

**SIEMENS**

*Ingenuity for life*

*Industry Online Support*

Home

## WinCC data connection to the cloud

WinCC V7.5, Amazon WebServices

<https://support.industry.siemens.com/cs/ww/en/view/109760955>

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

	<b>Legal information .....</b>	<b>2</b>
<b>1</b>	<b>Introduction .....</b>	<b>4</b>
	1.1 Overview.....	4
	1.2 Principle of operation.....	4
	1.3 Construction and communication .....	5
	1.4 Components used .....	6
<b>2</b>	<b>Useful information .....</b>	<b>7</b>
	2.1 Basics .....	7
<b>3</b>	<b>Configuration .....</b>	<b>9</b>
	3.1 Requirements .....	9
	3.2 Overview.....	9
	3.3 Creating a certificate .....	9
	3.4 WinCC V7.5.....	15
	Requirements .....	15
	Copy certificate.....	16
	Configuring a Cloud Connector .....	17
	3.5 Test the MQTT connection.....	19
	3.6 Analyzing the Cloud data .....	21
<b>4</b>	<b>Appendix .....</b>	<b>23</b>
	4.1 Service and Support.....	23
	4.2 Links and literature .....	24
	4.3 Change documentation .....	24



# 1 Introduction

## 1.1 Overview

With Industry 4.0, the "Cloud" is also becoming increasingly important for industry. Data is sent from sensors and actuators of the machine to the cloud where it is reused and processed for analysis purposes. This is useful, among other things, for troubleshooting and machine optimization.

As of WinCC V7.5, the "Cloud Connector" provides a way of sending variables from the WinCC variable budget to the cloud (Amazon Web Services, or AWS for short).

## 1.2 Principle of operation

The Cloud Connector uses the so-called "MQTT" protocol for communication to the Cloud.

The central element of communication via MQTT is the MQTTBroker. The entire data exchange between the "clients" runs via this broker.

The "WinCC Cloud Connector" is configured as an "MQTTClient". It sends (published) the selected tags to the MQTTBroker.

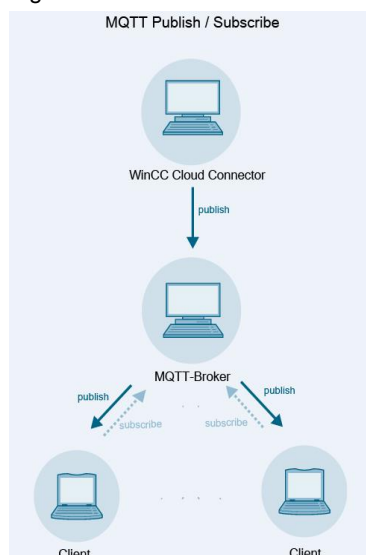
From this central location, the data is available in the cloud for further processing.

The "WinCC Cloud Connector" functions as a so-called "Publisher", which makes the data freely available for further processing. The WinCC system cannot be configured as "Consumer". This means that the WinCC system can store data in the cloud but has no read access to the data in the cloud.

In this example, the cloud service "AWS" is the "MQTT" broker. The broker has a specific broker address and a port via which communication is established. You can see the structure of the address in the following figure.

<b>Broker Address:</b>	a1bccde1f23-ats.iot.eu-central-1.amazonaws.com
------------------------	--

Figure 1-1 MQTT communication

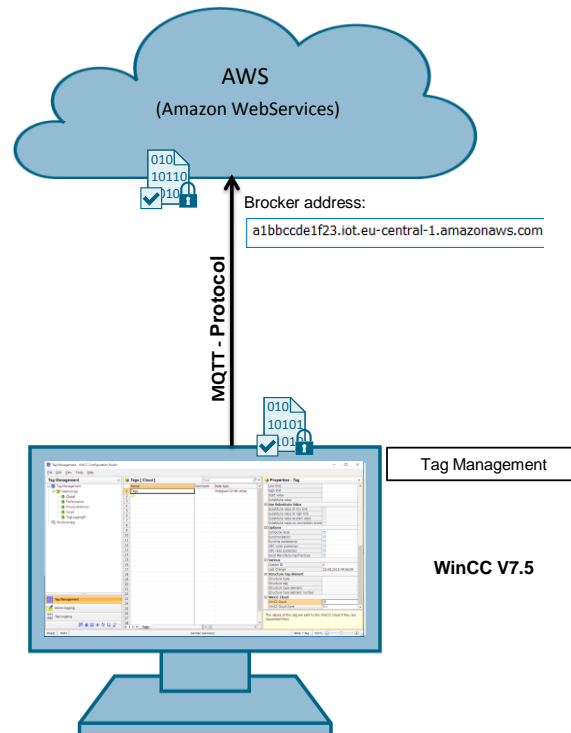


The basics of "MQTT" can be found in section [2.1](#).

## 1.3 Construction and communication

As of WinCC V7.5, you can use the WinCC Cloud Connector to establish direct communication in the cloud without requiring additional hardware. By using the "PublicKey" encryption method, the connection is protected from external access.

Communication is established with the Windows service "CCloudConnect" via an "MQTT channel" to the cloud. The service "CCloudConnect" is the "MQTTClient" and uses the port 8883 or 443 depending on the cloud used. If desired, the variables can only be rewritten to the cloud if the value changes.



The basics of the Public Key procedure can be found in section [2.1](#).

## 1.4 Components used

This application example was created with these hardware and software components:

Table 1-1

Components	Quantity	Article number	Note
SIMATIC WinCC V7.5	1	6AV63.1-....7-5...	
SIMATIC WinCC Cloud Connector V7.5	1		License necessary, without a license you can transfer up to 5 tags for testing.
AWS account	1	--	Link: <a href="https://console.aws.amazon.com">https://console.aws.amazon.com</a>
AWS License	1	--	--

## 2 Useful information

### 2.1 Basics

#### MQTT Protocol

The "Message Queue Telemetry Transport" is a simple protocol on TCP/IP level. It is suitable for the exchange of messages between devices with limited functionality and for transmission over unreliable networks. The standard is particularly suitable for "Machine to Machine" communication or for the "Internet of Things" (IoT) communication due to the simple and simple Publish/Subscribe principle.

