



**zenon**  
by COPA-DATA

# IloT Services manual

## IloT Services Manual

v.14



**COPA-DATA**

© 2024 Ing. Punzenberger COPA-DATA GmbH

All rights reserved.

Distribution and/or reproduction of this document or parts thereof in any form are permitted solely with the written permission of the company COPA-DATA. Technical data is only used for product description and are not guaranteed properties in the legal sense. Subject to change, technical or otherwise.

# Table of contents

<b>1</b>	<b>Welcome to COPA-DATA help</b>	<b>8</b>
<b>2</b>	<b>IloT Services</b>	<b>9</b>
<b>3</b>	<b>Basic knowledge</b>	<b>12</b>
3.1	Architecture	14
3.2	Internet connection	14
3.3	Configuration files (Docker)	15
3.4	Minimum password requirements	16
3.5	Certificates for IloT Services	17
<b>4</b>	<b>Possible use cases</b>	<b>17</b>
4.1	Service Engine > Web Engine: Remote control	19
4.2	Report Engine > Service Engine: Create data predictions	21
4.2.1	Case A) Passive reception of data predictions	22
4.2.2	Case B) Active request of data predictions	23
<b>5</b>	<b>Communication - Proxy Service</b>	<b>24</b>
5.1	IloT Services communication ports	25
5.2	Services, ports and URLs	27
5.3	Addresses and URLs in Service Configuration Studio	29
5.4	Configurable services in the Service Configuration Studio	30
5.5	Monitor and restart services	37
<b>6</b>	<b>Installation</b>	<b>38</b>
6.1	Installation	39
6.1.1	Installation: Standalone vs. parallel vs. virtual machine	42
6.1.2	Kubernetes	43
6.1.3	Update paths	44
6.1.4	Compatibility	44
6.2	Getting Started	52
6.2.1	Welcome to COPA-DATA help	54
6.2.2	Getting Started Guide (Windows)	54
6.2.3	Welcome to COPA-DATA help	76
6.2.4	Getting Started Guide (Docker)	76

<b>7 Service Configuration Studio .....</b>	<b>100</b>
7.1 User interface .....	101
7.1.1 Header .....	102
7.1.2 Visualization of the missing user authorization .....	103
<b>8 Certificate Management.....</b>	<b>104</b>
8.1 Certificate Management.....	106
8.2 Certificate Bundles.....	107
8.2.1 Revoke of certificate bundles.....	109
8.2.2 Generate new certificate bundles (Docker) .....	109
8.2.3 Generate new certificate bundles (Windows native) .....	111
8.2.4 Certificate Management via IIoT Services CLI.....	112
8.3 Data Hub - save location .....	115
<b>9 Data Storage.....</b>	<b>115</b>
9.1 Evacuate data centrally.....	116
9.2 Provide evacuated data.....	117
9.3 Administration in Service Configuration Studio.....	118
9.3.1 Data Storage Overview .....	119
9.3.2 Linked Service Engine.....	122
<b>10 Data Modeling .....</b>	<b>124</b>
10.1 Terminology for COPA-DATA Data Modeling.....	125
10.2 Construction Kit.....	126
10.2.1 Construction Kit Libraries.....	126
10.2.2 Construction Kit layer .....	127
10.2.3 Types .....	128
10.2.4 TAGs .....	129
10.3 Tenants .....	129
10.4 Data access.....	130
10.5 Configuration and display .....	130
10.5.1 Tenants.....	131
10.5.2 Construction Kit Management.....	133
10.5.3 Type Explorer .....	135
10.5.4 GraphQL Editor .....	137
10.6 Trend Visualizer .....	137
10.6.1 Trend views.....	138
10.6.2 Data sources.....	144
10.6.3 Datasets .....	146



<b>11 Identity Service: Central authentication service</b> .....	<b>148</b>
11.1 External identity providers.....	150
11.2 Identity Service .....	150
11.2.1 Login .....	151
11.2.2 User role: Identity Administrator .....	156
11.2.3 Identity Service - user interface.....	157
11.3 Identity Management.....	174
11.3.1 Users (internal login).....	175
11.3.2 Groups.....	181
11.3.3 Access control .....	194
11.3.4 Report permissions.....	199
11.3.5 Identity providers (for external logins) .....	207
11.3.6 Clients .....	221
11.3.7 Settings .....	238
11.3.8 Navigation bar.....	243
<b>12 Platform configuration</b> .....	<b>243</b>
12.1 Service connections .....	244
12.2 HTTPS certificate .....	245
12.2.1 Change HTTPS certificate.....	247
12.2.2 Change "Issued by" for custom certificate.....	250
12.2.3 Certificates .....	251
<b>13 Device Management</b> .....	<b>266</b>
13.1 General.....	267
13.2 Devices.....	268
13.2.1 Detail view - Devices.....	271
13.2.2 Configure device for Device Management.....	276
13.3 Packages.....	280
13.3.1 Deploying zenon projects for Device Management .....	282
13.4 Deployment task.....	283
13.4.1 Create deployment tasks .....	285
13.4.2 Detail view - Deployment task.....	292
<b>14 IIoT API</b> .....	<b>295</b>
14.1 Service Engine - third-party application: Provide process data.....	296
14.2 Report Engine > third-party application: Provide report data.....	298
14.2.1 Data sources for Report Engine .....	300
14.2.2 Multiple Service Engine instances .....	301
14.3 IIoT API.....	302

14.4 Login to Swagger API documentation.....	302
14.5 Status bits for variables.....	302
14.6 Navigation bar.....	302
<b>15 IloT Services Gateway.....</b>	<b>303</b>
15.1 Installation.....	304
15.2 Configuration.....	304
15.2.1 Configuration in zenon6.ini.....	306
<b>16 IloT Services - configurations in Engineering Studio.....</b>	<b>307</b>
16.1 Trust.....	307
16.2 IloT Services.....	307
16.2.1 Connection to IloT Services.....	308
16.2.2 Access permission for variables.....	309
16.2.3 Data Storage.....	309
16.2.4 Identity Service.....	314
16.2.5 Device Management.....	323
16.3 Data Hub.....	328
16.3.1 Connect to Data Hub.....	329
16.3.2 Configure variables.....	329
16.4 Connectors.....	330
16.4.1 IloT Services Gateway.....	331
16.4.2 Data Hub driver.....	333
16.4.3 IloT Services Connector.....	333
16.5 Checklist: Connection between Service Engine and IloT Services.....	334
<b>17 Appendices.....</b>	<b>334</b>
17.1 Advanced configurations.....	335
17.1.1 Installation options.....	335
17.1.2 Configurations for individual services.....	338
17.1.3 Configurations for several services (configured centrally).....	344
17.1.4 Configurations for several services (configured decentrally).....	346
17.1.5 Adjustments when changing the host name.....	347
17.2 IloT API: Query historic variables.....	348
17.3 Docker commands.....	348
17.3.1 Completely delete installation.....	349
17.4 IloT Services - Diagnosis and LOG messages.....	350
17.4.1 IloT Services (Windows native).....	350
17.4.2 IloT Services (Docker).....	350
17.4.3 IloT Services (Docker on Windows).....	351

17.4.4 Activation of zenon logging for Docker .....	351
17.4.5 Additional modules in the Diagnosis Viewer .....	352
17.5 Troubleshooting .....	353
17.5.1 Checklist: Verify basic configuration .....	353
17.5.2 Docker .....	355
17.5.3 HSTS problems during new installation .....	356
17.5.4 Identity Service .....	356
17.5.5 IIoT API: Error codes .....	357
17.5.6 Windows hibernation: Different timestamps (Docker on Windows) .....	359

# 1 Welcome to COPA-DATA help

## **GENERAL HELP**

If you cannot find any information you require in this help chapter or can think of anything that you would like added, please send an email to [documentation@copadata.com](mailto:documentation@copadata.com).

## **LICENSES AND SERVICES**

If you find that you need other zenon services or licenses, our staff will be happy to help you. Email [sales@copadata.com](mailto:sales@copadata.com).

## **PROJECT SUPPORT**

You can receive support for any real project you may have from our customer service team, which you can contact via email at [support@copadata.com](mailto:support@copadata.com).

## 2 IIoT Services



The IIoT Services link local production sites to a global production network.

The IIoT Services are an extension of the zenon software platform.

### FUNCTIONS

**The IIoT Services supplement the zenon Software Platform with the following functions:**

- ▶ Cross-site networking:  
Secure connection of selected zenon applications to remote sites using standard Internet connections.
- ▶ Integration of 3rd party applications:  
You can easily integrate 3rd party applications into the zenon software platform with the IIoT API.
- ▶ Central authentication service:  
Unified user authentication via the **Identity Service** for selected zenon applications.
- ▶ Distribution of software packages to devices:  
The distribution of zenon projects for Service Engine on devices is administered using the

**Device Management** service. You can create software packages from existing zenon projects. These packages can be deployed to devices instantly or scheduled.

The modular structure of the IloT Services allows for a wide variety of application scenarios within the zenon software platform. Possible usage scenarios are described in the respective services.

## COMPATIBLE APPLICATIONS

Selected zenon applications can be connected to IloT Services via appropriate connectors.

### Compatible zenon applications:

- ▶ Service Engine
- ▶ Report Engine
- ▶ Web Engine

You can also integrate a wide variety of 3rd party applications in the zenon Software Platform with **IloT API**.

### Compatible 3rd party applications include, for example:

- ▶ Applications developed by your company
- ▶ Third-party manufacturer applications (e.g. ERP systems or MES)
- ▶ Dashboard applications (e.g. Grafana)
- ▶ Mobile applications

In principle, every 3rd party application that can exchange data via a REST interface is compatible with the IloT Services.

## EXTENDED AREA OF APPLICATION

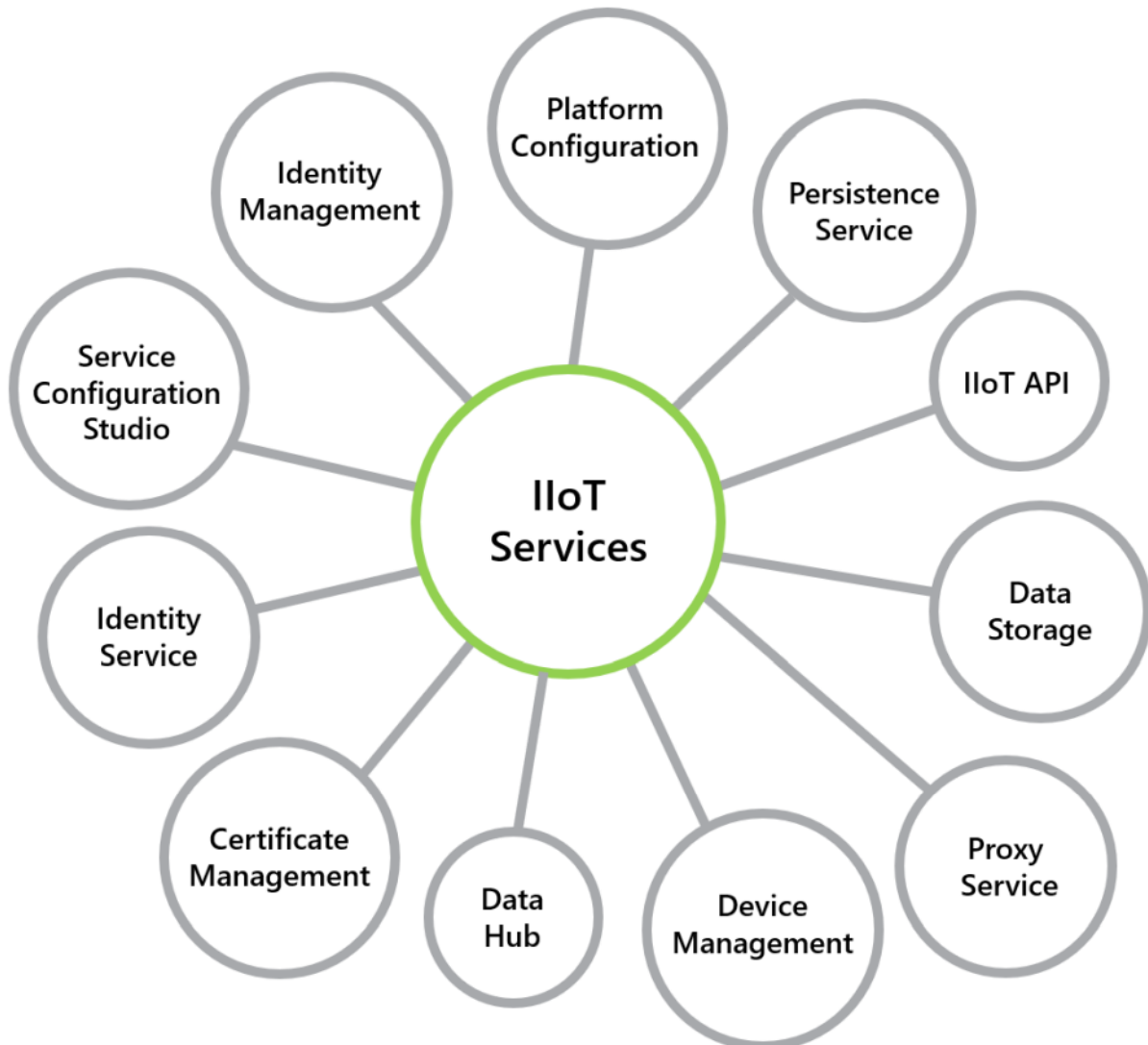
The table shows the benefits of using the IloT Services:

Description	zenon without IloT Services	zenon with IloT Services
Network infrastructure	<b>Requirements:</b> <ul style="list-style-type: none"> <li>▶ Stable local network connections</li> <li>▶ High bandwidth required</li> <li>▶ Protected network infrastructure</li> </ul>	<b>Requirements:</b> <ul style="list-style-type: none"> <li>▶ Connections may be interrupted temporarily</li> <li>▶ Connections with low bandwidth are generally sufficient</li> <li>▶ Public network infrastructure (unprotected) is sufficient</li> </ul>
Network connections	No compensation of temporary	Compensation of temporary

Description	zenon without IloT Services	zenon with IloT Services
	interruptions of the connection.	interruptions of the connection.
Connection to third-party applications	<p><b><u>Either via:</u></b></p> <ul style="list-style-type: none"> <li>▶ zenon API</li> <li>▶ Add-In Framework</li> <li>▶ Self-developed drivers</li> </ul> <p>Connection usually within the production network.</p>	<p><b><u>Uniformly via:</u></b></p> <ul style="list-style-type: none"> <li>▶ IloT API</li> </ul> <p>Connection either within the production network or via the Internet.</p>
Primary area of application	<ul style="list-style-type: none"> <li>▶ secure local networks (LAN)</li> </ul>	<ul style="list-style-type: none"> <li>▶ secure local networks (LAN)</li> <li>▶ insecure wide area networks (WAN)</li> </ul>
Cross-site networking	<p>Not supported by default.</p> <p>Only possible by encryption on the network level (VPN).</p>	<p>Supported by default.</p> <p>IloT Services autonomously encrypt all required connections at application level.</p> <p>Standard Internet connections are sufficient to securely connect sites with each other.</p> <p>A VPN is not required.</p>

### 3 Basic knowledge

#### INTERNAL SERVICES OF THE IIoT SERVICES



The graphic shows some logical units and internal services of the IIoT Services.

Logical units are:

1. IIoT Services – umbrella term for the sum of all internal services.

All other elements of this illustration are internal services.

A typical IIoT Services installation consists of a multitude of internal services.

#### Internal services are for example:

- ▶ **Identity Service** – authorizes access of users and clients.
- ▶ **IIoT API** – allows third-party applications to access the IIoT Services.
- ▶ **Data Storage** – Central storage of archive data (historical variable values)



Internal services are automatically connected to each other and fundamentally set up during the installation of the IIoT Services. How the internal services are installed (on page 39) depends on the installation option selected.

## EXTERNAL SERVICES FOR THE IIOT SERVICES



A use case for the IIoT Services:

1. A Service Engine instance generates process data as an external service.
2. The process data is fed into the IIoT Services using the Data Hub.
3. Third-party applications can access the process data as external services by means of the IIoT API.

The amount of internal services of the IIoT Services that are involved in a data transaction always depends on the specific use case.

You can connect different external services to the IIoT Services. External services are all applications that you can connect to IIoT Services but are not part of a IIoT Services installation themselves.

### Examples of external services are:

- ▶ Service Engine
- ▶ Report Engine
- ▶ Third-party applications

You must connect external services to the IIoT Services yourself and configure them accordingly. In a typical use case (on page 17), you must also install and configure a number of other applications in addition to the IIoT Services.

### ⚠ Attention

zenon applications:

- ▶ zenon applications that are not part of the internal services of the IloT Services are always treated as external services by the IloT Services.
- ▶ This also applies where both zenon applications and the IloT Services have been installed on the same computer through the same platform setup.

For this, see the installation recommendations (on page 42).

## 3.1 Architecture

The data flows in the IloT Services are protected by a multi-stage security concept. This begins in the transport layer of the network traffic.

### Communication is secured by:

- ▶ Trusted **Certificate Bundles** for internal services and zenon applications.
- ▶ Automatic verification of the send and receive permissions of messages on the protocol level.
- ▶ Central user authentication with **Identity Service** for users and client applications.

The security concept of the IloT Services thus also protects communication via public non-secure networks such as the internet. You do not require a VPN for cross-site connections. A standard internet connection is enough.

## 3.2 Internet connection

The IloT Services have only low requirements for network connections. Basically, even narrowband internet connections are sufficient to connect applications. In addition, temporary connection interruptions are compensated for by IloT Services.

However, the connection quality needed for the operation of a specific application always depends on the particular use case.

### Important parameters for the quality of internet connections are:

- ▶ Latency
- ▶ Bandwidth
- ▶ Connection stability

When planning a use case, you must determine the quantities of data to be sent via the internet connection and in which intervals. This determines the required connection quality.

### 3.3 Configuration files (Docker)

You can download the configuration files for IloT Services from the zenon website.

#### The download contains:

- ▶ IloT Services configuration files: `.env` and `docker-compose.yml`
- ▶ PDF file: **IloT Services Help** (including **Getting Started Guide**)

#### To download the configuration files:

- ▶ Go to the **copadata.com** website
- ▶ Go to the following subpage:  
**Downloads -> Product-Downloads -> Software -> Current versions -> IloT Services**
- ▶ Download the `.zip` file with the latest version of **IloT Services** (Docker).

**Note:** You must log in to the COPA-DATA website with your user account for this download. Registration is free.

#### **.ENV FILE**

The `.env` file contains configuration data for user names, logins and the database connection. The file is provided with empty variable fields. The configuration files are read when the IloT Services are initialized.

#### To do this, you must:

- ▶ configure the `.env` file with the values for your system.

The file will be loaded again every time Docker is started. But not all values will be reset when an initialized system is restarted!

The values that have to be set once during the initial configuration can be found in the `.env` file.

#### **Tip**

##### **Subsequent editing of the `.env` file**

Once the IloT Services have been initialized for the first time, the `.env` file should not be edited again. This helps you avoid having to make extensive manual configurations of an existing system.

#### **DOCKER-COMPOSE.YML**

The `docker-compose.yml` file contains basic settings for the configuration of the IloT Services.

#### You need this file to:

- ▶ Initialize the IloT Services via the command line.

- ▶ Start the already-initialized IIoT Services via the command line.

The file is fully configured and should not be edited.

### DOCKER-COMPOSE.OVERRIDE.YML

The **docker-compose.override.yml** file gives you the option to enable the **Persistence Service** port on the host system. You then have access to the **Persistence Service** through tools such as **Mongodump** and **Mongorestore**.

#### To do this, you must:

- ▶ Start **docker-compose.override.yml** together with **docker-compose.yml**.

The file is fully configured and should not be edited.

### DOCKER-COMPOSE.WEB-ENGINE.YML

You need the optional **docker-compose.web-engine.yml** file if you want to use **Web Engine** together with the IIoT Services.

#### To do this, you must:

- ▶ Configure the relevant section for "**HTML Web Engine**" in the **.env** file.
- ▶ Start **docker-compose.web-engine.yml** together with **docker-compose.yml**.

Further configurations are not necessary in this file.

## 3.4 Minimum password requirements

The minimum password requirements must be met for every password assigned for IIoT Services. This is due to technical reasons and thus also applies for protected test environments.

Unsuitable passwords can cause malfunctions in IIoT Services.

The minimum password requirements in IIoT Services are:

- ▶ Password length: At least 8 characters
- ▶ One uppercase letter (A - Z)
- ▶ One lowercase letter (a-z)
- ▶ One numeric character (0 - 9)
- ▶ One special character (!#\$%&'()\*+,-./\;:<=>?[]@^\_`{|}~)

### Information

The password complexity can be configured in the Service Configuration Studio in **Identity Management** in the settings node.

Only when all the requirements have been met is a password regarded as being suitable. Unsuitable passwords fail to meet at least one of the above-mentioned requirements.

When configuring passwords, a difference must be made between two cases:

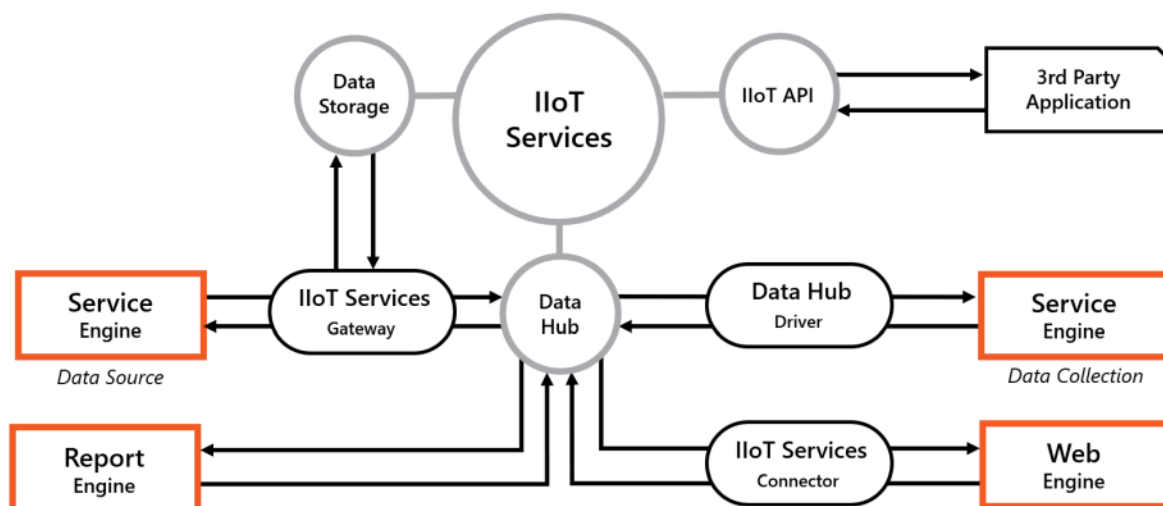
- ▶ Configuration using GUI:  
Configuration of a password in Service Configuration Studio is validated during configuration. You are only able to configure suitable passwords here.
- ▶ Configuration using the configuration file:  
It is technically possible to configure unsuitable passwords in the `.env` file. This leads to authentication problems between services.

**Important:** Only use suitable passwords that fully meet the minimum password requirements.

## 3.5 Certificates for IIoT Services

You can find detailed information about certificate handling in Service Engine in the **Certificates** (on page 251) section in **Platform configuration** (on page 243).

## 4 Possible use cases



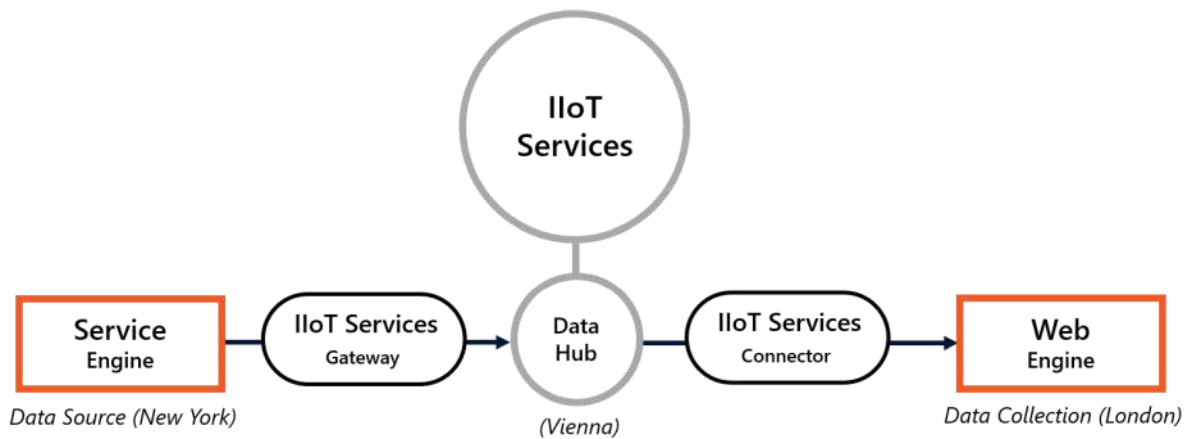
IIoT Services: Networking of zenon applications, zenon services and third-party applications.

This section describes supported use cases for the IIoT Services.

**The IIoT Services can be used to connect the following services to one another:**

- ▶ Select zenon applications (Service Engine for example)
- ▶ Selected zenon services (**Data Storage** for example)
- ▶ Deployment of zenon project data to devices (for example, computers, virtual machines, Raspberries or Linux).
- ▶ Third-party applications (via the IIoT API)

## 4.1 Service Engine > Web Engine: Remote control



IIoT Services allow the Web Engine to access process screens of a Service Engine.

**Web Engine** provides process screens of a Service Engine for access via browser. Using IIoT Services, the **Web Engine** can be operated at a different site than Service Engine.

### AREA OF APPLICATION

#### You can use Web Engine as:

- ▶ Remote visualization of a Service Engine
- ▶ Remote control of a Service Engine

### SUPPORTED DATA ACTIONS


You can carry out the following data actions in Service Engine by means of the **Web Engine**:

Supported data action	Access permission variable*
Read alarms	<i>Read only</i>
Acknowledge alarms	<i>Read-write</i>
Comment on alarms	<i>Read-write</i>
Set causes of alarms	<i>Read-write</i>
Variables** - read	<i>Read only</i>
Variables** - write	<i>Read-write</i>
Archive data*** - read	<i>Read only</i>



Supported data action	Access permission variable*
Read events	<i>Read only****</i>
Comment on events	<i>Read and write</i>

- \* \* Required access authorization in Service Engine (data source).
- \*\* simple variable type (no structure variables, no arrays).
- \*\*\* Only as a curve in Extended Trend.
- \*\*\*\* No access authorization is required for system events.

 **Information**

You can find detailed information on the **Web Engine** in the **HTML Web Engine** node.



## 4.2 Report Engine > Service Engine: Create data predictions

### AREA OF APPLICATION

Data predictions attempt to derive the future development of variables from recorded variable values of the past.

#### Examples of this are:

- ▶ Prediction of consumption figures:  
Predictions can be made, for example, on how much electricity will probably be consumed.
- ▶ Prediction of material consumption:  
Predictions can be made, for example, about when an inventory will probably be depleted.
- ▶ Anomaly detection:  
Identifies unusual deviations between predicted and actual variable values. This can point to defects in production.

All data predictions are based on historical variable values.

### PREDICTION MODEL

This use case requires that a prediction model for data predictions already exists in Report Engine. How you can create a prediction model for your data is documented in detail in the Help for Report Engine.

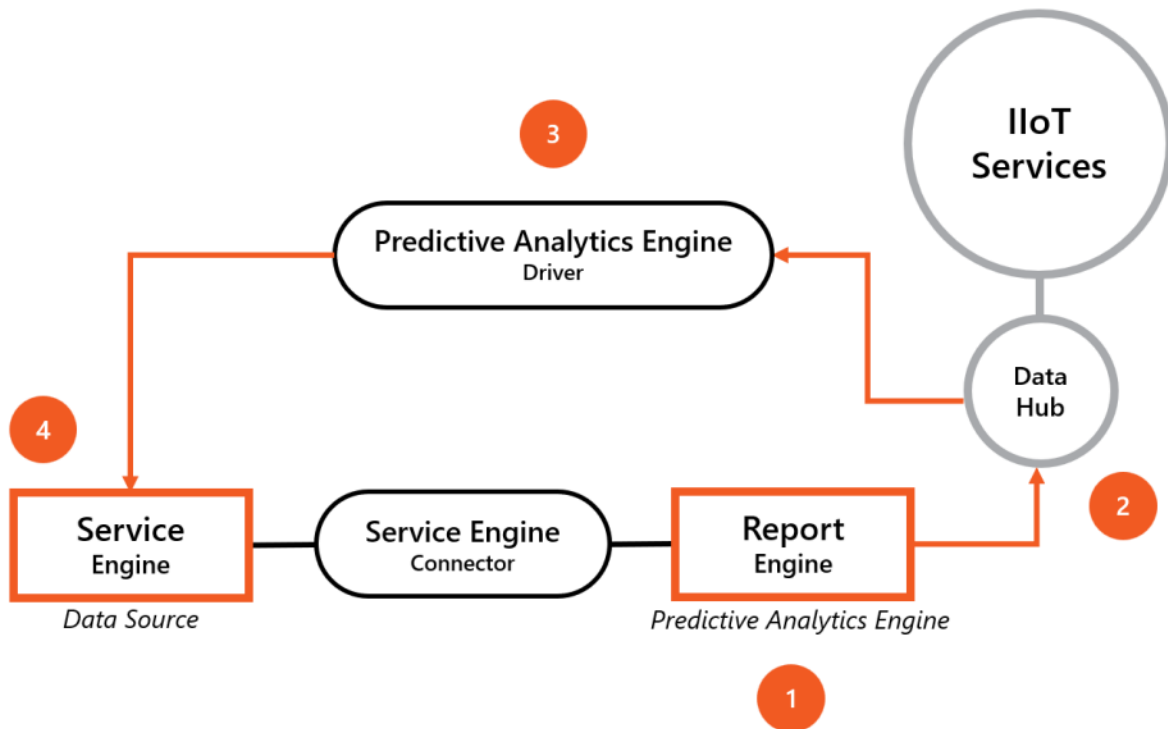
There are two cases in which data predictions can be used by Service Engine.



#### **Information**

You can find more detailed information in the **Report Engine** section.

#### 4.2.1 Case A) Passive reception of data predictions



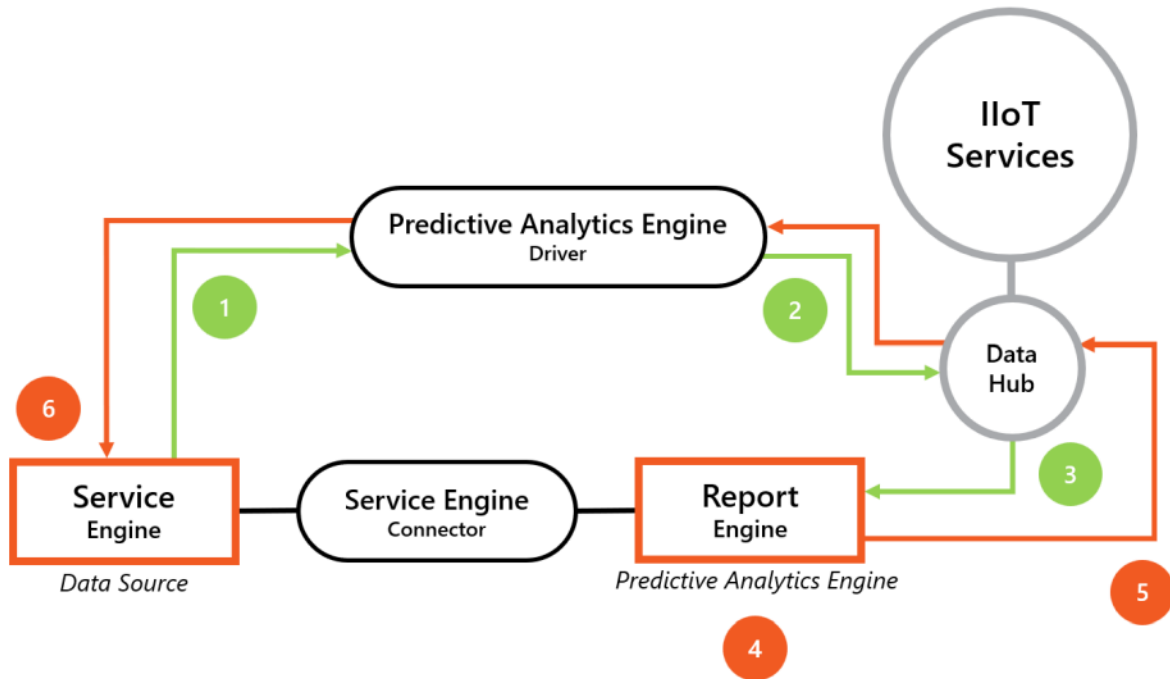
Service Engine is in this case a mere receiver of data predictions.

**The procedure is as follows:**

1. Report Engine creates a data prediction.
2. The data prediction is transmitted from Report Engine to **Data Hub** .
3. **Predictive Analytics Engine Driver** retrieves the data prediction from the **Data Hub** and forwards it to Service Engine.
4. Service Engine works with the data prediction.

In this case, Report Engine decides when a data prediction is created.

#### 4.2.2 Case B) Active request of data predictions



In this case, Service Engine actively requests a data prediction from Report Engine.

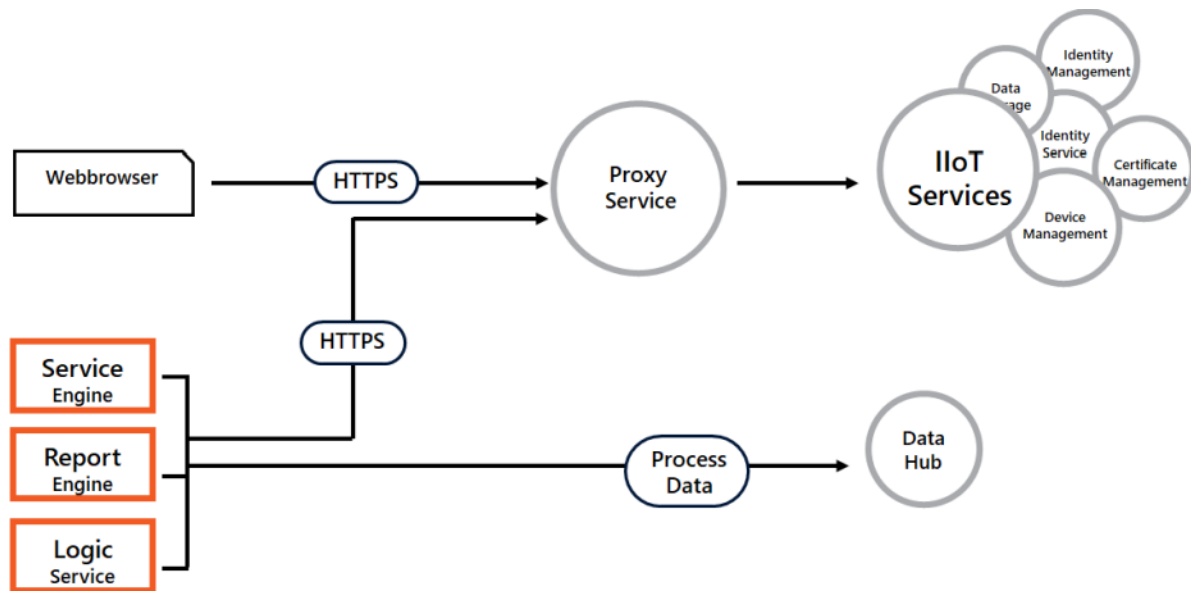
**The procedure is as follows:**

1. Service Engine triggers the creation of a data prediction.
2. This request is sent to **Data Hub** with **Predictive Analytics Engine Driver**.
3. **Data Hub** transmits the prediction request to Report Engine.
4. Report Engine creates a data prediction based on the parameters of the request.
5. The data prediction is sent to Service Engine with **Data Hub** and **Predictive Analytics Engine Driver**.
6. Service Engine works with the data prediction.

