Configuring of the CloudConnect 7 with Microsoft Azure

TIA Portal V15.1 / SIMATIC CC712 / Cloud / MQTT

https://support.industry.siemens.com/cs/ww/en/view/109766675

Siemens Industry Online Support

Legal information

Use of application examples

Application examples illustrate the solution of automation tasks through an interaction of several components in the form of text, graphics and/or software modules. The application examples are a free service by Siemens AG and/or a subsidiary of Siemens AG ("Siemens"). They are non-binding and make no claim to completeness or functionality regarding configuration and equipment. The application examples merely offer help with typical tasks; they do not constitute customer-specific solutions. You yourself are responsible for the proper and safe operation of the products in accordance with applicable regulations and must also check the function of the respective application example and customize it for your system.
Siemens grants you the non-exclusive, non-sublicensable and non-transferable right to have the application examples used by technically trained personnel. Any change to the application examples is your responsibility. Sharing the application examples with third parties or copying the application examples or excerpts thereof is permitted only in combination with your own products. The application examples are not required to undergo the customary tests and quality inspections of a chargeable product; they may have functional and performance defects as well as errors. It is your responsibility to use them in such a manner that any malfunctions that may occur do not result in property damage or injury to persons.

Disclaimer of liability

Siemens shall not assume any liability, for any legal reason whatsoever, including, without limitation, liability for the usability, availability, completeness and freedom from defects of the application examples as well as for related information, configuration and performance data and any damage caused thereby. This shall not apply in cases of mandatory liability, for example under the German Product Liability Act, or in cases of intent, gross negligence, or culpable loss of life, bodily injury or damage to health, non-compliance with a guarantee, fraudulent non-disclosure of a defect, or culpable breach of material contractual obligations. Claims for damages arising from a breach of material contractual obligations shall however be limited to the foreseeable damage typical of the type of agreement, unless liability arises from intent or gross negligence or is based on loss of life, bodily injury or damage to health. The foregoing provisions do not imply any change in the burden of proof to your detriment. You shall indemnify Siemens against existing or future claims of third parties in this connection except where Siemens is mandatorily liable.
By using the application examples you acknowledge that Siemens cannot be held liable for any damage beyond the liability provisions described.

Other information

Siemens reserves the right to make changes to the application examples at any time without notice. In case of discrepancies between the suggestions in the application examples and other Siemens publications such as catalogs, the content of the other documentation shall have precedence.
The Siemens terms of use (https://support.industry.siemens.com) shall also apply.

Security information

Siemens provides products and solutions with industrial security functions that support the secure operation of plants, systems, machines and networks.
In order to protect plants, systems, machines and networks against cyber threats, it is necessary to implement – and continuously maintain – a holistic, state-of-the-art industrial security concept. Siemens' products and solutions constitute one element of such a concept.
Customers are responsible for preventing unauthorized access to their plants, systems, machines and networks. Such systems, machines and components should only be connected to an enterprise network or the Internet if and to the extent such a connection is necessary and only when appropriate security measures (e.g. firewalls and/or network segmentation) are in place.
For additional information on industrial security measures that may be implemented, please visit https://www.siemens.com/industrialsecurity.
Siemens' products and solutions undergo continuous development to make them more secure. Siemens strongly recommends that product updates are applied as soon as they are available and that the latest product versions are used. Use of product versions that are no longer supported, and failure to apply the latest updates may increase customer's exposure to cyber threats.
To stay informed about product updates, subscribe to the Siemens Industrial Security RSS Feed at: https://www.siemens.com/industrialsecurity.

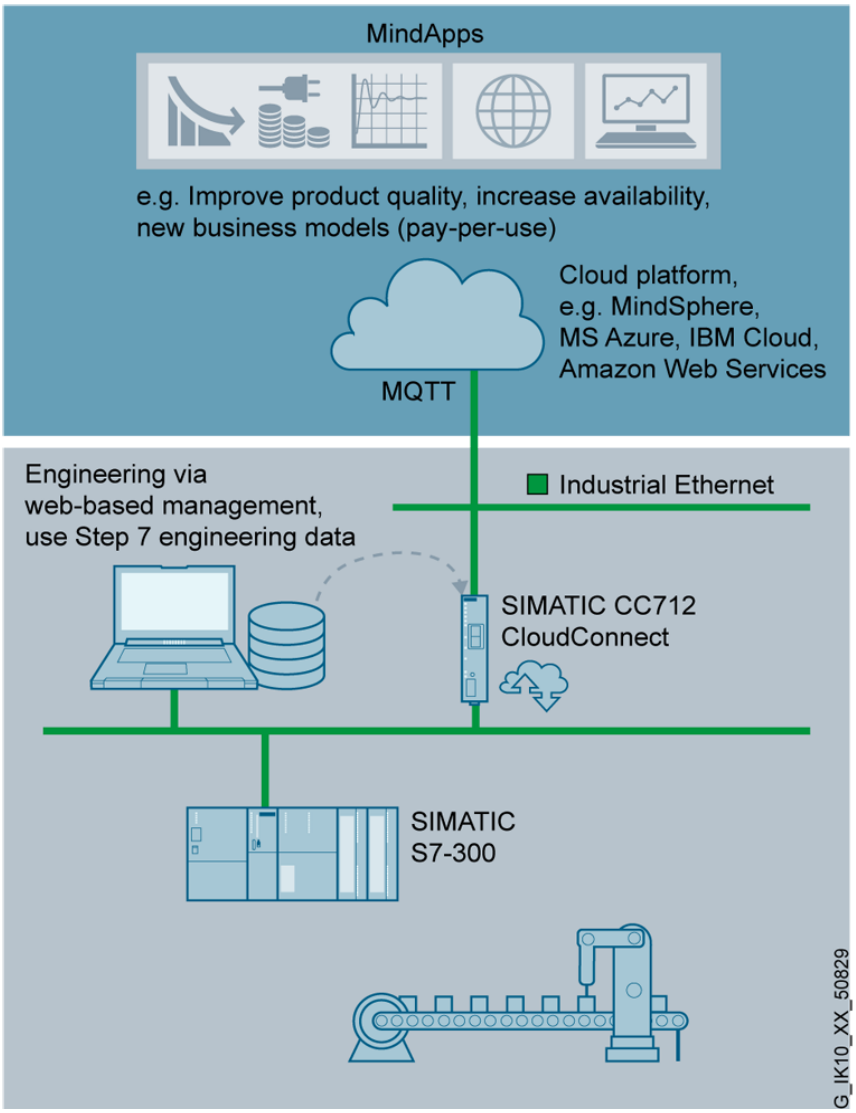
Table of contents

1 Introduction

1.1 Overview

Cloud computing is an important prerequisite for exploiting the benefits of digitization in the industry. With the SIMATIC CloudConnect 7 Industrial IoT Gateways, existing systems can also be easily connected to a wide variety of cloud platforms that support the standardized MQTT protocol, such as Microsoft Azure.

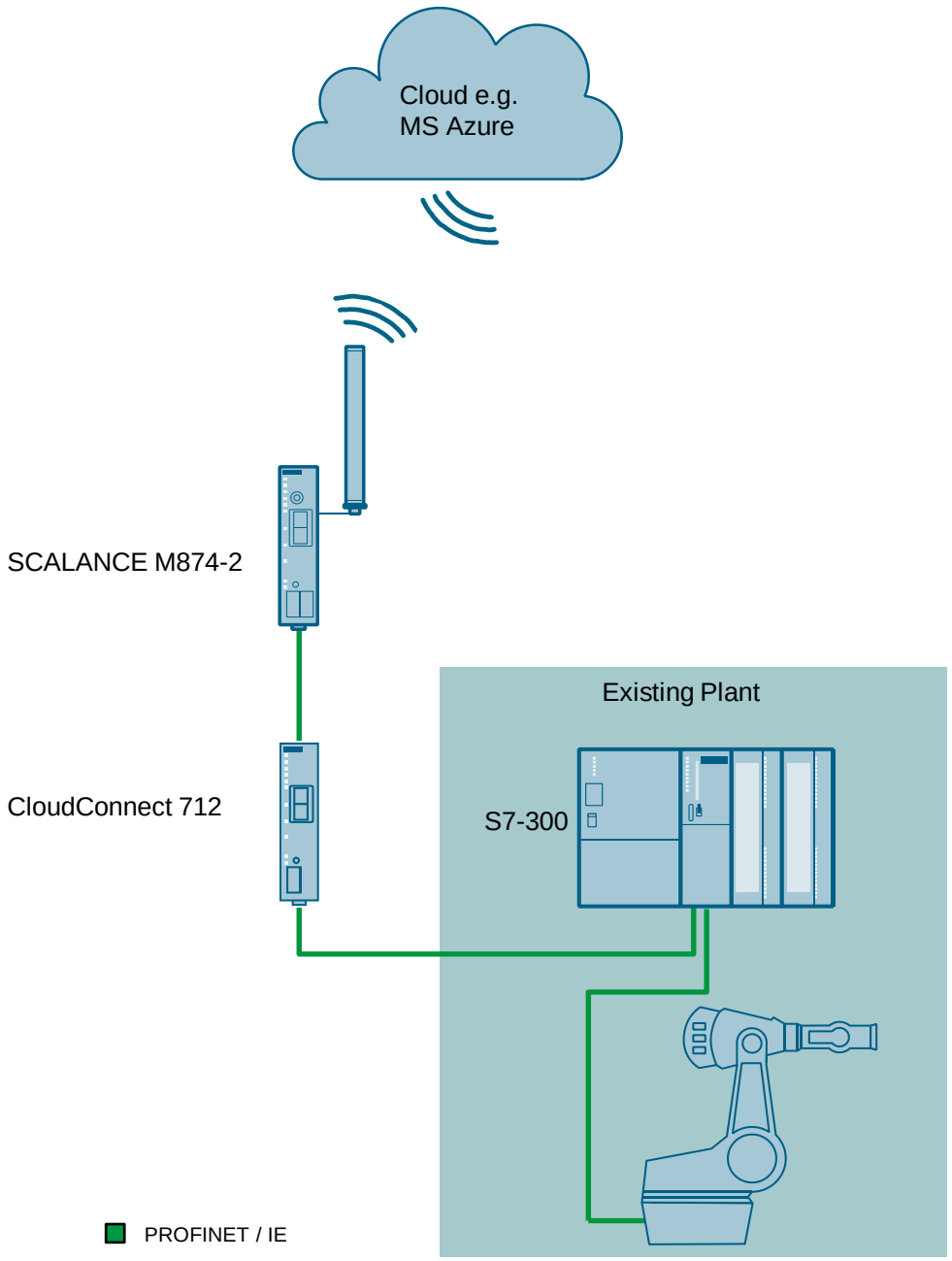
Figure 1-1



1.2 Applicative implementation

The application example shows you how you can connect new and existing systems to a cloud platform. In the example, a SIMATIC S7 300 CPU is connected to Microsoft Azure via Ethernet. This is realized via the IoT Gateway SIMATIC CloudConnect 712. An existing project planning in STEP 7 does not have to be changed, since CloudConnect 712 is configured via its own Web Based Management.

Figure 1-2



1.3 Function principle of the CloudConnect 7 Gateway

The Industrial IoT Gateway SIMATIC CloudConnect 7 (SIMATIC CC7) makes it possible to read data easily and reliably from S7-based devices and transmits them to various cloud platforms such as MindSphere, Microsoft Azure or Amazon Web Services (AWS)using the standardized MQTT protocol. The data management for existing S7 controllers can continue to be imported for quick and easy configuration.

SIMATIC CC712 enables the connection of a SIMATIC CPU via Industrial Ethernet using the S7 protocol.

SIMATIC CC716 enables the connection of up to seven SIMATIC CPUs via Industrial Ethernet or PROFIBUS/MPI.

The connection to Cloud systems via Internet or mobile communication can either be made via an existing network infrastructure or can be directly realized through the combination with the Industrial Ethernet routers SCALANCE M.

In addition, the data read by subordinate S7 stations via SIMATIC CC 7 can be made available as OPC UA variables (server). This enables standardized data exchange, e.g. with MES systems or HMIs and controllers from other manufacturers.

Advantages

- IoT data transfer to cloud-based solutions for existing SIMATIC S7 systems (investment protection).
- Quick and fault-free configuration by data transfer from SIMATIC STEP 7 or TIA Portal
- Event-driven communication reduces the network load and the data exchange costs

Note MQTT is based on a publish/subscribe mechanism. Devices send messages to a topic (Publish). Devices can also create a subscription at the MQTT Broker and receive all subscribed messages forwarded by the broker. The subscriber function is not implemented up until FW 1.1.5.

1.4 Components used

The following hardware and software components were used to create this application example:

Hardware components

Table 1-1

Components	Quantity	Article number	Note
SIMATIC CloudConnect CC712	1	6GK1411-1AC00	Firmware V1.1.5
SCALANCE M874-2	1	6GK5874-2AA00-2AA2	-
SIMATIC S7-300	1	9ES7 315-2EH14-0AB0	-

Software components

Table 1-2

Components	Quantity	Article number	Note
STEP 7 V5.6 SP1	1	6ES7810-4CC11-0YA5	-
Microsoft Azure	1		With the following services: • IoT Hub • Stream Analytics Orders • Storage account
Browsers	1	Any browser	Google Chrome was used.

This application example consists of the following components:

Table 1-3

Components	File name	Note
Documentation	109766675_CloudConnect_Azure_DOC_en_V20.pdf	This document
Project	109766675_CloudConnect_CODE_V20.zip	STEP 7 project and CC 7 project engineering file

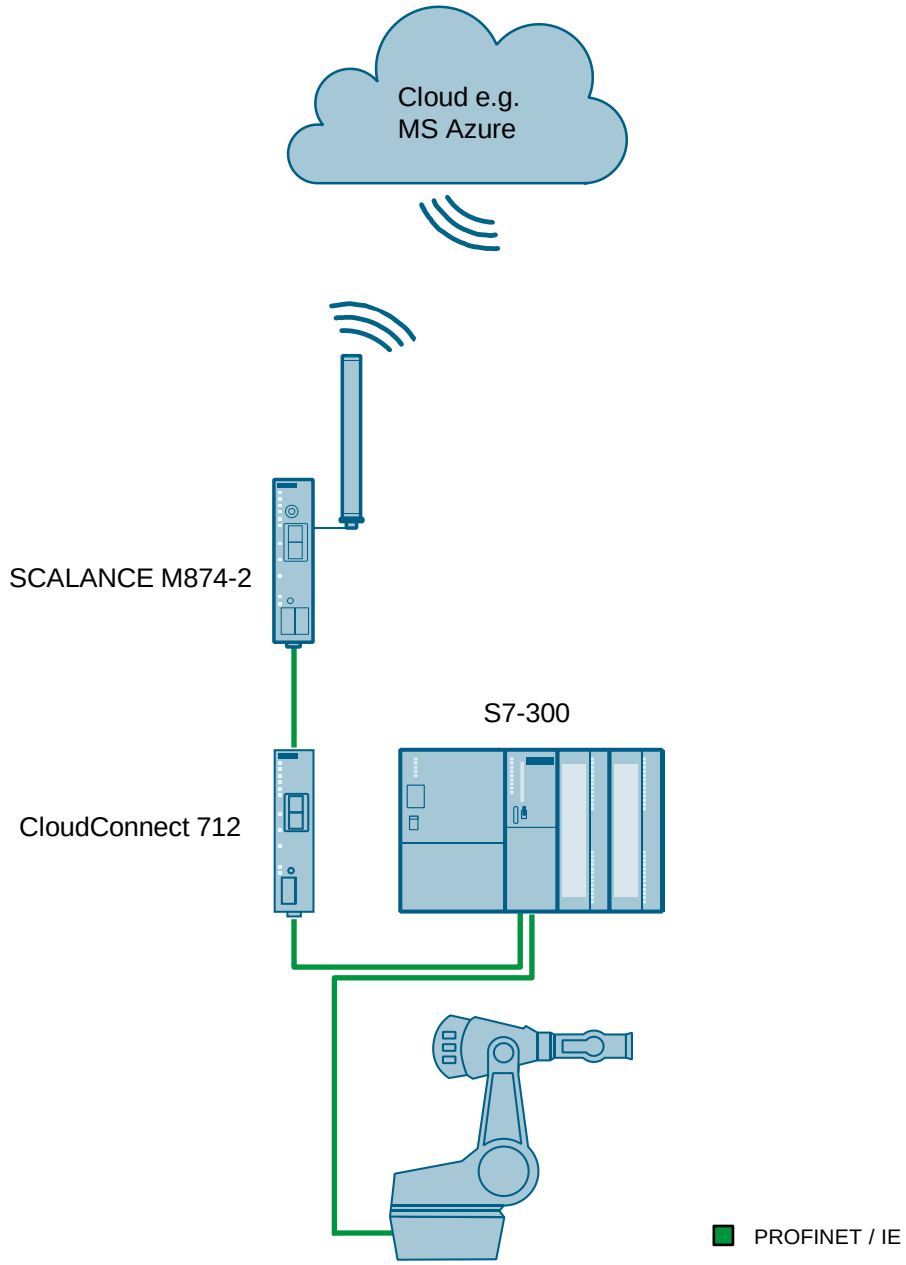
2 Engineering

This chapter shows you the required configuration steps. You will also find instructions on how to put the sample project into operation.

