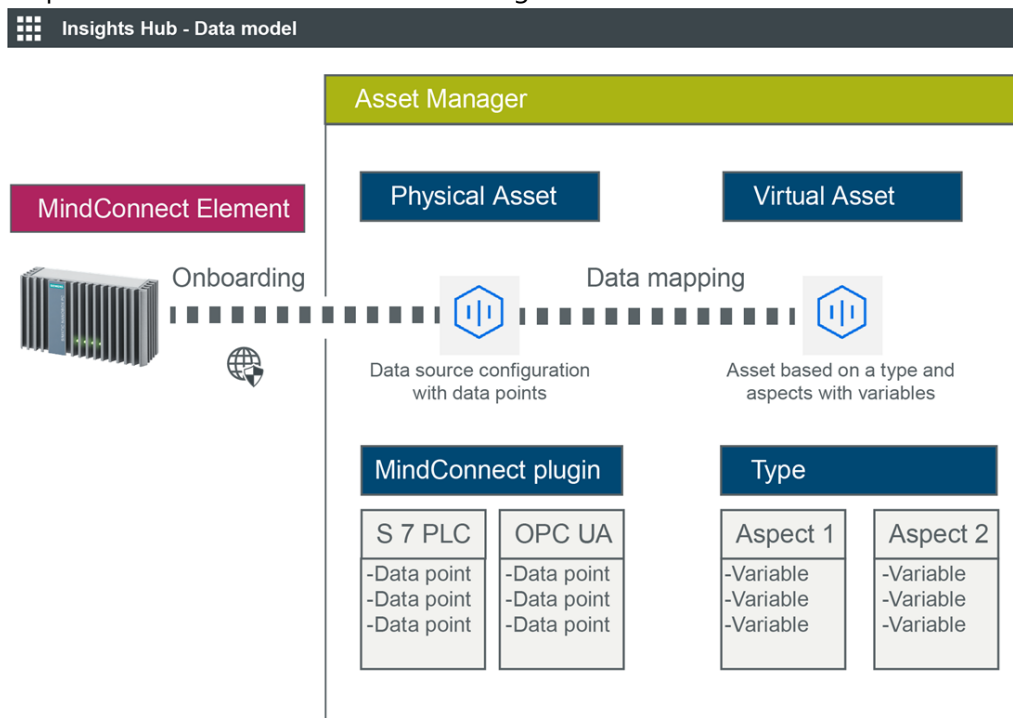


If the network settings are changed by the new configuration data like a new IP address is updated, then the MindConnect Software Agent's web browser must be opened again by using the new IP address of the system. In that case, it might be possible that the diagnosis messages will be displayed twice in the diagnosis messages section. To resolve the issue, restart the virtual machine.

4.9 Configuring data in Asset Manager for MindConnect Software Agent

After onboarding a MindConnect Software Agent, you need to configure the data in Asset Manager. You have to set up a data connection to receive data from your MindConnect Software Agent.

In order to use the data from your MindConnect Software Agent in Insights Hub you need to map the received data to the Asset Manager data model:



Asset Manager uses the following areas:

- Assets
- Types
- Aspects

To configure the data in Asset Manager, follow these steps:

- [Creating an aspect and variables for MindConnect Software Agent](#)

In this step you create aspects and variables you want to use in Insights Hub.

- [Creating a type in Asset Manager for MindConnect Software Agent](#)

In this step you create an asset type to enable data mapping.

- [Adding a data source for MindConnect Software Agent](#)

The data source defines the reading of the data from the MindConnect Software Agent.

- [Mapping an aspect to a data source for MindConnect Software Agent](#)

In this final step you map the data of the MindConnect Software Agent to the aspects and variables in Insights Hub.



In case of role changes or reassignment of roles, it might take up to 15 minutes for current configuration to be effective.

4.10 Creating an aspect and variables for MindConnect Software Agent

To use the data of your MindConnect Element in Insights Hub you need to create aspects and variables in Asset Manager.

Aspects are combined, pre-configured data and form the context for the evaluation of industrial processes. An aspect can consist of several variables. Within the industry process, assets transfer the aspects as time series data in Insights Hub.


In Asset Manager you can create aspect types. Aspect types are pre-configured templates for aspects. The advantage of aspects types is to use one type for several assets. For example, you can create one aspect type for all generators of a wind farm with the variable rotation speed.

For information on creating an asset, refer ["Creating an asset for MindConnect Software Agent"](#).

Procedure

To add an aspect type in Asset Manager, e. g. "Generator", follow these steps:

1. On the start screen click "Aspects".

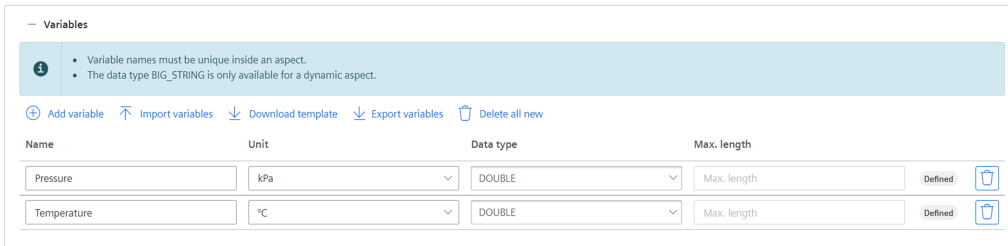
2. To create a new aspect click .

3. Enter your Tenant ID for the aspect, e. g. "betauser.generator".

All custom aspects and types must be named as "<TenantID> .xxx"

- 4. Enter a name and description for the aspect e. g. "Generator".
- 5. Follow these steps for each variable, e. g. "Pressure" and "Temperature":
 - Enter variable data.

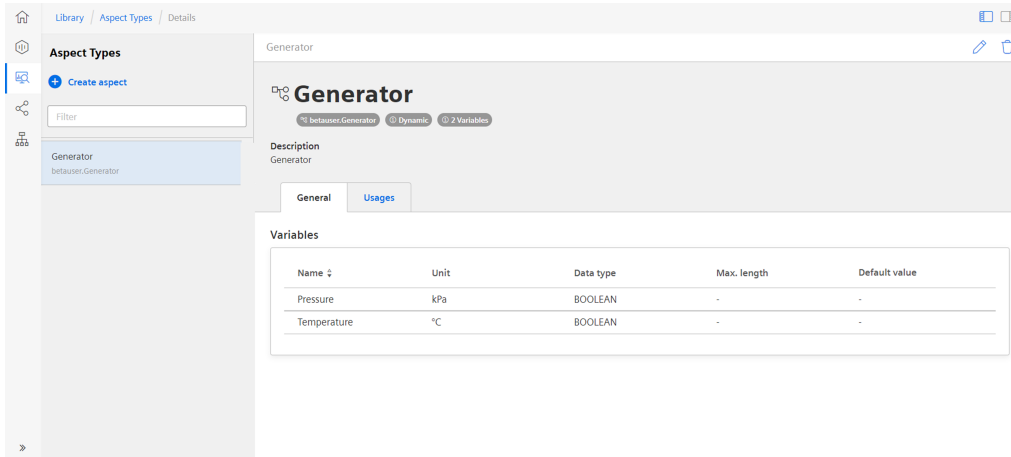
The units and data types specified here will need to match exactly(also case sensitive) with the physical data source.



- Click "Add variable" to add other variables.
- 6. Click "Save".

Result

The new aspect type with its variables is available in the aspect list.



4.11 Creating a type in Asset Manager for MindConnect Software Agent

To enable data mapping, you first have to create an asset type. An asset type is a pre-configured template for an asset. The asset type predefines which aspects are integrated into the template.


You have to link aspects to an asset type to enable the connection to a data point.
For information on creating an asset, refer ["Creating an aspect and variables for MindConnect Software Agent"](#).


Requirements

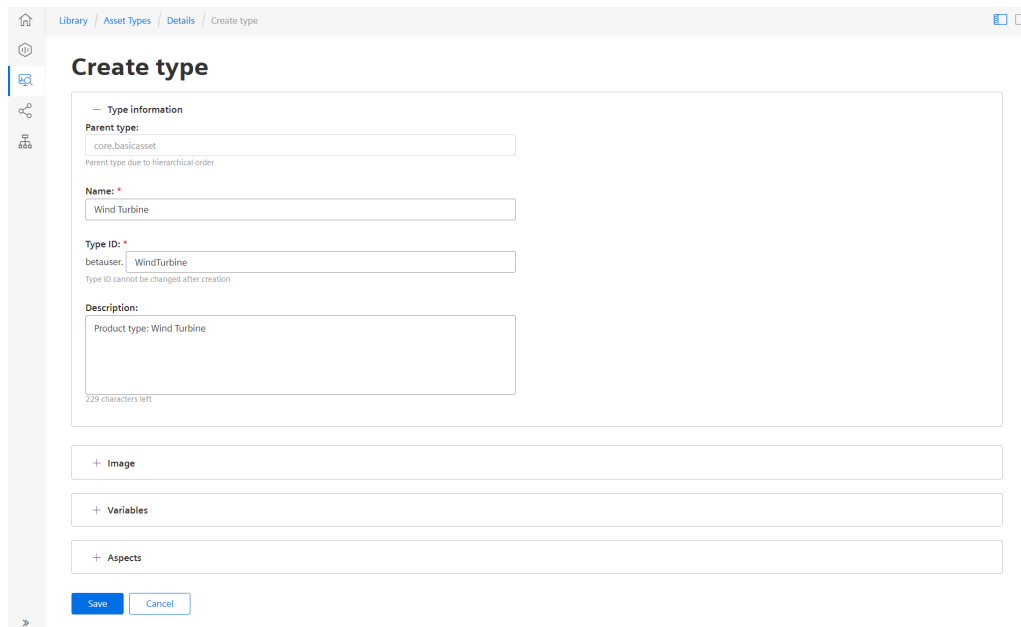
- You have created an aspect.

Procedure

To create an asset type proceed as follows:

1. Click on the "Types" tab in Asset Manager.
2. Click on "BasicDevice".
3. To create a new asset type click .
4. Enter ID and name for asset type, e. g. "Wind turbine".

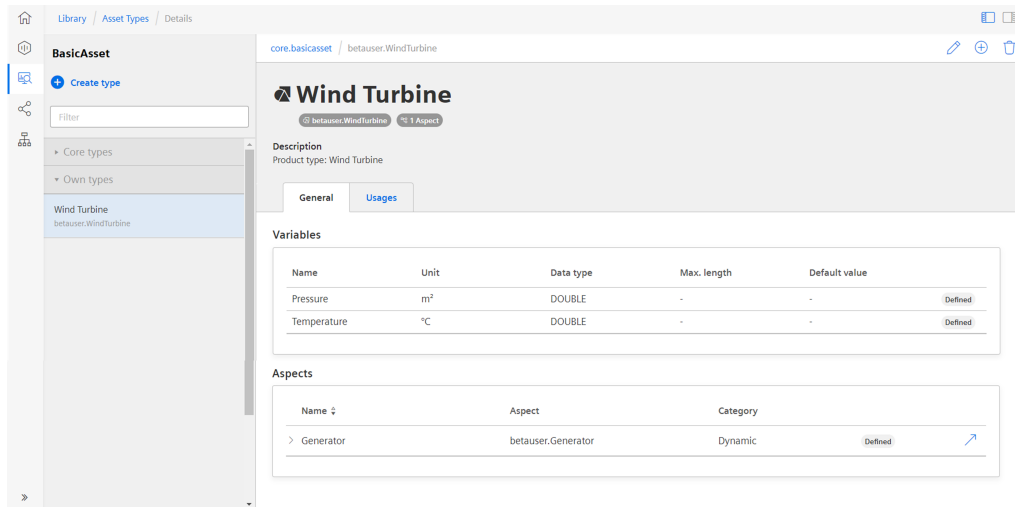
 The ID must be named as "TenantID.xxx".



5. Click "Image" to add an image to the aspect type.(optional)
6. Click "Variables" to add variable(s) to the aspect type.(optional)
7. Click "Aspects" and click "Browse aspects" to select an aspect from the dropdown menu and then click "Add". For more information on adding aspect type. see ["Creating an aspect and variables for MindConnect Software Agent"](#).
8. Click "Save" to save the asset type .

Result

The new asset type is successfully created. The new asset type is now available in the presets. The following graphic shows the new available asset type "Wind turbine" in assets.



4.12 Adding a data source for MindConnect Software Agent

To receive the data of your MindConnect Software Agent you need to add a data source. The data source specifies the protocol and reading cycle that is used to transfer the data from your asset to the MindConnect Software Agent. Within the data source, you enter the IP address of the asset inside of your network.

Requirement

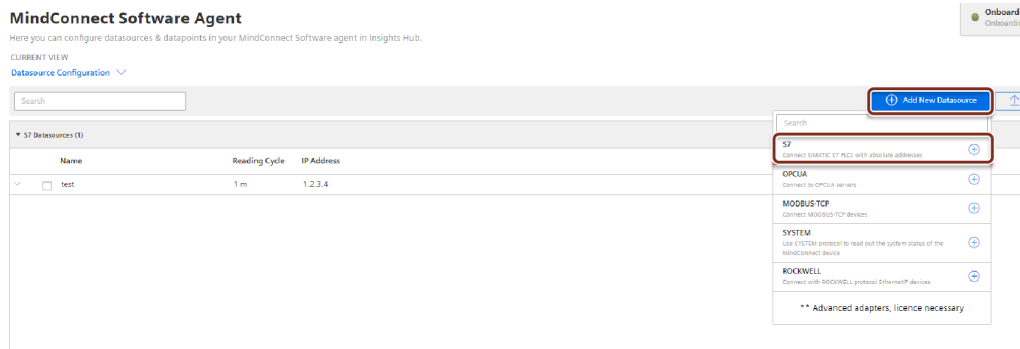
- You have created an asset and an aspect.
- You have enabled the connection to the MindConnect Software Agent.
- You have the IP address of the asset inside of your network.


Procedure

To add a data source to an asset of type MindConnect follow these steps:

1. Select the asset in the "Assets" tab, for example: "Wind turbine".
2. Click on the asset icon, for example: "MindConnect Software Agent".

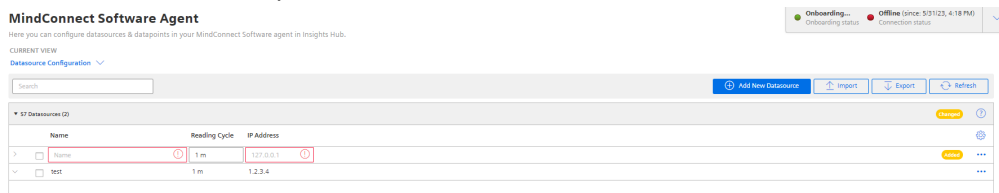
In the Data Configuration view, click "Add New Datasource" and select the datasource to
3. add a new datasource.





- The default reading cycle is 1 minute, which is one day.
- You can find additional information on supported protocols in the chapter [Overview of supported protocols for MindConnect Software Agent](#).

4. Enter the datasource parameters.



5. Click "Save".

Result

You have now created a new data source. The new data source is available at the asset details of your MindConnect Software Agent.

The following graphic shows the data source added:



Cloning of Datasource

Clone of datasource creates a copy of datasource (including copy of datapoints). User needs to provide new name for datasource.

4.13 Adding data points for MindConnect Software Agent

A data point is a measurable value of an asset that can be represented numerically and graphically. Examples of a data point are temperature or pressure. You can add data points to a data source to collect the data for example from a control unit. In the next step you have to link the data points of a data source with the respective variables of an aspect.

You can find more information about how to send data in chapter [Send commands for MindConnect Software Agent](#).

Limitations

A single datapoint cannot be mapped to two variables in the same aspect.

Health status

- The health status shows the quality of the connection of the data point. You can click on the status to get further information. For more information about quality code, see [Quality code settings](#).
- The datapoints health status are shown as "Unknown", if the device status is "Offline".

Requirement

- You have created a data source.

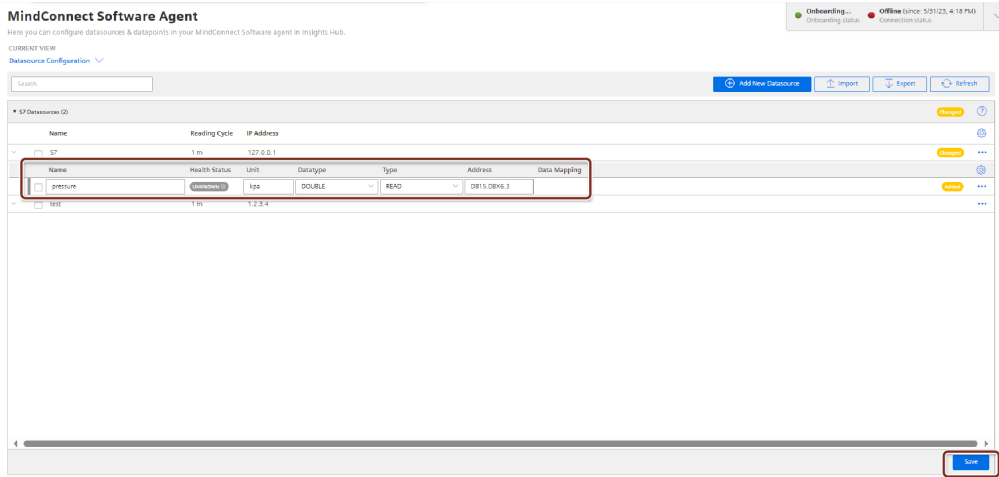
Procedure

To add a data point to a data source, for example: "Pressure", follow these steps:

- Select the asset in the "Assets" tab, for example: "Wind turbine".
- Click the asset icon, for example: "MindConnect IoT2050".
- Click "Add Datapoint" corresponding to the selected datasource.



Enter the data point data.



4.

5. Click "Save".

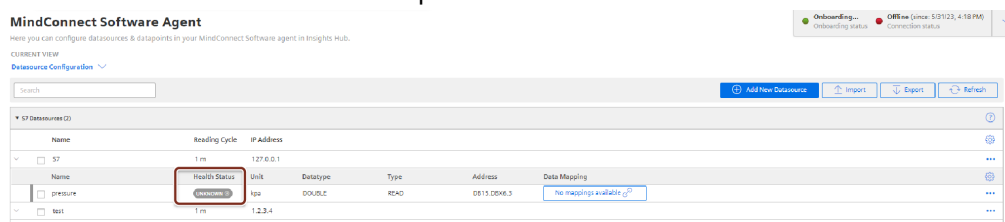


- The units and data types specified here will need to match exactly with the aspects and variables. If they are different, the aspect cannot be connected to the data point.
- The protocol datatypes specify the Datapoint Address. You can find additional information on protocol datatypes in the chapter [Overview of supported protocols for MindConnect Software Agent](#).
- "Data Acquisition Mode" defines the access type of datapoint. There are three acquisition types; "READ", "WRITE" and "READ&WRITE". To write data to a datapoint, "WRITE" or "READ&WRITE" type needs to be selected. Default value is "READ".
- It is possible to use hysteresis value in this field. This reduces the number of read events. The hysteresis filters signals and reduces the response to short-term signal fluctuations. The maximum value for hysteresis length is limited to 5.

Result

The new data point is available at the data source.

The health status of the new data point is shown here.



Cloning of Datapoints

Cloning of datapoint creates a copy of datapoint. The datapoint is cloned without a name(user needs to enter the name manually) and data mappings(in case there are any existing data mappings for the datapoints).

4.14 Mapping an aspect to a data source for MindConnect Software Agent

Data mapping is matching variables of an aspect with the respective data points of a data source.

- Variables of an aspect represent the Industrial IoT data.
- Data points of a data source represent the data of the MindConnect Software Agent.

To use the data of your MindConnect Software Agent you have to map them to the respective variables of an aspect.

Requirement

You have created an asset based on your desired aspect and asset type.



Browser compatibility

Microsoft Edge browser do have some issues with the user interface (example: "Mapping"). Use another browser like, "Chrome" or "Firefox".

Data mapping is done in two ways, which are mentioned and explained in below procedures.

- [By using in-cell mapping functionality.](#)
- [From "Advance Mappings" or "Datapoint Mapping" option.](#)

Map a variable to a data point by using in-cell mapping functionality

To map a variable to a data point by using in-cell mapping functionality, follow these steps:

1. Select the asset in the "Assets" tab, for example: "Wind turbine1".
2. Click the MindConnect Software Agent Plugin icon.

Click "No mapping available" to map a variable in the Data configuration view for the data points added.

3.

Name	Health Status	Datatype	Address	Data Mapping
OPCUA	2 m	SERVERNAME	opc.tcp://127.0.0.1:4840	BASIC USERNAME ***** NONE
DP1	UNKNOWN	LONG	address	No mappings available

4. Enter and select the variable to map the data point.

Name	Reading Cycle	Server Name	Server Address	Authentication Type	Username	Password	Security Mode	Certificate
Windturbine	1 m	1	opc.tcp://127.0.0.1:4840	NONE	---	---	NONE	
Name	Health Status	Datatype	Address	Data Mapping				
Pressure	UNKNOWN	DOUBLE	rsp[Index]=1[Identifier]	mapping				

mapping

- > MappingTestingDataOwnerAsset2 1 Variables
- > MappingTestingDataOwnerAsset3 1 Variables
- > MappingTestingDataOwnerAsset4 1 Variables
- vibrations DOUBLE
 - generator_wasting
- > MappingTestingDataOwnerAsset6 1 Variables

Only data types that match exactly with the aspects and variables are available. If they are different, the aspect can't be connected to the data point.

Map a variable to a data point from "Advance Mappings" or "Datapoint Mapping" option

To map a variable to a data point by "Advance Mappings" or "Datapoint Mapping" option, follow these steps:

1. Select the asset in the "Assets" tab, for example: "Wind turbine1".
2. Click the MindConnect Software Agent Plugin icon.
3. Click "Datapoint Mapping" as shown in the image.

Name	Health Status	Datatype	Address	Data Mapping
OPCUA	2 m	SERVERNAME	opc.tcp://127.0.0.1:4840	BASIC USERNAME ***** NONE ASKUSAgent1
DP1	UNKNOWN	LONG	address	No mappings available

Datapoint Mapping

Clone

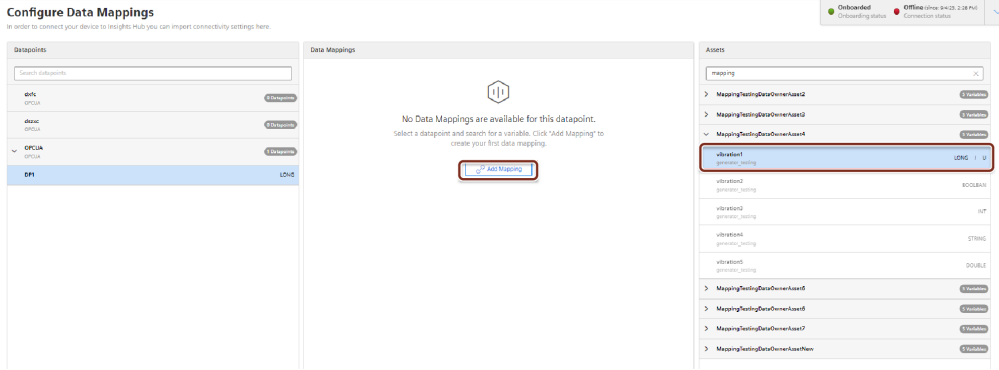
Delete

To map a datapoint to a datasource by "Advance mapping", select the "Advance mapping" option on the Mindconnect Software Agent plugin homepage. The below image displays the Advance mapping option.

The screenshot shows the MindConnect Software Agent configuration page. On the left sidebar, under 'Data source Configuration', the 'Advanced Mappings' option is highlighted with a red box. The main area shows a list of data sources with columns for Name, Health Status, Datatype, Address, and Data Mapping. A 'MindConnect Software Agent' dialog box is open, showing options for 'Data source Configuration', 'Agent Settings', 'Advanced Mappings', and 'Network Update'.

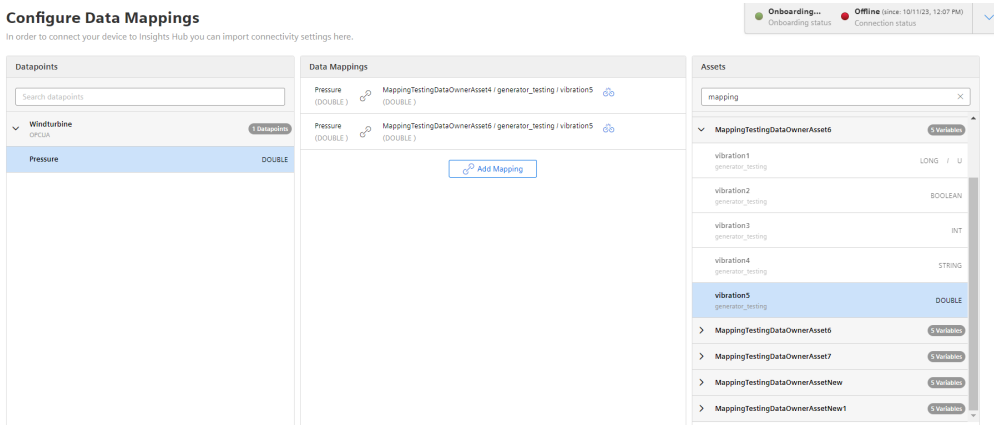
4.14 Mapping an aspect to a data source for MindConnect Software Agent

4. Enter the variable to map in the Assets tab to select the variable and click "Add Mapping".



In "Advance mapping", select the datapoint to be mapped in the datapoint window before selecting the variable.

5. To map multiple data point, select an another variable to be mapped and click "Add Mapping". The below image shows the multiple data mapping.



Result

The data point is now mapped to the variable. User can also perform mappings for multiple datapoints.

The following graphic shows a data mapped variable:

OPCUA Datasources (1)						
Name	Reading Cycle	Server Name	Server Address	Authentication Type	Username	
Windturbine	1 m	1	opc.tcp://127.0.0.1:4840	NONE	---	
Name	Health Status	Datatype	Address	Data Mapping		
Pressure	UNKNOWN	DOUBLE	ns=[Index];s=[Identifier]	MappingTestingDataOwnerAsset4 / generator_testing / vibration5		

The following graphic shows a Multiple data mapped variable:

Name	Reading Cycle	Server Name	Server Address	Authentication Type	Username	Password	Security Mode	Certificate	Event Type
OPCUA	1 m	dsbc	opc.tcp://127.0.0.1:4840	NONE	---	---	CERTIFICATE	opcua.crt	DataSourceEvent
OPCDA	1 m	dsbc	opc.tcp://127.0.0.1:4840	NONE	---	---	CERTIFICATE	opcua.crt	DataSourceEvent
OPCUA	2 m	SERVERNAME	opc.tcp://127.0.0.1:4840	BASIC	USERNAME	*****	NONE		AKAIndgenEvent

Name	Health Status	Datatype	Address	Data Mapping
DPI	OK	LONG	address	3 Mappings available (2)

4.15 Configuring Network settings

Network configuration of MindConnect Software Agent requires information on the ethernet interfaces for data acquisition (ethernet labeled with X2P1) and Industrial IoT (ethernet labeled with X1P1). If your company uses a proxy server, it must also be configured to connect MindConnect Software Agent to Industrial IoT. Contact your IT administrator for details on your local network settings.

After enabling the connection to the MindConnect Software Agent, you can edit the network configuration. You can enter either a static IP address or use DHCP. The DHCP option is only possible, if there is a DHCP server available in your company network.

Network settings

All MCSA Docker containers are running in host network mode only, one MCSA container is chosen to have static IP addresses in the device configuration, if it is necessary that the IP addresses of the Linux host system is to be configured by the asset of the chosen MCSA Docker container.




Requirement

It is necessary that the host network interfaces are configured by the MCSA Docker containers which are configured with the static IP addresses, otherwise it is possible that another IP address will be assigned by DHCP during runtime.

DHCP Network settings

These settings are required for the Linux host system where MCSA for Docker can be installed. In some network environment it is possible that the Linux host system receives a new IP address after restarting the host system depending on the DHCP client configuration. Therefore, it is recommended to add the following line to the file "/etc/dhcp/dhclient.conf" of the Linux host system

```
send dhcp-client-identifier = hardware
```



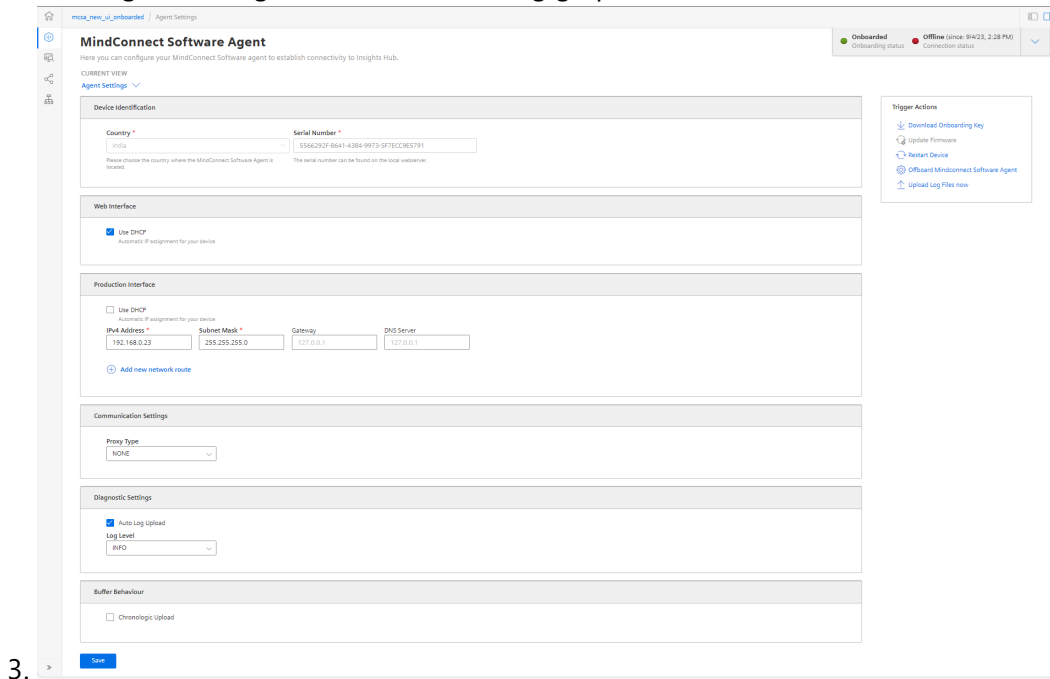
This configuration is recommended on SIEMENS SIMATIC IOT2050 Advanced-PG2 with Industrial OS 3.2.2 or higher.

Procedure

To configure the network settings, follow these steps:

1. Select the asset in the "Asset" tab.
2. Click the asset icon for example "MindConnect Software Agent".

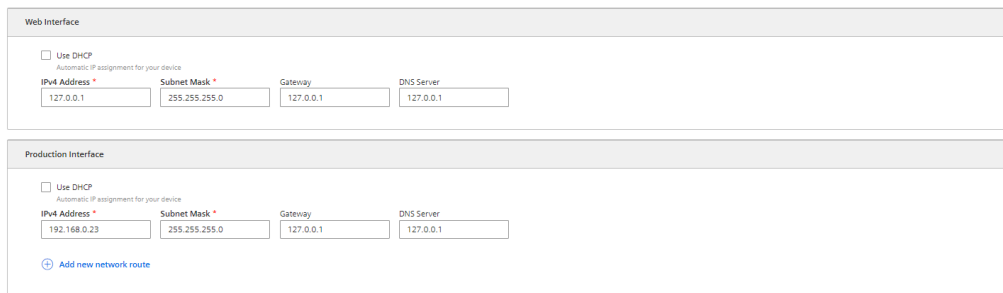
In th Agent settings section, the following graphic shows the "Edit MindConnect" screen.



3.

Enable "DHCP" if the DHCP server is available in a company network or enter the address information for static IP address.

4. The following graphic shows the IP address input fields:





- It is recommended to add network routes instead of using Gateway field. It is applicable for "Production Interface" only.

5. Enter the proxy data area "Communication Settings" if necessary and click "Save".

- In this case, contact your network administrator to get the proxy data. For Proxy IP address input field, it is also possible to define the port number, for example: 127.0.0.1:8080.
- For proxy authentication type NTLM: The domain and the username have to be provided as "username@domain" or as "domain/username".



If nothing else is configured manually, MindConnect Software Agent will try to obtain IP addresses for both adapters via DHCP.

6. Enter the available router gateways used in your company network.

Production Interface

Use DHCP
Automatic IP assignment for your device

[+ Add new network route](#)

IP Address *	Subnet Mask *	Gateway *	
<input type="text" value="127.0.0.1"/>	<input type="text" value="127.0.0.1"/>	<input type="text" value="127.0.0.1"/>	
<input type="text" value="127.0.0.1"/>	<input type="text" value="127.0.0.1"/>	<input type="text" value="127.0.0.1"/>	

7. Click "Save" to complete the configuration.

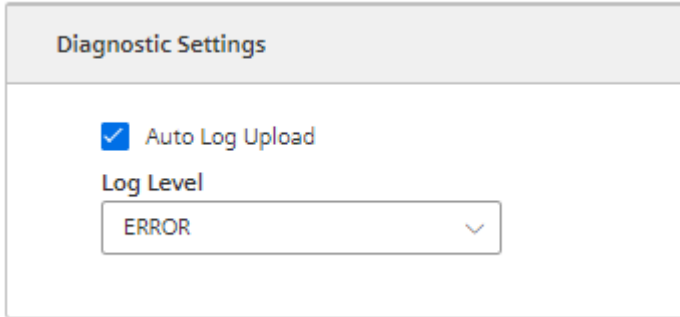
4.16 Configuring Dagnostic settings

Diagnostic Settings

This section contains the configurations related with logging. To perform a diagnostic settings change, follow these steps:

1. In "Asset" tab, select the asset.
2. Open MindConnect plugin.

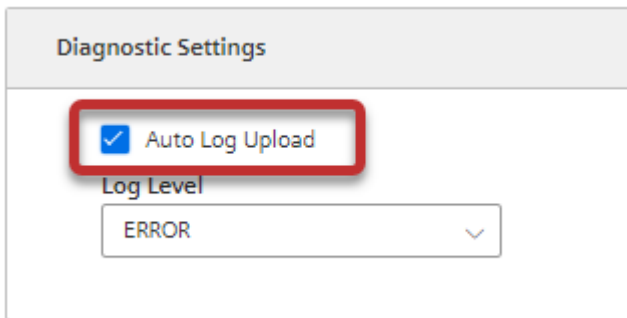
3. In the Agent settings view, make the changes in Auto Log Upload or Log Level.



