SIEMENS

SICAM GridEdge
Engineering Guide

V2.12

Manual

E50417-H7640-C641-B6

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-B6.02

Edition: 09.2023

Version of the product described: V2.12

Copyright

Trademarks

SIPROTEC, DIGSI, SIGRA, SIGUARD, SIMEAS, SAFIR, SICAM, and Insights Hub 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.

System engineers, commissioning engineers, persons entrusted with the configuration of the app.

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 – Protection Automation
Customer Support Center

Tel.: +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

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 the SICAM GridEdge solution with the standardized OPC UA PubSub (MQTT) protocol or the MQTT protocol with JSON encoding (to IEC 62541 requirements) – no firmware changes for devices in your station are required.

Using the IoT standard protocols and applying the highest security standards makes IoT connection of existing legacy installations a lucrative prospect.

Upgrading existing installations is simple:

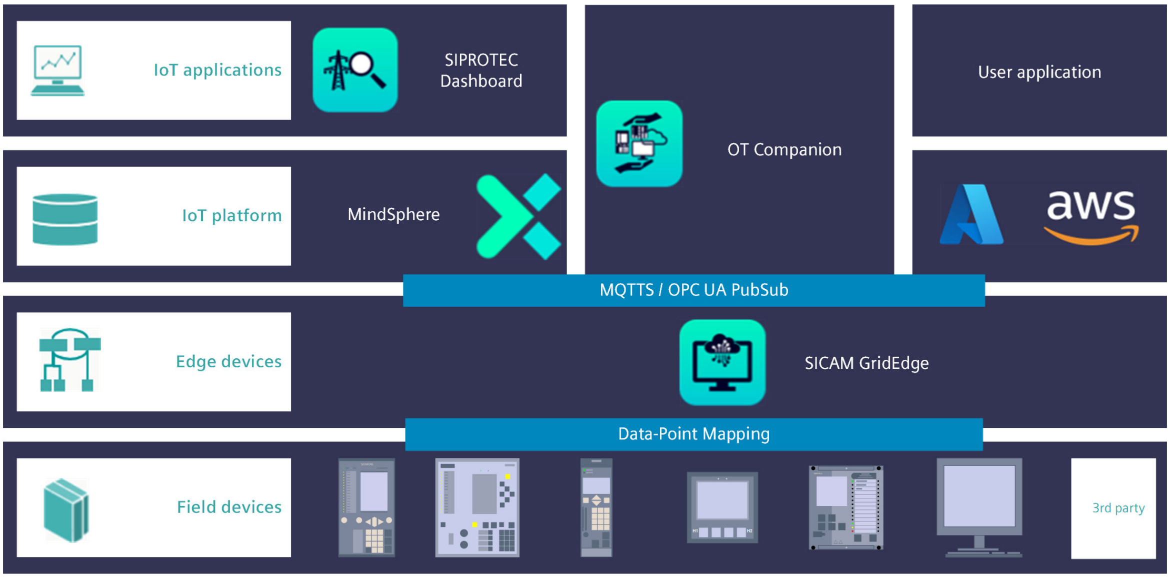
- Continue using existing infrastructure and hardware
- Install SICAM GridEdge on your station
- Configure SICAM GridEdge

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.

System Overview



[ge_application_area, 1, en_US]

2 System Configuration

NOTE

Examples of installations or folders do not contain the specific information about the version. The version-specific information is displayed using the letter x:

`SICAM_GridEdge_2.6.3_x86_64.zip` is displayed like `SICAM_GridEdge_x.x.x_x86_64.zip`

2.1 Hardware/Virtual Machine Requirements

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

- **SIMATIC IPC 227E** (MLFB: 6ES7647-8BD31-0CA1)
  - x86-64 CPU architecture
  - 240 GB SSD
  - 8 GB RAM
  - 2 LAN ports
  - Additionally, the following components are necessary:
    - SIMATIC Industrial OS V3.2.2 (MLFB: 6ES758, contact your Siemens partner)
    - Siemens LOGO!POWER 24 V / 2.5 A (MLFB: 6EP3332-6SB00-0AY0)
- **SIMATIC IPC 127E** (MLFB: 6AG4021-0AB11-0BA0)
  - x86-64 CPU architecture
  - 64 GB SSD
  - 4 GB RAM
  - 2 LAN ports
  - Additionally, the following components are necessary:
    - SIMATIC Industrial OS V3.2.2 (MLFB: 6ES758, contact your Siemens partner)
    - Siemens LOGO!POWER 24 V / 2.5 A (MLFB: 6EP3332-6SB00-0AY0)
- **RUGGEDCOM APE1808LNX** (MLFB: 6GK6015-0AL20-0GH0)
  - x86-64 CPU architecture
  - 64 GB eMMC
  - 8 GB RAM
  - 2 LAN ports
  - Additionally, the following component is necessary:
    - RUGGEDCOM RX1500 series as base unit
- **Virtual Machine (HyperV or VMware)**
  - CPU (4 cores, 4 threads) with x86-64 architecture with minimum 1.6 GHz
  - 4 GB RAM
  - 64 GB HDD
  - 2 LAN ports
  - Additionally, the following operating system is necessary:
    - Debian OS 11 – Bullseye

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, refer to *5.4 Making a Backup and Restore*.

2.2 Preparing the Hardware

SIEMENS IPC 127E/227E

- ✧ Install and wire the SIMATIC IPC 127E/227E.

  Refer to the SIMATIC IPC 127E Quick Install Guide (*https://support.industry.siemens.com/cs/document/109764313/simatic-ipc127e-quick-install-guide?dti=0&lc=en-WW*) or the SIMATIC IPC 227E Quick Install Guide (*https://support.industry.siemens.com/cs/ww/de/view/109477819*).

- ✧ Connect the monitor and keyboard.

- ✧ Connect the SIMATIC IPC to the LAN in the station and the WAN (required for connection to external cloud platform and for fetching updates of operating system).

- ✧ Prepare a USB Service Stick for the installation of the operating system.

  Refer to the Industrial OS – Getting Started Guideline (*https://support.industry.siemens.com/cs/ae/en/view/109795683*) and the SIMATIC Industrial OS Installation Manual (*https://support.industry.siemens.com/cs/document/109780979/simatic-industrial-os?dti=0&lc=en-WW*).

You can now continue with the installation and configuration of the SIMATIC Industrial OS (refer to *2.4.1.1 Installing SIMATIC Industrial OS*).

SIEMENS APE1808LNX

The APE1808LNX has 2 Ethernet ports – one internal port and one on the front panel. For a proper network separation, one port must be connected to the station network and one port must be connected to the WAN. The port for the substation LAN is the internal port with the name **eth0**. The port for the WAN is the port on the front panel with the name **eth1**.

- ✧ Install and wire the RUGGEDCOM and the APE1808LNX.

  Refer to the RUGGEDCOM RX1500 Installation Manual (*https://support.industry.siemens.com/cs/document/82166529/ruggedcom-rx1500-installation-manual?dti=0&lc=en-WW*).

- ✧ Connect the monitor and keyboard.

- ✧ Ensure that Ethernet ports of the APE1808LNX module are not yet connected to the station network and the WAN.

  For more information on the description of LAN adapters, refer to the RUGGEDCOM APE1808 Configuration Manual (*https://support.industry.siemens.com/cs/document/109769739/ruggedcom-ape1808-configuration-manual-for-ape1808lnx-ape1808w10?dti=0&lc=en-CN*).

You can now continue with the configuration of the Debian operating system (refer to *2.4.2.2 Configuring Debian OS*). You can skip the installation.

2.3 Setting up a Virtual Machine

This description is focused on information relevant to prepare the virtual machine for the SICAM GridEdge installation. For more information on how to set up a virtual machine, refer to the official Hyper-V-Manager or VMware documentation.

Microsoft Windows Host

- ✧ Enable virtualization on the Microsoft Windows host machine.
- ✧ Open the program Hyper-V-Manager.
- ✧ Create one virtual switch for the WAN and one virtual switch for the Station Network.
- ✧ Create a virtual machine as a **Generation 2** for modern OS.
- ✧ In the section **Security**, select the template **Microsoft UEFI Certificate Authority** so that the Linux ISO is accepted for booting.

  - or -

- ✧ If this is not successful, disable **Enable Secure Boot**.
- ✧ Right-click the created virtual machine, select **Connect** and start it.

You can now continue with the installation and configuration of the Debian operating system (refer to *2.4.2.1 Installing Debian OS*).

VMware

You need a running VMware machine.

- ✧ Set up a new virtual machine without any predefined operating system.
- ✧ Ensure that you have a hard disk drive, CD/DVD and LAN configured.
- ✧ Download the first ISO file for your desired version of the Linux Debian operating system.
- ✧ Define the ISO file in the virtual CD/DVD drive.
- ✧ Start the virtual machine and boot from your ISO file.

You can now continue with the installation and configuration of the Debian operating system (refer to *2.4.2.1 Installing Debian OS*).

2.4 Operating System Installation and Configuration

2.4.1 SIMATIC Industrial OS

2.4.1.1 Installing SIMATIC Industrial OS

- ✧ Connect the USB Service Stick to the switched off SIMATIC IPC.
- ✧ Switch on the IPC and open the BIOS settings.
- ✧ 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.

Only for SIMATIC IPC227E:

- ✧ Open the firmware selection menu.
- ✧ Select the **Setup Utility** option on the **Main Page**.
- ✧ Select **Boot Configuration** under **Advanced**.
- ✧ Assign the **Enabled** value to the firmware setting **xHCI Mode**.

For all SIMATIC IPC:

- ✧ 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

Ensure that the USB Service Stick is not plugged in. After the installation is finished, the SIMATIC IPC will reboot.

2.4.1.2 Configuring SIMATIC Industrial OS

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

✧ Configure the localization settings (keyboard language, layout, region, etc.).

NOTE

A network cable for WAN must be connected to the **X1P1** port.

✧ Do not allow to terminate the xserver with the keyboard. A xserver installation is not needed to run SICAM GridEdge.

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

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. For more information refer to the **Industrial OS – Getting Started** guideline (*https://support.industry.siemens.com/cs/ae/en/view/109795683*).

✧ For a network seperation between the WAN and the Station Network, configure the network settings accordingly for the network adapter **enp3s0** (port X2P1). For the gateway, use 0.0.0.0 and leave the DNS server empty – except there is an internal DNS server in your internal network.

NOTE

Siemens recommends using a static IP address.

✧ If required, define the proxy settings.

✧ If required later on in the operation environment, enable the firewall.

✧ Define the host name of the SIMATIC IPC.

✧ Set up the time synchronization for the SIMATIC IPC with the 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 a first/primary NTP server 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 (for example, from *https://www.ntppool.org/*).

NOTE

Since a time synchronization is necessary for a proper connection between SICAM GridEdge and the cloud platform, the NTP must be configured properly. SICAM GridEdge as well as all connected devices must be synchronized with the NTP server. Once SICAM GridEdge is synchronized with the NTP server, you can use SICAM GridEdge for the synchronization of the connected devices.

✧ If **Active Directory** is intended in your company network, activate it.

✧ Configure at least one APT mirror (Advanced Package Tool).
Select an address from the list nearby the final location of the SIMATIC IPC.
Enable **Main** and **Contrib** but keep **Non-free** disabled to define which packages can be loaded from the mirror.

✧ Consider disabling the root login for security reasons (for information about securing a Linux system, refer to *https://www.debian.org/doc/manuals/securing-debian-manual/index.en.html*).

✧ Define the user's full name as **Edge** so the user's user ID (used for logging on) is **edge**.

✧ Set a password.

✧ Enable **sudo** for this user.

✧ Define the frequency of the software updates, for example, daily or weekly.
The SIMATIC IPC installs the selected packages, loads and installs packages from the internet via the WAN connection.

NOTE

To keep your installation up to date and install also security relevant fixes, it is needed to set up a linux update server. For more information, refer to **SIMATIC Industrial OS – Setting up a Linux update server for SIMATIC IPCS** (*https://support.industry.siemens.com/cs/gr/en/view/109769641*).

✧ Select **OK**.

✧ Keep the autostart function enabled for the service stick.

The SIMATIC IPC reboots.

NOTE

If you need to configure or reconfigure some settings of the SIMATIC Industrial OS, refer to the **Industrial OS – Getting Started** guideline (*https://support.industry.siemens.com/cs/ae/en/view/109795683*).

2.4.2 Debian OS

2.4.2.1 Installing Debian OS

For more information about the Debian installation, refer to the Debian documentation (refer to *https://www.debian.org/releases/bullseye/amd64/index.en.html*).

✧ Select the graphical installation and follow the instructions on your screen.

✧ Select your language (for example, en-US, American.Keymap).

✧ Select the Ethernet connection to the Internet as default.

✧ If automatic DHCP settings are not available to you, configure your network manually. Ensure that the IP addresses match your surrounding.

✧ Enter the host name but keep the domain name empty.

✧ Define the root password, the standard user (edge) and the password for **edge**.

✧ Select your timezone.

✧ Use the entire disk, all in one partition.

NOTE

The graphical installation offers a complex storage configuration. However, you only need to configure a simple hard disk drive.

✧ If iSCSI is available to you, select iSCSI.

- or -

✧ If iSCSI is not available to you, keep the iSCSI target empty.

✧ Go back, select **Finish** and **Continue**.

✧ Select your preconfigured hard disk drive (at least 80 GB) as the destination storage device.

✧ Select the guided partitioning.

✧ Use the entire disk and select the virtual disk.

✧ Select all files in one partition and write the changes to the hard disk.

The hard disk drive is configured.

✧ If no installation media is available to you, select **No** and continue.

✧ As soon as an Internet connection is available to you, choose a network mirror for the latest packages. Siemens recommends choosing a package manager from the location of the devices you want to connect to SICAM GridEdge.

✧ If necessary, configure the connection to your proxy server.

✧ Ensure that there is no ISO file in your virtual CD/DVD drive and reboot.

2.4.2.2 Configuring Debian OS

For the configuration of the operating system, you must have knowledge of the text editor **vi**.

✧ Log on as the root user to the system.

Configuring the Ports for Substation LAN, WAN and DNS Server

The names **eth0** for the substation LAN and **eth1** for WAN are used as examples.

✧ Open the file **/etc/network/interfaces**:

```
vi /etc/network/interfaces
```

✧ Enter a static IP address for the eth0 interface:

```
auto eth0
iface eth0 inet static
address 172.17.26.201
netmask 255.255.255.0
```

✧ Save your changes.

✧ Open the file **/etc/network/interfaces**:

```
vi /etc/network/interfaces
```

✧ Enter a static IP address for the eth1 interface:

```
auto eth1
iface eth1 inet static
address 192.168.78.2
netmask 255.255.255.0
gateway 192.168.78.1
```

✧ Save your changes.

✧ Open the file **/etc/resolv.conf**:

```
vi /etc/resolv.conf
```

✧ Add a nameserver suitable for your environment:

```
nameserver 8.8.8.8
```

✧ Save your changes.

✧ Reboot the system:

```
reboot
```

Validating the Network Settings

✧ Check the connections of the ports:

```
ifconfig
```

✧ Ensure that the 2 connections, eth0 and eth1, are displayed with the defined IP addresses.

✧ Plug in the LAN cables to the ports:
– Substation LAN to switch
– WAN to front panel of APE

✧ Check the transmission to the WAN:

```
ping -c 4 www.ntp.org
```

✧ Ensure that the answer consists of 4 lines containing the time information in ms.

Updating the Operating System

✧

```
apt update
apt upgrade
```

Configuring the Keyboard Layout

This section is only necessary in case you want to change the keyboard layout to QWERTZ.

✧ Open the file **/etc/profile**:

```
vi /etc/profile
```

✧ Add these lines between **export PATH** and **if [...]**:

```
if [ -z “${LANG}” ]; then
LANG=”en_US.utf8”
fi
export LANG
```

✧ Log off the system.

✧ Log on as the root user.

✧ Install the package locales:

```
apt update
apt install locales
```

NOTE

If the installation does not start automatically, enter `dpkg-reconfigure locales` and select `en_US.UTF-8 UTF-8 -> 3 en_US.UTF-8`.

✧ Install the console setup:

```
apt install console-setup
```

✧ Select `UTF-8, Latin-1 - western Europe, VGA, 8x16`.

NOTE

If the installation does not start automatically, enter `dpkg-reconfigure console-setup`.

Configuring the SSH Server

✧ Install the ssh-server package:

```
apt update
apt install openssh-server
```

✧ Open the file **/etc/ssh/sshd_config**:

```
vi /etc/ssh/sshd_config
```

✧ Remove the **#** symbol in front of **Port 22**.

✧ Change the **AddressFamily** to **any**.

✧ Change the **ListenAddress** to the IP address of the to the IP address of the substation network. Ensure that the address is not accessible from the internet.

✧ Change the **PermitRootLogin** to **no**.

✧ Restart the OpenSSH server:

```
service sshd restart
```

✧ Open the file **/etc/hostname**:

```
vi /etc/hostname
```

✧ Change the name in the file to your desired name for the machine (for example, rug-2-ape-2).

✧ Save your changes.

Configuring the User

✧ Install the sudo package:

```
apt update
apt install sudo
```

✧ Create the user **edge**:

```
adduser --shell /bin/bash edge
```

✧ Define a password for the user.

✧ Add the user **edge** to the sudo group:

```
usermod -a -G sudo edge
```

NOTE

Check that the SSH connection is working on user **edge**. Try to become a super-user.

Setting Up the NTP Server

For virtual machines, enable the time synchronization between the virtual machine and the host system.

NOTE

Since a time synchronization is necessary for a proper connection between SICAM GridEdge and the cloud platform, the NTP must be configured properly. SICAM GridEdge as well as all connected devices must be synchronized with the NTP server. Once SICAM GridEdge is synchronized with the NTP server, you can use SICAM GridEdge for the synchronization of the connected devices.

✧ Install the NTP package:

```
apt update
apt install ntp
```

✧ Check if the installation was successful:

```
ntpq -pn
```

✧ Ensure that a table is displayed containing the IP addresses from which the NTP server will synchronize.

✧ Ensure that at least one line starts with *****.

✧ Ensure that the entries in the column **reach** are not zero (377 is optimal).

2.5 SICAM GridEdge Installation

2.5.1 Installing SICAM GridEdge

✧ Log on as the user **edge**.

✧ Install the unzip package:

```
sudo apt-get update && sudo apt-get install unzip -y
```

✧ Copy the ZIP file of the setup bundle (ZIP file downloaded via OSD) to the SIMATIC IPC using SCP.

- or -

✧ Copy the ZIP file of the package to the SIMATIC 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, refer to *2.5.2 Mounting the USB Drive*.

✧ Extract the ZIP file and change the directory to the extracted folder:

```
unzip SICAM_GridEdge_x.x.x_x86_64.zip -d SICAM_GridEdge_x.x.x
cd SICAM_GridEdge_x.x.x
```

✧ Add execution rights to scripts:

```
chmod +x *.sh
```

✧ Before starting the installation, ensure that you have a WAN connection as docker is downloaded and installed during the setup.

✧ Start the SICAM GridEdge installation:

```
./sicamgridedge_setup.sh
```

✧ To select the interface on which the SICAM GridEdge Web interface is available, enter the IP address of the Ethernet adapter which is connected to your station network.

✧ Check if the devices in the substation use an IP address within the IP address range used internally by the SICAM GridEdge software (typically starting from 172.17.0.0/16).
If this is the case, refer to *Checking Docker Network Configuration, Page 89*.

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

NOTE

If you update the network settings of the SIMATIC 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:

```
./sicamgridedge.sh -n
```

NOTE

After the SIMATIC IPC is set up (Industrial OS, network, NTP, firewall, SICAM GridEdge), Siemens recommends making a full backup as an image file using the SIMATIC IPC Image & Partition Creater.
For more information about the usage of the tool, refer to the corresponding documentation:

- Document collection – *https://support.industry.siemens.com/cs/products?mfn=ps&pnid=16804&lc=en-WW*
- Operating manual – *https://support.industry.siemens.com/cs/document/109780775/simatic-ipc-image-partition-creator-v3-6?dti=0&lc=en-WW*
- Compact user manual – *https://support.industry.siemens.com/cs/document/109807263/simatic-ipc-image-partition-creator-v3-6-2-product-information?dti=0&lc=en-WW*

2.5.2 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_x.x.x_x86_64.zip
```

✧ Copy the SICAM GridEdge setup data into the home directory:

```
edge@NANOBOX-3:~$ cp /media/usb-drive/SICAM_GridEdge_x.x.x_x86_64.zip ~
```

✧ Unmount the USB drive:

