SIEMENS

SICAM GridEdge Engineering Guide

V2.3

Manual

Preface

Table of Contents

1 Introduction

2 System Configuration

3 SICAM GridEdge Configuration

4 Security

E50417-H7640-C641-A6



NOTE

For your own safety, observe the warnings and safety instructions contained in this document, if available.

Disclaimer of Liability

Subject to changes and errors. The information given in this document only contains general descriptions and/or performance features which may not always specifically reflect those described, or which may undergo modification in the course of further development of the products. The requested performance features are binding only when they are expressly agreed upon in the concluded contract.

Document version: E50417-H7640-C641-A6.05

Edition: 06.2021

Version of the product described: V2.3

Copyright

Copyright © Siemens 2020 – 2021. All rights reserved.

The disclosure, duplication, distribution and editing of this document, or utilization and communication of the content are not permitted, unless authorized in writing. All rights, including rights created by patent grant or registration of a utility model or a design, are reserved.

Trademarks

SIPROTEC, DIGSI, SIGRA, SIGUARD, SIMEAS, SAFIR, SICAM, and MindSphere are trademarks of Siemens. Any unauthorized use is prohibited.

Preface

Purpose of the Manual

This manual describes the engineering steps to connect devices in the station network using SICAM GridEdge with secure communication to the Siemens cloud platform MindSphere or any other cloud-based platforms.

Scope

This manual covers only the SICAM GridEdge-related settings and engineering steps.
For general engineering guidelines, refer to the corresponding documents.

Target Audience

System engineers, commissioning engineers, persons entrusted with the setting, selective protection and control equipment, and operational crew in electrical installations and power plants.

Additional Support

For questions about the system, contact your Siemens sales partner.

Customer Support Center

Our Customer Support Center provides a 24-hour service.

Siemens AG
Smart Infrastructure – Digital Grid
Customer Support Center
Phone: +49 911 2155 4466
E-mail: *energy.automation@siemens.com*

Training Courses

Inquiries regarding individual training courses should be addressed to our Training Center:

Siemens AG
Siemens Power Academy TD
Humboldtstrasse 59
90459 Nuremberg
Germany

Phone: +49 911 9582 7100
E-mail: *poweracademy@siemens.com*
Internet: *www.siemens.com/poweracademy*

Notes on Safety

This document is not a complete index of all safety measures required for operation of the equipment (module or device). However, it comprises important information that must be followed for personal safety, as well as to avoid material damage. Information is highlighted and illustrated as follows according to the degree of danger:



DANGER

DANGER means that death or severe injury **will** result if the measures specified are not taken.

✧ Comply with all instructions, in order to avoid death or severe injuries.



WARNING

WARNING means that death or severe injury **may** result if the measures specified are not taken.

✧ Comply with all instructions, in order to avoid death or severe injuries.



CAUTION

CAUTION means that medium-severe or slight injuries **can** occur if the specified measures are not taken.

✧ Comply with all instructions, in order to avoid moderate or minor injuries.

NOTICE

NOTICE means that property damage **can** result if the measures specified are not taken.

✧ Comply with all instructions, in order to avoid property damage.



NOTE

Important information about the product, product handling or a certain section of the documentation which must be given attention.

OpenSSL

This product includes software developed by the OpenSSL Project for use in OpenSSL Toolkit (*http://www.openssl.org/*).

This product includes software written by Tim Hudson (*tjh@cryptsoft.com*).

This product includes cryptographic software written by Eric Young (*eay@cryptsoft.com*).

Table of Contents

Preface ... **3**

1 Introduction ... **6**

2 System Configuration ... **7**

2.1 SIEMENS CP-8050 ... 8

2.1.1 Updating the SIEMENS CP-8050 Firmware ... 8

2.1.2 Preparing SD Card for Installation ... 9

2.1.3 Installing SICAM GridEdge with Prepared SD Card ... 13

2.2 SIEMENS IPC 227E ... 14

2.2.1 Installing SIMATIC Industrial OS ... 14

2.2.2 Installing SICAM GridEdge ... 16

2.2.3 Mounting the USB Drive ... 17

2.2.4 Example Installation ... 18

3 SICAM GridEdge Configuration ... **19**

3.1 Access to SICAM GridEdge Web Interface ... 20

3.2 General Settings ... 20

3.2.1 Configuring the Cloud Connection ... 21

3.2.2 Configuring the Data Filter ... 25

3.3 Application Configuration ... 26

3.3.1 Configuring the IEC 61850 Client ... 27

3.3.2 Data-Point Mapping for the IEC 61850 Client ... 32

3.3.3 Data-Point Selection for the IEC 61850 Client ... 34

3.3.4 Configuring the DIGSI 4 Client ... 36

3.3.5 Configuring the SNMP Client ... 37

3.3.6 Configuring the WMI Client ... 40

3.3.7 Collecting Data from Windows Computers ... 42

3.4 Connection Status ... 42

3.5 Maintenance ... 44

3.6 Asset Information ... 44

4 Security ... **46**

4.1 Security Requirements ... 47

4.2 User Management ... 47

4.3 Backup and Restore ... 49

4.4 Diagnosis ... 51

4.5 Certificate Management ... 52

4.6 TCP-UDP Ports ... 54

1 Introduction

The Internet of Things (IoT) is poised to be a driver of growth in many business sectors in the coming years, including the energy industry. In simple terms, IoT is about networking electronic devices over the Internet. For power-supply systems, connecting to IoT enables all components within a station to make data available in a cloud-based platform. Applications can then be used to consolidate, link, evaluate, and visualize the information for application-specific purposes.

You can utilize the resulting benefits to:

- Enhance the transparency of the plant and equipment status and conditions (such as the availability of electrical operating values and equipment)
- Plan predictive maintenance and optimize services and resources
- Increase the availability of the power-supply system

SIPROTEC and SICAM – products and solutions for protection engineering, station automation, power quality, and measurement – can be connected easily using SICAM GridEdge to MindSphere and other cloud-based platforms.

The connectivity is enabled by using SICAM GridEdge solution with the standardized OPC UA PubSub (MQTT) protocol (to IEC 62541 requirements) – no firmware changes for devices in your station are required.

Using the IoT standard OPC UA PubSub (MQTT) protocol and applying the highest security standards makes IoT connection of existing legacy installations a lucrative prospect.

Upgrading existing installations is simple:

- Continue using existing infrastructure and hardware
- Install SICAM GridEdge on your station
- Configure SICAM GridEdge

MindSphere – the IoT Operating System from Siemens

MindSphere is the open, cloud-based IoT operating system from Siemens offering data analysis, versatile connectivity, tools for developers, applications, and services.

With all these functions, however, data security always takes highest priority. MindSphere fulfills the basic rules of the industry-relevant security standards as well as recommendations from regulatory authorities for handling data in cloud environments.

2 System Configuration

Hardware Requirements

Siemens recommends one of the following systems to run SICAM GridEdge properly:

- **SIEMENS CP-8050** (MLFB: 6MF2805-0AA00)
  - ARM32 CPU Architecture
  - 512 MB RAM
  - 2 LAN ports
  - Additionally, the following hardware is necessary:
    - SD card 2GB (MLFB: 6MF1213-1GA05-0AA0)
    - Power supply PS-8620 24-60VDC 12W (MLFB: 6MF2862-0AA00)
    - Power supply PS-8622 110-220VDC 12W (MLFB: 6MF2862-2AA00)
- **SIEMENS IPC 227E** (MLFB: 6ES7647-8BD31-0CA1)
  - X86 CPU Architecture
  - 240 GB SSD
  - 8 GB RAM
  - 2 LAN ports
  - **SIMATIC INDUSTRIAL OS** (MLFB: 6ES7648-6LA81-0YA8)
    - Single-license software
    - License for download



NOTE

If you already have a running SICAM GridEdge system and want to upgrade to a newer version, you have to create a backup of the current configuration and restore the backup after updating the system, see *4.3 Backup and Restore*.

2.1	SIEMENS CP-8050	8
2.2	SIEMENS IPC 227E	14

2.1 SIEMENS CP-8050

2.1.1 Updating the SIEMENS CP-8050 Firmware

NOTE

You need firmware version 04 on your SIEMENS CP-8050 device to run SICAM GridEdge properly.

If you do not have firmware version 04 running on your SIEMENS CP-8050, prepare an SD card and perform the following steps to update your device.

NOTE

Since delivery of SIEMENS CP-8050 does not include an SD card, the card has to be ordered separately (see *Hardware Requirements, Page 7*).

NOTE

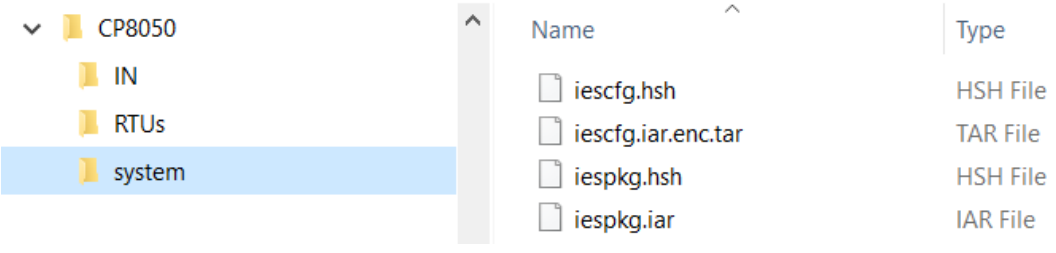
The SD card has to be empty and formatted using FAT32 file system.

- ✧ Open the appropriate **SIOS** Web page:
  https://support.industry.siemens.com/cs/document/109783989/sicam-a8000-cp-8050-package-v0440-?dti=0&lc=de-WW
- ✧ Select **SICAM WEB Update** and download the **SWEBUpdate.zip** file to your computer.
- ✧ On your computer, create an **IN** folder on the empty SD card and copy the **CPCI8504.F40** file from the **SWEBUpdate.zip** into it.



[sc_sd_card_content_FW04, 1, en_US]

- ✧ Insert the SD card into the SIEMENS CP-8050 device.
  The installation starts and will take approx. 4 minutes. Afterwards, the device will reboot automatically.
- ✧ Insert the SD card into your computer and check its content.
  There should be 3 folders: **RTUs**, **system**, and **IN**.
  If the folders **IN** and **RTUs** are empty and the **system** folder contains a few files as seen below, the update has been successful.



[sc_sd_card_content_after_FW04_update, 1, en_US]

2.1.2 Preparing SD Card for Installation

In order to install the SICAM GridEdge system, it is necessary to prepare an SD card with the SICAM GridEdge installation files and mount the SD card to the SIEMENS CP-8050 afterwards.

NOTE

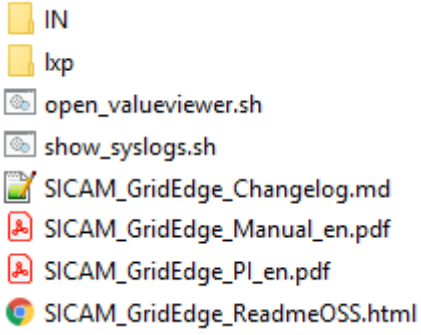
Since delivery of SIEMENS CP-8050 does not include an SD card, the card has to be ordered separately (see *Hardware Requirements, Page 7*).

NOTE

The SD card has to be empty and formatted using FAT32 file system.

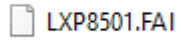
Content of the SD Card

Extract the content of the setup bundle (ZIP file) to the SD card. It should look like this:



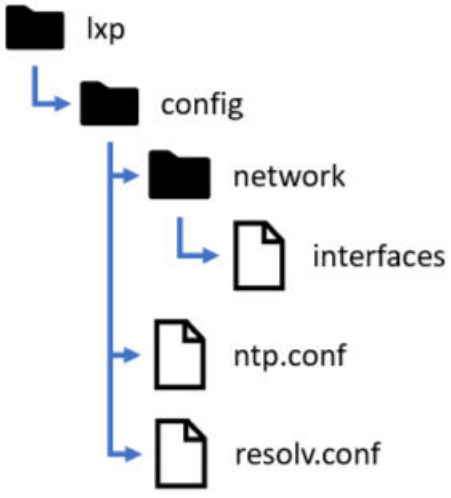
[sc_sd-card_content1, 1, --_--]

Make sure the IN folder only contains this file:



[sc_sd-card_content2, 1, --_--]

Underneath the folder **lxp** there is a folder named **config** which contains a default configuration.



[sc_sd_card_content, 1, en_US]

The configuration files are:

- **network/interfaces**
  Configuration of the IP addresses
- **ntp.conf**
  Configuration of the NTP client for time synchronization
- **resolv.conf**
  Configuration of the naming server

In order to configure the IP addresses and the connection to an NTP server, the content of the SD card needs to be adjusted.



NOTE

Each file can be adjusted according to the specific needs.

You can change the configuration by removing the SD card (after turning off the SIEMENS CP-8050) and changing the files directly on the SD card using a computer. Afterwards, plug in the SD card again and power on the SIEMENS CP-8050.

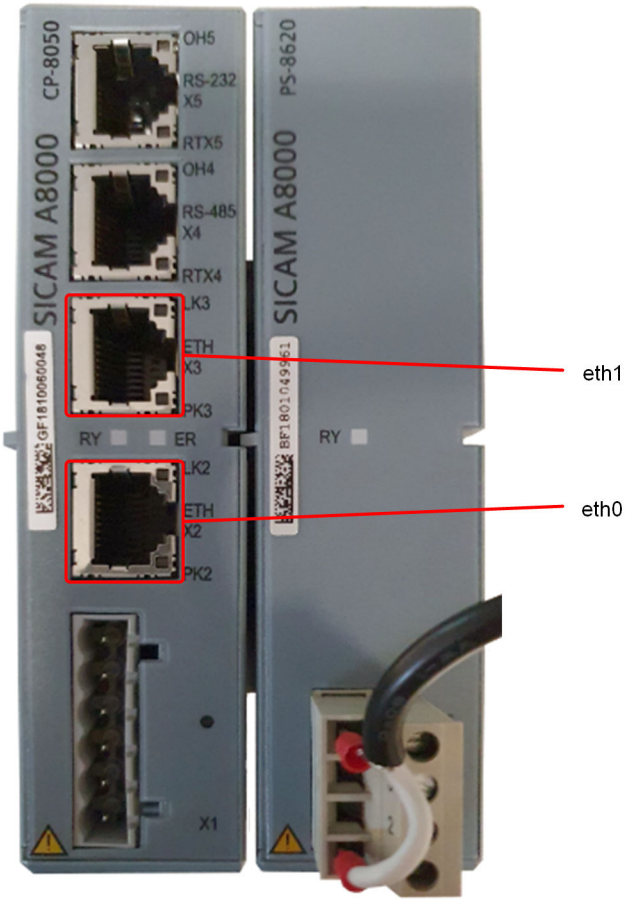


NOTE

Use a Linux-compatible text editor (for example Notepad++) to modify the configuration files. This is necessary because Linux has a slightly different text format than Windows operating systems.

Configuring the IP Addresses

This configuration is done in the file **network/interfaces**. The SIEMENS CP-8050 comes with 2 Ethernet interfaces, **eth0** (X2) and **eth1** (X3).



[ge_cp-8050_eth, 1, --_--]

Figure 2-1 The 2 Ethernet Interfaces of the CP-8050

Prerequisites

SIEMENS CP-8050 is installed and wired properly.
SIEMENS CP-8050 is connected to **station network** on port X2 (eth0).
SIEMENS CP-8050 is connected to **wide area network** on port X3 (eth1).

Procedure

✧ In order to set specific IP addresses, adjust the file **network/interfaces** accordingly:

```
iface lo inet loopback

auto eth0
iface eth0 inet static
     address 172.16.0.27
     netmask 255.255.0.0

auto eth1
iface eth1 inet static
     address 192.168.1.27
```

```
        netmask 255.255.255.0
        gateway 192.168.1.1
```

✧ It is also possible to configure the usage of DHCP.
For example, a configuration for **eth1** looks as follows:

```
iface lo inet loopback

auto eth0
iface eth0 inet static
        address 172.16.0.27
        netmask 255.255.0.0

auto eth1
allow-hotplug eth1
iface eth1 inet dhcp
```



NOTE

It is **not recommended** to use DHCP in a production environment because of cybersecurity constraints.

Configuring the Name Server (DNS)

This configuration is done in the file **resolv.conf**.

SICAM GridEdge needs a proper name server configuration for the cloud connection.

✧ The Google name server is configured by default. If required, adjust the file according to the needs of your IT infrastructure.

```
nameserver 8.8.8.8
```

Configuring the NTP Client for Time Synchronization

This configuration is done in the file **ntp.conf**.

SICAM GridEdge needs a proper time synchronization for the cloud connection.

✧ Adjust the file **ntp.conf** according to your needs.

```
server 0.pool.ntp.org iburst
server 1.pool.ntp.org iburst
server 2.pool.ntp.org iburst
server 3.pool.ntp.org iburst

# Allow only time queries, at a limited rate, sending KoD when in excess.
# Allow all local queries (IPv4, IPv6)
restrict default nomodify nopeer noquery limited kod
restrict 127.0.0.1
restrict [::1]
```

If you have your own NTP time servers in the network, use them instead of the global default given.

If you do not have your own private NTP server within your network, consider using public severs in your area (e.g. from *https://www.ntppool.org/*)

2.1.3 Installing SICAM GridEdge with Prepared SD Card

NOTICE

Security issue

After the installation of SICAM GridEdge the SSH access is enabled by default and the remote-host identification/fingerprint is changed. The username is root and the password is empty.

- ✧ To disable the SSH access, connect to the CP-8050 via SSH and enter the command **/extern/lxp/install/disable-ssh.sh**
- ✧ After executing the script, the CP-8050 is not accessible via SSH anymore.

NOTICE

Possible corruption of data structure

Do not power off the SIEMENS CP-8050 device during installation.