4. Click "Save".

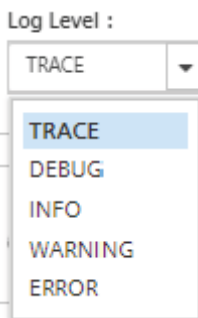
Auto Log Upload

If Auto Log Upload is enabled, the device uploads all the generated logs to Insights Hub periodically. Auto Log upload functionality for the device is enabled by default.



Log Levels

Log level represents the log level of MindConnect device. There are five possible log levels, and the hierarchy is as follows in lowest (TRACE) to highest (ERROR) priority. In "TRACE" mode, the device will log extensively and in "ERROR" mode device will only log error messages.



The selected log level and logging mechanism works as logging only selected level and the higher levels.

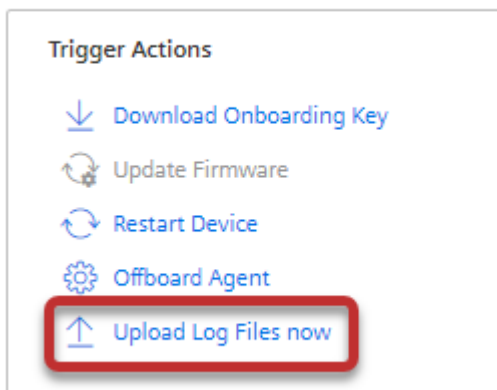
Log level is set to "INFO" by default.

Auto Log Level Change

- “TRACE/DEBUG” log levels provide more verbose logs which will be helpful to troubleshoot issues, however they produce more files. If the log level is set to “TRACE/DEBUG”. It will be automatically changed to INFO after one day.
- Auto log level change operation will not be synchronized with the asset’s device configuration.

Upload Logs Now

If you click “Upload Logs Now”, the device uploads the latest logs to Insights Hub regardless status of Auto Log Upload. It can be used for troubleshooting purposes.



Configuring Buffer Mechanism

In buffer mechanism, there are two options:

- Default Buffer Mechanism: It provides parallel upload from cache and real time data. It prioritizes newest data to old data while storing (works as a last in, first out (LIFO))
- Chronological Buffer Mechanism: It is chronological upload of data. If "Chronologic Upload" is selected, the buffer mechanism will prioritize oldest data to new data (works as first in, first out (FIFO)).

You can configure the buffer behavior from "Network and Diagnostic Settings" screen.



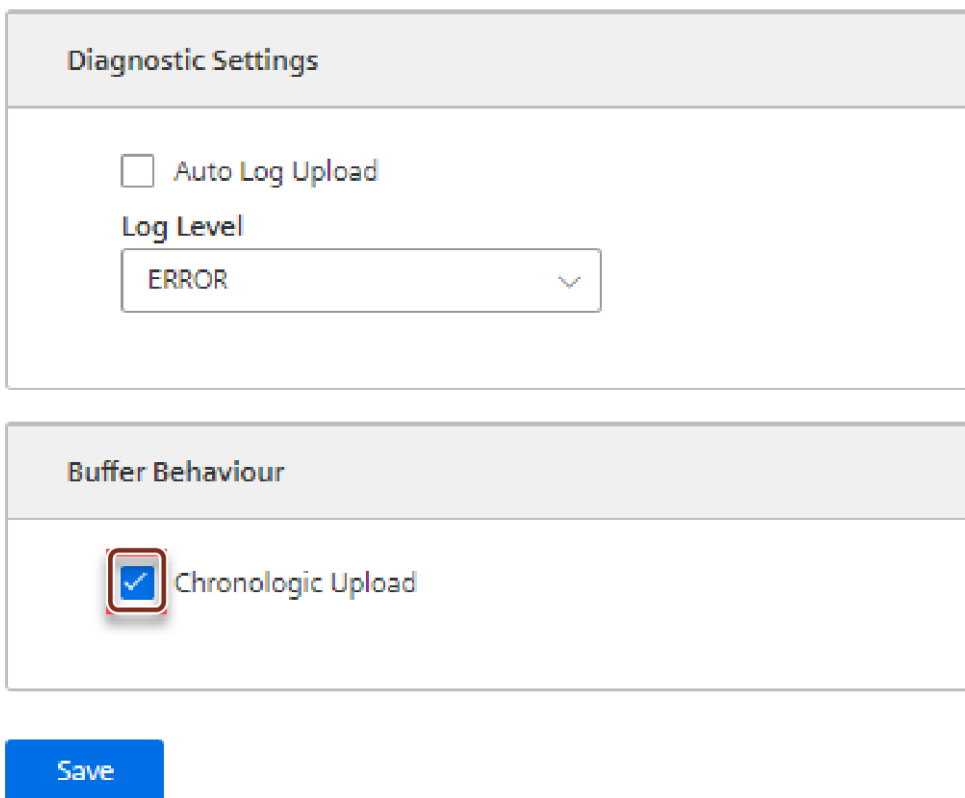
If the buffer behavior is changed, it restarts the data collection process and this process takes few minutes.

 **Data loss**

The data collection will be stopped during the time of buffer behavior change. The amount of data collection is stopped for few minutes, it depends on restart of the device. It may take longer time on slow devices like, Software Agent.

To perform a buffer behavior change proceed as follows:

1. In "Asset" tab, select the asset.
2. Open "MindConnect" plugin.
3. In the Agent settings view, select "Chronological Upload" in "Buffer Behaviour" section.



The screenshot displays the configuration interface for the MindConnect Software Agent. It is divided into two main sections: "Diagnostic Settings" and "Buffer Behaviour".

Diagnostic Settings: This section includes an unchecked checkbox for "Auto Log Upload" and a "Log Level" dropdown menu currently set to "ERROR".

Buffer Behaviour: This section features a checked checkbox for "Chronologic Upload", which is highlighted with a red border.

At the bottom of the interface is a blue "Save" button.

Chronologic Upload Specification

- If there is a bad network connection or no connection at all, the data is going to be stored in cache memory. In "Chronologic Upload", overwritten of cache memory is not possible. Only if there is any space on cache memory, the data is going to be written to it. If the cache memory reaches out it's limit and filled with data, then the data is not going to be saved on cache memory. It will cause data loss until some data is uploaded.
- As chronological upload the flow of real data to cloud will take longer time comparing to default behavior.
- The events are not cached in any case of the disconnection. Therefore, "Chronologic Upload" is not applicable for the event upload.

4.17 Browsing datapoint of a data source for MindConnect Software Agent

MindConnect devices types and software agents support browsing of data points for the selected data source so that the data points can be added from the current device configuration.



- This feature is only supported for OPC UA, S7+, IEC61850 and MTConnect protocols.
- During configuration of data points via browsing feature, performance may get impacted depending on the configuration and data points in Data Sources.

Supported protocols for Browsing

The following table shows the protocols which supports Browsing with the supported version of MindConnect Software Agent(MCSA):

Protocol	Browsing type	MCSA-Windows	MCSA-Docker(amd64) version	MCSA-Docker(arm64) version
BACnet ¹	static	NA	NA	V03.06.20.00 b002

Protocol	Browsing type	MCSA-Windows	MCSA-Docker(amd64) version	MCSA-Docker(arm64) version
IEC61850 ¹	dynamic	V03.06.00.09 b002	V03.06.01.02 b002	V03.06.20.00 b001
MTConnect ¹	dynamic	V03.06.00.09 b002	V03.06.01.02 b002	V03.06.20.00 b001
OPC UA	dynamic	V03.06.00.15 b005	V03.06.02.01 b003	V03.06.20.00 b002
S7+ ¹	dynamic	V03.06.00.09 b002	V03.06.01.02 b002	V03.06.20.00 b001
SystemInfo	static	V03.06.00.22 b003	V03.06.03.00 b003	V03.06.21.00 b003

1) "MC Advanced package" is needed to use these protocols.

- Static : For static browsing a predefined datapoint catalogue dependend on the MindConnect device and/or protocol type will be provided.
- Dynamic : Current datapoint information will be retrieved from the selected device - this might take some time depending on the device configuration.

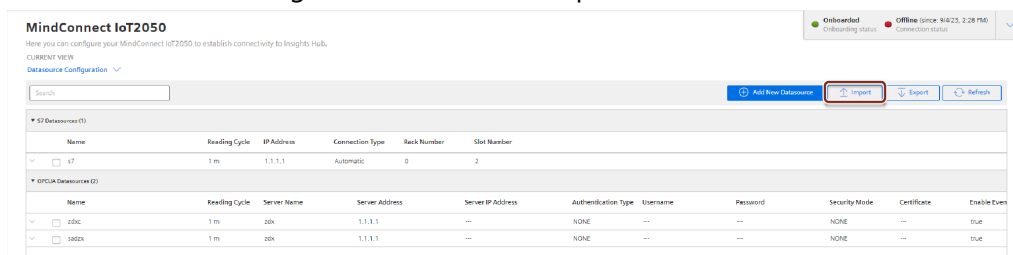
Prerequisite

- You have created a data source.
- After creating the data source, click "Save" and "Apply changes".

Procedure

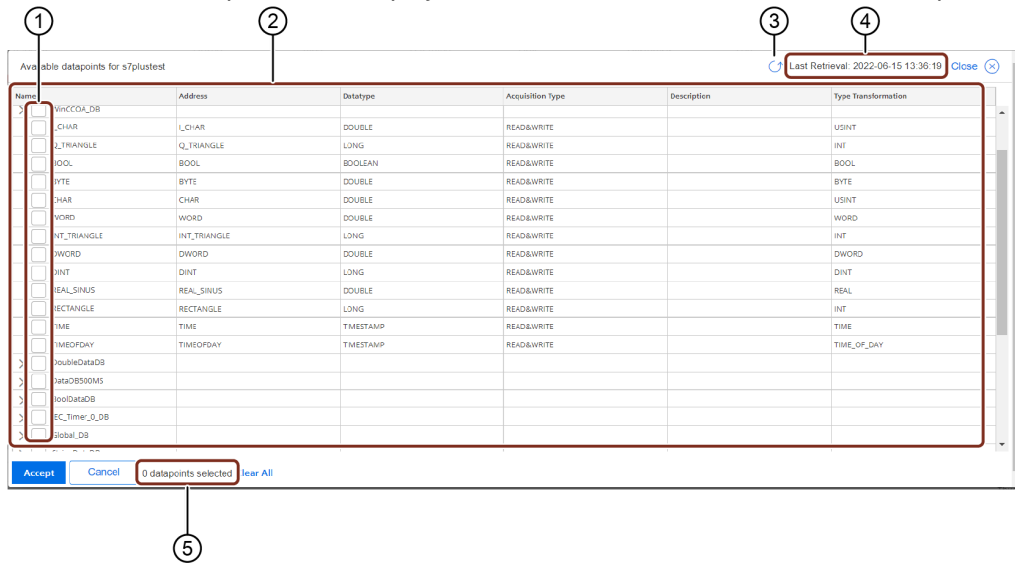
To browse the datapoints of a data source, follow these steps:

1. In the "Assets" tab, select the asset.
2. Click MindConnect Software Agent plugin.
3. In "Datasource Configuration" view, click "Import".



Result

The available datapoints are displayed for the selected data source. for example:

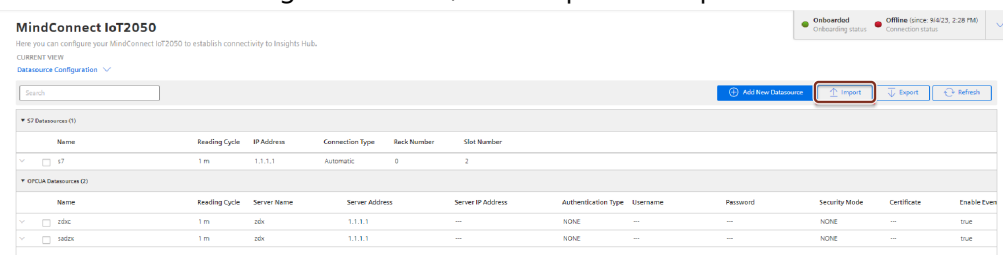



- Check the structure in the template file. It differs for each plugin type.
- The mapping notation should be in following format : **AssetName->AspectName->VariableName.**

Procedure

To import the data source configuration for an asset of the type MindConnect Software Agent, follow these steps:

1. In the "Assets" tab, select the asset.
2. Click MindConnect Software Agent plugin.
3. In "Datasource Configuration" view, click "Import" to import a file.



4. In the "Import File" tab, browse the data source configuration file and click .

Import Datasources

In order to connect your device to Insights Hub you can import connectivity settings here.

[Back](#)

Import Source Selection

Import File
Use this option if you do have your datasource configuration available as .xlsx file.

[Download Template File](#)

Selected File *

Drop items here or [Browse files](#)

Up to 25 MB. File name without special character. Supported file type *.xlsx.

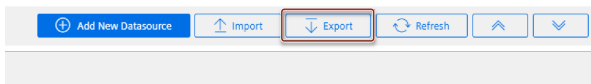
Browse existing datasource
Use this option if you would like to browse an existing data source.

Selected Data Source *

Windturbine



- To check the format of the data configuration file before importing the configuration, download the template file by clicking download template.
- The template file consists of an example data configuration with datapoint mappings. In the below given screenshot, the information related to data source and datapoint declarations for S7 and it can switch to each protocol from the bottom of the file (e.g S7, OpcUa, modbus-tcp, etc).
- "Export" option makes the user to export the existing data source configuration of an asset, where the existing data source configuration is exported as file and can be imported to overwrite or add to the existing configuration.



- The supported protocols for import and export configurations are S7, OPC UA, Modbus-TCP, Rockwell, System, FanucFocas, S7+, Sinumerik, IEC61850, MTConnect and BACnet.
- For OPC UA Data source, configurations like OPC UA security certificates need to be added manually and are not supported via export and import.
- For IEC61850 Data source, configurations such as SCD file need to be added manually and are not supported via export and import.

5.To delete and add new data configuration, select "Overwrite existing configuration" or to add new data configuration to the existing data configuration, select "Add to existing configuration".

Import Datasources

In order to connect your device to Insights Hub you can import connectivity settings here.

[Back](#)

Preview of imported Datasource configurations

57 Datasources
Total

2
including 1 datapoints

Import Configuration

- Overwrite existing configuration**
 All existing datasources and datapoints will be deleted. New datasources and datapoints will be created as imported.
- Add to existing configuration**
 New datasources and datapoints will be added. No existing resource will be deleted during import.

Start import

By clicking "Start import" we are going to create the defined resources for you.

6. Click "Start import".

The latest import feature now supports the import of **Multimapped datapoints**, allowing upto 5 datapoints mapped with a variable. The below image displays the import file details.

Data source configuration information														Datapoint mapping information (optional)										
Type	Datasource	Read Cycle	Unit	Datapoint	Datatype	Unit	Category	Subcategory	Variable	On Data	Hysteresis	Mapping 1	Mapping 2	Mapping 3	Mapping 4	Mapping 5								
DS	ds1	1m		dp1	DOUBLE		CPU		LoadAvg1	false	0													
DP												MappingTestingDataOwnerAsset2->generator_testing->vibrations	Mapping1	MappingTestingDataOwnerAsset3->generator_testing->vibrations										
DS	ds2	1m		dp1	DOUBLE		CPU		LoadAvg1	false	0													
DP												MappingTestingDataOwnerAsset2->generator_testing->vibrations	Mapping1	MappingTestingDataOwnerAsset4->generator_testing->vibrations										

- ① Data source configuration information
- ② Datapoint mapping information (optional)

- If there are validation errors while importing, the user needs to resolve all the errors to complete the import. User can refer to "errors" for resolving errors in excel sheet.

- If the values for datasource Import and Export are not specified during import replace the values by default values. For the list of default values, refer to [Default values for datasource Import and Export](#).

Result

Data source configuration are imported with mapped datapoints. The new data sources is available in the asset details of MindConnect Software Agent. Datamapping is available corresponding to the datapoints.

MindConnect Software Agent
 Here you can configure your MindConnect Software agent to establish connectivity to Insights Hub.
 CURRENT VIEW
 Datasource Configuration

Onboarding... Offline since 5:11:22, 4:18 PM

Search name

Add New Datasource Import Export Refresh

57 Datasources (2)

Name	Reading Cycle	IP Address	Health Status	Unit	Datatype	Address	Data Mapping
57	1 m	127.0.0.1	Unknown	kpa	DOUBLE	DB15.DBK6.3	MappingTestingDataOwnerAsset / generator_testing / vibration5
pressure	---						
test	1 m	1.2.3.4					

- Asset name needs to be unique in the environment. If multiple assets are with the same name in the environment, then the datapoint mappings may have discrepancy.
- Asset needs to be available before importing the configuration. Asset will not be created during import configuration.
- Datapoint name needs to be unique in excel sheet across data sources and protocols.
- Datapoint mapping of a datapoint with multiple variables of multiple assets is not supported.
- Importing of datapoint mappings is an async process.



The mapping process is performed asynchronously, once the import operation is finalized. Depending on the data size, the mapping creation process will vary on time.

Limitations of Import feature

The limitations of Import feature are,

- Refreshing the browser page during import will interrupt the import process.
- Leading space characters in the AssetName field can result in mapping issues during Excel export and import procedures.
- Ensure reading cycle has **integer** values before importing.
- Double-check the hysteresis values as per the data type.
- For boolean fields, any values other than **true** will be imported as **false**.
- Non mandatory fields will be imported as **blank** in case fields are not specified.
- Validate that the Asset, Aspects and variable exists in the tenant.

4.19 Configuring MindConnect Software Agent using API

AgentManagement API

You can configure MindConnect Software Agent via api calls with public API's that are offered from Industrial IoT. To update the data source configuration of AgentManagement api, refer to the endpoint "Data Source Configuration Operations" in [Agent Management Service – API Specification](#).

For more information on how to authenticate and how to get the information related with the MindConnect element, refer to [Develop for Industrial IoT](#).

This below information will show, how to structure the configuration part for the above api request for specific industrial protocols.

Protocol configurations

You can configure the device to AgentManagement using the below protocol specific configurations that needs to be configured in the api call.



In case the body structure is not as expected, the configuration might be rejected or may lead to corrupt configuration. Always verify the operation from MindConnect Element UI.

The json configuration in body part of the request consists of below key-value pairs. All the documented key-value pairs given below are important. The customData child fields of dataPoints and dataSource items are free formatted fields and should be a valid json. Below is the configuration body:

```
{
  "name": "DataSource Name",
  "customData": {
    "protocol": "Name of the protocol",
    "protocolData": { },
    "readCycleInSeconds": "Value"
  },
  "description": "",
  "dataPoints": [
    {
      "id": "a37d9e1fee6b4",
      "name": "DatapointName",
      "description": "-",

```

```

        "unit": "Unit",
        "type": "Type",
        "customData": {
            "dataPointData": { }
        }
    }
]
}

```



The above key-value pairs are important for the body, if missing any key-value pair will result in configuration failure.

Each protocol has its unique `protocolData` representing its protocol specific fields and `dataPointData` field for representing its unique datapoint configuration. In order to get the successful configuration for each one of the protocol, the free formatted parts of the body needs to be a valid json. Otherwise, the configuration will be failed.

The below given an example of how to configure a datasource with one datapoint for S7 protocol:



- The below json content can be changed as required, do not depend on it strictly.
- The free formatted fields "protocolData" and "dataPointData" has a specific configuration to S7 protocol.

```

{
    "name": "S7DS",
    "customData": {
        "protocol": "S7",
        "protocolData": {
            "ipAddress": "192.168.0.1",
            "manualRackAndSlot": "Automatic",
            "rackNumber": "0",
            "slotNumber": "2"
        },
        "readCycleInSeconds": "1"
    },
    "description": "",
    "dataPoints": [
        {

```

```
"id": "a37d9e1fee6b4",
"name": "DatapointName",
"description": "-",
"unit": "%",
"type": "LONG",
"customData": {
  "datapointData": {
    "address": "DB1.DBWORD0",
    "hysteresis": "0",
    "onDataChanged": false,
    "acquisitionType": "WRITE"
  }
}
]
```

Getting Configuration Details of Protocols

To get the configurations details for other protocols such as Modbus, Ethernet IP etc, the API of AgentManagement can be used to get the configuration details. The initial configuration can be done via UI and then using the below API config, it can be extracted and used for API calls and later for structuring.



The json content of each protocol varies and should be extracted after an initial UI configuration.

To get the data source configuration of AgentManagement api, refer to the endpoint "Data Source Configuration Operations" in [Agent Management Service – API Specification](#)..

Managing MindConnect Software Agent

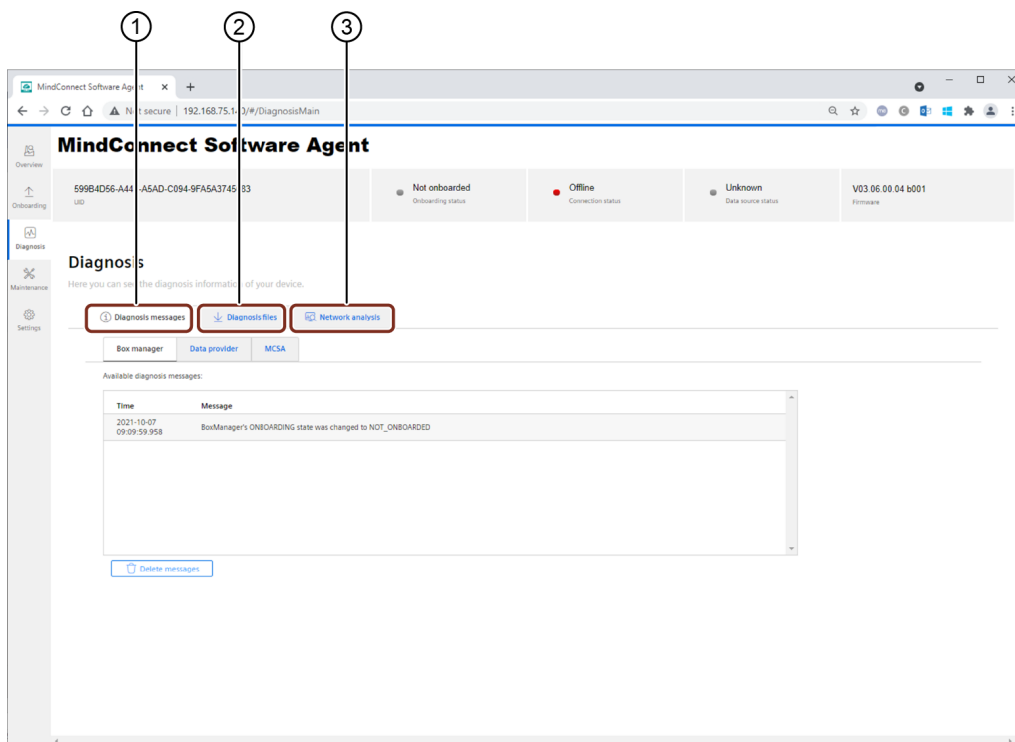
5

5.1 Diagnosing MindConnect Software Agent

The MindConnect Software Agent's web UI provides a diagnosis tab to display diagnosis messages and download diagnosis, log and system files.

Diagnosis tab

In the navigation menu, click "Diagnosis" tab to open the "Diagnosis" area. It provides following features:




- ① Diagnosis messages
- ② Diagnosis files
- ③ Network analysis


Diagnosis messages

The "Diagnosis messages" section provides a list of currently stored diagnosis messages in the web UI of the following components in separate sub-tabs:

- Box manager: Shows current states like onboarding, network connection, or data source connection states.
- Data provider: Shows diagnosis messages of Modbus TCP, Rockwell and system information data sources.

 Diagnosis messages of OPC UA and S7 data sources are currently not available.

- MCSA: Shows diagnosis information of the internal MindConnect Software Agent.

 Currently unexpected errors and file transfer settings related messages will be shown.

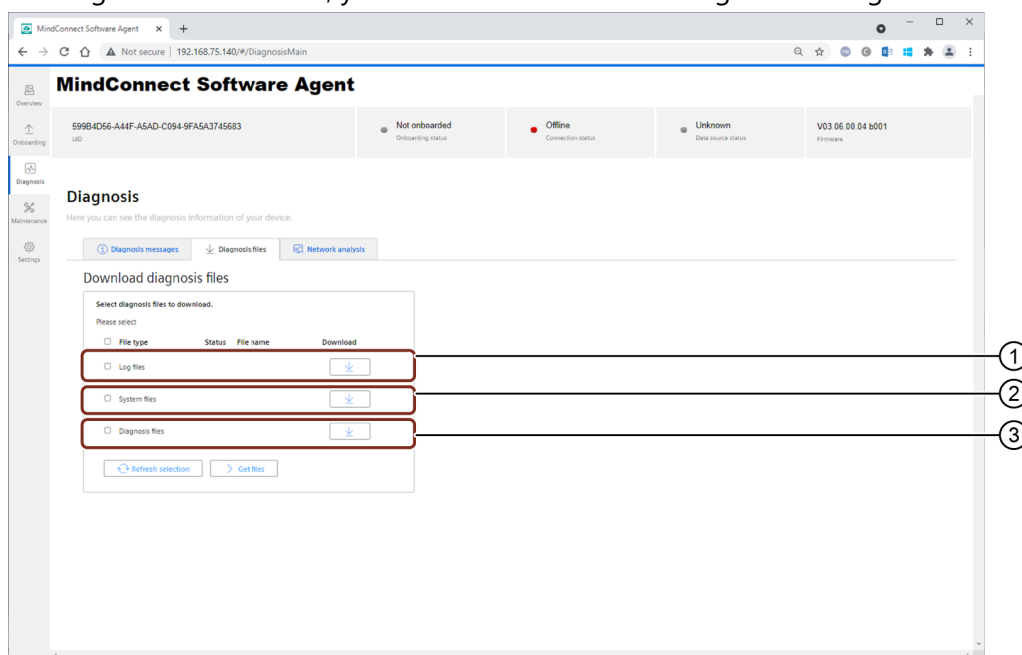
In “Diagnosis messages” section, the last diagnosis message will be displayed. You can download the previous diagnosis messages from the “Diagnosis files” section.

If the diagnosis messages section is open for a long time, the last 50 diagnosis messages will be displayed.

With the "Delete messages" button, the internal buffer of the currently visible component's diagnosis buffer will be deleted.


Diagnosis files

In “Diagnosis files” section, you can download the following kind of diagnosis files:



- ① Log files
- ② System files
- ③ Diagnostic files

To download the diagnosis files, select the checkbox. Thereafter, click "Get files" button to start the collection and preparation process. When the preparation process completed, the download buttons will be enabled, and you can the download the created diagnosis file packages by clicking download buttons.

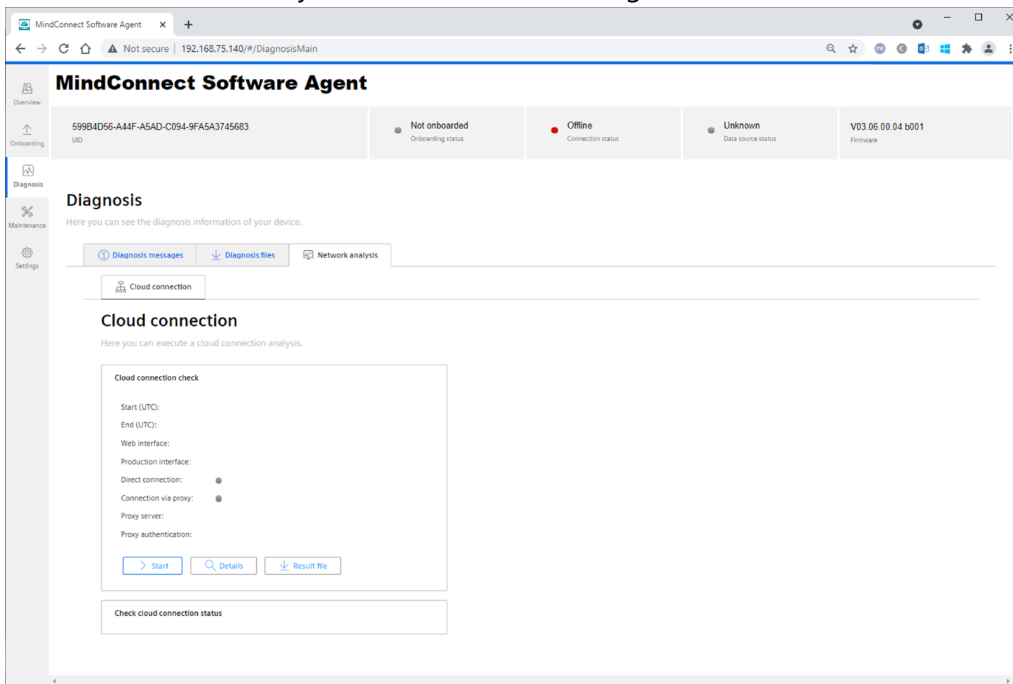


If the files are not downloaded by the browser, check the download is blocked by the browser and enable the download for MindConnect Software Agent.

Network analysis

Cloud connection check

In "Network Analysis" section, a cloud connection check can be executed to verify the connection to Industrial IoT cloud is possible. By clicking the "Start" button an automatic cloud connection check will be executed by MindConnect Software Agent.



After the test has been executed the following test results will be shown:

- Start and end time of the test in UTC format.
- Current IP addresses of web and production interfaces.
- Result of direct connection test.
- Result of connection test via proxy server if the proxy server is configured in asset manager.
- Proxy server and proxy authentication info if they are configured in asset manager.

After clicking the "Details" button the result log of the executed cloud connection check will be shown in a dialog. The result log can also be downloaded as a file by clicking the "Result file" button.

Cloud connection check status

The current status and the final status at the end of the command execution will be shown in the cloud connection check status area.



- It might be possible that the execution of the cloud connection check will take some time depending on the current network configuration.
- This feature is available with MindConnect Software Agent V03.06.00.04 b006 or higher.

Cloud connection status messages are also available in the MCSA tab in the diagnosis messages section.

5.2 Device Maintenance

The maintenance activities for the device can be performed in "Maintenance" area.

Maintenance area

In the navigation menu, click "Maintenance" tab to open the "Maintenance" area. It provides following features:

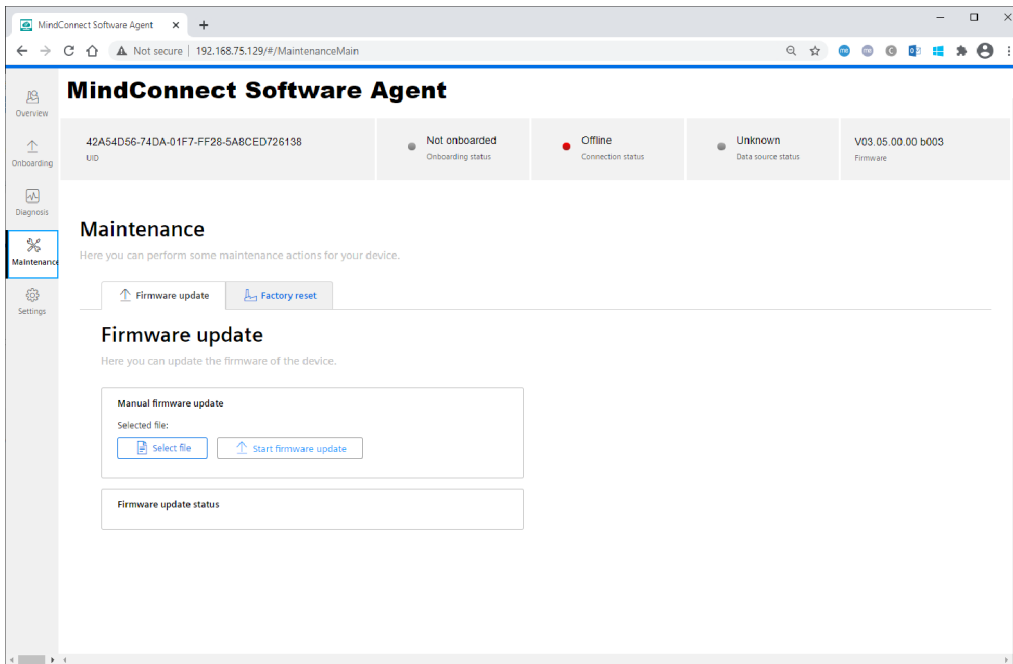
- Firmware update
- Factory reset

Firmware update

In "Firmware update" section, a new firmware version can be updated to MindConnect Software Agent.



Make sure to download the correct fw.tar file from SIOS.




Manual firmware update

To select the new fw.tar file of the new MindConnect Software Agent firmware version, click "Select file" button.

To upload the firmware update package to the device, click "Start firmware update" button to start the firmware update process.

Firmware update status

The status of the firmware update process will be displayed in the "Firmware update status" section.