2.1 Hardware setup

In the following figure you can see the hardware structure used in the example:

Figure 2-1



The robot is simulated in a SIMATIC S7-300 CPU.

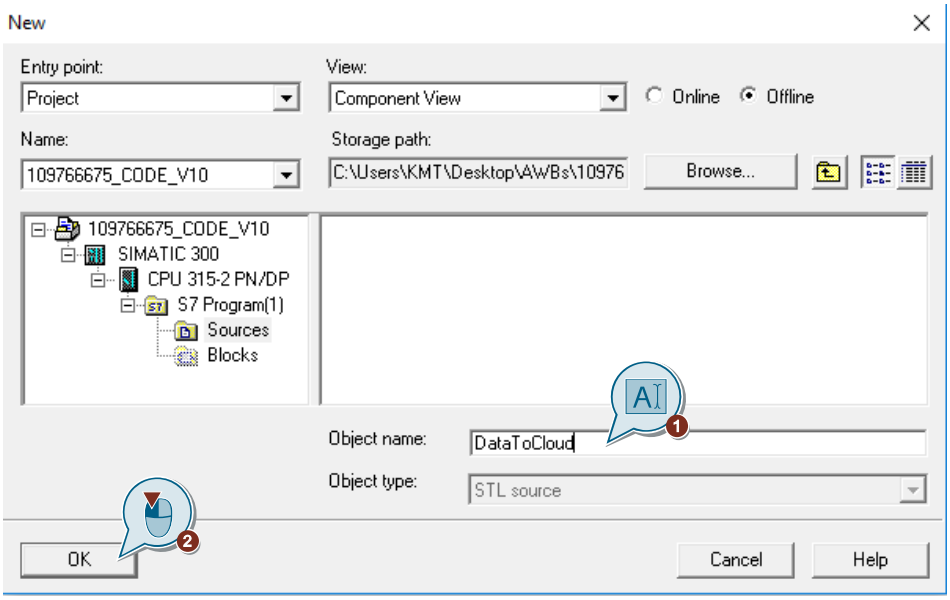
2.2 Configuration

In order to connect your existing system to a cloud service (e.g. MS Azure), project planning in Web Based Management of the CloudConnect 7 gateway and in the cloud used is necessary. You do not have to make any changes to your STEP 7 project if the "PUT/GET" function is activated in the controller. The data points sent to the cloud can be created manually or by importing an existing data block source.

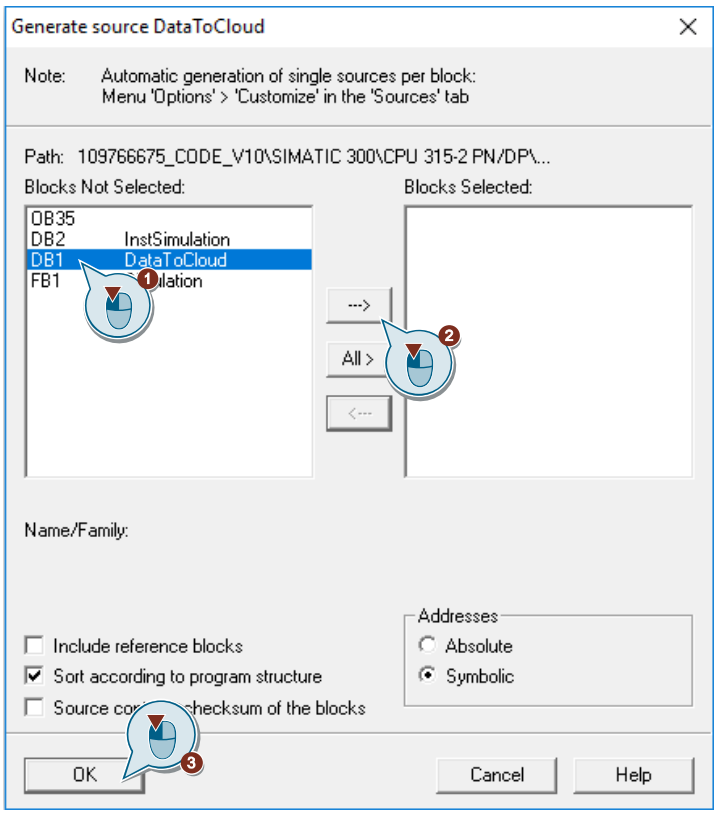
2.2.1 Export data block source from a STEP 7 project

This chapter describes how to create and export a data block source in SIMATIC Manager. The prerequisite for this is that you save/store the relevant data in data blocks. If you want to create the data points manually, you can also select other memory areas.

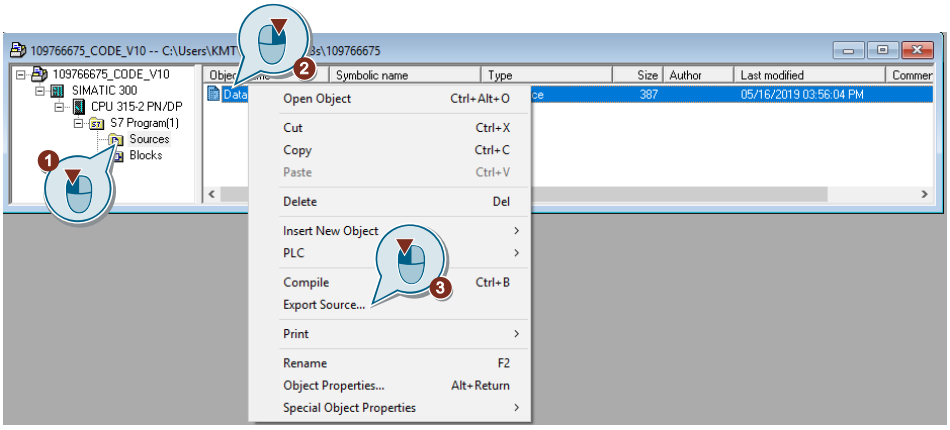
1. Open your STEP 7 project with SIMATIC Manager.
2. Open the editor, e.g. by opening a block.
3. Generate a block source via "File > Generate Source...".
4. Assign a meaningful name (e.g. the name of the data block) and confirm the dialog with "OK".



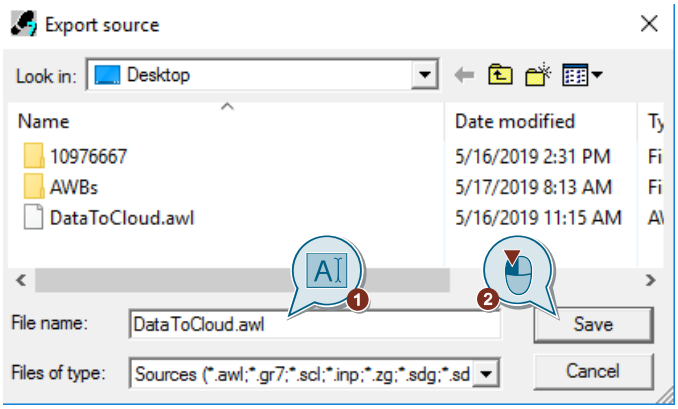
5. Select the data block that contains the data to be sent to the cloud. Click "OK" to confirm your selection.



6. Close the editor and switch to the "Sources" folder. Select the generated source and export it via "Export Source...".



7. Save the file to any location with the ".awl" extension.



The export of the data block as source has been completed.

2.2.2 Commissioning CloudConnect 7

CloudConnect 7 is configured using its own Web Based Management (WBM). No additional software is required.

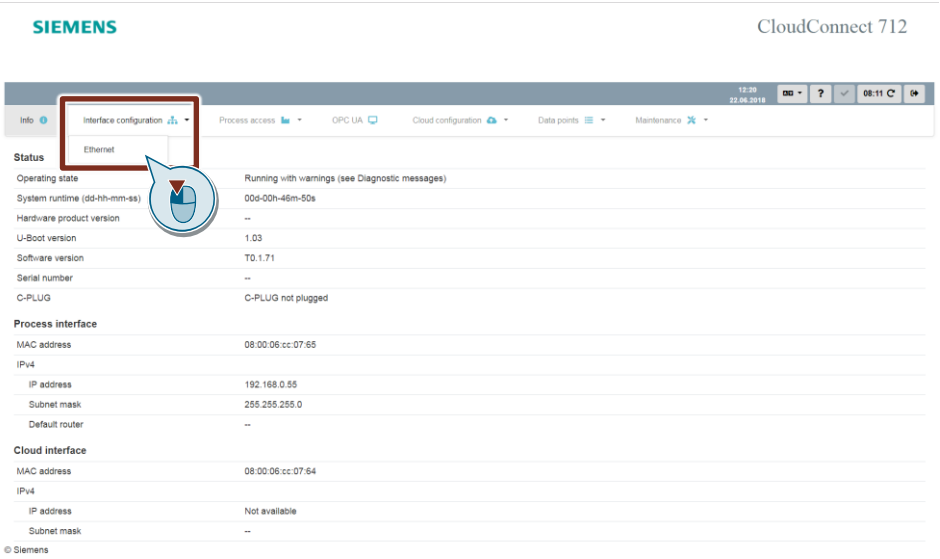
1. Connect your programming device to interface X2.
2. Open any web browser and enter the default IPv4 address in the address bar: "192.168.0.55".
3. Log on to the device with the default user data:
   - User Name: admin
   - Password: admin

   After the first login, you will be prompted to change the access data.

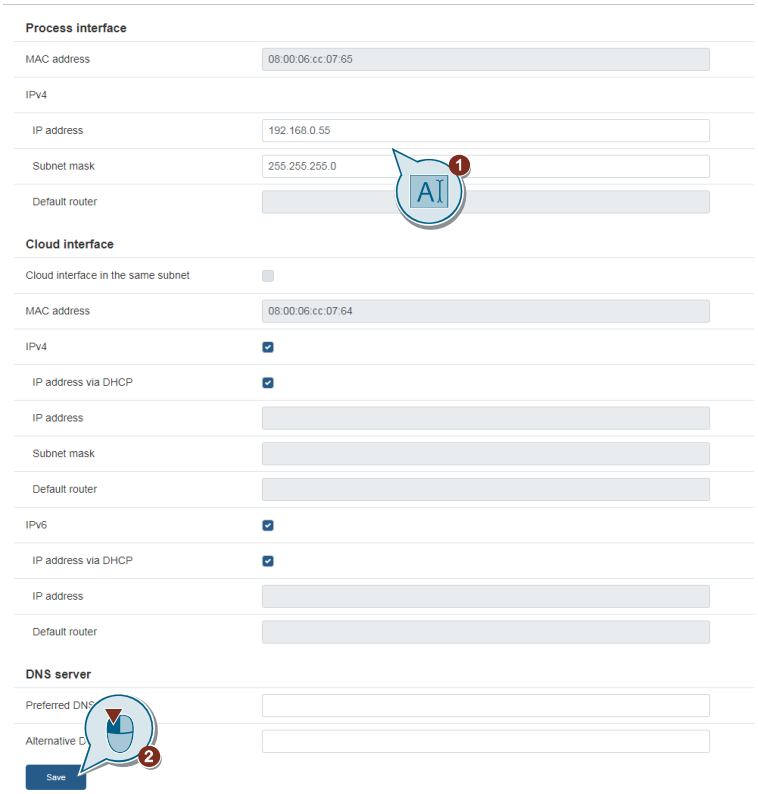
General settings

To make the general settings, proceed as follows:

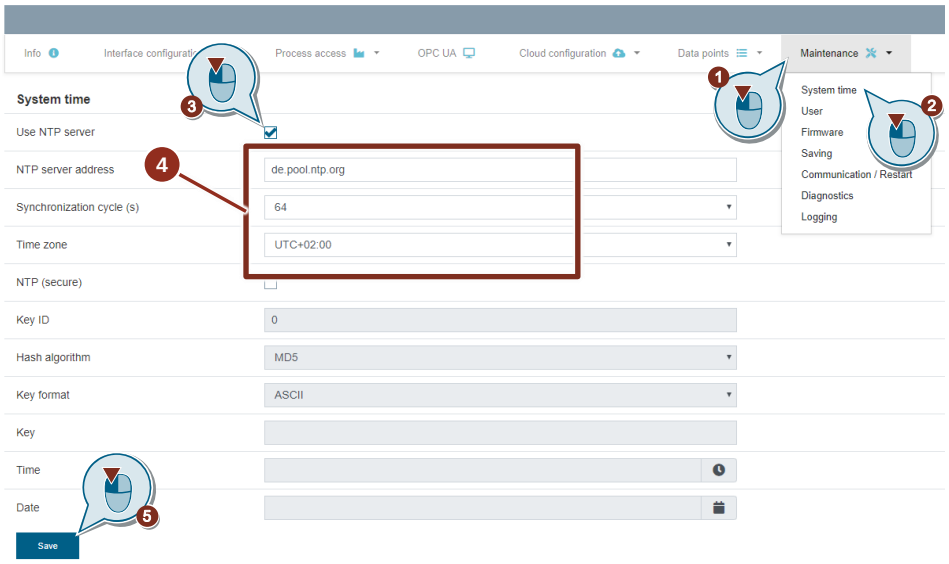
1. Switch to the "Interface configuration" tab.