In this case, Service Engine decides when a data prediction is created.

## 5 Communication - Proxy Service

From zenon version 11.2, communication with the IIoT Services is carried out via a central Proxy Service.



The following is applicable for communication via Proxy Service:

- ▶ The Proxy Service is the central starting point for overall HTTPS communication with the IIoT Services.
- ▶ As a result, only a central URL for the connection to the IIoT Services still needs to be configured.
 

**Note:** Ensure that the port for the Proxy Service is not blocked by firewall rules. The forwarding to the individual services of the IIoT Services is carried out via the Proxy Service.
- ▶ If the central IIoT Services URL is entered in a web browser, Service Configuration Studio is opened.
- ▶ The Data Hub communicates process data. The protocol used is therefore not HTTPS traffic and therefore does not use the Proxy Service.
 

**Note:** Ensure that the port for the Data Hub is not blocked by firewall rules.

## 5.1 IIoT Services communication ports

IIoT Services service	Description	Default port
<b>Proxy Service</b>	<p>The central entry point to the IIoT Services for HTTP traffic.</p> <p>The following IIoT Services are supported by the Proxy Service:</p> <ul style="list-style-type: none"><li>▶ Service Configuration Studio</li><li>▶ <b>Identity Service</b></li><li>▶ <b>Identity Management</b></li><li>▶ <b>Certificate Management</b></li><li>▶ <b>Data Storage</b></li><li>▶ <b>Platform Configuration</b></li><li>▶ <b>IIoT API</b></li><li>▶ <b>Device Management</b></li></ul> <p>HTTP-based communication is forwarded to the individual services internally. You can find a detailed list of the individual services and their internal ports in the <b>Services, Ports and URLs</b> (on page 27) chapter.</p>	9443
<b>Data Hub</b>	Central data transfer hub that receives information from services and distributes it to other services. The	9411

IIoT Services service	Description	Default port
	communication is event-based.	

## 5.2 Services, ports and URLs

This table offers you an overview of all services and ports in the IIoT Services. This information applies both to when the IIoT Services runs in a Docker environment and to the IIoT Services on Windows.

Docker container or Windows Service	URL* (default port)	Description	Default state
<b>proxy-service</b> (Proxy Service)	<i>https://[mycomputer.mydo main.com]:9443</i> Port 9443.	The central starting point in IIoT Services services for HTTP traffic.	<i>running</i>
<b>data-hub</b> (Data Hub)	No configuration in Service Configuration Studio. Port 9411.	Central data transfer hub that receives information from services and distributes it to other services. The communication is event-based.	<i>running</i>
<b>data-storage</b> (Data Storage)	No configuration in Service Configuration Studio. Port 9460.	Service for saving data.	<i>running</i>
<b>certificate-management</b> (Certificate Management)	<i>https://[mycomputer.mydo main.com]:9410</i>	Controls access of services to the <b>Data Hub</b> .	<i>running</i>
<b>identity-service</b> (Identity Service)	<i>https://[mycomputer.mydo main.com]:9430</i>	Central authentication. Verifies the login to the IIoT Services.	<i>running</i>
<b>identity-management</b> (Identity Management)	<i>https://[mycomputer.mydo main.com]:9431</i>	Provides the configuration interface for the <b>Identity Service</b> .	<i>running</i>
<b>data-modeling</b> (Data Modeling)	<i>https://[mycomputer.mydo main.com]:9440</i>	Administration and storage of data in the zenon software platform. You can create and administer your own data models.	<i>running</i>
<b>device-management</b> (Device Management)	<i>https://[mycomputer.mydo</i>	Deploys Service Engine files for configured devices.	<i>running</i>

Docker container or Windows Service	URL* (default port)	Description	Default state
	<i>main.com]:9415</i>		
<b>platform-configuration</b> (Platform Configuration)	<i>https://[mycomputer.mydo main.com]:9470</i>	Provides support for configurations in the IIoT Services	<i>running</i>
<b>iiot-api</b> (IIoT API)	<i>https://[mycomputer.mydo main.com]:9400</i>	Offers an API for data access of external systems and external applications to the zenon software platform.	<i>running</i>
<b>persistence-service</b> (Persistence Service)	No configuration in Service Configuration Studio. No port.	Database that is used by the various services for storing data. Runs in the background.	<i>running</i>
<b>iiot-services-redis</b> (---)	No configuration in Service Configuration Studio. Port 6379.	Internal service for communication.	<i>running</i>
<b>service-configuration-studio</b> (Service Configuration Studio)	<i>https://[mycomputer.mydo main.com]:9450</i>  <b>Note:</b> From version 11, Service Configuration Studio can also be called up with <i>localhost:9450</i> if the IIoT Services are running in a Docker environment.	Central administration interface of IIoT Services.	<i>running</i>

\*Replace *[mycomputer.mydomain.com]* with the computer host name.

 **Tip**

You can also define ports for services yourself using advanced configurations (on page 335).



### 5.3 Addresses and URLs in Service Configuration Studio

The administration of IIoT Services is set up and configured in Service Configuration Studio. The following services are important for the use of the IIoT Services:

Web interface	Description	Login
<b>Service Configuration Studio</b>	<p>Central administration interface for all user accounts and further services of the IIoT Services.</p> <p>Contains all web interfaces except <b>Identity Service</b>.</p>	Only users with the <i>Administrator</i> user role can log in.
<b>Identity Service</b>	<p><b>Identity Service</b> is the central login service for users and clients.</p> <p>Every user can configure basic settings for their own user account in Service Configuration Studio.</p>	All users with a user account in <b>Identity Service</b> can log in.



## 5.4 Configurable services in the Service Configuration Studio

A number of IIoT services have been integrated into Service Configuration Studio. The configuration interfaces of services can also be called up individually.

**The following services are integrated in Service Configuration Studio:**

Service	Description	Login	Service Configuration Studio URLs
Service Configuration Studio	Central administration interface for all user accounts and further services of the IIoT Services.	<p>Only administrators of the respective services can work actively in Service Configuration Studio.</p> <p>In principle, the following applies: All services are displayed in Service Configuration Studio. However, only the nodes for which administrator rights are present due to login can be configured.</p>	<p><i>https://[IIoT Services URL]:9443/</i></p> <p><b>Example:</b> <i>https://mydomain.local:9443/</i></p>



Service	Description	Login	Service Configuration Studio URLs
<b>Identity Service</b>	<p>Central login service for users and clients.</p> <p>You can find further information in relation to this in the <b>Identity Service</b> (on page 150) section.</p>	<p>Every user can configure basic settings for their own user account in the web interface.</p>	<p><i>https://[IIoT Services URL]:9443/identity</i></p> <p><b>Example:</b> <i>https://mydomain.local:9443/identity</i></p>
<b>Certificate Management</b>	<p>Administers Certificate Bundles that secure communication for the IIoT Services.</p> <p>You can find further information in relation to this in the <b>Certificate Management</b> (on page 104) section.</p>	<p>Only users with the <i>Certificate Administrator</i> user role can use this interface.</p>	<p><i>https://[IIoT Services URL]:9443/certificate-management</i></p> <p><b>Example:</b> <i>https://mydomain.local:9443/certificate-management</i></p>



Service	Description	Login	Service Configuration Studio URLs
<b>Identity Management</b>	<p>Comprehensive administration of users, clients and connected applications.</p> <p>You can find further information in relation to this in the <b>Identity Management</b> (on page 174) section.</p>	<p>Only users with the <i>Identity Administrator</i> user role can use this interface.</p>	<p><i>https://[IoT Services URL]:9443/identity-management</i></p> <p><b>Example:</b> <i>https://mydomain.local:9443/identity-management</i></p>



Service	Description	Login	Service Configuration Studio URLs
<b>IIoT API</b>	<p>You can connect any number of 3rd party applications to IIoT Services via the REST API.</p> <p>Service Configuration Studio offers a test environment and the documentation of the API.</p> <p>You can find further information in relation to this in the <b>IIoT API</b> (on page 295) section.</p>	<p>Configuration of this service in Service Configuration Studio is possible without login.</p> <ul style="list-style-type: none"> <li>▶ If a user wants to retrieve the data manually via the API, the user must authorize themselves in Service Configuration Studio by clicking a button.</li> <li>▶ The user requires access permissions for the zenon project of the data the user is retrieving.</li> </ul>	<p><i>https://[IIoT Services URL]:9443/iiot-api</i></p> <p><b>Example:</b> <i>https://mydomain.local:9443/iiot-api</i></p>



Service	Description	Login	Service Configuration Studio URLs
<b>Platform Configuration</b>	<p>Supports, for initial configurations of the IloT Services:</p> <p>Creation of initial user account for <b>Identity Service</b></p> <p>Configuration of the HTTPS certificates to be used.</p> <p>You can find further information in relation to this in the <b>Platform Configuration</b> (on page 243) section.</p>	<p>In the course of setup, a user will be created for login.</p>	<p><i>https://[IloT Services URL]:9443/platform-configuration</i></p> <p><b>Example:</b> <i>https://mydomain.local:9443/platform-configuration</i></p>
<b>Device Management</b>	<p>Deployment of zenon projects on devices.</p> <p>Provides project data as software packages for Service Engine on the devices.</p> <p>You can find further information in relation to this in the <b>Device Management</b> (on page 266) section.</p>	<p>Only users with the <i>Device Management Administrator</i> user role can use this interface.</p>	<p><i>https://[IloT Services URL]:9443/device-management</i></p> <p><b>Example:</b> <i>https://mydomain.local:9443/device-management</i></p>



Service	Description	Login	Service Configuration Studio URLs
<b>Data Storage</b>	<p>Central storage space for alarm data, archived data and event data from one or more Service Engine.</p> <p>You can find further information in relation to this in the <b>Data Storage</b> (on page 115) section.</p>		<p><i>https://[IoT Services URL]:9443/data-storage</i></p> <p><b>Example:</b> <i>https://mydomain.local:9443/data-storage</i></p>
<b>Data Modeling</b>	<p>Service for the central administration and storage of data in the zenon software platform. You can create and administer your own data models.</p> <p>You can find further information in relation to this in the <b>Data Modeling</b> (on page 124) section.</p>		<p><i>https://[IoT Services URL]:9443/data-modelling</i></p> <p><b>Example:</b> <i>https://mydomain.local:9443/data-modelling</i></p>

**Tip**

You can make advanced settings for the IIoT Services via the configuration files. However, this is only necessary in exceptional cases.

Communication - Proxy Service





## 5.5 Monitor and restart services

Where you can monitor and restart the services of the IIoT Services depends on the installation option selected for the IIoT Services.

### DOCKER

In Docker, each service of the IIoT Services runs **as a separate container**. This applies for both the **Docker on Windows** and **Docker on Linux** installation options.

In both cases, you can stop and restart containers using the command line interface (CLI).

#### Which command line application you use depends on the operating system:

- ▶ Windows: **PowerShell**
- ▶ Linux: **Bash**

You required to open the command line with administrator privileges.

Description	Command
List all running containers (without stopped ones)	<code>docker ps</code>
List all available containers (including stopped ones)	<code>docker ps -a</code>
Stop a particular container	<code>docker stop &lt;container-name or container ID&gt;</code>
Stop all running Docker containers	<code>docker stop \$(docker ps -a -q)</code>
Start a particular container (the container must be stopped)	<code>docker start &lt;container-name or container ID&gt;</code>
Restart a particular container	<code>docker restart &lt;container-name or container ID&gt;</code>

### DOCKER ON WINDOWS

In **Docker Desktop for Windows**, the **Dashboard** also offers you a graphical user interface for managing containers. Here, you can visually monitor the status of individual containers and restart them with a mouse click.

### WINDOWS-NATIVE

In this installation option, the services of the IIoT Services run **as Windows services**. You can use the **Services** service manager to monitor the services and restart them, if necessary.

 **Info**

Automatic restart of services:

Services of the IIoT Services automatically restart under certain circumstances.

**A distinction needs to be made here between two different cases:**

- ▶ During the initial start, it can happen that due to delays, individual services restart themselves. This is normal system behavior as long as not all services completely restart.
- ▶ If an already installed service restarts itself during ongoing operation, this can be a sign of malfunction. In this case, the LOG messages contain further information.

This applies for all installation options of the IIoT Services.

## 6 Installation

In this section you will find information for installing IIoT Services and for the initial setup on Windows or Docker.



## 6.1 Installation

It is recommended to always install the latest IIoT Services release. Existing installations can be upgraded within the recommended update paths (on page 44).

### INSTALLATION VARIANTS OF THE IIOT SERVICES

IIoT Services offer the same range of functions in all installation options.

**Please note the following differences:**

	IIoT Services (Docker on Windows)	IIoT Services (Docker on Linux)	IIoT Services (Windows native)
<b>Application area</b>	<ul style="list-style-type: none"> <li>▶ Test environments</li> </ul>	<ul style="list-style-type: none"> <li>▶ Test environments</li> <li>▶ Productive environments</li> </ul>	<ul style="list-style-type: none"> <li>▶ Test environments</li> <li>▶ Productive environments</li> </ul>
<b>Host operating system</b>	Windows	Linux	Windows
<b>Method of installation</b>	Configuration files	Configuration files	As native Windows application via a .ISO file  The installation of the IIoT Services is integrated in the <b>Setup of the software platform.</b>
<b>Internal services</b>	Docker services as a Linux container	Docker services as a Linux container	Windows Services
<b>Monitoring of internal</b>	<ul style="list-style-type: none"> <li>▶ <b>Windows</b></li> </ul>	<ul style="list-style-type: none"> <li>▶ With Shell</li> </ul>	<b>Windows Management Console.</b>



	IloT Services (Docker on Windows)	IloT Services (Docker on Linux)	IloT Services (Windows native)
<b>services</b>	<b>PowerShell</b> <ul style="list-style-type: none"> <li>▶ With GUI via <b>Docker Dashboard</b></li> </ul>	No GUI available.	
<b>Minimum number of computers for test environment</b>	<ul style="list-style-type: none"> <li>▶ 1 computer for the IloT Services and all clients (Windows host OS)</li> </ul>	<ul style="list-style-type: none"> <li>▶ 1 computer for the IloT Services (Linux host OS)</li> <li>▶ 1 computer for clients (Windows host OS)</li> </ul>	1 computer for the IloT Services and all clients (Windows host OS)
<b>Minimum number of computers for productive environment</b>	<ul style="list-style-type: none"> <li>▶ 1 dedicated computer for the IloT Services.</li> <li>▶ Separate computers for clients.</li> </ul>	<ul style="list-style-type: none"> <li>▶ 1 dedicated computer for the IloT Services.</li> <li>▶ Separate computers for clients.</li> </ul>	<ul style="list-style-type: none"> <li>▶ 1 dedicated computer for the IloT Services.</li> <li>▶ Separate computers for clients.</li> </ul>

**Note:** The installation options of IloT Services are basically the same for the administration in the Service Configuration Studio.

### ⚠️ **Attention: Fixed user context in "Docker on Windows"**

A IIoT Services installation in **Docker Desktop for Windows Docker on Windows** is started in a **fixed user context**.

#### **Example: User A installs IIoT Services using Docker Desktop for Windows.**

- ▶ **User A** has access to IIoT Services through their user account.
- ▶ **User B** does not have access to IIoT Services through their user account on the same computer.

**Hint:** You can get around this limitation on a test system by using a shared user account.

## 6.1.1 Installation: Standalone vs. parallel vs. virtual machine

In general, it is recommended to install IIoT Services as standalone applications on a dedicated computer.

### STANDALONE INSTALLATION

With a standalone installation, other than IIoT Services, no further zenon services are installed.

#### **Standalone installation is recommended for:**

- ▶ All installation options of IIoT Services (Docker and Windows native)
- ▶ All computer types (physical computer and VMs)
- ▶ All uses (test systems and productive systems)

Standalone installation ensures a clear separation of connected communication partners in IIoT Services networks.

### PARALLEL INSTALLATION

In a parallel installation, both IIoT Services as well as other zenon services are installed on the same computer.

Parallel installation is only recommended for separately documented cases. An example of this is the test environment in the Getting Started Guide for the IIoT Services (Docker on Windows) installation option.

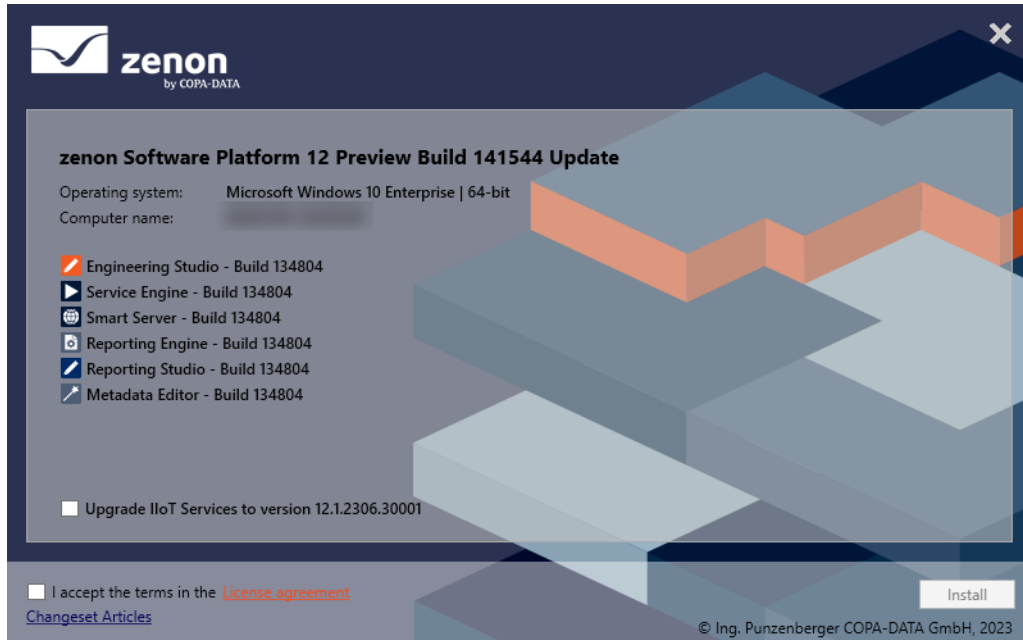
### INSTALLATION ON A VIRTUAL MACHINE

#### **⚠Attention**

If you run **IIoT Services** on a virtual machine with Docker containers: First check whether AVX commands are supported by the underlying hypervisor.

### 6.1.1.1 Build update IIoT Services

As of version 12, IIoT Services versions can also be updated when installing a build update. In this case, an option for updating the IIoT Services version to the current version is offered when the setup is called.



#### **Procedure:**

- ▶ Checkbox for upgrading IIoT Services is deactivated:  
IIoT Services are not updated. They remain in the version already installed on the system.
- ▶ Checkbox for upgrading IIoT Services is activated:
  - ▶ IIoT Services are updated to the current version.
  - ▶ The task performs a silent installation of the IIoT Services setup without rebooting.
  - ▶ If the installation is successful, a button for manual reboot is offered at the end.  
Do a reboot before starting IIoT Services. This ensures the correct operation of all services.

### 6.1.2 Kubernetes

In the Docker installation option, the IIoT Services services are installed in Linux containers. This meets the requirements for operating IIoT Services in a Kubernetes cluster.

#### **In particular, you should note:**

- ▶ The configuration files `docker-compose.yml` and `.env` provided with IIoT Services can be used as a foundation for creating Kubernetes configuration files.
- ▶ You must create customized Kubernetes configuration files for your specific environment.

**The following application scenarios are possible:**

- ▶ self-hosted Kubernetes cluster (*on-premise*)
- ▶ third-party hosted Kubernetes cluster of cloud providers such as Amazon (*Amazon Kubernetes Cluster*), Google (*Google Kubernetes Engine*) or Microsoft (*Azure Kubernetes Service*)

By using the Kubernetes container management, you can provide, scale and manage containers automatically.

 **Hint**

The use of IIoT Services in a Kubernetes cluster requires relevant prior knowledge and is generally recommended only for enterprise environments.

### 6.1.3 Update paths

**The following update paths are recommended for IIoT Services:**

- ▶ Version 2.0 to 2.1
- ▶ Version 2.x to 10.0
- ▶ Version 10.0 to 10.x
- ▶ 10.x to higher versions

Available configurations will be automatically carried over during the update. It is recommended to perform a backup of **Persistence Instance** before every version update.

### 6.1.4 Compatibility

The IIoT Services typically connect zenon applications and third-party applications to one another. It must be ensured that all connected applications are compatible with one another.

The following applies for a IIoT Services installation:

- ▶ Install the most recent version of the IIoT Services.
- ▶ The IIoT Services version must be at least just as high as the version of the connected zenon applications.



- ▶ All connected zenon applications must be compatible with the installed IIoT Services version.



### Information

Backward compatibility:

The IIoT Services support components of the zenon software platform from version 10 and higher.

#### 6.1.4.1 Renaming of Service Grid to IIoT Services

With version 12, the **Service Grid** and its Services and components were renamed to **IIoT Services**. The graphical user interface of the **IIoT Services** and apps (programs) and the help have been adjusted accordingly.

Previous versions up to and including 11.2	From version 12
Service Grid	IIoT Services
Service Grid Hub Controller	Certificate Management
Service Grid API	IIoT API
Service Grid Persistence	Persistence Service
Service Grid Studio	Service Configuration Studio
Service Grid Proxy	Proxy Service
Service Grid Gateway	IIoT Services Gateway
Service Grid Egress Connector	Data Hub Driver
Service Grid Ingress Connector	IIoT Services Gateway components.

#### 6.1.4.2 Compatibility of version 12 with previous versions

With version 12, the connection between Engineering Studio project configurations to IIoT Services and communication between the individual services was simplified.

For existing project configurations in Engineering Studio, it is expressly recommended that the connections to the IIoT Services and the configuration for individual services are reconfigured.

You can find detailed information on the configuration in the **IIoT Services - configuration in Engineering Studio** (on page 307) section.

### 6.1.4.3 Compatibility of version 11.2 with previous versions

From version 11.2 and higher, the individual services of IIoT Services are addressed using a central URL. The addressing of services was by means of port numbers in previous versions. The default port number for IIoT Services is *9443*. This port number can be adjusted by means of configuration.

If the central IIoT Services URL is entered in a web browser, Service Configuration Studio starts.

#### COMPATIBILITY NOTE - IIOT SERVICES 11.2

The following is applicable in order to work seamlessly with a zenon installation with IIoT Services:

- ▶ Service Engine or Engineering Studio in version 11 communicate with IIoT Services version 11.2 or higher:  
Build *117398* or higher for Service Engine or Engineering Studio must be installed.  
The following configurations must also be updated:
  - ▶ **Service Node Configuration Tool**  
When entering a **Connection** setting, add the */hub-controller* sub-path to the central URL.  
**Example:** *https://hostname.local/hub-controller*  
**Attention:** From version 12, the **Service Node Configuration Tool** has been replaced with the **IIoT Services Connection Wizard**.
  - ▶ Configuration in Engineering Studio  
It is not necessary to specify a subpath for configurations in Engineering Studio. The same URL is used for **Identity Service** and **Data Storage**. Entering the central URL is sufficient. The URL of the corresponding properties must be configured as URL + port.  
**Examples:**  
URL for **Identity Service** (**Network** property group, **Identity Service**, property: **URL**)  
URL for **Data Storage** (**Network** property group, **Data Storage**, property: **URL**)  
*hostname.local:9443*

### 6.1.4.4 IIoT Services update

You can migrate a IIoT Services installation to a higher version with little effort.

How to perform an update:

1. Back up the existing **Persistence Instance**.
2. Stop the IIoT Services.
3. Reinstall the IIoT Services in accordance with the installation option.

- ▶ IIoT Services (Docker): The `.env` file for the new version must be configured with the necessary values. Afterwards, the IIoT Services are initialized with the `docker-compose.yml`.
  - ▶ IIoT Services (Windows-native): Carry out the setup of the new version.
4. Restart the IIoT Services.

You have now updated the IIoT Services.

### Hint

Existing certificate bundles of an old IIoT Services version are usually compatible with the new version and do not need to be issued again.

The **Persistence Instance** with all configurations of the IIoT Services is migrated automatically.

The backup of the **Persistence Instance** is a security precaution. This means that a restore is possible in the event of an error.

## 6.1.4.5 Update MongoDB

From version 12, the update of MongoDB has been made much simpler for the user. MongoDB persistence instances can thus be updated to the most recent version that is used by the IIoT Services. Subsequent change is not possible.

Please also note the **Backup and restore – persistence instance** node in order to back up your data before an update.

### UPDATE FOR WINDOWS (NATIVE)

The updating of MongoDB for Windows operating systems is fully integrated into the setup. No additional manual steps are necessary.

### UPDATE FOR DOCKER

The following requirements are necessary for updating MongoDB in a Docker environment:

- ▶ The tool **CopaData.ServiceGrid.Tools.PersistenceManagementCli.exe** is installed on the computer running Docker Desktop for Windows.
- ▶ The installation is done by running `PersistenceManagementCli.x64.msi`.  
The data are stored in the following folder:  
`%programfiles%\zenon\zenon Platform 14\IIoT Services\PersistenceManagementCli`.
- ▶ The **MongoDB Command Line Database Tools** are installed.

- ▶ The PATH environment variable has been extended with the path to the MongoDB Command Line database tools (see previous step), e.g.:  
`C:\Tools\mongodb-database-tools-windows-x86_64-100.7.0\bin`
- ▶ The current version of the IIoT Services is installed and running.
- ▶ The .ENV file with the current settings and the docker-compose .YML file for the new version are available in their own Windows folder.
- ▶ Port 27017 is available on the computer for connecting to the MongoDB database.

## RUN UPDATE

In the Docker environment, do the following:

1. Open an elevated PowerShell.
  2. Navigate to the storage location of the CLI, e.g. (default path): `%programfiles%\zenon\zenon Platform 14\IIoT Services\PersistenceManagementCli`.
  3. Enter the following command:  
`CopaData.ServiceGrid.Tools.PersistenceManagementCli.exe docker upgrade`
- ▶ The tool starts and guides you through the update process step by step. Necessary parameters are queried. The update process is continued after the necessary parameters are entered. In addition, information and a log are displayed directly in the tool.

### 6.1.4.6 Login to the Identity Service after an update or upgrade

After an update or upgrade of the IIoT Services version, it may happen that logging in to the Identity Service in the web browser is no longer possible.

In this case, clear the cache of your web browser. In addition, you can call up the login screen in a private window of the web browser.

### 6.1.4.7 IIoT Services Gateway

The **IIoT Services Gateway** connects IIoT Services to zenon applications. It also ensures compatibility between different release versions.



#### Information

Recommendation: Generally speaking, you should always use the version of **IIoT Services Gateway** that corresponds to the installed version of IIoT Services.

## VERSION CHECK

Different versions of IIoT Services and **IIoT Services Gateway** can communicate with one another on the basis of a common protocol.

For communication, a check is carried out to see which version of the protocol is used by the individual components. The check is successful if all components use the same major version of the protocol. Minor versions can be different. If the major version is different for a component, communication is no longer possible.

### Example:

- ▶ Components with *20.00* can communicate with *20.10*.
- ▶ Components with *20.10* cannot communicate with *30.10*



### Information

Valid major version for IIoT Services 14: 20

**Note:** For versions of the zenon Software Platform prior to version 14, all components must correspond exactly. This also includes the minor version.

### 6.1.4.7.1 Installation

For the connection between zenon applications and IIoT Services, the appropriate version of the **IIoT Services Gateway** must be selected and installed.

The following applications use the **IIoT Services Gateway**:

- ▶ Service Engine
- ▶ Engineering Studio
- ▶ Report Engine
- ▶ Reporting Studio

**Important:** You must always execute both installers (x86 and x64) on each client. This way, you ensure that these clients can connect to the IIoT Services.

**Tip**

Check the installation:

Under **Apps and features**, the Windows operating system shows a separate entry for each installed version of the **IloT Services Gateway**.

## 6.1.4.7.2 Configuration

### PRIOR CONSIDERATIONS

Several versions of the **IloT Services Gateway** can be installed on a computer at the same time. The system cannot use these versions at the same time however. Only one version of the **IloT Services Gateway** can ever be centrally configured and used.

These processes can install a **IloT Services Gateway**:

- ▶ Installation of zenon applications via the platform setup.
- ▶ Build update of installed zenon applications.
- ▶ Installation of the **IloT Services Gateway** via two separate installers (x64 and x86).

In practice, several versions of the **IloT Services Gateway** are typically installed on a computer at the same time.

**Hint**

Use several versions alternately:

You can use several versions of the **IloT Services Gateway** alternately on one computer. For each change, you must configure the respective required version of the **IloT Services Gateway** manually in *zenon6.ini*.

### DEFAULT CONFIGURATION

By default, zenon applications always connect to IloT Services via the most-recently-installed version of the **IloT Services Gateway**.

The default configuration covers the usual application purposes and therefore does not generally need to be adjusted manually by the user.

### MANUAL CONFIGURATION

Manual configuration of the **IloT Services Gateway** by the user is only required in a few cases.

You can use manual configuration to stipulate to the system which version of the **IloT Services Gateway** zenon applications connect to the IloT Services.

**General requirement:**

Several versions of the **IloT Services Gateway** are installed on the computer.

**Manual configuration can, for example, be necessary in the following cases:**

- ▶ Subsequent downgrade of a zenon installation
- ▶ Parallel installations of different zenon versions on one computer
- ▶ Connection from zenon applications to different versions of the IloT Services
- ▶ The zenon version used does not support the latest version of the **IloT Services Gateway**.
- ▶ The connection should be established with a current **IloT Services Gateway** to the IloT Services of an older version.

 **Hint**

Restart applications and services:

You must restart the following components after manual configuration of the **IloT Services Gateway**:

- ▶ All zenon apps connected to the IloT Services: Service Engine, Engineering Studio and Reporting Studio
- ▶ The Windows service for the Report Engine service node (if you are using Report Engine): *zanMQTTClientxxxx*

The new configuration is only effective after restarting these applications and services.

### 6.1.4.7.3 Configuration in zenon6.ini

The **IloT Services Gateway** is configured centrally in the `%cd_system%\zenon6.ini` file. This setting is applicable for all zenon applications installed on the computer.

The default configuration is as follows:

**[ServiceGridGateway]**

*Version=LAST*

In this configuration, zenon applications connect to the most recent version of the **IloT Services Gateway** that is installed on the computer.

## Example of configuration for version 11.0:

### [ServiceGridGateway]

*Version=11\_0*

In this example, zenon applications connect to **IloT Services Gateway 11**.

### SYNTAX

The syntax for manual configuration of the version is "**MM\_N**". The first two figures "**MM**" define the version number of the major release. The last figure "**N**" defines the minor release.

#### **Hint**

Configure the figure for the minor release:

The last figure must always be given, including for major releases, such as **IloT Services Gateway 11** for example. In this case, you must configure the value "*11\_0*".

## 6.2 Getting Started

In this node, you can find detailed information on putting IloT Services into operation in Windows and Docker environments.





**COPA-DATA**

© 2024 Ing. Punzenberger COPA-DATA GmbH

All rights reserved.

Distribution and/or reproduction of this document or parts thereof in any form are permitted solely with the written permission of the company COPA-DATA. Technical data is only used for product description and are not guaranteed properties in the legal sense. Subject to change, technical or otherwise.

## 6.2.1 Welcome to COPA-DATA help

### GENERAL HELP

If you cannot find any information you require in this help chapter or can think of anything that you would like added, please send an email to [documentation@copadata.com](mailto:documentation@copadata.com).

### LICENSES AND SERVICES

If you find that you need other zenon services or licenses, our staff will be happy to help you. Email [sales@copadata.com](mailto:sales@copadata.com).

### PROJECT SUPPORT

You can receive support for any real project you may have from our customer service team, which you can contact via email at [support@copadata.com](mailto:support@copadata.com).

## 6.2.2 Getting Started Guide (Windows)

In this node, you find out how you install IIoT Services on a Windows computer and initially configure it.



### Information

These instructions were written on an operating system in English.

### 6.2.2.1 System requirements

Note the following system requirements to install IIoT Services:

- ▶ General

You can find information on installation via Setup in the **Installation and update** section in the **Installation** (on page 39) chapter.

- ▶ Operating system

You can find information on supported operating systems in the **Installation and update** section in the **Windows operating systems (2/2)** node.

Update your Windows operating system to the latest version.

- ▶ Browser

The following browsers are supported:

- ▶ Google Chrome
- ▶ Mozilla Firefox
- ▶ Microsoft Edge
- ▶ Apple Safari

**Note:** Always use the most recent version of the respective browser.

- ▶ Storage space

For the installation of IIoT Services, at least 6 GB of free storage space is required on the storage medium.

You can find the required storage space for further zenon components in the **Installation and update** section in the **Engineering Studio** node.

- ▶ Requirements

Ensure that the following points have been met:

- ▶ Sufficient resources for the smooth operation of all installed applications (CPU, RAM, storage space).
- ▶ Working internet connection.
- ▶ There must be Windows administrator rights.

### 6.2.2.2 Further requirements

To check your Windows installation, the following requirements must be met:

- ▶ An installation of Service Engine and Engineering Studio.
- ▶ Make sure that the version of **IIoT Services Gateway** is installed that corresponds to the version of IIoT Services to be installed.
- ▶ Ensure that this installation is licensed accordingly.

 **Info**

This installation can be present on your own computer or on the same computer as the Windows installation.

### 6.2.2.3 Configure IIoT Services

In this node, you can find further information on the following topics:

1. Install zenon (on page 56)
2. Activate the licenses for IloT Services (on page 57)
3. Configure IloT Services (on page 58)
4. Configure HTTPS trust setting (on page 59)
5. Summary and next steps (on page 61)

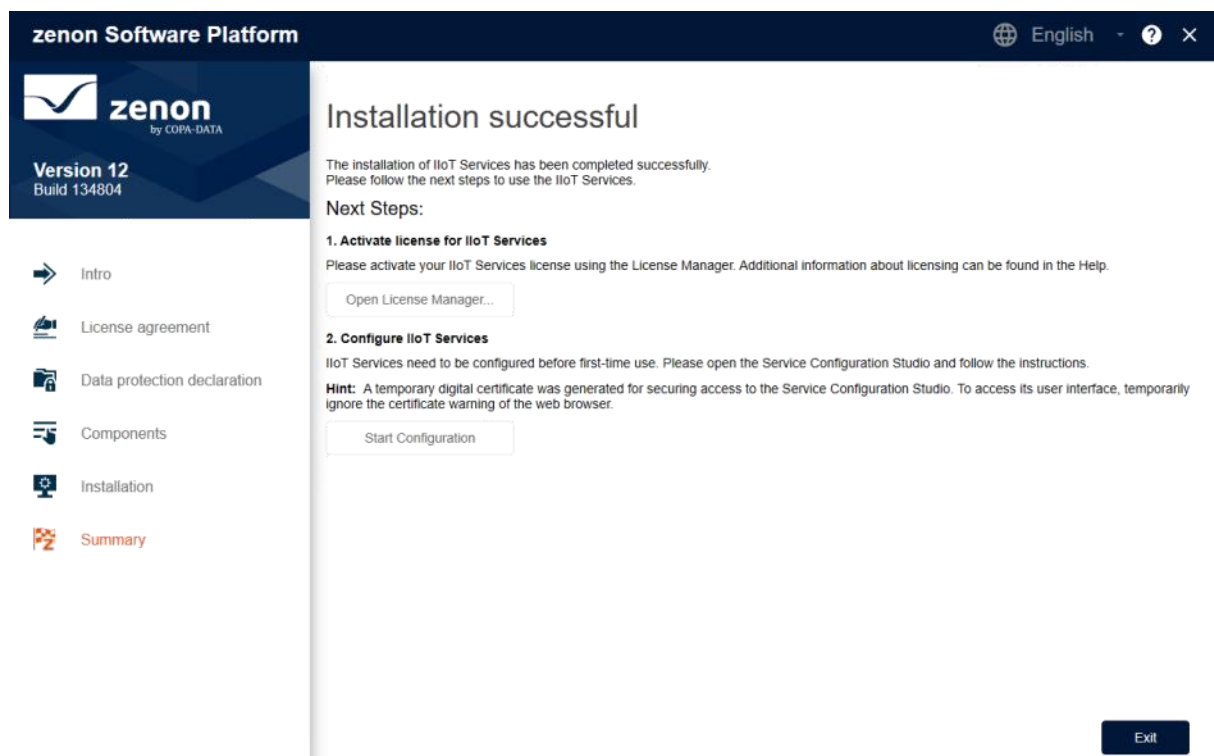
### 6.2.2.3.1 Install zenon

Carry out the following steps to install zenon:

1. Double-click on the ISO file.
2. Double-click, in the mounted drive, on the file named START.exe. Setup will start.
3. Carry out the further installation steps. You can find further information in the **zenon Softwareplattform Standardinstallation** node in the **Konfiguration und Installation** node.