```
edge@NANOBOX-3:~$ sudo umount /dev/sdb1
```

2.5.3 Example Installation

Below you can find an example of the installation steps.

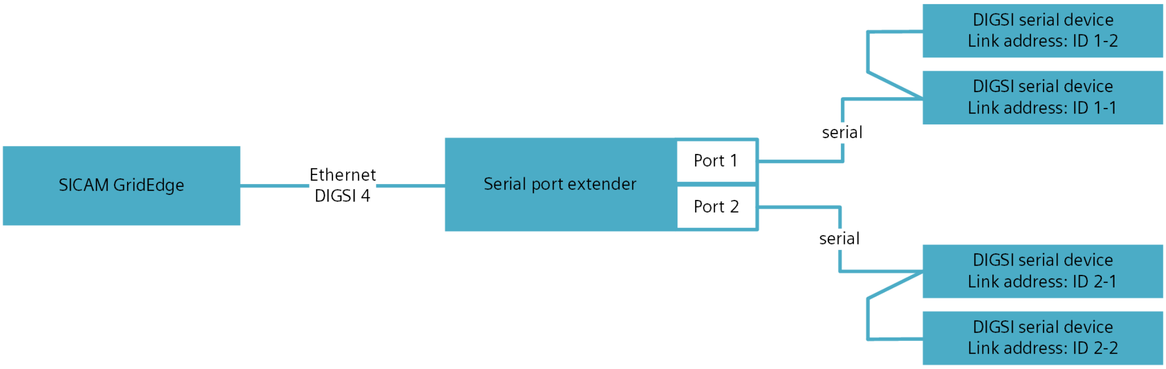
```
edge@localhost:~/SICAM_GridEdge_x.x$ id
uid=1000(edge) gid=1000(edge) groups=1000(edge),997(docker)
edge@localhost:~$ ls
SICAM_GridEdge_x.x_x86_64.zip
edge@localhost:~$ unzip SICAM_GridEdge_x.x_x86_64.zip  -d SICAM_GridEdge_x.x
Archive:  SICAM_GridEdge_x.x_x86_64.zip
  inflating: SICAM_GridEdge_x.x/.env
  inflating: SICAM_GridEdge_x.x/SICAM_GridEdge_Changelog.md
  inflating: SICAM_GridEdge_x.x/SICAM_GridEdge_Manual_en.pdf
  inflating: SICAM_GridEdge_x.x/SICAM_GridEdge_PI_en.pdf
 extracting: SICAM_GridEdge_x.x/SICAM_GridEdge_ReadmeOSS.zip
  inflating: SICAM_GridEdge_x.x/TtyDetect.py
  inflating: SICAM_GridEdge_x.x/TtyDriver_setup.sh
  inflating: SICAM_GridEdge_x.x/docker-compose-1.29.2-Linux-x86_64
  inflating: SICAM_GridEdge_x.x/docker-compose.yml
  inflating: SICAM_GridEdge_x.x/dumpstats_cron.sh
   creating: SICAM_GridEdge_x.x/examples/
   creating: SICAM_GridEdge_x.x/examples/IEC61850_Data_Mapping/
  inflating: SICAM_GridEdge_x.x/examples/IEC61850_Data_Mapping/
IEC61850_Mapping_SIP4_WearMonitoring.csv
   creating: SICAM_GridEdge_x.x/examples/Configuration_File/
  inflating: SICAM_GridEdge_x.x/examples/Configuration_File/
ConfigurationFile.csv
  inflating: SICAM_GridEdge_x.x/hwclock_cron.sh
   creating: SICAM_GridEdge_x.x/images/
  inflating: SICAM_GridEdge_x.x/images/sicam_gridedge.tar
  inflating: SICAM_GridEdge_x.x/moxa-real-tty-drivers-for-linux-4.x.x-driver-
v4.0.tgz
  inflating: SICAM_GridEdge_x.x/open_valueviewer.sh
  inflating: SICAM_GridEdge_x.x/show_syslogs.sh
  inflating: SICAM_GridEdge_x.x/sicamgridedge.ini
  inflating: SICAM_GridEdge_x.x/sicamgridedge.sh
  inflating: SICAM_GridEdge_x.x/sicamgridedge_modules.sh
  inflating: SICAM_GridEdge_x.x/sicamgridedge_setup.sh
  inflating: SICAM_GridEdge_x.x/ssh_cron.sh
   creating: SICAM_GridEdge_x.x/templates/
   creating: SICAM_GridEdge_x.x/templates/WMI/
  inflating: SICAM_GridEdge_x.x/templates/WMI/WMI.csv
   creating: SICAM_GridEdge_x.x/templates/SNMP/
  inflating: SICAM_GridEdge_x.x/templates/SNMP/Hopf.csv
  inflating: SICAM_GridEdge_x.x/templates/SNMP/SICAMRTUsAK3.csv
  inflating: SICAM_GridEdge_x.x/templates/SNMP/Meinberg.csv
  inflating: SICAM_GridEdge_x.x/templates/SNMP/Ruggedcom.csv
  inflating: SICAM_GridEdge_x.x/templates/SNMP/SICAMA8000.csv
  inflating: SICAM_GridEdge_x.x/templates/SNMP/Hirschmann.csv
  inflating: SICAM_GridEdge_x.x/templates/SNMP/Cisco.csv
  inflating: SICAM_GridEdge_x.x/templates/SNMP/SIMATICNET.csv
  inflating: SICAM_GridEdge_x.x/templates/SNMP/Default.csv
 extracting: SICAM_GridEdge_x.x/version.info
edge@localhost:~$ cd SICAM_GridEdge_x.x
edge@localhost:~/SICAM_GridEdge_x.x$ chmod +x *.sh
edge@localhost:~/SICAM_GridEdge_x.x$ ./sicamgridedge_setup.sh
```

2.6 Setting Up Serial Connections

2.6.1 Serial Connection

A serial connection can be established with the DIGSI 4 or Modbus protocol.

Connection with DIGSI 4



[ge_serial_connection_digsi, 2, en_US]

The device on which SICAM GridEdge is installed is connected via Ethernet to a serial port extender (for example, Moxa NPort). The serial port extender is additionally connected to one or more serial devices. Using the DIGSI 4 protocol, the serial port extender can receive data from the serial devices and transfer them to SICAM GridEdge.

Several serial devices can be connected via a serial bus line topology (RS485) and via different ports of the serial port extender. These ports as well as the IP address must be configured using the configuration software of the serial port extender.

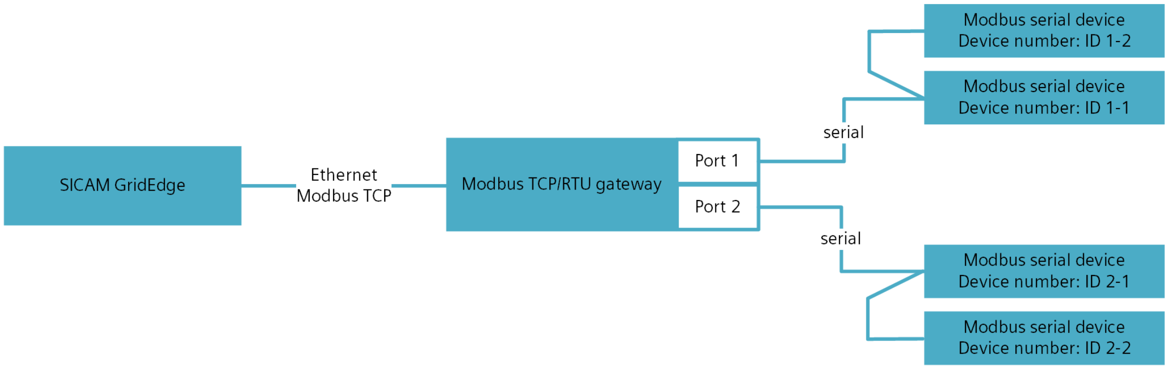
Every connected serial device must be additionally identified with a unique address called link address. This link address must be defined with the configuration software of the SIPROTEC 4 device.

For more information about the addition of devices, refer to *Adding Serial Devices, Page 29*.

The serial port extenders NPort 5210, 5230, 5410, 5430, 5600 and 5650 Series are supported. For more information about the setup, refer to *2.6.2 Setting Up the Ethernet-To-Serial Hardware*.

Only the service interface on the rear side of the SIPROTEC 4 or SIPROTEC Compact Class device (RS232 or RS485) is supported as a serial port. An optional serial-interface card in the device might be necessary.

Connection with Modbus



[ge_serial_connection_modbus, 1, en_US]

The device on which SICAM GridEdge is installed is connected via Ethernet to a Modbus TCP/RTU gateway. The Modbus TCP/RTU gateway is additionally connected to one or more Modbus serial devices. Using the Modbus protocol, the Modbus TCP/RTU gateway can receive data from the serial devices and transfer them to SICAM GridEdge. The data is sent in the Modbus serial format by the serial devices and adapted to the Modbus TCP format by the gateway.

Several serial devices can be connected via a serial bus line topology (RS485) and via different ports of the Modbus TCP/RTU gateway. These ports as well as the IP address must be configured using the configuration software of the Modbus TCP/RTU gateway.

Every connected serial device must be additionally identified with a unique number called unit identifier. This unit identifier must be defined with the configuration software of the Modbus serial device.

Example:

- 192.168.1.30: IP address of the Modbus TCP/RTU gateway
- 502: Port number
- 24: Unique device number

For more information about the addition of devices, refer to *Adding Serial Devices, Page 29*.

2.6.2 Setting Up the Ethernet-To-Serial Hardware

For a connection between SICAM GridEdge and serial devices, additional hardware is required. You either need a serial port extender (for DIGSI 4 protocol) or a Modbus TCP/RTU gateway (for Modbus). For more information, refer to *2.6.1 Serial Connection*.

Configuring a Moxa Device (DIGSI 4 protocol)

SICAM GridEdge supports a Moxa serial device driver as a serial port extender.

You can configure the Moxa serial port extender using the Moxa Web user interface. For more information about the usage of the software, refer to the official Moxa documentation.

✧ Open the Moxa Web user interface.

✧ Search for your serial port extender.

✧ Open the configuration page of the serial port extender.

✧ Navigate to the configuration page for the network settings.

✧ Enter the IP address of the serial port extender in the network settings. You need the IP address for adding serial devices in SICAM GridEdge (refer to *Adding Serial Devices, Page 29*).

✧ Navigate to the configuration page for the operating mode.

✧ Set the operating mode of the serial port extender to **TCP Server Mode**.

✧ If it is necessary in the unlikely case, adapt the default values of the port number. You need the port number for adding serial devices in SICAM GridEdge.

✧ Navigate to the configuration page for the serial settings.

✧ Adjust the settings (for example, the baud rate and interface) for the port in accordance with how your devices are connected to the serial port extender.

✧ Ensure that **FIFO** is enabled for the used serial ports.

✧ Save your changes.

The serial port extender is set up and can be added in the subpage **Serial Devices** in SICAM GridEdge.

Configuring a Modbus TCP/RTU Gateway

✧ Use the tools provided by the vendor (for example, a configuration tool or a build-in Web server).
For more information, refer to the official vendor documentation.

2.7 Uninstalling SICAM GridEdge

✧ Connect to your device using the SSH access.

✧ Navigate to the folder to which you extracted your ZIP file of the setup bundle (refer to *2.5.1 Installing SICAM GridEdge*).

✧ Start the SICAM GridEdge uninstallation:

```
./sicamgridedge_uninstall.sh
```

The uninstallation process runs automatically.
During the uninstallation, all SICAM GridEdge-related data is deleted.

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.

NOTE

If you plan to upgrade your installed version of SICAM GridEdge lower than 2.4, you need to re-configure your system after the upgrade.

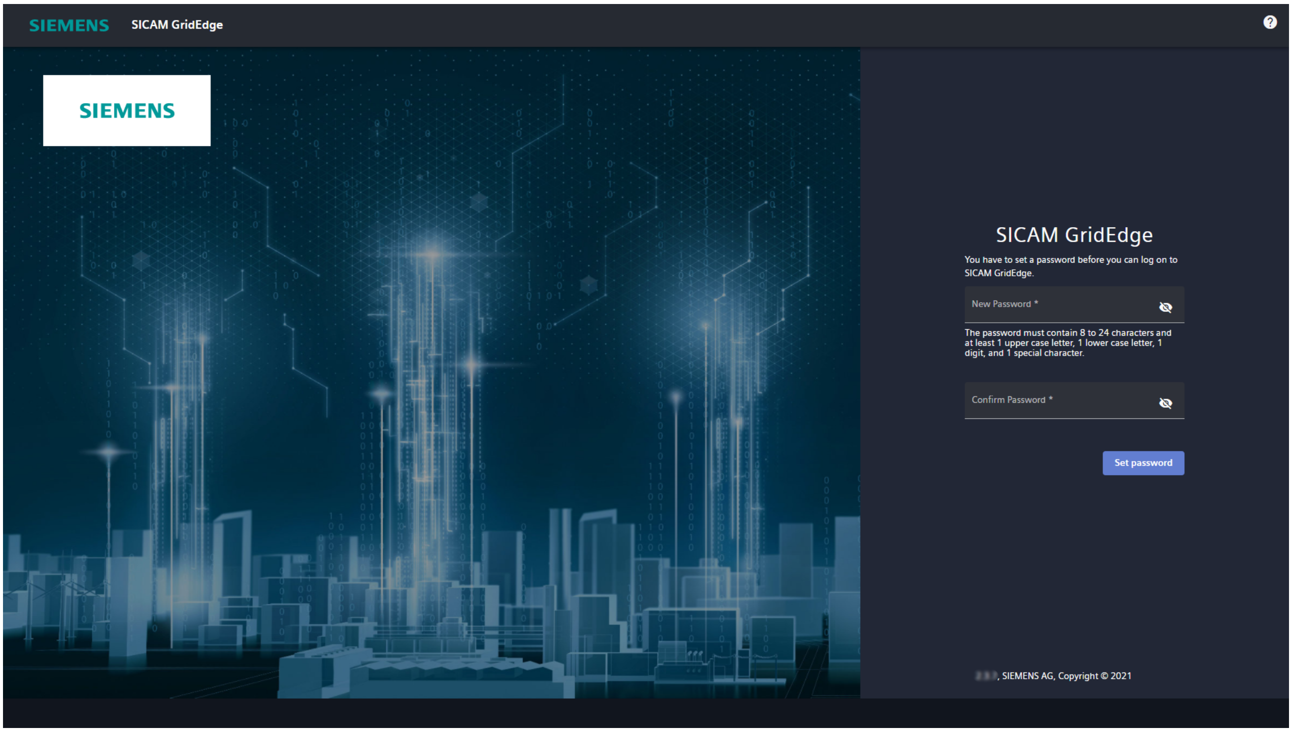
Ensure to delete all your asset information in your cloud platform.

3.1 Access to SICAM GridEdge Web Interface

NOTE

Access to SICAM GridEdge Web interface is secured with a self-signed certificate.
Ensure to use this certificate properly (refer to *5.8 TCP-UDP Ports*) in order to avoid the security concerns reported by your Web browser.

The SICAM GridEdge Web interface is available at *https://<STATION_LAN_IP>:8900*, for example *https://192.168.1.10:8900*.



SICAM GridEdge

You have to set a password before you can log on to SICAM GridEdge.

The password must contain 8 to 24 characters and at least 1 upper case letter, 1 lower case letter, 1 digit, and 1 special character.

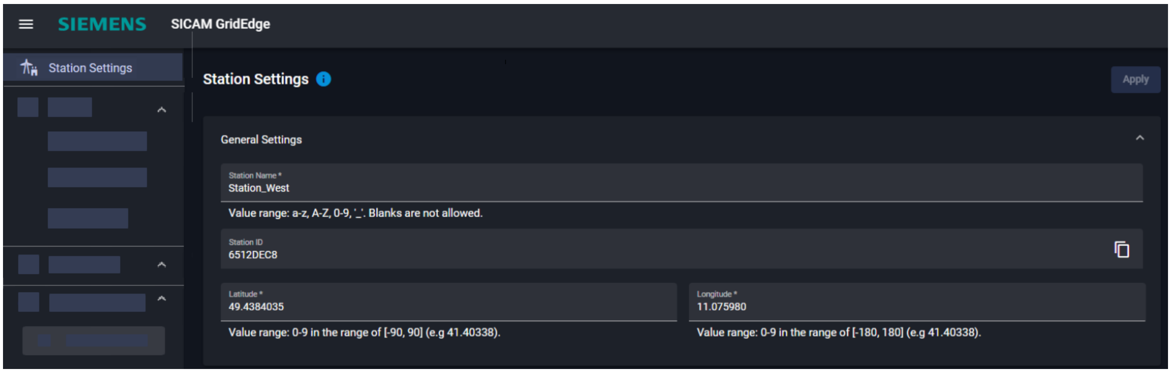
[redacted], SIEMENS AG, Copyright © 2021

[sc_SICAM_GridEdge_WebInterface, 5, 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 Configuring the Station Settings



Station Settings

General Settings

Station Name *
Station_West

Value range: a-z, A-Z, 0-9, '_'. Blanks are not allowed.

Station ID
6512DEC8

Latitude *
49.4384035

Value range: 0-9 in the range of [-90, 90] (e.g 41.40338).

Longitude *
11.075980

Value range: 0-9 in the range of [-180, 180] (e.g 41.40338).

[sc_station_settings, 4, en_US]

Figure 3-2 Station Settings

✧ Open the page **Station Settings**.

✧ Enter a **Station Name** that is unique in your cloud platform.

✧ Enter the GPS coordinates (**Latitude** and **Longitude**) of your SICAM GridEdge location (for example, **41.40338**). If needed, use a geolocation tool to retrieve the coordinates (for example, *https://www.latlong.net/*).

✧ If necessary, configure the connection to a proxy server (refer to *3.5.1 Configuring a Connection via a Proxy Server*).

✧ To exclude sensitive data from being published to the cloud platform, disable **Publish sensitive data to cloud connection**.

Diagnosis and log files are not transferred to the cloud platform. Local network addresses and geolocation information are removed from the asset information file before being transferred to the cloud platform.

✧ Select **Apply**.

3.3 Device Connection Configuration

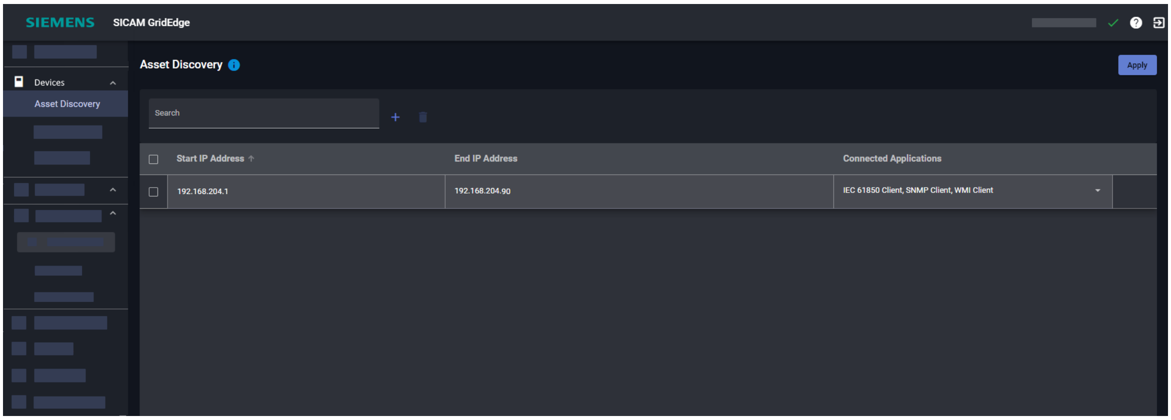
3.3.1 Adding Ethernet Devices Automatically

You can monitor your substation and search for new devices that will automatically be added to SICAM GridEdge. You can be informed about new devices that are detected in a defined IP range and get the corresponding asset information. This action is supported for the following protocols:

- IEC 61850 Client
- SNMP Client
- WMI Client

NOTE

If you want to rename a device before it is automatically onboarded in the cloud platform, you must deactivate the cloud connection before starting the search for new devices. After the search, you can change the name in the subpage **Ethernet Devices**.



Asset Discovery

☐	Start IP Address ↑	End IP Address	Connected Applications
☐	192.168.204.1	192.168.204.90	IEC 61850 Client, SNMP Client, WMI Client

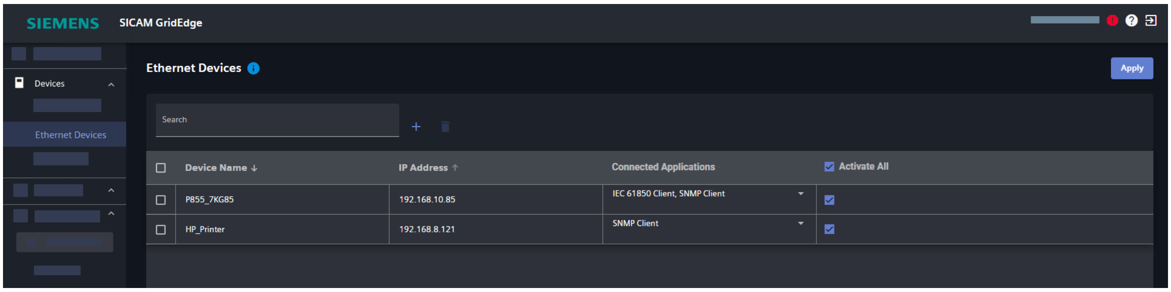
[sc_asset_discovery, 2, en_US]

- ✧ Navigate to the page **Devices**.
- ✧ Open the subpage **Asset Discovery**.
- ✧ Enter the first IP address within the IP range needed for consideration.
- ✧ Enter the last 3 digits of the last IP address within the IP range needed for consideration.
- ✧ Select the protocol in **Connected Applications**.
- ✧ Select **Apply**.

SICAM GridEdge starts to search for new devices in the defined IP address range. This search is automatically repeated every hour.
In case a new device is detected, the device will be listed in the subpage **Ethernet Devices** and in the page **Connection Status**. The name of the device is taken from the protocol.

3.3.2 Adding Devices Manually

Adding Ethernet Devices



Ethernet Devices

☐	Device Name ↓	IP Address ↑	Connected Applications	☑ Activate All
☐	P855_7KG85	192.168.10.85	IEC 61850 Client, SNMP Client	☑
☐	HP_Printer	192.168.8.121	SNMP Client	☑

[sc_add_del_Ethernet, 4, en_US]

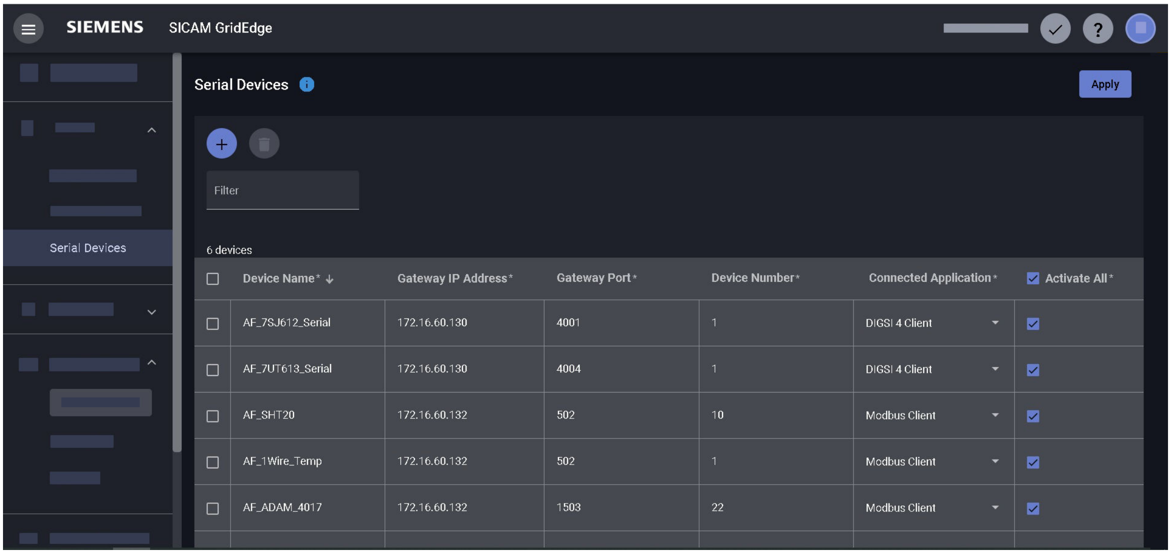
Figure 3-3 Ethernet Devices

- ✧ Navigate to the page **Devices**.
- ✧ Open the subpage **Ethernet Devices**.
- ✧ Select the icon +.
- ✧ Enter the **Device Name** which is to be used to transfer data to the cloud.
- ✧ Enter the **IP Address** of the device.

✧ Choose the protocol used to fetch data from the device in the field **Connected Application**.
If, for example, **IEC 61850 Client** is enabled, SICAM GridEdge will automatically try to connect to the devices configured for the protocol IEC 61850 Client.

✧ Select **Apply**.

Adding Serial Devices



6 devices

☐	Device Name*	Gateway IP Address*	Gateway Port*	Device Number*	Connected Application*	☑ Activate All*
☐	AF_7SJ612_Serial	172.16.60.130	4001	1	DIGSI 4 Client	☑
☐	AF_7UT613_Serial	172.16.60.130	4004	1	DIGSI 4 Client	☑
☐	AF_SHT20	172.16.60.132	502	10	Modbus Client	☑
☐	AF_1Wire_Temp	172.16.60.132	502	1	Modbus Client	☑
☐	AF_ADAM_4017	172.16.60.132	1503	22	Modbus Client	☑

[sc_add_del_Serial, 5, en_US]

Figure 3-4 Serial Devices

Make sure the corresponding hardware is set up – a Modbus TCP/RTU gateway for a Modbus connectiona or a serial port extender for a DIGSI 4 connection.

✧ Navigate to the page **Devices**.

✧ Open the subpage **Serial Devices**.

✧ Select the icon +.

✧ Enter the **Device Name** which is to be used to transfer data to the cloud.

✧ Enter the IP address and port number of the Modbus TCP/RTU gateway in the fields **Gateway IP Address** and **Gateway Port**. These are defined using the configuration software of the gateway.

- or -

✧ Enter the IP address and port number of the DIGSI 4 serial port extender in the fields **Gateway IP Address** and **Gateway Port**. These are defined using the configuration software of the serial port extender (refer to *2.6.2 Setting Up the Ethernet-To-Serial Hardware*).

✧ Enter the unique unit identifier of the Modbus device in the field **Device Number**. This number is defined in the configuration software of the serial device.

- or -

✧ Enter the link address of the SIPROTEC 4 device in the field **Device Number**. This address is defined in the DIGSI 4 configuration software of the SIPROTEC 4 device.

✧ Choose the protocol used to fetch data from the device in the field **Connected Application**.

✧ Select **Apply**.

3.3.3 Deactivating Device Connections

All device connections are activated by default. Device connections can be deactivated for service or maintenance work.

✧ Navigate to the page **Devices**.

✧ To deactivate an Ethernet device connection, open the subpage **Ethernet Devices**.

✧ To deactivate a serial device connection, open the subpage **Serial Devices**.

✧ Clear the checkbox of the desired device in the column **Activate All**.

✧ Select **Apply**.

The connection of the selected device is deactivated. The connection remains inactive until the checkbox **Activate All** is selected.

The deactivation is displayed in the page **Connection Status**.

3.3.4 Deleting Devices

✧ Navigate to the page **Devices**.

✧ To delete an Ethernet device connection, open the subpage **Ethernet Devices**.

✧ To delete a serial device connection, open the subpage **Serial Devices**.

✧ Select the device you want to delete from the list.

✧ Select the icon 🗑.

✧ Confirm the deletion.

The device is deleted from SICAM GridEdge.

The device is not deleted from the cloud platform. If necessary, manually delete the device in the cloud platform as well.

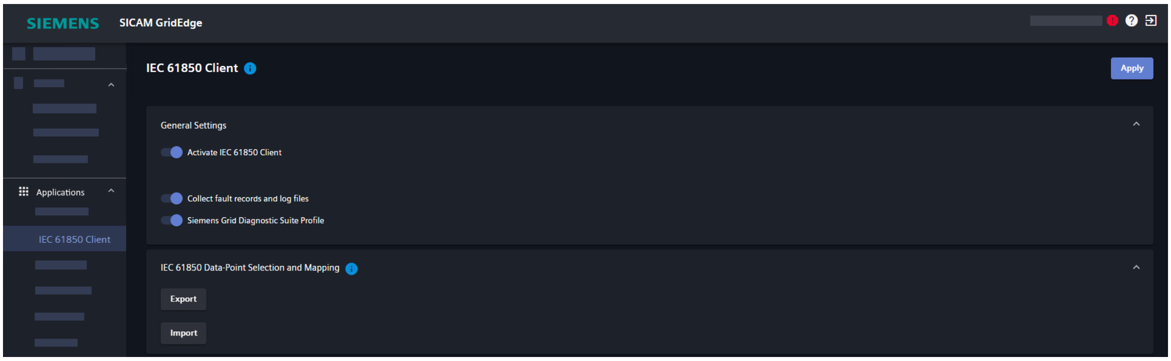
3.4 Application Configuration

To collect data from connected devices in the substation, you need to configure the used protocols.

3.4.1 IEC 61850 Client

3.4.1.1 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.



IEC 61850 Client

General Settings

Activate IEC 61850 Client

Collect fault records and log files

Siemens Grid Diagnostic Suite Profile

IEC 61850 Data-Point Selection and Mapping

[sc_SICAM_GridEdge_IEC61850_Client, 9, en_US]

Figure 3-5 IEC 61850 Client

- ✧ Configure the **Ethernet Devices** (refer to *Adding Ethernet Devices, Page 28*) and assign them to the IEC 61850 protocol.
- ✧ Navigate to the page **Applications**.
- ✧ Open the subpage **IEC 61850 Client**.
- ✧ If files (COMTRADE, COMFEDE) from devices are to be fetched and transferred to the external cloud platform, enable **Collect fault records and log files**.
- ✧ If you want to send data to a SIPROTEC Grid Diagnostic Suite application, enable **Siemens Grid Diagnostic Suite Profile**.

All needed data are transferred to the cloud platform. These data will be additionally transferred to the manually selected data points (refer to *3.4.3 DIGSI 4 Client*).

- ✧ Enable **Activate IEC 61850 Client** so all devices defined for IEC 61850 connection (refer to *Adding Ethernet Devices, Page 28*) are considered for data retrieval.
- ✧ Select **Apply**.

NOTE

Onboarding the devices in the cloud may take several minutes.

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

NOTE

It is not possible to retrieve data from devices secured according to IEC 62351.

Protection Devices

Table 3-1 Protection Devices – Grid Events

Grid Events	Examples 61850 Path
Device not healthy: LDN	Application/LLN0$ST$Health Q0_Bay1/LLN0$ST$Health
Relay pickup: LDN	Q0_Bay1/PTRC1$ST$Str
Relay trip: LDN	Q0_Bay1/PTRC1$ST$Tr
Hotspot temp. warning: LDN	PTS1_49HotSpot1/HTSP_PTTR1$ST$HSTWarn PTS2_49HotSpot1/HTSP_PTTR1$ST$HSTWarn

Grid Events	Examples 61850 Path
Hotspot temp. alarm: LDN	PTS1_49HotSpot1/HTSP_PTTR1$ST$HSTAlm PTS2_49HotSpot1/HTSP_PTTR1$ST$HSTAlm
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_SCBR1$ST$SumIxA
ΣIx L2: LDN	CB1_CBWearMonitoring/PIx_SCBR1$ST$SumIxB
ΣIx L3: LDN	CB1_CBWearMonitoring/PIx_SCBR1$ST$SumIxC
ΣI²t L1: LDN	CB1_CBWearMonitoring/I2t_SCBR1$ST$SumI2tA
ΣI²t L2: LDN	CB1_CBWearMonitoring/I2t_SCBR1$ST$SumI2tB
ΣI²t L3: LDN	CB1_CBWearMonitoring/I2t_SCBR1$ST$SumI2tC
Make time: LDN	CB1_CBWearMonitoring/MkTm_SCBR1$MX$MakeTime
2P Endur. L1: LDN	CB1_CBWearMonitoring/P2P_SCBR1$ST$EnduA
2P Endur. L2: LDN	CB1_CBWearMonitoring/P2P_SCBR1$ST$EnduB
2P Endur. L3: LDN	CB1_CBWearMonitoring/P2P_SCBR1$ST$EnduC
Breaking-current sum	CB1/XCBR1$ST$SumSwARs
Breaking-current sum L1	CB1/XCBR1$ST$SumSwARsA
Breaking-current sum L2	CB1/XCBR1$ST$SumSwARsB
Breaking-current sum L3	CB1/XCBR1$ST$SumSwARsC
Circuit breaker Operation Counter	CB1/XCBR1$ST$OpCnt
Disconnector Operation Counter	Dc1/XSWI1$ST$OpCnt

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

Measured Values	Examples 61850 Path
Circuit breaker position	CB1/XCBR1$ST$Pos
Disconnector position	Dc1/XSWI1$ST$Pos
79 successful	CB1_79AutoReclosing/GEN_RREC1/Successful
Blk. by binary input	CB1_79AutoReclosing/GEN_RREC1/BlkBinInp

Measured Values	Examples 61850 Path
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	PTRC1$ST$Str.dirGeneral
Direction L1	PTRC1$ST$Str.dirPhsA
Direction L2	PTRC1$ST$Str.dirPhsB
Direction L3	PTRC1$ST$Str.dirPhsC
Direction neutral	PTRC1$ST$Str.dirNeut
Pickup L1	PTRC1$ST$Str.phsA
Pickup L2	PTRC1$ST$Str.phsB
Pickup L3	PTRC1$ST$Str.phsC
Pickup neutral	PTRC1$ST$Str.neut
Fault distance	Ln1/SE_RFLO1$MX$FltDis

Power Quality Devices

Table 3-5 Power Quality Devices – Grid Events

Grid Events	Examples 61850 Path
Device Health	LLN0$ST$Health
Battery Failure	ZBAT1$ST$BatLo
Fault Record Stored	PQA_RDRE1$ST$RcdMade
Frequency Variation Event Start	PQA_QFVR1$ST$VarStr
Voltage Unbalance Event Start	PQA_QVUB1$ST$VarStr
Voltage Variation Event Start	PQA_QVVR1$ST$VarStr
Voltage Swell Event	PQA_QVVR1$ST$SwlStr
Voltage Dip Event	PQA_QVVR1$ST$DipStr
Voltage Interruption Event	PQA_QVVR1$ST$IntrStr
Affected Phases by a Voltage Variation Event	PQA_QVVR1$ST$AffPhs

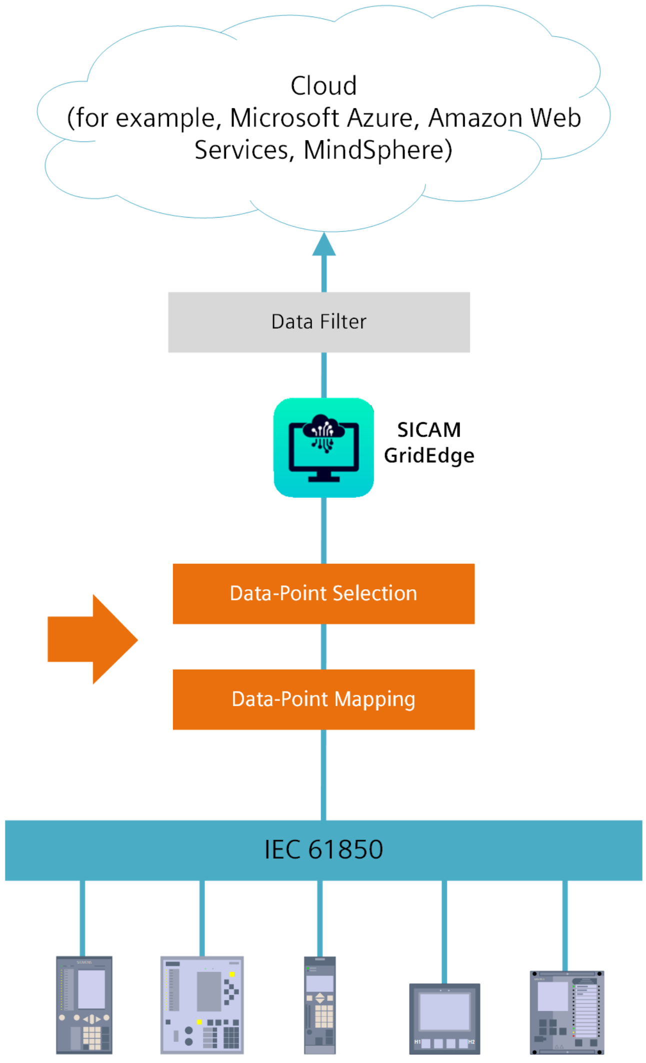
Table 3-6 Power Quality Devices – Measured Values

Measured Values	Examples 61850 Path
Voltage Variation Event Level	PQA_QVVR1$MX$VVa
Voltage Variation Event Duration	PQA_QVVR1$MX$VVaTm
Phase to Ground Voltage - Phase A	PQA2MMXU1$MX$PhV$phsA
Phase to Ground Voltage - Phase B	PQA2MMXU1$MX$PhV$phsB
Phase to Ground Voltage - Phase C	PQA2MMXU1$MX$PhV$phsC
Phase to Phase Voltage - Phase AB	PQA2MMXU1$MX$PPV$phsAB

Measured Values	Examples 61850 Path
Phase to Phase Voltage - Phase BC	PQA2MMXU1$MX$PPV$phsBC
Phase to Phase Voltage - Phase CA	PQA2MMXU1$MX$PPV$phsCA
Phase to Ground Voltage (Single Phase)	PQA2MMXN1$MX$Vol
Phase to Ground Voltage - Neutral	PQA2MMXU1$MX$PhV$neut
Average Phase to Phase Voltage	PQA2MMXU1$MX$AvPPVPhs
Phase Current - Phase A	PQA2MMXU1$MX$A$phsA
Phase Current - Phase B	PQA2MMXU1$MX$A$phsB
Phase Current - Phase C	PQA2MMXU1$MX$A$phsC
Phase Current (Single Phase)	PQA2MMXN1$MX$Amp
Phase Current - Neutral	PQA2MMXU1$MX$A$neut
Average Phase Current	PQA2MMXU1$MX$AvAPhs
Active Power - Phase A	PQA2MMXU1$MX$W$phsA
Active Power - Phase B	PQA2MMXU1$MX$W$phsB
Active Power - Phase C	PQA2MMXU1$MX$W$phsC
Total Active Power	PQA2MMXU1$MX$TotW
Active Power (Single Phase)	PQA2MMXN1$MX$Watt
Reactive Power - Phase A	PQA2MMXU1$MX$VAr$phsA
Reactive Power - Phase B	PQA2MMXU1$MX$VAr$phsB
Reactive Power - Phase C	PQA2MMXU1$MX$VAr$phsC
Total Reactive Power	PQA2MMXU1$MX$TotVAr
Reactive Power (Single Phase)	PQA2MMXN1$MX$VolAmpr
Apparent Power - Phase A	PQA2MMXU1$MX$VA$phsA
Apparent Power - Phase B	PQA2MMXU1$MX$VA$phsB
Apparent Power - Phase C	PQA2MMXU1$MX$VA$phsC
Total Apparent Power	PQA2MMXU1$MX$TotVA
Apparent Power (Single Phase)	PQA2MMXN1$MX$VolAmp
Power Factor - Phase A	PQA2MMXU1$MX$PF$phsA
Power Factor - Phase B	PQA2MMXU1$MX$PF$phsB
Power Factor - Phase C	PQA2MMXU1$MX$PF$phsC
Power Factor	PQA2MMXU1$MX$TotPF
Power Factor (Single Phase)	PQA2MMXN1$MX$PwrFact
Cosinus Phi - Phase A	PQA2MMXU1$MX$ActivePF$phsA
Cosinus Phi - Phase B	PQA2MMXU1$MX$ActivePF$phsB
Cosinus Phi - Phase C	PQA2MMXU1$MX$ActivePF$phsC
Cosinus Phi	PQA2MMXU1$MX$TotActivePF
Cosinus Phi (Single Phase)	PQA2MMXN1$MX$ActivePwrFact
Voltage Imbalance - Negative sequence component	PQA2MSQI1$MX$ImbNgV
Current Imbalance - Negative sequence component	PQA2MSQI1$MX$ImbNgA
Voltage Imbalance - Zero sequence component	PQA2MSQI1$MX$ImbZroV
Current Imbalance - Zero sequence component	PQA2MSQI1$MX$ImbZroA
Frequency	PQA4MMXU1$MX$Hz
Frequency (Single Phase)	PQA4MMXN1$MX$Hz
Total Harmonic Distortion Voltage - Phase A	PQA2MHAI1$MX$ThdPhV$phsA
Total Harmonic Distortion Voltage - Phase B	PQA2MHAI1$MX$ThdPhV$phsB
Total Harmonic Distortion Voltage - Phase C	PQA2MHAI1$MX$ThdPhV$phsC
Total Harmonic Distortion Voltage - Phase AB	PQA2MHAI1$MX$ThdPPV$phsAB
Total Harmonic Distortion Voltage - Phase BC	PQA2MHAI1$MX$ThdPPV$phsBC

Measured Values	Examples 61850 Path
Total Harmonic Distortion Voltage - Phase CA	PQA2MHAI1$MX$ThdPPV$phsCA
Total Harmonic Distortion Voltage (Single Phase)	PQA2MHAN1$MX$ThdVol
Total Harmonic Distortion Current - Phase A	PQA2MHAI1$MX$ThdA$phsA
Total Harmonic Distortion Current - Phase B	PQA2MHAI1$MX$ThdA$phsB
Total Harmonic Distortion Current - Phase C	PQA2MHAI1$MX$ThdA$phsC
Total Harmonic Distortion Current (Single Phase)	PQA2MHAN1$MX$ThdAmp
Short Term Flicker - Phase A	PQA2MFLK1$MX$PhPst$phsA
Short Term Flicker - Phase B	PQA2MFLK1$MX$PhPst$phsB
Short Term Flicker - Phase C	PQA2MFLK1$MX$PhPst$phsC
Long Term Flicker - Phase A	PQA2MFLK1$MX$PhPlt$phsA
Long Term Flicker - Phase B	PQA2MFLK1$MX$PhPlt$phsB
Long Term Flicker - Phase C	PQA2MFLK1$MX$PhPlt$phsC
Harmonic Voltage Array - Phase A	PQA2MHAI1$MX$HPhV$phsAHar
Harmonic Voltage Array - Phase B	PQA2MHAI1$MX$HPhV$phsBHar
Harmonic Voltage Array - Phase C	PQA2MHAI1$MX$HPhV$phsCHar
Harmonic Voltage Array - Phase AB	PQA2MHAI1$MX$HPPV$phsABHar
Harmonic Voltage Array - Phase BC	PQA2MHAI1$MX$HPPV$phsBCHar
Harmonic Voltage Array - Phase CA	PQA2MHAI1$MX$HPPV$phsCAHar
Maximum Harmonic Voltage Array - Phase A	MAX_PQA2MHAI1$MX$HPhV$phsAHar
Maximum Harmonic Voltage Array - Phase B	MAX_PQA2MHAI1$MX$HPhV$phsBHar
Maximum Harmonic Voltage Array - Phase C	MAX_PQA2MHAI1$MX$HPhV$phsCHar
Maximum Harmonic Voltage Array - Phase AB	MAX_PQA2MHAI1$MX$HPPV$phsABHar
Maximum Harmonic Voltage Array - Phase BC	MAX_PQA2MHAI1$MX$HPPV$phsBCHar
Maximum Harmonic Voltage Array - Phase CA	MAX_PQA2MHAI1$MX$HPPV$phsCAHar
Harmonic Voltage Array (Single Phase)	PQA2MHAN1$MX$HaVol
Maximum Harmonic Voltage Array (Single Phase)	MAX_PQA2MHAN1$MX$HaVol
Harmonic Power Array - Phase A	PQA2MHAI1$MX$HW$phsAHar
Harmonic Power Array - Phase B	PQA2MHAI1$MX$HW$phsBHar
Harmonic Power Array - Phase C	PQA2MHAI1$MX$HW$phsBHar
Harmonic Power Array (Single Phase)	PQA2MHAN1$MX$HaWatt
Total Real Energy Supply	MMTR1$ST$SupWh
Real Energy Supply (Single Phase)	MMTN1$ST$SupWh
Total Real Energy Demand	MMTR1$ST$DmdWh
Real Energy Demand (Single Phase)	MMTN1$ST$DmdWh
Total Reactive Energy Supply	MMTR1$ST$SupVarh
Reactive Energy Supply (Single Phase)	MMTN1$ST$SupVarh
Total Reactive Energy Demand	MMTR1$ST$DmdVarh
Reactive Energy Demand (Single Phase)	MMTN1$ST$DmdVarh
Total Net Apparent Energy	MMTR1$ST$TotVAh
Net Apparent Energy (Single Phase)	MMTN1$ST$TotVAh

3.4.1.2 Data-Point Selection and Mapping



[dw_selection_mapping, 1, en_US]

NOTE

For more information and examples, refer to the public Github repository *https://github.com/siemens/sicam-gridedge-configurationtemplates*.

If you want to define a data-point selection as well as a data-point mapping, you must import one combined file only.

Data-Point Selection

You can import a CSV file which allows you to select data points from any IEC 61850 device for data retrieval to SICAM GridEdge.

Data-Point Mapping

You can import a CSV file which allows you 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.

NOTE

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.

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

3.4.1.3 Selecting and Mapping Data Points

NOTE

If **Siemens Grid Diagnostic Suite Profile** is enabled, data relevant for those cloud applications will automatically be selected - regardless of the selection in the data-point mapping and selection file.

NOTE

It is not possible to retrieve data from devices secured according to IEC 62351.

✧ Navigate to the page **Applications**.

✧ Open the subpage **IEC 61850 Client**.

✧ Under **IEC 61850 Data-Point Selection and Mapping**, select **Import**.

✧ Upload your data-point mapping/data-point selection file (refer to *3.4.1.5 Format of the Data-Point Selection and Mapping File*).

SICAM GridEdge assists you in finding possible syntax errors in the imported file by providing a summary of the found errors.

✧ If syntax errors are found, select **here** to download the summary and adapt the file accordingly.

3.4.1.4 Changing and Deleting the Data-Point Selection and Mapping File

Changing the Selection/Mapping

✧ Navigate to the page **Applications**.

✧ Open the subpage **IEC 61850 Client**.

✧ Under **IEC 61850 Data-Point Selection and Mapping**, select **Export**.

Your currently used data-point selection and mapping file is downloaded.

✧ Use the downloaded file to do your changes.

✧ Select **Import**.

✧ Upload your changed data-point mapping/data-point selection file.

Deleting the Selection/Mapping

✧ Navigate to the page **Applications**.

✧ Open the subpage **IEC 61850 Client**.

✧ Under **IEC 61850 Data-Point Selection and Mapping**, select **Import**.

✧ Upload an empty data-point mapping/data-point selection file (0 bytes).

The previously used file is overwritten.
As the new file is empty, SICAM GridEdge does no longer select or map data points.

3.4.1.5 Format of the Data-Point Selection and Mapping File

To define a data mapping or a data-point selection that can be used in SICAM GridEdge, it is required to create a CSV file in a predefined format. The file contains up to 3 columns that are separated by a semicolon. Data-point mapping and data-point selection is combined in one file only.

Column IED Name

This column contains the name of the IED to which the mapping or selection is applied.

By using regular expressions, it is possible to select a specific subset of IEDs - for example, IED_00000[1-9] selects the devices IED_000001, IED_000002, ... IED_000009.

NOTE

SICAM GridEdge perceives the name of the IED as a combination of the actual IED name and the name of the logical device. To detect the actual IED name, SICAM GridEdge uses an algorithm:

IED with multiple logical devices

- IED: IEC 61850 Device 1
  - Logical device: MyDeviceMMXU1
  - Logical device: MyDeviceCALH2
  - Logical device: MyDeviceCSWI3

SICAM GridEdge detects **MyDevice** as the IED name.

IED with one logical device

- IED: IEC 61850 Device 1
  - Logical device: MyDeviceMMXU1

SICAM GridEdge detects **MyDeviceMMXU1** as the IED name.

Ensure to consider this behavior when entering the IED name in the data-point selection and mapping file.

Column Source

This column contains the data model as defined in the device.

By using regular expressions, it is possible to select a specific subset of data points - for example, .*MMXU.* selects all logical nodes containing MMXU.

Column Replacement

This column contains the desired data model that is used for publishing the data to the cloud platform.

A **Replacement** is only needed for data-point mapping and stays empty for the data-point selection.

Example for Data-Point Selection

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

In the example:

- All data points from any logical node **MMXU** of the IEDs starting with the name **IED_000** are transferred to SICAM GridEdge.

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.

Example for Data-Point Mapping

```
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:

- The data point with the name **EXT/pdGGIO2001$ST$ISCSO1** of the devices whose IED name starts with **IED_000** are mapped to **CB1_CBWearMonitoring/PIx_SCBR1$ST$SumIxA** and transferred to SICAM GridEdge.
- The data point with the name **EXT/pdGGIO2001$ST$ISCSO3** of the devices with IED name **IED_000001** to **IED_000009** are mapped to **CB1_CBWearMonitoring/PIx_SCBR1$ST$SumIxC** and transferred to SICAM GridEdge.

NOTE

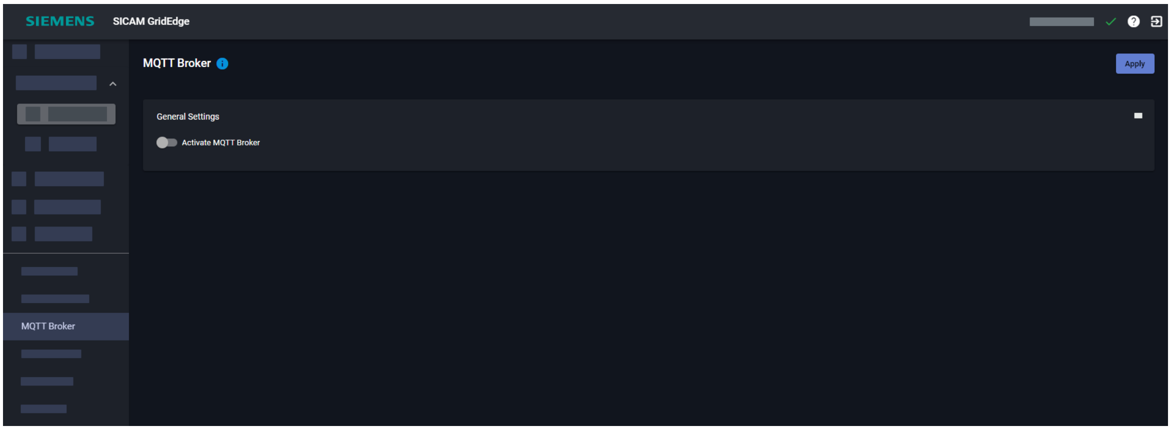
Data points may only be mapped on the IEC 61850 **Data Object** level. Therefore, always use a mapping in the following format:

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

3.4.2 MQTT Broker

3.4.2.1 Configuring the MQTT Broker

The MQTT broker is used to fetch operational data from a Siemens Assetguard IoT device (using the MQTT protocol) and transfer them via SICAM GridEdge to the external cloud platform.



[sc_mqtt_broker, 1, --_--]

Figure 3-6 MQTT Broker

Enabling the MQTT Connection

The IP address of your SICAM GridEdge is registered in the MQTT client device.

✧ Add the MQTT-client device to SICAM GridEdge (refer to *3.3.2 Adding Devices Manually*).

✧ Open the page **MQTT Broker**.

✧ Enable **Activate MQTT Broker**.

✧ Select **Apply**.

SICAM GridEdge creates a file that is compressed as a tar.gz file. The file name contains the time stamp of the MQTT message (for example, 1624264289000.tar.gz). This file is sent to the cloud platform.

3.4.3 DIGSI 4 Client

3.4.3.1 Configuring the DIGSI 4 Client

NOTE

For Ethernet-connected devices, Siemens recommends using the IEC61850 protocol if available.

NOTE

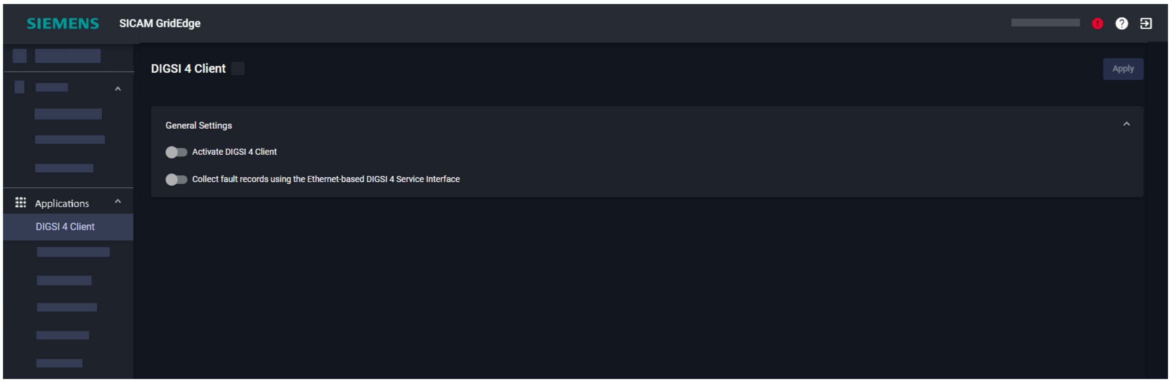
SICAM GridEdge can only establish a DIGSI 4 communcation if the following requirements are met:

- The device is configured with a default installation bundle version of DIGSI 4 up to V4.96 containing the corresponding device drivers. Device drivers that were later manually added cannot be processed by SICAM GridEdge.
- If the device is connected to SICAM GridEdge using an EN100 module, no security or password must be configured.
- If the device is connected to SICAM GridEdge using an EN100 module, the option **DIGSI via EN100 module** is not disabled for the device in DIGSI 4 (refer to DIGSI documentation).