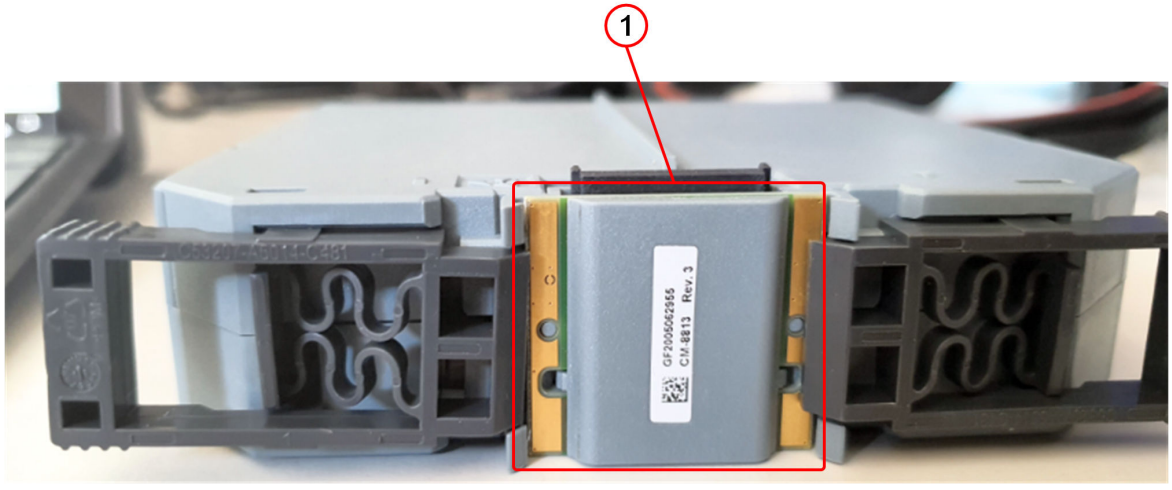
- ✧ In order to check if the installation has completed successfully, open your Web browser and connect to SICAM GridEdge Web Interface (see *3.1 Access to SICAM GridEdge Web Interface*).
- ✧ If SICAM GridEdge Web Interface is not accessible within 30 minutes, the installation has failed. In this case, re-create the SD Card as described in *2.1.2 Preparing SD Card for Installation* and repeat the installation.

To install SICAM GridEdge

NOTE

After installation of SICAM GridEdge the file system is erased and created newly.
In case of updating your SICAM GridEdge version, create a backup of your configuration before.

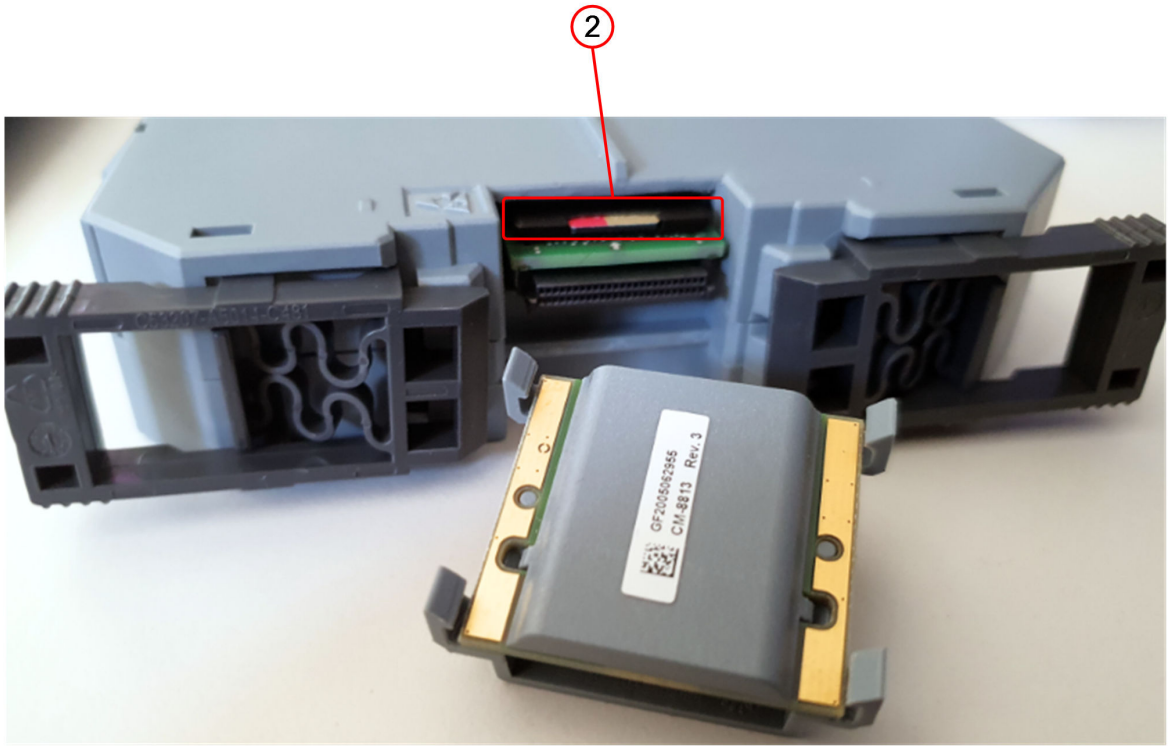
The SD card slot is located behind a plug of the SIEMENS CP-8050.



[ge_cp-8050_card_slot1, 1, --_--]

(1) Plug of the SD card slot

- ✧ Remove the plug to get access to the SD card slot.



[ge_cp-8050_card_slot2, 1, --_--]

(2) SD card slot

✧ Insert the SD card into the slot, apply the plug, and start the SIEMENS CP-8050.

NOTE

SICAM GridEgde is installing automatically. This may take several minutes.

2.2 SIEMENS IPC 227E

2.2.1 Installing SIMATIC Industrial OS

Prerequisites

- SIMATIC IPC 227E is installed and wired properly; refer to the SIMATIC IPC227E Quick Install Guide (*https://support.industry.siemens.com/cs/ww/de/view/109477819*).
- Monitor is connected to IPC
- Keyboard is connected to IPC
- IPC is connected to station network and wide area network (required for connection to external cloud platform and for fetching updates of operating system)
- Prepared USB Service Stick for installation of the operating system (for creation instructions refer to Installation Manual of SIMATIC Industrial OS **SIMATIC_Industrial_OS_Vxxxx_Installation_Manual.pdf**)

Installing SIMATIC Industrial OS

✧ Connect USB Service Stick to switched off IPC

✧ Switch on IPC and open BIOS settings.

NOTE

Follow the instructions in chapter 3 "Boot the target with SIMATIC Industrial OS" as written in the section "Prerequisites". Especially see when and how long to press the <ESC> button to get into the BIOS.

- ✧ Open the **Setup Utility** (SCU) and enable **USB Boot** in the **Boot** submenu. Then exit SCU via **Exit saving changes**.
- ✧ Execute the steps in section **Procedure** of the installation manual and boot from the attached USB Service Stick.
- ✧ Select **Install system**.
- ✧ Verify that the installed SSD and the **image-industrial-os-ipc-.....wic.gz** file are selected.

NOTE

If you repeat the installation, the program might find backups. If you want to install completely new, select **Reboot and continue without restoring**.

NOTE

After the installation is finished, the IPC will reboot.
Do not unplug the USB Service Stick because packages will be partly installed from this medium during first boot procedure.

Configuration of SIMATIC Industrial OS

After the first boot of the IPC, SIMATIC Industrial OS shows a setup menu which guides you through the first boot.

NOTE

A network cable for Wide Area Network must be connected to the **X1P1** port.

- ✧ Select **enp2s0** and define the IP settings for the port **X1P1** (DHCP/Static, IP Address, Subnetmask, Gateway, DNS).

NOTE

It is strongly recommended to use a **static IP address**.

NOTE

If the network configuration between the commissioning and the operation environment differs, you can reconfigure this using the tool **industrial-setup** later on.

- ✧ For network seperation between Wide Area Network and Station Network, configure the network settings accordingly for network adapter **enp3s0**. For Gateway, use 0.0.0.0 here and leave the DNS empty except there is an internal DNS server in your internal network.

NOTE

It is strongly recommended to use a **static IP address**.

- ✧ Configure the localization settings (keyboard language, layout, region, etc.).
- ✧ Define the host name of the IPC.

✧ Setup the **Time Synchronization** for the IPC with NTP, for example:
`0.de.pool.ntp.org,1.de.pool.ntp.org,2.de.pool.ntp.org,3.de.pool.ntp.org`

NOTE

If an NTP Server is available in your network, add this as first/primary NTP server.

NOTE

Since a time synchronization is necessary for a proper connection between GridEdge and the cloud platform, it is strongly recommended to configure NTP properly.

✧ Configure at least 1 APT mirror (Advanced Package Tool).

✧ Select an address from the list nearby the final location of the IPC.

✧ Enable **Main** and **Contrib**, but keep **Non-free** disabled to define which packages can be loaded from the mirror.

✧ Do not disable the **root** login. For security reasons, set a password for the user **root**.

✧ Define the **User Login Credentials** and password.

✧ Enable **sudo** for this user.

✧ Define the frequency of the software updates, for example, daily or weekly.

✧ Define **Proxy Settings** if required.

✧ Enable the **Firewall** if required later on in the operation environment.

✧ Install the following additional package in the **Development Tools** menu:
Essential development tools (IPC)/Linux Containers/Docker CE

✧ Select **no driver/support** for **PROFINET Settings**.

The IPC now installs the selected packages and loads and installs packages from the Internet via the WAN connection.

The installation ends with the message *`You have completed ...`* and some standard warnings about possibly failed installations. These are checked in the next step. Confirm with **OK** and the IPC will reboot.

At the first login, check with the command **`docker version`** if the docker framework has been installed. If no version is replied, check the installation of the **Docker CE** package.

NOTE

If you need to configure or reconfigure some settings of the SIMATIC Industrial OS, you can use the following command: **`sudo industrial-setup`**

2.2.2 Installing SICAM GridEdge

✧ Copy the complete content of the package to the IPC using SSH.

- or -

✧ Copy the complete content of the package to the IPC using a USB stick.

NOTE

Keep in mind that the SIMATIC Industrial OS does not automatically mount the USB stick. This has to be done manually, see *2.2.3 Mounting the USB Drive*GridEdge manual, chapter 2.3 Mounting the USB Drive.

✧ Extract the package and change the directory to the extracted folder.

- ✧ Add execution rights to scripts: **chmod +x *.sh**
- ✧ Execute the script **sicamgridedge_setup.sh** with administrator rights.
- ✧ When prompted, enter the IP address of the interface connected to the substation network (X2P1) .

After the installation, the SICAM GridEdge system is up and running.



NOTE

If you update the network settings of the IPC where SICAM GridEdge is running, it is necessary to re-create the self-signed certificate used by the SICAM GridEdge Web Interface.

To do so, execute the following script:

sicamgridege_setup.sh -n

2.2.3 Mounting the USB Drive

To mount the USB drive, execute the following commands:

- ✧ Identify the USB drive:
  edge@NANOBOX-3:~$ sudo fdisk -l

The result of this command may look as follows:

```
[sudo] password for edge:
Disk /dev/sda: 28 GiB, 30016659456 bytes, 58626288 sectors
Units: sectors of 1 * 512 = 512 bytes
Sector size (logical/physical): 512 bytes / 512 bytes
I/O size (minimum/optimal): 512 bytes / 512 bytes
Disklabel type: gpt
Disk identifier: 21602A5F-D802-4696-B737-AC1F52D3F17A

Device Start End Sectors Size Type
/dev/sda1 2048 133119 131072 64M EFI System
/dev/sda2 133120 58626254 58493135 27.9G Linux filesystem

Disk /dev/sdb: 3.8 GiB, 4009754624 bytes, 7831552 sectors
Units: sectors of 1 * 512 = 512 bytes
Sector size (logical/physical): 512 bytes / 512 bytes
I/O size (minimum/optimal): 512 bytes / 512 bytes
Disklabel type: dos
Disk identifier: 0xc3072e18

Device Boot Start End Sectors Size Id Type
/dev/sdb1 * 63 7831551 7831489 3.8G c W95 FAT32 (LBA)
```

The last entry in this case is the USB stick (/dev/sdb1).

- ✧ Create a target folder for mounting:
  edge@NANOBOX-3:~$ sudo mkdir /media/usb-drive
- ✧ Mount the USB drive:
  edge@NANOBOX-3:~$ sudo mount /dev/sdb1 /media/usb-drive -o umask=000
- ✧ List the content of the mounted drive:
  edge@NANOBOX-3:~$ ls /media/usb-drive

The content will look like this:

```
SICAM_GridEdge_1.1
```

✧ Copy the SICAM GridEdge setup data into the home directory:
edge@NANOBOX-3:~$ cp -r /media/usb-drive/SICAM_GridEdge_1.1 ~

✧ Unmount the USB drive:
edge@NANOBOX-3:~$ sudo umount /dev/sdb1

2.2.4 Example Installation

Below you can find an example of the installation steps.

```
edge@NANOBOX-3:~$ id
uid=1000(edge) gid=1000(edge) groups=1000(edge),1001(docker)
edge@NANOBOX-3:~$ cd setup_x86_64/
edge@NANOBOX-3:~/setup_x86_64$ chmod +x *.sh
edge@NANOBOX-3:~/setup_x86_64$ ls -la
total 21664
drwxr-xr-x  3 pi pi     4096 Dec  9 17:12 .
drwxr-xr-x 13 pi pi     4096 Dec  9 17:10 ..
-rw-r--r--  1 pi pi 11747993 Dec  9 17:00 docker-compose-1.23.2-Linux-x86_64
-rw-r--r--  1 pi pi     3885 Dec  9 17:00 docker-compose.yml
-rwxr-xr-x  1 pi pi     1831 Dec  9 17:00 dumpstats_cron.sh
-rw-r--r--  1 pi pi      436 Dec  9 17:00 .env
drwxr-xr-x  2 pi pi     4096 Dec  9 17:01 images
-rwxr-xr-x  1 pi pi      178 Dec  9 17:00 open_valueviewer.sh
-rwxr-xr-x  1 pi pi     1579 Dec  9 17:00 show_syslogs.sh
-rw-r--r--  1 pi pi     4550 Dec  9 17:01 SICAM_GridEdge_Changelog.md
-rw-r--r--  1 pi pi      295 Dec  9 17:00 sicamgridedge.ini
-rw-r--r--  1 pi pi  3925536 Dec  9 17:01 SICAM_GridEdge_Manual_en.pdf
-rwxr-xr-x  1 pi pi    13801 Dec  9 17:00 sicamgridedge_modules.sh
-rw-r--r--  1 pi pi   590205 Dec  9 17:01 SICAM_GridEdge_PI_en.pdf
-rw-r--r--  1 pi pi  5800729 Dec  9 17:01 SICAM_GridEdge_ReadmeOSS.html
-rwxr-xr-x  1 pi pi    14321 Dec  9 17:00 sicamgridedge_setup.sh
-rwxr-xr-x  1 pi pi    20722 Dec  9 17:00 sicamgridedge.sh
-rw-r--r--  1 pi pi       13 Dec  9 17:01 version.info
edge@NANOBOX-3:~/setup_x86_64$ sudo ./sicamgridedge_setup.sh
```

3 SICAM GridEdge Configuration

This section contains a guideline for configuring a SICAM GridEdge for use in combination with the Siemens Grid Diagnostic Suite Applications.

3.1	Access to SICAM GridEdge Web Interface	20
3.2	General Settings	20
3.3	Application Configuration	26
3.4	Connection Status	42
3.5	Maintenance	44
3.6	Asset Information	44

3.1 Access to SICAM GridEdge Web Interface

The SICAM GridEdge Web interface is available at *https://<STATION_LAN_IP>:8900*, for example *https://192.168.1.1:8900*.



[sc_SICAM_GridEdge_WebInterface, 4, en_US]

Figure 3-1 Access to the SICAM GridEdge Web Interface

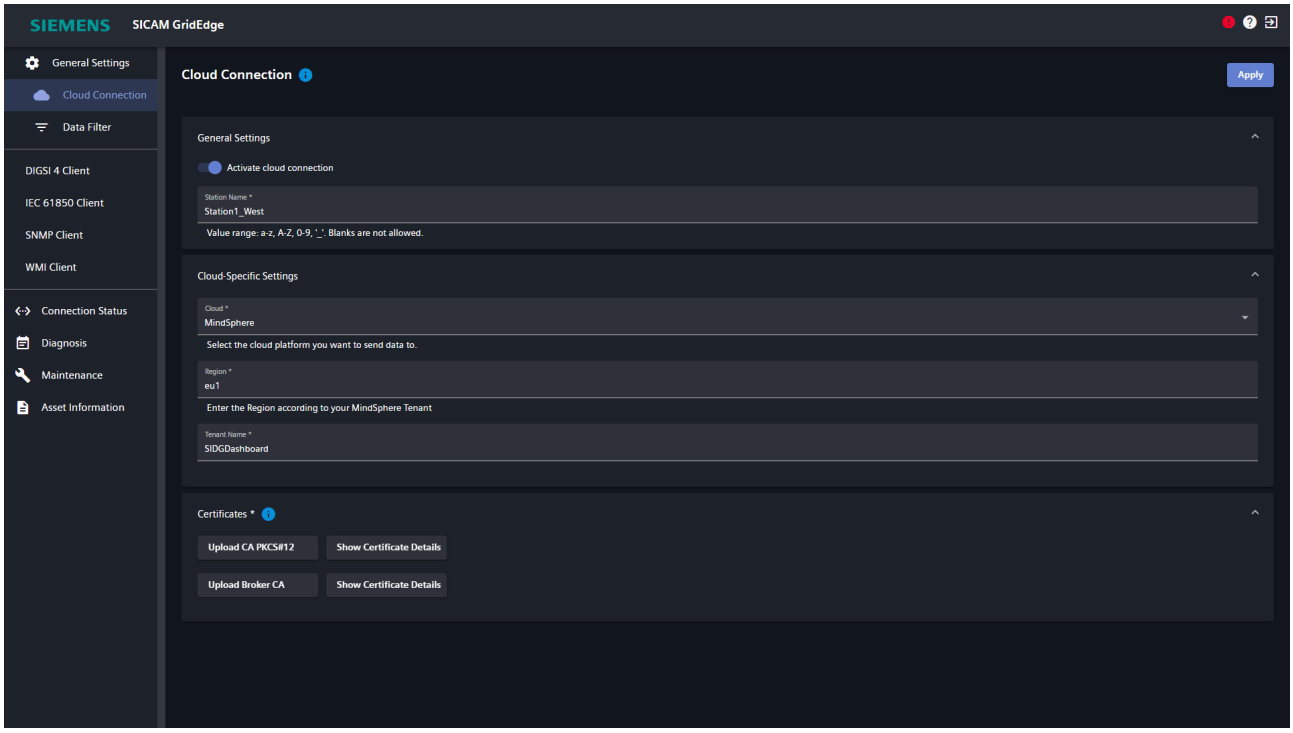
When you log on to SICAM GridEdge for the first time you need to set a password.

