

SIEMENS

SINUMERIK SINUMERIK EDGE

Operating Manual

Industrial Edge, the SIEMENS Edge Computing Platform	1
Platform Security	2
Data Privacy	3
Hardware Specs	4
Connectivity Plan	5
Service Stick	6
Machine Tool Framework Licensing Model	7
Manage MySINUMERIK Edge MindSphere Applications	8
Install Required System Applications	9
Enable Access to SINUMERIK	10
Enable Access to S7 master device	11
Enable Access to OPC-UA	12
Enable Access to a Fanuc controller device	13
SINUMERIK Edge Sensor Adapter	14
ET200 Sensor Adapter	15
SINUMERIK Edge MQTT Client	16

SIEMENS

SINUMERIK SINUMERIK EDGE

Operating Manual

<u>Configure an Application</u>	17
<u>Reverse Proxy with Local User Management</u>	18
<u>Data provisioning to MindSphere IoT Data Model</u>	19
<u>AppSDK</u>	20
<u>Local Diagnostic Dashboard Application</u>	21
<u>Time Behavior</u>	22
<u>OPC-UA Server as a northbound interface</u>	23
<u>Samba Share</u>	24

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.

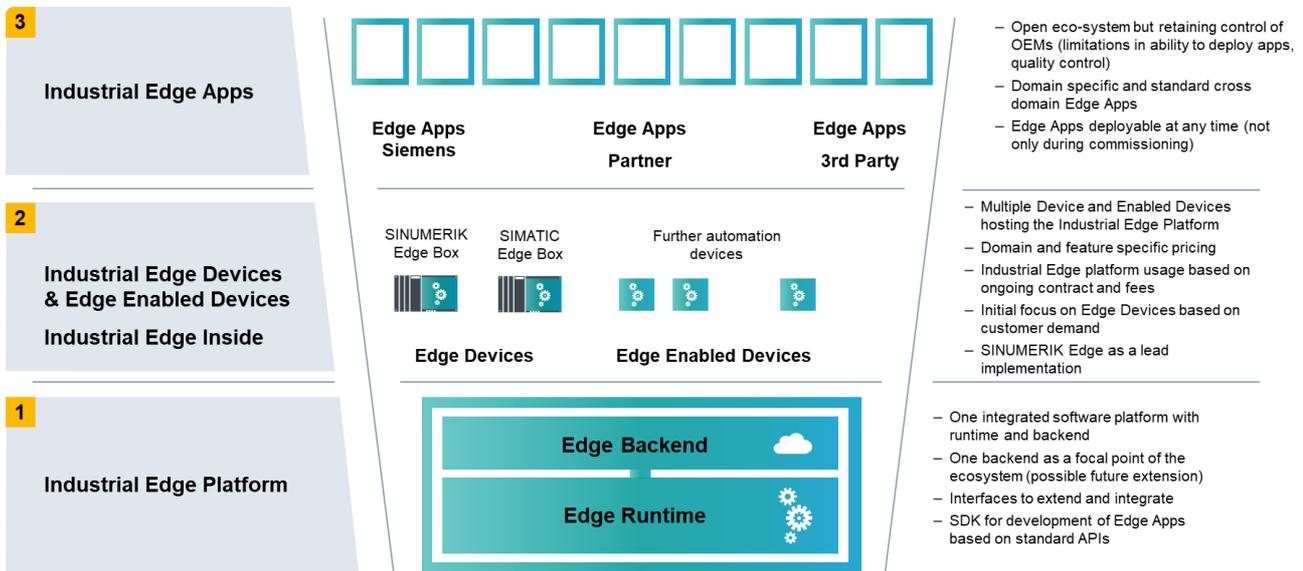
Industrial Edge for Machine Tools - Digitalization Beyond Cloud

Industrial Edge for Machine Tools is a SIEMENS Edge Computing Platform for the Machine Tool domain that enables you to build, operate and maintain your software solutions on distributed devices. It comprises the runtime itself, an easy to handle execution environment and a central management backend.



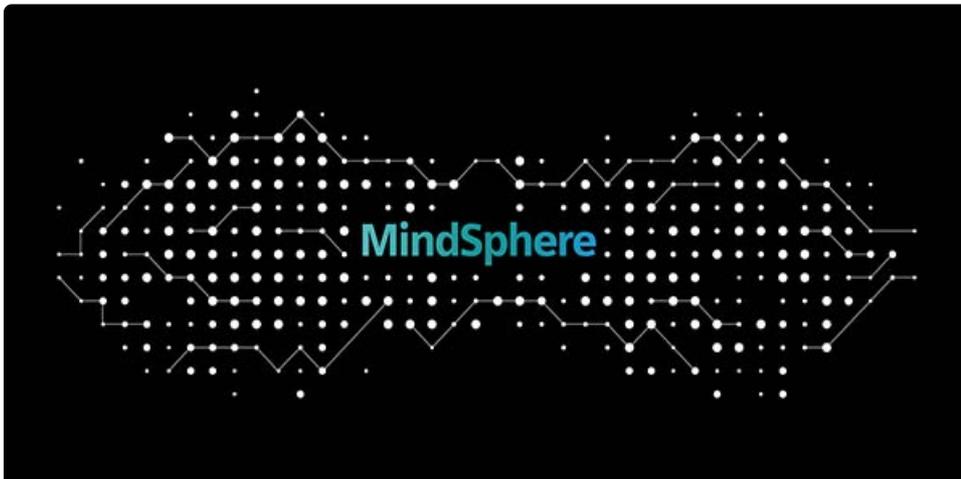
- Enabling downloadable applications – opening a door for continuous business with still unknown software products
- Protecting sensitive data but enabling their processing
- Defending automation systems – increasing security
- Enabling advanced applications (including Machine Intelligence (AI))
- Defending critical resources of automation system –power for additional functionality
- Adding flexibility to address unknown future performance requirements
- Opening a sales channel to machine users
- Increasing the value of automation systems

Industrial Edge comes with an integrated execution and management platform, hardware runtime environments as well as preinstalled system applications.



What is Insights Hub?

Insights Hub is an open iot operating system provided and operated by SIEMENS



[Insights Hub Home](#) [Insights Hub Documentation](#) [Insights Hub Developer Documentation](#)

Execution Environment for Industrial Apps

Exenia stands for EXecution ENvironment for Industrial Apps. It provides the environment required to run Apps on embedded devices running Linux as Operating System. It also provides the tools required to address the different concerns of the apps:

- insulating (sandboxing)
- separation of machine and factory network
- packaging
- provisioning (delegated to the base system)
- and updating applications (life cycle management)

Exenia's role is similar to that of the Docker daemon for executing Docker containers and extends to include various network, security layer and openness functions.

Exenia makes it possible to fully integrate the Edge devices into a corresponding backend and provides out of the

box remote services like

- app management
- metering services
- logging services
- authentication

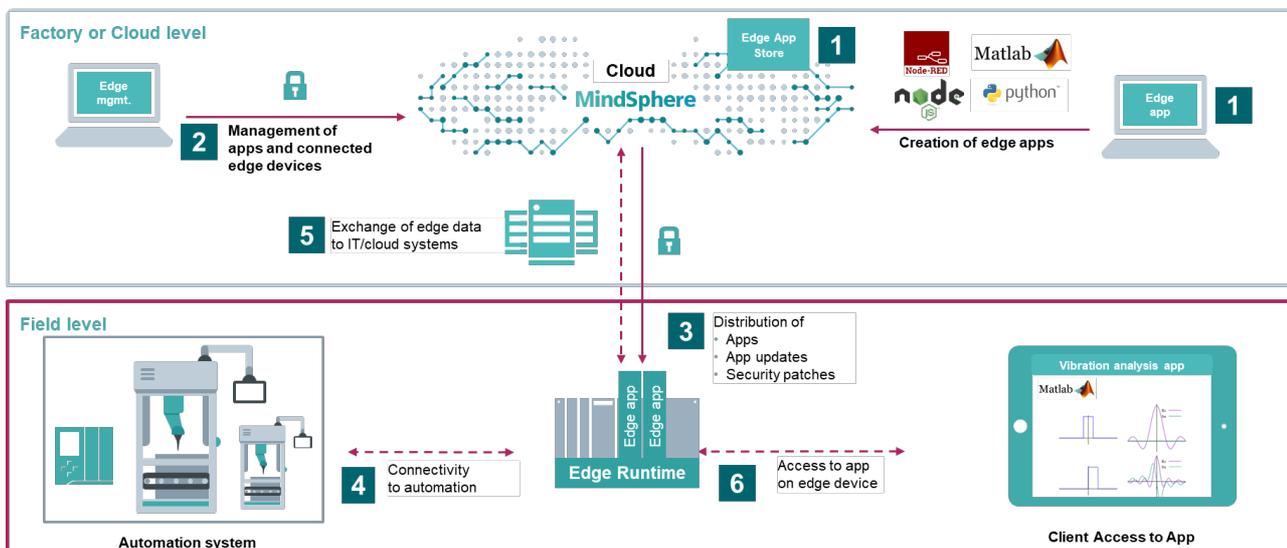
Exenia, as a *generic architecture*, is a modular framework using different base technologies. It is a component developed at SIEMENS and created mostly by integrating established OSS software. It is designed to be configurable according to the intended use-cases and the device's operational constraints.

Industrial Applications

Industrial applications (indapps) are ready to ship packaged containers. They include all metadata and configuration needed to be hosted on Industrial Edge runtime. Indapps can seamlessly integrate to system functionalities. App SDKs for different languages provide interfaces for system integration support the own applications.

Industrial Edge for Machine Tools, a Siemens Edge Computing Platform for the Machine Tool Domain

Industrial Edge for Machine Tools is the SIEMENS Edge Computing Platform for the Machine Tool domain to host applications from different vendors on a computing platform close to the shopfloor. Thus enables the extensions of automation, deployment of demanding streamprocessing and learning algorithms as well as the hosting from integration code to site automation.



Industrial Edge addresses the following core functionality

1) Write applications in various programming languages, participating from the whole power of the docker community

- Simple creation of applications
- Publishing of applications to different tenants

2) Comprehensive **Edge Device Management**

- Simple onboarding of Edge devices operated in industrial networks
- Secured firmware management with power fail-safe update over the air

3) Integrated **Application Management** for deployment, configuration and lifecycle management

4) System services for **Automation Connectivity** (SINUMERIK)

- Parameter Access
- High Frequency streaming data from SINUMERIK 840D sl

5) Integrated connectivity for **Insights Hub IoT**

- Easy configuration of IoT Model

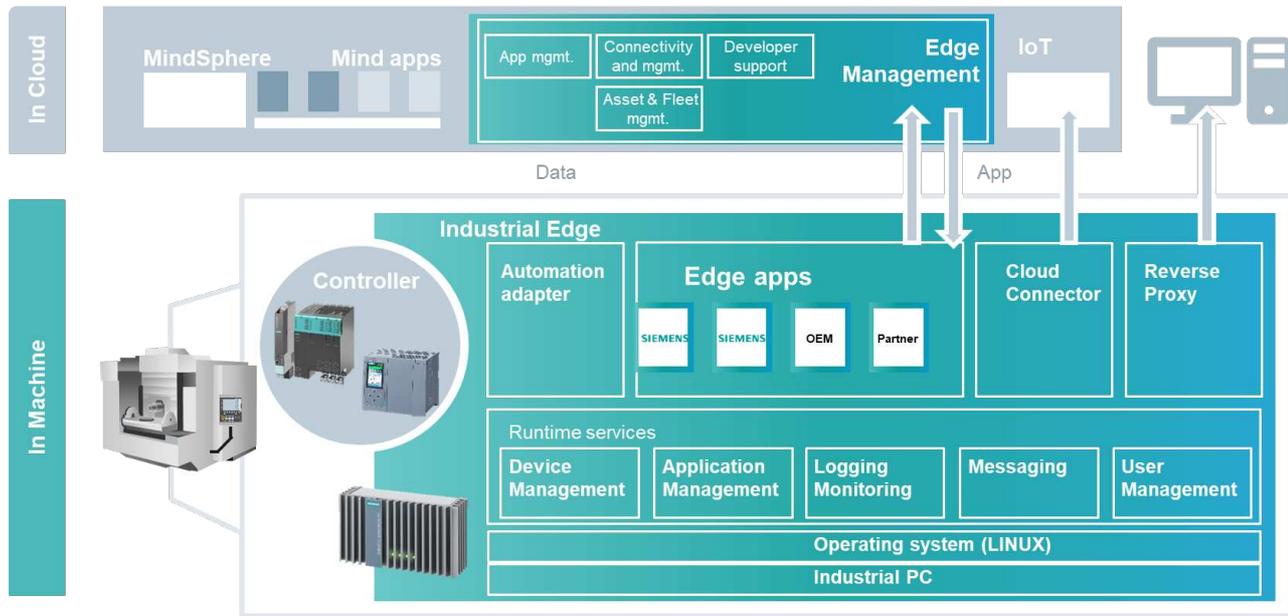
- Usage of visual analyzer, Monitor and notification services

6) Publish Web Applications on Site

- Reverse proxy for controlled publishing from Web Apps on site
- Integrated user management for on site access control

Architectural Concept - Overview

The Industrial Edge offers a comprehensive Eco System for Industry.



It consists of an Industrial Edge runtime and a corresponding backend.

1) Industrial Edge Runtime

The Industrial Edge Runtime offers a remote manageable application hosting engine based on industrial grade hardware and LINUX operating system. The Application engine is fully containerized and integrates Edge Apps with management, logging, monitoring with the corresponding backend. Integrated Adapters connect automation devices by configuration. A messaging system allows inter App communication and easy integration between device and cloud adapters. Insights Hub cloud connectivity is built in and opens integration to Insights Hub world. The reverse proxy with user management allows secure on site access to Web UI's from applications.

- Device Management services for onboarding, network configuration and power cut safe software update over the air
- Application Management - deploy, configure, remove, start, stop, reset
- Logging and Monitoring clients offer a supervision of Edges and Applications from backend side
- The messaging system is used for data integration from apps and guarantees qualities even for high frequency data transfer
- On site user management allows to administer users, groups and roles for direct Web Access through the reverse proxy
- The Automation adapter serves for parameter access as well as for high frequency data streaming
- The cloud connector offers an out of the box integration to Insights Hub world

2) Insights Hub Backend - Industrial Edge Services

The Insights Hub Backend Services for Industrial Edge leverages full Insights Hub functionality and opens the

world of Edge computing.

- App Management for choosing and lifecycle management of apps
 - App Publishing for Application developers to integrate to the global App repository including controlled access management
 - Secured industrial grade connectivity
 - Powerful asset and fleetmanagement including visual analyzer and notification services
 - Hosting and operation from own MindApps
 - Consumption from 3rd party MindApps
-

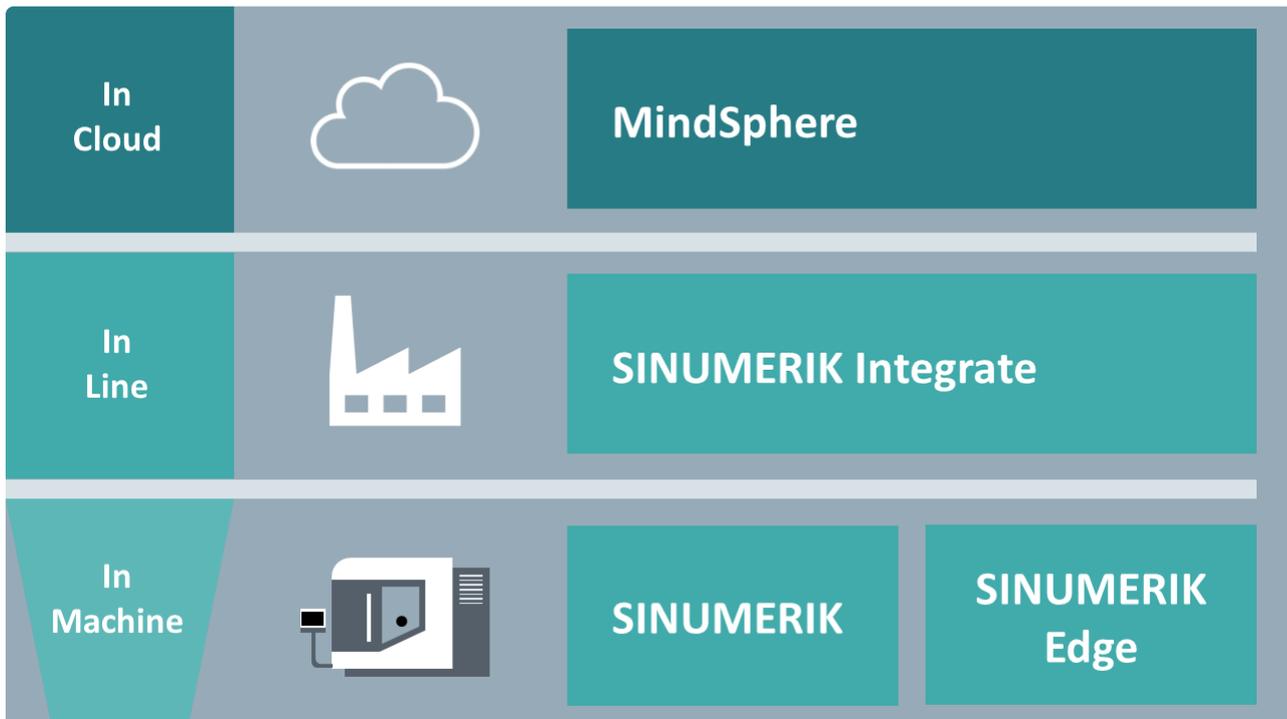
Platform Security

Overview

SINUMERIK Edge is a remote-controlled Edge-Device, which can be used within an extended IoT/OT architecture both as field gateway and computation node for any user workloads. The SINUMERIK Edge thus enables vertical information and data processing flow between all layers:

- In Machine
- In Line
- In Cloud

Digitalization layers:



This also includes the temporary or permanent storage of process data. Thus, SINUMERIK Edge is responsible for ensuring that its security architecture does not allow any regression/regression of the data erosion of the existing network security and data protection level. To the individual security mechanisms of SINUMERIK Edge, it is necessary to organizational support here as well.

SINUMERIK Edge is a standard IPC with a special operating system that forms together with Insights Hub the SINUMERIK Edge Ecosystem. The SINUMERIK Edge offers high-frequency data access to internal control data, additional computing power at the machine, update capability through the connection to Insights Hub – finally a secure platform for applications that generate added value based on the data.

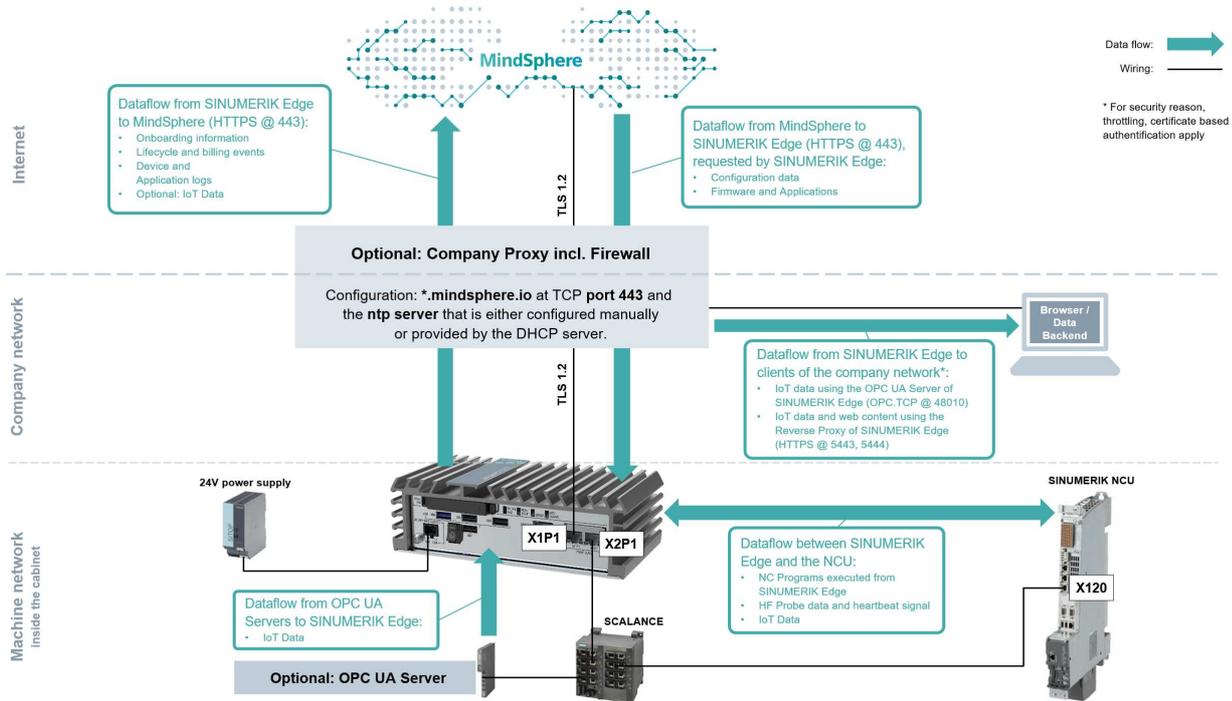
The SINUMERIK Edge is a product of its own. The SINUMERIK Edge apps that can be executed are separate products with corresponding order numbers.

With the App-SDK package the customer can develop his own apps (e.g. Eclipse as development environment). To

publish the created apps and deploy them on SINUMERIK Edge devices, Manage MySINUMERIK Edge /App Management is required.

The SINUMERIK Edge works in the daily operations without Insights Hub. However, the commissioning and the installation/configuration of firmware and SINUMERIK Edge apps requires the connection to Insights Hub.

Connection and wiring of SINUMERIK Edge:



The SINUMERIK Edge is equipped with 2 physical network connections (RJ45), which, according to the manual, are to be used for the connection to the In Machine and In Line Level.

Make sure that the port assignment is correct for the following reasons:

- For the "In Machine" network, a mainly unprotected communication is assumed
- For the "In Machine" network, an uncontrolled connectivity to higher networks (In Line, In Cloud) is not possible.

The SINUMERIK Edge guarantees the isolation of the network through a multi-level network architecture of both networks, which is only overcome by an application-defined data flow. Using container technology, further mechanisms exist for Isolation of the workload (edge application) in terms of network, memory and CPU resources.

The communication of the SINUMERIK Edge in the direction of "In Cloud" and "In Line" is always established via an encrypted end-to-end channel (TLS 1.2). In addition, the integration a PKI-based trust chain is supported. Thus, both a restriction to only allowed communication partners as well as the trustworthy transmission is ensured. For the in-line data exchange in environments with special security requirements a client-based authorization via client certificates is possible in addition.

The initial exchange of the required certificates for secure communication between Edge Management System (In Cloud) and SINUMERIK Edge (In Machine) is implemented during the so-called onboarding process. The onboarding process includes the exchange of a "shared secret" that connects a logical device (Insights Hub Asset) with a physical device (SINUMERIK Edge). Since this exchange does not happen via the same communication infrastructure, compromising may occur during the onboarding. A second aspect of onboarding is the linking / integration of Insights Hub IoT Services (Timeseries Store, File Store, Monitor, ...) in the correct Insights Hub Tenants. The SINUMERIK Edge-Platform also ensures that a data flow into a tenant or asset not designated for this purpose can be established at no point.

 Note

The basis for this is an existing Insights Hub Subscription (at least an IoT Value Plan S).

The SINUMERIK Edge communicates solely through outgoing connections. This means that no exposition of the SINUMERIK Edge is needed on In Line or In Cloud Level. This scenario is not recommended.

Regardless of this configuration, the access to the Insights Hub endpoints from the SINUMERIK Edge must be guaranteed temporarily. This concerns the onboarding, the firmware update or the (de)-installation of edge applications. The SINUMERIK Edge not only enables applications (Industrial App) to provide data via a controlled way In Cloud, rather these applications can provide user interfaces and/or interfaces (APIs) to create new workflows (in line) or to supplement existing ones. For this purpose, applications may provide their own user and access management capabilities. The corresponding security notes can be found in the respective documentation.

The communication of the SINUMERIK Edge with the SINUMERIK takes place only via the "In Machine" network and is encrypted according to the respective protocols. However, the authorization mechanisms vary depending on the protocol used. Since some protocols are secured with weak protection mechanisms, it is important in these cases to adhere to adequate password guidelines and to ensure organizationally that passwords are never or only in urgent cases stored.

In order to maintain a high security level of the SINUMERIK Edge over a long period of time the firmware is continuously developed and hardened, based on multiple vulnerability checks, virus scans as well as penetration tests that had been performed for the SINUMERIK Edge software. This is necessary in order to adapt to the increasing cyber security threat situation. As part of the SINUMERIK Edge firmware, an update mechanism is available for this purpose, which is integrated into the corresponding IT process as part of a continuous security strategy.

The SINUMERIK Edge does not provide an onboard virus scanner as part of the firmware. The customer needs to run virus scans for SINUMERIK Edge before uploading their applications to the Insights Hub.

The in- and outbound communication is protected by a firewall that is configured and activated as part of the SINUMERIK Edge firmware. Not needed firewall rules had been removed. The interfaces cannot be accessed directly from a SINUMERIK Edge application without using the predefined adapter functions of the App-SDK.

Users with IP based filtering on their firewall can use the following two static IPs for whitelisting the data upload traffic:

- 75.2.111.226
- 99.83.250.213

A strong password policy forces the customer to change the password of the default user of SINUMERIK Edge's firmware (linux console) and the Miniweb at first login. This is described in the system manual.

By default, `edge` user that is used for Linux console login will have its password expiration date set to 90 days. If desired, users can change the default password expiration duration by issuing below command. Passing the number `-1` as number of days will remove expiration duration indefinitely. Allowed values for number of days are `-1, 30, 90, 180` and `360`.

```
sudo chage --maxdays <number-of-days> edge
```

In addition, the SINUMERIK Edge is protected against undesired manipulation or weakening of the security features on both firmware and application level as follows:

SINUMERIK Edge Security Features

SINUMERIK Edge follows security guidance from international standards such as *IEC 62443-4-2 Security for Industrial Automation and Control Systems Part 4-2: Technical Security Requirements for IACS Components*.

Data protection in general

Protects the manufacturing process through application-specific access control.

Protects industrial business by focusing on longterm stability and avoidance of incompatible changes (if possible).



1. Security Hardware Element

Security Hardware Element is a chip, that has an initial secret for the secure boot chain to build on and disk encryption.

2. BIOS protection and secure boot chain

BIOS protection is based on a password, to avoid changes; secure boot chain: only the SINUMERIK Edge operating system or service stick may boot.

3. Disk encryption

The data is decrypted only on the device where the hard drive is built in (device decrypts data upon booting process). The encryption is based on a secret, which can only be decrypted on that device.

4. Physical network isolation

There are two interfaces: X1 P1 to external network and X2 P1 to machine network. Those interfaces cannot be bridged. That makes it impossible for externals to attack the machine tool controller through the Edge data access and allows processing only by certified apps and through security layers.

5. Peripherals integrity protection

Only keypad, mouse and known devices (onboarding stick; service USB stick, etc.) are supported. Other devices are ignored.

6. Industrial-grade, hardened Linux OS

Linux operating system, which is hardened by our security standards, e.g. internal communication via protected virtual network layers.

7. Minimum number of runtime components

The operating system is designed in an efficient manner, which means only necessary, specially tailored components are used, which minimizes the possibilities for externals to attack the device.

8. No root access

There is no root user access to the system. A standard user only has limited access, so that side-loading of apps/viruses is not possible.

9. System backup and recovery

A system backup and recovery can only be done by a service stick, so that e.g. any backup from unprotected systems are avoided.

10. Resource management and quality of service

There is a limitation of resource usage for apps, so that the system components always have enough processing power to operate. This eliminates the risk of denial of service attacks.

11. Managed devices and updates over the air

Applications strictly need to be deployed on devices via cloud. That ensures integrity and availability according to SINUMERIK Edge security paradigm/ concept.

12. End-to-end security with Insights Hub Edge Management

TLS 1.2 is used for the connection between the device and Insights Hub, which prevents the spying of production relevant data and protects the intellectual property of the machine user.

13. Managed certificates

Miniweb creates a certificate, that can be imported to the client browser to secure the communication between browser and Edge. In that way a secure end-to-end connection is established.

14. Role-based app access to secured system services

Only authorized apps may access certain services to ensure security.

15. Secured data access

Access to App UIs is established via SINUMERIK Edge Miniweb (HTTPS connection via Port 5443). Miniweb then roots further to the App, which results in a single control point for outbound communication.

16. Sandboxed app runtime

An isolated container-based environment is used, which ensures that apps do not disturb each other nor the system. The run in dedicated isolated environments with defined interfaces to the system.

17. Container-based process isolation

Apps are isolated from each other. A prioritization and scheduling of processes is done by the platform, which results in enhanced stability and reliability of the system.

18. Non-privileged containers

Containers may never directly access the Linux kernel, only via interfaces (described in Developer Documentation). That results in enhanced stability of the system.

19. Platform interaction over defined APIs

Access to system services/ interfaces and internal communication only is established via software interfaces delivered by the App-SDK. In this way, our interfaces for external communication are being addressed, too.

20. Edge App intellectual property protection

The app container uploaded to Insights Hub is encrypted.

21. Resource quotas

Every container gets its own quota (resources), which result in enhanced stability and reliability of the system.

22. User and role access management

Roles, users and login can be configured via Miniweb, which prevents unauthorized externals accessing Edge application data.

Further security features

SINUMERIK Adapter protects the manufacturers' intellectual property by removing sensitive content in HF Probe data.

SINUMERIK Edge Security Disclaimer

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

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

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

For additional information on industrial security measures that may be implemented, please visit <https://www.siemens.com/industrialsecurity>.

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

To stay informed about product updates, subscribe to the Siemens Industrial Security RSS Feed under <https://www.siemens.com/industrialsecurity>.

Data transfer and storage

Transfer of exported data files have to be secured by technical means like encrypted emails and USB-Sticks, etc., especially in the public internet. Exported data files have to be stored access restricted within the production area (e.g. access restriction to sharepoints, data bases, etc. by user management with credentials)

Multi-factor authentication on Insights Hub

You can further increase security by activating multi-factor authentication (MFA). Activating MFA is therefore recommended for your tenant. MFA adds another layer of authentication to standard to authentication by adding a user name and password. Multi-factor authentication is not a standard Insights Hub setting. Contact Insights Hub for activation.

Data Privacy

Siemens complies with the principles of data protection, in particular the principle of data minimization. This is privacy by design.

SINUMERIK Edge platform only uses essential data that is required for it to function.

Data listed below is required for login functionality. The storage of this data is appropriate and limited to what is necessary, as it is essential to identify the authorized operators.

This data cannot be stored anonymously or pseudonymized, as otherwise the purpose of identifying the operating personnel couldn't be achieved. - IP addresses - User credentials - Linux Terminal - Reverse Proxy - Samba Server - VNC Server - Application specific user credentials

Logs are frequently deleted from device and uploaded to Insights Hub according to the usage intensity. For the offline usage, logs are kept in device until being connected to Insights Hub.

The customer in the role of the Insights Hub tenant owner is responsible for keeping or deleting log files that are stored in Insights Hub.

The above data is secured according to IEC62443 by SL-1 for usage of SINUMERIK Edge in a low risk environment, SL-2 for usage in standard environments and SL-3 for usage in critical infrastructural environments.

 **Important Note**

You must ensure that the data being collected by any sensors (e.g. audio streams, images, videos, etc.) do not contain any personal data.

Hardware Specs

Hardware	Specification
SIMATIC IPC127E (Picobox PC)	6AG4021-0AD11-0CC0
Processor / Memory / Security Hardware Element	[D] Atom E3940 (4C/4T) / 4 GB RAM with Security Hardware Element
Version / Ethernet / USB	[1] Basic version; 2x Ethernet RJ45, 2x USB3.0
Operating system	[0] Without operating system
Mass storage	[B] 64 GB SSD

Hardware	Specification
SIMATIC IPC227E (Nanobox PC)	6ES7647-8BD31-0CV1
Processor / Security Hardware Element	[D] Celeron N2930 (4C/4T) / Security Hardware Element
Working memory	[3] 8 GB RAM
Device variant / COM interface	[1] Box: Basic / without COM
Operating system	[0] without operating system
Mass storage	[C] 240 GB SSD
Software	[V] with Industrial Edge - SINUMERIK software
Mounting accessories	[1] DIN rail mounting

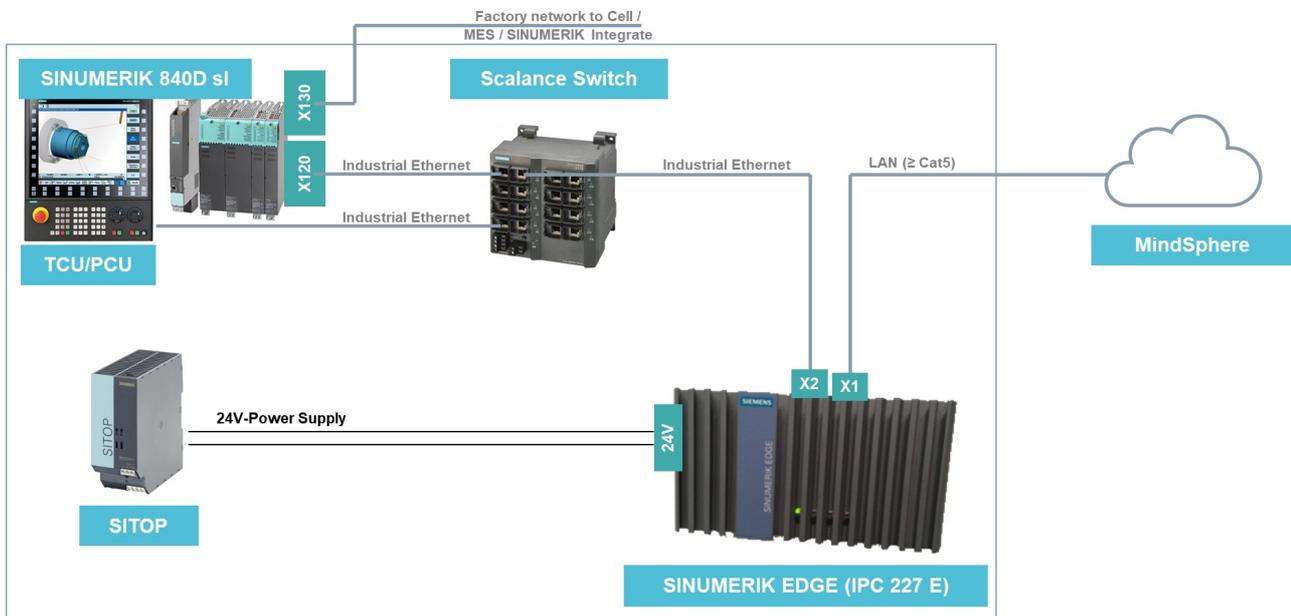
Hardware	Specification
SIMATIC IPC427E (Microbox PC)	6AG4141-5BC30-0GV8
Processor / Network Interface	[5] Core i5-6442EQ; 3X Gigabit Ethernet (IE/PN)
Mounting accessories	[B] DIN rail mounting
Working memory	[C] 16 GB RAM
Extension	[3] Two RS232/RS485, without PCIe
Operating system	[0] without operating system
Drive Changeable	[0] without external mass storage
Mass storage	[G] 480 GB SSD
Software Configuration	[V] Industrial Edge - SINUMERIK software
Power Supply / Security Hardware Element	[8] 24 V DC industrial power supply and Security Hardware Element

Please refer to [support page](#) for detailed information.

Connectivity Plan

Connecting Industrial Edge to Machine and Insights Hub

Industrial Edge separates machine network from cloud connection to separate IT-networks from operational networks. Therefore, fixed usage of ethernet interfaces has to be done. Note that Industrial Edge extends automation which means that machine integration to cells and overlaying factory automation can remain the same as up to now. For sure Edge Applications are capable to connect to those as well (which is not reflected into the diagram for complexity reasons.)



Note: The following IP address range is preserved for SINUMERIK Edge internal usage, it's expected that this address range is not used in customer network. - 10.0.0.0 - 10.255.255.255 - 192.168.214.0 - 192.168.214.255

Service Stick

Industrial Edge runtime by SIEMENS is an edge device which allows remote operation and maintenance of the runtime itself, the applications and configuration. The productive runtime is ruggedized according to security. To protect production environment separation of machine and factory net is built in by design.

Comprehensive logging services provide feedback for operation of the runtime and hosted applications.

BIOS Update

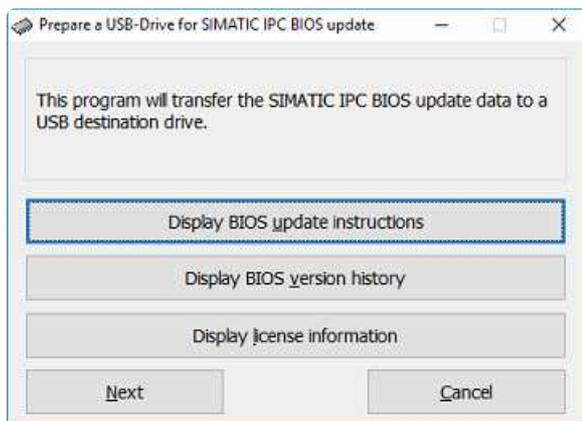
Warning: BIOS firmware installation may reset previous BIOS configurations.

Prerequisites:

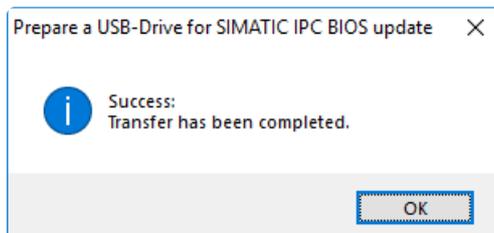
* A USB flash drive * BIOS firmware files

Note: In IPC227E devices, to update BIOS from older versions to 20.01.15 and newer versions, previous BIOS flash settings needs to be erased. To do so, please refer to [erase previous BIOS settings with BIOS update](#).

After obtaining BIOS firmware update files, run the executable named BIOS2USB which is included in the BIOS firmware update file whilst the USB flash drive is connected to PC.



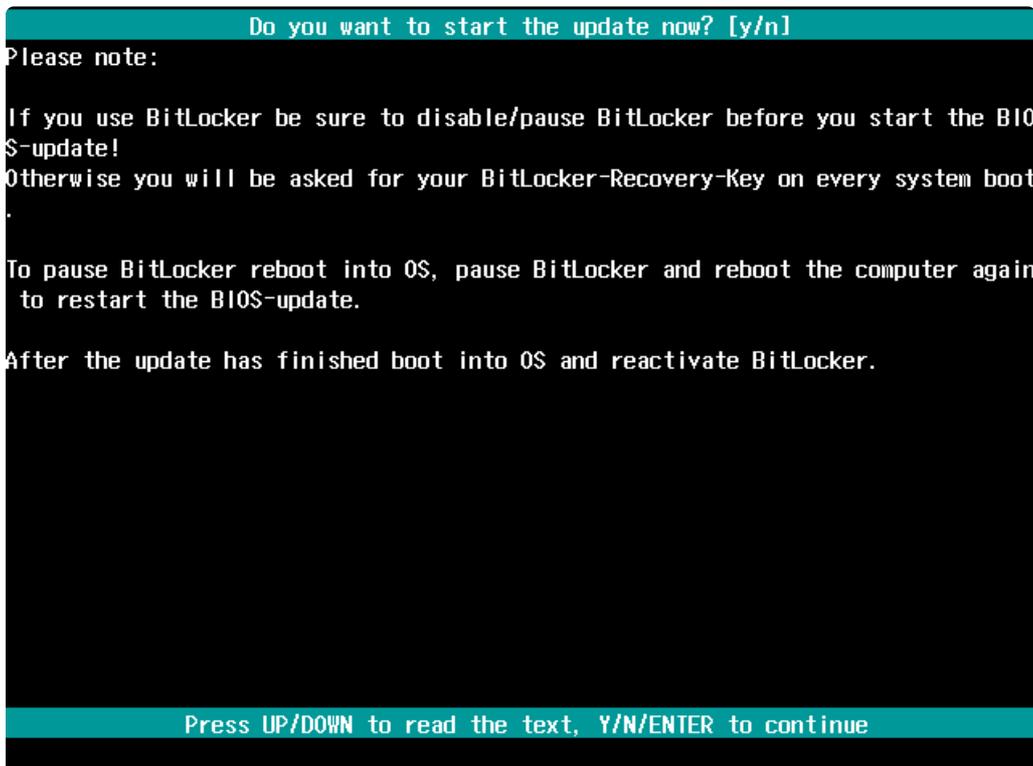
From the window opened, click **Next** to begin install and **OK** to dialogues until success dialog.



After the installation to flash drive is complete, disconnect flash drive from PC and plug it into Industrial Edge device. Powerup device and press **ESC** during power on.



From UEFI menu, enter to BIOS Update . To start BIOS firmware installation press Y until the installation starts.



During the install do not unplug flash drive or do not power off device. Doing so may result in irreversible broken state. After the installation is complete, device will automatically reboot. After a complete boot up flash drive can be unplugged safely.

Erase previous BIOS settings with BIOS update

In order to make BIOS update process to erase previous BIOS flash settings, please modify contents of downloaded files as specified below.

1. Find update.afc file after extraction.
2. Find the line starting with -f V200115.bin -fm -fd -a -n -Ra.
3. Remove option -n .
4. Save changes and exit.
5. Continue following steps from BIOS update.

Firmware Installation via Service Stick

Prepare an Industrial Edge Service Stick

To download service sticks, please refer to section [Download Service Stick Package](#)

To prepare a comprehensive service stick, use `indedge.ipc.200E-servicestick-user_<version>.img.gz`

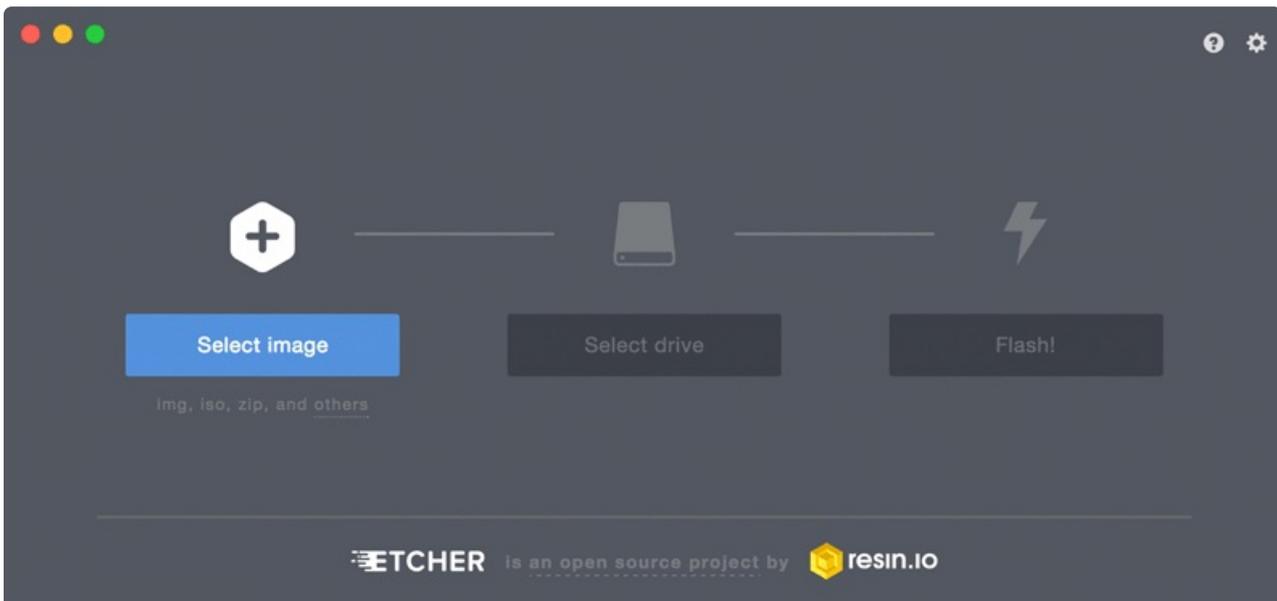
Note: This comprises as well the needed runtime software components which will be installed on Industrial Edge hardware.

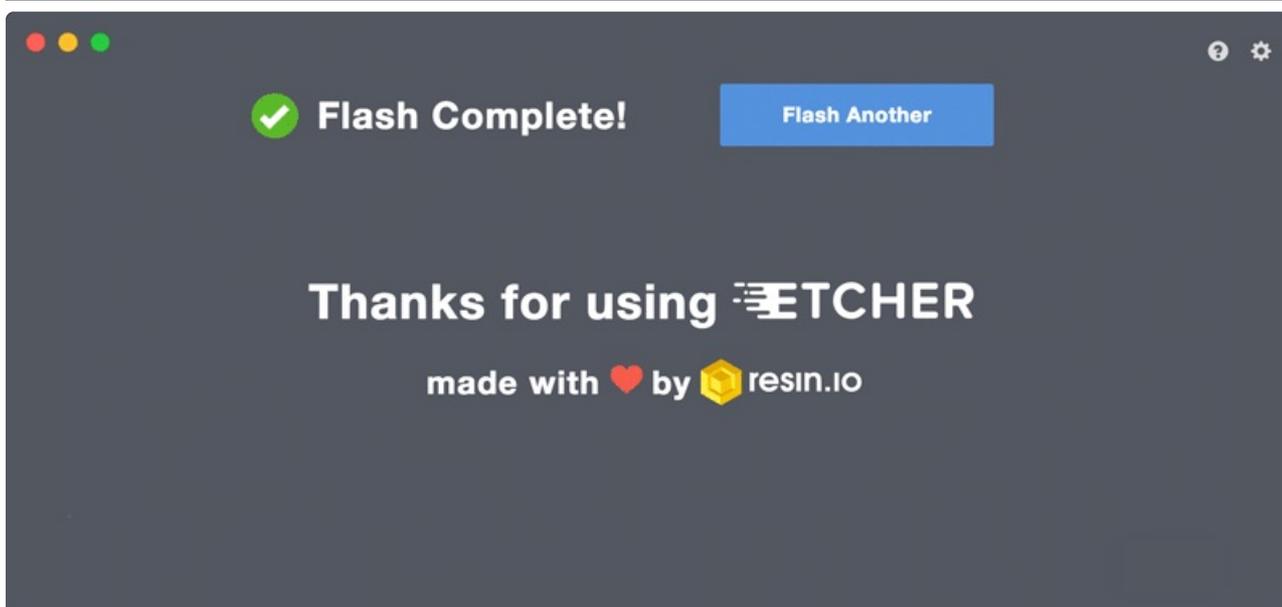
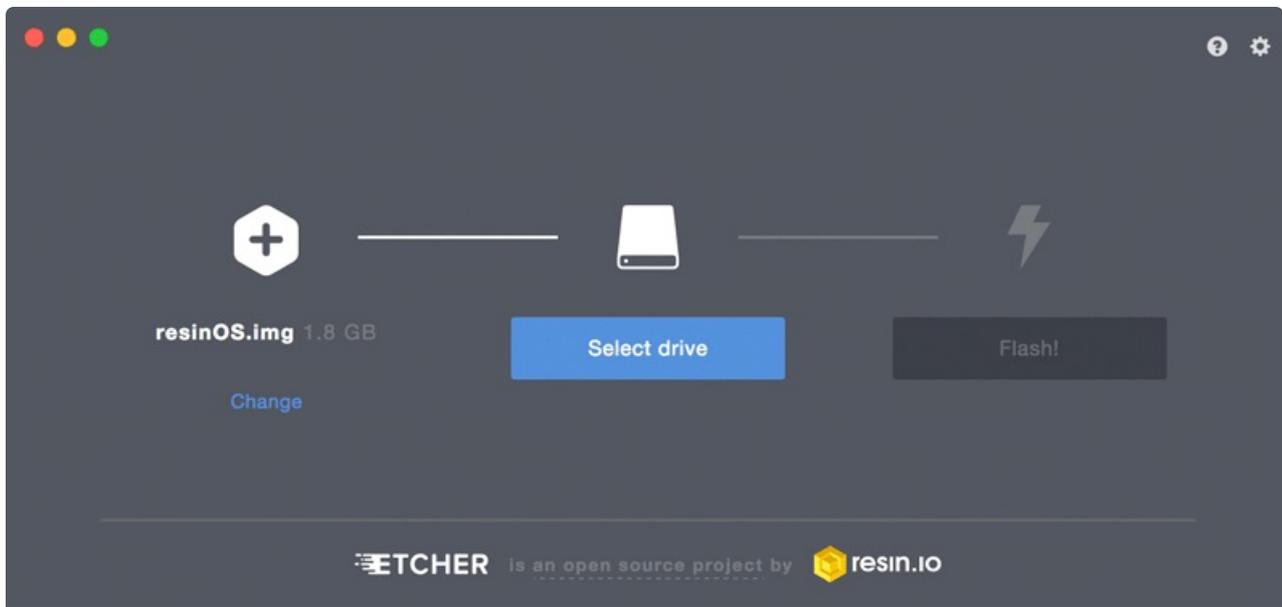
The next step is to flash the image onto an appropriate USB stick with [Etcher](#), a simple, cross platform USB writer and validator. Once you have Etcher installed, start it up. To give Etcher access to your USB stick, your system may prompt you to grant administrative privileges.

To create a bootable Industrial Edge service stick follow these steps:

- Click 'Select image' and find `indedge.ipc.200E-servicestick-user_<version>.img.gz`
- Insert USB stick. Etcher will automatically detect it. If you plugged more than one stick or SD-Cards you will need to select the appropriate one with 'Select drive'.
- Click the 'Flash!' button.

Note: USB stick size has to be 16GB or more





Enable Boot from USB in BIOS

To enable boot from USB the BIOS settings have to be changed. To do so attach power, keyboard and screen to the Industrial Edge. Press **ESC** during power on to enter the BIOS settings. Choose the menu item **SCU** by using arrow and return keys. Go to menu item **Boot** choose **USB Boot** and set value to **Enabled**.

Leave the boot menu and save settings by pressing **F10** .

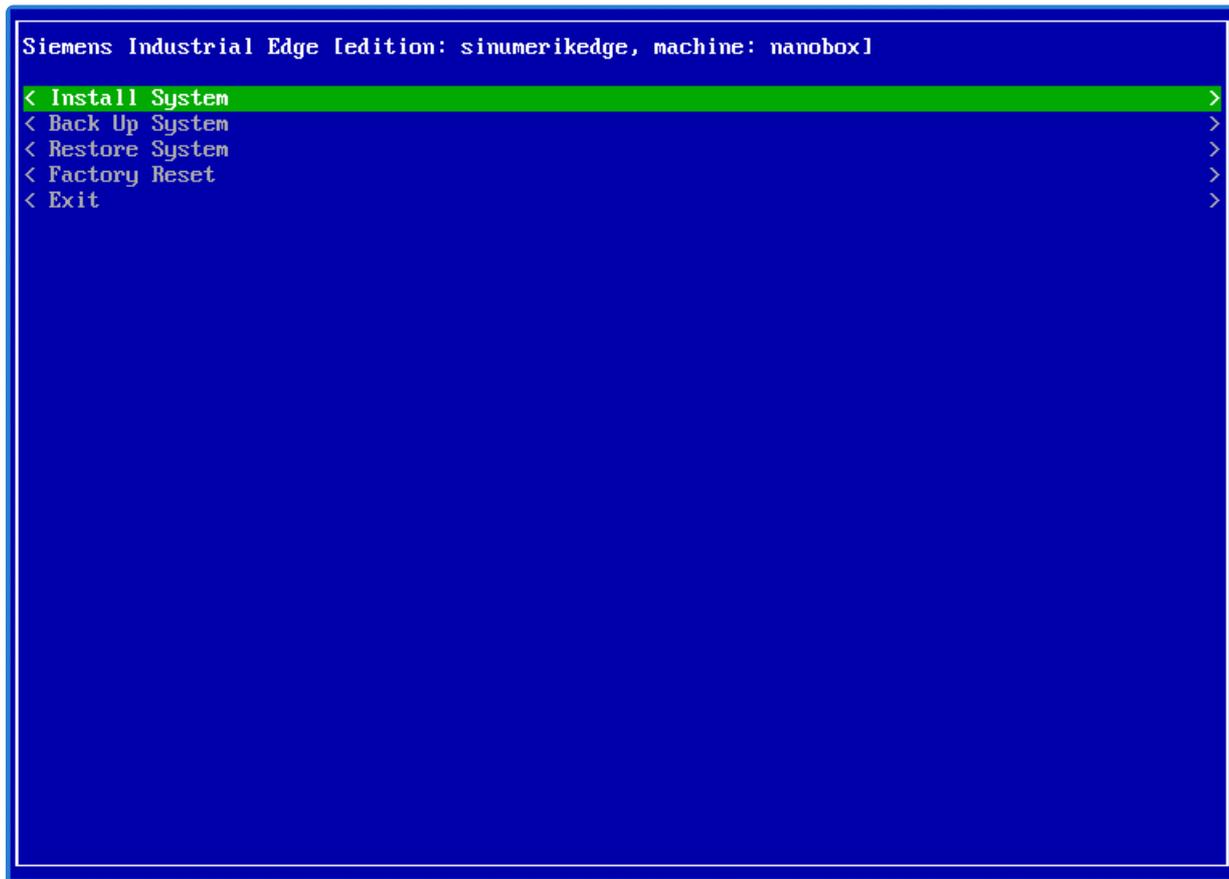
Now it is time to **plug the prepared service stick** and power on again.

Hold the **ESC** - Key during boot process and enter the **Boot Manager** . Choose **EFI USB Device** under **EFI Boot Devices** and confirm it with the return key.

Note: Industrial Edge device will refuse to boot up unsigned images.
If encountered with a such state, make sure that a signed image is installed to device.

Install System

The system is now booted from the Industrial Edge service stick and comes up with the service menu.



Note: Navigation is done with arrow keys; selection is done with space bar; confirmation is done with return key

Choose **Install system** and select the industrial-image in the next screen. Confirm to install and wipe all data on box.

The installation is now automatically executed. After completion is signaled, **Installation Complete** screen is shown. In this screen, recovery key should be noted and kept in secure location to use it for further operations. This recovery key will be used for backup and restore operations.

Reboot the system and unplug the service stick.

```
Siemens SINUMERIK Edge [edition: sinumerikedge, machine: nanobox]
< Install System
<
< Ch Install industrial-image-sinumerikedge-nanobox.swu to sda?
< (X) (n)
<
< Installation Complete!
Ch <
(X) < Encrypted Filesystem created with recovery key "7cdf2020-94e3-4962-95be-f9dc1bd4923d" this
is needed for backup/restore/factory reset
<
< Please reboot the device, USB drive should not be removed until reboot completes!
No < Reboot >
```

System Startup

Industrial Edge now boots up. To login with edge choose

User: `edge`

For password, please refer to [default passwords](#)

You will be asked to change the default password during initial login.

Note:

It is strongly advised to change the default passwords immediately.

Password Policy:

Minimum 8 characters. Includes at least one from each character set; uppercase, lowercase, digit, special.

Boot System

Industrial Edge devices have their bootloader system powered by `Efibootguard` bootloader. This enables devices to have fail-save update mechanism.

Backup & Restore

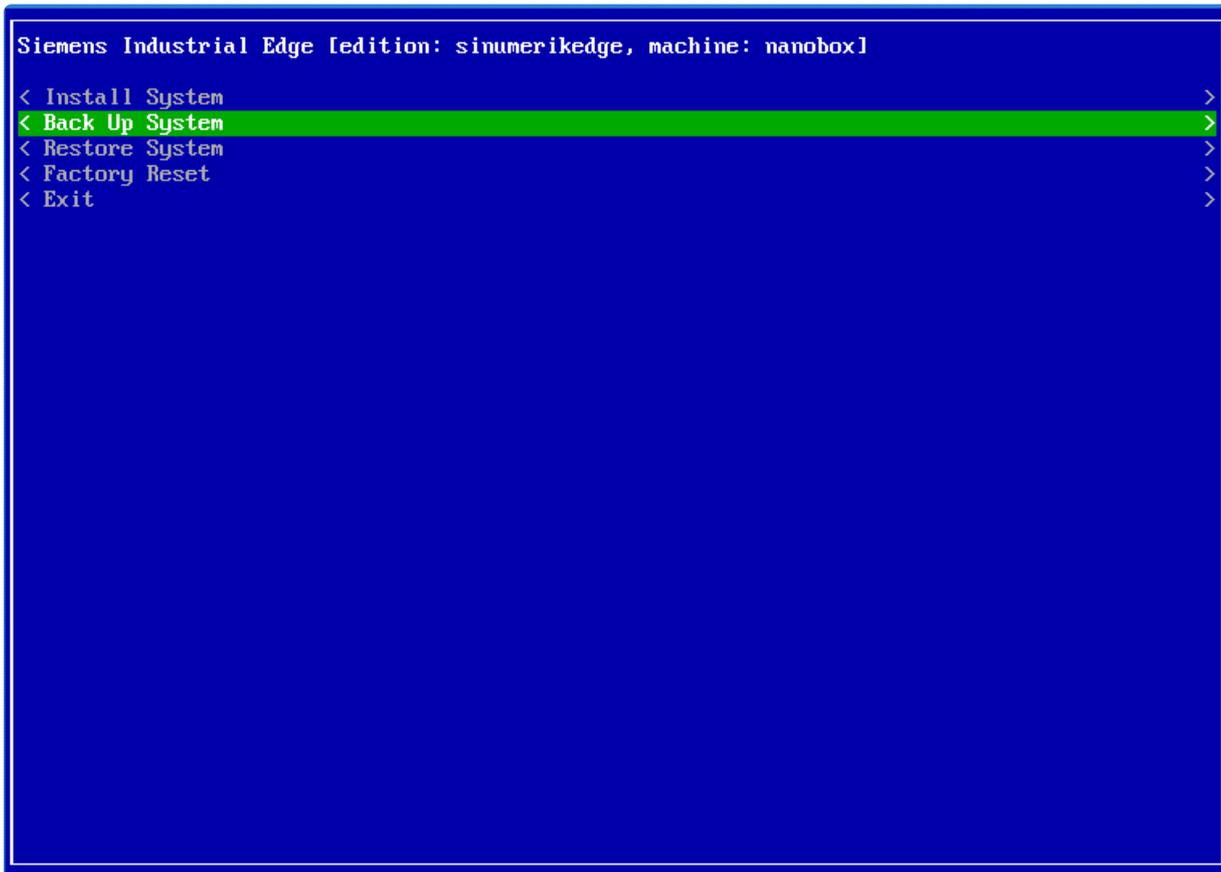
Backup restore via service stick menu only works for Edge devices which were commissioned via service stick, where passphrase was set during commissioning. It does **NOT** work for Edge devices which were pre-commissioned in the factory. However, one still can commission again a factory pre-commissioned Edge device via service stick, if desired. Restore is only possible with exactly the identical service stick which was used for backing up. Therefore the recommended backup restore solution is the manual option as described below in the Manual Backup System chapter. This works in any case, using arbitrary USB devices and keeping the protection by encryption at any time.

Note: Because of disk encryption, content based backup and restore is not feasible.

Note: There are two ways to backup and restore. [Automatic backup system](#) and [manual backup system](#), [automatic restore system](#) and [manual restore system](#).

Automatic Backup System

Once the system is booted, a service menu comes up. There is a "Backup System" option to backup the image to a USB stick.



Select the "Backup System" option, on the next screen select the destination partition and check the "Backup active system partitions" option.

Note: Only FAT32 formatted USBs are supported. You can backup the system to both, bootable service-stick USB and your personal USB. You can also transfer and restore your images. Create a folder with the name "backups" on your personal USB. Now, if you want to restore your image, the service-stick will use that directory as a backup folder and you will be able to restore the backup image.

Note: A recovery passphrase **must** be set while in service stick installation process and it should be kept in a secure location. **Beware**, if the recovery passphrase is lost, it is not possible to recover previous backup again.

```
Siemens Industrial Edge [edition: sinumerikedge, machine: nanobox]
< Back Up System
<
< Choose the system drive to backup:
< (X) sda on ( Micron_5100_MTFD ) -- 240057 MB
<
< Choose the destination partition:
< (X) sdb1 (12G free) partition on USB Flash Drive disk

The following partitions will be backed up:
- Configuration
- User data

[X] Backup active system partitions?
< Next >
< Back >
```

The backup operation will be started. The backup folder's name default format is YYYY-MM-DD_HH-mm. After the backup is finished, the directory name can be changed. Your backup images are stored in the "backups" folder.

Manual Backup System

PREPARATION

Manual backup operation requires SINUMERIK Edge service stick and a large USB storage stick to store backup (If you want to utilize it under windows fat32 or NTFS formatted). As alternative, you might create a big SINUMERIK Edge service media and manually move the second partition to the end of your media and expand your first primary partition using tools like parted/gparted (on Linux) or e.g. diskpart (on Windows). Afterwards the partition layout would look e.g. like this:



Note: Your primary partition then will be fat32 format and introduces therefore a maximum file size limit of 4GB.

Attach a screen and a keyboard to your device prior to powering it on.

STEPS

1. Connect the service stick (and if so your backup USB drive to the Box)
2. Boot from the SINUMERIK Edge Service Stick
3. Press `Alt + F1` to open a console
4. Login with `root:root`
5. Identify the location of your USB devices by performing `fdisk -l` Let's assume the backup device partition was identified as `/dev/sdc1`
6. Mount your storage device `mkdir -p /media/backup` `mount -rw /dev/sdc1 /media/backup`
7. Perform the backup `dd bs=4M if=/dev/sda status=progress | gzip -9 -c | split -b 4G - backup.gz > /media/backup/backup.gz` Note: Since this is a binary disk copy and compression it takes a very long time. Do not interrupt the process. E.g. with an average transfer rate of 15MB/s the 250GB will take ~5h to perform the full backup
8. Sync all outcomes to the media `sync /media/backup` This will lead to example picture below:

```
Filesystem      Size  Used Avail Use% Mounted on
udev            3.9G   0 3.9G   0% /dev
tmpfs           787M   0 778M   2% /run
/dev/sdb2       662M  648M   0 100% /
tmpfs           3.9G   0 3.9G   0% /dev/shm
tmpfs           5.0M   0 5.0M   0% /run/lock
tmpfs           3.9G   0 3.9G   0% /sys/fs/cgroup
tmpfs           787M   0 787M   0% /run/user/0
/dev/sdb1       149G  2.6G 146G   2% /media/backup
root@localhost:~# dd bs=4M if=/dev/sda status=progress | gzip -9 -c | split -b 4000M - backup.gz > ./ba
240010657792 bytes (240 GB, 224 GiB) copied, 8281.03 s, 29.0 MB/s
57234+1 records in
57234+1 records out
240057409536 bytes (240 GB, 224 GiB) copied, 8281.97 s, 29.0 MB/s
root@localhost:~# sync
root@localhost:~# ls
backup.gz backup.gzaa backup.gzab backup.gzac backup.gzad backup.gzae backup.gzaf backup.gzag backup.gzah backup.
root@localhost:~# ls -l
total 43924500
-rwxr-xr-x 1 root root      0 Apr 10 12:00 backup.gz
-rwxr-xr-x 1 root root 4194304000 Apr 10 12:05 backup.gzaa
-rwxr-xr-x 1 root root 4194304000 Apr 10 12:36 backup.gzab
-rwxr-xr-x 1 root root 4194304000 Apr 10 12:53 backup.gzac
-rwxr-xr-x 1 root root 4194304000 Apr 10 12:58 backup.gzad
-rwxr-xr-x 1 root root 4194304000 Apr 10 13:03 backup.gzae
-rwxr-xr-x 1 root root 4194304000 Apr 10 13:09 backup.gzaf
-rwxr-xr-x 1 root root 4194304000 Apr 10 13:14 backup.gzag
-rwxr-xr-x 1 root root 4194304000 Apr 10 13:19 backup.gzah
-rwxr-xr-x 1 root root 4194304000 Apr 10 13:24 backup.gzai
-rwxr-xr-x 1 root root 4194304000 Apr 10 13:46 backup.gzaj
-rwxr-xr-x 1 root root 3035645466 Apr 10 14:18 backup.gzak
root@localhost:~#
```

Metrics 240GB Bitcopy / 8280 secs / 44GB Storage : time in this case was limited by the write performance of the USB harddrive.