DIGSI 4 Client is used to fetch the following data from the SIPROTEC 4/SIPROTEC 4 Compact devices and transfer them to the external cloud platform:

- The protection settings and their changes (only if the option **Settings group change** is disabled in the SIPROTEC 4 device)
- The available fault records (must be enabled for Ethernet-connected devices)
- The available asset data

This data is retrieved from the devices on initial connection, on reconnection after communication interruptions, and cyclically every hour. Every 30 minutes it is checked whether the devices are still online.



DIGSI 4 Client

General Settings

Activate DIGSI 4 Client

Collect fault records using the Ethernet-based DIGSI 4 Service Interface

[sc_digsi4client, 2, en_US]

Figure 3-7 DIGSI 4 Client

✧ Configure the **Ethernet Devices** (refer to *Adding Ethernet Devices, Page 28*) and assign them to the DIGSI 4 protocol.

✧ Configure the **Serial Devices** (refer to *Adding Serial Devices, Page 29*).

For a serial connection, set up the corresponding serial port extender (refer to *2.6.2 Setting Up the Ethernet-To-Serial Hardware*).

✧ Navigate to the page **Applications**.

✧ Open the subpage **DIGSI 4 Client**.

✧ Enable **Activate DIGSI 4 Client** so all devices defined for a DIGSI 4 connection (refer to *3.3.2 Adding Devices Manually*) are considered for data retrieval.

✧ If your Ethernet-connected devices should fetch fault records, enable **Collect fault records using the Ethernet-based DIGSI 4 Service Interface**.

✧ Select **Apply**.

3.4.4 Modbus Client

3.4.4.1 Configuring the Modbus Client

The Modbus Client is used to fetch data from devices with a built-in Modbus TCP server and transfer them via SICAM GridEdge to the external cloud platform. This includes sensors (for example, weather and process sensors like pressure, temperature, or fill levels) as well as input devices for detection of contacts, process status, limit violations or standard 20 mA/10 V analog inputs. Data can only be read from the Modbus server devices. Writing of Modbus registers in the Modbus devices is not supported.

Devices with a Modbus RTU (serial line) server can also be included using a Modbus TCP/RTU gateway.

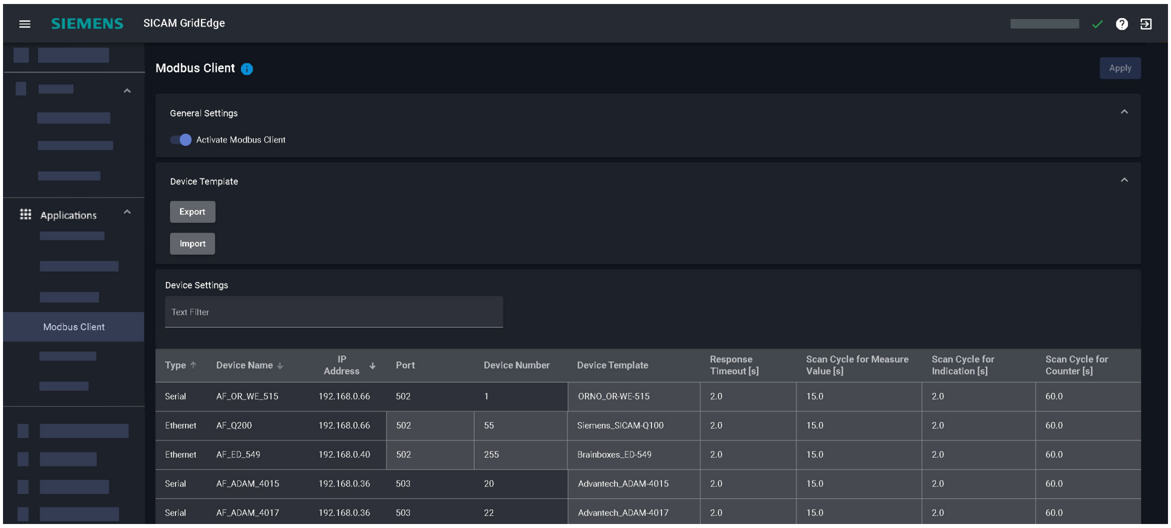
For a specification of the Modbus communication protocol refer to the Modbus user organization on *https://modbus.org*.

Supported Modbus Registers

- Coils
- Discrete Inputs (read only)
- Input Registers
- Holding Registers (read only)

Supported Modbus Functions

Function Code	Function Name
01	Read Coils
02	Read Discrete Inputs
03	Read Holding Registers
04	Read Input Registers



Type	Device Name	IP Address	Port	Device Number	Device Template	Response Timeout [s]	Scan Cycle for Measure Value [s]	Scan Cycle for Indication [s]	Scan Cycle for Counter [s]
Serial	AF_OR_WE_515	192.168.0.66	502	1	ORNO_OR-WE-515	2.0	15.0	2.0	60.0
Ethernet	AF_Q200	192.168.0.66	502	55	Siemens_SICAM-Q100	2.0	15.0	2.0	60.0
Ethernet	AF_ED_549	192.168.0.40	502	255	Brainboxes_ED-549	2.0	15.0	2.0	60.0
Serial	AF_ADAM_4015	192.168.0.36	503	20	Advantech_ADAM-4015	2.0	15.0	2.0	60.0
Serial	AF_ADAM_4017	192.168.0.36	503	22	Advantech_ADAM-4017	2.0	15.0	2.0	60.0

[sc_conf_modbus, 4, en_US]

Figure 3-8 Modbus Client

- ✧ Configure the **Ethernet Devices** (refer to *Adding Ethernet Devices, Page 28*) and assign them to the Modbus protocol.
- ✧ Configure the **Serial Devices** (refer to *Adding Serial Devices, Page 29*).

  For a serial connection, set up the corresponding Modbus TCP/RTU gateway IP address.
- ✧ Navigate to the page **Applications**.
- ✧ Open the subpage **Modbus Client**.
- ✧ Configure your **Device Settings**.
- ✧ Enable **Activate Modbus Client** so all devices defined for a Modbus connection (refer to *3.3.2 Adding Devices Manually*) are considered for data retrieval.
- ✧ Select **Apply**.

Once changes are applied, a list of request messages is created, the TCP communication is established, the data from the devices are requested cyclically and are forwarded to the cloud.

Device Settings

The discovered Modbus devices are visualized in a table format.

Column Name	Description	Default Value	Value Range
Type	Type of the connection to the Modbus device Read-only		Ethernet or Serial
Device Name	Name of the Modbus device Read-only, configurable in the subpage **Ethernet Devices** or **Serial Devices**		
IP Address	For Ethernet connection: ● IP address of the connected Modbus device ● Read-only, configurable in the subpage **Ethernet Devices** For serial connection: ● IP address of the Modbus TCP/RTU gateway ● Read-only, configurable in the subpage **Serial Devices**		

Column Name	Description	Default Value	Value Range
Port	For Ethernet connection: • TCP port number of the Modbus device For serial connection: • TCP port number of the Modbus TCP/RTU gateway • Read-only, configurable in the subpage **Serial Devices**	502	1 to 65535
Device Number	For Ethernet connection: • Unique Modbus server device address/Unit identifier of the Modbus device For serial connection: • Unique Modbus server device address/Unit identifier of the Modbus device connected to the Modbus TCP/RTU gateway • Read-only, configurable in the subpage **Serial Devices**	1	1 to 247 and 255
Device Template	Configured device template for the Modbus device	–	Template name (select from loaded templates)
Response Timeout	Time limit until the Modbus server must response to a request from the Modbus client	2.0	0.1 s to 60.0 s (100 ms to 1 min in 0.1 s steps, i.e. with one fractional digit)
Scan Cycle for Measure Values	Minimum time differences on Modbus communication side between the requests for data of the individual data types The assignments of the information in the Modbus registers of a Modbus device to the data types is done in the associated device template The transmission cycle of the data to the cloud platform can differ from the scan cycles on Modbus side	10.0	0.5 s to 3600.0 s (500 ms to 1 h in 0.1 s steps, i.e. with one fractional digit)
Scan Cycle for Indications		2.0	
Scan Cycles for Counter		60.0	

Additionally, some settings are fixed and are listed for information only:

Setting Name	Description	Value
Retry Limit	Number of request-retries after exceeding the response timeout until the Modbus server device is reported as disconnected	2
Scan Cycle on Error	Retry cycle for sending request telegrams to a Modbus device in case the Modbus device does not response to requests from the Modbus client (e.g., if the Modbus device is disconnected)	30 s
TcpKeepAliveEnabled	State of the TCP KeepAlive enabled	True
TcpKeepAliveInterval	Number of seconds a TCP connection will remain idle before the first TCP KeepAlive probe is sent to the remote	20

Setting Name	Description	Value
TcpKeepAliveInterval	Number of seconds a TCP connection will wait for a TCP KeepAlive response before sending another probe	5
TcpKeepAliveRetryCount	Amount of TCP KeepAlive probes with no response that will be sent before the connection is terminated	3

Device Template

Device Template allows you to communicate to any Modbus device from the SICAM GridEdge. A device template contains all required mapping information for reading individual data from the Modbus device and converts them to data points that can be sent to the cloud service.

The template file is a CSV file with the following CSV definitions:

- Column delimiter is a semicolon (“;”)
- Decimal delimiter for floating-point number is a dot (“.”)
- Rows that start with a hash character (“#”) are interpreted as comments and are ignored

NOTE

For more information and examples, refer to the public Github repository *https://github.com/siemens/sicam-gridedge-configurationtemplates*.

Example:

```
# Siemens SICAM Q100: Class A Power Quality Instrument and Power Monitoring
Device
#
DataObjectName;Activated;RegisterType;RegisterNumber;DataType;Unit;DataFormatOnB
us;BitOffset;ScalingFactor;ScalingOffset
#
# Device Status Indications
Device_OK;1;Holding;101;Indication;;1Bit;0;
Battery_failure;1;Holding;101;Indication;;1Bit;2;
#
# Measured Values (Instantaneous Values)
Va;1;Holding;201;MV;V;Float32;;1;0
Vb;1;Holding;203;MV;V;Float32;;1;0
Vc;1;Holding;205;MV;V;Float32;;1;0
VN;0;Holding;207;MV;V;Float32;;1;0
```

In the example, the mappings for six data points, 2 indications and 4 measured values are described. However, only 3 of the measured values will be requested from the Modbus device because the data object “VN” is configured to be not activated.

Column Name	Range	Description
DataObjectName	• String, min. 1 and max. 128 characters • All characters are allowed including slash (/) and backslash (\). • Data object names must be unique within a Modbus device. • Data object name cannot start with a slash or a backslash. • Data object name cannot end with a slash or a backslash. • Slash and backslash characters represent a hierarchy. • The data object name includes a maximum of 2 hierarchy parts, e.g., hierarchyPart1/hierarchyPart2/dataObjectName	Name of a data object that shall be read via Modbus
Activated	0 or false: no other than 0 or true: yes	Determines whether the data object shall be read by Modbus, evaluated, and transmitted to the cloud platform. The entries in the device template can contain the full amount of data that are offered from the device but not all might be of interest for further processing
RegisterType	One of the following strings (not case sensitive): • CoilStatus or Coils or 0 • InputStatus or DiscreteInputs or 1 • Input or InputRegisters or 3 • Holding or HoldingRegisters or 4	Register type to read from
RegisterNumber	1 to 65535	Start register number of the data object in the register type
DataType	One of the following strings (not case sensitive): • SPS or Indication • MV • Counter • Border	Type of the data object that corresponds to type to the cloud platform. For more information on the data type **Border**, see below.
Unit	A Measuring Unit string, e.g. V, A, kV, degC, %H, hPa (max. 64 characters)	Measuring Unit • for measured values and counters only • for transmission to the cloud
DataFormatOnBus	Refer to *Data Formats on Bus, Page 46*	Format of transmitting the data object via Modbus

Column Name	Range	Description
BitOffset	0 to 15	Only for indications transmitted in an input or holding register. Offset of the indication in this register
ScalingFactor	Any floating-point value	Factor with which the read value from Modbus is multiplied before transmitting to the cloud platform
ScalingOffset	Any floating-point value	Numeric value with which the read value from Modbus is added before transmitting to the cloud platform

For measured values and counters the resulting value is calculated by: ResultingValue = (ReadValue * ScalingFactor) + ScalingOffset

Data type **Border**: In case the Modbus client requests data from a Modbus server device that are in the same register but do not follow each other directly, the Modbus client reads not needed data between the requested registers.The aim is to optimize request calls.

Example: The Modbus client requests an Int16 MV1 from the holding register 101 as well as an Int16 MV2 from the holding register 109. In this case, one request telegram is sent requesting all registers from 101 to 109. However, only the registers 101 and 109 for the MV1 and MV2 are evaluated.

Depending on the implementation in the Modbus server and the data mapping for the device, this could lead to a Modbus exception response as the registers between the requested ones cannot be mapped. In this case, a Border entry has to be included in the device template so that the requests are split in 2 separate telegrams. After the mapping entry for MV1, a line must be entered. This results in one request being sent for MV1 and one request being sent for MV2.

```
Border1;1;Holding;102;Border;;;;;
```

Data Formats on Bus

Data from Modbus devices with the following Data Formats on Bus can be interpreted by the Modbus Client in GridEdge:

DataTypeOnBus	Data Format Description	Range	Invalid Sign	Used Modbus Registers	Data Type in Cloud
1 Bit	1 bit in a bit register	1 = On 0 = Off	no	1 (Coil or Discrete Input)	Indication (single-point), Events
1 Bit + BitOffset	1 bit in a word register	1 = On 0 = Off	no	1/16 (Input or Holding registers)	Indication (single-point), Events
Float32	IEEE 32-bit Floating-point number, Big endian[1]	-10^{38} to +10^{38}	NaN = invalid INF = overflow	2 (Input or Holding registers)	Measured value, Timeseries
Float32_LE	IEEE 32-bit Floating-point number, Little endian[2]	-10^{38} to +10^{38}	NaN = invalid INF = overflow	2 (Input or Holding registers)	Measured value, Timeseries
Int16	16-bit signed integer	-32768 to +32767	no	1 (Input or Holding register)	Measured value, Timeseries
Int16Inv80	16-bit signed integer	-32768 to +32767	-32768 (0x8000) = invalid	1 (Input or Holding register)	Measured value, Timeseries

[1] Big endian: The most significant byte of the value is contained in the Modbus register that is read first.

[2] Little endian: The least significant byte of the value is contained in the Modbus register that is read first.

DataTypeOnBus	Data Format Description	Range	Invalid Sign	Used Modbus Registers	Data Type in Cloud
Uint16	16-bit unsigned integer	0 to +65535	no	1 (Input or Holding register)	Measured value, Timeseries
Int32	32-bit signed integer, Big endian	-2147483648 to 2147483647	no	2 (Input or Holding registers)	Measured value or Counter, Timeseries
Int32_LE	32-bit signed integer, Little endian	-2147483648 to 2147483647	no	2 (Input or Holding registers)	Measured value or Counter, Timeseries
UInt32	32-bit unsigned integer, Big endian	0 to +4294967295	no	2 (Input or Holding registers)	Measured value or Counter, Timeseries
UInt32_LE	32-bit unsigned integer, Little endian	0 to +4294967295	no	2 (Input or Holding registers)	Measured value or Counter, Timeseries

Device Template

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

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

Import: A newly created or modified Modbus device template can be imported to the SICAM GridEdge system. After successful import, the device template will be available for the assignment. The syntax of the device template is checked during the import. In case of an error an error message is issued and a list with the error description is provided.

Data Transfer to the Cloud

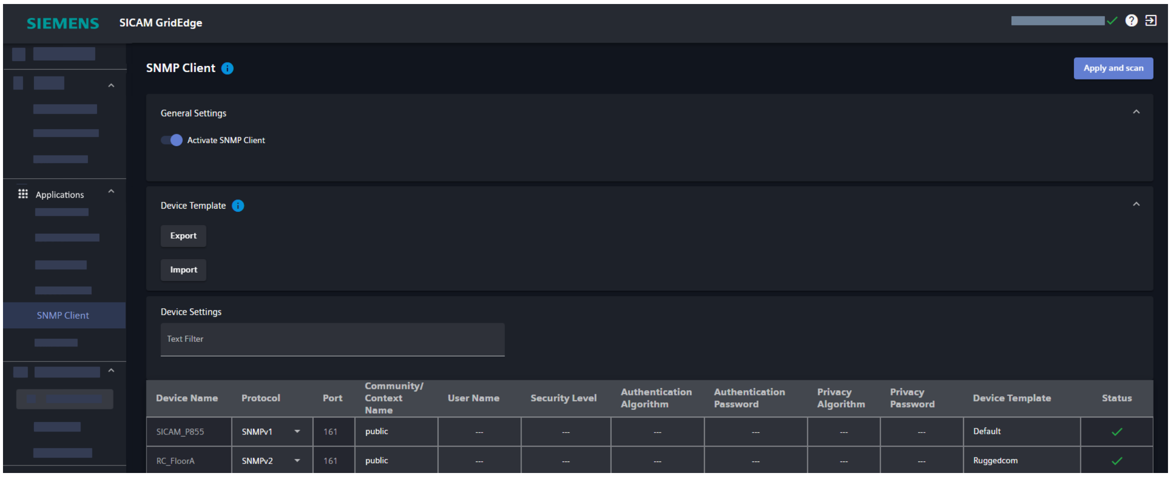
Independently of the Modbus data points defined in the device templates, the indication **Modbus$ST$ChLiv** (Channel Live) is always automatically added for every Modbus device for transmission to the cloud. This indication shows the status of the connection to the Modbus device (false: offline, true: online).

3.4.5 SNMP Client

3.4.5.1 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.

If **Activate SNMP Client** is enabled, all devices defined for an SNMP connection are considered for data retrieval.



SNMP Client

General Settings

Activate SNMP Client

Device Template

Device Settings

Device Name	Protocol	Port	Community/ Context Name	User Name	Security Level	Authentication Algorithm	Authentication Password	Privacy Algorithm	Privacy Password	Device Template	Status
SICAM_P855	SNMPv1	161	public	—	—	—	—	—	—	Default	✓
RC_FloorA	SNMPv2	161	public	—	—	—	—	—	—	Ruggedcom	✓

[sc_conf_snmp, 7, en_US]

Figure 3-9 SNMP Client

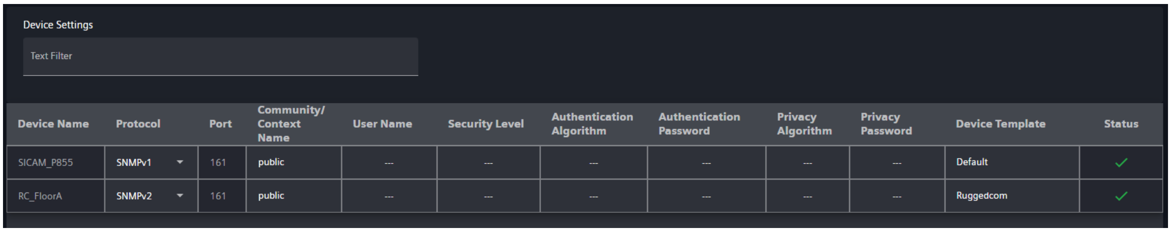
- ✧ Add the SNMP devices (refer to *3.3.1 Adding Ethernet Devices Automatically* or *3.3.2 Adding Devices Manually*).
- ✧ Navigate to the page **Applications**.
- ✧ Open the subpage **SNMP Client**.
- ✧ Enable **Activate SNMP Client**.

All detected SNMP devices are listed.

- ✧ Configure your **Device Settings**.
- ✧ Select **Apply and scan**.

Device Settings

The devices configured for SNMP that are available in the page **Ethernet devices** are visualized in table format.



Device Settings

Device Name	Protocol	Port	Community/ Context Name	User Name	Security Level	Authentication Algorithm	Authentication Password	Privacy Algorithm	Privacy Password	Device Template	Status
SICAM_P855	SNMPv1	161	public	—	—	—	—	—	—	Default	✓
RC_FloorA	SNMPv2	161	public	—	—	—	—	—	—	Ruggedcom	✓

[sc_conf_snmp_table, 3, en_US]

Column Name	Description	Configurable Parameter[3]
Device Name	Name 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	✓

[3] For configurable parameters, user input is required

Column Name	Description	Configurable Parameter[3]
Security Level	Configured security level for SNMP device (Supported by SNMPv3 Protocol devices)	✓
Authentication Algorithm	Configured authentication algorithm for SNMP device (Supported by SNMPv3 Protocol devices)	✓
Authentication Password	Configured authentication password for the SNMP device (Supported by SNMPv3 Protocol devices)	✓
Privacy Algorithm	Configured privacy algorithm for SNMP device (Supported by SNMPv3 Protocol devices)	–
Privacy Password	Configured privacy password for the SNMP device (Supported by SNMPv3 Protocol devices)	✓
Device Template	Configured device template for the SNMP device	✓
Configuration Status	Status of the device Possible values are Valid, Invalid, and Pending: • 🟩 Valid Device settings are configured successfully • 🟥 Invalid Device is discovered, but missing/invalid device configuration settings • 🟨 Pending 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 SNMP device from SICAM GridEdge. 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 delimited with a semicolon (";"). It contains 1 line per asset information in the following format:

```
Name;Address;Type;DefaultValue;Mapping
```

Template Column Name	Description
Name	Attribute name of the asset
Address	For every attribute name, there is a communication address (OID) used to read the asset information from the SNMP device. If kept empty, the asset information value configured under DefaultValue is used in the asset information file
Type	Type used to define the number of values fetched from the device • Single: A single value is fetched from the device. Used if an information is available at the given communication address (OID) • Multiple: Multiple values are fechted from the device. Used if information is available in a SNMP table column (refer to DG Product Inventory MIB for an example)

[3] For configurable parameters, user input is required

Template Column Name	Description
DefaultValue	Value used as the default value of the device attribute if no information is available at the given communication address (OID) or if the address is empty
Mapping	Target location where the attribute value will be located in the SICAM GridEdge asset information file structure

NOTE

Siemens provides several SNMP templates. The provided templates help you to create your own template.

- If you want to create different templates for devices of the same family, use the provided template of the same device family as a reference.
- If no device-specific template applies, use the provided default template as a reference.
- If your device is based on a DG Product Inventory MIB file structure, use the provided SICAM A8000 template as a reference.

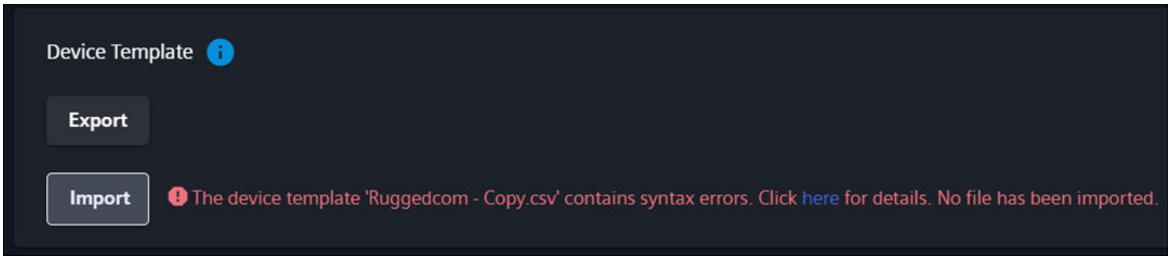
NOTE

For more information and examples, refer to the public Github repository *https://github.com/siemens/sicam-gridedge-configurationtemplates*.