3.2 General Settings

To configure the SICAM GridEdge basic settings for the SIEMENS Grid Diagnostic Suite Applications, the following steps have to be executed:

- Configure the cloud connection
- Configure the data filter (optional)

3.2.1 Configuring the Cloud Connection



[sc_SICAM_GridEdge_Cloud_connection, 5, en_US]

Figure 3-2 Cloud Connection

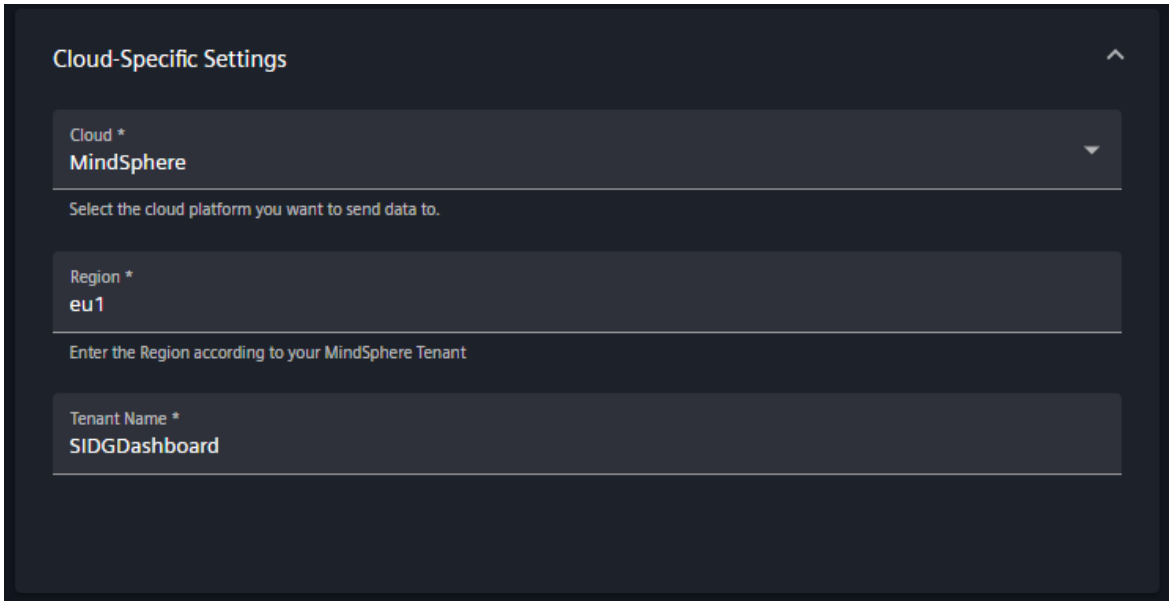
- ✧ Activate the Cloud Connection with the slider on the top.
- ✧ Enter the **Station Name** where your SICAM GridEdge is located (e.g. **Station1_West**).

NOTE

The name should be unique in your cloud platform.

- ✧ From the Cloud list box select the cloud platform you want to send data to (MindSphere, Azure, On-Premise). Depending on the selection or option you will have to choose different settings.

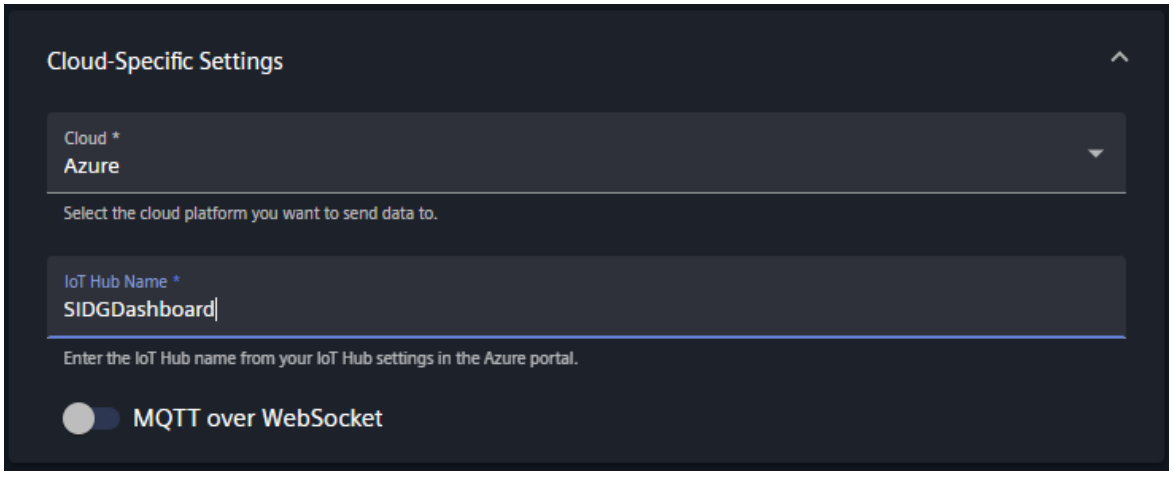
MindSphere-Specific Settings



[sc_mindsphere_spec, 2, en_US]

- ✧ Enter the **Region** according to your MindSphere Tenant.
  Example: You have to enter the region (bold text) of the complete address:
  https://<MindSphere Tenant Name>.**eu1**.mindsphere.io.
- ✧ Enter the **Tenant Name** according to your MindSphere Tenant.
  Example: You would only have to enter the tenant name (bold text) of the complete address:
  https://**<Tenant Name>**.eu1.mindsphere.io.

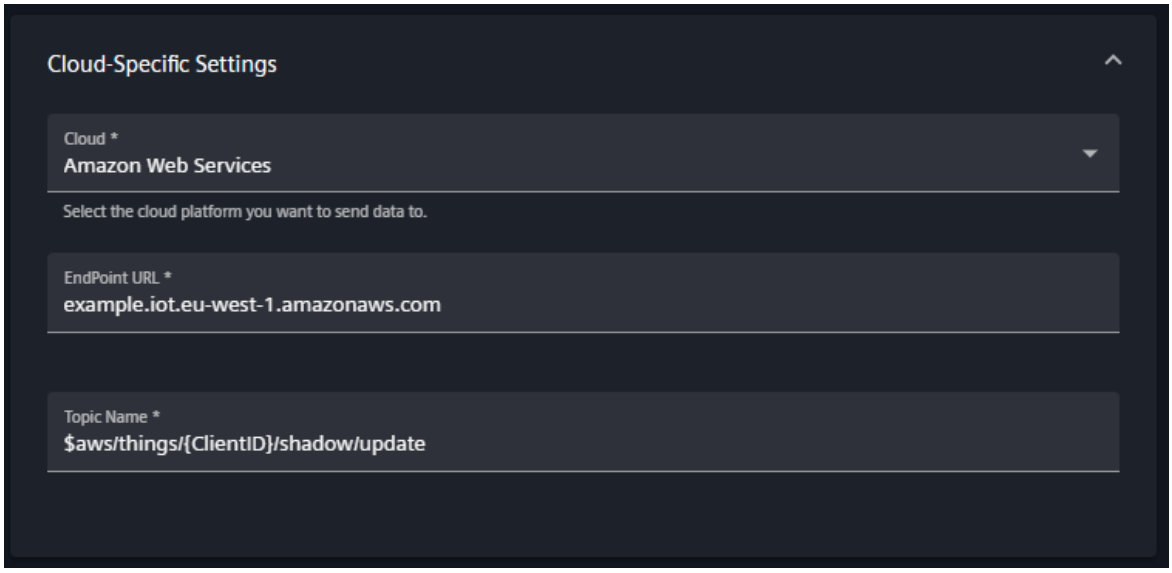
Azure-Specific Settings



[sc_azure_spec, 2, en_US]

- ✧ Enter the **IoT Hub Name** according to your configuration visible in Azure portal.
- ✧ Enable **MQTT over WebSockets** to send data via Websockets instad of native MQTT (this option can help solving issues with firewall limitations in your network).

Amazon Web Services (AWS) Settings



[sc_aws_spec, 1, en_US]

✧ Enter the **EndPoint URL** of your AWS account.

✧ Enter the **Topic Name** for which you want to publish data.

NOTE

For the Topic Name it is possible to use tags which are replaced later on in the SICAM GridEdge system for publishing data.

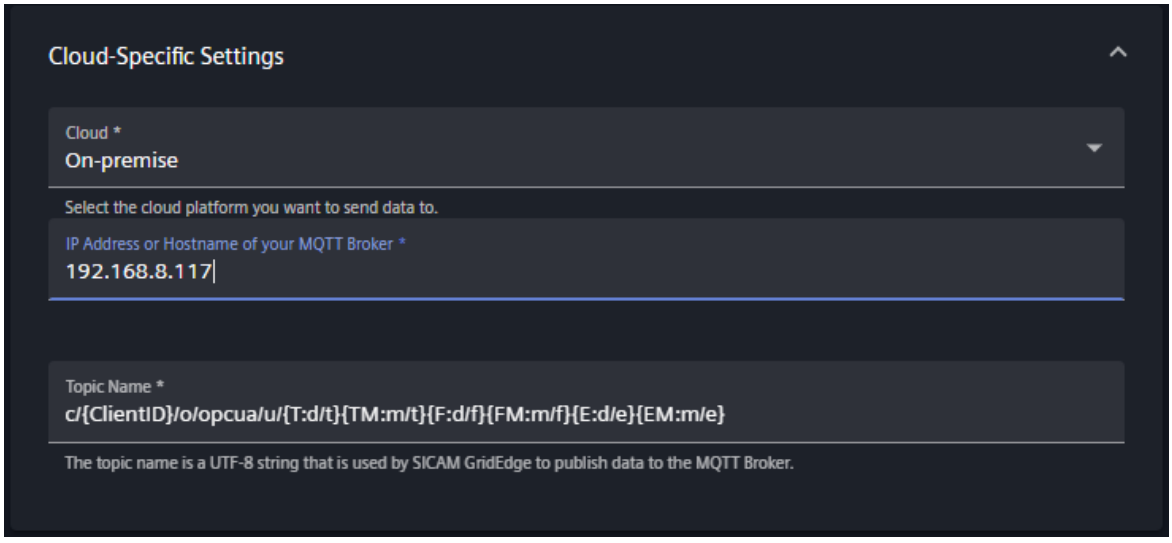
- {ClientID}: Is replaced by the Publisher ID of the device
- {T:d/t}{TM:m/t}{F:d/f}{FM:m/f}{E:d/e}{EM:m/e}: Defines subtopics or subdirectories depending on the message type
- Abbreviation Meaning
  - T Time Series key and delta frame
  - TM Time Series meta frame
  - E Events key and delta frame
  - EM Events meta frame
  - F Files key and delta frame
  - FM Files meta frame

Examples with c/{ClientID}/o/opcua/u/{T:d/t}{TM:m/t}{F:d/f}{FM:m/f}{E:d/e}{EM:m/e}
and Client ID = "Q100_7KG95_GF1609500232":

Resulting topic name for time series delta frames: **c/Q100_7KG95_GF1609500232/o/opcua/u/d/t**

Resulting topic name for events meta frame: **c/Q100_7KG95_GF1609500232/o/opcua/u/m/e**

On-Premise Settings



[sc_on-premise_spec, 2, en_US]

✧ Enter the **IP Address or Hostname** of your MQTT Broker.

✧ Enter the **Topic Name** for which you want to publish data.

NOTE

For the Topic Name it is possible to use tags which are replaced later on in the SICAM GridEdge system for publishing data.

- {ClientID}: Is replaced by the Publisher ID of the device
- {T:d/t}{TM:m/t}{F:d/f}{FM:m/f}{E:d/e}{EM:m/e}: Defines subtopics or subdirectories depending on the message type
- Abbreviation Meaning
  - T Time Series key and delta frame
  - TM Time Series meta frame
  - E Events key and delta frame
  - EM Events meta frame
  - F Files key and delta frame
  - FM Files meta frame

Examples with c/{ClientID}/o/opcua/{VersionMS}/u/{T:d/t}{TM:m/t}{F:d/f}{FM:m/f}{E:d/e}{EM:m/e}
and Client ID = "Q100_7KG95_GF1609500232":

Resulting topic name for time series delta frames: **c/Q100_7KG95_GF1609500232/o/opcua/v3/u/d/t**

Resulting topic name for events meta frame: **c/Q100_7KG95_GF1609500232/o/opcua/v3/u/m/e**

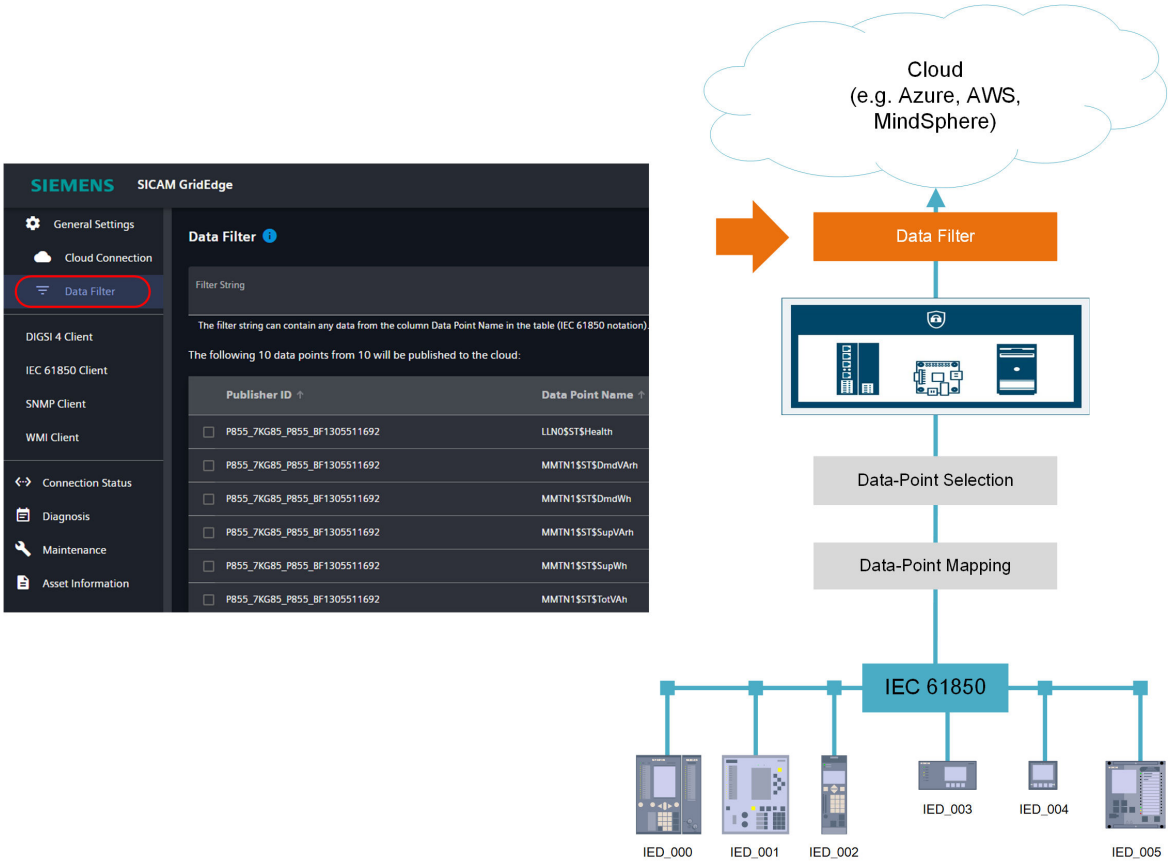
✧ To upload a (intermediate) Certificate Authority in a PKCS#12 container format, click **CA PKCS#12 File**.
If your PKCS#12 container is encrypted with a password, enter the password in the import dialog. If your PKCS#12 file is not encrypted, leave the corresponding field empty.
Click **Open** to proceed.
For further information on certificate handling refer to *4.5 Certificate Management*.

✧ Upload the Certificate Authority of the MindSphere Broker.

✧ **Apply** the changes.

3.2.2 Configuring the Data Filter

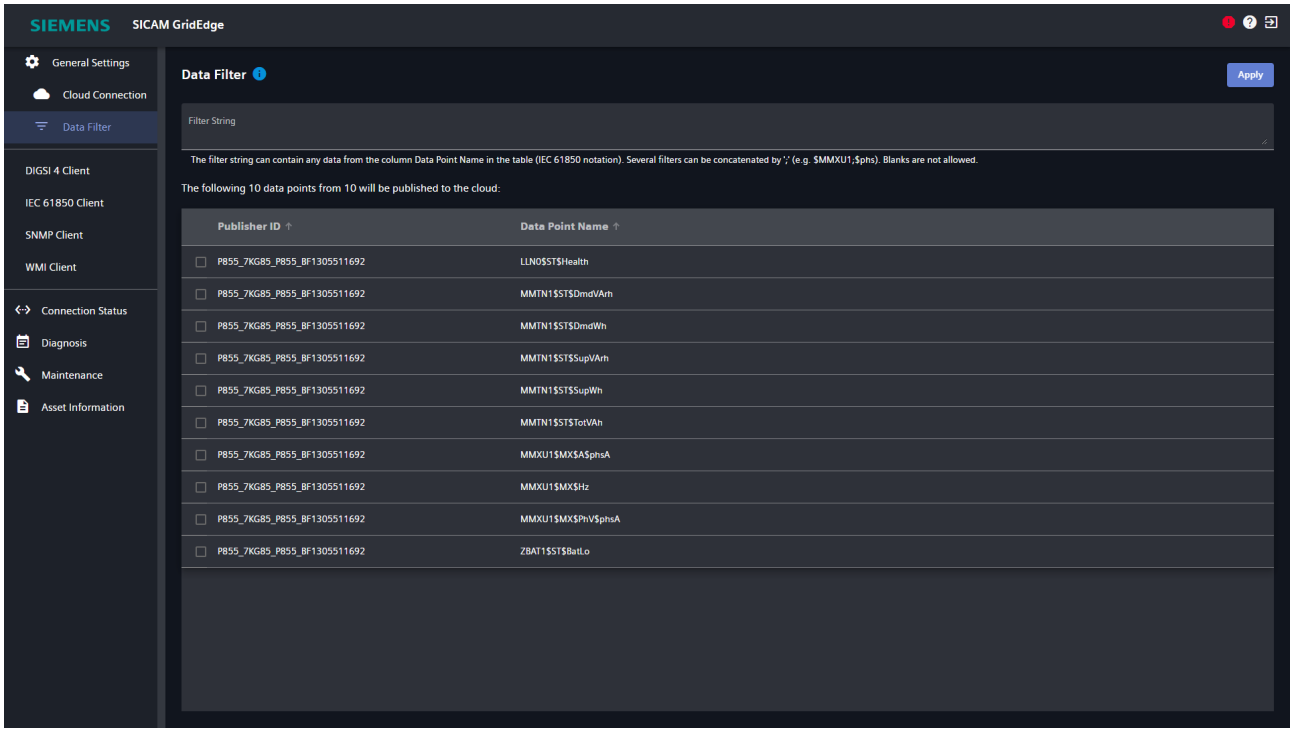
In the section **Data Filter**, you can optionally enter a filter string to filter which data is to be transmitted to the external cloud platform.