The MQTT protocol is distinguished by the following features:

- Lightweight protocol with low transport overhead
- Minimal network bandwidth requirements due to push mechanism
- Reconnect function after termination of connection
- Resending of messages after disconnection
- Mechanism for notifying prospects of an unforeseen disconnection of a client
- Easy to use and implement with a small set of commands
- Encryption of messages with SSL/TLS possible

#### Note

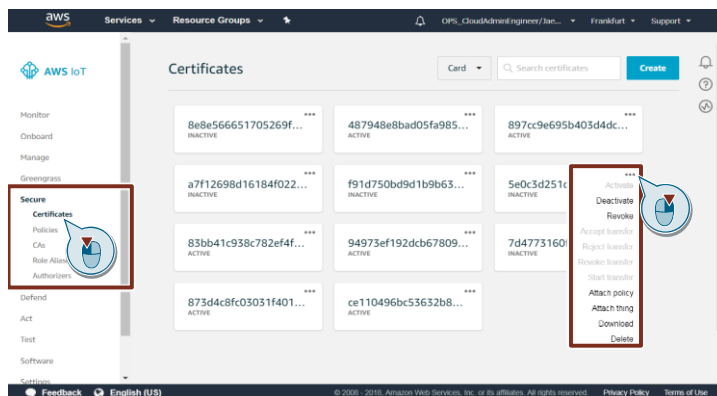
Further information on "MQTT" can be found at <https://www.mqtt.org> and in the AWS documentation under the keyword "Message Broker for AWS IoT" [https://docs.aws.amazon.com/de\\_de/iot/latest/developerguide/](https://docs.aws.amazon.com/de_de/iot/latest/developerguide/)

#### Encryption

AWS uses the asymmetric "Public-Key" procedure. With "Public-Key" the communication is secured with certificates.

The certificates are managed by "AWS IoT" in the certificates area. In this area you can revoke, delete or re-download the certificates:

Figure 2-1



If certificates are created via "OneClick Certificate", the following certificates are created:

Table 2-1

Certificate	Ending
Private key	*.private.pem.key
Public key	*.public.pem.key
Device certificate	*-certificate.pem.crt

Additionally, you can download a CA-Root Certificate (AWS).

**Note** The CA certificate is valid until 2038. The other certificates are valid until 2050.  
You can revoke the certificates at any time via "AWS IoT".

To establish a connection, the device requires the "private key" and the CA certificate to recognize the connection partner (AWS). These keys must be entered in the "Cloud Connector" settings in WinCC.

### Data buffer

A data buffer is created for communication via MQTT. The tags to be transmitted are buffered in this data buffer. By default, the size of the data buffer is set to "1000".

This feature allows short disconnects to the cloud to be overcome without data loss. As soon as the connection is restored after a connection termination, the variable values are automatically saved from the data buffer to the cloud.

The data buffer is only activated when the connection to the cloud is lost.

**Note** Basics of the "WinCC Cloud Connector" can be found in the manual "WinCC V7.5: Working with WinCC" in the section "SmartTools"  
<https://support.industry.siemens.com/cs/mdm/109760739?c=115485367563&lc=de-WW>



## 3 Configuration

### 3.1 Requirements

Amazon Web Services has an account set up and licensed.

Additional information is available at <https://console.aws.amazon.com>

### 3.2 Overview

The following steps are required to connect WinCC V7.5 to the Cloud (AWS) using the Cloud Connector:

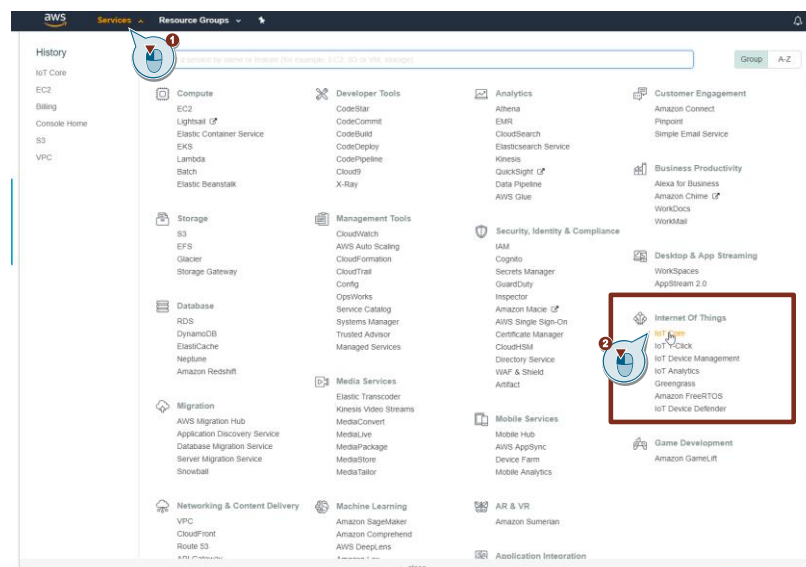
1. Create a certificate for establishing a connection (in AWS)
2. Setting the Endpoint for Communication (in AWS)
3. Settings for the Cloud Connector (in WinCC)
4. Configure and test variables (in WinCC).