**Note:** You must select, for the **Components** step, **IloT Services**. The **Lizenzmanagement** component is already preselected and cannot be deselected. All other components are optional.

4. Ensure, after the necessary restarting of the computer, that you can activate (mount) the ISO file again. Otherwise the installation will not be carried out correctly.



**Note:** Do not close the **Installation successful** window. You still need it to activate the licenses and to configure IIoT Services.

### ⚠ Attention

If you have nevertheless unintentionally closed the **Installation successful** window, you can continue configuration via the **Service Configuration Studio** home page and **zenon Lizenzmanagement**.

Name	Sample values	Description
<b>Service Configuration Studio</b>	<i>https://mycomputer.mydomain.com:9443</i> System-specific value*	You can continue the configuration of IIoT Services in <b>Service Configuration Studio</b> .

\* Replace mycomputer.mydomain.com in the URLs with your computer's FQDN (on page 73).

### 6.2.2.3.2 Activate license for IIoT Services

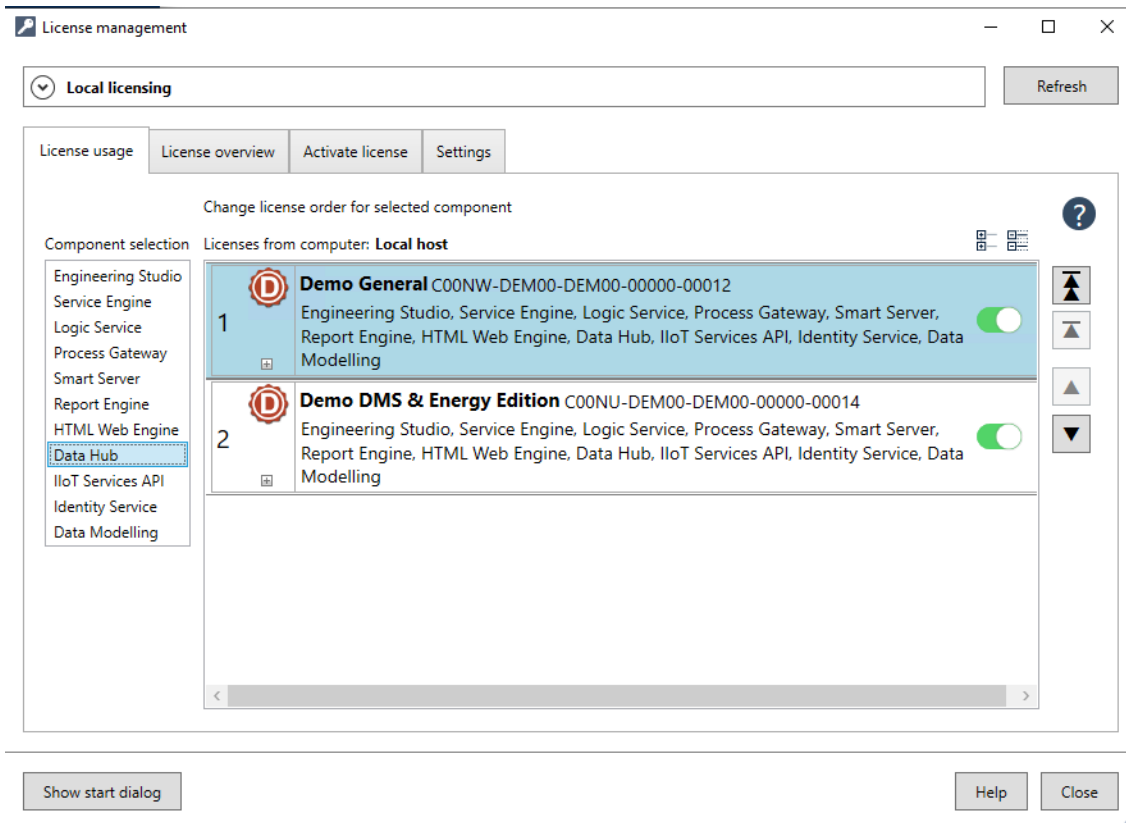
You have several options for licensing. Use either

- ▶ the supplied demo licenses or
- ▶ your own **zenon** licenses

To install the demo licenses:

1. Click, in the **Installation successful** window, in the **1. Activate license for IIoT Services** section, on the **Open License Manager** button.
2. In the **License management** window that is opened, click on **Advanced options**.
3. In the **License management** window that is opened, click on **Advanced license administration**.
4. Activate the necessary licenses for **Data Hub**, **IIoT Services API**, **Identity Service** and **Data Modeling**. To do this, move the slider to the right. The green background shows that the license has been activated.
5. Use the cursor buttons to move the activated licenses to the top.

6. Close the dialog by clicking on the **Close** button.



You can also use your own, pre-existing **zenon** licenses. You can find information about licensing in the Licensing node in the Licensing in a few steps node.

### **Attention**

All **zenon** components that you use in **IloT Services** must also be licensed.

You can find information in relation to this in the Licensing node in the Licensing components - overview node.

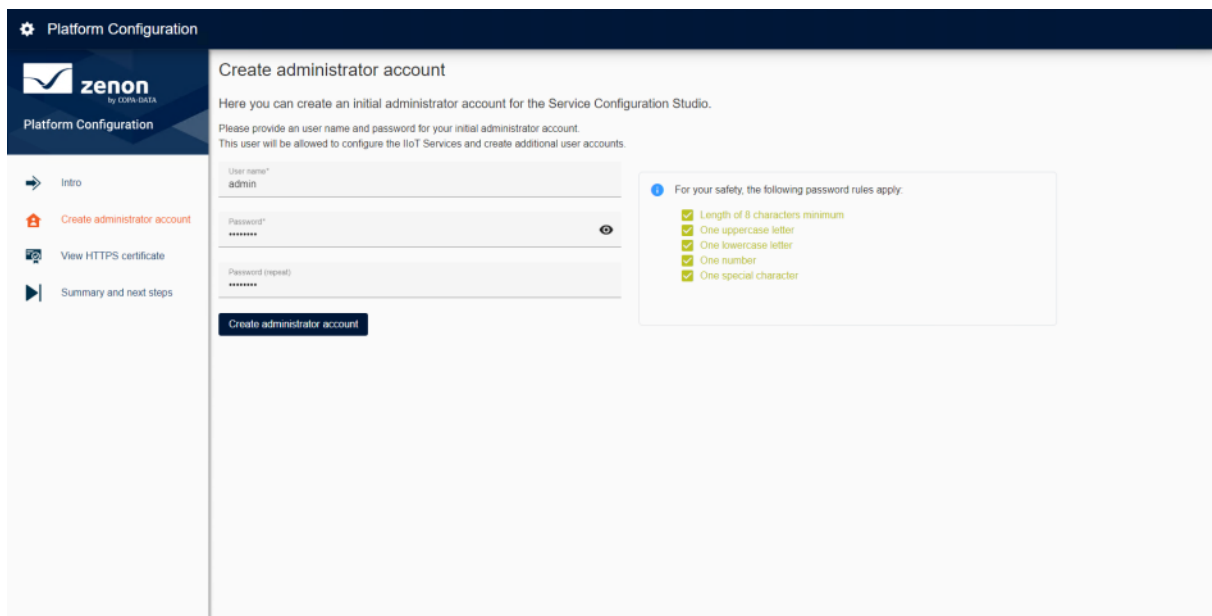
### 6.2.2.3.3 Configure IloT Services

You configure the administrator account with the following steps.

1. Click, in the **Installation successful** window, in the **2. Configure IloT Services** section, on the **Start Configuration** button.

**Note:** In **Service Configuration Studio**, you can continue the configuration of the platform at a later point in time by clicking on the **Platform Configuration** button. The configuration is continued from the point where it was stopped.

2. In the **Platform Configuration** window, click on the **Get started** button.
3. Enter a user name in the **Create administrator account** window.
4. Enter a password. Note the given password criteria. If the password criteria are adhered to, the font color changes to green.
5. Enter the password again. If the two entries of the password match, the **Create administrator account** button is activated.
6. Click on this button. The creation of the administrator account is thus completed.



**Platform Configuration**

**zenon**  
by COSMOS DATA

Platform Configuration

- Intro
- Create administrator account**
- View HTTPS certificate
- Summary and next steps

### Create administrator account

Here you can create an initial administrator account for the Service Configuration Studio.  
Please provide an user name and password for your initial administrator account.  
This user will be allowed to configure the IIoT Services and create additional user accounts.

User name\*  
admin

Password\*  
\*\*\*\*\*

Password (repeat)  
\*\*\*\*\*

**Create administrator account**

For your safety, the following password rules apply:

- Length of 8 characters minimum
- One uppercase letter
- One lowercase letter
- One number
- One special character

**Note:** This user is also authorized to configure IIoT Services and to create further users

### **Attention**

Note the password in a secure place. If the password is forgotten, there is no possibility to retrieve it.

#### 6.2.2.3.4 View HTTPS certificate

IIoT Services use an HTTPS certificate for secure communication. To trust the HTTPS certificate, the root certificate must be trusted.

To install the root certificate, proceed as follows:

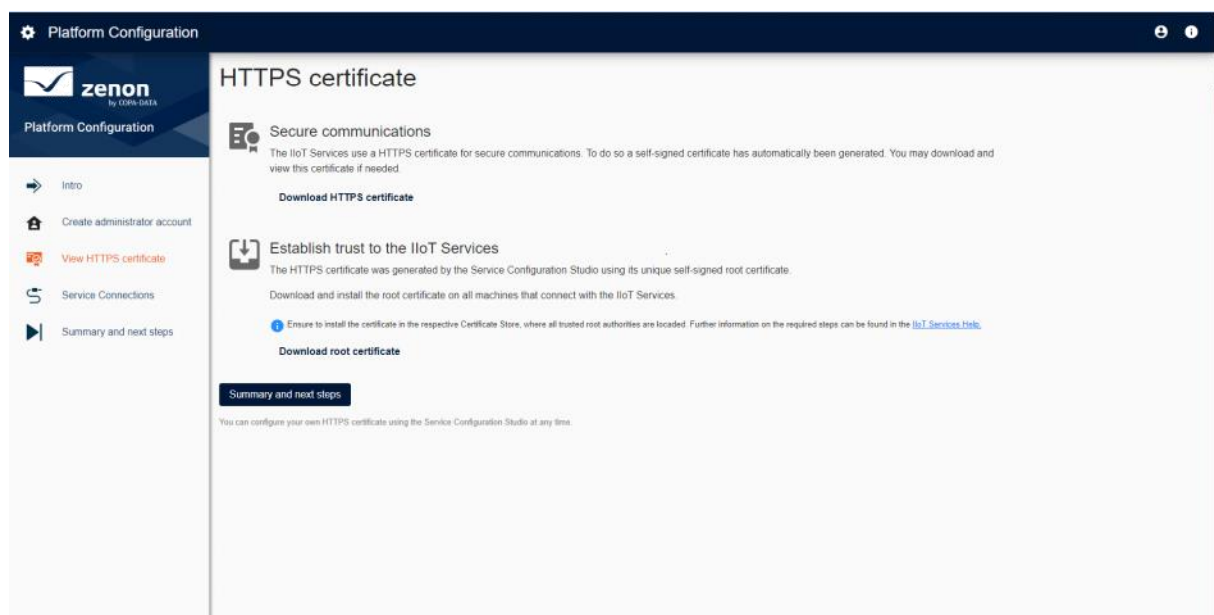
1. Click, in the **HTTPS certificate** window, on the **Download root certificate** button.

2. Open the downloaded certificate and install it in the **Trusted Root Certification Authorities Store**. You can find information on the procedure in the **HTTPS-Vertrauensstellung** (on page 258) node in the **Vertrauensstellung konfigurieren** (on page 261) node.
3. After successful installation of the root certificate, click on the **Summary and next steps** button.

### Attention

When installing IloT Services for the first time, your browser will issue a security warning. At this stage, you cannot verify the certificate yet. To complete the installation, you must ignore the security warnings this one time.

**Note:** Also install the root certificate on all clients that you want to connect to IloT Services.



### 6.2.2.3.5 Service Connections

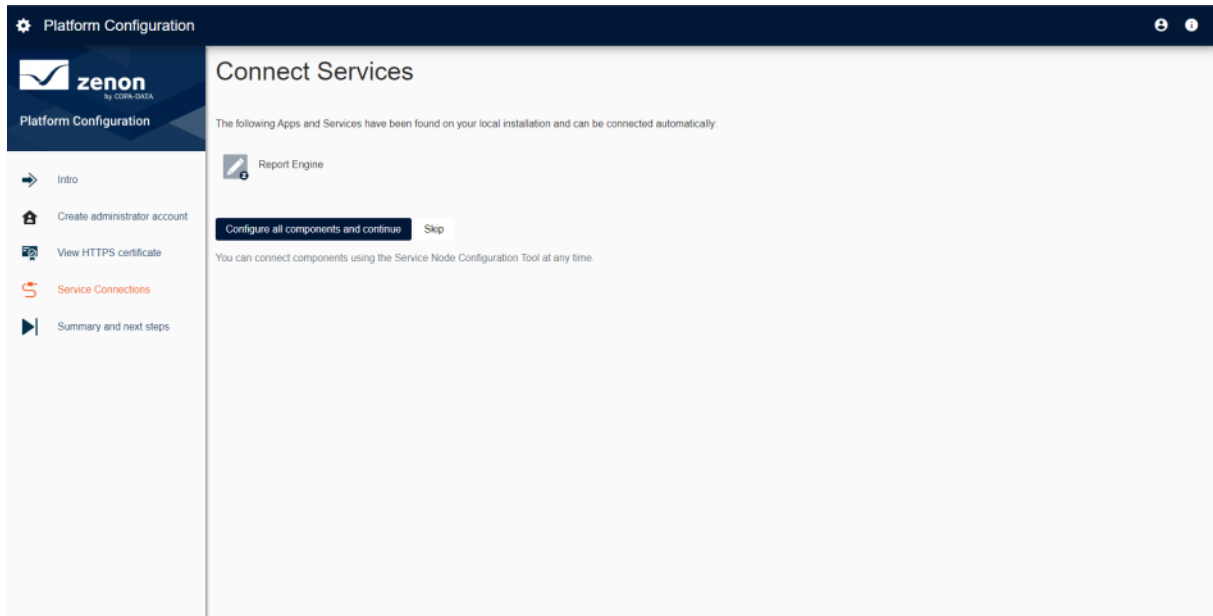
If you have installed additional **zenon** components, you can connect them to **IloT Services**. Components are, for example, **Engineering Studio**, **Service Engine** or **Report Engine**.

Click, in the **Connect Services** window, on the **Configure all components and continue** button.

### Information

In **Service Configuration Studio**, you have at all times the possibility to connect further **zenon** components to **IloT Services**.



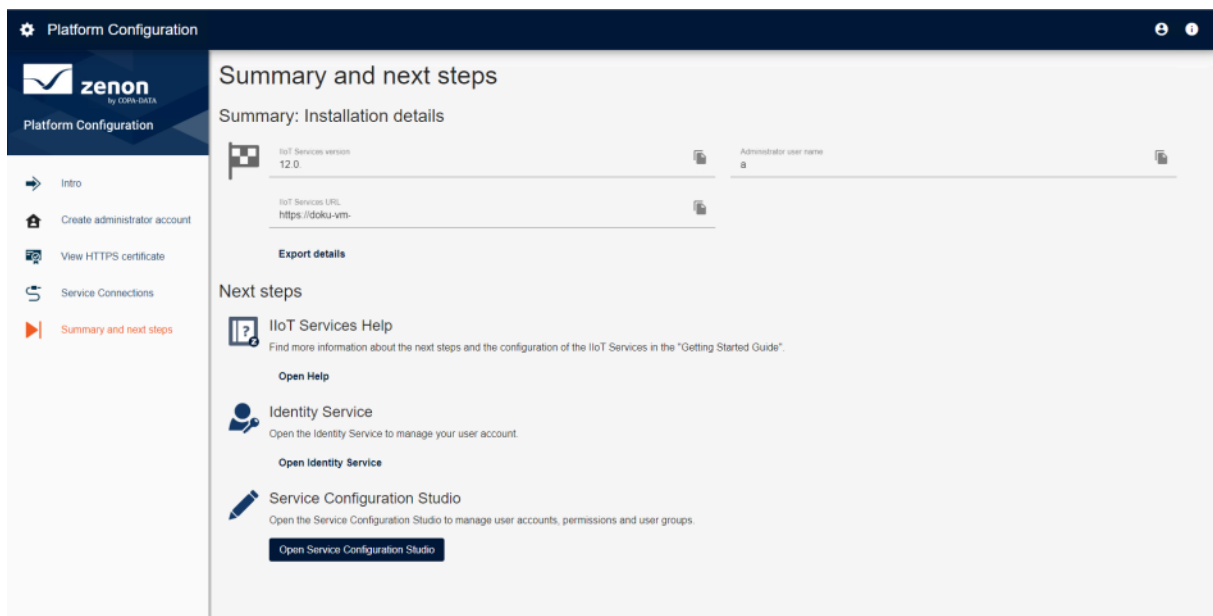


### 6.2.2.3.6 Summary and next steps

Here you can find a summary of the installation details as well as information about the next steps.

You have the following possibilities:

1. Start the online help.
2. Edit your user account with the **Identity Service** (on page 174).
3. You can administer users and authorizations In **Service Configuration Studio**, you can administer users, groups and permissions, among other things.



### Tip

Create the link for **Service Configuration Studio** as a bookmark in your browser.

Name	Sample values	Description
<b>Service Configuration Studio</b>	<p><i>https://mycomputer.mydomain.com:9443</i></p> <p>System-specific value*</p>	In the <b>Service Configuration Studio</b> , only users with administrator rights can fully administer the IIoT Services.

\* Replace mycomputer.mydomain.com in the URLs with your computer's FQDN (on page 73).

## 6.2.2.4 Configuration

In this node, you can find information on setting up the following components:

1. Engineering Studio
2. Service Engine
3. IIoT API

### 6.2.2.4.1 Engineering Studio

The connections must be configured beforehand in order for Engineering Studio and Service Engine to be able to communicate with IIoT Services.

### 6.2.2.4.2 Connection to IIoT Services

#### CREATE CONNECTION FOR A PROJECT

To do this, carry out the following steps:

1. Highlight the project in Engineering Studio.
2. Go to the **Network** node in the project properties
3. Go to property group **IIoT Services settings**.
4. Activate the **Activate IIoT Services** checkbox.  
This activates the configuration of the **Connection settings** property as well as the ... **button**.

5. Click on the **... button** . The **IloT Services Connection Wizard** is started.
6. Enter the URL of your IloT Services installation and follow the instructions in the wizard.  
Skip the step for Report Engine.
7. Once the **IloT Services Connection Wizard** has been successfully configured, you will find the used **IloT Service URL** and the **Client-ID** in the input field of the connection settings.

**Note:** You can find further information on the **IloT Services Connection Wizard** in the **IloT Services Connection Wizard** node in the **Welcome** section.

### 6.2.2.4.3 Configure variables

In order to use variables in IloT Services, they must be configured for it in Engineering Studio.

Only variables with **simple data type** are supported.

To configure variables:

1. Select the desired variable.
2. Open the **Authorization/eSignature** group in the properties.
3. Switch to the **IloT Services settings** subgroup.
4. Configure the variable for use in IloT Services.

Configurable properties:

#### **Access permission**

Access right of a variable in IloT Services. Select from drop-down list:

- ▶ *None*: Variable is not available in IloT Services.
- ▶ *Read*: IloT Services has read access to this variable.
- ▶ *Read and write*: IloT Services have read and write access to this variable.

**Note:** For reasons of security, access permission should only be set to the extent that they are actually required.

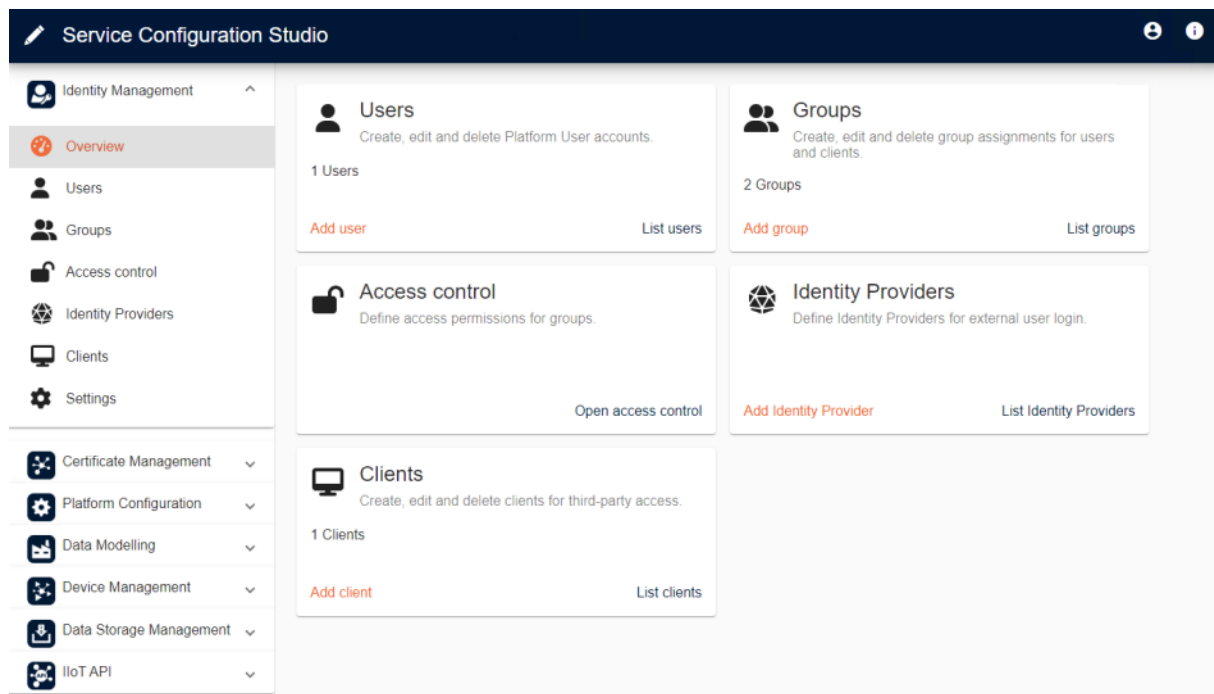
### 6.2.2.4.4 Starting Service Engine

Start **Service Engine** after configuration:

1. Save the project with all the changes.
2. Click on the **Geänderte Service Engine Dateien erzeugen** button.
3. Click on the **Service Engine starten** button.

### 6.2.2.4.5 Identity Management

In **Identity Management**, you administer users, groups, resources and privileges.



Assign the *Administrator* user the right to access Service Engine via IIoT Services.

To do this, follow the instructions in the following chapters.

### 6.2.2.4.6 Creating a group and adding users

To create a user group:

1. Navigate in **Service Configuration Studio** to the **Identity Management** menu item.
2. Click on the **Groups** submenu.
3. Click on the **Add Group** button.
4. Assign the group name *Users*.
5. Click on **Add**.

The *Users* user group has been created.

To add a user to the **Users** user group:

1. Select the **Users** group.
2. Click on the **Add user** button.
3. Select the *Administrator* user.

**Note:** The *Administrator* user is displayed in the list as *admin admin* (first name; last name).

4. Click on **Add**.

You have thus added the *Administrator* user of the *Users* user group.

#### 6.2.2.4.7 Add resource and add role

To add the Service Engine resource to the *Users* user group:

1. Ensure that Service Engine has been started.
2. Navigate in **Service Configuration Studio** to the **Identity Management** menu item.
3. Click on the **Access Control** submenu.
4. Select the *Users* user group under **Groups**.
5. Click on the **Add Resources** button.
6. Select your project in the overview.
7. Click on the **Add** button.

You have thus added the resource to the *Users* user group.

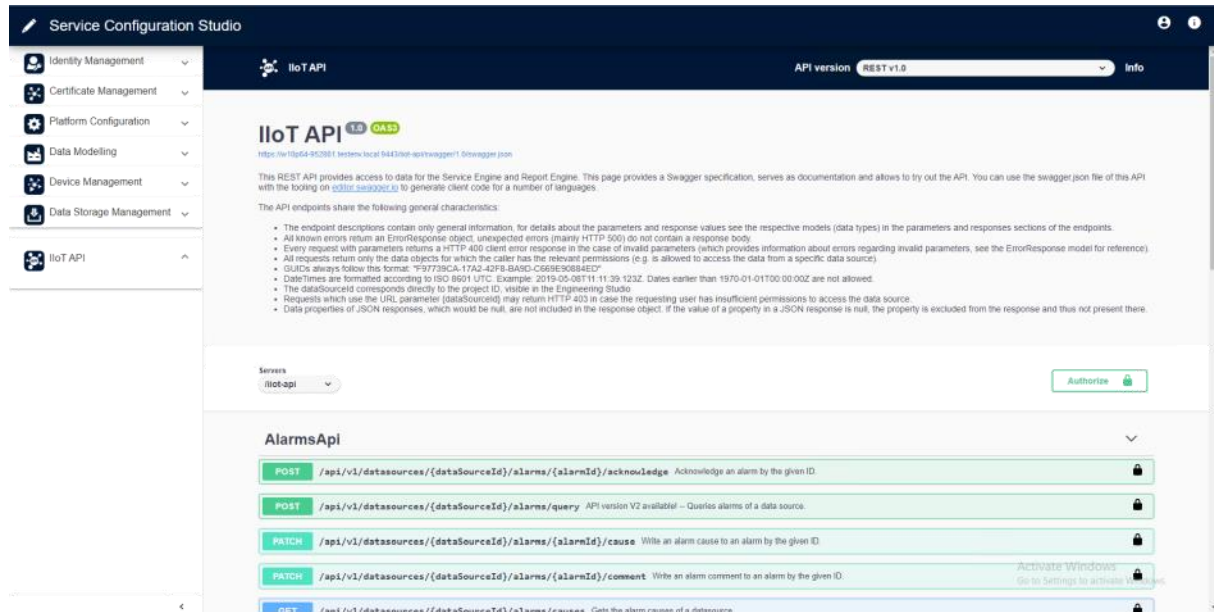
To assign the necessary role to the resource:

1. Click on the **...** button under **Assigned Resources**.
2. Select **Manage roles**.
3. Select the following permission: *Data Read*.
4. Click on the **Submit** button.

You have thus assigned the necessary role to the resource. The *Administrator* user can access the released variables in Service Engine via IIoT API.

### 6.2.2.4.8 IIoT API

In **Service Configuration Studio**, you access the IIoT API manually as a user. With the IIoT API, you can retrieve data from the IIoT Services.



There are two possibilities:

- ▶ For test purposes, you access the IIoT API manually in **Service Configuration Studio**.
- ▶ In a productive environment, a client application automatically accesses the IIoT API. To do this, you need an accordingly programmed 3rd party application.

### 6.2.2.4.9 User authorization

For a manual query using the IIoT API, you must authorize yourself. To authorize a user in the IIoT API:

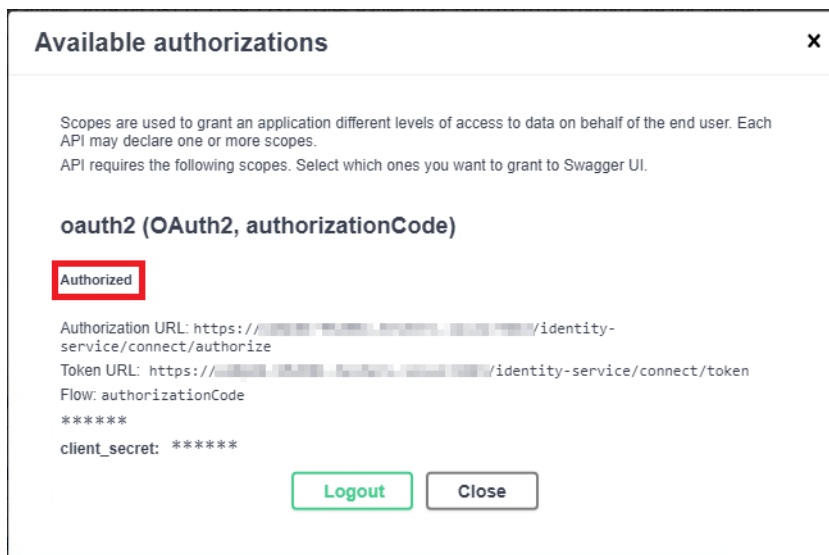
1. Ensure that Service Engine has been started.
2. Open the **Service Configuration Studio**.
3. Go to the **IIoT API** button.
4. Click on the green **Authorize** button. A window opens.  
**Note:** You are not authorized by default. The icon shows an opened lock.
5. Ensure that the value for the **client\_id** field is set to *swagger\_demo\_api*.
6. Activate the following checkboxes:

- ▶ **iiotServicesAPI**

- ▶ **dataStorageAPI**

**Note:** You thus determine the scope of the application.

7. Click on the **Authorize** button.
  8. After successful authorization, the system shows the message *Authorized*.
  9. Click on the **Close** button. Authorization remains active.
- Note:** If you are authorized, you will see the locked icon.



### Info

You can find the complete list of IIoT API error codes in the Troubleshooting (on page 353) node in the IIoT API error codes (on page 357) node.

## 6.2.2.4.10 Test 1: Query available project

With this test, you check to see which projects you can use in Service Engine.

### SELECT ENDPOINT

1. Ensure that Service Engine has been started.
2. Start **Service Configuration Studio**.
3. Go to the **IIoT API** button.
4. Ensure that the user authorization for the IIoT API (on page 66) has been carried out.

5. Check whether the value *REST v1.0* is set as **API version** in the header.
6. Go to the **DataSourcesApi** category.
7. Go within the category to the line with the */api/v1/datasources* endpoint.

You must configure this endpoint for the following query.

### AlarmsApi

- POST `/api/v1/datasources/{dataSourceId}/alarms/{alarmId}/acknowledge` Acknowledge an alarm by the given ID. 🔒
- POST `/api/v1/datasources/{dataSourceId}/alarms/query` Queries alarms of a data source. 🔒

### ArchivesApi

- GET `/api/v1/datasources/{dataSourceId}/archives/{archiveId}` Gets the metadata of the archive for the given archive id. 🔒
- POST `/api/v1/datasources/{dataSourceId}/archives/{archiveId}/query` Queries historic data from archives of a data source. 🔒
- GET `/api/v1/datasources/{dataSourceId}/archives` Gets all archive metadata of the data source. 🔒

### DataSourcesApi

- GET `/api/v1/datasources/{dataSourceId}` Returns the requested data source. 🔒
- GET `/api/v1/datasources` Returns all available data sources that are accessible for the authenticated user. 🔒

The returned data sources are sorted by their name in ascending order.

**Parameters** Try it out

No parameters

**Responses**

Code	Description	Links
200	Ok. Returns the requested data sources.	No links

## QUERY PROJECT

1. Click on the blue **GET** button in the line. This expands the endpoint.
2. Click on the **Try it out** button.
3. Click on the **Execute** button.



4. Copy the *dataSourceId* into a text file. You need this value for the following test.  
**Note:** It is identical to the project ID of your project.

## RESULT

The query shows the available project.

**Note:** Ensure that the project is in the **Online** state.

### 📌 Note for programmers

#### Code sample: Response body

```
{
  "dataSources": [
    {
      "name": "ZENON14_DEMO",
      "dataSourceId": "d3058681-c6a8-4b2e-908d-610676fce605",
      "state": "Online"
    }
  ]
}
```

### 6.2.2.4.11 Test 2: Query available variables and variable values

With this test, you will access the variables and variable values enabled in the zenon project via IIoT Services.

#### OPEN ENDPOINT

1. Ensure that Service Engine is running.
2. Ensure that the user authorization for the IIoT API (on page 66) has been carried out.
3. Start **Service Configuration Studio**.
4. Go to the **IIoT API** menu item.
5. Check whether the value *REST v1.0* is set as **API version** in the header.
6. Go to the **Variables API** category.
7. Go to the the line with the */api/v1/datasources/{dataSourceId}/variables/query* endpoint.

You must configure the query in this endpoint.

## CONFIGURE QUERY

1. Click on the green **Post** button.
2. Click on the **Try it out** button. You have thus activated the input field for the **dataSourceId**.
3. Enter the **dataSourceId** (identical to the zenon project ID).  
**Note:** You have thus defined the target project for the query. (Example: Initial query (on page 72))
4. Change the following points in the **Query specification**:
  - a) *fields*: Replace the predefined **"string"** with **"name", "value"**.  
You thus define the data fields for the query.
  - b) *nameFilter*: Replace the predefined **"string"** with **"\*"**.  
You use this placeholder to query all values unfiltered. (Example: custom query (on page 72))
5. Then click on **Execute** to perform the query.
6. The query is acknowledged as follows: **"Code 200" "Ok. Returns the queried variables."**
7. The **"Response body"** section shows the query result. (Example: query result (on page 73)).

The query result shows the released variables and their variable values from the specified zenon project.

### VariablesApi ▼

GET
/api/v1/datasources/{dataSourceId}/variables/{variableName} Gets the data of a single variable.
🔒

PATCH
/api/v1/datasources/{dataSourceId}/variables/{variableName} Sets the value of a single variable.
🔒

POST
/api/v1/datasources/{dataSourceId}/variables/query Queries the data of multiple variables.
🔒

Only variables with the Service Grid Access Permissions "Read-only" or "Read-write" are returned. The returned variables are sorted by their name in ascending order. It is possible to use this endpoint to get all variables of a data source by specifying only the "name" field and the "\*" (asterisk) wildcard for the variable name.

Parameters

Try it out

Name	Description
<b>dataSourceId</b> * required string(\$uuid) (path)	Id of respective data source  <div style="border: 1px solid #ccc; padding: 2px; width: fit-content; margin-top: 5px;">dataSourceId - Id of respective data source</div>

Request body required

application/json ▼

Query specification:

[Example Value](#) | [Schema](#)

```

{
  "fields": [
    "string"
  ],
  "nameFilter": {
    "variableNames": [
      "string"
    ]
  }
}
                    
```

### 6.2.2.4.12 Query specifications

You can find the query specifications in this section.