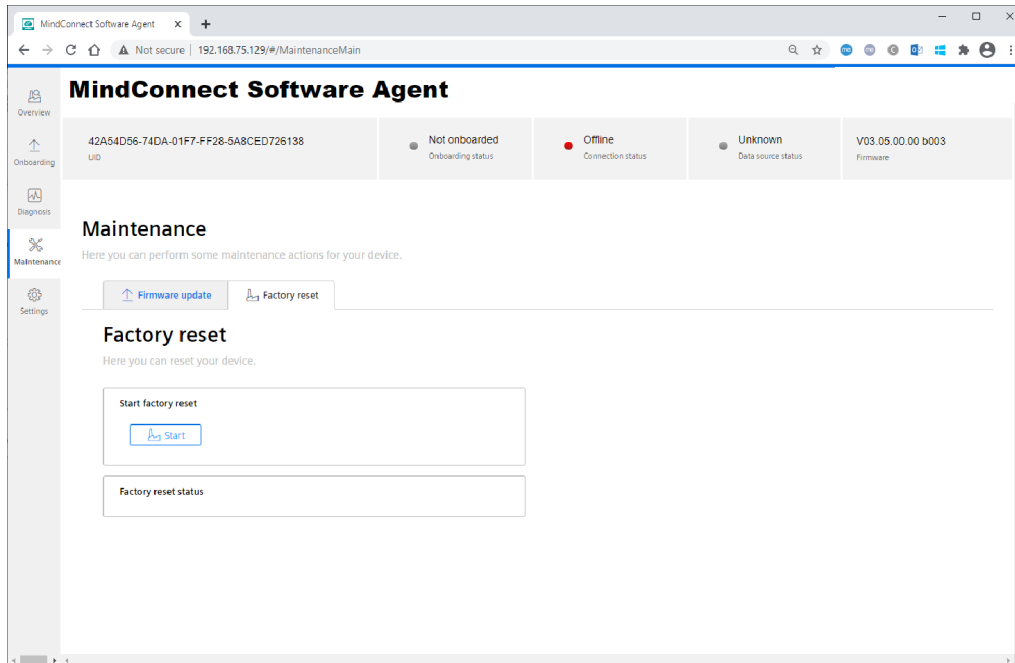
- After the new firmware version has been updated, MindConnect Software Agent system will be rebooted. It is recommended to close the current browser window or to reload the page after the reboot.
- It might be possible that the firmware update status does not switch from "started" to "succeeded" because, the reboot of the system was too fast and the UI did not get success message. Therefore, in this case the current browser window should be closed or reloaded after a couple of minutes.

Factory reset

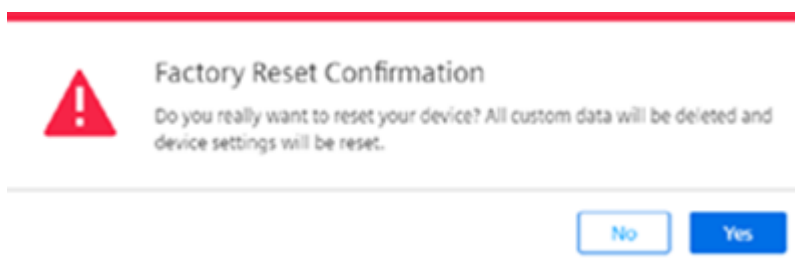
Start factory reset

In "Factory reset" section, a factory reset of MindConnect Software Agent can be performed. This will delete all customer data like collected time series data and asset data. Furthermore, the

network settings will be reset.



After clicking the "Start" button, a confirmation dialog will be shown before the factory reset will be executed.



Factory reset status

The status of the factory reset process will be displayed in the "Factory reset status" section.



- After the factory reset has been executed, MindConnect Software Agent system will be rebooted, and it is recommended to close the current browser window or to reload the page after the reboot.
- Because the network settings will also be reset, it might be possible that the device will get new IP addresses from the DHCP server. The current IP addresses can be found by opening the MindConnect Software Agent VM in Hyper-V-Manager.
- If the device is onboarded before factory reset execution, the asset needs to be offboarded in Asset Manager and the device has to be onboarded again.

5.3 Settings in MindConnect Software Agent

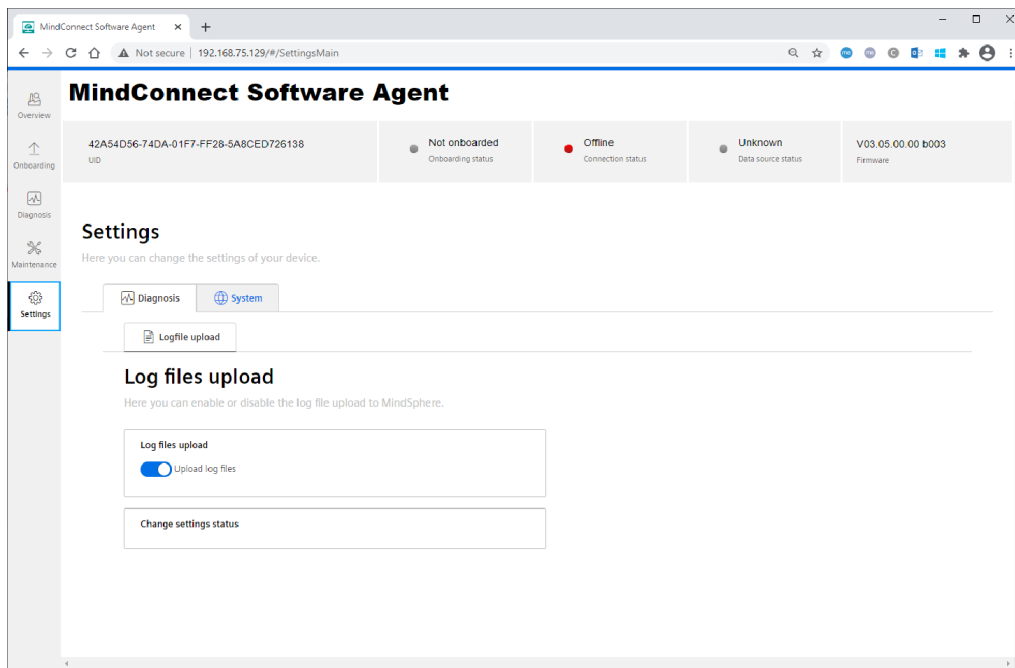
You can change the log file upload settings and system time using “Settings” area in MindConnect Software Agent.

Settings area

In the navigation menu, click "Settings" tab to open the "Settings" area. It provides following features:


- Diagnosis
- System

Diagnosis settings



Log files upload

The log files upload section displays the current status log file upload setting. To enable or disable the log file upload functionality, click the "Upload log files" toggle button.



While changing the log upload setting, it will overwrite the log upload settings of the asset’s device configuration. This change will not be synchronized with the asset’s device configuration.

Change settings status

The status of changing the log files upload settings process is displayed in the "Change settings status" section.

Diagnostic settings

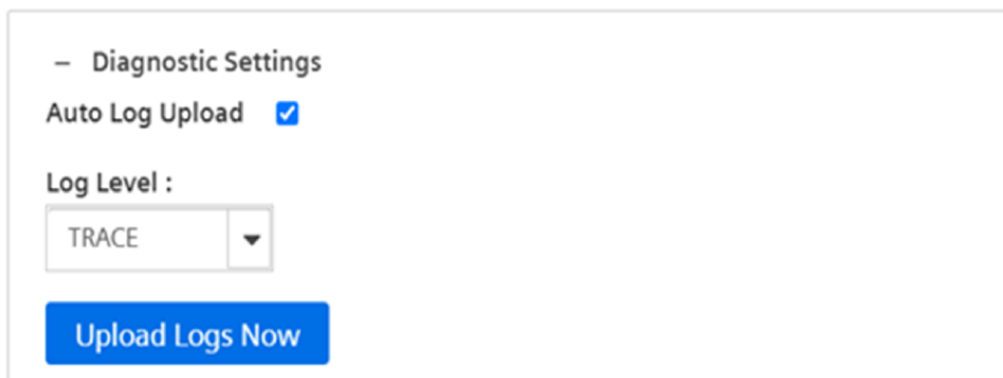
This section has the configurations related with diagnostics setting such as level of logging.

Log Level

MindConnect Software Agent log level can be set from diagnostic configuration. The five different values of log levels are

- TRACE
- DEBUG
- INFO
- WARNING
- ERROR.

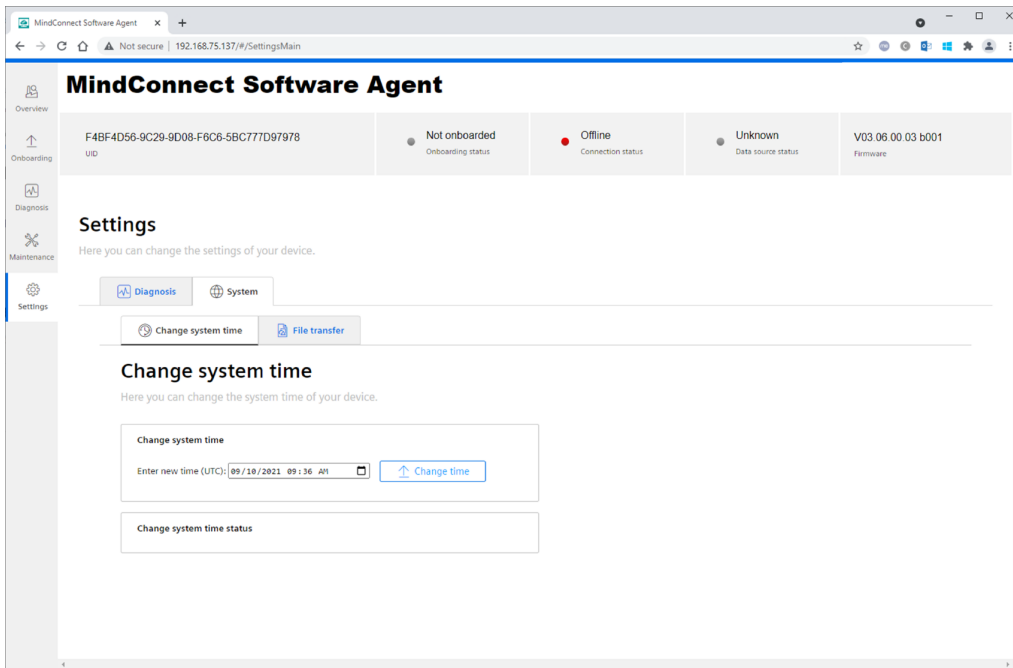
The behaviour of the logging on the device will be included to the selected level and the upper log levels only. The lower log levels will not be logged.



Log Upload


Log upload: It means, the device is going to upload logs generated to Insights Hub. The log upload on the device is enabled by default and it is possible to disable this feature. "Upload Logs Now" triggers the upload of the device log files immediately. This feature triggers the log upload regardless of the auto log upload status.

System settings



Change system time

In “Change system time” section, the current Windows host system time will be displayed in UTC format. A new system time can be updated using the time edit field. To start the change system time process, click "Change time" button.

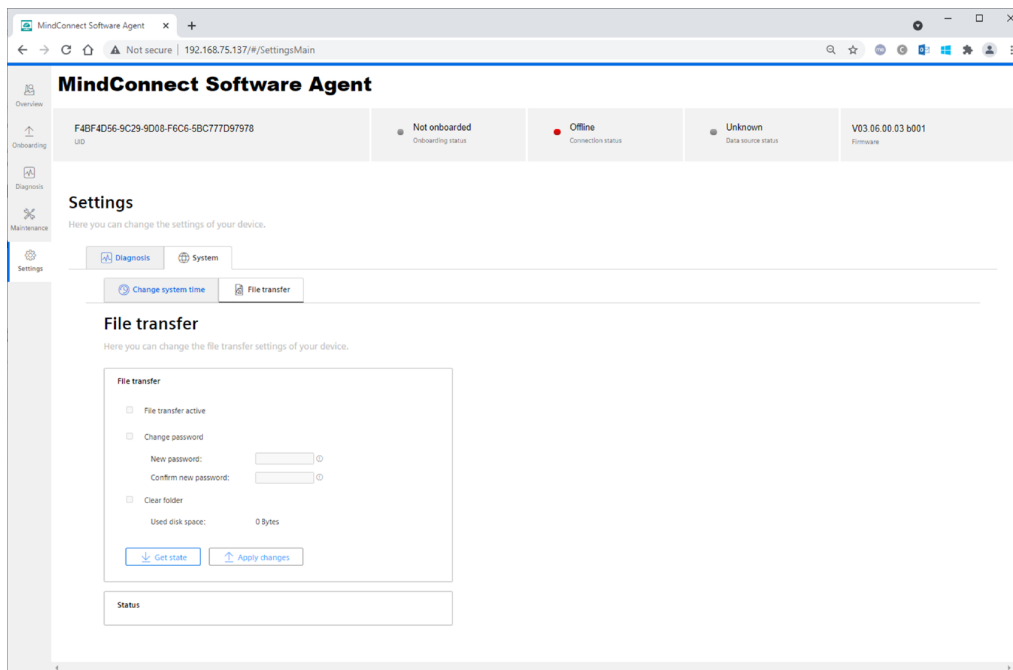


- It is recommended to use Google Chrome for changing the system time, so that the new time can be updated by using date and time picker which is not supported by all browsers (e.g. Firefox).
- If you change the system time, this may lead to some abrupt behavior on the data ingested.

Change system time status

The status of changing the system time process is displayed in the "Change system time status" section.

Drop a file copy for File transfer



In "File transfer" section, click "Get state" button to get the current state of the file transfer service. In this section, following actions can be executed:

- Functionality to transfer files to Insights Hub can be enabled or disabled.
- Password can be changed.
- Shared "filetransfer" folder can be cleaned up manually.

Click "Apply changes" button to execute selected actions.



File transfer functionality is available from the version MindConnect Software Agent V03.06.00.03 b001.

Service enablement

- File transfer service can be enabled or disabled by checking or unchecking the "File transfer active" check-box.
- By default, this feature is disabled and needs to be enabled first before it can be used.
- First enablement will take some time because further components will be installed on the system.



- Before disabling the file transfer service, it is recommended to disconnect all network mappings to the shared "filetransfer" folder.
- File transfer service needs to be enabled and re-configured after the firmware update, if it had been configured before.
- It is recommended to drop a file to Integrated Data Lake(IDL) in case the agent is online.

Prerequisites

During first enablement of file transfer feature, it is necessary that following URLs can be accessed:

- [Debian](#)
- [Debian Security](#)

Changing password

To access MindConnect Software Agent shared folder, it is necessary to provide a password. Afterwards, the shared "filetransfer" folder can be mapped as a network drive. For example, using MindConnect Software Agent's IP address and the user "Insights Hub" and the provided password as credentials.

Example: \\192.168.0.47\filetransfer

Clean folder

If some files cannot be transferred to the upload folder, it is important to clean the shared "filetransfer" folder manually.

File transfer status

- While getting current file transfer state or changing file transfer configuration the current process and execution result will be shown in the file transfer status section.
- Furthermore, these execution results will also be available in the MCSA tab on the diagnosis messages pane.

Transferring files to Industrial IoT

After mapping the shared "File transfer" folder, you can copy the files from the local system to the mapped network drive. These files are required to be moved to internal upload folders immediately because the mapped network drive is not allowed to use as a file storage.

There will be two sub-folders in the shared "File transfer" folder so that the files can be uploaded to different targets on Industrial IoT starting from MCSA V03.06.00.13 b004:

- fs
 - Files will be uploaded to file storage (fs).
 - Maximum file size: 10MB
- idl
 - Files will be uploaded to Integrated Data Lake(IDL).
 - Maximum file size: 200MB



- The shared "File transfer" folder size has a limit of 600MB (starting from MCSA V03.06.00.13 b004).
- The files are being automatically deleted to prevent the exceeding supported file size limit with unnecessary use of disk space in the shared "File transfer" sub-folder.
- Files directly located in the shared "File transfer" folder will not be uploaded or deleted automatically, but they can be deleted manually using "Clean folder" functionality mentioned above (starting from MCSA V03.06.00.13 b004 or later).

Drop a file copy to Integrated Data Lake (IDL)

- In IDL, you can upload the files/objects and add the related metadata to the files/objects. IDL file names must be in the character set '[a-zA-Z0-9.!*'() _-/=]'. For more information about IDL, see [Integrated Data Lake](#) documentation.

Metadata file name should contain metadata in lowercase prefix, for example `object_metadata.json`. Metadata file extension should be `.json`. Metadata and JSON file needs

- to be uploaded together.

Metadata of the associated file/object is uploaded by the "objectName" field in the `.json`

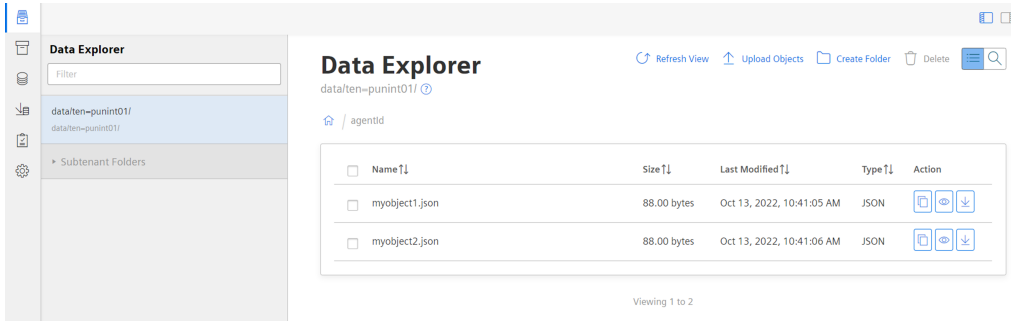
- content. If this field is missing, metadata of the file/object will not be uploaded.
- Example metadata format:

```
{
  "tags": [
    "tag1",
    "tag2",
    "tag3"
  ],
```


```
"objectName": "object.objecttext"  
}
```

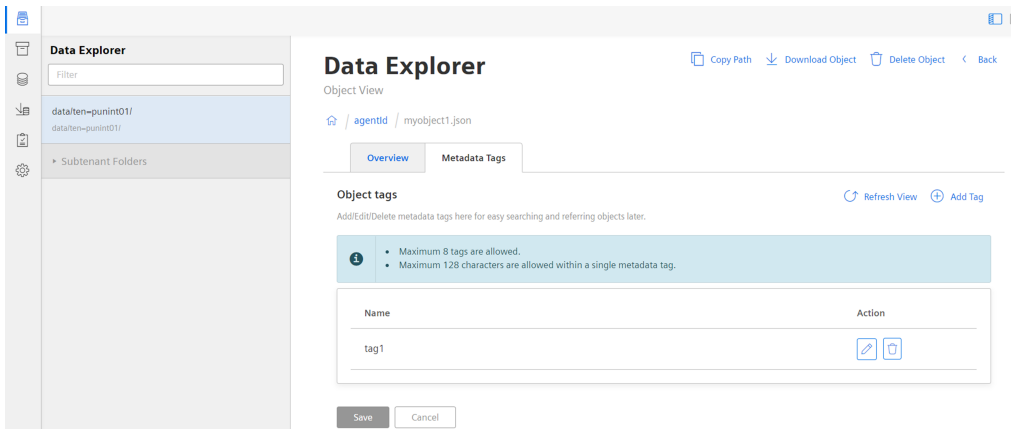
In IDL Manager UI, files/objects will be uploaded as /agentId/objectName, so files can

- be uploaded under this folder. No other sub-folders will be created.



- Files/Objects with metadata will be uploaded to IDL as specified in the .json content. Click


 to display the file/object details and added metadata.




- If a new file is uploaded with the same name that already exists in IDL, then it will overwrite the existing file.


5.4 Firmware update in Asset Manager for MindConnect Software Agent

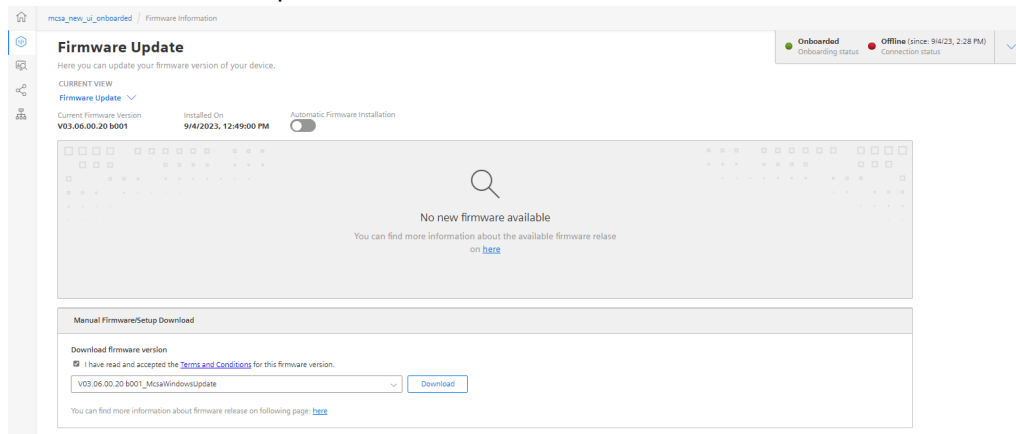
In Asset Manager, you can update the firmware of your MindConnect Element.

 **Outdated version**
Please keep your firmware always updated.

 **Data loss**
Please note that data loss can occur during the time of the firmware update. The amount of data loss depends on the reading and uploading cycle.

To perform a firmware update, follow these steps:

1. Select the asset in the "Asset" tab.
2. Open the MindConnect Software agent plugin.
3. Click next to "Firmware" on the button .
4. Navigate to "Firmware Update" view in the MindConnect Software Agent overview page.
5. Select the available product version and click "Download" and Install the firmware update.



Incomplete firmware update

If the connection is interrupted while the new firmware is being downloaded, note that the downloaded content might be lost if the connection cannot be recovered via the box. For example, if the connection is interrupted while 50% of the firmware are downloaded, the process might be canceled. In that case you have to click firmware update on the user interface to restart the process. It is still possible to do manual firmware updates via Local Web server. To update the firmware via Local Web server URL, see [Device Maintenance](#)

Canceling an Online Firmware update

If the firmware update process is triggered from UI then the cancel button will be activated. By clicking "Cancel Firmware Update" the ongoing operation will be interrupted and cancelled.



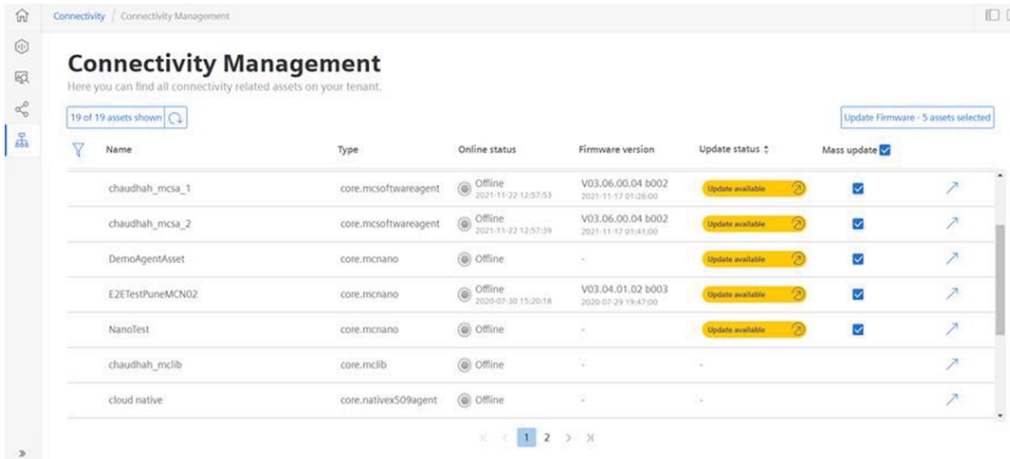
The firmware update operation can take longer time depending on the network quality.

Once the cancellation operation successful, it is possible to re-trigger the online firmware update by clicking "Update Firmware".

Firmware updates for multiple devices

In Asset Manager under "Connectivity Management" tab, you can trigger firmware updates for multiple devices using "Mass update" selection. This allows you to update the selected firmware devices like, MindConnect Software Agent.

To update the firmware for multiple devices, select assets in the "Connectivity Management" tab under "Mass Update" and click "Update Firmware".



5.5 Automatic firmware update of MindConnect Software Agent

In Asset Manager, the firmware of your MindConnect Software Agent is updated by both manually and automatically. If the auto firmware update option is enabled, MindConnect Software Agent is automatically updated with the new version when it is released.



- If the system is already updated with a new version available for the device and the auto firmware update option is enabled later, MindConnect Software Agent will be not triggered to update the previous released version. Auto firmware update will work only for further releases.
- If the auto firmware update is enabled, manual firmware update operation is not allowed.
- If the firmware update job is in progress triggered by the auto firmware update, then "Cancel" button will be activated. By clicking "Cancel" button, the ongoing operation will be interrupted and cancelled. If an auto firmware update trigger is cancelled, it will not be triggered again for the same firmware release.

To perform auto firmware update, follow these steps:

1. Select the asset in the "Asset" tab.
2. Open the MindConnect plugin.
3. In the firmware update view, enable "Automatic Firmware Installation".
4. Accept the terms and conditions and click "Update".

Firmware Update

Here you can update your firmware version of your device.

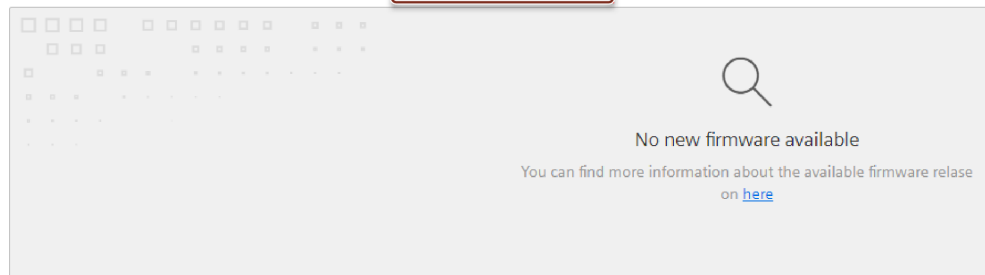
CURRENT VIEW

Firmware Update ▾

Current Firmware Version
V03.06.00.20 b001

Installed On
9/4/2023, 12:49:00 PM

Automatic Firmware Installation



Manual Firmware/Setup Download

Download firmware version

I have read and accepted the [Terms and Conditions](#) for this firmware version.

V03.06.00.20 b001_McsaWindowsUpdate ▾

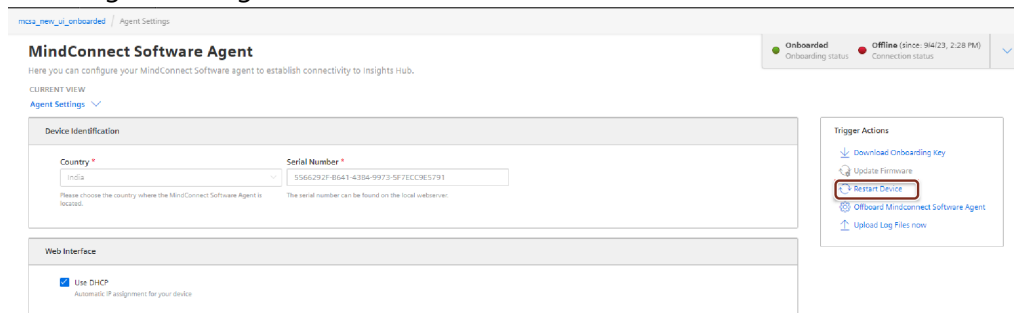
Download

You can find more information about firmware release on following page: [here](#)

5.6 Remote restart for MindConnect Software Agent

By using the remote restart function in the MindConnect Element Plugin, you can restart your device without having to use the on / off button on the device. This makes it easier to restart boxes that are difficult to reach.


If an active restart process is in progress, no further process can be created in the user interface. The following picture shows the restart device button in the MindConnect Element plugin screen in the Agent settings window.



5.7 Send commands for MindConnect Software Agent

The commanding functionality provides you to send data directly from cloud applications and from Insights Hub applications to your devices. The first example of this functionality was remote restart. The send command functionality is extended to cover writing data to the field via S7 and OPC UA plugins and is also supported for advanced driver protocols IEC61850, S7+ and Sinumerik. It is possible to write data in the following data types:

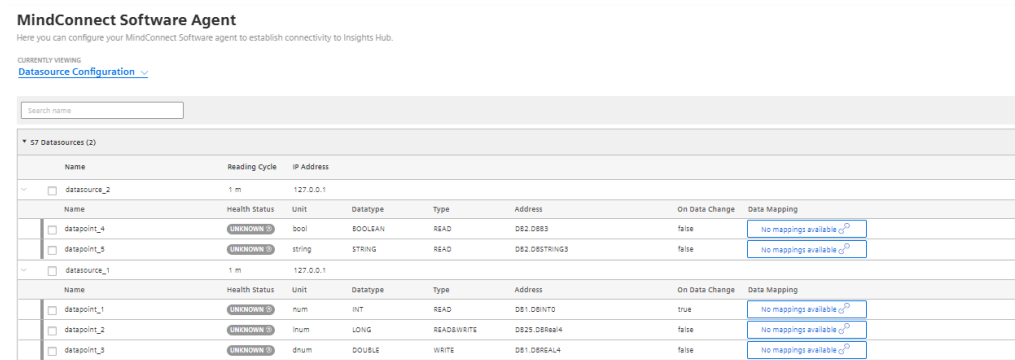
- Integer
- Long
- Double
- Boolean
- Float
- String (OPC UA only)

 **It is important to know the limitations of your devices, before you set a specific value for a datapoint.**

- Failure to check value ranges within your controllers may result in damages to your devices. We recommend to set and verify limits within your local program to block values out of device limits.
- If there is an ongoing command for the datapoint, the user will not be allowed to create a new one until the ongoing specific datapoint is finalized.

User interface

The following screen shows the data source configuration screen:



The “Type” column represents “Data Acquisition Mode” type and provides the following values:

Value	Description
Read	Within this type you can only collect data.
Write	Within this type you can only send data.

Value	Description
Read&Write	Within this type you can collect and send data.

The "Send a value" button is only visible on writeable data point types. This creates a command instance on cloud platform on Edge area for execution.

Commanding Device via API

In order to command the device, there are 3 critical id's that needs to be get from the system. Those id's are deviceId, datasourceId and datapointId. To get the ID's, follow these steps:

Getting deviceId

You can "GET" the "id" of your device using the "id" of your asset with a below request.
/api/devicemanagement/v3/devices?assetId={id} In the response, device id will be displayed. For more information, [Device Management Service](#) see documentation.

Getting datasourceId and datapointId

In the second step, we need to make a request to mindconnectdevicemanagment service to "GET" the id of the datasource and the datapoint.

/api/mindconnectdevicemanagement/v3/devices/{assetId}/dataConfig

In the response of this request the id's will be displayed and should be exdtracted for the final api call. Below is the response for the above request. The "id" field in dataSource item represents the datasourceId and the dataPointId represents the "id" of the datapoint.

```
{
  "id": "392fe515-5b61-439d-814d-b37b9fa7ef7b",
  "agentId": "25137086d6c141b682d9fcb135c8168e",
  "uploadCycle": "10",
  "configurationId": "1650623649731",
  "dataSources": [
    {
      "id": "326340f5-88c6-409a-a5d9-03e95ce7af94",
      "name": "WindTurbine",
      "description": "datasource_description",
      "protocol": "S7",
      "readCycleInSeconds": "60",
      "protocolData": {
        "ipAddress": "192.168.1.1",
        "manualRackAndSlot": "Automatic",
        "rackNumber": "0",
        "slotNumber": "2"
      }
    },
  ],
}
```

```

    "dataPoints": [
      {
        "id": "6efc38d1-b4e7-4e6e-98ce-cb6b3b3f36b2",
        "dataPointId": "36cd56f91c154",
        "name": "Energy",
        "description": "description",
        "unit": "kw",
        "dataType": "DOUBLE",
        "dataPointData": {
          "address": "DB1.DBD1",
          "hysteresis": "0",
          "onDataChanged": false,
          "acquisitionType": "READ"
        }
      }
    ]
  }
}

```

The final api call is to deploymentworkflow service. For more information, see [Deployment Workflow Service](#). A "POST" request to the below endpoint should be made, `/api/deploymentworkflow/v3/instances`

The body of the request should be, as below example:

```

{
  "deviceId": "f5168f95-2cc6-4a2c-b598-bfd5dadfc4df",
  "model": {
    "key": "mdsp-core-commandDispatcher"
  },
  "data": {
    "type": "datapoint-write",
    "createdBy": "user@siemens.com",
    "version": "v1.0",
    "to": "some_protocol",
    "payload": {
      "desiredValue": "7",
      "dataSourceId": "10d9c36c-69f7-4c33-8624-f67537e142a4",
      "dataPointId": "b932b9da42f04",
      "protocol": "some_protocol"
    }
  }
}

```

In the below list, there are some fields which require certain data only:

Field Name	Allowed Values
to	OPCUA, S7, IEC61850, S7PLUS, SINUMERIK
protocol	OPCUA, S7, IEC61850, S7PLUS, SINUMERIK
version	v1.0
type	datapoint-write
key	mdsp-core-commandDispatcher

The following list shows the details of the commanding functionality:

- If command operation fails, then the box will set the state of the job to "FAILED" indicating some more details in the message column of the command itself. On the other hand, the state of the job will be "EXECUTED", if the command operation succeeded. These updated states can be checked via Deployment Workflow's endpoint GET /instances too.
- The commanding operations are executed in a chronological order, starting first from the oldest to the newest. The execution of those commands is synchronized with the configuration updates to avoid inconsistencies between the device side content and cloud side content.
 - In order to keep the device configuration content up to date with the backend side do not forget to click the "Apply changes" button. Otherwise, some of your commands will get rejected by the device side, for example a command is sent for a "READ" typed datapoint.
- Boolean type is only working strictly for 'true' and 'false' values.