### 3.3 Creating a certificate

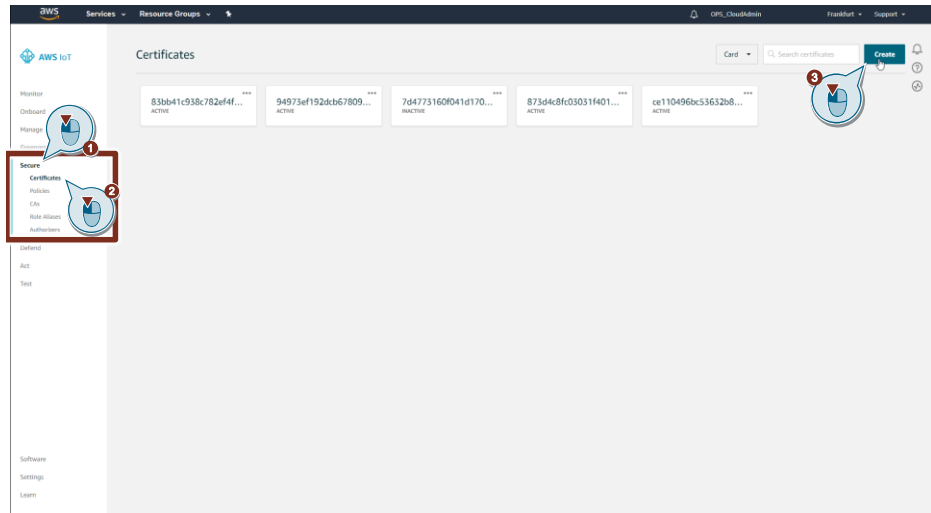
1. Open the AWS Cloud Service using the following link:  
<https://console.aws.amazon.com>
2. Log in with your login data.
3. Click on "Services" (1) in the upper menu bar and open the first item "IoT Core" (2) in the category "Internet of Things".

#### Note

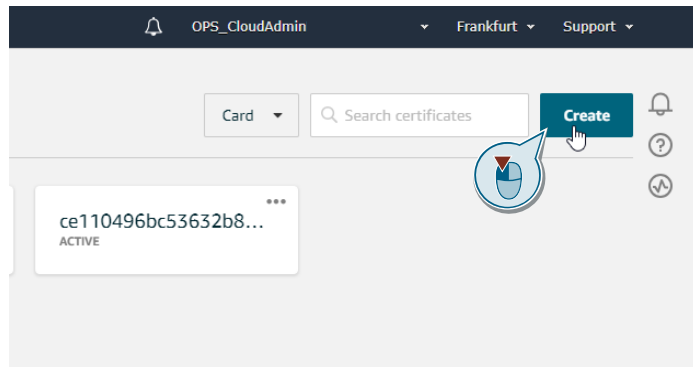
The first time you start the "IoT" core, you will get a "First Steps" introduction. To get to the screenshot shown, perform the Introduction.



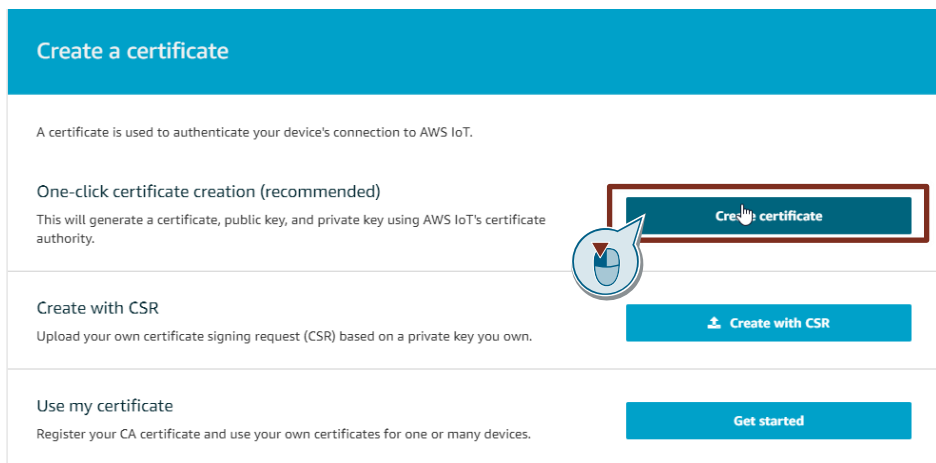
4. On the left menu bar, click Secure (1) and select Certificates (2).  
In the main window you can see your existing certificates.



5. To create a new certificate, click on the "Create" button at the top right.



6. In the "Create a certificate" dialog, click the first button to create a "OneClick certificate". This certificate is recommended by AWS.

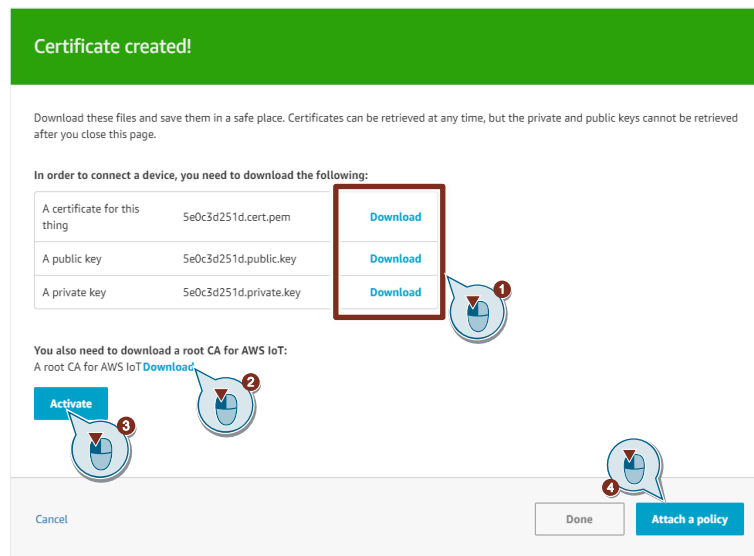


- In the next step you can download the certificates and a "Root CA". The following certificate types are available