### 6.2.2.4.13 Initial query

#### Code Sample:

```
{
  "fields": [
    "string"
  ],
  "nameFilter": {
    "variableNames": [
      "string"
    ]
  }
}
```

Initial query

### 6.2.2.4.14 Custom query

#### Code Sample:

```
{
  "fields": [
    "name", "value"
  ],
  "nameFilter": {
    "variableNames": [
      "*"
    ]
  }
}
```

Query of variables and variable values

### 6.2.2.4.15 Query result

#### Code Sample:

```
{
"variables": [
{
"name": "MY_VARIABLE",
"value": "1"
}
]
}
```

The shared variable and the variable value are in the "Response body" section.

### 6.2.2.5 Appendix

In this node, you can find further information on the following topics:

1. Determine FQDN (on page 73)
2. Monitoring services (on page 73)
3. Test environment vs. productive environment (on page 74)

#### 6.2.2.5.1 Determine FQDN (Fully Qualified Domain Name)

To determine the **FQDN** of the Windows computer:

1. Open the command line using the **Windows + R** keyboard shortcut.
2. Enter **cmd.exe**.
3. Enter the **ping localhost** command.
4. The **Command Line Interface** shows your computer's FQDN, among other things.
5. Convert the FQDN to lower-case letters.

You have now determined the FQDN that you need for use in the IloT Services.

#### 6.2.2.5.2 Monitor services

All services in IloT Services are automatically started by the operating system. You can check the status of IloT Services services with the following steps:

1. Open the command line using the **Windows + R** shortcut.

2. Enter **services.msc**.
3. Confirm the entry with **Enter**. This then opens the console for the administration of services.
4. You can find the services at: **zenon** <servicename>
5. All **zenon** services must in principle be in *running* state.  
**Note: Data Storage** can also be in **exited** state (because it is not used).

### 6.2.2.5.3 Test environment vs. productive environment

The test environment described in this guide is quicker and easier to set up than a typical productive environment.

The fundamental differences are:

	Test environment	Productive environment
<b>Installation option</b>	<ul style="list-style-type: none"> <li>▶ IloT Services (Windows native)</li> </ul>	<ul style="list-style-type: none"> <li>▶ IloT Services (Windows native)</li> <li>▶ IloT Services (Docker on Linux)</li> </ul>
<b>Number of computers</b>	<ul style="list-style-type: none"> <li>▶ A computer for IloT Services and all clients</li> </ul>	<ul style="list-style-type: none"> <li>▶ A computer for IloT Services</li> <li>▶ Dedicated computers for clients</li> </ul>
<b>Network topology</b>	All applications run on the same computer.	<p>The applications run on different computers.</p> <p>The computers can be distributed over different remote locations.</p>
<b>Passwords</b>	It is possible to use predefined passwords in a protected test environment.	For all logins, it is essential that you assign your own secure passwords.



**COPA-DATA**

© 2024 Ing. Punzenberger COPA-DATA GmbH

All rights reserved.

Distribution and/or reproduction of this document or parts thereof in any form are permitted solely with the written permission of the company COPA-DATA. Technical data is only used for product description and are not guaranteed properties in the legal sense. Subject to change, technical or otherwise.

## 6.2.3 Welcome to COPA-DATA help

### GENERAL HELP

If you cannot find any information you require in this help chapter or can think of anything that you would like added, please send an email to [documentation@copadata.com](mailto:documentation@copadata.com).

### LICENSES AND SERVICES

If you find that you need other zenon services or licenses, our staff will be happy to help you. Email [sales@copadata.com](mailto:sales@copadata.com).

### PROJECT SUPPORT

You can receive support for any real project you may have from our customer service team, which you can contact via email at [support@copadata.com](mailto:support@copadata.com).

## 6.2.4 Getting Started Guide (Docker)

This guide describes how you install and initially configure the IIoT Services on the Docker containerization software. It explains the installation of IIoT Services on Docker for Windows. It can also be used for Docker for Linux and other container solutions such as Podman or Kubernetes.

The container images supplied by COPA-DATA are based on Linux and can be run on Docker for Windows as well as on Docker for Linux and other container platforms.

The target group is users who have little or no experience with Docker.

#### Info

These instructions were written on an operating system in English.

### 6.2.4.1 System requirements

Note the following system requirements to install IIoT Services:

- ▶ General

Docker, Engineering Studio and Service Engine are installed on one computer.



- ▶ Browser

The following browsers are supported:

- ▶ Google Chrome
- ▶ Mozilla Firefox
- ▶ Microsoft Edge
- ▶ Apple Safari

**Note:** Always use the most recent version of the respective browser.

- ▶ Storage space

For the installation of IIoT Services, at least 6 GB of free storage space is required on the storage medium.

You can find the required storage space for further zenon components in the **Installation and update** section in the **Engineering Studio** node.

- ▶ Requirements

Ensure that the following points have been met:

- ▶ Sufficient resources for the smooth operation of all installed applications (CPU, RAM, storage space).
- ▶ The CPU must support hardware virtualization.
- ▶ CPU hardware virtualization must be activated in the BIOS.
- ▶ Working internet connection.
- ▶ Ensure that you have Windows administrator rights on the computer.

## 6.2.4.2 Further requirements

To check your Docker installation, the following requirements must be met:

- ▶ An installation of Service Engine and Engineering Studio.
- ▶ Ensure that the version of IIoT Services Gateway is installed that corresponds to the version of IIoT Services to be installed.
- ▶ Ensure that this installation is licensed accordingly.

### Information

In this guide, the entire installation is carried out on one computer.

### ⚠ Attention

If you run IIoT Services on a virtual machine with Docker containers:

First check whether AVX commands are supported by the underlying hypervisor.

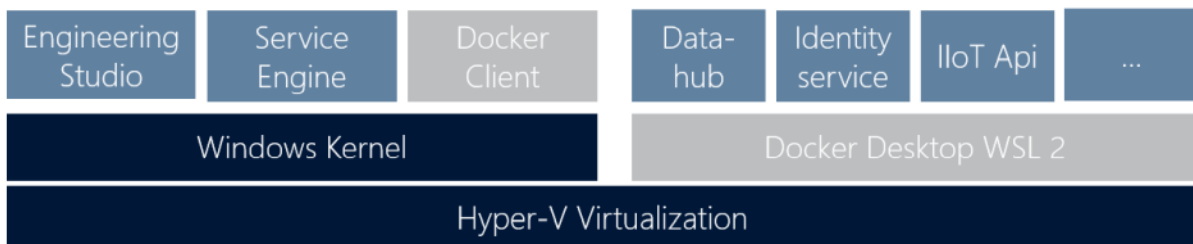
## 6.2.4.3 System architecture

In this guide, the entire installation is carried out on one computer. This includes Service Engine and Engineering Studio as a native Windows installation and at the same time IIoT Services as a Docker installation.

**Note:** You can obtain the container images from Docker Hub (<https://hub.docker.com/u/copadata>).

### SHORT DESCRIPTION OF DOCKER

Docker is a technology for the container-based execution of software applications. The applications run in containers independently of the host operating system. The container images supplied by COPA-DATA are based on the Linux operating system. Thanks to the Windows Subsystem for Linux 2 (WSL 2), such Linux containers can also be executed on a Windows host operating system.



The Hyper-V hardware visualization layer from Microsoft hosts the Windows operating system and the Windows Subsystem for Linux 2 (WSL 2).

### 6.2.4.3.1 Installation of Docker for Windows

Before you can install the **IIoT Services** for Docker on a Windows host system, you must first install Docker for Windows and the Windows Subsystem for Linux (WSL) 2 from Microsoft. Proceed in the following way:

1. Ensure that hardware virtualization (on page 98) is activated for the CPU.
2. Configure an *elevated PowerShell* (on page 99). The *elevated PowerShell* is a PowerShell with administrator rights. You can use it to subsequently initialize and administer **IIoT Services**.

3. Download the current version of **Docker for Windows** from the Docker manufacturer's web site (docker.com) (<https://www.docker.com/>).
4. Install **Docker for Windows** with the **WSL2 engine**.
5. Follow the link shown to <https://aka.ms/wsl2kernel>.
6. Download the *WSL2 Linux kernel update package for x64 machines*.
7. Install the update package
8. Start **Docker for Windows**.
9. Check whether Docker has been configured for the use of Linux containers. This is the default setting of Docker.

### 6.2.4.3.2 Installation of Docker for Linux

In this section, you can find brief instructions for installing **Docker für Ubuntu**.

1. Install Docker.
2. To do this, follow the detailed installation instructions on the provider's website (<https://docs.docker.com/engine/install/ubuntu/>).
  - ▶ Information about other distributions is also available on this website.
  - ▶ Keep in mind the requirements for installation.
- ▶ Configure your computer. To do this, follow the further instructions in this **Getting Started Guide**.

### 6.2.4.4 Basic configuration of ENV file

In order to install IIoT Services, you must adapt the ENV file supplied by COPA-DATA. You will find this file in a package that you can download from the COPA-DATA website.

Carry out the following steps to configure the *ENV* file:

You can download the configuration files for IIoT Services from the COPA-DATA (<https://www.copadata.com/en/downloads/product-downloads/>) website.

The download contains:

- ▶ IIoT Services configuration files: *.env* and *docker-compose.yml*
- ▶ One PDF file: **IIoT Services** (on page 9)

To download the configuration files:

- ▶ Go to the COPA-DATA (<https://www.copadata.com/en/downloads/product-downloads/>) website.

- ▶ You must log in to the COPA-DATA website with your user account for this download. Registration is free.
  - ▶ Then filter for IIoT Services in **Select Category**
  - ▶ Download the ZIP file with the appropriate version of **IIoT Services** (Docker).
1. Create a working directory. This is used to store the Docker configuration files.
 

**Note:** Under Windows, you can use `C:\iiot-services` as the working directory.

**Note:** Under Linux, you can use `/home/<user>/iiot-services` as the working directory.
  2. Unzip the ZIP file into your working directory. There you will find the `ENV` file.
  3. Open the `ENV` file with a text editor.
  4. Enter the values for the corresponding configuration entries in the `ENV`.
  5. Save the changes.
  6. Check whether the `.env` file still contains the leading period (".").
 

**Note:** Some file operations in the Windows operating system can remove the dot. In this case, rename the file from `"env"` to `".env"`.

## CONFIGURE ENV FILE

The following entries are necessary for the configuration of the `ENV` file.

Entry	Sample values	Description
<b>Datenbank</b>		
<b>Persistence_Username=</b>	<code>iiot_user</code>	You can choose the usernames yourself.
<b>Persistence_Password=</b>	<code>iiot_Changeme123!</code>	You can define the password yourself.  <b>Note:</b> Note the minimum password requirements (on page 16)!
<b>Persistence_Uri=</b>		Optional entry; is not needed
<b>Machine settings</b>		
<b>MACHINE_HOSTNAME=</b>	<code>mycomputer.mydomain.com</code>  System-specific value: <ul style="list-style-type: none"> <li>▶ Determine the FQDN host name of your</li> </ul>	Frequent configuration errors on MACHINE_HOSTNAME are: <ul style="list-style-type: none"> <li>▶ Use of capital letters</li> </ul>

Entry	Sample values	Description
	Windows computer. (To do this, use the command line command <b>ping localhost</b> ) <ul style="list-style-type: none"> <li>▶ FQDN must be entered in continuous lowercase letters.</li> </ul>	

### 6.2.4.5 Commissioning

Once you have entered the configuration values into the *ENV* file, you can initialize IloT Services.

To do this, carry out the following steps:

1. Download Docker images (on page 81)
2. Initialize IloT Services (on page 81)
3. Start and monitor services

#### 6.2.4.5.1 Download Docker images

Carry out the following steps to download the Docker images:

1. Start Docker.
2. Ensure that the *ENV* file (on page 79) has been fully configured.
3. Open the *elevated PowerShell*. (Windows) or a terminal (Linux).
4. Change to your working directory where you have saved the Docker configuration files.
5. Download the containers with the command.  
*docker compose pull*

This downloads the images from *hub.docker.com* (<https://hub.docker.com/u/copadata>).

#### 6.2.4.5.2 Initialize IloT Services

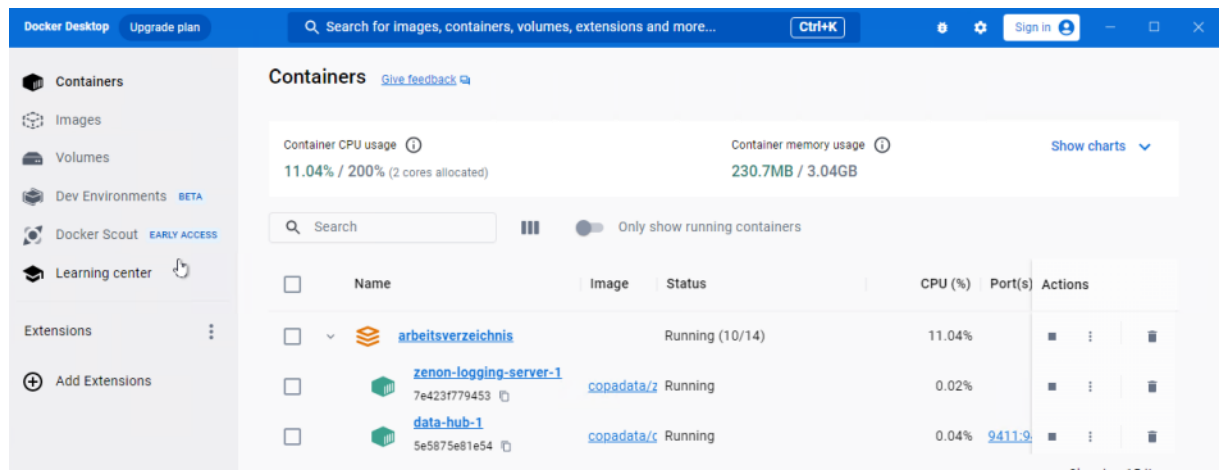
Then carry out the following steps to install IloT Services:

1. Start the containers with the command  
*docker compose up -d*

- Windows only: If necessary, confirm the Windows firewall enable for IIoT Services.  
**Note:** The firewall blocks the services until they are approved. This can lead to timeouts. The initialization will fail as a result. In this case, you must restart the initialization.
- Check if all containers are in the *Running* state.

`docker ps -a`

**Note:** Under Windows, you can also check the state of the container in the **Docker Dashboard**.



## 6.2.4.6 Configure IIoT Services

In this section, you will find information on the following topics:

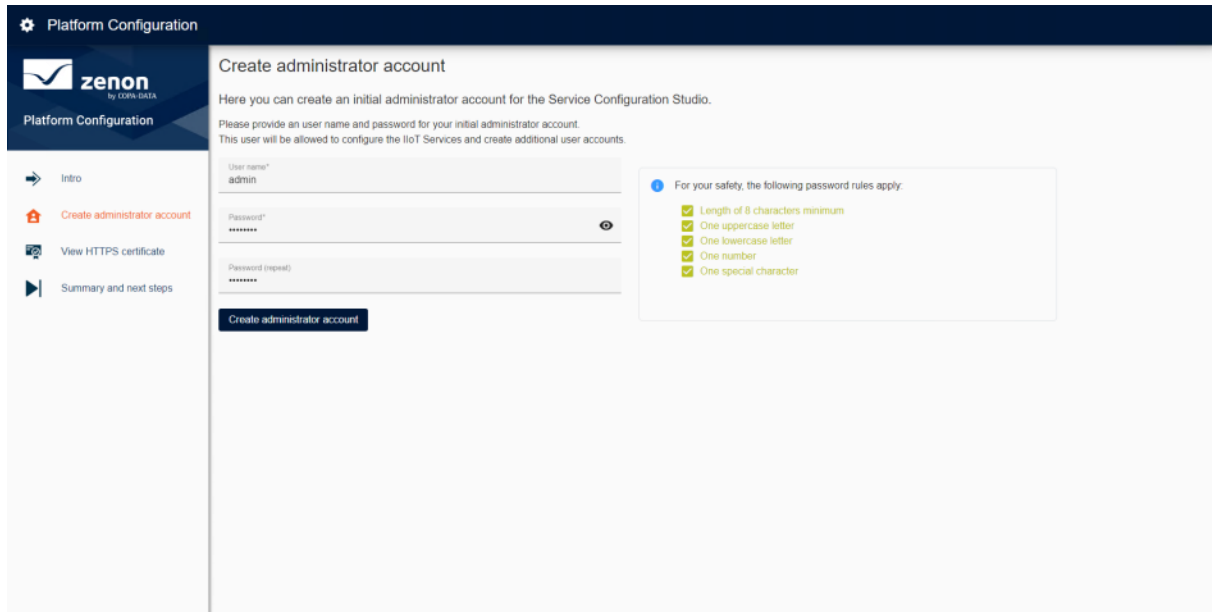
- Create administrator account (on page 82)
- Configure HTTPS trust setting (on page 83)
- Summary and next steps (on page 84)

### 6.2.4.6.1 Create administrator account

After the first installation of the IIoT Services, use the following steps to configure the administrator account.

- Open the following address in the browser `https://mycomputer.mydomain.com:9443` and follow the steps set out.
- In the **Platform Configuration** window, click on the **Get started** button.
- Enter a user name in the **Create administrator account** window.
- Enter a password. Note the given password criteria. If the password criteria are adhered to, the font color changes to green.

5. Enter the password again. If the two entries of the password match, the **Create administrator account** button is activated.
6. Click on this button. The creation of the administrator account is thus completed.



**Note:** This user is also authorized to configure IIoT Services and to create further users

### Attention

Note the password in a secure place. If the password is forgotten, there is no possibility to retrieve it.

#### 6.2.4.6.2 HTTPS certificate - Creating a trust relationship

IIoT Services use an HTTPS certificate for secure communication. To trust the HTTPS certificate, the root certificate must be trusted.

To install the root certificate, proceed as follows:

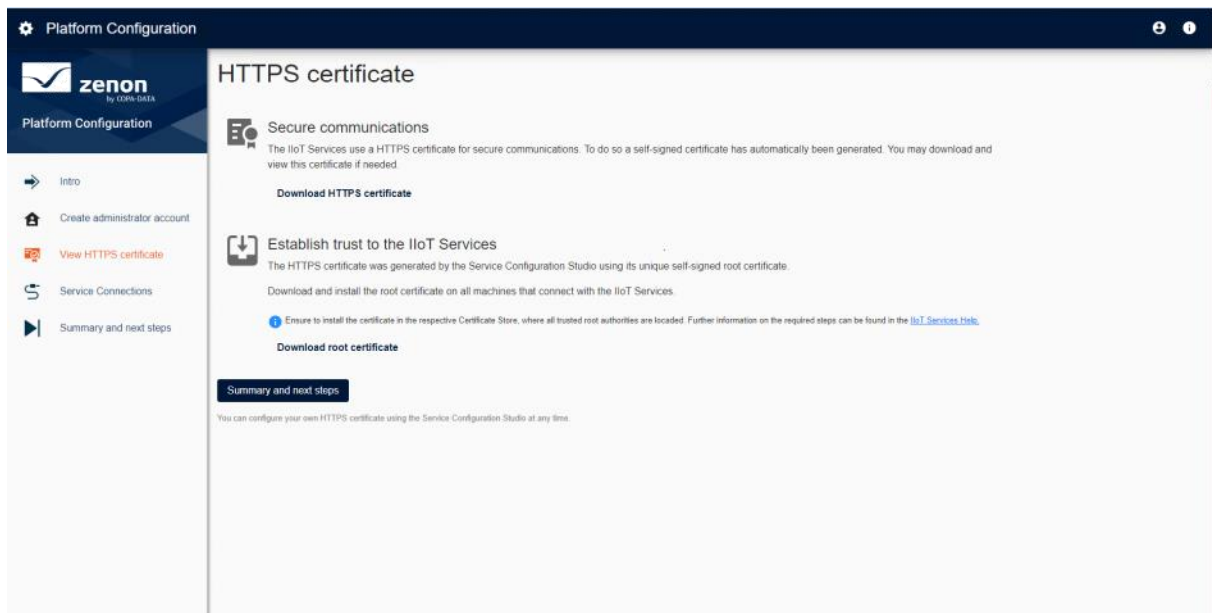
1. Click, in the **HTTPS certificate** window, on the **Download root certificate** button.
2. Open the downloaded certificate and install it in the **Trusted Root Certification Authorities Store** of Windows. To do this, open the Microsoft app `Certlm.msc`. Navigate to the node **Trusted Root Certification Authorities Store -> Certificates**. In the context menu of the **Certificates** node, you will find the menu item: **All tasks > Import**. A wizard opens with which you can import the certificate.  
You can find further information on this in the **Trust** (on page 258) section and in the **Configure trust** (on page 261) chapter.

3. After successful installation of the root certificate, click on the **Summary and next steps** button.

### Attention

When installing IloT Services for the first time, your browser will issue a security warning. At this stage, you cannot verify the certificate yet. To complete the installation, you must ignore the security warning this one time.

**Note:** Also install the root certificate on all clients that you want to connect to IloT Services.



### 6.2.4.6.3 Summary and next steps

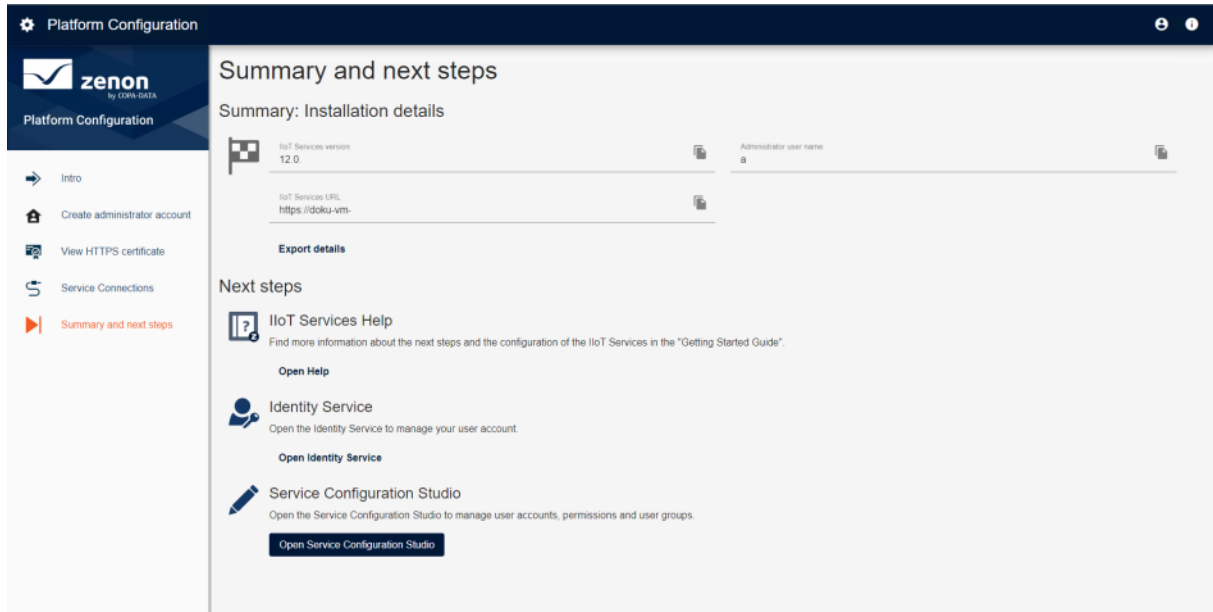
Here you can find a summary of the installation details as well as information about the next steps.

You have the following possibilities:

1. Start the online help.
2. Edit your user account with the **Identity Service** (on page 174).



3. You can administer users and authorizations In **Service Configuration Studio**, you can administer users, groups and permissions, among other things.



**Tip**

Create the link for **Service Configuration Studio** as a bookmark in your browser.

Name	Sample values	Description
<b>Service Configuration Studio</b>	<i>https://mycomputer.mydomain.com:9443</i> System-specific value*	In the <b>Service Configuration Studio</b> , only users with administrator rights can fully administer the IIoT Services.

\* Replace mycomputer.mydomain.com in the URLs with your computer's FQDN (on page 73).

### 6.2.4.7 Configuration

In this section, you will find information for setting up the following components:

1. Engineering Studio
2. Service Engine
3. IIoT API

### 6.2.4.7.1 Engineering Studio

The connections must be configured beforehand in order for Engineering Studio and Service Engine to be able to communicate with IIoT Services.

### 6.2.4.7.2 Connection to IIoT Services

#### CREATE CONNECTION FOR A PROJECT

To do this, carry out the following steps:

1. Highlight the project in Engineering Studio.
2. Go to the **Network** node in the project properties
3. Go to property group **IIoT Services settings**.
4. Activate the **Activate IIoT Services** checkbox.  
This activates the configuration of the **Connection settings** property as well as the ... **button**.
5. Click on the ... **button** . The **IIoT Services Connection Wizard** is started.
6. Enter the URL of your IIoT Services installation and follow the instructions in the wizard.  
Skip the step for Report Engine.
7. Once the **IIoT Services Connection Wizard** has been successfully configured, you will find the used **IIoT Service URL** and the **Client-ID** in the input field of the connection settings.

**Note:** You can find further information on the **IIoT Services Connection Wizard** in the **IIoT Services Connection Wizard** node in the **Welcome** section.

### 6.2.4.7.3 Configure variables

In order to use variables in IIoT Services, they must be configured for it in Engineering Studio.

Only variables with **simple data type** are supported.

To configure variables:

1. Select the desired variable.
2. Open the **Authorization/eSignature** group in the properties.
3. Switch to the **IIoT Services settings** subgroup.
4. Configure the variable for use in IIoT Services.

Configurable properties:

**Access permission**

Access right of a variable in IloT Services. Select from drop-down list:

- ▶ *None*: Variable is not available in IloT Services.
- ▶ *Read*: IloT Services has read access to this variable.
- ▶ *Read and write*: IloT Services have read and write access to this variable.

**Note:** For reasons of security, access permission should only be set to the extent that they are actually required.

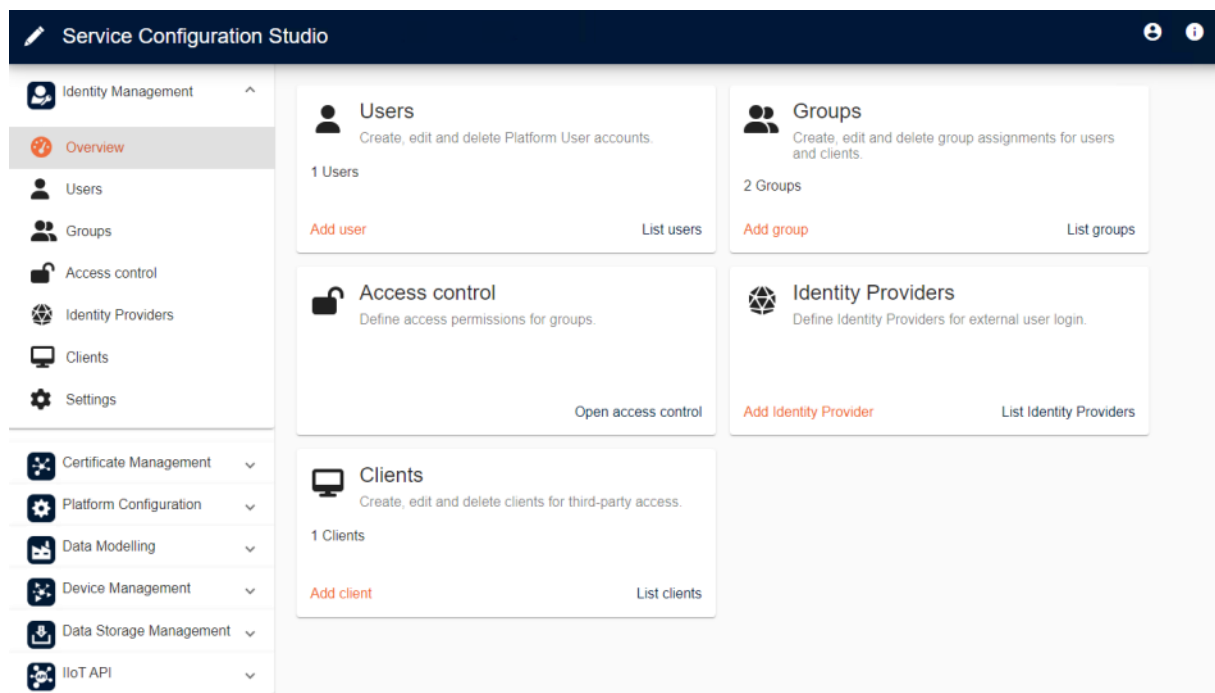
### 6.2.4.7.4 Starting Service Engine

Start **Service Engine** after configuration:

1. Save the project with all the changes.
2. Click on the **Geänderte Service Engine Dateien erzeugen** button.
3. Click on the **Service Engine starten** button.

### 6.2.4.7.5 Identity Management

In **Identity Management**, you administer users, groups, resources and privileges.



Assign the *Administrator* user the right to access Service Engine via IIoT Services.

To do this, follow the instructions in the following chapters.

### 6.2.4.7.6 Creating a group and adding users

To create a user group:

1. Navigate in **Service Configuration Studio** to the **Identity Management** menu item.
2. Click on the **Groups** submenu.
3. Click on the **Add Group** button.
4. Assign the group name *Users*.
5. Click on **Add**.

The *Users* user group has been created.

To add a user to the **Users** user group:

1. Select the **Users** group.
2. Click on the **Add user** button.
3. Select the *Administrator* user.

**Note:** The *Administrator* user is displayed in the list as *admin admin* (first name; last name).

4. Click on **Add**.

You have thus added the *Administrator* user of the *Users* user group.

### 6.2.4.7.7 Add resource and add role

To add the Service Engine resource to the *Users* user group:

1. Ensure that Service Engine has been started.
2. Navigate in **Service Configuration Studio** to the **Identity Management** menu item.
3. Click on the **Access Control** submenu.
4. Select the *Users* user group under **Groups**.
5. Click on the **Add Resources** button.
6. Select your project in the overview.
7. Click on the **Add** button.

You have thus added the resource to the *Users* user group.

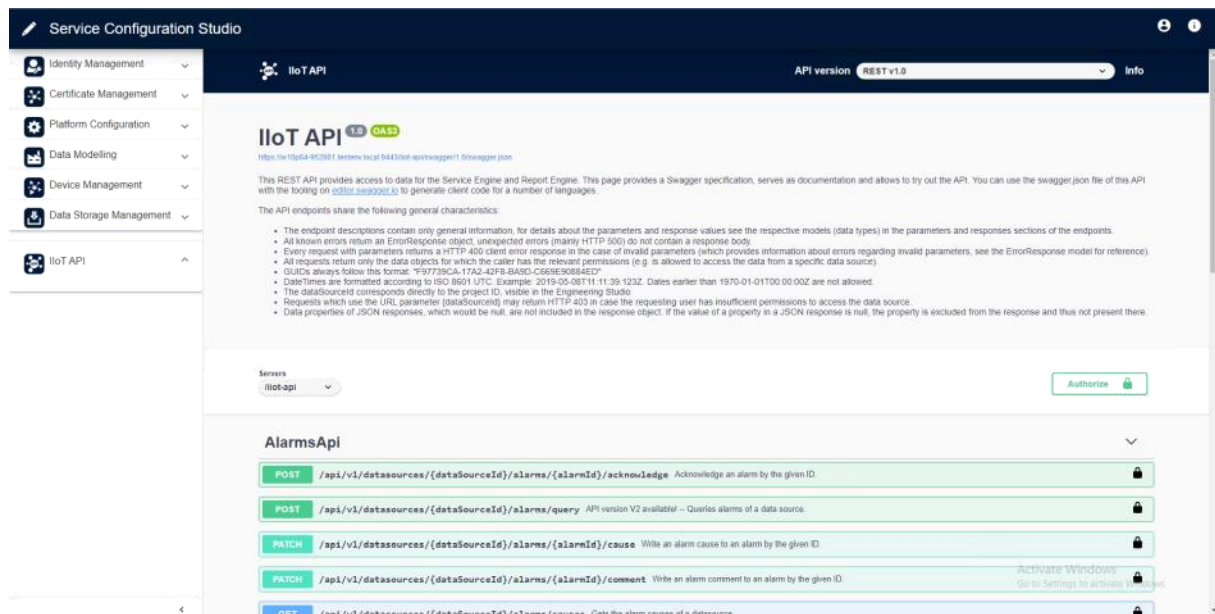
To assign the necessary role to the resource:

1. Click on the **...** **button** under **Assigned Resources** .
2. Select **Manage roles**.
3. Select the following permission: *Data Read*.
4. Click on the **Submit** button.

You have thus assigned the necessary role to the resource. Tthe *Administrator* user can access the released variables in Service Engine via IIoT API.

### 6.2.4.7.8 IIoT API

In **Service Configuration Studio**, you access the IIoT API manually as a user. With the IIoT API, you can retrieve data from the IIoT Services.



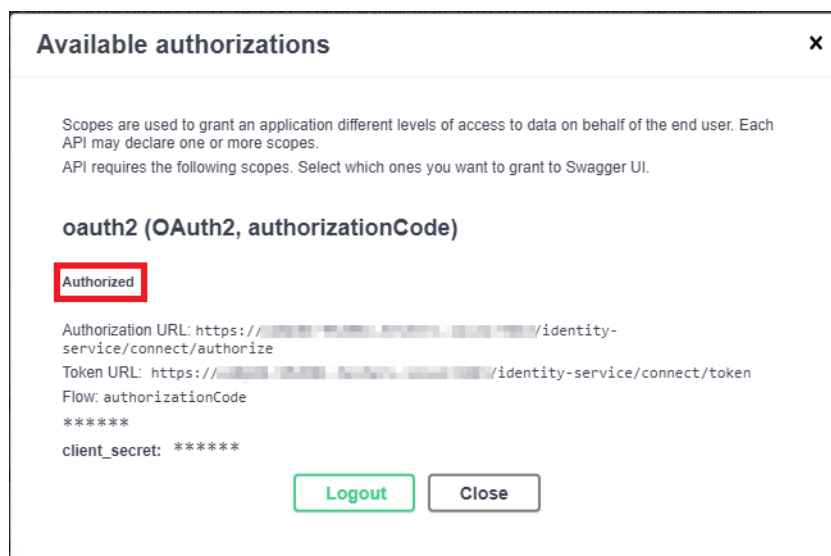
There are two possibilities:

- ▶ For test purposes, you access the IIoT API manually in **Service Configuration Studio**.
- ▶ In a productive environment, a client application automatically accesses the IIoT API. To do this, you need an accordingly programmed 3rd party application.

### 6.2.4.7.9 User authorization

For a manual query using the IIoT API, you must authorize yourself. To authorize a user in the IIoT API:

1. Ensure that Service Engine has been started.
2. Open the **Service Configuration Studio**.
3. Go to the **IIoT API** button.
4. Click on the green **Authorize** button. A window opens.  
**Note:** You are not authorized by default. The icon shows an opened lock.
5. Ensure that the value for the **client\_id** field is set to *swagger\_demo\_api*.
6. Activate the following checkboxes:
  - ▶ **iiotServicesAPI**
  - ▶ **dataStorageAPI****Note:** You thus determine the scope of the application.
7. Click on the **Authorize** button.
8. After successful authorization, the system shows the message *Authorized*.
9. Click on the **Close** button. Authorization remains active.  
**Note:** If you are authorized, you will see the locked icon.