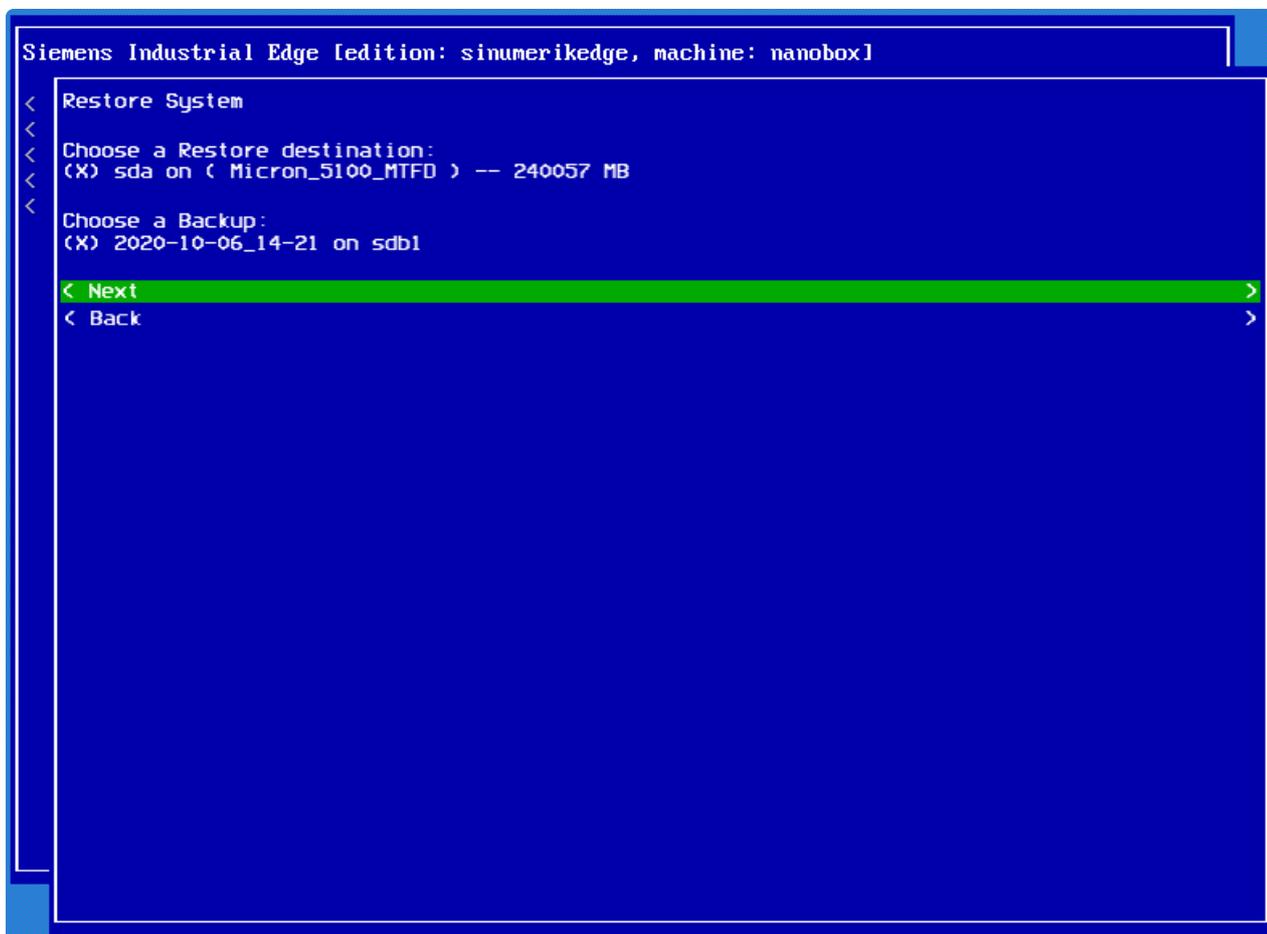
1. Now the backup has been finished and you can remove your SINUMERIK Edge Service Stick

Automatic Restore System

Once the system is booted, the service menu comes up. Select the "Restore System" option.

```
Siemens Industrial Edge [edition: sinumerikedge, machine: nanobox1]
< Install System >
< Back Up System >
< Restore System >
< Factory Reset >
< Exit >
```

On the next screen, select the backup image you want to restore and proceed with the "Restore backup" option.



After the restoring operation is completed, unplug your USB stick and reboot the system.

Note: Whilst restoring a backup, devices **must** boot from their original service stick. Booting up from any other service stick will fail to restore a backup.

Manual Restore System

1. Repeat the actions from [Backup System](#) 1-6
2. Perform the restore `cat /media/backup/backup.gz* | gunzip -c | dd bs=64k of=/dev/sda status=progress`

Note: Since this is a binary disk copy and compression it takes a very long time. Do not interrupt the process.

Note: This will override the whole harddisk.

Encrypted Disk

During the first boot, industrial installer generates an initial boot key to unlock and access the encrypted file system on device boot. So that, you may want to save this key to a secure location to use it later in case of any failure on booting from disk.

Backup Initial Boot Key

1. Plug your bootable USB into device
2. Choose `Backup Initial Boot Key` from boot menu
3. Select the location on the target device in which to store backed-up key

Restore Initial Boot Key

1. Plug your bootable USB into device
2. Choose **Restore Initial Boot Key** from boot menu
3. Choose the key you want to restore from list of backed-up keys

Default Passwords

Default password is provided among files in service stick in "Password.txt".

Note:

It is strongly advised to change the default passwords immediately.

Password Policy:

Minimum 8 characters. Includes at least one from each character set; uppercase, lowercase, digit, special.

New Asset License Model: Machine Tool Framework

Machine Tool Framework Licensing Model is being introduced with SINUMERIK Edge 3.3 Release, where it is possible to benefit from modular licensing.

- "Machine Tool Framework" basic license will be granted to your asset upon onboarding.
- "Machine Tool Framework (pro)" license is used to enable high end features and subscribe up to 25 HF datapoints for SINUMERIK Adapter in your asset.
- "Machine Tool Framework (pro) +25" license is used to subscribe to additional 25 HF datapoints for SINUMERIK Adapter in your asset.

How may I use Machine Tool Framework (Pro) license and Machine Tool Framework (Pro) +25 license?

You will need to either purchase from S-DEX or contact your local Siemens sales representative to obtain Machine Tool (Pro) and Machine Tool Framework (Pro) +25 licenses. The number of licenses you agreed will be available to your tenant shortly afterwards. You will then need to explicitly assign your licenses for your assets individually, as explained in the "Manage MySINUMERIK Edge /App Management" topic.

An asset may have only one Machine Tool Framework (pro) license.

An asset may have more than one Machine Tool Framework (pro) +25 license.

As long as your asset is onboarded, you may revoke your assigned licenses back from your asset so that they will be available for your tenant and can be assigned to another assets. Revoking a license will decrease limit of allowed HF data subscriptions for that asset, which may lead to inconsistencies depending on the Edge applications installed in your asset.

Machine Tool Framework licensing model will only be compatible with SINUMERIK Edge firmware 3.3 and later

If you wish to onboard and use a SINUMERIK Edge asset with firmware before 3.3, your asset will need to have SINUMERIK Edge Single Licensing Model. In order to do so, you will need to explicitly make your decision while configuring your asset for the first time, as defined in the onboarding section of "Manage MySINUMERIK Edge Insights Hub Applications" topic. If you don't make an explicit decision, your SINUMERIK Edge asset will have Machine Tool Framework licensing model by default.

If your SINUMERIK Edge asset has Machine Tool Framework licensing model and firmware version before 3.3, you will no longer be able to install or configure edge applications in your SINUMERIK Edge asset; you will be asked to update your asset to firmware 3.3 or later.

It will not be possible to switch an asset from Machine Tool Framework licensing model to SINUMERIK Edge Single Licensing model. You need to make your licensing model decision carefully while configuring an asset for the first time.

I already have an asset onboarded before Sinumerik Edge 3.3 Release

Your current licensing model is SINUMERIK Edge Single Licensing model. You will not need any additional license as long as you keep using firmware version before 3.3.

If you wish to upgrade to firmware 3.3 or later, you will need to assign pro license to your asset in order to keep your edge apps benefiting from high end features (based on the number of HF data points being subscribed, you may need to assign additional licenses as well). To get the additional licenses needed, please contact local Siemens sales representative.

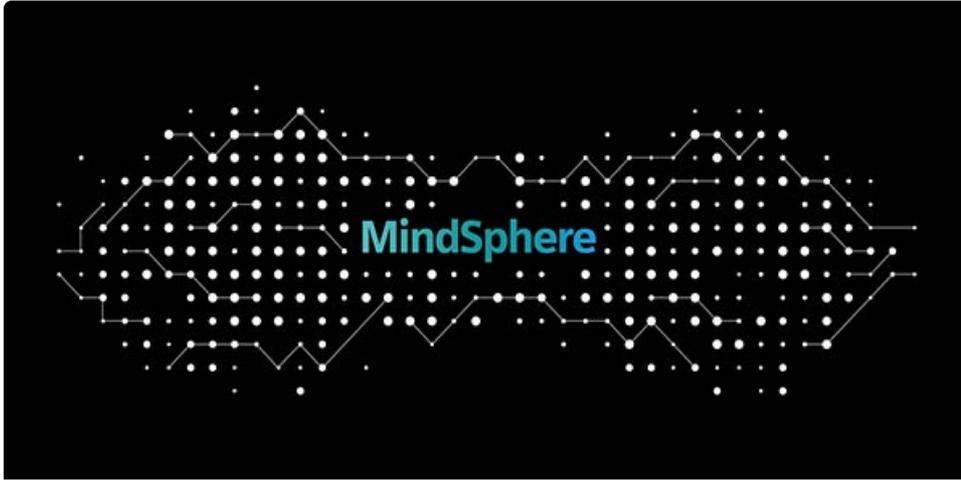
Once your SINUMERIK Edge Single License expires (which is an annual license, renewed annually by system as long as your asset is onboarded), * If you have firmware version 3.3 or later, the license will be converted to Machine Tool Framework license * If you have firmware before 3.3, the license will be kept as the same SINUMERIK Edge Single License

How may I track my assigned Machine Tool Framework (Pro) and Machine Tool Framework (Pro) +25 licenses?

Tenant summary feature in the "Manage MySINUMERIK Edge /App Management" section can be used to track assigned and available licenses, further details can be found in the relevant section.

Manage MySINUMERIK Edge Insights Hub Applications

Overview Insights Hub Overall



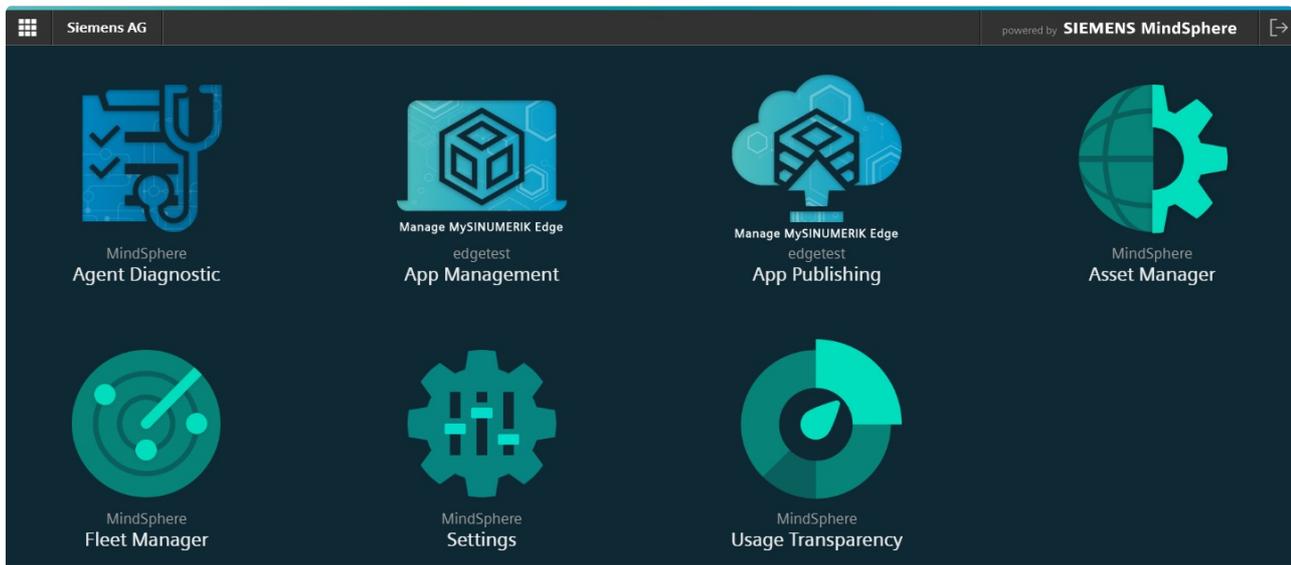
For further details about Insights Hub please refer to the pages listed below:

- [Insights Hub Home](#)
- [Insights Hub Documentation](#)
- [Insights Hub Developer Documentation](#)

Industrial Edge Backend Applications

Required roles need to be assigned to the user account to continue using the Industrial Edge backend applications.

1) Login to Insights Hub with your credentials. Then from the Insights Hub Launchpad choose *Settings*.

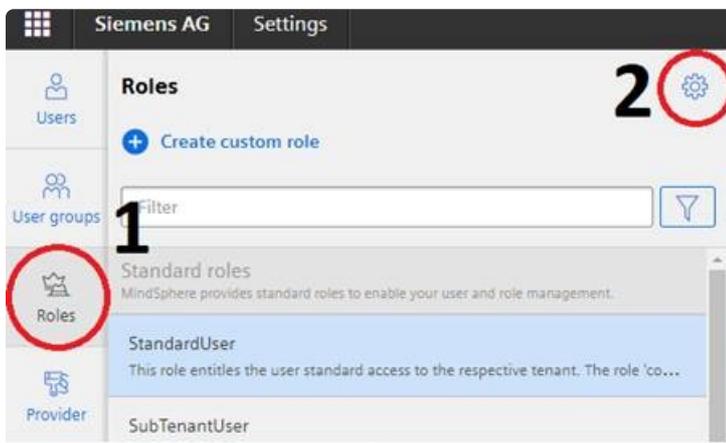


Note: As a prerequisite, to create new asset, the *AssetManager (mdsp:core:assetmanager.admin)* role should be assigned to your user. Tenant admin(s) of each IoT tenant can enable this role for their tenants by following the steps below:

- Login to the IoT tenant with a tenant admin account, Open Settings from Insights Hub Launch Pad



- Select Roles and open the Configurations Menu



- Enable "assetmanager-admin" role, Click "Next" button and then click "Save" Button.

Edit assignment for roles configuration Step 1 of 3

Select roles to use them in your tenant additionally. Deselect roles to remove them from your tenant.

Note that removing roles from this tenant might remove permissions granted to users.

Filter Filter ▾

Deselect all

Application roles
MindSphere applications provide individual roles to extend your user and role management.

<input type="checkbox"/>	agentdiagnostic (mdsp:core) admin Role grants admin access for Agent Diagnostic UI
<input type="checkbox"/>	agentdiagnostic (mdsp:core) standarduser Role grants StandardUser access for Agent Diagnostic UI
<input checked="" type="checkbox"/>	assetmanager (mdsp:core) admin Role grants admin access for Asset Manager
<input type="checkbox"/>	assetmanager (mdsp:core) standarduser Role grants standarduser access for Asset Manager
<input type="checkbox"/>	assetmanager (mdsp:core) subtenantuser

* You have one unsaved change.

Reset Cancel Next

2) Search for the account name from the left search bar under Users and click **Edit direct assignments**.

Siemens AG Settings powered by SIEMENS MindSphere

Users + Create user

Search: industrial

Edge, Industrial
industrial@siemens.com

User type Edit user type

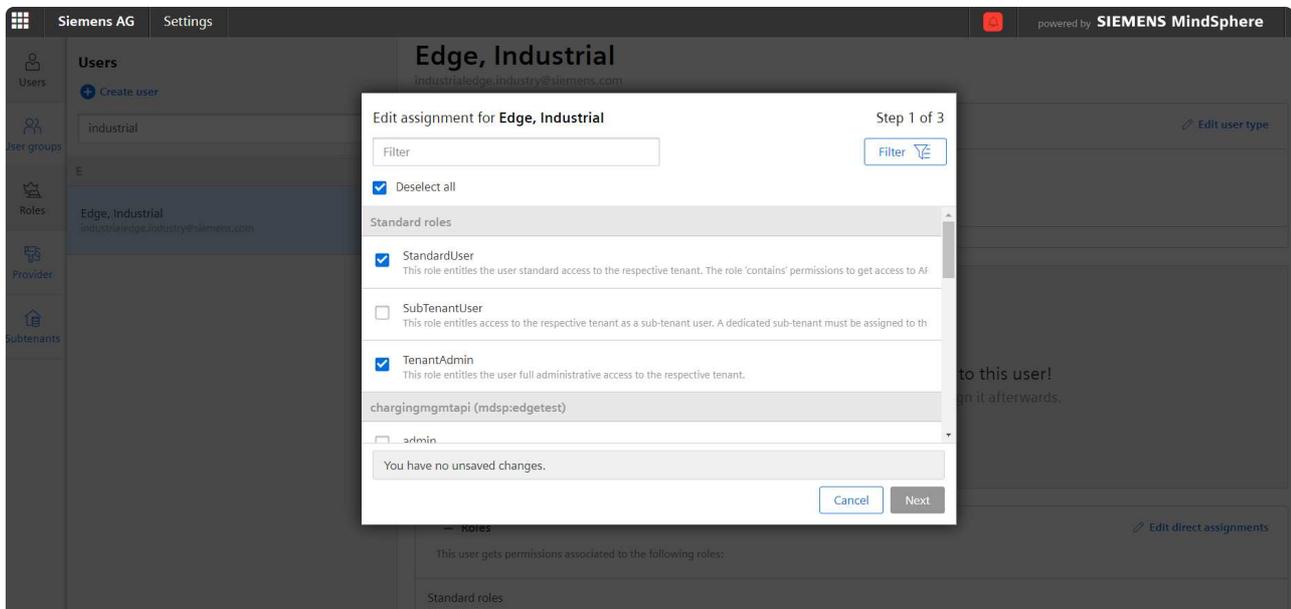
Global user
A global user can access all data within the tenant.

Roles Edit direct assignments

This user gets permissions associated to the following roles:

Standard roles

3) **Edit assignment** window helps to select required roles for applications to be used. Additional to "StandardUser" role, all user and admin roles listed under the related application name should be selected. For instance, the application related roles for an application are likely to be: * mdsp.[OPERATOR_TENANT_NAME].[APPLICATION_NAME].user and * mdsp.[OPERATOR_TENANT_NAME].[APPLICATION_NAME].admin.



4) To use the *Manage MySINUMERIK Edge /App Management* and *Manage MySINUMERIK Edge /App Publishing* applications, the roles listed below should be assigned respectively for each application in the **Edit role assignment** window:

Roles for **Manage MySINUMERIK Edge /App Management**:

- mdsp:edgetest:edgeappmgmt.user
- mdsp:edgetest:edgeappmgmt.admin

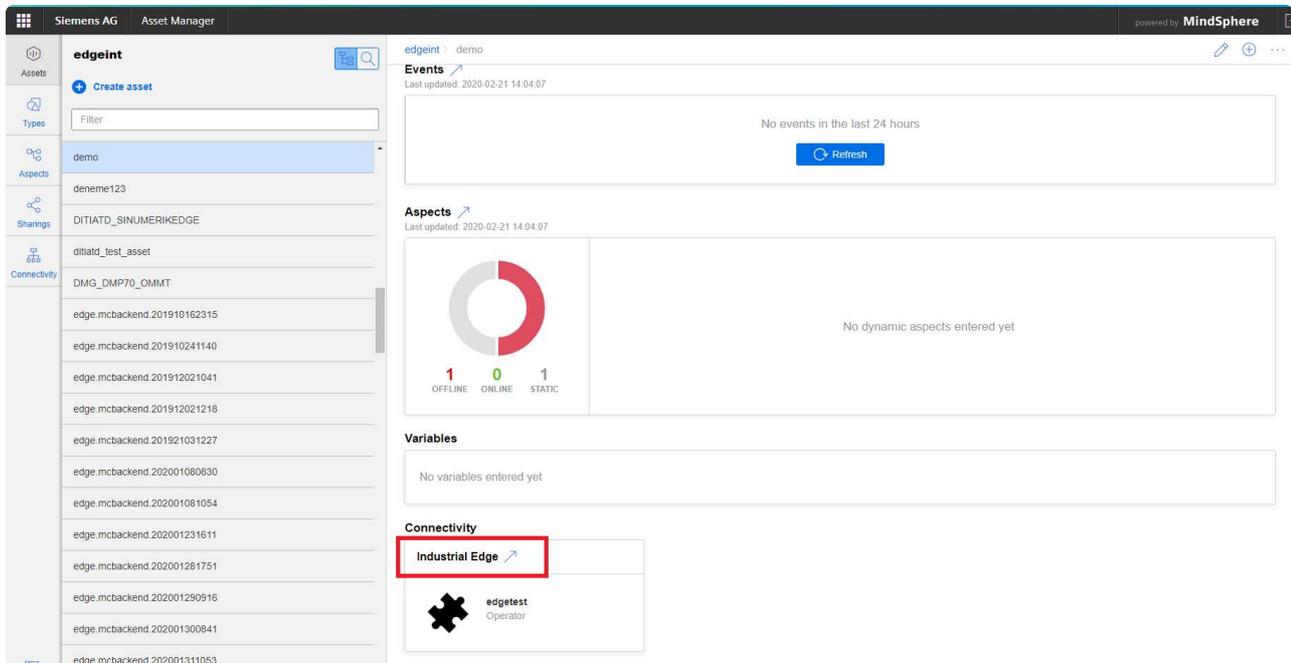
Roles for **Manage MySINUMERIK Edge /App Publishing**:

- mdsp:edgetest:edgeapppublish.user
- mdsp:edgetest:edgeapppublish.admin

Additionally, to enable and use Industrial Edge plugin of Asset Manager, below roles should be assigned in same window:

Roles for **Asset Manager Industrial Edge plugin**:

- mdsp:edgetest:edgeassetconfig.user
- mdsp:edgetest:edgeassetconfig.admin
- mdsp:core:assetmanager.admin

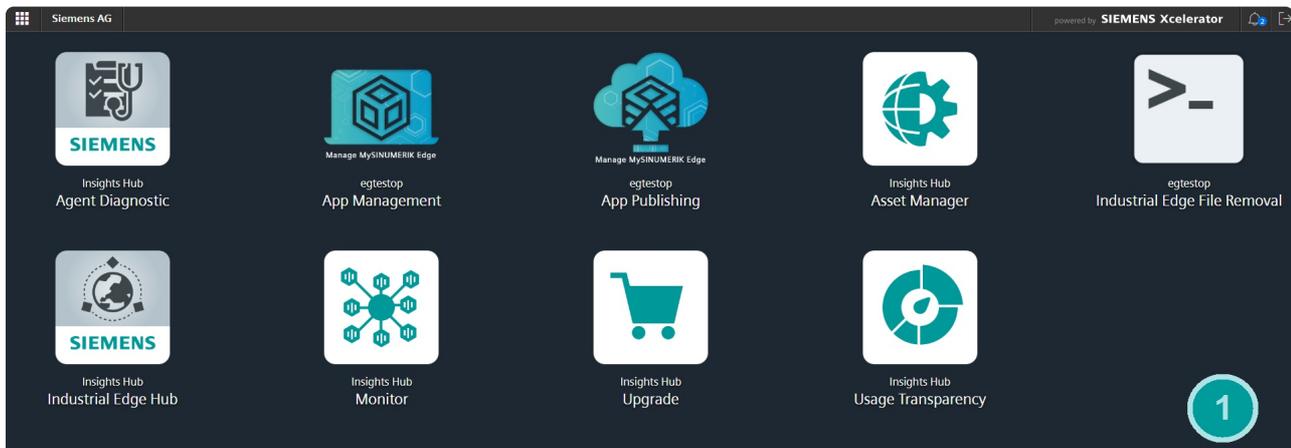


5) Click Close and log-out. After the first log-in, the related applications will be ready to use in the Insights Hub Launchpad.

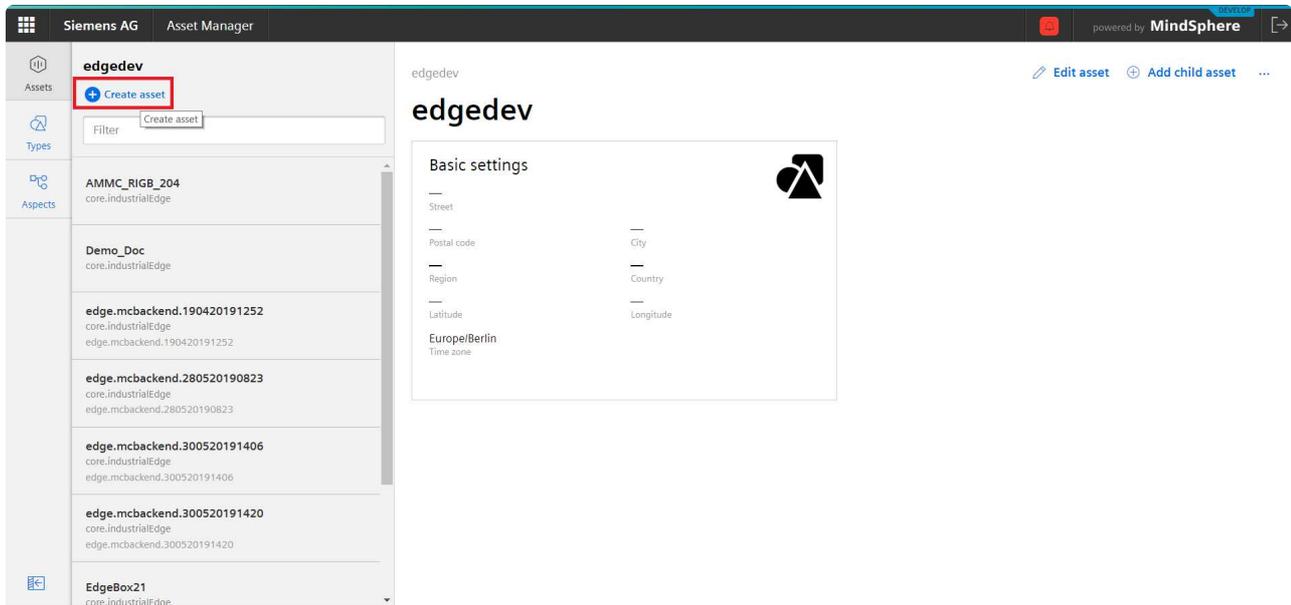
Onboarding

Create and Onboard Industrial Edge Asset

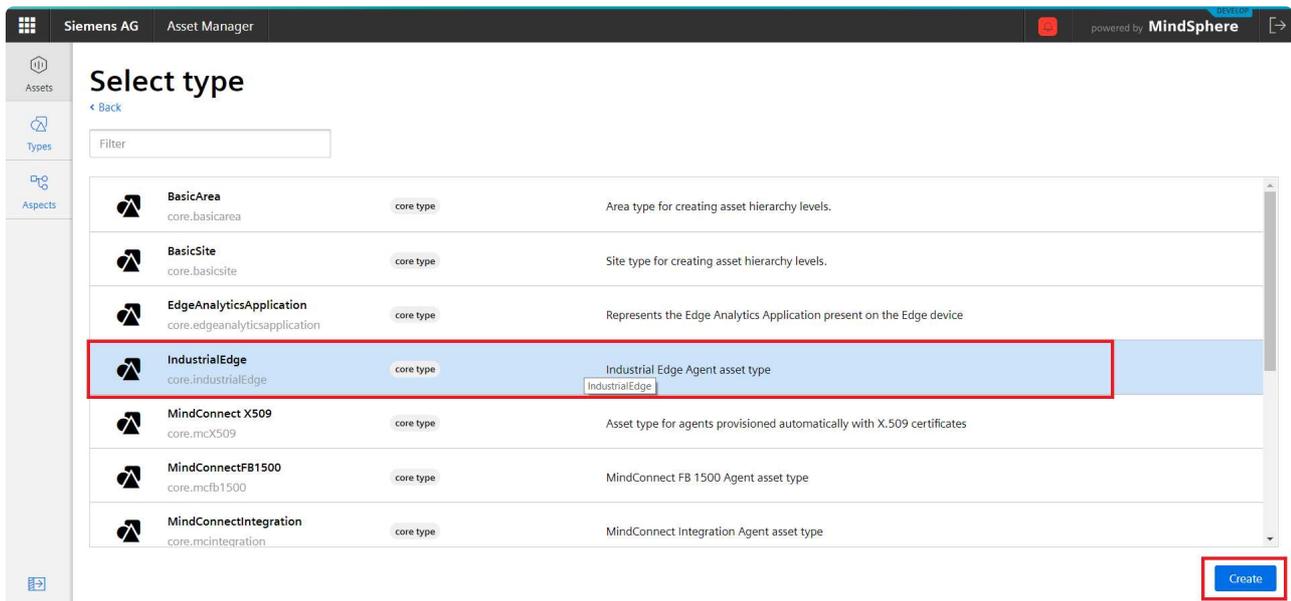
1) Login to Insights Hub with your credentials. Then choose *Asset Manager* from the Insights Hub Launchpad.



2) Click the "+" icon to create a new asset.

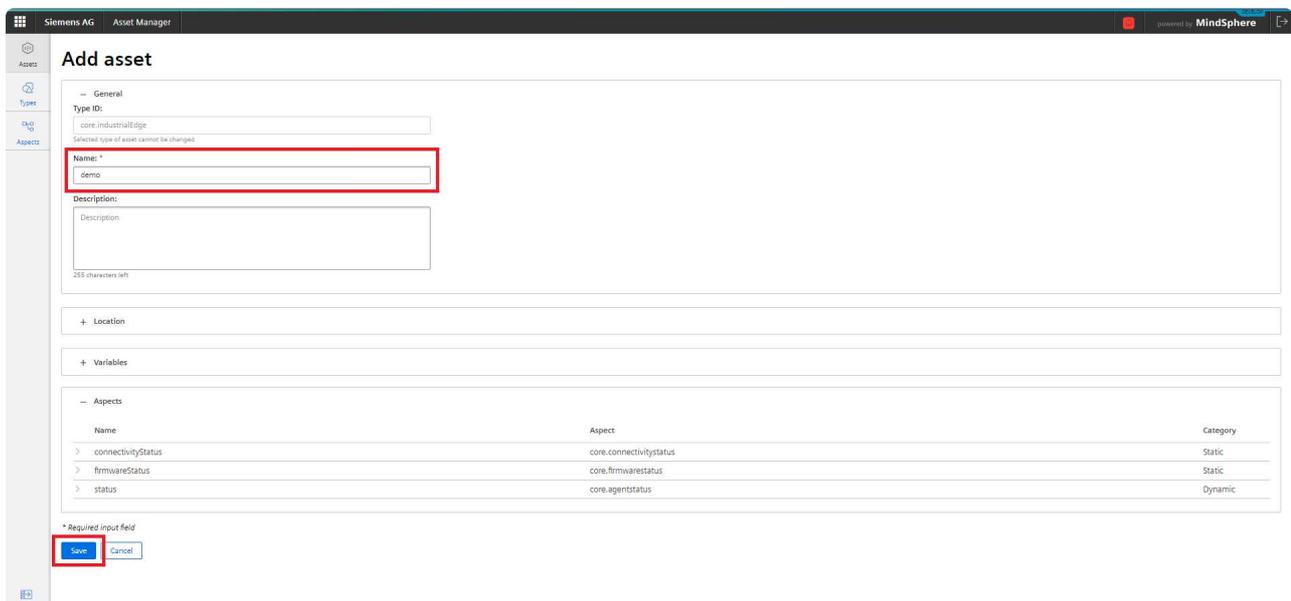


3) Select Industrial Edge as type.

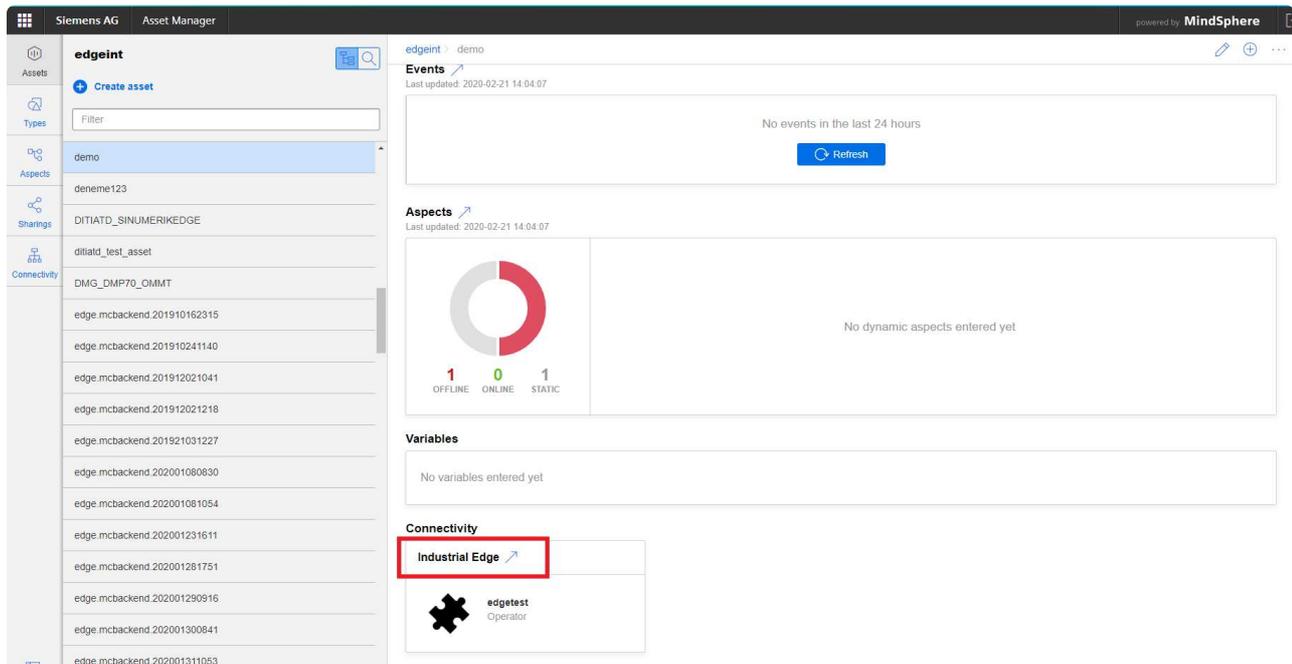


4) Input data to your new asset and click Save.

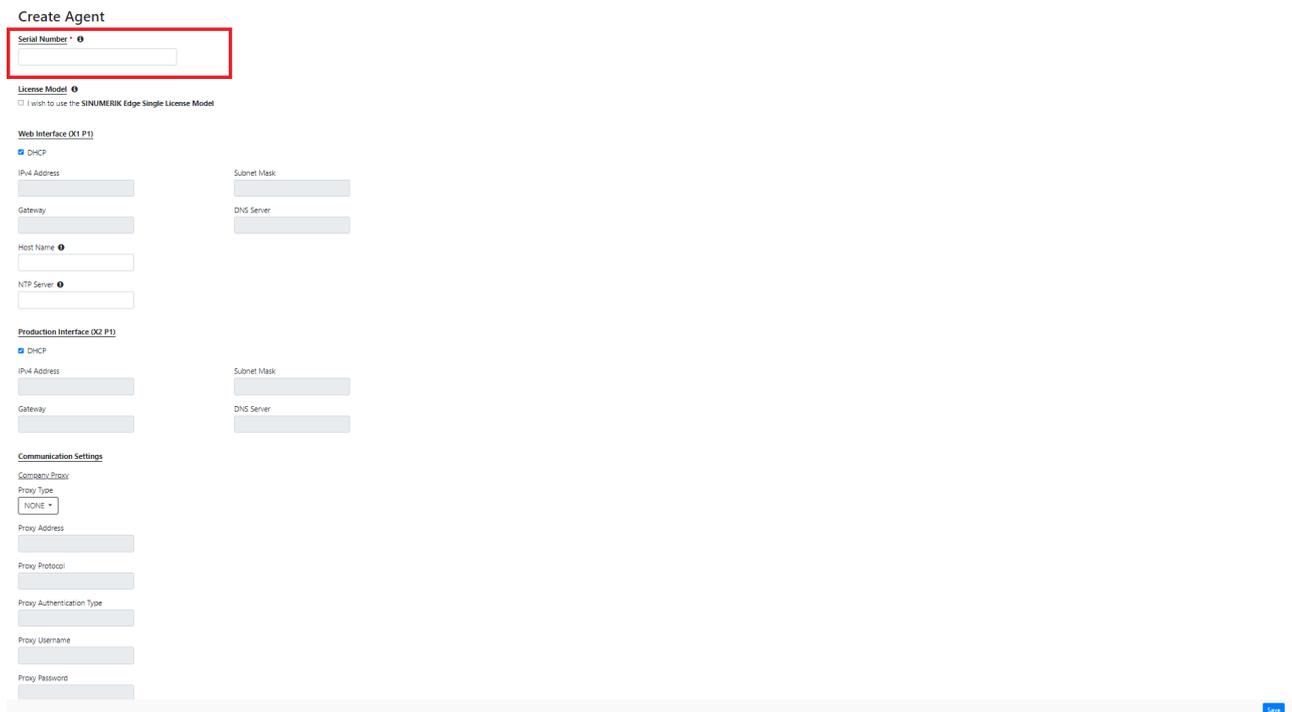
Hint: Adding the address and GPS coordinates is not mandatory but will help you in managing your fleet.



5) Select your asset from the asset list and click on **right arrow** icon to navigate to industrial edge plugin for your asset configuration.



When an asset is created, serial number should be defined for one time according to box information that it is written on label under box. Please check the serial number format from info icon in the following figure. If the serial number is not valid, onboarding fails. Also a serial number can be used only in one asset, otherwise error message is shown while creating agent.

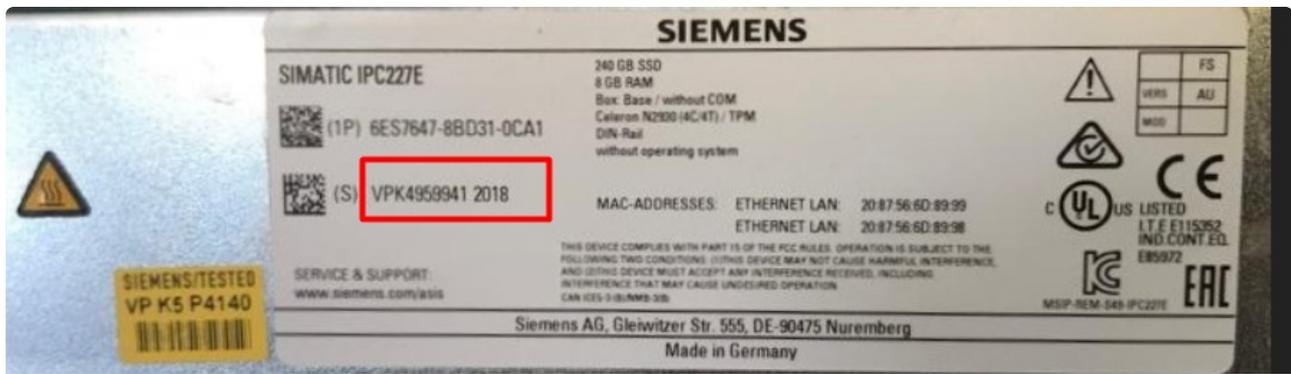


Create Agent

Serial Number * ⓘ

Sample Serial Number
format: '(S) VP K1234567
2018'

The red box in following figure shows a serial number field (VPK4959941 2018).



6) Machine Tool Framework Licensing Model is used by default for the onboarded assets. If you wish to onboard an asset with SINUMERIK Edge Single Licensing Model, please make your selection accordingly. Further details about the licensing models can be found in the "Machine Tool Framework Licensing Model" section.

Create Agent

Serial Number

License Model

I wish to use the SINUMERIK Edge Single License Model

Web Interface (X1 P1)

DHCP

IPv4 Address Subnet Mask

Gateway DNS Server

Host Name

NTP Server

Production Interface (X2 P1)

DHCP

IPv4 Address Subnet Mask

Gateway DNS Server

Communication Settings

Company Proxy

Proxy Type

Proxy Address

Proxy Protocol

Proxy Authentication Type

Proxy Username

Proxy Password

[Save](#)

7) From the **Hardware** tab, identify your network configuration. This comprises DHCP settings as well as the proxy configuration.

If the box uses static IP to reach the Insights Hub, * from the **Web interface (X1 P1)** section, **DHCP** checkbox should be *disabled*, * the **IPv4 Address**, **Subnet Mask**, **Gateway** and **DNS Server** information should be filled.

If the box uses dynamic IP to reach the Insights Hub, * from the **Web interface (X1 P1)** section, the **DHCP** checkbox should be *enabled*. * other information sections should be disabled automatically.

If it's desired to connect the box by a hostname, the **Host Name** field can be set. It should be noted that this option is only valid for in presence of local DNS. After these configurations, the device can be accessed by hostname, eg local diagnostic dashboard application can be accessed by `https://<hostname>:5443/diag` on a web browser.

For the **Production Interface (X2 P1)**, currently only static IP is supported, the **DHCP** checkbox should be *disabled* for SINUMERIK devices. Necessary **IPv4 Address** and **Subnet Mask** information should be filled.

If Proxy is used to reach the Insights Hub, the **Proxy Type** should be *FIXED*. The proxy input format is `http://<proxy ip-address>:<port>` .

If Proxy is not used to reach the Insights Hub, the **Proxy Type** should be *NONE*. (If you are not aware of your

company proxy, please contact your local IT administration).

Note: There are certain global NTP servers preconfigured. If needed, you can configure local NTP Server from **NTP Server** section. Please refer to **Time Behavior** chapter for further details of system time settings.

When the configurations are completed, click **Save**.

Create Agent

Serial Number

License Model I wish to use the SINUMERIK Edge Single License Model

Web Interface (X1 P1)

DHCP

IPv4 Address Subnet Mask

Gateway DNS Server

Host Name

NTP Server

Production Interface (X2 P1)

DHCP

IPv4 Address Subnet Mask

Gateway DNS Server

Communication Settings

Catagory Filter

Proxy Type

Proxy Address

Proxy Protocol

Proxy Authentication Type

Proxy Username

Proxy Password

Save

7) Download the **Onboarding Key** by clicking "Create and Export Onboarding Key" button.

Note: Since this is a common config format the browser may ask you if you want to keep this file dependent on the local security settings.

Siemens AG Asset Manager powered by MindSphere

Industrial Edge Plugin demo_doc IndustrialEdge

Overview Hardware Firmware

Industrial Edge

Device Type:	INDUSTRIALEGE
License Model Preference:	Machine Tool Framework License Model
Onboarding Status:	Ready For Onboarding
Connection Status:	
Serial Number:	110620191228
Configuration Object:	Create and Export Onboarding Key

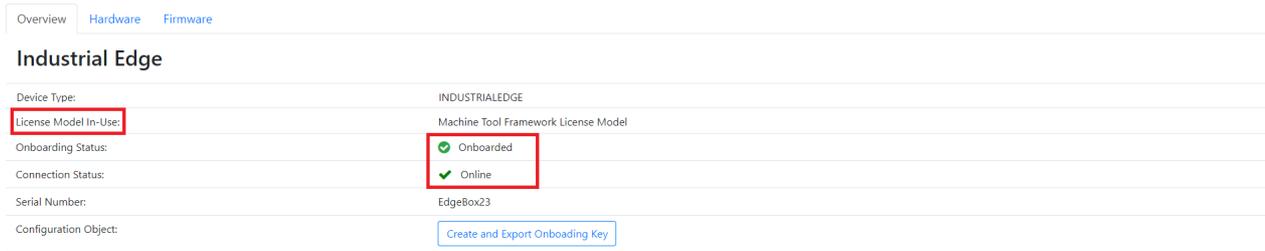
Offboard

Manage MySINUMERIK Edge Readme OSS v3.4.0

8) Copy the downloaded configuration file to a USB-Stick(which should be fat32 formatted). Then plug the stick to your SINUMERIK Edge, the Onboarding process will be started automatically. Refresh the page to inspect the state change from *Onboarding* to *Onboarded* on the Overview Tab.

Note If the state does not change in 5 minutes, you can download the onboarding related logs from **Diagnostic Application** and check the cause of the problem.

Note Do not turn off or reboot SINUMERIK Edge device and do not unplug onboarding USB device until Insights Hub reports online/onboarded status on Manage MySINUMERIK Edge /App Management UI.

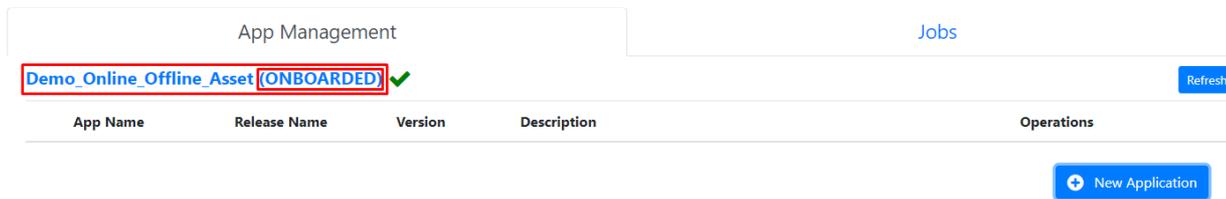


The screenshot shows the 'Industrial Edge' overview page with the following details:

Device Type:	INDUSTRIALEEDGE
License Model In-Use:	Machine Tool Framework License Model
Onboarding Status:	✓ Onboarded
Connection Status:	✓ Online
Serial Number:	EdgeBox23
Configuration Object:	Create and Export Onboarding Key

After the asset is **onboarded**, **License Model In-Use** section will be appeared instead of **License Model Preference** section. The actual license model will be displayed in this area.

9) An **Onboarded Asset** is displayed with the appropriate status on Manage MySINUMERIK Edge /App Management UI.



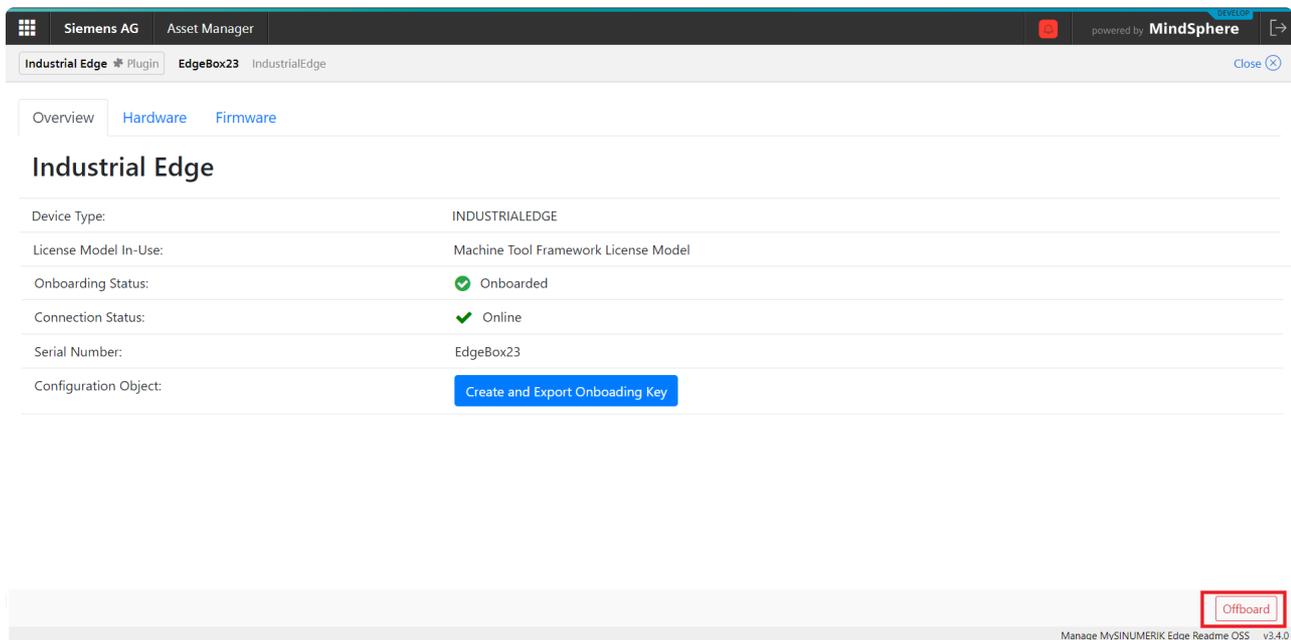
The screenshot shows the 'App Management' interface with the following details:

App Name	Release Name	Version	Description	Operations
Demo_Online_Offline_Asset				Refresh

Buttons: [New Application](#)

Offboard Asset

1) To offboard an onboarded asset, click the **Offboard** button in the Overview section.



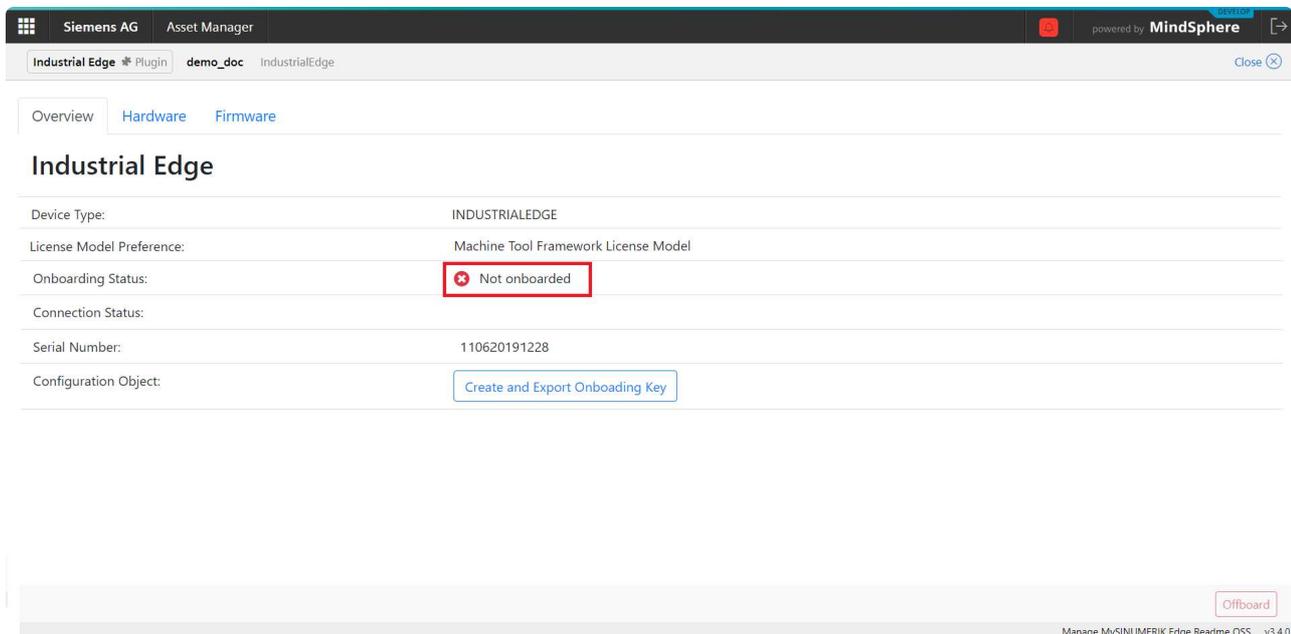
The screenshot shows the 'Industrial Edge' overview page with the following details:

Device Type:	INDUSTRIALEEDGE
License Model In-Use:	Machine Tool Framework License Model
Onboarding Status:	✓ Onboarded
Connection Status:	✓ Online
Serial Number:	EdgeBox23
Configuration Object:	Create and Export Onboarding Key

Buttons: [Offboard](#)

Footer: Manage MySINUMERIK Edge Readme OSS v3.4.0

2) After this operation the status will be changed to *Onboarding* which means that the asset is offboarded.

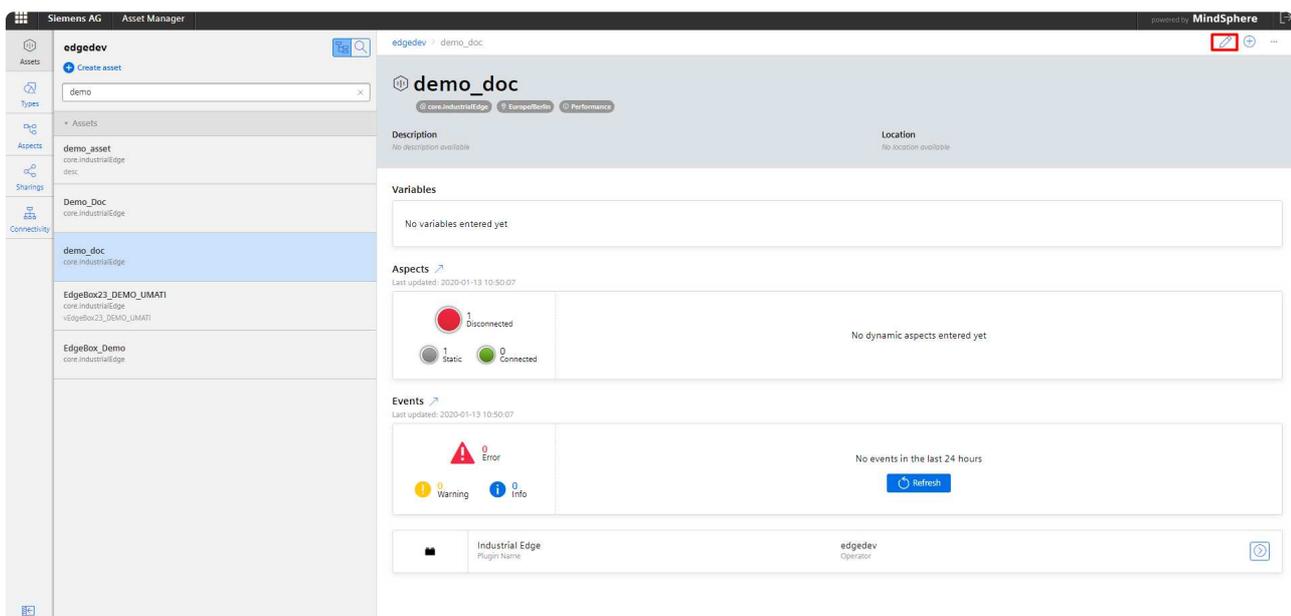


3) An Offboarded Asset is displayed with the appropriate status on Manage MySINUMERIK Edge /App Management UI.

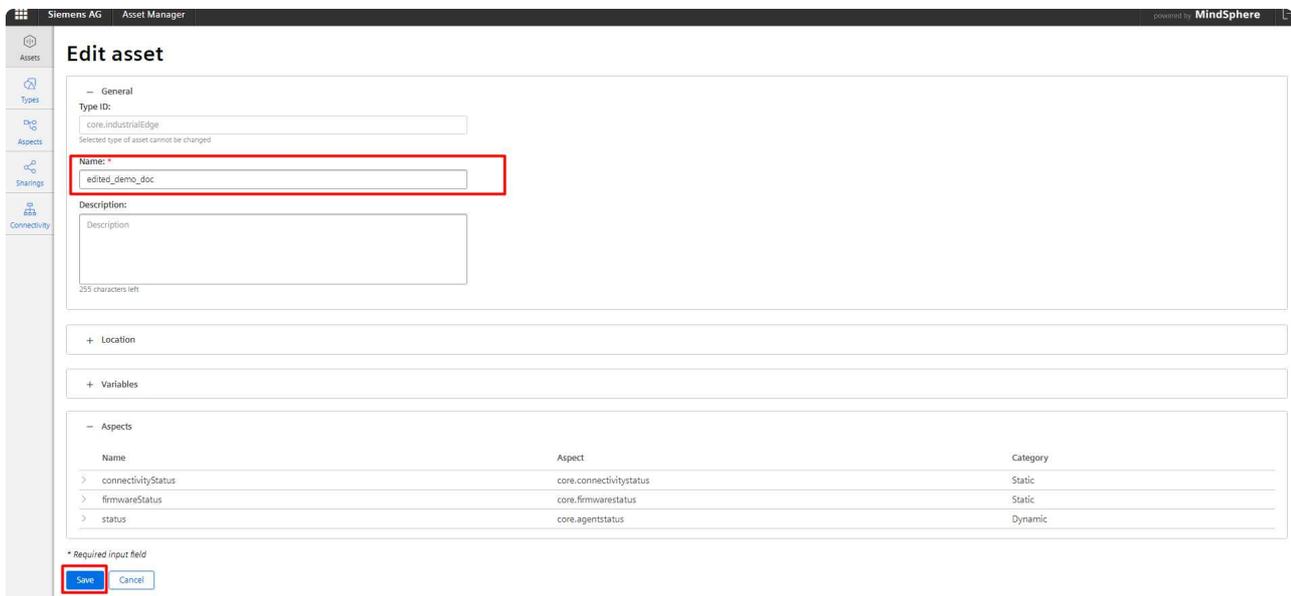


Editing Asset Name

1) To edit asset name, click the pencil icon on *Insights Hub / Asset Manager* application.



2) After this operation, click the **Save** button.



Note After changing asset name, reonboarding operation is not required.

Online Status of an Asset

Once the asset is onboarded, a periodic health status message is broadcast from the asset to Insights Hub. This ensures the network availability between the asset and the backend services. An onboarded asset, therefore, can be either **online** or **offline** according to its health status. Online Status of an Asset can be monitored from the *Manage MySINUMERIK Edge /App Management* application and *Insights Hub / Asset Manager* application.

Online State

An **Onboarded** asset will be **online** as long as the network connection between the asset and Insights Hub is established.

Operations, such as application installation, firmware installation and configurations are permitted only if the asset is **Online**.

1) Manage MySINUMERIK Edge /App Management

An **Online** asset is displayed with a green tick, as demonstrated below:



2) Insights Hub / Asset Manager

An **Online** asset is displayed in new label with a check mark, as demonstrated below:

edge.mcbackend.testautomation.onboarded.asset.01

Overview Configuration Firmware

Device Type: INDUSTRIALEEDGE

Onboarding Status: ✔ Onboarded

Connection Status: ✔ Online

Serial Number: 300420190843

Create and Export Onboarding Key

Offboard

Offline State

An **Onboarded** asset will be **offline** when network connection between the asset and Insights Hub is terminated. All operations are disabled for an **Offline** asset.

1) Manage MySINUMERIK Edge /App Management

An **Offline** asset is displayed with an exclamation mark and a message, as demonstrated below:

App Management Jobs

Demo_Online_Offline_Asset (ONBOARDDED) ! Refresh

Device is Offline

Device is offline, operations are disabled.

App Name	Release Name	Version	Description	Operations
----------	--------------	---------	-------------	------------

2) Insights Hub / Asset Manager

An **Offline** asset is displayed in new label with a cross mark, as demonstrated below:

EDGE.MCBACKEND.070520191053

Overview Configuration Firmware

Device Type: INDUSTRIALEEDGE

Onboarding Status: ✔ Onboarded

Connection Status: ✘ Offline

Serial Number: edgemcbackend070520191053

Create and Export Onboarding Key

Offboard

Unknown State

An **Onboarded** asset will be in **unknown** state when there is no available information about connection status. All operations are disabled for an asset in **Unknown** state.

An asset in **Unknown** state is displayed with a question mark and a message, as demonstrated below:

App Management Firmware Management Jobs

Demo_Online_Offline_Asset (ONBOARDDED) ? Refresh

Device status is unknown

Device connection status is not known, operations are disabled.

App Name	Release Name	Version	Description	Operations
----------	--------------	---------	-------------	------------

Download NCU Package

Click **Download** tab to see NCU package detail information.

Click **Download Icon** to download NCU package.

Note: Only NCU packages which are compatible with the firmware version of the asset are listed.

Note: Please follow the security guidelines for "Data transfer and storage", see platform security.

Overview Hardware Firmware **Download**

NCU Package

Name	Version	Description	Compatible Firmware Versions	
NCU_package	v1.0.0	NCU package 1.0.0	v3.0.0, v3.1.0	

Download Service Stick Package

Click **Download** tab to see Service Stick package detail information.

Click **Download Button** to see multiple Service Stick packages.

Click **Download Icon** to download Service Stick package.

Note: Please download all partitions of the related compressed package then extract to get to the whole package.

Note: Only Service Stick package which is compatible with the firmware version of the asset is listed.

Note: Please follow the security guidelines for "Data transfer and storage", see platform security.