[dw_data_filter, 1, en_US]

For the SIEMENS Grid Diagnostic Suite Applications, it is not required to add a filter here.

If no filter string is entered, all data will be published. Several filter keys can be entered separated by semicolons. The effect of the data filter on the data points can be viewed in the resulting table:



[sc_SICAM_GridEdge_data_filter, 4, en_US]

Figure 3-3 Data Filter

✧ Set the filter string, for example, to **`Hz;TotW`**.

All data points which either match Hz or TotW will be published.

NOTE

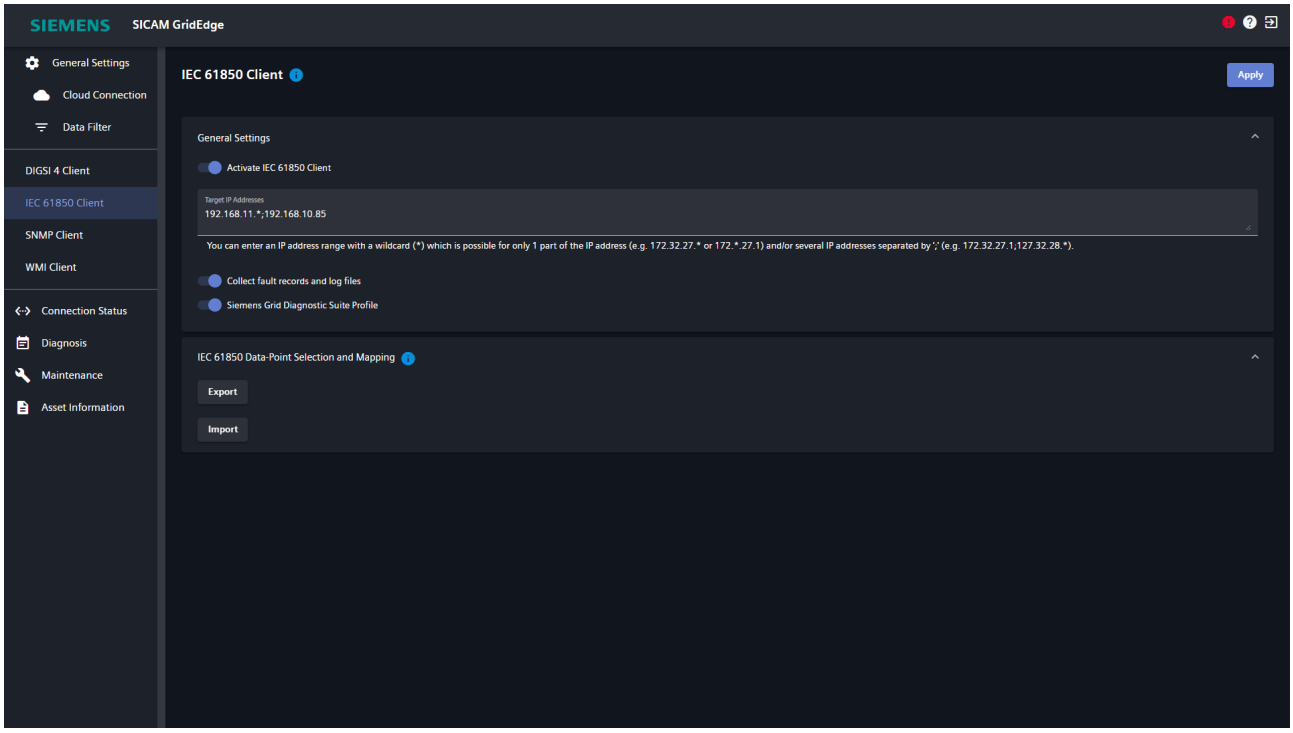
As a help for selecting the filters properly, adding a semicolon (";") at the end of the filter string will show all possible data points to be selected in the data table below.

3.3 Application Configuration

To configure the SICAM GridEdge application settings for the SIEMENS Grid Diagnostic Suite Applications, you have to configure the IEC 61850 Client.

3.3.1 Configuring the IEC 61850 Client

IEC 61850 Client is used to fetch data from IEC 61850 devices and transfer them via SICAM GridEdge to the external cloud platform.



[sc_SICAM_GridEdge_IEC61850_Client, 6, en_US]

Figure 3-4 IEC 61850 Client

- ✧ Activate **IEC 61850 Client**.
- ✧ Add the IP address range of the devices in the station network or dedicated IP addresses in **Target IP Addresses**.

  Example: `Target IP Addresses = 192.168.11.*;192.168.10.85`

  If IEC 61850 Client is enabled, SICAM GridEdge will automatically scan for devices in the IP range **192.168.11.1** to **192.168.11.254** and will additionally communicate with the device **192.168.10.85**.
- ✧ If files (COMTRADE, COMFEDE) from devices are to be fetched and transferred to the external cloud platform, enable **Collect fault records and log files**.
- ✧ Select **Siemens Grid Diagnostic Suite Profile** as **Data Profile**.
- ✧ **Apply** the changes.

The Siemens Grid Diagnostic Suite Profile describes data which is used by SIPROTEC Grid Diagnostic Suite Applications. If used, only data needed for this is fetched from the IEC61850 devices.

SICAM GridEdge will transfer relevant data based on the determined device type (protection device, Power Quality device) to the cloud platform.

Protection Devices

Table 3-1 Protection Devices – Grid Events

Grid Events	Examples 61850 Path
Device not healthy: LDN	Application/LLN0STHealth Q0_Bay1/LLN0STHealth
Relay pickup: LDN	Q0_Bay1/PTRC1STStr
Relay trip: LDN	Q0_Bay1/PTRC1STTr
Hotspot temp. warning: LDN	PTS1_49HotSpot1/HTSP_PTTR1STHSTWarn PTS2_49HotSpot1/HTSP_PTTR1STHSTWarn
Hotspot temp. alarm: LDN	PTS1_49HotSpot1/HTSP_PTTR1STHSTAlm PTS2_49HotSpot1/HTSP_PTTR1STHSTAlm
Changed settings	n.a. (event is generated by GridEdge)

Table 3-2 Protection Devices – Measured Values

Measured Values	Examples 61850 Path
Active Power (total): LDN	TotW
Reactive Power (total): LDN	TotVAr
Frequency: LDN	Hz
Phase-to-phase voltage L12: LDN	PPV$phsAB
Phase-to-phase voltage L23: LDN	PPV$phsBC
Phase-to-phase voltage L31: LDN	PPV$phsCA
Phase-to-ground voltage L1: LDN	PhV$phsA
Phase-to-ground voltage L2: LDN	PhV$phsB
Phase-to-ground voltage L3: LDN	PhV$phsC
Calculated zero-sequence voltage: LDN	PhV$res
Calculated zero-sequence current: LDN	A$res
Phase current L1: LDN	A$phsA
Phase current L2: LDN	A$phsB
Phase current L3: LDN	A$phsC

Table 3-3 Protection Devices – Condition Monitoring Values

Measured Values	Examples 61850 Path
ΣIx L1: LDN	CB1_CBWearMonitoring/PIx_SCBR1STSumIxA
ΣIx L2: LDN	CB1_CBWearMonitoring/PIx_SCBR1STSumIxB
ΣIx L3: LDN	CB1_CBWearMonitoring/PIx_SCBR1STSumIxC
ΣI²t L1: LDN	CB1_CBWearMonitoring/I2t_SCBR1STSumI2tA
ΣI²t L2: LDN	CB1_CBWearMonitoring/I2t_SCBR1STSumI2tB
ΣI²t L3: LDN	CB1_CBWearMonitoring/I2t_SCBR1STSumI2tC
Make time: LDN	CB1_CBWearMonitoring/MkTm_SCBR1MXMakeTime
2P Endur. L1: LDN	CB1_CBWearMonitoring/P2P_SCBR1STEnduA
2P Endur. L2: LDN	CB1_CBWearMonitoring/P2P_SCBR1STEnduB
2P Endur. L3: LDN	CB1_CBWearMonitoring/P2P_SCBR1STEnduC
Breaking-current sum	CB1/XCBR1STSumSwARs
Breaking-current sum L1	CB1/XCBR1STSumSwARsA
Breaking-current sum L2	CB1/XCBR1STSumSwARsB
Breaking-current sum L3	CB1/XCBR1STSumSwARsC

Measured Values	Examples 61850 Path
Circuit breaker Operation Counter	CB1/XCBR1STOpCnt
Disconnector Operation Counter	Dc1/XSWI1STOpCnt

Table 3-4 Protection Devices – Protection Manager / Level 1 Information

Measured Values	Examples 61850 Path
Circuit breaker position	CB1/XCBR1STPos
Disconnector position	Dc1/XSWI1STPos
79 successful	CB1_79AutoReclosing/GEN_RREC1/Successful
Blk. by binary input	CB1_79AutoReclosing/GEN_RREC1/BlkBinInp
Blk. by circuit breaker ready sup.	CB1_79AutoReclosing/GEN_RREC1/BlkCBsup
Blk. by strtsig. superv.	CB1_79AutoReclosing/GEN_RREC1/BlkStrtSup
Blk. by action time exp.	CB1_79AutoReclosing/GEN_RREC1/BlkActTm
Blk. by max.d.t. expiry	CB1_79AutoReclosing/GEN_RREC1/BlkDTexp
Blk. by max. d.t. delay	CB1_79AutoReclosing/GEN_RREC1/BlkDTdlyEx
Blk. by evolving fault	CB1_79AutoReclosing/GEN_RREC1/BlkEvolFlt
Blk. by no cycle	CB1_79AutoReclosing/GEN_RREC1/BlkMatchCy
Blk. by protection	CB1_79AutoReclosing/GEN_RREC1/BlkByProt
Blk. by dead-line check	CB1_79AutoReclosing/GEN_RREC1/BlkDLC
Blk. by loss of voltage	CB1_79AutoReclosing/GEN_RREC1/BlkVltFail
Blk. by max. cycles	CB1_79AutoReclosing/GEN_RREC1/BlkMaxCyc
Direction	PTRC1STStr.dirGeneral
Direction L1	PTRC1STStr.dirPhsA
Direction L2	PTRC1STStr.dirPhsB
Direction L3	PTRC1STStr.dirPhsC
Direction neutral	PTRC1STStr.dirNeut
Pickup L1	PTRC1STStr.phsA
Pickup L2	PTRC1STStr.phsB
Pickup L3	PTRC1STStr.phsC
Pickup neutral	PTRC1STStr.neut
Fault distance	Ln1/SE_RFLO1MXFltDis

Power Quality Devices

Table 3-5 Power Quality Devices – Grid Events

Grid Events	Examples 61850 Path
Device Health	LLN0STHealth
Battery Failure	ZBAT1STBatLo
Fault Record Stored	PQA_RDRE1STRcdMade
Frequency Variation Event Start	PQA_QFVR1STVarStr
Voltage Unbalance Event Start	PQA_QVUB1STVarStr
Voltage Variation Event Start	PQA_QVVR1STVarStr
Voltage Swell Event	PQA_QVVR1STSwlStr
Voltage Dip Event	PQA_QVVR1STDipStr
Voltage Interruption Event	PQA_QVVR1STIntrStr
Affected Phases by a Voltage Variation Event	PQA_QVVR1STAffPhs

Table 3-6 Power Quality Devices – Measured Values

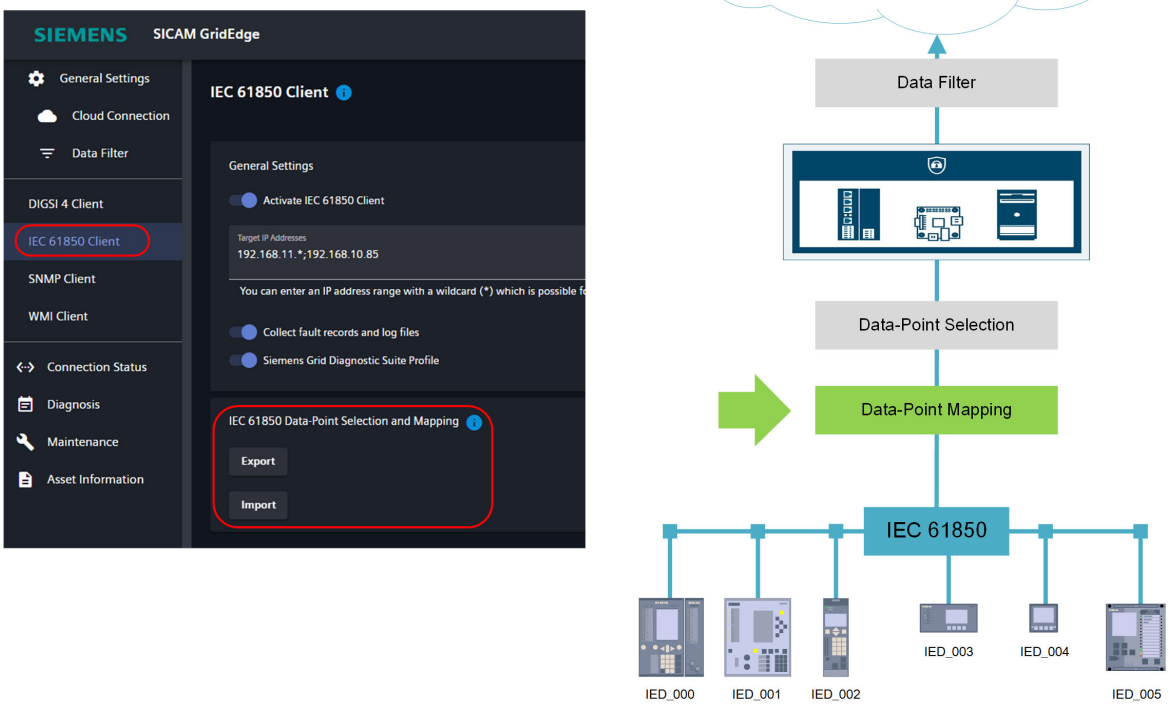
Measured Values	Examples 61850 Path
Voltage Variation Event Level	PQA_QVVR1MXVVa
Voltage Variation Event Duration	PQA_QVVR1MXVVaTm
Phase to Ground Voltage - Phase A	PQA2MMXU1MXPhV$phsA
Phase to Ground Voltage - Phase B	PQA2MMXU1MXPhV$phsB
Phase to Ground Voltage - Phase C	PQA2MMXU1MXPhV$phsC
Phase to Phase Voltage - Phase AB	PQA2MMXU1MXPPV$phsAB
Phase to Phase Voltage - Phase BC	PQA2MMXU1MXPPV$phsBC
Phase to Phase Voltage - Phase CA	PQA2MMXU1MXPPV$phsCA
Phase to Ground Voltage (Single Phase)	PQA2MMXN1MXVol
Phase to Ground Voltage - Neutral	PQA2MMXU1MXPhV$neut
Average Phase to Phase Voltage	PQA2MMXU1MXAvPPVPhs
Phase Current - Phase A	PQA2MMXU1MXA$phsA
Phase Current - Phase B	PQA2MMXU1MXA$phsB
Phase Current - Phase C	PQA2MMXU1MXA$phsC
Phase Current (Single Phase)	PQA2MMXN1MXAmp
Phase Current - Neutral	PQA2MMXU1MXA$neut
Average Phase Current	PQA2MMXU1MXAvAPhs
Active Power - Phase A	PQA2MMXU1MXW$phsA
Active Power - Phase B	PQA2MMXU1MXW$phsB
Active Power - Phase C	PQA2MMXU1MXW$phsC
Total Active Power	PQA2MMXU1MXTotW
Active Power (Single Phase)	PQA2MMXN1MXWatt
Reactive Power - Phase A	PQA2MMXU1MXVAr$phsA
Reactive Power - Phase B	PQA2MMXU1MXVAr$phsB
Reactive Power - Phase C	PQA2MMXU1MXVAr$phsC
Total Reactive Power	PQA2MMXU1MXTotVAr
Reactive Power (Single Phase)	PQA2MMXN1MXVolAmpr
Apparent Power - Phase A	PQA2MMXU1MXVA$phsA
Apparent Power - Phase B	PQA2MMXU1MXVA$phsB
Apparent Power - Phase C	PQA2MMXU1MXVA$phsC
Total Apparent Power	PQA2MMXU1MXTotVA
Apparent Power (Single Phase)	PQA2MMXN1MXVolAmp
Power Factor - Phase A	PQA2MMXU1MXPF$phsA
Power Factor - Phase B	PQA2MMXU1MXPF$phsB
Power Factor - Phase C	PQA2MMXU1MXPF$phsC
Power Factor	PQA2MMXU1MXTotPF
Power Factor (Single Phase)	PQA2MMXN1MXPwrFact
Cosinus Phi - Phase A	PQA2MMXU1MXActivePF$phsA
Cosinus Phi - Phase B	PQA2MMXU1MXActivePF$phsB
Cosinus Phi - Phase C	PQA2MMXU1MXActivePF$phsC
Cosinus Phi	PQA2MMXU1MXTotActivePF
Cosinus Phi (Single Phase)	PQA2MMXN1MXActivePwrFact
Voltage Imbalance - Negative sequence component	PQA2MSQI1MXImbNgV
Current Imbalance - Negative sequence component	PQA2MSQI1MXImbNgA
Voltage Imbalance - Zero sequence component	PQA2MSQI1MXImbZroV
Current Imbalance - Zero sequence component	PQA2MSQI1MXImbZroA