#### Info

You can find the complete list of IIoT API error codes in the Troubleshooting (on page 353) node in the IIoT API error codes (on page 357) node.

### 6.2.4.7.10 Test 1: Query available project

With this test, you check to see which projects you can use in Service Engine.

#### SELECT ENDPOINT

1. Ensure that Service Engine has been started.
2. Start **Service Configuration Studio**.
3. Go to the **IloT API** button.
4. Ensure that the user authorization for the IloT API (on page 66) has been carried out.
5. Check whether the value *REST v1.0* is set as **API version** in the header.
6. Go to the **DataSourcesApi** category.
7. Go within the category to the line with the */api/v1/datasources* endpoint.

You must configure this endpoint for the following query.

### AlarmsApi ▼

POST /api/v1/datasources/{dataSourceId}/alarms/{alarmId}/acknowledge Acknowledge an alarm by the given ID. 🔒

POST /api/v1/datasources/{dataSourceId}/alarms/query Queries alarms of a data source. 🔒

### ArchivesApi ▼

GET /api/v1/datasources/{dataSourceId}/archives/{archiveId} Gets the metadata of the archive for the given archive id. 🔒

POST /api/v1/datasources/{dataSourceId}/archives/{archiveId}/query Queries historic data from archives of a data source. 🔒

GET /api/v1/datasources/{dataSourceId}/archives Gets all archive metadata of the data source. 🔒

### DataSourcesApi ▼

GET /api/v1/datasources/{dataSourceId} Returns the requested data source. 🔒

GET /api/v1/datasources Returns all available data sources that are accessible for the authenticated user. 🔒

The returned data sources are sorted by their name in ascending order.

**Parameters** Try it out

No parameters

**Responses**

Code	Description	Links
200	Ok. Returns the requested data sources.	No links

## QUERY PROJECT

1. Click on the blue **GET** button in the line. This expands the endpoint.
2. Click on the **Try it out** button.
3. Click on the **Execute** button.
4. Copy the *dataSourceId* into a text file. You need this value for the following test.  
**Note:** It is identical to the project ID of your project.



## RESULT

The query shows the available project.

**Note:** Ensure that the project is in the **Online** state.

### ■ Note for programmers

#### Code sample: Response body

```
{
  "dataSources": [
    {
      "name": "ZENON14_DEMO",
      "dataSourceId": "d3058681-c6a8-4b2e-908d-610676f6ce605",
      "state": "Online"
    }
  ]
}
```

### 6.2.4.7.11 Test 2: Query available variables and variable values

With this test, you will access the variables and variable values enabled in the zenon project via IIoT Services.

#### OPEN ENDPOINT

1. Ensure that Service Engine is running.
2. Ensure that the user authorization for the IIoT API (on page 66) has been carried out.
3. Start **Service Configuration Studio**.
4. Go to the **IIoT API** menu item.
5. Check whether the value *REST v1.0* is set as **API version** in the header.
6. Go to the **Variables API** category.
7. Go to the the line with the `/api/v1/datasources/{dataSourceId}/variables/query` endpoint.

You must configure the query in this endpoint.

#### CONFIGURE QUERY

1. Click on the green **Post** button.

2. Click on the **Try it out** button. You have thus activated the input field for the **dataSourceId**.
3. Enter the **dataSourceId** (identical to the zenon project ID).  
**Note:** You have thus defined the target project for the query. (Example: Initial query (on page 72))
4. Change the following points in the **Query specification**:
  - a) *fields*: Replace the predefined **"string"** with **"name", "value"**.  
You thus define the data fields for the query.
  - b) *nameFilter*: Replace the predefined **"string"** with **"\*"**.  
You use this placeholder to query all values unfiltered. (Example: custom query (on page 72))
5. Then click on **Execute** to perform the query.
6. The query is acknowledged as follows: **"Code 200" "Ok. Returns the queried variables."**
7. The **"Response body"** section shows the query result. (Example: query result (on page 73)).

The query result shows the released variables and their variable values from the specified zenon project.

### VariablesApi ▼

GET
/api/v1/datasources/{dataSourceId}/variables/{variableName}
Gets the data of a single variable.
🔒

PATCH
/api/v1/datasources/{dataSourceId}/variables/{variableName}
Sets the value of a single variable.
🔒

POST
/api/v1/datasources/{dataSourceId}/variables/query
Queries the data of multiple variables.
🔒

Only variables with the Service Grid Access Permissions "Read-only" or "Read-write" are returned. The returned variables are sorted by their name in ascending order. It is possible to use this endpoint to get all variables of a data source by specifying only the "name" field and the "\*" (asterisk) wildcard for the variable name.

Parameters

Try it out

Name	Description
<b>dataSourceId</b> * required string(\$uuid) (path)	Id of respective data source  <div style="border: 1px solid #ccc; padding: 2px; font-family: monospace; font-size: 0.8em; margin-top: 5px;">dataSourceId - Id of respective data source</div>

Request body required

application/json ▼

Query specification:

[Example Value](#) | [Schema](#)

```

{
  "fields": [
    "string"
  ],
  "nameFilter": {
    "variableNames": [
      "string"
    ]
  }
}
                    
```

### 6.2.4.7.12 Query specifications

You can find the query specifications in this section.

### 6.2.4.7.13 Initial query

#### Code Sample:

```
{
  "fields": [
    "string"
  ],
  "nameFilter": {
    "variableNames": [
      "string"
    ]
  }
}
```

Initial query

### 6.2.4.7.14 Custom query

#### Code Sample:

```
{
  "fields": [
    "name", "value"
  ],
  "nameFilter": {
    "variableNames": [
      "*"
    ]
  }
}
```

Query of variables and variable values

### 6.2.4.7.15 Query result

#### Code Sample:

```
{
"variables": [
{
"name": "MY_VARIABLE",
"value": "1"
}
]
}
```

The shared variable and the variable value are in the "Response body" section.

### 6.2.4.8 Appendix

Here you can find information on the following topics:

1. Test environment vs. productive environment (on page 97)
2. Determine FQDN (on page 73)
3. Check CPU hardware virtualization (on page 98)
4. Elevated PowerShell (on page 99)

#### 6.2.4.8.1 Test environment vs. productive environment

The test environment described in this guide is easier to set up than a typical productive environment.

The fundamental differences are:

	Test environment	Productive environment
<b>Installation option</b>	IloT Services (Docker on Windows)	<ul style="list-style-type: none"> <li>▶ IloT Services (Windows native)</li> <li>▶ IloT Services (Docker on Windows)</li> </ul>
<b>Number of computers</b>	A computer for IloT Services and all clients	<ul style="list-style-type: none"> <li>▶ A computer for IloT Services</li> <li>▶ Dedicated computers for clients</li> </ul>
<b>Network topology</b>	All applications run on the same computer.	<p>The applications run on different computers.</p> <p>The computers are usually distributed across different remote sites.</p>
<b>Multi-user system</b>	Not suitable as a multi-user	Suitable as a multi-user system.

	Test environment	Productive environment
	system.	
<b>Passwords</b>	It is possible to use predefined passwords in a protected test environment.	For all logins, it is essential that you assign your own secure passwords.

### 6.2.4.8.2 Installation options for IloT Services

Here you can find an overview of the different types of installation of IloT Services, as well as the instructions that you can use for the installation.

Type of installation	Instruction
Windows on-premises installation	Getting started guide - Windows (on page 54)
Installation of Docker on Windows	Follow the instructions in this guide (on page 78)
Installation of Docker on Linux	Follow the instructions in this guide (on page 79)
Docker in the cloud	Follow the basic steps in this guide and adapt the configuration files for your preferred cloud platform.
Kubernetes	Follow the basic steps in this guide and adapt the configuration files for Kubernetes.

### 6.2.4.8.3 Determine FQDN (Fully Qualified Domain Name)

To determine the **FQDN** of the Windows computer:

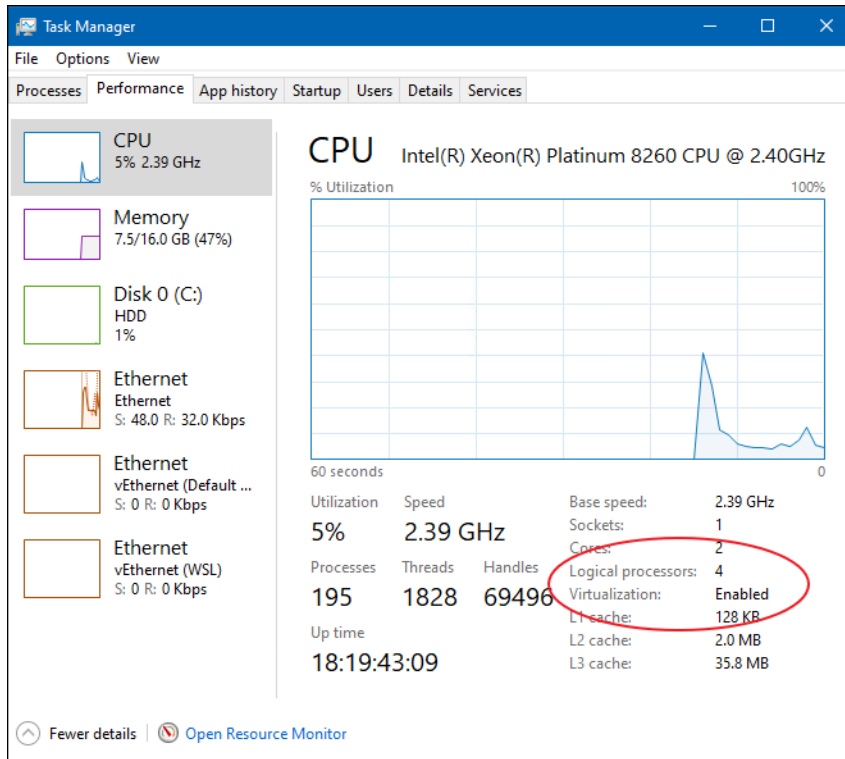
1. Open the command line using the **Windows + R** keyboard shortcut.
2. Enter **cmd.exe**.
3. Enter the **ping localhost** command.
4. The **Command Line Interface** shows your computer's FQDN, among other things.
5. Convert the FQDN to lower-case letters.

You have now determined the FQDN that you need for use in the IloT Services.

### 6.2.4.8.4 Check CPU hardware virtualization

To check whether the CPU hardware virtualization has been activated:

1. Open the **Task-Manager**.
2. Click on the **Performance** tab.
3. Go to the **CPU** category there.
4. If your system is correctly configured, you will find the **Virtualization: Enabled** entry under the CPU graph.



### 6.2.4.8.5 Elevated PowerShell

An *elevated PowerShell* is a PowerShell with administrator rights. You can use it to subsequently initialize and administer IIoT Services.

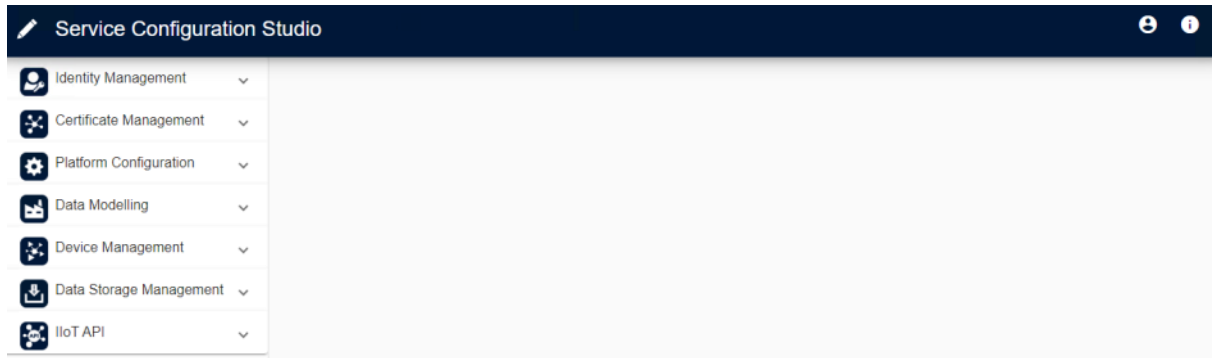
To create an *elevated PowerShell*:

1. Make sure that you have Windows administrator privileges on the test computer.
2. Create this link to your desktop: `%SystemRoot%\system32\WindowsPowerShell\v1.0\powershell.exe`
3. Right-click on the link to open the context menu.
4. Select the **Run as Administrator** option.

5. The *elevated PowerShell* is started.

## 7 Service Configuration Studio

The Service Configuration Studio is the central administration interface of the IIoT Services.



Valid for the Service Configuration Studio:

- ▶ The configuration interface is called up by entering a URL.
  - ▶ All services can be called up in a configuration interface. In this case, navigation contains each service as a main node.
- ▶ The user must log on before using the Service Configuration Studio.
  - ▶ Login is via **Identity Service** (on page 150).
  - ▶ The logged-in user must have the appropriate authorization to configure the particular service.
- ▶ Only services can be configured, for which the logged-in user has the appropriate authorizations.
- ▶ Options, dialogs and nodes are always visualized in the context of the logged-in user. This means: if a user does not have authorization, the respective configuration option for the user is hidden or is visualized with a corresponding notice.



### Information

You can find an overview of the URLs from individual configuration web pages in the **Addresses and URLs in the Service Configuration Studio** (on page 29) section.





## 7.1 User interface

The Service Configuration Studio user interface consists of different areas. View and structure of the configuration depend on the service.

Element	Description
<b>Header</b> (on page 102)	Toolbar with user-specific actions.
<b>Main nodes</b>	<p>Tree view of the IIoT Services with configuration options for each service.</p> <p>The subnodes subordinate to the main nodes can be displayed as expanded or collapsed with a mouse click. Individual nodes are expanded or collapsed by clicking on the node.</p> <ul style="list-style-type: none"> <li>▶ Arrow down: Expands the node view</li> <li>▶ Arrow up: Reduces the node view</li> </ul> <p>The display of the main node depends on the width of the browser window.</p> <ul style="list-style-type: none"> <li>▶ If this window is wide enough, a symbol and the service name or the name of the subnode will be displayed for each service.</li> <li>▶ If the window width is very small, only the service or its subnodes will be displayed.</li> </ul>
<b>Show/hide main nodes</b>	<p>The width of the main node is adjusted by clicking on the button:</p> <ul style="list-style-type: none"> <li>▶ &lt;: Reduces the display of the node and its subnodes to symbol view</li> <li>▶ &gt;: Expands the display of the node and its subnodes to symbol view + node names.</li> </ul>
<b>Subnodes</b>	By clicking on the subnode, the configuration options from the particular service is displayed in the configuration area.
<b>Configuration area</b>	<p>Options for configuring the service.</p> <p>Depending on the service, lists from existing configurations will also be displayed in this area. These lists can be sorted and filtered.</p>

Element	Description
	<ul style="list-style-type: none"> <li>▶ By clicking on the existing project configuration content, this can be changed in configuration dialogs.</li> <li>▶ By clicking on the appropriate buttons, new configuration content can be created and configured in configuration dialogs.</li> </ul>
<b>Configuration dialog</b>	Depending on the configuration's content, your own configuration dialogs will be displayed on the right side.

### 7.1.1 Header

 	
Button	Description
<b>User</b>	User-specific actions: <ul style="list-style-type: none"> <li>▶ <i>User Profile</i> Shows information about the user who is currently logged in. <b>Note:</b> You can find detailed information on this in the <b>Identity Service</b> (on page 150) section.</li> <li>▶ <i>Logout</i> Logs the current user out of Service Configuration Studio. The login dialog is shown in the browser after logout.</li> </ul>
<b>Information</b>	Visualizes the licensed system services in a dialog.

## DIALOG - SERVICE INFORMATION

### THE INFORMATION BUTTON IS VISUALIZED

#### Service information

**Identity Service**

Version: 12.1.2304.10001-BETA-master  
License status: Licensed

**Certificate Management**

Version: 12.1.2304.10001-BETA-master  
License status: Licensed

**Platform Configuration**

Version: 12.1.2304.10001-BETA-master

This dialog visualizes information about the individual IIoT Services.

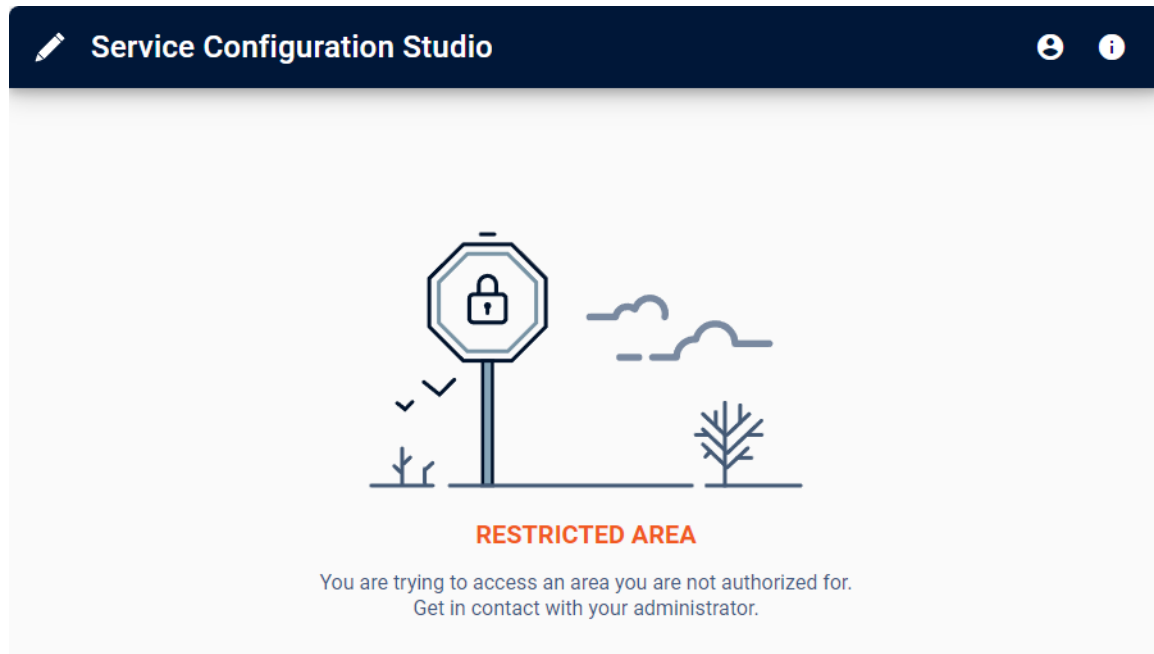
**Note:** This dialog can be closed with a click.

Option	Description
<b>Name of the service</b>	Name of the installed service.
<b>Version</b>	Version of the installed service.
<b>License status</b>	License status of the installed service.

### 7.1.2 Visualization of the missing user authorization

Options, dialogs and nodes are always visualized in the context of the logged-in user. Login is via the Identity Service in IIoT Services.

This means: if a user does not have authorization, the respective configuration option for the user is hidden or is visualized with a corresponding notice.



This illustration shows the display in Service Configuration Studio for the current logged-in user if there is no permission.



### Information

You can find further information on user administration in IloT Services in the **Identity Service** (on page 148) section.

## 8 Certificate Management

The **Certificate Management** node contains two components:

- ▶ **Certificate Management:** Is responsible for the access permissions of the individual services. It decides which Services get access and passes this information on to the **Data Hub**. In order to allow zenon applications access to **Certificate Management**, the user must use the **IloT Services Connection Wizard** to connect these to the **Certificate Management** and allow individual credentials to be generated for each Service. This ensures that only authorized Services can provide and consume data.
- ▶ **Data Hub:** Is the actual data distributor. In coordination with the **Certificate Management**, this decides which Services may connect

with it and send or receive data. The **Data Hub** distributes the notifications and guarantees the delivery of system-critical events to the recipients.



### Information

In the case of integration projects, each of the subordinate projects can communicate with another Data Hub. However, several projects can also access the same Data Hub.

## DATA HUB

As the central data transfer hub, it receives information of services and distributes it. The **Data Hub** is always installed on the same computer as the **Certificate Management** by default. A separate Certificate Bundle is needed for communication with **Certificate Management**.

With a standard installation, it is not necessary to change settings for the **Data Hub**. IIoT Services configure all required settings by default.

Configurations for the Data Hub are created by default from version 14. Adjustment is possible by means of a configuration file.

- ▶ Save location: *C:\Program Files\Common Files\zenon\DataHub*
- ▶ File name: *CDDataHub.conf*

The respective LOG level can also be adjusted in the *CDDataHub.conf* file. The corresponding entries have the provided configuration file with the corresponding comments.

### ⚠ Attention

The **Data Hub** service starts with a delay of approximately two minutes after system start.

## 8.1 Certificate Management

Connection state	Service type	FQDN	Serial number	Valid until	Created at	Created by	Revoke
Online	HubController	Docu-iiot-01.testenv.local	66911ABB1DC920 48A0AC22EDE66 E0D6E	Jun 19, 2028, 11:26:40 PM	Jun 20, 2023, 11:26:40 PM	HubController	Revoke
	DataHub	Docu-iiot-01.testenv.local	59A326536A70BA 4F999872C8CD85 5CAB	Jun 19, 2028, 11:26:45 PM	Jun 20, 2023, 11:26:45 PM	HubController	Revoke
Offline	ServiceGridApi	Docu-iiot-01.testenv.local	00FAB1BE2C94E B4B40A305990FE DFAF0B0	Jun 19, 2028, 11:26:55 PM	Jun 20, 2023, 11:26:55 PM	System	Revoke
Never connected	WebEngine	Docu-iiot-01.testenv.local	00BA39F1BE36A4 2D4BBD052A5A2 485C07D	Jun 19, 2028, 11:26:57 PM	Jun 20, 2023, 11:26:57 PM	System	Revoke
Never connected	Service Engine	ATSZG-WKS287.copa-data.internal	00E48BA4742E 48946A622A10F4 C57C1E0	Jun 19, 2028, 11:45:41 PM	Jun 20, 2023, 11:45:41 PM	admin admin	Revoke
Never connected	Engineering Studio	ATSZG-WKS287.copa-data.internal	00CAE511E389CF 1B438C90CBDDC EED0E62	Jun 19, 2028, 11:45:42 PM	Jun 20, 2023, 11:45:42 PM	admin admin	Revoke

Configuration for Certificate Management is integrated into Service Configuration Studio.

**Certificate Management** takes on the task of access verification for the **Data Hub**. In order to access a **Data Hub**, Services require credentials and **Certificate Bundles** from the **Certificate Management**. This verification is initiated by the **Data Hub**.

**General procedure:**

1. The client receives the **Certificate Bundle** and the credentials contained therein from the **Service Node Configuration Tool**.
2. The client connects to the **Data Hub**.
3. The **Data Hub** checks the access permission by querying the **Certificate Management**.
4. Depending on the result, the **Data Hub** either provides access to the client or declines it.

**The tabs that are shown by Certificate Management depend on the variant installed:**

IloT Services (Docker)	IloT Services (Windows native)
<p><b>Tab:</b></p> <ul style="list-style-type: none"> <li>▶ Certificates</li> </ul>	<p><b>Tabs:</b></p> <ul style="list-style-type: none"> <li>▶ Data Hub</li> <li>▶ Data Hub configuration</li> <li>▶ Certificates</li> </ul>



## 8.2 Certificate Bundles

Connection state	Service type	FQDN	Serial number	Valid until	Created at	Created by	Revoke
● Online	HubController	Docu-iiot-01.testenv.local	66911ABB1DC920 48A0AC22EDE66 E0D6E	Jun 19, 2028, 11:26:40 PM	Jun 20, 2023, 11:26:40 PM	HubController	Revoke
	DataHub	Docu-iiot-01.testenv.local	59A326536A70BA 4F999872C8CD85 5CAB	Jun 19, 2028, 11:26:45 PM	Jun 20, 2023, 11:26:45 PM	HubController	Revoke
● Offline	ServiceGridApi	Docu-iiot-01.testenv.local	00FAB1BE2C94E B4B40A305990FE DFAF0B0	Jun 19, 2028, 11:26:55 PM	Jun 20, 2023, 11:26:55 PM	System	Revoke
○ Never connected	WebEngine	Docu-iiot-01.testenv.local	00BA39F1BE36A4 2D4BBD052A5A2 485C07D	Jun 19, 2028, 11:26:57 PM	Jun 20, 2023, 11:26:57 PM	System	Revoke
○ Never connected	Service Engine	ATSZG-WKS287.copa-data.internal	00EC4BBA4742E 48946A622A10F4 C57C1E0	Jun 19, 2028, 11:45:41 PM	Jun 20, 2023, 11:45:41 PM	admin admin	Revoke
○ Never connected	Engineering Studio	ATSZG-WKS287.copa-data.internal	00CAE511E389CF 1B438C90CBDDC EED0E62	Jun 19, 2028, 11:45:42 PM	Jun 20, 2023, 11:45:42 PM	admin admin	Revoke

This subpage shows all connections in IIoT Services set up with Certificate Bundles (CB).

In addition, you can download the self-signed root certificate of IIoT Services using **DOWNLOAD CA CERTIFICATE**. You require this certificate file to establish a HTTPS trust relationship (on page 260).

### CERTIFICATE BUNDLES

Column	Description
<p><b>Connection state</b></p>	<p>Shows the state of the connection between services and <b>Certificate Management</b>:</p> <ul style="list-style-type: none"> <li>▶ <i>Online</i>: This service is currently connected.</li> <li>▶ <i>Disconnected</i>: This service is currently not connected.</li> <li>▶ <i>Never connected</i>: This service has never been connected before</li> <li>▶ <i>Connection lost</i>: The connection has been interrupted with this service.</li> </ul> <p>If you move the mouse pointer over an entry, a pop-up (mouseover) also shows this information:</p> <ul style="list-style-type: none"> <li>▶ <i>Connection state changed</i>: Timestamp when the service last changed a connection state.</li> </ul> <p>No state is displayed for services that do not</p>

Column	Description
	establish a direct connection to <b>Certificate Management</b> .
<b>Service type</b>	The service type is an internal name of the service.
<b>FQDN</b>	Fully-qualified domain name of the computer to which the certificate bundle is assigned.
<b>Serial number</b>	The serial number of the certificate.
<b>Valid until</b>	Date and time until which the certificate is valid and can be used by the respective service.
<b>Created at</b>	Date and time when the certificate was created.
<b>Created by</b>	The service or the user that creates the connection.  <b>Note:</b> If the user that created the Certificate Bundle is deleted from the IDS, then the user ID of the user will be displayed here.
<b>Revoke</b>	With this button you can revoke the certificate bundle for the selected service.  After selecting <b>Revoke</b> , the following is displayed: <ul style="list-style-type: none"> <li>▶ The time (UTC) of the <b>Revoke</b></li> <li>▶ The user who executed the <b>Revoke</b></li> </ul> A <b>Revoke</b> is only necessary if the certificate bundle is potentially compromised (on page 109). Normally, you continue to use the certificate bundle created during installation.

**⚠ Attention**

The **Revoke** of a certificate bundle interrupts communication between services. Before each **Revoke**, check and make sure if this intervention is appropriate and necessary for the respective service (on page 109).



## 8.2.1 Revoke of certificate bundles

Each connection between a service and **Certificate Management** requires its own certificate bundle. Each certificate bundle can be revoked separately using Revoke (on page 107).

Certificate bundles should only be revoked for specific reasons.

### REASONS FOR A REVOKE

As soon as there are any indications that a certificate bundle could be compromised, it should be revoked.

Possible reasons for a revoke:

- ▶ The certificate including the private key has been stolen.
- ▶ Secret certificate information such as the private key is publicly available.

A Revoke has the following consequences:

- ▶ The respective service can no longer connect to IIoT Services.
- ▶ The exchange of data between the affected service and IIoT Services has been interrupted.

To restore functionality, you must generate a new certificate bundle. The exact procedure depends on the chosen installation option for IIoT Services.

#### Attention

The certificate bundle for **Certificate Management** should not be revoked using **Revoke**. If the certificate bundle for **Certificate Management** is thought to be compromised, a complete re-installation of the IIoT Services is required.

## 8.2.2 Generate new certificate bundles (Docker)

For the IIoT Services (Docker) installation option, there are several different ways to generate new certificate bundles for affected services.

### OPTION A) WINDOWS-BASED SERVICES

This option applies for the following services under Windows:

- ▶ Service Engine
- ▶ Engineering Studio
- ▶ Report Engine

- ▶ Web Engine (on Windows)

### To generate a new certificate bundle:

1. Revoke the certificate bundle for the selected service using **Revoke** in Service Configuration Studio.
  - a) To do this, go to the **Certificate Bundles** subnode in the **Certificate Management** main node.  
A list of all certificate bundles is shown.
  - a) In the **Revoke** column, click on the **Revoke** button in the entry for the corresponding bundle.
2. Use the **IloT Services Connection Wizard** to generate a new certificate bundle for the connection between the service and IloT Services.
3. Restart the service.

In this way, you have secured the communication for the selected service with a new certificate bundle.

#### **Hint**

Certificate Bundles can also be generated with the **IloT Services CLI** (on page 112).

## OPTION B) DOCKER-BASED SERVICES

### This option applies for the following services in Docker:

- ▶ All IloT Services
- ▶ Web Engine (in Docker)

### To generate new certificate bundles for a Docker-based service:

1. Revoke the certificate bundle for the selected service using **Revoke** in the web interface of **Certificate Management**.
2. Stop all services of the IloT Services with this Docker command:  
*docker-compose down*
3. Delete the volume of the affected service (see table below) with this Docker command:  
*docker volume rm <volume>*
4. Start all services of the IloT Services with this Docker command:  
*docker-compose up*  
When the service is started, deleted volumes will be created again and, if necessary, new certificate bundles will be created automatically.

In this way, you have secured the communication for the selected service with a new certificate bundle.

### 8.2.3 Generate new certificate bundles (Windows native)

For the IIoT Services (Windows native) installation option, you can generate new certificate bundles for affected services in the same way.

1. Revoke the certificate bundle for the selected service using **Revoke** in Service Configuration Studio.
  - a) To do this, go to the **Certificate Bundles** subnode in the **Certificate Management** main node.  
A list of all certificate bundles is shown.  
  
In the **Revoke** column, click on the **Revoke** button in the entry for the corresponding bundle.
1. Use the **IIoT Services Connection Wizard** to establish the connection between the service and IIoT Services.
2. Restart the service.

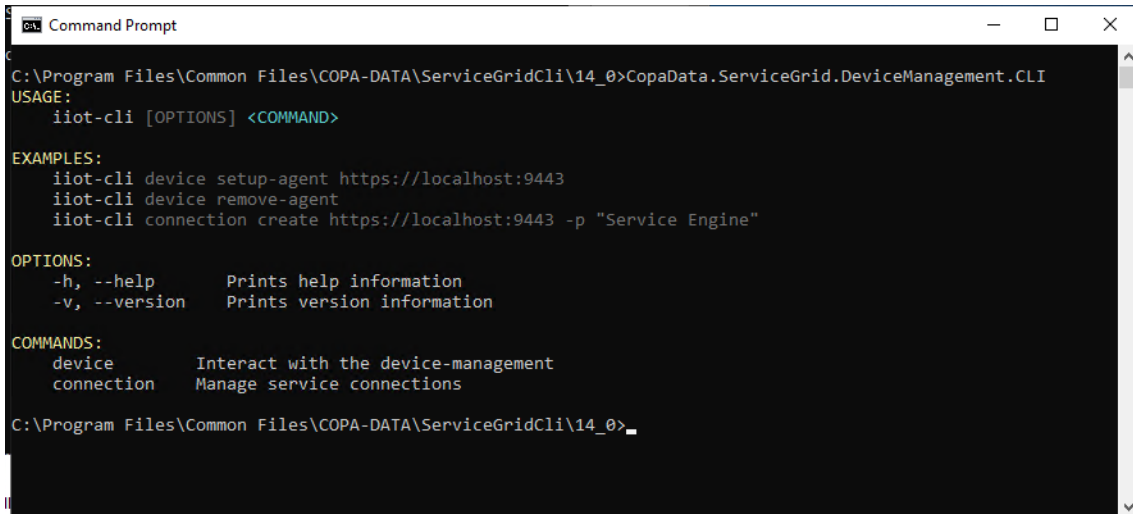
In this way, you have secured the communication for the selected service with a new certificate bundle.

#### **Hint**

Certificate Bundles can also be generated with the **IIoT Services CLI** (on page 112).

## 8.2.4 Certificate Management via IIoT Services CLI

From version 14, Certificate Bundles can also be created with the IIoT Services CLI.



```

C:\Program Files\Common Files\COPA-DATA\ServiceGridCli\14_0>CopaData.ServiceGrid.DeviceManagement.CLI
USAGE:
  iiot-cli [OPTIONS] <COMMAND>

EXAMPLES:
  iiot-cli device setup-agent https://localhost:9443
  iiot-cli device remove-agent
  iiot-cli connection create https://localhost:9443 -p "Service Engine"

OPTIONS:
  -h, --help      Prints help information
  -v, --version   Prints version information

COMMANDS:
  device          Interact with the device-management
  connection     Manage service connections

C:\Program Files\Common Files\COPA-DATA\ServiceGridCli\14_0>_
    
```

The **IIoT Services CLI** offers context-dependent execution. This means that you are shown the available TAGs step by step when executing the tool. If you expand the command, the next time it is called up the TAGs for the previously-used TAGs are shown, etc.

Additionally, when creating Certificate Bundles, a service can be selected in a graphical preview directly in the CLI after entering the command.

### 8.2.4.1 Requirements - Client for IIoT Services CLI in Identity Management

If you execute the commands of the **IIoT Services CLI** with a script, you can quickly and easily install certificates on the respective client or register the device for Device Management (on page 276).

If you use client access data for the authentication through **IIoT Services CLI**, a corresponding **Client** (on page 221) must be available. Create this client in **Identity Management**. The client must have the following configuration:

Parameter	Description
<b>Client Type</b>	<i>Custom OAuth 2.0 client</i>
<b>Client ID</b>	<i>CLI</i>
<b>Grant types</b>	<i>ClientCredentials</i>
<b>Allowed scopes</b>	<ul style="list-style-type: none"> <li>▶ <i>identityAPI.full_access</i></li> <li>▶ <i>certificateManagementAPI</i></li> <li>▶ <i>deviceManagementAPI</i></li> </ul>

## 8.2.4.2 Generate Certificate Bundle via CLI

Execute the following commands to generate a Certificate Bundle via CLI:

1. Start the command line interface as an administrator
  - ▶ Windows:
    - a) Go to the save folder of the tool. The path for this is the following by default: C:\Program Files\Common Files\COPA-DATA\ServiceGridCli\14\_0
    - a) Start the command line interface as an administrator.
    - b) Start the IIoT Services CLI with the following command:  
*cd C:\Program Files\Common Files\COPA-DATA\ServiceGridCli\14\_0\*
    - c) *CopaData.ServiceGrid.DeviceManagement.CLI*  
The CLI window shows the available commands.
  - ▶ Linux & Docker:  
Start the tool with the command *sudo iiot-cli*  
**Note:** Commands and parameters are identical for Linux and Windows.
2. Expand the command using the command *connection create + URL + Port*  
**Example:** *CopaData.ServiceGrid.DeviceManagement.CLI connection create https://myComputer.myDomain:9443*
3. A list of the available IIoT Services services is shown in text form.
4. Use the arrow keys to select the service from the list that is to be generated for the Certificate Bundle
5. Confirm the selection with the space key and enter key.
6. The command is generated and executed on the basis of your selection.
7. The steps executed are displayed in the CLI directly.

As an option, the command can be entered and executed directly without contextual support.