5.8 Using MindConnect Software Agent's Hyper-V VM

This chapter will give some information about MindConnect Software Agent's Hyper-V VM and how to use it in Windows Hyper-V-Manager.

Opening the VM

To open MindConnect-SoftwareAgent VM , start Windows Hyper-V-Manager and connect MindConnect-SoftwareAgent VM.

Autostart

MindConnect Software Agent's VM will be configured during installation process and automatically restarts after the restart of Windows host.

System restart

In Windows Hyper-V Manager, restart the MindConnect Software Agent manually. To restart the VM, click the following button:



System shutdown

In Windows Hyper-V Manager, shut down the MindConnect Software Agent manually. To shut down the VM, click the following button:



Troubleshooting

Black screen is shown

If the system is running for a while with a black screen, click into the VM or press any key to view system information.

System gets stuck during start-up

If the system is stuck after starting the Hyper-V VM, restart the VM as described above.

MindConnect Software Agent's VM is shut down, before the restart of Windows host

If MindConnect Software Agent's VM is shut down before the restart of Windows host, then the VM must be started manually again.

5.9 Managing or maintaining the virtual machines or instances

MindConnect Software Agent can manage and maintain the multiple virtual machines or instances by using the setup program manually or via Windows "Control Panel" → "Programs and Features".

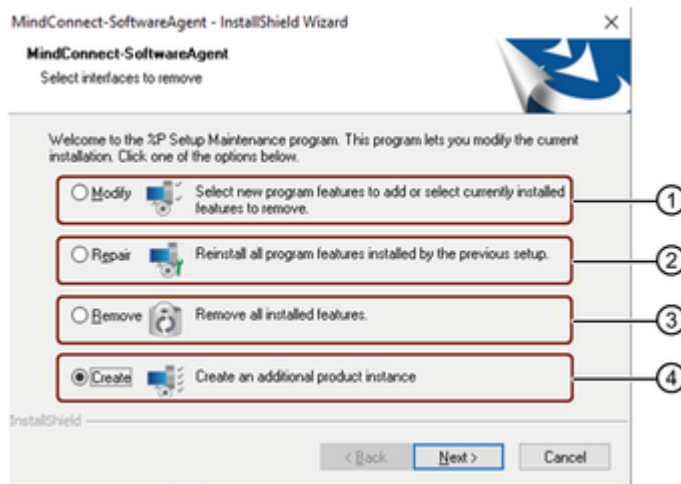


Installation of multiple MindConnect Software Agent instances is supported from the version MCSA V03.05.00.03 b005.

Procedure to create multiple virtual machines or instances

To create the multiple instances in MindConnect Software Agent, follow these steps:

1. Open "setup.exe" file, click "Yes" to make the changes to the device.
2. In "Maintenance" dialog, select "Create" and then click "Next":



- ① Modifies the existing feature or instance
 - ② Reinstalls all program features installed by the previous setup
 - ③ Uninstalls or removes all the installed feature or the selected instance
 - ④ Creates a additional product instance
3. Select the network interfaces and click "Next".



- The setup will create external Hyper-V switches for MindConnect Software Agent to get its own IP address in the network and can be reached from outside of the Windows PC/IPC.
- The setup automatically detects the available network adapters and attempts to make a suitable pre-selection if it finds network adapters with X1 and X2 in their names (which should be the case on SIMATIC IPCs).
- If only one network adapter is available in PC, select a network adapter for the web interface only.

4. Select "Custom" setup type to install (recommended) and click "Next".

5. Configure the virtual machine settings and click "Next".

For the virtual machine settings, see [Onboarding and installing MindConnect Software Agent in Windows](#).

6. Change "Destination Folder", if required and click "Next".

7. Review the settings and click "Next".

8. Click "Install".
9. After the installation, restart your PC.

Result

The second instance is successfully installed.

Procedure to modify multiple virtual machines or instances

A MindConnect Software Agent virtual machine can be modified by starting the setup program manually or via Windows "Control Panel" → "Programs and Features".



Multi instances

- Only one instance can be modified at a time. If you want to modify another MindConnect Software Agent instance setup must be started again.
- Instances which are stopped are started again during setup or modifying the other instances.

To modify the multiple instances in MindConnect Software Agent, follow these steps:

1. Open "setup.exe" file, click "Yes" to make the changes to the device.
2. In "Maintenance program", select "Modify" and click "Next".
3. Select the installed virtual machine (VM) to be modified from the list and click "Next".
4. Select the generated virtual switches to be modified and click "Next".
5. Configure the virtual machine settings and click "Next".
6. Click "Finish" to modify the virtual machine in MindConnect Software Agent.

Result

The selected virtual machine instance is successfully modified.

Procedure to repair multiple virtual machines or instances

A MindConnect Software Agent virtual machine can be repaired by starting the setup program manually or via Windows "Control Panel" → "Programs and Features".



Multi instances

- Only one instance can be repaired at a time! If you want to repair another MindConnect Software Agent instance setup must be started again.
- During the repair process, the selected MindConnect Software Agent instance's virtual machine will be configured using the settings which had been applied during its installation process. Furthermore, the virtual hard disk will be replaced by the original hard disk i.e., all customer data and settings will be lost and MindConnect Software Agent instance needs to be onboarded again.

To repair the multiple instances in MindConnect Software Agent, follow these steps:

1. Open "setup.exe" file, click "Yes" to make the changes to the device.
2. In "Maintenance program", select "Repair" and click "Next".
3. Select the installed virtual machine (VM) to be modified from the list click "Next".
4. Select the generated virtual switches to be modified and click "Next".
5. Configure the virtual machine settings and click "Next".
6. Click "Finish" to modify the virtual machine in MindConnect Software Agent.

Result

The selected virtual machine instance is successfully repaired.

Procedure to removing multiple virtual machines or instances

A MindConnect Software Agent virtual machine can be removed by using setup program manually or via Windows "Control Panel" → "Programs and Features".



Multi instances

Only one instance can be deleted at a time. If you want to delete the "MindConnect Software Agent " completely, then every single instance must be deleted. The last instance will delete the complete folder structure.

To remove or uninstall MindConnect Software Agent, follow these steps:

1. Open "setup.exe" file, click "Yes" to make the changes to the device.
2. In "Maintenance program", select "Remove" and click "Next".
3. Click "Yes" to confirm and remove the installed virtual machines (VM's).

4. Select the generated virtual switches to be removed and click "Next".



If the virtual switches are still needed, click "Next" without selecting a virtual switch.

5. Select the list of all installed virtual machines (VM's) to be removed and click "Next". 6. Click "Finish" to remove the virtual machines (VM's) completely from the PC.

Result

The virtual machines (VM's) is successfully removed or uninstalled.

5.10 Configuring MindConnect Software Agent in Docker

The MCSA configuration will be automatically started during MCSA installation, but it can also be started manually by executing the "mcsa-config.sh" script with admin privileges in the MCSA installation folder.



It is mandatory to execute the MCSA installation with root privileges

- Either, directly as root, or
- By getting root rights using "su" command.
- "mcsa-config.sh" can be started using "sudo" command to execute it with root rights. If the configuration script is not started as root, a message will be shown to start as root and the script will be terminated. It is also necessary to start "mcsa-config.sh" script directly in the MCSA installation folder to make sure that the internally used files will be available during script execution.

MCSA configuration

After the installation, select the network adapters of the host system which are used by the MCSA containers as web and production interfaces, if the MCSA configuration is started for the first time.

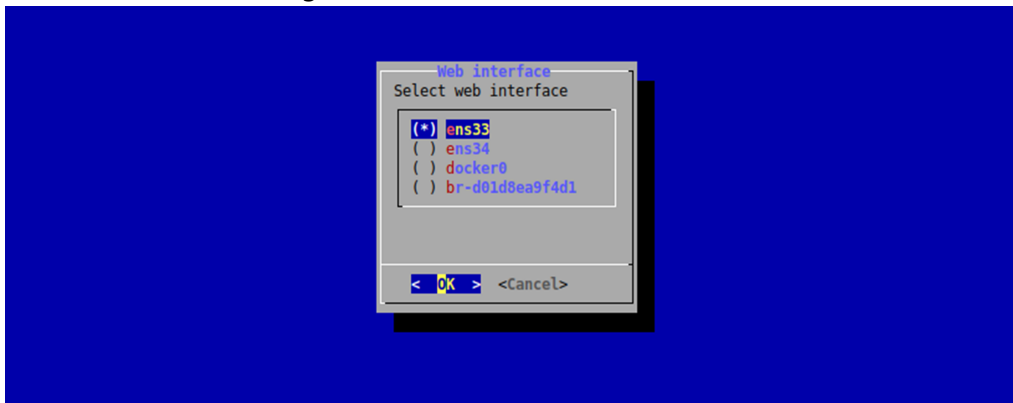
These settings are necessary for the static network settings need to be applied via asset manager UI.



- Be aware that MCSA containers directly use the Linux host's network interfaces and selecting web and production interfaces is only necessary for applying network interface settings via device configuration in asset manager.
- If the Linux host is having further network interfaces, it might be possible that MCSA Docker containers will communicate with Industrial IoT and the data sources using these network interfaces.
- Therefore, it is recommended that only the host's network interface, which is selected as web interface provided with internet access.

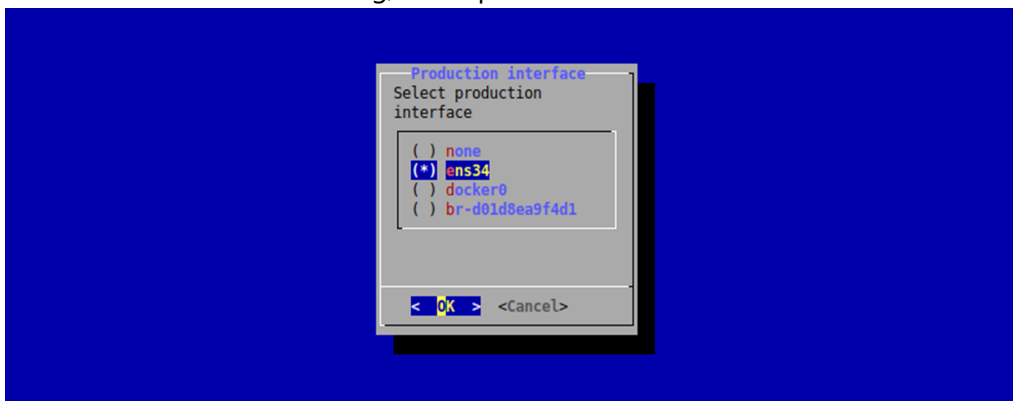
To configure the MCSA in Docker, follow these steps:

1. In Web interface dialog, select web interface and click "OK".



It is mandatory to select Web interface.

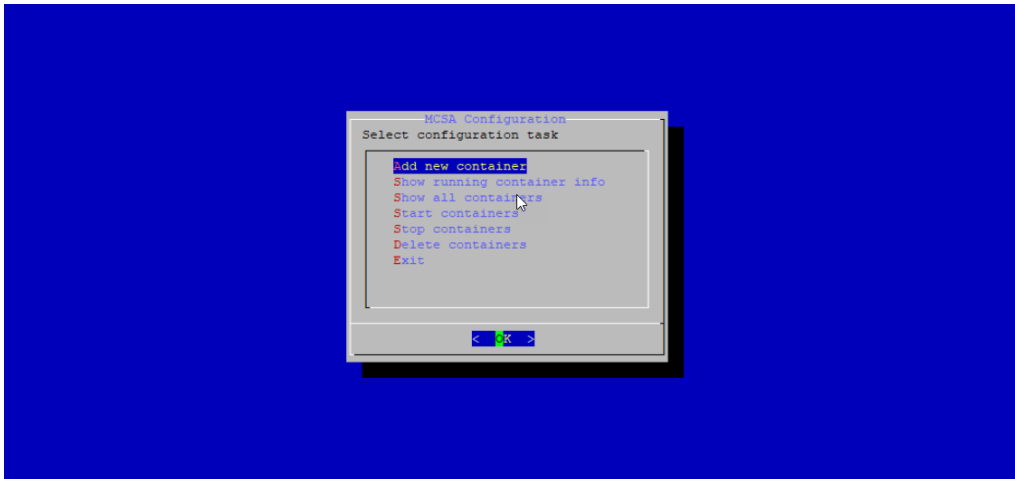
2. In Production interface dialog, select production interface and click "OK".



MCSA configuration main menu

The MCSA configuration will display a menu to perform following tasks:

- Add new MCSA Docker container.
- Show information of running MCSA Docker containers.
- Show status of all MCSA Docker containers¹⁾.
- Start exited/stopped MCSA Docker containers.
- Stop up/started MCSA Docker containers.
- Delete MCSA Docker containers.
- Exit



You can select a task by using "Up/Down" keys and pressing "Enter" key and you can close the main menu by selecting "Exit" task.



- On slower systems, it is possible when switching between different dialogs a blank black screen is displayed while system data is being collected.
- ¹⁾ : Available since MCSA in Docker V03.06.02.06 b002, or later.

Add new MCSA Docker container

For adding a new MCSA Docker container, provide the following values:

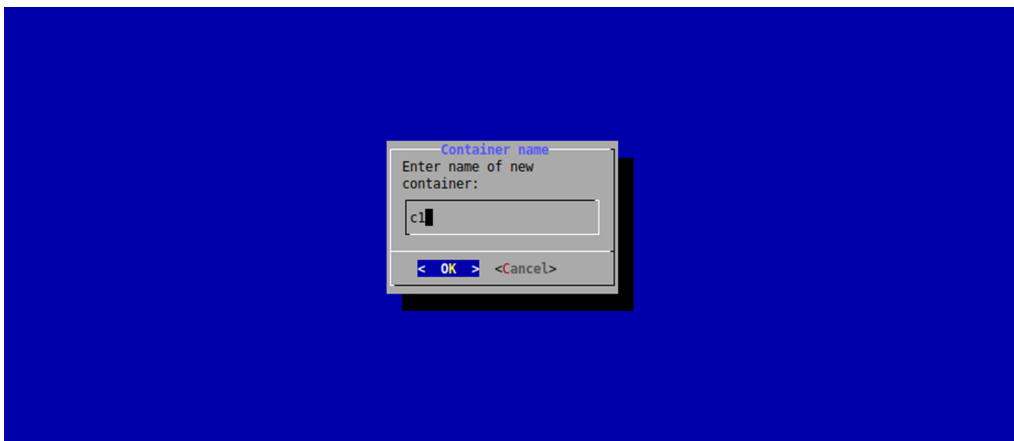
- Container name
- HTTP port
- MQTT port
- WinCC OA PMON port
- WinCC OA data port
- WinCC OA event port
- WinCC OA SNMP port

- CodeMeter port
- File transfer folder

TCP Ports

- Providing unique TCP ports for every MCSA Docker container is necessary because MCSA Docker containers run in host network mode of Docker.
- Therefore, after entering the TCP port number value it will be checked, if the port is already in use on the system.
- Although it is checked, if the entered port number is already in use, it is recommended to check the currently used ports of the already existing MCSA Docker containers beforehand, because it might be possible that the already used port is currently not active and therefore, it is not detected automatically.
- TCP port numbers should be entered in the allowed range (1 ... 65535).
- Because many ports are already standardized and used by other applications and protocols, port numbers in the upper number range is considered to be used.
- Information about already used and allowed port numbers can be found on following page: [List of TCP and UDP](#) port numbers.

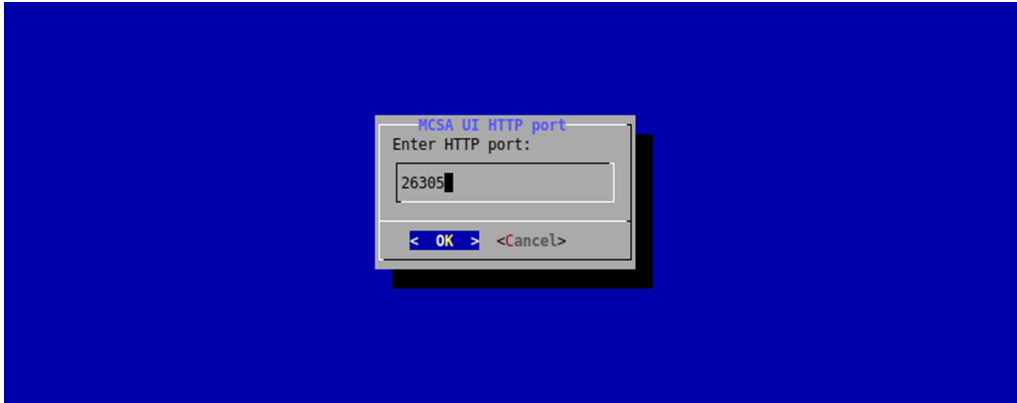
Container name



During creation of the MCSA Docker container an "mcsa_1" postfix will be added to the name of the container automatically (example: c1_mcsa_1), it is not necessary to add "mcsa" to the name in this dialog.

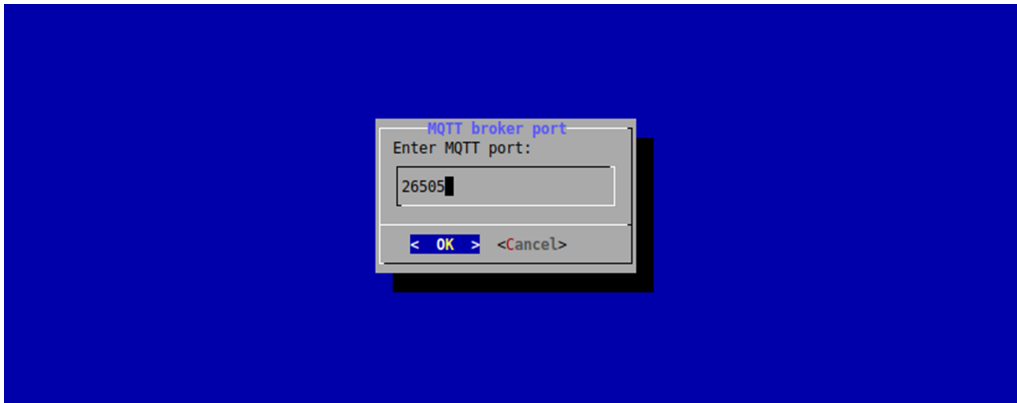
HTTP port

MCSA Docker containers are running in host network mode, it is mandatory to define a system unique TCP port which will be used to access the local web server in the Docker container.



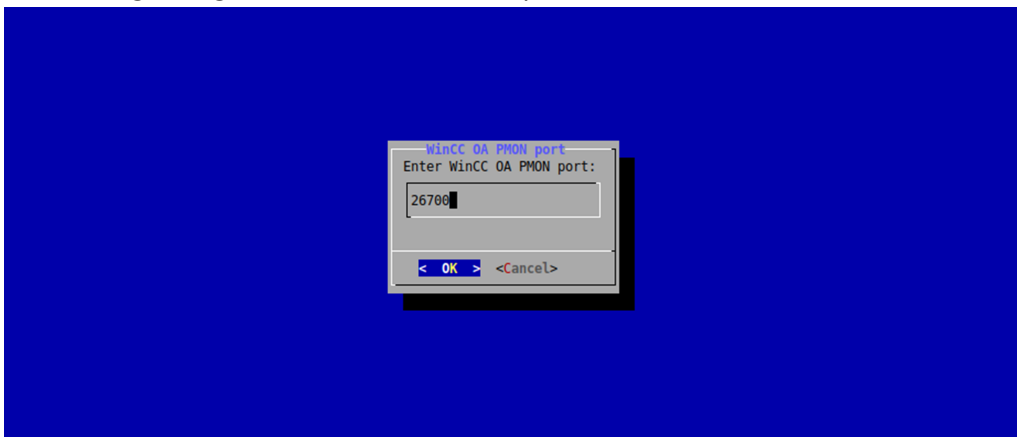
MQTT port

It is also necessary to define a unique MQTT port for every MCSA Docker container.



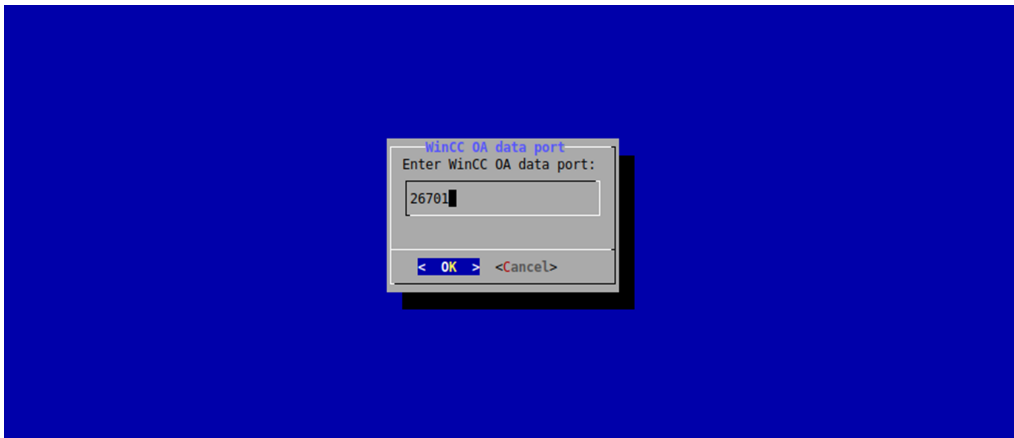
WinCC OA PMON port

In following dialog, the WinCC OA PMON port can be entered:



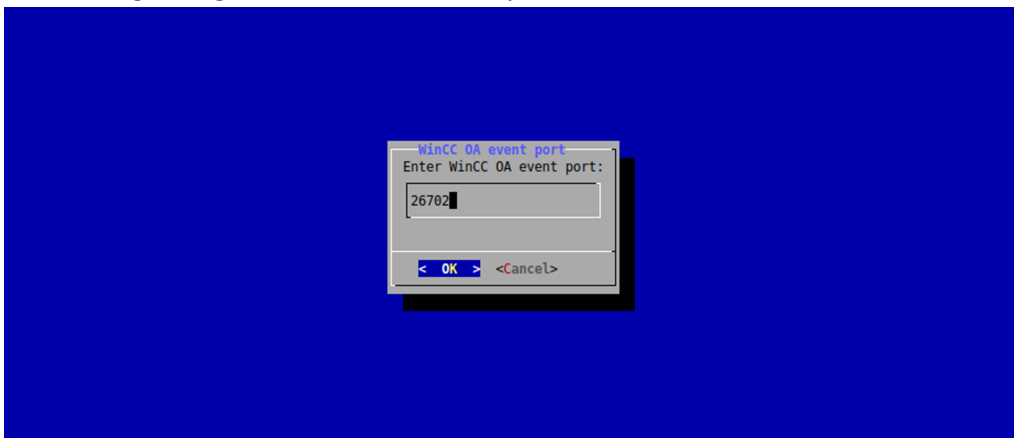
WinCC OA data port

In following dialog, the WinCC OA data port can be entered:



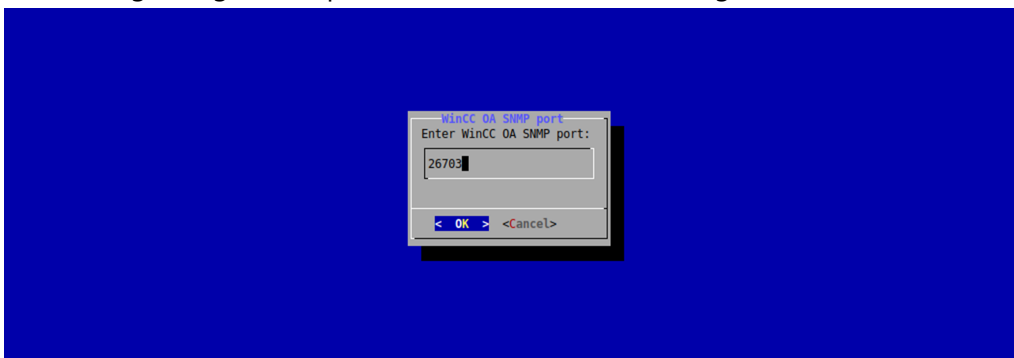
WinCC OA event port

In following dialog, the WinCC OA event port can be entered:



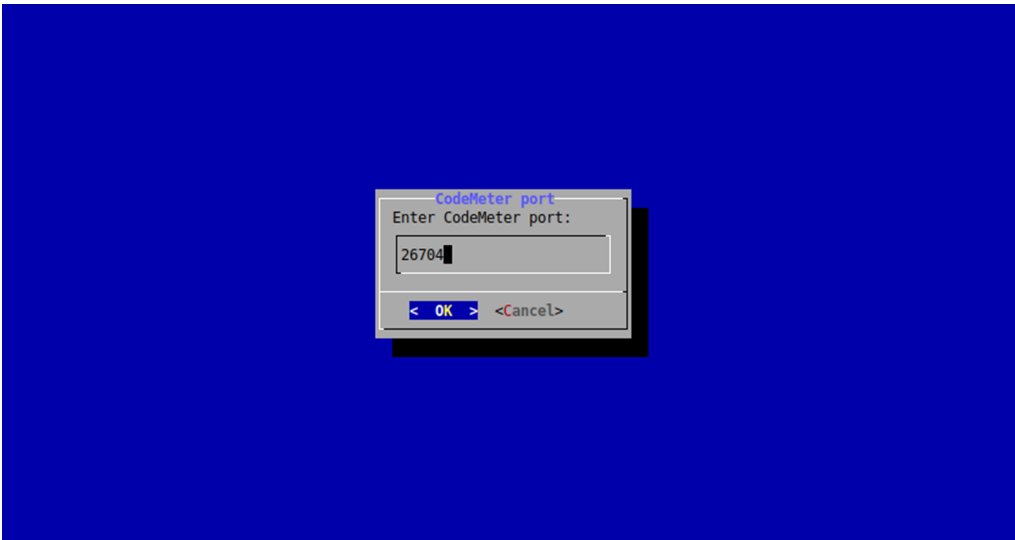
WinCC OA SNMP port

In following dialog, SNMP port for WinCC OA can be configured:



CodeMeter port

In following dialog, CodeMeter port can be entered:



- CodeMeter port is required to use advanced drivers in multiple MCSA Docker containers in parallel.
- To use advanced drivers in these MCSA Docker containers, delete the existing MCSA Docker containers and re-create to assign the CodeMeter port.

File transfer folder

File transfer is supported starting from MCSA in Docker V03.06.02.07 b001 and V03.06.20.01 b001. To transfer files a local folder of the Linux host should be specified. Following folder will be used by default.

- /opt/siemens/mindconnect/mcsa-filetransfer/

Example folder,

- /opt/siemens/mindconnect/mcsa-filetransfer/c1_mcsa_1



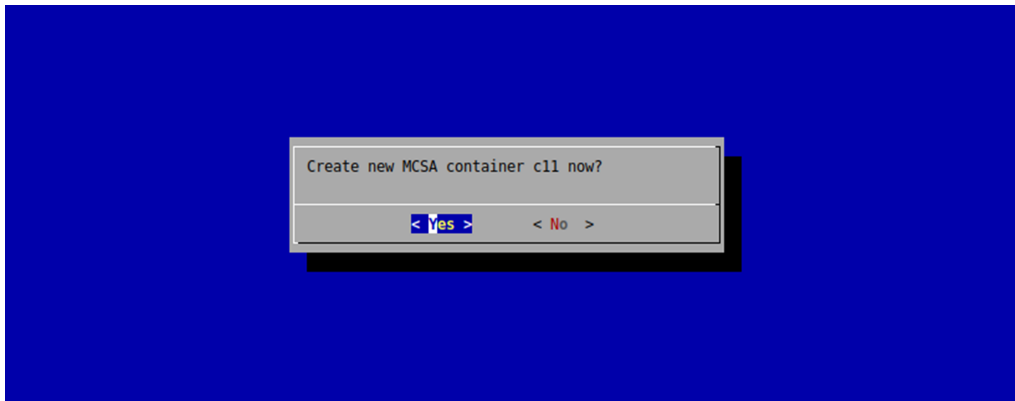
The entered file transfer folder is deleted, if the file name already exists.



- When copying files to the 'fs' and 'idl' sub folders in the MCSA container's local file transfer folder, it is required to set full read and write permissions for all users and groups so that the copied files can internally be moved to other folders.
- When files should be copied using a Samba file share, the local folder of MCSA container should be located on the Samba file share of the Linux host system.

Confirmation

After all settings are entered and the confirmation to create the new MCSA container is given, then a new container will be created.



The main menu is displayed again after the new MCSA Docker container is created.

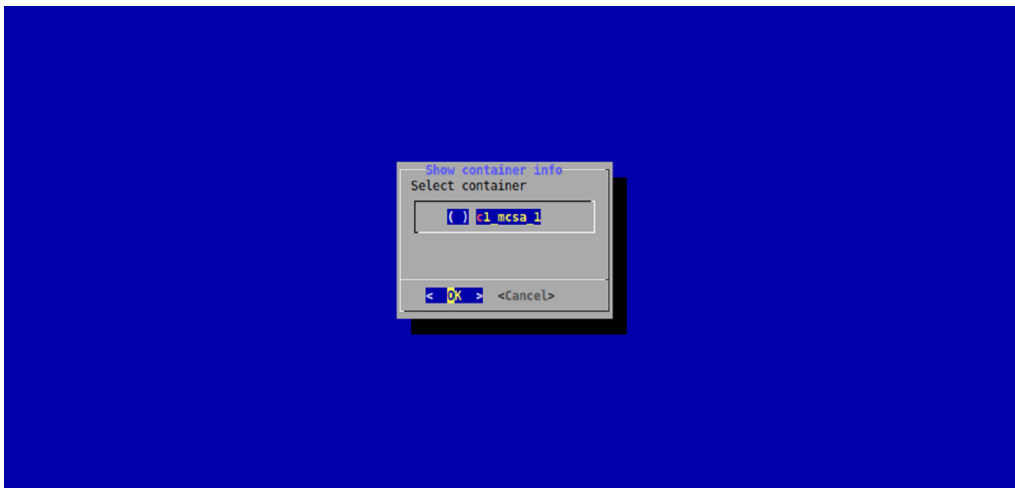


- After creation of an MCSA Docker container, the system will set up internally which takes some time. Hence, it is recommended to wait for 2 minutes before trying to onboard the system, or to create another MCSA container.
- MCSA Docker containers will automatically be restarted after the system restart.

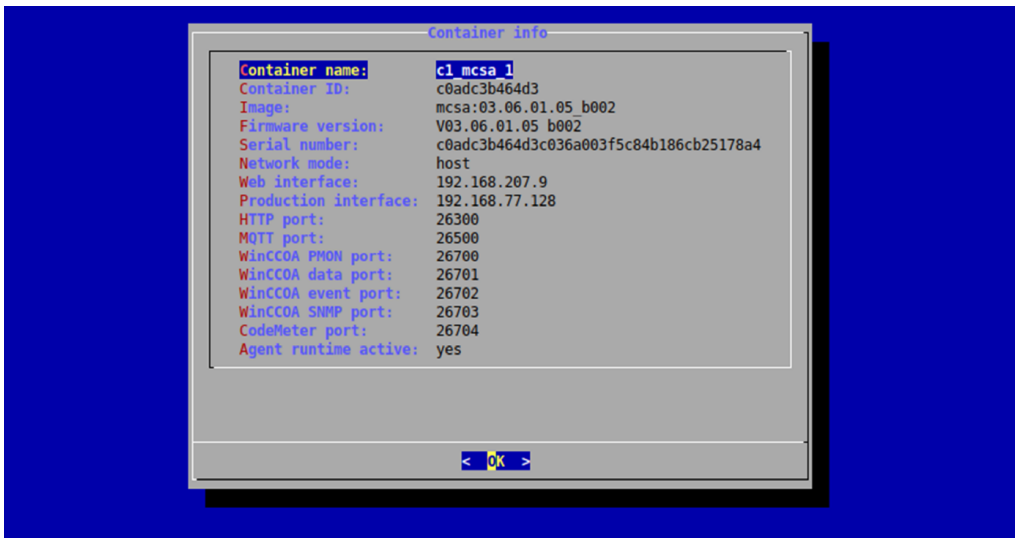
Show running container info

In the main menu, Select "Show running container info", currently running MCSA container information is displayed.

In the first dialog, the MCSA Docker container can be selected:



After selecting a MCSA container and click "OK", the following information is displayed:



Show all containers

Select "Show all containers" to display the status of all MCSA containers:



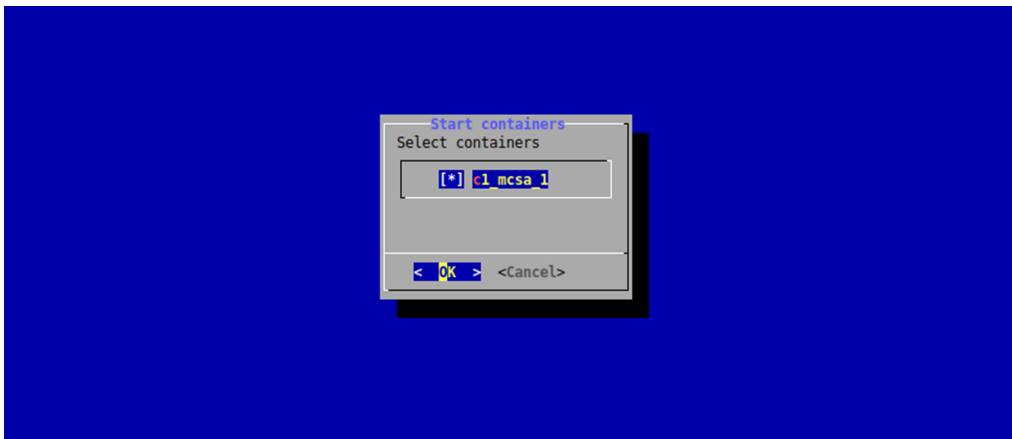
The following table describes the status of container,

Status	Description
up	Container is running

Status	Description
down	Container is not running

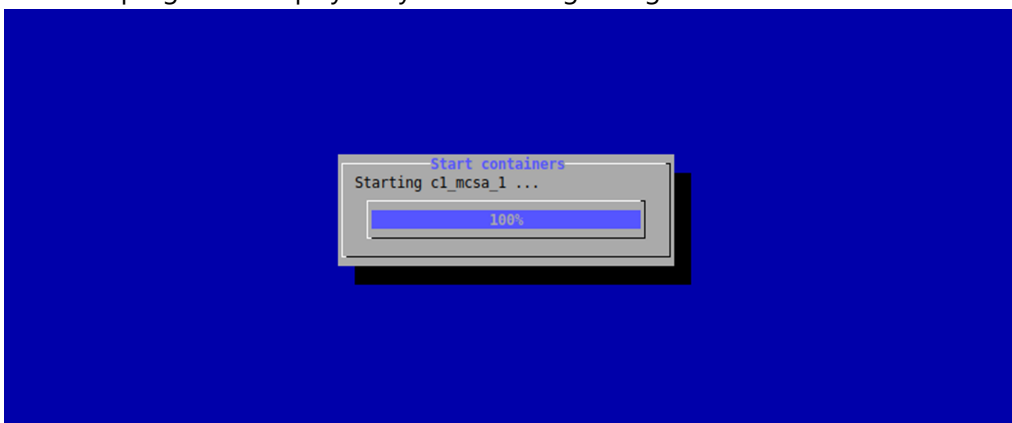
Start Docker container

In the main menu, Select "Start containers" to display list of all exited or stopped MCSA Docker containers:



Select the containers to be started and click "OK" to start the containers.