Measured Values	Examples 61850 Path
Frequency	PQA4MMXU1MXHz
Frequency (Single Phase)	PQA4MMXN1MXHz
Total Harmonic Distortion Voltage - Phase A	PQA2MHAI1MXThdPhV$phsA
Total Harmonic Distortion Voltage - Phase B	PQA2MHAI1MXThdPhV$phsB
Total Harmonic Distortion Voltage - Phase C	PQA2MHAI1MXThdPhV$phsC
Total Harmonic Distortion Voltage - Phase AB	PQA2MHAI1MXThdPPV$phsAB
Total Harmonic Distortion Voltage - Phase BC	PQA2MHAI1MXThdPPV$phsBC
Total Harmonic Distortion Voltage - Phase CA	PQA2MHAI1MXThdPPV$phsCA
Total Harmonic Distortion Voltage (Single Phase)	PQA2MHAN1MXThdVol
Total Harmonic Distortion Current - Phase A	PQA2MHAI1MXThdA$phsA
Total Harmonic Distortion Current - Phase B	PQA2MHAI1MXThdA$phsB
Total Harmonic Distortion Current - Phase C	PQA2MHAI1MXThdA$phsC
Total Harmonic Distortion Current (Single Phase)	PQA2MHAN1MXThdAmp
Short Term Flicker - Phase A	PQA2MFLK1MXPhPst$phsA
Short Term Flicker - Phase B	PQA2MFLK1MXPhPst$phsB
Short Term Flicker - Phase C	PQA2MFLK1MXPhPst$phsC
Long Term Flicker - Phase A	PQA2MFLK1MXPhPlt$phsA
Long Term Flicker - Phase B	PQA2MFLK1MXPhPlt$phsB
Long Term Flicker - Phase C	PQA2MFLK1MXPhPlt$phsC
Harmonic Voltage Array - Phase A	PQA2MHAI1MXHPhV$phsAHar
Harmonic Voltage Array - Phase B	PQA2MHAI1MXHPhV$phsBHar
Harmonic Voltage Array - Phase C	PQA2MHAI1MXHPhV$phsCHar
Harmonic Voltage Array - Phase AB	PQA2MHAI1MXHPPV$phsABHar
Harmonic Voltage Array - Phase BC	PQA2MHAI1MXHPPV$phsBCHar
Harmonic Voltage Array - Phase CA	PQA2MHAI1MXHPPV$phsCAHar
Maximum Harmonic Voltage Array - Phase A	MAX_PQA2MHAI1MXHPhV$phsAHar
Maximum Harmonic Voltage Array - Phase B	MAX_PQA2MHAI1MXHPhV$phsBHar
Maximum Harmonic Voltage Array - Phase C	MAX_PQA2MHAI1MXHPhV$phsCHar
Maximum Harmonic Voltage Array - Phase AB	MAX_PQA2MHAI1MXHPPV$phsABHar
Maximum Harmonic Voltage Array - Phase BC	MAX_PQA2MHAI1MXHPPV$phsBCHar
Maximum Harmonic Voltage Array - Phase CA	MAX_PQA2MHAI1MXHPPV$phsCAHar
Harmonic Voltage Array (Single Phase)	PQA2MHAN1MXHaVol
Maximum Harmonic Voltage Array (Single Phase)	MAX_PQA2MHAN1MXHaVol
Harmonic Power Array - Phase A	PQA2MHAI1MXHW$phsAHar
Harmonic Power Array - Phase B	PQA2MHAI1MXHW$phsBHar
Harmonic Power Array - Phase C	PQA2MHAI1MXHW$phsBHar
Harmonic Power Array (Single Phase)	PQA2MHAN1MXHaWatt
Total Real Energy Supply	MMTR1STSupWh
Real Energy Supply (Single Phase)	MMTN1STSupWh
Total Real Energy Demand	MMTR1STDmdWh
Real Energy Demand (Single Phase)	MMTN1STDmdWh
Total Reactive Energy Supply	MMTR1STSupVarh
Reactive Energy Supply (Single Phase)	MMTN1STSupVarh
Total Reactive Energy Demand	MMTR1STDmdVarh
Reactive Energy Demand (Single Phase)	MMTN1STDmdVarh
Total Net Apparent Energy	MMTR1STTotVAh
Net Apparent Energy (Single Phase)	MMTN1STTotVAh

3.3.2 Data-Point Mapping for the IEC 61850 Client

In the section **Data-Point Selection and Mapping** of **IEC 61850 Client** you can import a CSV file which allows to map data points from any IEC 61850 address/path to another IEC 61850 address/path. Such mapped data points are automatically selected for data retrieval.

This is required if your devices are using a different IEC 61850 addressing scheme than expected by the cloud applications. If you consider to view **wear monitoring** data from SIPROTEC4 devices in SIPROTEC Dashboard with data modeled with a GGIO structure, it is necessary to apply a mapping. You can find an example file in the ZIP bundle of SICAM GridEdge.



[dw_data_point_mapping, 1, en_US]

NOTE

For SIPROTEC 4 devices you can find an example mapping file in the setup bundle: **examples/IEC61850_Data_Mapping/IEC61850_Mapping_SIP4_WearMonitoring.csv**.

In order to define a data mapping that can be used in SICAM GridEdge, it is required to create a CSV file in a predefined format. The file contains the IED names where the mapping is to be applied to (column **IedName**), the data model as defined in the device (**Source**) and the desired data model that is used for publishing the data to the cloud (**Replacement**).

The columns in the CSV file are separated by semicolon ";".

NOTE

In the CSV file it is possible to configure Data Mapping and Data Selection.

Example CSV File

```
IedName;Source;Replacement
IED_000.*;EXT/pdGGIO2001$ST$ISCSO1;CB1_CBWearMonitoring/PIx_SCBR1$ST$SumIxA
IED_00000[1-9];EXT/pdGGIO2001$ST$ISCSO3;CB1_CBWearMonitoring/PIx_SCBR1$ST$SumIxC
```

In the example above

- the data point with the name **EXT/pdGGIO2001STISCSO1** of the devices whose IED name starts with "IED_000" will be mapped to **CB1_CBWearMonitoring/PIx_SCBR1STSumIxA** and selected for being transferred to SICAM GridEdge,
- the data point with the name **EXT/pdGGIO2001STISCSO3** of the devices with IED name **IED_000001** to **IED_000009** will be mapped to **CB1_CBWearMonitoring/PIx_SCBR1STSumIxC** and selected for being transferred to SICAM GridEdge.

NOTE

Data points may only be mapped on the IEC 61850 **Data Object** level. Therefore, always use a mapping in the following format:

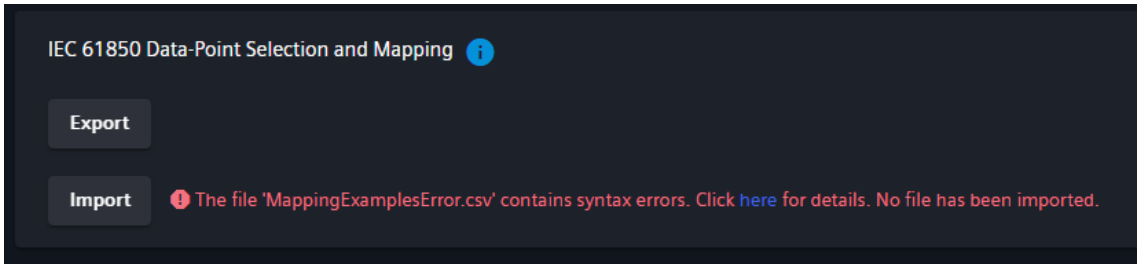
{Logical Device Instance}/{Logical Node Name Prefix}{Logical Node Class}{Logical Node Name Suffix}$ {Functional Class Name}${**Data Object** Name}

NOTE

By using regular expressions, which is allowed for the column **IedName**, it is also possible to select a specific subset of IedDevices, e.g. “IED_00000[1-9]” would select the devices IED_000001, IED_000002, ... IED_000009 for mapping.

NOTE

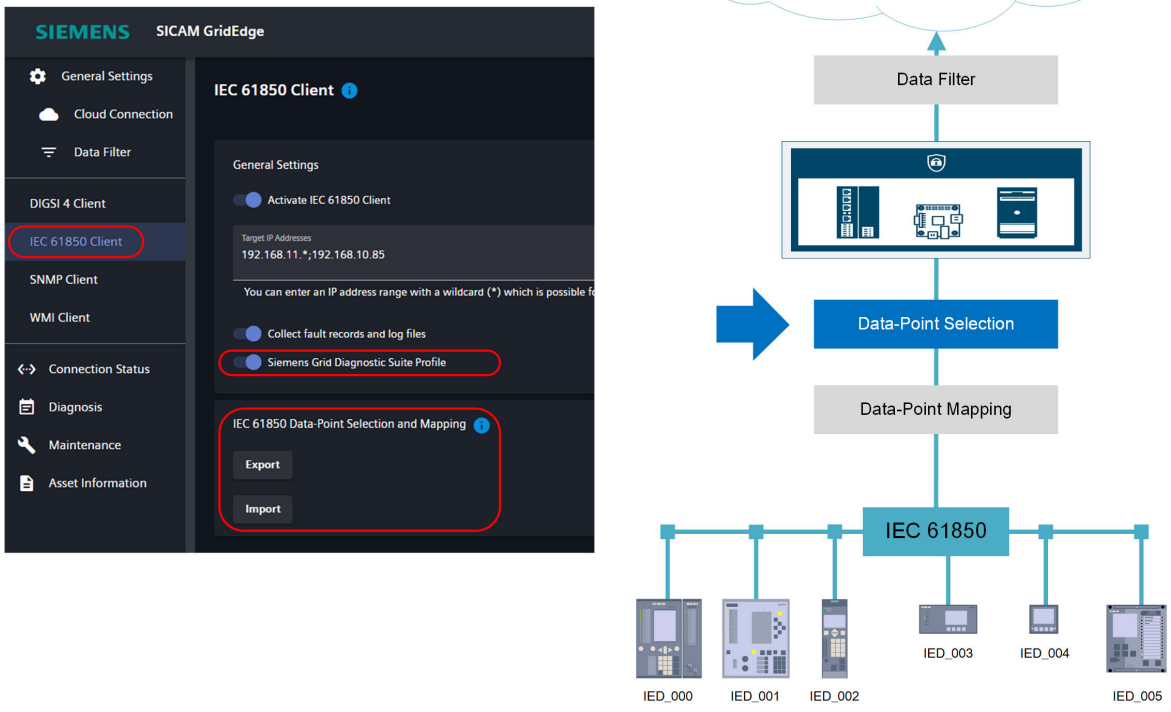
SICAM GridEdge will assist you in finding possible syntax errors in the imported CSV file by providing a summary of the found errors. You can download this summary by clicking the link in the text message next to the **Import** button.



In order to view the currently active IEC 61850 data mapping you can use the **Export** function which will create and save a CSV file containing the defined mapping/selection.

3.3.3 Data-Point Selection for the IEC 61850 Client

In the section **Data-Point Selection and Mapping** of **IEC 61850 Client** you can import a CSV file which allows to select data points from any IEC 61850 device for data retrieval to SICAM GridEdge.



[dw_data_point_selection, 1, en_US]

NOTE

If SIPROTEC Grid Diagnostic Suite Profile is enabled, data relevant for those cloud applications will be automatically selected, regardless of the selection you defined in the imported CSV file.

In order to define a data selection that can be used in SICAM GridEdge, it is required to create a CSV file in a predefined format. The file contains the IED names where the mapping is to be applied to (column **IedName**), the data model as defined in the device (**Source**) and the desired data model that is used for publishing the data to the cloud (**Replacement**). As for data point selection Replacement is not needed the column must be left empty.

The columns in the CSV file are separated by semicolon ";".

NOTE

In the CSV file it is possible to configure Data Mapping and Data Selection.

Example CSV File

```
IedName;Source;Replacement
IED_000.*;.*MMXU.*
IED_00000[1-9];.*MMXU.*
```

In the example above all data points from any Logical Node **MMXU** of the IEDs starting with the name **IED_000** will be selected for being transferred to SICAM GridEdge.

NOTE

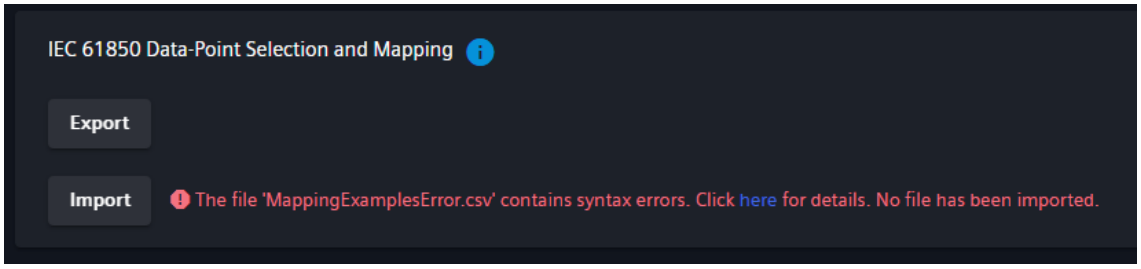
By using regular expressions, which is allowed for the column **Source**, it is also possible to select a specific subset of data points, e.g. ".*MMXU.*" would mark all Logical Nodes containing MMXU for selection.

NOTE

It is not allowed to use regular expressions for data-point selection and map the selected ones directly to another IEC 61850 adress/path.

NOTE

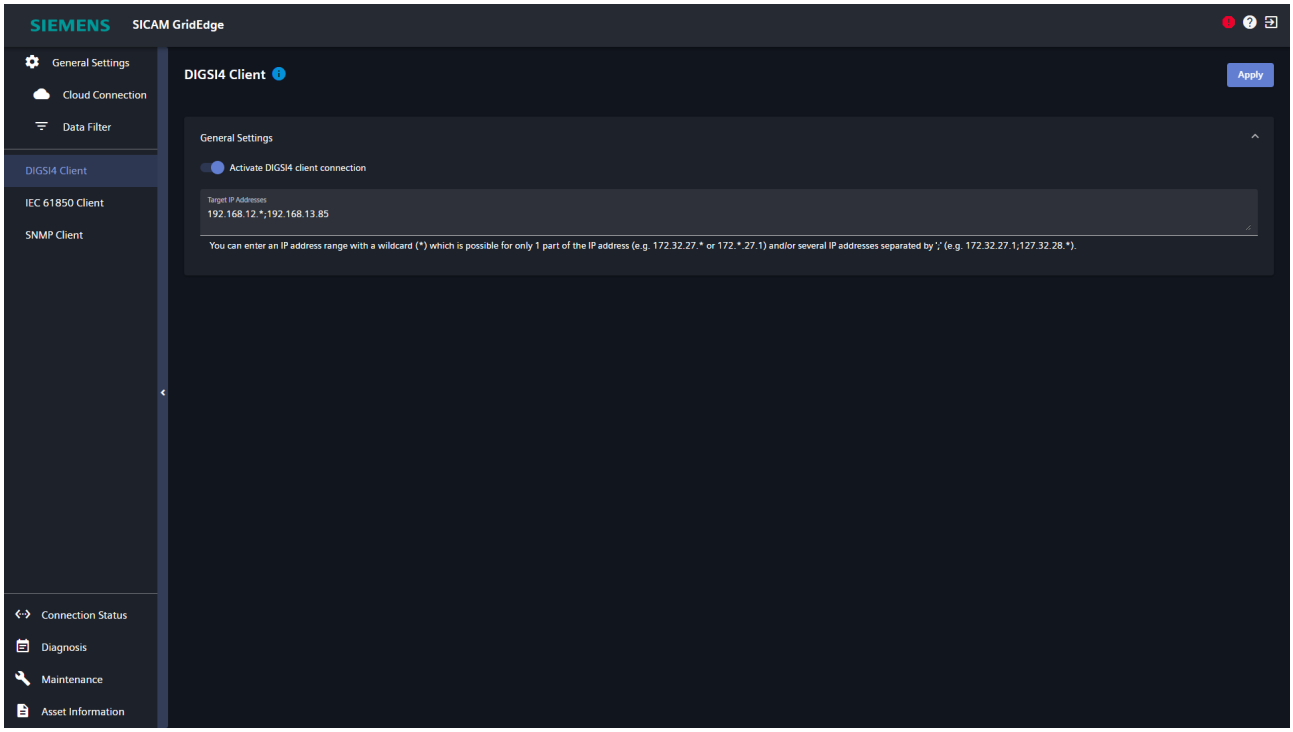
SICAM GridEdge will assist you in finding possible syntax errors in the imported CSV file by providing a summary of the found errors. You can download this summary by clicking the link in the text message next to the **Import** button.



In order to view the currently active IEC 61850 data selection and mapping you can use the **Export** function which will create and save a CSV file containing the defined mapping/selection.

3.3.4 Configuring the DIGSI 4 Client

DIGSI 4 Client is used to fetch the parameter set from SIPROTEC 4 / SIPROTEC Compact devices and to transfer them via SICAM GridEdge to the external cloud platform. Receiving and sending of the parameter set will be done on initial connection to the device and in case of parameterization changes.



[sc_digsi4, 1, de_DE]

NOTE

DIGSI 4 Client is only available in the SICAM GridEdge packages for Intel hardware.

- ✧ Activate **DIGSI 4 Client**.
- ✧ Add the IP address range of the SIPROTEC 4 / SIPROTEC Compact devices in the station network or dedicated IP addresses in **Target IP Addresses**.