- ▶ **Syntax:** *CopaData.ServiceGrid.DeviceManagement.CLI connection create [URL + Port] -p "Servicename"*
- ▶ **Example:** *CopaData.ServiceGrid.DeviceManagement.CLI connection create https://myComputer.myDomain:9443 -p "IIoT API"*

### OPTIONAL TAGS

TAGs	Description
-h	Shows commands, TAGs and information in relation to

TAGs	Description
--help	this in the CLI window.
-d --use-device-code	<p>Type of login to the <b>Identity Service</b> for execution of the CLI command via device code.</p> <p><b>Note:</b> Use this TAG for example if you do not want to be able to use a web browser on the executing client for login to the Identity Service.</p>
-c --client-id	<p>Unique ID of the client for login to the <b>Identity Service</b> while the command is executed.</p> <p><b>Note:</b> Use this TAG for example if you do not want to be able to use a web browser on the executing client for login to the Identity Service. Use this TAG together with the TAG for the <b>Client Secret</b>. Also ensure that the given client is configured with the necessary access permissions (= creation of connections) in <b>Identity Management</b>.</p>
-s --client-secret	<p>Client secret for login to the <b>Identity Service</b> when executing the command.</p> <p><b>Note:</b> Use this TAG for example if you do not want to be able to use a web browser on the executing client for login to the Identity Service.</p> <p>Use this TAG together with the TAG for the <b>Client ID</b>. Also ensure that the given client is configured with the necessary access permissions (= creation of connections) in <b>Identity Management</b>.</p>
-p --service [IIoT Services Service Name]	<p>Name of the existing service for which the Certificate Bundle (connection) is generated by means of a command.</p> <p><b>Note:</b> Several Certificate Bundles can be generated in one command.</p> <p><b><i>COPADATA.SERVICEGRID.DEVICEMANAGEMENT.CLI CONNECTION CREATE HTTPS://MYCOMPUTER.MYDOMAIN:9443 -P "IIOT API" -P "SERVICE ENGINE -P REPORT ENGINE</i></b></p>

## 8.3 Data Hub - save location

Configurations for the Data Hub are created by default from version 14. Adjustment is possible by means of a configuration file.

- ▶ Save location: *C:\Program Files\Common Files\zenon\DataHub*
- ▶ File name: *CDDataHub.conf*

The respective LOG level can also be adjusted in the *CDDataHub.conf* file. The corresponding entries have the provided configuration file with the corresponding comments.

### SAVE LOCATION FOR DATA HUB DATA

The **Hub Controllers** data is stored in the following save location:

- ▶ *%CD\_SYSTEM%/ServiceGrid/HubController*

### MONGODB CONFIGURATION FILE

The name of the

The *mongod.cfg* configuration file is saved in the following save location:

- ▶ *%CD\_SYSTEM%/ServiceGrid/Persistence*

### UPDATE

In the event of an update, all data from version 10 will be adjusted to the current storage structure.



#### Information

Delete your browser cache after an update. As a result, it is ensured that, when logging in to the Identity Service, no outdated or saved login data is used.

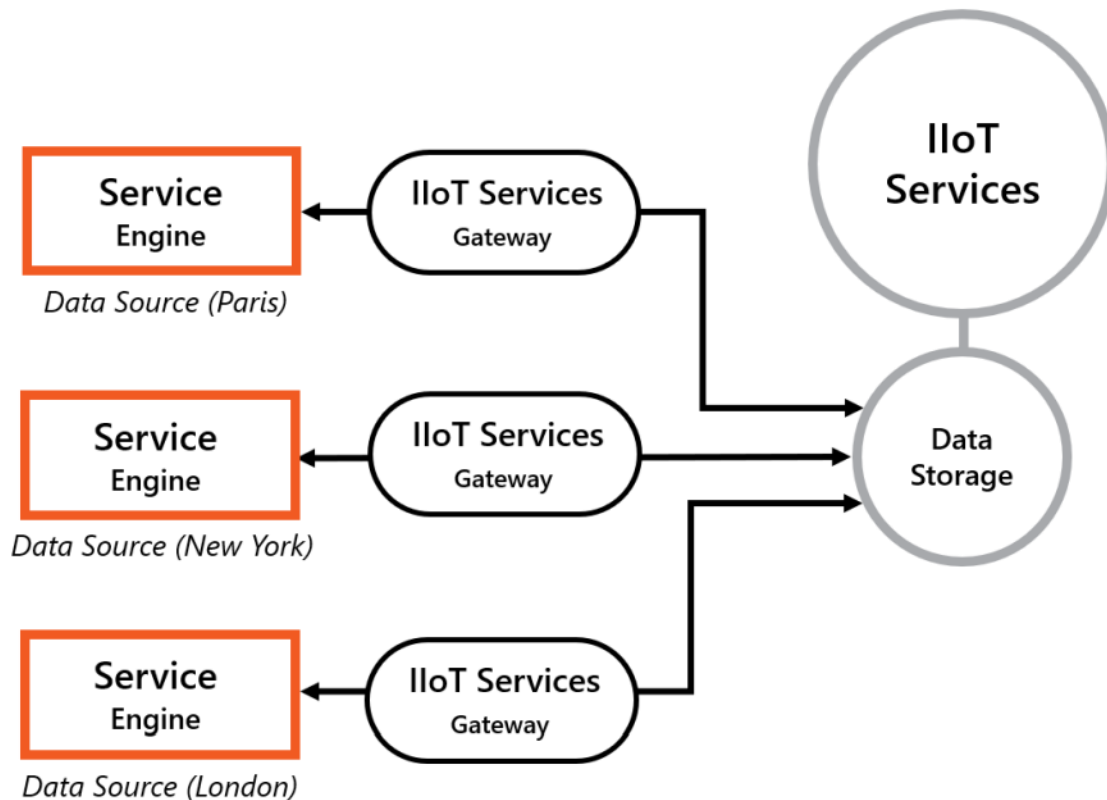
## 9 Data Storage

**Data Storage** enables you to store data centrally via the IIoT Services and make it available for other applications. You administer **Data Storage** in Service Configuration Studio.

You can find notes on configuration in Engineering Studio in the **IIoT Services - configuration in Engineering Studio** (on page 307) node.

## 9.1 Evacuate data centrally

You can use **Data Storage** to evacuate alarm data, archive data and event data from several Service Engine instances into IloT Services, and to read it back again. Archive data is historical variable values. The complete process runs transparently for the user. No user input is necessary regardless of the configuration.



You can store the data of multiple Service Engine instances centrally in Data Storage. Every Service Engine can read back its own data from Data Storage.

**Important:** Each Service Engine can only read back its own data!

### AREA OF APPLICATION

You can use Data Storage as:

- ▶ Central evacuation location for data from Service Engine instances.
- ▶ Central data source for reading back data in Service Engine instances.

The data is deleted in Service Engine (data source) once it has been successfully evacuated to **Data Storage**.



## SUPPORTED DATA ACTIONS

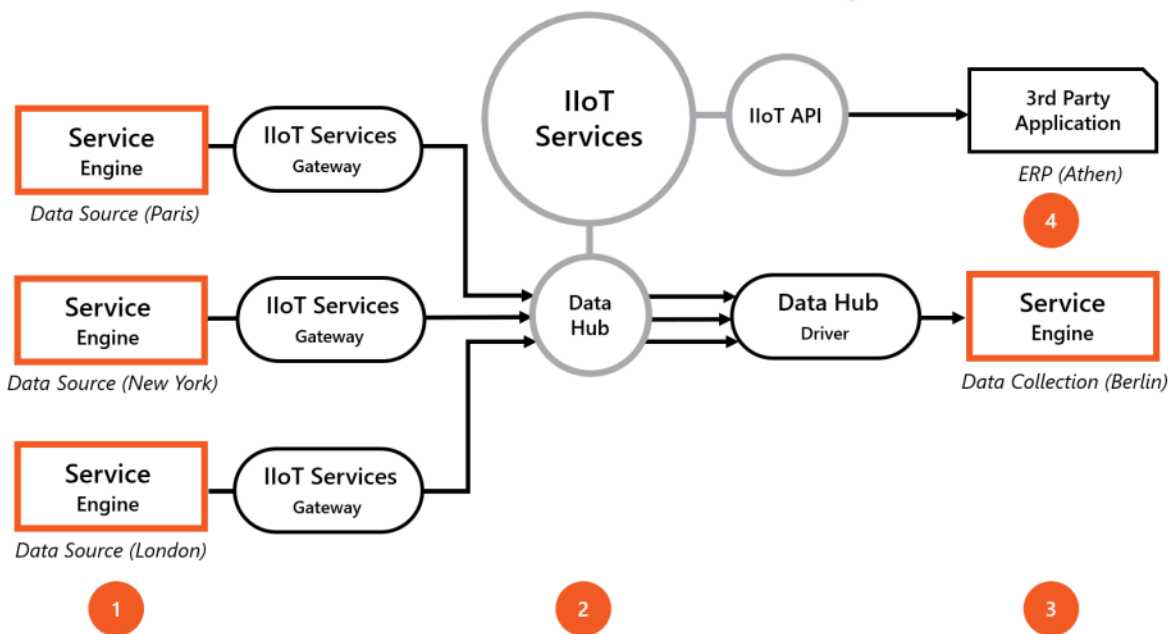
When transferring data from Service Engine to **Data Storage**, data is transferred and saved in unchanged form. This also applies to reading back the data from Data Storage to Service Engine.

Supported data types	Access permission variable*
Alarms	None
Archive data	Read only
Events	None

\*required access permission in Service Engine (data source).

## 9.2 Provide evacuated data

You can use the IIoT API to query archive data from **Data Storage** and provide it to third-party applications. Archive data is historical variable values.



Archive data from Data Storage can be queried using the IIoT API.

## AREA OF APPLICATION

You can use this use case for the following scenarios:

- ▶ Reading archive data from Data Storage
- ▶ Provision of archive data for third-party applications

## SUPPORTED DATA ACTIONS

When transferring data from **Data Storage** to the IIoT API , archive data is transferred in unchanged form. Access to Data Storage is read only. A **Data Storage** query using the IIoT API therefore has no effect on the data in Data Storage.

Supported data types	Variable access authorization*
Archive data	Read only

\*required access authorization in Service Engine (data source).

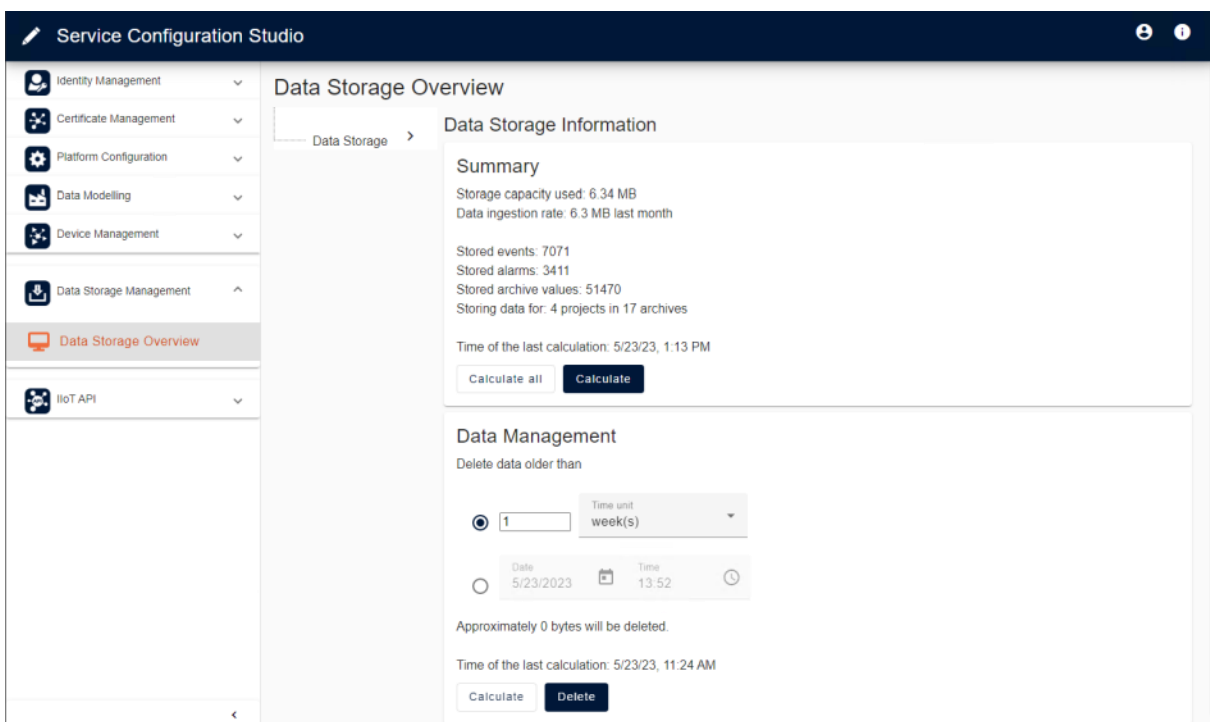
## 9.3 Administration in Service Configuration Studio

The service for **Data Storage** in the Service Configuration Studio allows the following:

- ▶ Display of database statistics
- ▶ Display of project statistics
- ▶ Manage data saved in **Data Storage**

The start takes place:

- ▶ via Service Configuration Studio
- OR:
- ▶ as external HTML site: [https://\[FQDN\]:9443/data-storage](https://[FQDN]:9443/data-storage)  
**Example:** <https://iiot-docu-v8.testenv.local:9443/data-storage>

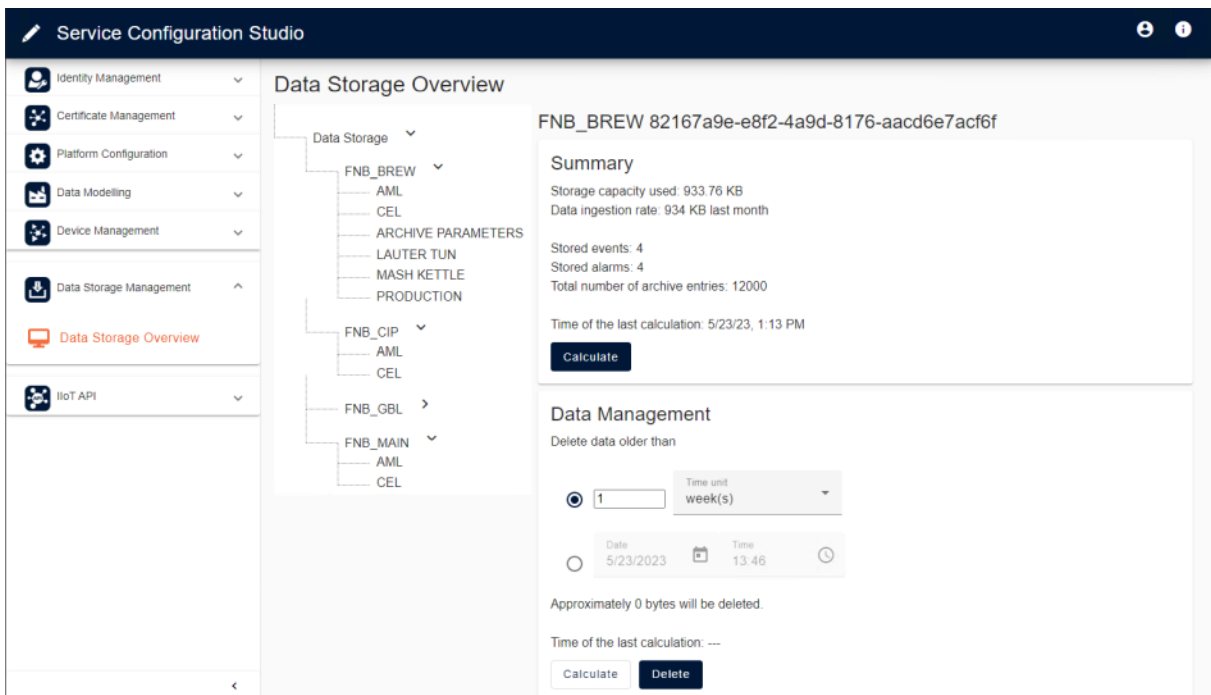


### 9.3.1 Data Storage Overview

You can get an overview of the saved data in the Overview tab.

**Areas:**

- ▶ Summary (on page 119): Saved objects
- ▶ Data Management (on page 121): Deletion of objects
- ▶ Service Engine (on page 122): Objects for each linked Service Engine



#### 9.3.1.1 Summary

You get an overview of all saved information in this node.

#### Data Storage Information

##### Summary

Storage capacity used: 6.34 MB  
 Data ingestion rate: 6.3 MB last month

Stored events: 7071  
 Stored alarms: 3411  
 Stored archive values: 51470  
 Storing data for: 4 projects in 17 archives

Time of the last calculation: 5/23/23, 1:13 PM

Display	Description
Storage capacity used:	Amount of storage used. This includes data storage and index storage.
Data ingestion rate:	Data ingestion per month.
Stored events:	Saved events.
Stored alarms:	Saved alarms.
Stored archive values:	Stored archive values.
Storing data for:	Number of saved projects and archives.
Time of the last calculation:	Time of the last calculation.
Calculate	Starts calculation for the Service Engine project page. <b>Note:</b> With large amounts of data, the calculation can take a very long time.
Calculate all	Starts calculation for all Service Engine project pages. <b>Note:</b> With large amounts of data, the calculation can take a very long time.

## CYCLICAL CALCULATION OF THE STATISTICS DATA

Depending on the size of the database, the calculation of the statistics can take some time. For this reason, the calculation is carried out cyclically via a service.

The start time and calculation time can be set using *appsettings.json* with *ManagementCacheConfiguration* .

### **Parameter:**

*IntervalHours*: Setting for the hour intervals in which the automatic statistics calculation is to be carried out.

*StartCalculationTime*: Start of the first statistics calculation.

### **Example:**

```
"ManagementCacheConfiguration": {
  "IntervalHours": 12,
  "StartCalculationTime": "02:00:00"
}
```

### 9.3.1.2 Data management

You administer the objects in **Data Storage** in this node. You can calculate the size of the storage occupied and delete data.

#### Data Management

Delete data older than

Time unit  
 week(s)

Date  
 5/23/2023

Time  
 13:52

Approximately 0 bytes will be deleted.

Time of the last calculation: 5/23/23, 11:24 AM

Calculate
Delete

Option	Description
<b>Input field</b>	Entry of the numeric value for <b>Time Unit</b> . Configures the time period for the action to be executed.
<b>Time Unit</b>	Time unit from numerical field. Select from drop-down list: <ul style="list-style-type: none"> <li>▶ Hour(s)</li> <li>▶ Day(s)</li> <li>▶ Week(s)</li> <li>▶ Month(s)</li> <li>▶ Years()</li> </ul>
<b>Date/Time</b>	Timestamp, up to which data is deleted.
<b>Time of last calculation:</b>	Time of the last calculation. Indication of the amount of data to be deleted.
<b>Calculate</b>	Calculates the extent of data to be deleted. The basis is the set time filter.  <b>Note:</b> With large amounts of data, the calculation can take a very long time.
<b>Delete</b>	Deletes data selected on the basis of the filter. Data from all subnodes is included.

Option	Description
	<p><b>Note:</b> With large amounts of data, deletion can take a very long time.</p>

## DELETE DATA

The time period for the deletion of data can be set in two ways.

- ▶ Data that is older than a certain time period. This is selected by means of configuration in the **Time Unit** option.  
This time period can be defined in complete hours, days, weeks months or years in the past. Smaller units are ignored in each case. 1 full hour thus means: Minutes and seconds are not taken into account.
- ▶ Data that is older than a certain timestamp. They are selected using the **Date/Time** option.

### Example:

- ▶ The time filter is set to: Delete data that is older than 1 hour.
- ▶ Current time on deletion: 13:30:23
- ▶ All data from before 12:00:00 is deleted.

### 9.3.2 Linked Service Engine

Each linked Service Engine is represented by its own node.  
In the subnodes, data is displayed for:

- ▶ Archive
- ▶ Lot archive
- ▶ AML

▶ CEL

- Data Storage ▾
  - FNB\_BREW ▾
    - AML
    - CEL
    - ARCHIVE PARAMETERS
    - LAUTER TUN
    - MASH KETTLE
    - PRODUCTION
  - FNB\_CIP ▾
    - AML
    - CEL
  - FNB\_GBL >
  - FNB\_MAIN ▾
    - AML
    - CEL

### FNB\_BREW 82167a9e-e8f2-4a9d-8176-aacd6e7acf6f

#### Summary

Storage capacity used: 933.76 KB  
 Data ingestion rate: 934 KB last month

Stored events: 4  
 Stored alarms: 4  
 Total number of archive entries: 12000

Time of the last calculation: 5/23/23, 1:13 PM

**Calculate**

---

#### Data Management

Delete data older than

1 Time unit  
week(s)

Date 5/23/2023 Time 13:46 🕒

Approximately 0 bytes will be deleted.

Time of the last calculation: ---

Calculate Delete

Display	Description
Storage capacity used:	Amount of storage used. This includes data storage and index storage.
Data ingestion rate:	Data growth per month.
Stored events:	Stored events for CEL and <b>Continuous export</b> .
Stored alarms:	Stored alarms for AML and <b>Continuous export</b> .
Stored archive values:	Stored archive values.
Time of the last calculation:	Time of the last calculation.
Calculate	Starts calculation for the Service Engine project page. <b>Note:</b> With large amounts of data, the calculation can take a very long time.

## 10 Data Modeling

Data Modeling is a central service of the zenon Software Platform. It offers a central repository for all types of structured data both of the zenon Software Platform as well as custom data models. The data is available via a **GraphQL** (on page 137) interface.

zenon Data Modeling is based on a relational model, similar to an Entity-Relationship model. Modular data models are defined in **Construction Kit Libraries**.

### EXAMPLE

Example of a scheme of a data model and the data contained therein:



Scheme for data model

#### Management of the data models:

- ▶ Support of tenants
- ▶ Import and removal of models
- ▶ Validation of models
- ▶ Administration of versions

#### Operative use of data models:

- ▶ Comprehensive **GraphQL** interface, which enables modifying and querying data and querying metadata.
- ▶ **GraphQL Editor** with autocomplete and integrated scheme documentation
- ▶ Online scheme update when changing the data model
- ▶ Validation of **GraphQL** mutations to scheme breaches



**Note:** zenon Data Modeling is still in development. Over time, there will be more and more data and functionality available.

## 10.1 Terminology for COPA-DATA Data Modeling

In this documentation, the English version of the Data Modeling terms is used regardless of the display language.

Term	Description
<b>Association</b>	Relationship between entities of a certain type. It has incoming/outgoing multiplicity and a description.
<b>Attribute</b>	A property of an entity with a value. It has a simple data type and a description.
<b>Construction Kit (CK)</b>	The Data Model, i.e. all metadata together within a <b>Tenant</b> . Metadata consists of, for example, type definitions, tags etc. The Data Model is made up of different <b>Construction Kit Libraries</b> .
<b>Construction Kit Library (CKL)</b>	A logically-coherent scheme, which has its own metadata, and can be added to a <b>Construction Kit</b> by means of import.
<b>Entity</b>	Instance of a defined <b>Type</b> .
<b>Namespace</b>	A prefix for the types within a <b>Construction Kit Library</b> . <b>Functions:</b> <ul style="list-style-type: none"> <li>▶ Makes naming conflicts less likely</li> <li>▶ Enables better identification of <b>Types</b></li> </ul>
<b>Tag</b>	Semantic information that can be added to the definition of <b>Attributes</b> or <b>Associations</b> . It is for further categorization and classification.
<b>Tenant</b>	Highest organization level in the <b>Data Modeling service</b> . Each <b>Tenant</b> has its own <b>Construction Kit</b> .
<b>Type</b>	Definition of objects through names, inheritance, <b>Associations</b> and <b>Attributes</b> .

## 10.2 Construction Kit

The **Construction Kit** is all metadata together in a **Tenant** of Data Modeling. The **Construction Kit** is made up of different **Construction Kit Libraries**.

The following is configured in the **Construction Kit**:

- ▶ **Types**: Logical objects in the data model. On the basis of the defined **Types**, corresponding instances (**Entities**) can be generated.
- ▶ **Attributes**: The properties that the respective **Types** have are configured. **Attributes** are assigned to **Types** and have a certain data type. Instances of the respective **Types** can be used to set the values of the corresponding attributes **Attributes**.
- ▶ **Associations**: Stipulate which instances of different types can be linked to one another.
- ▶ **Inheritance**: Configures the inheritance structure of the defined **Types**.
- ▶ **Association Tags**: When configuring **Associations**, defined **Association Tags** can be linked.
- ▶ **Attribute Tags**: When configuring **Attributes**, defined **Attribute Tags** can be linked.

**Construction Kit Libraries** can exhibit dependencies on one another with:

- ▶ **Inheritance**: Reference to basic **Type** that has been configured in another **Construction Kit Library**.
- ▶ **Associations**: Reference from associated **Type** that has been configured in another **Construction Kit Library**.
- ▶ **Attribute Tag**: Use of an **Attribute Tag** that has been configured in another **Construction Kit Library**.
- ▶ **Association Tag**: Use of an **Association Tag** that has been configured in another **Construction Kit Library**.

### 10.2.1 Construction Kit Libraries

A **Construction Kit Library (CKL)** is a logical scheme for a certain area of application. It contains the **Types**, including **Associations**, **Attributes** and **Tags** that are required for a certain usage or solution.

**Construction Kit Libraries** can be imported into the **Construction Kit** of a **Tenant**. Imported **Construction Kit Libraries** can also be deleted. However, this is only possible if no other **Construction Kit Libraries** are based on them.

**Attention**: When a **Construction Kit Library** is deleted, the definitions and their instances are deleted.

**Construction Kit Libraries** are versioned; a new version of a **Construction Kit Library** must always contain all definitions contained in the previous versions (principle: grow only).

**Construction Kit Libraries** can have dependencies. You thus configure the other **Construction Kit Libraries** on which they are based. To do this, you derive your **Types** from **Types** configured there or create **Associations** to the **Types** configured there.

**Metadata of a Construction Kit Library:**

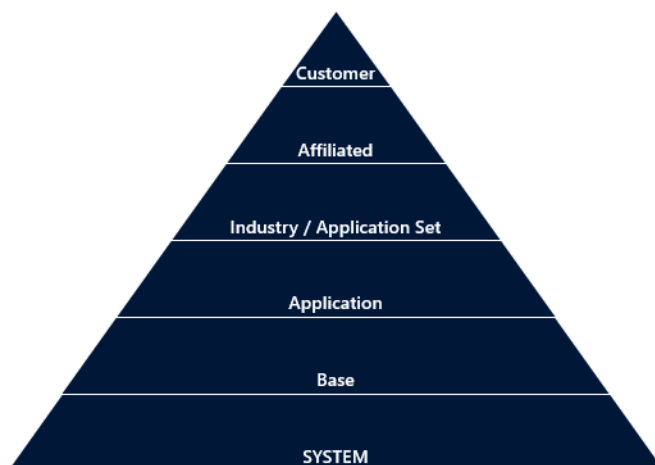
- ▶ unique ID
- ▶ Version
- ▶ Display name for display in the user interface
- ▶ unique Namespace
- ▶ Assignment to a Layer
- ▶ Dependencies on other **CKLs**:
  - ▶ GUID
  - ▶ Version

## 10.2.2 Construction Kit layer

Each **Construction Kit** consists of **Layers**. Each **Construction Kit Library** configures an assigned layer.

**Construction Kits** serve different purposes and are developed by different groups of people. Layers offer a simple possibility for structuring.

A **Construction Kit Library** can be dependent on other **Construction Kit Libraries** that are configured on the same layer or a layer below.

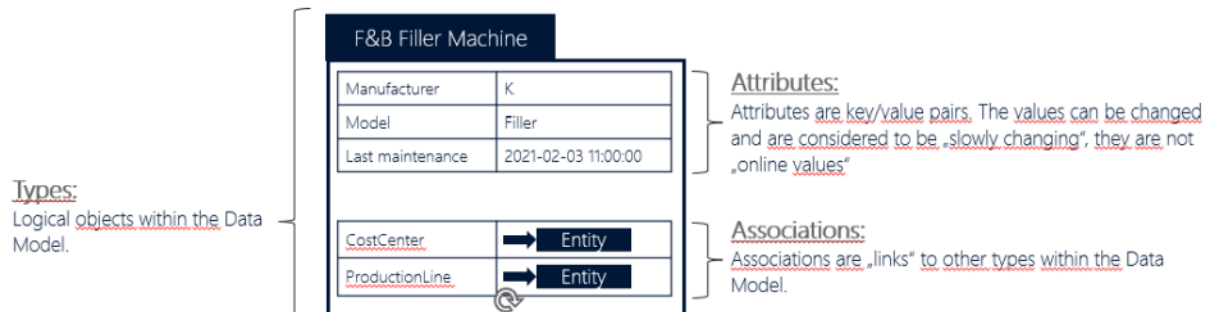


Display of all available layers.

Only the company COPA-DATA can create **Construction Kit Libraries** for the **System**, **Base** and **Application** layers.

## 10.2.3 Types

A **Type** is uniquely identifiable from the namespace of the **Construction Kit Library** + name (**Construction Kit ID**). **Types** have **Attributes** and **Associations** to other **Types**. They can be derived from other **Types** (simple inheritance).



Example of a **Type** with **Attribute** and **Associations**.

### 10.2.3.1 Attributes

**Attributes** are configured to types. A significant part of the definition is the name of the **Attribute**.

The Name:

- ▶ Must be unique in the inheritance tree of the **Type**
- ▶ Must not be identical to the name of an **Association**

A **Value Type** must also be given with the definition.

The following are available:

- ▶ *Integer*
- ▶ *String*
- ▶ *DateTime*
- ▶ *StringArray*
- ▶ *Boolean*
- ▶ *Double*
- ▶ *IntArray*
- ▶ *Binary*

### 10.2.3.2 Associations

**Associations** are configured to **Types**. This type is the **Source Type** for the **Association**. A significant part of the definition is the name of the **Association**.

The Name:

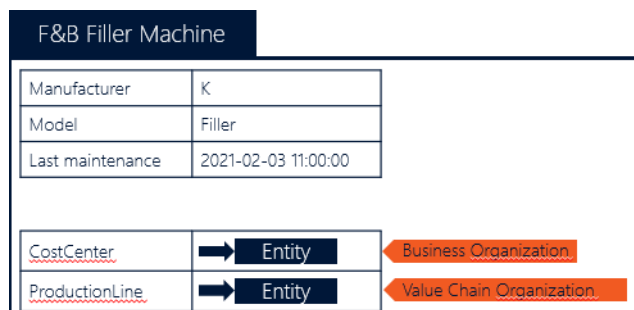
- ▶ Must be unique in the inheritance tree of the **Type**
- ▶ Must not be identical to the name of an **Attribute**

Further components for the definition of an **Association** are:

- ▶ **Target Type**: associated **Type**
- ▶ **Multiplizität**: Can be present in the form  $N$  (as many as desired) or *ZeroOrOne* (zero or one). A distinction is made between two types:
  - ▶ **Source** multiplicity: Denotes how many instances of the **Source Type** can be linked for this **Association**.
  - ▶ **Target** multiplicity: Denotes how many instances of the **Target Type** can be linked for this **Association**.

### 10.2.4 TAGs

**Attribute TAGs** and **Association TAGs** add additional information to the definitions of **Attributes** and **Associations**. These **TAGs** are configured within a **Construction Kit Library**. Defined TAGs are available for the definition of **Attributes** and **Associations**. They serve to categorize and classify **Attributes** and **Associations**.



Example of a **Type** with the **Associations** "Cost Center" and "Production Line" and the assigned **Association TAGs** "Business Organization" and "Value Chain Organization".

## 10.3 Tenants

A **Tenant** (mandant) is a logical separation (instance) of all the data that concerns Data Modeling. It comprises all metadata and data of a **Construction Kit**.

The following is applicable here:

- ▶ Each instance of the **Data Modeling Service** supports several Tenants.
- ▶ The default Tenant "*zenon*" is created during initialization.
- ▶ Each Tenant contains its own **Construction Kit**.

## 10.4 Data access

For program access to Data Modeling data, COPA-DATA provides a GraphQL interface. GraphQL is a language for data queries and data manipulation. You can find details in relation to this in the freely-available open-source documentation.

The **GraphQL Editor** (on page 137) in the Data Modeling service offers a simple graphical possibility to detect the **GraphQL** scheme, and to query and to change data.

## 10.5 Configuration and display

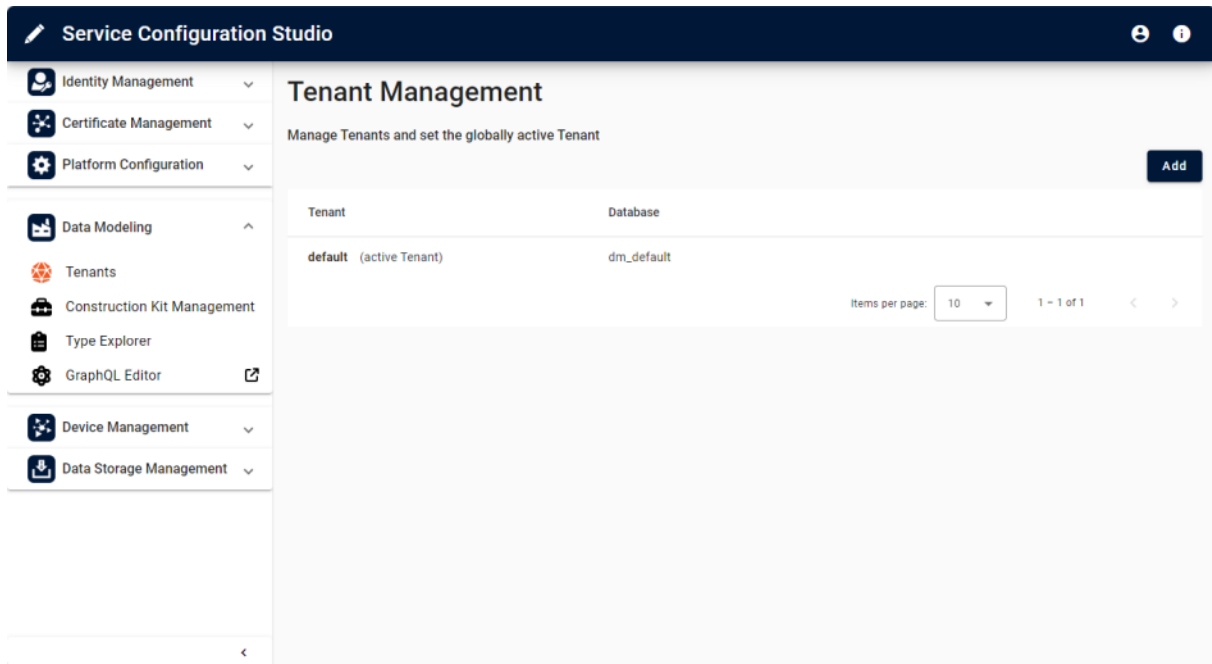
Data Modeling is configured and queried in Service Configuration Studio.

**Note:** Activate your license before configuration in Service Configuration Studio.

### To configure and use Data Modeling:

1. Open the Service Configuration Studio.
2. Click on the **Data Modeling** entry.
3. Open the desired tab:
  - ▶ **Tenants:** Creation and administration of the tenants.
  - ▶ **Construction Kit Management:** Administration of **Construction Kit Libraries**.
  - ▶ **Type Explorer:** Overview of all **Types** of installed **Construction Kit Libraries**.

- ▶ **GraphQL Editor:** Starts the **GraphQL Editor** (on page 137).