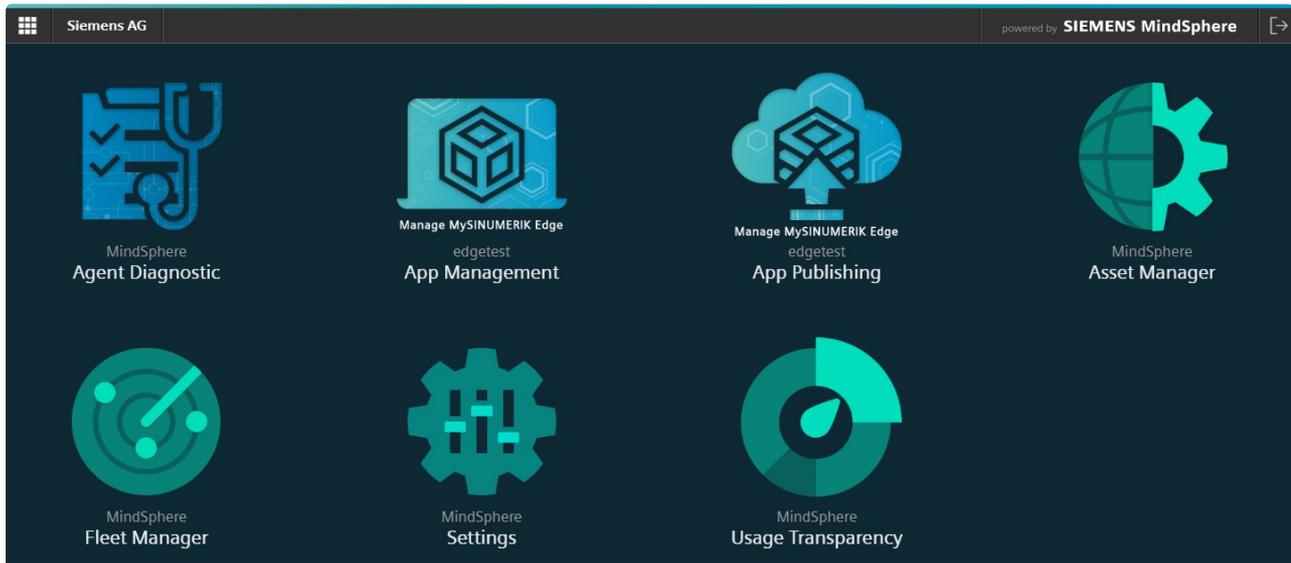
Overview Hardware Firmware **Download**

NCU Package

Name	Version	Description	Compatible Firmware Versions	
Ncu-Package	v3.0.0	NCU Release for v3.0.0	v3.0.0	

Service-Stick Package

Name	Version	Description	Compatible Firmware Versions	
Service-Stick-Package	v3.0.0	Service Stick Release for v3.0.0	v3.0.0	                            



Listing Assets

This feature is used to display the assets that belong to your tenant.

- 1) When the user opens the page, assets are automatically displayed in the asset pane
- 2) The user can search assets by typing keywords in the **Search** text box. Asset names containing the supplied keyword are filtered.



Listing Applications Releases and Application Instances

This feature is used to list the application releases and the application instances.

- 1) Select an Asset
- 2) Select the "App Management" tab
- 3) This section shows the "Application Release and Application Instance Management" table
- 4) This section shows the "Application Release" entry
- 5) Click the Expand/Collapse Icon to display/hide the "Application Instances" that are installed from the "Application Release"

6) This section shows the "Application Instance" entries

The screenshot displays the 'App Management' interface. On the left, a sidebar lists assets from 'Asset 1' to 'Asset 15', with 'Asset 4' selected. The main area shows 'Asset 4 (ONBOARDED)' with a green checkmark and a 'Refresh' button. Below this is a table of applications with columns for 'App Name', 'Release Name', 'Version', 'Description', and 'Operations'. The first application is 'My App' with release 'release-2' (v1.0.12). The second application is 'Performance Measure' with release 'release-1' (v1.2.10). Below the application table, there are two sections for application instances. The first instance is 'Performance Measure.release-1' with a status of 'RUNNING' and a green cloud upload icon. The second instance is 'Error Handler.release-13' with a status of 'RUNNING' and a red cloud upload icon. The third application is 'Some App' with release 'release-9' (v2.4.0). Below it, an instance 'Some App.release-9' is shown with a status of 'STOPPED' and a red cloud upload icon. At the bottom right, there is a 'New Application' button.

Deploying Application to Asset

This feature is used to deploy a release of an application to asset.

- 1) Choose your *Industrial Edge* asset
- 2) Select the "App Management" tab
- 3) Click the **New Application** button
- 4) A new window will be opened where you can select the application and release you want to deploy. Select the application. You can use the search area to find the application.
- 5) When you select the application, release table displays releases of that application with details. Select the "Release Version" you like to deploy to your asset. * Click the **Additional Documents** icon to display the "Additional Documents" list and download the relevant documents, e.g. "Release Notes" etc., from that list
- 6) Click the check-box to accept "Terms and Conditions". The "Terms and Conditions" document should be read before proceeding to the next step. Click the **Accept Terms and Conditions** link to download the document. You can select any of the available languages for the document from the language drop down menu.
- 7) Click the **Save** button to start the deployment job.
- 8) Click the "Jobs" tab and the "Installation" sub tab.
- 9) Here you can find the installation job you have started in the previous step.

App Management

Asset 4 (ONBOARDED) ✓ Refresh

App Name	Release Name	Version	Description	Operations
My App	release-2	v1.0.12	Description for release-2	Install Remove
Performance Measure	release-1	v1.2.10	Description for release-4	Install Remove

Instance Name	Status	Cloud Upload	Operations
Performance Measure.release-1	RUNNING	🟢	⊙ ⚙️ 🗑️

Instance Name	Status	Cloud Upload	Operations
Error Handler.release-13	RUNNING	🔴	🗑️ ⚙️ 🗑️

Instance Name	Status	Cloud Upload	Operations
Some App.release-9	STOPPED	🔴	🗑️ ▶️ 🗑️

New Application

New Application for Asset 4

Search

App 1
App 2
App 3
App 4
App 5
App 6
App 7

Releases for App 3

Release Version	Name	Description
v1.0.12	release-2	Description for release-2
v2.0.12	release-5	Description for release-5
v1.2.10	release-1	Description for release-1
v2.4.0	release-9	Special release for customer A

5.a

Accept Terms and Conditions EN

Cancel Save

App Management

Asset 4 (ONBOARDED) ✓ Refresh

App Installation Removal Configure

Action	Software Type	Software Version	Artifact Name	State	Message	Update Date	Create Date
INSTALL	APP	v742.484	string	ACTIVATED	Activated.	4/2/18, 2:28 PM	4/2/18, 2:28 PM
INSTALL	APP	V00.01.00.00b43	simumerik_edge_dynamic_app_201803301438.swu	FAILED	Initial state on MindSphere is not DOWNLOAD, confusingly aborting update.	4/2/18, 2:16 PM	4/2/18, 10:53 AM
INSTALL	APP	V00.01.00.00b43	simumerik_edge_dynamic_app_201803301438.swu	ACTIVATED	Update installed.	4/2/18, 2:27 PM	4/2/18, 8:59 AM

Installing Application Instance

This feature is used to install the previously deployed application release. Currently, only one application instance can be created from one application release.

1) Select an Asset

2) Select the "App Management" tab

3) Click the **Install** button of a deployed "Application Release" from the list

4) Observe the status from the "Jobs" tab and the "Configure" sub tab.

Known Issues: Currently, there is a synchronization issue between assets and cloud. When an installation is initialized, the Application is instantly created in the cloud but it may take some time to complete the actual installation in the asset. The status of the installation can be monitored from the "Configuration Jobs" section as mentioned.

The screenshot displays the 'App Management' interface. On the left, a search bar is labeled '1'. Below it is a list of assets from 'Asset 1' to 'Asset 15', with 'Asset 4' highlighted in blue. The main area is titled 'App Management' and labeled '2'. It shows 'Asset 4 (ONBOARDED)' with a green checkmark and a 'Refresh' button. Below this is a table of application releases:

App Name	Release Name	Version	Description	Operations
My App	release-2	v1.0.12	Description for release-2	3 Install Remove
Performance Measure	release-1	v1.2.10	Description for release-4	Install Remove

Below the releases table is a table of application instances:

Instance Name	Status	Cloud Upload	Operations	
Performance Measure.release-1	RUNNING	🟢	⚙️ 🗑️	
Error Handler	release-13	v2.0.12	Description for release-5	Install Remove
Error Handler.release-13	RUNNING	🔴	⚙️ 🗑️	
Some App	release-9	v2.4.0	Special release for customer A	Install Remove
Some App.release-9	STOPPED	🔴	⚙️ 🗑️	

At the bottom right, there is a 'New Application' button.

Configuring Application Instance

This feature is used to update the configuration of an application instance.

1) Select an Asset

2) Select "App Management" tab

3) Click "Expand" icon of a deployed "Application Release" from list

4) Click the "Edit App Instance Configuration" icon of the "Application Instance", for which you want to edit configuration

5) This action opens "Configuration Edit" window

6) Click on parameter values to update

7) Use icons to add new configuration parameter or remove existing one.

8) Alternatively, click on drop down and select "code" option to edit the configuration in json/text format.

9) Click **Save** to save the configuration update and deploy the changes to the asset.

10) Observe the status from "Jobs" tab and "Configure" sub tab.

Known Issues: Currently, there is a synchronization issue between assets and cloud. When configuration of an application instance is updated, the update instantly shows effect in Cloud and UIs. Therefore, the updated configuration will be displayed when the "Edit App Instance Configuration" is clicked a second time. However, it takes some time for the configuration to show effect, even the application in the asset may need to be restarted. The real status of the configuration operation in the asset can be monitored from the jobs section as mentioned.

App Management

Jobs

Asset 4 (ONBOARDED) ✓

App Name	Release Name	Version	Description	Operations		
My App	release-2	v1.0.12	Description for release-2	Install Remove		
Performance Measure	release-1	v1.2.10	Description for release-4	Install Remove		
Instance Name				Status	Cloud Upload	Operations
Performance Measure.release-1				RUNNING	●	⊞ ⚙
Error Handler	release-13	v2.0.12	Description for release-5	Install Remove		
Instance Name				Status	Cloud Upload	Operations
Error Handler.release-13				RUNNING	●	⊞ ⚙
Some App	release-9	v2.4.0	Special release for customer A	Install Remove		
Instance Name				Status	Cloud Upload	Operations
Some App.release-9				STOPPED	●	⊞ ⚙ ▶

New Application

Config Edit

Asset 4 (ONBOARDED)

Tree View

object (2)

- specificConfig (1)
 - param param
 - loggingConfig
 - append journal
 - severity debug

Cancel Save

Warning

If the value which is edited is in string format, different steps need to be applied in "Configuration Edit" window not to encounter parsing problems on SINUMERIK Edge side

- Option-1: using Tree view

Config Edit

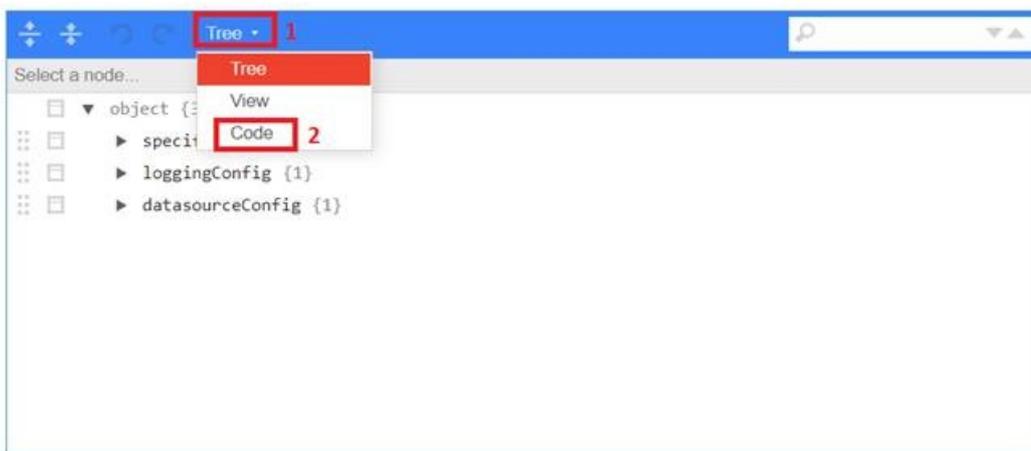


Cancel

Save

- Option-2: using Code view

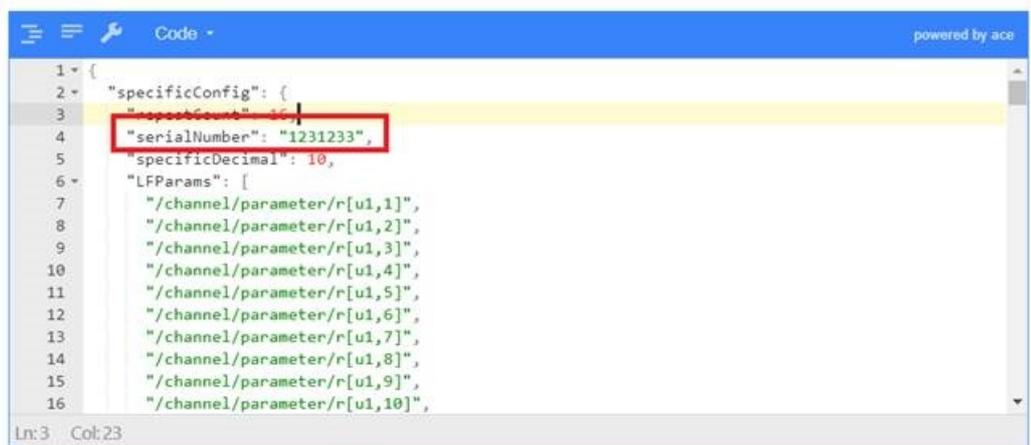
Config Edit



Cancel

Save

Config Edit



Cancel

Save

Start/Stop Application Instance

This feature is used to start/stop application instances.

- 1) Select an Asset
- 2) Select the "App Management" tab
- 3) Click the "Expand" icon of a deployed "Application Release" from the list
- 4) Start or Stop the selected "Application Instance": * To start an "Application Instance", click the **Start** icon for an application which has "STOPPED" status * To stop an "Application Instance", click the **Stop** icon for an application which has "RUNNING" status
- 5) Observe the status from the "Jobs" tab and the "Configure" sub tab.

Known Issues: Currently, there is a synchronization issue between assets and cloud. When an application instance is started or stopped, the cloud and UI's are instantly updated and display the new status of the "Application Instance". However, it takes some time for the asset to actually start or stop applications. The real status of this operation in the asset can be monitored from the jobs section as mentioned.

The screenshot displays the 'App Management' interface. On the left, a search bar is labeled '1'. Below it is a list of assets from 'Asset 1' to 'Asset 15', with 'Asset 4' selected. The main area shows the 'App Management' tab labeled '2'. It features a table of application releases. The first release, 'My App', has a status of 'RUNNING' and is annotated with '3' pointing to its expand icon. Below this, a detailed view of an instance shows its status as 'RUNNING', with '4' pointing to the status field. The second release, 'Performance Measure', has a status of 'STOPPED' and is annotated with '4.a' pointing to its status field. The 'Jobs' tab is labeled '5'.

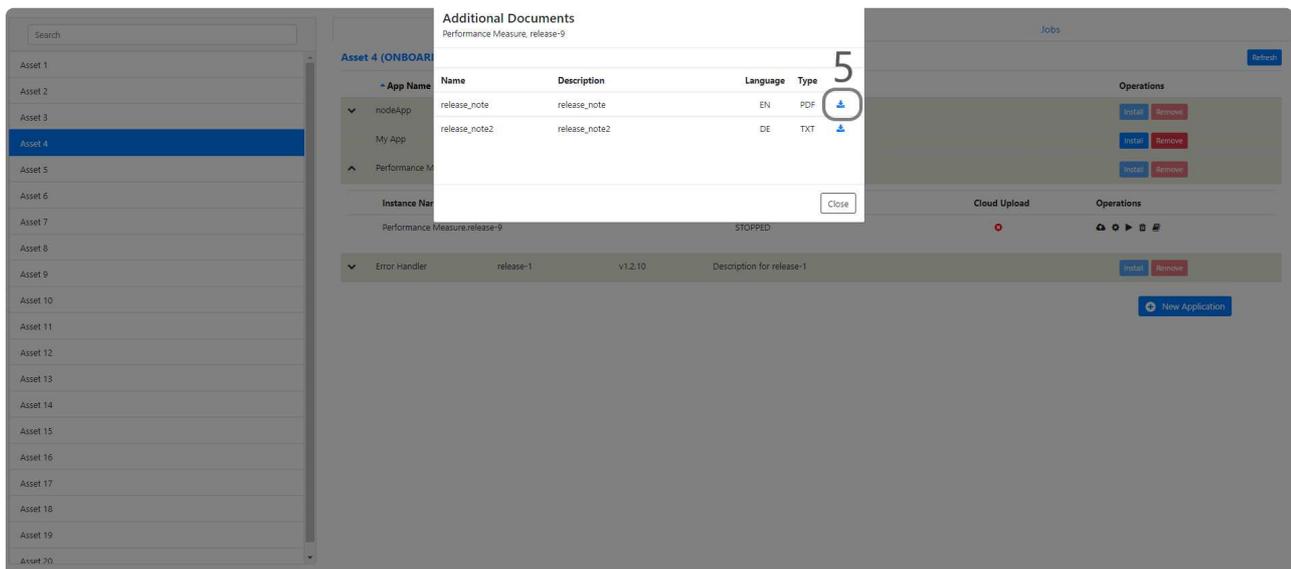
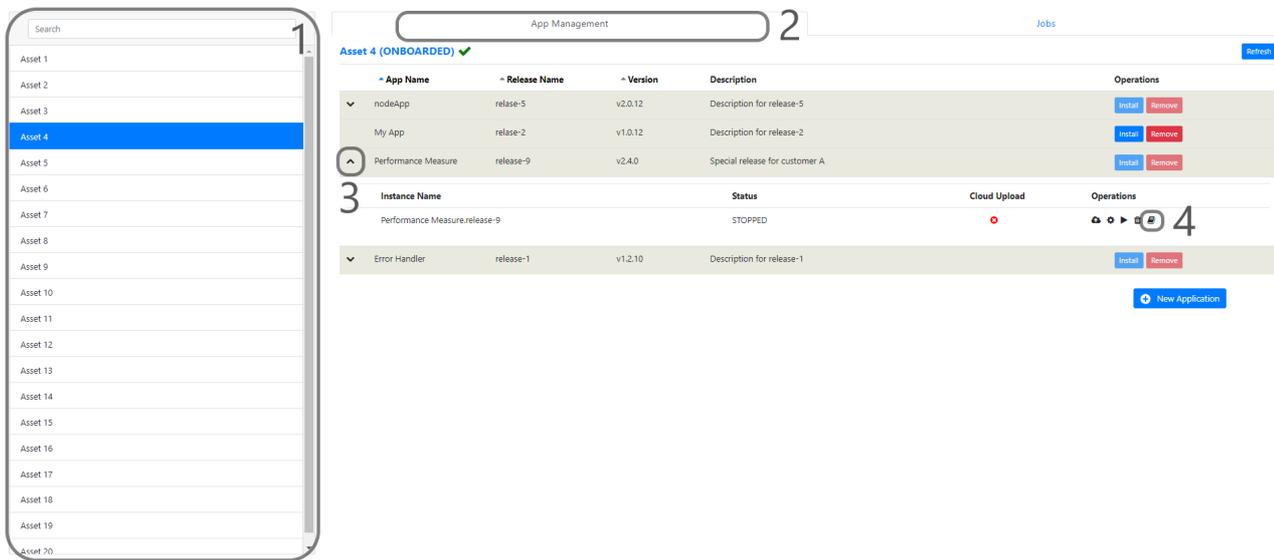
App Name	Release Name	Version	Description	Operations
My App	release-2	v1.0.12	Description for release-2	Install Remove
Performance Measure	release-1	v1.2.10	Description for release-4	Install Remove
Error Handler	release-13	v2.0.12	Description for release-5	Install Remove
Some App	release-9	v2.4.0	Special release for customer A	Install Remove

Instance Name	Status	Cloud Upload	Operations
Performance Measure.release-1	RUNNING	Green dot	Start/Stop icons
Error Handler.release-13	RUNNING	Red dot	Start/Stop icons
Some App.release-9	STOPPED	Red dot	Start/Stop icons

Download Additional Documents

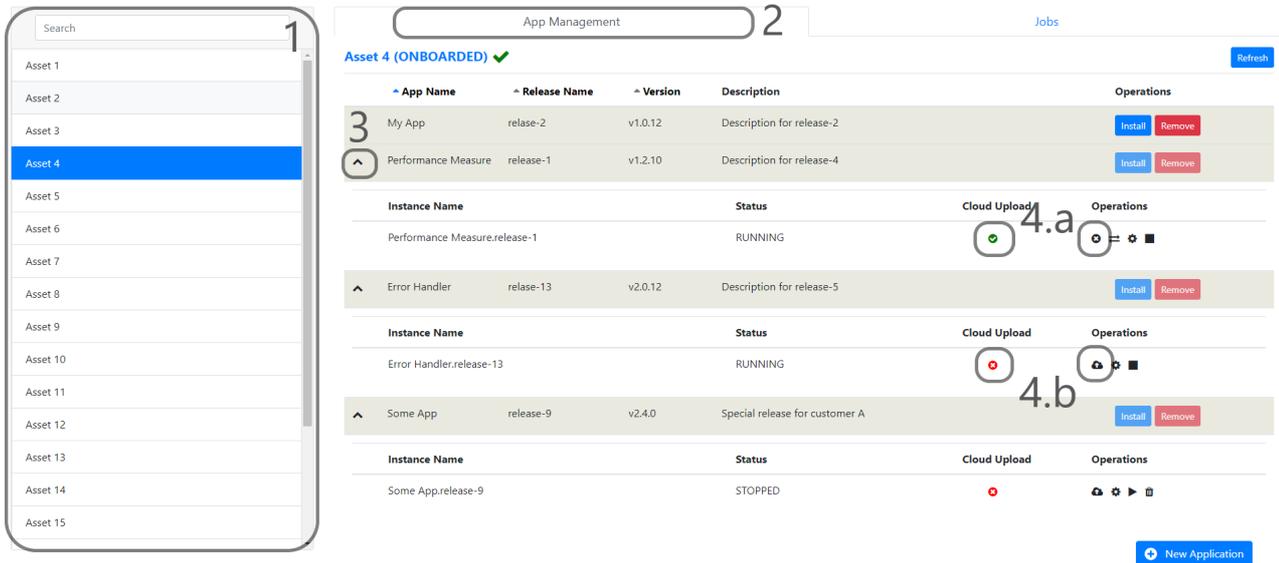
This feature is used to view/download additional documents, e.g. "Release Notes" etc.

- 1) Select an Asset
- 2) Select the "App Management" tab
- 3) Click the "Expand" icon of a deployed "Application Release" from the list
- 4) Click the **Additional Documents** icon to display the "Additional Documents" window
- 5) Click the **Download** icon to download the available documents.



Enabling/Disabling Cloud Upload

- 1) Select an Asset
- 2) Select the "App Management" tab
- 3) Click the "Expand" icon of a deployed "Application Release" from the list
- 4) Enable or Disable the **Cloud Upload** feature of the "Application Instances": * To disable the cloud upload feature, click the **Disable Upload Cloud** icon for an application which has "Cloud Upload: Enabled" status * To enable cloud upload feature, click the **Enable Upload Cloud** icon for an application which has "Cloud Upload: Disabled" status
- 5) Observe the status from the "Jobs" tab and the "Configure" sub tab.



Data Mapping

- 1) Select an Asset
- 2) Select the "App Management" tab
- 3) Click the "Expand" icon of a deployed "Application Release" from the list
- 4) This section displays the "Application Instance" list
- 5) Click the **Data Mapping** icon to display the "Data Mapping" List

In order to add a new Mapping:

- 6) Search source param and SINUMERIK UID by typing keywords in the **Search** box
- 7) Click the **Pick** button of the (source) parameter for which you want to define a new mapping
- 8) From the "Data Owner" asset list, select a data owner asset. The source parameter value will be sent to that asset
- 9) Select one of the aspect types from the the **Aspect Type** drop down. The source parameter's value will be sent to that aspect type of the previously selected asset.
- 10) Search variable by typing keywords in the **Search** box
- 11) Select one of the parameters (as destination) by clicking the **Select** button.
- 12) The source parameter value is now mapped to the selected destination parameter.

App Management Jobs

Asset 4 (ONBOARDED) Refresh

App Name	Release Name	Version	Description	Operations
My App	release-2	v1.0.12	Description for release-2	Install Remove
Performance Measure	release-1	v1.2.10	Description for release-4	Install Remove

Instance Name	Status	Cloud Upload	Operations
Performance Measure.release-1	RUNNING	✓	⊞ ⊞ ⊞ ⊞

App Name	Release Name	Version	Description	Operations
Error Handler	release-13	v2.0.12	Description for release-5	Install Remove

Instance Name	Status	Cloud Upload	Operations
Error Handler.release-13	RUNNING	✗	⊞ ⊞ ⊞ ⊞

App Name	Release Name	Version	Description	Operations
Some App	release-9	v2.4.0	Special release for customer A	Install Remove

Instance Name	Status	Cloud Upload	Operations
Some App.release-9	STOPPED	✗	⊞ ⊞ ⊞ ⊞

➕ New Application

Siemens AG Manage MySINUMERIK Ed... powered by MindSphere

Data Mapping
Source: filterappdatasource3

Search by Source Param or Sinumerik UID

Source Param	Description	Unit	Type	SinumerikUid	
ENC1_POS_1	ENC1_POS_1	%	DOUBLE	ENC1_POS1	Pick

Asset	Aspect	Variable	
DataOwner_EdgeBox21	systemtestaspect_allDatPoints	ENC1POS1	⊞

ENC1_POS_2	ENC1_POS_2	%	DOUBLE	ENC1_POS2	Pick
ENC1_POS_3	ENC1_POS_3	%	DOUBLE	ENC1_POS3	Pick

Close

Siemens AG Manage MySINUMERIK Ed... powered by MindSphere

Data Mapping
Source: filterappdatasource3 -> ENC1_POS_1 (DOUBLE, %)

Search

Position

Search by variable

Variable	Unit	Data Type	
ENC1POS1	%	DOUBLE	Select
ENC1POS2	%	DOUBLE	Select
ENC1POS3	%	DOUBLE	Select

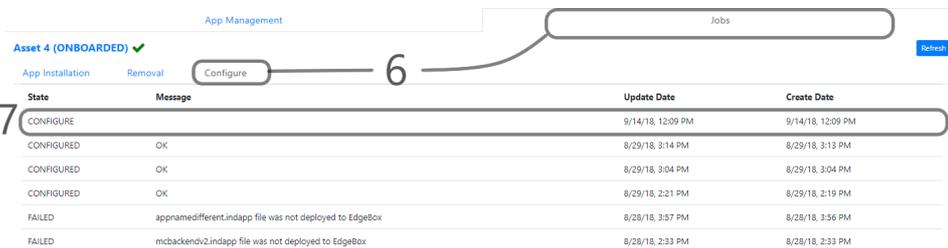
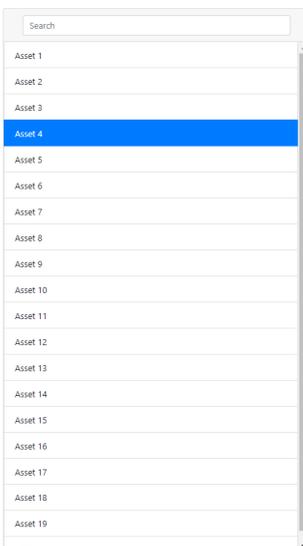
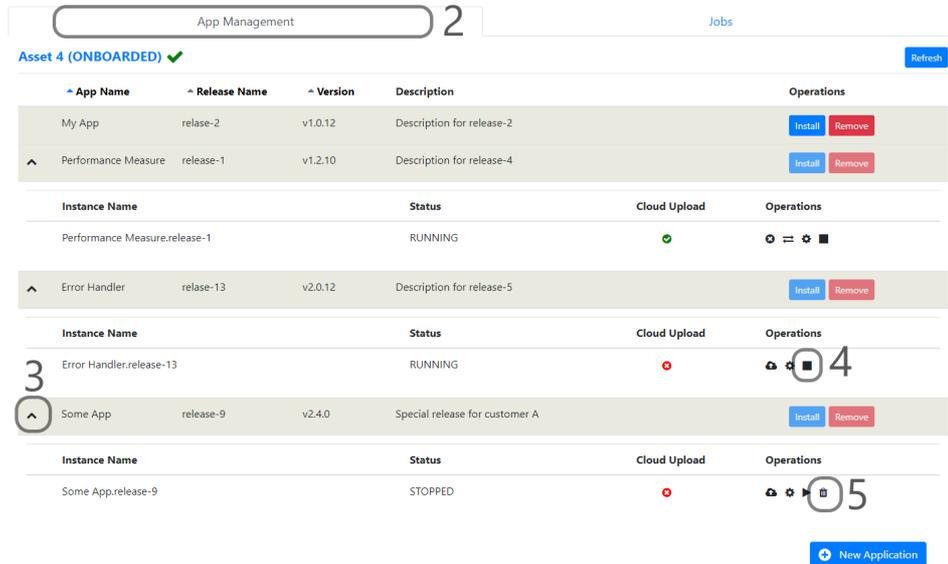
Close

Removing Application Instance

- 1) Select an Asset
- 2) Select the "App Management" tab
- 3) Click the "Expand" icon of a deployed "Application Release" from the list
- 4) If the Application Instance's status is not "Stopped", first click the **Stop** button to stop it and make the **Remove App Instance** icon visible.
- 5) Click the **Remove App Instance** icon to remove the application.
- 6) Click the "Jobs" tab and the "Configure" sub tab.
- 7) Observe the status from the list

Warning

Please **disable** cloud upload feature of an application before **uninstalling**.



1) Select an Asset

2) Select the "App Management" tab

3) Click the **Remove** button of an "Application Release" which you want to remove. Note that there must be no application instance created to remove applications. If so, just follow the *Removing Application Instance* section first.

4) Click the "Jobs" tab and the "Removal" sub tab.

5) Observe the status from the list

App Management

Jobs

Asset 4 (ONBOARDED) ✓ Refresh

App Name	Release Name	Version	Description	Operations
My App	release-2	v1.0.12	Description for release-2	Install Remove
Performance Measure	release-1	v1.2.10	Description for release-4	Install Remove

Instance Name	Status	Cloud Upload	Operations
Performance Measure.release-1	RUNNING	✓	⊞ ⚙️ 🗑️

App Name	Release Name	Version	Description	Operations
Error Handler	release-13	v2.0.12	Description for release-5	Install Remove

Instance Name	Status	Cloud Upload	Operations
Error Handler.release-13	RUNNING	✗	⊞ ⚙️ 🗑️

App Name	Release Name	Version	Description	Operations
Some App	release-9	v2.4.0	Special release for customer A	Install Remove

Instance Name	Status	Cloud Upload	Operations
Some App.release-9	STOPPED	✗	⊞ ⚙️ ▶️ 🗑️

New Application

App Management

Jobs

Asset 4 (ONBOARDED) ✓ Refresh

App Installation Removal Configure

State	Message	Update Date	Create Date
REMOVED	OK	8/13/18, 4:01 PM	8/13/18, 4:00 PM
REMOVED	OK	8/13/18, 9:20 AM	8/13/18, 9:19 AM
REMOVED	OK	8/7/18, 1:53 PM	8/7/18, 1:53 PM
REMOVED	OK	7/24/18, 11:36 AM	7/24/18, 11:35 AM
REMOVED	OK	7/24/18, 11:35 AM	7/24/18, 11:34 AM
REMOVED	OK	7/24/18, 11:31 AM	7/24/18, 11:31 AM
REMOVED	App (b30d18df-6ea5-48db-b995-1938774c274 - cba8832e-95e0-4017-8b29-4f99707a0b0f) is not installed OK	7/24/18, 11:30 AM	7/24/18, 11:30 AM
REMOVED	OK	7/20/18, 10:20 AM	7/20/18, 10:19 AM
REMOVED	OK	7/20/18, 8:51 AM	7/20/18, 8:51 AM

Application Instance Configuration Integrity

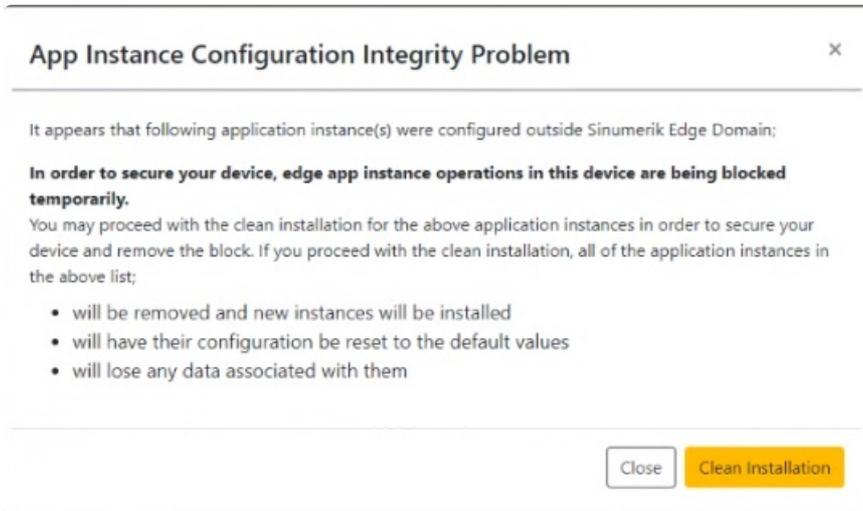
Manage MySINUMERIK Edge /App Management is the only authorized way of managing application instances in your device. Other use cases, such as using Insights Hub API's, will by-pass some major validations in the SINUMERIK Edge back-end services which may eventually lead to security vulnerabilities or integrity issues caused by misconfigurations.

If any of the application instances in a device are configured without using Manage MySINUMERIK Edge /App Management, SINUMERIK Edge backend services will not reflect those changes to your device and blocks your device for further configurations temporarily; you will be notified via an Integrity Problem pop-up. The application instance(s), whose configuration(s) are not accepted, are also listed in the pop-up.

In order to remove the block of your device, you may either;

- Click the "Clean Installation" button in the warning pop-up, which will remove and re-install the application instance(s) listed in the pop-up.
- Manually delete and re-install the application instance(s) listed in the pop-up

Please be aware that both of those operations will remove the app instance(s) and create new one(s); which will cause loss of any data/configuration that is associated with the removed app instance(s).



Trial Application Management

This feature provides managing applications with trial license.

Note: Trial license must be given to your tenant by operator. For detail information, you should communicate with your local sales representative.

1) After deploying trial application listing App Management list and license status shown like:

- display active trial status with tick mark.
- display expired trial status with exclamation mark.

2) Display a tooltip which given status and expiration date information when hovering mouse tick or exclamation marks.

3) Click 'App License Management' button to open license management pop up to manage trial application.

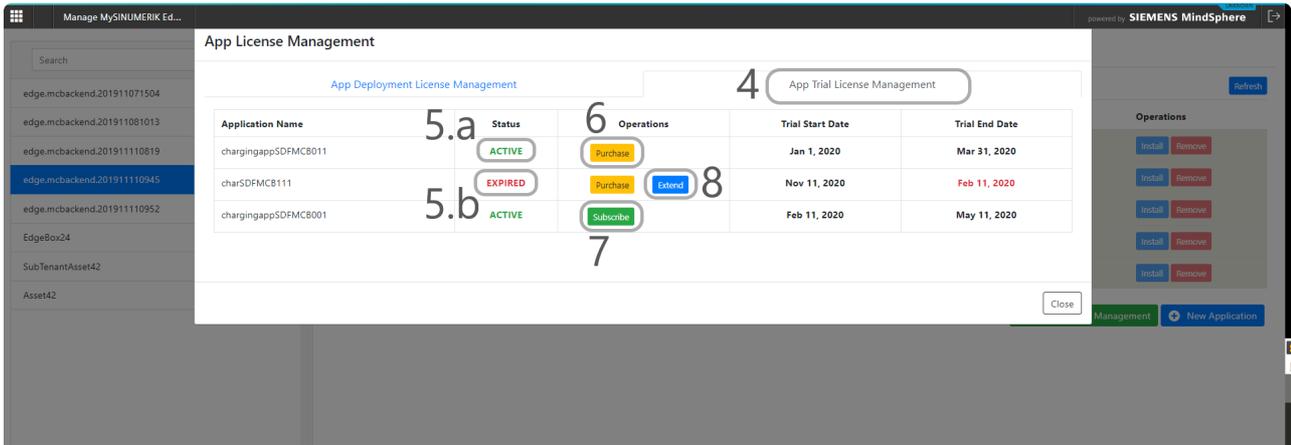
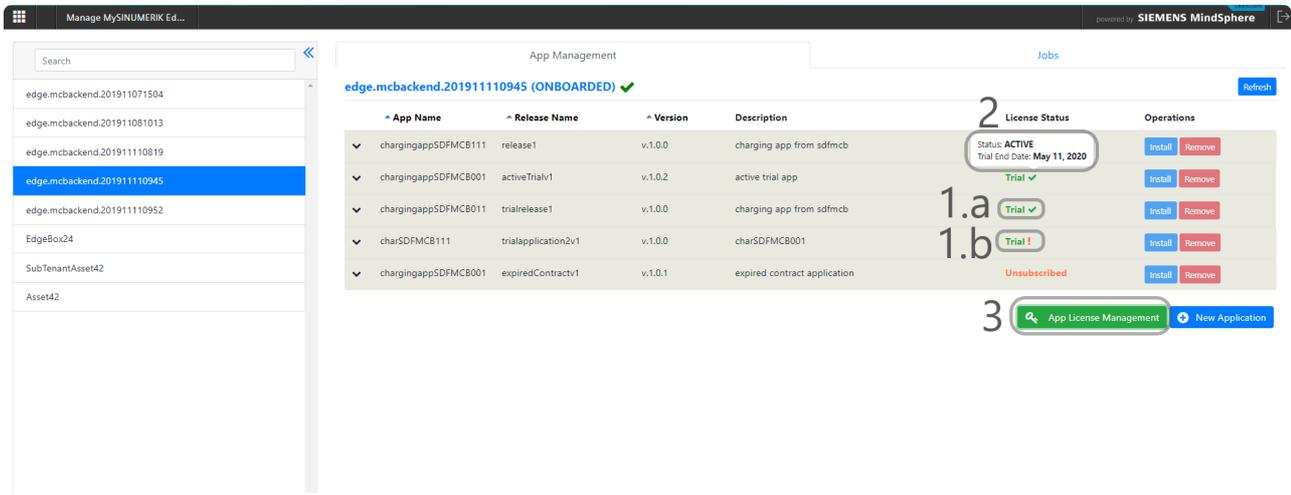
4) Select 'App Trial License Management' tab to list the applications with trial license.

5) Display trial application status * display 'ACTIVE' status, trial application can be used as a normal application end of the expiration date. * display 'EXPIRED' status, trial application cannot be used.

6) Click 'Purchase' button to purchase trial application which does not have any contract, confirmation pop up is shown.

7) Click 'Subscribe' button to subscribe trial application which has expired contract, confirmation pop up is shown.

8) Click 'Extend' button, trial license period can be extended if available license is given by the operator, if not contact your local sales representative.

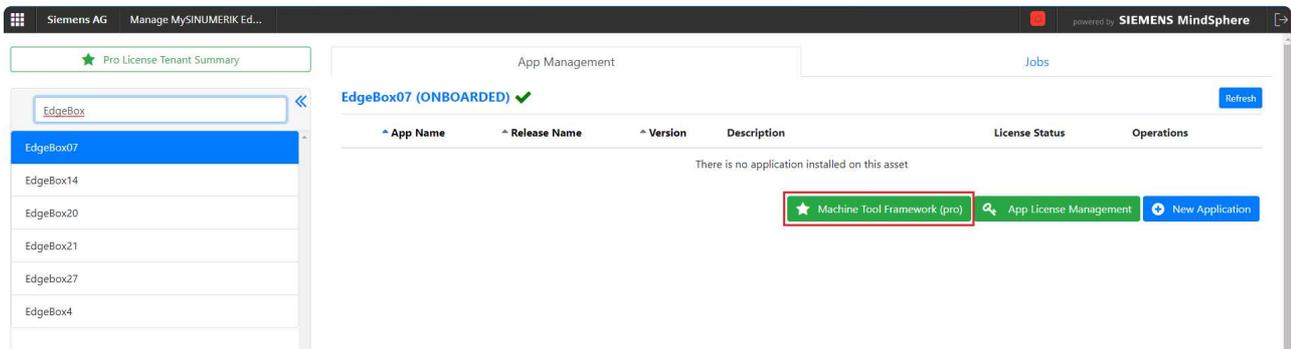


Machine Tool Framework License Management

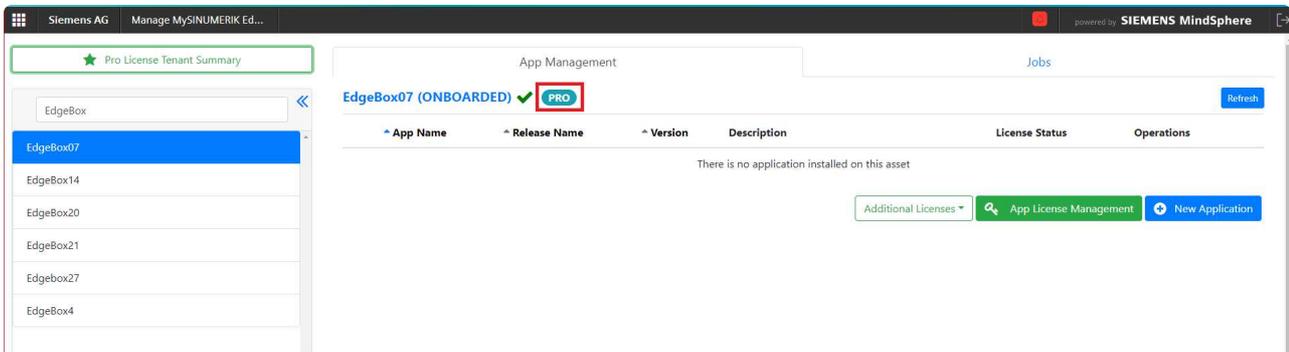
Using Machine Tool Framework Licenses

You can use the pro license, if you need, you can also use an additional license. Please refer to [New Asset License Model: Machine Tool Framework](#) chapter for further details of pro and additional licenses.

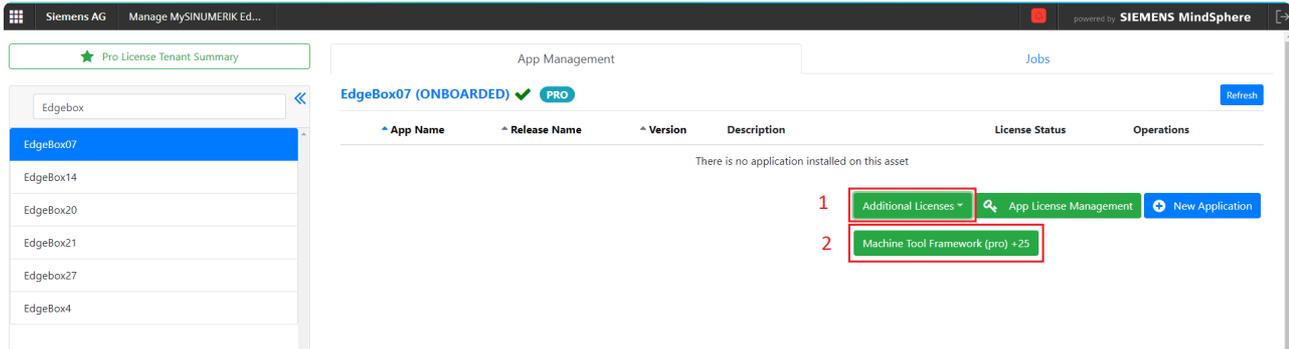
In order to assign Machine Tool Framework License to an asset, select an asset and then click Machine Tool Framework (pro) License button.



Once the license is assigned, the "Pro" badge will appear near the asset name.



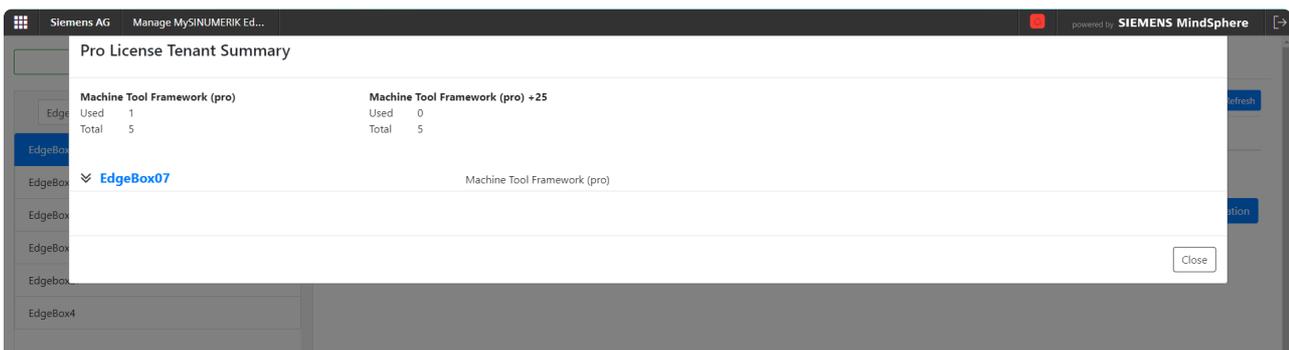
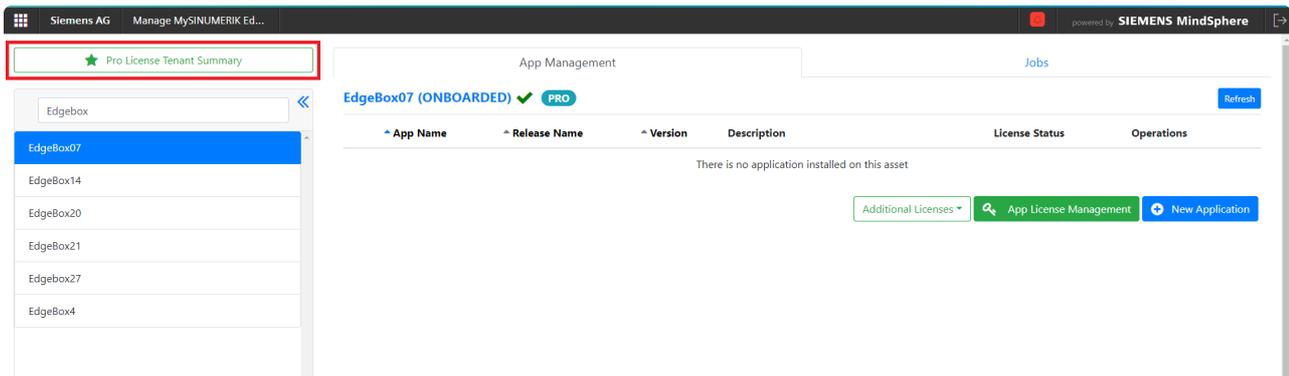
If you wish to assign additional licences to your asset, you may click **Additional Licenses** button and select **Machine Tool Framework (pro) +25**.



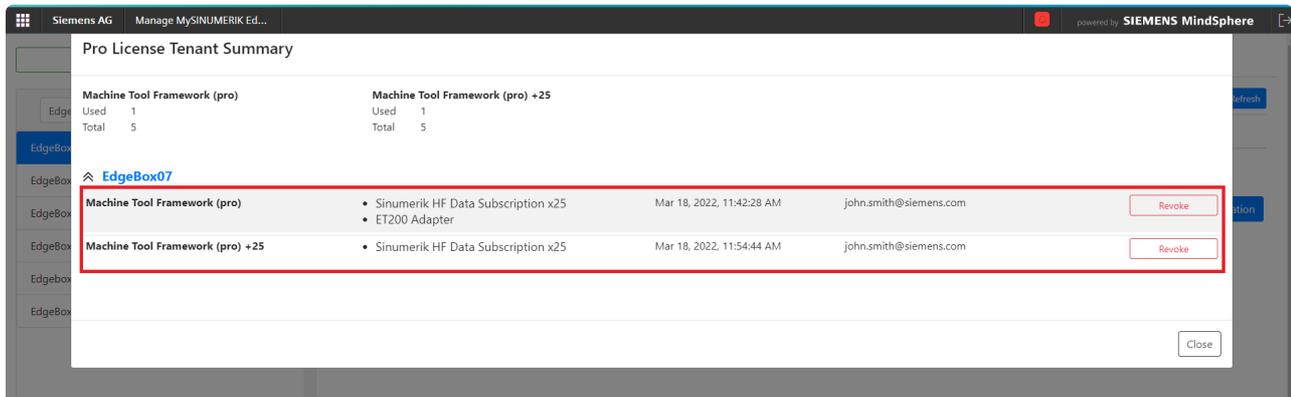
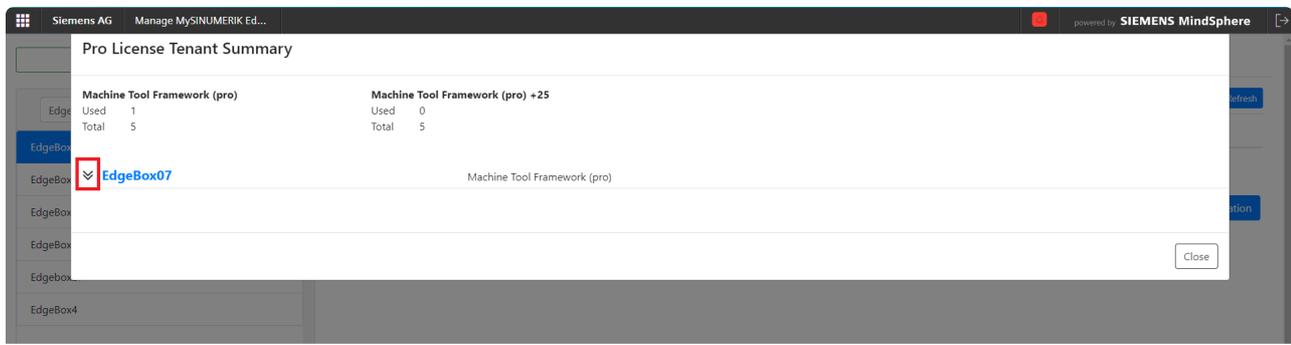
Machine Tool Framework License Tenant Summary

By clicking **Pro License Tenant Summary** button, you can track

- Total number of licenses you have in your tenant
- Total number of licenses assigned to assets
- Assets having license(s)



You may display further details about assets' assigned licenses by clicking the expand button



Revoking Machine Tool Framework Licenses

If you want to revoke a license from an asset, you can do so from Pro License Tenant Summary. Click **Revoke** button to revoke Machine Tool Framework (pro) or additional licences.

Important Note: 'Machine Tool Framework (pro) +25' needs to be revoked first in order to revoke 'Machine Tool Framework (pro)' License.

Warning

You can not revoke licenses if an asset is removed, please contact your technical support for further details

Pro License Tenant Summary

Machine Tool Framework (pro)	Machine Tool Framework (pro) +25
Used 1	Used 1
Total 5	Total 5

Warning You can not revoke licenses if an asset is removed, please contact your technical support for further details

EdgeBox07

Machine Tool Framework (pro)	<ul style="list-style-type: none"> Sinumerik HF Data Subscription x25 ET200 Adapter 	Mar 22, 2022, 12:03:53 PM	john.smith@siemens.com	Revoke
Machine Tool Framework (pro) +25	<ul style="list-style-type: none"> Sinumerik HF Data Subscription x25 	Mar 22, 2022, 12:06:12 PM	john.smith@siemens.com	Revoke

Firmware Management with Asset Manager Industrial Edge Plugin

The Industrial Edge provides a power fail-safe update over the air mechanism for the management of the overall firmware.

Note: The firmware update forces a reboot of the Industrial Edge to activate it. The download may take some time depending on the bandwidth. During this time the Industrial Edge still operates as usual.

Note: Firmware version updates may cause compatibility issues between firmware and previously installed edge applications. You should uninstall/remove every edge application (also system applications like adapterframework) from the box before proceeding with a firmware update in order to avoid compatibility issues.

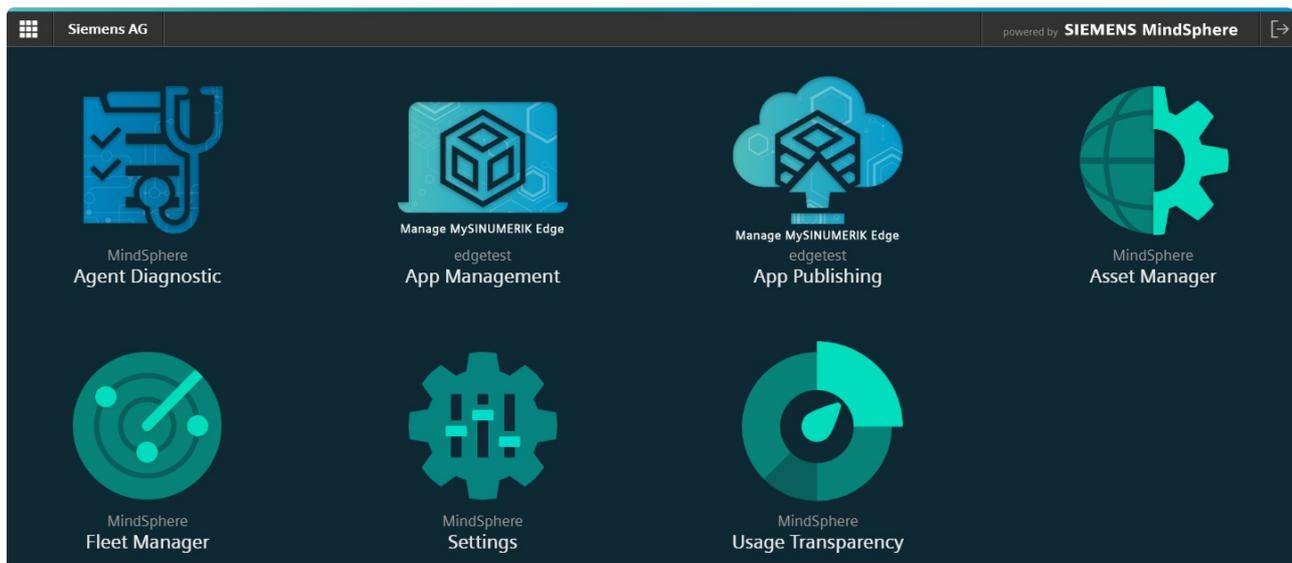
Once the firmware update is completed, you can install the latest edge applications that are compatible with your firmware by using Manage MySINUMERIK Edge /App Management.

Choose the *Asset Manager* from the Insights Hub Launchpad and click on "Industrial Edge"

- 1) Select the "Firmware" tab
- 2) Display the device's current firmware information. The **Current Firmware** and **Current Version** are displayed.
- 3) A message box is shown displaying the available firmware version(s) for **Latest Hotfix**, **Latest Minor Release** and **Latest Release** based on the device's current firmware information.
- 4) When the page is loaded, firmware releases are listed with the release version, name, description, additional documents and the end of support date. Search firmware releases by typing keywords in the **Search Firmware** box. You can search the release version, name and description.

In order to install a new firmware release:

- 5) Click a release which will be installed on the device from the firmware release list.
- 6) Select the "Terms and Conditions" language from dropdown list. Click the **Accept Terms and Conditions** link to read terms and conditions in the selected language. Click the checkbox to accept terms and conditions.
- 7) After accepting terms and conditions, the **Install** button will be enabled. Click the **Install** button to install the firmware release on SINUMERIK Edge.
- 8) You can follow the installation status from the "Firmware Installation Jobs" button.



Overview Hardware **Firmware** 1

Current Firmware: **Industrial Edge IPC 200E Firmware** 2
 Current Version: **v5.4.1**

New Firmware Version(s) available 3
 Latest Hotfix: v5.4.6
 Latest Minor Release: v5.5.0
 Latest Release: v6.0.4

Search Firmware Release 8 **Firmware Installation Jobs**

Release	Name	Description	End Of Support
v6.0.4	indegree.ipc200E_prod_release_v6.0.4	indegree.ipc200E_prod_release_v6.0.4	Apr 10, 2027
v6.0.2	indegree.ipc200E_prod_release_v6.0.2	indegree.ipc200E_prod_release_v6.0.2	Apr 10, 2027
v5.5.0	indegree.ipc200E_prod_release_v5.5.0	indegree.ipc200E_prod_release_v5.5.0	Apr 3, 2026
v5.4.6	indegree.ipc200E_prod_release_v5.4.6	indegree.ipc200E_prod_release_v5.4.6	Apr 23, 2023
v5.4.1	indegree.ipc200E_prod_release_v5.4.1	indegree.ipc200E_prod_release_v5.4.1	Apr 14, 2024

23 Pages / 113 Firmwares Firmwares Per Page: 5

6 Accept Terms and Conditions EN 7

Fw Installation Jobs for demo_doc

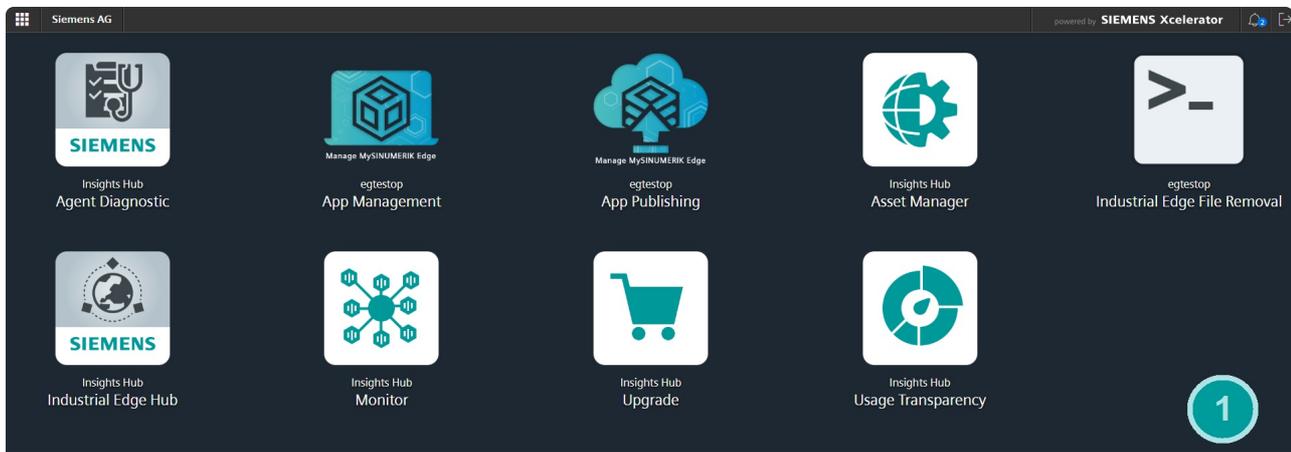
Software Version	Artifact Name	State	Message	Update Date	Create Date
v0.2	indegree.ipc200E_dev_v2.0.0-27.swu	ACTIVATED	Update Installed.	5/22/19, 3:55 PM	5/22/19, 3:40 PM
V.01	indegree.ipc200E_dev_CUSTOMBYEDGEINTEGRATION_v2.0.0-25-20190407191133.swu	FAILED	State is not DOWNLOAD, confusingly aborting update.	5/22/19, 3:39 PM	5/22/19, 3:30 PM
V.01	indegree.ipc200E_dev_CUSTOMBYEDGEINTEGRATION_v2.0.0-29-20190408112503.swu	FAILED	Error processing update chunk, aborting.	5/22/19, 3:27 PM	5/22/19, 2:37 PM

Download Log Files From Monitor

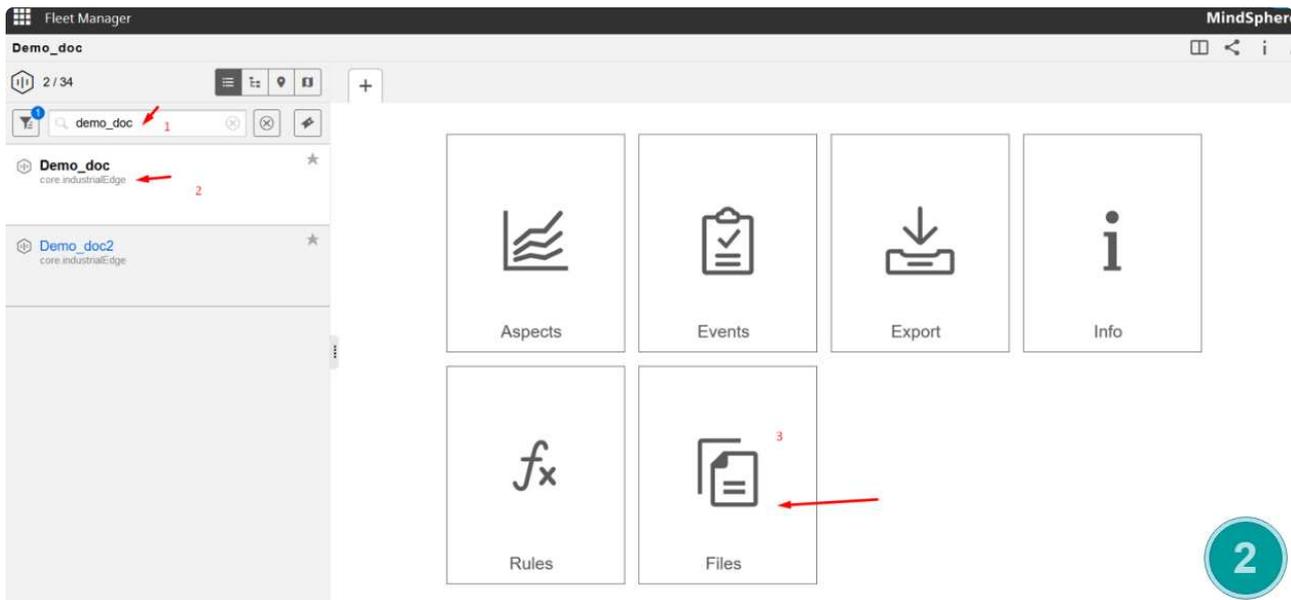
Log Files include journal logs of components and applications in the SINUMERIK Edge. To show components and applications logs to users, these files are sent to Insights Hub. So that the app developer can use these application or system logs for further analyzes.

1) Login to the Insights Hub with your credentials. Then from the Insights Hub Launchpad choose *Monitor*.