  Example: `Target IP Addresses = 192.168.12.*;192.168.13.85`

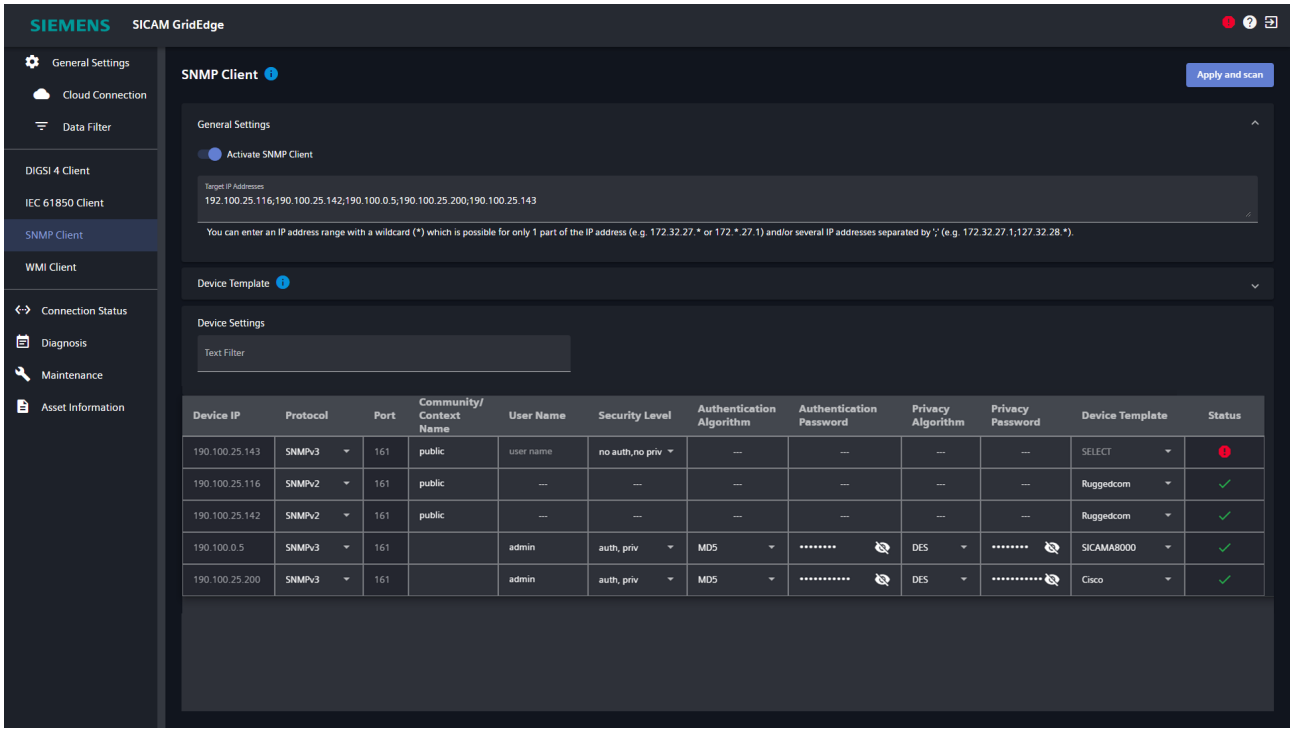
  If DIGSI4 Client is enabled, SICAM GridEdge will automatically scan for devices in the IP range **192.168.12.1** to **192.168.12.254** and will additionally communicate with the device **192.168.13.85**.
- ✧ Apply the changes.

NOTE

DIGSI 4 Client tries to receive data from the configured devices with an interrogation cycle of 30 minutes.

3.3.5 Configuring the SNMP Client

The SNMP Client is used to fetch data from devices with activated SNMP protocol and transfer them via SICAM GridEdge to the external cloud platform.



[sc_conf_snmp, 3, en_US]

Figure 3-5 SNMP Client

- ✧ Activate **SNMP Client**.
- ✧ Add the IP address range of the devices in the station network or dedicated IP addresses in **Target IP Addresses**.

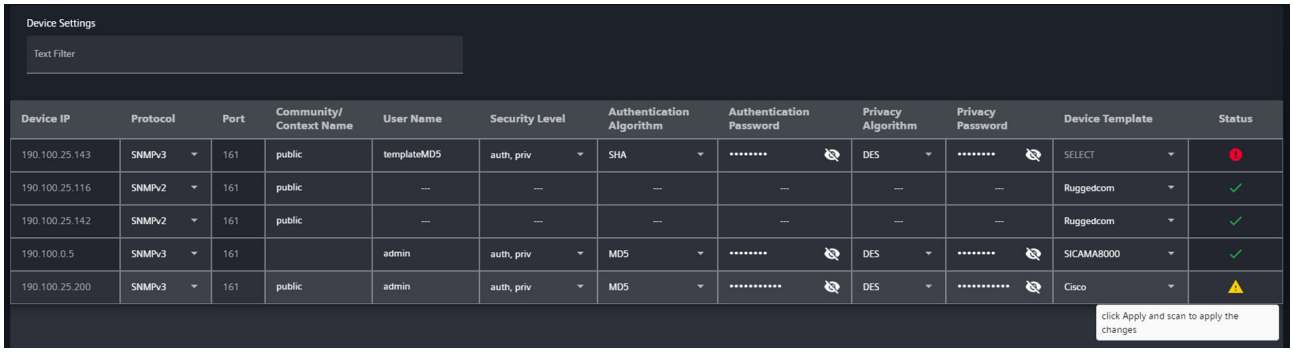
  Example: `Target IP Addresses = 192.168.11.*;192.168.10.85`

  If SNMP Client is enabled, SICAM GridEdge will automatically scan for devices in the IP range **192.168.11.1** to **192.168.11.254** and will additionally communicate with the device **192.168.10.85**.
- ✧ Click **Apply and scan**.

Once changes are applied, SICAM GridEdge will scan for the devices which are defined in the Target IP Addresses.

Device Settings

The discovered SNMP devices are visualized in table format.



[sc_conf_snmp_table, 2, en_US]

Column Name	Description	Configurable Parameter[1]
Device IP	IP address of the SNMP device	
Protocol	Configured version of the SNMP protocol (SNMPv1/v2/v2U/v3)	✓
Port	Configured for SNMP communication	✓
Community/Context Name	Configured name of the community/context	✓
User Name	Configured user name for the SNMP device	✓
Privacy Password	Configured privacy password for the SNMP device (Supported by SNMPv3 Protocol devices)	✓
Authentication Password	Configured authentication password for the SNMP device (Supported by SNMPv3 Protocol devices)	✓
Device Template	Configured device template for the SNMP device	✓
Status	The status of the device Possible values are Green, Red, and Yellow: • Green Device settings are configured successfully • Red Device is discovered, but missing/invalid device configuration settings • Yellow Modified configuration settings are not applied yet	

NOTE

Click **Apply and scan** to let the changes of the configurable parameters take effect.

NOTE

When **Target IP Addresses** is entered with wildcard characters, the scan of SNMP devices may take approx. 30 mins for discovering SNMP devices in that range and the scanning progress can be visualized from the connection status page.

1 For configurable parameters, user input is required

Device Template

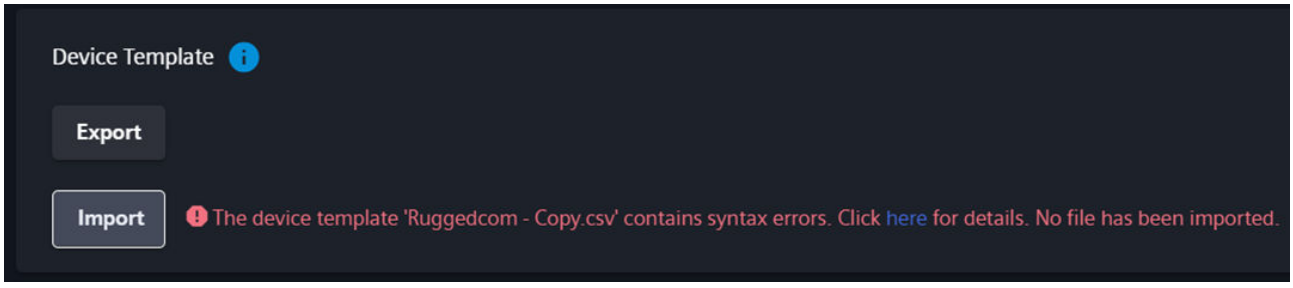
Device Template allows you to communicate to any SNMP device from the SICAM Grid Edge. The device template file contains the information about the OID (Object Identifiers) and mapping information which is required to fetch the asset information.

The template file is a CSV file. It is currently delimited with Semicolon (";") It contains 1 line per asset information in the following format: `Name;Address;Type;DefaultValue;Mapping`

Example: Default Device Template

```
Name;Address;Type;DefaultValue;Mapping
VendorName;;Single;Siemens;VendorName
SysName;1.3.6.1.2.1.1.5.0;Single;SNMPDevice;DeviceName
Location;1.3.6.1.2.1.1.6.0;Single;;LocationName
HardwareId;;Single;;AssetUuid
DeviceType;;Single;Default;HwProduct.0/ProdCompDescription
DeviceModel;;Single;;HwProduct.0/ProdCompName
SerialNumber;;Single;;HwProduct.0/ProdCompSerialNumber
OrderNumber;;Single;;HwProduct.0/ProdCompOrderNumber
HwVersion;;Single;;HwProduct.0/ProdCompVersion
FwVersion;;Single;;FwSwComponent.0/ProdCompVersion
FwName;;Single;Device firmware;FwSwComponent.0/ProdCompName
FwDescription;;Single;Device firmware;FwSwComponent.0/ProdCompDescription
SwVersion;;Single;;FwSwComponent.1/ProdCompVersion
SwName;;Single;Device Software;FwSwComponent.1/ProdCompName
SwDescription;;Single;Device Software;FwSwComponent.1/ProdCompDescription
```

Device Template provides **Export** of all templates and **Import** of a single device template.



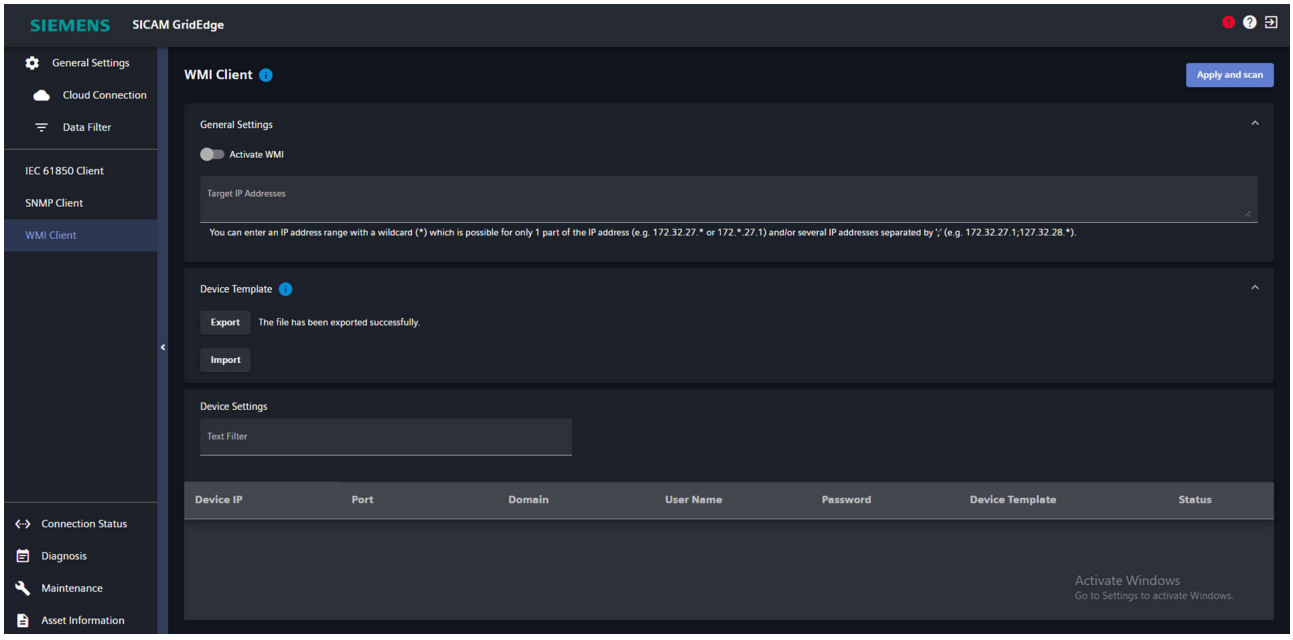
[sc_device_template_import-export, 1, en_US]

Export: All the available SNMP device templates will be downloaded as archive file (ZIP format).

Import: A newly created or modified device template can be imported to the SICAM GridEdge system. After successful import, the device template will be available for the assignment.

3.3.6 Configuring the WMI Client

The WMI Client is used to fetch data from devices with WMIC requests and to transfer them via SICAM GridEdge to the external cloud platform.



[sc_wmi_client, 1, en_US]

- ✧ Activate **WMI Client**.
- ✧ Add the IP address range of the devices in the station network or dedicated IP addresses in **Target IP Addresses**.

  Example: `Target IP Addresses = 192.168.11.*;192.168.10.85`

  If WMI Client is enabled, SICAM GridEdge will automatically scan for devices in the IP range **192.168.11.1** to **192.168.11.254** and will additionally communicate with the device **192.168.10.85**.
- ✧ Click **Apply and scan**.

Once changes are applied, SICAM GridEdge will scan for the devices which are defined in the Target IP Addresses.

Device Settings

The discovered WMI devices are visualized in table format.

Column Name	Description	Configurable Parameter[2]
Device IP	IP address of the WMI device	✗
Port	Configured for WMI communication	✓
Domain	Configured domain for the WMI device **NOTE** For local networks where domain is not available, the computer name has to be entered here.	✓
User Name	Configured user name for the WMI device	✓
Password	Configured password for the WMI device	✓

2 For configurable parameters, user input is required

Column Name	Description	Configurable Parameter[2]
Device Template	Configured device template for the WMI device	✓
Status	The status of the device Possible values are Green, Red, and Yellow: • Green Device settings are configured successfully • Red Device is discovered, but missing/invalid device configuration settings • Yellow Modified configuration settings are not applied yet	



NOTE

Click **Apply and scan** to let the changes of the configurable parameters take effect.

Device Template

Device Template allows you to communicate to any WMI device from the SICAM Grid Edge. The device template file contains the information about the OID (Object Identifiers) and mapping information which is required to fetch the asset information.

The template file is a CSV file. It is currently delimited with Semicolon (";") It contains 1 line per asset information in the following format: `Name;Address;Type;DefaultValue;Mapping`

Example: Default Device Template

```
Name;Address;Type;DefaultValue;Mapping
PCVendor;select manufacturer from win32_computersystem;Single;;VendorName
MACAddress;select caption
PCName;select name from win32_computersystem;Single;;DeviceName
DeviceType;select systemtype from win32_computersystem;Single;Windows;HwProduct/
ProdCompDescription
DeviceModel;select model from win32_computersystem;Single;;HwProduct/
ProdCompName
SerialNumber;select serialnumber from win32_bios;Single;;HwProduct/
ProdCompSerialNumber
OSVersion;select version from win32_operatingsystem;Single;;FwSwComponent.0/
ProdCompVersion
OSName;select name from win32_operatingsystem;Single;;FwSwComponent.0/
ProdCompName
OSVendor;select description from win32_operatingsystem;Single;;FwSwComponent.0/
ProdCompVendor
SwVendor;select vendor from win32_product where vendor like '%siemens
%';Multiple;;FwSwComponent.1/ProdCompVendorName
SwVersion;select version from win32_product where vendor like '%siemens
%';Multiple;;FwSwComponent.1/ProdCompVersion
SwName;select name from win32_product where vendor like '%siemens
%';Multiple;;FwSwComponent.1/ProdCompName
```

2 For configurable parameters, user input is required

3.3.7 Collecting Data from Windows Computers

SICAM GridEdge can collect data from Windows computers via the network using WMIC. WMIC must be configured properly on each Windows computer to be monitored.



NOTE

WMIC stands for Windows Management Instrumentation Command-line.
Refer to *https://docs.microsoft.com/en-us/windows/desktop/wmisdk/wmic*.

SICAM GridEdge requires the WMIC executable to get all data defined in the template attributes.
In Windows environments the **WMIC.exe** file is available at **C:\Windows\System32\wbem**. Check if this file exists on your system.

Configuring WMIC functionality

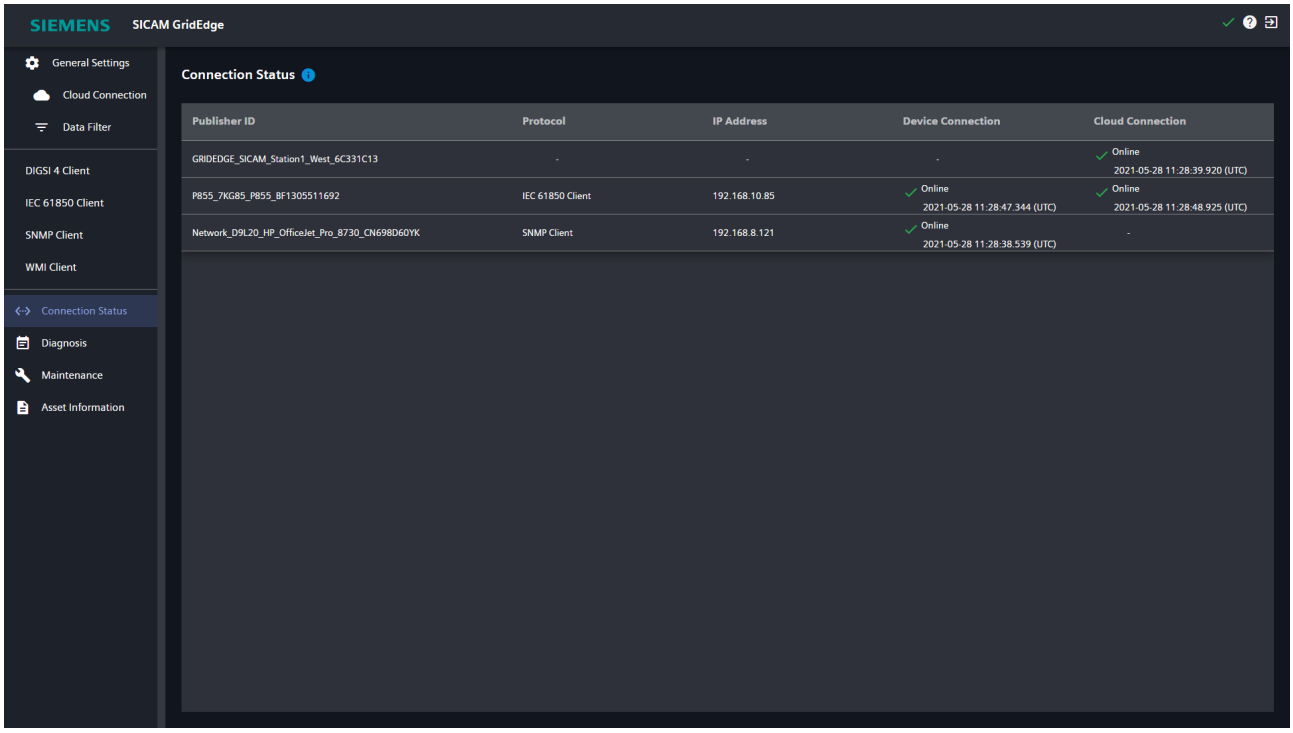
You can configure WMIC functionality using the following commands:

```
netsh advfirewall firewall set rule group="windows management instrumentation
(wmi)" new enable=yes
```

3.4 Connection Status

Using the **Connection Status** menu, you can easily check the connection status for all devices to the cloud platform and to the devices themselves.
The table contains the following columns:

- Publisher ID: This is the ID which is used to transfer data to the cloud platform
- Protocol: The protocol used to connect to the device. For SNMP, possible values are SNMPv1/v2/v2U/v3.
- IP Address: The IP address of the device
- Device Connection: Shows if the device is currently connected, and also a time stamp when the status changed the last time
- Cloud Connection: Shows if the device is currently connected to the cloud platform, and also a time stamp when the status changed the last time