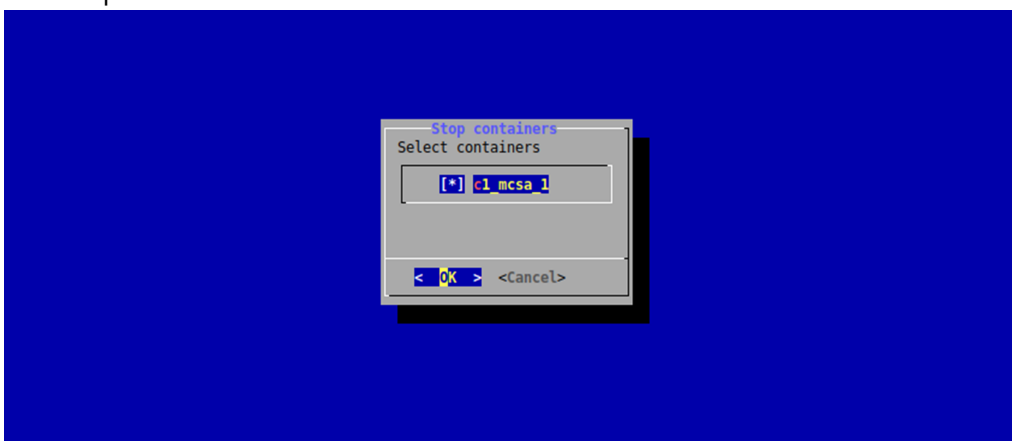
The start progress is displayed by the following dialog:



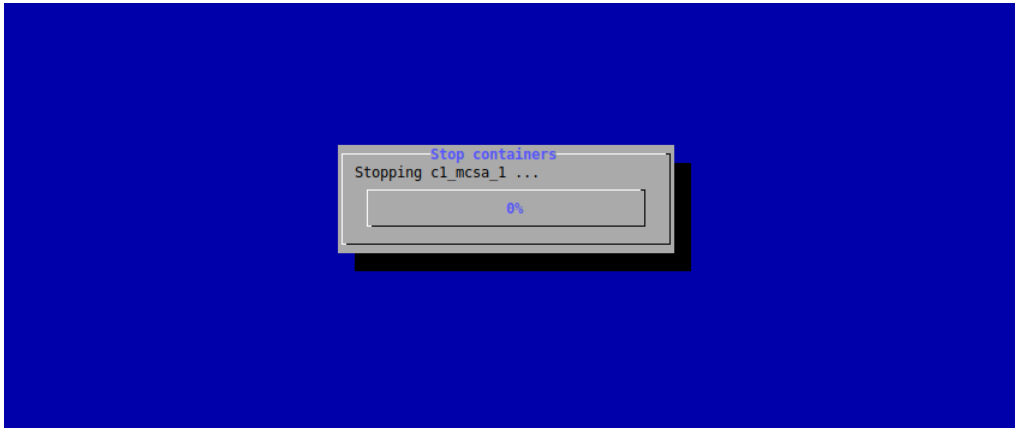
After all the selected containers are started, the main menu is displayed again.

Stop Docker container

In the main menu, a list of all up/running MCSA Docker containers are displayed, after selecting the "Stop containers" task:



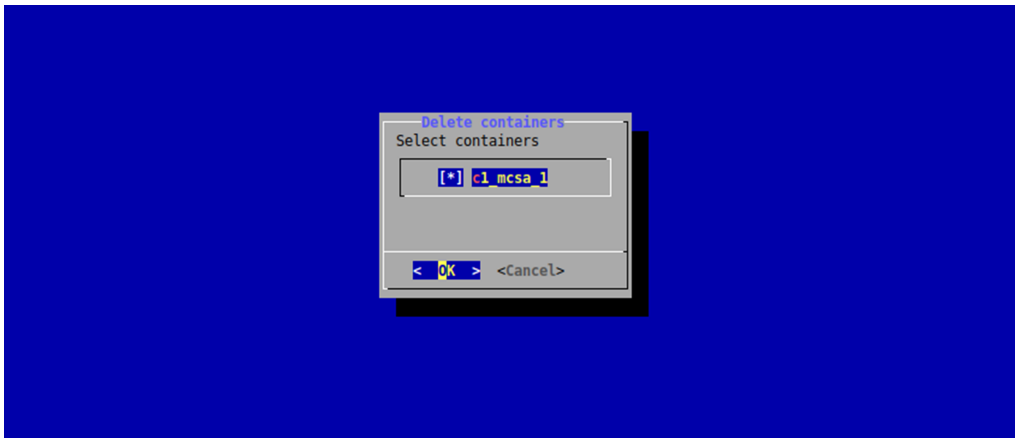
While stopping the containers, following dialog is displayed:



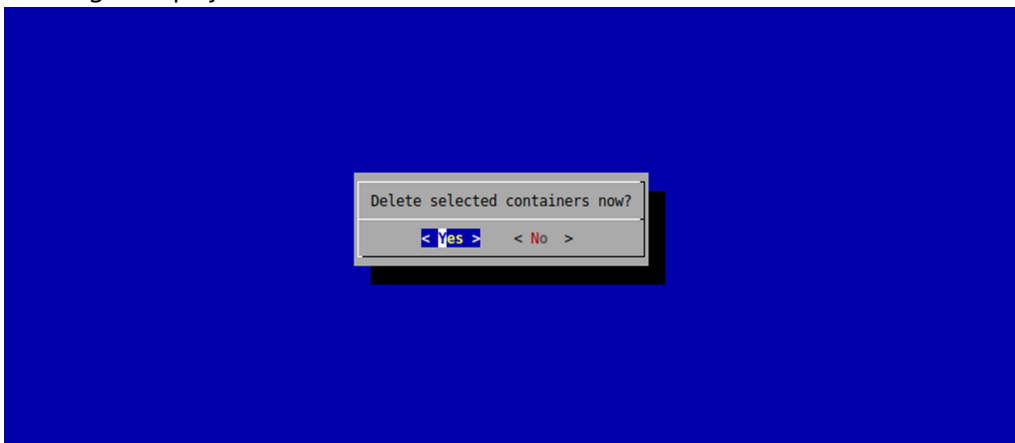
After all the selected containers are stopped, the main menu is displayed again.

Delete Docker container

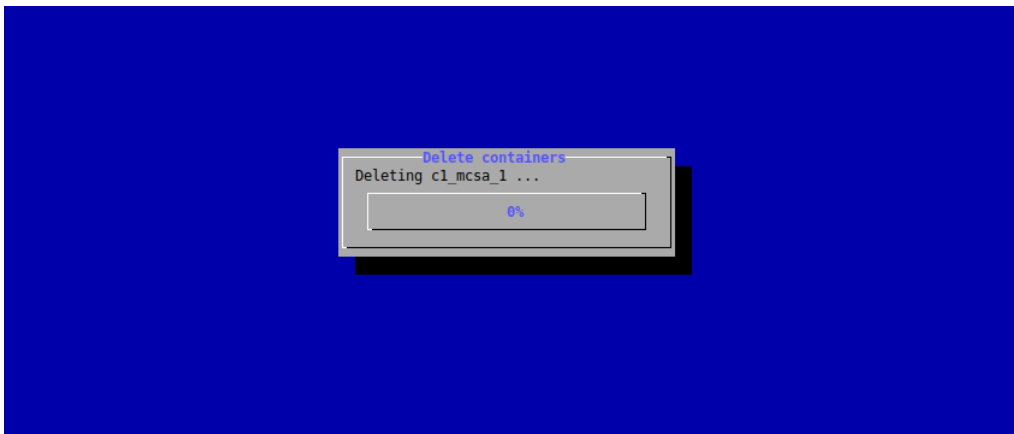
In the main menu, MCSA Docker containers can be deleted after selecting the "Delete containers" task and select the containers to be deleted from the following dialog:



A dialog is displayed to confirm the containers to be deleted:



The deletion progress is displayed by following dialog:



After all the containers are deleted, the main menu is displayed again.

5.11 Troubleshooting

Error	Problem	Possible cause	Possible remedy
MCN L1-RUN/STOP IoT2040 USER LED ORANGE	<ul style="list-style-type: none"> - MindConnect Element cannot onboard to Insights Hub - No Internet connection 	<p>Network connection problem:</p> <ul style="list-style-type: none"> - Either IP address is not valid or configured IP address already exists in the network of MindConnect Nano - Either disabled or invalid configured Proxy - Proxy is offline - Interrupted connection - IP address is configured via DHCP, but there is no internet connection. - Firewall blocks MindConnect Elements - Your company's router is damaged 	<ul style="list-style-type: none"> - Check your configuration connection: If configured IP and Proxy are valid - Check physical connection: your company's router, Ethernet cables etc.

Error	Problem	Possible cause	Possible remedy
MCN L2 - ERROR LED IoT2040 USER LED ORANGE	- Although an asset uploaded to Insights Hub Monitor. - MindConnect Nano/IoT2040 cannot onboard to Insights Hub	- No connection to data source - The address of the data point configuration can be incorrect - Incorrect asset configuration - Not accomplished asset configuration (Network Connection) Invalid ID of MindConnect Nano	Check the connection between MindConnect Nano and data sources (Plant Network ports and cables-S7/OPC UA Server) - Check the connection between MindConnect Nano and data sources (Plant Network ports and cables-S7/OPC UA server) - Check data sources configuration. - Check configuration of each data point. - Check configuration of your asset - (Network Configuration). - Check if MindConnect Nano ID is correct.
MCN L2- ERROR LED blinking RED IoT2040 USER LED blinking RED	Data loss	MindConnect Nano/IoT2040 was too long offline, so it could not send data to Insights Hub and the storage is full.	- Check outbound connection - Check Ethernet cables - Check Proxy (IP address, User Authentication can be required)
MCN L2- ERROR LED RED IoT2040 USER LED	Firmware update error	- Technical problems with a new version of firmware - Incorrect firmware type - Certificate problems, Authentication problems etc.	- Make sure that you are using the correct firmware type (MindConnect Nano/IoT2040). - MindConnect Nano/IoT2040 will automatically restart and then firmware update will be carried out after a while. - If MindConnect Nano/IoT2040 does not restart automatically, then restart it manually: by switching on and off the "power button" on MindConnect Nano and by switching off/on the power supply for MindConnect IoT2040.
MCN L3- MAINT LED ORANGE IoT2040 USER LED blinking	Onboarding failed	- Configuration file on the USB stick is invalid - Internal error	- Make sure that the data on the USB stick still is valid. (The data, which you exported to the USB stick, is still valid only for 7 days.). If it is expired, use the asset configuration to export a new valid configuration to your USB stick. - Check asset configuration and reconfigure, if it is required and export a new configuration to USB stick.

Error	Problem	Possible cause	Possible remedy
MCN L3-MAINT LED blinking RED IoT2040 USER LED blinking	<ul style="list-style-type: none"> - Problems with USB stick - Although no LED lights are shown (except PC ON/WD with constant GREEN) and internet connection is OK, MindConnect Nano still cannot be onboarded to Insights Hub - System Error 	<ul style="list-style-type: none"> - Incorrect formatting of USB stick (no FAT or FAT32) - USB stick is damaged - Write error, USB stick is write-protected or its memory is full. - Configuration file is invalid (damaged, illegible) - See also below <p>Problems with USB stick:</p> <ul style="list-style-type: none"> - Configuration file in USB stick cannot be read or accepted by MindConnect Nano: - Problems with configuration file - Configuration file is located in an incorrect directory. - Expired configuration file on the USB stick - The configuration file is invalid or not copied to the USB stick Unknown 	<p>Check format and partition of the USB stick. It must be FAT or FAT32 formatted and may only contain a single partition.</p> <ul style="list-style-type: none"> - Try a new USB stick - Remove and plug an USB stick into MindConnect Nano - Check the diagnosis file on the USB stick. - Check the name of the configuration file. It must have MindConnect Nano ID. Do not change the name of the downloaded file. - Check whether the directory is valid. (Configuration file must be in the root directory of the USB stick.) - Make sure that the data on the USB stick is still valid. (The data, which you exported to the USB stick, is still valid only for 7 days.) If it is expired, use the asset configuration to export a new valid configuration to your USB stick. - Switch MindConnect Nano off and on again. - If the problem persists, contact your Siemens Support/„Expert Center“.

Log files

Overview

Log files are generated continuously and automatically uploaded when the "Auto Log Upload" is enabled in the following scenarios:

- Log files are uploaded every time the device is started.
 - All the log files are uploaded after midnight.

- Once a log file reaches its maximum file size, it is uploaded as zip file.
 - Using "Upload Logs Now" option to upload log files manually.

Log files are uploaded in tar.gz format with a maximum file size limit of 10MB with following MindConnect Firmware version.

- MindConnect Software Agent for Hyper-V V03.06.00.17 b003
 - MindConnect Software Agent for Docker V03.06.02.04 b002

Concatenating log file archive parts

Linux

On Linux, the downloaded log file archive parts is concatenated as follows:

```
cat fileArchiv.tar.gz.parta* > fileArchiv.tar.gz
```

Windows

On Windows, the downloaded log file archive parts is concatenated as follows:


```
type fileArchiv.tar.gz.parta* > fileArchiv.tar.gz
```

For information on USB commands troubleshooting, refer to [USB commands](#).

6.1 Overview of supported protocols for MindConnect Software Agent

The following are the supported protocols for MindConnect Software Agent:

- S7
- OPC UA
- Modbus TCP IP
- System
- Rockwell
- S7+^{1,2}
- Fanuc Focas^{1,2}
- Sinumerik^{1,2}
- IEC61850^{1,2}
- MTConnect^{1,2}
- BACnet^{1,2,3}



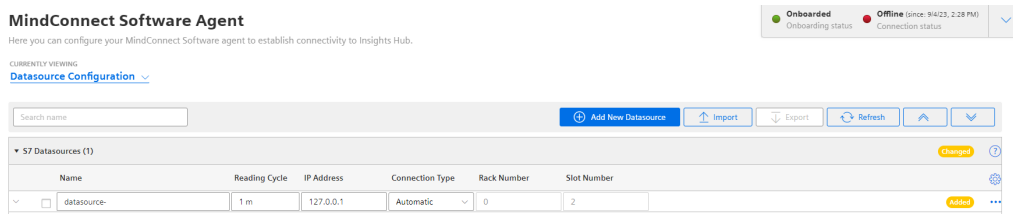

- "1" - This adapter is an enhancement to the MindConnect Device. To enable this functionality, you need to buy the Add-on MindConnect Advanced Driver Extension (Pricebook ID: MP1AXAD00). You can directly buy it through the In Platform Purchase by pressing the shopping chart.

24 of 37
Advanced Driver Licenses Upgrade ↗

- "2" Version MindConnect Software Agent V03.06.00.00 b008 and "MindConnect Advanced Driver Extension" is required to support these protocol.
- "3" - BACnet is not supported by MCSA for Hyper-V (Windows) and MCSA for Docker V3.6.2.x. It is currently supported by MCSA for Docker for ARM64 (aarch64) starting with V03.06.20.00 b002.
- Currently Google Chrome or Microsoft Edge web browsers are supported.
- Fanuc Focas is not available for Linux.

6.2 Overview of S7 protocol for MindConnect Software Agent

The following image shows the data source input for the S7 protocol, click "Add New Datasource" to add new datasource.

Datasource name should be entered without any space.

You can choose between automatic and manual connection type.

- Automatic: This mode tries to find slot and rack number automatically.
- Manual: In this mode you can enter the rack and slot number manually.

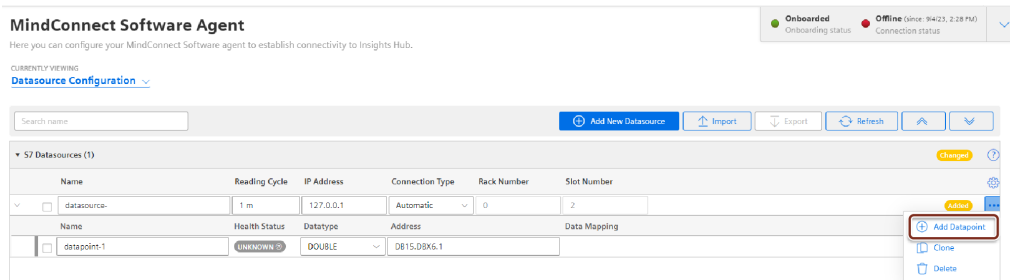
For S7 connection type the PG type-programmer-type-connection is used thus you will not be able to make use of PG connection.

Symbolic access

This solution does not allow full symbolic access.

S7 data point parameter

To collect the data of your S7 device, click "Add Datapoint" to add new datapoint. The following image shows the data point parameter window:



Requirements for S7-1200 and S7-1500

- Put/Get communication must be permitted (can be found e.g. S7-1500 -> Properties -> Protection & Security -> Connection mechanisms).
- The "Optimized block access" of the data blocks that you want to read must be deactivated (can be found in the data block properties).

Address format examples

Detailed examples:

Example address format DB15.DBX6.3:

DB15.DBX6.3

Area indicator			Data type	Offset address		
DB15	':'	DB	X	6	':'	3
Datablock address	Separator	Datablock	Bool	Offset Byte	Separator	Offset Bit
Reads 3rd bit of byte 6 of datablock 15						

Example address format IW10:

IW10

Area indicator	Data type	Offset address
I	W	10
Process Input	Word	Offset Byte
Reads a word of input starting from offset 10		

Overview

If you want to read data out of other areas, please replace “DB15.DB” from the examples with the area indicator from the list below:

Attention: only certain address examples work with Inputs and Outputs (see²⁾).

S7		Industrial IoT		
Data type	Length/unsigned/signed	Data type (length)	Address example	Description
Bool	1 bit	BOOLEAN (1 bit)	DB15.DBX6.3 ²⁾	Reads 3rd bit of byte 6 of datablock 15
Byte USInt	1 byte / unsigned	INT (4 bytes) LONG (8 bytes) DOUBLE *(8 bytes)* ¹⁾	DB15.DBB4 ²⁾ DB15.DBBYTE4	Reads an unsigned byte starting from offset 4 out of datablock 15.
SInt	1 byte / signed			
Char	1 byte / signed		DB15.DBCHAR6	Reads a char starting from offset 6 of datablock 15.
Word	2 bytes / unsigned		DB15.DBW10 ²⁾	Reads an unsigned word
UInt	2 bytes / unsigned		DB15.DBWORD10	starting from offset 10 of datablock 15.
Int	2 bytes / signed		DB15.DBINT12	Reads a signed integer starting from offset 12 out of datablock 15.
DINT	4 bytes / signed		DB15.DBDINT28	Reads a signed double integer starting from offset 28 of datablock 15.
DWord	4 bytes / unsigned	LONG (8 bytes)	DB15.DBDW24 ²⁾	Reads an unsigned double

S7		Industrial IoT		
UDInt	4 bytes / unsigned	DOUBLE * (8 bytes)* ¹⁾	DB15.DBDWORD24	word starting from offset 24 of datablock 15.
Real	4 bytes / signed	DOUBLE (8 bytes)	DB15.DBD32 ²⁾	Reads a floating-point
			DB15.DBREAL32	number starting from offset 32 of datablock 15.
String	Length of variable, max. 254 bytes	STRING (max. 254 bytes)	DB15.DBSTRING10	The maximum string length (Byte10) is read first. Then the number of bytes that Byte10 indicates are number read. After that the of bytes that Byte11 indicates are extracted from the byte array that is the result of second read operation. For example: - (Byte10)-30 - (Byte11)-4 - (Byte12-Byte15)-TEST First read result: 30 Second read result: 4TEST We will extract TEST from the second read result by the second read result by considering Byte11's value.
String	Min. 100 bytes , max. 254 bytes		DB15.DBSTRING10,100	Reads 100 bytes of string starting from offset 10.

¹⁾ When DOUBLE is used for integers, they are converted to a floating-point number.

²⁾ For the areas Inputs and Outputs only certain address examples work.



Signed values

If you want to read a signed value, you have to use the respective signed datablock.

Example:

DB1831.DBW508 is unsigned. You can use DB1831.DBINT508 instead.



Real data type

If you want to write a value to REAL data type, you have to use “REAL” instead of “DBD” in the address.

Example:

DB15.DBD32 or DB15.REAL32 can be used for reading. You can use DB15.REAL32 for writing.

Area Types

S7 datapoint addresses must contain an area type.

Area indicator	Area types	Description
C	Counter	Reads Counter value of hardware.
DB	Datablock	Reads datablock value from hardware.
DI	Instance Data	Reads data directly from hardware.
I	Process Input	Reads Input value of Process image.
M	Memory	Reads Memory value of hardware.
PI	Peripheral Input	Reads Input value directly from hardware.
PQ	Peripheral Output	Reads Output value directly from hardware.
Q	Process Output	Reads Input value of Process image.
T	Timer	Reads Timer value of hardware.

Area Number

S7 datapoint addresses must contain area number.

E.g.: DB10 (10. datablock)


Data Types

The following table shows the data types:

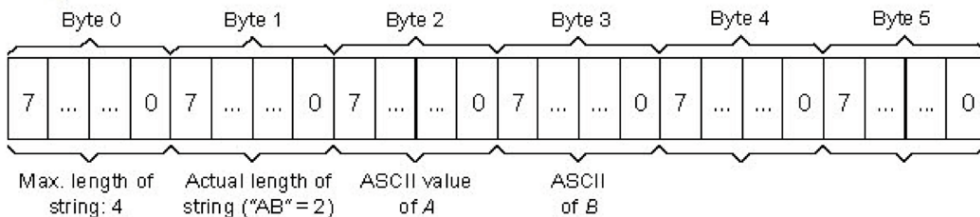
Data type	Length	Date range
BOOLEAN	1 bit	True to False

Data type	Length in bytes	Format
STRING[n] or STRING	n+2	ASCII character of any length. n specifies the length of the character string. A maximum length of 254 characters is permitted. If no length is specified, the default setting is 254 characters.

Data type	Examples of format used
STRING[2]	'AB'
STRING[55]	'The character string can consist of up to 55 characters'

 You must enclose your character string in single quotation marks.

The following example shows the byte order when specifying the datatype STRING[4] with the output value 'AB'.



*** Tod**

TIME_OF_DAY (Time)	32	Time is in steps of 1 ms	TOD#0.0.0.0 to TOD#23:59:59.999	L TOD#1:10:3.3 L TIME_OF_DAY#1:10:3.3
--------------------	----	--------------------------	---------------------------------	--

*** Time**

Returns milliseconds.

Format:

The DT (DATE_AND_TIME) datatype saves the information on date and time of day in BCD format.

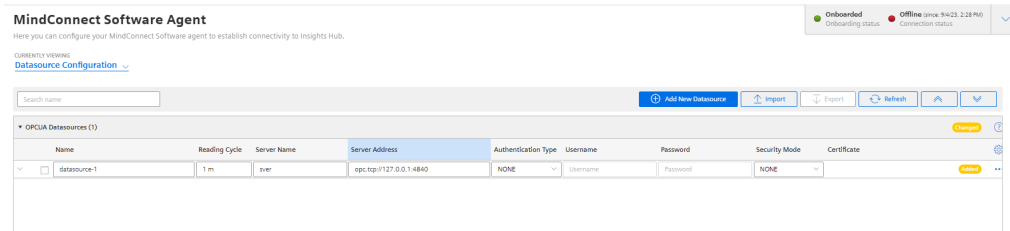
The following table shows the properties of datatype DT:

Length (bytes)	Format	Range of values	Example of value input
8	Date and time (year-month-day)		

6.3 Overview of OPC UA protocol for MindConnect Software Agent

OPC UA datasource parameter

The following image shows the data source input window for the OPC UA protocol:

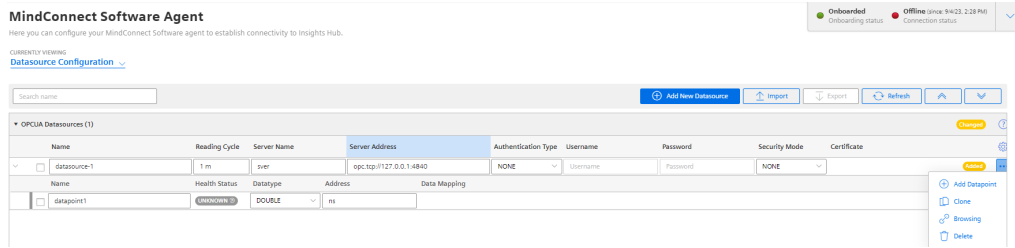


For the OPCUA protocol, the data source input supports the following parameters:

Parameter	Description
Protocol	Shows the selected protocol type
Name	Name of the data source
Description	Add a description for data source
Reading Cycle	Enter a reading cycle for the data source
OPC UA Server Name	Enter the name of the OPC UA Server Name
OPC UA Server Address	Enter the OPC UA Server Address
OPC UA Server IP Address	Enter the OPC UA Server IP Address
OPC UA Authentication Type	You can choose between the following types: - NONE: No authentication enabled - BASIC: Enables the OPC UA BASIC authentication
OPC UA Security Mode	You can choose between the following modes: - NONE: No security mode - CERTIFICATE: Enables to upload a certificate in the following formats: *.pfx, *.pf12, *.cer, *.crt, *.der, *.p7b, *.p7r, *.spc
Enable OPC UA Events	You can enable the transfer and takeover of events and alarms in the OPC UA protocol to Insights Hub. Operation Insight shows all events and alarms in the "Events" extension of the agent asset. Limits: - For Nanobox the proposed limit is 25 events/alarms per second - For IoT2040 the proposed limit is 10 events/alarms per second

OPC UA data point parameter

In order to collect the data of the OPCUA device, click "Add Datapoint" to add new datapoint. The following image shows the data point parameter window:




OPC UA Data Access Specification

OPC UA Data Access Specification does not specify a certain representation for OPC UA Addresses (NodeId). A NodeId is represented by a combination of:

- NamespaceIndex
- IdentifierType
- Identifier

OPC UA Client Driver addresses have the following syntax: ns=;=.



OPC browsing is not supported.

For more information refer to the table below:

Field	Description
NamespaceIndex	The index of the OPC UA Server namespace in which the address resides. If the index is 0, the entire ns=;= clause is omitted.
IdentifierType	The type of address. OPC UA supports the following four address types: i: A numeric address represented with 32-bit unsigned integer s: A string address containing characters that can be encoded using UTF-8 g: A GUID address in the format of XXXXXXXX-XXXX-XXXX-XXXX-XXXXXXXXXXXX b: An opaque address (such as a byte string)
Identifier	The address that is formatted as a string. This address may be numeric, string, GUID, or opaque.

Examples NodeId

Below you can see examples of an OPC UA Addresses (NodeId) representation:

String:

String IdentifierType	Example

String IdentifierType	Example
ns=[id];s=[string]	ns=5;s=Counter1

Attribute NodeId	Value NodeId
NamespaceIndex	5
IdentifierType	String
Identifier	Counter1

 **String for Identifier**

The string you enter at the four Identifier will be case sensitive.

Numeric:

Numeric IdentifierType	Example
ns=[id];i=[number]	ns=0;i=3190 OR

Attribute NodeId	Value NodeId
NamespaceIndex	0
IdentifierType	Numeric
Identifier	3190 [BaseEventType_LocalTime]

Guid:

Guid IdentifierType	Example
ns=[id];g=[guid]	ns=1;g=0d4e10fa-b9e1-4842-bca6-887c7d8c31f0

Base64(Opaque):

Base64(Opaque) IdentifierType	Example
ns=[id];b=[base64]	ns=2;b=M/RbKBSRVkePCePcx24oRA==

Datatypes Conversion

The following table shows the Datatype Conversion:

IEC61131 elementary datatypes	OPC UA built-in datatypes	Industrial IoT Type

IEC61131 elementary datatypes	OPC UA built-in datatypes	Industrial IoT Type
BOOL	Boolean	boolean
SINT	SByte	int
USINT	Byte	int
INT	Int16	int
UINT	UInt16	int
DINT	Int32	int
UDINT	UInt32	int
LINT	Int64	long
ULINT	UInt64	long
BYTE	Byte	int
WORD	UInt16	int
DWORD	UInt32	int
LWORD	UInt64	long
REAL	Float	double
LREAL	Double	double
STRING	String	string
CHAR	Byte	string
WSTRING	String	string
WCHAR	UInt16	int
DT DATE_AND_TIME	DateTime	n/a
DATE	DateTime	n/a
TOD TIME_OF_DAY	DateTime	n/a
TIME	Double	double



“NodeID” is not a valid part of the OPC string anymore.

OPC UA Event Type

You can choose default event type or one of the custom event types created in environment.

OPC UA Event Types

OPC UA plugins supports custom event types to be uploaded to Insights Hub. Select the correct event type from the below drop-down menu, to get those events on Industrial IoT. In the dropdown menu, the events owned by the specific environment and the default event type "DataSourceEvent" is shown only.

Enable Events	Event Type		
false	DataSourceEvent	Added	...
true	DataSourceEvent	Added	...

DataSourceEvent
CustomDataSourceEvent

The event types are summarized as below:

Data Source Event Type	It is the default event type which can collect some static fields of events from OPC UA server.
Custom Event Type	These types can be created by user/owner of environment, and they can collect both static and extra fields from OPC UA server.

A new event type must be created from "AgentBaseEvent" type with required extra fields and then, it can be selected from the event drop-down list which is shown during OPC UA server configuration.



- If there is no created custom event type in environment, "Data Source Event Type" will be selected by default.
- Both, data source events and custom events will be uploaded to Industrial IoT. They can be displayed on Insights Hub Monitor regarding to their types. For more information on displaying events, refer to [Introduction to Events](#) in Insights Hub Monitor documentation.

Create custom event type via API

It is possible to create custom event types with extra fields via Event Management API. For more information on the service, see [Event Management - API Overview](#).

Below is the api to call using a technical user `/api/eventmanagement/v3/eventTypes`.

The following template shows the payload of the call:

```
{
  "name": "SomeCustomEventType",
  "parentId": "core.connectivity.event.type.AgentBaseEvent",
  "ttl": 35,
  "scope": "LOCAL",
  "fields": [
    {
      "name": "Message",
      "filterable": false,
      "required": false,
      "updatable": true,
      "type": "STRING"
    },
    {
      "name": "testField1",
      "filterable": false,
      "required": false,
      "updatable": true,
      "type": "STRING"
    },
    {
      "name": "testField2",
      "filterable": false,
      "required": false,
      "updatable": true,
      "type": "STRING"
    },
    {
      "name": "testField3",
      "filterable": false,
      "required": false,
      "updatable": true,
      "type": "STRING"
    }
  ]
}
```



- The “name” field in body must be same as the “browseName” of the field which will be collected in the OPC UA Server. It is case-sensitive.
- Name for "Event Type" needs to be unique
- The “type” field must be “STRING” for all data types.
- The “scope” field should always be given as “Local” unless a particular reason is required to make it "Public".
- The field with name “Message” is the static field and it is not included to custom event types. It is needed to be added as an extra field.
- The fields Time, Severity and SourceName in the Event type are reserved fields and should not be created as extra fields.

OPCUA Browsing

OPCUA browsing feature enables the browsing of nodes on an OPC server for configuring the MindConnect Elements in an automated procedure.

Limitations

Unsupported data types in the browsing results are listed below, the nodes with

- unsupported types will not be shown in the browsing result.
 - Image, ImageBMP, ImageGIF, ImageJPG, ImagePNG
 - Enumeration
 - Number
 - Structure
 - Argument
 - ByteString
 - Range
 - EuInformation

If the time consumption is more than 90 minutes for browsing a datasource then the

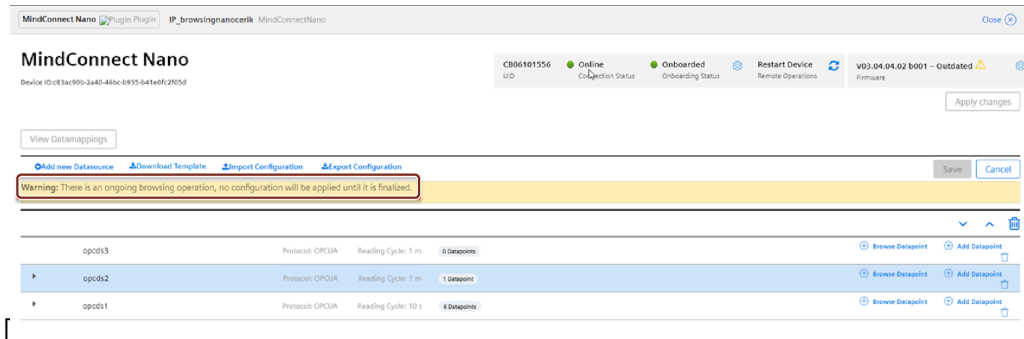
- operation would be cancelled by the device.