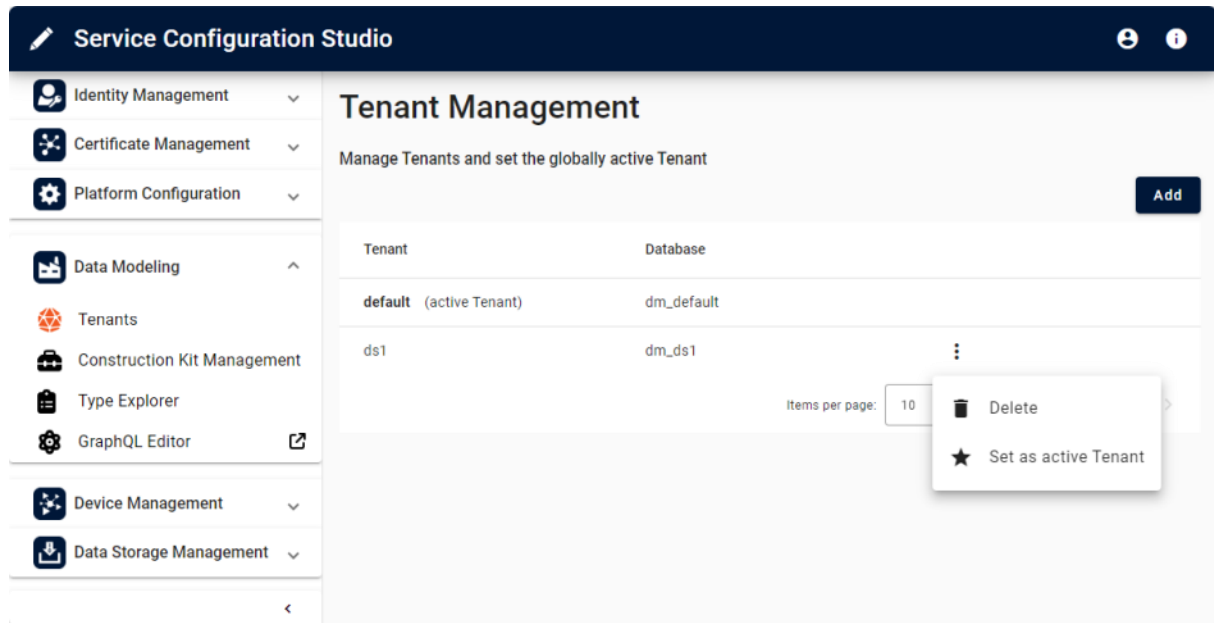
## 10.5.1 Tenants

You administer and configure **Tenants** here. A **Tenant** (mandant) is a logical separation (instance) of all the data that concerns Data Modeling. It comprises all metadata and data in a **Construction Kit**.

Each instance of the **Data Modeling Service** supports several **Tenants**. The **Tenant "zenon"**, created by the system and available from the start, is used by default by all applications that access Data Modeling.

**Recommendation:** Use the default **Tenant** in the current version.

The selected (active) **Tenant** determines the **Tenant** in which all operations in the user interface of Data Modeling take place.



## CREATE TENANT

### To create a Tenant:

1. Click on the **Add** button.  
The dialog to enter the ID is displayed.
2. Enter the desired **Tenant ID**.  
Rules:
  - ▶ Must start with a letter.
  - ▶ Must only contain letters and numbers.
  - ▶ Maximum length 50 characters.
3. Click on the **Save** button.
4. The new **Tenant** is saved and displayed.

## ADMINISTER TENANT

### To administer a Tenant:

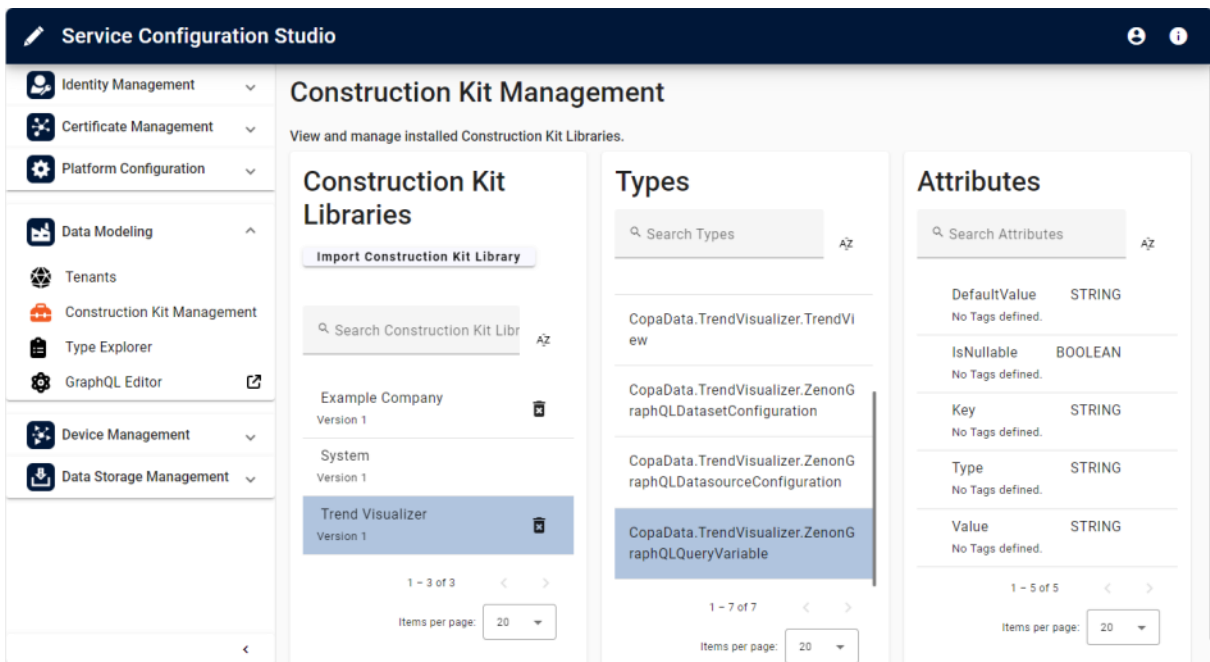
1. Click on the **Tenant**.
2. Click on the button with the three dots. This is only available for **Tenants** that are not active.  
The context menu is displayed.



3. Select the desired action:
  - ▶ **Delete:** The **Tenant** is deleted from the system.
  - ▶ **Set as active tenant:** The **Tenant** is set as an active **Tenant**. It is always only one **Tenant** that can take on this role.

## 10.5.2 Construction Kit Management

You manage your **Construction Kit Libraries** for the selected **Tenant** in this tab. Display of the **Types** and **Attributes** of the selected **Construction Kit Library**.



### CONSTRUCTION KIT LIBRARY MANAGEMENT DIALOG

Administration and display of the installed **Construction Kit Libraries**.

Column	Description
<b>Construction Kit Libraries</b>	Display of the installed <b>Construction Kit Libraries</b> . You can filter, sort, add and remove them.  For details, see the <b>Administer Construction Kit Libraries</b> section.
<b>Types</b>	Shows all <b>Types</b> that are present in the selected <b>Construction Kit Library</b> .

Column	Description
<b>Attributes</b>	Shows all <b>Attributes</b> that have been configured in the selected <b>Type</b> .

## MANAGE CONSTRUCTION KIT LIBRARIES

You can filter, sort, add and remove **Construction Kit Libraries**.

### FILTERING AND SORTING

To filter the display:

- ▶ Enter the desired term in the text field.

To sort the display:

- ▶ Click on the **AZ** symbol.

### ADD CONSTRUCTION KIT LIBRARY

#### To add a Construction Kit Library:

1. Click on the **Import Construction Kit Library** button.  
This opens the import field.
2. Drag the desired library onto the target field.  
Or click on the field and select the desired file from the file dialog.
3. Click on the **Import** button.

### REMOVE CONSTRUCTION KIT LIBRARY

Construction Kit Libraries can also be removed. You can either delete all existing versions of a **CKL** or just the selected version.

#### To remove a Construction Kit Library:

1. Select the desired **Library**.  
Only **CKLs** that are not based on further **CKLs** can be removed.
2. Click on the Trashcan symbol.  
The **Remove Construction Kit Library** dialog is opened.
3. Select which data is to be removed:
  - a) **Remove instances of types uniquely defined by this Construction Kit Library version:**  
Removes only this version of the selected **CKL**.
  - b) **Remove all versions:** Removes all versions of the selected **CKL**.

- Click on the **Remove** button.

The Construction Kit Library is removed. When deleting, all data that has been saved in this **CKL** is removed.

**Attention:** The removal of a **Construction Kit Library** is a significant action. The scheme of the **Construction Kit Library** and all data contained in this scheme is deleted irreversibly.

### 10.5.3 Type Explorer

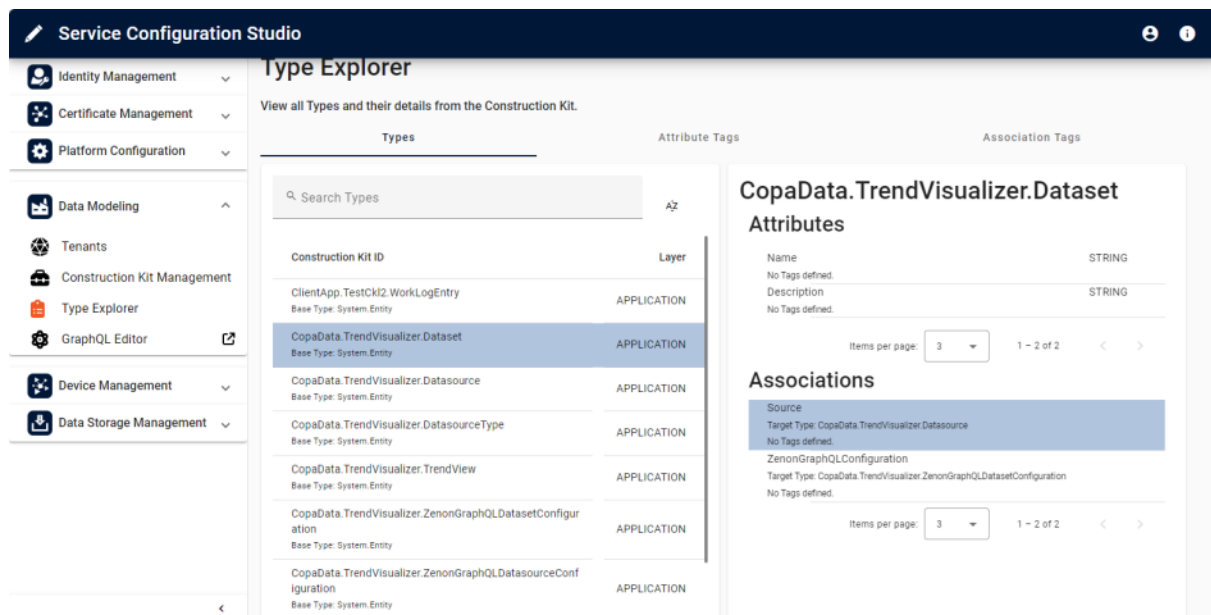
View of the **Types** and their details for all installed **Construction Kit Libraries** of the selected **Tenant**. Details are shown for:

- ▶ **Types**
- ▶ **Attribute Tags**
- ▶ **Association Tags**

The display can be filtered and sorted alphabetically.

## TYPES

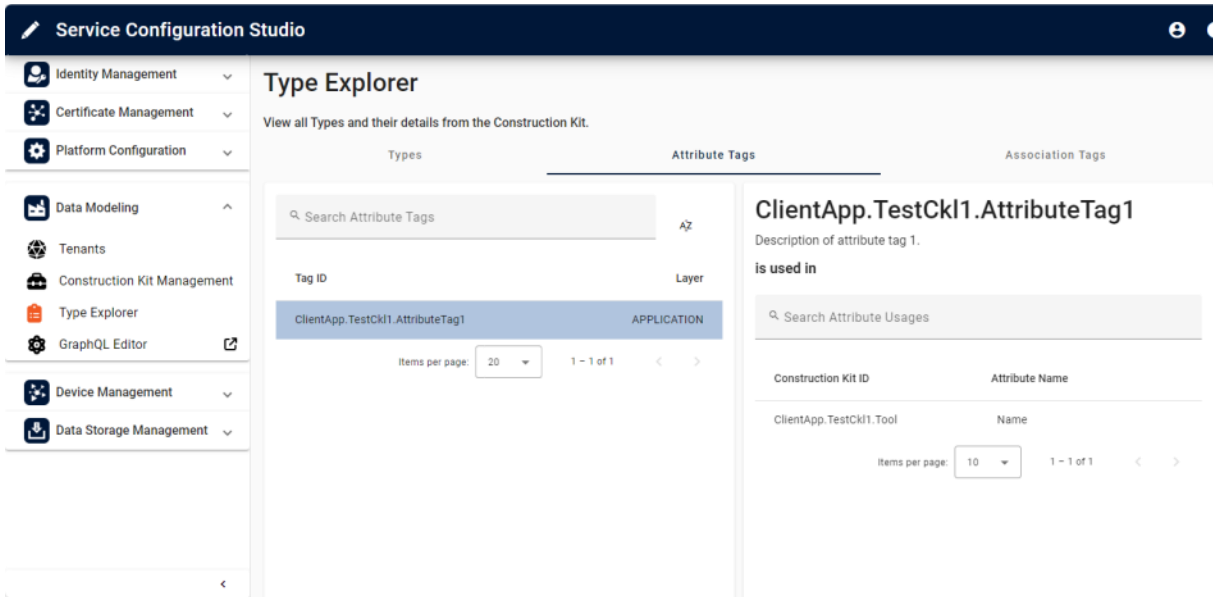
Display of all **Types** and the attendant linked **Attributes** and **Associations**.



Select a **Type** in order to display the respective linked **Attributes** and **Associations**.

## ATTRIBUTE TAGS

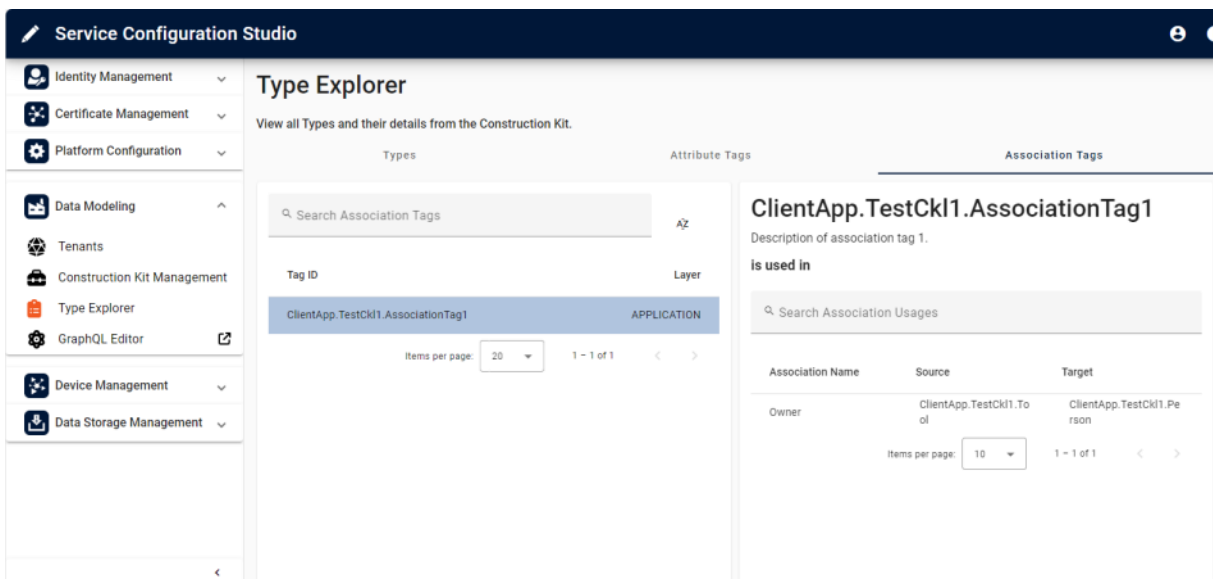
Overview of where **Attribute Tags** are used.



Select an **Attribute Tag** in order to display where it is used.

## ASSOCIATION TAGS

Overview of where **Association Tags** are used.



Select an **Association Tag** in order to display where it is used.

## 10.5.4 GraphQL Editor

Click on the tab to start the **GraphQL Playground** for the **GraphQL Editor** for the selected **Tenant** in a new window or a new tab.

Queries, **Mutations** and **Subscriptions** can be created with the editor.

A **GraphQL scheme** contains **Queries** and **Mutations** for all **Types** and metadata of the **Construction Kit**. The **GraphQL scheme** can be viewed using the **GraphQL Editor**. In the **GraphQL Editor**, you can find the accompanying **GraphQL scheme** documentation in **Docs** on the right border.



### Information

the **GraphQL Editor** corresponds to the **GraphQL Interface** of the Report Engine in terms of appearance and design of the user interface. However, both differ in their functionality. Both use a **GraphQL Playground**.

## 10.6 Trend Visualizer

IIoT Services enables the deployment of a **Trend Visualizer**.

The **Trend Visualizer** can be deployed by means of a Docker image or Kubernetes/Helm. An example for **Trend Visualizer** is available via **/trend-visualizer** at the IIoT Services URL.

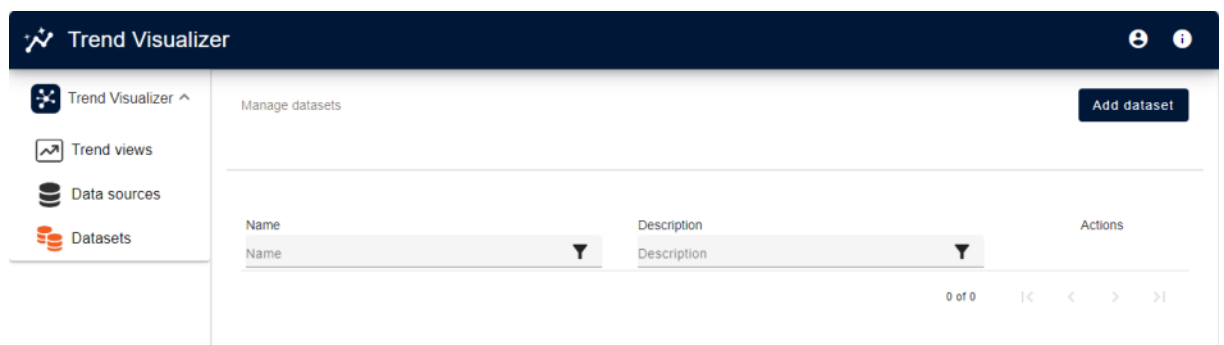
It is configured and displayed in IIoT Services.

The **Trend Visualizer** consists of:

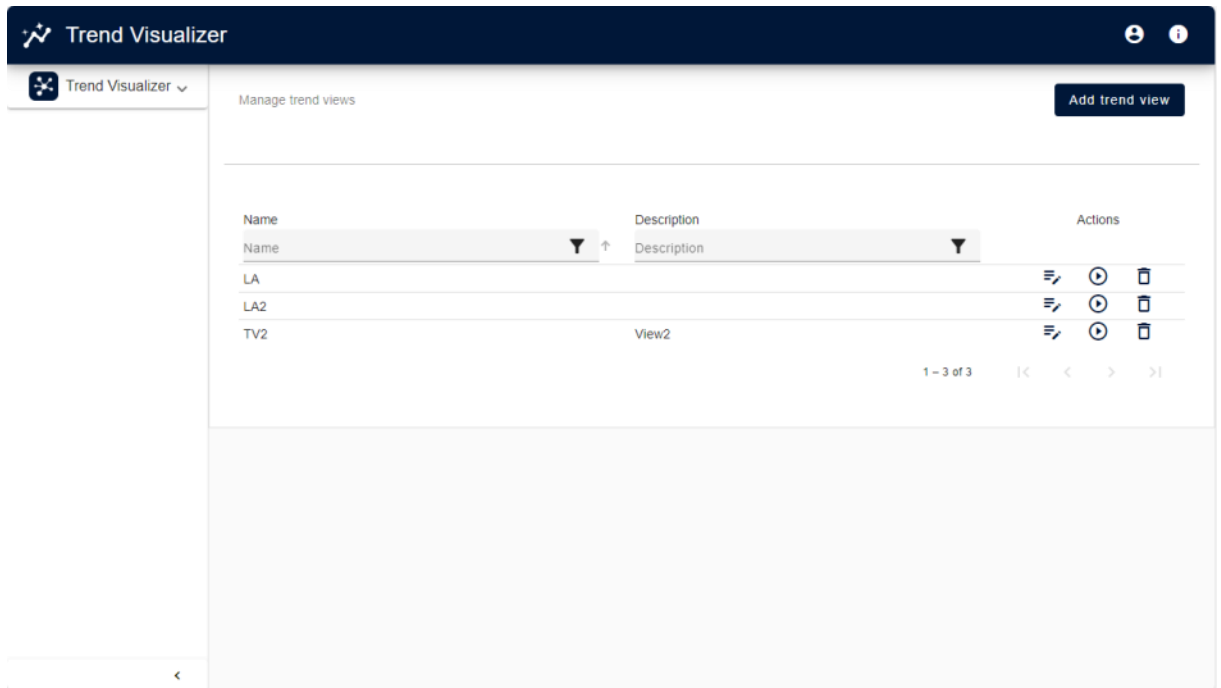
- ▶ **Trend views (start page)**
- ▶ **Data sources**
- ▶ **Datasets**

### START PAGE

- ▶ A dataset can be configured (on page 146) if there is not one present already.

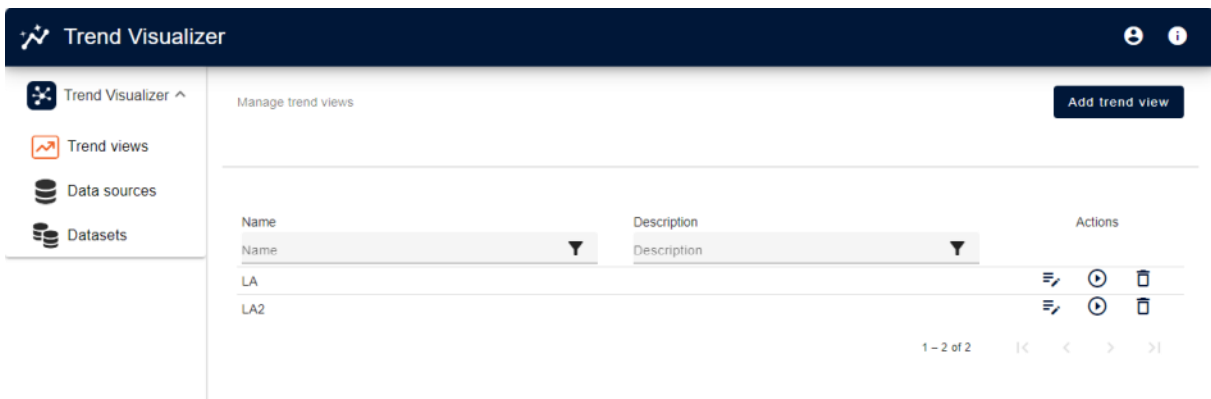


- ▶ A view (on page 138) can be configured if there is a dataset present.



### 10.6.1 Trend views

Display of trends.



Object	Description
Tabs	Creation and editing of <b>Trend views</b> and configuration of the data sources and data sets.
<b>Manage trend views</b>	Display of the configured trends.  You can do the following with each <b>Trend view</b> in the list via the symbols:

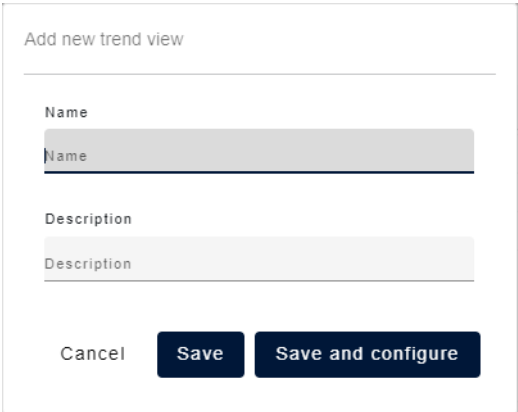
Object	Description
	<ul style="list-style-type: none"><li>▶ Edit</li><li>▶ View</li><li>▶ Delete</li></ul>
<b>Add trend view</b>	Opens the dialog to add a <b>Trend view</b> .

### ADD TREND

To add a trend:

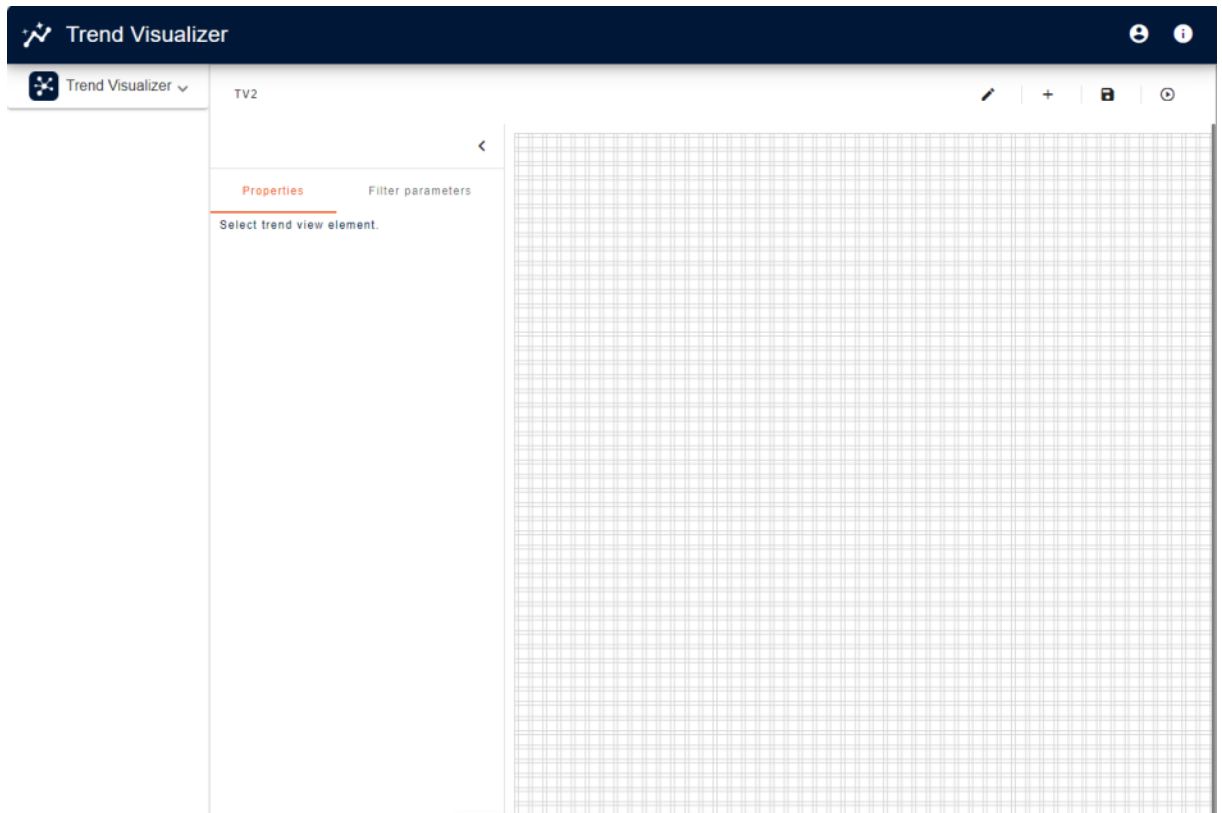
1. Click on the **Add trend view** button.

The dialog to add it is opened.



The dialog box is titled "Add new trend view". It features two input fields: "Name" and "Description". Below these fields are three buttons: "Cancel", "Save", and "Save and configure".

2. Configure the name and supplementary text.



3. Save the **Trend view** by clicking on **Save** or open the configuration by clicking on the **Save and configure** button.

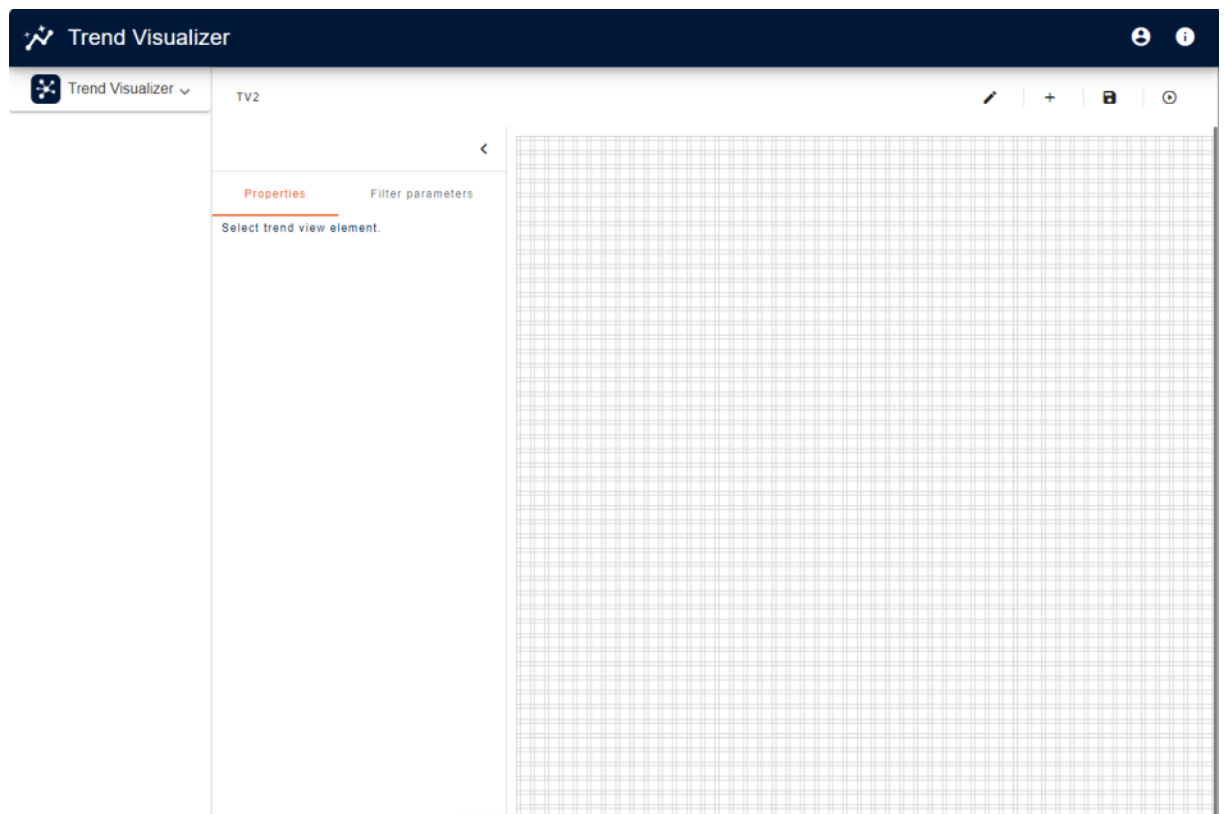
### 10.6.1.1 Configuration

Configure **Trend views**.

1. Open the dialog via the button on the start page or the **Trend views** tab.
2. Give it a name and add supplementary text.
3. Click on **Save and configure**.



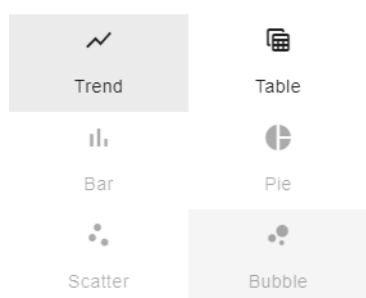
The content area is opened.



### Symbols:

- ▶ **Pen:** Enables the editing of the name and the supplementary text.
  - ▶ **+:** Opens the dialog to add an object.
  - ▶ **Disk:** Saves the **Trend view**.
  - ▶ **>:** Shows the configured **Trend view**.
4. Open the dialog to add an object by clicking on **+**.

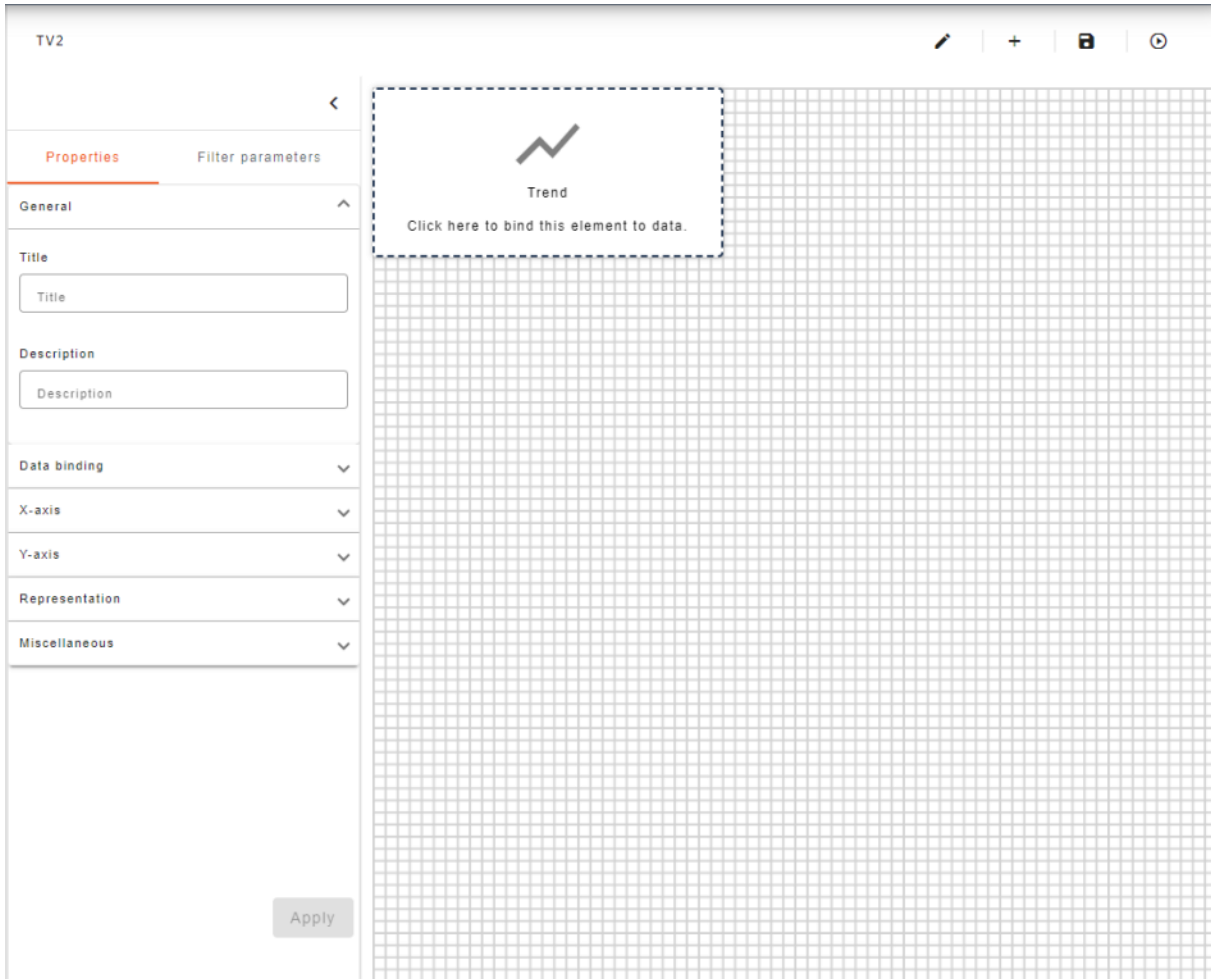
The selection dialog is opened.