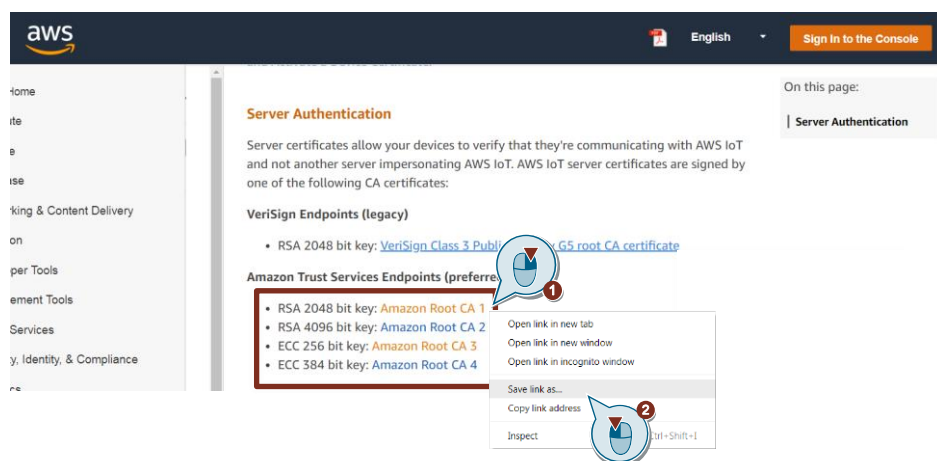
Table 3-1

Ending	Type
cert.pem	Certificates for the Client
public.key	Public key
privat.key	Private key
pem	Certificate of the Certification Authority (CA)

- Download all certificates at the top of the page and save them to your computer (1).
- Additionally, download the CA-Root certificate (2).



- Under Amazon Trust Services Endpoints, right-click one of the certificates and select "Save link as...".
- Close the window after the download.

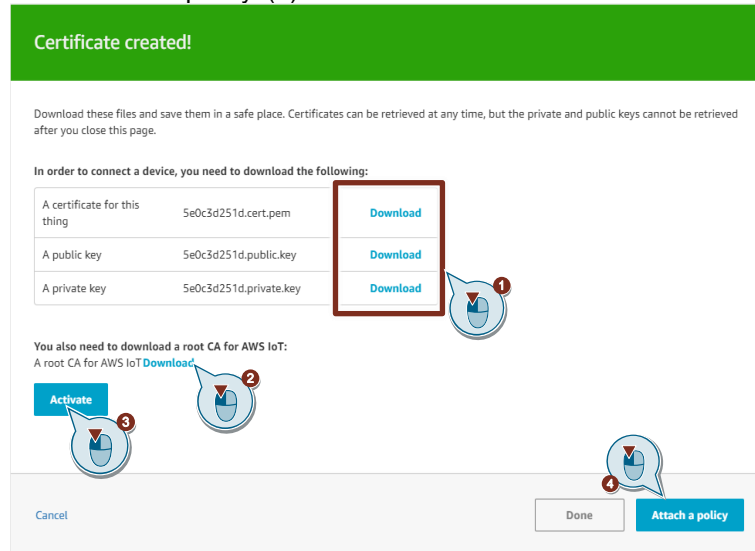


**Note**

Use one of the Amazon Trust Services Endpoints certificates. These are recommended by Amazon.

You can choose between the two Public-Key methods "RSA" and "ECC" as well as different encryption strengths.

- 11. Click on the "Activate" button to activate the certificate (3)
- 12. Click 'Attach a policy' (4).

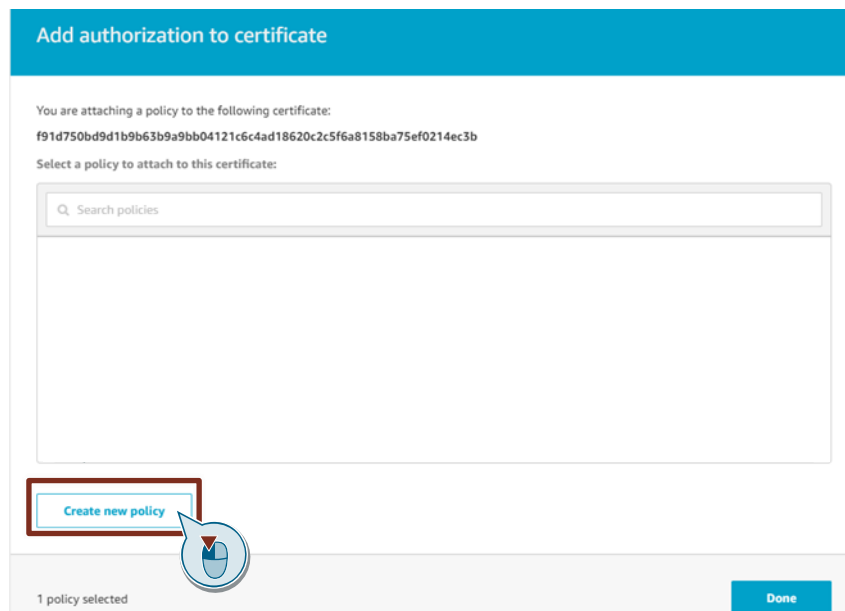


Existing policies are displayed in the window.

**Note**

If you do not want to add a policy, click the "Done" button. This creates and activates the certificate.

- 10. To create a new policy, click "Create new policy".



#### Example configuration without restrictions:

1. Enter a name (1). You can choose any name you like.
2. Enter "\*" under Action (2) and "\*" under Resource ARN (3). Here you define restrictions. With the "\*" you allow everything.
3. Activate the option box "Allow" (4).
4. Click the "Create" button (5).