If the OPCUA Server has more than 150K browsable nodes under 'Root/Objects' folder,

- then the browsing operation will be cancelled by the device.



Configuration jobs can only be applied after browsing operation is completed. If configuration job is applied during a browsing operation, below warning message is displayed on data source configuration page.



Type Conversion

Conversions of node supported types to Industrial IoT are mentioned in below table, if the OPC Type is not included in the below table, then that would be converted to STRING.

OPC Type	Cloud Type
Boolean	BOOLEAN
Float	DOUBLE
Double	DOUBLE
Duration	DOUBLE
SByte	INT
Byte	INT
Int16	INT
Int32	INT
Integer	INT
UInt16	INT
Int64	LONG
UInt32	LONG
UInt64	STRING
String	STRING

If the connection to OPCUA Server is disconnected during browsing, then the whole operation of browsing is failed. It is expected from the customer to trigger the browsing

- result again in those situations.

If a node with supported node type is not fulfilling the required fields on server side which is browsed than this node will be excluded, and it will not affect the whole browsing flow.

- The excluded node and its child nodes will not be displayed in browsing results.
- The default type for "Acquisition type" for browse result will be READ.

Performance of OPCUA Browsing

The browsing of an OPCUA server can be a time-consuming task depending on the number of existing nodes on the server. Below table describes the time consumption for idle devices which only perform browsing operations to OPC servers.

Number of Nodes	Type of Device	Time Consumed
5K	MindConnect Nano	~6 min
75K	MindConnect Nano	~16 min
150K	MindConnect Nano	~36 min



The reading cycles of datasources can be affected during the OPCUA browsing operation, as it requires a huge performance activity on the MindConnect Element.

6.4 Overview of Modbus TCP protocol for MindConnect Software Agent

The Modbus protocol for the MindConnect Software Agent. You can select the protocol type Modbus TCP while adding a new data source in Asset Manager.



Modbus configuration

The Modbus configuration view is only visible after a successful onboarding of the MindConnect Software Agent.

The following picture shows the protocol selection in Asset Manager:



For more information about how to create a new data source see chapter [Adding a data source for MindConnect Software Agent](#).

Modbus TCP data source parameter

In order to connect a Modbus TCP device, you need to select the Modbus TCP protocol and enter the following data source parameters:

Parameter	Description
IP Address	IP address of the Modbus device
Port	Port number of the Modbus device (default: 502)

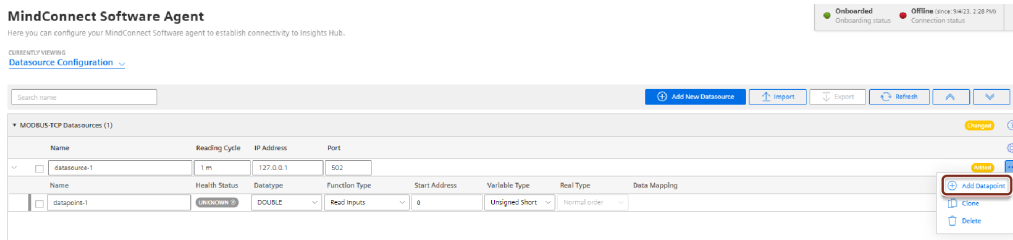
The following parameters are optional and can be adjusted for collecting data from slow Modbus devices:

Parameter	Description
byteTimeout	You can set the timeout interval between two consecutive bytes of the same message received from the Modbus device. If the delay between is longer than the given timeout, an error will be generated. Range: 500ms (default) ... 2000ms
responseTimeout	You can set the timeout interval used to wait for a response from the Modbus device. If the waiting before receiving the response is longer than the given timeout, an error will be generated. Range: 500ms (default) ... 60000ms
responseSuspensionTime	If a byte timeout or a response timeout was detected, then this waiting time is added before the next request is started. During this time any response from the Modbus device will be flushed. Range: 0ms ... 45000ms. (default: 1000ms)
requestDelay	You can set the time between the response from the Modbus device and the next request to this Modbus device. Range: 0ms (default) ... 10000ms

Modbus TCP data point parameter

In order to collect the data of the Modbus TCP device, click "Add Datapoint" to add new datapoint.

The following picture shows the data point parameter window:



The following table shows the parameter of the Modbus TCP data point window:

Parameter	Description
Data Type	Data type supported by backend (e.g. INT).
Slave Number	Address/Slave number of the Modbus device.
Start Address	Start address (offset) of the data.
Quantity	Quantity of data to be read.
VariableType	You can choose the following variable types of the Modbus data to be read: 1: char : 8 bits, 2: unsigned char : 8 bits, 3: short : 16 bits, 4: unsigned short : 16 bits, 5: long : 32 bits, 6: unsigned long : 32 bits, 7: float : 32 bits, 8: double : 64 bits, 9: ascii-text : 8 bits / char
Real Type	Real type - determines, if the registers of real values have to be processed in reversed order. 0: Normal order, 1: Reversed order, 2: Byte swap order, 3: Word swap order, Real types 2 and 3 are available from V03.04.02.01.
Integer Byte Order	It determines in which byte order format the read value will be processed (default: 0) 0: Normal order (big-endian) 1: Reversed order (little-endian byte swap) 2: Byte swap order (big-endian byte swap) 3: Word swap order (little-endian) Note: Integer byte order is available for 16 bits and 32 bits variable types only, and it is supported for the version starting from MindConnect Software Agent, MCSA for Hyper-V V03.06.00.11 b001 and MCSA for Docker V03.06.01.04 b001
Response Address Offset	Offset of the data to return in register units.

Parameter	Description
Response Quantity	Quantity of the returned data. Only for string data a value greater than 1 is supported.

TCP Gateway slave number

If you are using a TCP Gateway, you must select the appropriate slave number for the configuration of the data points.

The following table shows the parameter of the Modbus TCP datapoint window for Function Type and Acquisition Type:

Function Type	Acquisition Type
The function type depends on the type of the data (see manual of the Modbus device).	The acquisition type depends on the selected function type.
1: Read Coils	Read
2: Read Inputs	Read
3: Read Holding Registers	Read
4: Read Input Registers	Read
5: Write Single Coil ¹⁾	Write
6: Write Single Register ^{1),2)}	Write
15: Write Multiple Coils ¹⁾	Write
16: Write Multiple Registers ^{1),3)}	Write
22: Mask Write Register ¹⁾	Write
23: Read/Write Multiple Registers ¹⁾	Write

- Currently function codes 1..4 are supported.
- ¹⁾ Supported since MindConnect Software Agent V03.06.00.22 b002, MindConnect Software Agent in Docker V03.06.023.00 b002, MindConnect Software Agent in Docker for aarch64 V03.06.21.00 b003.
- ²⁾ Used to write values to data points with variable types using a single register (example: short).
- ³⁾ Used to write values to data points with variable types using one or more registers (example: long or double).

Data type	Length	Data type number	Data range
long	32 bits	5	-2147483648 to 2147483647
unsigned long	32 bits	6	0 to 4294967295
float	32 bits	7	-3.402823e+38 to -1.175 495e-38 +1.175 495e-38 to +3.402823e+38
double	64 bits	8	-1.7976931348623158e+308 to -2.2250738585072014e-308 +2.2250738585072014e-308 to +1.7976931348623158e+308
ascii-text	8 bits / char	9	

Examples:

Example	Data type	Function type	Start address	Variable type	Response Address Offset	Response Quantity
Reading the first Holding Register, number 40001, has the start address 0.	int	Read Holding Registers	0	unsigned short or short	0	1
VariableType: 4 or 3 (unsigned short or short) Reading the second Input Register, number 30002, has the start address 1.	int	Read Input Registers	1	unsigned short or short	0	1
Reading a float (32 bits) from Input Register 30108 / 30109, has the start address 107.	double	Read Input Registers	107	float (reads two registers)	0	1
Reading a string. This example describes to read four letters from register 40006 and 40007. Each register contains two characters.	string	Read Holding Registers	5	unsigned short	0	2 (registers)
Reading a Boolean from the Holding Register 40011, has the start address 10. If the whole Holding Register has the value 0 then it is displayed as 0. If one bit(or more) has the value 1 then it will be displayed as 1.	Boolean	Read Holding Registers	10	unsigned short or short	0	1

Using Modbus register addresses directly

Usually, it is necessary to enter Modbus registered address decremented by 1 as "start address", but it may lead to confusion when comparing the data point's "start address" with the registered

address from Modbus device's manual. Therefore, enter a negative value in the "response address offset" field to directly use the registered address from the Modbus device's manual as "start address". In case a negative value has been entered as "response address offset", this value will internally be subtracted from the given "start address" number to read the data from Modbus device. Positive "response address offset" values will be handled to address specific data within the read data if several registers need to be read to acquire the data from Modbus device as data block and the necessary data itself is only a part of that data block.

Supported since:

- MCSA for Hyper-V V03.06.00.11 b001
- MCSA for Docker V03.06.01.04 b001

Samples:

	Using decremented start address	Using address from manual	Getting data from a read data block
Registered address from Modbus device manual	303	303	64001
Start address	302	303	64001 ¹⁾
Quantity	1	1	27
Response address offset	0	-1	11
Response quantity	1	1	16

¹⁾ Sample start offset as documented in SENTRON PAC manual - can be used without decrementing it by 1.

6.5 Overview of SYSTEM protocol for MindConnect Software Agent

You can use the protocol SYSTEM to implement a system information adapter for analysis purposes. The SYSTEM protocol can collect the following information from MindConnect Software Agent:

- Overall CPU load
- Overall memory consumption
- Network traffic
- Application specific data
 - CPU load memory consumption

- Disk usage

You can choose the SYSTEM protocol as a data source without configuring specific system parameters, except the reading cycle.

After creating the data source you can configure the following categories in a new data point:

- CPU
- Memory
- Network
- Disk

The following image shows the data point input window for the SYSTEM protocol:

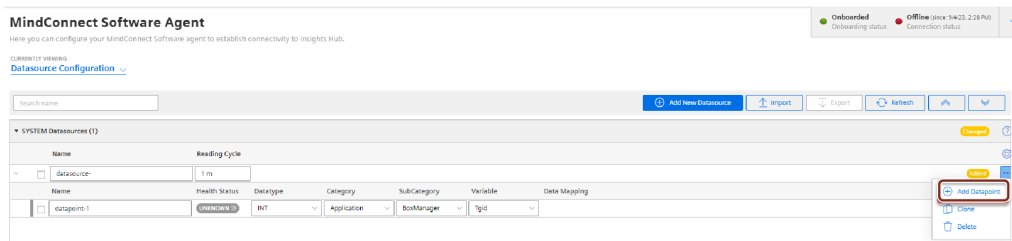


Each category has its own set of variables which will be described in the following.

SYSTEM protocol data point parameter

In order to collect the data of the SYSTEM protocol device, click "Add Datapoint" to add new datapoint.

The following image shows the data point parameter window:



Application information

Application provides the following available applications:

- MindEdgeRuntimeSystem/java
- DataProvider
- BoxManager
- S7 Plugin
- OPC UA Plugin
- XTools
- Mosquitto

The following table shows the available variables for the applications:

Variable	Data type	Address
Name	string	/application/<subcategory>/name
State	stri	/application/<subcategory>/state
Tgid	int	/application/<subcategory>/tgid
Ngid	int	/application/<subcategory>/ngid
Pid	int	/application/<subcategory>/pid
PPid	int	/application/<subcategory>/ppid
TracerPid	int	/application/<subcategory>/tracerpid
Uid	string	/application/<subcategory>/uid
Gid	string	/application/<subcategory>/gid
FDSize	int	/application/<subcategory>/fdsize
Groups	string	/application/<subcategory>/groups
NStgid	int	/application/<subcategory>/nstgid
NSpid	int	/application/<subcategory>/nspid
NSpgid	int	/application/<subcategory>/nspgid
NSsid	int	/application/<subcategory>/nssid
VmPeak	long	/application/<subcategory>/vmpeak
VmSize	long	/application/<subcategory>/vmsize
VmLck	long	/application/<subcategory>/vmlck
VmPin	long	/application/<subcategory>/vmpin
VmHWM	long	/application/<subcategory>/vmhwm
VmRSS	long	/application/<subcategory>/vmrss
VmData	long	/application/<subcategory>/vmdata
VmStk	long	/application/<subcategory>/vmstk
VmExe	long	/application/<subcategory>/vmexe

Variable	Data type	Address
VmLib	long	/application/<subcategory>/vmlib
VmPTE	long	/application/<subcategory>/vmpte
VmPMD	long	/application/<subcategory>/vmpmd
VmSwap	long	/application/<subcategory>/vmswap
HugetlbPages	long	/application/<subcategory>/hugetlbpages
Threads	int	/application/<subcategory>/threads
SigQ	string	/application/<subcategory>/sigq
SigPnd	string	/application/<subcategory>/sigpnd
ShdPnd	string	/application/<subcategory>/shdpnd
SigBlk	string	/application/<subcategory>/sigblk
SigIgn	string	/application/<subcategory>/sigign
SigCgt	string	/application/<subcategory>/sigcgt
CapInh	string	/application/<subcategory>/capinh
CapPrm	string	/application/<subcategory>/capprm
CapEff	string	/application/<subcategory>/capeff
CapBnd	string	/application/<subcategory>/capbnd
CapAmb	string	/application/<subcategory>/capamb
Seccomp	int	/application/<subcategory>/seccomp
Speculation_Store_Bypass	string	/application/<subcategory>/speculation_store_bypass
Cpus_allowed	int	/application/<subcategory>/cpus_allowed
Cpus_allowed_list	string	/application/<subcategory>/cpus_allowed_list
Mems_allowed	int	/application/<subcategory>/mems_allowed
Mems_allowed_list	string	/application/<subcategory>/mems_allowed_list
voluntary_ctxt_switches	int	/application/<subcategory>/voluntary_ctxt_switches

Variable	Data type	Address
nonvoluntary_ctxt_switches	int	/application/<subcategory>/nonvoluntary_ctxt_switches

CPU information

The following table shows the available variables for the category CPU information:

Variable	Data type	Description
LoadAvg1	double	Number of processes in state R(runnable) or D(disk sleep) averaged over 1 minute.
LoadAvg5	double	Number of processes in state R(runnable) or D(disk sleep) averaged over 5 minutes.
LoadAvg10	double	Number of processes in state R(runnable) or D(disk sleep) averaged over 15 minutes.
ProcessCount	string	String containing number of currently runnable processes/threads and number of scheduling processes/threads that currently exist on the system.
LastPidUsed	long	Pid of the process that was most recently created.
CurrentProcessCount	long	Number of currently runnable processes/threads.
ScheduledProcessCount	long	Number of scheduling processes/threads that currently exist on the system.

Disk information

Disk collects information about disk usage and provides the following subcategories:

- persistent_masdata
- persistent_appconfig
- persistent
- root

The following table shows the available variables for the category Disk information:

Variable	Data type	Address	Description
Available	long	/disk/dev/<subcategory>/available	Available space in bytes.

Variable	Data type	Address	Description
Size	long	/disk/dev/<subcategory>/size	Partition size in bytes.
Used	long	/disk/dev/<subcategory>/used	Used space in bytes.

KERNEL information

The following table shows the available variables for the category KERNEL information:

Variable	Data type	Address
OsRelease	string	/kernel/osrelease
OsType	string	/kernel/ostype
Version	string	/kernel/version

Memory information

The following table shows the available variables for the category Memory information:

Variable	Data type	Address
Active	long	/memory/active
Active(anon)	long	/memory/active(anon)
Active	long	/memory/active
Active(anon)	long	/memory/active(anon)
Active(file)	long	/memory/active(file)
AnonPages	long	/memory/anonpages
Available	long	/memory/available
Bounce	long	/memory/bounce
Buffers	long	/memory/buffers
Cached	long	/memory/cached
CommitLimit	long	/memory/commitlimit
Committed_AS	long	/memory/committed_as
DirectMap4K	long	/memory/directmap4k

Variable	Data type	Address
DirectMap4M	long	/memory/directmap4m
Dirty	long	/memory/dirty
Inactive	long	/memory/inactive
Inactive(anon)	long	/memory/inactive(anon)
Inactive(file)	long	/memory/inactive(file)
KernelStack	long	/memory/kernelstack
LowFree	long	/memory/lowfree
LowTotal	long	/memory/lowtotal
Mapped	long	/memory/mapped
MemFree	long	/memory/memfree
MemTotal	long	/memory/memtotal
MLocked	long	/memory/mlocked
NFS_Unstable	long	/memory/nfs_unstable
PageTables	long	/memory/pagetables
SHMem	long	/memory/shmem
SLab	long	/memory/slab
SReclaimable	long	/memory/sreclaimable
SUnreclaim	long	/memory/sunreclaim
SwapCached	long	/memory/swapcached
SwapFree	long	/memory/swapfree
SwapTotal	long	/memory/swaptotal
Unevictable	long	/memory/unevictable
VMAllocChunk	long	/memory/vmallocchunk
VMAllocTotal	long	/memory/vmalloctotal
VMAllocUsed	long	/memory/vmallocated
WriteBack	long	/memory/writeback

Variable	Data type	Address
WriteBackTmp	long	/memory/writebacktmp

Network information

The following table shows the available variables for the category Network information:

Variable	Data type	Address	Description
ArpFilter	long	/network/arpfilter	
BusyPollRxPackets	long	/network/busypollrxpackets	
BytesReceived	long	/network/bytesreceived	Alias for InOctets.
BytesSend	long	/network/bytessend	Alias for OutOctets.
DelayedAckLocked	long	/network/delayedacklocked	Number of delayed acks further delayed because of locked socket.
DelayedAckLost	long	/network/delayedacklost	Number of times that quick ack mode was activated.
DelayedAcks	long	/network/delayedacks	Number of delayed acks sent.
EmbryonicRsTs	long	/network/embryonicrst	Number of resets received for embryonic SYN_RECV sockets.
InBcastOctets	long	/network/inbcastoctets	
InBcastPkts	long	/network/inbcastpkts	
IncePkts	long	/network/incepckts	
IncSumErrors	long	/network/incsumerrors	
Inect0Pkts	long	/network/inect0pkts	
Inect1Pkts	long	/network/inect1pkts	
InMcastOctets	long	/network/inmcastoctets	
InMcastPkts	long	/network/inmcastpkts	
InNoEctPkts	long	/network/innoectpkts	

Variable	Data type	Address	Description
InNoRoutes	long	/network/innoroutes	
InOctets	long	/network/inoctets	Bytes received.
InTruncatedPkts	long	/network/intruncatedpkts	Number of truncated packets received.
IpReversePathFilter	long	/network/ipreversepathfilter	
ListenDrops	long	/network/listendrops	Number of SYNs to LISTEN sockets that were dropped.
ListenOverflows	long	/network/listenoverflows	Number of times the listen queue of a socket overflowed
LockDroppedIcmps	long	/network/lockdroppedicmps	ICMP packets dropped because socket was locked.
OfoPruned	long	/network/ofopruned	Packets dropped from out-of-order queue because of socket buffer overrun.
OutBcastOctets	long	/network/outbcastoctets	
OutBcastPkts	long	/network/outbcastpkts	
OutMcastOctets	long	/network/outmcastoctets	
OutMcastPkts	long	/network/outmcastokts	
OutOctets	long	/network/outoctets	Bytes sent.
OutOfWindowIcmps	long	/network/outofwindowicmps	ICMP packets dropped because they were out-of-window.
PAWSActive	long	/network/pawsactive	Active connections rejected because of timestamp.
PAWSEstab	long	/network/pawsestab	Packets rejected in established connections because of timestamp.
PAWSPassive	long	/network/pawspassive	Passive connections rejected because of timestamp.

Variable	Data type	Address	Description
PruneCalled	long	/network/prunecalled	Packets pruned from receive queue because of socket buffer overrun.
RcvPruned	long	/network/rcvpruned	Packets pruned from receive queue.
SyncookiesFailed	long	/network/syncookiesFailed	Number of invalid SYN cookies received.
SyncookiesRecv	long	/network/syncookiesrecv	Number of SYN cookies received.
SyncookiesSent	long	/network/syncookiesent	Number of SYN cookies sent.
TCPAbortFailed	long	/network/tcpabortfailed	Number of times unable to send RST due to no memory.
TCPAbortOnClose	long	/network/tcpabortonclose	Connections reset due to early user close.
TCPAbortOnData	long	/network/tcpabortondata	Connections reset due to unexpected data.
TCPAbortOnLinger	long	/network/tcpabortonlinger	Connections aborted after user close in linger timeout.
TCPAbortOnMemory	long	/network/tcpabortonmemory	Connections aborted due to memory pressure.
TCPAbortOnSyn	long	/network/tcpabortonsync	Connections reset due to unexpected SYN.
TCPAbortOnTimeout	long	/network/tcpabortontimeout	Connections aborted due to timeout.
TCPAckSkippedChallenge	long	/network/tcpackskippedchallenge	
TCPAckSkippedFinWait2	long	/network/tcpackskippedfinwait2	
TCPAckSkippedPAWS	long	/network/tcpackskippedpaws	
TCPAckSkippedSEQ	long	/network/tcpackskippedseq	
TCPAckSkippedSYNRecv	long	/network/tcpackskippedsynrecv	
TCPAckSkippedTimeWait	long	/network/tcpackskippedtimewait	

Variable	Data type	Address	Description
TCPAutoCorking	long	/network/tcpautocorking	
TCPBacklogDrop	long	/network/tcpbacklogdrop	
TCPChallengeAck	long	/network/tcpchallengeack	
TCPDeferAcceptDrop	long	/network/tcpdeferacceptdrop	
TCPDirectCopyFromBacklog	long	/network/tcpdirectcopyfrombacklog	Bytes directly in process context from backlog.
TCPDirectCopyFromPrequeue	long	/network/tcpdirectcopyfromprequeue	Bytes directly received in process context from prequeue.
TCPDSACKIGNoRedNoUndo	long	/network/tcpdsackignoreundo	
TCPDSACKIGNoRedOld	long	/network/tcpdsackignoreold	
TCPDSACKOfoRecv	long	/network/tcpdsackoforecv	DSACKs for out of order packets
TCPDSACKOfoSent	long	/network/tcpdsackofosent	DSACKs sent for out of order packets.
TCPDSACKOldSent	long	/network/tcpdsackoldsent	DSACKs sent for old packets.
TCPDSACKRecv	long	/network/tcpdsackrecv	DSACKs received.
TCPDSACKUndo	long	/network/tcpdsackundo	Congestion window recovered without slow start using DSACK.
TCPFACKReorder	long	/network/tcpfackreorder	Number of times reordering was detected using FACK.
TCPFastOpenActive	long	/network/tcpfastopenactive	
TCPFastOpenActiveFailL	long	/network/tcpfastopenactivefail	
TCPFastOpenCookieReqD	long	/network/tcpfastopencookiereqd	
TCPFastOpenListenOverflow	long	/network/tcpfastopenlistenoverflow	
TCPFastOpenPassive	long	/network/tcpfastopenpassive	
TCPFastOpenPassiveFail	long	/network/tcpfastopenpassivefail	

Variable	Data type	Address	Description
TCPFastRetrans	long	/network/tcpfastretrans	Fast retransmits.
TCPForwardRetrans	long	/network/tcpforwardretrans	Forward retransmits.
TCPFromZeroWindowAdv	long	/network/tcpfromzerowindowadv	
TCPFullUndo	long	/network/tcpfullundo	Congestion windows fully recovered without slow start.
TCPHPAcks	long	/network/tcphpacks	Predicted acknowledgments.
TCPHPHits	long	/network/tcphphits	Packet headers predicted.
TCPHPHitsToUser	long	/network/tcphphitstouser	Packet headers predicted and directly queued to user.
TCPHYStartDelayCWND	long	/network/tcphystartdelaycwnd	
TCPHYStartDelayDetect	long	/network/tcphystartdelaydetect	
TCPHYStartTrainCWND	long	/network/tcphystarttraincwnd	
TCPHYStartTrainDetect	long	/network/tcphystarttraindetect	
TCPKeepAlive	long	/network/tcpkeepalive	Number of ACK packets sent to keep TCP flow alive.
TCPLossFailures	long	/network/tcplossfailures	Timeouts in loss state.
TCPLossProbeRecovery	long	/network/tcplossproberecovery	
TCPLossProbes	long	/network/tcplossprobes	
TCPLossUndo	long	/network/tcplossundo	Congestion windows recovered without slow start after partial ack.
TCPLostRetransmit	long	/network/tcplostretransmit	Retransmit lost.
TCPMD5NotFound	long	/network/tcpmd5notfound	
TCPMD5Unexpected	long	/network/tcpmd5unexpected	
TCPMemoryPressures	long	/network/tcpmemorypressures	Number of times TCP ran low on memory.
TCPMINTTLDrop	long	/network/tcpminttldrop	

Variable	Data type	Address	Description
TCPMTUPFail	long	/network/tcpmtupfail	
TCPMTUPSuccess	long	/network/tcpmtupsuccess	
TCPOfoDrop	long	/network/tcpofodrop	
TCPOfoMerge	long	/network/tcpofomerge	
TCPOfoQueue	long	/network/tcpofoqueue	
TCPOrigDataSent	long	/network/tcporigdatasent	
TCPPartialUndo	long	/network/tcppartialundo	Congestion windows partially recovered using Hoe heuristic.
TCPPrequeued	long	/network/tcpprequeued	Packets directly queued to recvmg prequeue.
TCPPrequeueDropped	long	/network/tcpprequeuedropped	Packets dropped from prequeue.
TCPPureAcks	long	/network/tcppureacks	Acknowledgments not containing data payload received.
TCPRcvCoalesce	long	/network/tcprcvcoalesce	
TCPRcvCollapsed	long	/network/tcprcvcollapsed	Packets collapsed in receive queue due to low socket buffer.
TCPRenoFailures	long	/network/tcprenofailures	Timeouts after reno fast retransmit.
TCPRenoRecovery	long	/network/tcprenorecovery	Times recovered from packet loss due to fast retransmit.
TCPRenoRecoveryFail	long	/network/tcprenorecoveryfail	Classic Reno fast retransmits failed.
TCPRenoReorder	long	/network/tcprenoreorder	
TCPreqQFullDoCookies	long	/network/tcpreqqfulldocookies	
TCPreqQFullDrop	long	/network/tcpreqqfulldrop	
TCPretransFail	long	/network/tcpretransfail	

Variable	Data type	Address	Description
TCPSACKDiscard	long	/network/tcpsackdiscard	
TCPSACKFailures	long	/network/tcpsackfailures	Timeouts after SACK recovery.
TCPSACKMerged	long	/network/tcpsackmerged	
TCPSACKRecovery	long	/network/tcpsackrecovery	Times recovered from packet loss by selective acknowledgements.
TCPSACKRecoveryFail	long	/network/tcpsackRecoveryFails	SACK retransmits failed.
TCPSACKReneging	long	/network/tcpsackreneging	Bad SACK blocks received.
TCPSACKReorder	long	/network/tcpsackreorder	Number of times reordering was detected using SACK.
TCPSACKShifted	long	/network/tcpsackshifted	
TCPSACKShiftFallback	long	/network/tcpsackshiftfallback	
TCPSchedulerFailed	long	/network/tcpschedulerfailed	Times receiver scheduled too late for direct processing.
TCPSlowStartRetrans	long	/network/tcpslowstartretrans	Retransmits in slow start.
TCPSpuriousRTOS	long	/network/tcpspuriousrtos	
TCPSpuriousRTXHostQueues	long	/network/tcpspuriousrtxhostqueues	
TCPSYNChallenge	long	/network/tcpsynchallenge	
TCPSYNRetrans	long	/network/tcpsynretrans	
TCPTimeouts	long	/network/tcptimeouts	Other TCP timeouts.
TCPTimeWaitOverflow	long	/network/tcptimewaitoverflow	
TCPToZeroWindowAdv	long	/network/tcptozerowindowadv	
TCPTSReorder	long	/network/tcptstreorder	Number of times reordering was detected using timestamp.
TCPWantZeroWindowAdv	long	/network/tcpwantzerowindowadv	

Variable	Data type	Address	Description
TCPWinProbe	long	/network/tcpwinprobe	Number of ACK packets to be sent at regular intervals to make sure a reverse ACK packet opening back a window has not been lost.
TW	long	/network/tw	
TWKilled	long	/network/twkilled	TCP sockets finished time wait in slow timer.
TWRecycled	long	/network/twrecycled	Time wait sockets recycled by timestamp.

6.6 Overview of Rockwell protocol for MindConnect Software Agent

The following image shows the data source input window for the Rockwell protocol:



Rockwell data source parameter

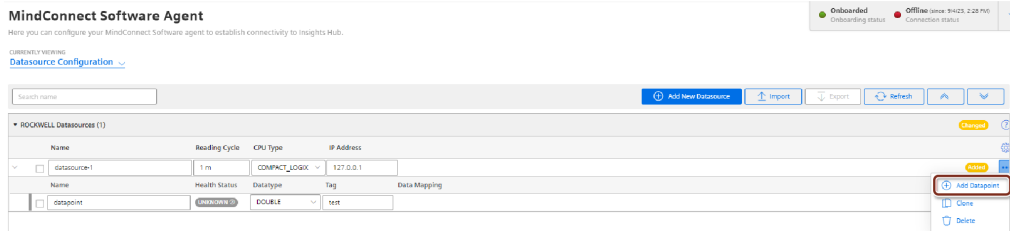
In order to connect a Rockwell device, you need to select the Rockwell protocol and enter the following data source parameters:

Parameter	Description
CPU type	Shows available CPU types: - COMPACT_LOGIX - CONTROL_LOGIX - MICRO_800 - OTHER_CPU Currently not available: - FLEX_LOGIX - MICRO_LOGIX - SOFT_LOGIX - PLC5 - SLC500

Parameter	Description
IP address	IP address of the Rockwell controller.
Route parameters	Here you can define the routing path parameters - like rack, slot, node, and/or ControlNet port numbers - needed to access the controller (default: 1,0).

Rockwell data point parameter

In order to collect the data of your Rockwell device, click "Add Datapoint" to add new datapoint.



The following table shows the data point parameter:

Parameter	Description
Data Type	Data type supported by backend (e.g. INT).
Tag	Name of the tag that has to be recorded.


The following table shows the recommended data type selection:

Rockwell data type	Length	Data range ¹	Industrial IoT Data type
BOOL	1 bit	0 or 1	BOOLEAN
SINT	1 byte	-128...+127	INT
USINT ²	1 byte	0...255	INT
INT	2 bytes	-32,768...+32,767	INT
UINT ²	2 bytes	0...65,535	INT
DINT	4 bytes	-2,147,483,648...+2,147,483,647	INT
UDINT ²	4 bytes	0...4,294,967,295	INT
REAL	4 bytes	- 3.40282347E38...-1.17549435E-38 (negative values) - 0 - 1.17549435E-38-...3.40282347E38 (positive values)	DOUBLE

Rockwell data type	Length	Data range ¹	Industrial IoT Data type
SSTRING ²	0 .. 255 bytes	ASCII	STRING
STRING ²	0 .. 255 bytes	ASCII	STRING

¹" Values have been taken from Logix 5000 Controllers I/O and Tag Data Programming Manual.

²" Available since MindConnect Nano/IoT2040 V03.04.04.03 b001, MCSA V03.06.00.17 b003, D-MCSA V03.06.02.02 b002 and MindConnect IoT2050 V03.07.00.03 b003.



PCL data types

Currently only these PLC data types are supported.


6.7 Overview of S7+ protocol for MindConnect Software Agent

The following image shows the data source input window for the S7+ protocol:



In order to connect a S7+ device, you need to select the S7+ protocol and enter the following data source parameters:

Parameter	Description
IP Address	IP address or hostname of the S7+ device
PLC Type	The following PLCs are supported: - S7-1200 - S7-1500 - S7-1500 Software Controller - ET200SP - PLCSIM (Advanced)

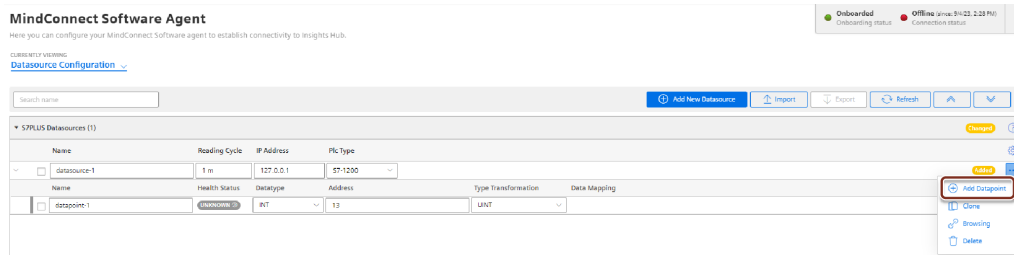


Maximum limit for the number of connections is 64.

S7+ data point parameter

In order to collect the data of your S7+ device, click "Add Datapoint" to add new datapoint.