2. Adapt the IP address and the subnet mask to your system. Save the settings.



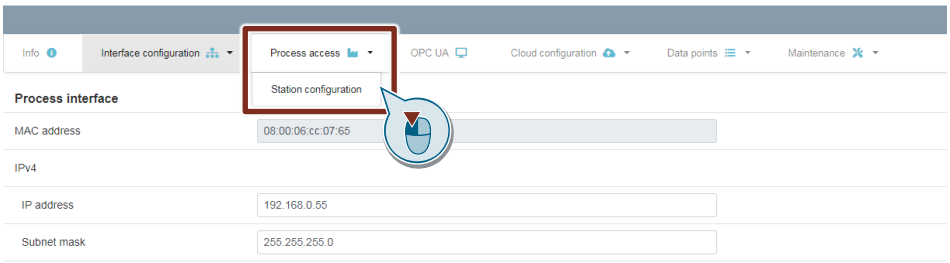
3. Switch to the "Maintenance > System time" tab.
4. Activate the use of an NTP server and set it up.



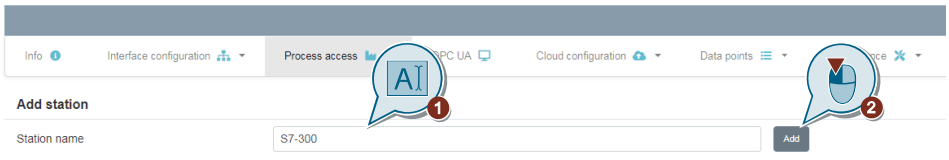
Addition of station

To connect your control to the CloudConnect 7, proceed as follows:

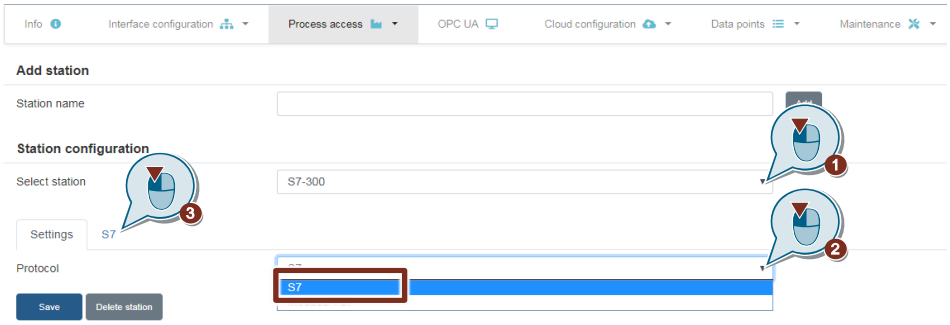
1. Switch to the "Process access" tab.



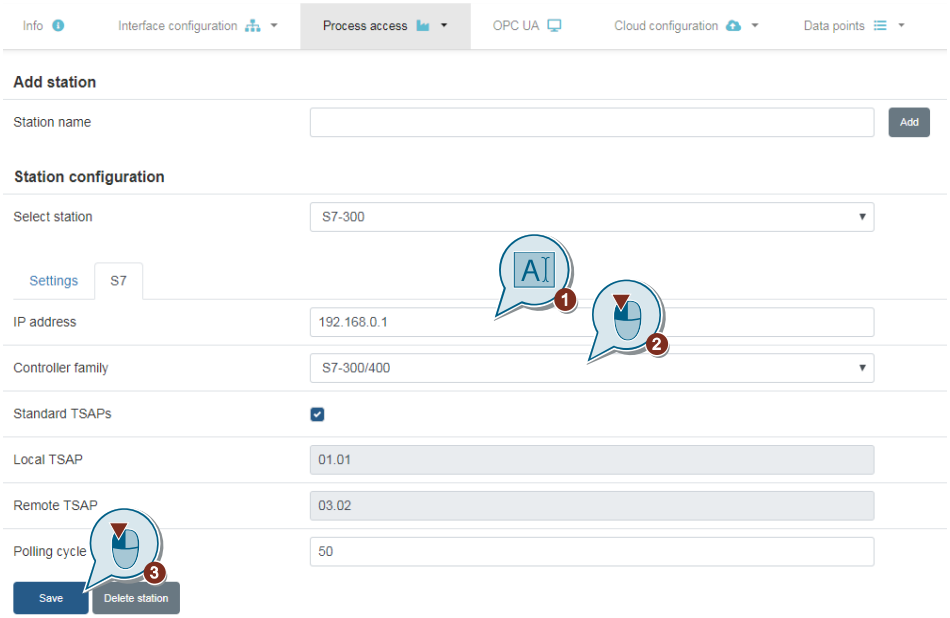
2. Add a new station. Enter the station name and press "Add". Close the following dialog window with "OK".



3. Select the newly created station and select "S7" as protocol for this example. Then switch to the "S7" tab.



4. Enter the IP address of the controller and select the corresponding controller family. If you do not use the standard TSAP, remove the check mark and enter the assigned TSAP. Save the settings.

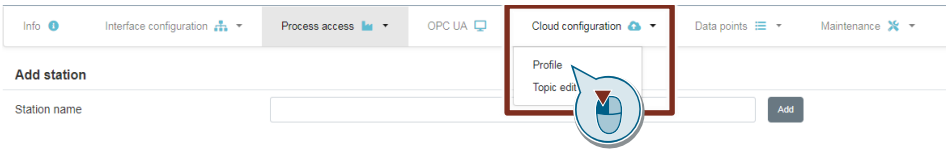


Cloud configuration for connection to Microsoft Azure

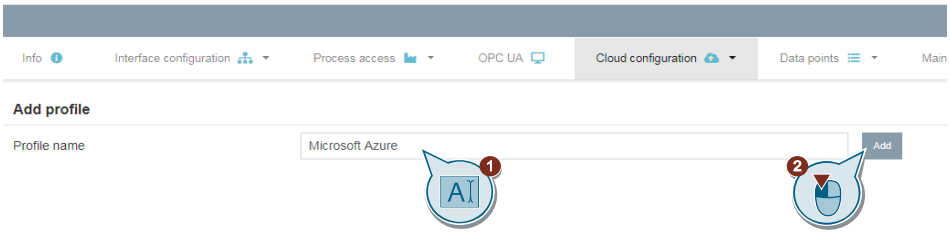
Follow the steps below to connect to Microsoft Azure.

Note To connect to the various cloud systems, you create profiles that contain the configuration data. You can create several profiles, but only one profile can be activated at a time.

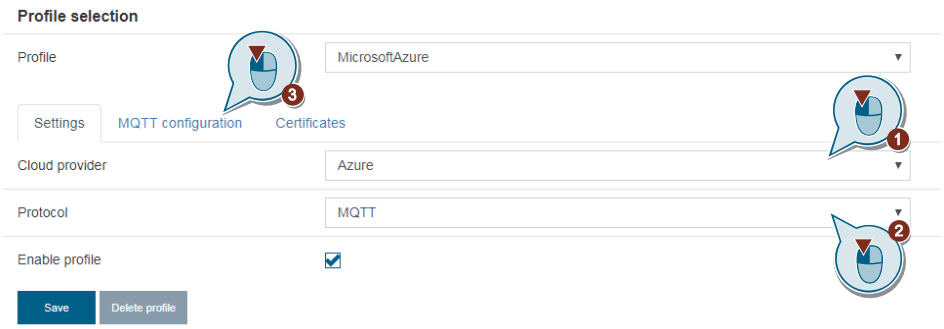
1. Go to the "Cloud configuration > Profile" tab.



2. Enter a meaningful profile name and press "Add". Confirm the dialog with "OK".



3. Select your cloud operator and the protocol to use. Currently only the protocol "MQTT" is supported.
Then switch to the "MQTT configuration" tab.



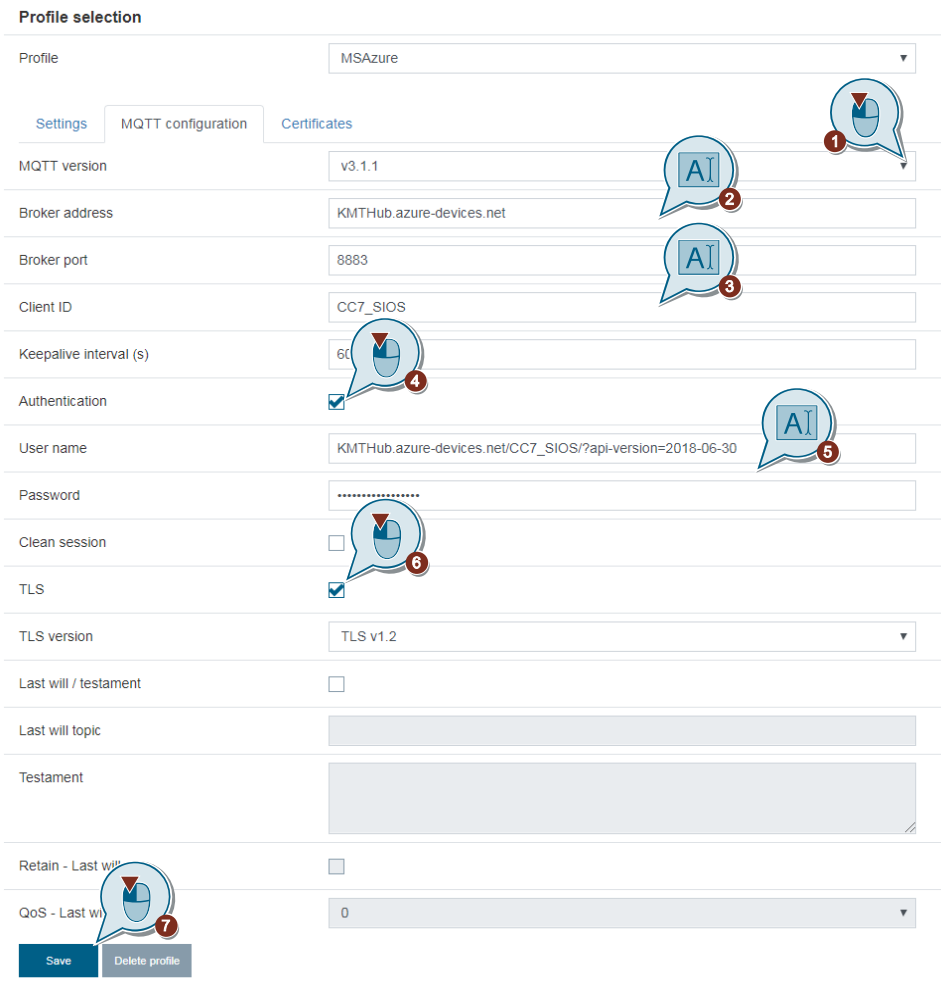
4. Select "v3.1.1" as "MQTT version" and enter the address of your Microsoft Azure IoT Hub as "Broker address". These can be found in the overview of the IoT Hub under "Hostname". The name is composed as follows: "HUBNAME.azure-devices.net".

Note First, create an IoT Hub in MS Azure (see chapter 2.2.3).

5. Enter a unique name as "Client ID". The device logs on to the IoT Hub under this name. Check the box for "Authentication".

6. Enter your credentials for Microsoft Azure. Note that the User name must be prefixed. This consists of your IoT Hub name, a "/", the DeviceId, another "/" and "?api-version=2018-06-30" (e.g. "Siemens.azure-devices.net/CC7_SIOS/?api-version=2018-06-30"). Check "TLS" to activate encryption, select version "v1.2" and save your entries.

Note The password input depends on the authentication procedure. If you use the procedure "X.509 CA Signed", you do not need a password and leave the field empty. If you use the "Symmetric key" procedure, enter the key created in step "Create SAS Token" as the password here.



7. Open a new tab in your browser to download the root certificate from Microsoft Azure. This can be found on the following website: "https://baltimore-cybertrust-root.chain-demos.digicert.com/info/index.html"

   Select the certificate of your region and insert the certificate in any text editor. Save the certificate with the file extension ".cer". Then switch back to the CloudConnector WBM tab.

Root Certificate Details:

Serial Number:
020000B9

Subject:
CN=Baltimore CyberTrust Root
O=Baltimore
OU=CyberTrust
C=IE

Validity period:
Not Before: 12-May-2000
Not After : 12-May-2025

Fingerprints:
MD5: AC:B6:94:A5:9C:17:E0:D7:91:52:9B:B1:97:06:A6:E4
SHA1: D4:DE:20:D0:5E:66:FC:53:FE:1A:50:88:2C:78:DB:28:52:CA:E4:74
SHA256: 16:AF:57:A9:F6:76:B0:AB:12:60:95:AA:5E:BA:DE:F2:2A:B3:11:19:D6:44:AC:95:CD:4B:93:DB:F

Key:
Size: 2048 bit RSA
Key Usage: Certificate Sign, CRL Sign
Basic Constraints: CA:TRUE

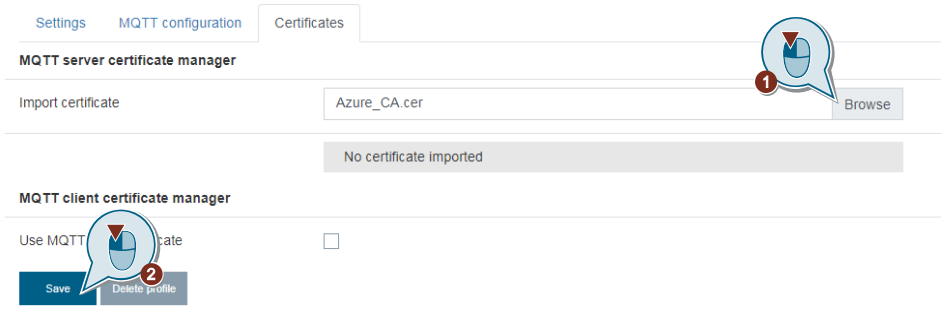
Subject Key Identifier:
E5:9D:59:30:82:47:58:CC:AC:FA:08:54:36:86:7B:3A:B5:04:4D:F0

Signature Algorithm:
sha1WithRSAEncryption

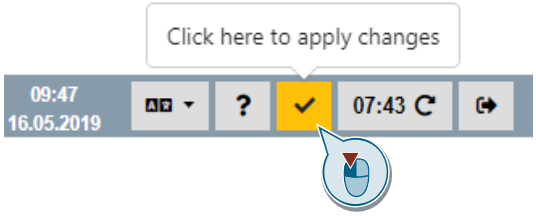
Certificate:

```
-----BEGIN CERTIFICATE-----
MIIDdzCCAl+gAwIBAgIEAgAAuTANBgkqhkiG9w0BAQUFADBaMQswCQYDVQQGEwJJ
RTESMBAGA1UEChMJQmFsdGltb3JlMRMwEQYDVQQLEwpDeWJlclRydXN0MSIwIAYD
VQQDExlCYWx0aW1vcmUgQ3liZXJUcnVzdCBSb290MB4XDTAwMDUxMjE4NDYwMFoX
DTI1MDUxMjIzNTkwMFowWjELMAkGA1UEBhMCSUUxEjAQBgNVBAoTCUJhbHRpbW9y
ZTETMBEGA1UECxMKQ3liZXJUcnVzdDEiMCAGA1UEAxMZQmFsdGltb3JlIEN5YmVy
VHJ1c3QgUm9vdDCCASIwDQYJKoZIhvcNAQEBBQADggEPADCCAQoCggEBAKMEuyKr
mD1X6CZymrV51Cni4eiVgLGw41uOKymaZN+hXe2wCQVt2yguzmKiYv60iNoS6zjr
IZ3AQSsBUnuId9Mcj8e6uYi1agnnc+gRQKfRzMpijS3ljwumUNKoUMMo6vWrJYeK
mpYcqWe4PwzV9/lSEy/CG9VwcPCPwBLKBsua4dnKM3p31vjsufFoREJIE9LAwqSu
XmD+tqYF/LTdB1kC1FkYmGP1pWPgkAx9XbIGevOF6uvUA65ehD5f/xXtabz5OTZy
dc93Uk3zyZAsuT3lySNTPx8kmCFcB5kpvcY67Oduhjprl3RjM71oGDHweI12v/ye
jl0qhqdNkNwnGjkCAwEAAaNFMEMwHQYDVR0OBBYEFOWdWTCCR1jMrPoIVDaGezq1
BE3wMBIGA1UdEwEB/wQIMAYBAf8CAQMwDgYDVR0PAQH/BAQDAgEGMA0GCSqGSIb3
DQEBBQUAA4IBAQCFDF2O5G9RaEIFoN27TyclhAO992T9Ldcw46QQF+vaKSm2eT92
9hkTI7gQCvlYpNRhcL0EYWoSihfVCr3FvDB81ukMJY2GQE/szKN+OMY3EU/t3Wgx
jkzSswF07r51XgdIGn9w/xZchMB5hbgF/X++ZRGjD8ACtPhSNzkE1akxehi/oCr0
Epn3o0WC4zxe9Z2etciefC7IpJ5OCBRLbf1wbWsaY71k5h+3zvDyny67G7fyUIhz
ksLi4xaNmjICq44Y3ekQEe5+NauQrz4wlHrQMz2nZQ/1/I6eYs9HRCwBXbsdtTLS
R9I4LtD+gdwyah617jzV/OeBHRnDJELqYzmp
-----END CERTIFICATE-----
```

8. Switch to the "Certificates" tab. Select the certificate you just saved and save the settings. Confirm the dialog that opens with "OK".