Example: Default Device Template

```
Name;Address;Type;DefaultValue;Mapping
VendorName;;Single;Siemens;VendorName
DeviceName;1.3.6.1.2.1.1.5.0;Single;SNMPDevice;HwProduct.0/ProdCompName
Location;1.3.6.1.2.1.1.6.0;Single;;LocationName
HardwareId;;Single;;AssetUuid
DeviceFamily;;Single;Default;DeviceFamily
DeviceModel;;Single;;DeviceModel
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.



The device template 'Ruggedcom - Copy.csv' contains syntax errors. Click here for details. No file has been imported.

[sc_device_template_import-export, 1, en_US]

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

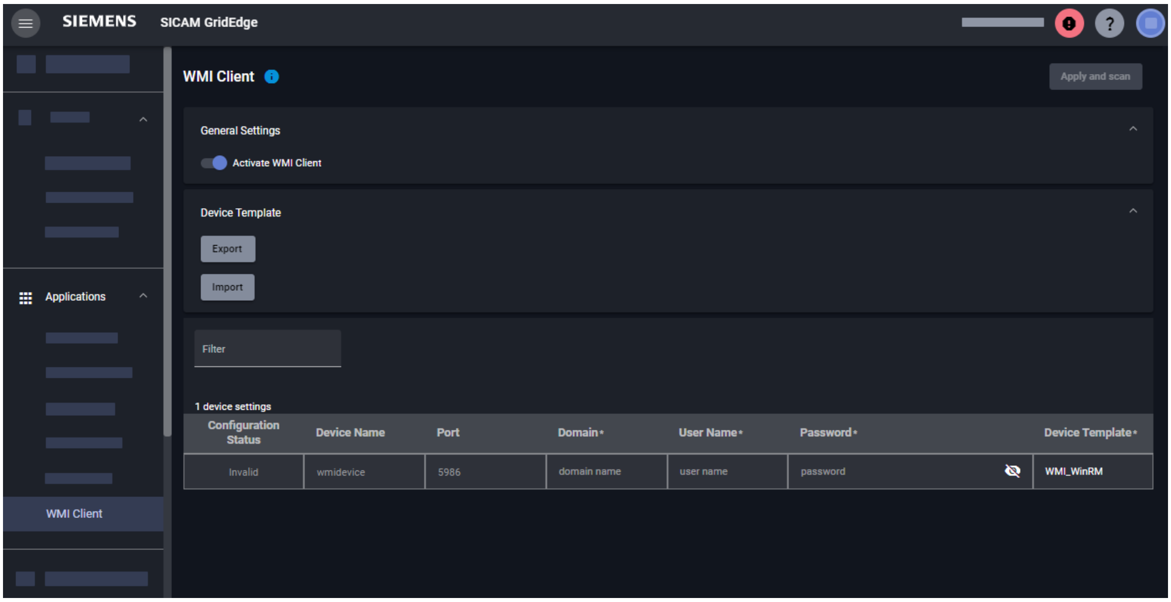
Import: A newly created or modified device template can be imported to the SICAM GridEdge system. After successful import, the device template will be available for the assignment.

3.4.6 WMI Client

3.4.6.1 Configuring the WMI Client

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

If **Activate WMI Client** is enabled, all devices defined for a WMI connection are considered for data retrieval.



WMI Client

General Settings

Activate WMI Client

Device Template

1 device settings

Configuration Status	Device Name	Port	Domain*	User Name*	Password*	Device Template*
Invalid	wmidevice	5986	domain name	user name	password	WMI_WinRM

[sc_wmi_client, 6, en_US]

Figure 3-10 WMI Client

- ✧ Add the WMI devices (refer to *3.3.1 Adding Ethernet Devices Automatically* or *3.3.2 Adding Devices Manually*).
- ✧ Navigate to the page **Applications**.
- ✧ Open the subpage **WMI Client**.
- ✧ Enable **Activate WMI Client**.

All detected WMI devices are listed.

- ✧ Make your **Device Settings**.
- ✧ Select **Apply and scan**.

Device Settings

The devices configured for WMI that are available in the page **Ethernet devices** are visualized in table format.

Column Name	Description	Configurable Parameter[4]
Device Name	Name of the WMI device	–
Port	Configured port for the WMI communication	✓
Domain	Configured domain for the WMI device **NOTE** For local networks where the domain is not available, the computer name has to be entered here.	✓

[4] For configurable parameters, user input is required

Column Name	Description	Configurable Parameter[4]
User Name	Configured user name for the WMI device	✓
Password	Configured password for the WMI device	✓
Device Template	Configured device template for the WMI device	✓
Configuration Status	Status of the device Possible values are Valid, Invalid and Pending • 🟩 Valid Device settings are configured successfully • 🟥 Invalid Device is discovered but missing/invalid device configuration settings • 🟨 Pending Modified configuration settings are not applied yet	–

Device Template

Device Template allows you to communicate to any WMI device from SICAM GridEdge. 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 delimited with a semicolon. It contains one line per asset information in the following format:

```
Name;Address;Type;DefaultValue;Mapping
```

NOTE

For more information and examples, refer to the public Github repository *https://github.com/siemens/sicam-gridedge-configurationtemplates*.

Example: Default Device Template

```
Name;Address;Type;DefaultValue;Mapping
PCVendor;computersystem get manufacturer;Single;;VendorName
MACAddress;nicconfig
get caption,description,macaddress,ipaddress;Single;;NetworkComponent.0/
ProdNetworkCompMACAddr
DeviceName;computersystem get name;Single;;HwProduct/ProdCompName
DeviceFamily;computersystem get systemtype;Single;Windows;DeviceFamily
DeviceModel;computersystem get model;Single;;DeviceModel
SerialNumber;bios get serialnumber;Single;;HwProduct/ProdCompSerialNumber
OSVersion;os get version;Single;;FwSwComponent.0/ProdCompVersion
OSName;os get name;Single;;FwSwComponent.0/ProdCompName
OSVendor;os get manufacturer;Single;;FwSwComponent.0/ProdCompVendorName
SwVendor;product where \"Vendor like '%Siemens%' or Name like '%.net
runtime%'\" get vendor;Multiple;;FwSwComponent.1/ProdCompVendorName
SwVersion;product where \"Vendor like '%Siemens%' or Name like '%.net
runtime%'\" get version;Multiple;;FwSwComponent.1/ProdCompVersion
SwName;product where \"Vendor like '%Siemens%' or Name like '%.net runtime%'\"
get name;Multiple;;FwSwComponent.1/ProdCompName
WindowsPatchVersion; qfe get hotfixid;Multiple;;FwSwComponent.2/ProdCompVersion
WindowsPatchName; qfe get description;Multiple;;FwSwComponent.2/ProdCompName
```

[4] For configurable parameters, user input is required

3.4.6.2 Collecting Data from Microsoft Windows Computers

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

NOTE

WinRM stand for Microsoft Windows Remote Management. For more information, refer to *https://learn.microsoft.com/en-us/windows/win32/winrm/portal*.

3.4.6.3 Setting Up WinRM for Microsoft Windows for HTTPS

For more information, refer to the official Microsoft documentation.

NOTE

If you upgrade SICAM GridEdge from a version lower than V2.12 and configured the WMI client with user-defined templates, these templates must be manually converted for Microsoft WinRM.

- Create a self-signed certificate.
- Start the Microsoft WinRM service:

  ```
  Start-Service WinRM
  ```

- Fill in the hostname and the certificate thumbprint in the command. Enable the Microsoft WinRM listener for HTTPS (port 5986):

  ```
  winrm create winrm/config/Listener?Address=*+Transport=HTTPS
  '@{Hostname="Hostname";CertificateThumbprint="CertificateThumbprint"}'
  ```

- Open the port 5986:

  ```
  New-NetFirewallRule -Name "WinRM-HTTPS-In" -DisplayName "WinRM-HTTPS-In"
  -Enabled True -Direction Inbound -Protocol TCP -LocalPort 5986
  ```

- Allow basic Microsoft WinRM authentication:

  ```
  winrm set winrm/config/service/auth '@{Basic="true"}'
  ```

- Enable the PowerShell Remoting:

  ```
  Enable-PSRemoting -Force
  ```

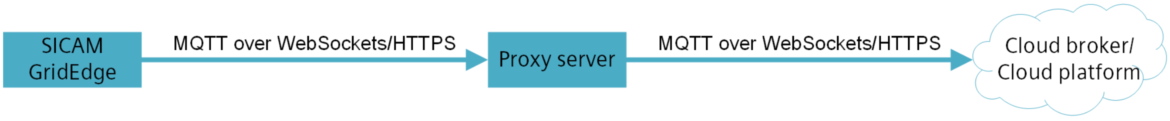
Microsoft WinRM for HTTPS is set up on your Microsoft Windows machine.

Remote management of your system is possible using PowerShell commands.

3.5 Cloud Connection Configuration

3.5.1 Configuring a Connection via a Proxy Server

If a proxy server is integrated in your network configuration, a connection between SICAM GridEdge and the proxy server must be established. Only if connected, SICAM GridEdge can transfer data to the cloud platform.


SICAM GridEdge
MQTT over WebSockets/HTTPS
Proxy server
MQTT over WebSockets/HTTPS
Cloud broker/ Cloud platform

[ge_proxy_configuration, 1, de_DE]

NOTE

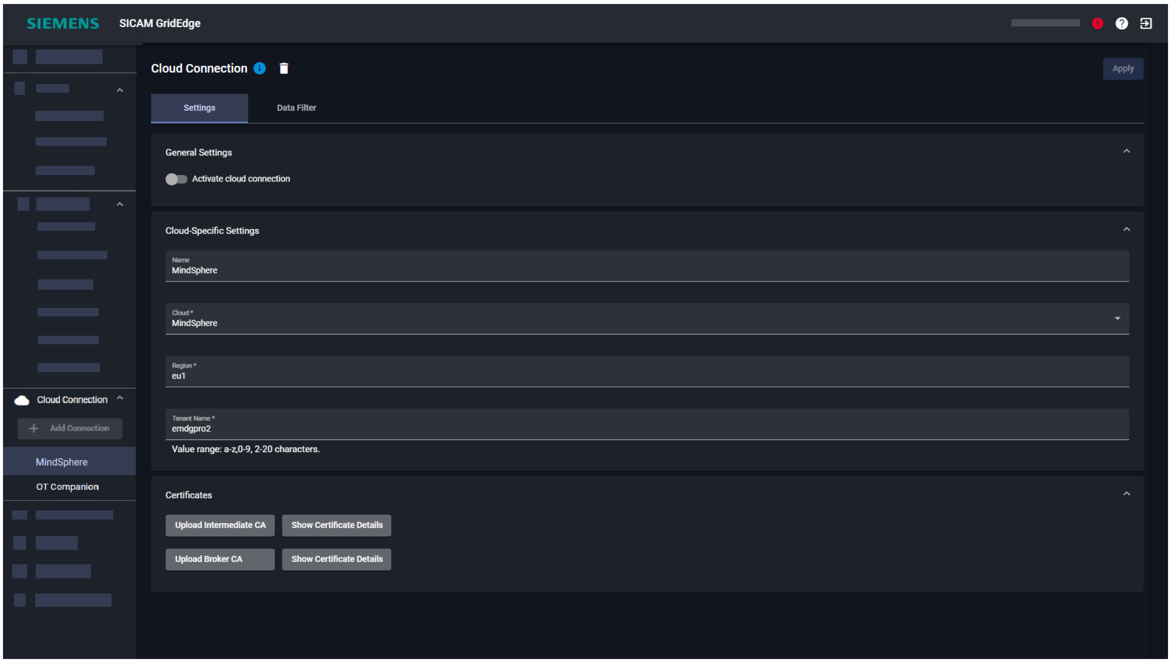
The configuration of a proxy server is not available for the Mindsphere OPC UA PubSub cloud connection.

- ✧ Open the page **Station Settings**.
- ✧ Enable **Use Proxy**.
- ✧ Enter the host address and the port number of the proxy server.
- ✧ If needed, enter the user name and passwort for the proxy server. Whether these settings are optional, depends on your network configuration.
- ✧ Enable the MQTT over WebSocket option in the cloud connection page.

The connection to the proxy server is established.
SICAM GridEdge can transfer data via the proxy server to the cloud platform.

3.5.2 Configuring the Cloud Connection

You can configure up to 2 cloud connections. Each cloud connection has to be configured individually.



General Settings

Activate cloud connection

Cloud-Specific Settings

Name: MindSphere

Cloud *: MindSphere

Region *: eu1

Tenant Name *: emdgpro2

Value range: a-z,0-9, 2-20 characters.

Certificates

[sc_SICAM_GridEdge_Cloud_connection, 10, en_US]

Figure 3-11 Cloud Connection

- ✧ Navigate to the page **Cloud Connection**.

A list of all connections is displayed underneath **Cloud Connection**.

- ✧ Choose the cloud connection you want to configure.
- ✧ Open the tab **Settings**.
- ✧ Enable **Activate cloud connection**.
- ✧ Enter a unique name for the cloud connection.
- ✧ From the page **Cloud Connection**, select the subpage of the cloud platform you want to send data to. Depending on the option you will have to choose different settings.
- ✧ Make the cloud-specific configurations (refer to *3.5.3 Configuring Cloud-Specific Settings*).

Uploading Certificates

For further information on certificate handling, refer to *5.9.2 Connection between Devices and Cloud Platform*.

✧ To upload a (intermediate) certificate authority in a PKCS#12 container format, select **Upload Intermediate CA**.

✧ If your PKCS#12 container is encrypted with a password, enter the password in the import dialog.

- or -

✧ If your PKCS#12 file is not encrypted, leave the corresponding field empty.

✧ Select **Open**.

NOTE

To publish data to the Microsoft Azure cloud platform, SICAM GridEdge communicates with the cloud service Microsoft Azure IoT Hub and Device Provisioning Service (DPS). To establish a connection to both services, both certificates must be uploaded to SICAM GridEdge.

For more information, refer to the official Microsoft documentation.

✧ If you use Microsoft Azure as a cloud platform, select **Upload DPS CA** and choose the certificate authority for the Azure IoT Hub Device Provisioning Service (DPS).

✧ If you use Microsoft Azure as a cloud platform, select **Upload IoT Hub CA** and choose the certificate authority for the Microsoft Azure IoT Hub.

- or -

✧ If you don't use Microsoft Azure as a cloud platform, select **Upload Broker CA** and choose the certificate authority of the broker to which the data will be sent to.

✧ Select **Apply**.

NOTE

If you use MindSphere as a cloud platform, refer to the IoT Engineering Guide for more information about the required certificates (*MindSphere IoT Engineering Guide*).

Uploading an Onboarding Key (MindConnectLib)

To establish a connection to MindSphere via MindConnectLib, an onboarding key must be uploaded to SICAM GridEdge.

✧ In the **Asset Manager** of MindSphere, create an asset of the type MindConnectLib.

✧ Open the MindConnectLib settings of the created asset.

✧ Create an onboarding key of the security type SHARED_SECRET.

✧ Copy the generated text of the onboarding key to a .JSON file.

✧ In the page **Cloud Connection** for the MindConnectLib connection, select **Upload**.

✧ Upload the .JSON file as the onboarding key.

The tenant name is filled in automatically.

✧ Select **Apply**.

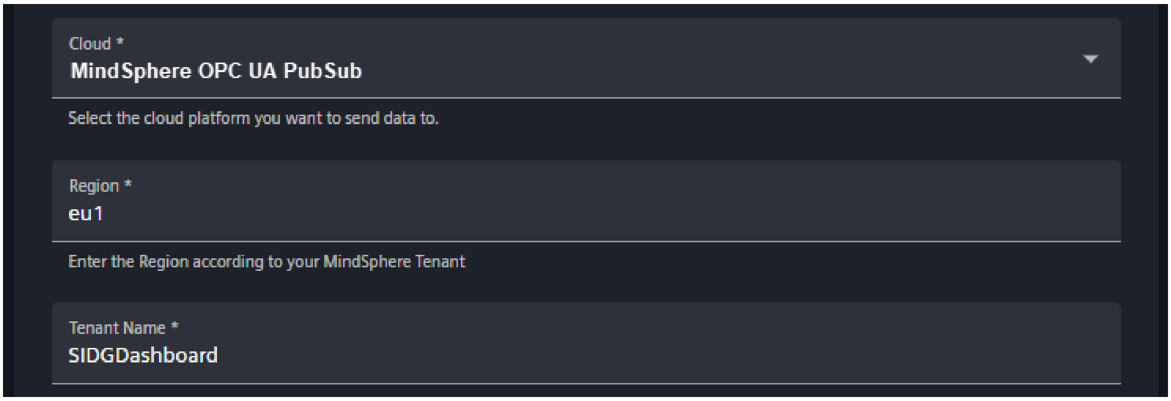
The connection is only established after a data point mapping is defined and at least one data point was transferred (refer to *3.5.5 Configuring the MindConnectLib Data Point Mapping*).

3.5.3 Configuring Cloud-Specific Settings

3.5.3.1 Configuring a Mindsphere OPC UA PubSub Connection

NOTE

The OPC UA PubSub format is used for the binary encoding of the data to be transmitted to the cloud platform. You can use the following client implementation as a reference:
https://github.com/siemens/opc-ua-pubsub-dotnet



Cloud *
MindSphere OPC UA PubSub
Select the cloud platform you want to send data to.

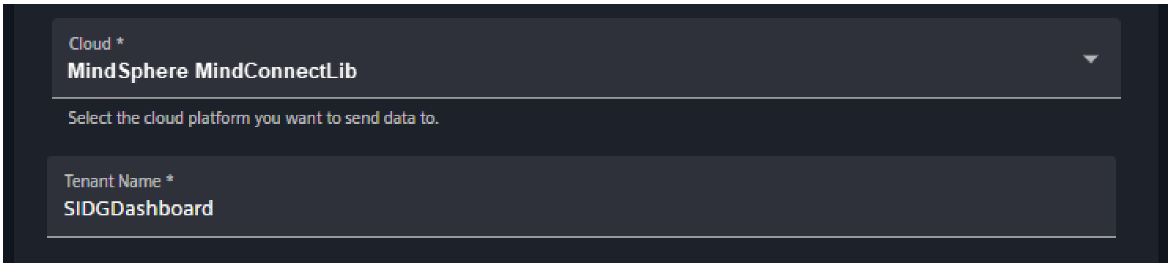
Region *
eu1
Enter the Region according to your MindSphere Tenant

Tenant Name *
SIDGDashboard

[sc_mindsphere_spec, 4, en_US]

✧ 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.

3.5.3.2 Configuring a Mindsphere MindConnectLib Connection



Cloud *
MindSphere MindConnectLib
Select the cloud platform you want to send data to.

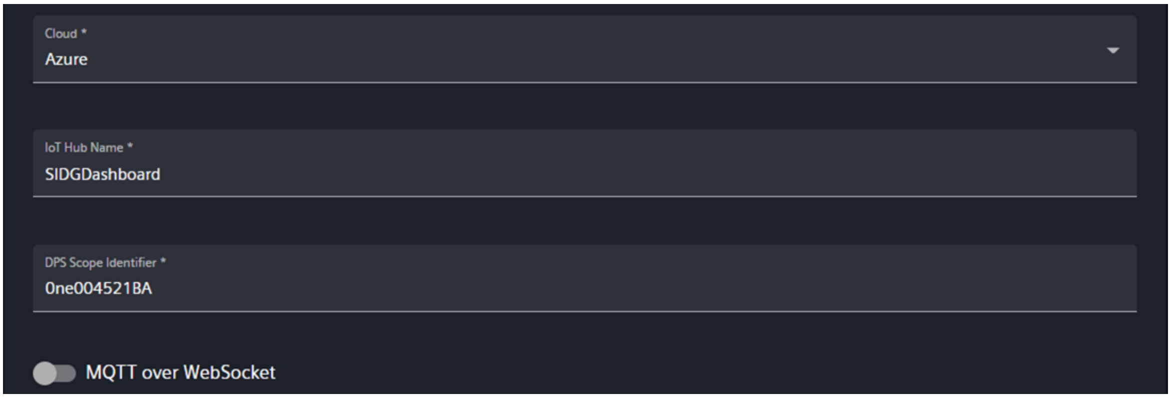
Tenant Name *
SIDGDashboard

[sc_mindsphere_mindconnectlib, 1, en_US]

✧ Upload an onboarding key of MindSphere (refer to *3.5.2 Configuring the Cloud Connection*).

The tenant name is automatically taken from the onboarding key information.

3.5.3.3 Configuring a Microsoft Azure Connection



Cloud *
Azure

IoT Hub Name *
SIDGDashboard

DPS Scope Identifier *
0ne004521BA

MQTT over WebSocket

[sc_azure_spec, 4, en_US]

✧ Enter the **IoT Hub Name** according to your configuration visible in the Microsoft Azure portal.

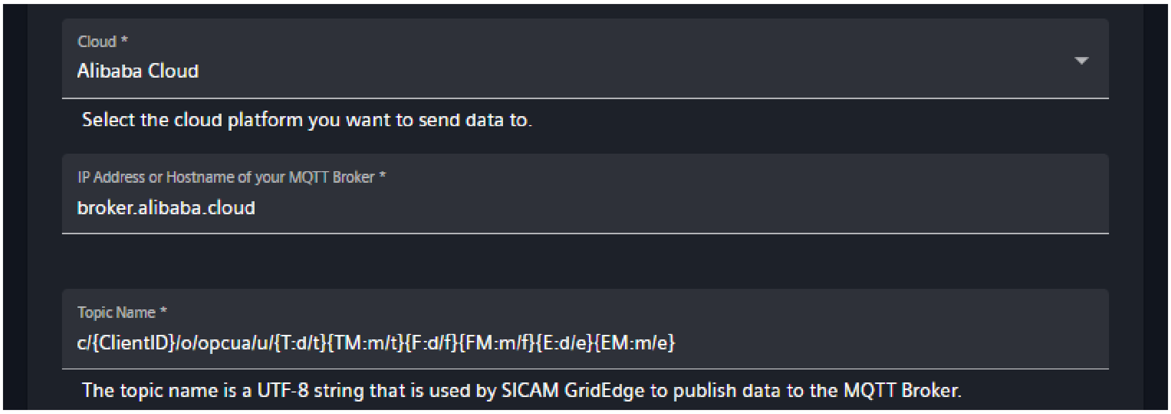
✧ Enter the **DPS Scope Identifier** (Device Provisioning Service) according to your configuration in the Microsoft Azure portal.

✧ 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).

3.5.3.4 Configuring an Alibaba Connection

NOTE

The OPC UA PubSub format is used for the binary encoding of the data to be transmitted to the cloud platform. You can use the following client implementation as a reference:
https://github.com/siemens/opc-ua-pubsub-dotnet



Cloud *
Alibaba Cloud

Select the cloud platform you want to send data to.

IP Address or Hostname of your MQTT Broker *
broker.alibaba.cloud

Topic Name *
c/{ClientID}/o/opcua/u/{T:d/t}{TM:m/t}{F:d/f}{FM:m/f}{E:d/e}{EM:m/e}

The topic name is a UTF-8 string that is used by SICAM GridEdge to publish data to the MQTT Broker.

[sc_alibaba_spec, 2, en_US]

✧ Enter the **IP Address or Hostname** of your MQTT Broker running on Alibaba Cloud.

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

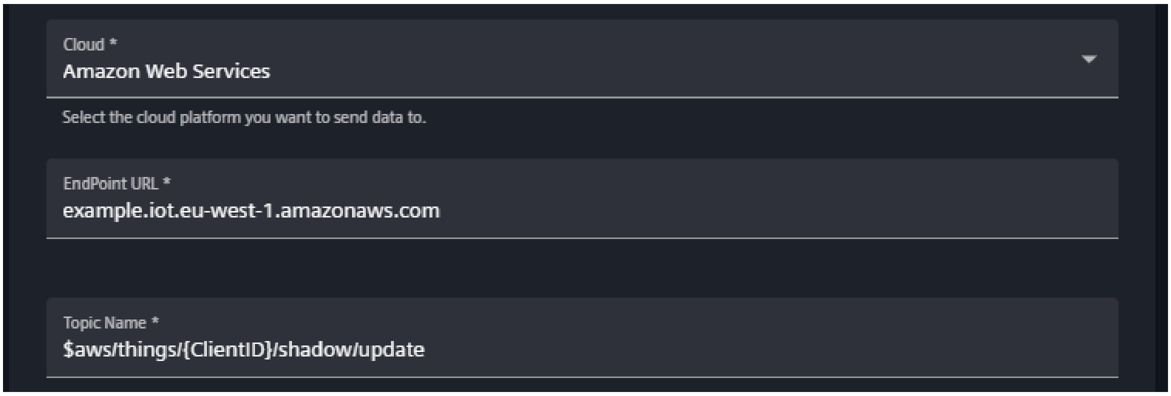
NOTE

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

Examples with GridEdge/{ClientID} and Client ID = "Q100_7KG95_GF1609500232":
Resulting topic name: **GridEdge/Q100_7KG95_GF1609500232**

3.5.3.5 Configuring an Amazon Web Services Connection



Cloud *
Amazon Web Services

Select the cloud platform you want to send data to.

EndPoint URL *
example.iot.eu-west-1.amazonaws.com

Topic Name *
$aws/things/{ClientID}/shadow/update

[sc_aws_spec, 2, en_US]

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

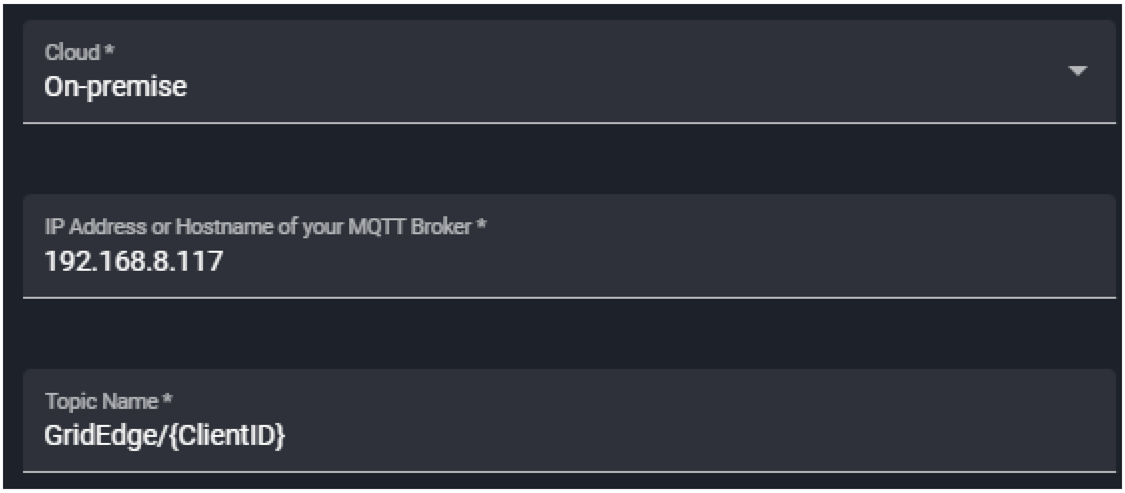
✧ Enter the **Topic Name** for which you want to publish data.

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

3.5.3.6 Configuring an On-Premise Connection



Cloud *
On-premise

IP Address or Hostname of your MQTT Broker *
192.168.8.117

Topic Name *
GridEdge/{ClientID}

[sc_on-premise_spec, 4, 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.

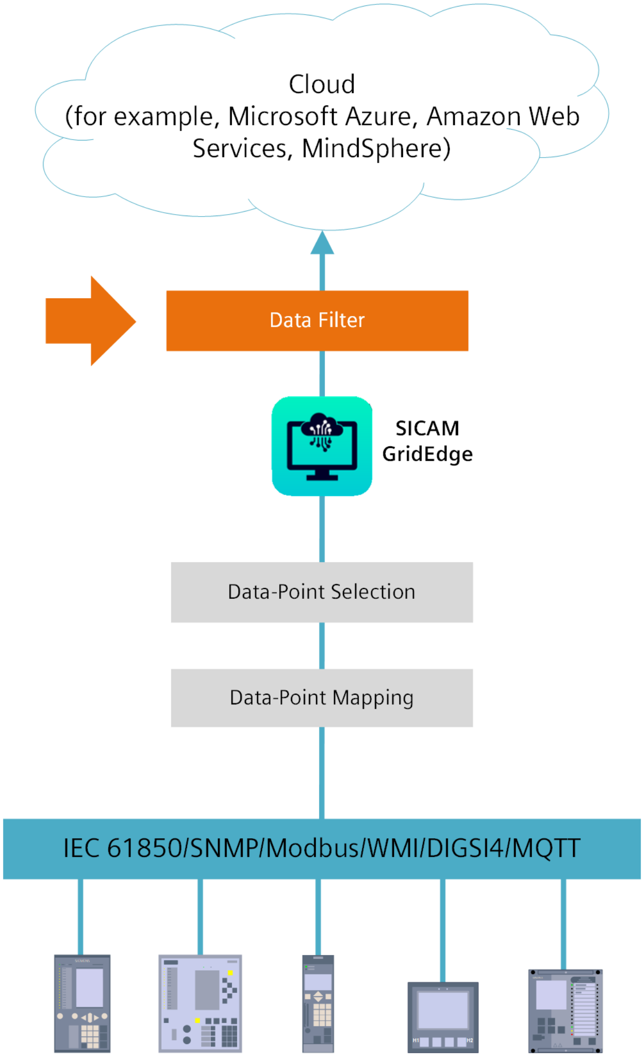
- {ClientID}: Is replaced by the Publisher ID of the device

3.5.4 Configuring the Data Filter

NOTE

Only data collected from the IEC 61850 Client and the Modbus Client will be shown in the page **Data Filter**. If no data selection or profile has been configured in the protocol applications, no data points are shown.

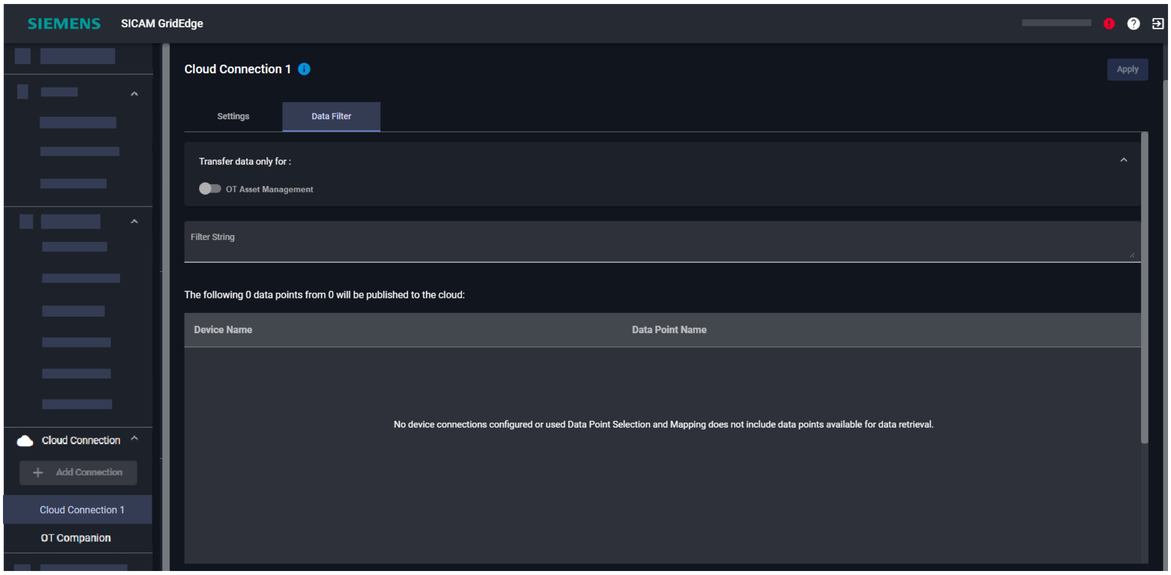
In the tab **Data Filter** of the page **Cloud Connection**, you can optionally enter a filter string to filter which data is to be transmitted to the external cloud platform.


Cloud
(for example, Microsoft Azure, Amazon Web Services, MindSphere)
Data Filter
SICAM GridEdge
Data-Point Selection
Data-Point Mapping
IEC 61850/SNMP/Modbus/WMI/DIGSI4/MQTT

[dw_data_filter, 4, 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:



The following 0 data points from 0 will be published to the cloud:

Device Name	Data Point Name

No device connections configured or used Data Point Selection and Mapping does not include data points available for data retrieval.

[sc_SICAM_GridEdge_data_filter, 8, en_US]

Figure 3-12 Data Filter

- ✧ Navigate to the page **Cloud Connection**.
  A list of all connections is displayed underneath **Cloud Connection**.
- ✧ Choose the cloud connection for which you want to configure the data filter.
- ✧ Open the tab **Data Filter**.
- ✧ If you send data only to an OT Asset Management application, enable **OT Asset Management**.

  Only events and needed files (AssetInfo, diagnosis, protection settings) are transferred to the cloud platform.
- ✧ 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.

3.5.5 Configuring the MindConnectLib Data Point Mapping

To establish a connection to MindSphere via MindConnectLib, data points must be mapped manually.

You must have uploaded an onboarding key of MindSphere (refer to *Uploading an Onboarding Key (MindConnectLib), Page 55*).

- ✧ Open the page **Cloud Connection** for your MindConnectLib connection.
- ✧ Open the tab **MindConnectLib**.
- ✧ For each data point, select the correct signal type in the list box **TI**.
  The types TI30, TI31 and TI36 are supported.
- ✧ Enter the process-technical address of the data point in the text box **PDA**.
  For more information, refer to the NXpower Monitor documentation.
- ✧ Enter the correct unit of the data point in the text box **Unit**.

✧ Select **Apply**.

NOTE

The data points in SICAM GridEdge must be manually exported and afterwards imported and mapped in MindSphere.

✧ To export the mapping file, select the icon ⤓.

The data point mapping is exported as a CSV file.

✧ Import the data point mapping file in the **Asset Manager** of MindSphere.

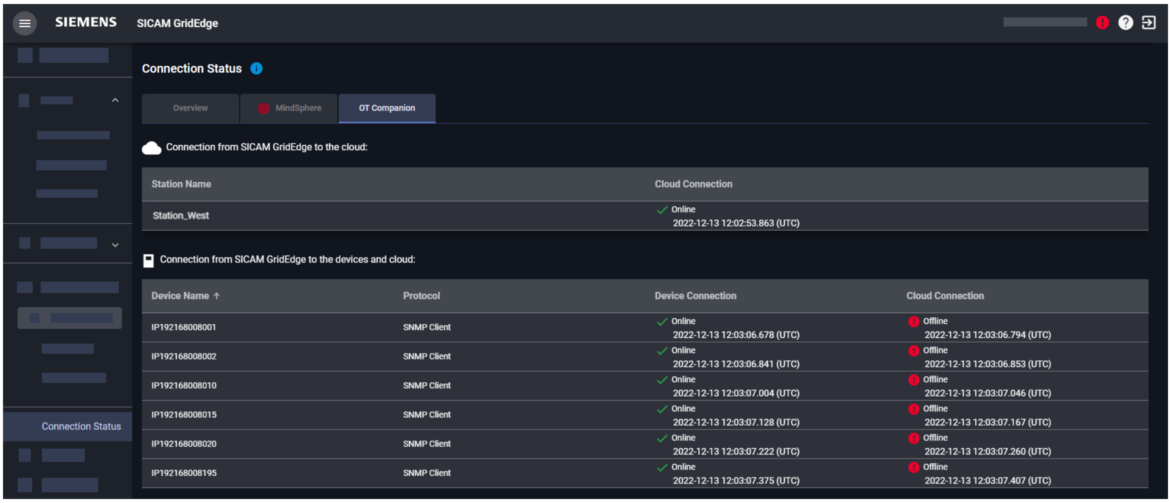
✧ Manually map the data points in the **Asset Manager**.
For more information, refer to the MindSphere documentation.

4 Diagnosis/Runtime

4.1 Connection Status

You can easily check the connection status for all devices to all configured cloud platforms and to the devices themselves.
On the tab **Overview**, you can see a graphical representation of the status of all cloud connections and all device connections.
In addition, the status of each cloud connection is displayed in detailed in an individual tab.
The individual tab is structured the following columns:

- Device Name: This is the device name which is used to transfer data to the cloud platform.
- Protocol: Shows the application/client name which connects to the device (for example, SNMP client, WMI client).
- 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



Connection from SICAM GridEdge to the cloud:

Station Name	Cloud Connection
Station_West	✓ Online 2022-12-13 12:02:53.863 (UTC)

Connection from SICAM GridEdge to the devices and cloud:

Device Name ↑	Protocol	Device Connection	Cloud Connection
IP192168008001	SNMP Client	✓ Online 2022-12-13 12:03:06.678 (UTC)	! Offline 2022-12-13 12:03:06.794 (UTC)
IP192168008002	SNMP Client	✓ Online 2022-12-13 12:03:06.841 (UTC)	! Offline 2022-12-13 12:03:06.853 (UTC)
IP192168008010	SNMP Client	✓ Online 2022-12-13 12:03:07.004 (UTC)	! Offline 2022-12-13 12:03:07.046 (UTC)
IP192168008015	SNMP Client	✓ Online 2022-12-13 12:03:07.128 (UTC)	! Offline 2022-12-13 12:03:07.167 (UTC)
IP192168008020	SNMP Client	✓ Online 2022-12-13 12:03:07.222 (UTC)	! Offline 2022-12-13 12:03:07.260 (UTC)
IP192168008195	SNMP Client	✓ Online 2022-12-13 12:03:07.375 (UTC)	! Offline 2022-12-13 12:03:07.407 (UTC)

[sc_SICAM_GridEdge_conection_status, 8, en_US]

Figure 4-1 Connection Status

NOTE

In case of a MindSphere OPC UA PubSub connection, an explicit cloud connection is established only for devices connected via IEC 61850 or Modbus. For all other protocols, the data is sent with the PublisherID of SICAM GridEdge.
In case of a MindSphere MindConnectLib connection, all data from all devices are sent with the PublisherID of SICAM GridEdge.
For all others, a seperate cloud connection is established for each device.

NOTE

MindSphere connections via MindConnectLib are not permanent connections. The displayed connection status with the corresponding time stamps only represent the result of the last sent operation. The displayed connection status might not show the actual connection status.

4.2 Maintenance

NOTE

Depending on your assigned user role, the amount of tiles and options of the **Maintenance** page varies.

4.2.1 Deleting Unused Device Templates

You can delete unused SNMP/WMI templates that are not assigned to a device. You cannot delete the **Default.csv** template.

✧ Open the page **Maintenance**.

✧ Select **Delete** in the tile **Device Templates**.

✧ Follow the instructions on the screen.

4.2.2 Making an Update

✧ Open the page **Maintenance**.

✧ Select **Update** in the tile **SICAM GridEdge Version**.

✧ Upload the SICAM GridEdge ZIP file which can be downloaded from the OSD.

✧ The installation process runs automatically.

4.2.3 Configuring a Network-Attached Storage

You can connect your SICAM GridEdge to a network-attached storage (NAS). If configured, SICAM GridEdge automatically stores all your asset information files on this NAS (refer to *4.3.1 Displaying Asset Information*). Every time the asset information change, a new asset information file is automatically created and sent to the NAS in the CSV format.

To prevent overwriting, every file name is unique as it contains a time stamp. You cannot delete the files on your NAS via SICAM GridEdge.

✧ Open the page **Maintenance**.

✧ Select **Configure File Services** in the tile **Services**.

✧ Enter the network path of your NAS location.

✧ If your NAS is secured, enter your user name and password.

✧ Enable **Activate**.

✧ Select **Apply**.

The connection to your NAS is configured.

The asset information files are automatically stored on your NAS.

4.2.4 Adding SSH Access

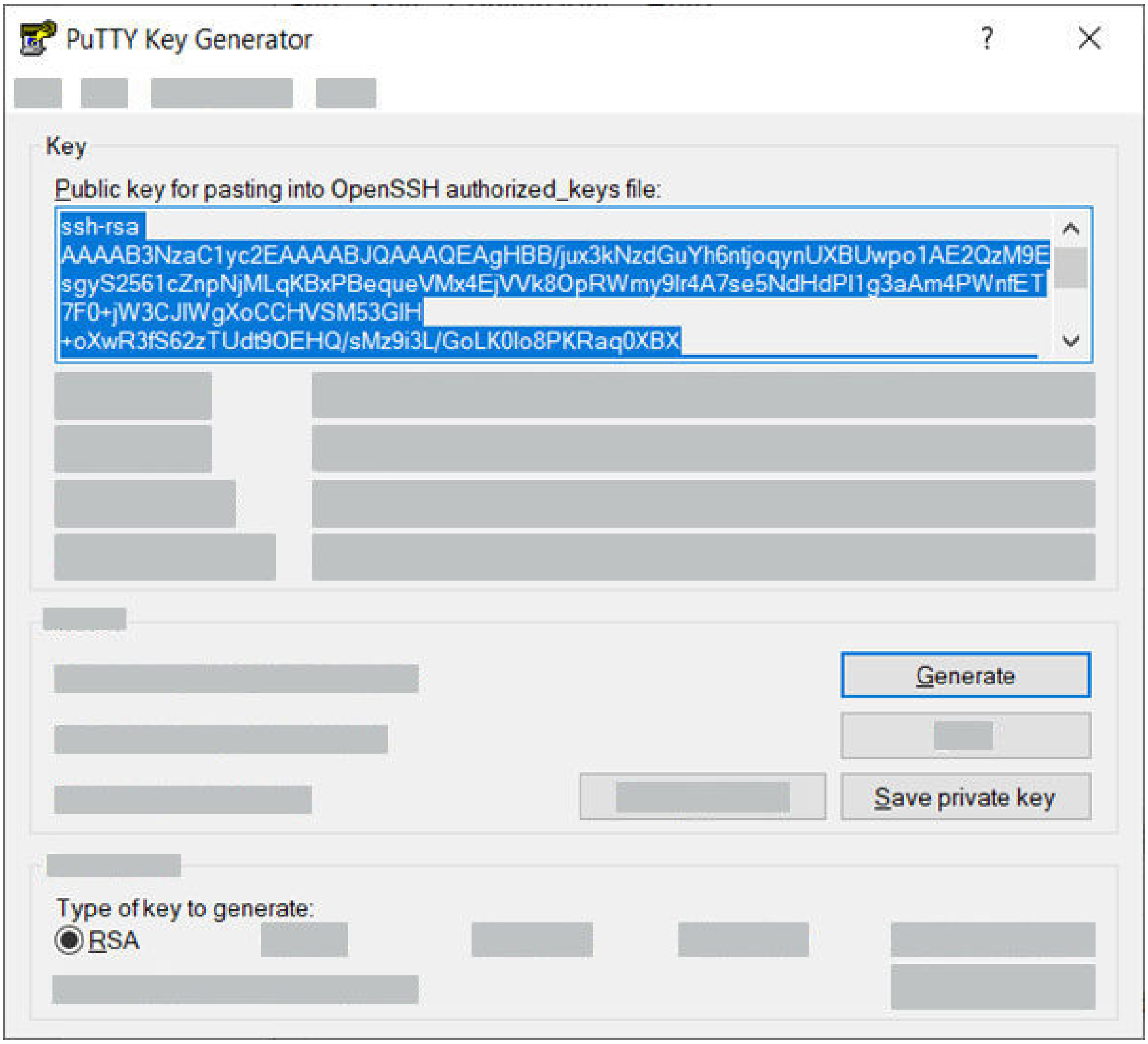
You can upload a generated public key which can be used for enabling the SSH access to your SICAM GridEdge host computer.

Enabling SSH Access

✧ Create a SSH key pair.
Siemens recommends using the Putty key generator. For more information, refer to the official Putty documentation (refer to *Putty key generator*).

✧ Select **RSA** as the key type.

✧ Generate the key.



Public key for pasting into OpenSSH authorized_keys file:

```
ssh-rsa
AAAAB3NzaC1yc2EAAAABJQAAAQEAgHBB/jux3kNzdGuYh6ntjoqynUXBUwpo1AE2QzM9E
sgyS2561cZnpNjMLqKBxPBequeVMx4EjVVk8OpRWmy9Ir4A7se5NdHdPI1g3aAm4PWnfET
7F0+jW3CJIWgXoCCHVSM53GIH
+oXwR3fS62zTUdt9OEHQ/sMz9i3L/GoLK0Io8PKRaq0XBX
```

Type of key to generate:
● RSA

[sc_putty_2, 2, en_US]

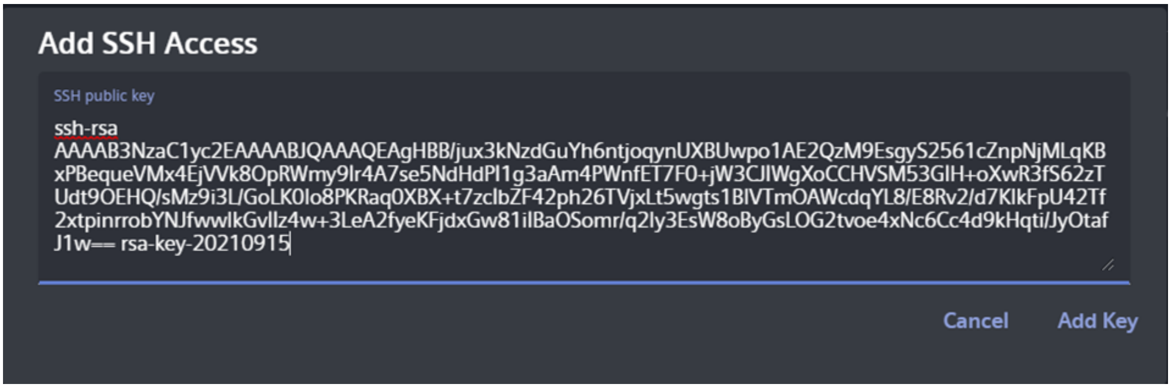
✧ To create a random private key pair, move the mouse cursor around inside the area **Key**.

✧ Copy the selected text. This text is the public key and has to be uploaded to the device later.

✧ Save the private key to a location of your choice on your local computer.
You will need this key later when you want to connect to your SICAM GridEdge device via SSH.

✧ Open the page **Maintenance**.

✧ Select **Configure SSH Access** in the tile **Services**.