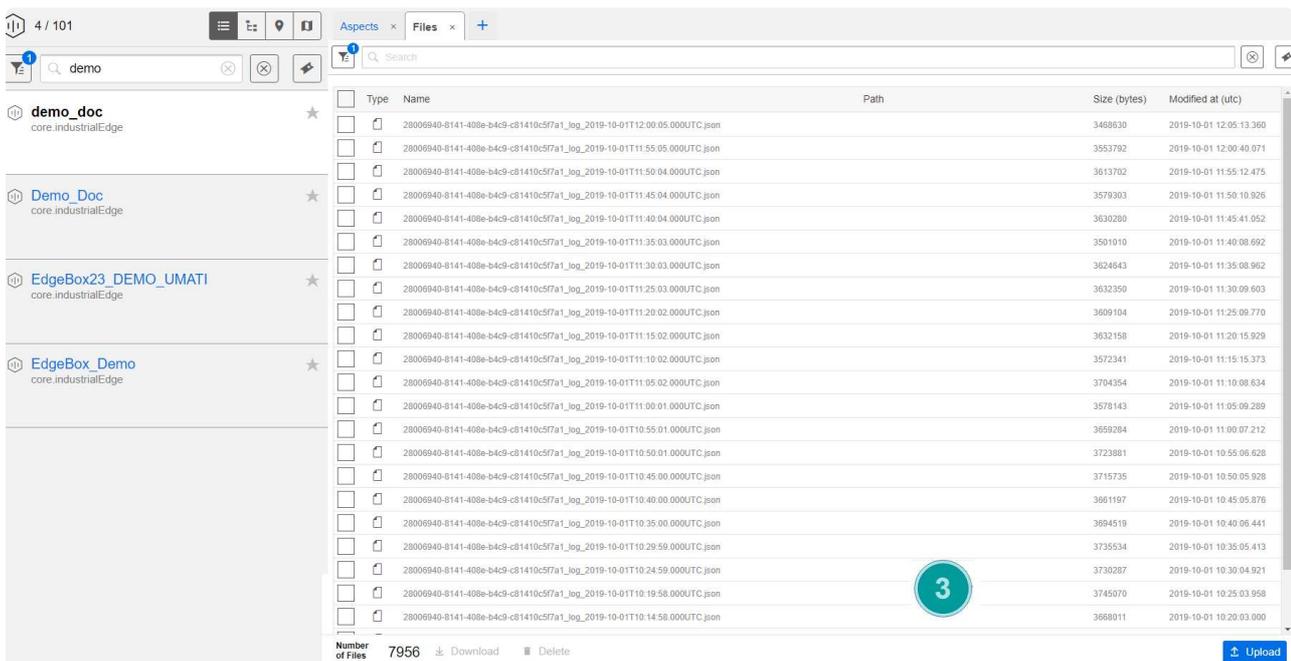
Note: As a prerequisite, an agent asset (Industrial Edge) should be created from the *Asset Manager* and the asset status should be onboarded.



2) Find your asset through the search box and click it, then select the Files.



3) All log files which are uploaded to the Insights Hub should be listed in this section. Search, filter, download, delete operations are possible through this pane.



SINUMERIK Edge applications can be published to Insights Hub using **Manage MySINUMERIK Edge /App Publishing** UI. More information regarding usage and step by step tutorial can be found in Developers manual.

Install System Applications

After onboarding a new SINUMERIK EDGE you will need to install System applications to enable common SINUMERIK EDGE platform functionality.

Installation of AdapterFramework Application

The AdapterFramework is a system component of SINUMERIK EDGE that enables communication between applications and datasources. A datasource is a logical object which can be a real hardware device – like a SINUMERIK NCU – or an internal dataset of an application.

Select the application "*adapterframework*" with the released version related to the firmware version installed on your SINUMERIK EDGE to install it on your connected SINUMERIK EDGE device.

Please refer to chapter [Application Management](#) for detailed information how to install an application on your SINUMERIK EDGE device.

Any additional configuration over Insights Hub backend is not necessary for this application.

Security information

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

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

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

For additional information on industrial security measures that may be implemented, please visit <https://www.siemens.com/industrialsecurity>.

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

To stay informed about product updates, subscribe to the Siemens Industrial Security RSS Feed under <https://www.siemens.com/cert>.

Enable access to a SINUMERIK controller

Variants of SinumerikAdapter applications and supported devices

hardware setup	application setup	supported features	supported devices
SINUMERIK Solutionline & SINUMERIK ONE / Ethernet connection	SinumerikAdapter-Edge-Vxx & SinumerikAddOn4Edge_xxx	full functionality	SINUMERIK ONE 1740/1750/1760 (all GIV versions) ; 840D SL (GIV 4.5 SP4; GIV 4.7 and newer)
SINUMERIK Solutionline & SINUMERIK ONE / Ethernet connection	SinumerikAdapter-Edge-Vxx	without high frequency data collection	SINUMERIK ONE 1740/1750/1760 (all GIV versions) ; 840D SL (GIV 4.5 SP4; GIV 4.6 * ; GIV 4.7 and newer)
SINUMERIK Powerline / MPI connection	SinumerikAdapterPowerLine-Edge-Vxx	without high frequency data collection	840 PL (GIV 7.4.36) **

* GIV 4.6: does not support high frequency data collection. Do not install SinumerikAddOn4Edge package!

** tested with IE/PB LINK PN IO MLFB: 6GK1411-5AB10

Most likely functioning (but not part of the test)

- 840 PL newer than GIV 7.4.36

Attention

The support of Powerline controllers is not available in general. To get this feature unlocked, please contact the SIEMENS support and clarify the compatibility to your specific setup and additional hardware requirements.

Installation of the SinumerikAdapter application

The SinumerikAdapter is an application used to connect the SINUMERIK EDGE to a SINUMERIK machine and provide data and service connectivity to SINUMERIK EDGE applications.

Select the application "*sinumerikadapte*" with the released version related to the firmware version installed on your SINUMERIK EDGE to install it on your connected SINUMERIK EDGE device.

Hint

If you have unlocked the Powerline connectivity feature, you have to choose the correct variant of the SINUMERIK Adapter application (Please review the [Variants](#) section).

Please refer to chapter [Application Management](#) for detailed information how to install an application on your SINUMERIK EDGE device.

For detailed description how to configure SinumerikAdapter please refer to the chapter below.

Preconditions

- To use the SinumerikAdapter, the system application "adapterframework" must be installed.
- To use the SinumerikAdapter's custom alarm texts feature, the system application "sambaserver" must be installed.
- If high frequency data is required, the SinumerikAddOn4Edge package must be installed on the SINUMERIK controller.
- To use high frequency data, the license "*Machine Tool Framework (pro)*" is required.
- The SINUMERIK license "SINUMERIK Operate /NCU" (6FC5800-0AS00-0YB0) is needed to run SINUMERIK.
- The SINUMERIK license "Run MyHMI /3GL" (6FC5800-0AP60-0YB0) is needed to run SINUMERIK Edge.

Remarks & Version Restrictions

- **Restriction:** Currently SinumerikAdapter only supports the connection to a single NCU. Multi-NCU scenarios are not supported.
- **Remark:** In case SinumerikAdapter does not deliver data while using a NCU serial number with leading zeros, please review the Troubleshooting section.
- **Restriction:** Only English language is supported for alarm texts.

Installation on SINUMERIK controller

If high frequency data is required, there must be an add-on installation on the SINUMERIK controller. To download this package, [please follow this instructions](#).

For detailed information how to prepare the SINUMERIK controller for gathering data via SINUMERIK EDGE, please refer to the SinumerikEdgeHFDataCommissioning manual delivered with the SinumerikAddOn4Edge package matching the version of the corresponding SinumerikAdapter.

Configuration of the SinumerikAdapter application

Ethernet Connection settings

Hint

The Ethernet connection is only available, if you have installed the *SinumerikAdapter* application. It will not work with an installed *SinumerikPowerLineAdapter* release variant. (Please review the [Variants](#) section)

The SinumerikAdapter ships with an IP address of 192.168.214.1. This allows it to communicate with the default machine network of a SINUMERIK NCU.

To change this configuration, the datasource configuration of the **SinumerikAdapter** IndApp needs to be edited. Use the configuration backend in the Insights Hub for this modification.

Relevant part of SinumerikAdapter configuration

```

"datasourceConfig": {
  "providedDatasource": [
    {
      ...
      "meta": {
        "ipAddress": "192.168.214.1",
        "controlType": "840Dsl",
        "serialNumber": ""
      },
      ...
    },
    ...
  ],
  ...
}

```

element	explanation
ipAddress	The IP Address of the connected Machine.
controlType	Must be set to '840Dsl' or 'ONE'. See chapter (Control Type)[./sinumerikadapter.md#control-type]
serialNumber	The serial number of the connected machine. See chapter (Serialnumber) [./sinumerikadapter.md#serialnumber]

Control Type

The SinumerikAdapter supports the two control types: "SINUMERIK 840D sl" and "SINUMERIK ONE". The default configuration of the SinumerikAdapter fits to the manufacturer settings of a "SINUMERIK 840D sl". The default controlType is "840Dsl". For communication with a SINUMERIK ONE the controlType in the configuration needs to be changed to "ONE".

The SinumerikAdapter supports the listed control types:

- "840Dsl"
- "ONE"

If the configured controlType does not match to one of those, the SinumerikAdapter will not start.

Attention

The SinumerikAdapter does not validate the configured controlType against the connected device. As such, connection issues may occur if the configured controlType differs from the connected machine.

Serialnumber

The SinumerikAdapter needs to be configured with the correct serial number of the connected NCU. If the configured serial number does not match with the connected NCU, the SinumerikAdapter will report a license error and block all access to the machine.

To configure the serial number, the providedDatasource configuration of the **SinumerikAdapter** IndApp needs to be edited. Use the configuration backend in the Insights Hub to do so.

You can find the serial number of your machine by using the HMI

(Setup -> Mach. Data -> General MD -> 18030[0] \$MN_HW_SERIAL_NUMBER)

or under this BTSS address:

8884 ↓ Period 1 of the test license active remaining time 3000 h

General machine data

17530	\$MN_TOOL_DATA_CHANGE_COUNTER	1FH	po
17540	\$MN_TOOLTYPES_ALLOWED	3FFH	po
17600	\$MN_DEPTH_OF_LOGFILE_OPT	5	re
17610[0]	\$MN_DEPTH_OF_LOGFILE_OPT_PF	100	re
17610[1]	\$MN_DEPTH_OF_LOGFILE_OPT_PF	10	re
17610[2]	\$MN_DEPTH_OF_LOGFILE_OPT_PF	30	re
17900	\$MN_UDI_FUNCTION_MASK	0H	po
17950	\$MN_IS_AUTOMATIC_MEM_RECONFIG	1	po
17951	\$MN_AUTOMATIC_MEM_RECONFIG_FILE	/siemens/sinu...	po
18030[0]	\$MN_HW_SERIAL_NUMBER	000060073316A...	po
18040[0]	\$MN_VERSION_INFO	Numeric ContSI...	po
18040[1]	\$MN_VERSION_INFO	99.19.02 04/11...	po
18040[2]	\$MN_VERSION_INFO	7/12/16 16:07:...	po
18040[3]	\$MN_VERSION_INFO	840SL-73	po
18040[4]	\$MN_VERSION_INFO	SOC2	po
18042[0]	\$MN_CC_VERSION_INFO		po
18042[1]	\$MN_CC_VERSION_INFO		po
18042[2]	\$MN_CC_VERSION_INFO		po

Hardware series number

General MD	Channel MD	Axis MD	User views	Control Unit parameter
------------	------------	---------	------------	------------------------

Search

Cancel

Continue search

Attention

Do not change any other section of the SinumerikAdapter's datasourceConfig other than the datasourceId and meta.

MPI Connection settings

Hint

The MPI connection is only available, if you have installed the *SinumerikPowerLineAdapter* release variant of the SinumerikAdapter application. If this variant is not available for installation, please contact the SIEMENS support to get it unlocked. (Please review the [Variants](#) section)

The MPI connectivity requires a installed gateway component, which enables Ethernet to MPI routing. The SIEMENS Support will help you with that setup.

The SinumerikPowerLineAdapter must be configured to connect a SINUMERIK NCU through this gateway.

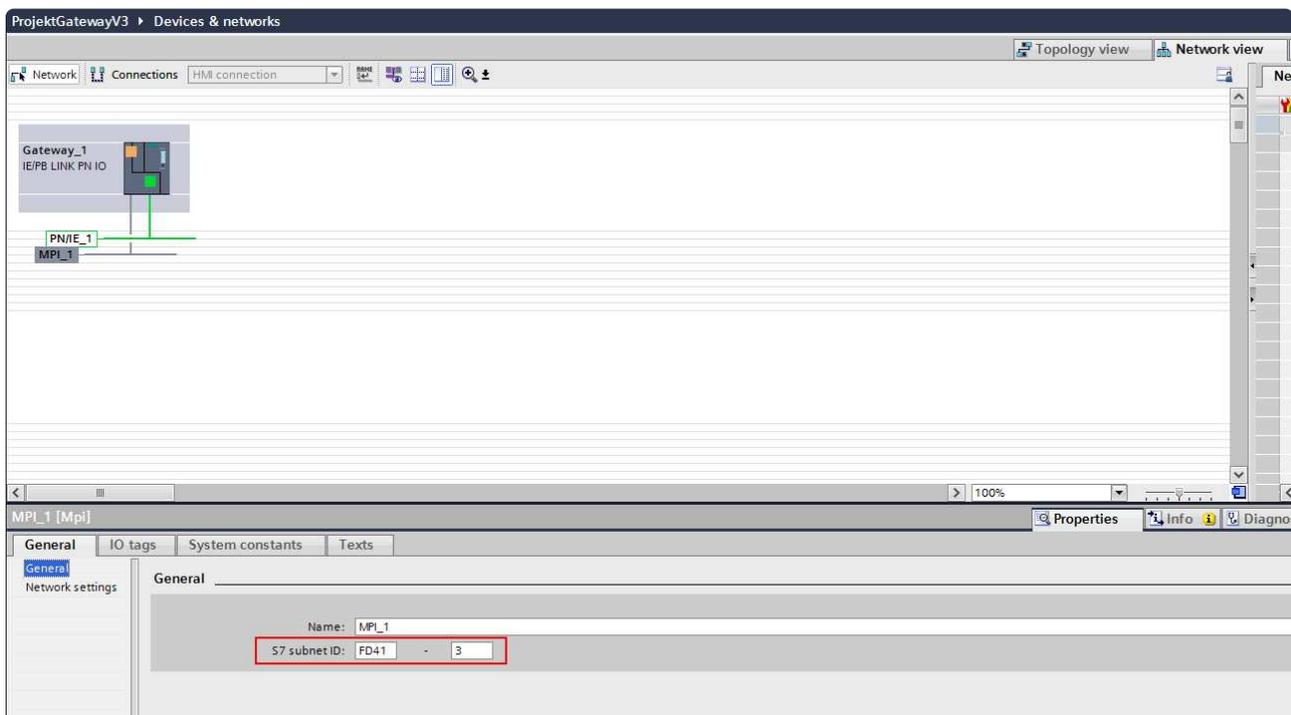
Relevant part of SinumerikAdapter configuration

```

"datasourceConfig": {
  "providedDatasource": [
    {
      ...
      "meta": {
        "gatewayAddress": "192.168.214.1",
        "MPIAddress": "13",
        "controlType": "840Dpl",
        "subnet": "FD41-3"
      },
      ...
    },
    ...
  ],
  ...
}

```

element	explanation
gatewayAddress	The IP Address of your gateway component.
MPI Address	The MPI Address of the connected Machine.
controlType	Must be set to '840Dpl'
subnet	The <i>S7-Subnet-ID</i> of the connected MPI network of your gateway. This information can be found in the network configuration of the installed gateway component (most common: TIA portal project - see screenshot). Must not be empty! If your connected gateway does not require a S7-Subnet configuration, just configure this as "0000-0"



Custom Alarmtexts

The SinumerikAdapter offers the possibility to use custom HMI alarm text files. Those texts will be used for alarm reports.

To use custom alarm texts with SinumerikAdapter, you need to copy the relevant files into the Samba share of the SINUMERIK Edge.

!!! Hint: You can mount the Samba share of the SINUMERIK Edge to the Sinumerik HMI to copy those files. The usage of Samba Server is documented [here](#).

!!! Attention: Only english language is supported.

Instructions:

- Navigate to the folder "sinumerikadapter" in the SINUMERIK Edge Samba share.
- Create the required folder structure for lng and cfg folders, based on your HMI setup. The supported folder structure is:

```
/user/sinumerik/hmi/lng
/user/sinumerik/hmi/cfg
/oem/sinumerik/hmi/lng
/oem/sinumerik/hmi/cfg
/addon/sinumerik/hmi/lng
/addon/sinumerik/hmi/cfg
```

- Copy the **.hmi* and **.qm* files from the *lng* folders of the HMI file system into the corresponding folders on the SINUMERIK Edge Samba share.
- Copy the *slaesvccconf.xml* and *slaesvcadapconf.xml* files from the *cfg* folders of the HMI file system into the corresponding folders on the SINUMERIK Edge Samba share.
- Restart the SinumerikAdapter application.

Provided Services

parameter-service/v1

The SinumerikAdapter enables access to a SINUMERIK NCU by implementing a parameter-service/v1 provider. General information about configuration and usage of the parameter-service are documented in the [service documentation](#).

Attention

You don't need to change the parameter-service/v1 section of the SinumerikAdapter. The service will be configured automatically. Only configure connected applications.

For a **reading** operation, "accessType" 'r' must be added in order to configure the service correctly. You don't have to specify datapoints for reading access.

FIREWALL PERMISSIONS

The SinumerikAdapter activates a firewall that protects parameters from being written without permission. For modifying parameter access, an application must require access, using accessType "w" and specify a list of required parameters. Those parameters will be used to fill the SinumerikAdapters whitelist. All write requests will be denied unless they are whitelisted.

example:

```
"datasourceConfig": {
  "requiredDatasource": [{
    "datasourceId": "SINUMERIK_NCU1",
    "type": "SINUMERIK",
    "services": {
      "parameter-service/v1": {
        "access": [{
          "accessType": "w",
          "datapoints": [{
            "address": "some whitelisted parameter"
          }]
        }]
      }
    }
  }]
}
```

subscription-service/v1

The SinumerikAdapter publishes data from a SINUMERIK NCU by implementing a subscription-service/v1 provider. Please navigate to the datasource configuration chapter in the [service documentation](#) for information on how to receive data from the SinumerikAdapter.

Attention

You don't need to change the subscription-service/v1 section of the SinumerikAdapter. The service will be configured automatically. Only configure connected applications.

Diagnosis

The SinumerikAdapter application is set to logging level "WARN" as default. Please be aware, the most warning messages in the logfile do not have a "going" message. To recognize, if a warning is still present, you have to switch to loglevel "INFO". Anyway, most warning messages will be written in a periodic way, so it will be enough to review the timestamp of the message. Please also review the [Diagnostic](#) documentation to get information, how to access logging informations.

Hint

The SinumerikAdapter logging consists of two separate logfiles: sinumerikadapter and sinumerikservice.

Security information

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

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

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

For additional information on industrial security measures that may be implemented, please visit

<https://www.siemens.com/industrialsecurity>.

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

To stay informed about product updates, subscribe to the Siemens Industrial Security RSS Feed under <https://www.siemens.com/cert>.

Troubleshooting

1) For more diagnostic information, change the log level of the `sinumerikadapter IndApp` to "INFO". This information can be found in the `SinumerikAdapter`'s log file.

2) Configuration of a serial number with leading zeros fail.

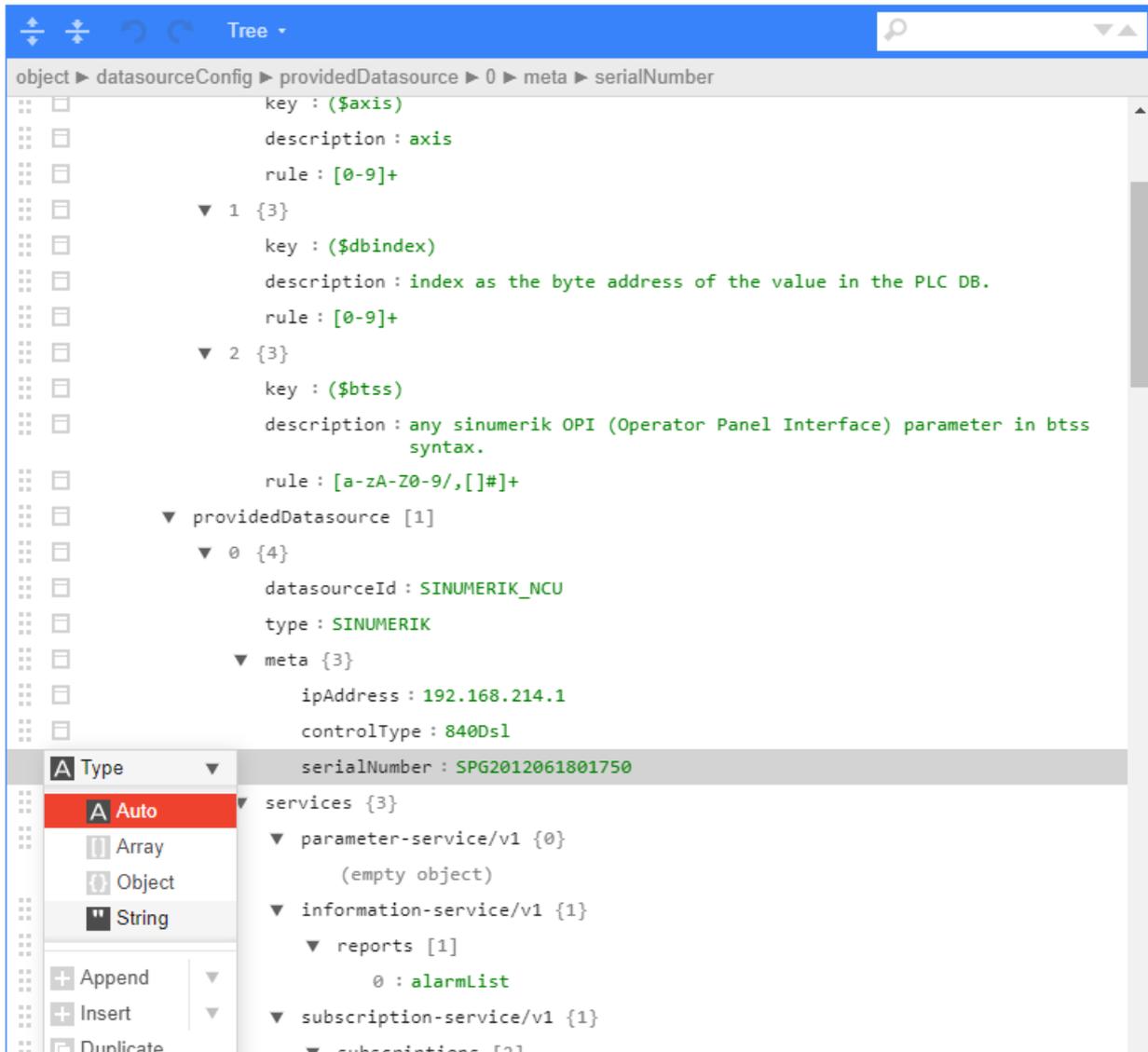
Details:

If you configure a NCU's serial number with leading zeros in the connection settings of `SinumerikAdapter`, the serial number check of the `SinumerikAdapter` might fail and the connection from `SINUMERIK Edge` to `SINUMERIK NCU` will not work.

Workaround:

In the `AppManagement` UI, edit the configuration of the `SinumerikAdapter` as follows: reconfigure the `sinumerikadapter IndApp` while using the tree view of the configuration editor. Change the field type of `serialNumber` from `Auto` to `String` (see image).

Config Edit



3) My application does not receive any HF data.

Please check, if you have installed sufficient licenses. You can review the AdapterFramework UI for further diagnostics.

Enable Access to a S7 master device

The S7adapter application is acting as a IO-Supervisor for Profinet devices.

Hardware setup

Connect the machine network interface of the SINUMERIK EDGE to an ethernet or profinet port of your S7 device. During onboarding of the EDGE in the Insights Hub, make sure that the ip address of the EDGE's production interface (machinelan0) does not collide with other hardware connected to the system.

Software installation

Install the S7adapter application on your SINUMERIK EDGE instance. Configure the Address of the S7 device, by configuring the S7adapter application.

In the S7adapter configuration, you will find a provided datasource of type "S7Device". Use the "meta" object to configure the IP address, Rack and Slot of the S7 device. Review the hardware configuration of the machine in your engineering tool (TIA portal) to find this information.

Hint

It is recommended to rename the datasourceID to some understandable name. "PLC_1" is just a placeholder.

example

```
"datasourceConfig": {
  "providedDatasource": [
    {
      "datasourceid": "PLC_1",
      "type": "S7Device",
      "meta": {
        "ipAddress": "192.168.214.1",
        "rack": 0,
        "slot": 2
      }
    }
  ]
}
```

Supported devices

Any device acting as a certified Profinet/Profibus master and supporting absolute parameter access over S7 protocol communication can be connected.

Official supported

- SIMATIC S7 300 CPU

Most likely functioning (but not part of the test)

- SIMATIC S7 400 CPU
- WinAC CPU
- SIMATIC S7 1200 (in 300/400 compatibility mode)
- SIMATIC S7 1500 (in 300/400 compatibility mode)
- SINAMICS Drives CPU (G120)

Attention

S7adapter application is only tested with SIMATIC S7 300 CPU.

Security information

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

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

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

For additional information on industrial security measures that may be implemented, please visit <https://www.siemens.com/industrialsecurity>.

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

To stay informed about product updates, subscribe to the Siemens Industrial Security RSS Feed under <https://www.siemens.com/cert>.

Enable Access To OPC-UA

Introduction

The OPC-UA Adapter is an application used to connect the SINUMERIK Edge to OPC-UA servers.

Overview

The OPC-UA Adapter allows access of data from multiple OPC-UA servers. The OPC-UA Adapter can then be used in the following ways:

- Accessing data via Parameter Service
- Subscribing for data on change
- Configuring the event processor in the OPC-UA Adapter to calculate new values based on the OPC-UA Data and access them through Parameter Service or subscription

In order to use data from the OPC-UA Adapter an application has to address the correct data points. In case the application uses the event processing feature, it additionally has to configure the OPC-UA Adapter to pre-process the data (See Event Processor).

Compatibility with OPC-UA Versions

The OPC-UA Adapter supports the following versions of the OPC-UA standard:

- 1.00
- 1.02
- 1.03
- 1.04

Data subscription

To subscribe data on change, the application has to configure the data requirements against the OPC-UA Adapter.

Here is an example configuration of an applicaiton using the OPC-UA Adapter (Subscription and Parameter Service):

```

{
  "specificConfig": {},
  "loggingConfig": {
    "appender": "JOURNAL_APPENDER",
    "severity": "INFO"
  },
  "datasourceConfig": {
    "requiredDatasource": [
      {
        "datasourceId": "OPCUAADAPTER1",
        "type": "OPCUA",
        "services": {
          "parameter-service/v1": {
            "access": [
              {
                "accessType": "r",
                "datapoints": [
                  {
                    "address": "ext::opcua::sinumerik::NS0|Numeric|2278"
                  }
                ]
              }
            ]
          }
        },
        "subscription-service/v1": {
          "subscriptions": [
            {
              "messageId": "opcua_adapter_data",
              "messageName": "opcua_adapter_data",
              "quality": "quality_all",
              "datapoints": [
                {
                  "address": "ext::opcua::sinumerik::NS0|Numeric|2278"
                }
              ]
            }
          ]
        }
      }
    ]
  }
}

```

Addressing Scheme

In order to access values from a connected OPC-UA server, there is an address required to identify the data item. The OPC-UA Adapter has two different address spaces:

- OPC-UA value addresses
- Internal (calculated) value addresses

OPC-UA Addresses

OPC-UA addresses have the following format:

```
ext::opcua::<Connection Name>::<OPC-UA Namespace>|<Node ID Type>|<Node ID>
```

The **Connection Name** is the name of the connection as provided in the configuration of the OPC-UA Adapter.

The **OPC-UA Namespace** is the OPC-UA namespace. Example **NS2** for namespace 2.

The **Node ID Type** is the type of the node ID according to the OPC-UA standard. The following types are supported:

- String
- Numeric
- Opaque

Internal (Calculated) Addresses

Calculated variable addresses have the following format:

```
ext::var_t::<Node ID>
```

The **Node ID** is a string which uniquely represents the calculated value. The value has to be calculated via the event processor.

See the Event Processor chapter for more detail.

Connecting to OPC-UA servers

In order to access OPC-UA data, the OPC-UA Adapter has to connect to at least one OPC-UA server.

Preconditions

To connect to an OPC-UA server, the server needs to be accessible in the machine network. If the OPC-UA server to connect to is the SINUMERIK OPC-UA server, then this server must be activated and configured in the SINUMERIK HMI.

Configuration

The OPC-UA connection configuration is part of the specific configuration of the OPC-UA Adapter. Here is an example:

```

"specificConfig": {
  "mca": [
    {
      "name": "mca.adapterconfig::opcua",
      "config": {
        "connections": [
          {
            "name": "sinumerik",
            "message_security_mode": "SignAndEncrypt",
            "security_policy": "Basic256Sha256",
            "url": "opc.tcp://192.168.100.200:4840",
            "login": {
              "pw": "password",
              "user": "username"
            },
            "pki": {
              "client_cert": "Client certificate in PEM format",
              "client_private_key": "Private key for the certificate in PEM format"
            }
          }
        ]
      }
    }
  ]
}

```

MCA in this configuration stands for machine controller adapter. The section contains the configuration for all connections to the controller in the OPC-UA Adapter. On the SINUMERIK Edge 'mca' can contain only one item. The name property of this one item must be **"mca.adapterconfig::opcua"**

Within the connections section it is possible to configure multiple individual connections. Each of them has a name property. The names have to be unique. In this example the only one connection is named **sinumerik**. When data points of the OPC-UA Adapter are referenced, this name is used in the address string to identify the OPC-UA connection.

List of supported message securities:

- None
- Sign
- SignAndEncrypt

List of supported security policies:

- None
- Basic128Rsa15
- Basic256
- Basic256Sha256

Basic128Rsa15 and *Basic256* marked **DEPRECATED** in the standard therefore it is suggested to use *Basic256Sha256* policy when encryption is necessary.

See OPC-UA specification for more detail about OPC-UA message security and security policies.

The **"login"** and **"pki"** properties are not mandatory. They are only required if the server needs them to be able to establish connection.

Certificate creation

When creating a client certificate for the adapter to be able to connect to the OPC-UA server two important properties has to be set: * **subjectAltName=URI:urn:MachineAgent** * Case sensitive so the "urn:MachineAgent" has to be the same always otherwise the agent fails to verify the given certificate. * **authorityKeyIdentifier** has to be included in the certificate file otherwise the agent fails to verify the certificate.

After creating the certificate and private key PEM files **the content of the files** has to be pasted into the configuration.

See OPC-UA specification for more detail about OPC-UA certificates.

Event processor documentation

The event processor allows us to configure and execute event processing programs to monitor the controller's state. These programs can contain multiple processor flows. Every flow executes different kind of operations and always started with a trigger.

Overview of processor types

Three main category is known by the Machine Agent. - **Triggers** - Triggers are the starting point of each processor program - They are responsible to start an execution flow within the Agent - Output port: - **triggered** - **Filters** - Filters can separate the flow sequence based on different conditions - They are capable of defining multiple outputs for the same processor program - Two output ports: - **filtered** - If the condition defined by the filter was not met - **passed** - If the condition defined by the filter was met - **Functions** - These processors can execute different types of operations on specified data - They can execute mathematical operations on the data - They can gather or send data - One output port: - **exec** - **DTS connectors** - These processors are used, to transfer different types of data to the DTS - The DTS will then accumulate and then upload data to a server side application. - The target application will be determined based on the name of the Event Processor job.

How to create a processor

All processors must be encapsulated, in order to make each of them uniquely identifiable for linking.

```
{
  "name": "name",
  "processor": { ... },
  "links": [ ... ]
}
```



Parameters



How to Link processors together

Every processor type must produce an output value. In another way every processor must have one or more **ports** that can be used to create links between them. These links define a many-to-many relation between the

processors which means that one processor can have multiple links to other ones and can be linked to more than one. Links always have to be placed in the configuration of the processor that is sending the output. We have to specify the port and the target processor's name that also exists in the program.

Event Processing

Event Processing is the mechanism that is used to gather and make basic manipulation on data.

Value Caching

Data that is being processed is always cached by the Event Processor to make it faster and to keep consistency during processing. There are 2 types of caches within the Event Processor. - Global Cache - Cycle Cache

Global Cache

Is used to constantly keep the latest values of variables quickly available for the Event Processor.

Values within the Global Cache are kept up-to-date by the MCA via its subscription mechanism. Changes made by a Processor to a variable's value will be detected by the Global Cache and the change will be propagated toward the MCA service, to be written to the machine.

Only those variables are stored in the Global Cache, which are referenced by at least one Processor. If a new processor is configured during runtime, which references a variable that was not yet referenced, will be automatically added to the cache.

Cycle Cache

Is mirrored from the Global Cache the moment a new [Processing Cycle](#) starts. This Cycle Cache will only store values that were, until the Cycle start, referenced.

Values of variables will **NOT** be changed in the Cycle Cache during the Cycle's execution time! Changes made to those variables will only take effect in the Global Cache, and only after the MCA service notifies it of the change! However changes to an internal variable's value **will take effect** in the Cycle Cache!

The Cycle Cache will be deleted only when the Cycle has completed.

Event Processor layers

Event processing is a complex operation, consisting of multiple layers. Each of these layers have a different set of responsibilities. The layers, from the bottom to the top, are: - Processors - Workflows - Programs - Cycles

Event Processor Processors

Processors are the basic building blocks within the Event Processor. Each processor instance is responsible for a single, well defined operation.

A Processor consists of a [Processor](#) and its [Wrapper](#).

NOTE: Executing a processor more than once in a [Processing Cycle](#) will result in an error! To avoid this you can use the [Once per cycle filter](#).

Event Processor Workflow

In most cases single processor cannot cover a whole functionality. Thus Processors can be [linked together](#) to create complex operations. Such an independent chain of processors is called a Workflow.

Event Processor Program

Each Application can freely define Workflows. To make handling these Workflows together easier, an Application can define multiple workflows within one Event Processor configuration. These Workflows then will be executed independently from one another.

Synchronising or data sharing between Workflows can be achieved using internal variables.

There can be 2 types of Event Processor Programs: - **System Programs**: Can only be defined by the server side entity called System. These programs are unique in a way, that they will be executed before the Application programs. - **Application Programs**: Can be freely defined by Applications.

Event Processor Cycle

The Event Processor executes workflows in cycles. When a new cycle starts a new **Cycle Cache** for values is created. This means, that value changes that are made by Workflows in the Cycle or changes that occur on the Machine will not be visible within the Cycle! This mechanism is there to ensure consistency of data throughout the whole Cycle.

Example program

The following program will create a subscription on the specified variable change address (*variable_change_trigger*) and will gather data with the help of the *value_set_builder* on every value change. When the data is ready the *data_sender* will forward it through the configured dts service.

```

{
  "sys_programs": [],
  "app_programs": [{
    "app_name": "my_app",
    "config": {
      "processors": [
        {
          "name": "on_change_simulated",
          "processor": {
            "__t": "variable_change_trigger",
            "desired_update_cycle_ms": 300,
            "address": "ext::tst_south::test/zerotohundred"
          },
          "links": [{
            "port_name": "triggered",
            "target_processor": "status_vs_builder"
          }
        ]
      },
      {
        "name": "status_vs_builder",
        "processor": {
          "__t": "value_set_builder",
          "value_set_name": "machine_status",
          "values": [
            {
              "value_name": "status",
              "address": "ext::tst_south::test/zerotohundred",
              "desired_update_cycle_ms": 300
            }
          ]
        },
        "links": [
          {
            "port_name": "exec",
            "target_processor": "data_sender_1"
          }
        ]
      },
      {
        "name": "data_sender_1",
        "processor": {
          "__t": "data_sender",
          "channel_name": "data"
        },
        "links": []
      }
    ]
  }
]}

```

Processors

Triggers

Triggers are used to start the execution of an [Event Processor Workflow](#). Each trigger has one output port: - **triggered**: Is fired, when the trigger condition is met. E.g.: when the right time period has passed using a cyclic trigger.

Cyclic trigger

The cyclic trigger can be used to start a [workflow](#) periodically.

Configuration:

```
{
  "_t": "cyclic_trigger",
  "cycle_in_milliseconds": 2000
}
```

NOTE: The Machine Agent cannot guarantee normal operation when the cyclic trigger is set to be triggered in less than 300ms!

 Parameters 

Variable change trigger

The variable change trigger executes when the value of a variable changes. The variable can be a calculated one, calculated by the Event Processor, or a data point provided by an external adapter.

Configuration:

```
{
  "_t": "variable_change_trigger",
  "desired_update_cycle_ms": 300,
  "address": "app::var_t::/oeo_tmp"
}
```

 Parameters 

Startup trigger

The startup trigger executes once per startup of the Machine Agent, or the first time when an application's configuration takes effect. This type of trigger can be used to set default values or gather preliminary data from the controller.

Configuration:

```
{
  "_t": "startup_trigger"
}
```

Filters

Filters are used to introduce logical separation of the flow sequence based on different conditions. They can be used to produce different outputs by the same flow, based on certain input values. Each filter has 2 output ports: -

filtered - Is fired when the condition, defined by the filter, was not met - **passed** - Is fired when the condition, defined by the filter, was met

Condition filter

The condition filter is used to evaluate an expression in a [workflow](#).

Configuration

```
{
  "_t": "condition_filter",
  "desired_update_cycle_ms": 300,
  "condition": {...}
}
```

 Parameters 

Once per cycle filter

The once per cycle filter can be used to execute the subsequent part of the flow only once in a processing cycle. For example, if you have multiple variable triggers triggering a processing cycle at once, then you can use this filter to ensure that the subsequent parts of the flow is only executed once.

Configuration

```
{
  "_t": "once_per_cycle_filter",
}
```

Functions

Functions are used for different auxiliary operations on a set of data. All functions have one output port, which is called: **exec**

Variable calculator

The variable calculator is used to set calculated variables. In system programs, the component can be used to store the result in `glob::cache_value...` global cache. All apps can write to `ext::var_t:...` or opc ua addresses, or their local caches. These are in turn readable by all application programs.

This is how a variable calculator is configured:

```
{
  "_t": "variable_calculator",
  "target_address": "ext::adapter::address",
  "desired_update_cycle_ms": 300,
  "expression": {...}
}
```

NOTE: Changing the value of a variable will not trigger a [Variable change trigger](#) within the same [Processing Cycle](#)! The only exceptions are variables stored in the *Transient Storage*.
For more information on addressing see [Addressing](#).

Value set builder

- The result port is always "exec".

Configuration:

```
{
  "_type": "value_set_builder",
  "value_set_name": "my_value_set",
  "values": [
    {
      "value_name": "my_value",
      "address": "ext:tst::address",
      "desired_update_cycle_ms": "100"
    }
  ]
}
```

Produced data structure:

DTS connectors

DTS Connectors are used to forward different types of data towards a server side application.

DTS is a robust data uploader, which is capable of buffering incoming data, in order to prevent data loss, in case of a slow network connection, or a short network outage.

DTS always uploads its content to the server using the name of the Event Processor job.

Data sender

Is used to upload variables, using different channels of the DTS.

Configuration

```
{
  "_t": "data_sender",
  "channel_name": "data"
}
```

The output port is `exec`.

Expressions

Expressions are used by certain processors, to define complex mathematical or logical functions. The Machine Agent supports the following types of expressions:

- Unary expression
- Binary expression
- Const expression
- Variable expression

Unary Expression

Unary expressions contain an operator and one operand.

! (not) is the only supported operator.

The **operand** can be any expression (unary, binary, const, variable).

Definition:

```
{
  "_t": "unary_expr",
  "operator": "!",
  "expr": {...}
}
```

 Parameters 

Binary Expression

Binary expressions have one operator and a left and right operands. Binary expressions are evaluated from the left to the right. Both operand can be any expression (unary, binary, const, variable).

Definition

```
{
  "_t": "binary_expr",
  "operator": "||",
  "left": {...},
  "right": {...}
}
```

 Parameters 

NOTE: - Logical operators do not support short-circuiting! This means, that regardless of the result of the expression left, the expression right is going to be evaluated! - Operands are not type restricted! This means, that operators will try to cast operands into a common type, on which they could execute the operation.

Constant Expression

The constant expression is used to represent a constant value in an expression.

Definition:

```
{
  "_t": "const_expr",
  "value": 3
}
```

 Parameters 

Variable Expression

The variable expression is used to represent the current value of a variable (e.g. an SINUMERIK NC variable) in an expression.

Definition:

```
{
  "_t": "variable_expr",
  "address": "ext:tst:address"
}
```

 Parameters 

Complete OPC-UA Adapter Config Example

Here is a complete example of an OPC-UA Adapter configuration:

```
{
  "specificConfig": {
    "machineAgentConfiguration": {
      "dts": {
        "configs": [
          {
            "app_name": "listenerapp",
            "config": {
              "channels": [
                {
                  "buffer_config": {
                    "files_per_folder": 100,
                    "size_in_mb": 500,
                    "size_per_file_in_mb": 2
                  },
                  "connection_name": "default",

```

```

    "name": "info"
  },
  {
    "buffer_config": {
      "files_per_folder": 100,
      "size_in_mb": 500,
      "size_per_file_in_mb": 2
    },
    "connection_name": "default",
    "name": "opcua_adapter_data"
  }
]
}
}
],
},
"eventproc": {
  "sys_programs": [],
  "app_programs": [
    {
      "app_name": "listenerapp",
      "config": {
        "processors": [
          {
            "name": "on_change_opcuatest",
            "processor": {
              "__type": "variable_change_trigger",
              "__t": "variable_change_trigger",
              "desired_update_cycle_ms": 50,
              "address": "ext::opcua::sinumerik::NS0|Numeric|2278"
            },
            "links": [
              {
                "port_name": "triggered",
                "target_processor": "vsbuilder1"
              }
            ]
          },
          {
            "name": "vsbuilder1",
            "processor": {
              "__type": "value_set_builder",
              "__t": "value_set_builder",
              "value_set_name": "example_vs",
              "values": [
                {
                  "value_name": "example_value",
                  "address": "ext::opcua::sinumerik::NS0|Numeric|2278",
                  "desired_update_cycle_ms": 50
                }
              ]
            },
            "links": [
              {
                "port_name": "exec",
                "target_processor": "data_sender_1"
              }
            ]
          }
        ],
        "name": "data_sender_1",
        "processor": {
          "__type": "data_sender",
          "__t": "data_sender",
          "channel_name": "opcua_adapter_data"
        },
        "links": []
      }
    }
  ]
}
]

```


Enable Access to a Fanuc controller device

Hardware setup

Fanuc controller device should be connected with the SINUMERIK EDGE platform via its machine network interface. During onboarding of the EDGE platform through Insights Hub, it should be controlled that the ip address of the EDGE's production interface X2P1 (machinelan0) does not collide with other hardware connected to the system.

Software installation

Before the installation of FanucAdapter, **AdapterFramework** app should be installed and configured on the corresponding Edge platform instance. Chapter [Installation of AdapterFramework](#) could be visited for a detailed explanation about the installation procedure.

After that, **FanucAdapter** application can be installed through Insights Hub. It is crucial to configure device IP and port number written in the specificConfig part of the meta config as follows:

```
"specificConfig": {  
  "FanucIP": "192.168.214.200",  
  "FanucPort": 8193,  
  "FanucTimeout": 10  
}
```

FanucIP and *FanucPort* details are mandatory to setup a TCP/IP connection to the Fanuc controller. Moreover, *FanucTimeout* is used to configure the maximum amount of time to wait for a focus library function call before the expiration. These parameters are required by the Focas library. Besides, *FanucTimeout* is an optional field and could be removed from the configuration.

Supported devices

It should be stated that during the implementation and test phases, **Fanuc Simulator** is utilized as Fanuc controller device. Nevertheless, the following list shows the supported Fanuc controller models in theory:

- Fanuc 30i
- Fanuc 31i
- Fanuc 32i
- Fanuc 35i-B

Precautions

FanucAdapter Life-Cycles

1. **Cold-start** - Represents the first startup of the microservice. First device access is expected between 10sec and 60sec.
 2. **Hot-start** - Represents the connection is alive and actively serving the client microservices.
 3. **Warm-start** - Represents the situation when device connection is lost after it is established once. FanucAdapter stays in this state for 60sec then restarts.
-

Sinumerik Edge Sensor Adapter

Introduction and Goals

Sensor Adapter (SA) is a summary name for a system designed to enable the collection, transmission, and processing of data that can be collected by a production-related sensor in an industrial environment. We first aimed to support TCP / IP-based sensors connected to the EdgeBox network connector. Of these, we focus on the processing of images provided by the industrial IP Camera.

The goal is to create a generic SA that provides a unified API for sensor manufacturers to connect their sensors to the Sinumerik Edge environment. Another goal is to provide software developers with secure and efficient access to sensor data from machinelan for their data processing applications.

The sensors can send high-frequency (HF) data with a sampling frequency of up to 44.1 kHz and a depth of 16 bits. A typical example of this is the audio information collected by microphones. In contrast, sensors can send low-frequency (LF) 1-100 Hz data, which can be orders of magnitude larger data than high-frequency data. A good example of this is the high-resolution image information sent by cameras. The processing and transmission of HF and LF data based on these requires a slightly different approach, but the structure and main functions of the system are the same.

IP Camera technical requirements

- TCP/IP based communication
- RTSP data transfer
- H.264 codec
- Dual channel support (primary and secondary stream)

Definition of the Image_stream

The Image_stream is a series of preprocessed images (pictures) from the IP camera's primary or secondary stream in raw (uncompressed) RGB format. A subscribed consumer will get the oldest available Image_stream picture from the buffer.

Resolution: Any of the IP camera's standard resolutions (e.g. 1920*1080, 1280*720, ..., 320*200)

Framerate: Any real number. (e.g. 25, 20, 10, 2, 0.5, 0.1, etc.)

Note: If the setting is not equal to the camera's own framerate, the last available picture from the camera will be used.

Format: RGB (uncompressed)

Note: The SA's CPU and RAM usage is depending on resolution and framerate of stream.

Definition of the Live_stream

The Live_stream is a series of preprocessed images (pictures) from the IP camera's primary or secondary stream in (compressed) JPEG format. A subscribed consumer will get the next available package of JPG images.

Note: the default limit of the Live_stream's buffer size is 300 frames.

Resolution: Any of the IP camera's standard resolutions (e.g. 704*576, 640*480, 320*200)

Framerate: Any integer number. (e.g. 30, 25, 20, 10, 5, etc.) *Note:* If the setting is not equal to the camera's own framerate, the last available picture from the camera will be used.

Format: JPEG

Note: The SA's CPU and RAM usage is depending on resolution and framerate of the rtsp stream.

Installation

Select the application "**sensoradapter**" with the released version related to the firmware version installed on your SINUMERIK EDGE to install it on your connected SINUMERIK EDGE device. The current application is available in two different versions that differ in the resources available: - 1CPU: It is limited to use maximum 100% CPU - 2CPU: It is limited to use maximum 200% CPU

Note: the Sinumerik EdgeBox (Picobox (IPC127E), Nanobox (IPC227E) and Microbox(IPC427E)) contains 4 CPU cores (400%)

Please refer to chapter [Application Management](#) for detailed information how to install an application on your SINUMERIK EDGE device.

Configuration

Initial Configuration of the IP camera

1. Software config

Before connecting the IP camera to the EdgeBox with a LAN cable, it needs to be accurately preconfigured as follows: - Connect it with a standard LAN cable (UTP Cat5e) to a PC (e.g. a simple Windows laptop) - Open the camera's built-in web page with a web browser. The default IP address (or site name), username and password can be found in the camera's own documentation. - Set up the desired IP address (MachineLan), change the default username and password. - Set up the maximum necessary image resolution and fps values for the primary and secondary streams.

Note: do not use unnecessarily big values for the quality, it can cause unnecessary CPU load on the Edgebox. - Set up the RTSP URL and port (if it can't be changed, just note it down for later SA configuration). **2. Hardware config** - Connect the Camera with a standard LAN cable (UTP Cat5e) to the IPC (e.g. Edge NanoBox or MicroBox)

Configuration of Sensor Adapter

Before configuring the SA, please ensure that the IP Camera(s) configured to provide only the amount of images that is absolutely necessary, in minimum required resolution. For configuration, please use the [Insights Hub configuration UI](#). You shall fill out the correct databus connection values, primary and secondary stream credentials & URLs, subscription parameters.

Scenario 1 - Connect to 1 camera using its primary stream (FullHD, 2 fps)

Sensoradapter metaconfig - Example #1

```

{
  "databusConfig": {
    "connectionstring": "rnd:databus.databus.indapp-net.industrialedge.io:8883",
    "credentials": {
      "password": "",
      "username": ""
    },
    "permissions": []
  },
  "datasourceConfig": {
    "providedDatasource": [
      {
        "datasourceId": "ExampleCamera",
        "meta": {
          "driver_parameters": {
            "image": {
              "rtsp_username": "[username]",
              "rtsp_password": "[password]",
              "rtsp_url": "[rtsp://]<camera_ip_address>[:rtsp_port][:/path/to/image]"
            }
          }
        },
        "services": {
          "subscription-service/v1": {
            "subscriptions": [
              {
                "datapoints": [
                  {
                    "address": "image"
                  },
                  {
                    "address": "timestamp"
                  },
                  {
                    "address": "pan"
                  },
                  {
                    "address": "sensoradapter_subscription_message_count"
                  }
                ],
                "merge": true,
                "messageId": "ExampleCamera1",
                "quality": "sensor_500ms"
              }
            ]
          }
        },
        "type": "camera"
      }
    ]
  },
  "lifecycleConfig": {
    "appStart": false
  },
  "machineConfig": {
    "subscriptions": {}
  },
  "system_service": false
}

```

Sensoradapter metaconfig - Explanation #1

- Line 3: databusConfig\connectionstring: Port 8883 defines encrypted channel. For non-encrypted connection use 1883; Note: Encrypted channel is enforced.
- Line 13: datasourceConfig\providedDatasource\datasourceId: "ExampleCamera" is a user-defined ID for the

camera the sensor driver will connect to. In order to connect to this camera instance, use the same on client side in *requiredDatasource*.

- Line 15: `datasourceConfig\providedDatasource\driver_config`: In order to read an rtsp stream from the IP camera, fill in **image** with "*rtsp_url*" and if necessary "*rtsp_username*" and "*rtsp_password*" fields in the given format, along with subscribing to "*image*" **datapoint** (line 29.). A true value from the configuration can look like this:

```
"driver_parameters": {
  "image": {
    "rtsp_username": "myuser",
    "rtsp_password": "myStr0ngPassword",
    "rtsp_url": "rtsp://192.168.1.100:554/channel_1"
  }
}
```

Note: As you'll see in later scenarios, in order to create a *live stream*, use "**livestream**" in the given format, along with subscribing to "**livestream**" **datapoint**. Both streams are optional and can function independently from each other. As a result, you can use either of the streams or both simultaneously. Preferably camera's **secondary stream** is used as a SA **live_stream** source, **primary stream** is used as a SA **image_stream** source.

- Line 25: `datasourceConfig\providedDatasource\services\subscription-service/v1/subscriptions`: *Datapoints*, *quality* and *messageID* attributes need to match in **sensoradapter config** and **Consumer application metaconfig**.
- Line 27: `datasourceConfig\providedDatasource\services\subscription-service/v1/subscriptions\datapoints`: In order to read the **image stream**, subscribe to "*image*" **datapoint**, along with filling in `driver_config` with *image_rtsp_source*.

Note: As in the later scenarios you'll see, in case you want to read the *live stream*, subscribe to the "**livestream**" **datapoint**, along with filling in `driver_config` with *livestream_rtsp_source*.

- Line 32: `datasourceConfig\providedDatasource\services\subscription-service/v1/subscriptions\datapoints`: *timestamp* value is for internal use only! As of version 0.2.0, this attribute represents a timestamp of the sensor payload.
- Line 35: `datasourceConfig\providedDatasource\services\subscription-service/v1/subscriptions\datapoints`: You can get some PTZ parameters from the camera like **pan**, *tilt*, and *zoom*. However, these are not implemented yet (as of version 0.4.1).
- Line 38: `datasourceConfig\providedDatasource\services\subscription-service/v1/subscriptions\datapoints`: **sensoradapter_subscription_message_count** represents the sequence number of the message related to the subscription.
- Line 43: `datasourceConfig\providedDatasource\services\subscription-service/v1/subscriptions\quality`: You can set the sampling frequency in the given format. Supports up to 5 messages per second (*sensor_200ms*). One message can contain 1 **imagestream** image, and a sequence of images for the **livestream** corresponding to the time elapsed since the previous message.
- Line 48: `datasourceConfig\providedDatasource`: **type** specifies the driver to be used in the sensor adapter for the given data-source. In this case, "*camera*" is a driver supporting IP cameras with h264 streams over RTSP.
- Line 53: `lifecycleConfig\appStart`: In case you want to manually start your application, set **appStart** to *false*. For automatic start, please set the value to *true*.
- Line 58: `system_service`: As Sensor Adapter is not a system application, this attribute needs to be "*false*".

Consumer application metaconfig - Example #1

```

{
  "databusConfig": {
    "connectionstring": "rnd:databus.databus.indapp-net.industrialedge.io:8883",
    "credentials": {
      "password": "",
      "username": ""
    },
    "permissions": []
  },
  "datasourceConfig": {
    "requiredDatasource": [
      {
        "datasourceId": "ExampleCamera",
        "meta": {
          "driver_parameters": {}
        },
        "services": {
          "subscription-service/v1": {
            "subscriptions": [
              {
                "datapoints": [
                  {
                    "address": "image"
                  },
                  {
                    "address": "timestamp"
                  },
                  {
                    "address": "pan"
                  },
                  {
                    "address": "sensoradapter_subscription_message_count"
                  }
                ],
                "messageId": "ExampleCamera1",
                "messageName": "example_camera_image",
                "quality": "sensor_500ms"
              }
            ]
          }
        },
        "type": "camera"
      }
    ]
  },
  "machineConfig": {
    "subscriptions": {}
  },
  "lifecycleConfig": {
    "appStart": false
  },
  "system_service": false
}

```

Consumer application metaconfig - Explanation #1

- Line 13: `datasourceConfig\requiredDatasource\datasourceId`: Connect to the camera (**ExampleCamera**) defined in *Sensoradapter metaconfig* (*providedDatabases*).
- Line 19: `datasourceConfig\requiredDatasource\services\subscription-service/v1\subscriptions`: *Datapoints*, *quality* and *messageId* attributes need to match in *Sensoradapter metaconfig* and *client config*.
- Line 23: `datasourceConfig\requiredDatasource\services\subscription-service/v1\subscriptions\datapoints`: Subscribing to *image* datapoint, which is the **primary stream**.
- Line 36: `datasourceConfig\requiredDatasource\services\subscription-service/v1\subscriptions\datapoints`: While

developing the source code of the application, value of *messageName* needs to be included in *messageIdList* when registering Consumer on Databus.

Scenario 2 - Connect to 1 camera using its primary (FullHD, 0.5 fps) and its secondary (VGA, 15 fps) stream

Sensoradapter metaconfig - Example #2

```
{
  "databusConfig": {
    "connectionstring": "rnd:databus.databus.indapp-net.industrialedge.io:8883",
    "credentials": {
      "password": "",
      "username": ""
    },
    "permissions": []
  },
  "datasourceConfig": {
    "providedDatasource": [
      {
        "datasourceId": "ExampleCamera",
        "meta": {
          "driver_parameters": {
            "image": {
              "rtsp_username": "[username]",
              "rtsp_password": "[password]",
              "rtsp_url": "[rtsp://<camera_ip_address>[:rtsp_port][/path/to/image]"
            },
            "livestream": {
              "rtsp_username": "[username]",
              "rtsp_password": "[password]",
              "rtsp_url": "[rtsp://<camera_ip_address>[:rtsp_port][/path/to/livestream]"
            },
            "buffer_size": [max_frame_count]
          }
        }
      }
    ],
    "services": {
      "subscription-service/v1": {
        "subscriptions": [
          {
            "datapoints": [
              {
                "address": "image"
              },
              {
                "address": "timestamp"
              },
              {
                "address": "pan"
              },
              {
                "address": "sensoradapter_subscription_message_count"
              },
              {
                "address": "livestream"
              }
            ],
            "merge": true,
            "messageId": "ExampleCamera1",
            "quality": "sensor_2000ms"
          }
        ]
      }
    }
  }
}
```

```

    }
  },
  "type": "camera"
}
]
},
"lifecycleConfig": {
  "appStart": false
},
"machineConfig": {
  "subscriptions": {}
},
"system_service": true
}

```

Sensoradapter metaconfig - Explanation #2

- Line 15: `datasourceConfig\providedDatasource\meta\driver_parameters`: In order to use **image-** and **live streams** at the same time, fill in `driver_parameters` according to the above demonstrated format. The `buffer_size` parameter defines the maximum number of images in the livestream buffer. `buffer_size=-1` turns off the buffer limit. The default value is 300 (if the parameter is not set). A true value from the configuration can look like this:

```

"driver_parameters": {
  "image": {
    "rtsp_username": "myuser",
    "rtsp_password": "myStr0ngPassword",
    "rtsp_url": "rtsp://192.168.1.100:554/channel_1"
  },
  "livestream": {
    "rtsp_username": "myuser",
    "rtsp_password": "myStr0ngPassword",
    "rtsp_url": "rtsp://192.168.1.100:554/channel_2"
    "buffer_size": 180
  }
}
}

```

- Line 35: `datasourceConfig\requiredDatasource\services\subscription-service/v1\subscriptions\datapoints`: Don't forget to subscribe to `"image"` datapoint, as you want to use **image stream**.
- Line 47: `datasourceConfig\requiredDatasource\services\subscription-service/v1\subscriptions\datapoints`: Don't forget to subscribe to `"livestream"` datapoint, as you want to use **live stream**.
- Line 52: `datasourceConfig\requiredDatasource\services\subscription-service/v1\subscriptions\quality`: For example 0.5 messages per second set as sampling rate. A true value from the configuration can look like this:

Consumer application metaconfig - Example #2

```

{
  "databusConfig": {
    "connectionstring": "rnd:databus.databus.indapp-net.industrialedge.io:8883",
    "credentials": {
      "password": "",
      "username": ""
    },
    "permissions": []
  },
  "datasourceConfig": {
    "requiredDatasource": [
      {
        "datasourceId": "ExampleCamera",
        "meta": {
          "driver_parameters": {}
        },
        "services": {
          "subscription-service/v1": {
            "subscriptions": [
              {
                "datapoints": [
                  {
                    "address": "image"
                  },
                  {
                    "address": "timestamp"
                  },
                  {
                    "address": "pan"
                  },
                  {
                    "address": "sensoradapter_subscription_message_count"
                  },
                  {
                    "address": "livestream"
                  }
                ],
                "messageId": "ExampleCamera1",
                "messageName": "example_camera_image",
                "quality": "sensor_2000ms"
              }
            ]
          }
        },
        "type": "camera"
      }
    ]
  },
  "machineConfig": {
    "subscriptions": {}
  },
  "lifecycleConfig": {
    "appStart": false
  },
  "system_service": false
}

```

Scenario 3 - Connect to 2 cameras using:

- Camera 1 primary (FullHD, 0.5 fps) and secondary (VGA, 15 fps) streams
 - Camera 2 secondary (VGA, 15 fps) stream
-

Sensoradapter metaconfig - Example #3

```
{
  "databusConfig": {
    "connectionstring": "rnd:databus.databus.indapp-net.industrialedge.io:8883",
    "credentials": {
      "password": "",
      "username": ""
    },
    "permissions": []
  },
  "datasourceConfig": {
    "providedDatasource": [
      {
        "datasourceld": "ExampleCamera",
        "meta": {
          "driver_parameters": {
            "image": {
              "rtsp_username": "[username]",
              "rtsp_password": "[password]",
              "rtsp_url": "[rtsp://]<camera_ip_address>[:rtsp_port]/[path/to/image]"
            },
            "livestream": {
              "rtsp_username": "[username]",
              "rtsp_password": "[password]",
              "rtsp_url": "[rtsp://]<camera_ip_address>[:rtsp_port]/[path/to/livestream]"
            }
          }
        },
        "buffer_size": [max_frame_count]
      }
    ],
    "services": {
      "subscription-service/v1": {
        "subscriptions": [
          {
            "datapoints": [
              {
                "address": "image"
              },
              {
                "address": "timestamp"
              },
              {
                "address": "pan"
              },
              {
                "address": "livestream"
              },
              {
                "address": "sensoradapter_subscription_message_count"
              }
            ],
            "merge": true,
            "messageld": "ExampleCamera1",
            "quality": "sensor_2000ms"
          }
        ]
      }
    },
    "type": "camera"
  },
  {
    "datasourceld": "OtherExampleCamera",
    "meta": {
      "driver_parameters": {
        "livestream": {
          "rtsp_username": "[username]",
          "rtsp_password": "[password]",

```

```

    "rtsp_url": "[rtsp://]<camera_ip_address>[:rtsp_port][/path/to/livestream]"
    "buffer_size": [max_frame_count]
  }
}
},
"services": {
  "subscription-service/v1": {
    "subscriptions": [
      {
        "datapoints": [
          {
            "address": "timestamp"
          },
          {
            "address": "pan"
          },
          {
            "address": "livestream"
          },
          {
            "address": "sensoradapter_subscription_message_count"
          }
        ],
        "merge": true,
        "messageId": "OtherExampleCamera1",
        "quality": "sensor_2000ms"
      }
    ]
  },
  "type": "camera"
}
],
},
"lifecycleConfig": {
  "appStart": false
},
"machineConfig": {
  "subscriptions": {}
},
"system_service": true
}

```

Sensoradapter metaconfig - Explanation #3

- Line 13: `datasourceConfig\providedDatasource\datasourceId`: The first camera instance, called `"ExampleCamera"`.

Note: In order to use both camera instances, you have to subscribe to both `datasourceIDs` (see: line 47).

- Line 15: `datasourceConfig\providedDatasource\meta\driver_parameters`: A true value from the configuration can look like this:

```

"driver_parameters": {
  "image": {
    "rtsp_username": "myuser",
    "rtsp_password": "myStr0ngPassword",
    "rtsp_url": "rtsp://192.168.1.100:554/channel_1"
  },
  "livestream": {
    "rtsp_username": "myuser",
    "rtsp_password": "myStr0ngPassword",
    "rtsp_url": "rtsp://192.168.1.100:554/channel_2"
  }
}

```

Note: The `livestream_buffer_size` parameter is missing, so its value will be the default 300.

- Line 60: `datasourceConfig\providedDatasource\datasourceId`: The second camera instance, in this example called "*OtherExampleCamera*".
- Line 62: `datasourceConfig\providedDatasource\meta\driver_parameters`: **Live stream** can be used independently from **image stream**. A true value from the configuration can look like this:

```
"driver_parameters": {  
  "livestream": {  
    "rtsp_username": "myuser",  
    "rtsp_password": "myStr0ngPassword",  
    "rtsp_url": "rtsp://192.168.1.99:554/Streaming/Channels/102"  
    "buffer_size": 180  
  }  
}
```

Note: The IP address necessarily differs from the first camera instance (*see: line 15.*). The camera manufacturer can also differ, so the `/path/to/livestream` can be different.

- Line 83: `datasourceConfig\providedDatasource\services\subscription-service/v1/subscriptions/datapoints`: Datapoint for the **livestream** used as a source for consumer apps.