The following image shows the data point parameter window:



The following table shows the parameter of the S7+ data point window:

Parameter	Description
Datapoint type	The following datapoint types are supported: - int - long - double - boolean - string
Datapoint Address	The PLC connection must be available (symbolic addressing is used).
Type Transformation	The transformation type is the interpretation of data of the peripheral device. For the datatypes above the following transformation types are available (see also table below): - int: UINT, USINT, UDINT, SINT, INT, DINT, WORD, BYTE, DWORD - long: UINT, USINT, UDINT, ULINT, SINT, INT, DINT, LINT, WORD, BYTE, DWORD, LWORD, DATE, DATETIME, TIME, TIME_OF_DAY, LDATETIME, LTIME, LTOD, DTL, S5TIME - double: REAL, LREAL - boolean: BOOL - string: STRING, WSTRING, DATE, DATETIME, TIME, TIME_OF_DAY, LDATETIME, LTIME, LTOD, DTL, S5TIME
Data Acquisition Mode	The following modes are supported: - READ - WRITE - READ and WRITE

The following table shows the transformation type of the S7+ data point window:

Transformation type	Description
BOOL	Boolean
BYTE	8 bit integer unsigned
WORD	Bit field (16 bit)

Transformation type	Description
DWORD	Bit field (32 bit)
LWORD	Bit field (64 bit)
USINT	8 bit integer unsigned
UINT	16 bit integer unsigned
UDINT	32 bit integer unsigned
ULINT	64 bit integer unsigned
SINT	8 bit integer signed
INT	16 bit integer signed
DINT	32 bit integer signed
LINT	64 bit integer signed
REAL	32 bit float
LREAL	64 bit float
DATE	Date, number of days since 1.1.1970
DATETIME	Date and time
TIME	Time in milliseconds (32 bit), value range from -24d 20h 31m 23s 648ms to +24d 20h 31m 23s 647ms
TIME_OF_DAY	Number of milliseconds since start of the day (32 bit)
LDATETIME	Date and time
LTIME	Time in nanoseconds (64 bit), value range from -106751d 23h 47m 16s 854ms 775us 808ns to +106751d 23h 47m 16s 854ms 775us 807ns
LTOD	Number of milliseconds since start of the day (64 bit)
DTL	12 Byte struct, value range from 1970-01-01-00:00:00.0 to 2554-12-31-23:59:59.999999999 (steps in nanoseconds)
S5TIME	Time in milliseconds (16 bit), value range from 0h 0m 0s 0ms to 2h 46m 30s 0ms
STRING	String (8 bit characters)
WSTRING	String (16 bit characters)

6.8 Overview of Fanuc Focas protocol for MindConnect Software Agent



This protocol is supported for Windows based application only.

The following image shows the data source input window for the Fanuc Focas protocol:



The following device types are supported:

- FS31i-A
- FS35i-B
- FS0i-D
- FS32i-B
- PMi-A
- FS30i-B
- FS0i-F Plus iHMI
- FS0i-F
- FS0i-F Plus
- FS30i-B 32AX
- FS30i-B 48AX
- FS30i-B iHM
- FS30i-B Plus
- FS31i-B Plus
- FS31i-B
- FS31i-B5 Plus
- FS31i-B5
- FS31i-LB
- FS31i-PB
- FS31i-WB

- FS32i-B Plus

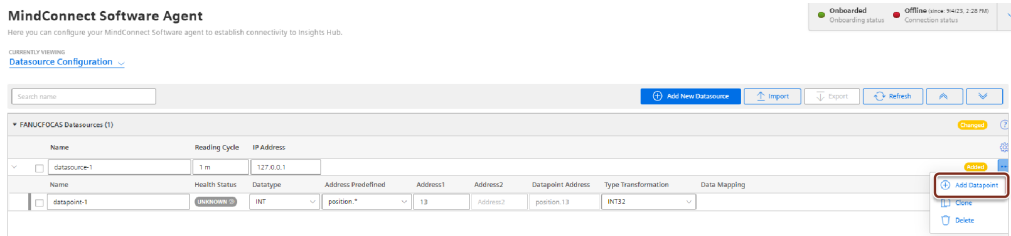
In order to connect a Fanuc Focas device, you need to select the Fanuc Focas protocol and enter the following data source parameter:

Parameter	Description
IP Address	The IP address (and optional port – separated by ‘:’) of the device must be filled in Datasource.

Fanuc Focas data point parameter

In order to collect the data of the Fanuc Focas device, click "Add Datapoint" to add new datapoint.

The following picture shows the data point parameter window:



Follow the simple rules to fill the parameters for the Fanuc Focas:


1. Choose a predefined component for the Datapoint Address.
2. For every "*" or "?" in the listed item an extra field is displayed, which must be filled as per above example screenshot.
3. The field "Datapoint Address" is the final address string and displayed read only. It is the result of selected address with combo boxes and user defined parts.
4. The fields "Type" and "Type Transformation" are limited to the possible types, depending on the selection of the address component.

The following table shows the parameter of the all components, including possible datatype, explanation and example:

Address	Data type	Comment
position. Example: position. *(0... ⁹⁹	- int32, - default supported	The function can read the position of a defined axis or of all axis. Note: When reading ALL_AXIS the output structure is model dependent.
programblock.<number > number values: 1...Program name, 2...Block number	- string(1), - int32(2), - default supported	The function reads always both items.

Address	Data type	Comment
alarmstring	- string, - default supported	These two alarm functions are mapped to a string.
pmcdata... Example: pmcdata. *(0...99; 0...65535	Depends on transformation: - int8, int16, int32, float, double	With this function you can read different type of data from PMC address range. The "adrttype" specifies different address ranges. For the various models of CNC machines different ranges of different size exist. It is the responsibility of the user to configure the address in the correct range. The driver will not check range depending on the model.
modal.. . number values: 1...data, *(0...3), 2...flag1, *(0...3), 3...flag2, *(0... ³	- int32(1), - uint8(2), - uint8(3), - default supported	This function call is rather complex and comprises a lot or variation. The Fanuc Focas driver only supports the type = 108 variant for current active T code. The resulting data comprises a "4-byte" data field and two "1-byte" flag fields. The interpretation of these fields is machine model dependent, but this must be done by the application.
statinfo.<number> number values: *(0...99) see comment for value meaning.	- int16, - default supported	All elements are read with one function call. There are several more but according to requirements they are not needed. 1. hdck: Status of manual handle retrace; 2. tmmode: T/M mode selection; 3. aut: AUTO/MANUAL mode selection; 4. run: Status of automatic operation; 5. motion: Status of axis movement,dwell; 6. mstb: Status of M,S,T,B function; 7. emergency: Status of emergency; 8. alarm: Status of alarm; 9. edit: Status of program editing
param. <paramnumber>.<axis number>. Example: param. * (0...32767;0...99)	Depends on transformation: - boolean, - int8, - int16, - int32	The parameters are dependent on the axis or axis independent (axisnumber 0).
For axis specific parameter, it is possible to read the parameter for all axis or only for a specific axis.		


Address	Data type	Comment
diag.<diagnumber>.<axisnumber>, * (0...32767;0...99)	Depends on transformation: - boolean, - int8, - int16, - int32, - float	There are diagnosis values with the axis dependent, and axis independent (axisnumber 0). For axis specific diagnosis values, it is possible to read the values for all axis or only for a specific axis.
feedrate	- int32, - default supported	One function for one value.
spindlespeed	- int32, - default supported	One function for one value.
sysinfo	- string	Maximum length of read value is 20 characters. format:<cn c_type><series><version><mt_type>

 You need to ensure the parameters entered are valid for Fanuc Focas protocol.

6.9 Overview of Sinumerik protocol for MindConnect Software Agent

The following image shows the data source input window for the Sinumerik protocol:



 The supported device types are S7 SINUMERIK, example S7 840D sl.

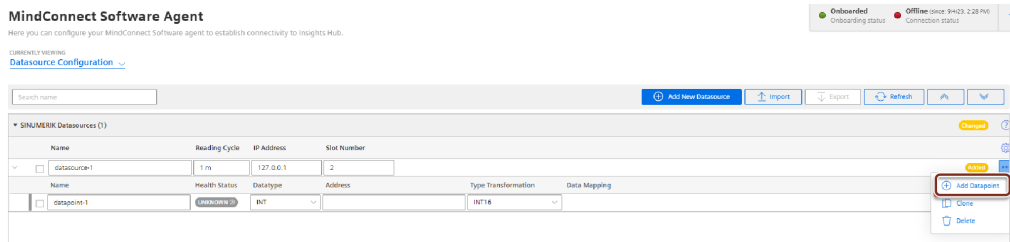
In order to connect a Sinumerik device, you need to select the Sinumerik protocol and enter the following data source parameters:

Parameter	Description
IP Address	IP address of the device.

Parameter	Description
Slot Number	Choose the correct slot number, where the "NC unit" of the device is mounted.

Sinumerik data point parameter

In order to collect the data of the Sinumerik device, click "Add Datapoint" to add new datapoint. The following picture shows the data point parameter window:



The following table shows the parameter of the Sinumerik data point window:

Parameter	Description
Datapoint Address	Peripheral address strings in WinCC OA must be entered in a symbolic manner using the Siemens BTSS format. Examples: S7Conn1./Nck/Spindle/speedOvr[1], NCK2.@SinumerikErrors@
Type	The following datapoint types are supported: - int, - long, - double, - boolean, - string
Type Transformation	For the above datatypes, the following transformation types are available (see also table below): - int: INT16, INT32, UINT16, UINT32, BYTE; - long: INT16, INT32, UINT16, UINT32, BYTE, DATETIMELONG; - double: FLOAT, DATETIMELONG; - boolean: BIT; - string: STRING, DATETIMELONG, BLOB
Data Acquisition Mode	The following modes are supported: - READ, - WRITE, - READ and WRITE

The following table shows the transformation type of the Sinumerik data point window:

Transformation type	Description
---------------------	-------------

Transformation type	Description
UNDEFINED	Default
INT16	16 Bit Integer signed
INT32	32 Bit Integer signed
UINT16	16 Bit Integer unsigned
BYTE	Byte
FLOAT	Floating-point value
BIT	Boolean
STRING	Text
UINT32	32 Bit Integer unsigned
DATETIME	Date/Time variable (used for S7 300 and S7 400 models)
BLOB	Blob
BITSTRING	Bit pattern
DATETIMELONG	Date/Time variable (used for S7 1200 models)

6.10 Overview of IEC61850 protocol for MindConnect Software Agent

IEC61850 defines an architecture to meet the needs of electrical substation automation. It defines a data model and the communication services for the interaction with and between the elements of a substation such as feeders, breakers, protection devices, etc.


The following image shows the data source input window for the IEC61850 protocol:



In order to connect a IEC61850 device, you need to select the IEC61850 protocol and enter the following data source parameters:

Parameter	Description
-----------	-------------

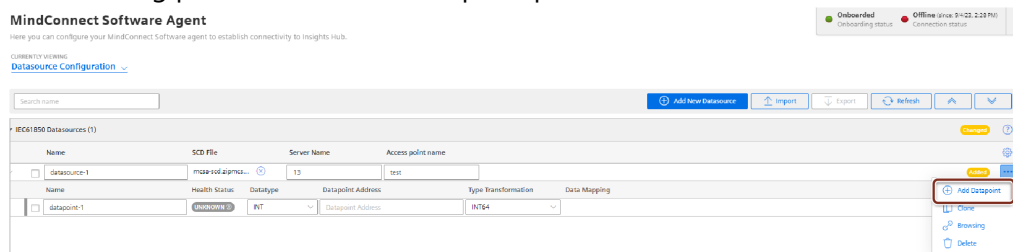
Parameter	Description
SCD File	Choose a valid SCD file. It contains the connection details (IP address, server name, access point) and the data (logical nodes, data types, data points, ...). The SCD File must have a valid extension: *.xml, *.zip, *.tgz, *.tar.gz.
Server Name	Name of the Intelligent Electronic Devices (IED) must match to the SCD file.
Access point name	Name of the access point must match to the SCD file.



- The IED name within the SCD file must be set to "Industrial IoT Client" or to the serial number of the device.
- Server Name and Access point must match with the data in the SCD file. It is necessary for a double check of the configuration.

IEC61850 data point parameter

In order to collect the data of the IEC61850 device, click "Add Datapoint" to add new datapoint. The following picture shows the data point parameter window:



The following table shows the parameter of the IEC61850 data point window:

Parameter	Description
Datapoint Address	The browse string, as defined in the SCD file. Example: MSC_SRV01CTRL / ATCC1 \$ST\$HiTapPos\$stVal
Type	The following datapoint types are supported: int, long, double, boolean, string

Parameter	Description
Type Transformation	For the above datatypes, the following transformation types are available (see also table below): - int: INT8, INT16, INT32, INT64, UINT8, UINT16, UINT32; - long: INT8, INT16, INT32, INT64, UINT8, UINT16, UINT32, BITSTRING, TIMESTAMP; - double: FLOAT32, FLOAT64, INT32, INT64, UINT8, UINT16, UINT32, BITSTRING, TIMESTAMP; - boolean: BOOL; - string: OCTET_STRING64, VISIBLE_STRING64, VISIBLE_STRING255, TIMESTAMP
Data Acquisition Mode	The following modes are supported: READ (spontaneous / reports), WRITE READ and WRITE

6.11 Overview of MTConnect protocol for MindConnect Software Agent

MTConnect is a manufacturing technical standard to retrieve process information from numerically controlled machine tools.

The following image shows the data source input window for the MTConnect protocol:



In order to connect a MTConnect device, you need to select the MTConnect protocol and enter the following data source parameter:

Parameter	Description
URL	The URL of the MTConnect device. The port is also part of the URL. Example: <code>http://mtconnect.mazakcorp.com:5610/</code>

MTConnect data point parameter

In order to collect the data of the MTConnect device, click "Add Datapoint" to add new datapoint.

The following picture shows the data point parameter window:



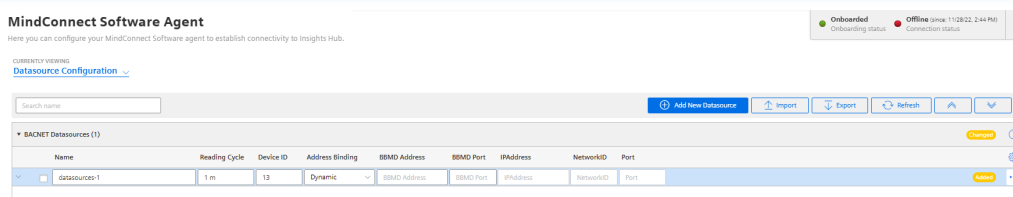
The following table shows the parameter of the MTConnect data point window:

Parameter	Description
Datapoint Address	ID of the DataItem from the MTConnect device. Example (excerpt of an xml-file): <code><DataItem category="SAMPLE" coordinateSystem="MACHINE" id="xpm" name="Xabs" nativeUnits="MILLIMETER" subType="ACTUAL" type="POSITION" units="MILLIMETER" /></code> → Datapoint Address: xpm
Type	The following datapoint types are supported: int, long, double, boolean, string

6.12 Overview of BACnet protocol for MindConnect Software Agent

BACnet (Building Automation and Control Networks) is a normed protocol for building automation and was designed by ASHRAE (American Society of Heating, Refrigerating and Air-Conditioning Engineers) in order to provide a consistent and intra-operative standard for data communication in and with systems of building automation.

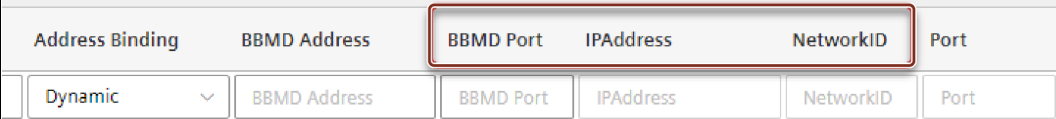
- When you attempt to browse online, If your device is not reachable or the configuration does not match the actual device(such as an incorrect IP address or device ID),default browsing result is displayed which displays the supported object types and their property types.
- BACNet is limited to Port 1(Production network). Port 2 cannot be used for BACNet connection.



Parameters

Parameters required to set BACnet are,

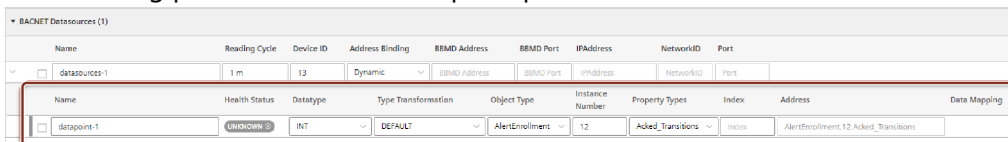
The following table shows the parameter of the BACnet window:

Parameter	Description
Device ID	The unique identification number for the BACnet device.
Address Binding	<p>There are two possibilities to set the BACnet/IP address for a device</p> <p>Dynamic : If dynamic is selected, the address is assigned dynamically where the driver determines the BACnet/IP address from the BACnet devices.</p> <p>Static : If Static is selected, the BACnet/IP address must be allocated by the user, thus an automatic update is not performed. If there is a change in the information it must be updated manually by the user in the adequate fields as shown below:</p>  <p>The highlighted parameters in the above image are the mandatory parameters to be entered.</p> <p>BACnet IPAddress : IP address of the BACnet device (If the same IP address or Device Id is used twice, only one connection can be established).</p> <p>BACnet Port : The UDP port for the communication to the BACnet device.</p> <p>BACnetNetwork ID : The number of network ID the device resides (max. 65535).</p>
BBMD IpAddress	Broadcast Management Device IP Address.
BBMD Port	Broadcast Management Device Port Number

BACnet – Datapoint

In order to collect the data of the BACnet device, click "Add Datapoint" to add new datapoint.

The following picture shows the datapoint parameter window:



The following table shows the parameters of the BACnet data point,

Parameter	Description
Type	<p>The following datapoint types are supported:</p> <ul style="list-style-type: none"> - int - long - double - boolean - string

Parameter	Description
Type Transformation	For the datatypes, the following transformation types are available: <ul style="list-style-type: none">- Default- Boolean- UnsignedInteger- SignedInteger- Real- Double- Octets- String- BitString- Enummerated- Date- Time- DateTime
Data Acquisition Mode	The following modes are supported: <ul style="list-style-type: none">- READ- WRITE- READ&WRITE

Parameter	Description
BACnet Object Type	<p>The following object types are supported:</p> <ul style="list-style-type: none"> - Accumulator - Accumulator - AnalogInput - AnalogOutput - AnalogValue - Averaging - BinaryInput - BinaryOutput - BinaryValue - BitStringValue - Calendar - CharacterStringValue - Command - DateValue - DatePatternValue - DateTimeValue - DateTimePatternValue - Device - EventEnrollment - GlobalGroup - IntegerValue - LargeAnalogValue - LifeSafetyPoint - LifeSafetyZone - LoadControl - Loop - MultistateInput - MultistateOutput - MultistateValue - NotificationClass - OctetStringValue - PositiveIntegerValue - Program - PulseConverter - Schedule - TimeValue - TimePatternValue - TrendLog - TrendLogMultiple
BACnet Instance Number (Object ID)	<p>The instance of the object provides the unique identification for the type of the objects.</p>
Property types	<p>Each object type has a specific list of Property types; the following are the Property types supported:</p> <ul style="list-style-type: none"> - APDU_Segment_Timeout - APDU_Timeout - Accepted_Modes

Parameter	Description
	<ul style="list-style-type: none"> - Ack_Required - Acked_Transitions - Active_COV_Subscriptions - Active_Text - Active_VT_Sessions - Adjust_Value - Alarm_Value - Alarm_Values - Align_Intervals - All_Writes_Successful - Application_Software_Version - Average_Value - Backup_Failure_Timeout - Buffer_Size - Controlled_Variable_Value - Controlled_Variable_Units - COV_Increment - COV_Period - COV_Resubscription_Interval - Change_Of_State_Count - Change_Of_State_Time - Client_COV_Increment - Configuration_Files - Count - Count_Before_Change - Count_Change_Time - Database_Revision - Date_List - Daylight_Savings_Status - Deadband - Description - Description_Of_Halt - Device_Address_Binding - Device_Type - Derivative_Constant - Derivative_Constant_Units - Direct_Reading - Effective_Period - Elapsed_Active_Time - Enable - Error_Limit - Event_Algorithm_Inhibit - Event_Algorithm_Inhibit_Ref - Event_Detection_Enable - Event_Enable - Event_Message_Texts - Event_Message_Texts_Config - Event_Parameters - Event_State

Parameter	Description
	<ul style="list-style-type: none"> - Event_Time_Stamps - Event_Type - Exception_Schedule - Fault_Values - Feedback_Value - Firmware_Revision - High_Limit - In_Process - Inactive_Text - Input_Reference - Instance_Of - Integral_Constant - Integral_Constant_Units - Interval_Offset - Is_UTC - Last_Notify_Record - Last_Restart_Reason - Last_Restore_Time - Life_Safety_Alarm_Values - Limit_Enable - Limit_Monitoring_Interval - List_Of_Object_Property_References - Local_Date - Local_Time - Location - Logging_Object - Logging_Record - Logging_Type - Log_Buffer - Log_DeviceObjectProperty - Log_Interval - Low_Limit - Maintenance_Required - Max_APDU_Length_Accepted - Max_Info_Frames - Max_Master - Max_Pres_Value - Max_Segments_Accepted - Maximum_Output - Maximum_Value - Member_Of - Min_Pres_Value - Minimum_Off_Time - Minimum_On_Time - Minimum_Output - Minimum_Value - Mode - Model_Name - Notification_Class

Parameter	Description
	<ul style="list-style-type: none"> - Notification_Threshold - Notify_Type - Number_Of_APDU_Retries - Number_Of_States - Object_Identifier - Object_List - Object_Name - Object_Property_Reference - Object_Type - Operation_Expected - Out_Of_Service - Output_Units - Polarity - Prescale - Present_Value - Priority - Priority_Array - Priority_For_Writing - Profile_Name - Program_Change - Program_Location - Program_State - Proportional_Constant - Proportional_Constant_Units - Protocol_Object_Types_Supported - Protocol_Revision - Protocol_Services_Supported - Protocol_Version - Pulse_Rate - Reason_For_Halt - Recipient_List - Record_Count - Records_Since_Notification - Reliability - Reliability_Evaluation_Inhibit - Relinquish_Default - Resolution - Restart_Notification_Recipients - Scale - Scale_Factor - Schedule_Default - Segmentation_Supported - Setpoint - Setpoint_Reference - Setting - Silenced - Start_Time - State_Description - State_Text

Parameter	Description
	<ul style="list-style-type: none"> - Status_Flags - Stop_Time - Stop_When_Full - System_Status - Time_Delay - Time_Delay_Normal - Time_Of_Active_Time_Reset - Time_Of_Device_Restart - Time_Of_State_Count_Reset - Time_Synchronization_Recipients - Tracking_Value - Total_Record_Count - Trigger - UTC_Offset - Units - Update_Interval - Update_Time - VT_Classes_Supported - Value_Before_Change - Value_Change_Time - Value_Set - Vendor_Identifier - Vendor_Name - Weekly_Schedule - Zone_Members - _Error
Index	<p>The index provides the referencing of an element in an array. If the array index is not specified, the whole array will be mapped.</p>

7.1 Data center locations

You can license Insights Hub on different regions in various data centers.

The following table shows the regions and the data center location for each region:

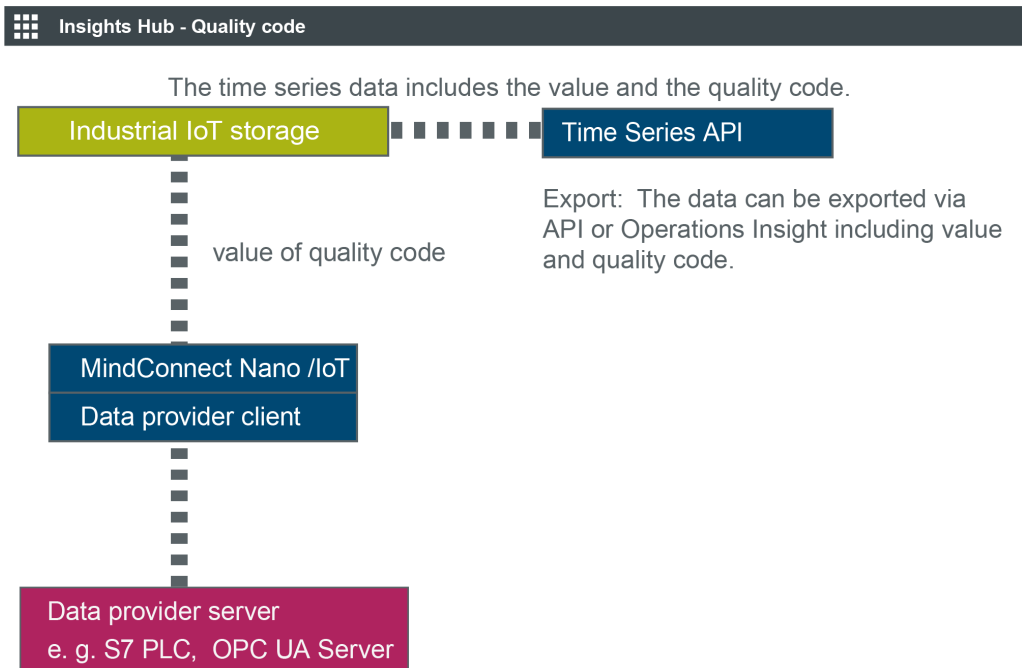
Region	Data center location	infrastructure provider
Europe 1	Frankfurt, Germany (eu1)	Amazon Web Services
China 1	Shanghai, China (cn1)	Alibaba Cloud

7.2 Using quality code

The quality code measures the quality of the connection from a data provider to the MindConnect Software Agent.

If you export the time series value (e.g. with Insights Hub Monitor) you can see the data points with its connected quality code. This helps you to analyze time ranges where no data is available. This will avoid drawing false conclusions from a null value.

The following graphic shows a dataflow overview of the quality code:



If the data provider (e.g. S7 PLC, OPC UA Server) is healthy it sends the Quality Code as 0 and if there are issues depending on protocol usage, the value is non Zero indicating the issue matching quality code.

7.3 Quality codes OPC UA and S7 protocol

The following table is based on the OPC UA standard and shows the possible quality codes for OPC UA and S7:

Quality code (hex)	Quality code (dec)	Short description	Long description
0x00000000	0	GOOD	Good, all items could be read.
0x00BA0000	12189696	GOOD_INCOMPLETE	Good results may be incomplete - at least one item could be read.
0x002F0000	3080192	GOOD_OVERLOAD	Sampling has slowed down due to resource limitations.
0x40920000	1083310080	UNCERTAIN_INITIAL_VALUE	Uncertain Initial Value - initial value.
0x80000000	-2147483648	BAD	Bad - generic error.
0x80020000	-2147352576	BAD_INTERNAL_ERROR	An internal error occurred as a result of a programming or configuration error.

Quality code (hex)	Quality code (dec)	Short description	Long description
0x80050000	-2147811328	BAD_COMMUNICATION_ERROR	A low level communication error occurred.
0x80090000	-2146893824	BAD_UNKNOWN_RESPONSE	An unrecognized response was received from the server.
0x800A0000	-2146828288	BAD_TIMEOUT	Bad Timeout - Timeout occurred.
0x800B0000	-2146762752	BAD_SERVICE_UNSUPPORTED	Bad Service Unsupported - service unsupported.
0x80100000	-2146435072	BAD_TOO_MANY_OPERATIONS	Bad Too Many Operations - The request could not be processed because it specified too many operations.
0x80130000	-2146238464	BAD_SECURITY_CHECKS_FAILED	Indicates security problems.
0x801F0000	-2145452032	BAD_ACCESS_DENIED	Bad Access Denied - Access denied.
0x80210000	-2145320960	BAD_IDENTITY_TOKEN_REJECTED	Bad Identity Token Rejected.
0x80330000	-2144141312	BAD_NODE_ID_INVALID	The syntax of the node ID is not valid.
0x80340000	-2144075776	BAD_NODE_ID_UNKNOWN	Bad item address.
0x80360000	-2143944704	BAD_INDEX_RANGE_INVALID	The syntax of the index range parameter is invalid.
0x803A0000	-2143682560	BAD_NOT_READABLE	Read operation(s) has problem.
0x803B0000	-2143617024	BAD_NOT_WRITABLE	Write operation(s) has problem.
0x803D0000	-2143485952	BAD_NOT_SUPPORTED	Operation is not supported.
0x803E0000	-2143420416	BAD_NOT_FOUND	A requested item was not found or a search operation ended without success.
0x804F0000	-2142306304	BAD_SERVER_URI_INVALID	The ServerUri is not a valid URI.
0x80740000	-2139881472	BAD_TYPE_MISMATCH	Type conversion has problem.
0x807D0000	-2155675648	BAD_TCPSERVER_TOO_BUSY	The server cannot process the request because it is too busy.
0x80820000	-2138963968	BAD_TCP_INTERNAL_ERROR	TCP internal error occurred.
0x80860000	-2138701824	BAD_SECURE_CHANNEL_CLOSED	The secure channel has been closed.

Quality code (hex)	Quality code (dec)	Short description	Long description
0x80890000	-2138505216	BAD_CONFIGURATION_ERROR	Lack of configuration info.
0x808D0000	-2138243072	BAD_OUT_OF_SERVICE	OPC service has problems.
0x809B0000	-2137325568	BAD_NO_DATA	No data exists for the requested time range or event filter.
0x809D0000	-2137194496	BAD_DATA_LOST	Data is missing due to collection started/stopped/lost.
0x80AB0000	-2136276992	INVALID_ARGUMENT	Bad Invalid Argument - all items could not be read.
0x80AC0000	-2136211456	BAD_CONNECTION_REJECTED	Connection problem.
0x80AD0000	-2136145920	BAD_DISCONNECT	The server has disconnected from the client.
0x80AF0000	-2136014848	BAD_INVALID_STATE	The operation cannot be completed because the object public String getValue() { return value; } is closed.
0x80B80000	-2135425024	BAD_REQUEST_TOO_LARGE	Request too large.
0x80D70000	-2133393408	BAD_BOUND_NOT_FOUND	No data found to provide upper or lower bound value.

7.4 Quality codes Modbus protocol

The following table shows the possible quality codes for devices that use the Modbus protocol:

Quality code (hex)	Quality code (dec)	Short description	Long description
0x00000000	0	Good	No error occurred
0x80050000	-2147155968	Communication error	Modbus connection reset for connection
0x80310000	-2144272384	No communication	Communication with the data source is defined but not established and there is no last known value available
0x803A0000	-2143682560	Not readable	The access level does not allow reading or subscribing to the node

Quality code (hex)	Quality code (dec)	Short description	Long description
0x80790000	-2139553792	No subscription	There is no subscription available for this session
0x80AB0000	-2136276992	Invalid argument	One or more arguments are invalid
0x80330000	-2144141312	NodeIdInvalid	Parser bad node syntax
0x809E0000	-2137128960	Data unavailable	Expected data is unavailable for the requested time range due to an unmounted volume, an offline archive or tape, or similar reason for temporary unavailability
0x809F0000	-2137063424	Entry exists	The data or event was not successfully updated because no matching entry exists
0x803C0000	-2143551488	Out of range	The value was out of range
0x80270000	-2144927744	Session not activated	The session cannot be used because ActivateSession has not been called
0x808B0000	-2138374144	Device failure	There has been a failure in the device/data source that generates the value that has affected the value
0x803D0000	-2143485952	Not supported	The server cannot retrieve a bound for the variable
0x80630000	-2140995584	Type definition invalid	The type definition node ID does not reference an appropriate type node
0x800D0000	-2146631680	Server not connected	The operation could not complete because the client is not connected to the server.
0x80730000	-2139947008	Write not supported	The server does not support writing the combination of value status and timestamps provided
0x807D0000	-2139291648	Data source busy	Previous read request of data source is still in progress

7.5 Quality codes SYSTEM protocol

The following table shows the possible quality codes for devices that use the SYSTEM adapters:

Quality code (hex)	Quality code (dec)	Short description	Long description
0x00000000	0	Good	No error occurred

Quality code (hex)	Quality code (dec)	Short description	Long description
0x803A0000	-2151284736	Not readable	The access level does not allow the operation the to the Node (reading or subscribing)
0x807D0000	-2139291648	Data source busy	Previous read request of data source is still in progress

7.6 Quality codes Rockwell protocol

The following table shows the possible quality codes for devices that use the Rockwell protocol:

Quality code (hex)	Quality code (dec)	Short description	Long description
0x00000000	0	Good	No error occurred
0x80010000	-2147418112	Unexpected error	An unexpected error occurred
0x80020000	-2147352576	Internal error	An internal error occurred
0x80030000	-2147287040	Out of memory	Not enough memory for operation
0x80050000	-2147155968	Communication error	Connection to device failed
0x80090000	-2146893824	Unknown response	Received an unsolicited message
0x800A0000	-2146828288	Timeout	The operation timed out
0x800B0000	-2146762752	Service unsupported	Service is not supported
0x800F0000	-2146500608	Nothing to do	Nothing to send
0x801F0000	-2145452032	Access denied	User does not have permission for requested operation
0x80330000	-2144141312	Invalid tag	Requested item (tag) is not known
0x805E0000	-2141323264	Node does not exist	Info file does not exist
0x80630000	-2140995584	Invalid type definition	The type definition does not reference an appropriate type
0x80740000	-2139881472	Type mismatch	Data type is not supported
0x80780000	-2139619328	Too many publish requests	Pending buffer is full

Quality code (hex)	Quality code (dec)	Short description	Long description
0x807D0000	-2139291648	Data source busy	Previous read request of data source is still in progress
0x80840000	-2138832896	Request interrupted	Request interrupted
0x80850000	-2138767360	Request timeout	Receive timeout occurred
0x80B10000	-2135883776	No data available	No more data available
0x80B60000	-2135556096	Invalid syntax	Syntax error
0x80B80000	-2135425024	Request too large	Buffer is too small
0x80CE0000	-2133983232	Invalid response	Received an invalid reply

7.7 Quality codes S7+, Fanuc Focas, Sinumerik, IEC61850 and MTConnect

The following table shows the possible quality codes for devices that use the S7+, Fanuc Focas, Sinumerik, IEC61850 and MTConnect protocol:

Quality code (hex)	Quality code (dec)	Short description	Long description
0x00000000	0	GOOD	Value quality is good
0x80AD0000	-2136145920	BAD_DISCONNECT	The device is not connected
0x80AC0000	-2136211456	BAD_CONNECTION_REJECTED	The device is deactivated
0x80AB0000	-2136276992	INVALID_ARGUMENT	Invalid value (marked by device or our driver)

7.8 Offline buffer

In order to calculate the buffer time for MindConnect Software Agent you can use the following formula:

$$\text{Buffer time} = \frac{\text{Buffer size}}{\text{Number of data points (Read cycle)} * \text{Bytes per data point}}$$

MindConnect Software Agents data buffer is 500 MB. When the buffer is at full capacity, the new incoming data will overwrite the oldest data.