9. Activate the settings you have made. The device automatically logs into Microsoft Azure at the IoT Hub.



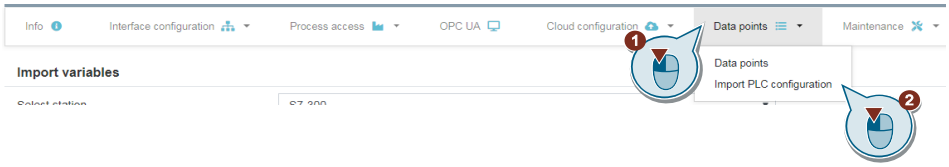
Creating data points

You have two options for creating data points. Either you create each data point manually or you import a data block source that contains the data points.

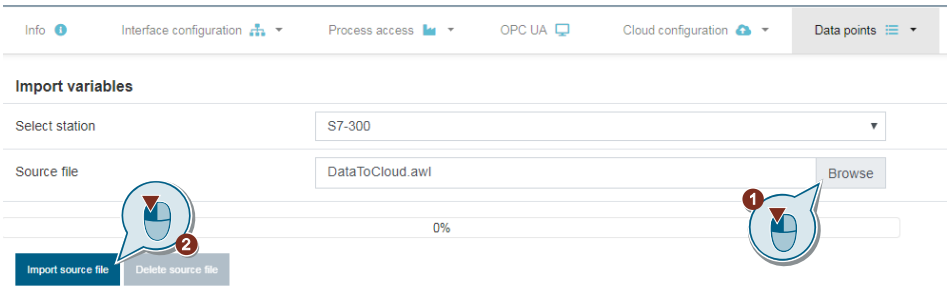
The following configurations are shown using MS Azure as an example.

Importing the data points

1. Switch to the "Data points > Import PLC configuration" tab.



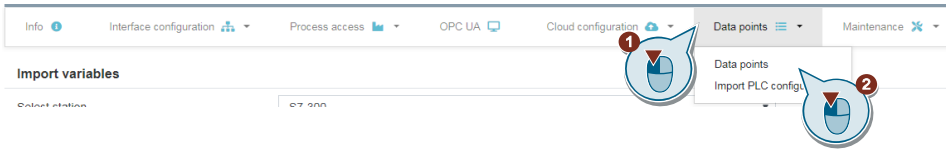
2. Select the block source created in chapter 2.2.1 and import the file.



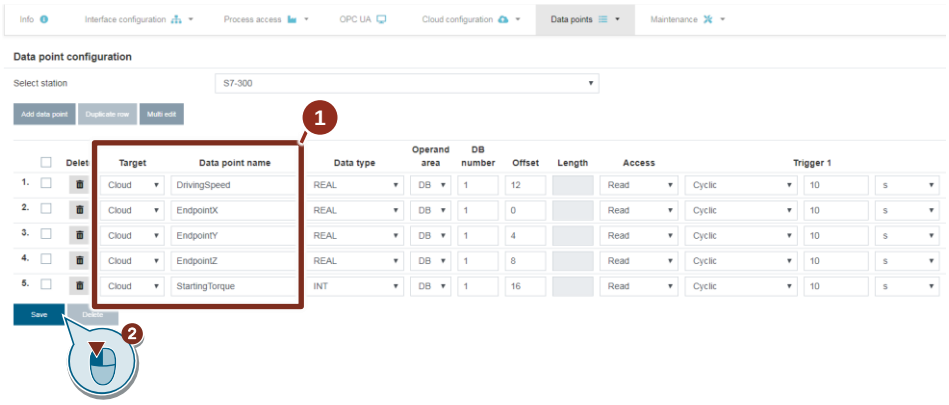
3. Select the data points you want to import or import all data points.

Note If you want to import data points from several data blocks, first import all the required data points before you start the assignment.

4. Change to the tab "Data points > Data points".

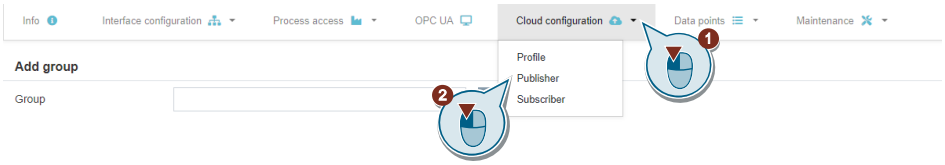


5. Select "Cloud" as "Target" and adjust the names of the data points if necessary. Save the settings.



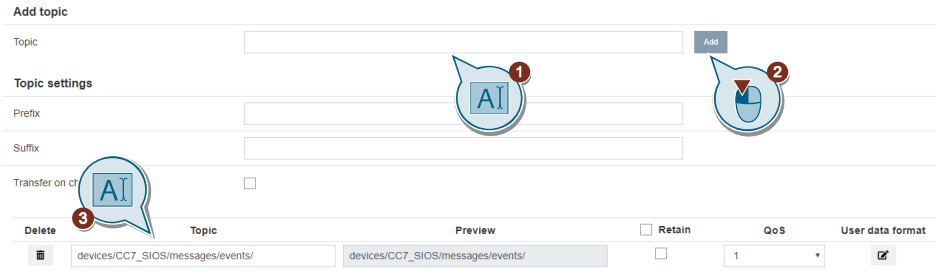
Note With firmware V1.1.5 there is an error with the name resolution. Remove the special characters from the datapoint names.

6. Switch to the tab "Cloud configuration > Publisher".



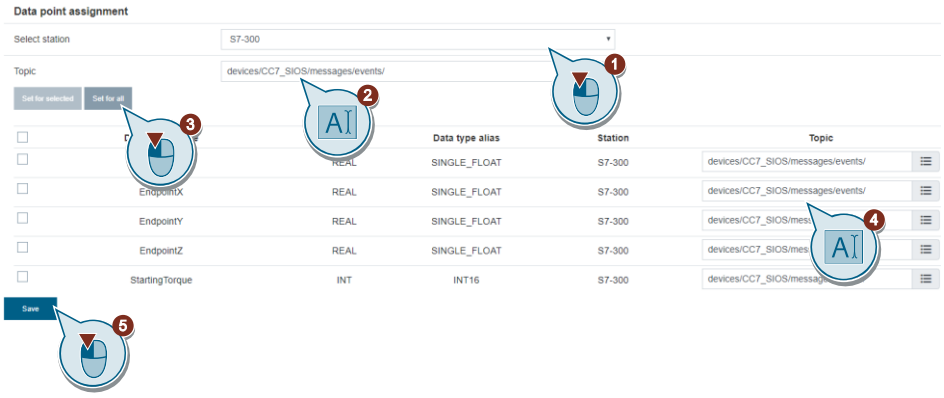
Note No groups can be created for an active Azure profile.

7. Create a new topic.

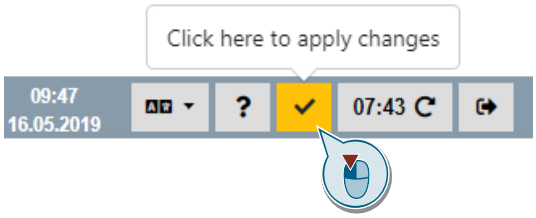


Note The topic must meet cloud specific requirements. For Microsoft Azure, enter "devices/{device_id}/messages/events/" (default endpoint).

8. Assign the data points to the newly created topic.

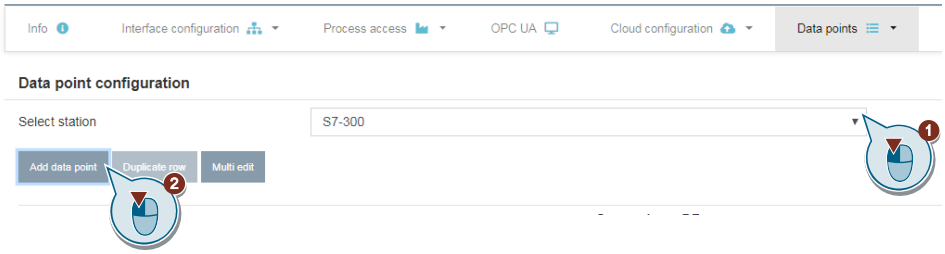


9. Activate the settings you have made.

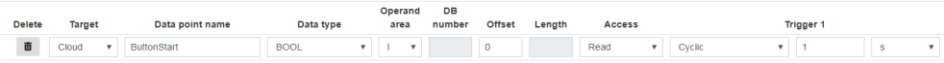


Manual creation of the data points

1. Go to the "Data Points > Data Points" tab.
2. Select the control and add a new data point.

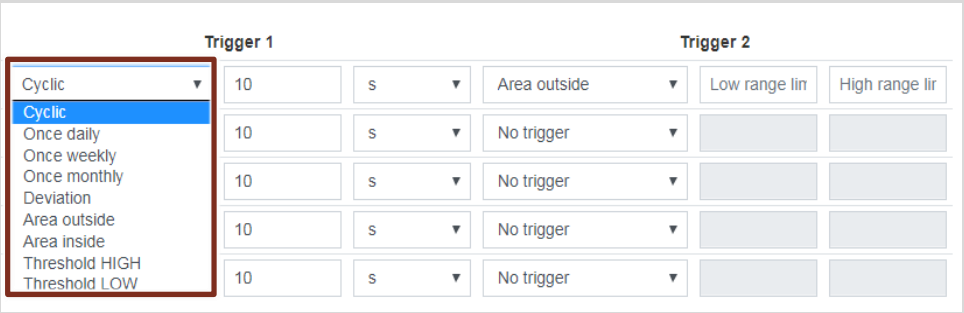


3. Configure the data point as necessary and then save the parameterization.

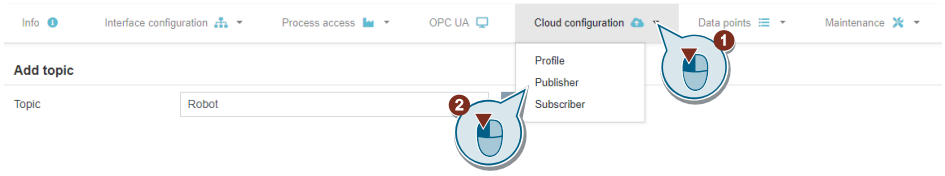


Note

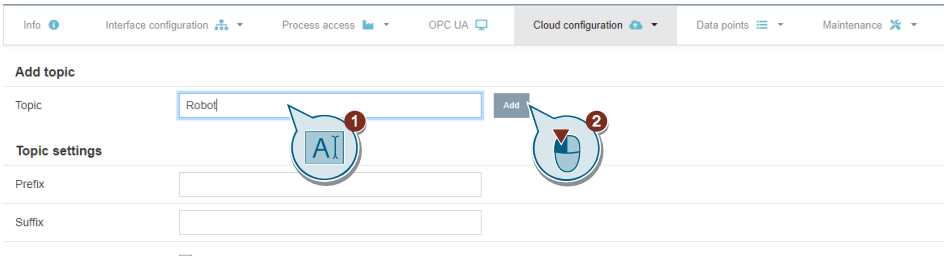
You can configure two different triggers per data point. You can see the different trigger types in the picture.



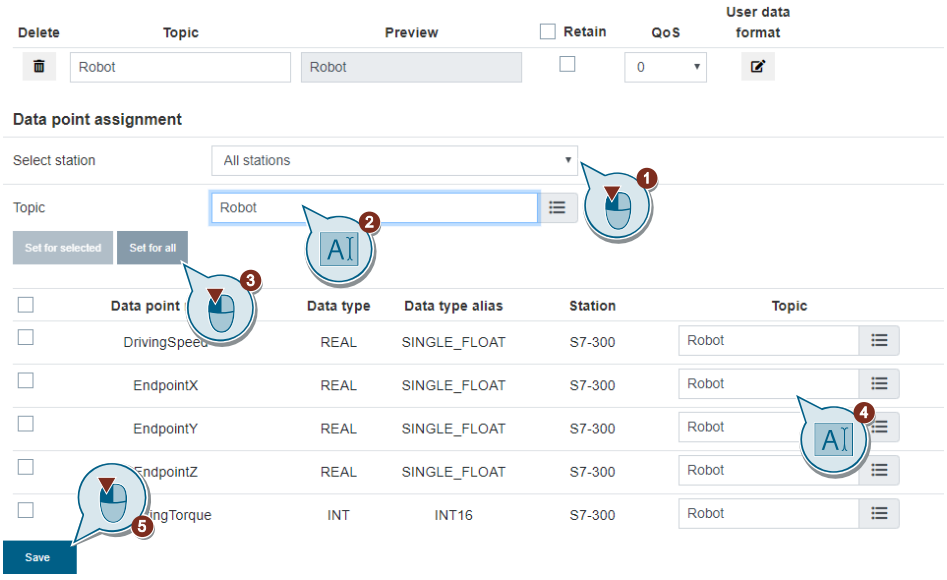
4. Switch to the "Cloud configuration > Publisher" tab.



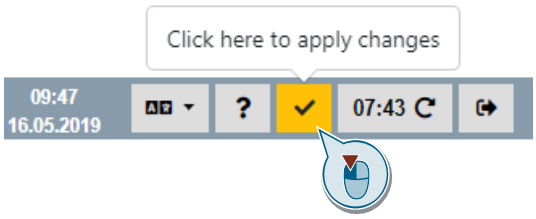
5. Create a new topic.