[sc_SICAM_GridEdge_conection_status, 4, en_US]

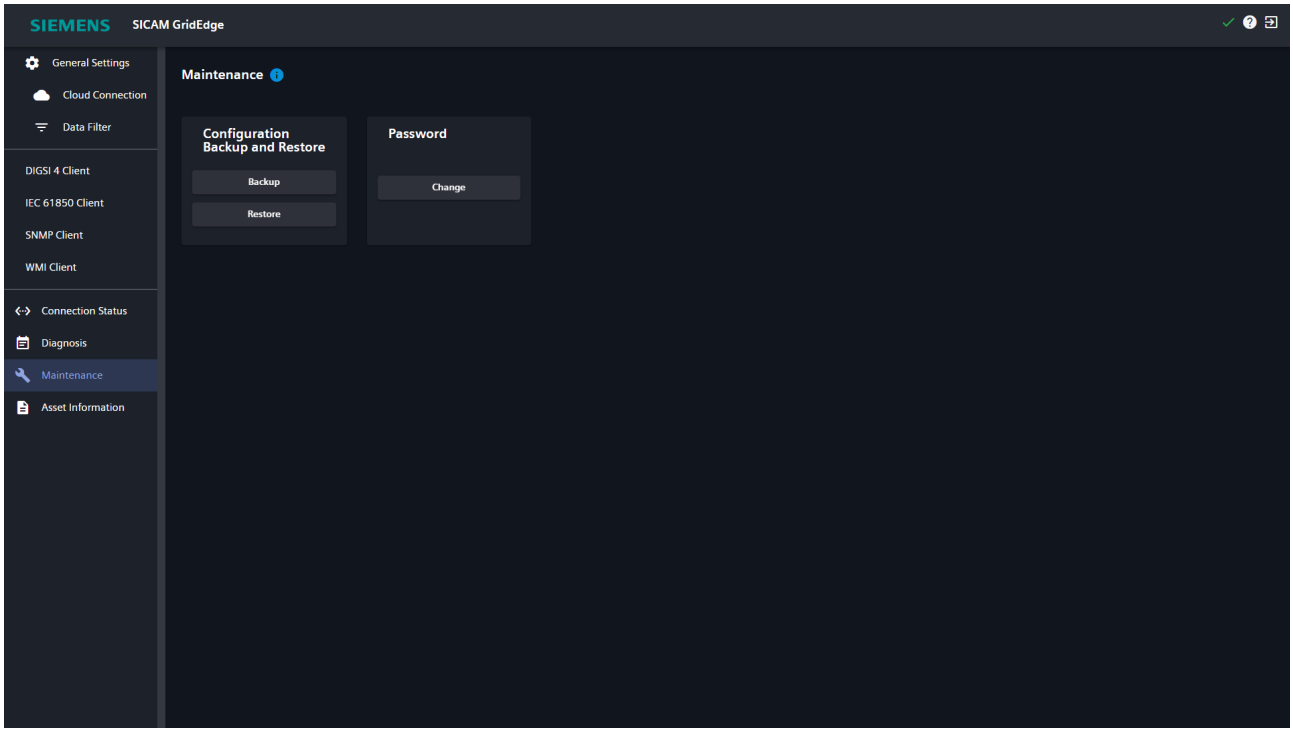
Figure 3-6 Connection Status

NOTE

Since asset information data retrieved by SNMP Client will be sent with the PublisherID of SICAM GridEdge, the cloud-connection status for invidividual SNMP devices will not be shown.

3.5 Maintenance

Using the **Maintenance** menu, you can backup and restore the configuration of SICAM GridEdge and also change the password of the Web interface.



[sc_SICAM_GridEdge_Maintenance, 5, en_US]

Figure 3-7 Maintenance

Configuration Backup & Restore

In the **Configuration Backup & Restore** tile, you can backup and restore configuration data of your SICAM GridEdge system. Since the backup of the configuration data contains sensitive data, the backup will be encrypted using the entered password with a AES128-SHA256 algorithm.

Password

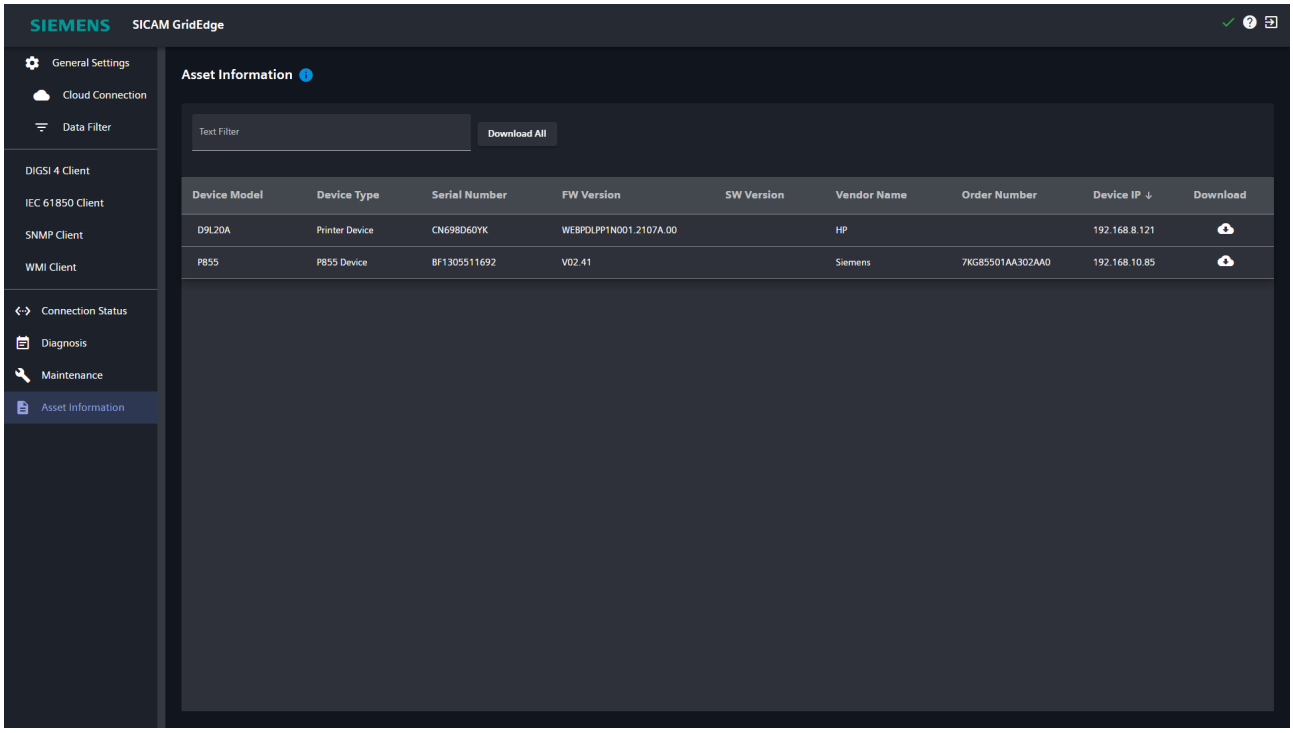
In the **Password** tile, you can change the password of the current logged in user.

3.6 Asset Information

SICAM GridEdge provides the possibility to view collected asset information from each device, if available.
You can optionally use a **Text Filter** in order to define the data to be shown in the data table.

NOTE

Only collected asset information from SNMP devices will be shown.



[sc_asset_info, 2, en_US]

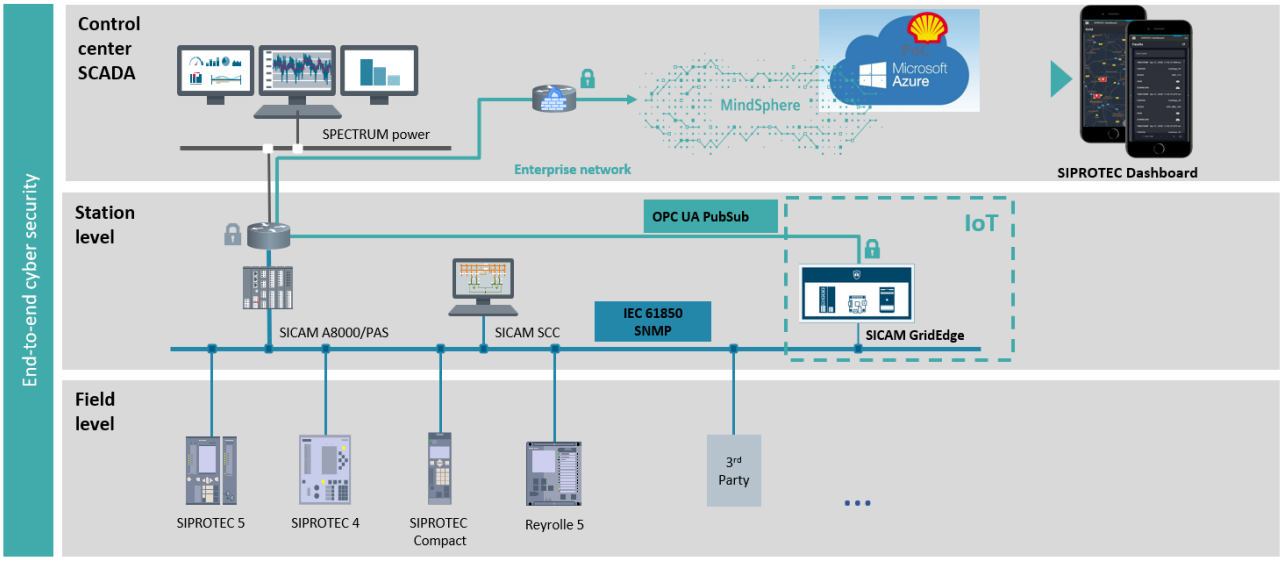
Figure 3-8 Asset Information

You can individually download the asset information collected for each device, or download all asset information for the devices matching the currently entered text filter as an archive file (ZIP).

4 Security

4.1	Security Requirements	47
4.2	User Management	47
4.3	Backup and Restore	49
4.4	Diagnosis	51
4.5	Certificate Management	52
4.6	TCP-UDP Ports	54

4.1 Security Requirements



[sc_SICAM_GridEdge_security, 4, en_US]

Figure 4-1 Security Overview

The most important security requirements are:

- Authentication and authorization of the user
- Assurance of the integrity of the transmitted data
- Collecting and saving log files
- Operation of the system in a protected environment (physical security)
- Assure system restoration without or only with marginal data loss in case of a system failure
- Activation only of required services and ports
- Confidentiality of sensitive configuration data

SIMATIC Industrial OS

For security guidelines regarding SIMATIC Industrial OS, refer to the manual of SIMATIC Industrial OS.

NOTE

Detailed information about securing a Linux system can be found in the manual from debian.org (*https://www.debian.org/doc/manuals/securing-debian-manual/index.en.html*)

4.2 User Management

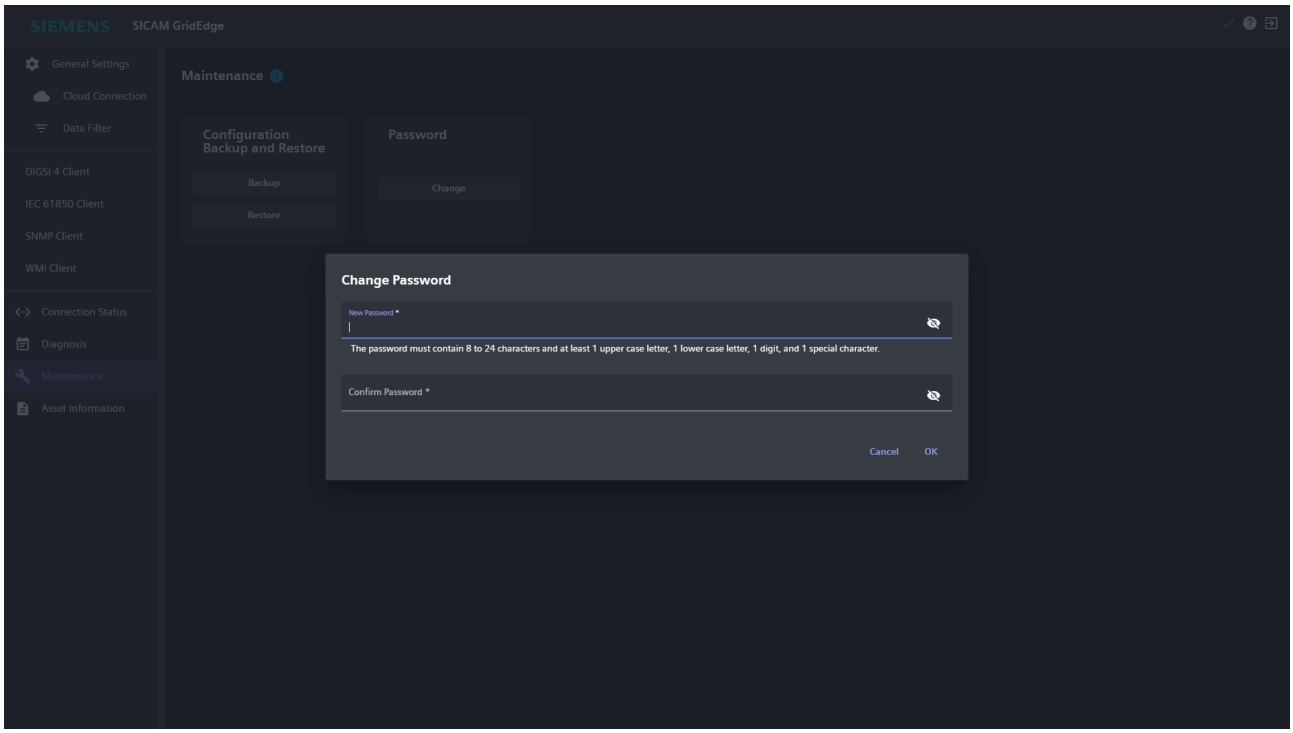
In SICAM GridEdge only 1 user account is supported. For the first login a password for the user has to be set.

NOTE

Only the salt and the password hash are stored in the database. Therefor the algorithm HMACSHA256 is used.

Changing the Password

You can change the password in the **Password** tile of the **Maintenance** page (see *Password, Page 44*).



[sc_SICAM_GridEdge_sec_passwordchange, 5, en_US]

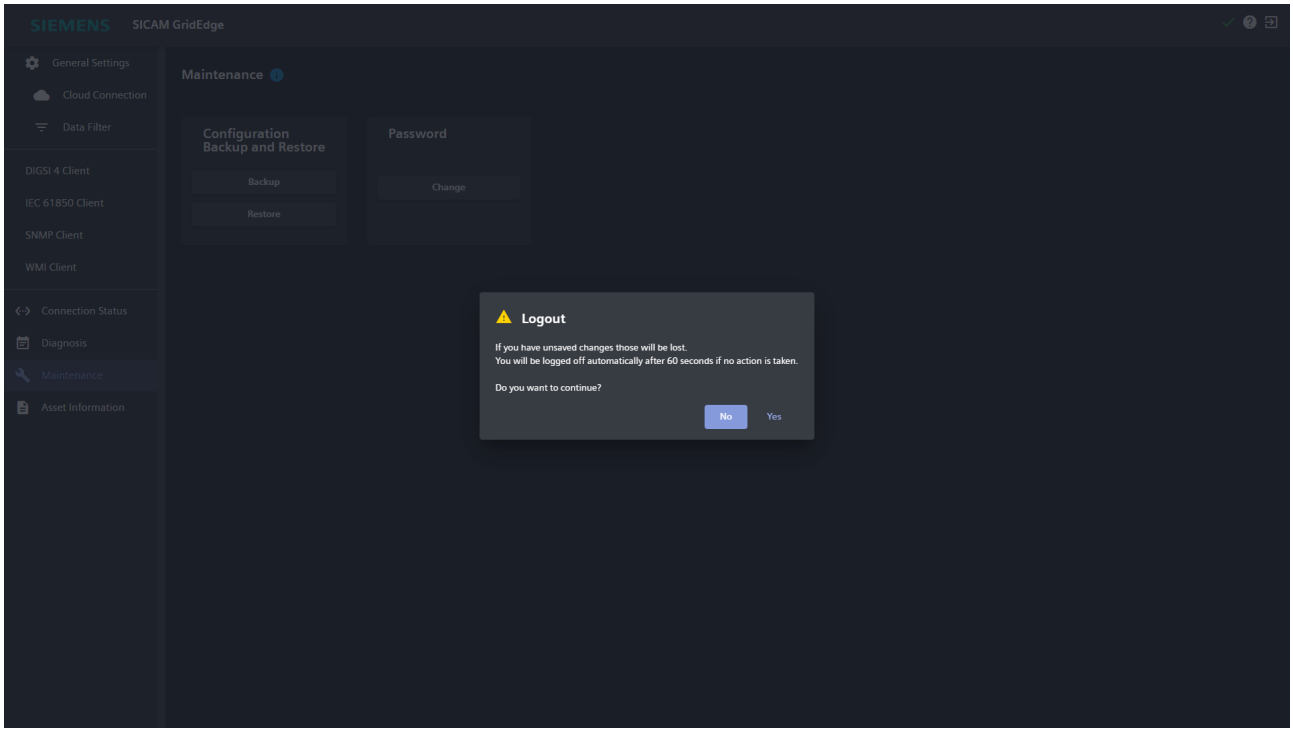
Figure 4-2 Change Password

Logging Off

For a proper logoff from SICAM GridEdge, either close all instances of your Web browser or log out using the corresponding symbol in the upper right corner:



Also, if you leave SICAM GridEdge Web interface unattended the system will automatically log off your current session after 20 minutes.



[sc_SICAM_GridEdge_logoff, 4, en_US]

Figure 4-3 Logout

4.3 Backup and Restore

SICAM GridEdge manages the components of a system and all project data associated to the system. Project data is stored – encrypted with a machine key – in a database and can be exported/imported using the *3.5 Maintenance* page of the SICAM GridEdge Web interface.

In order to save a project as a backup file and restore it later, you can archive the project created in SICAM GridEdge with the current time stamp.