```
ssh-rsa
AAAAB3NzaC1yc2EAAAABJQAAAQEAgHBB/jux3kNzdGuYh6ntjoqynUXBUwpo1AE2QzM9EsgyS2561cZnpNjMLqKB
xPBequeVMx4EjVVk8OpRWmy9lr4A7se5NdHdPl1g3aAm4PWnfET7F0+jW3CJIWgXoCCHVSM53GlH+oXwR3fS62zT
Udt9OEHQ/sMz9i3L/GoLK0lo8PKRaq0XBX+t7zclbZF42ph26TVjxLt5wgts1BIVTmOAWcdqYL8/E8Rv2/d7KlkFpU42Tf
2xtpinrrobYNJfwwlkGvllz4w+3LeA2fyeKFjdxGw81ilBaOSomr/q2ly3EsW8oByGsLOG2tvoe4xNc6Cc4d9kHqti/JyOtaf
J1w== rsa-key-20210915
```

[sc_putty_3, 1, en_US]

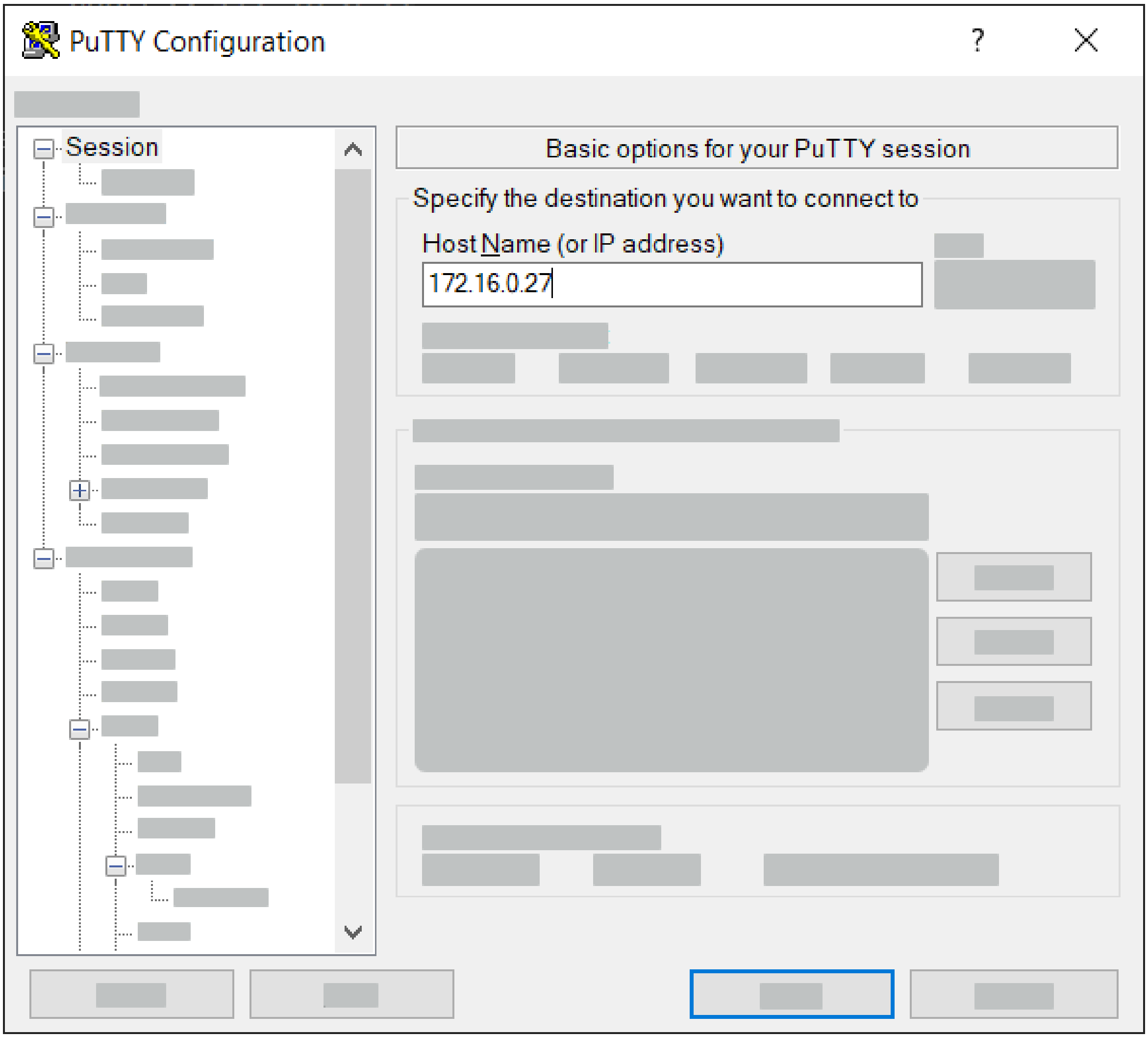
✧ Paste the copied text. You can add multiple public keys.

✧ Select **Add Key**.

After uploading an SSH public key, it may take up to 1 minute until the key is activated in the SICAM GridEdge host computer.

Connecting to SICAM GridEdge Device

✧ To connect to your SICAM GridEdge device, open Putty and enter the IP address of your substation LAN (for example, 172.16.0.27).


PuTTY Configuration
?
Session
Basic options for your PuTTY session
Specify the destination you want to connect to
Host Name (or IP address)

172.16.0.27

[sc_putty_4, 2, en_US]

- ✧ In **Category** on the left side, navigate to **Connection > SSH > Auth**.
- ✧ Browse for your **Private key file for authentication** and select **Open**.

Removing Public Keys from Device

- ✧ Navigate to the file **/root/.ssh/authorized_keys**.
- ✧ To remove all public keys, remove this file.

4.2.5 Configuring SICAM GridEdge as an SNMP Agent

You can configure SICAM GridEdge to act as an SNMP agent. Doing this, any SNMP manager using the SNMPv3 protocol can connect to the SNMP agent and poll certain information from SICAM GridEdge (for example, security logs).

To enable polling, you must configure the SNMP agent parameters.

You must be logged on either with the role **Administrator** or **SECADM**.

- ✧ Open the page **Maintenance**.
- ✧ Select **Configure SNMP Agent** in the tile **Services**.
- ✧ Enter the user name for the SNMP agent.

- ✧ Select the security level.
- ✧ Select the authentication algorithm.
- ✧ Enter the authentication password.
- ✧ Select the privacy algorithm.
- ✧ Enter the privacy password.
- ✧ Select **Apply**.

The SNMP agent is configured.

The SNMP manager can poll from the SNMP agent. The SNMP agent can respond a polling with a maximum of the last 50 messages.

NOTE

The MIB files for your SNMP manager are part of your SICAM GridEdge setup bundle.

NOTE

To enable sending traps, refer to *5.6.1.2 Configuring an SNMP Manager for Traps*.

4.3 Asset Information

NOTE

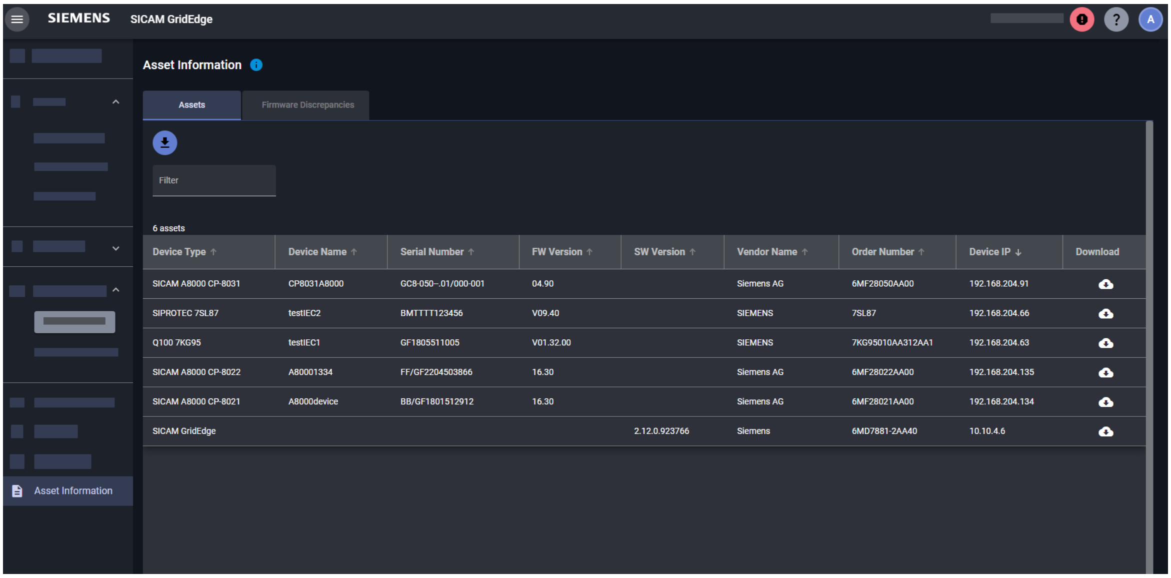
The asset information are stored in an encrypted format in the SICAM GridEdge database.

4.3.1 Displaying Asset Information

SICAM GridEdge provides the possibility to view collected asset information from every device, if available.

- ✧ Open the page **Asset Information**.
- ✧ Open the tab **Assets**.
- ✧ If needed, use the **Text Filter** to define the data to be shown in the data table.

All available asset information are automatically displayed.



6 assets

Device Type ↑	Device Name ↑	Serial Number ↑	FW Version ↑	SW Version ↑	Vendor Name ↑	Order Number ↑	Device IP ↓	Download
SICAM A8000 CP-8031	CP8031A8000	GC8-050–.01/000-001	04.90		Siemens AG	6MF28050AA00	192.168.204.91	☁
SIPROTEC 7SL87	testIEC2	BMTTTT123456	V09.40		SIEMENS	7SL87	192.168.204.66	☁
Q100 7KG95	testIEC1	GF1805511005	V01.32.00		SIEMENS	7KG95010AA312AA1	192.168.204.63	☁
SICAM A8000 CP-8022	A80001334	FF/GF2204503866	16.30		Siemens AG	6MF28022AA00	192.168.204.135	☁
SICAM A8000 CP-8021	A8000device	BB/GF1801512912	16.30		Siemens AG	6MF28021AA00	192.168.204.134	☁
SICAM GridEdge				2.12.0.923766	Siemens	6MD7881-2AA40	10.10.4.6	☁

Downloading Asset Information

- ✧ Open the page **Asset Information**.
- ✧ Open the tab **Assets**.
- ✧ Select the cloud icon in the column **Download** of the desired device.

  - or -

- ✧ Select the icon ⬇.

The asset information collected for the device is downloaded in the ZIP format.

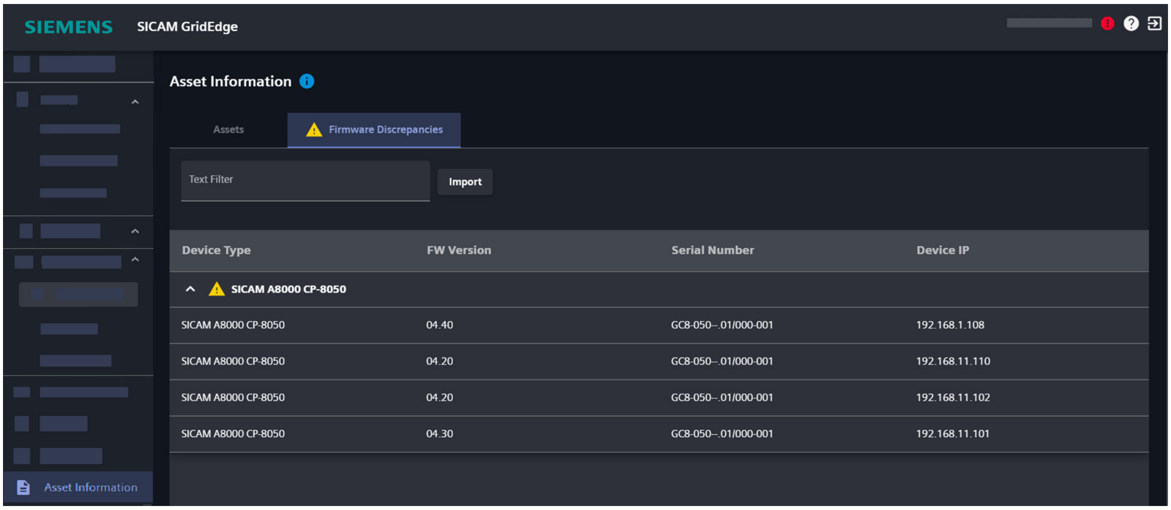
4.3.2 Checking for Firmware-Version Discrepancies

SICAM GridEdge can detect possible discrepancies in the firmware versions of connected devices.

- ✧ Open the page **Asset Information**.
- ✧ Open the tab **Firmware Discrepancies**.

SICAM GridEdge automatically compares the firmware versions fetched from the devices based on the device type (device family and model).

All discrepancies in the firmware versions are marked with a warning symbol.

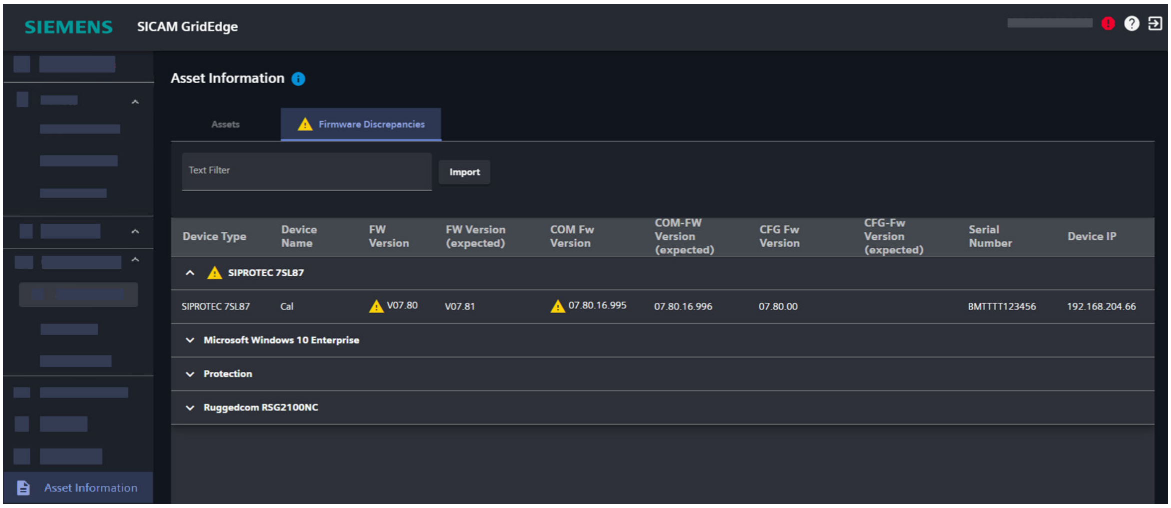


Device Type	FW Version	Serial Number	Device IP
⚠ SICAM A8000 CP-8050			
SICAM A8000 CP-8050	04.40	GC8-050--.01/000-001	192.168.1.108
SICAM A8000 CP-8050	04.20	GC8-050--.01/000-001	192.168.11.110
SICAM A8000 CP-8050	04.20	GC8-050--.01/000-001	192.168.11.102
SICAM A8000 CP-8050	04.30	GC8-050--.01/000-001	192.168.11.101

✧ If you want to compare if each device has the same firmware version as specified in an user-defined configuration file, upload a configuration file.

✧ To do so, select **Import** and select your configuration file (refer to *4.3.3 Creating a Configuration File*).

SICAM GridEdge compares the firmware version of each device between the version fetched from the device and the version defined in the configuration file.
All discrepancies in the firmware versions are marked with a warning symbol.



Device Type	Device Name	FW Version	FW Version (expected)	COM Fw Version	COM-FW Version (expected)	CFG Fw Version	CFG-Fw Version (expected)	Serial Number	Device IP
⚠ SIPROTEC 7SL87									
SIPROTEC 7SL87	Cal	⚠ V07.80	V07.81	⚠ 07.80.16.995	07.80.16.996	07.80.00		BMTTTT123456	192.168.204.66
Microsoft Windows 10 Enterprise									
Protection									
Ruggedcom RSG2100NC									

4.3.3 Creating a Configuration File

You can import a configuration file in the CSV format to define the expected firmware versions. This file has to be self-created and is not provided by Siemens.

✧ Create your configuration file in the CSV format. Use 1 line per IP address with expected firmware versions with the following syntax:

ID;BayName;VoltageLevel;DeviceName;IPaddress;Type;TemplateName;CPUFW;COMFW;CFG

The column CPUFW contains the expected firmware version of the CPU.
The column COMFW contains the expected firmware version of the communication module.
The column CFG contains the expected firmware version of the configuration module.

Example:

```
ID;BayName;VoltageLevel;DeviceName;IPaddress;Type;TemplateName;CPUFW;COMFW;CFG
1;6SOUTE.1;6;Cal;30.0.6.72;SIPROTEC5 7SA87;;8.3;8.3;8.3
2;6SOUTE.1;6;PP1;30.0.134.73;SIPROTEC5 7SA87;;7.3;7.3;7.3
3;4CBOSECT.1;4;Cal;30.0.4.52;SIPROTEC5 6MD85;;8.3;8.3;8.3
4;4CBOSECT.1;4;PP1;30.0.4.53;SIPROTEC4 7SJ85;;7.5;7.4;7.5
```

4.4 Health Monitoring

You can monitor the health status of SICAM GridEdge via SNMPv3 (hrSWRun table in the standard HOST-RESOURCES-M).
To do so, configure the SNMP agent (refer to *4.2.5 Configuring SICAM GridEdge as an SNMP Agent*) and enter the object identifiers (OID) of the SICAM GridEdge container in the monitoring system.

Container Name	Object Identifier
ge-configmanager	1.3.6.1.2.1.25.4.2.1.7.1
ge-webinterface	1.3.6.1.2.1.25.4.2.1.7.2
ge-datastore	1.3.6.1.2.1.25.4.2.1.7.3
ge-ssmservice	1.3.6.1.2.1.25.4.2.1.7.4
ge-broker	1.3.6.1.2.1.25.4.2.1.7.5
ge-modbusclient	1.3.6.1.2.1.25.4.2.1.7.6
ge-wmiclient	1.3.6.1.2.1.25.4.2.1.7.7
ge-iec61850client	1.3.6.1.2.1.25.4.2.1.7.8
ge-snmpclient	1.3.6.1.2.1.25.4.2.1.7.9
ge-mqttbroker	1.3.6.1.2.1.25.4.2.1.7.10
ge-datapublisher	1.3.6.1.2.1.25.4.2.1.7.11
ge-digsi4client	1.3.6.1.2.1.25.4.2.1.7.12

5 Security

5.1 General Information

Management of Security-related Issues

To report a security vulnerability affecting a Siemens product or solution, contact Siemens via this Internet page: *https://new.siemens.com/global/en/products/services/cert/vulnerability-process.html*.

Information on validated security vulnerabilities that directly involve Siemens products are published in the Siemens Security Advisories (refer to *https://new.siemens.com/global/en/products/services/cert.html#Security-Publications*).

Security Update Management

For software and firmware updates, Siemens offers a systematic patch management service. For more information, refer to *https://www.siemens.com/global/en/products/energy/energy-automation-and-smart-grid/grid-security/operational-security.html*.

Information on software and firmware updates including third-party components is part of the respective release notes. Release notes are part of each delivery and are available in the SIOS portal (refer to *https://support.industry.siemens.com/cs/products?search=SICAM%20GridEdge&mfn=ps&o=DefaultRanking-Desc&lc=en-US*).

5.2 Security Requirements

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*)

5.3 User Management

5.3.1 Access Control

5.3.1.1 Login Attempts

The login attempts of a user are restriced based on 3 parameters:

- Maximum login attempts
  The maximum number of sequential login attempts for a user is set to 5.

- Time lapse
  The time range after which the number of login attempts is set back to 0 after the last unsuccessful attempt is set to 5 minutes.
- Blocked duration
  The time duration for which the user account remains blocked after the maximum number of login attempts is reached is set to 30 minutes.

If you log on with wrong credentials, the login attempts are counted. Once the maximum number of login attempts has been reached, logging on is not possible for 30 minutes. If this 30 minutes has elapsed, login can be attempted again.

NOTE

The login cannot be attempted if the following conditions are met:

- The login is blocked.
- The device time is not synchronized with a central time server and is earlier than the total of the login-blocked time and the blocked duration.

5.3.1.2 Logging Off

If you leave the SICAM GridEdge Web interface unattended for 20 minutes, the system will automatically log off your current session. You can also log off manually.

✧ Close all instances of your Web browser.

- or -

✧ Navigate to the user menu in the upper-right corner.

✧ Select **Logout**.

You are logged off the system.

5.3.2 Local User Management

The local user management is the default setting within SICAM GridEdge.

5.3.2.1 User Role

With the local user management, only one user with the role **Administrator** is used within SICAM GridEdge. This user is assigned a unique password during the installation process.

5.3.2.2 Changing the Password

When the local user management is enabled, you can change the password of the logged-on user. This option is disabled in case the central user management (LDAP) is activated.

✧ Navigate to the user menu in the upper-right corner.

✧ Select **Reset password**.

✧ Enter your current password.

✧ Enter your new password.

✧ Confirm that you want to change your password.

Your password is changed.

5.3.3 Central User Management (LDAP)

You can configure a connection to your repository-based user management (LDAP) of your IT infrastructure. If configured, SICAM GridEdge fetches the existing accounts from the LDAP server with the specified role definitions.

5.3.3.1 Supported LDAP User Roles

SICAM GridEdge restricts the permissions of the users according to the given roles.

Rights	Functionality of Rights	Assignment of Supported Roles					
		VIEWER	ENGINEER	SECADM	SECAUD	RBACMGMT	Administrator
None	Viewing general information	■	■	■	■	■	■
Change CFG	Changing/downloading/uploading the configuration	–	■	–	–	–	■
Audit trail	Audit trail	–	–	–	■	–	■
SW change	Change software	–	–	–	–	–	■
RBAC mgmt	RBAC management	–	–	–	–	■	■
Security management	Managing and performing the security functions	–	–	■	–	–	■

5.3.3.2 Enabling the Central User Management

To configure the connection to your LDAP server in SICAM GridEdge, you must use your local user account.

✧ Open the page **Maintenance**.

✧ Select **Configure** in the tile **User Management**.

✧ Enable **Use LDAP**.

✧ Enter the IP address of your LDAP server in the field **IP Address**, for example ldap://127.0.0.1.

✧ Enter the port number of your LDAP server in the field **Port**, for example, 386.

✧ Enter the corresponding directory of the LDAP server to limit the search in the field **Search Base**, for example, ou=ldap,dc=ldap,dc=dsiemens,dc=com.

✧ Enter a number of cached user accounts between 1 and 21 in the field **User Cache Size**. To disable the user-cache feature, set the size to 0.

If the LDAP server is not available, the defined number of users can still log on. The user accounts of those users who last logged on to SICAM GridEdge are available for login.

✧ If the operating system of the LDAP server is Linux and based on OpenLDAP, enable **Use DN for Login**.

The distinguished name (DN) is used for the login, combining the user name and the parent distinguished name.

The field **User Parent DN** is activated.

✧ If the operating system of the LDAP server is Linux, enter the parent distinguished name in the field **User Parent DN**. The **User Parent DN** must be identical to the **Search Base**.

✧ Upload the CA certificate of your LDAP server under **Upload CA Cert**.
The certificate is used to establish a secure connection between the LDAP server and SICAM GridEdge.

✧ Upload the root CA certificate of your LDAP server under **Upload Root CA Cert**.
The certificate is used to verify the token generated to get the role and authentication information.

✧ Select **Apply**.

The connection to your LDAP server is established.

The user accounts with the corresponding roles are fetched from the LDAP server.

NOTE

If a role is defined on the LDADP server which is not supported by SICAM GridEdge, the user will be logged on to SICAM GridEdge with the role **Viewer**.

5.3.3.3 Disabling the Central User Management

You can disable the central user management (LDAP) and switch back to the local user management.

- ✧ Open the page **Maintenance**.
- ✧ Select **Configure** in the tile **User Management**.
- ✧ Disable **Use LDAP**.
- ✧ Select **Apply**.

The connection to your LDAP server is terminated.
You are logged off. You need to log back on with your local user account.

5.3.3.4 Resetting the LDAP Server Configuration

You need to be logged on either with the role **Administrator** or **RBACADM**.

- ✧ Open the page **Maintenance**.
- ✧ Select **Reset** in the tile **User Management**.
- ✧ Confirm that you want to reset the LDAP server configuration.

All LDAP-related configuration data are cleared.
You are logged off. You need to log back on with your local user account.

5.4 Making a 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 and imported.

NOTE

The local security log file is not included in the backup.

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

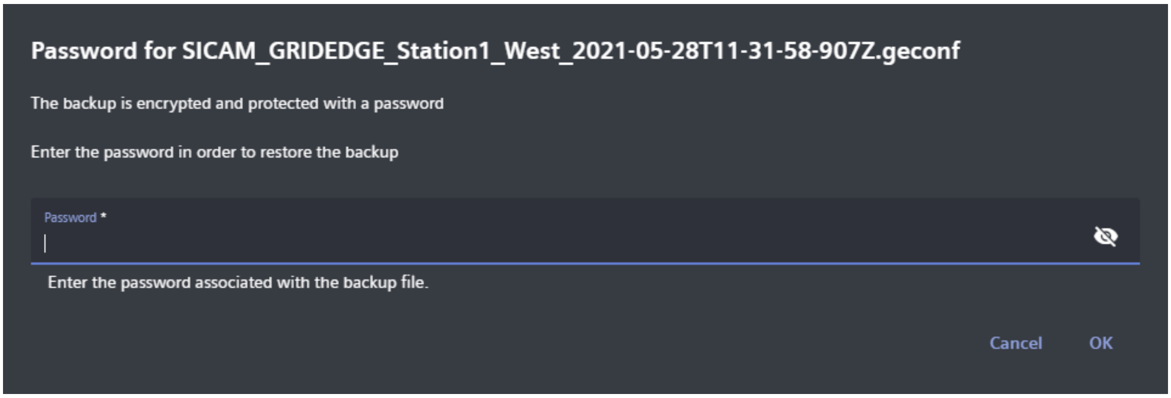
- ✧ Open the page **Maintenance**.
- ✧ Select **Backup** in the tile **Configuration**.

✧ Enter the password to be used to protect your archived project.

✧ Select **Save**.

Restoring a Project

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



Password for SICAM_GRIDEDGE_Station1_West_2021-05-28T11-31-58-907Z.geconf

The backup is encrypted and protected with a password

Enter the password in order to restore the backup

Password *

Enter the password associated with the backup file.

[sc_SICAM_GridEdge_sec_restore, 7, en_US]

Figure 5-1 Restoring a Project

✧ Open the page **Maintenance**.

✧ Select **Restore** in the tile **Configuration**.

✧ Enter the **Password**.

✧ Select **OK**.

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

5.5 Resetting Configuration Data

✧ Open the page **Maintenance**.

✧ Select **Reset** in the tile **Configuration**.

✧ Enter your password.

✧ Confirm that you want to reset your configurations.

All configuration data are deleted except the user management and the syslog server configuration. You are redirected to an empty **Station Settings** page.

5.6 Security Logging

5.6.1 Syslog Security Logging

5.6.1.1 Configuring syslog Security Logging

You can activate the logging of security-relevant events by connecting to a syslog server.

✧ Open the page **Maintenance**.

✧ Select **Configure** in the tile **Security logs**.

✧ Enter the IP address or the host name of your syslog server.

✧ Enter the port of the syslog server.

✧ Enable **Activate syslog server connection**.

✧ Select **Apply**.

All security-relevant events are logged onto the configured syslog server.

5.6.1.2 Configuring an SNMP Manager for Traps

SICAM GridEdge can send security-relevant messages as SNMP traps via the SNMPv3 protocol to an SNMP manager.
To enable sending these SNMP traps, you must configure the SNMP manager parameters.

NOTE

The port 162 should be open on the SNMP manager machine to receive traps.

✧ Open the page **Maintenance**.

✧ Select **Configure** in the tile **Security Logs**.

✧ Navigate to the section **Configure SNMP Manager connection**.

✧ Enter the user name for the SNMP manager.

✧ If necessary, change the security level. The security level **Auth, Priv** is selected by default.

✧ Select the authentication algorithm.

✧ Enter the authentication password.

✧ Select the privacy algorithm.

✧ Enter the privacy password.

✧ Enable **Activate SNMP Trap**.

✧ Select **Apply**.

SNMP traps based on security-relevant messages are sent to the SNMP manager.

NOTE

The MIB files for your SNMP manager are part of your SICAM GridEdge setup bundle.

NOTE

SICAM GridEdge can also act as an SNMP agent (refer to *4.2.5 Configuring SICAM GridEdge as an SNMP Agent*).

5.6.1.3 Resetting the syslog Server Configuration

You must be logged on either with the role **Administrator** or **SECADM**.

✧ Open the page **Maintenance**.

✧ Select **Reset Configuration** in the tile **Security logs**.

✧ Confirm that you want to reset the syslog server configuration.

All syslog-related configuration data are cleared.
No more messages are sent to the syslog server.
The SNMP trap configurations are deleted.

5.6.1.4 Structure of a Security-Log Entry

A security-log entry is built up with the following elements:

Element	Description
Severity (level)	Severity levels: • Event • Alarm
Date	Date when the event is logged
Time	Time when the event is logged • T Time • hh:mm:ss.ttt Time when the event is created • +hh:mm Time deviation from GMT
IP address or port name	IP address or port name of the product or subcomponent that generates the log entry
Module name	The name of the product module that generates the log entry
BOM	Byte order mark for UTF8 encoding
Product name	The name of the product that generates the log entry
Indication text	The message part of a syslog event Depending on the event, the indication text can contain variable additional information (%A1%, %A2%, %A3%, and %A4%).

5.6.1.5 Syslog Events

Severity Level Event

The following table shows syslog messages at the severity level ***Event***.

Table 5-1 Syslog Messages at Severity Level Event

Event	Additional Information	
Storage capacity of the security audit decreased below the set threshold of %A1% entries.	%A1%	Threshold of the storage capacity set by users or the default value ***80***
User %A1% initiated a remote session from %A2% in the role(s) of %A3%.	%A1%	Account ID
	%A2%	IP address of the remote workstation
	%A3%	Role(s) which are assigned to the user and separated with commas in the list
User %A1% changed the settings related to user authentication: %A2% server: IP address [set to value %A3%].	%A1%	Account ID
	%A2%	Protocol (LDAP)
	%A3%	IP address
User %A1% logged out.	%A1%	Account ID
The interactive session with the user %A1% has been terminated due to time-out (%A2%).	%A1%	Account ID
	%A2%	Time-out threshold set by the user or the default value (20 minutes) for the user inaction After this duration, the existing user-interactive session is terminated.

Event	Additional Information	
User %A1% modified password of the account %A2% (%A3%-managed account).	%A1%	Account ID of the user that performs the activity
	%A2%	Account ID that is affected by the activity
	%A3%	Account type
User %A1% downloaded configuration settings from %A2%.	%A1%	Account ID
	%A2%	User-identified remote workstation (for example, engineering tool) with which the modifications are initiated to be carried out If a PC software is used, then it is the IP address of the PC.
User %A1% changed the configuration settings from %A2%.	%A1%	Account ID
	%A2%	User-identified remote workstation (for example, engineering tool) with which the modifications are initiated to be carried out If a PC software is used, then it is the IP address of the PC.
User %A1% viewed the audit log from %A2%.	%A1%	Account ID
	%A2%	User-identified remote workstation (for example, engineering tool) with which the modifications are initiated to be carried out If a PC software is used, then it is the IP address of the PC.
User %A1% uploaded firmware version from %A2% to %A3%	%A1%	Account ID
	%A2%	Current version
	%A3%	Higher version
User %A1% changed settings related to secure communication: %A2% [set to value %A3%].	%A1%	Account ID
	%A2%	Certificate type
	%A3%	Certificate name
User %A1% has changed configuration settings for %A2% from %A3%	%A1%	Account ID
	%A2%	Configuration page name
	%A3%	IP address
User %A1% has changed configuration settings for Proxy %A2% [set to value %A3%] from %A4%	%A1%	Account ID
	%A2%	Field name
	%A3%	Field changed value
	%A4%	IP address
User %A1% has changed configuration settings for %A2% [set to value %A3%] from %A4%	%A1%	Account ID
	%A2%	Field name
	%A3%	Field changed value
	%A4%	IP address
User %A1% has reset the configuration from %A2%	%A1%	Account ID
	%A2%	IP address
User %A1% has restored the configuration using backup file %A2% from %A3%	%A1%	Account ID
	%A2%	File name
	%A3%	IP address
User %A1% added SSH public key from %A2%	%A1%	Account ID
	%A2%	IP address
User %A1% downloaded the configuration settings [%A2%] from %A3%	%A1%	Account ID
	%A2%	File/Config file name
	%A3%	IP address

Severity Level Alarm

The following table shows syslog messages at the severity level ***Alarm***.

Table 5-2 Syslog Messages at Severity Level Alarm

Alarm	Additional Information	
3 incorrect password entries in succession were attempted while logging on with account %A1% (%A2%-managed account) from %A3%.	%A1%	Account ID
	%A2%	Account types: • For product-managed (local) user accounts, the account type is ***LOCAL***. • For LDAP users, the account type is ***LDAP***.
	%A3%	It can be one of the following information: • User-identifiable name of the product where login attempts were detected • If a remote workstation is used, %A3% is the IP address of the remote workstation.
Repeated attempts to log on with account %A1% (%A2%-managed account) from %A3%	%A1%	Account ID
	%A2%	Account types: • For product-managed (local) user accounts, the account type is ***LOCAL***. • For LDAP users, the account type is ***LDAP***.
	%A3%	It can be one of the following information: • User-identifiable name of the product where login attempts were detected • If a remote workstation is used, %A3% is the IP address of the remote workstation.
User %A1% initiated a restart from %A2% with action: %A3%.	%A1%	Account ID
	%A2%	User-identified remote workstation (for example, engineering tool) with which the modifications are initiated to be carried out. If a PC software is used, then it is the IP address of the PC.
	%A3%	Additional information on the exact action which triggered the restart, for example, settings download
Attempted download of invalid firmware file(s) from %A1%	%A1%	Source of the unauthorized configurations, for example, IP address of the PC
User account %A1% (%A2%-managed account) blocked for the next %A3% minutes after too many attempts to log in unsuccessfully from %A4%.	%A1%	Account ID
	%A2%	Account types: • For local user accounts, the account type is LOCAL. • For LDAP users, the account type is LDAP.
	%A3%	The default number of minutes during which the account remains blocked (30)
	%A4%	It can be one of the following information: • User-identifiable name of the product where login attempts were detected • If a remote workstation is used, %A4% is the IP address of the remote workstation.

5.6.2 Local Security Logging

5.6.2.1 Overview

SICAM GridEdge provides a security audit trail function which chronologically acquires and categorizes security-relevant events according to the origin and severity. When a security-related event occurs, SICAM

GridEdge automatically records the event in a locally saved log. This local security logging is always active and cannot be deactivated.

The security log has a maximum capacity of 4096 entries. If the entries of the security log exceed the 100 % capacity limit, the oldest entry is automatically overwritten. As soon as the capacity limit of 80 % is reached, this is automatically logged. In that case, Siemens recommends a backup of the security log (refer to *5.6.2.2 Downloading Local Security Log File*).

Example:

Entry 4097 exceeds the 100 % limit and deletes entry number 0001. Entry 4098 deletes entry number 0002.

5.6.2.2 Downloading Local Security Log File

You must be logged on either with the role **Administrator** or **SECAUD**.

✧ Open the page **Maintenance**.

✧ Select **Download** in the tile **Security logs**.

A log entry about the download is added to the security log.

The security log file **ge-security.log** is downloaded as a text file in a ZIP folder.

5.6.2.3 Deleting Local Security Log File

You must be logged on either with the role **Administrator** or **SECADM**.

✧ Open the page **Maintenance**.

✧ Select **Delete** in the tile **Security logs**.

✧ Confirm that you want to delete the security log file.

The security log file is deleted.

5.7 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

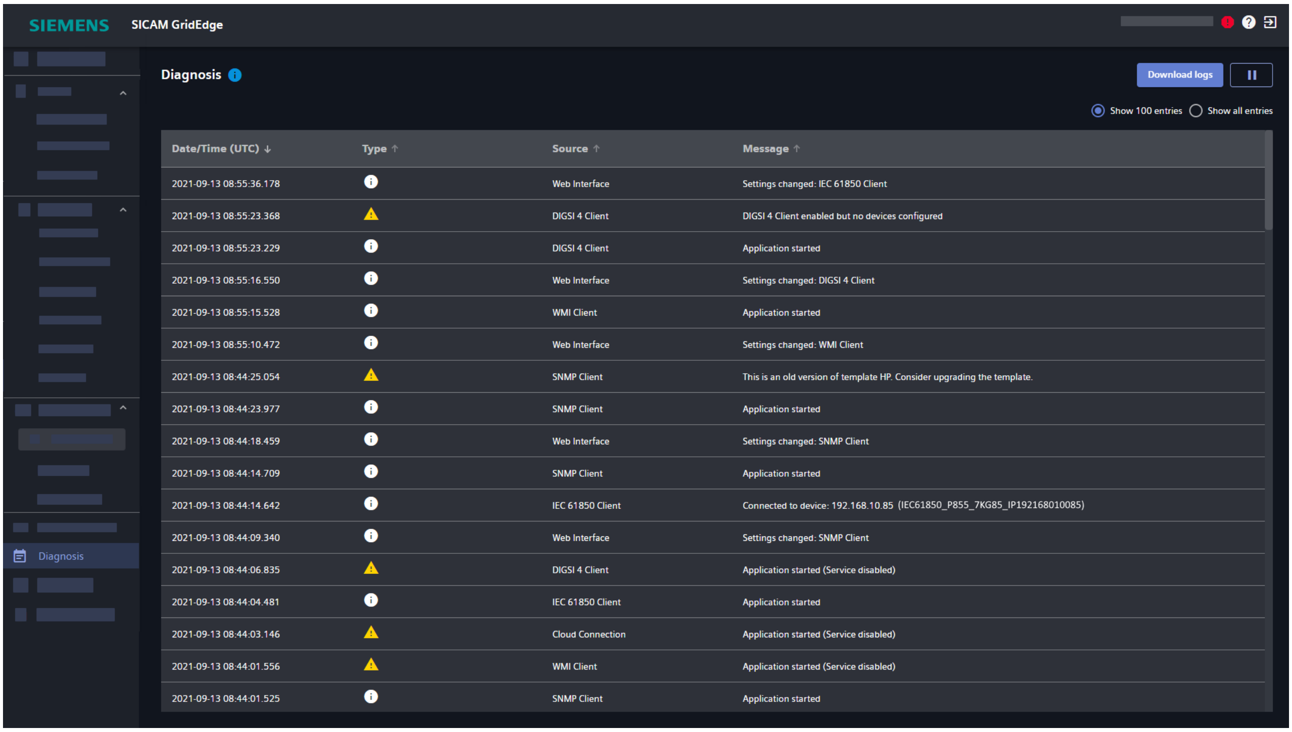
Per default, only the last 100 log entries will be shown.

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.



Date/Time (UTC) ↓	Type ↑	Source ↑	Message ↑
2021-09-13 08:55:36.178	ⓘ	Web Interface	Settings changed: IEC 61850 Client
2021-09-13 08:55:23.368	⚠	DIGSI 4 Client	DIGSI 4 Client enabled but no devices configured
2021-09-13 08:55:23.229	ⓘ	DIGSI 4 Client	Application started
2021-09-13 08:55:16.550	ⓘ	Web Interface	Settings changed: DIGSI 4 Client
2021-09-13 08:55:15.528	ⓘ	WMI Client	Application started
2021-09-13 08:55:10.472	ⓘ	Web Interface	Settings changed: WMI Client
2021-09-13 08:44:25.054	⚠	SNMP Client	This is an old version of template HP. Consider upgrading the template.
2021-09-13 08:44:23.977	ⓘ	SNMP Client	Application started
2021-09-13 08:44:18.459	ⓘ	Web Interface	Settings changed: SNMP Client
2021-09-13 08:44:14.709	ⓘ	SNMP Client	Application started
2021-09-13 08:44:14.642	ⓘ	IEC 61850 Client	Connected to device: 192.168.10.85 (IEC61850_P855_7KG85_IP192168010085)
2021-09-13 08:44:09.340	ⓘ	Web Interface	Settings changed: SNMP Client
2021-09-13 08:44:06.835	⚠	DIGSI 4 Client	Application started (Service disabled)
2021-09-13 08:44:04.481	ⓘ	IEC 61850 Client	Application started
2021-09-13 08:44:03.146	⚠	Cloud Connection	Application started (Service disabled)
2021-09-13 08:44:01.556	⚠	WMI Client	Application started (Service disabled)
2021-09-13 08:44:01.525	ⓘ	SNMP Client	Application started

[sc_SICAM_GridEdge_sec_logging, 9, en_US]

Figure 5-2 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 cloud connection 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.

5.8 TCP-UDP Ports

Table 5-3 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. A custom-signed Web interface certificate can also be uploaded. ● 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 *5.9.2 Connection between Devices and Cloud Platform*)

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 5-4 Used TCP-UDP ports

Communication Protocol	Network	Server/ Client	TCP/UDP	Port	Description
DIGSI 4	LAN	Client	UDP	50 000	Communication with a device using DIGSI 4 Client in station network
DNS	WAN	Client	UDP	53	Used by MQTT for domain name resolution
HTTP	WAN	Client	TCP	80	Certificate Validation

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
LDAP	LAN	Client	TCP	389 (Preferred)	Communication with a LDAP server
Modbus	LAN	Client	TCP	1 to 65535 (preferred 502)	Communication with a device using Modbus in station network
Moxa NPort Serial Device Driver, Data Port	LAN	Client	TCP	4001 to 4005 (depending on NPort device type)	Default values of the data communication to the serial-device driver The values can differ depending on your configuration of the port numbers in the NPort Administrator software.
MQTT	LAN	Server	TCP	1883	Communication with a device using MQTT in station network
NTP	WAN/LAN (depending on configuration)	Client	UDP	123	**Time Synchronization** for the IPC with NTP
OPC UA PubSub / MQTT	WAN	Client	TCP	8883	Publishing of data to a MQTT broker for Internet of Things (IoT)
SMB	LAN	Client	TCP	445	Communication with network-attached storage(NAS) in station network
SNMP	LAN	Client	UDP	161, 162	Communication with a device using SNMP in station network
SNMP	LAN	Server	UDP	161, 162	Communication with SNMP manager
SSH	LAN	Server	TCP	22	Secure Shell for configuration of the IPC
Syslog	LAN	Client	UDP	514 (preferred)	Communicating with syslog server
WinRM	LAN	Client	TCP	5986	Communicating with Microsoft Windows system for collecting WMI data

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/

5.9 Certificate Management

5.9.1 Connection to the Web Interface

For the connection to the Web interface, a self-signed certificate is automatically created during the start of SICAM GridEdge.

You can also use a custom certificate. In case a problem with your custom certificate is detected (for example, not matching IP addresses, exceeded expiry date), this certificate is automatically replaced by a new self-signed certificate from SICAM GridEdge.

5.9.1.1 Uploading a Custom Certificate

Instead of using the default self-signed certificate for the connection to the Web interface, you have the possibility to upload an own certificate.

You must be logged on either with the role **Administrator** or **SECADM**.

✧ Open the page **Maintenance**.

✧ Select **Download** in the tile **Webinterface certificate**.

The CSR is downloaded with the necessary information from SICAM GridEdge.

✧ Sign the certificate with your CA.

✧ Select **Upload** in the tile **Webinterface certificate**.

✧ Navigate to your certificate file (.pem or .crt file format).

✧ Confirm that you want to upload a new certificate.

✧ Select **OK**.

After the successful upload, you are logged off and the Web interface is restarted.

✧ Refresh the logon page.

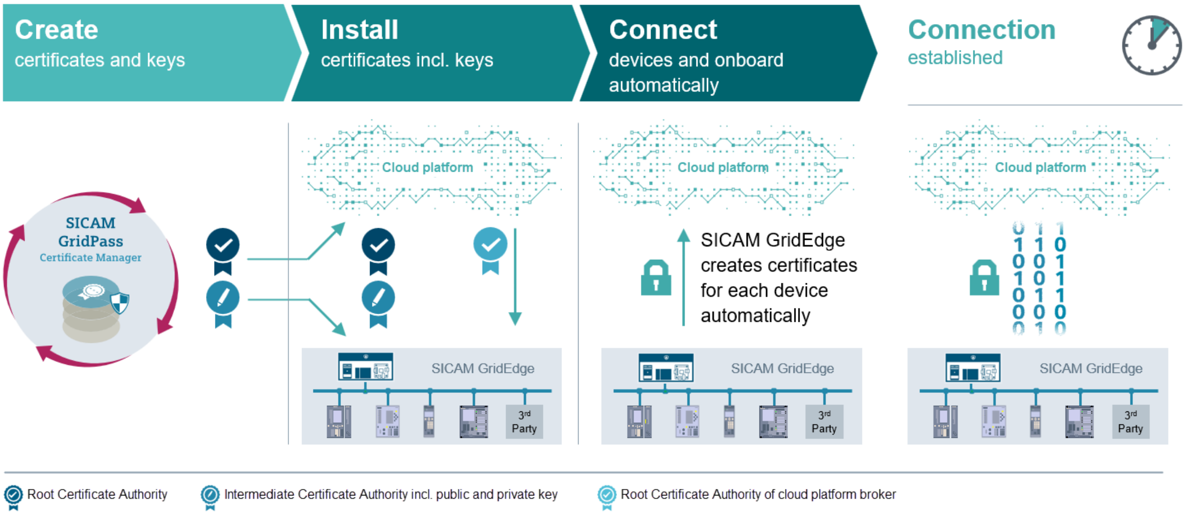
✧ Log back on.

Your custom certificate is used for the connection to the SICAM GridEdge Web interface.

5.9.2 Connection between Devices and Cloud Platform

SICAM GridEdge automatically creates a client certificate for each connected device with the configured intermediate certificate authority which is used for a secured cloud connection.

The following figure describes the process.


Create
certificates and keys
Install
certificates incl. keys
Connect
devices and onboard automatically
Connection
established
SICAM
GridPass
Certificate Manager
Cloud platform
Cloud platform
Cloud platform
SICAM GridEdge creates certificates for each device automatically
SICAM GridEdge
SICAM GridEdge
SICAM GridEdge
3rd Party
3rd Party
3rd Party
Root Certificate Authority
Intermediate Certificate Authority incl. public and private key
Root Certificate Authority of cloud platform broker

[sc_SICAM_GridEdge_sec_certman, 4, en_US]

Figure 5-3 Certificate Management Process

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

In order to enable the mandatory end-to-end encryption (TLS) between SICAM GridEdge and the MQTT Broker of the cloud platform, it is required to upload the (intermediate) certificate authority to the 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

If you use MindSphere as a cloud platform, refer to the IoT Engineering Guide for more information about the required certificates (*MindSphere IoT Engineering Guide*).

If a client actively establishes a cloud connection, a certificate is created for the device. This certificate is stored in the SICAM GridEdge database and used for the cloud connection. This does not apply to those protocols sending data with the PublisherID of SICAM GridEdge instead.

NOTE

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

NOTE

If you need to update the intermediate certificate authority (for example, 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.

6 Troubleshooting

6.1 Troubeshooting List

Problem	Possible Cause	Solution
Web interface is not reachable	The installation of SICAM GridEdge was unsuccessfull.	Refer to *6.4 Checking the Installation Status*.
	The connection between the SICAM GridEdge installation and the configuration PC is broken.	Refer to *6.3 Checking the Device Connection*.
	At least one device in the substation uses an IP address within the IP address range that is used by SICAM GridEdge.	Refer to *6.2 Adapting IP Ranges for Containers*.
The connection status of IEC 61850 devices is displayed incorrectly in SIPROTEC Dashboard	The time of the host system on which SICAM GridEdge is running differs too much from the time within the cloud platform.	Refer to *6.5 Checking the Time Synchronization*.
Devices are offline or not connected in the cloud platform	The tenant certificate has not been uploaded successfully to the cloud platform.	Check in the cloud platform if the tenant certificate is uploaded successfully Refer to *6.6 Checking the Cloud Connection*.
	The client certificate cannot be generated for the cloud connection (SICAM GridEdge or connected device).	Check in SICAM GridPass (or your prefered certificate manager) if the created certificates are valid and not corrupt. If required, create new certificates. Refer to *6.6 Checking the Cloud Connection*.
	Error message "BadUserNameOrPassword" in diagnosis log No more free resources are available in the cloud platform.	Check in the cloud platform if the resource limit has been reached. If required, order additional resources.

6.2 Adapting IP Ranges for Containers

SICAM GridEdge runs several Docker containers on the host system. Each container has a unique IP address within a range defined by the Docker runtime. This range typically starts from 172.17.0.0/16 (current default). In case one or more devices in your substation use an IP address within this range, SICAM GridEdge will not be able to work properly.

Checking Docker Network Configuration

- Connect to your device using the SSH access.
- Query the IP addresses:

```
sudo ip -4 addr
```

- Check the output for conflicts between the **docker0** adapter and the Ethernet interfaces **enp[...]**.
- In case of no conflict, log off the system.

  – or –
- Create the file **/etc/docker/daemon.json** with the following content:

```
{
  "default-address-pools" : [
    {
      "base" : "172.31.0.0/16",
      "size" : 24
    }
  ]
}
```

✧ Reboot the system:

```
sudo reboot
```

Your system reboots.

6.3 Checking the Device Connection

In case the user interface cannot be reached, the connection between the SICAM GridEdge device and the configuration PC might be broken.

✧ Open a command line interface.

✧ Enter the command **ping** followed by the IP address of the SICAM GridEdge device, for example:

```
ping 192.168.1.190
```

✧ Wait for the reply of the SICAM GridEdge device.

✧ If no reply is received, check the IP configuration that was configured during the SICAM GridEdge installation.

- or -

✧ If no reply is received, check the network configuration with your local IT administrator.

6.4 Checking the Installation Status

In case the user interface cannot be reached, the installation might have been unsuccessfull.

The SSH access is enabled (refer to *4.2.4 Adding SSH Access*).

✧ Connect to your device using the SSH access.

✧ Open a command line interface.

✧ If you have an IPC or a virtual machine, enter the command **sudo docker ps**.

✧ Wait for the reply of the containers.

✧ Check if all containers have the status **Up**.

✧ If the status of at least one container is not **Up**, restart the device or use the command **shutdown --reboot** using the SSH access.

✧ If the status remains unchanged, re-install SICAM GridEdge.

- or -

✧ If the status remains unchanged, contact the customer support.

6.5 Checking the Time Synchronization

In case the time displayed in the upper-right corner of the user interface is incorrect, the connection to the NTP server might be broken.

The SSH access in enabled.

✧ Connect to your device using the SSH access.

✧ Query the state of the time synchronization:

```
ntpq -pn
```

✧ Ensure that a table is displayed containing the IP addresses from which the NTP server will synchronize.

✧ Ensure that at least one line starts with *****.

✧ Ensure that the entries in the column **reach** are not zero (377 is optimal).

✧ If no reply is received or the table does not meet the requirements, check the NTP configuration that was set up during the SICAM GridEdge installation.

- or -

✧ Check the network configuration with your local IT administrator (for example, configuration of the port usage for NTP).

6.6 Checking the Cloud Connection

If the cloud connection cannot be established, there might be a problem with the certificates or the data transmission.

Checking the Certificates

✧ Open the page **Diagnosis**.

✧ Check in the diagnosis log for a certificate that cannot be created.

✧ If a certificate cannot be created, upload the correct certificate in the page **Cloud Connection**.

✧ Select **Show Certificate Details**.

✧ Check if the certificate is expired.

✧ If the certificate is expired, upload a valid certificate.

✧ Check if the issuer of the certificate is the certificate authority uploaded in your cloud platform.

✧ Navigate to your cloud platform and check if the certificate authority is uploaded correctly.

Checking the Data Transmission

✧ Check if your devices or SICAM GridEdge was not onboarded before with the same name in the cloud platform.

✧ If the device or SICAM GridEdge was onboarded with the same name, change the name in the SICAM GridEdge configuration or delete the created device in the cloud platform.

✧ Open the tab **Data Filter** in the page **Cloud Connection**.

✧ Check if data is fetched from the devices via the table of the tab **Data Filter**.

✧ If no data is fetched, configure the data collection in your protocols.
For example for the IEC61850 Client: Make sure **Siemens Grid Diagnostic Suite Profile** is enabled or that **IEC61850 Data-Point Selection and Mapping** is configured.

Glossary

BIOS

Basic input/output system

CA

Certificate authority

CSR

Certificate signing request

CSV

Comma-seperated values

DNS

Domain name system

IEC

International electrotechnical commission

IoT

Internet of things

IPC

Industrial PC

MIB

Management Information Base

MQTT

Message queuing telemetry transport

MV

Measured value

NAS

Network-attached system

OPC UA

OPC unified architecture

OSD

Online software delivery (software ordering portal)

PKCS

Public key cryptography standards

RTU

Remote terminal unit

SPS

Single-point status (single-point indication)

TCP

Transmission control protocol