6. Assign the data points to the newly created topic.



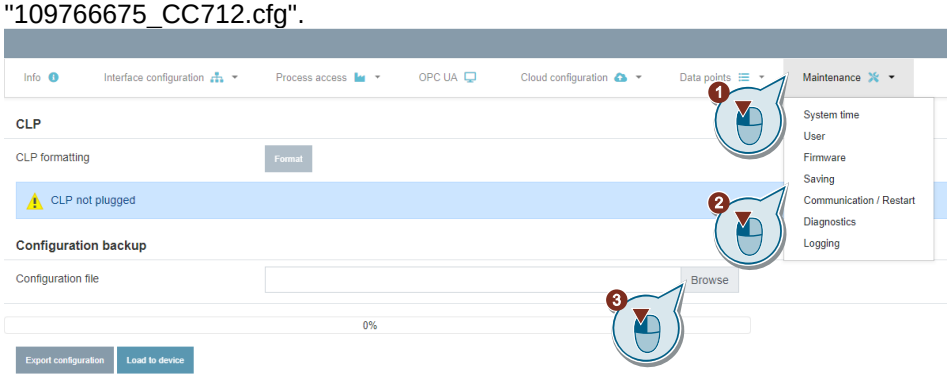
7. Activate the settings you have made.



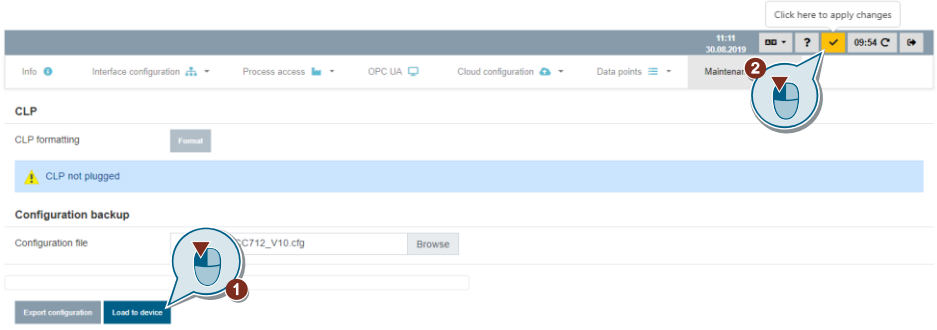
Import of the project file

To save yourself the general project engineering effort, you can load the supplied project file into CloudConnect 7.

1. Switch to the "Maintenance > Saving" tab and select the downloaded file "109766675_CC712.cfg".



2. Load the file and confirm the dialogs. Then activate the changes.



Hinweis The user data is not changed. The certificates of the profiles have to be imported again.

2.2.3 Setting up Microsoft Azure

To integrate CloudConnect 7 as a gateway into Microsoft Azure, you need the following service:

- IoT Hub.

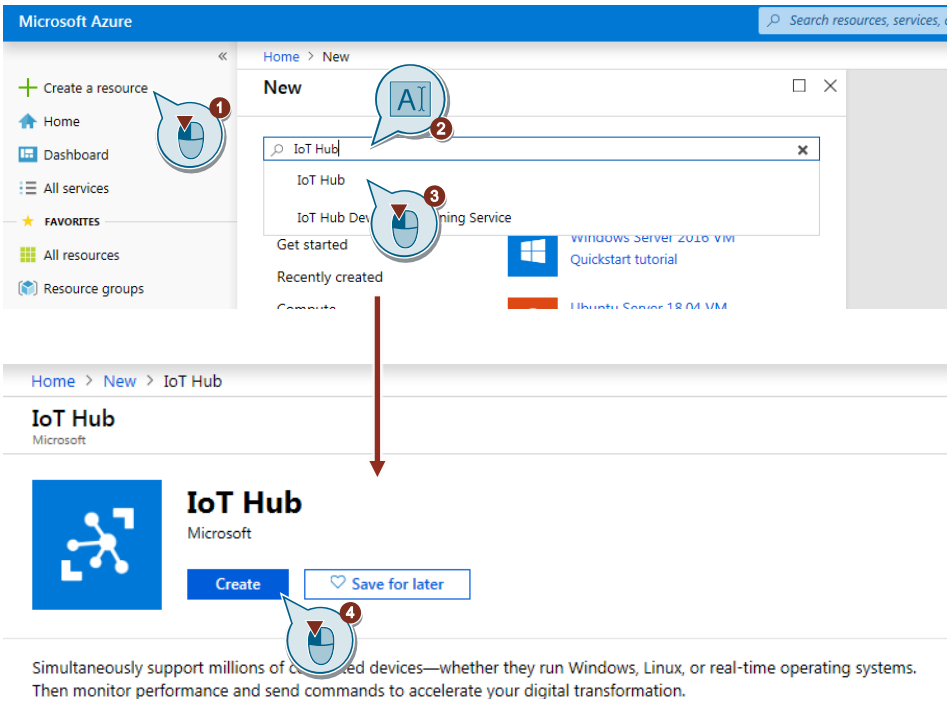
The display of the data can be realized in different ways. The following services were used in the application example:

- Stream Analytics Orders
- Storage account

Creating IoT Hub

To connect CloudConnect 7 Gateways you have to create an IoT Hub.

1. Log in with your Microsoft Azure account on "https://portal.azure.com/".
2. Create a new IoT Hub via "Create a resource > Create".



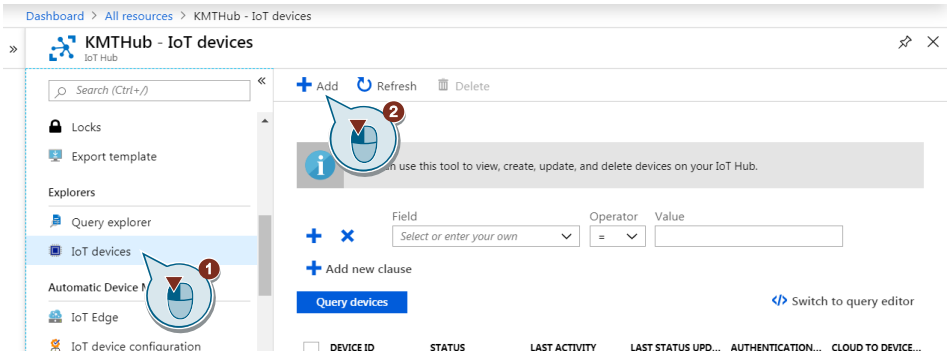
3. Enter all the relevant data and complete the creation.

Note You can create one free IoT Hub per Azure subscription for testing purposes. In the "Size and scale" tab, select "F1: Free tier".

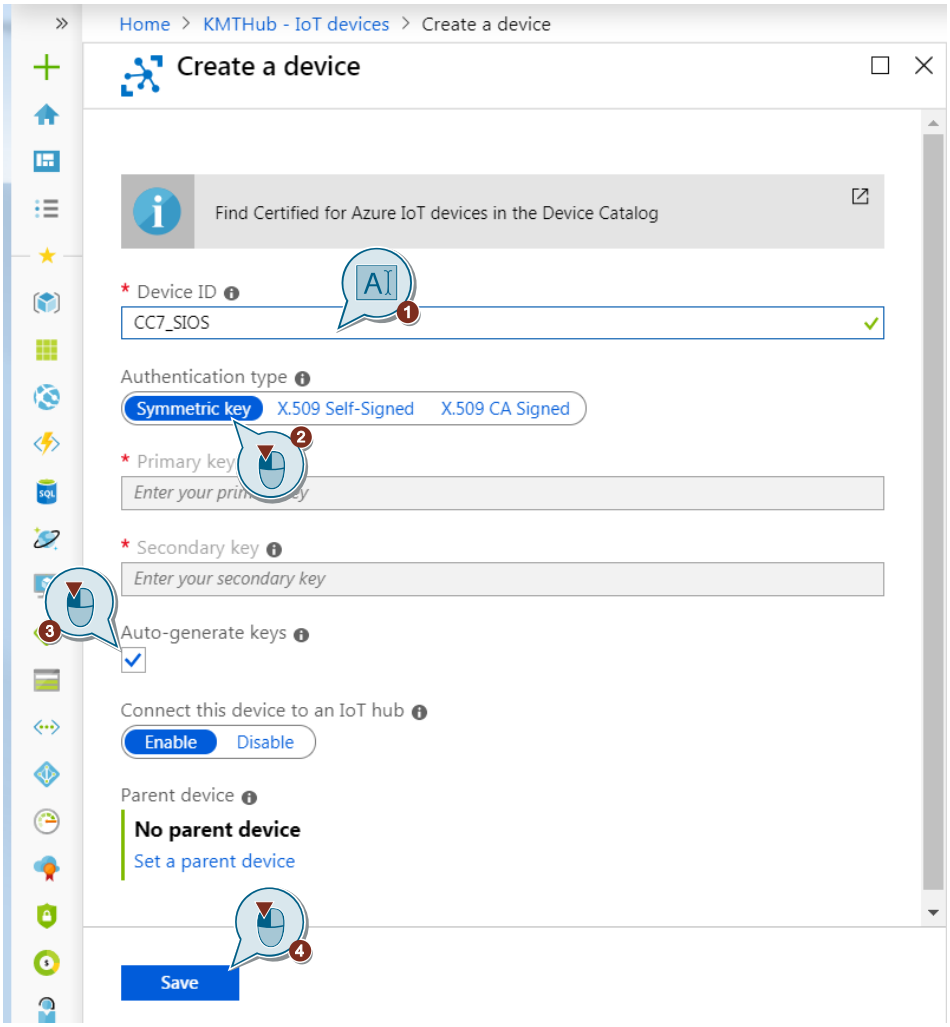
Creating device in IoT Hub

In the following chapter you create a device with the authentication method "Symmetric key".

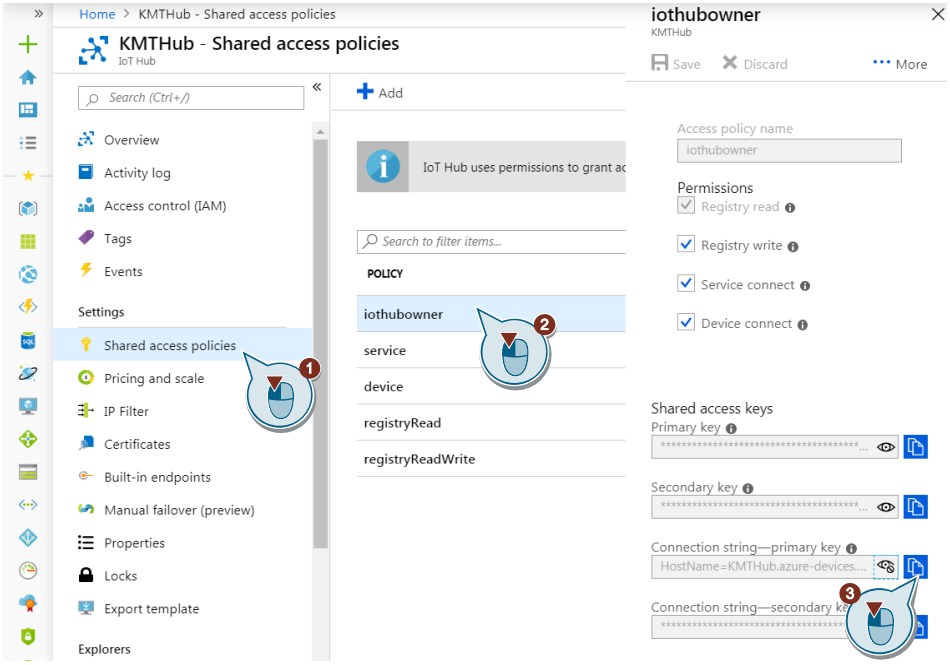
1. Add a new device via "IoT devices > Add".



2. Enter the "Device ID" assigned in chapter 2.2.2 and select "Symmetric key". Activate the option "Auto-generate keys" and save the settings.



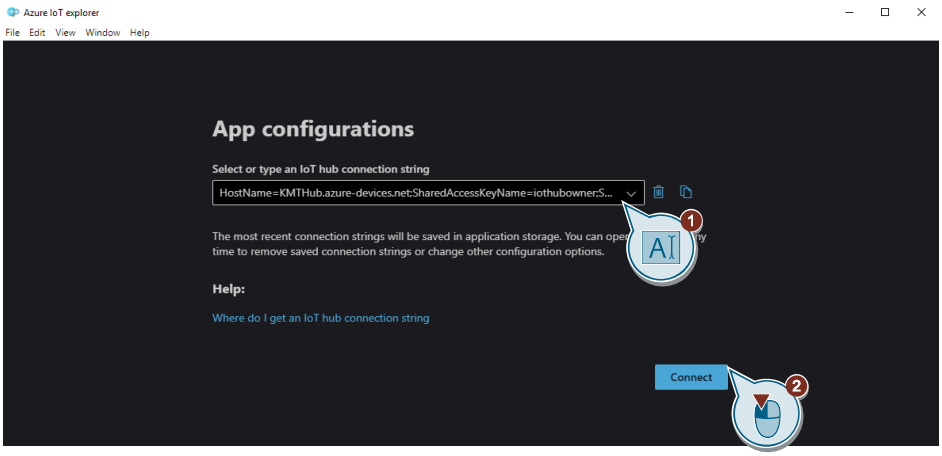
3. Navigate to "Shared access policies" and copy the "Connection string - primary key" of the "iothubowner" policy. You need this key once for the setup of the "Azure IoT Explorer".



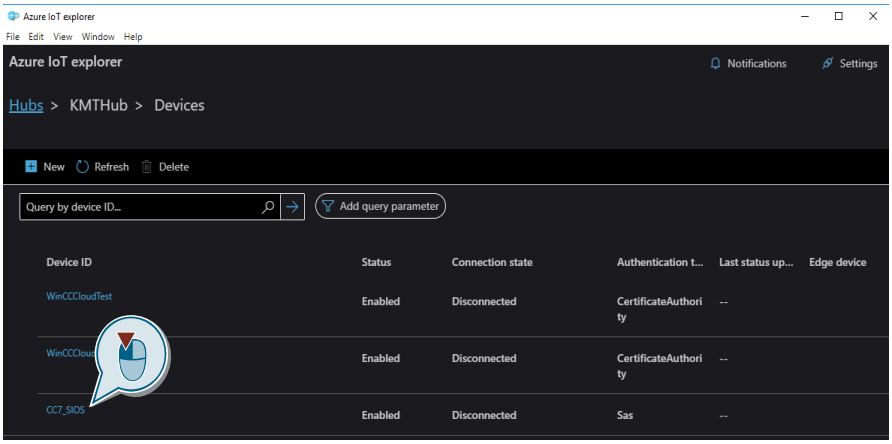
4. Download the "Azure IoT Explorer" from the following website: \6\ and install it on your PC.

Note Use Version V0.10.15 or higher.