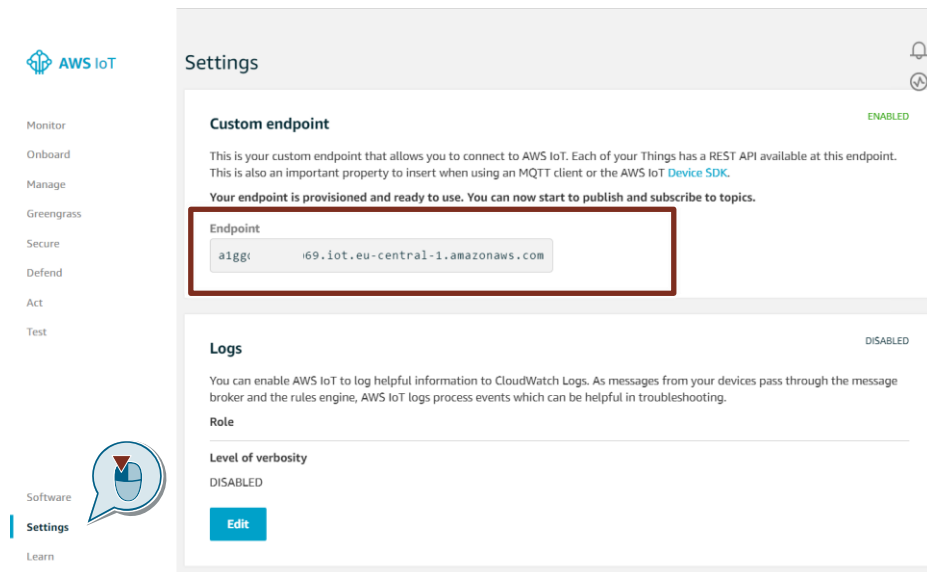
The screenshot shows the 'Create a policy' interface. At the top, there is a blue header with the text 'Create a policy'. Below the header, there is a text area with instructions: 'Create a policy to define a set of authorized actions. You can authorize actions on one or more resources (things, topics, topic filters). To learn more about IoT policies go to the Policies documentation page.' Below this, there is a 'Name' field with the value 'WinCCnoRestrictions' and a callout bubble with the number '1' pointing to it. Underneath is the 'Add statements' section, which includes a 'Policy statement' field with the text 'the types of actions that can be performed by a resource.' and an 'Advanced mode' toggle. The 'Action' field contains '\*' and has a callout bubble with '2'. The 'Resource ARN' field also contains '\*' and has a callout bubble with '3'. Below these fields is the 'Effect' section with 'Allow' checked and 'Deny' unchecked, with a callout bubble with '4'. A 'Remove' button is to the right. At the bottom right, there is a 'Create' button with a callout bubble with '5' pointing to it. An 'Add statement' button is at the bottom left.

5. Click the "Done" button.

The screenshot shows the 'Add authorization to certificate' interface. At the top, there is a blue header with the text 'Add authorization to certificate'. Below the header, there is a text area with instructions: 'You are attaching a policy to the following certificate: f91d750bd9d1b9b63b9a9bb04121c6c4d18620c2c5f6a8158ba75ef0214ec3b'. Below this, there is a text area with the instruction 'Select a policy to attach to this certificate:'. Below this is a search box with the text 'Search policies'. Below the search box is a 'Create new policy' button. At the bottom left, there is a status bar with the text '1 policy selected'. At the bottom right, there is a 'Done' button with a callout bubble pointing to it.

### Configuring the Endpoint

1. Click on "Settings" in the AWS IoT navigation.



The screenshot displays the AWS IoT Settings interface. On the left is a navigation menu with options: Monitor, Onboard, Manage, Greengrass, Secure, Defend, Act, Test, Software, Settings (highlighted), and Learn. The main content area is titled "Settings" and features a "Custom endpoint" section, which is marked as "ENABLED". This section includes explanatory text and a message: "Your endpoint is provisioned and ready to use. You can now start to publish and subscribe to topics." Below this, the "Endpoint" field is highlighted with a red box, showing the value "a1gg1:69.iot.eu-central-1.amazonaws.com". The "Logs" section below is marked as "DISABLED" and includes a "Level of verbosity" dropdown set to "DISABLED" and an "Edit" button.

2. Make a note of the "Endpoint address".



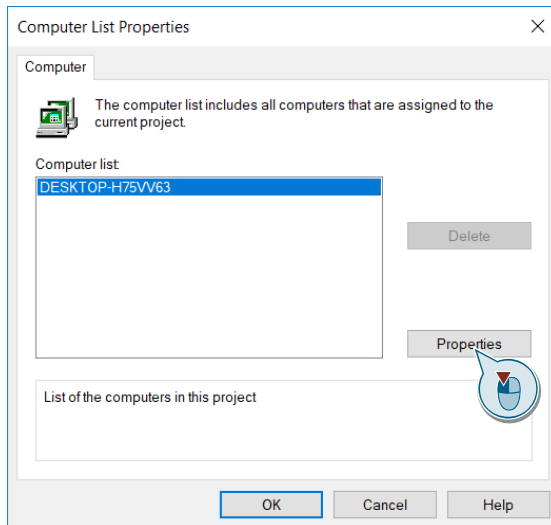
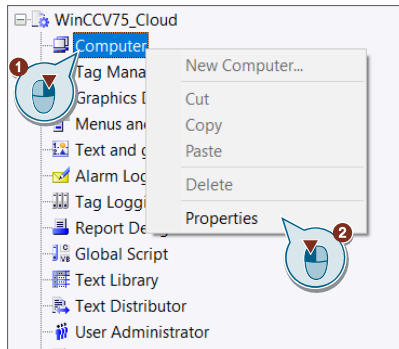
## 3.4 WinCC V7.5

### Requirements

- Certificates from AWS.
- Endpoint address of AWS.

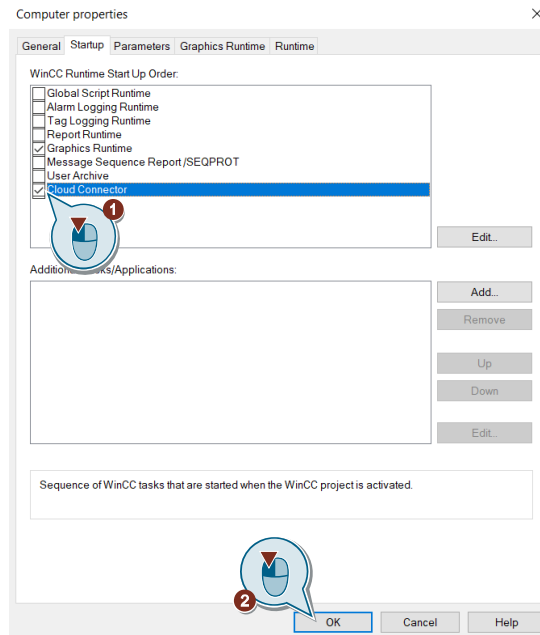
### Activate the "Cloud Connector" in the computer properties.