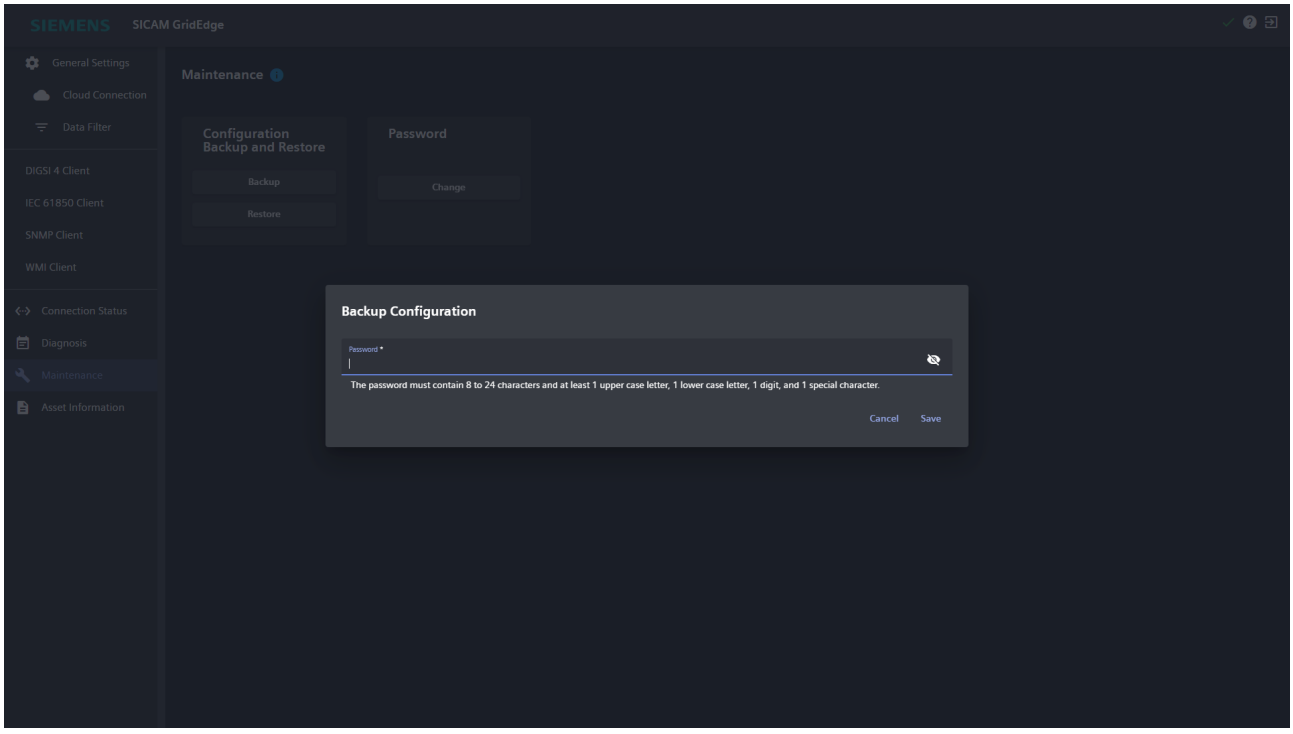
NOTE

The backup will be encrypted with the entered password and AES128-SHA256 encryption.

NOTE

Each time you update to a newer version of SICAM GridEdge, it is recommended to use the backup and restore mechanism.

Archiving a Project



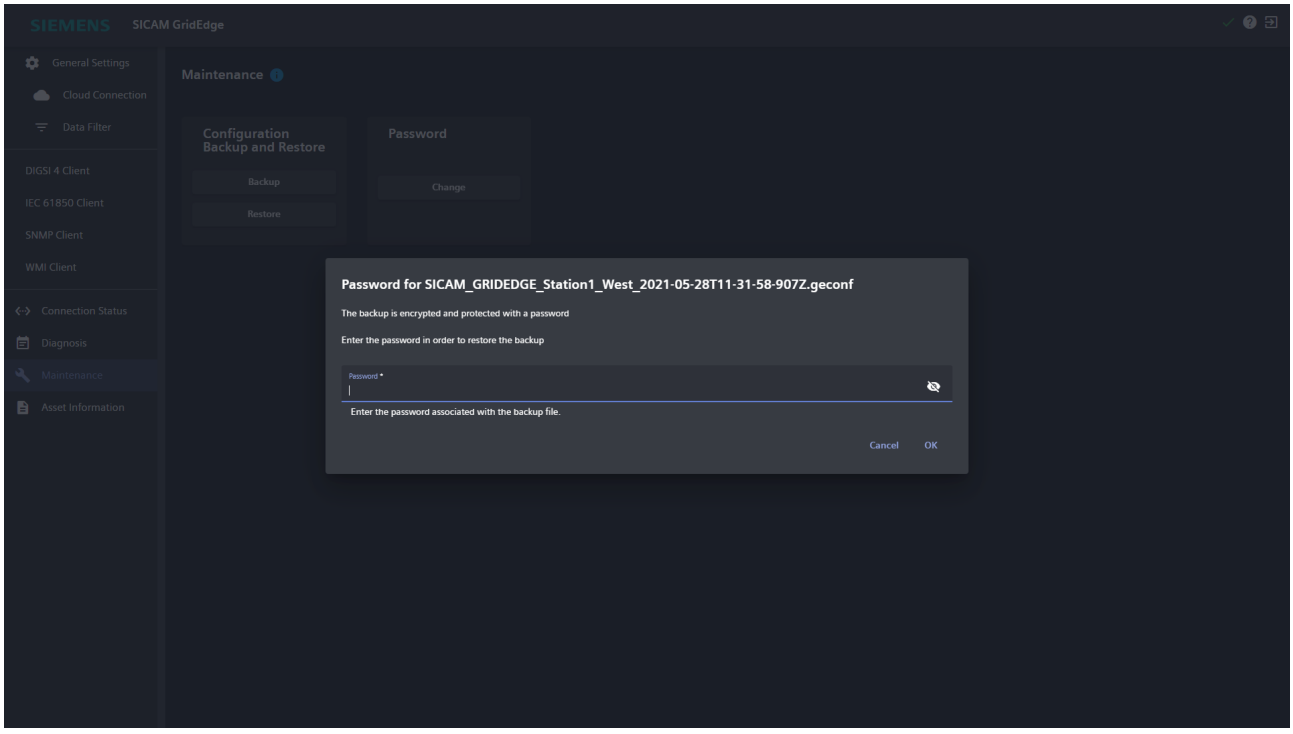
[sc_SICAM_GridEdge_sec_backup_pw, 5, en_US]

Figure 4-4 Archiving a Project with Password Protection

- ✧ On the **Maintenance** page, in the **Configuration Backup & Restore** tile, click **Backup**.
- ✧ In the **Backup Configuration** dialog, enter the **Password** to be used to protect your archived project.
- ✧ Click **Save**.

Restoring a Project

In order to restore a project you have to select your previously created backup file and enter the used password.



[sc_SICAM_GridEdge_sec_restore, 5, en_US]

Figure 4-5 Restoring a Project

- ✧ On the **Maintenance** page, in the **Configuration Backup & Restore** tile, click **Restore**.
- ✧ In the **Restore Configuration** dialog, enter the **Password**.
- ✧ Click **OK**.

NOTE

After restoring all modules, SICAM GridEdge will be restarted with the restored configuration.

4.4 Diagnosis

General

SICAM GridEdge provides a diagnosis log which chronologically acquires and categorizes system relevant events according to their origin and severity. It can be accessed via **Diagnosis**.

Furthermore, the **Diagnosis** menu allows you to download all relevant log files from the SICAM GridEdge system.

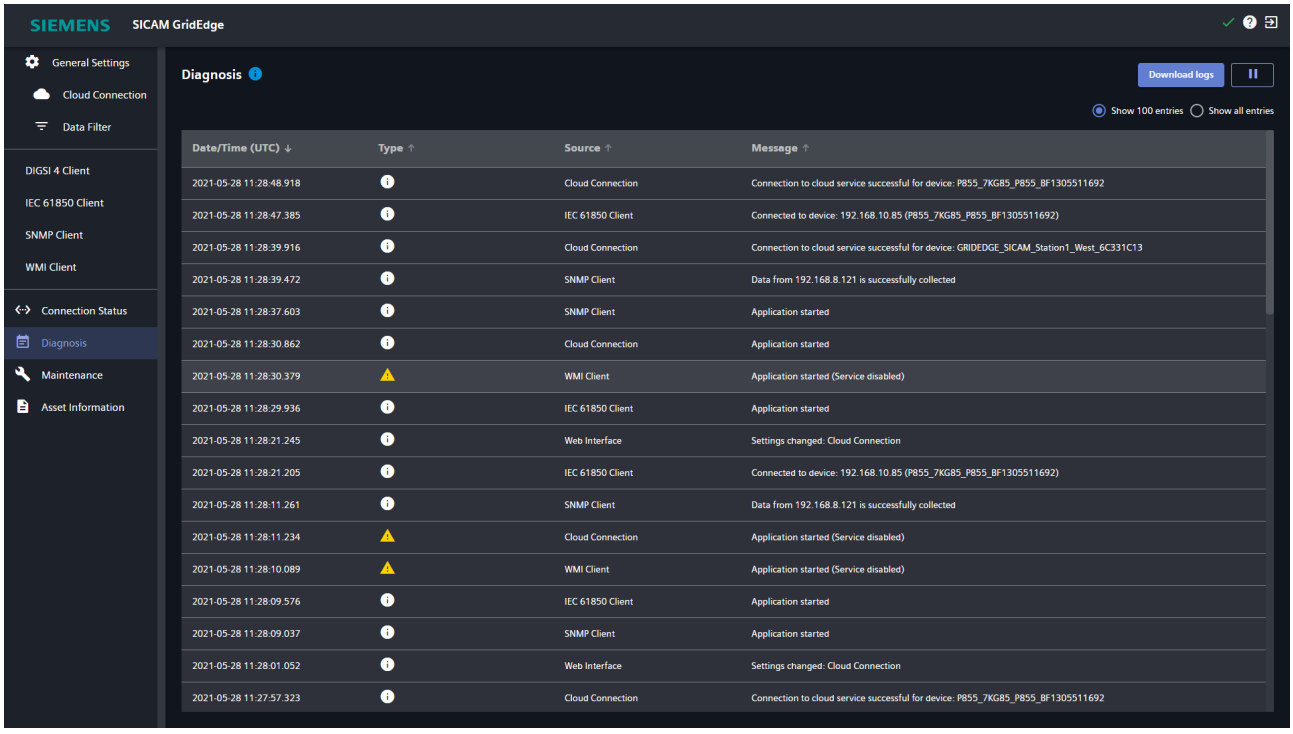
NOTE

Per default, only the last 100 log entries will be shown.

To select the amount of log entries to be show, use the radio buttons in the upper right corner.

NOTE

Per default, the diagnosis log will automatically be updated.
If you need to avoid scrolling, e.g. for a detailed investigation, the update mechanism can be paused by using the Pause symbol ⏸ in the upper right corner.



[sc_SICAM_GridEdge_sec_logging, 6, en_US]

Figure 4-6 Diagnosis Log

Structure of Events

Element	Description
Date/Time (UTC)	Date and Time when the event was received or logged Time format: yyyy-mm-dd hh:mm:ss.tt (time when the event was created) All events are written in UTC time.
Type	Levels of the event: Info > Warning > Error
Source	The name of the source that generated the log entry
Message	The message part of an event Depending on the event, the message text can contain additional information of the affected component (for example Publisher ID, Device IP Address).

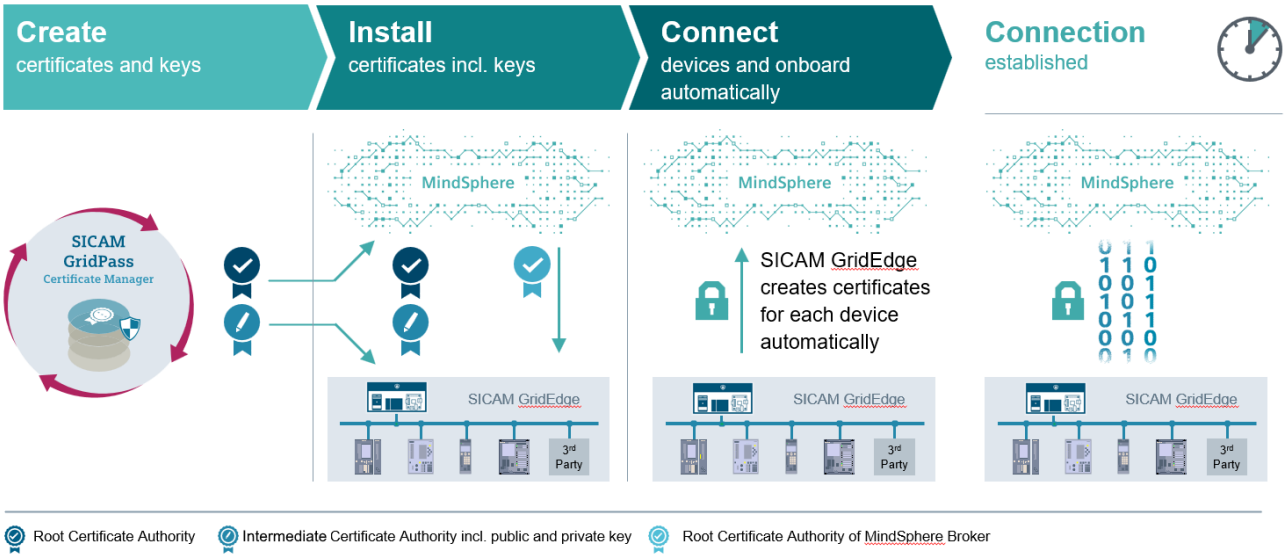
Download Log Information

For documentation purposes, you can easily download all available log information by clicking **Download Logs** in the upper right area.

4.5 Certificate Management

SICAM GridEdge automatically creates a client certificate for each connected device with the configured intermediate certificate authority.

The following figure describes the process.



[sc_SICAM_GridEdge_sec_certman, 3, en_US]

Figure 4-7 Certificate Management Process

With SICAM GridPass you can easily generate a intermediate certificate authority which includes all needed information for SICAM GridEdge.

To enable a TLS secured connection to a cloud platform, SICAM GridEdge needs an intermediate certificate authority (including public and private key; this certificate needs SHA-256 with RSA-4096 encryption) uploaded to the Web interface as well as the root certificate authority of the cloud platform (refer to *3.2.1 Configuring the Cloud Connection*).

In order to enable the mandatory end-to-end encryption (TLS) between the SICAM GridEdge and the MQTT Broker of MindSphere, it is required to upload the (intermediate) certificate authority to SICAM GridEdge Web Interface (including public and private key; this certificate needs SHA-256 with RSA-4096 encryption) as well as the root certificate authority of the cloud platform.

NOTE

The details how to create/get the required certificates are described in the *MindSphere IoT Engineering Guide*.

Whenever SICAM GridEdge finds a new device in the station network (refer to *3.2 General Settings*) a certificate is created for the device which is used for the cloud connection and stored in the SICAM GridEdge database.

NOTE

The device certificates are created using SHA-256 with RSA-4096 encryption.

NOTE

If you need to update the intermediate certificate authority (e.g. because it is expired or revoked), you only need to upload the updated intermediate certificate authority to the SICAM GridEdge system. SICAM GridEdge will automatically update also the created device certificates based on the new intermediate certificate authority.

4.6 TCP-UDP Ports

Table 4-1 Overview of the SICAM GridEdge security features

Topic	Description
HTTPS	For access to the Web interface of SICAM GridEdge as well as for the transfer of files to MindSphere, the secure HTTPS communication protocol is used. Unencrypted HTTP access is not supported. SICAM GridEdge supports the following HTTPS features: • The open source software OpenSSL is used for the TLS implementation. • SICAM GridEdge generates a self-signed TLS-certificate and is therefore not signed and confirmed by a certification authority. When using the SICAM GridEdge Web Interface, all browsers will show a message regarding an unknown certificate warning about an untrusted connection. Due to the authentication scheme used by browsers, Siemens cannot provide certificates (for example, during assembly) to be used for HTTPS with browsers. This is because either the DNS name or the IP address of the device has to be part of the signed certificate, both of which are ultimately determined after installation at the site of the customer. That is why the products generate a self-signed certificate after the IP address has been set. This self-signed certificate has to be trusted in a secure way on all clients used to access this device. You can find the recommended way of trusting self-signed certificates in the document Certificate trusting in Web browsers. You can find this document at *http://www.siemens.com/gridsecurity*, Downloads > Downloads Cyber Security General > Application Notes. The certificate is generated once during first startup of SICAM GridEdge and uses all available IP addresses as well as the hostname. • The transfer of files received from clients/devices to Mindsphere is encrypted. Therefor the corresponding certificate is used.
MQTT	• SICAM GridEdge establishes a TLS secured connection to the external cloud platform. To do so, SICAM GridEdge automatically creates certificates for the connected clients based on the configured certificate authority (refer to *4.5 Certificate Management*)



NOTE

Deploy in a secured environment only: Siemens recommends protecting network access to its energy automation products with appropriate mechanisms (for example, firewalls, segmentation, VPN). It is advised to configure the environment according to the operational guidelines in order to run the devices in a protected IT environment.

You can find the recommended security guidelines to Secure Substations at *http://www.siemens.com/gridsecurity*, Cyber Security General Downloads > Manuals.

The following table lists the programs and services that communicate between members of the network. If 2 members are in different subnetworks, the ports and protocols must be opened in the firewalls between the subnetworks.

Table 4-2 Used TCP-UDP ports

Communication Protocol	Network	Server/ Client	TCP/UDP	Port	Description
HTTPS	LAN	Server	TCP	8900	TLS Connection to a Web browser for configuration of SICAM GridEdge
HTTPS	WAN	Client	TCP	443	TLS Connection to Mindsphere for uploading files
IEC 61850	LAN	Client	TCP	102	Communication with a device using IEC 61850 in station network

Communication Protocol	Network	Server/ Client	TCP/UDP	Port	Description
SNMP	LAN	Client	UDP	161, 162	Communication with a device using SNMP in station network
OPC UA PubSub (MQTT)	WAN	Client	TCP	8883	Publishing of OPC UA encoded data to a MQTT broker for Internet of Things (IoT)
DNS	WAN	Client	UDP	53	Used by MQTT for domain name resolution
NTP	WAN/LAN (depending on configuration)	Client	UDP	123	**Time Synchronization** for the IPC with NTP



NOTE

If you have configured a proxy for filtering by URL, keep in mind that the URLs for **Uploading Files** and for **MQTT Connection** differ.

Defaults for MindSphere:

- **MQTT**: mqtt.eu1.mindsphere.io
- **File Transfer**: https://gateway.eu1.mindsphere.io/