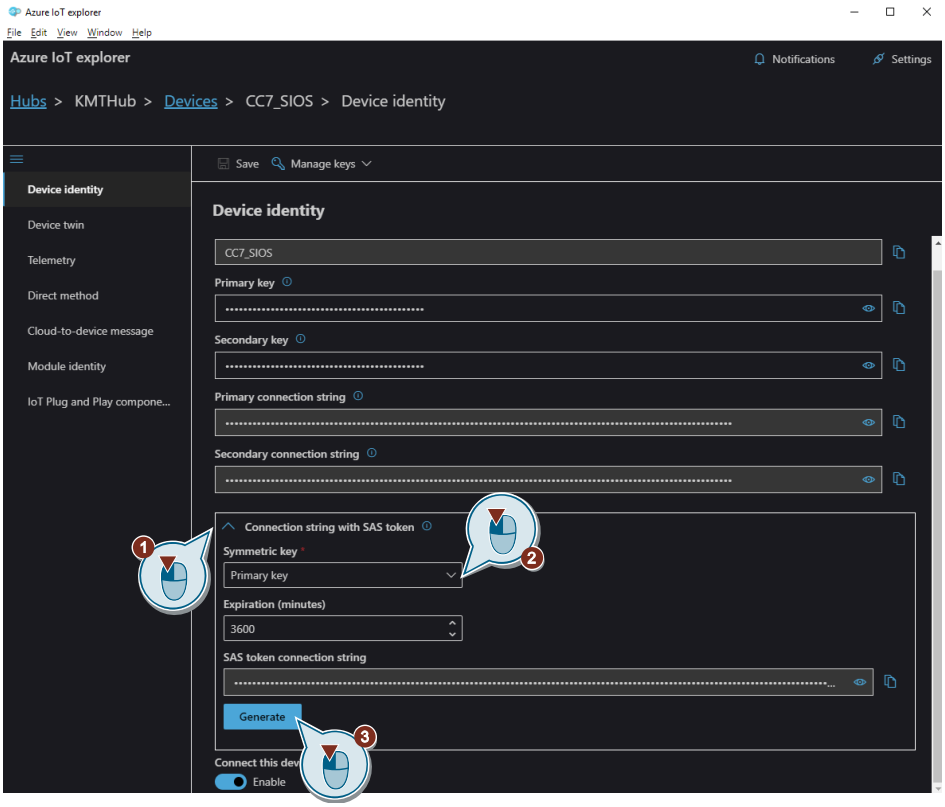
5. Start the Device Explorer and insert the connection string and the hostname of your IoT Hub. Then click on "Connect".



6. Click on your newly created Device.



7. Generate a "SAS Token" as shown in the picture.



8. Display the generated token and copy the string to "[...]SharedAccessSignature=". This part of the SAS token serves as the password in the CloudConnect 7 configuration. Save it and exit the Azure IoT Explorer.

Setting up a Blob memory and a Stream Analytics job

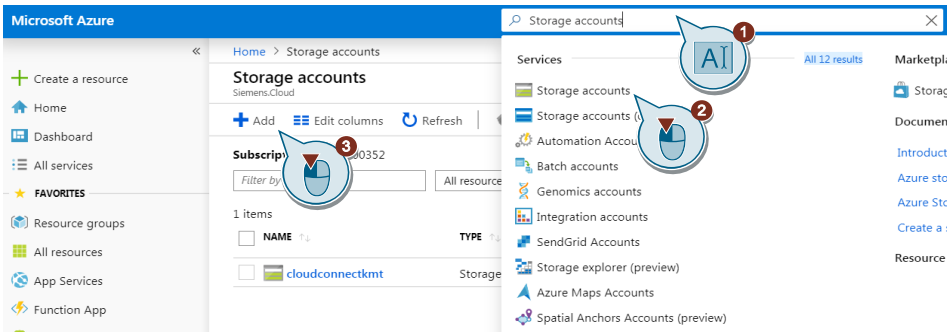
In this chapter, you set up a storage account and a Stream Analytics job so that you can store the data in Microsoft Azure. The data can be further processed at any time.

Note

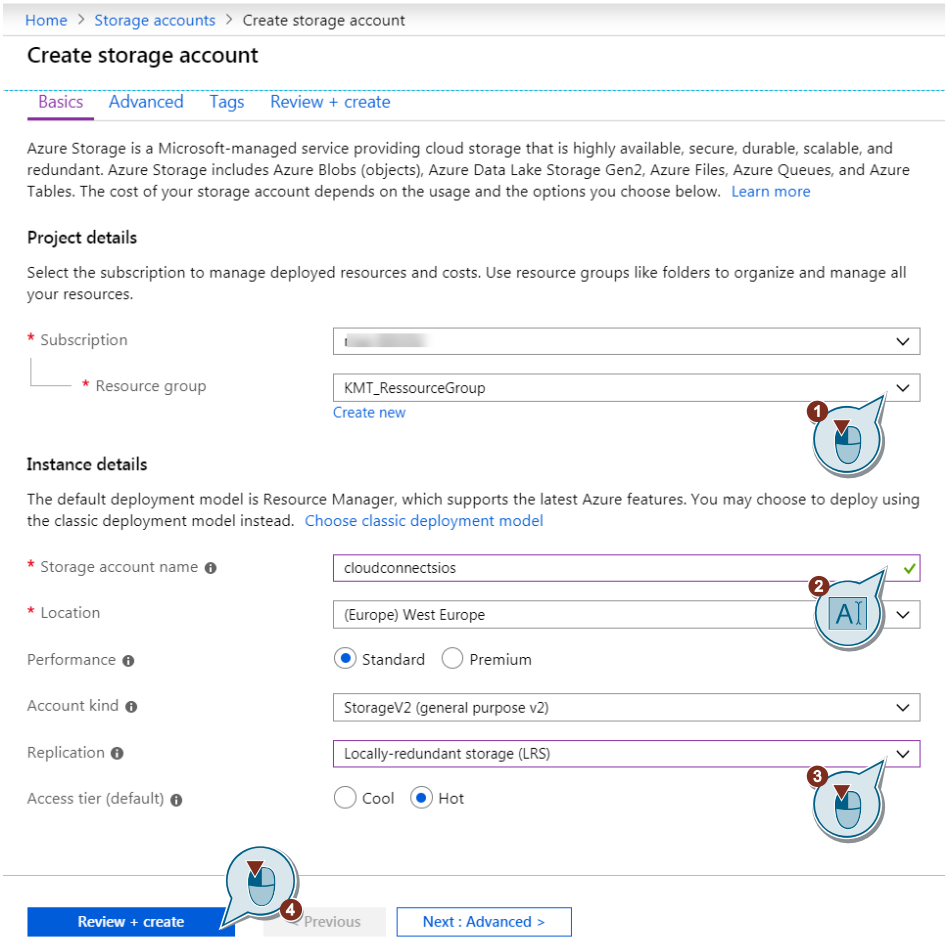
The services used here are not free of charge. The costs are based on usage and can be viewed on the following pages.
"https://azure.microsoft.com/en-us/pricing/details/storage/"

"https://azure.microsoft.com/en-us/pricing/details/stream-analytics/"

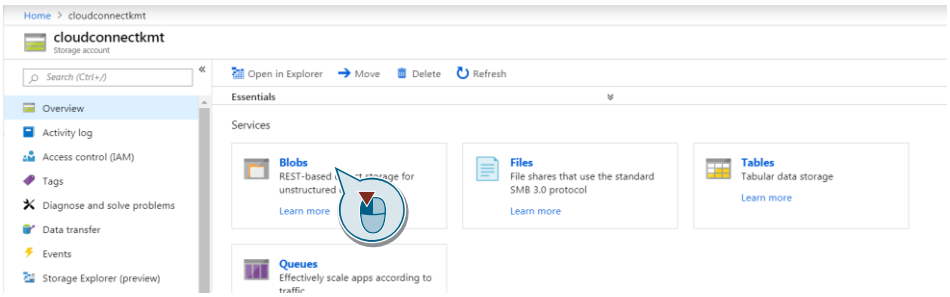
1. Switch over to the Azure Portal. Now set up a storage account so that the CloudConnect 7 data can be stored.
2. Locate the "Storage accounts" service and add a new account there.



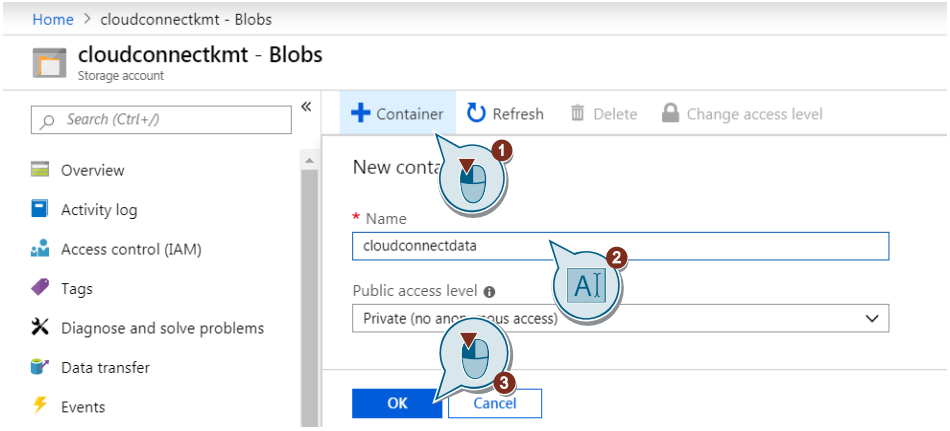
3. Select your resource group and then enter a globally unique name for the storage account. Select any redundancy setting ("Replication"). LRS is the most cost-effective variant. Confirm the settings with "Review + Create".



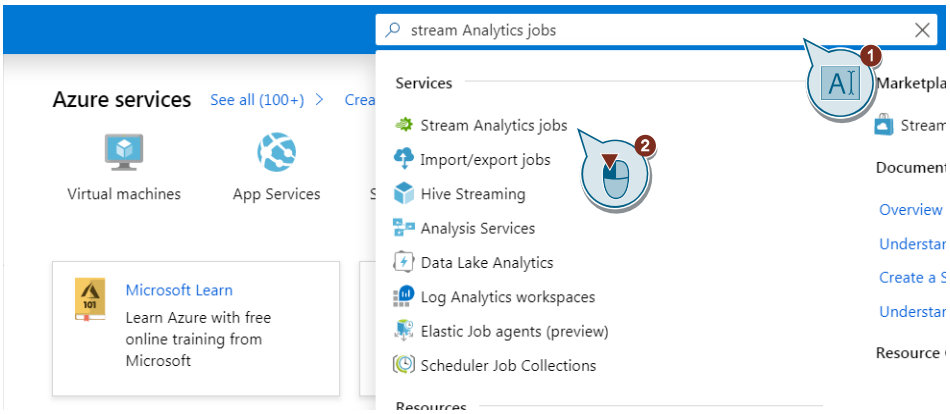
4. Check your entries and confirm them with "Create".
5. Open the storage account you just created and create a blob of storage. Click on "Blobs".



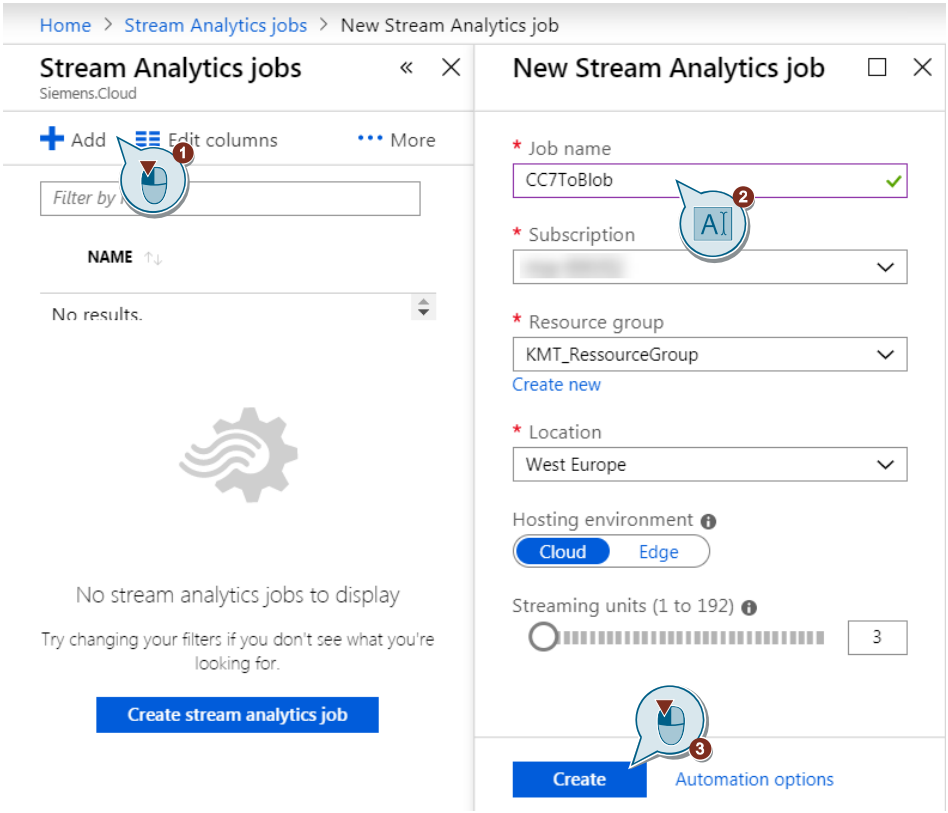
6. Create a new "container". Enter a name and confirm the setting with "OK".



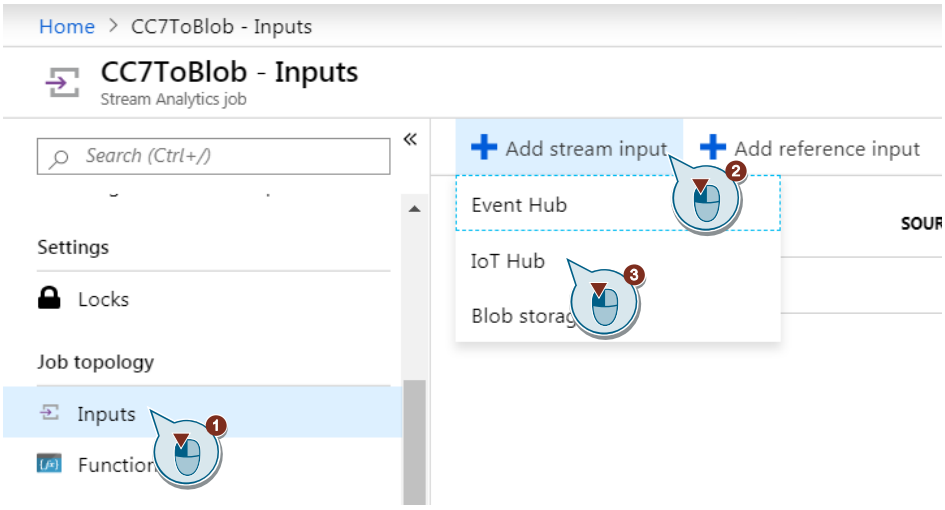
7. Now set up a "Stream Analytics Job" that writes the CloudConnect 7 data to the blob storage account you just created. Search for the service "Stream Analytics jobs" and add a new account there.