1. Open a project in WinCC Explorer.
2. Right-click on "Computer" and select "Properties".



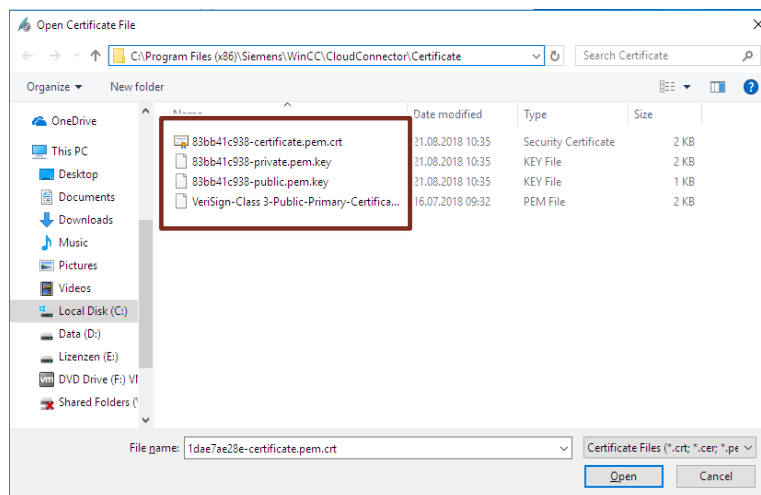
## 3 Configuration

3. Select the "Startup" tab.
4. Activate the option box for the Cloud Connector and close the window with OK.



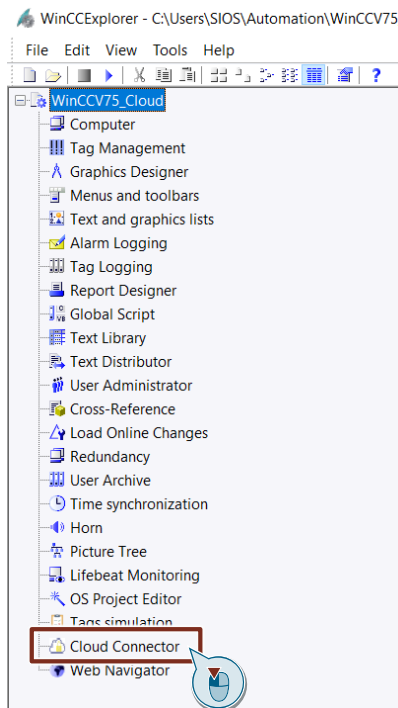
### Copy certificate

1. Open the File Explorer on the WinCC computer.
  2. Open the path  
C:\Program Files (x86)\Siemens\WinCC\CloudConnector\Certificate
- Note:** The name "Program Files (x86)" may differ depending on the operating system version used.
3. Copy the four certificates from section 3.3, no.7 into the specified file path.

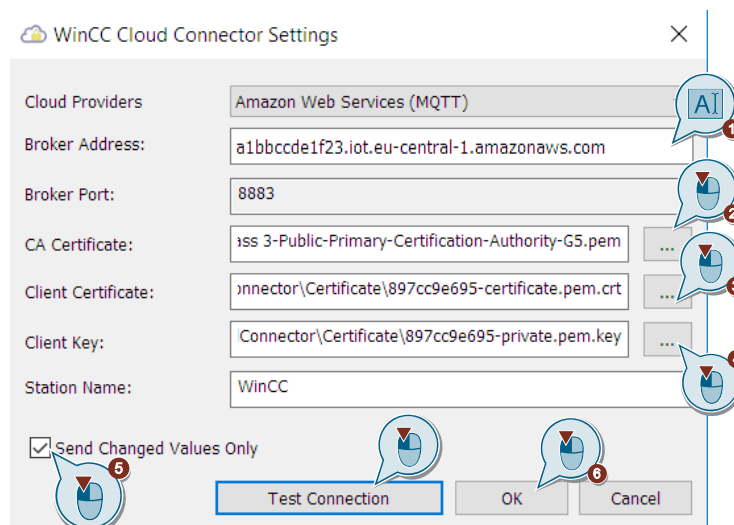


### Configuring a Cloud Connector

1. Double-click "Cloud Connector" in the WinCC project navigation.



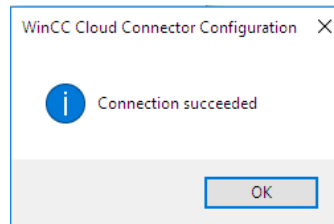
2. Enter the noted Brocker address in the field (1).  
 Click on the "..." button under "CA Certificate" and select the "CA-Root" certificate with the extension ".pem" in the File Explorer (2).  
 Click on the "..." button under "Client Certificate" and select the device certificate with the extension ".pem.crt" in the File Explorer (3).  
 Click on the "..." button under "Client Key" and select the "Private Key" with the extension ".pem.key" in the File Explorer (4).  
 The "Station Name" name can be freely selected.



**Note**

You can choose between "Amazon Web Services", "Microsoft Azure" and a general channel that you have to configure yourself at the cloud provider.