Consumer_1 application metaconfig - Example #3/1

```

{
  "databusConfig": {
    "connectionstring": "rnd:databus.indapp-net.industrialedge.io:8883",
    "credentials": {
      "password": "",
      "username": ""
    },
    "permissions": []
  },
  "datasourceConfig": {
    "requiredDatasource": [
      {
        "datasourceId": "ExampleCamera",
        "meta": {
          "driver_parameters": {}
        },
        "services": {
          "subscription-service/v1": {
            "subscriptions": [
              {
                "datapoints": [
                  {
                    "address": "image"
                  },
                  {
                    "address": "timestamp"
                  },
                  {
                    "address": "pan"
                  },
                  {
                    "address": "sensoradapter_subscription_message_count"
                  },
                  {
                    "address": "livestream"
                  }
                ],
                "messageId": "ExampleCamera1",
                "messageName": "example_camera_image",
                "quality": "sensor_2000ms"
              }
            ]
          }
        },
        "type": "camera"
      }
    ],
    "machineConfig": {
      "subscriptions": {}
    },
    "lifecycleConfig": {
      "appStart": false
    },
    "system_service": false
  }
}

```

Consumer_2 application metaconfig - Example #3/2

```

{
  "databusConfig": {
    "connectionstring": "rnd:databus.indapp-net.industrialedge.io:8883",
    "credentials": {
      "password": "",
      "username": ""
    },
    "permissions": []
  },
  "datasourceConfig": {
    "requiredDatasource": [
      {
        "datasourceId": "OtherExampleCamera",
        "meta": {
          "driver_parameters": {}
        },
        "services": {
          "subscription-service/v1": {
            "subscriptions": [
              {
                "datapoints": [
                  {
                    "address": "timestamp"
                  },
                  {
                    "address": "pan"
                  },
                  {
                    "address": "livestream"
                  },
                  {
                    "address": "sensoradapter_subscription_message_count"
                  }
                ],
                "merge": true,
                "messageId": "OtherExampleCamera1",
                "messageName": "other_example_camera_image",
                "quality": "sensor_2000ms"
              }
            ]
          }
        },
        "type": "camera"
      }
    ]
  },
  "machineConfig": {
    "subscriptions": {}
  },
  "lifecycleConfig": {
    "appStart": false
  },
  "system_service": false
}

```

Non-functional requirements (NFRs)

Sensor Adapter's performance is measured by its latency on the databus's consumer (customer's application) side. The sensoradapter indapp has two versions that differ only in the amount of resources that can be used. The SA 1CPU version limited to 100% of CPU, the SA 2CPU version can use 200% CPU (a max CPU value is 400% in a box with 4 CPU cores). RAM limit is 512 MB in both cases. The image processing performance is highly dependent on:

- the hardware configuration (nanobox, picobox or microbox is used)
- the **camera** configuration (primary & secondary RTSP stream's resolution and fps values)
- The Sensor Adapter's configuration (quality, buffer size)
- The one- or two-CPU **version** of SA is used

			NANOBOX		PICOBX		MICROBOX	
			average latency (ms)					
			image	live	image	live	image	live
Sensoradapter_0.5.2-1CPU	NFR_BASIC Camera1: image: 1920*1080 5 fps live: 704*576 15 fps	consumer1	939	1652	733	1443	477	1261
	NFR_MAX_LOAD Camera1&2: image: 1920*1080 5 fps live: 704*576 15 fps	consumer1	3120	3758	2749	3638	950	1545
		consumer2	3240	4056	2681	3554	945	1543
Sensoradapter_0.5.2-2CPU	NFR_BASIC Camera1: image: 1920*1080 5 fps live: 704*576 15 fps	consumer1	760	1540	580	1365	480	1231
	NFR_MAX_LOAD Camera1&2: image: 1920*1080 5 fps live: 704*576 15 fps	consumer1	1640	2230	798	1661	518	1298
		consumer2	1650	2180	815	1705	508	1288

> *Latency measured with camera settings when primary stream values are equal to image stream values, and camera's secondary stream values are equal to live stream settings. Higher fps values provided by camera than required by the sensoradapter, will cause decrease in performance because of extra load on sensoradapter at the preprocess phase.*

> * __Example: __ if your application will use 800x600 resolution images in every 10 seconds, then **do not use** higher resolution (for example wqhd (2560 x 1440)) and higher framerate (for example 60 fps) settings on the camera side, because it will consume unnecessary CPU-time on Edgebox. Try to set-up the camera to minimal data output regarding to your actual usecase (800x600 pixel @ 0.1 fps).*

ET200 Sensor Adapter

Introduction

The ET200 Sensor Adapter application allows the user to collect low / high frequency sensor data from the matching configuration of the of the Siemens SIMATIC ET 200SP analog and / or digital interfaces. The gathered sensor information is provided through databus in a merged comma-separated values (csv) file for further analysis in any appropriate application. In this documentation for example we assume that you are using Analyze My Workpiece /Capture4Analysis for receiving output data.

This documentation presents only the installation and use of a possible solution from the countless variations. In our example, the system supports 4 analog channels with 10 kHz sampling rate separately, and 8 digital channels at 2 kHz each, plus a PT100 resistance thermometer at maximum 2 kHz sampling rate. All the hardware requirements and configurations are reflecting to this exemplified setup. ET200 Sensor Adapter was thoroughly tested and measured with the corresponding configuration.

Experimental: Optionally the collected data can be combined with the Sinumerik Adapter HF data in one, time-synchronized JSON output. For that, you additionally need to use "ET200_sensor_timesync" and "ntp_server" applications. Current version of the timesync app was not tested on many ET200 configurations. This documentation will help you test the feature, but if not interested, you can skip NCU- and timesync-specific paragraphs.

Hardware requirements

SIMATIC ET 200SP:

Component	Name	Article number	Single parts	Unit	Quantity
ET 200SP	DIN rail 35 mm, length: 483 mm, for 19" cabinets	6ES710-8MA11	1	Pieces	1
ET 200SP Power <i>(optional)</i>	SIMATIC ET 200SP PS, 1-phase, 24 V DC / 5 A	6EP7133-6AB00-0BNO	1	Pieces	1
ET 200SP CPU	CPU 1512SP-1 PN	6ES7512-1DK01-0AB0	1	Pieces	1
ET 200SP CPU	Memory card, 12 MB	6ES7954-8LE03-0AA0	1	Pieces	1
ET 200SP CPU	BusAdapter 2xRJ45	6ES7193-6AR00-0AA0	1	Pieces	1
ET 200SP I/O Interface Module	IM 155-6 PN HF/2 V4.2	6ES7155-6AU01-0CN0	1	Pieces	1
ET 200SP I/O Interface Module	AI 2xUI/ 2I4-wire HS	6ES7134-6HB00-0DA1	1	Pieces	2
ET 200SP analog input module	ET 200SP AI 4XRTD/TC 2-/3-/4-WIRE HF	6ES7134-6JD00-0CA1	1	Pieces	1
ET 200SP digital input module	DI 8x 24 V DC High Speed	6ES7131-6BF00-0DA0	1	Pieces	1
ET 200SP I/O Interface Module	BusAdapter 2xRJ45	6ES7193-6AR00-0AA0	1	Pieces	1
ET 200SP I/O Interface Module	BU type A0, push-in terminals, without aux. terminals, new load group	6ES7193-6BP00-0DA0	1	Pieces	2
ET 200SP I/O Interface Module	BU type A0, Push-in terminals, without AUX terminals, bridged to the left	6ES7193-6BP00-0BA0	1	Pieces	2
Non-configured articles	PROFINET strain relief (5 units)	6ES7193-6RA00-1AN0	4	Package	1
Individual / network article	IE TP cord RJ45/RJ45, 4x2, 0.5 m	6XV1870-3QE50	1	Pieces	1

Hint: The above configuration supports 4 analog, 8 digital and a analog PT100 thermometer, but regarding the actual use case it can be freely customized.

Various analog and digital sensors

It is possible to attach numerous of various sensors to the ET 200SP. Vibration sensors, accelerometers, thermometers, noise dosimeters, light sensors etc.

Specifically supported PT100 resistance thermometer

The ET 200SP analog interface specifically supports different resistance thermometers ([see documentation here](#)).

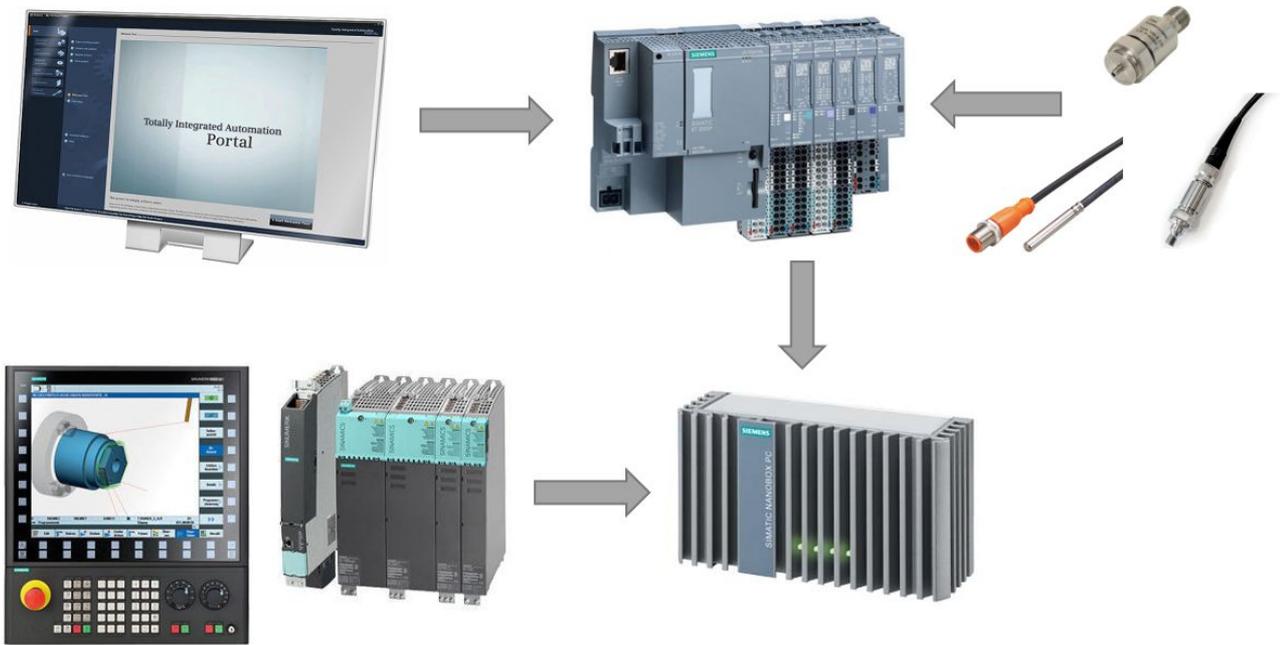
In the described use case, the [ifm electronic TS2289](#) was used.

Prerequisites:

- Industrial Edge for Machine Tools IPC: [nanobox SIMATIC IPC227E](#) or [microbox SIMATIC IPC427E](#)
 - A Windows PC with [TIA portal](#) installed
 - A *Sinumerik NCU* connected and configured to the *Sinumerik Adapter* on Industrial Edge for Machine Tools IPC (Optional, if using the experimental *timesync* app)
-

SIMATIC ET 200SP hardware configuration and wiring diagram

Schematic illustration of components



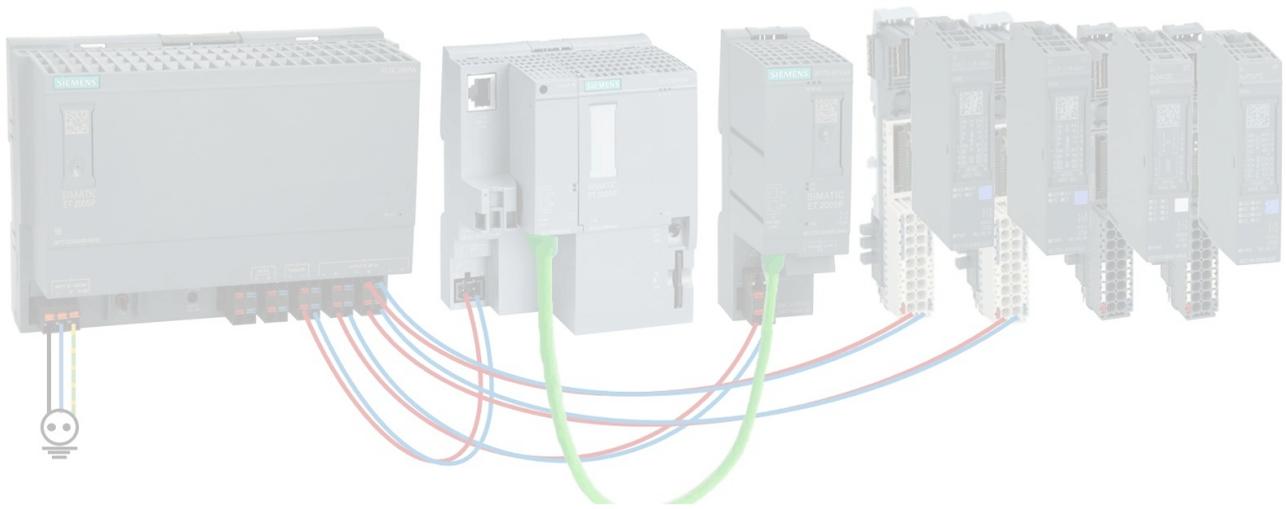
Wiring the EdgeBox & the SINUMERIK 840D sl

[Check the wiring here.](#)

Note: Network switch necessary when using NCU and ET200

Wiring of the SIMATIC ET 200SP components

The following figure shows the ET 200SP components and their basic wiring without the sensor connections. The black/blue/yellow-green cables are connected to the main power source (EU AC230V/50Hz). The red/blue wires are the DC24V power cords to power the peripherals. The thick green cable is a RJ45/RJ45 Profinet cable. All components are mounted on a top-hat rail. It is important to use server modules as termination for the backplane bus.



To connect a sensor to a digital or analog interface, please refer the appropriate interface modul's user manual. For an example, the 4-wire PT100 resistance thermometer is connected to the High Feature analog interface like this:



Note: During operation the overall assembled configuration looks [like this](#).

Commissioning Industrial Edge for Machine Tools

[Installation](#) of the operating system on IPC

[Connecting](#) to the Insights Hub

Installation of the indapps

To use the ET200 Sensor Adapter, various Edge apps are required. These apps can be installed on the Edge via the Insights Hub *Manage MySINUMERIK Edge App Management* application. The [Application Management guide](#)

provides help for installing and configuring Edge Apps. For the best result, please download the latest productive app version available in App Management.

Tip: To ensure a fast and smooth installation, all Edge Apps should be added one after the other (same for the installation of the app instances). Otherwise, the installation process may be disrupted.

App Overview

AppName	Version	Description
adapterframework	5.2.0-004	AdapterFramework is a component for managing installed device adapters and App to App communication.
sinumerikadapter	7.0.0-004	SinumerikAdapter is a component for managing access to SINUMERIK 840Dsl or SINUMERIK ONE for getting low frequency and high frequency data from controller.
ntp_server	V2.0.2	Provides an NTP server on the machinelan interface port 123, using the local time on the EdgeBox.
ET200_sensor_adapter	V1.0.0	Adapter application for ET200 based sensor data acquisition solutions. Supporting multiple analog and digital input modules.
ET200_sensor_timesync	0.8.0	Provides Sinumerik HF Data extended with sensor data from ET200 Sensor Adapter synchronized on timestamps. The synchronization is done on the timestamps provided by the NCU and the ET 200SP. Please make sure that these devices have the same time. You can use ET200_ntp_server as an option to provide an NTP server accessible to both the NCU and the ET 200SP device.
amw4analysis	v2.3.0.0.12	Analyze My Workpiece \Capture4Analysis is a Industrial Edge for Machine Tools application which enables the user to acquire data from the SINUMERIK CNC controller, store it, and share it to both SIEMENS or any other application.

Configuration of the Indapps

For error-free use of the apps, various parameters must be adjusted in the app settings. For configuration, the app can be started on the Edge. The configuration is done in a JSON editor of the App Management ([Configuration of Indapps](#)). Further information on the JSON file format is available at the following [link](#).

ET200_sensor_timesync:

The "ET200_sensor_timesync" application can be configured through Insights Hub. The configuration stored in JSON format, a sample file with explanation [is here](#).

ET200 Sensor Adapter:

Beside the possibility to configure on the Insights Hub, the ET200 Sensor Adapter application has a standalone graphical configurator user interface. Please read the *ET200 Sensor Adapter Configurator* [documentation here](#).

Commissioning HF Probe and EdgeFs on the NCU

To be able to use the HF functionality on a SINUMERIK control, additional software [must be installed](#) on the SINUMERIK NCU.

TIA portal configuration

Procedure

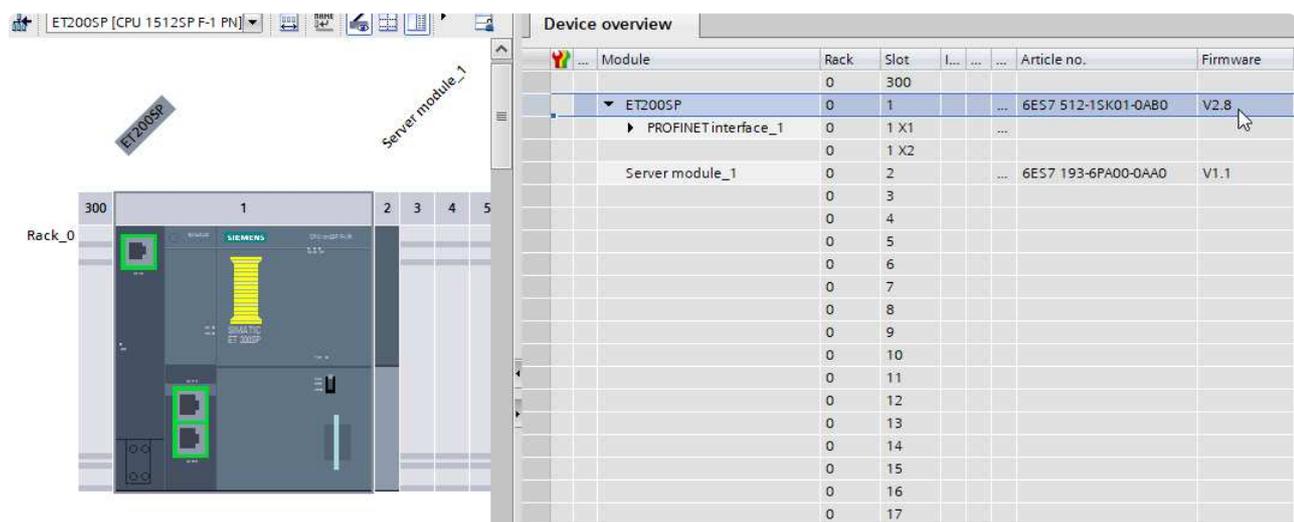
1. Load preconfigured project into TIA Portal V16

Importing the TIA project on a Windows 10 based PC with preinstalled TIA Portal is so simple that you just have to double-click on the project file. The project contains the expected ET 200SP configuration, yet, smaller differences are possible, for example, in the physical order or number of the installed interfaces. You have to modify the project according to the real ET 200SP configuration.

Hint: The application download folder contains a V16 project file, which can be imported and used under TIA Portal version V17 and V18 too.

2. Check Hardware configuration:

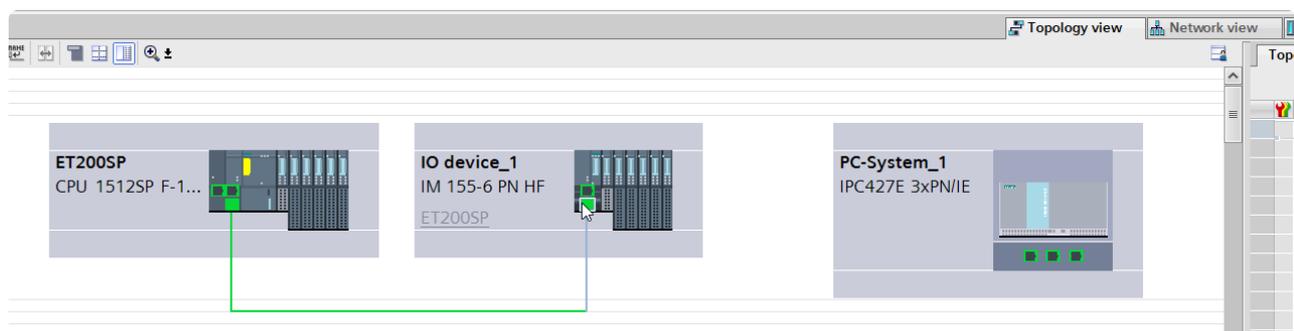
a. **Devices & networks -> Device overview:** Do the used Hardware modules match those in the TIA project? (Article number, firmware version)



The screenshot shows the 'Device overview' window in TIA Portal. On the left, a rack diagram shows an ET200SP module in slot 1 and a Server module_1 in slot 2. On the right, a table lists the modules:

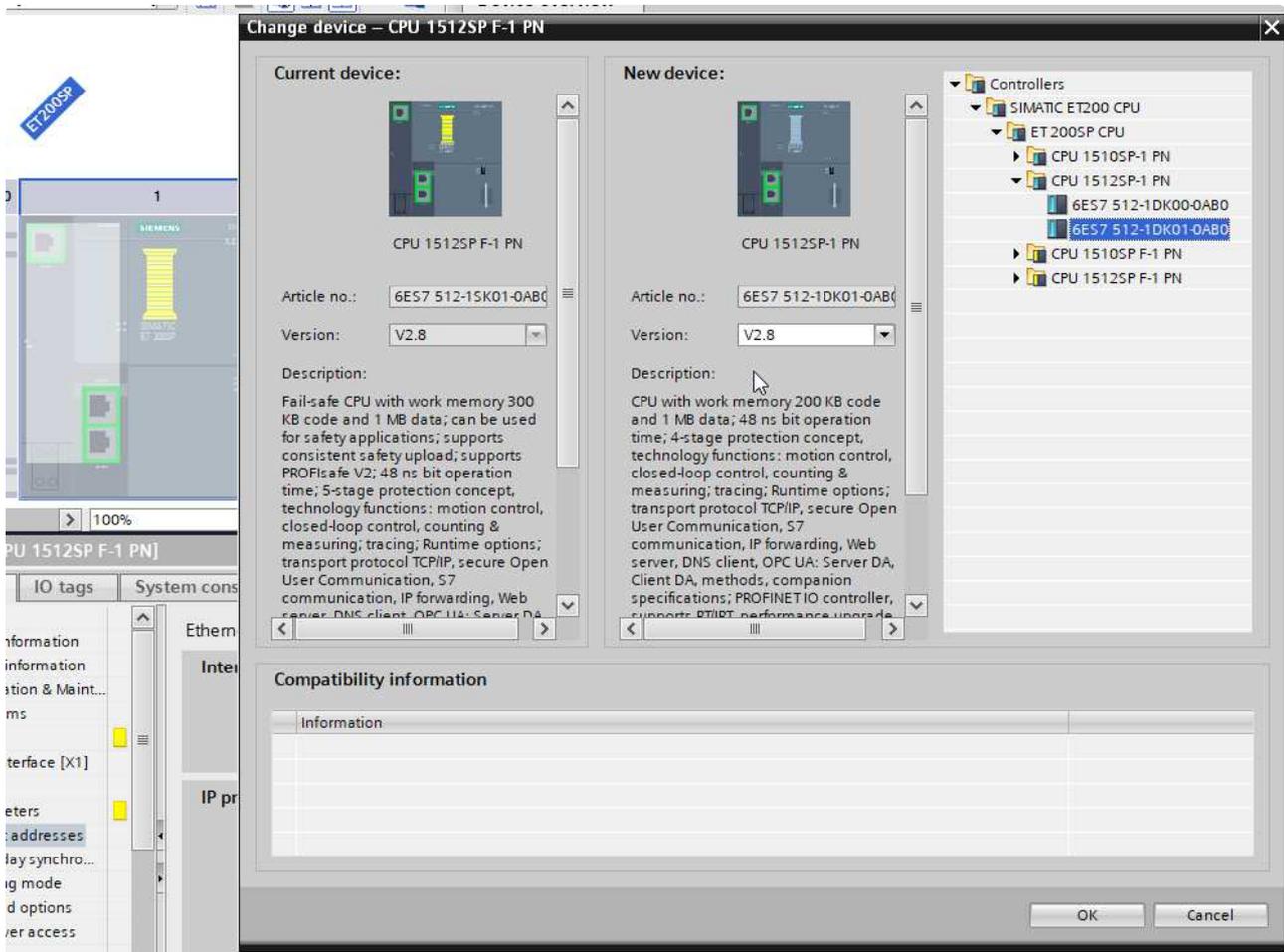
Module	Rack	Slot	I...	...	Article no.	Firmware
ET200SP	0	300				
PROFINET interface_1	0	1	X1		6ES7 512-1SK01-0AB0	V2.8
Server module_1	0	2	X2		6ES7 193-6PA00-0AA0	V1.1
	0	3				
	0	4				
	0	5				
	0	6				
	0	7				
	0	8				
	0	9				
	0	10				
	0	11				
	0	12				
	0	13				
	0	14				
	0	15				
	0	16				
	0	17				

b. **Devices & networks: Topology view:** Are the ports connected correctly? (No deviations are allowed here)



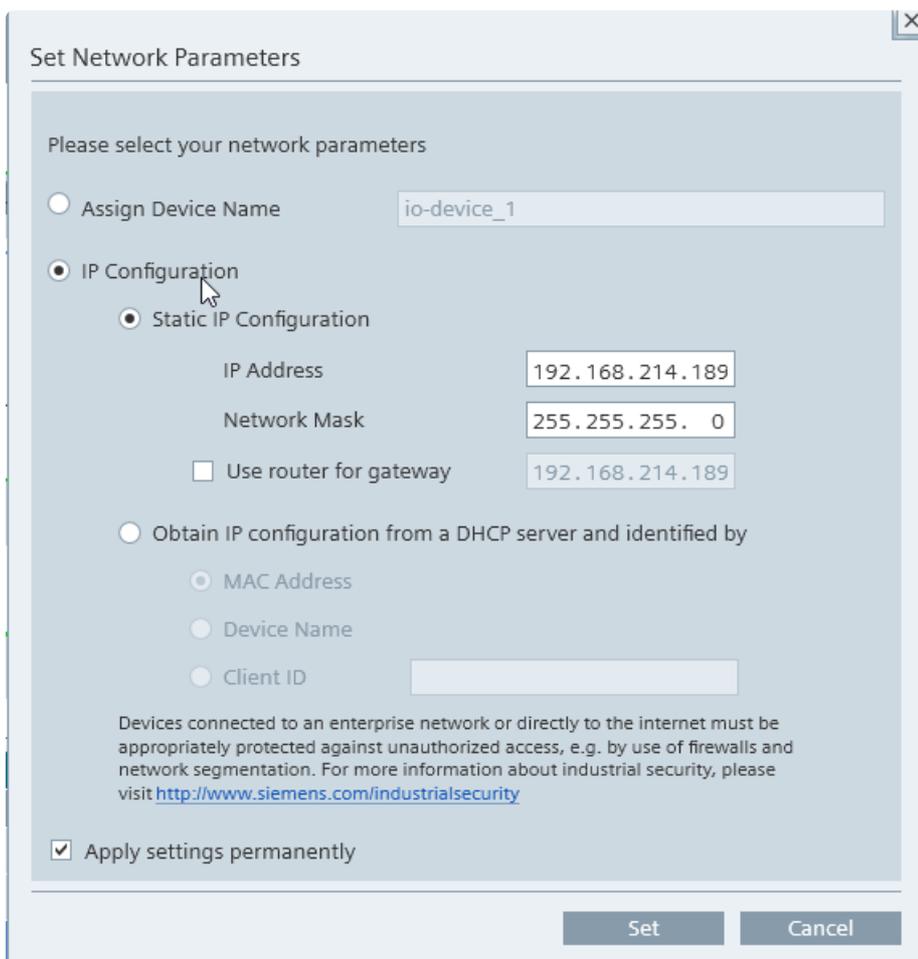
c. **Online accesses -> Display reachable nodes -> Network Analysis:** Do the IP addresses and PROFINET names of the reachable network nodes match those projected in the TIA project?

Projected IP configuration (Device -> Properties -> PROFINET interface [X1]):



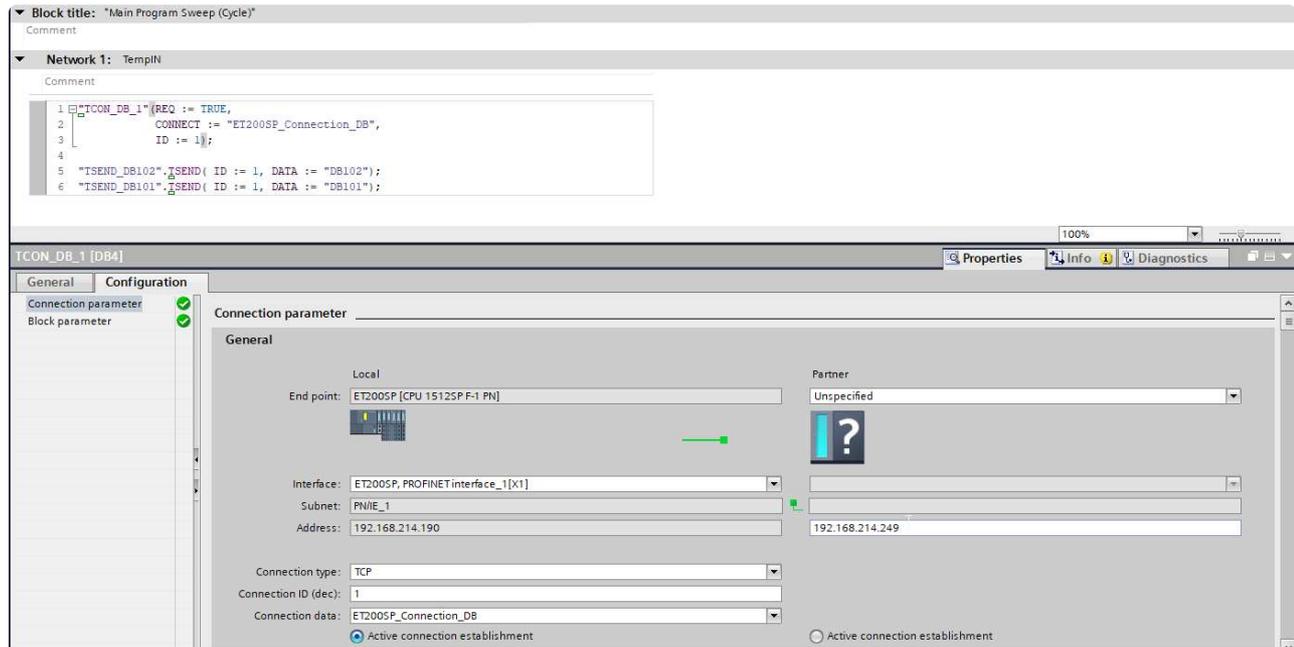
b. Adjust wiring if ports do not match those in the project

c. Adapt IP addresses and PROFINET names of the accessible nodes to TIA project



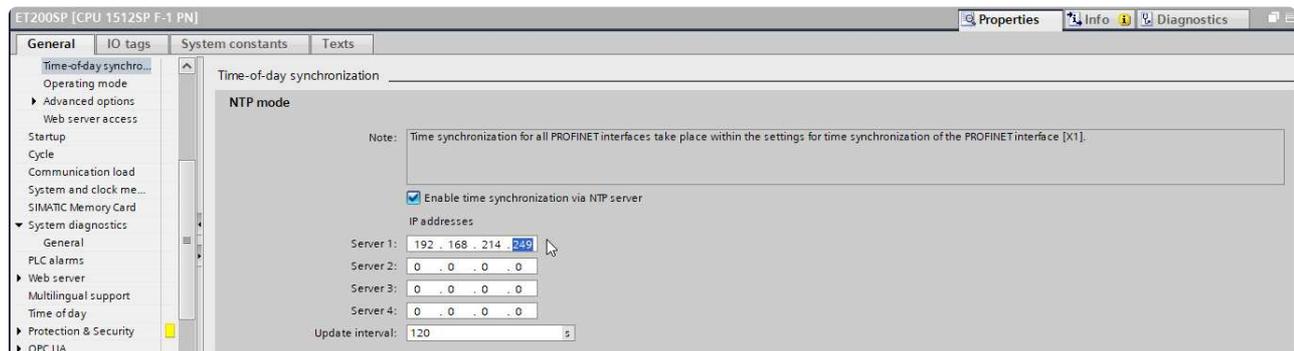
4. Configure IP address of data transmission in Main [OB1] -> TCON_DB_1

(IP address of connection partner needs to be the Edge's IP address)

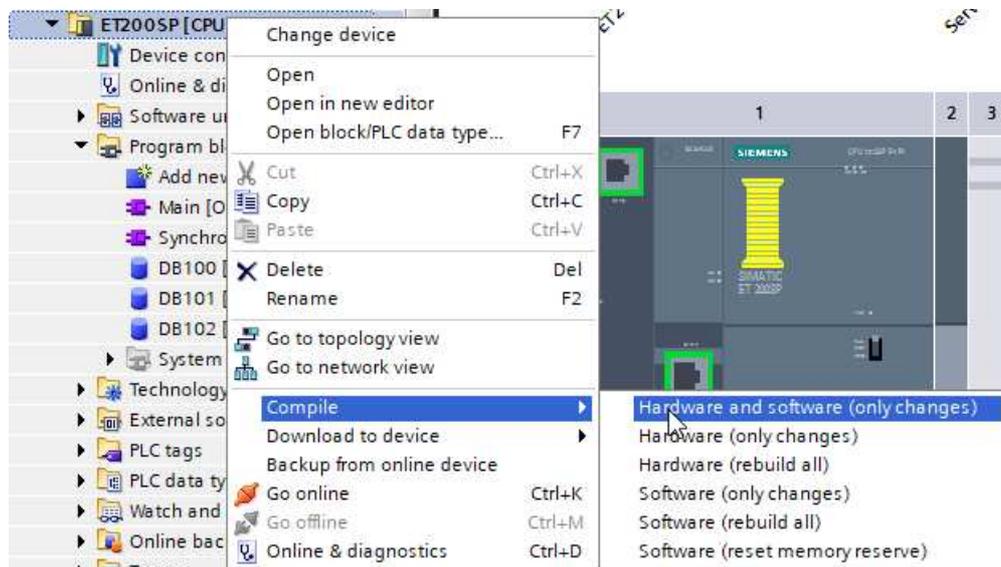


5. Select IP address of NTP time server in ET 200SP Properties | Time-of-day synchronization

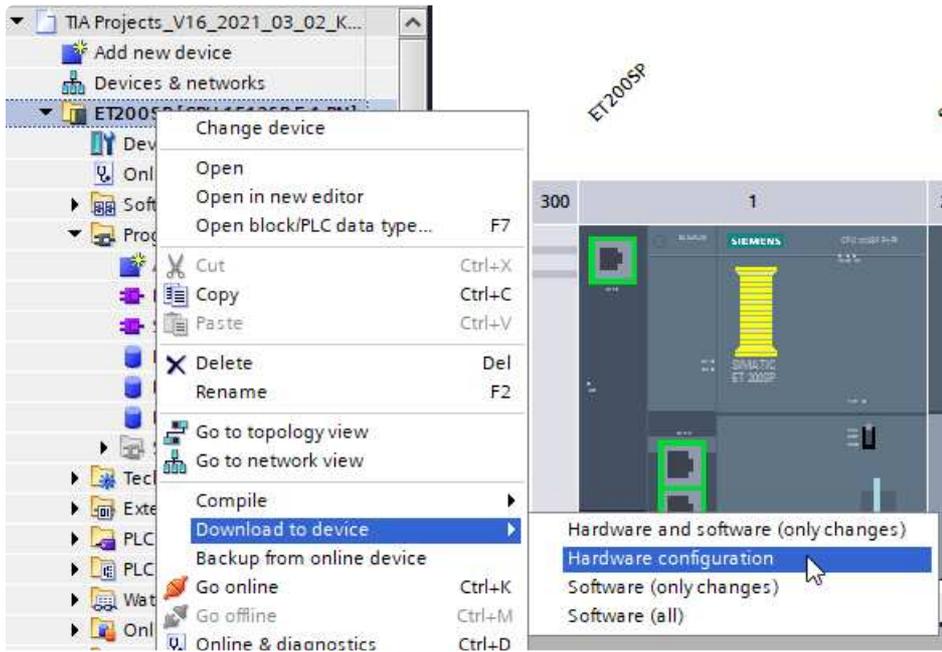
(Server 1 needs to contain the Edge's IP address)



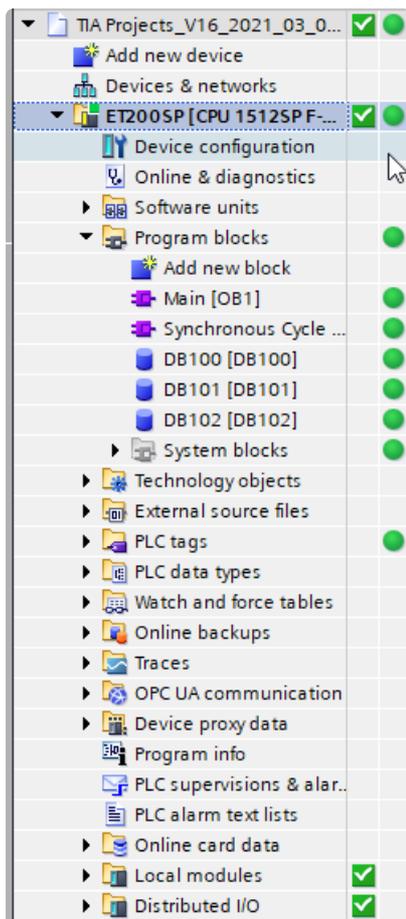
6. Compile software and hardware



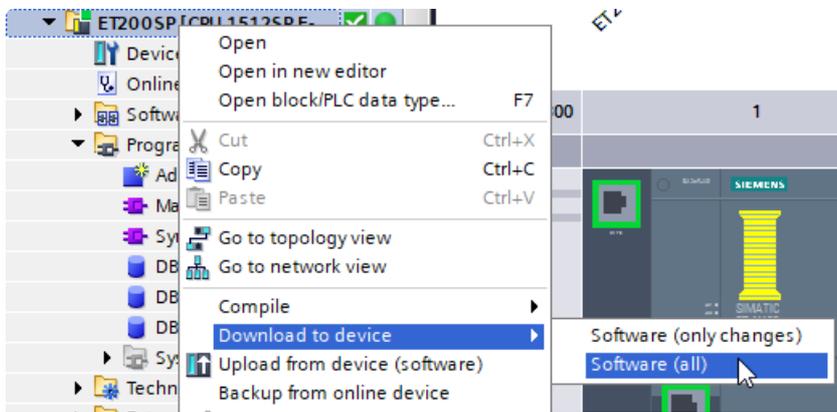
7. Load hardware configuration into controller



8. Go online and check if all devices are error free



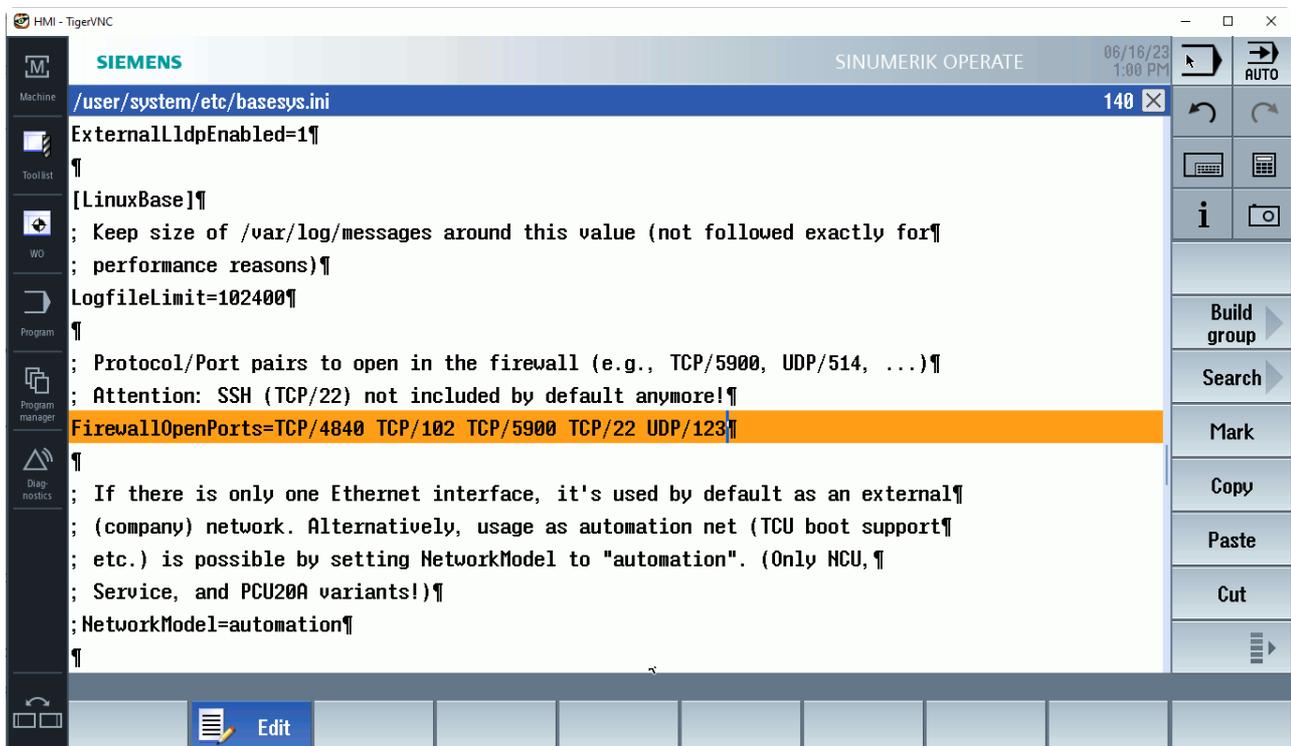
9. Load software into controller



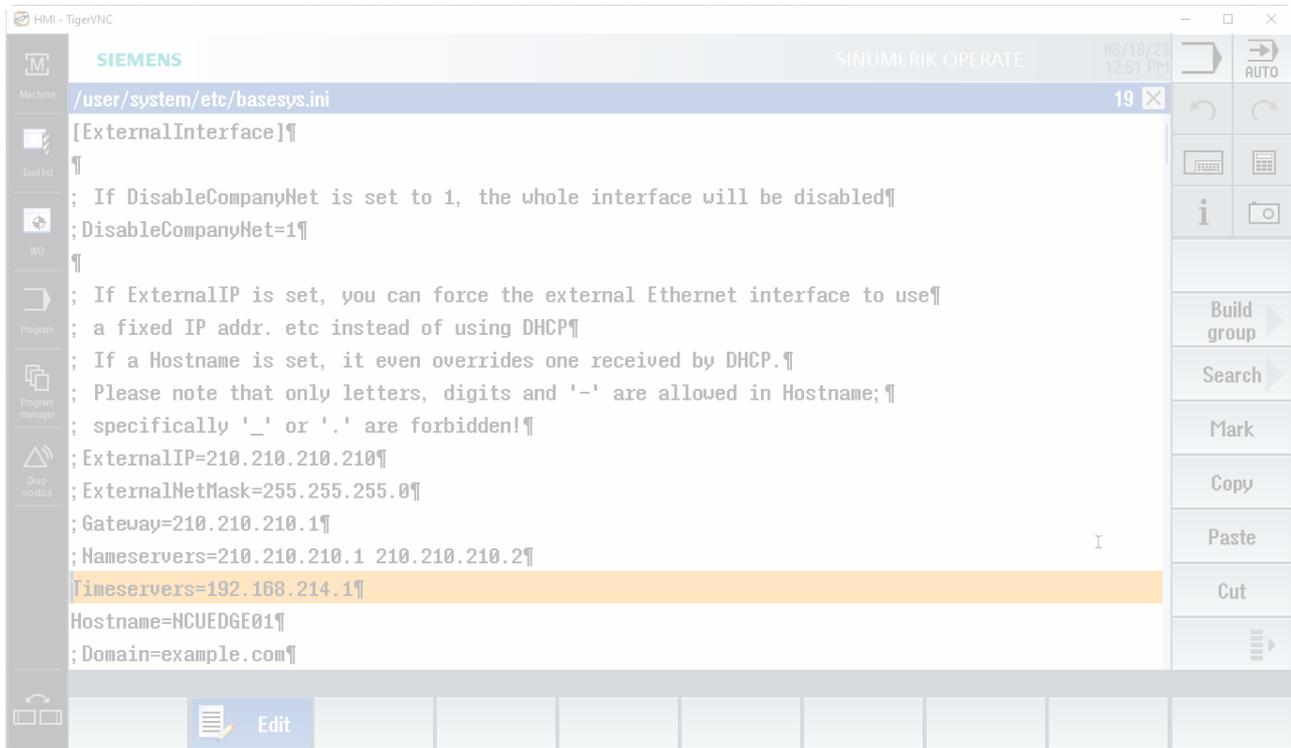
NTP setup on the NCU

To record synchronized data, all devices need to share a common system time. Therefore, the Edge Box hosts a NTP server application. If you use a PCU to operate the NCU, use the WinSCP application to access the described files. To enable the time server synchronization on the NCU, you can use the following steps:

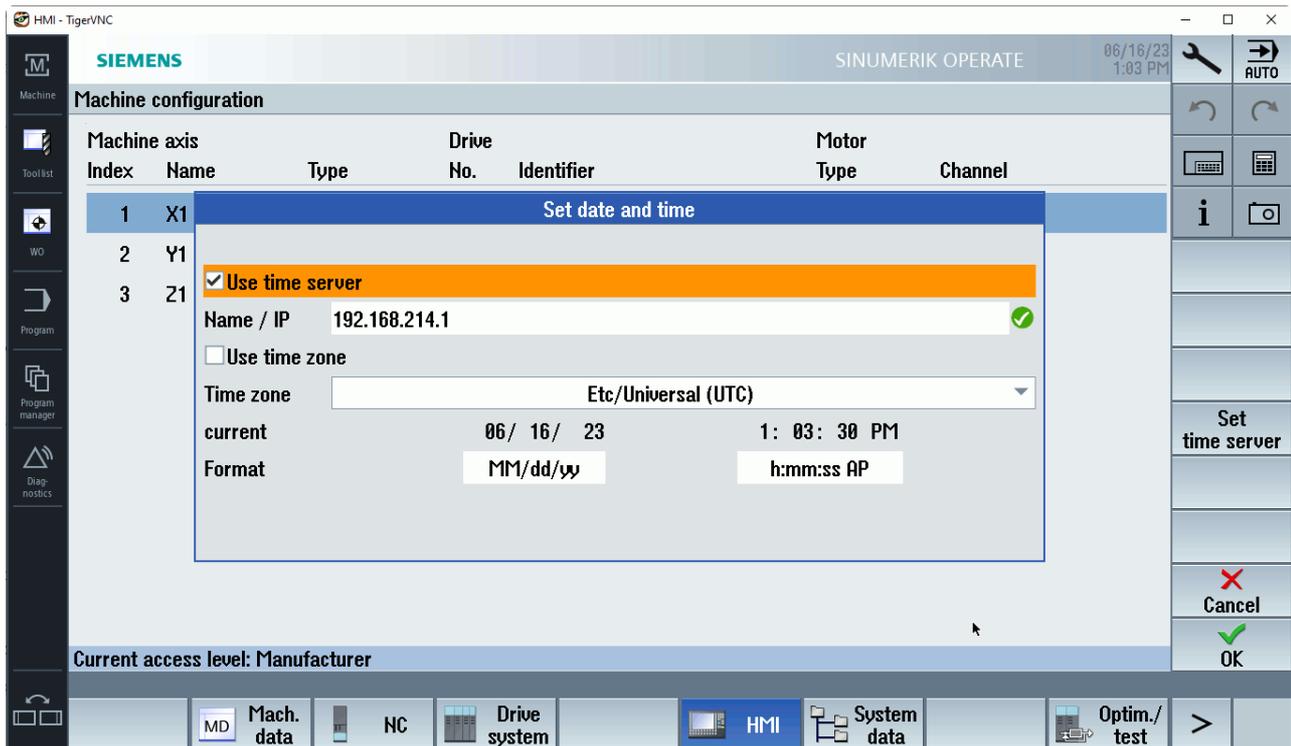
1. Go to Setup -> System data -> System CF-Card -> user -> system -> etc -> basesys.ini and open it. (WinSCP path: card/user/system/etc/basesys.ini)
2. Remove the semicolon character in front of the entry FirewallOpenPorts= "TCP/5900 TCP/102" and add the port for the timeserver (UDP/123)



3. Add the IP address of the NTP time server (Edge's IP address)



4. Restart the NCU and check the status of the time server connection (Setup -> HMI -> Date Time)



Warning: Make sure that the time synchronization is active. Green checkmark if active, red X if inactive.

Note: This option is not available on the PCU

5. If the time server is active, proceed with the Indapp checkup

Indapp checkup

Procedure

To check if all indapps are running without errors, the following steps can be performed:

1. Check whether all applications are running in the diagnostics UI

(Local Diagnostics Application UI: <https://\<box ip>:5443/diag>) under App Management

The screenshot displays the 'Edge Apps' section of a diagnostics UI. It features a list of four applications, each with a status of 'running'. The applications are:

- ET200_ntp_server** (version: 1.0.1) with buttons for 'Browse Configuration', 'Display Logs', and 'Download App Log'.
- ET200_sensor_adapter** (version: 0.8.0) with buttons for 'Browse Configuration', 'Display Logs', and 'Download App Log'.
- ET200_sensor_timesync** (version: 0.8.0) with buttons for 'Browse Configuration', 'Display Logs', and 'Download App Log'.
- amw4analysis** (version: 2.4.1.0.18-5NAPSHOT) with buttons for 'Browse Configuration', 'Open UI', 'Display Logs', and 'Download App Log'.

2. The app logs can also be checked here (Display Logs)

App Logs

a. ET200_sensor_adapter

-- Logs begin at Thu 2021-07-15 13:45:54 UTC. --

```
Jul 16 10:11:31 exenia runc[292]: 1626430289 INFO ET200_sensor_adapter : ET200 gapfilled packet Packageld/Linecount: 11058 / 2500
Jul 16 10:11:31 exenia runc[292]: 1626430289 INFO ET200_sensor_adapter : buffer 220148 (55036) 2 11059
Jul 16 10:11:31 exenia runc[292]: 1626430290 INFO ET200_sensor_adapter : ET200 gapfilled packet Packageld/Linecount: 11059 / 2500
Jul 16 10:11:31 exenia runc[292]: 1626430290 INFO ET200_sensor_adapter : buffer 220168 (55036) 1 11060
Jul 16 10:11:31 exenia runc[292]: 1626430290 INFO ET200_sensor_adapter : ET200 gapfilled packet Packageld/Linecount: 11060 / 2500
Jul 16 10:11:31 exenia runc[292]: 1626430290 INFO ET200_sensor_adapter : buffer 220188 (55036) 2 11061
Jul 16 10:11:31 exenia runc[292]: 1626430290 INFO ET200_sensor_adapter : ET200 gapfilled packet Packageld/Linecount: 11061 / 2500
Jul 16 10:11:31 exenia runc[292]: 1626430290 INFO ET200_sensor_adapter : buffer 220208 (55036) 1 11062
Jul 16 10:11:31 exenia runc[292]: 1626430290 INFO ET200_sensor_adapter : ET200 gapfilled packet Packageld/Linecount: 11062 / 2500
Jul 16 10:11:31 exenia runc[292]: 1626430291 INFO ET200_sensor_adapter : buffer 220228 (55036) 2 11063
Jul 16 10:11:37 exenia runc[292]: 1626430291 INFO ET200_sensor_adapter : ET200 gapfilled packet Packageld/Linecount: 11063 / 2500
Jul 16 10:11:37 exenia runc[292]: 1626430291 INFO ET200_sensor_adapter : buffer 220249 (55036) 1 11064
Jul 16 10:11:37 exenia runc[292]: 1626430291 INFO ET200_sensor_adapter : ET200 gapfilled packet Packageld/Linecount: 11064 / 2500
Jul 16 10:11:37 exenia runc[292]: 1626430291 INFO ET200_sensor_adapter : buffer 220269 (55036) 2 11065
Jul 16 10:11:37 exenia runc[292]: 1626430291 INFO ET200_sensor_adapter : ET200 gapfilled packet Packageld/Linecount: 11065 / 2500
Jul 16 10:11:37 exenia runc[292]: 1626430291 INFO ET200_sensor_adapter : buffer 220290 (55036) 1 11066
Jul 16 10:11:37 exenia runc[292]: 1626430291 INFO ET200_sensor_adapter : ET200 gapfilled packet Packageld/Linecount: 11066 / 2500
Jul 16 10:11:37 exenia runc[292]: 1626430292 INFO ET200_sensor_adapter : buffer 220310 (55036) 2 11067
Jul 16 10:11:37 exenia runc[292]: 1626430292 INFO ET200_sensor_adapter : ET200 gapfilled packet Packageld/Linecount: 11067 / 2500
Jul 16 10:11:37 exenia runc[292]: 1626430292 INFO ET200_sensor_adapter : buffer 220330 (55036) 1 11068
Jul 16 10:11:37 exenia runc[292]: 1626430292 INFO ET200_sensor_adapter : ET200 gapfilled packet Packageld/Linecount: 11068 / 2500
Jul 16 10:11:37 exenia runc[292]: 1626430292 INFO ET200_sensor_adapter : buffer 220350 (55036) 2 11069
Jul 16 10:11:37 exenia runc[292]: 1626430292 INFO ET200_sensor_adapter : ET200 gapfilled packet Packageld/Linecount: 11069 / 2500
Jul 16 10:11:37 exenia runc[292]: 1626430292 INFO ET200_sensor_adapter : buffer 220369 (55036) 1 11070
Jul 16 10:11:37 exenia runc[292]: 1626430292 INFO ET200_sensor_adapter : ET200 gapfilled packet Packageld/Linecount: 11070 / 2500
Jul 16 10:11:37 exenia runc[292]: 1626430293 INFO ET200_sensor_adapter : buffer 220390 (55036) 2 11071
Jul 16 10:11:37 exenia runc[292]: 1626430293 INFO ET200_sensor_adapter : ET200 gapfilled packet Packageld/Linecount: 11071 / 2500
Jul 16 10:11:37 exenia runc[292]: 1626430293 INFO ET200_sensor_adapter : buffer 220410 (55036) 1 11072
Jul 16 10:11:37 exenia runc[292]: 1626430293 INFO ET200_sensor_adapter : ET200 gapfilled packet Packageld/Linecount: 11072 / 2500
Jul 16 10:11:37 exenia runc[292]: 1626430293 INFO ET200_sensor_adapter : buffer 220431 (55036) 2 11073
Jul 16 10:11:37 exenia runc[292]: 1626430293 INFO ET200_sensor_adapter : ET200 gapfilled packet Packageld/Linecount: 11073 / 2500
Jul 16 10:11:37 exenia runc[292]: 1626430293 INFO ET200_sensor_adapter : buffer 220452 (55036) 1 11074
Jul 16 10:11:37 exenia runc[292]: 1626430293 INFO ET200_sensor_adapter : ET200 gapfilled packet Packageld/Linecount: 11074 / 2500
Jul 16 10:11:37 exenia runc[292]: 1626430294 INFO ET200_sensor_adapter : buffer 220472 (55036) 2 11075
```

Note: The log may look different based on the actual adapter version installed. Warning: Depending on the size of the log, even longer loading times should be expected.

b. ET200_ntp_server

```
Jul 16 10:13:40 exenia runc[255]: 192.168.214.190.50726 > 10.3.0.2.ntp: NTPv4, length 48
Jul 16 10:13:40 exenia runc[255]: Client, Leap indicator: (0), Stratum 0 (unspecified), poll 4 (16s), precision -6
Jul 16 10:13:40 exenia runc[255]: Root Delay: 1.000000, Root dispersion: 1.000000, Reference-ID: (unspec)
Jul 16 10:13:40 exenia runc[255]: Reference Timestamp: 0.000000000
Jul 16 10:13:40 exenia runc[255]: Originator Timestamp: 0.000000000
Jul 16 10:13:40 exenia runc[255]: Receive Timestamp: 0.000000000
Jul 16 10:13:40 exenia runc[255]: Transmit Timestamp: 3835419100.673282896 (2021/07/16 10:11:40)
Jul 16 10:13:40 exenia runc[255]: Originator - Receive Timestamp: 0.000000000
Jul 16 10:13:40 exenia runc[255]: Originator - Transmit Timestamp: 3835419100.673282896 (2021/07/16 10:11:40)
Jul 16 10:13:40 exenia runc[255]: 10:11:40.673720 IP (tos 0xb8, ttl 64, id 49859, offset 0, flags [DF], proto UDP (17), length 76)
Jul 16 10:13:40 exenia runc[255]: 10.3.0.2.ntp > 192.168.214.190.50726: NTPv4, length 48
Jul 16 10:13:40 exenia runc[255]: Server, Leap indicator: (0), Stratum 11 (secondary reference), poll 4 (16s), precision -24
Jul 16 10:13:40 exenia runc[255]: Root Delay: 0.000000, Root dispersion: 0.011047, Reference-ID: 127.127.1.0
Jul 16 10:13:40 exenia runc[255]: Reference Timestamp: 3835419091.229770709 (2021/07/16 10:11:31)
Jul 16 10:13:40 exenia runc[255]: Originator Timestamp: 3835419100.673282896 (2021/07/16 10:11:40)
Jul 16 10:13:40 exenia runc[255]: Receive Timestamp: 3835419100.673622382 (2021/07/16 10:11:40)
Jul 16 10:13:40 exenia runc[255]: Transmit Timestamp: 3835419100.673711287 (2021/07/16 10:11:40)
Jul 16 10:13:40 exenia runc[255]: Originator - Receive Timestamp: +0.000339485
Jul 16 10:13:40 exenia runc[255]: Originator - Transmit Timestamp: +0.000428390
Jul 16 10:13:40 exenia runc[255]: 10:12:39.929844 IP (tos 0xb8, ttl 63, id 27798, offset 0, flags [DF], proto UDP (17), length 76)
```

c. ET200_sensor_timesync

```

Jul 16 10:12:28 exenia runc[17751]: 1626430348 INFO ET200_sensor_timesync : Latest sensor input: 2021-07-16T10:12:28.466288;0.0003616898148148148;-0.0014467592592592592;0.0007233796296296296;0.0003616898148148148;0;327.67;1;11294;0
Jul 16 10:12:28 exenia python3[17801]: ET200 Queue min : 2021-07-16 10:12:28.043094
Jul 16 10:12:28 exenia python3[17801]: Sinumerik timestampPrev: 2021-07-16 10:12:28.043000
Jul 16 10:12:28 exenia python3[17801]: Sinumerik timestamp : 2021-07-16T10:12:28.245000
Jul 16 10:12:28 exenia python3[17801]: Localtime : 2021-07-16 10:12:28.795072
Jul 16 10:12:28 exenia python3[17801]: nCnt: 15321
Jul 16 10:12:28 exenia python3[17801]: nQueueSizeBefore: 4233
Jul 16 10:12:28 exenia python3[17801]: Add required ET200 lines.
Jul 16 10:12:28 exenia python3[17801]: tET200Queue size (B/A/Diff): 4233 / 2213 / -2020
Jul 16 10:12:28 exenia python3[17801]: Produced json # 15320; PeriodMs: 2; ValueArraySize: 101; ET200RequiredSize: 2020; Extra ET200 lines: 0
Jul 16 10:12:28 exenia python3[17801]: -- LOOP-1 --
Jul 16 10:12:28 exenia python3[17801]: New sinumerik message Timestamp/ValueArraySize/Counter: 2021-07-16T10:12:28.447000 / 101 / 1488766
Jul 16 10:12:28 exenia python3[17801]: -- LOOP-2 --
Jul 16 10:12:28 exenia python3[17801]: ET200 Queue max : 2021-07-16 10:12:28.466288
Jul 16 10:12:28 exenia python3[17801]: ET200 Queue min : 2021-07-16 10:12:28.245097
Jul 16 10:12:28 exenia python3[17801]: Sinumerik timestampPrev: 2021-07-16 10:12:28.245000
Jul 16 10:12:28 exenia python3[17801]: Sinumerik timestamp : 2021-07-16T10:12:28.447000
Jul 16 10:12:28 exenia python3[17801]: Localtime : 2021-07-16 10:12:28.822475
Jul 16 10:12:28 exenia python3[17801]: nCnt: 15322
Jul 16 10:12:28 exenia python3[17801]: nQueueSizeBefore: 2213
Jul 16 10:12:28 exenia python3[17801]: Add required ET200 lines.
Jul 16 10:12:28 exenia python3[17801]: tET200Queue size (B/A/Diff): 2213 / 193 / -2020
Jul 16 10:12:28 exenia python3[17801]: Produced json # 15321; PeriodMs: 2; ValueArraySize: 101; ET200RequiredSize: 2020; Extra ET200 lines: 0
Jul 16 10:12:28 exenia python3[17801]: -- LOOP-1 --
Jul 16 10:12:28 exenia python3[17801]: New sinumerik message Timestamp/ValueArraySize/Counter: 2021-07-16T10:12:28.649000 / 101 / 1488867
Jul 16 10:12:28 exenia python3[17801]: -- LOOP-2 --
Jul 16 10:12:28 exenia python3[17801]: ET200 Queue max : 2021-07-16 10:12:28.466288
Jul 16 10:12:28 exenia python3[17801]: ET200 Queue min : 2021-07-16 10:12:28.447098

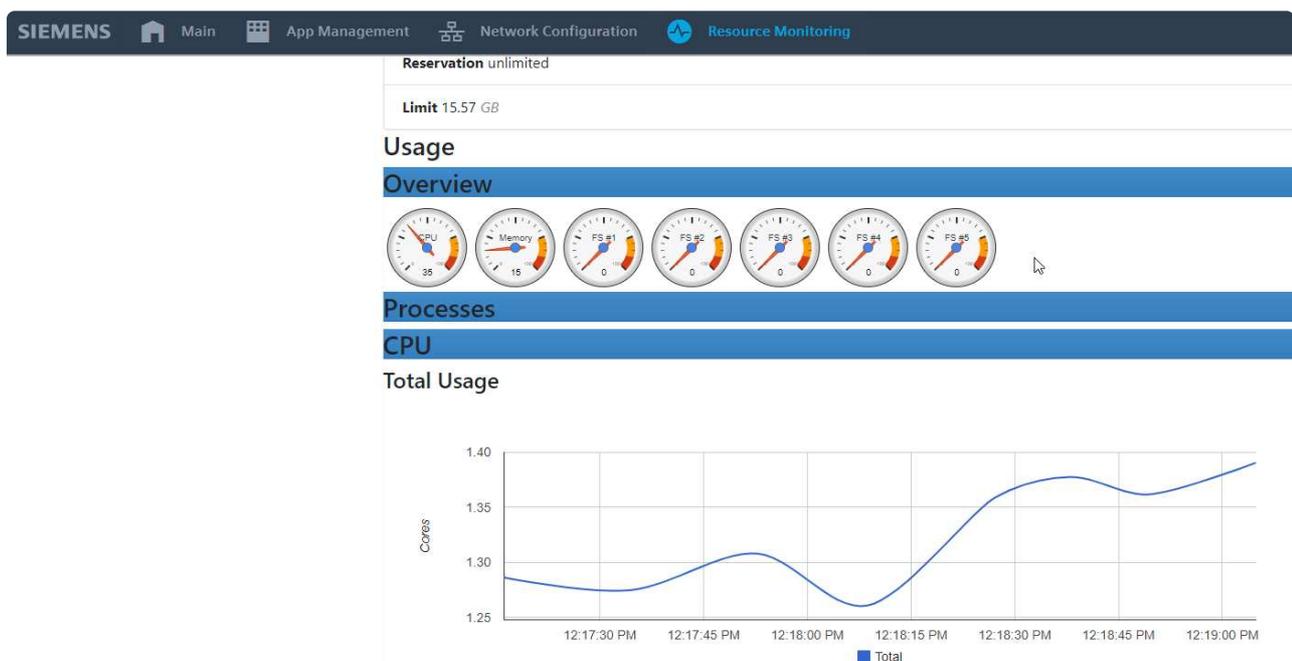
```

Error Handling

The apps require a lot of memory due to the large amounts of data. It may happen that the memory of one of the devices fills up and this leads to failure of the Sensor Adapter.

a. Check the system load of the Edge Box in the *Local Diagnostics Application* under *Resource Monitoring*

(high system loads can possibly result in errors, selection of a more powerful IPC (e. g. IPC 427E) is recommended).



b. - Memory Reset (MRES) of the PLC via TIA Portal: *ET200SP* -> *Online & diagnostics* -> *Online tools*

(after MRES you have to press the RUN button to start the CPU)



If all indapps are working as described, you can continue with the configuration of a test job for data recording.