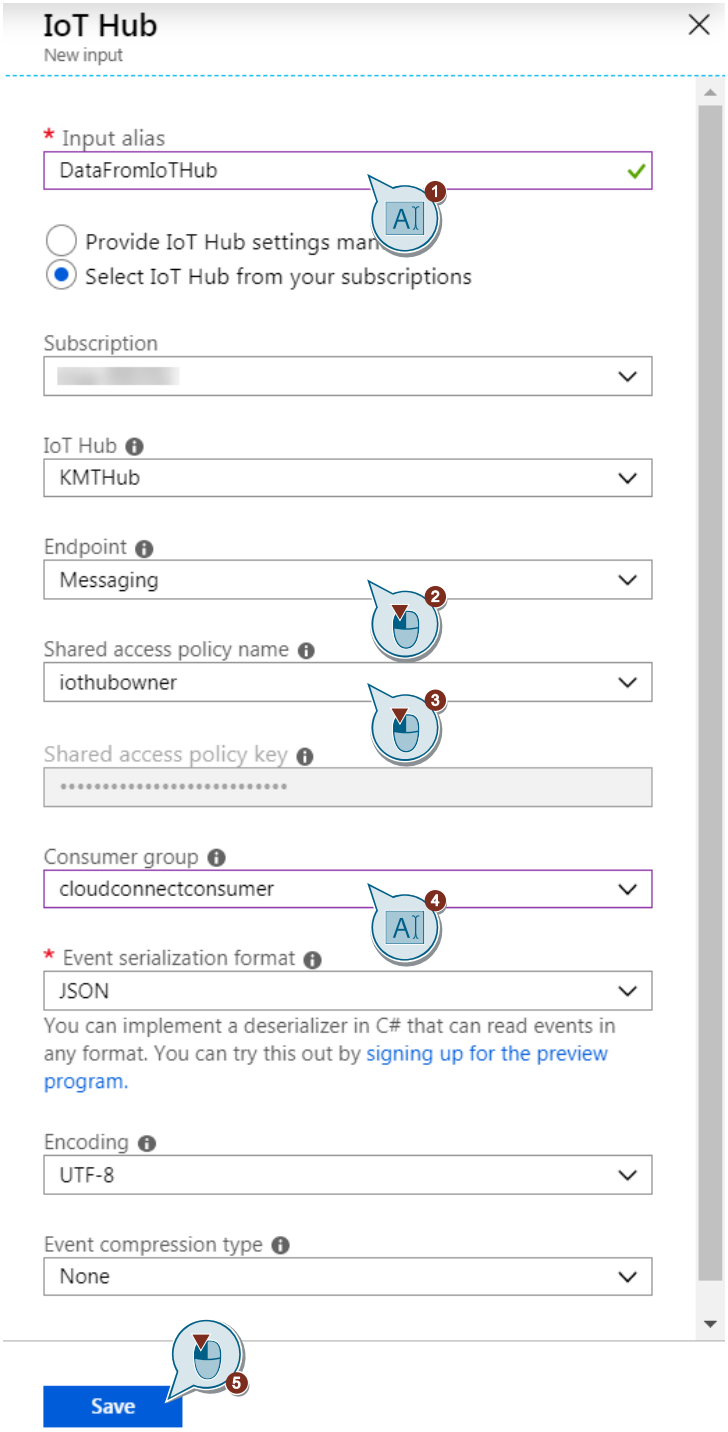
8. Find the service "Stream Analytics jobs" and add a new account to it. Then assign a unique name and confirm the entries with "Create".



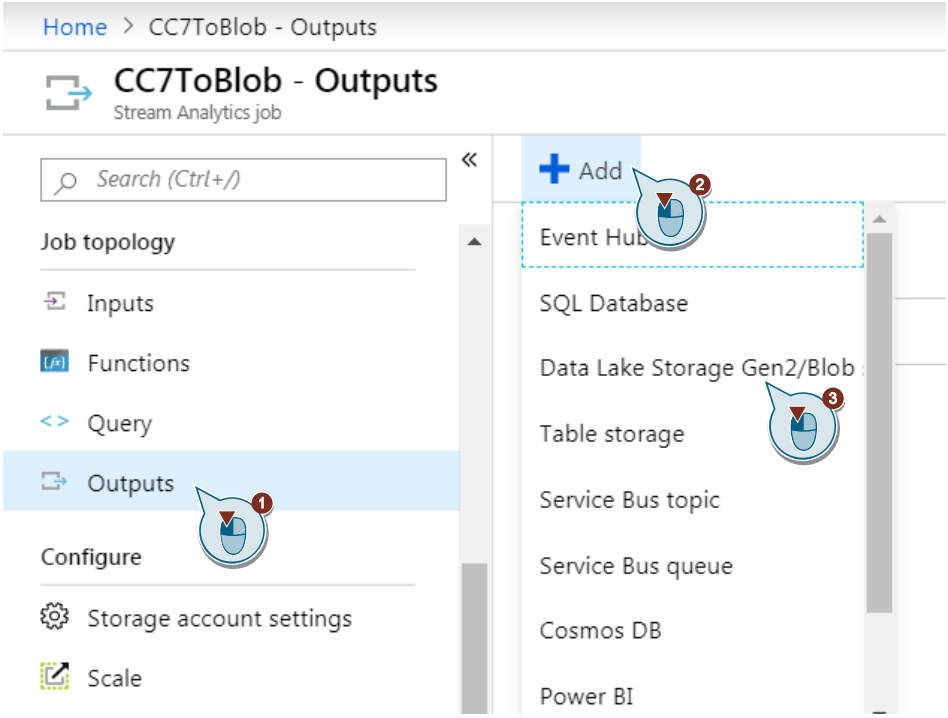
9. Open the job and add a new "Data Stream Input" ("Inputs"). Select "IoT Hub" as the source.



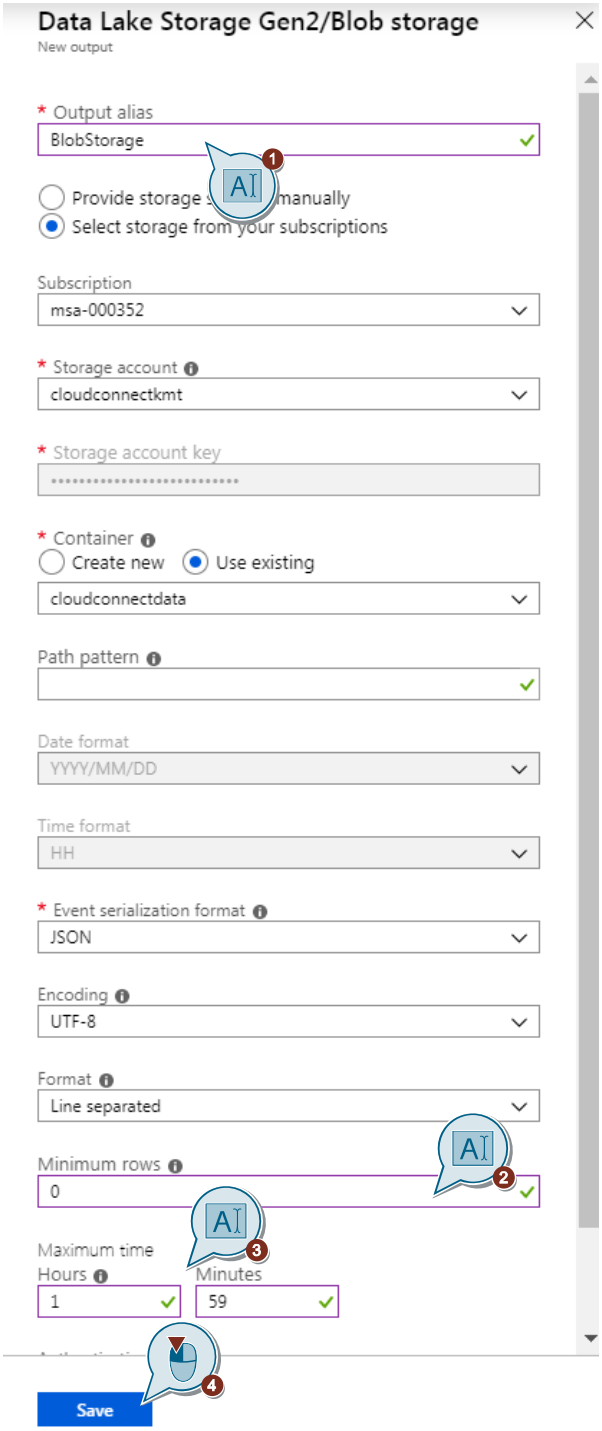
10. Enter a unique name and make sure "Messaging" is selected as the endpoint. Select "iothubowner" and your consumer group as your access policy. Then press "Save".



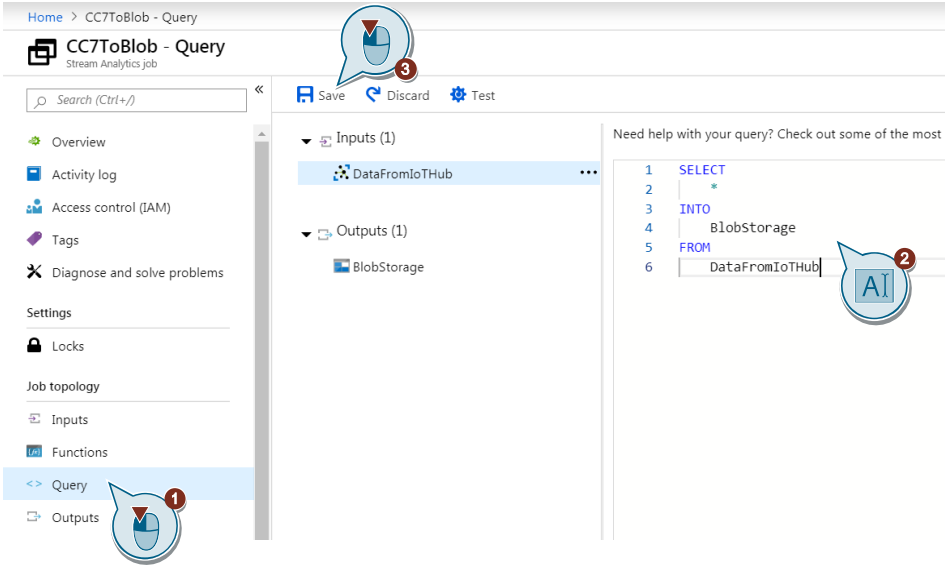
11. Now add an "Output" of the type "Data Lake Storage Gen2/Blob storage".



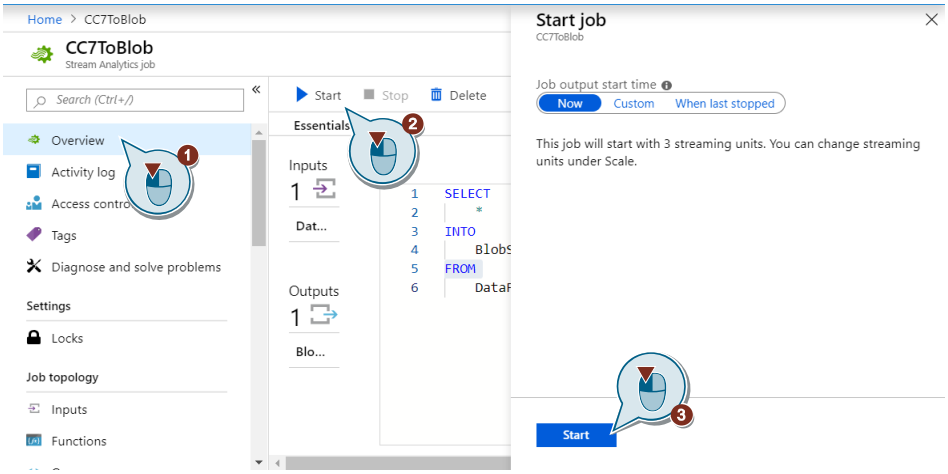
12. Enter a name for the output. Enter the value "0" for "Minimum rows" and the value "1 hour" and "59 minutes" for "Maximum time". Then save the settings.



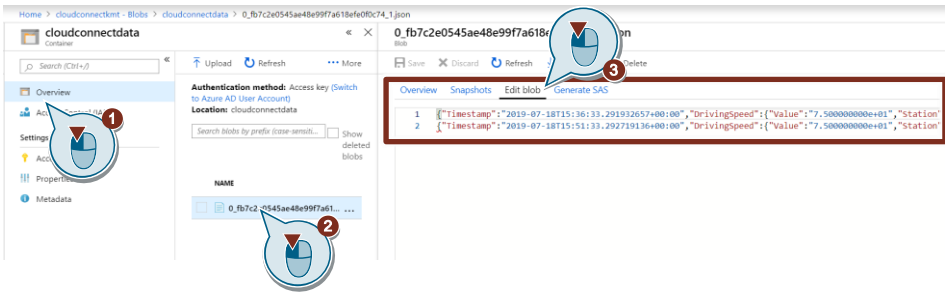
13. Now create a query that writes all data from the IoT Hub to the blob memory. Switch to "Query" and replace the expression "[YourOutputAlias]" with "BlobStorage" and the expression "[YourInputAlias]" with "DataFromIoTHub".



14. Switch to the "Overview" and start the job.



15. If you now open the blob memory, you can check the received data.



3 Useful information

If you use the authentication method "X.509, signed by certification authority" ("X.506, CA signed") in Microsoft Azure, you need a certification authority (CA) and an associated certificate.

3.1 Creation of certificates with OpenSSL

This chapter describes how to issue a Certificate Authority (CA) and associated self-signed certificates for testing purposes. The certificates are created with OpenSSL only.

You can download the OpenSSL software from the following link: "https://www.openssl.org/source/".

Generate certification authority (CA)

1. Run the openssl.exe file as an administrator.
2. Type the following command to create a "Private Key" for the Certificate Authority (CA).

```
genrsa -aes256 -out CA-Key.pem 2048
```

   The option "-aes256" encrypts the key with a password. The key has the name "CA-Key.pem" and is 2048 bit long.

3. Now type the following command to use the key to create a CA.

```
req -x509 -new -nodes -extensions v3_ca -key CA-Key.pem -days 1024 -
out CA-Root.pem -sha512
```

   A 1024 day CA with the name "CA-Root.pem" is created. Various additional attributes are queried during generation.

Issue Certificate (Public Key)

1. Type the following command to create a "Private Key" for the Certificate Authority (CA).

```
genrsa -out Cert-Key.pem 2048
```

   The key has the name "Cert-Key.pem" and is 2048 bit long.

2. Use the following command to create a certificate request.

```
req -new -key Cert-Key.pem -out Cert.csr -sha512
```

   The certificate request has the name "Cert.csr". Various additional attributes are queried again during generation.

Note The attribute "Common Name" (CN) must carry the verification code in conjunction with Microsoft Azure.

3. Type the following command to create a Public Key.

```
x509 -req -in Cert.csr -CA CA-Root.pem -CAkey CA-Key.pem -
CAcreateserial -out Cert-Pub.pem -days 365 -sha512
```

   The public key bears the name "Cert-pub.pem" and is valid for 365 days.

3.1 Creating certificates with OpenSSL and Azure IoT SDK

This chapter describes how to issue a Certificate Authority (CA) and associated self-signed certificates for testing purposes. The certificates are created with OpenSSL and Azure IoT SDK.

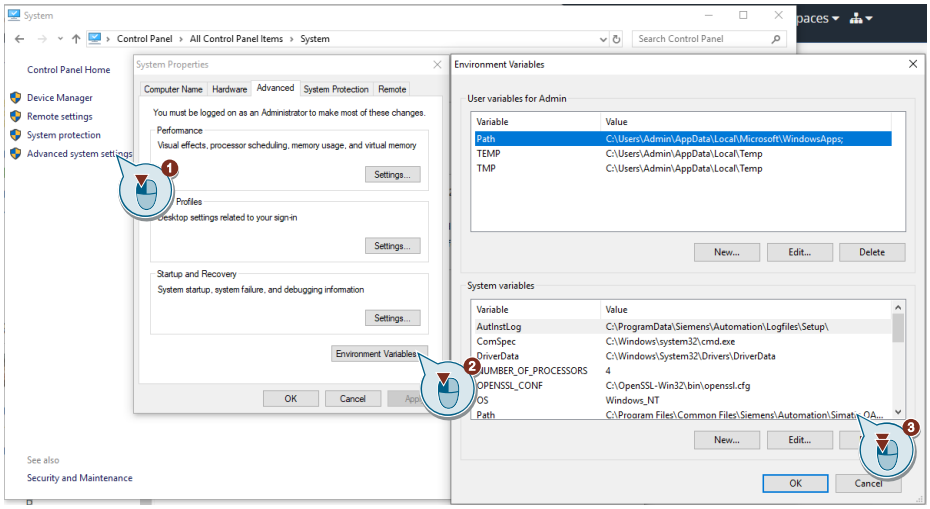
You can download the OpenSSL software from the following link: "https://www.openssl.org/source/".