3. Test the connection by clicking on the button "Test Connection" (5).

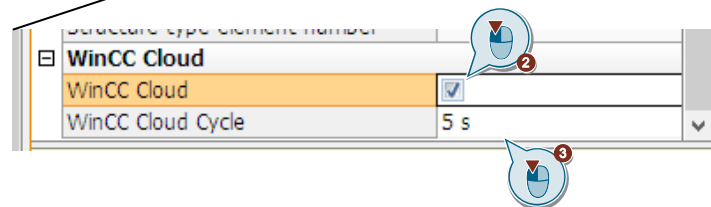
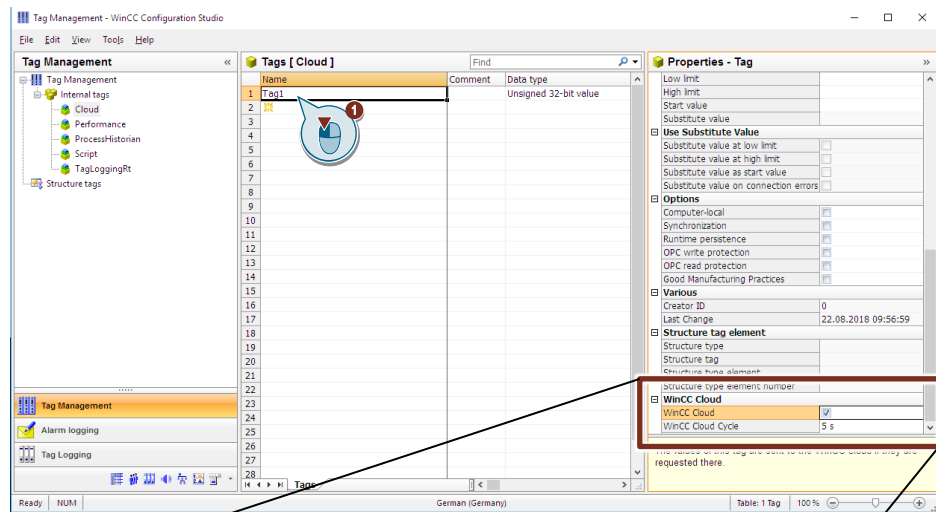


To close the settings window, click on the "OK" button (6).

The configuration of the Cloud Connector is now complete.

**Configuring HMI variables**

1. Open the "Tag management" in WinCC.
2. Create a new variable or select an existing one (1).
3. Activate the option box (2) in the properties of the variable under "WinCC Cloud".
4. Select an archiving cycle (3). You can define a separate archiving cycle for each variable.



### 3.5 Test the MQTT connection

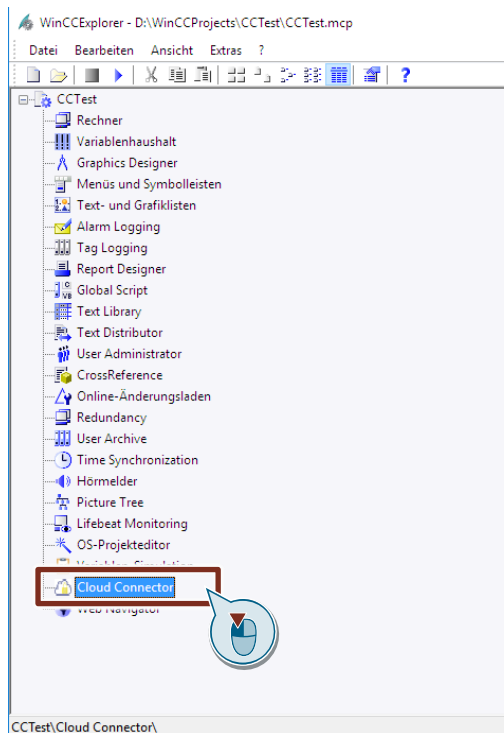
After you have configured the AWS cloud and the Cloud Connector, you can check whether the value of the variable is also stored in the cloud.

1. Start the WinCC V7.5 Runtime.
2. Simulate values for the variable.

**Note**

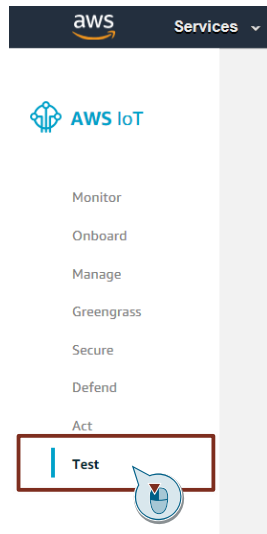
You can use the “Variable-Simulator” to do this, or use input fields to specify values for the variable.

Figure 3-1 variable simulation

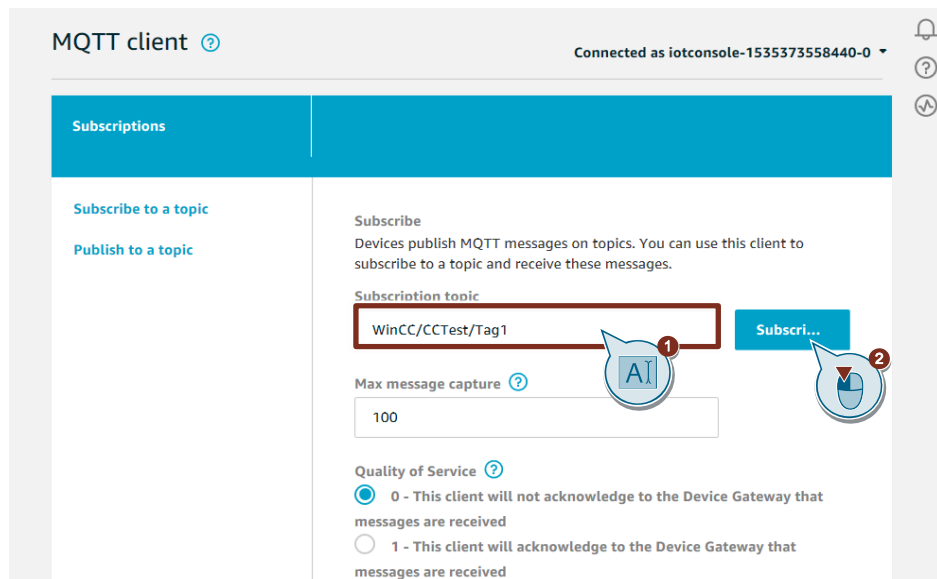


### 3 Configuration

3. Start the AWS IoT Core (as in described in section [3.3](#), No. 3).
4. Click in the navigation on the left side on "Test".