Output

The ET200_sensor_timesync application receives data from ET200 Sensor Adapter (CSV) and Sinumerik Adapter (JSON) and merges data from these sources. It assures that the time matching ET 200SP data are added to Sinumerik data. It sends the merged data in JSON format defined by Analyze My Workpiece /Capture4Analysis application via Databus. The Sinumerik Adapter JSON output (for further reference please check the Sinumerik Adapter documentation) has been extended with ET 200SP data.

The way of the extension is explained in the next JSON sample :


```

{
  "address" : "EXTERNAL",
  "timestamp" : "2018-01-15T12:48:11.322492",
  "quality_mode" : "hf",
  "period_ms" : 2,
  "meta": "timestamp;a1ch1;a1ch2;a2ch1;a2ch2;D1;T1;DBID;PackageID;Source",
  "content" : [
    { "value" : [
      [" 2018-01-15T12:48:11.322500;-2.171585648148148;0.9067563657407407;2.540147569444444;-4.18149
59490740735;1;18.88;20000;473731;0",
      " 2018-01-15T12:48:11.322600;-1.8543836805555554;0.8991608796296295;2.4877025462962963;-4.2379
19560185185;1;18.88;20000;473731;0",
      ... ],
      [" 2018-01-15T12:48:11.324500;3.9706307870370368;0.6752748842592592;1.4854600694444444;-5.4835
79282407407;1;18.88;20000;473731;0",
      " 2018-01-15T12:48:11.324600;4.259259259259259;0.6647858796296295;1.4015480324074074;-5.54687
5;1;18.88;20000;473731;0",
      ... ],
      ...
      [" 2018-01-15T12:48:11.522500;9.938151041666666;0.19133391203703703;1.1056857638888888;-8.0848
52430555555;1;18.88;20000;473731;0",
      " 2018-01-15T12:48:11.522600;9.908854166666666;0.17939814814814814;1.1603009259259258;-8.1434
46180555555;1;18.88;20000;473731;0",
      ... ]
    ],[Potential extra ET200 DATA block depending on the timestamp of the next Sinumerik hf json data]
  ] }
}

```

Explanation EXTERNAL datapoint:

- *"address"*: "EXTERNAL": defines ET200 data block
- *"timestamp"*: "2021-05-26T12:37:01.552000";: copy of the timestamp of the original Sinumerik HF JSON message
- *"quality_mode"*: "hf";: copy of the quality_mode of the original Sinumerik HF JSON message
- *"period_ms"*: 2,: copy of the period_ms of the original Sinumerik HF JSON message
- *"meta"*: "timestamp;a1ch1;a1ch2;a2ch1;a2ch2;D1;T1;DBID;PackageID;Source";: it is the format header of the messages coming from ET200 Sensor Adapter application
 - **timestamp**: sampling timestamp of ET200 data
 - **a1ch1**: analog input1, channel 1 converted value (Volts)
 - **a1ch2**: analog input1, channel 2 converted value (Volts)
 - **a2ch1**: analog input2, channel 1 converted value (Volts)
 - **a2ch2**: analog input2, channel 2 converted value (Volts)
 - **D1**: digital input1 (8 bits - 8 channels)
 - **T1**: analog temperature input (degrees of Celsius)
 - **DBID**: internal data related to data transfer from ET200 (user irrelevant)
 - **PackageID**: internal data related to data transfer from ET200 (user irrelevant)
 - **Source**: value 0 - original ET200 data; value 1 - lines generated by the gap-filling algorithm.
- *"content"*: [

```

{ "value" : [
  [" 2018-01-15T12:48:11.322500;-2.171585648148148;0.9067563657407407;2.540147569444444;-4.1
  814959490740735;1;18.88;20000;473731;0",
  " 2018-01-15T12:48:11.322600;-1.8543836805555554;0.8991608796296295;2.4877025462962963;-4.
  237919560185185;1;18.88;20000;473731;0",
  ... ],
  ...
  ,["Potential extra ET200 DATA block depending on the timestamp of the next Sinumerik HF JSON data]
  ] } ]
}

```

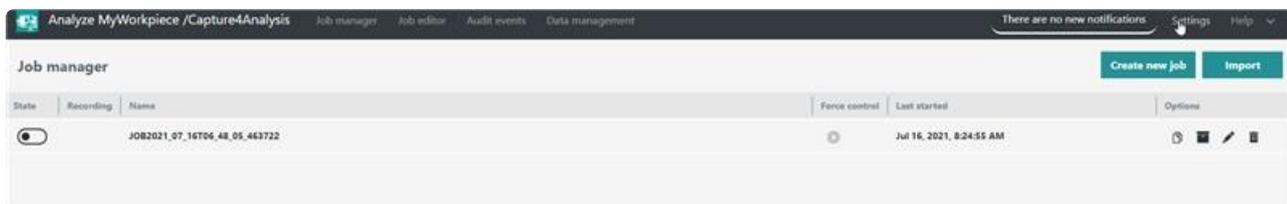
Values block (inside content) contains all data from ET200 between the Sinumerik HF timestamps of this and the next Sinumerik message.

Example use of synchronized data produced by the ET200_sensor_timesync

Configuration of an Analyze My Workpiece /Capture4Analysis test job

The configuration of the hardware should be completed up to the present state. Now the first test job for recording process data can be started. To do this, the Analyze My Workpiece /Capture4Analysis UI is started via *Open UI* using the *App Management* in the *Local Diagnostic Dashboard*. Before creating the test job, the recording of external data must be activated.

1. Open the *Settings* page



2. Enable *External sensor* slider

Settings

Enable or disable data streaming feature globally

Maximum chunk size for the data streaming messages

1 10 MB

Message queue address Topic name

Message queue username Message queue password

External sensor

Enable external sensor



Triggers

Show trigger times in UTC or local time zone

UTC

Use Sinumerik Edge system time or NCU time for time-based triggers

Sinumerik Edge system time is used.

3. Open *Job editor* and select desired HF and LF signals

Job editor

Job name * DEMO_JOB ✓

Variables External signals Triggers Settings

Variable	Remark	Sampling period	Unit
> <input checked="" type="checkbox"/> HF SIGNALS	<input type="text" value="Remark of HF SIGNALS"/>		

Low frequency signals 

+ Signal group name: * DEMO_LF_SIGNALS ✓ Sampling period: * 100 ms ✕

Signal device: * /Nck/HE_Probe/ ✓ Signal address: * recordingServoCounter ✓

4. Switch to External signals tab and enable the needed sensor signals

Variable	Address	Type
<input checked="" type="checkbox"/> Signals <ul style="list-style-type: none"> <input checked="" type="checkbox"/> External sensor signals <ul style="list-style-type: none"> <input checked="" type="checkbox"/> Analogue 1 channel 1 a1ch1 DOUBLE <input checked="" type="checkbox"/> Analogue 1 channel 2 a1ch2 DOUBLE <input checked="" type="checkbox"/> Analogue 2 channel 1 a2ch1 DOUBLE <input checked="" type="checkbox"/> Analogue 2 channel 2 a2ch2 DOUBLE <input checked="" type="checkbox"/> Digital 1 D1 INTEGER <input checked="" type="checkbox"/> Temperature 1 T1 DOUBLE <input checked="" type="checkbox"/> Source Source INTEGER 		

5. Activate and start test job

Job manager

State	Recording	Name	control	Last started	Options
<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	JOB2021_07_16T06_48_05_463722	Recording job JOB2021_07_16T06_48_05_463722 stopped successfully. ⚠	Jul 16, 2021, 10:16:20 AM	<input type="button" value="Download"/> <input type="button" value="Refresh"/> <input type="button" value="Search"/> <input type="button" value="Delete"/>

6. Stop test job and go to Data management

7. Download the job recordings

Analyze MyWorkpiece / Capture4Analysis There are new notifications

Job JOB2021_07_16T06_48_05_463722 Number of runs 10 Number of files 10

Jobrun	Recording start time	Recording end time	Number of files	Size of files	Actions
0a8e57ec-e0d2-4bfc-a5f1-c2bb29348805	Jul 16, 2021, 10:16:20 AM	Jul 16, 2021, 10:16:24 AM	1	222.07 kB	<input type="button" value="Download files"/> <input type="button" value="Delete"/>
0dd1cfe4-49cf-4899-84c0-565e6896694	Jul 16, 2021, 9:52:49 AM	Jul 16, 2021, 9:53:03 AM	1	938.74 kB	<input type="button" value="Download"/> <input type="button" value="Delete"/>
4db19ad9-3315-4836-b82c-c2d49d8b25fa	Jul 16, 2021, 9:46:42 AM	Jul 16, 2021, 9:46:54 AM	1	868.59 kB	<input type="button" value="Download"/> <input type="button" value="Delete"/>
d12813b5-d445-4d00-a498-2c03465c9c99	Jul 16, 2021, 9:46:06 AM	Jul 16, 2021, 9:46:20 AM	1	925.56 kB	<input type="button" value="Download"/> <input type="button" value="Delete"/>
ce3c561c-b6e3-4a72-af61-39a85d4e0413	Jul 16, 2021, 9:25:53 AM	Jul 16, 2021, 9:26:09 AM	1	949.73 kB	<input type="button" value="Download"/> <input type="button" value="Delete"/>
25c87038-1127-4991-b1f7-03aacc42228a	Jul 16, 2021, 9:15:48 AM	Jul 16, 2021, 9:16:04 AM	1	3.5 kB	<input type="button" value="Download"/> <input type="button" value="Delete"/>
fdafd908-6960-4aa0-9155-d092304f024c	Jul 16, 2021, 9:12:14 AM	Jul 16, 2021, 9:12:21 AM	1	2.39 kB	<input type="button" value="Download"/> <input type="button" value="Delete"/>
14515bca-c4fc-43dd-b29c-daffc40e3d26	Jul 16, 2021, 8:24:55 AM	Jul 16, 2021, 8:25:06 AM	1	32.25 kB	<input type="button" value="Download"/> <input type="button" value="Delete"/>

8. Open JSON file in JSON editor and check the Output Format for all the desired signals

ET200 Sensor Adapter Configurator

Introduction

The ET200 Sensor Adapter configuration is stored in a specific json file. Even though you can change the json content directly from the Insights Hub application configuration, it is strongly recommended to edit the configuration using ET200 Sensor Adapter configurator UI, which was specifically developed for this purpose. Nonetheless, for the proper setup of the adapter, gaining some knowledge about the relevant entities and fields in the corresponding json configuration file is mandatory.

Content

1. [Configuration fallback strategy](#) (correlation between Insights Hub and miniweb UI configs)
2. [Insights Hub \(IH\) configuration usage + json description](#)
3. [UI access via miniweb](#)
4. [Configurator UI](#)

1. Configuration fallback strategy

(correlation between Insights Hub and miniweb UI configs)

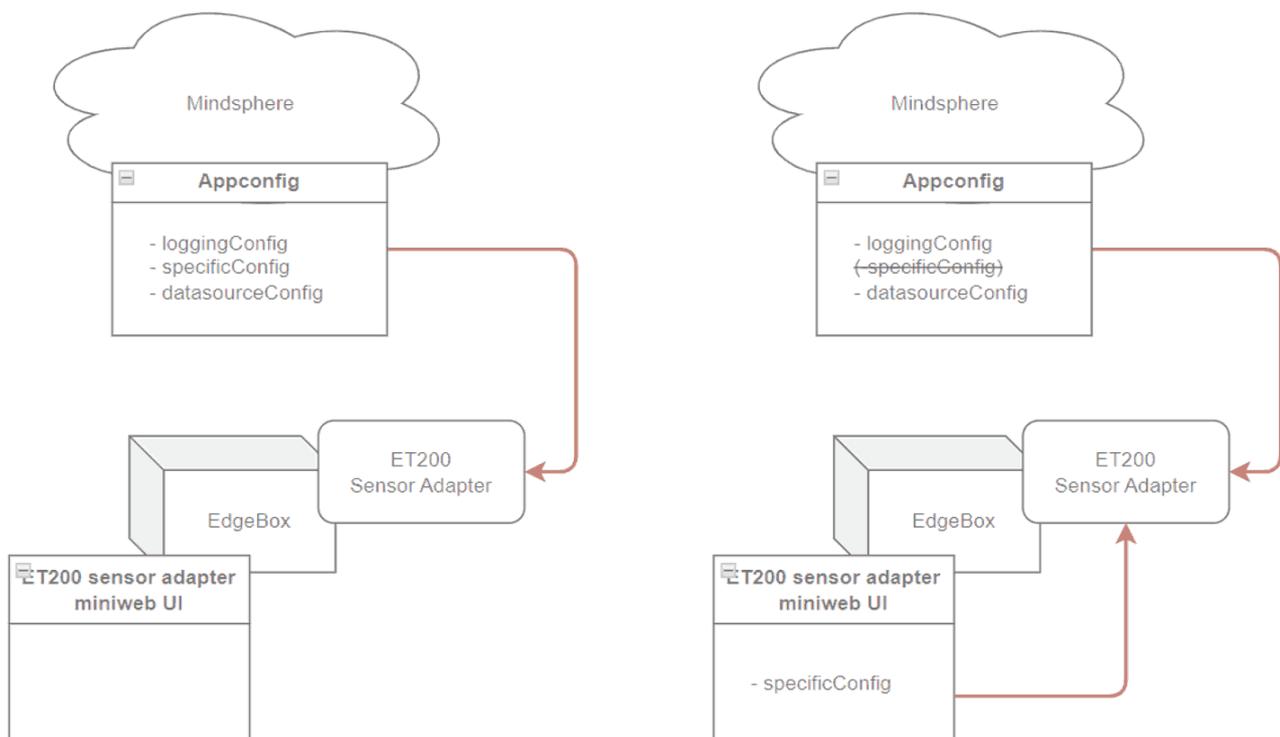
After installation and before starting ET200 Sensor Adapter, it can be configured via Insights Hub (IH).

Instance Name	Status	Cloud Upload	Operations
ET200_sensor_adapter	STOPPED		 ↓ Edit App Instance Configuration

The application launches with the IH configuration. After it is started, the `specificConfig` part of the IH configuration can be overridden via the ET200 Sensor Adapter Configurator User Interface (UI). The UI is reachable from the miniweb application, running on the Edgebox. After submitting the modified configuration on the UI, the application will automatically apply the changes within 2-15 seconds. Configuration changes made on the miniweb UI are saved locally on the box and do not appear in IH. Therefore, the IH configuration can not be modified via the UI. The configuration generated on the UI can be revoked ([Reset button](#)), and after resetting, the ET200 Sensor Adapter works according to the original `specificConfig`, stored in IH.

ET200 Sensor Adapter Configurator UI is available at url: https://<box ip>:5443/ET200_sensor_adapter/

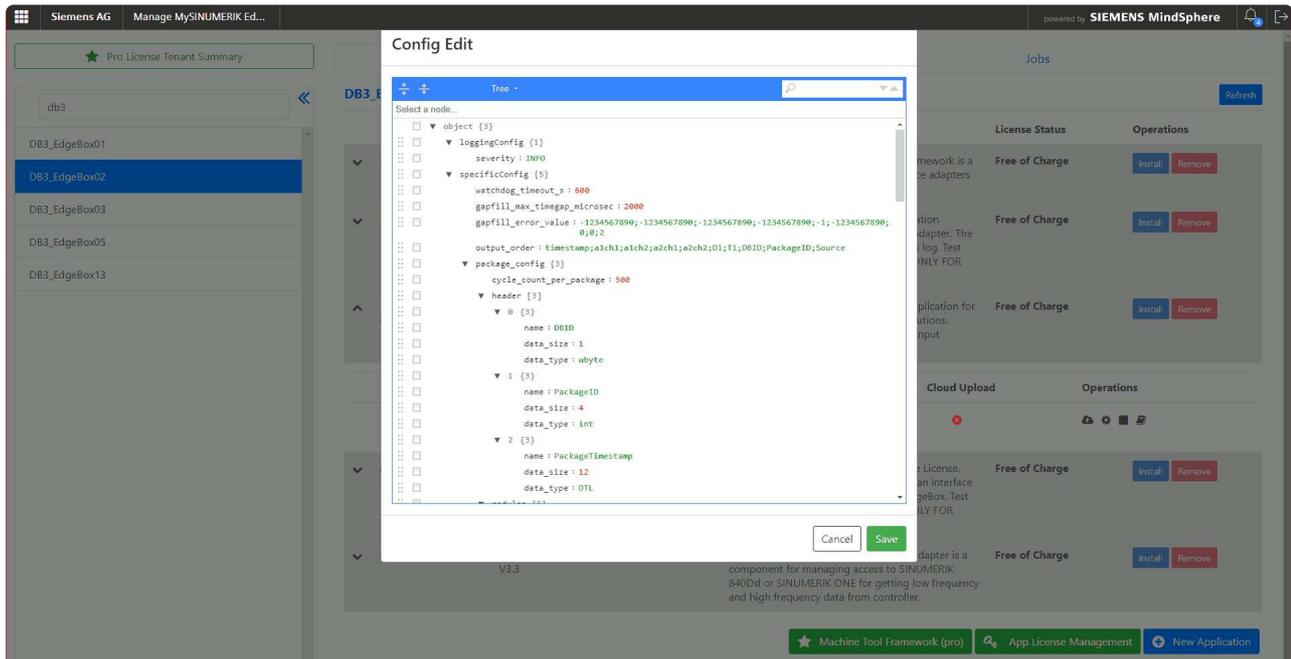
Hint: the last '/' is mandatory.



picture: configuring ET200 Sensor Adapter

2. Insights Hub configuration usage + json description

IH configuration pop-up window



picture: IH configuration pop-up window

During the launch, the application uses the IH configuration. With the miniweb configurator UI, the `specificConfig` part of this configuration can be overridden in a user-friendly way and the ET200 Sensor Adapter will reconfigure itself with the modified config in runtime within 2-15 seconds.

Hint: if the `specificConfig` configuration was set via the UI, the `specificConfig` part of the IH configuration becomes inactive, however, its content remains unchanged in IH. By pressing the Reset button on the UI, the original IH configuration is applied again in the ET200 Sensor Adapter, the local `specificConfig.json` is deleted by the UI. The IH `specificConfig` section is reloaded into the configurator for modification.

ET200 Sensoradapter configuration on Insights Hub

The configuration json file has 3 main parts:

1. loggingConfig

In `loggingConfig` the `logCfg.severity` (more verbose/less verbose) loglevel can be set.

Note: available `severity` values that can be set are: `DEBUG`, `INFO`, `WARN`, `ERROR`.

2. specificConfig

It is possible to modify the entire `specificConfig` part on IH, according to the description of the `specificConfig` block in [ET200 Sensor Adapter json documentation](#).

3. datasourceConfig

WARNING: It is recommended to leave the `datasourceConfig` section unchanged on IH and also do not clear the entire `specificConfig` content on IH, as the application will not be able to run in these cases.

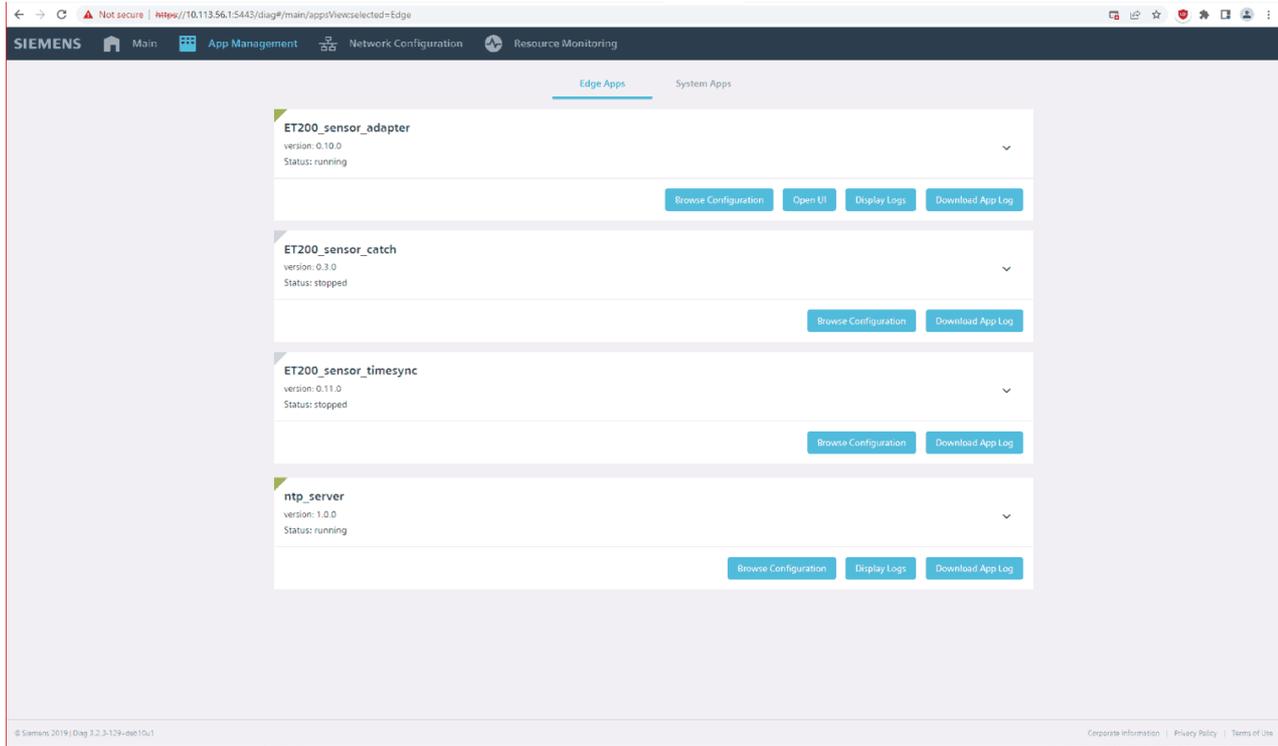
After stop/start on Insights Hub:

When ET200 Sensor Adapter is stopped and then started on the IH, the created and submitted `specificConfig` on the UI is not lost and it will be used. In case of reinstall on IH (stop, delete, remove, install), the UI configuration

will be lost, the application will restart with the config stored on IH.

3. The miniweb UI access

The configurator UI can be started via *diagnostic interface*, using the url: `https://<box ip>:5443/diag/`
In the main menu, choose the App Management tab, then on the loaded page's top, click to Edge apps, and on the ET200 Sensor Adapter's panel, the UI is reachable through the "Open UI" button. (App Management tab/Edge apps tab/ET200_sensor_adapter panel/"Open UI" button).

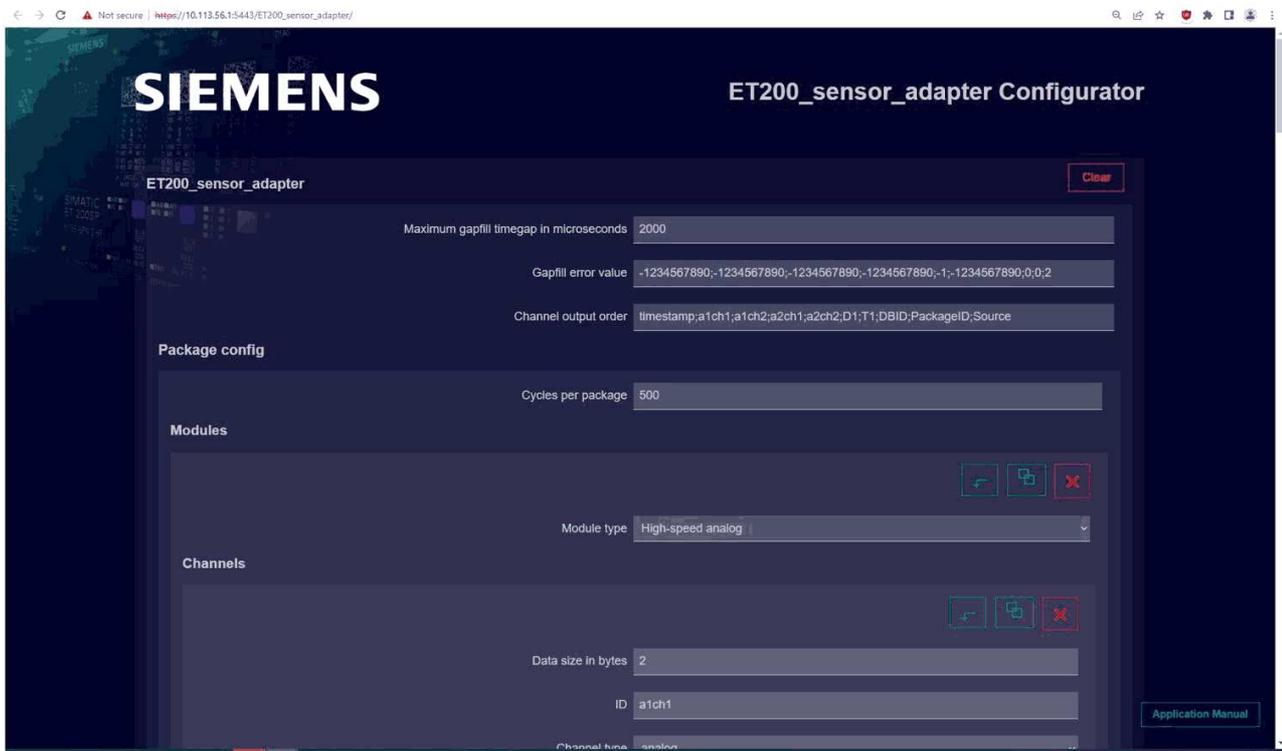


picture: Diagnostic interface

In other case, the UI via the miniweb is available at url: `https://<box ip>:5443/ET200_sensor_adapter/`

Hint: the last '/' is mandatory).

Both cases, either with the "Open UI" button or via the miniweb, the following UI interface will greet you:



picture: Configurator's initial page

4. Configurator UI

MAIN BUTTONS

Clear

Loads the minimal ("empty") configuration in the UI. This operation has no effect on the app, so no reconfiguration takes place until Submit button is pressed.

Reset

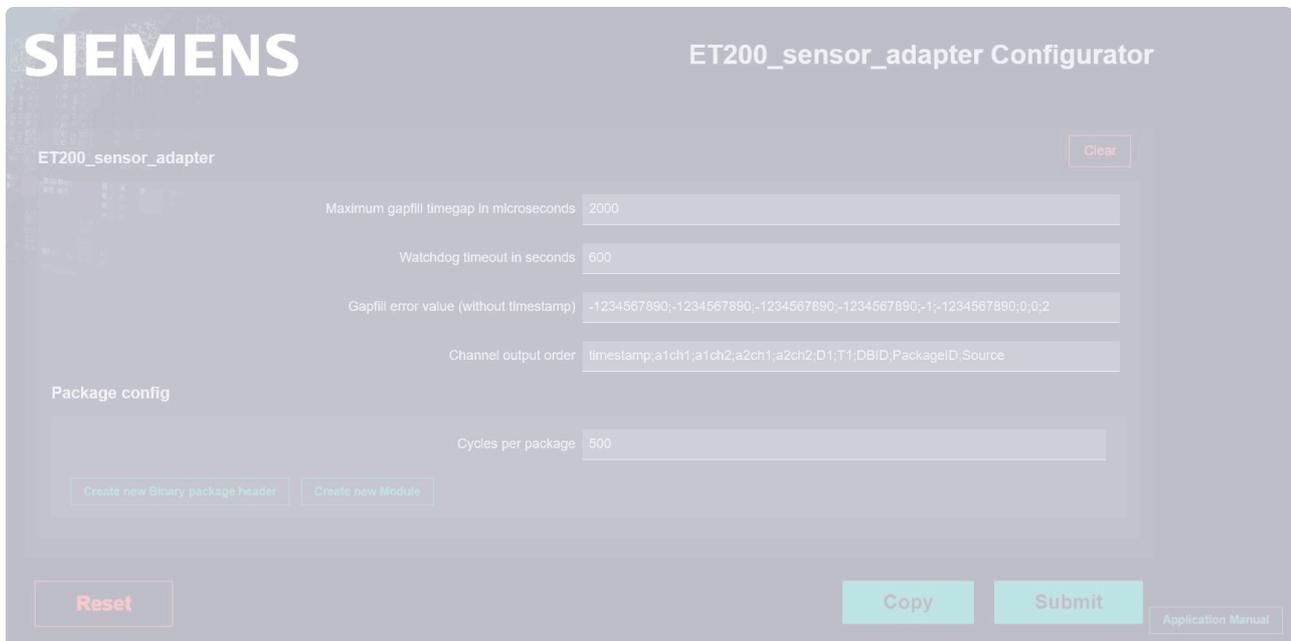
Deletes the local `specificConfig.json` file, reloads the `specificConfig` part of IH configuration into the UI and the ET200 Sensor Adapter will load it to the IH configuration within 2-15 seconds.

Copy

Creates the `specificConfig` json object, based on the content of the UI fields, and copies it to the clipboard. This can be utilized to backup the `specificConfig`. This can be manually added to the application's IH configuration.

Submit

Generates the `specificConfig.json` file based on the content of the UI fields, saves it and ET200 Sensor Adapter will load it within 2-15 seconds.



picture: Cleared Configurator with its main buttons.

SPECIFICCONFIG OVERVIEW

Hint: All these fields have a detailed description in the [ET200_sensor_adapter_json documentation](#).

Watchdog timeout in seconds: For how long ET200 Sensor Adapter should run while it receives no data.

Maximum gapfill timegap in microseconds: Naturally, timegaps between AP timestamps vary. The ET 200SP data series may have larger gaps and they are filled in using a kind of interpolation: based on the ET 200SP device's frequency, there is a calculated ideal timegap between the consecutive AP timestamps. Larger gaps are filled up using repetition of the sensor data, however, even larger gaps, which are over **Maximum gapfill timegap in microseconds**, are filled up with predefined error lines (**Gapfill error value**).

Gapfill error value: The predefined error line in csv format that is used to fill up the timegaps larger than the value of **Maximum gapfill timegap in microseconds**. This line does not contain the value for the timestamp, because that is generated using primitive interpolation. Any other value can be used to define this error line, the only exception is the value associated with the **Source** field which must be 2.

Channel output order: The preferred order of columns of the output csv file. This section has to be consistent with the header, module and channel values.

Package Config: `package_config` has to describe exactly the structure described within DB101 and DB102 data block via TIA Portal.

- Cycle count per package
- Header
- Modules
 - module types
 - oversampling
 - channels

CREATE SPECIFICCONFIG BLOCKS ON THE UI:

Header

- **Create new binary package header:** A new, empty header block appears on the UI, suitable to fill out its “Header name”, “Data size in bytes” and “Data type” values implicitly, according to the TIA portal settings.

Modules:

- **Create new Module:** A new, empty module block appears on the UI under Package config
- **Create new Channel:** A new, empty channel block appears on the UI under a Module

ICONS:

Hint: Hover over icon buttons to show their description.

-  **Up, down:** Change order between items in the same category.
-  **Duplicate:** The item, to which the button is related, will be duplicated with the same content filled in.
-  **Delete:** The item, to which the button is related, will be deleted.

UI MANUAL:

Application Manual

The corresponding manual can be reached with the use of “Application Manual” button and hide with the use of “Hide Manual” button.

SINUMERIK Edge MQTT Client

SINUMERIK Edge MQTT Client is an edge application that allows communication between an edge application and an external MQTT broker.

Configuration

SINUMERIK Edge MQTT Client can be configured in the following format:

```
{
  "specificConfig": {
    "brokers": [
      {
        "host": "<HOST>",
        "port": <PORT>,
        "label": "<BROKER-LABEL>",
        "clientId": "<CLIENT-ID>",
        "username": "<USERNAME>",
        "password": "<PASSWORD>",
        "quota": {
          "memory": {
            "threshold": <MEMORY-QUOTA-THRESHOLD>,
            "hysteresis": <MEMORY-QUOTA-HYSTERESIS>
          }
        }
      },
      ...
    ],
    "logLevel": "<LOG-LEVEL>"
  }
}
```

Explanation for the fields follow as:

- **HOST:** Hostname or IP address of the external broker. This address must be reachable via `factorylan0` interface.
- **PORT:** Port of the external broker.
- **LABEL:** Label to identify this broker by. This label is a handle to be used by the applications that make use of the SINUMERIK Edge MQTT Client. There may be more than one broker configured with the same label and the published data will be pushed to all of them.
- **CLIENT-ID:** Client ID to use while connecting to brokers, if omitted, an auto generated value is used.
- **USERNAME:** Username to be used in authentication, can be omitted if no authentication is required for broker.
- **PASSWORD:** Password to be used in authentication, can be omitted if no authentication is required for broker.
- **LOG-LEVEL:** Log level of the application. The valid options are `"trace"`, `"debug"`, `"info"`, `"warning"`, `"error"`, `"critical"`. The default is `"info"` when this option is not provided. Note that levels that are more verbose than `"info"` may severely degrade performance.
- **MEMORY-QUOTA-THRESHOLD:** Threshold in bytes for total message memory consumption of this broker. The consumption includes the size of in-flight/buffered/queued messages plus a fixed overhead per message (mostly negligible). If this value is exceeded, messages to this broker are started to be discarded. Defaults to `0`

which equally distributes the *available memory* (see below) between the brokers.

- **MEMORY-QUOTA-HYSTERESIS:** The value in bytes which controls when to stop discarding messages. Once the *MEMORY-QUOTA-THRESHOLD* is reached, messages are discarded until the memory consumption of messages for this broker becomes less than or equal to the value of *MEMORY-QUOTA-THRESHOLD - MEMORY-QUOTA-HYSTERESIS*. Defaults to lowest integral value of 10% of *MEMORY-QUOTA-THRESHOLD*.

As an example to memory quota configuration, let a broker have a threshold of **1500 MBytes** and hysteresis of **200 MBytes**. Once the total memory consumption of this broker increases past **1500 MBytes**, the message triggering this condition and the messages received after will be discarded until memory usage drops to **1300 MBytes**.

Further explanations:

- *APP-MEMORY-LIMIT:* Currently a fixed value of 2-gigabytes.
- *TOTAL-MEMORY-QUOTA:* Currently a fixed value of *APP-MEMORY-LIMIT - 200-megabytes*.
- *AVAILABLE-MEMORY:* Available memory calculated by subtracting the quota configured for brokers from the *TOTAL-MEMORY-QUOTA*. I.e. if you have a **broker-0** configured with a memory quota of 1.3-gigabytes and **broker-1** with a memory quota of 100-megabytes, **broker-3** & **broker-4** does not have any configured quotas, **broker-3** and **broker-4** will be automatically assigned a memory quota of 200-megabytes each.

Currently, the publishing to brokers are done with QoS = 2 and it cannot be changed.

Authentication

Version 0.4.0 of SINUMERIK Edge MQTT Client introduces username/password authentication mechanism to connect external MQTT brokers. In order to use username/password authentication, users must have their external MQTT brokers configured with username/password authentication. Users can specify username/password fields for relevant brokers in the configuration of SINUMERIK Edge MQTT Client application. For brokers that dont use authentication, these fields can be omitted.

E.g

```
{
  "specificConfig": {
    "brokers": [
      {
        "host": "10.0.1.1",
        "port": 1883,
        "label": "auth-broker",
        "username": "mqtt-user",
        "password": "mqtt-password"
      },
      {
        "host": "10.0.1.2",
        "port": 1883,
        "label": "no-auth-broker",
      },
      ...
    ],
    "logLevel": "debug"
  }
}
```

Statistics

By default, the application will print the application status & internal state of the communication with brokers at 15 second intervals. The stats contain information such as in-flight message count, the size of the in-flight messages and so on.

There are two kinds of statistics messages. The first one is *process statistics message* and the other is *broker statistics message*. For each broker, a separate line containing the statistics of that broker will be printed. The following is an example to a statistics message of an application configured with one broker:

```
2021-11-01 10:14:20 operator(): mem-rss-kb=9004;mem-peak-rss-kb=9004;mem-max-kb=2097152
2021-11-01 10:14:20 operator(): broker=broker-1;host=127.0.0.1;port=2885;msgs-in-flight=0;bytes-in-flight=0;queue-size=0;peak-queue-size=0;total-msgs=0;total-bytes=0;failed-msgs=0;failed-bytes=0;memory-quota=1937768449;memory-quota-hysteresis=193776844;msg-bw=0;bw=0
```

If we look in detail what these fields mean:

- First line is the process statistics message, where the meaning of the fields follow as:
 - **mem-rss-kb**: Current memory usage of the application in kilobytes.
 - **mem-peak-rss-kb**: Peak memory usage of the application in kilobytes since the launch of the application.
 - **mem-max-kb**: Maximum allowed memory usage of the application in kilobytes. If the memory usage exceeds this, the application will be killed, all queued/buffered/in-flight messages will be lost and the application will be restarted automatically.
- The second line is a broker statistics message, where:
 - **broker**: The label of the broker.
 - **host**: The hostname configured for the broker.
 - **port**: The port number configured for the broker.
 - **msgs-in-flight**: Messages that are *being sent*. These kind of messages:
 - May already be sent to the broker but not yet acknowledged (where **QoS > 0**),
 - buffered in the OS network layer or
 - queued in some lower layer of the application.
 - **bytes-in-flight**: The total size of the messages in flight.
 - **queue-size**: Messages that are currently queued and waiting to be sent (where **QoS = 0**).
 - **peak-queue-size**: Peak size that the queue has reached since the launch of the application.
 - **total-msgs**: Total number of messages that have been successfully sent so far.
 - **total-bytes**: Total bytes that have been successfully sent so far. The message is considered *sent* depending on QoS:
 - If QoS is 0, the message has been passed down to the OS network layer.
 - If QoS is greater than 0, the external broker has acknowledged the message.
 - **failed-msgs**: The number of messages that were not sent due to a failure. This can happen when messages are discarded due to being in a disconnected state for a long time or reaching the configured memory quota threshold.
 - **failed-bytes**: Total bytes of the failed messages.
 - **memory-quota**: The configured memory quota threshold for this broker.
 - **memory-quota-hysteresis**: The configured memory quota hysteresis for this broker.
 - **msg-bw**: Average of per-message bandwidth in bytes per second. Per-message bandwidth is calculated for each message depending on QoS:

- If QoS is 0, it is the size of the message divided by the duration it takes to be passed down to the OS network layer.
- If QoS is greater than 0, it is the size of the message divided by the duration it takes to receive acknowledge message from the external broker.
- **bw**: Average bandwidth (bytes per second) calculated towards the broker in the period since the last statistics message. It is calculated as the total size of the messages sent divided by the duration.

One can also explicitly trigger the stats message by sending SIGUSR1 to the application. This is only possible on a development image.

Limitations

The application is configured to use a maximum of 2GB of memory. If the communication with an external broker is slow (or lost, see below), the data being sent will end up being buffered in the application itself. If this happens continuously until the memory limit is reached (memory quota threshold of a broker), the application will start to discard messages until the memory usage is decreased by a certain amount (memory quota hysteresis of a broker).

Upon reaching the memory quota threshold of a broker, a warning level log will be printed to indicate the start of the messages being discarded:

```
discard: quota reached for '<broker-hostname>:<broker-port>', discard until hysteresis '<broker-memory-quota-hysteresis>' is sent, psize=<size of the first message being discarded>
```

After the memory consumption of the broker drops below the configured value, a warning level log `memory quota hysteresis reached on '<broker-hostname>:<broker-port>', stop discarding` is printed and the messages will not be discarded any more until the threshold is reached again.

The data sent towards a broker that was not connected at all is discarded.

If the connection to a broker is initially established and then it is lost, the data to be sent towards that broker will be buffered for 3 minutes. If the connection is not re-established in 3 minutes, all the buffered data will be discarded and no further buffering will be done until connection is re-established.

Overview

Industrial Edge App configuration

The configuration of an Industrial Edge App instance contains the following sections:

- **specific configuration** : This configuration section is specific to the application. Please refer to the App documentation if and how this section must be configured.
- **logging configuration** : This configuration section defines the log level of the application.
- **datasource configuration** : The SINUMERIK Edge provides several services for application communication. This configuration section is used to connect Edge applications to available sources of data.

In this section of the document, you will find essential information to configure your application. Some details are not included since they are not required or important from the application developer's aspect.

Sample Metaconfig

```
{
  "datasourceConfig": {
    "requiredDatasource": [
      {
        "datasourceId": "SINUMERIK_NCU1",
        "type": "SINUMERIK",
        "services": {
        }
      }
    ]
  },
  "loggingConfig": {
    "appender": "JOURNAL_APPENDER",
    "severity": "INFO"
  },
  "specificConfig": {
    "specificArray": [
      "item0",
      "item1",
      "item2"
    ],
    "specificDecimal": 10,
    "specificString": "sample value"
  }
}
```

Note

Objects that are labeled as mandatory, required only when their parent objects are provided.

Application specific

specificConfig

Path Application Name >> specificConfig

Type object, Mandatory

Usage

"specificConfig" section is reserved for the application's specific needs.

Example

```
{
  "specificConfig": {
    "specificArray" : ["item0", "item1", "item2"],
    "specificDecimal" : 10,
    "specificString" : "sample value"
  }
}
```

Logging

loggingConfig

Path Application Name >> loggingConfig

Type object, Mandatory

Usage

Sets the appender type and severity level for the application.

You can use appenders for setting logging location. The severity is for the levels of logging. Below appender types and severity levels can be used.

Appender Types

Name	Description
CONSOLE_APPENDER	Appender for printing logs only to console.
FILE_APPENDER	Appender for uploading the logs to a file, which is on the same directory with the application. Also prints the logs to console.
JOURNAL_APPENDER	Appender for uploading the logs only to journald.
SYSLOG_APPENDER	Appender for uploading logs to journald with their system time. Also prints the logs to console.

Log Severity

Name	Description
"INFO"	This level enables the logging for all levels except Debug level.
"DEBUG"	This level enables the usage of all logging levels.
"WARN"	This is the level for printing only warnings and errors.
"ERROR"	This level is only for error messages.

Example

```
"loggingConfig": {  
  "appender": "JOURNAL_APPENDER",  
  "severity": "INFO"  
},
```

Configure access

datasourceConfig

connecting applications to datasource instances

In SINUMERIK Edge, applications can share or require data to communicate with each other. Available data is defined as datasource instance - identified by a unique ID. In order to access data of available datasources, "datasourceConfig" section of "appconfig.json" needs to be configured properly.

"datasourceConfig" object consists of "providedDatasource" and "requiredDatasource" objects.

Inside "requiredDatasource" objects, the requirements of a data consuming application are defined. This application wants to access data of a datasource. Inside "providedDatasource" objects, the available data which is provided for other applications by several services are defined. Most known datasource providing application is the SINUMERIK adapter.

Every service has its own custom settings. Please refer to the corresponding service documentation of the supported services to get details about the configuration.

Rename datasources Each datasource instance is identified by a unique id. The id can be changed by changing the "datasourceId" to your needs. Take care, to modify the providers and corresponding consumers of the datasource consistent to not break any existing connections.

Example

The configuration of an sample data providing application looks like this

```
{
  "datasourceConfig": {
    "providedDatasource": [
      {
        "datasourceId": "downsample database",
        "type": "SAMPLE_DATA",
        "services": {
          "parameter-service/v1":{

          }
        }
      }
    ]
  }
}
```

This defines an available datasource of the type SAMPLE_DATA. The datasource instance can be renamed – for example: "datasourceId": "myMachine"

Attention!: Unless explicitly stated in the documentation of the corresponding app, do not change settings other than the datasourceId in the providedDatasource section.

Attention!: Do not change the type of a datasource!

After this, have a look to other installed Applications. An application which needs access to the datasource might look like this:

```
{
  "datasourceConfig": {
    "requiredDatasource": [
      {
        "datasourceId": "downsample database",
        "type": "SAMPLE_DATA",
        "services": {
          "parameter-service/v1":{

          }
        }
      }
    ]
  }
}
```

This datasource also has to address the new id to connect to the datasource. Otherwise this application will not work. * "datasourceId": "myMachine" *

Attention!: There will be no check and no feedback if you select a non existing "datasourceId". Please carefully check the configuration before saving the configuration to the SINUMERIK Edge.

Diagnose On configuration error, a short error message in the configuration jobs response can be found in the responsible configuration backend. Error details can be found in the logfiles. Also refer to the UI of the AdapterFramework - this can be found at the dashboard on the SINUMERIK Edge.

Attention: Always verify the resulting status of a configuration job.

Attention! There will be no warning or error message if you configure a subscription to datapoints which are not available. If the application does not get the subscribed data messages, you might get information in the log files of the datasource providing application.

data access services

Supported services are:

- `parameter-service/v1`
 - `subscription-service/v1`
 - `information-service/v1`
-

parameter-service/v1

Configuration

Path: datasourceConfig >> [required/provided]Datasource >> services >> parameter-service/v1

Type: object

Usage:

The parameter-service enables applications to read and write data on a connected datasource. Unless this service has the possibility to impact a connected datasource, the datasource providing application has the possibility to enable access protection. This means, that all datapoints which are not stated in the requiredDatasource section of the consuming application will be forbidden and access will be rejected. Please review the documentation of the corresponding application, how the access has to be configured.

Attention: It is the operator's responsibility to verify all data access for his setup!

Attention: Allowing writing access to parameters might be a security risk for connected datasources - such like a SINUMERIK machine.

Attention: Always refer to the application documentation to get details about the configuration needs of the specific application.

Example Sample configuration for write can be found below.

```
{
  "datasourceConfig": {
    "requiredDatasource": [
      {
        "datasourceId": "SINUMERIK_NCU1",
        "services": {
          "parameter-service/v1": {
            "access": [
              {
                "accessType": "w",
                "datapoints": [
                  {
                    "address": "/NC/"
                  }
                ]
              }
            ]
          }
        }
      }
    ],
    "type": "SINUMERIK"
  }
}
```

In the configuration above, user can write data to variables starts with "/NC/" for parameter service in "datasourceId" with "SINUMERIK_NCU1" and data source type as "SINUMERIK".

subscription-service/v1

Configuration

Path: datasourceConfig >> [required/provided]Datasource >> services >> subscription-service/v1

Type: object

Usage: The subscription-service enables applications to subscribe to provided data. The datasource providing application gets automatically configured out of the subscriptions of the installed applications.

For common applications you do not need to create the configuration manually. In most cases, the application will start with a default configuration which will work fine in most installations, so you do not need to create a subscription configuration. Anyway, you should always check the applications documentation how to configure the datasource access. There might be some details missing, so that you must include configuration details of the connected datasource to provide the correct data.

Attention: There will be no warning or error message if you configure a subscription to datapoints which are not available. If the application does not get the subscribed data messages, you might get information in the log files of the data providing application. Provided databus messages could include confidential data. Please refer to the documentation of the datasource providing application to get known of the details. If available data includes confidential information, verify that you only subscribe trusted consuming applications to this data. If the installed application is not trusted, remove the subscription for confidential message id's out of the subscription-service configuration.

Attention: It is the operator's responsibility to verify all data access for his setup!

Handling wildcards

If a subscription needs specific environment configuration which are only known at configuration time, the metaconfig of the application might use wildcards to help you configuring. Depending on the application, wildcards can be specified directly in the datasourceConfig object or in the application documentation. See the two examples below.

example:

```
{
  "datasourceConfig": {
    "wildcards": [
      {
        "key": "$id",
        "description": "array index of the parameter"
      }
    ]
  },
  "requiredDatasource": [
    {
      "services": {
        "subscription-service/v1": {
          "subscriptions": [
            {
              "datapoints": [
                {
                  "address": "CTRL_DATAPOINT($id)",
                  "description": "configure one datapoint for each required ID"
                }
              ]
            }
          ]
        }
      }
    }
  ]
}
```

In this example, you can see some descriptive texts, helping to configure the application: The **description** text in the datapoint object, and the **wildcard** object \$id, referenced by the parameter address.

information-service/v1

Configuration

Path: datasourceConfig >> [required/provided]Datasource >> services >> information-service/v1

Type: object

Usage: The information-service is used to access general information of a datasource instance.

This service must not be configured.

Example: Sample configuration for access to the report "alarmList".

```
"information-service/v1" : {  
  "reports":["alarmList"]  
}
```

Reverse Proxy with Local User Management

Basics

Connection

You can connect to ReverseProxy control panel via: `https://<EDGE_BOX_IP>:5443` (secure)

Login

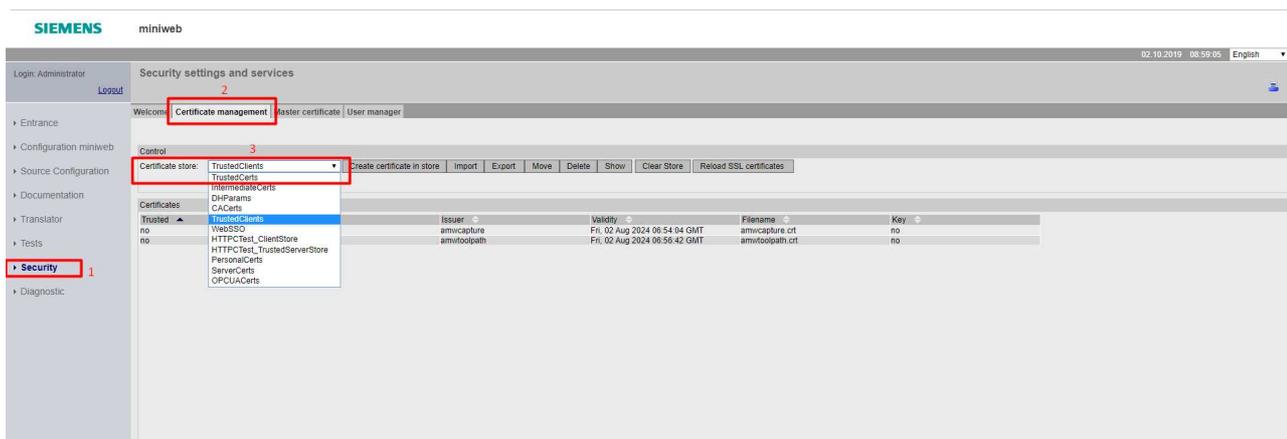
There's a built-in system user (Administrator). Username: Administrator For passwords of all built-in users, please refer to [default passwords](#) Please also see the Security Advice below. You will be asked to change the password for any user during initial login.

Security Advice

It is strongly advised not to expose the factorylan ports directly to the internet, and change default passwords immediately. Password Policy: Minimum 8 characters. Includes at least one from each character set; uppercase, lowercase, digit, special.

Certificate Management

You can create or import your own certificates to reverse proxy and export existing ones. Login as system admin and browse to "Security/Certificate management". On that page, you have the option to edit the content of the desired certificate stores.



Trusted	Issuer	Validity	Filename	Key
no	amvcapture	Fri, 02 Aug 2024 06:54:04 GMT	amvcapture.crt	no
no	amvfootpath	Fri, 02 Aug 2024 06:56:42 GMT	amvfootpath.crt	no

Server Certificates

Server certificates are used for authenticating the SSL server to remote clients. These certificates can be managed under the `ServerCerts` certificate store from reverse proxy UI. To use a certificate as a server certificate, the certificate file must be named as `SSLServerCert.crt`. By default, there is already an existing certificate named `SSLServerCert.crt`. This can be deleted in order to use another one, to do so, please refer to [Importing an SSL Server Certificate](#). Not having any certificate named `SSLServerCert.crt` will end up with an automatically generated server certificate. For users who want to create their server certificate, please refer to [Creating an SSL](#)

Server Certificate.

Creating an SSL Server Certificate

SSL server certificates can be created either by using [openssl command line utility](#), or by using [reverse proxy UI](#).

REVERSE PROXY UI

All below steps are must be run via an Administrator account, make sure the account in effect has administrative rights.

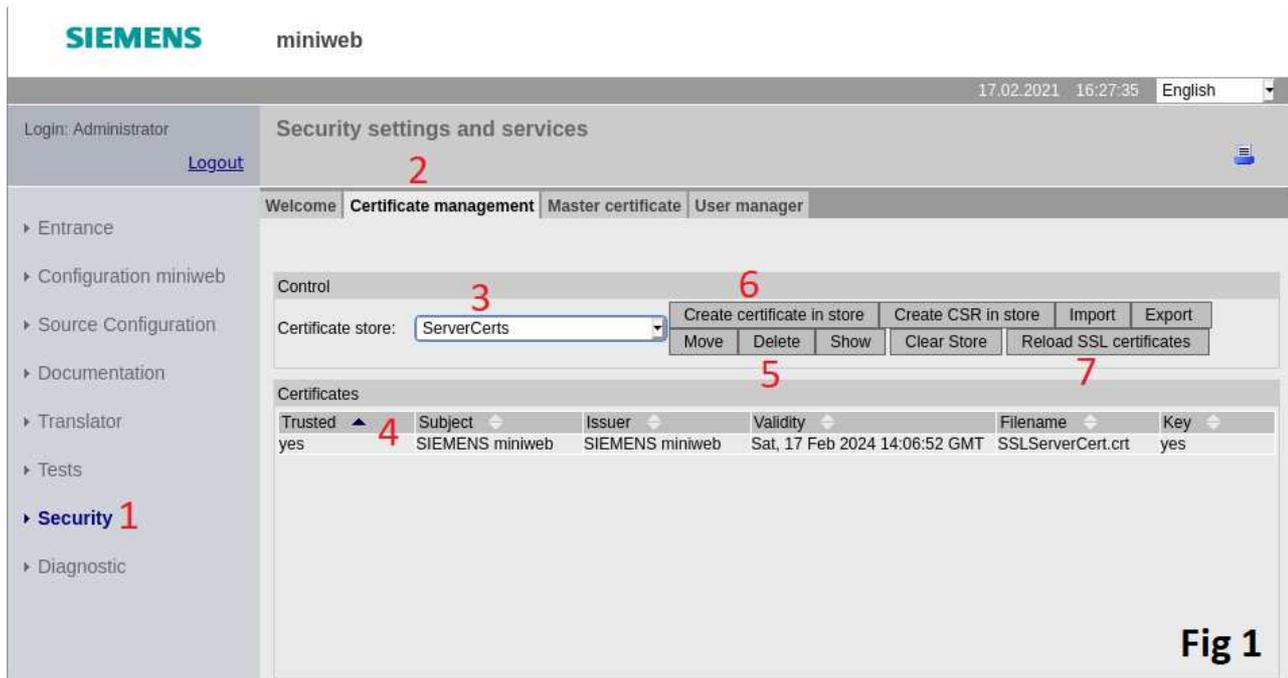


Fig 1

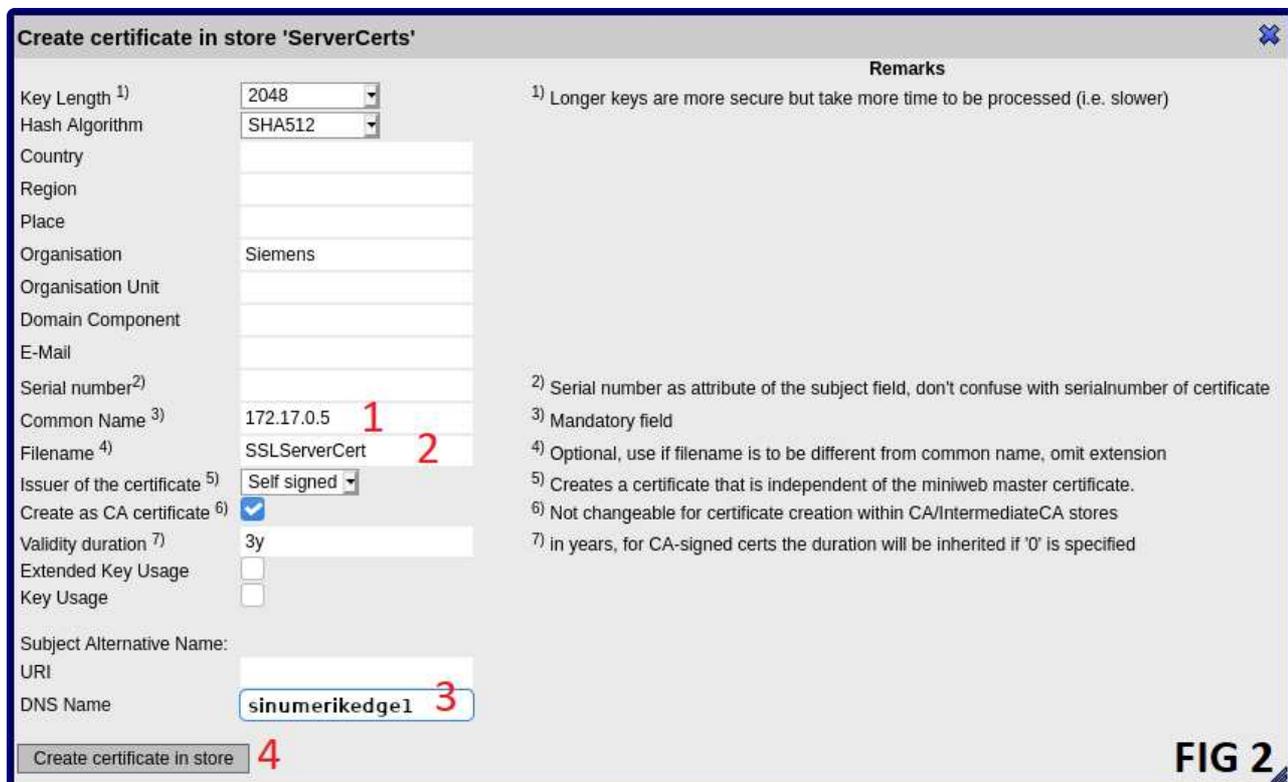


FIG 2

1. Navigate to **Security** page. (Fig 1)
2. Open **Certificate Management** tab. (Fig 1)
3. Click **Certificate Store** drop down box and select **ServerCerts** store. (Fig 1)

4. Click existing row where certificate name matches with `SSLServerCert.crt`. (Fig 1)

By default, reverse proxy will have a SSL server certificate created. In order to override this pre-existing certificate must be deleted. In case of lack of certificate, reverse proxy will automatically create one. 5. Click `Delete` button. (Fig 1) 6. Start creation of new certificate by clicking `Create certificate in store` button. (Fig 1) 1. Fill `Common Name` field with IP address of your device in case of IP based access is desired, otherwise anything arbitrary can be written. (Fig 2) 2. Fill `Filename` field exactly as "SSLServerCert". (Fig 2) 3. Fill `DNS Name` field with DNS name of your device in case of DNS based access is desired, otherwise this field can be left blank. (Fig 2) 4. Click `Create certificate in store` button. (Fig 2) 7. Click `Reload SSL certificates` button to make the created certificate to take in effect. (Fig 1) 1. Check the checkbox labeled 1. (Fig 3) 1. Click `Reload SSL certificates` button. (Fig 3)



OPENSSL COMMAND LINE

In order to create an SSL server certificate, the below instructions can be followed.

1. `openssl req -x509 -subj '/CN=Certificate Authority' -days 365 -newkey rsa:4096 -nodes -keyout ca.pem -out ca.crt`

This creates a certificate authority. The certificate authority (CA) is a certificate that is used for issuing and verifying SSL server certificates. To create a certificate authority, this command can be issued.

The command should create two files, namely `ca.crt`, which is a certificate authority and `ca.pem`, which is a private key for certificate authority `ca.crt`. These files are to be used for issuing an SSL server certificate.

2. `openssl req -subj '/CN=<PUBLIC-HOSTNAME-OR-IP-ADDRESS-OF-NANOBOX>' -days 365 -newkey rsa:4096 -nodes -keyout server.pem -out server.csr`

This creates an SSL Server certificate. In order to create an SSL server certificate for reverse proxy usage, this command can be issued. **Beware** that the common name (CN) field of the certificate must match with the hostname or IP address of edge device. Otherwise, the certificate would fail to authenticate.

The command should create two files, namely `server.csr`, which is a certificate signing request (CSR) and `server.pem`, which is a private key for `server.csr`. The CSR is to be signed by the CA to create a certificate for reverse proxy.

3. `openssl x509 -req -days 365 -in server.csr -extfile <(printf 'subjectAltName=DNS:<DNS>,IP:<IP>') -CA ca.crt -CAkey ca.pem -CAcreateserial -out server.crt`

This signs the SSL server CSR with CA. In order to issue a signed SSL server certificate for reverse proxy, this command can be issued.

The command should create a file named `server.crt`, which is a signed SSL server certificate. Recent web browsers like Chrome require certificates to include `subjectAltName` extension, hence users are required to specify their DNS name/IP address in resulting certificate. The `DNS:<DNS>` can be omitted if not used. The created certificate should be verifiable by the CA certificate. To do that, the below command can be issued.

```
openssl verify -CAfile ca.crt server.crt
```

The command should output `server.crt: OK` indicating that the certificate is indeed verifiable by CA.

Importing an SSL Server Certificate

In order to import an SSL server certificate to reverse proxy, the certificate and its key file need to be bundled as PKCS#12 format. To do that, the following command can be issued. The command is interactive and should prompt the user's input for a PKCS#12 password. This password must be non-zero length since reverse proxy requires a PKCS#12 file to be password protected. **Beware** that the file must be named as `SSLServerCert.p12` since reverse proxy with its default settings uses this predefined name.

```
openssl pkcs12 -export -clcerts -in server.crt -inkey server.pem -out SSLServerCert.p12
```

After getting the file ready, users can import the PKCS#12 file from reverse proxy UI. This can be done from the certificate management page. Users can navigate to this page by following the steps below.