Follow these steps:

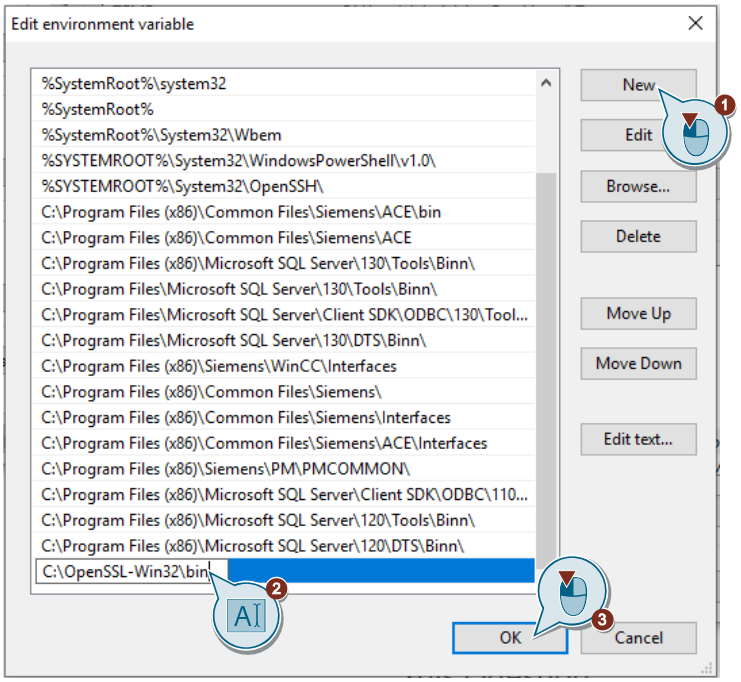
1. Add the OpenSSL directory to your path:

   Navigate to Control Panel > System

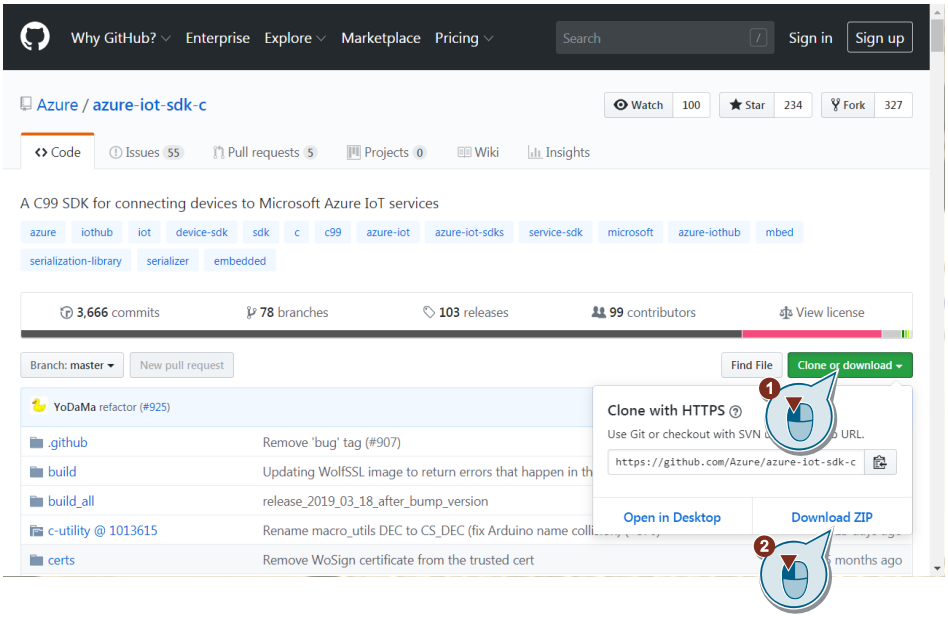
   Click "Advanced system settings" and then on "Environment Variables". Double click "Path" in System variables.



2. Click "New" and specify the installation path of OpenSSL. Click OK to confirm your entry.
   Restart your computer once the settings have been made.



3. Open the Github download page for "AzureIoT-Tools" at the following link: https://github.com/Azure/azure-iot-sdk-c.
4. Click the buttons "Clone or download" and "Download ZIP".



5. Extract the ZIP file. Then open the folder "azure-iot-sdk-c-master\tools\CACertificates". Copy the folder to the desktop, for example.

Creating CARoot certificate

Note Microsoft only officially authorizes the certificates created in Powershell for testing purposes. Please note that the security of these certificates is not guaranteed.

There is a Powershell in the "CACertificates" folder which facilitates the creation of scripts.
Open "Windows Powershell" as an administrator.

1. Enter the following command to allow the script.
   Confirm with "Y + Enter".

```
Set-ExecutionPolicy -ExecutionPolicy Unrestricted
```

2. Use the following command to specify the configuration of the OpenSSL application.

```
$ENV:openssl_conf = "C:\OpenSSL-Win32\bin\cnf\openssl.cnf"
```

Note: The OpenSSL installation path may be different on your computer.

3. Change the working directory in Powershell to the "CACertificates" folder. In this example, the folder is on the desktop.

```
cd "C:\Users\user1\Desktop\CACertificates"
```

4. Open the script "cacert.ps1" in Powershell with the following command.

```
. .\ca-certs.ps1
```

5. Enter the following command to verify the previous configuration steps.

```
Test-CACertsPrerequisites
```

6. To create a new CACertificate, enter the following commands one after the other in Powershell.

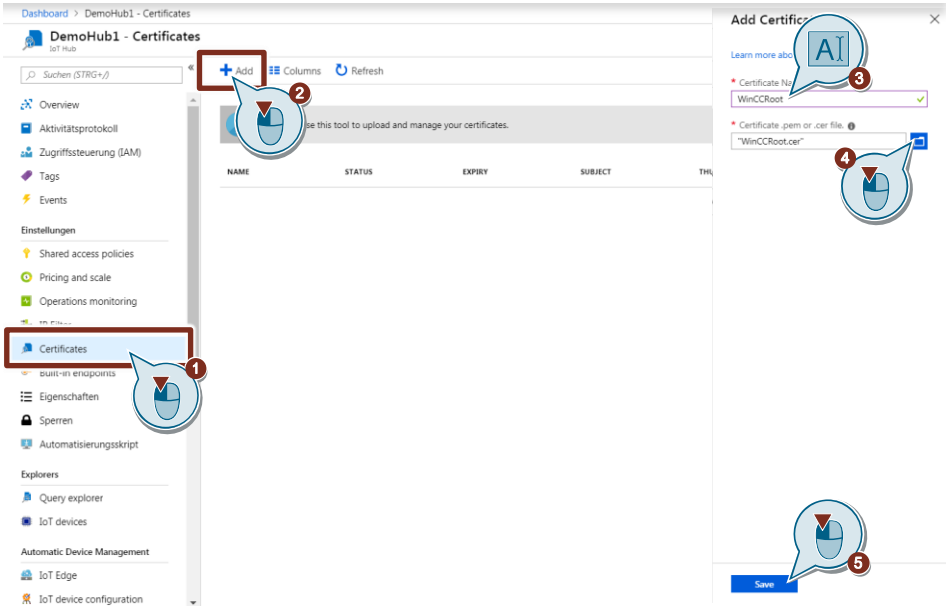
```
New-CACertsCertChain
```

ECC

Hinweis This function will create a total of three certificates. The necessary root certificate is the certificate with the name "RootCA".

Uploading the certificate to Azure

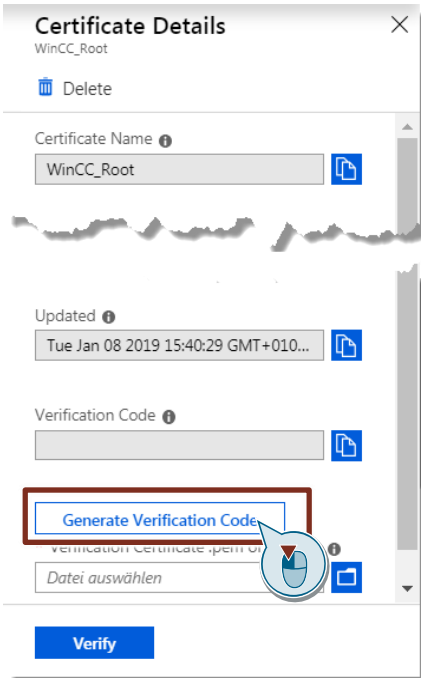
1. In the IoT Hub, switch to the "Certificates" section in the AzurePortal.
2. Click the "Add" button.
3. Enter a name for the certificate and select the root certificate.
4. Save the entries.



Verifying the CA certificate

You will then verify the newly created certificate.

1. Select the certificate in the main window and click "Generate Verification Code" at the right side of the screen.



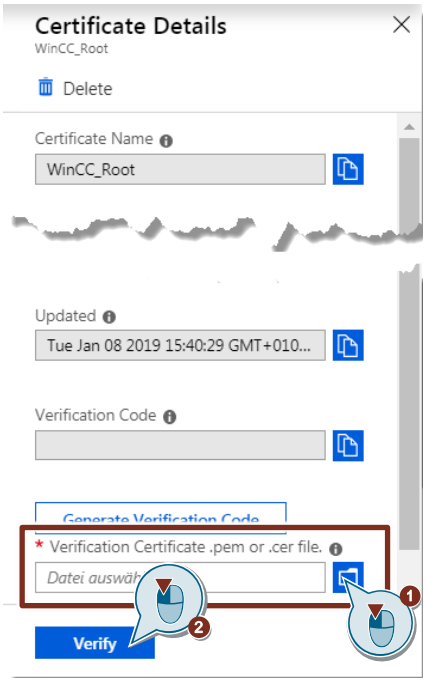
2. Copy the generated code.

3. Enter the following command to verify the CACertificate with the verification code. The script generates a certificate with the name "VerifyCert4" and saves it in your CACertificates folder.

```
New-CACertsVerificationCert 70B1053652273CCE22CC561630C8…
```

Note Enter the verification code from "Azure" instead of the specified string.

4. Upload the generated certificate to "Azure IoT":
   In the Azure Portal, select the generated certificate "VeriCert4" under "Verification Certificate .pem or .cer file" and click the "Verify" button.



Creating device certificate

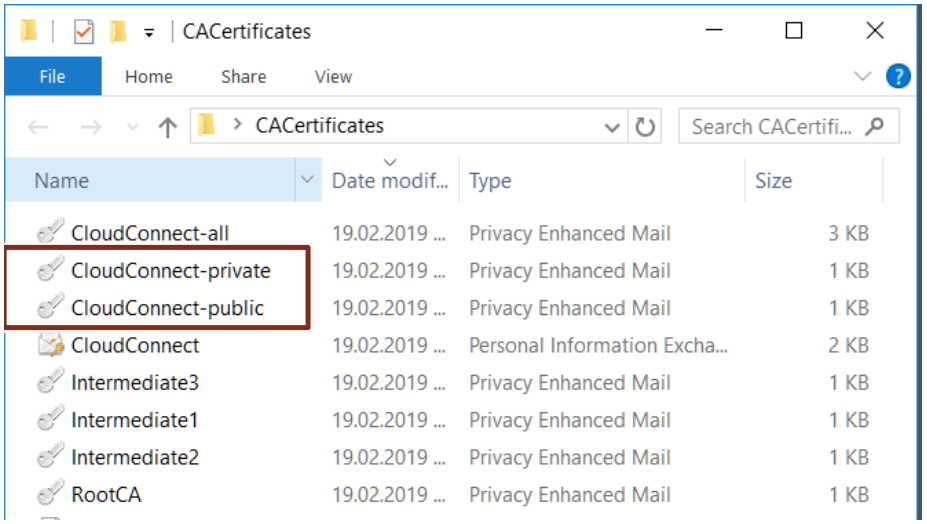
1. Enter the following command to create a new device certificate. Assign a password of your choosing.

```
New-CACertsDevice <Devicename>
```

Note The device name that is assigned here must match the one from the IoT device in Azure. This name must also be used in the configuration for CloudConnect 7 as "Client ID".

All certificates are created on the desktop in the folder "CACertificates".

2. You need the client certificate with the ending "public" and the client key with the ending "private". The name "CloudConnect" can differ depending on the device name assigned.



Note The certificates are accepted by Microsoft Azure because they were created using the root certificate, which you stored and verified in Azure.

4 Appendix

4.1 Service and support

Industry Online Support

Do you have any questions or need assistance?

Siemens Industry Online Support offers round the clock access to our entire service and support know-how and portfolio.

The Industry Online Support is the central address for information about our products, solutions and services.

Product information, manuals, downloads, FAQs, application examples and videos – all information is accessible with just a few mouse clicks:
support.industry.siemens.com

Technical Support

The Technical Support of Siemens Industry provides you fast and competent support regarding all technical queries with numerous tailor-made offers – ranging from basic support to individual support contracts. Please send queries to Technical Support via Web form:
www.siemens.com/industry/supportrequest

SITRAIN – Training for Industry

We support you with our globally available training courses for industry with practical experience, innovative learning methods and a concept that's tailored to the customer's specific needs.

For more information on our offered trainings and courses, as well as their locations and dates, refer to our web page:
www.siemens.com/sitrain

Service offer

Our range of services includes the following:

- Plant data services
- Spare parts services
- Repair services
- On-site and maintenance services
- Retrofitting and modernization services
- Service programs and contracts

You can find detailed information on our range of services in the service catalog web page:
support.industry.siemens.com/cs/sc

Industry Online Support app

You will receive optimum support wherever you are with the "Siemens Industry Online Support" app. The app is available for Apple iOS, Android and Windows Phone:
support.industry.siemens.com/cs/ww/en/sc/2067

4.2 Links and literature

Table 4-1

No.	Topic
\1\	Siemens Industry Online Support https://support.industry.siemens.com
\2\	Link to the entry page of the application example https://support.industry.siemens.com/cs/ww/en/view/109766675
\3\	Developer documentation https://developer.mindsphere.io/
\4\	MindSphere Forum https://community.plm.automation.siemens.com/t5/MindSphere/ct-p/MindSphere
\5\	Manual for SIMATIC CloudConnect 712 https://support.industry.siemens.com/cs/ww/en/ps/25621
\6\	Azure IoT Explorer https://github.com/Azure/azure-iot-explorer
\7\	Documentation AWS IoT Core https://docs.aws.amazon.com/iot/latest/developerguide/what-is-aws-iot.html

4.3 Change documentation

Table 4-2

Version	Date	Change
V1.0	08/2019	First version
V1.1	10/2019	• Correction of an error in the documentation. • Addition of a note
V2.0	03/2020	• Splitting the documentation by cloud providers • Recreating the variant with AWS