The following example shows the buffer time for a MindConnect Software Agent with 500 MB data buffer:

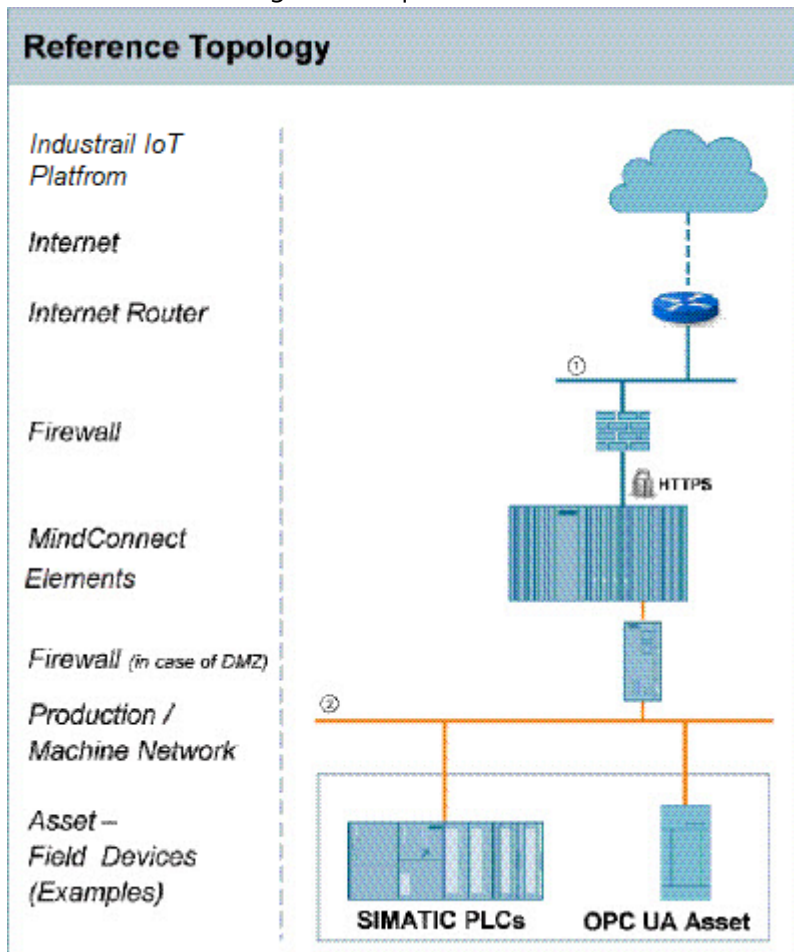
In this case, 120 bytes is the memory needed for one data point.

$$\text{Buffer time} = \frac{500,000,000 \text{ byte}}{250 \text{ 1/s} * 120 \text{ byte}} = 16,666.6 \text{ s} \triangleq 4.6 \text{ hrs}$$

7.9 Firewall Settings

It is recommended to use a firewall between the Internet and the MindConnect Software Agent, this is also recommended for communication to the automation network.

In the direction to Automation Network a firewall supporting NAPT (in case of DMZ, see section "List of abbreviations") or supporting the "Ghost-Mode" is required. Siemens offers many types of Firewalls for fulfilling these requirements.



① Corporate / Office Network with route to the internet or direct internet access, e.g. via a DSL modem

② Production / Machine Network

“Ghost-Mode”, also known as “Transparent Mode”, is used to protect individual, event alternating, devices by dynamically taking over the IP address.

Firewall/Proxy rules for MindConnect Software Agent

MindConnect Software Agent require open HTTPS and DNS ports for communication with Industrial IoT. You can open port 443 to enable this.

MindConnect Software Agent will connect to the following DNS names:

`<region>.mindsphere.io`

For `<region>` enter the area that was defined in your contract, example `*.eu1`.

Industrial IoT uses modern cloud principles (such as content delivery networks) to achieve high availability/scalability. The above mentioned DNS names can be resolved to a large range of IP addresses based on the context of the caller and the state of the backend.

If you are trying to log in from the firewall backend, you need `*.eu1.mindsphere.io` and in addition a Insights Hub Interactive Login Page URL is required, example `diswlogin.siemens.com`. The below given links are the examples for interactive logins in the browser for agents or application starting with `*.eu1.mindsphere.io`:

- `https://*.industrysoftware.automation.siemens.com`
- `https://identity.industrysoftware.automation.siemens.com`
- `https://www2.industrysoftware.automation.siemens.com`
- `https://content.industrysoftware.automation.siemens.com`
- `https://identityapi.industrysoftware.automation.siemens.com`
- `https://ws-apip.industrysoftware.automation.siemens.com`
- `https://cdn.auth0.com`
- `https://diswlogin.siemens.com`
- `https://static.mentor-cdn.com`

To communicate agent only, you will only need the `.eu1.mindsphere.io`.

7.10 List of abbreviations

Abbreviation	Description
DMZ	Demilitarized Zone (referred to a perimeter network)
GUI	Graphical User Interface
HTTPS	Hyper Text Transfer Protocol Secure

Abbreviation	Description
IoT	Internet of things
IoT2040	MindConnect IoT2040
IP	Internet Protocol
LAN	Local Area Network
MCN	MindConnect Nano
MSU	Industrial IoT Unit
NAPT	Network Address and Port Translation
OEM	Original Equipment Manufacturer
OPC UA	Open Platform Communications Unified Architecture
PC	Personal Computer
S7	STEP 7
UI	User Interface

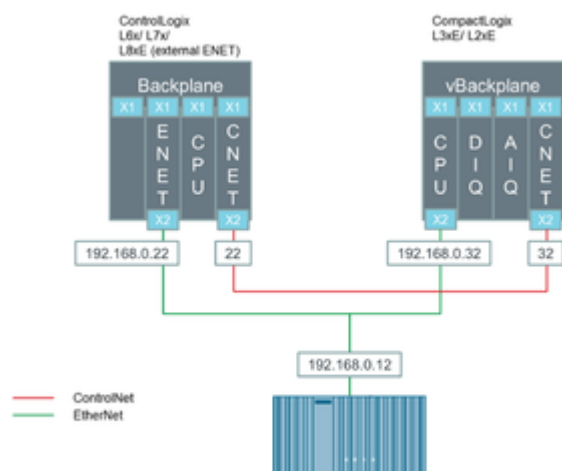
7.11 MindConnect EthernetIP - CIP Communication path (route parameters) settings

The CIP uses a method of encapsulating the messages adding communication path segments to the command segment. This leads to a longer and longer growing message as the number of routing stations grows.

As an example, the following simple layout is used to explain that fact.

The MindConnect is acting as a CIP client.

The CIP server is provided by a ControlLogix or CompactLogix.



Each CIP message contains the routing information to the target. Every time a bridge accepts such a CIP message it strips out its own address information and forwards the modified CIP message to the next addressee along the way. When there is no further routing information available the destination target has been reached and the CIP message will be interpreted. Once interpreted the response will be sent the same way back the request came. This means each bridge keeps a reference to the request package.

7.12 Case 1 - Accessing data inside an Allen- Bradley PLC

In this case, a ControlLogix uses the ENET bridge in slot 1 (0 based counting) for communicating with the CIP client. The processor module itself is in slot 2. An additional ControlNet Bridge is in slot 4 and is not used in this scenario.

The MindConnect sends a request to the ControlLogix on 192.168.0.22, slot 2.



This communication path (route parameters) is formed as follows:

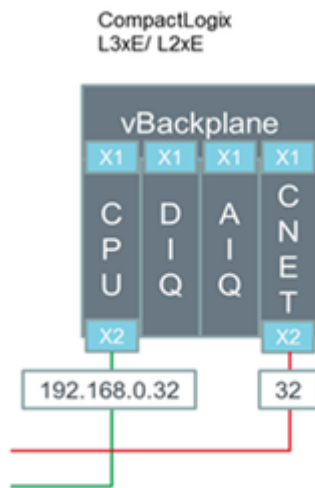
It recognizes the CIP message is not for it and therefore, it removes its address part (1) from the CIP message. The remaining CIP message is being forwarded to the processor module as indicated by the remaining address information (2). The message contains a reduced

communication path with the slot number. The processor removes that information and start interpreting the remaining message, as there is no further routing information in the packet. The following Wireshark packet analysis shows the additional segment.

7.13 Case 2 – Accessing the Allen- Bradley PLC via integrated Ethernet port

In this scenario, the CIP client sends some data into the CPU module using the integrated Ethernet port. In a CPU module with integrated Ethernet port, the Ethernet port is in the same slot as the CPU module.

The CIP client in the MindConnect sends a request package to the CPU module at 192.168.0.32 addressing the processor module in slot 0.



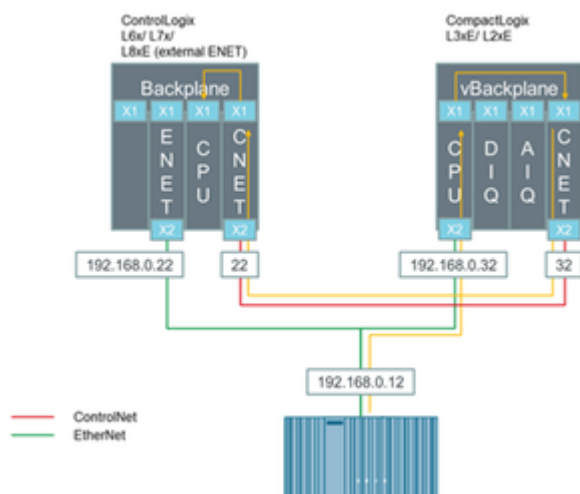
Following the previous schema, the above image represents the communication path (route parameters).

Following the previous made explanations, the CIP message travels first through the processor module to the backplane and it returns back to the processor module for interpretation. For such situations, it is possible to use an abbreviated communication path only containing the IPv4 address.

The MindConnect block uses the parameter "slot" to form the communication path (route parameters).

7.14 Case 3 – Accessing the Allen- Bradley PLC via the ControlNet interface

In this scenario, the CIP client reads data from the Allen- Bradley PLC. Now, the communication path will be through the CompactLogix acting as bridge between EtherNet/IP and ControlNet.



The yellow line in the above image represents the communication path (route parameters). In the communication path, the red marked sections always contain a network specific address. The blue marked part identifies the backplane or the interface to be used. It is not important that the backplane is physically existing or virtual. The green part identifies the slot number of the next bridge module (next hop) or the destination module.

7.15 MindConnect General Security Principles

The following are the security principles of MindConnect services:

- Communication between devices and Industrial IoT cloud services through HTTPS and signed URLs.
- Authentication and authorization using OAuth 2.0 mechanisms.
- Security tokens have a limited time span of validity and must be renewed.
- Before installation, firmware is signed and signature is validated by the device.

Onboarding agent (example, MindConnect Software Agent)

To onboard an agent, establish the trust between agent and agent management:

1. Create an agent in Asset Manager.
2. Define the network and security profile in Asset Manager.
3. Download the initial access token and network configuration to your local machine.
4. Deploy the initial access token to agent, for example via USB stick.

With the initial access token, the agent can prove it's identity towards agent management by:

- The Initial Access Token (IAT) is physically entitled to onboard the agent.
- The initial access token is valid for 7 days for security measures to avoid the misuse.

Registering an agent (example, MindConnect Software Agent)

To register an agent at agent management, follow the below OAuth 2.0 protocol: MindConnect Elements uses RSA3072 standard public/private keys in further communication. For example, the agent registers at agent management with the IAT and additionally, a JSON Web-Key is set according to RFC7517 that contains a self generated public key.

Accepting the registration (example, MindConnect Software Agent)

With this response, the agent is onboarded and agent management accepts the registration. There are two cases, the agent management responds with:

Case 1:

- The shared secret (valid for 7 days) – to be used to access token in the request.
- The re-registration access token (RAT) – to be used for the renewal of registration, once the registration is expired.

Case 2:

- The re-registration access token (RAT) – to be used for the renewal of registration, once the registration is expired.
- The agent management stores the public key received after registering an agent and uses it to verify the request access token from agent, which uses JWT signed with private key from now on. For more information, see [Onboarding an Agent](#).

Validity of the credentials

By default, each registered agent (either RSA 3072 or Shared Secret security profile) has its own credentials valid for 7 days and it must be renewed on a regular basis. After this period, Insights Hub will not grant any access tokens to the agent and the agent credentials will be invalid. The agent needs to re-register to Insights Hub by providing its Registration Access Token (RAT). Registration access tokens have no practical expiration times but each time a client refreshes its registration a new RAT is generated by Insights Hub.

API communication agent (e.g. MindConnect Software Agent)

Except the one for onboarding and registration, all Industrial IoT APIs require an access token: The Agent requests an access token from Agent IAM using a self signed JSON Web Token (JWT). The JWT is signed (see RFC-7515) with either the shared secret (Case 1) or the private key of the public / private key pair (Case 2) in Step 2. The JWT contains the tenantId
The granted access token is valid for 30 minutes. It is also a JWT and contains:

- tenantId

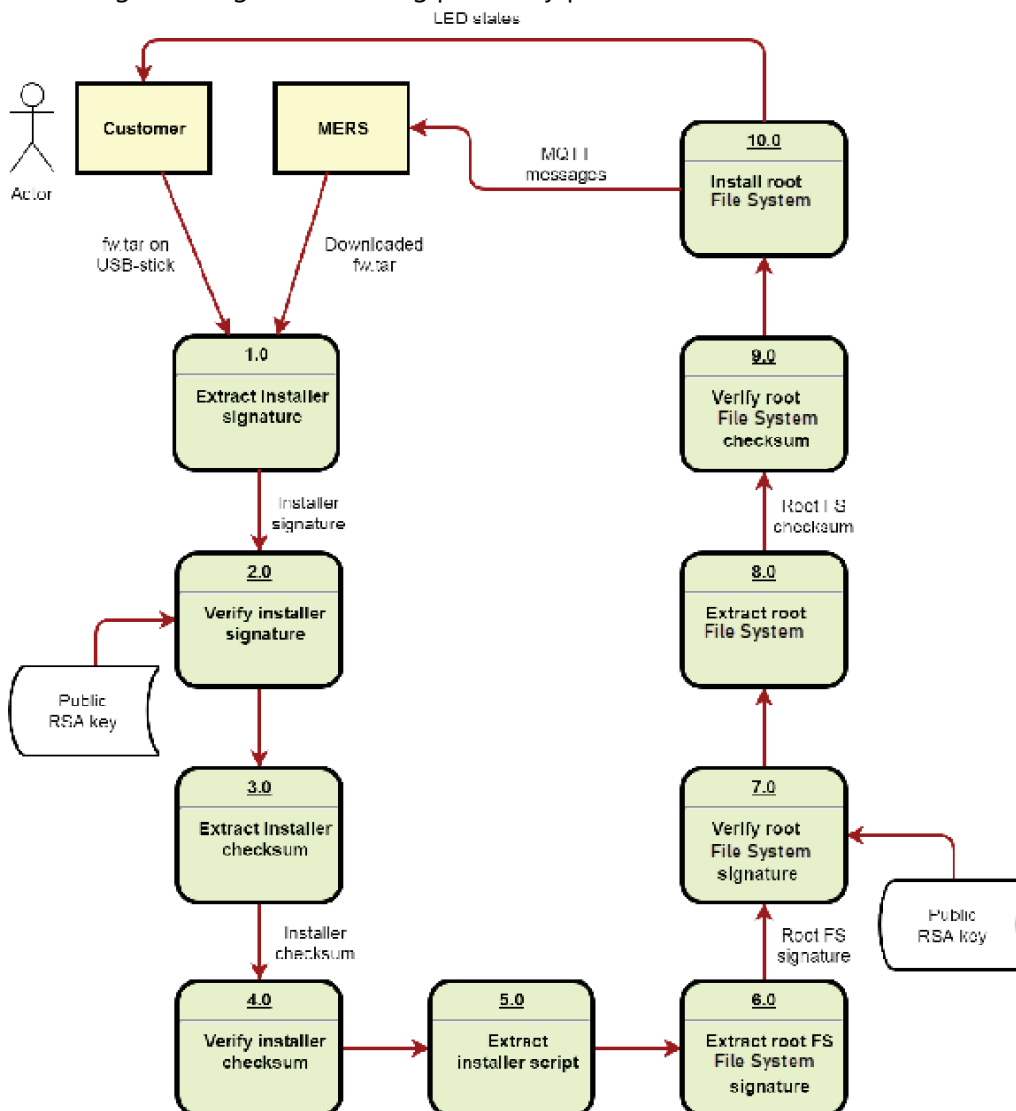
- scopes: It describes the type of services used in this token holder.

After expiry, a new token needs to be requested.

Firmware management

Firmware management is stored in secure cloud storage. Agent accesses secure storage through a signed URL issued by Insights Hub and it is valid for 7 days.

Firmware is signed with private key from Insights Hub. Firmware installer (MERS) on device, checks signature against matching public key provided at initial installation in the factory.



7.16 Differentiating MCSA between Windows and Linux

Datasource protocols

System protocol

Following system protocol variables are not supported in MCSA Docker containers:

kernel

- /kernel/osrelease
- /kernel/ostype
- /kernel/version

memory

- /memory/cmafree
- /memory/cmatotal
- /memory/available

network

- /network/pawspassive
- /network/tcpdirectcopyfrombacklog
- /network/tcpdirectcopyfromprequeue
- /network/tcpfackreorder
- /network/tcpforwardretrans
- /network/tcphphitstouser
- /network/tcpprequeued
- /network/tcpprequeuedropped
- /network/tcpschedulerfailed

disk

Affected sub categories:

- persistent
- persistent_appconfig
- persistent_massdata

7.17 DHCP Network settings

These settings are required for the Linux host system where MCSA for Docker can be installed. In some network environment it is possible that the Linux host system receives a new IP address after restarting the host system depending on the DHCP client configuration. Therefore, it is recommended to add the following line to the file `/etc/dhcp/dhclient.conf` of the Linux host system

```
send dhcp-client-identifier = hardware
```



This configuration is recommended on SIEMENS SIMATIC IOT2050 Advanced-PG2 with Industrial OS 3.2.2 or higher.

7.18 Samba Installation

For transferring the files to the local file transfer folder of a MCSA Docker container, it is required to set up a Samba file share on the Linux host system - for example when files are required to be copied from a Windows system.

Following sections show how Samba can be installed and configured on a Linux host system like Industrial OS V3.2.x.

Package manager configuration

During the initial setup of Industrial OS V3.2.2 or higher if there are no further apt mirrors are added or the apt sources list are not been extended manually, it is required to add the following mirror entries to apt sources lists on the host system before the Samba can be installed.

apt mirror configuration sample: `/etc/apt/sources.list.d/sources.list`

Debian package feed for Mentor Embedded Linux

- deb <http://ftp.debian.org/debian> bullseye main contrib non
- deb <http://ftp.debian.org/debian> bullseye-updates main contrib non

Adding a new user for Samba share

A new user can be added other than the already existing different user and can be used for the Samba share.

Below is an example of adding a new user "mindconnect" to the Linux system:

```
sudo adduser --no-create-home --disabled-password --disabled-login --gecos  
"" mindconnect  
sudo chage -E -1 -M -1 mindconnect
```

Installing Samba

In the following example Samba is installed without further user interaction.

```
sudo apt-get --allow-releaseinfo-change update  
sudo apt-get -y install debconf-utils  
echo "samba-common samba-common/workgroup string WORKGROUP" | sudo debconf  
-set-selections  
echo "samba-common samba-common/dhcp boolean true" | sudo debconf-set-sele  
ctions  
echo "samba-common samba-common/do_debconf boolean true" | sudo debconf-se  
t-selections  
sudo apt-get -y install samba
```

Adding user to Samba

The user needed for the Samba share can be added as follows.

```
smbpasswd -a -U mindconnect  
systemctl stop smbd  
systemctl start smbd
```



'smbpasswd' requests for a password needed to access the Samba share.

Samba Configuration

Example for Samba configuration that is to be added to `/etc/samba/smb.conf` file to use `/persistent_massdata/filetransfer` folder as Samba share is shown below.

```
#===== Global Settings =====  
[global]  
workgroup = WORKGROUP  
# dns proxy = no  
log file = /var/log/samba/log.%m  
max log size = 1000  
max disk size = 600  
logging = file  
syslog = 0  
panic action = /usr/share/samba/panic-action %d  
server role = standalone server
```

```

passwd backend = tdbsam
obey pam restrictions = yes
unix password sync = yes
passwd program = /usr/bin/passwd %u
passwd chat = *Enter\snew\s*\spassword:* %n\n *Retype\snew\s*\spasswor
d:* %n\n *password\supdated\ssuccessfully* .
pam password change = yes
map to guest = never
load printers = no
usershare allow guests = yes
security = user
#===== Share Definitions =====
[filetransfer]
comment = Data Directory
path = /persistent_massdata/filetransfer
guest ok = no
browseable = yes
read only = no
create mask = 0777
directory mask = 0777
force create mode = 777
force directory mode = 777

```



- Folder/persistent_massdata/filetransfer is to be created before it can be used as Samba share.
- The used mask and mode permissions in the sample Samba configuration above shown should be reviewed according to the company requirements.

Restart the Samba daemon after changing `/etc/samba/smb.conf` file as shown.

```

systemctl stop smbd
systemctl start smbd

```

System login Configuration initialization

On some Linux systems by default new files are created with strict file permissions. Therefore, permissions of the files which needs to be copied to the Samba share has to be changed so that they can be accessed from the MCSA Docker container - full read and write file permissions has to be granted.

To avoid changing the file permissions after copying the files to the Samba share, the `umask` value of the system's login configuration initialization is also be changed in `/etc/login.defs`

file as follows.

UMASK 002

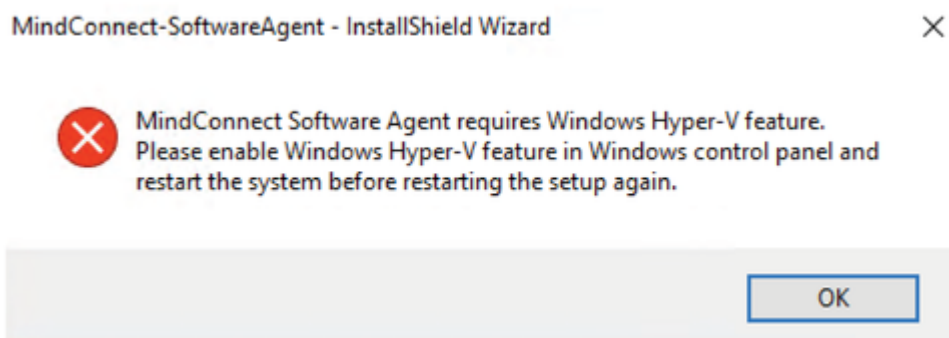


Make sure that the changes done does not violate the company's security requirements.

7.19 MindConnect Software Agent in HyperV Host system

Hyper-V not enabled on IPC

If Hyper-V feature is not installed and enabled on IPC, following dialog appears:

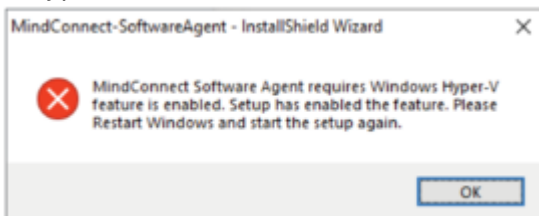


In this case the setup will end, and the Hyper-V Windows feature has to be enabled in Windows control panel.

Thereafter restart your Windows, open MindConnect Software Agent setup again.

Hyper-V not enabled on PC

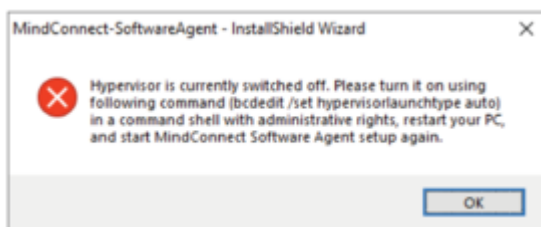
If Hyper-V feature is not installed and enabled on PC, following dialog appears:



In this case the setup will end and Windows has to be restarted before MindConnect Software Agent can be started again.

Windows Hyper-V is switched off

If the Windows Hyper-V is switched off, following dialog appears:



In this case the setup will end and the hypervisor has to be enabled manually using following command in a command prompt with administrative rights:

```
bcdedit /set hypervisorlaunchtype auto
```

Afterwards, Windows has to be restarted before MindConnect Software Agent setup can be started again.

7.20 Known restrictions of MindConnect Software Agent

This page provides some information about already known restrictions and provides workarounds to handle them.

Local UI

One browser window/tab only

It is highly recommended to open MindConnect Software Agent's local UI in one browser window/tab only, due to an already known issue diagnosis messages would be shown several times.

Diagnosis messages are shown twice

If the network settings are changed during onboarding or offboarding, it might be possible that the diagnosis messages will be displayed twice. To resolve the issue, restart the VM.

Date and Time picker is not shown to select new system time

Date & Time picker input fields are not supported in all web browsers (e.g. Mozilla Firefox). Use chromium based browsers like Google Chrome or Microsoft Edge.

Onboarding

Encrypted onboarding key

If the current encrypted onboarding key is not working, then the unencrypted onboarding data should be used for onboarding and offline configuration in MindConnect Software Agent UI.

Re-onboarding

If the asset has been offboarded in the Asset manager and the device is being onboarded again, it might be possible that the new onboarding configuration has to be applied twice because the system will internally offboard first and reboot later. Therefore, the new onboarding configuration has to be applied again in the local MindConnect Software Agent UI.

Firmware update

Update status does not change

If the firmware update status is not updated from "started" to "succeeded" because the reboot of the system was too fast, and the UI did not get the success message. In this case, the current browser window should be closed or reloaded after a couple of minutes.

Insights Hub Start For Free

The following are the known restriction for the Insights Hub Start for Free environment:

1. Maximum six data-points are available.
2. Maximum two data-sources are available.
3. Minimum data-ingest rate for agents of Insights Hub Start for Free environment should be less than 0.1kbps. This is applicable for MindConnect Software Agent also.
4. Insights Hub Start for Free restrictions in Industrial IoT are applicable for MCSA also.
5. In Insights HUB Start for Free, the lower reading cycles may lead to performance issues.

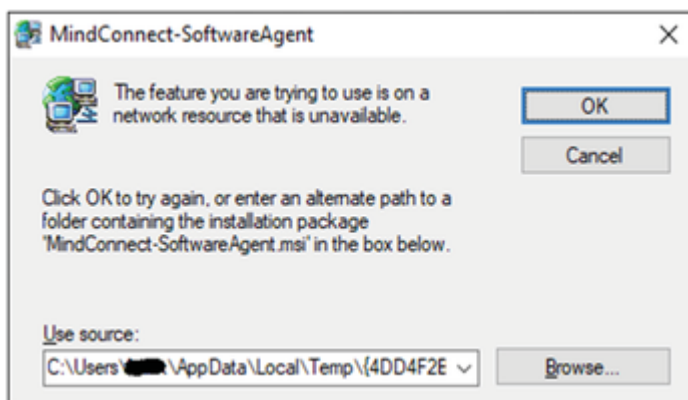
Multi MindConnect Software Agent VMs Installation

Multi MindConnect Software Agent VM installation

While adding, modifying, or removing a multiple VM in MindConnect Software Agent setup, all running MindConnect Software Agent VMs will be stopped and re-started after the setup process is completed.

MSI package cannot be found

If the .msi package is not found, search for the alternate path in the "C:\Users..\AppData" folder and enter the path containing installation package "MindConnect-SoftwareAgent.msi":



Installing new MindConnect Software Agent version

In case of an upgrade setup will show a message and abort afterwards, then uninstall the old MindConnect Software Agent version before installing new MindConnect Software Agent version by using the InstallShield setup.

7.21 Default values for datasource Import and Export

The below mentioned table provides you the default values for the datasource import and export.

Protocol	Type	Column	Default Value
S7	Datasource	Connection Type	Automatic
		Rack Number	0
		Slot Number	2
OPCUA	Datasource	AuthenticationType	None
		Security Mode	None
		PLC Type	S7-1200
MODBUS-TCP	Datasource	Port	502
		Byte Timeout	500
		Response Suspension Time	500
		Request Delay	0
			0
	Datapoint	Slave Number	1
		Start Address	0
		Quantity	1
		Variable Type	Unassigned short
		Integer Byte Order	Normal order
		Response Address Offset	0

Protocol	Type	Column	Default Value
MODBUS-RTU	Datapoint	Slave Number	1
		Start Address	0
		Quantity	1
		Variable Type	Unassigned short
		Response Address Offset	0
		Response Quantity	1
Sinumerik	Datasource	Slot Number	2
Bacnet	Datasource	Address Binding	Dynamic
All protocols	Datapoints	On data change	False
		Hysteresis	0

8.1 Glossary

Aspect

Aspects are a data modeling mechanisms for assets. Aspects group the data points based on logical sense. For example: The pump skid has an aspect e.g. "Energy_consumption" that contains the data points: "power", "current", "voltage" etc.

Aspect is specified in Asset Manager and its name can be freely chosen, but should bring together a logical grouping of data points and a physical asset.

Asset

An asset is a digital representation of a machine or an automation system with one or multiple automation units (e.g. PLC) connected to Insights Hub.

Data collection and data provisioning is based on so called (virtual) assets. This can be anything such as a pump, motor, PLC, an entire tool machine, a production line, a robot, a crane, a car, a wind turbine and so on. The data of an asset is collected and sent to Insights Hub to make that data available for further processing and analytics.

Asset Identifier

Asset Identifier is an identifier assigned by the manufacturer of the device, to which MindConnect Nano will be connected. After the onboarding process, MindConnect Nano is connected to this device. The serial number identifies the asset to which the data belongs.

Asset Manager

Asset Manager is a Web Graphical User Interface for asset configuration. According to these configurations, the following functions are available:

Asset Configuration: assets can be created, onboarded, modified, moved, offboarded or deleted.

Asset type

Asset type is a sort or kind of a product line made by one manufacturer.

Components

Components represent built-in functionality. Components are:

- Asset Manager
- Insights Hub Monitor
- Settings
- UTC Reporting

For the complete list and description of Components, refer to the documentation.

Data point

Data points refer to elements (variables), which allow values to be obtained from data sources (OPC UA or S7 etc.). They are combined into a relevant aspect. For example, "temperature" and "torque" are data points of an aspect "Energy_consumption".

Data points are configured in "Asset Manager". In "Insights Hub Monitor", their values are visualized as time series.

Data source

A data source is a physical element of a device, which can be monitored by Insights Hub. For example: OPC UA Server, S7.

Event

In "Insights Hub Monitor", an event is a change of a datapoint state. Events are used for the requests. With a rule it is possible to define the request, which will be created in Insights Hub when the event is triggered.

Besides the monitoring rule, a description of event (e.g. "The limit is exceeded, this may indicate damage in the pump"), the resulting action (e.g. "Please contact your hotline") and priority (urgent, important or info) can be lodged.

See also "request", "rule".

Last Connection

"Last Connection" status in "Asset Manager" gives the information, when a MindConnect Element was online for the last time.

MindConnect Element

MindConnect Elements are devices for transferring data and allow connectivity to Industrial IoT such as MindConnect Nano, MindConnect IoT2040 or MindConnect FB.

Industrial IoT

Siemens Industrial IoT operation system comprises the core cloud services and applications, whereas the MindConnect Element provides secure and easy connectivity from the field or machine to Industrial IoT. In Industrial IoT, submitted data by a MindConnect Element is processed and stored for analysis and further management purposes. For more information, refer to the documentation.

Industrial IoT Launchpad

Industrial IoT Launchpad is the entry point for components as well as for available applications.

Online/Offline Mode in Asset Manager

Online status signifies that the internet connection between the MindConnect Software Agent and Insights Hub is established and is in good health as the MindConnect Software Agent sends the data to the server. Offline mode means the absence of the internet connection and the MindConnect Software Agent is no longer able to send data to the server.

Insights Hub Monitor

Insights Hub Monitor is an easy-to-use basic analytics application of time series data that enables the user to gain deeper insights into their production system and the machine performance. It uses the assets, aspects and variables as data model for its functions.

Organization

Organization is the part of hierarchical asset configuration in Asset Manager. Within organization, areas/assets are specified.

As the administrator (OEM), you manage organizations, their customers and assets. As the user of an organization, you can access the assets assigned only to this organization.

An organization can be anything and is defined by the administrator depending on their requirements: customer, cost center, branch etc.

Request

Requests are the messages which log asset incidents based on predefined rules.

You can create manual requests as well as requests for the regular acquisition of measured quantities with measuring series.

See also "event", "rule".

Rule

With rules you can configure an automatic Insights Hub Monitoring of datapoints on events. For example, a request will be created automatically by the system, if a value exceeds or falls below a threshold (edge trigger).

See also "event", "request".

Settings

Settings is a Web Graphical User Interface for user, organization and role configuration.

Time series

Time series is a sequence of measurements which are produced by data sources over time. Analysis and visualization tools (e.g. Insights Hub Monitor) can retrieve collected time series and present it to the user after processing. In Asset Manager, the measurements, that have to be collected, can be specified.