1. Click `Security` on the navigation menu
2. Click `Certificate management` tab
3. Choose `ServerCerts` as the certificate store

Users should notice an existing auto-generated server certificate in the store named `SSLServerCert.crt`. In order to import another certificate, this should be removed. To do so, users can click on the certificate and then click the `Delete` (4) button. After this, users can get to import certificate dialog by clicking on the `Import` button (5). See `Fig 1` below. In the dialog, should users select `SSLServerCert.p12` file and fill the passphrase field. Beware that `Destination store` should read as `ServerCerts` and `SaveAs` should read as `SSLServerCert.crt`. Users can click the `Import` button to finalize the upload stage. Upon successful upload, a pop-up should appear notifying `Certificate successfully imported!`. After this, the `Reload SSL Certificates` (6) button should be clicked. Clicking this will create a confirmation prompt. After confirming, a pop-up could appear saying `Error on ReinitSSL: ReInitSSL failed, will be deferred until no connections active.`. This means the imported certificate can't be used until all the active SSL connections closed. Closing all browsers connected to reverse proxy at this point should suffice. Please note that closing a tab would not guarantee the connection is closed, so the whole browser process should be terminated.

SIEMENS miniweb

28.11.2019 17:33:52 English

Login: Administrator [Logout](#)

Security settings and services

Welcome | **Certificate management** | Master certificate | User manager

Control

Certificate store: **ServerCerts**

Create certificate in store | **Import** | Export | Move

Delete | Show | Clear Store | Reload SSL certificates

Certificates

Trusted	Subject	Issuer	Validity	Filename	Key
yes	SIEMENS miniweb	SIEMENS miniweb	Mon, 28 Nov 2022 15:33:43 GMT	SSLServerCert.crt	yes

1 Security

Diagnostic

Fig 1

Verifying Reverse Proxy SSL Server Certificate

The certificate authority (CA) file is used to verify the SSL server certificate of reverse proxy, and it is used for connecting reverse proxy securely. The CA file can be used by the client application such as browsers. For the most part, this can be achieved by importing CA files into user's system by using user's operating system.

An example with `curl` without using CA file should result in SSL error.

```
$ curl -L https://reverseproxy:5443/
curl: (60) SSL certificate problem: unable to get local issuer certificate
More details here: https://curl.haxx.se/docs/sslcerts.html

curl failed to verify the legitimacy of the server and therefore could not
establish a secure connection to it. To learn more about this situation and
how to fix it, please visit the web page mentioned above.
```

An example with `curl` using CA file should verify and connect reverse proxy using SSL.

```
$ curl --cacert ca.crt -L https://reverseproxy:5443/
<!DOCTYPE html><html xmlns="http...
```

Trusted Client Certificates

Trusted client certificates are used for making authenticated requests to reverse proxy. These certificates can be managed under the `TrustedClients` certificate store from reverse proxy UI. For users who want to create their client certificate, please refer to [Creating Client Certificate](#). To import a client certificate, please refer to [Importing Trusted Client Certificate](#).

Creating Client Certificate

In order to create a client certificate, the below instructions can be followed.

1. `openssl req -newkey rsa:4096 -keyout key.pem -out cert.csr -nodes -days 365`

This creates a private key & a certificate signing request. Client certificates work in pairs with private keys and certificates. In order to create a private key and certificate signing request (CSR), this command can be issued. A CSR is an intermediate certificate file that is to be signed to create a final certificate.

The command is interactive and will ask users to fill in several fields. The only field relevant for the reverse proxy is currently `Common Name` (CN) field. CN field matches the user name that will be seen by the applications behind reverse proxy while using a client certificate based authentication mechanism. Users are free to provide the appropriate information for other fields.

The command should create two files, namely `cert.csr`, which is a certificate signing request (CSR) and `key.pem`, which is a private key for the certificate.

2. `openssl x509 -req -in cert.csr -signkey key.pem -out cert.crt -days 365`

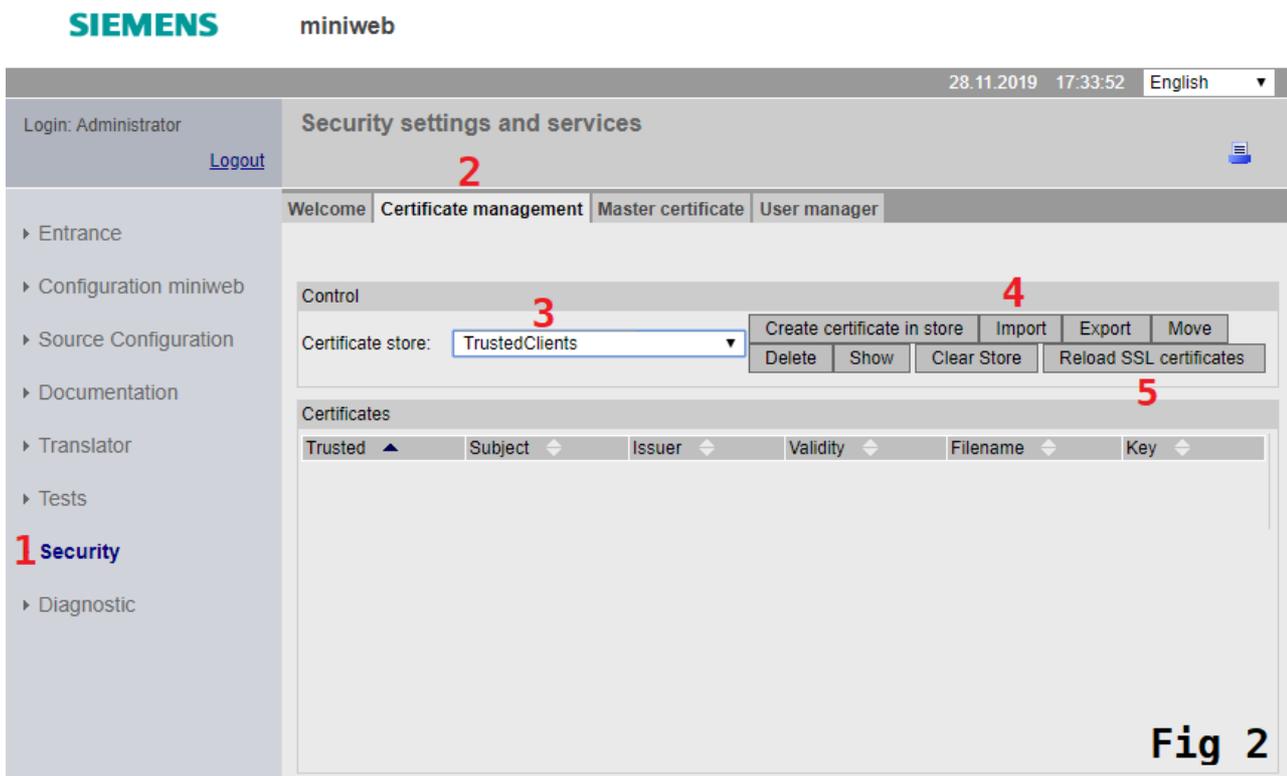
This creates a self-signed certificate. In order to create a self-signed certificate using private key and CSR files, this command can be issued.

The command should create a file named `cert.crt`, which is a self-signed certificate. This certificate can be imported to reverse proxy in order to allow it to verify the client.

Importing Trusted Client Certificate

In order to allow the reverse proxy to verify the user authenticity, the certificate file must be imported to it. This can be done from the certificate management page. Users can navigate to this page by clicking `Security` on the navigation menu (1), clicking on the `Certificate management` tab (2) and choosing the `TrustedClients` as the certificate store (3). Import dialog can be opened up by clicking on the `Import` button (4). For image, please see

Fig 2 below. The certificate import is completed upon selecting the appropriate certificate and clicking the **Import** button in the dialog menu. In order to imported certificates to take effect, users are required to reload certificates by clicking **Reload SSL certificates** (5) button and confirming popup.



Importing the PKCS#12 File to Windows

In order to authenticate using the client certificate, the certificate and key files need to be bundled as a PKCS#12 file. After having a PKCS#12 file, it can be imported by users operating system to enable browsers to use client certificate authentication mechanisms using those pairs. This file also can be used by applications like `curl`. For this documentation, Windows is chosen as an example.

The below command can be issued to create a PKCS#12 file from key and certificate pairs.

```
openssl pkcs12 -export -out bundle.p12 -in cert.crt -inkey key.pem
```

The command should create a file named `bundle.p12`, which can be double-clicked on to import it in the Windows operating system. After importing, the certificate can be used for authenticating the client.

Users

Administrator and Users

There's a built-in root user (Administrator) who can manage user accounts, their rights, and the overall system security. User cannot be deleted and is a member of all the user groups. This user is surely there (as long as you have an interactive user management). User can also create a "twin" administrator that is a member of the same groups as user is. But this twin won't receive all the new group memberships and won't be protected from deletion. However, the root user will be able to delete this twin, since, in order to be able to manage a user, the user executing the action must share all groups with that user.

So, you can create an own administrator by using the UserEditor. This admin can be authorized for your application's specific user groups. You can protect the user groups and users from other administrators.

Login: Administrator [Logout](#)

Security settings and services

Welcome | Certificate management | Master certificate | **User manager**

MINIWEB USER EDITOR
Management of user permissions

User list

- Administrator
- amwcapture
- amwtoolpath
- Anonymous
- Diag
- TraceUser
- User

Change user Administrator

Login: Administrator
Real name: Administrator User.
Description: Administrator of this miniweb
Preferred Language: e.g. en
Old password:
Password:
Confirm password:

User groups

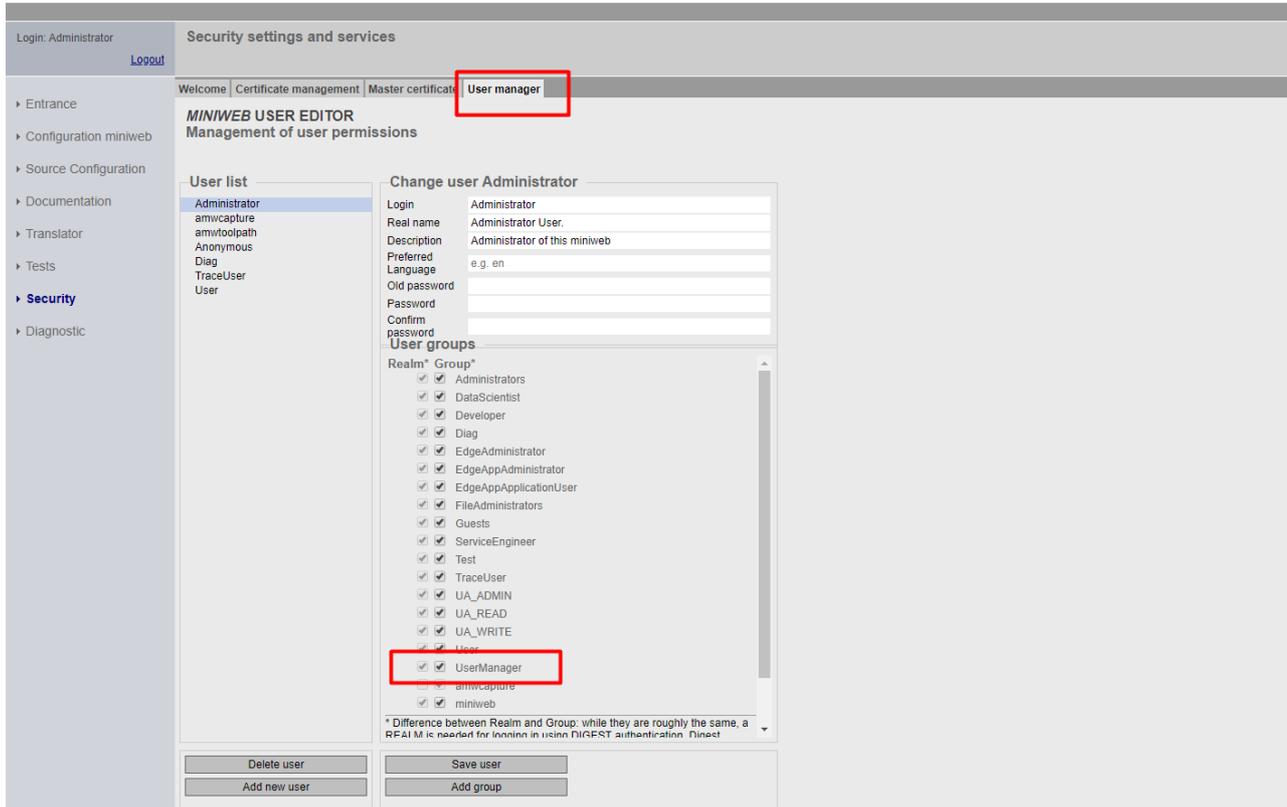
Realm*	Group*
<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/> Administrators
<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/> DataScientist
<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/> Developer
<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/> Diag
<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/> EdgeAdministrator
<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/> EdgeAppAdministrator
<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/> EdgeAppApplicationUser
<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/> FileAdministrators
<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/> Guests
<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/> ServiceEngineer
<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/> Test
<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/> TraceUser
<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/> UA_ADMIN
<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/> UA_READ
<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/> UA_WRITE
<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/> User
<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/> UserManager
<input type="checkbox"/>	<input checked="" type="checkbox"/> amwcapture
<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/> miniweb

* Difference between Realm and Group: while they are roughly the same, a REALM is needed for logging in using DIGEST authentication. Digest

Delete user | Add new user | Save user | Add group

User Credentials

A User who has UserManager group rights can set a new password for other users without knowing the old one under the UserEditor menu. There is no "Forgot Password" feature for users. Users can reset their password on their own, only if they know the old password. Also, there is a timeout limit for user sessions. It cannot be configured in runtime.



User Groups

There are predefined user groups for the system overall such as miniweb, User, Administrator, etc.. There are also app specific groups defined for several roles on Edge Applications:

Edge Administrator, Edge App User, Edge App Restricted User, Edge App Administrator

You may develop the application in accordance with the "X-User-Groups" header which transports group info. Moreover, you can add own user groups by using the UserEditor.

Language

The language is determined by the order of the precedence of a cookie, a websso login, an "accept-language" header or a system default in the system configuration. The preferred language in User Editor is not related to the user sessions.

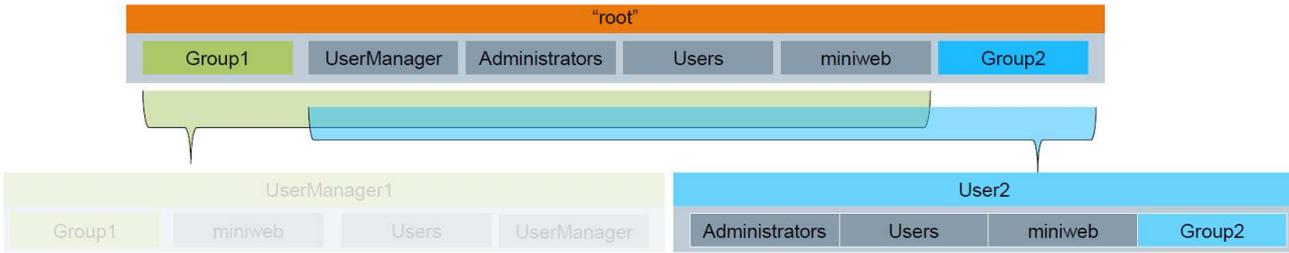
User/Group Management and Privileges



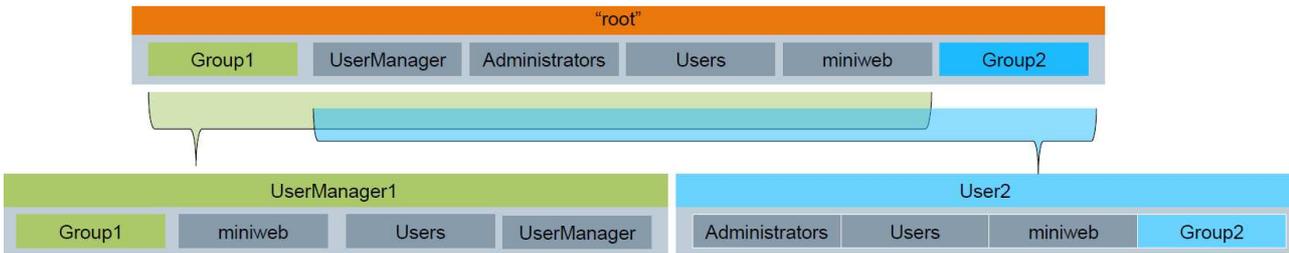
- The administrator (root) is a member of **All** existing and newly created groups in the server including:
 - miniweb: all users of the user database, including Anonymous
 - Users: all authenticated users
- The administrator can manage all users in the server
- Can create an equal twin which can be managed or deleted by the root administrator but the other way is not

possible

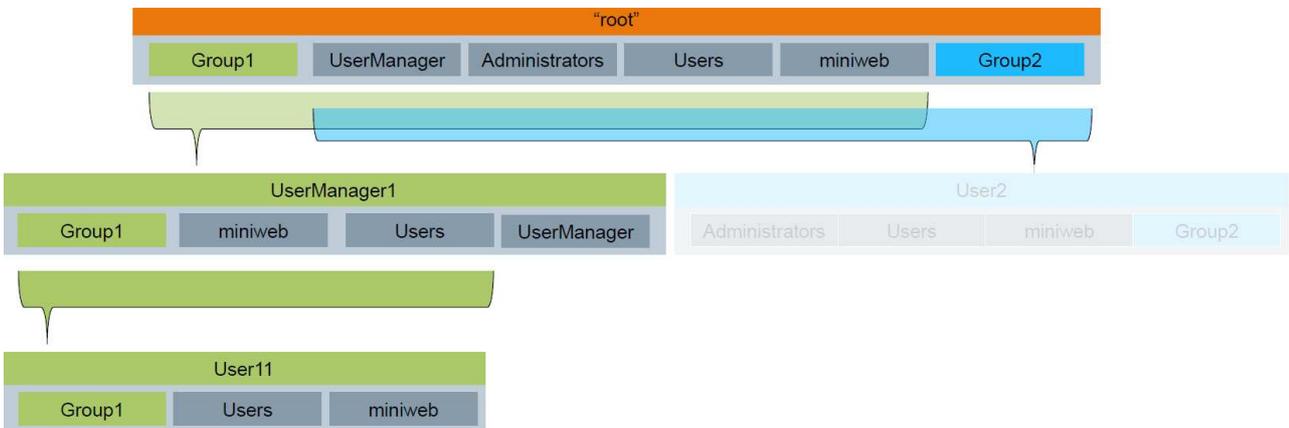
- For other privileged tasks (shutdown server, manage certificates, ...), the membership of group administrators is sufficient!



- The user lacks the membership of Group1 and UserManager, so cannot manage any other user
- The user is a member of Administrators, can call privileged actions



- The user lacks the membership of Group2 and Administrators, so can manage and create users which user shares all groups with (therefore not User2)
- Can create an equal twin by inheriting all of his groups to the twin and can be deleted by that twin
- Cannot manage the "Administrator" since user lacks the Group2 membership
- Cannot call privileged actions



- A regular user is only member of Group1
 - Can only use resources allowed for Group1 or Users
-

Data provisioning to Insights Hub IoT Data Model

Login to the Insights Hub with your credentials.

Note: As a prerequisite, an agent asset (Industrial Edge) should be created from the *Asset Manager* and asset status should be onboarded.

For data provisioning, there are three main steps:

- System Apps Configuration for Data Provisioning
- Custom Apps Configuration for Data Provisioning
- Monitoring Configuration for Data Provisioning from the *Monitor*

System Apps Configuration for Data Provisioning

To enable SINUMERIK EDGE for data provisioning the system application **SinumerikAdapter** must be installed and activated on the device. For more details how to do that please refer to the chapter [Enable access to SINUMERIK NCU](#).

Custom Apps Configuration for Data Provisioning

1) For data provisioning, a custom application should be installed to SINUMERIK Edge. First, find your onboarded asset and click the **New Application** button.

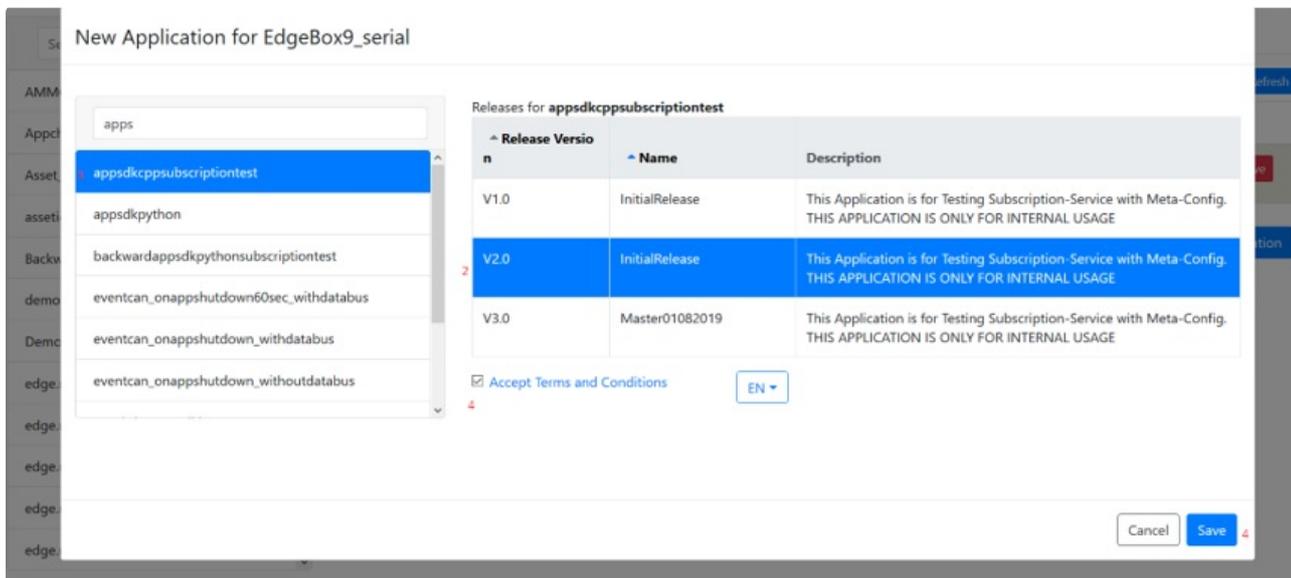
App Management Jobs

EdgeBox9_serial (ONBOARDED) ✓ Refresh

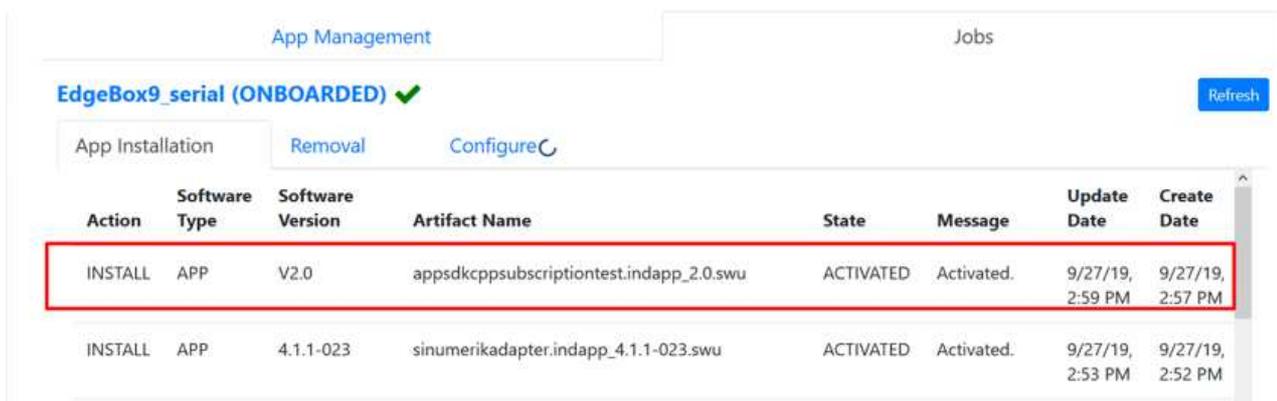
App Name	Release Name	Version	Description	Operations
sinumerikadapter	Test-candidate-Edge-V2.1	4.1.1-023	License type: Single License. Test candidate Edge V2.1 PRELIMINARY - ONLY FOR INTERNAL USAGE!	Install Remove

New Application

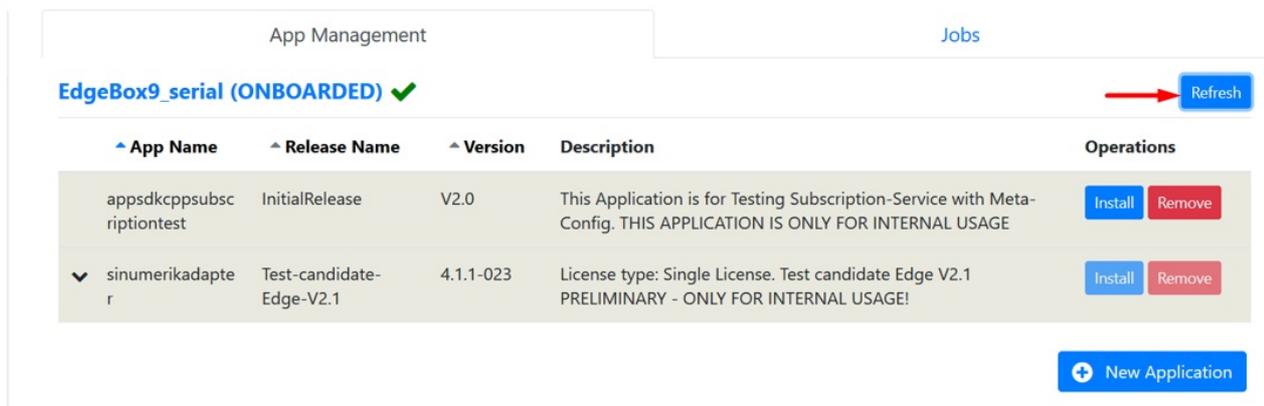
2) Select your custom application, select its release version and confirm the **Accept Terms and Conditions**. Finally, click the **Save** button. This operation will trigger downloading the app to SINUMERIK Edge.



3) On the "Jobs" tab, in the "Installation" section, the application downloading status can be seen. Also by clicking the **Refresh** button in the "Job" tab, the updated status can be seen. If the Status is "ACTIVATED", it means that the downloading operation is over.



4) After the "ACTIVATED" Status, go back to the "App Management" tab, click the **Refresh** button. Your custom application can be seen in the "App Management" tab.



5) To install the application that you downloaded, on the "App Management" tab click the **Install** button.

App Management Jobs

EdgeBox9_serial (ONBOARDED) ✓ Refresh

App Name	Release Name	Version	Description	Operations
↑ appsdkcppsubscriptiontest	InitialRelease	V2.0	This Application is for Testing Subscription-Service with Meta-Config. THIS APPLICATION IS ONLY FOR INTERNAL USAGE	Install Remove
▼ sinumerikadaptest	Test-candidate-Edge-V2.1	4.1.1-023	License type: Single License. Test candidate Edge V2.1 PRELIMINARY - ONLY FOR INTERNAL USAGE!	Install Remove

+ New Application

6) On the "Jobs" tab, in the "Configure" section, the application installation status can be seen. Also by clicking the Refresh button in the "Job" tab, the updated status can be seen. If the Status is "CONFIGURED" and the message is "OK", it means that the installing operation is over.

App Management Jobs

EdgeBox9_serial (ONBOARDED) ✓ Refresh

Installation Removal **Configure**

State	Message	Create Date	Update Date
CONFIGURED	OK	2018-08-29T11:17:06.660Z	
CONFIGURED	OK	2018-08-29T11:12:45.425Z	
CONFIGURED	OK	2018-08-29T08:44:09.831Z	
CONFIGURED	OK	2018-08-29T08:42:56.662Z	
CONFIGURED	OK	2018-08-29T08:36:51.306Z	

7) To start the application, on the "App Management" tab, click the expand icon on the left side of the application button, then click the Start icon from the operations section.

App Management Jobs

EdgeBox9_serial (ONBOARDED) ✓ Refresh

App Name	Release Name	Version	Description	Operations										
↑ appsdkcppsubscriptiontest	InitialRelease	V2.0	This Application is for Testing Subscription-Service with Meta-Config. THIS APPLICATION IS ONLY FOR INTERNAL USAGE	Install Remove										
<table border="1"> <thead> <tr> <th>Instance Name</th> <th>Status</th> <th>Cloud Upload</th> <th>Umati</th> <th>Operations</th> </tr> </thead> <tbody> <tr> <td>appsdkcppsubscriptiontest.InitialRelease</td> <td>STOPPED</td> <td>×</td> <td>×</td> <td>🔄 ⚙️ ▶️ 🗑️</td> </tr> </tbody> </table>				Instance Name	Status	Cloud Upload	Umati	Operations	appsdkcppsubscriptiontest.InitialRelease	STOPPED	×	×	🔄 ⚙️ ▶️ 🗑️	
Instance Name	Status	Cloud Upload	Umati	Operations										
appsdkcppsubscriptiontest.InitialRelease	STOPPED	×	×	🔄 ⚙️ ▶️ 🗑️										
▼ sinumerikadaptest	Test-candidate-Edge-V2.1	4.1.1-023	License type: Single License. Test candidate Edge V2.1 PRELIMINARY - ONLY FOR INTERNAL USAGE!	Install Remove										

+ New Application

8) On the "App Management" tab, the related application's status should be "RUNNING" afterwards.

App Management Jobs

EdgeBox9_serial (ONBOARDED) ✓ Refresh

App Name	Release Name	Version	Description	Operations
appsdkcppssubscriptiontest	InitialRelease	V2.0	This Application is for Testing Subscription-Service with Meta-Config. THIS APPLICATION IS ONLY FOR INTERNAL USAGE	Install Remove

Instance Name	Status	Cloud Upload	Umati	Operations
appsdkcppssubscriptiontest.InitialRelease	RUNNING	✖	✖	🗑️ ⚙️ 📄

sinumerikadapte r	Test-candidate-Edge-V2.1	4.1.1-023	License type: Single License. Test candidate Edge V2.1 PRELIMINARY - ONLY FOR INTERNAL USAGE!	Install Remove
-------------------	--------------------------	-----------	---	----------------

[+ New Application](#)

9) On the "Jobs" tab, the application's starting status can be seen. Also by clicking the Refresh button in the "Job" tab, the updated status can be seen. If the Status is "CONFIGURED", it means that the installing operation is over.

App Management Jobs

EdgeBox9_serial (ONBOARDED) ✓ Refresh

Installation Removal **Configure**

State	Message	Create Date	Update Date
CONFIGURED	OK	2018-08-29T11:17:06.660Z	
CONFIGURED	OK	2018-08-29T11:12:45.425Z	
CONFIGURED	OK	2018-08-29T08:44:09.831Z	
CONFIGURED	OK	2018-08-29T08:42:56.662Z	
CONFIGURED	OK	2018-08-29T08:36:51.306Z	

10) To be able to send data to Insights Hub through this custom application, the Cloud Upload functionality should be enabled. On the "App Management" tab, click the expand icon on the left side of the application button, then click the Cloud icon from the operations section.

App Management Jobs

EdgeBox9_serial (ONBOARDED) ✓ Refresh

App Name	Release Name	Version	Description	Operations
appsdkcppssubscriptiontest	InitialRelease	V2.0	This Application is for Testing Subscription-Service with Meta-Config. THIS APPLICATION IS ONLY FOR INTERNAL USAGE	Install Remove

Instance Name	Status	Cloud Upload	Umati	Operations
appsdkcppssubscriptiontest.InitialRelease	RUNNING	✖	✖	🗑️ ⚙️ 📄 ☁️

sinumerikadapte r	Test-candidate-Edge-V2.1	4.1.1-023	License type: Single License. Test candidate Edge V2.1 PRELIMINARY - ONLY FOR INTERNAL USAGE!	Install Remove
-------------------	--------------------------	-----------	---	----------------

[+ New Application](#)

11) On the "Jobs" tab, the application's configuring status can be seen. Also by clicking the **Refresh** button in the "Job" tab, the updated status can be seen. If the Status is "CONFIGURED", it means that the installing operation is over.

App Management		Jobs	
EdgeBox9_serial (ONBOARDED) ✓			Refresh
Installation	Removal	Configure	
State	Message	Create Date	Update Date
CONFIGURED	OK	2018-08-29T11:17:06.660Z	
CONFIGURED	OK	2018-08-29T11:12:45.425Z	
CONFIGURED	OK	2018-08-29T08:44:09.831Z	
CONFIGURED	OK	2018-08-29T08:42:56.662Z	
CONFIGURED	OK	2018-08-29T08:36:51.306Z	

12) After enabling, the Cloud Upload option should be green and a right/left arrow icon should appear in the operations options.

EdgeBox9_serial (ONBOARDED) ✓			Refresh		
App Name	Release Name	Version	Description	Operations	
appsdkcpsubscriptiontest	InitialRelease	V2.0	This Application is for Testing Subscription-Service with Meta-Config. THIS APPLICATION IS ONLY FOR INTERNAL USAGE	Install	Remove
Instance Name	Status	Cloud Upload	Umati	Operations	
appsdkcpsubscriptiontest.InitialRelease	RUNNING	✓	✗	⊕	⊖
sinumerikadaptr	Test-candidate-Edge-V2.1	4.1.1-023	License type: Single License. Test candidate Edge V2.1 PRELIMINARY - ONLY FOR INTERNAL USAGE!	Install	Remove

+ New Application

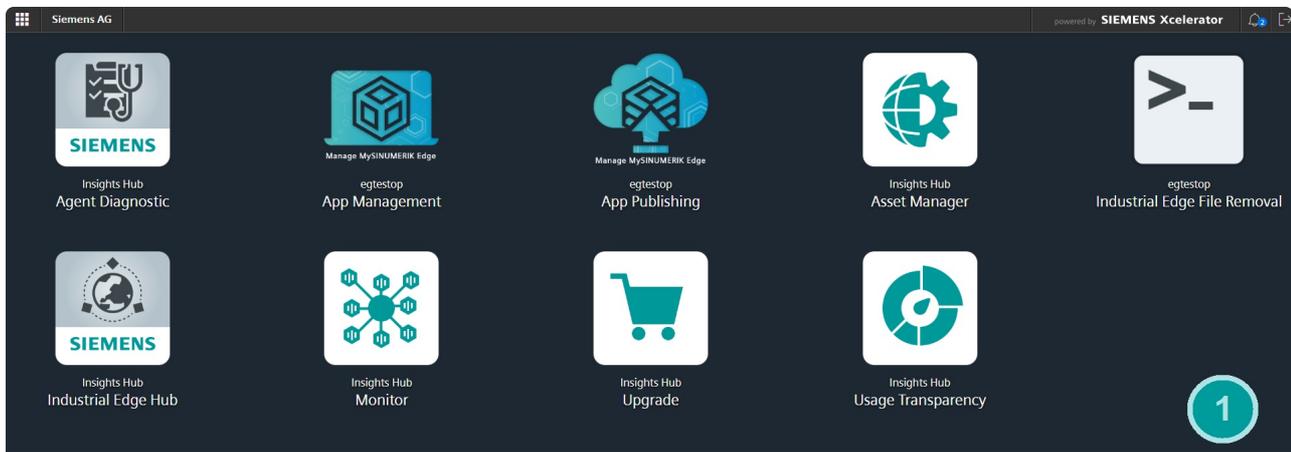
Warning

Please **disable** cloud upload feature of an application beforeuninstalling.

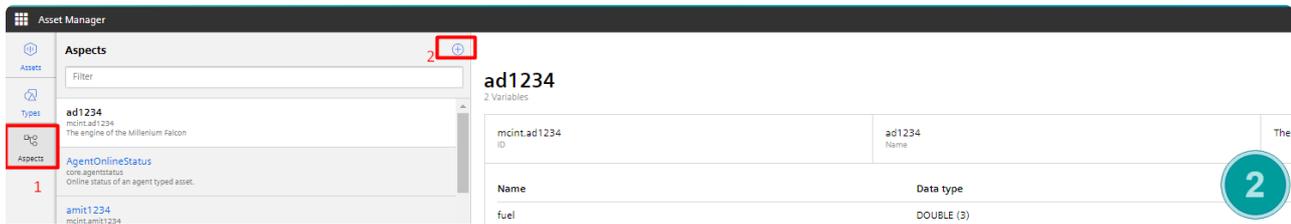
Monitoring Configuration for Data Provisioning from Monitor

A new asset should be created to monitor the data which is sent to the Insights Hub. This asset is different from the first **Agent** asset. This asset is called **Data Owner**.

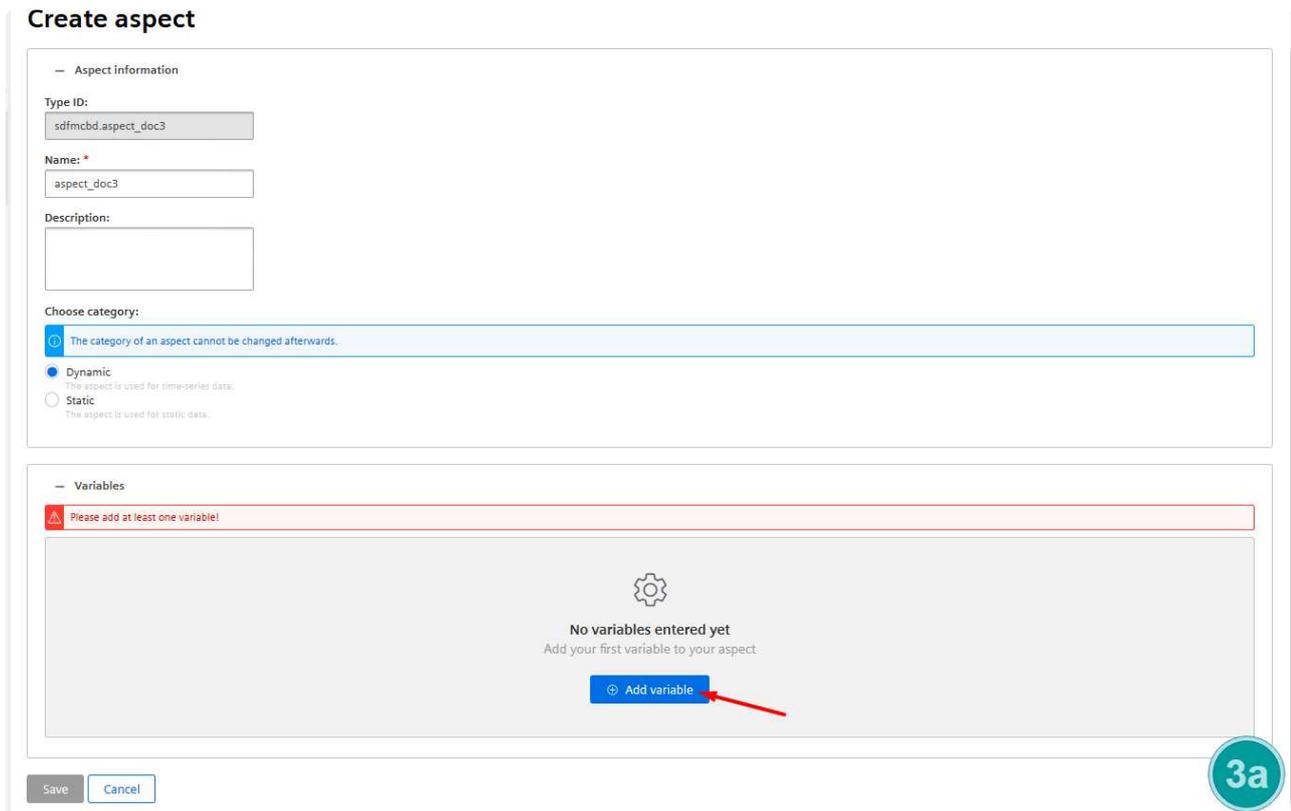
1) To create this new asset, choose the *Asset Manager* from the Insights Hub Launchpad.



2) As a first step an aspect type should be created for visualizing data points. Click **Aspects** then click the “+” button.



3) Fill mandatory fields. Add your variables' (Data Points)' names from the **Add variable** button.



Create aspect

— Aspect information

Type ID:
sdfmcbd.aspect_doc3

Name: *
aspect_doc3

Description:

Choose category:

The category of an aspect cannot be changed afterwards.

Dynamic
The aspect is used for time-series data.

Static
The aspect is used for static data.

— Variables

Variable names must be unique inside an aspect.
 Once a variable is added to the aspect it cannot be renamed or removed.

Add variable

Name	Data type	Unit	Max. length
PosX	DOUBLE	%	<input type="text"/>

3b

4) When you finish adding all variables click the Save button.

— Aspect information

Type ID:
sdfmcbd.aspect_doc3

Name: *
aspect_doc3

Description:

Choose category:

The category of an aspect cannot be changed afterwards.

Dynamic
The aspect is used for time-series data.

Static
The aspect is used for static data.

— Variables

Variable names must be unique inside an aspect.
 Once a variable is added to the aspect it cannot be renamed or removed.

Add variable

Name	Data type	Unit	Max. length
PosX	DOUBLE	%	<input type="text"/>
PosY	DOUBLE	%	<input type="text"/>
PosZ	DOUBLE	%	<input type="text"/>

4

5) After the Aspect type, an Asset Type which uses this aspect type should be created. Select **Types** on the *Asset Manager*, then click **Basic Device**.

Asset Manager | MindSphere

Assets

Filter

Types

Aspects

BasicAsset

BasicAgent

BasicApplication

BasicDevice

BasicHierarchy

DataOwner_demoTemp2

Demotemp_assettype

StgW_Type

TBUAssettype

core.basicasset > core.basicdevice

BasicDevice

7 Aspects

Aspect	Name
core.assetstatus	status

Name	Data type	Unit	Max. length	Default value	Default
manufacturer	STRING	-	255	-	Default

5

6) In the Basic Device section click the “+” button.

Asset Manager | MindSphere

Assets

Filter

Types

Aspects

assettype_data_temp4

assettype_doc3

basicdevice_position

BasicSimumerkAsset

data_owner_basic

encoderPositionAspectType

maktekFair

mckbackendbasic

mckbackendpostemp

releasecan2

core.basicasset > core.basicdevice

BasicDevice

1 Aspects

Aspect	Name
core.assetstatus	status

Name	Data type	Unit	Max. length	Default value	Default
manufacturer	STRING	-	255	-	Default

6

7) Fill in the mandatory fields. In the Aspects section select the Aspect that was created in previous section, click the Add button., then click Save.

Asset Manager | MindSphere

Assets

Filter

Types

Aspects

assettype_data_temp4

assettype_doc3

basicdevice_position

BasicSimumerkAsset

data_owner_basic

encoderPositionAspectType

maktekFair

mckbackendbasic

mckbackendpostemp

releasecan2

core.basicasset > core.basicdevice

Create type

Type information

Parent type: core.basicdevice

Type ID: sffmcbid_assettype_doc3

Name: *

Description:

Aspects *

sffmcbid_aspect_doc3

Name: *

aspect_doc3

Add aspect

Variables

Name	Data type	Unit	Max. length	Default value	Default
manufacturer	STRING	-	255	-	Default

Save Cancel

7

8) This section shows all related information.

assettype_doc3

1 Aspects

Asset Type Icon	sdfmcbd.assettype_doc3 ID	assettype_doc3 Name	Description
Aspect			
sdfmcbd.aspect_doc3	aspect_doc3		
core.assetstatus	status		

8

9) Using this Asset type, a Data Owner will be created. Select Assets on the Asset Manager, then click the "+".

The screenshot shows the 'Asset Manager' interface. On the left, the 'Assets' tab is selected and highlighted with a red box. A '+' button is also highlighted with a red box. The main area displays 'Basic settings' for an asset, including fields for Street, Postal code, Region, Latitude, Location, Country, and Longitude.

9

10) Select the Asset type that you created in a previous step.

The screenshot shows the 'Select type' dialog in the Asset Manager. The 'assettype_doc3' option is highlighted with a red box. The dialog lists various asset types with their respective aspect and variable counts. A 'Cancel' button is visible in the top right corner.

10

11) Fill in the mandatory fields and then click Save.

MindSphere

Add asset

General

Name:

Description:

Location

Street:

Postal code: Location:

Country: Region:

Geo-location

Latitude: Longitude:

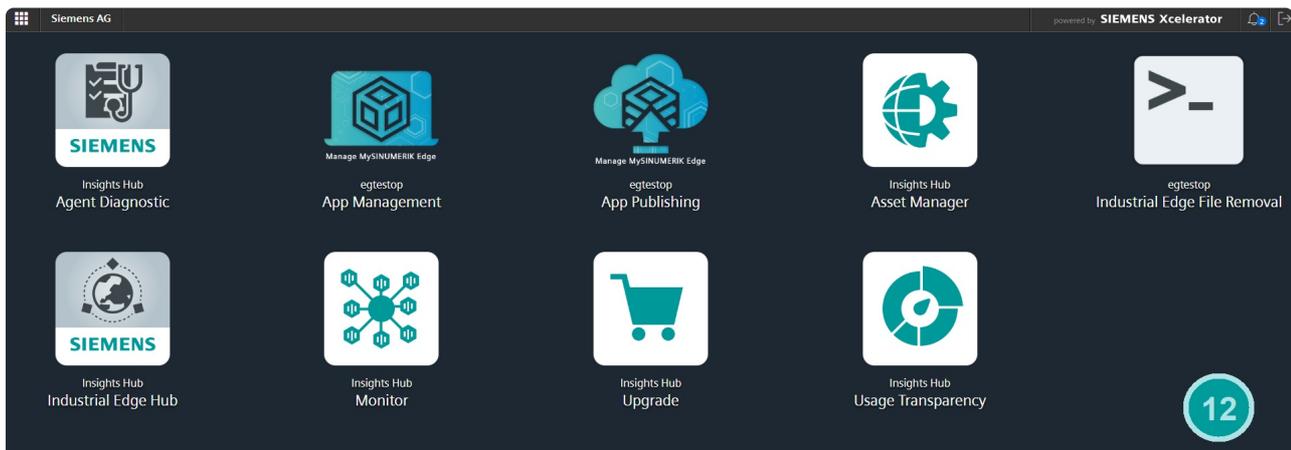
Aspects and variables

+ contactpoint		Contact point definition for basic asset hierarchy type			
Name	Data type	Max. length	Unit	Quality code	
contactType	STRING	255			
email	STRING	255			
faxNumber	STRING	255			
telephoneNumber	STRING	255			

* Required input field

11

12) After these steps Data Mapping should be configured for your custom application. Choose the *Manage MySINUMERIK Edge /App Management* from the Insights Hub Launchpad.



12

13) Find your Agent Asset first in the Asset list. On the "App Management" tab, click the expand icon on the left side, then click the arrow button for the "Data Mapping" functionality.

App Management Jobs

EdgeBox9_serial (ONBOARDED) Refresh

App Name	Release Name	Version	Description	Operations
↑ appsdkcppsubscriptiontest	InitialRelease	V2.0	This Application is for Testing Subscription-Service with Meta-Config. THIS APPLICATION IS ONLY FOR INTERNAL USAGE	Install Remove

Instance Name	Status	Cloud Upload	Umati	Operations
appsdkcppsubscriptiontest.InitialRelease	RUNNING	✓	✗	

▼ sinumerikadapter	Test-candidate-Edge-V2.1	4.1.1-023	License type: Single License. Test candidate Edge V2.1 PRELIMINARY - ONLY FOR INTERNAL USAGE!	Install Remove
--------------------	--------------------------	-----------	---	----------------

+ New Application
13

14) Click the Pick button to map the "Data Points" of the application with the Data Owner Asset's Aspects. This operation is mapping between Data Points that are coming from your SINUMERIK device and aspect names that you defined in the *Monitor*.

Search

- Dataowner_demoapp_onur4
- DataOwner_demodoc3
- dataowner.mcbackend
- Dataowner2_demoapp_onur4
- Demo_doc
- Demo_doc2
- Demo_doc3

Data Mapping

Source: demoappdatasource2

Source Param	Description	Unit	Type	SinumerikUid	
ENC1_POS_1	ENC1_POS_1	%	DOUBLE	ENC1_POS 1	Pick
ENC1_POS_2	ENC1_POS_2	%	DOUBLE	ENC1_POS 2	Pick
ENC1_POS_3	ENC1_POS_3	%	DOUBLE	ENC1_POS 3	Pick

Close

Jobs

Operations

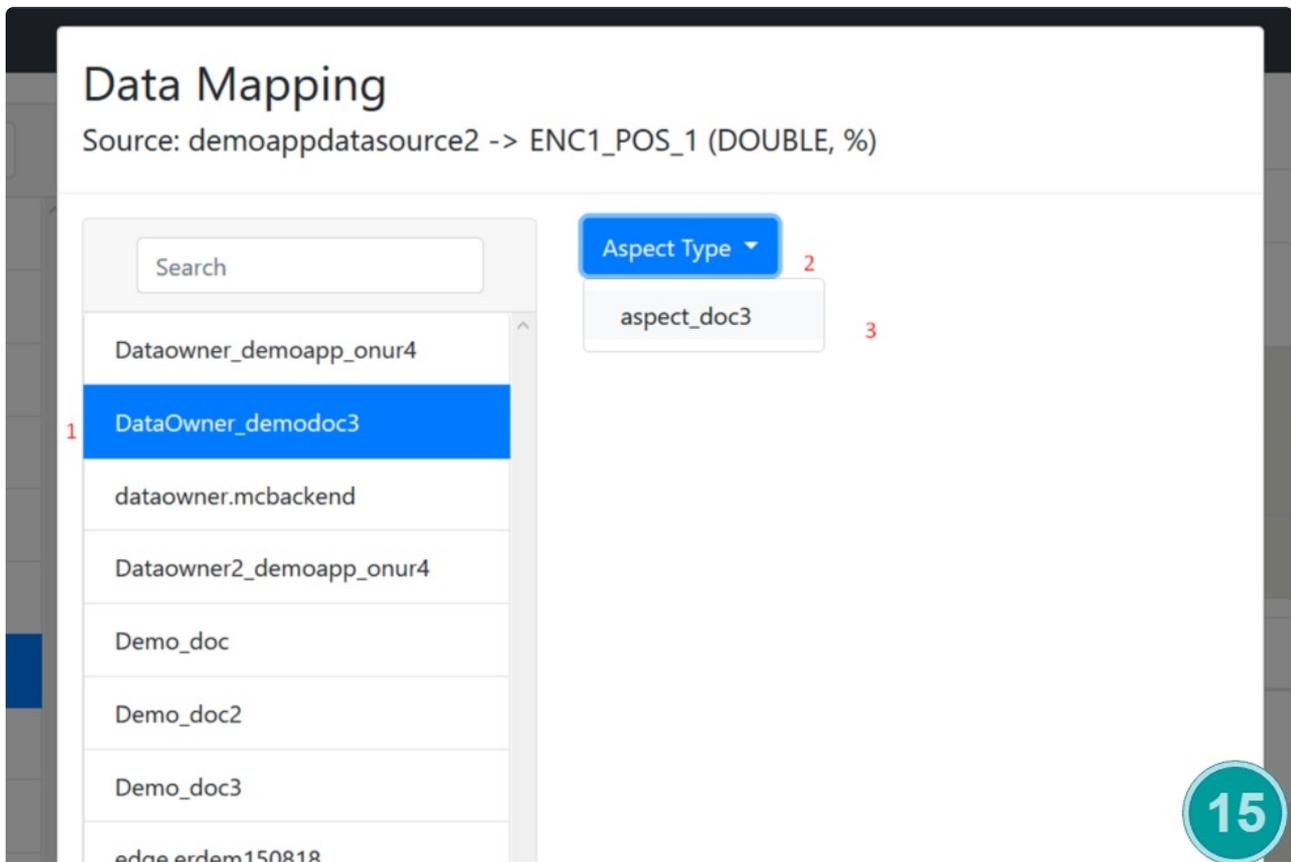
Install Remove

Install Remove

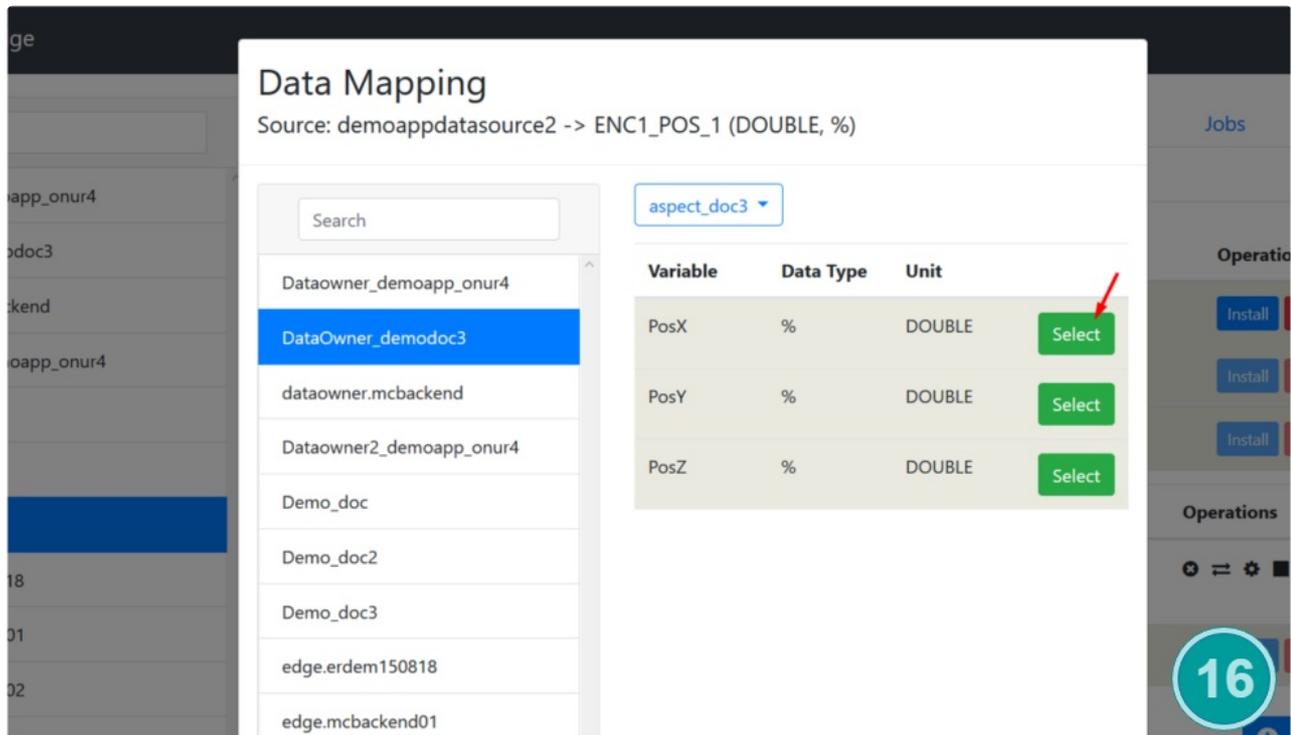
Install Remove

14

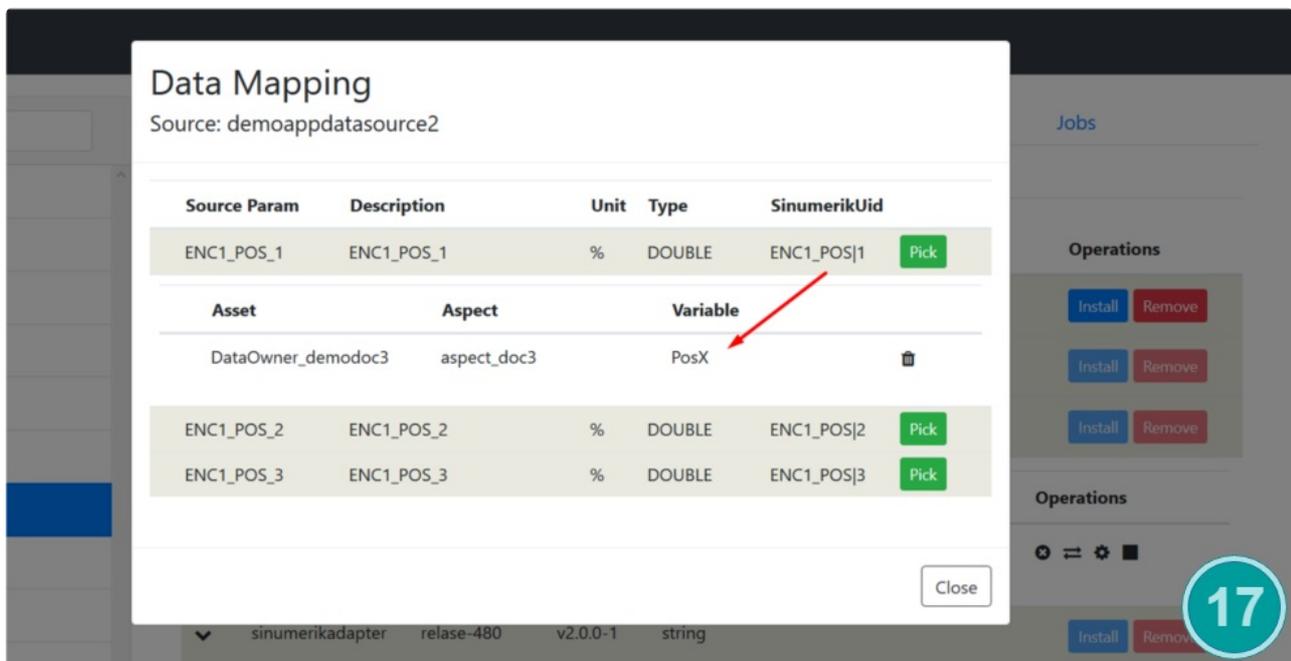
15) Select the Data Owner Asset that is created previously, then click the **Aspect Type** dropdown to select your type.



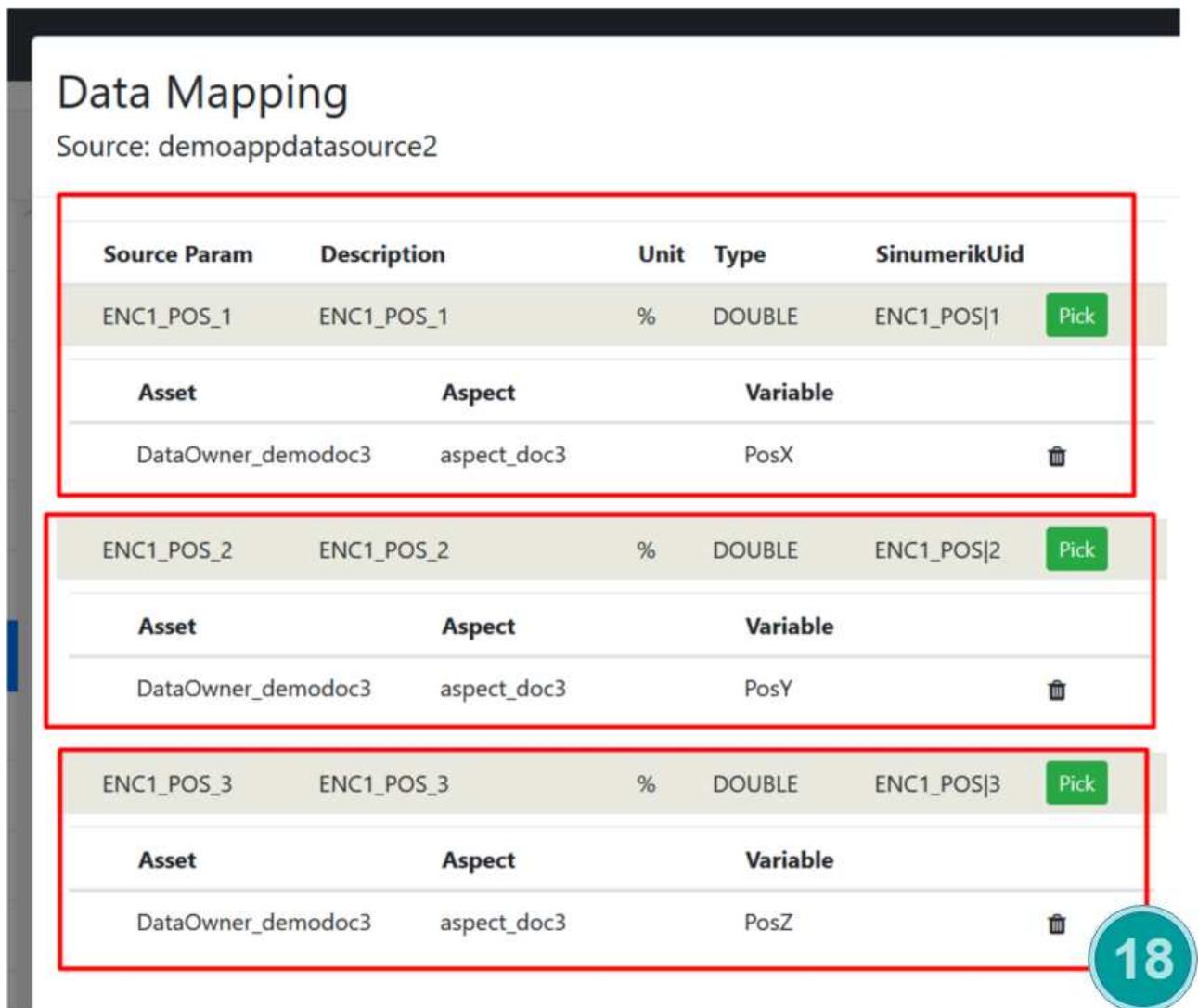
16) Select the Aspect Variable for the Data Point.



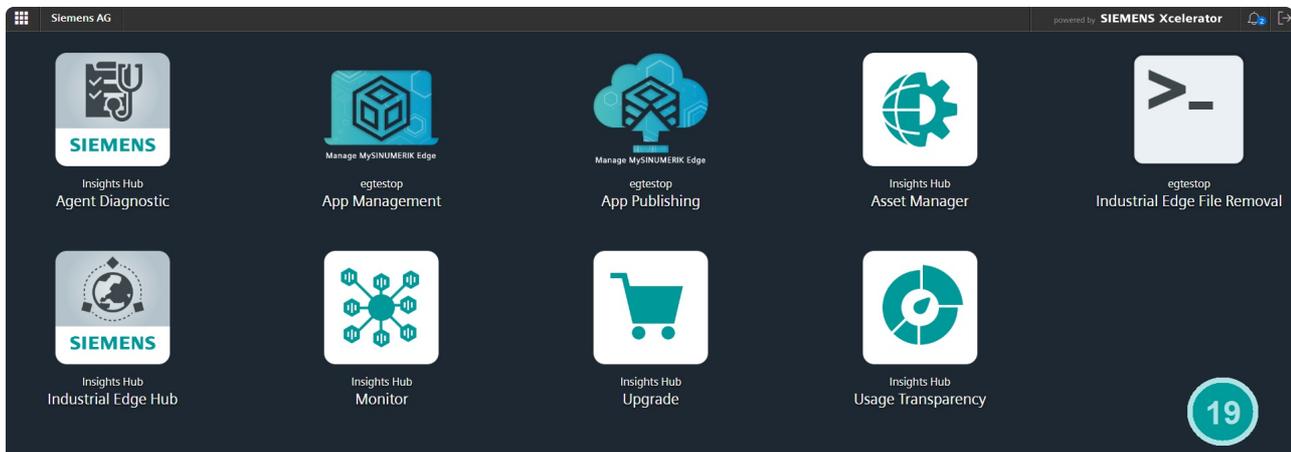
17) As a next step, a mapped Data Point and an Aspect Variable should be shown.