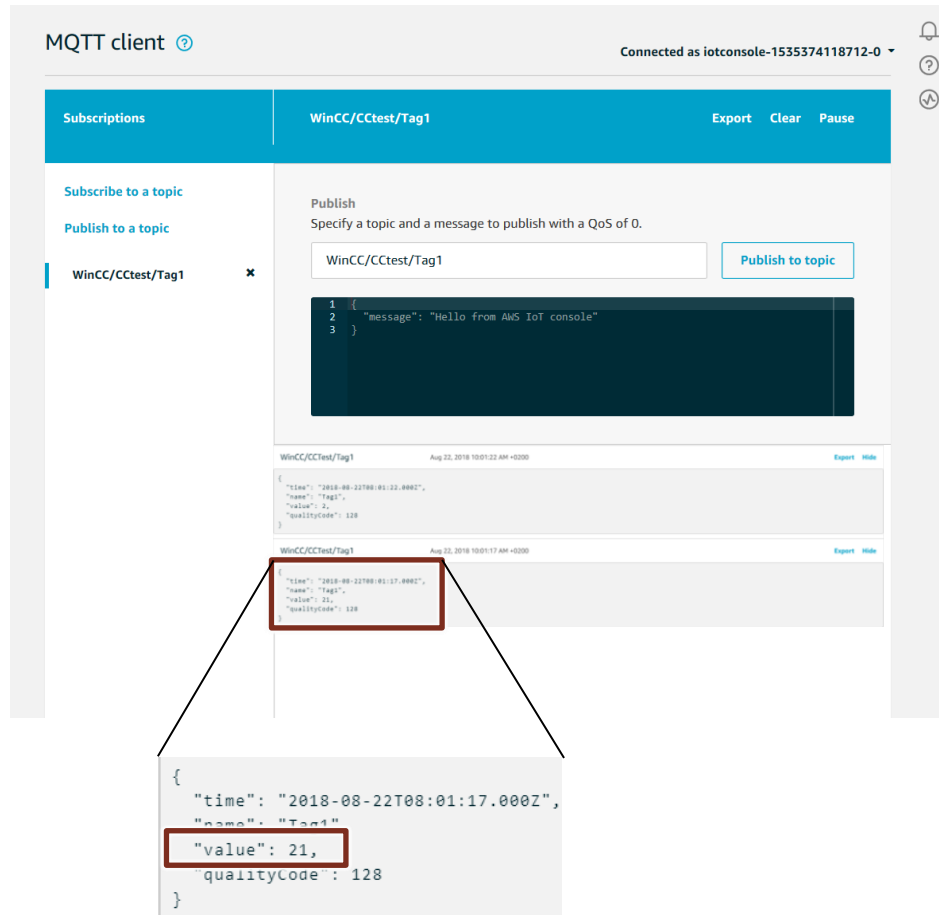


5. Under "Subscribe", enter the WinCC variable in the input field as follows.  
**StationName / WinCCProjectName / TagName**, in this example  
"WinCC/CCTest/Tag1"



6. Click on "Subscribe to topic".
7. The display changes. In the lower area you can see the current values of the variable, if the communication works.  
Note that values for the variable are only displayed after the set archiving cycle ("WinCC Cloud Circle").





### 3.6 Analyzing the Cloud data

With the variables in the cloud, you can now calculate and analyze more metrics. The cloud providers provide their own analysis tools for this purpose.

"Amazon WebServices" lets you analyze your data with "AWS IoT Analytics".

A link to the "AWS IoT Analytics" manual can be found in the section "Links and Literature".

-  Internet Of Things
- IoT Core
- IoT 1-Click
- IoT Device Management
- IoT Analytics**
- Greengrass
- Amazon FreeRTOS
- IoT Device Defender



## 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:

<https://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](http://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](http://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](http://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](http://support.industry.siemens.com/cs/ww/en/sc/2067)

## 4.2 Links and literature

Table 4-1

No.	Topic
\1\	Siemens Industry Online Support <a href="https://support.industry.siemens.com">https://support.industry.siemens.com</a>
\2\	Link to the article page of the application example <a href="https://support.industry.siemens.com/cs/ww/en/view/109760955">https://support.industry.siemens.com/cs/ww/en/view/109760955</a>
\3\	Manual WinCC V7.5: Working with WinCC, section WinCC/CloudConnector <a href="https://support.industry.siemens.com/cs/mdm/109760739?c=115485367563&amp;lc=de-WW">https://support.industry.siemens.com/cs/mdm/109760739?c=115485367563&amp;lc=de-WW</a>
\4\	Certificate management AWS <a href="https://aws.amazon.com/de/certificate-manager/faqs/">https://aws.amazon.com/de/certificate-manager/faqs/</a>
\5\	Developer Manual AWS IOT <a href="https://docs.aws.amazon.com/de_de/iot/latest/developerguide/iot-dg.pdf">https://docs.aws.amazon.com/de_de/iot/latest/developerguide/iot-dg.pdf</a>
\6\	Manual AWS IOT Guidelines <a href="https://docs.aws.amazon.com/de_de/iot/latest/developerguide/iot-policies.html">https://docs.aws.amazon.com/de_de/iot/latest/developerguide/iot-policies.html</a>
\7\	Link to "AWS IoT Analytics" Manual <a href="https://docs.aws.amazon.com/de_de/iotanalytics/latest/userguide/analytics-ug.pdf">https://docs.aws.amazon.com/de_de/iotanalytics/latest/userguide/analytics-ug.pdf</a>

## 4.3 Change documentation

Table 4-2

Version	Date	Change
V1.0	11/2018	First version