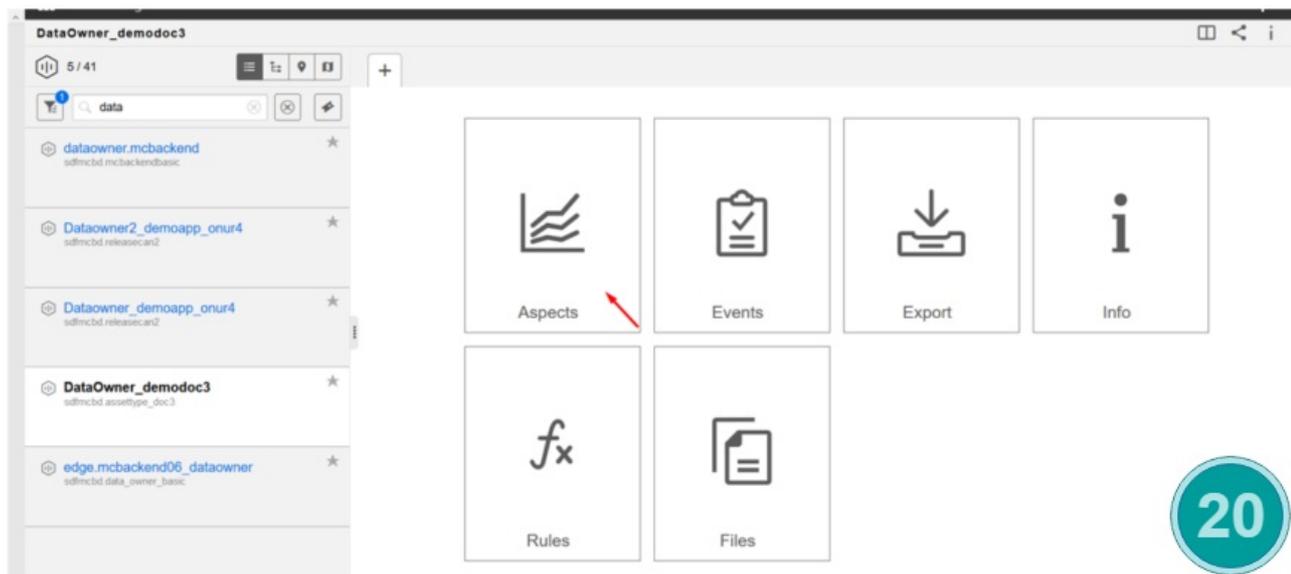
18) Continue the same steps to complete all mapping operations for other Data Points too.



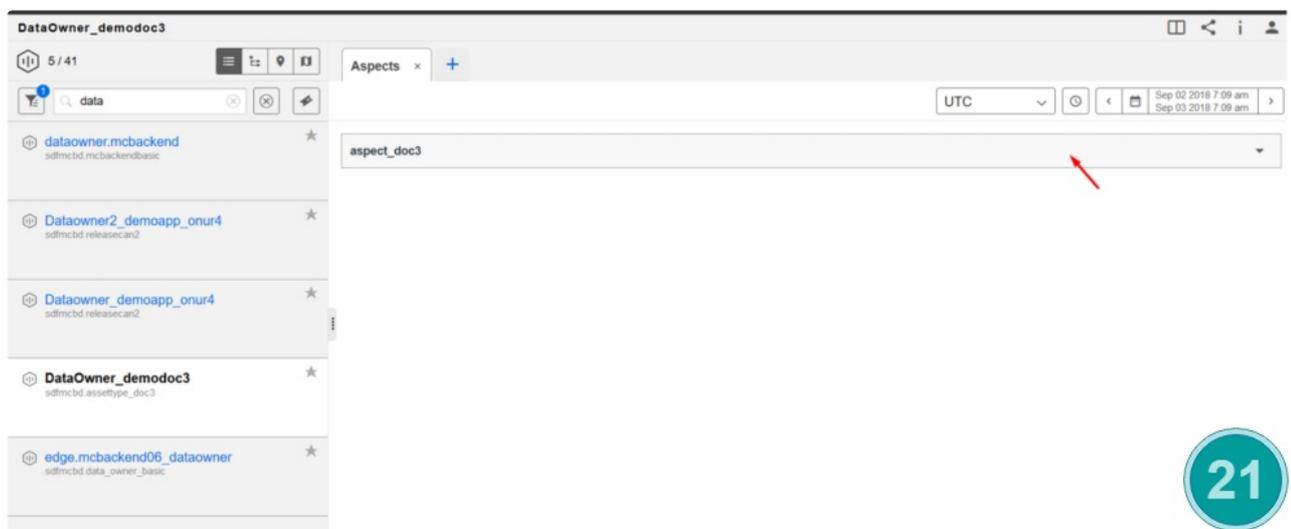
19) Connect a SINUMERIK machine to SINUMERIK Edge via cable. After that go to the *Monitor* on the Insights Hub Launchpad.



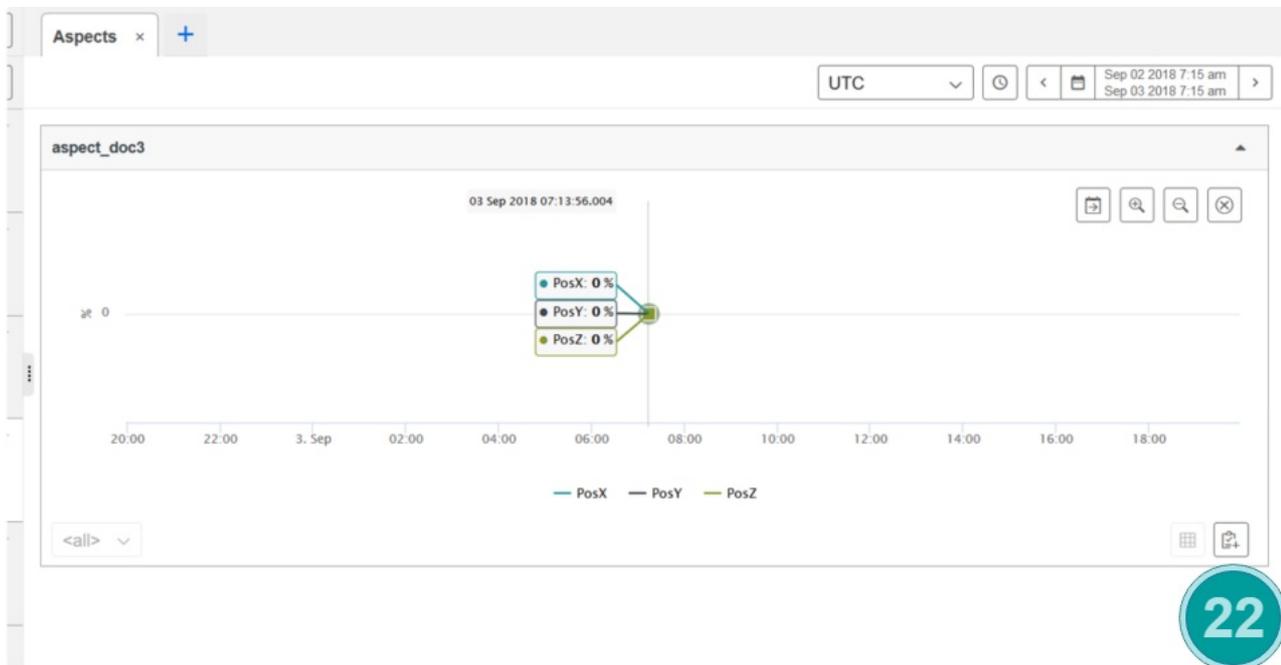
20) Select your Data Owner Asset then click Aspects



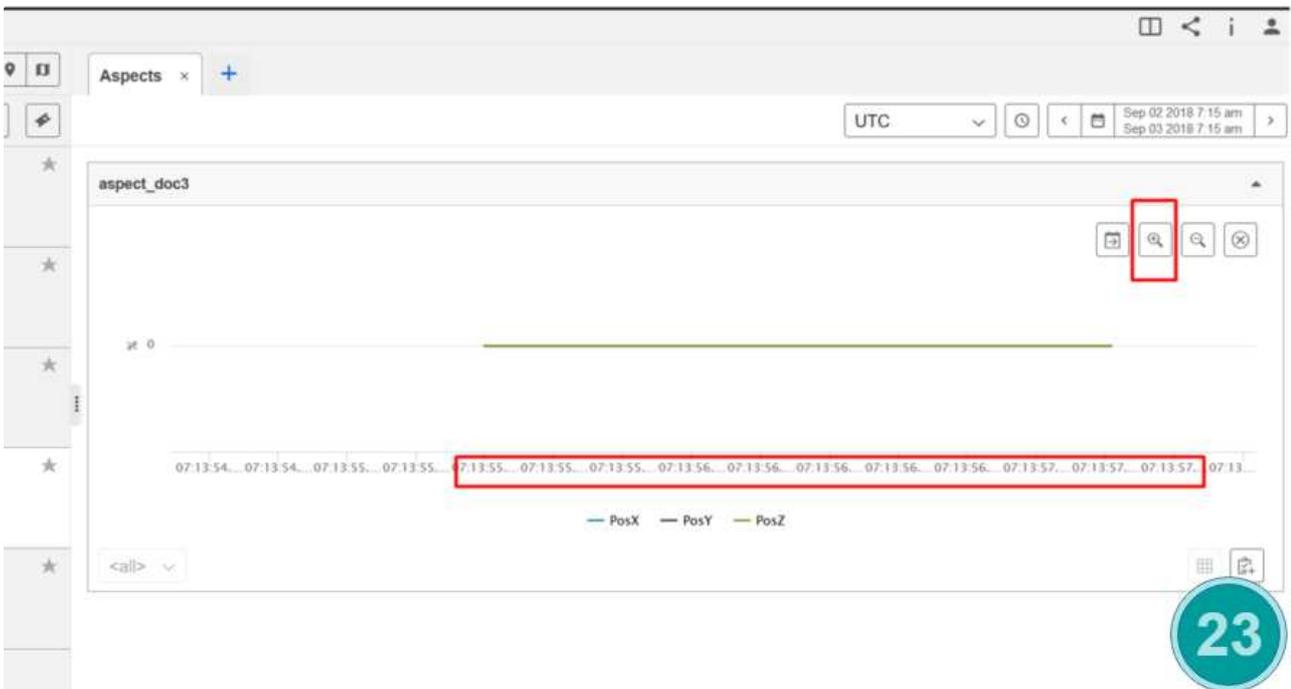
21) Expand the aspect name to see the data. Check the date/time range for the data.



22) Data Point names can be seen when mouse is on graph points.



23) Data Graph has Zoom In/Out and Date/Time selection features.



AppSDK

The Application Software Development Kit (AppSDK), is a collection of API's that enables Application Developers to gather and process data. By providing easy to use interfaces, AppSDK allows developers to quickly create new applications.

With AppSDK's facade, Application developers are able to:

- Use Eclipse Mosquitto based Databus,
- Read high frequency data from SINUMERIK device synchronously and/or asynchronously,
- Send high frequency data to Databus,
- Read Parameter Service data from SINUMERIK device with Adapter Framework,
- Write Parameter Service data to SINUMERIK device with Adapter Framework

with added functionalities like

- Logging functionalities,
- Event Mechanism for communication between industrial applications,
- Send heartbeat to the system about the status of the application,
- Read user-defined data in "specificConfig" object in the application's configuration,
- Get current system time

which are for the sole purpose of shortening the development lifecycle.

AppSDK Features

AppSDK API offers following features:

1) It supports three popular programming languages: C++, Java, Python

2) High frequency data operations

- Reading high frequency data from a Sinumerik device synchronously and asynchronously
- Pushing high frequency data to a Databus

3) Parameter Service data operations

- Reading Parameter Service data from a Sinumerik device
- Writing Parameter Service data to a Sinumerik device

4) File upload * Uploading file from Edge application to Insights Hub

5) Additional Features

- Advanced logging features
- Supports multithreading

- Watchdog support for ensuring applications always up and running
- Reverse proxy support
- Containerized simulator and development environment for ease of development
- GPU hardware acceleration support for 3D rendering tasks
- VNC server support for visualization (can be used together with or without GPU hardware acceleration)

Development Environment

With AppSDK development environment, application developers can use the full version of AppSDK without dealing with any dependency issues thanks to the containerized structure. All that needs to be done is downloading a development environment for your preferred language and running a Docker compose file.

With the development environment, a data simulator is supplied which can be used for simulating both Parameter Service and high frequency behavior of Sinumerik Devices by supplying data files with desired inputs. These input data files can be edited easily with any text editor or spreadsheet application like Microsoft Excel.

Application developers can easily create data files to mimic behavior of Sinumerik devices and feed these files to a data simulator and start the development with a given scenario fairly easy.

Further Details

The AppSDK offers extensive documentation for all supported programming languages and features with sample applications and code snippets.

Developer's manual [can be found here](#).

If you're interested in using the AppSDK, please contact your local sales representative.

Local Diagnostic Dashboard Application

Local Diagnostic Dashboard Application packs useful information about Sinumerik Edge. Main functionalities are:

- System information
- App management
- Network configuration

Using Application

Local Diagnostic Dashboard Application comes with firmware version ≥ 2.1 . In order to reach to the application, SINUMERIK Edge must have access to the internet. You can reach Diagnostic Application with the address `http://<device_ip>` or `https://<device_ip>` on a web browser. You can login with "Administrator" or the "Diag" user which is a predefined user for diagnostic purpose, the default password can be acquired as explained [here](#).

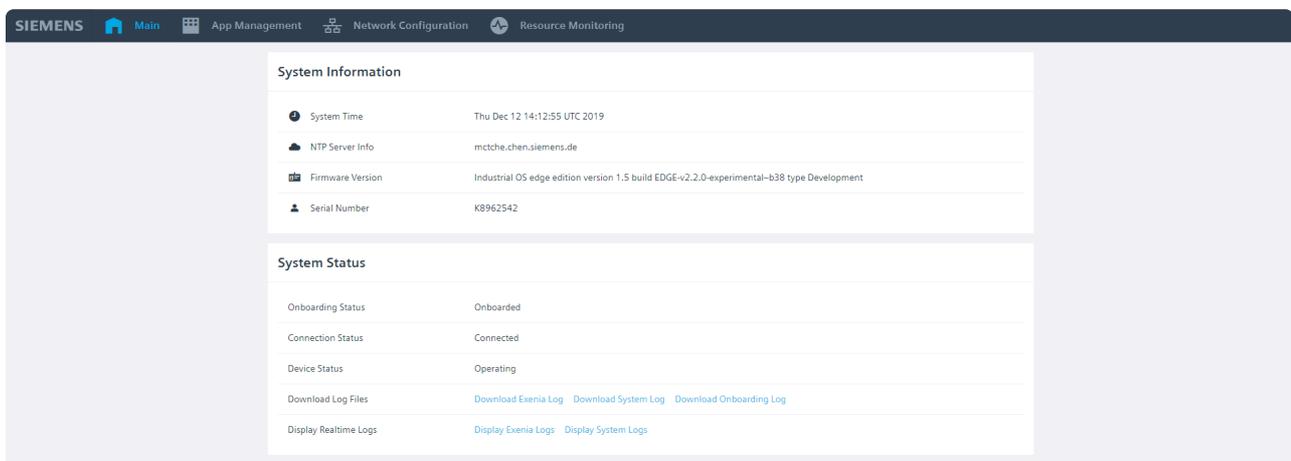
When you login successfully, you will need to create your new password. Once you created your new password, you will be directed to main page of ReverseProxy. You need to replace the URL with Local Diagnostic Dashboard Application's adress.

Warning

It should be noted that users should avoid opening multiple sessions into Diagnostic Dashboard Application for a better performance. Only one client session is supported.

System Information

In this section, useful information for SINUMERIK Edge can be found. Also system and Exeni logs can be downloaded. The onboarding status and downloading the onboarding related logs are available.



The screenshot displays the Siemens Local Diagnostic Dashboard Application interface. The top navigation bar includes the Siemens logo and menu items: Main, App Management, Network Configuration, and Resource Monitoring. The main content area is divided into two sections: System Information and System Status.

System Information	
System Time	Thu Dec 12 14:12:55 UTC 2019
NTP Server Info	mcctche.chen.siemens.de
Firmware Version	Industrial OS edge edition version 1.5 build EDGE-v2.2.0-experimental-b38 type Development
Serial Number	K8962542

System Status	
Onboarding Status	Onboarded
Connection Status	Connected
Device Status	Operating
Download Log Files	Download Exenia Log Download System Log Download Onboarding Log
Display Realtime Logs	Display Exenia Logs Display System Logs

System Time

Displays current time of your SINUMERIK Edge.

NTP Server Information

If configured during onboarding, displays NTP server currently used on SINUMERIK Edge.

Firmware Version

Displays current firmware version installed on SINUMERIK Edge.

Onboarding Status

Displays onboarding status.

Connection Status

Displays internet connection of SINUMERIK Edge.

Device Status

Displays task which is being handled by device. "Operating" means SINUMERIK Edge does not have any application installation or reconfiguration job in progress. The status changes with the transactions made on Insights Hub.

Attention: When an application installation, configuration change or an onboarding process starts, ReverseProxy is being restarted. Since Diagnostic Application is reachable via ReverseProxy, Local Diagnostic Dashboard Application will not be able to check the status of SINUMERIK Edge and you will see some error messages on the bottom right of your screen. You can find an example on the image below. On that case, SINUMERIK Edge is being onboarded. You need to wait approximately 45 seconds and refresh the web page. Then, you will need to login to ReverseProxy with "Administrator" as name and your new password which you created when you first logged in.

The screenshot shows the Siemens diagnostic dashboard for SINUMERIK Edge. The top navigation bar includes 'SIEMENS', 'Main', 'App Management', and 'Network Configuration'. The main content area is divided into two sections: 'System Information' and 'System Status'. 'System Information' displays: System Time (Fri Sep 13 09:45:46 UTC 2019), NTP Server Info (N/A), and Firmware Version (Industrial OS edge edition version 1.3 build EDGE-v2.1.0-77 type Development). 'System Status' displays: Onboarding Status (Offboarded), Connection Status (Connected), and Device Status (Operating). Below the status section are three buttons: 'Download Exenia Log', 'Download System Log', and 'Download Onboarding Log'. At the bottom right, there are two error messages: 'Error Operation Status' and 'Error Getting System Time', both indicating 'Http failure response for (unknown url): 0 Unk...'. The footer shows '© Siemens 2019 | Diag 1.6.4-73'.

Log Files

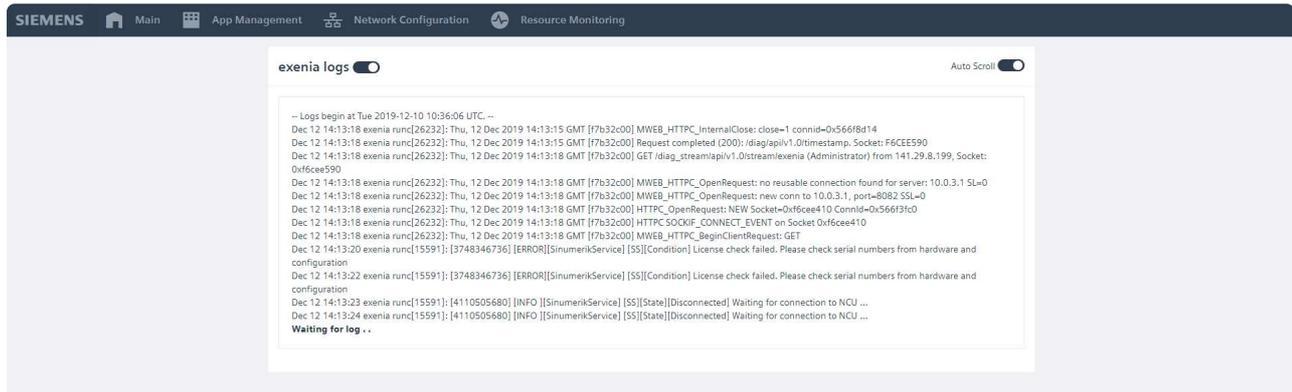
It is possible to get system wide logs. Exenia and system log files are served separately. Timespan of these log files are limited with one hour.

Onboarding Logs

Downloading the logs and checking the progress of onboarding is also available. The button is available when the SINUMERIK Edge is not onboarded. If you onboarded your SINUMERIK Edge, the button will not be available. When the onboarding process starts, the button for downloading the onboarding related logs will be available again.

Realtime Application Logs

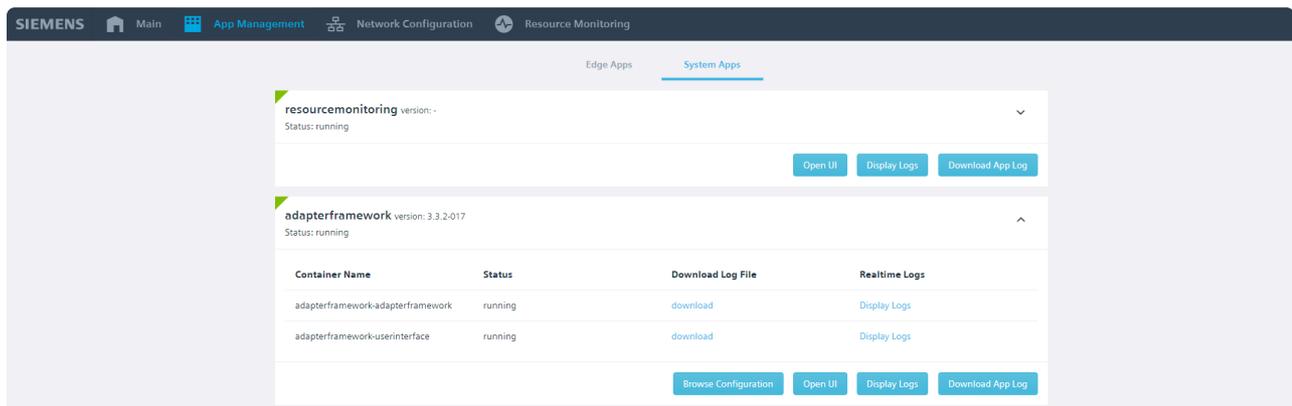
Realtime logs from SINUMERIK Edge can be observed by clicking display logs button.



By using switch on the left user can stop or start the logs. However in this case logs are discarded until its activated again.

App Management

In App Management it is possible to inspect installed System and Edge Applications. You can reach to configuration of your application, reach to the UI of your application, check the status of them and download their logs.



Application Listing

Application details, version and status are displayed for each app.

Container Listing

Containers are listed under applications for both single and multi container applications. Below images are examples of applications installed to SINUMERIK Edge.

SIEMENS Main App Management Network Configuration

Edge Apps System Apps

adapterframework version: 3.3.1-062
Status: running

Container Name	Status	Log File
adapterframework-adapterframework	running	download
adapterframework-userinterface	running	download

[Browse Configuration](#) [Open UI](#) [Download App Log](#)

databusconnector version: 1.5.0-33
Status: running

[Browse Configuration](#) [Download App Log](#)

databus version: 2.2.2.0
Status: running

[Download App Log](#)

SIEMENS Main App Management Network Configuration

Edge Apps System Apps

exampleapp version: 1.0.0
Status: running

Container Name	Status	Log File
exampleapp-exampleapp	running	download

[Browse Configuration](#) [Open UI](#) [Download App Log](#)

© Siemens 2019 | Diag 1.6.4-73 Corporate Information | Privacy Policy | Terms of Use

Application Configuration

Configuration of applications can be displayed by using browse configuration part on app listing.

exampleapp Configuration

```
{
  "appInfo": {
    "appClass": "exampleapp"
  },
  "datasourceConfig": {
    "requiredDatasource": [
      {
        "datasourceId": "SINUMERIK_NCUI",
        "services": [
          "parameter-service/v1": {
            "access": [
              {
                "accessType": "w",
                "datapoints": [
                  {
                    "address": "/NC/"
                  }
                ]
              }
            ]
          },
          "subscription-service/v1": {
            "subscriptions": [
              {
                "datapoints": [
                  {
                    "address": "EMCI_POS1"
                  }
                ]
              }
            ],
            "messageId": "sinumerik_hf_data",
            "messageName": "sinumerik_hf_data",
            "quality": "hf"
          }
        ]
      }
    ],
    "type": "SINUMERIK"
  }
},
"loggingConfig": {
  "appender": "JOURNAL_APPENDER",
  "severity": "INFO"
},
"specificConfig": {}
}
```

Easy UI Access

If any of the installed applications has an UI served over ReverseProxy an easy to use open UI button appears on listing which leads to UI of specific application.

Application Logs

It is possible to download log files for a specific application. Like Exenia and system log files, these are also limited with last one hour.

Container Logs

Container-wise log files are also served within container listing. This feature give flexibility of getting log files of containers separately.

Realtime Logs

It is possible to display realtime logs for both applications and application container by clicking display logs button.

Network Configuration

In network configuration, it is possible to inspect different network interfaces, their configurations and current status of these network interfaces. Proxy information of Edge Device is also shown in this part of application.

SIEMENS Main App Management Network Configuration Resource Usage

Web Interface (X1 P1)
Status: Online

Name	factorylan0
DHCP	Disabled
IPv4 Address	141.29.64.97
Subnet Mask	255.255.255.192
Gateway	141.29.64.65
DNS Server	129.103.99.201
NTP Server	mctche.chen.siemens.de
Host Name	Host1

Production Interface (X2 P1)
Status: Offline

Name	machinelan0
DHCP	Disabled
IPv4 Address	192.168.214.249
Subnet Mask	255.255.255.0
Gateway	N/A
DNS Server	N/A
NTP Server	N/A

Communication Settings

Proxy Type	FIXED
Proxy Address	http://194.138.0.3:9400
Proxy Protocol	HTTP
Proxy Authentication Type	BASIC
Proxy Username	N/A

© Siemens 2019 | Diag 2.1.0-dev-159 Corporate Information | Privacy Policy | Terms of Use

Resource Monitoring

In resource monitoring page it is possible to see system and application resource usages.

SIEMENS Main App Management Network Configuration Resource Monitoring



/

root

Subcontainers

- /init.scope
- /lxc
- /system.slice
- /user.slice

Isolation

CPU

Shares 1024 shares

Allowed Cores 0 1 2 3

Memory

Reservation unlimited

Limit 7.68 GB

© Siemens 2019 | Diag 2.1.0-dev-159 Corporate Information | Privacy Policy | Terms of Use

Diagnostic of Internal Communication

The Adapter Framework provides a website to view information about the system's configuration status. This can be found in the dashboard of the SINUMERIK Edge. Navigate to App Management -> System Apps -> adapterframework and click the button "Open UI". This button is available after you install the application from

Insights Hub to SINUMERIK Edge. You will find a set of different sections, including diagnostic information of the system's current configuration.

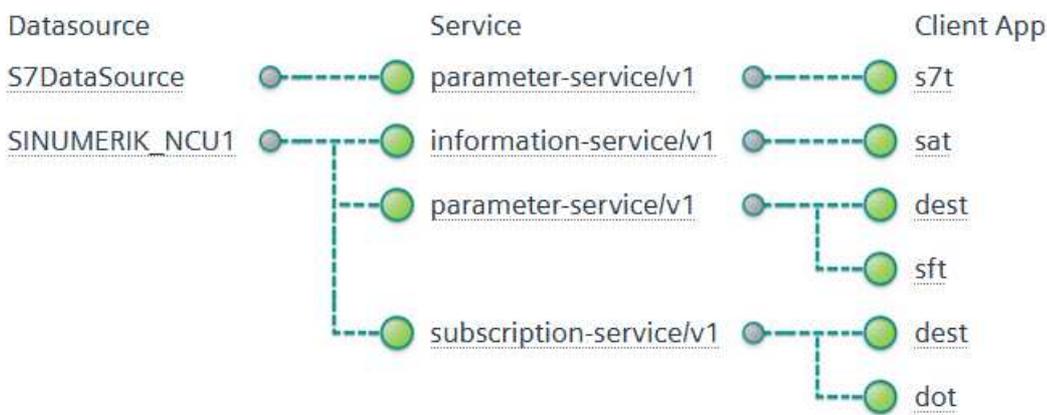
Time of Configuration

The timestamp (SINUMERIK Edge local time) of the last valid configuration job.

Attention: In some circumstances, a configuration job fails and the system does a rollback to the last valid configuration. In this case, the timestamp will show the time of the failed configuration job, even if the active valid configuration is older. Please always review the active configuration sections as well.

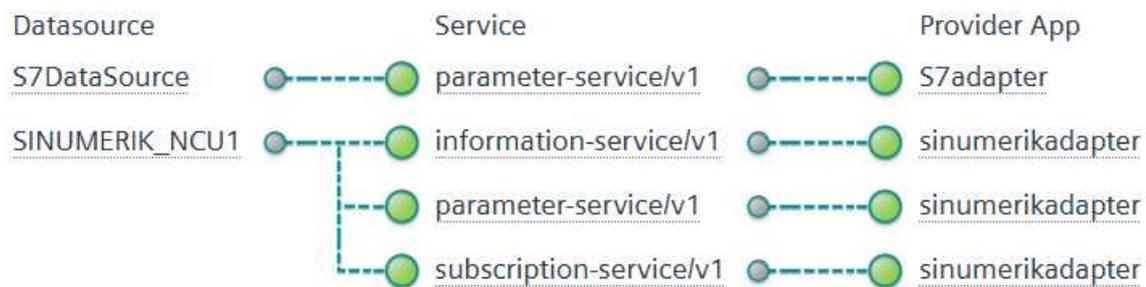
active configuration – client app oriented view

In this section you can find a graphical view of installed consumer applications and the services they request. Green bubbles indicate a successful configuration, while red bubbles indicate an error. Additional information is shown as a tooltip when the mousepointer is hovered over the text.



active configuration – service providers oriented view

In this section you can find a graphical view of available datasources and services which are used by consuming applications. Green bubbles indicate a successful configuration, while red bubbles indicate an error. Additional information is shown as a tooltip when the mousepointer is hovered over the text.



adapter framework raw json Configuration Data

The current configured routing information of the AdapterFramework.

Remark: Only services routed by the AdapterFramework are listed here. Not every consumer service is routed by the AdapterFramework. As such, the subscription-service/v1 will not be found in the routing information; this service is routed by the databus message broker.

Local Resource Monitoring

This is a tool for monitoring the local system's usage of CPU, memory and disk in realtime. Users can view the resource usage and statistics for the base system (root), exenia or for each separate container within exenia.

Warning

Users should avoid opening multiple local sessions of the resource monitoring tool. Only one client session is supported.



/

root

Subcontainers

/lxc

/system.slice

/user.slice

Isolation

CPU

Shares 1024 *shares*

Allowed Cores 0 1 2 3

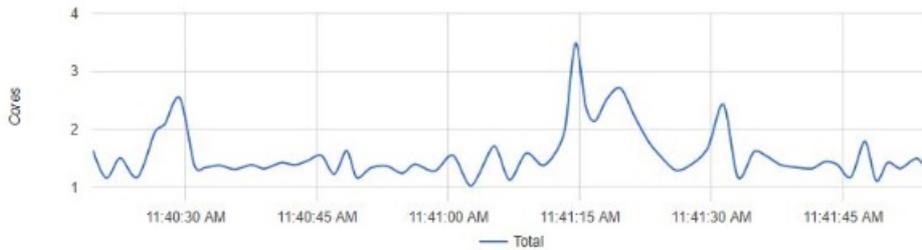
Memory

Resource monitoring for the base system

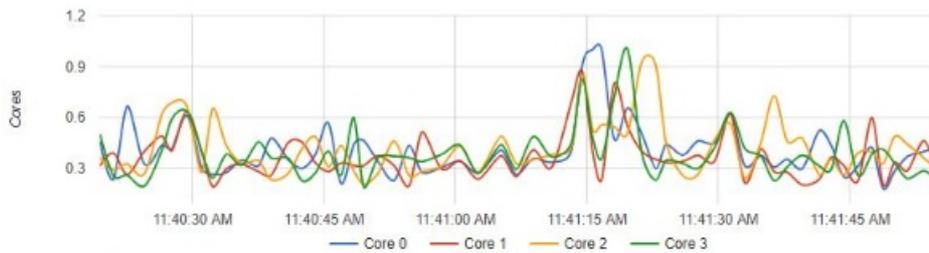
Users can view the CPU, memory and file system usage in realtime for the base system.

CPU

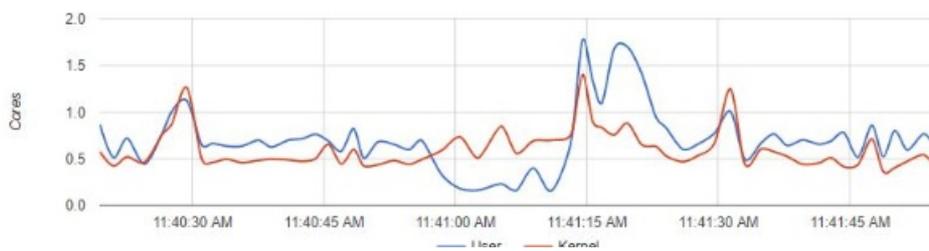
Total Usage



Usage per Core

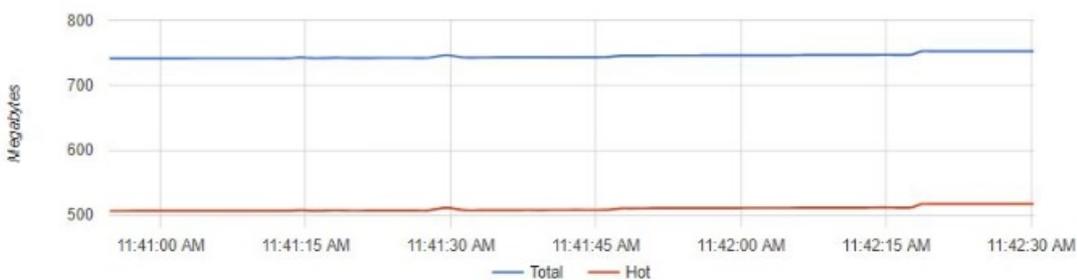


Usage Breakdown



Memory

Total Usage



Usage Breakdown

752.62 MiB / 7.68 GiB (9%)

Resource monitoring for exenia

Users can view the CPU, memory and file system usage in realtime for exenia. Users can access the exenia view from `root/lxc` for overall monitoring and `root/lxc/exenia` for individual processes' resource usage.

Resource monitoring for apps/exenia containers

Users can view the CPU, memory and file system usage in realtime for each application. Specific containers can be accessed from `root/lxc/exenia/<CONTAINERNAME>`.

Time Behavior

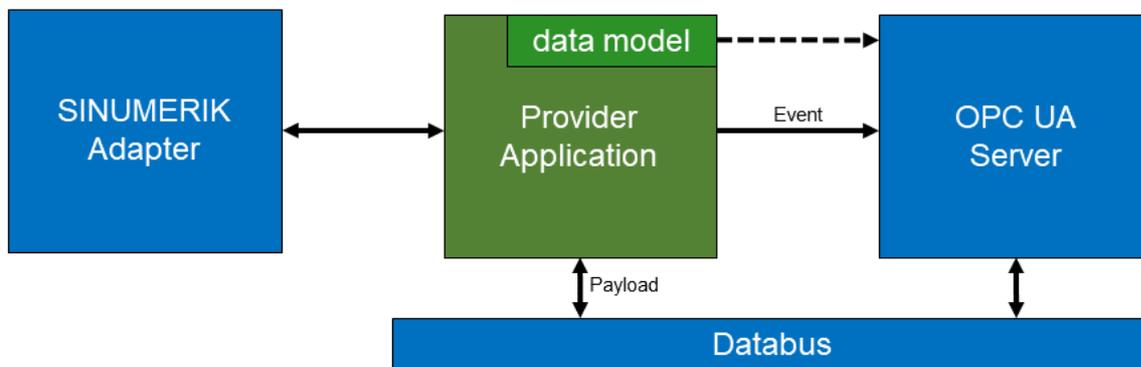
How to set system time on Edge device

In order to operate Edge device properly, system time needs to be set. SINUMERIK Edge behaves as follows for system time setting:

1. System time is set automatically under following conditions:
 - the networking of Edge device is configured using a DHCP server.
 - the DHCP server provides a NTP Server and NTP Server is accessible from Edge device
2. If NTP Server is explicitly configured during the phase of onboarding, then it will be used by Edge device. Please refer to [Onboarding](#) chapter for further details.
 - It is assumed that the configured NTP Server is not blocked by corporate firewall.
3. If no time server is explicitly configured, then default global NTP Servers are used.
 - It is assumed that the global NTP-Servers are not blocked by corporate firewall.
4. If no NTP Server is available or they are not accessible, then system time must be set manually via BIOS.

OPC UA Server as a northbound interface

OPC UA Server as a northbound interface is a reliable open platform communication among industrial devices. The OPC UA Server can be installed on a SINUMERIK Edge device as a northbound interface. The OPC UA Server itself doesn't communicate with the SINUMERIK, instead it offers an interface for other applications to host their data on the OPC UA Server. These so called "Provider" applications have their own OPC UA information model in the XML format, that can be created for example in SiOME. The provider application can then write data to the OPC UA Server and also receive data through the Databus, send events to the server to add and delete nodes and generate events. The data model is configured in the configuration of the provider application and automatically passed to the server.



Usually, the provider application will connect to the SINUMERIK via the SINUMERIK Adapter and write the data to the OPC UA Server.

A provider application uses the APP SDK functionality for writing/receiving data through the databus and transmitting data through events, so it can be developed in any language supported by the AppSDK.

One OPC UA Server can support multiple Provider applications, each with their own, independent data model.

Important Each Provider application has to implement his own unique namespace(s). It is not possible to load multiple same namespaces in parallel.

The development of a provider application is described in the Developer Manual.

Installation of OPC UA Server application

After onboarding a new SINUMERIK EDGE you will need to install the **OPC UA Server** application

Select the application "*opcuaserver*" with the released version related to the firmware version installed on your SINUMERIK EDGE to install it on your connected SINUMERIK EDGE device.

Please refer to chapter [Application Management](#) for detailed information how to install an application on your SINUMERIK EDGE device.

For detailed description how to configure a data provider application please refer to the Developer Manual.

Configuration of OPC UA Server application

In the "specificConfig" of the opcuaserver application, there is a XML Model stored as a string called "serverConfigXml". Here you can find some server settings like the permitted security policies. For a complete documentation, visit the site: https://documentation.unified-automation.com/uasdkcpp/1.5.4/html/L2ServerSdkServerConfig.html#server_config_xml_file. This configuration should not be changed except for setting the IP Address in the following certificate setting.

Important Be careful when changing settings. The certificate paths for example are required to stay the same.

There are two important configurations highlighted in this chapter.

Server Certificate:

The Server automatically generates a certificate on first startup, that is used when clients open a secure connection with the server. The information in this certificate can be configured in the ServerConfig.

Because the opcuaserver application is executed inside of a container, it doesn't have the IP Address of the host system (the edge box). Therefore, when the server generates its certificate, you have to manually set the IP Address in the `serverConfigXml` within the specificConfig in the App Instance Configuration. Change the `ServerCertificate>CertificateSettings>DNSName` to the address of your edge box, e.g. 192.168.10.2 .

If you don't do this, the following error will appear when connecting through a signed connection with the opcuaserver:



Important: The server certificate is rebuild everytime the serverConfigXml changes. Older server certificates which were saved as trusted lose their functionality.

Allow all SSL Certificates:

For establishing a secure connection, certificates are exchanged. These certificates are independent of the authentication and cannot be managed in any Insights Hub interface. Therefore, it is important to set `UaEndpoint>AutomaticallyTrustAllClientCertificates` to true (default, when installing opcuaserver). This does *not* mean that an unauthenticated client can connect to the opcuaserver and receive data, it only means that clients are able to establish a signed connection with the opcuaserver. The authentication still comes after the connection has been opened.

Connecting to the OPC UA Server

The connection with the OPC UA Server can be done with any OPC UA Client through the Web Interface (X1) of the edge box. The OPC UA Server will have the following address: `opc.tcp://[Edge_Box_Address]:48010` , e.g.: `opc.tcp://192.168.10.82:48010` . In this chapter, UaExpert is used as an example for a client.

Please note that anonymous logins are not permitted. You need to use either username and password, or a certificate to connect with the OPC UA Server.

User Management of OPC UA Server through ReverseProxy

The OPC UA Server relies on the ReverseProxy application for user management tasks. The ReverseProxy application provides a user interface through which groups, users and password assignment can be managed easily. Please refer to the System Services documentation for how to handle user management in the ReverseProxy application. For instance, we have added a user called "abc" to the user list and assigned him a password. In the UaExpert application, when connecting to the server, the user credentials can be provided as shown below:

Server Settings - UaServerCpp@opcuserver

Configuration
Configuration Name: UaServerCpp@opcuserver

Server Information
Endpoint Url: opc.tcp://141.29.64.120:48010
Reverse Connect:

Security Settings
Security Policy: None
Message Security Mode: None

Authentication Settings
 Anonymous
 Username: abc, Password: [dots], Store
 Certificate
 Private Key

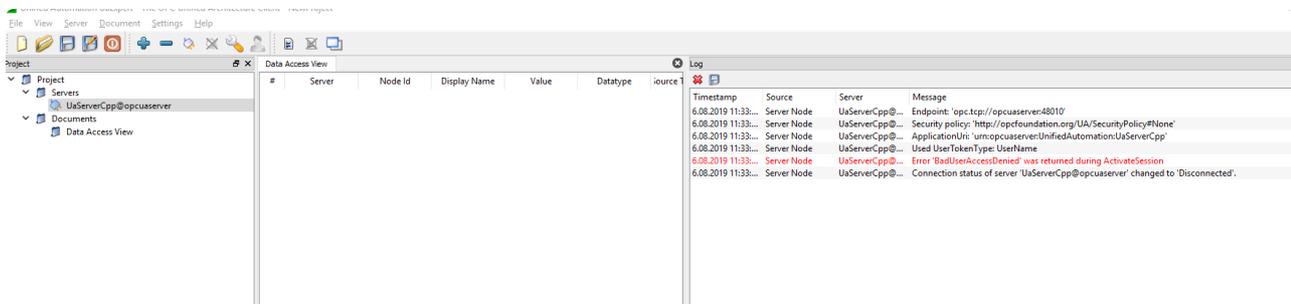
Session Settings
Session Name: rn:EVT01306NB:UnifiedAutomation:UaExpert

OK Cancel

After that, during the "Connect" operation, you can see the result of the login in the log panel of the UaExpert application as shown below:

Timestamp	Source	Server	Message
6.08.2019 11:31:...	General	UaServerCpp@...	Error: Publish failed [status=0x60790000]
6.08.2019 11:31:...	AddressSpaceM...	UaServerCpp@...	Unregister for ModelChangeEvents returned Good
6.08.2019 11:31:...	General	UaServerCpp@...	Error: Publish failed [status=0x60790000]
6.08.2019 11:31:...	Server Node	UaServerCpp@...	Connection status of server 'UaServerCpp@opcuserver' changed to 'Disconnected'.
6.08.2019 11:31:...	Server Node	UaServerCpp@...	Disconnect succeeded.
6.08.2019 11:32:...	Server Node	UaServerCpp@...	Endpoint: 'opc.tcp://141.29.64.120:48010'
6.08.2019 11:32:...	Server Node	UaServerCpp@...	Security policy: 'http://opcfoundation.org/UA/SecurityPolicy#None'
6.08.2019 11:32:...	Server Node	UaServerCpp@...	ApplicationUri: 'urn:opcuserver:UnifiedAutomation:UaServerCpp'
6.08.2019 11:32:...	Server Node	UaServerCpp@...	Used UserTokenType: UserName
6.08.2019 11:32:...	General	UaServerCpp@...	Reading Data Type Descriptions failed.
6.08.2019 11:32:...	General	UaServerCpp@...	Getting Data Type nodes failed.
6.08.2019 11:32:...	AddressSpaceM...	UaServerCpp@...	Registered for ModelChangeEvents
6.08.2019 11:32:...	Server Node	UaServerCpp@...	Connection status of server 'UaServerCpp@opcuserver' changed to 'Connected'.
6.08.2019 11:32:...	Server Node	UaServerCpp@...	Revised values: SessionTimeout=1200000, SecureChannelLifetime=3600000
6.08.2019 11:32:...	AddressSpaceM...	UaServerCpp@...	Browse on node '84' succeeded.
6.08.2019 11:32:...	TypeCache	UaServerCpp@...	Reading type info of NodeId NS0[Numeric]35 succeeded
6.08.2019 11:32:...	TypeCache	UaServerCpp@...	Reading type info of NodeId NS0[Numeric]33 succeeded
6.08.2019 11:32:...	TypeCache	UaServerCpp@...	Reading type info of NodeId NS0[Numeric]31 succeeded
6.08.2019 11:32:...	AddressSpaceM...	UaServerCpp@...	Browse on node '85' succeeded.
6.08.2019 11:32:...	TypeCache	UaServerCpp@...	Reading type info of NodeId NS0[Numeric]2004 succeeded
6.08.2019 11:32:...	TypeCache	UaServerCpp@...	Reading type info of NodeId NS0[Numeric]18 succeeded
6.08.2019 11:32:...	TypeCache	UaServerCpp@...	Reading type info of NodeId NS3[Numeric]1012 succeeded

Otherwise, the authentication will fail, indicated in the log panel as shown below:

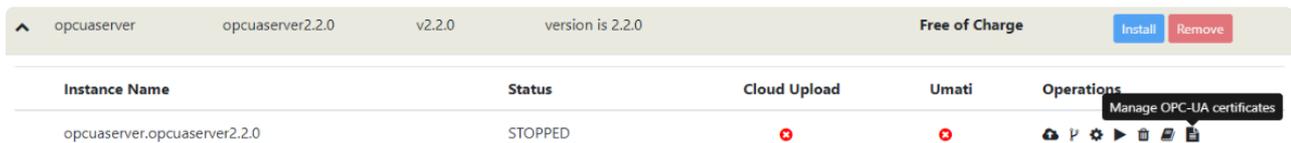


User Management of OPC UA Server with certificates

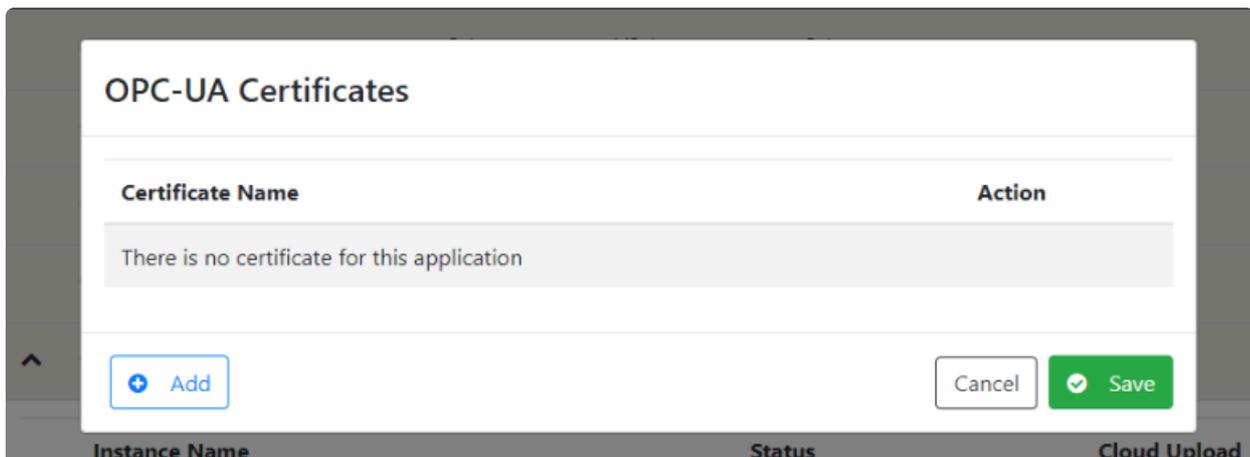
In addition to the user management of the ReverseProxy, the OPC UA Server also supports the authentication of clients with the help of provided certificates.

There are two ways to upload a certificate to OPC UA Server. First one is, as an App Owner, certificate file can be given inside meta config of data provider application. This part is already explained in detail at **Building Indapp** chapter in developer document.

Second way, as an End User, a certificate file can be uploaded to the opcuaserver application through *Manage MySINUMERIK Edge /App Management*. After installing the opcuaserver application, there will be a **Manage OPC UA certificates** icon for the opcuaserver application.



When the icon is clicked, a pop-up is opened for OPC UA certificate management. Your current certificate files are shown and you can add and remove certificates in this window. Certificate files can be added by clicking the **Add** button on the left. You can add multiple certificate files. Additionally, certificate files can be removed by clicking the **Remove** button.



OPC-UA Certificates

Certificate Name	Action
certificate.der	<input type="button" value="Remove"/>
certificate2.der	<input type="button" value="Remove"/>
certificate3.der	<input type="button" value="Remove"/>

After adding or removing your certificate files, changes can be saved by clicking the **Save** button on the right. A window will ask if you want to save the changes, click **Confirm**.

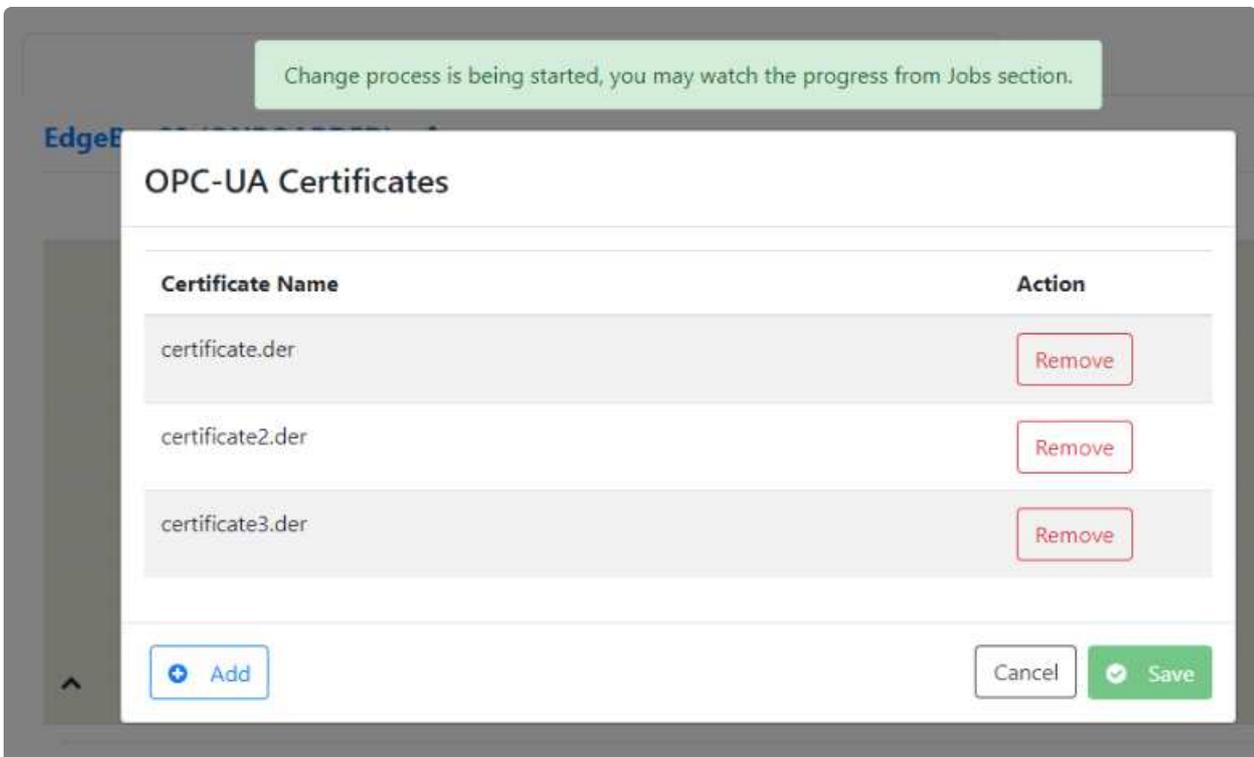
OPC-UA Certificates

Certificate Name	Action
certificate.der	<input type="button" value="Remove"/>
certificate2.der	<input type="button" value="Remove"/>
certificate3.der	<input type="button" value="Remove"/>

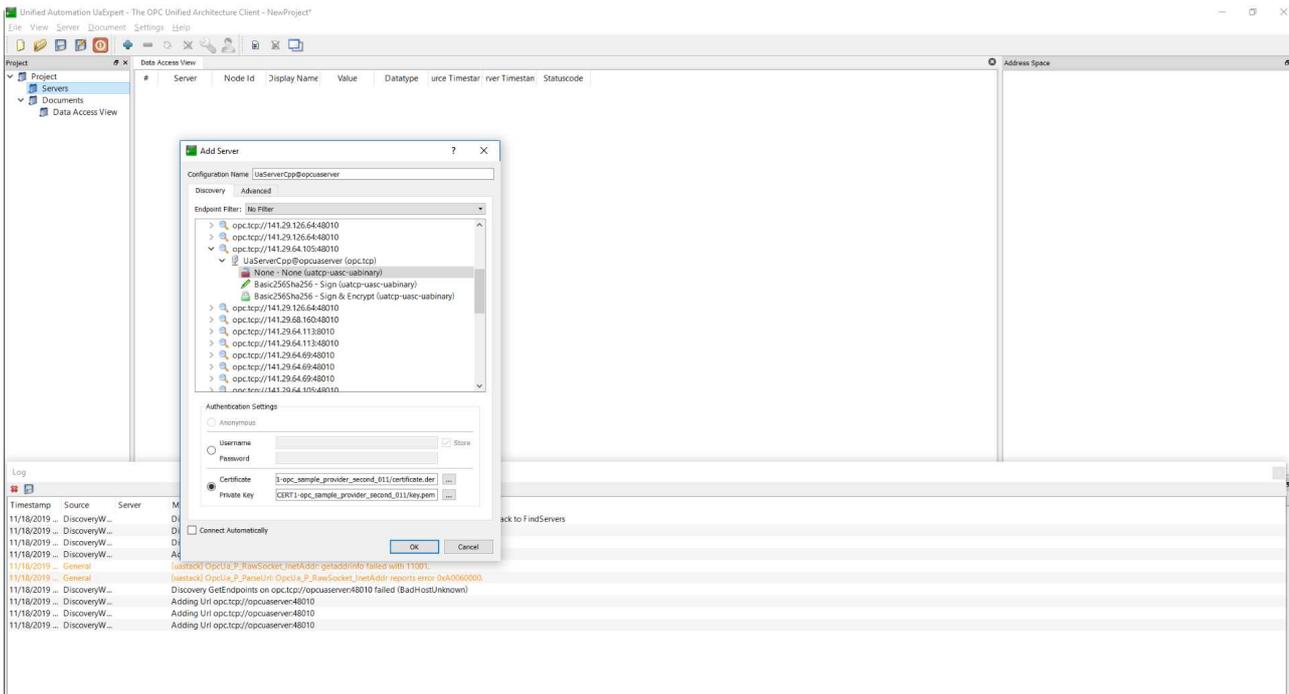
Save Changes

Changes will be saved. Do you want to continue?

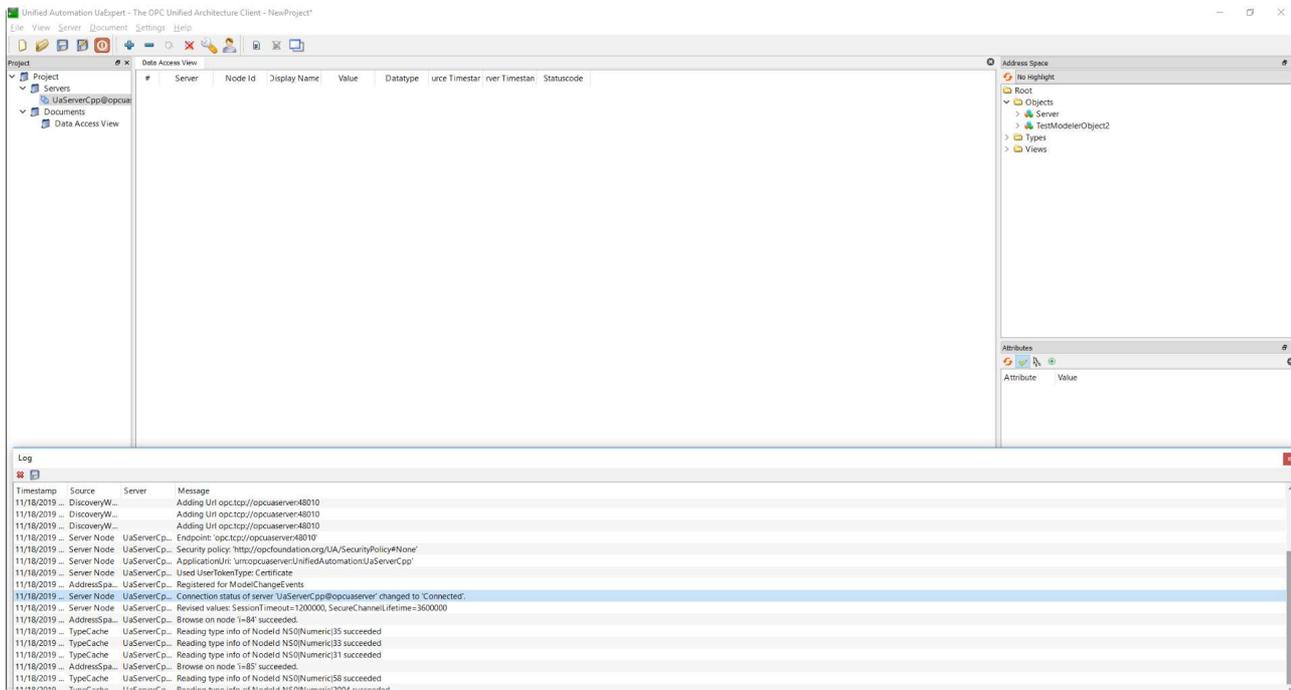
The status can be observed from the "Jobs" tab and the "Configure" sub tab. The OPC UA Certificates window can be closed by clicking the **Cancel** button.



The Following shows how to connect to the OPC UA Server using the UaExpert tool with certificates. When adding a server, the following dialog will pop up, where you can enter the certificate files.



After connecting to the OPC UA Server, the result of the connection attempt is shown in the log panel:



Connection Security

Instead of connecting with the Security Policy "None", you should use the Signed and Encrypted mode. By default, the Basic256Sha256 Sign and Basic256Sha256 Sign & Encrypt are configured security policies in the Configuration of the OPC UA Server.

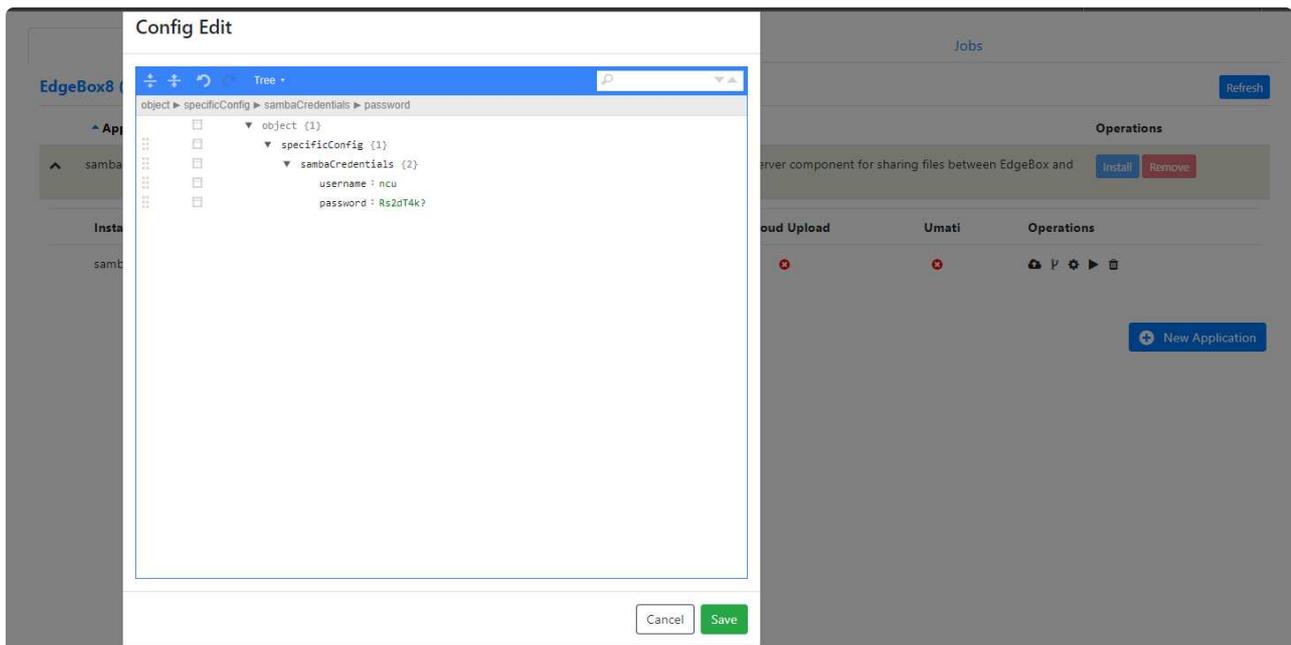
Samba Share

The Samba server on SINUMERIK Edge is disabled until it is configured. The server can be enabled only on the "machinelan0" interface which is in the internal factory network that cannot access the internet. In order to admit connections from Sinumerik NCU, the Samba server should be configured and enabled. To configure and enable the Samba server, a System App called **sambaserver** is needed to be installed on the SINUMERIK Edge.

Please refer to chapter [Application Management](#) for detailed information how to install an application on your SINUMERIK EDGE device.

⚠ Username and Password Warning

You can set your own username. You cannot use "root" or "edge" as username. Password must comply with following password policy. Password must have minimum 8 and maximum 11 characters including numbers, special characters (i.e. +-*_), lower and UPPER case letters. Username and password can be set in specificConfig->sambaCredentials section of sambaserver application configuration by Manage MySINUMERIK Edge /App Management UI.



In order to access samba folders on Edgebox from other machine (such as HMI Operate) running on machinelan0 network, You need to connect the address in following format :

<ip_address_of_edgebox_on_machinelan0_network>/share

Ex:

192.168.214.249/share