5. Select the object to be configured from the dialog.
6. Configure the selected object.

## TREND CONFIGURATION

Configure the trend.

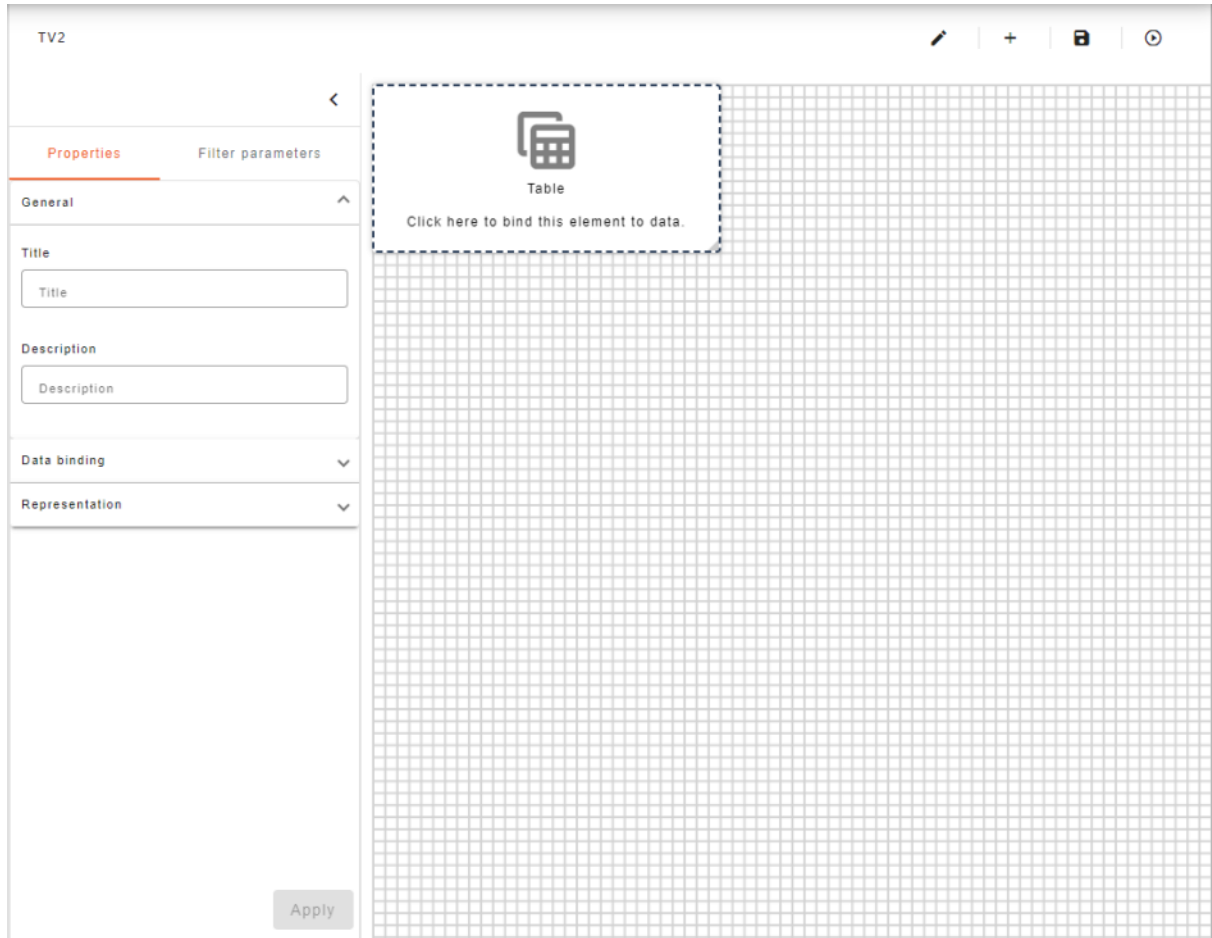


1. Give it a title and supplementary text.
2. Configure the data source.
3. Configure the dataset.
4. Configure the display of the X-axis.
5. Configure the display of the Y-axis.
6. Configure the type of display of the trend.
7. Configure the display of tool tips and highlighting.
8. Click on **Apply**.
9. Configure the filter.

Click on **Apply**.

## TABLE CONFIGURATION

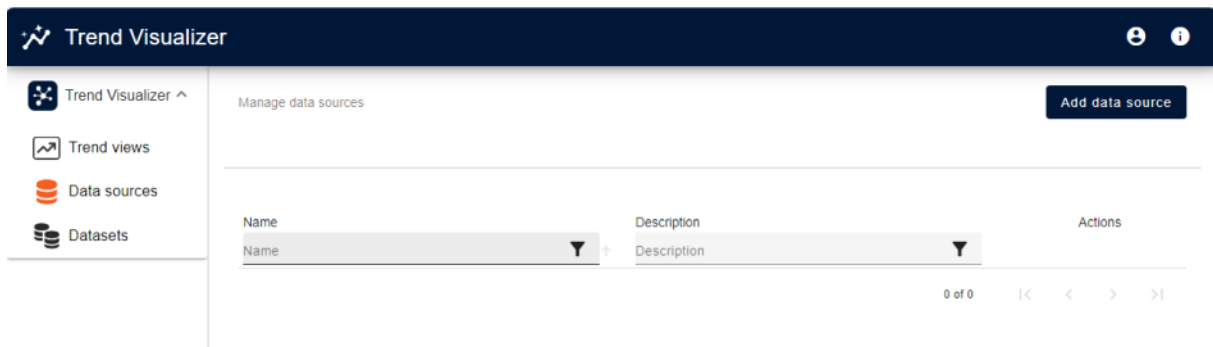
Configure the table.



1. Give it a title and supplementary text.
2. Configure the data source.
3. Configure the dataset.
4. Configure the type of display for the table:
  - a) Column filter
  - b) Column sorting
5. Click on **Apply**.
6. Configure the filter.
7. Click on **Apply**.

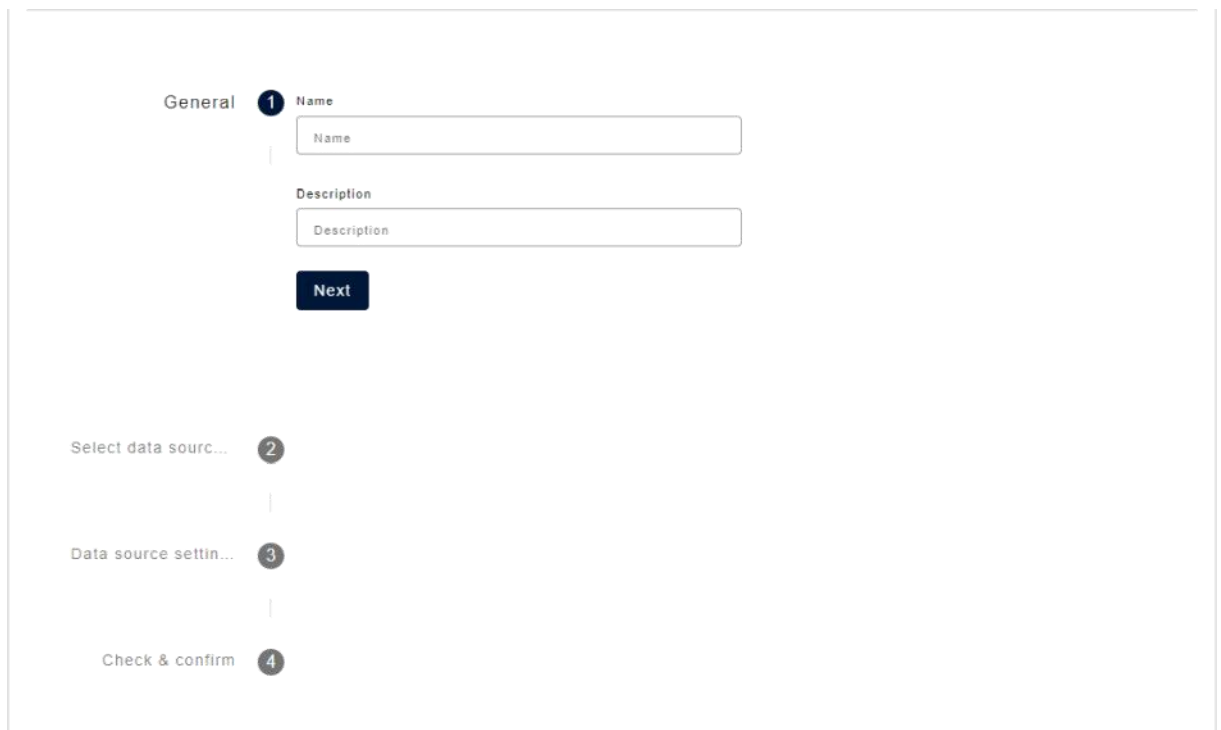
## 10.6.2 Data sources

To add data sources, click on the **Add data source** button.



### Configure:

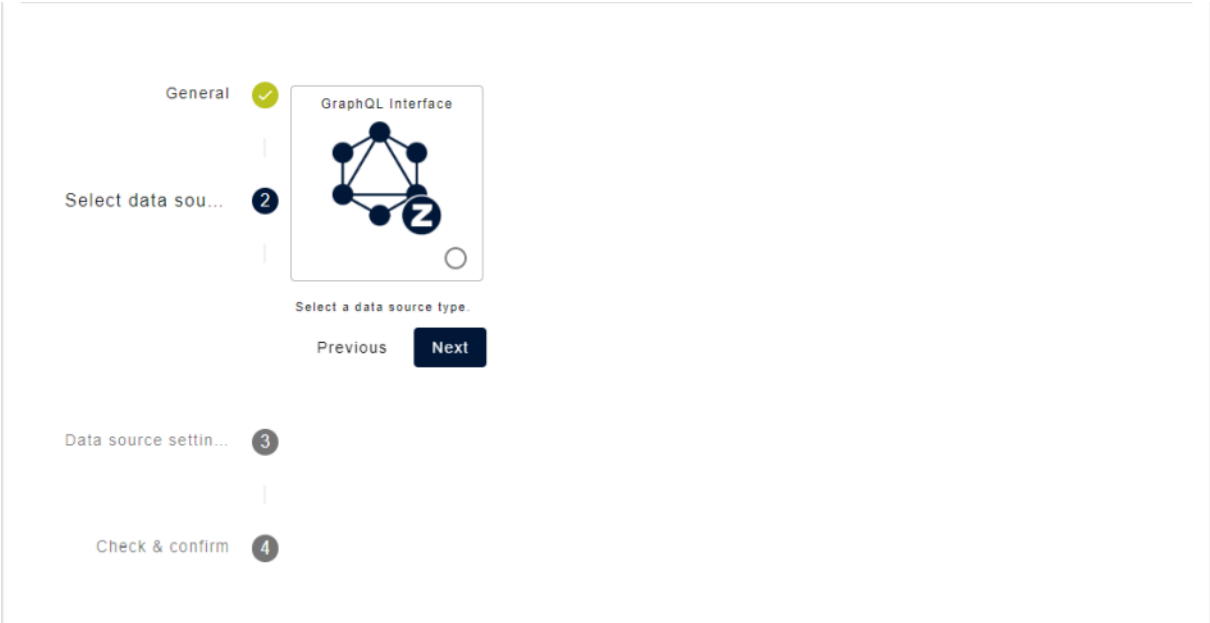
1. Name and description



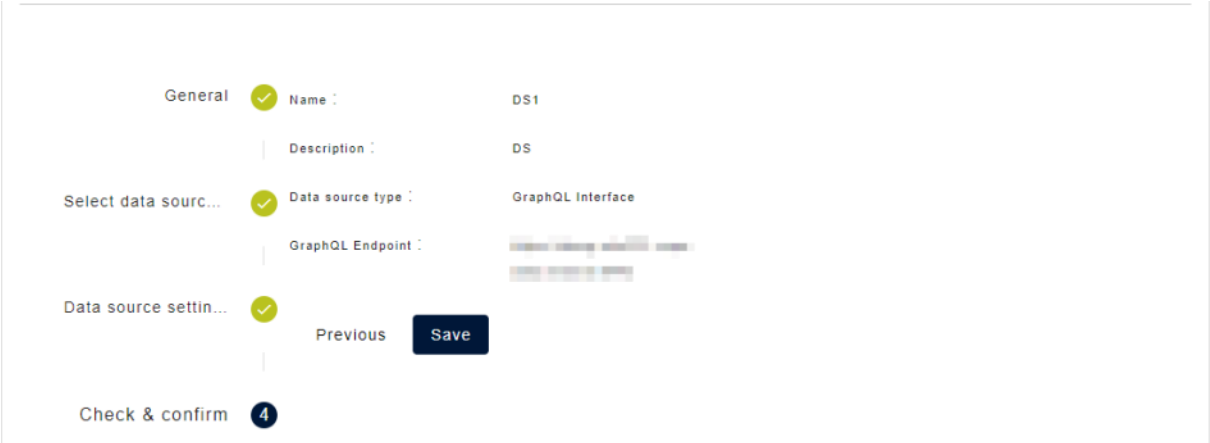
The configuration process is shown as a vertical sequence of four steps:

- General** (Step 1): Includes input fields for 'Name' and 'Description', and a 'Next' button.
- Select data source...** (Step 2): A selection step.
- Data source settin...** (Step 3): A settings step.
- Check & confirm** (Step 4): A final confirmation step.

2. Data source



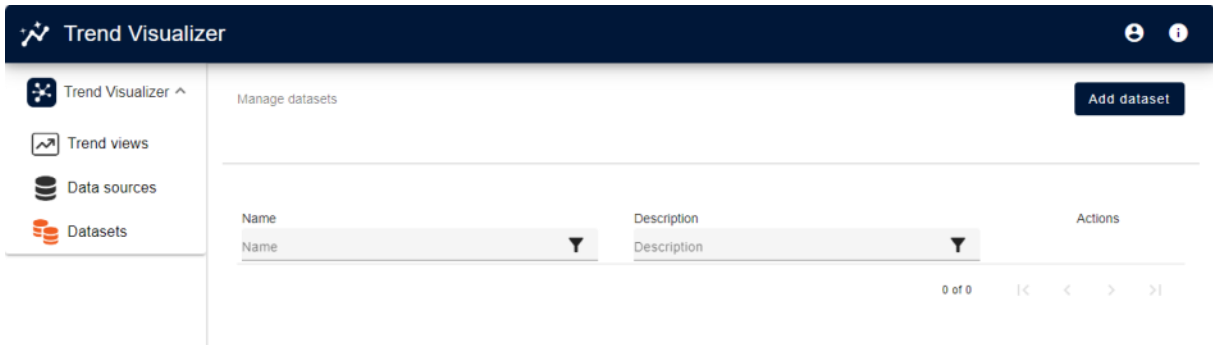
3. GraphQL Endpoint



Save the configuration.

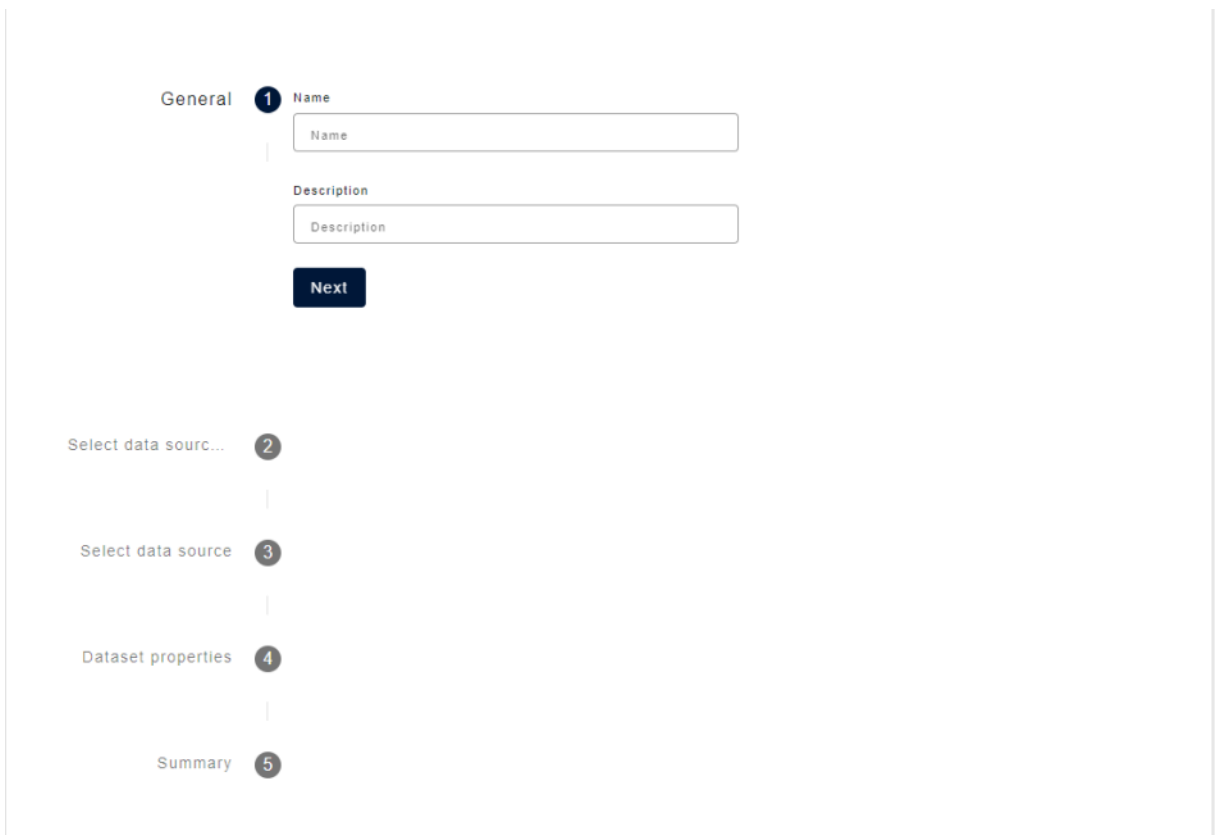
### 10.6.3 Datasets

To add a dataset, click on the **Add dataset** button.

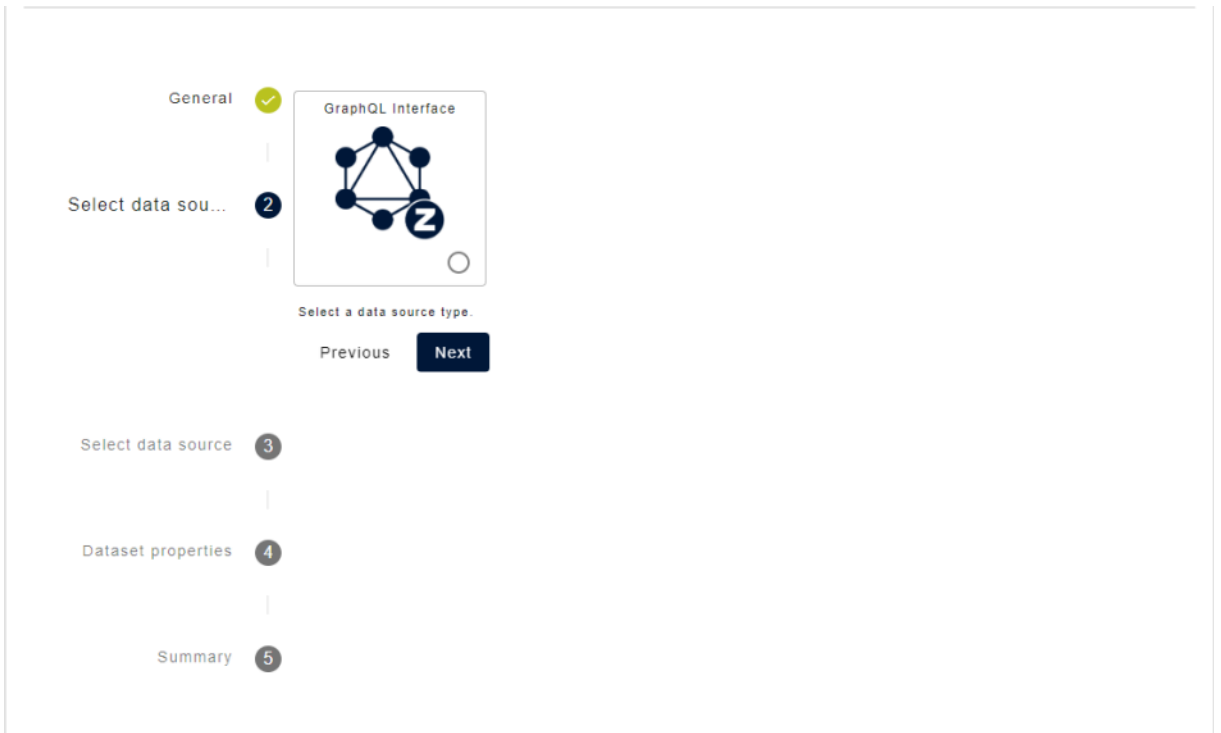


**Configure:**

1. Name and description



2. Data source



General

Select data source type **2**

GraphQL Interface

Select a data source type.

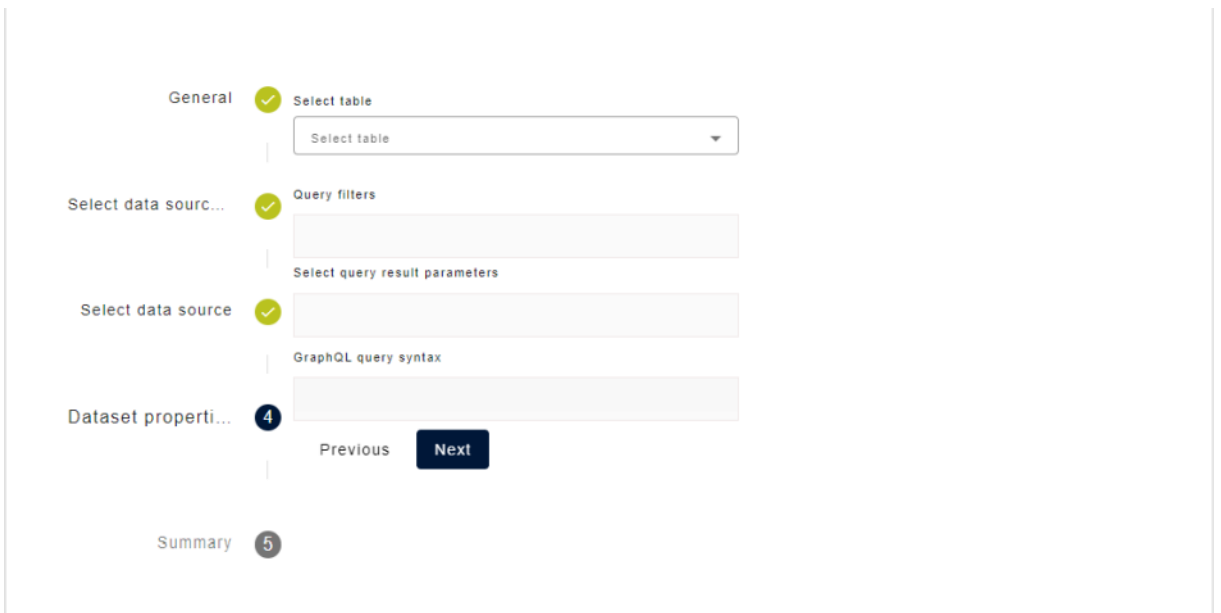
Previous Next

Select data source **3**

Dataset properties **4**

Summary **5**

3. Table, filter, TAG and GraphQL query syntax



General

Select table

Select table

Select data source type

Query filters

Select query result parameters

Select data source

GraphQL query syntax

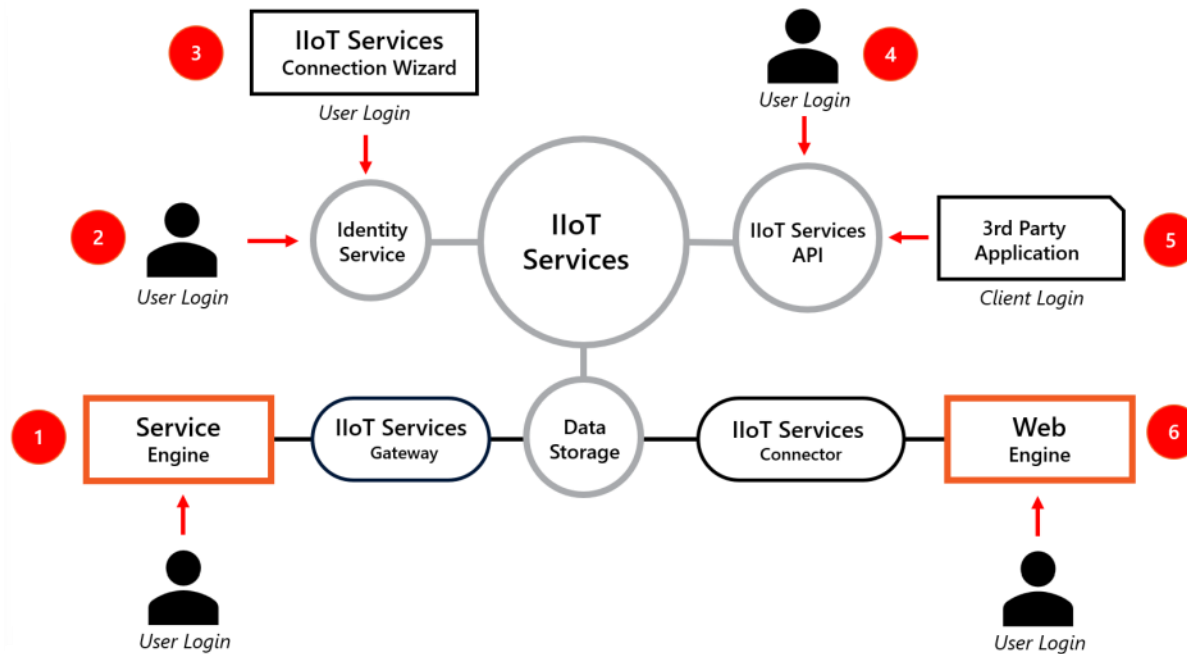
Dataset properties **4**

Previous Next

Summary **5**

Save the configuration.

## 11 Identity Service: Central authentication service



The Identity Service supports client/user logins for IIoT Services and applications connected with it.

The **Identity Service** is the central authentication service of IIoT Services. In addition, **Identity Service** also supports the authentication of selected zenon applications as well as 3rd party applications.





 **Information**

Login is via web browser, **HTML Web Engine** or in Service Engine with a **IDS Login** screen.

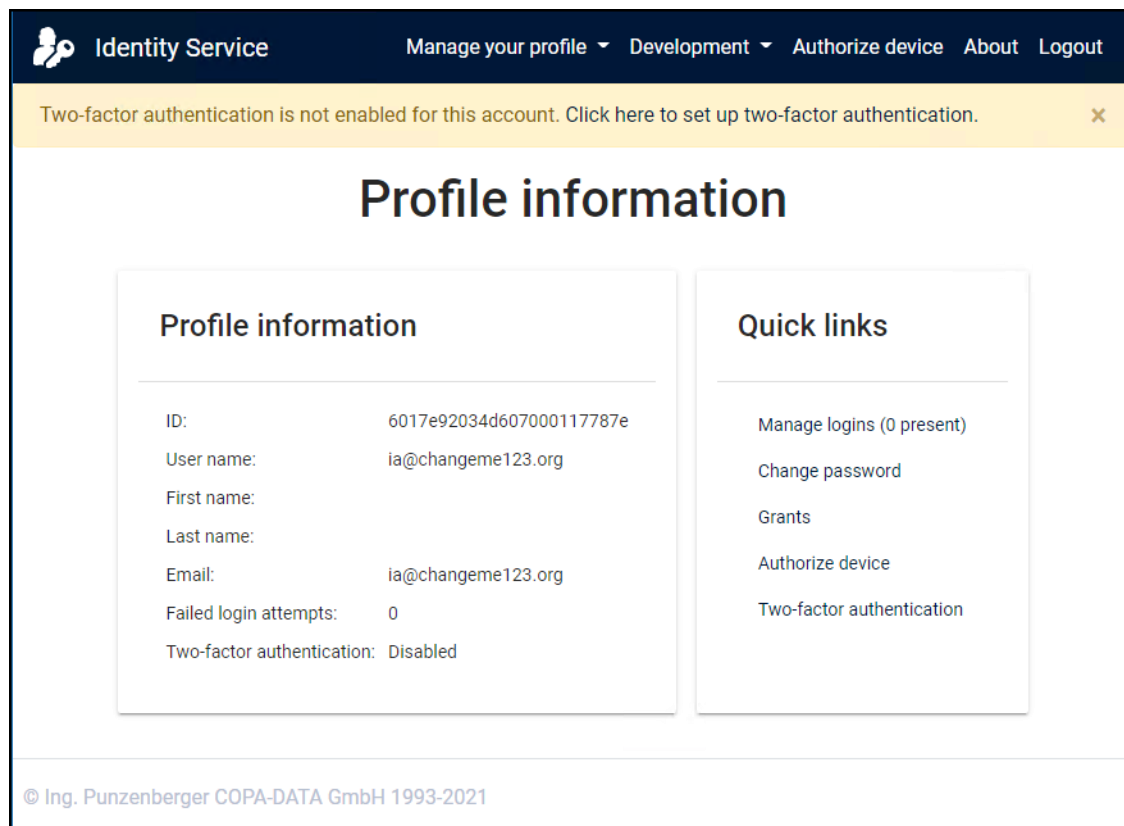
## 11.1 External identity providers

**Identity Service** supports the integration of external identity providers such as RADIUS or Azure AD.

Please note the following when using external identity providers:

- ▶ There are functional differences between the various providers. You can find more detailed information on this in the **Identity providers (for external logins)** (on page 207) node.
- ▶ Service Engine has more restrictive requirements on user names than **Identity Service**. You can find detailed information on this in the **IIoT Services - configuration in Engineering Studio** (on page 307) node in the **Compatibility table:** (on page 316) node **User names** (on page 316).

## 11.2 Identity Service



The screenshot shows the 'Identity Service' user profile page. At the top, there is a navigation bar with 'Identity Service' and links for 'Manage your profile', 'Development', 'Authorize device', 'About', and 'Logout'. A yellow banner below the navigation bar states: 'Two-factor authentication is not enabled for this account. Click here to set up two-factor authentication.' The main content area is titled 'Profile information' and is divided into two columns. The left column, 'Profile information', lists user details: ID (6017e92034d607000117787e), User name (ia@changeme123.org), First name, Last name, Email (ia@changeme123.org), Failed login attempts (0), and Two-factor authentication (Disabled). The right column, 'Quick links', contains links for 'Manage logins (0 present)', 'Change password', 'Grants', 'Authorize device', and 'Two-factor authentication'. At the bottom of the page, there is a copyright notice: '© Ing. Punzenberger COPA-DATA GmbH 1993-2021'.

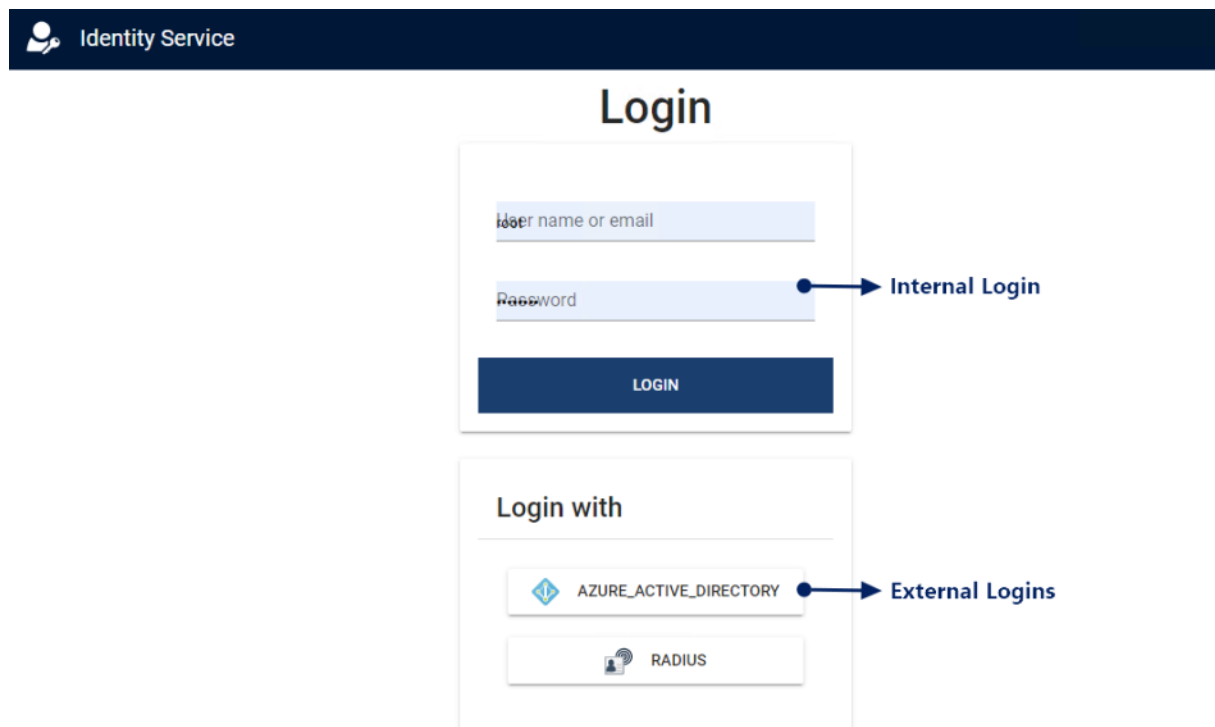
With the Identity Service in Service Configuration Studio, every logged-in user can change settings for their own account.

The **Identity Service** is the service for the central authentication of users and applications in IIoT Services.

The **Identity Service** in Service Configuration Studio supports the following functionality:

- ▶ Every user of IIoT Services can log in.
- ▶ Every user can make basic settings **for their own user account**.

## 11.2.1 Login



The screenshot shows the 'Identity Service' login interface. At the top, there is a dark blue header with the 'Identity Service' logo and name. Below the header, the main content area is titled 'Login'. It contains two main sections. The first section is for internal login, featuring a 'User name or email' input field, a 'Password' input field, and a 'LOGIN' button. An arrow points from the 'Internal Login' label to the 'Password' field. The second section is titled 'Login with' and contains two options: 'AZURE\_ACTIVE\_DIRECTORY' and 'RADIUS'. An arrow points from the 'External Logins' label to the 'AZURE\_ACTIVE\_DIRECTORY' option.

By default, users log in via an internal login in the Identity Service in Service Configuration Studio. You can also optionally configure the connection with external logins.

Users can use the login in the web interface of **Identity Service** to centrally authenticate themselves for all web interfaces of IIoT Services.

A distinction needs to be made between the login options:

- ▶ Internal login: Direct log in to a user account in **Identity Service**.
- ▶ External logins: Log in via an external **Identity Provider**.

Each time users log in, they can choose between all login options with which their user account in **Identity Service** is linked at the time of logging in. The differences between internal login and external login are documented separately (on page 154).

## PLATFORM USER FOR ZENON

You can use the user authentication via **Identity Service** not only for IIoT Services but also for other services of the zenon software platform. You can find details in relation to this in the **Identity Service: central authentication service** (on page 148) section.

### ⚠ Attention

#### Lock after failed logins

Five consecutive failed attempts to log in to a user account will result in **Identity Service** blocking the respective user account for security reasons.

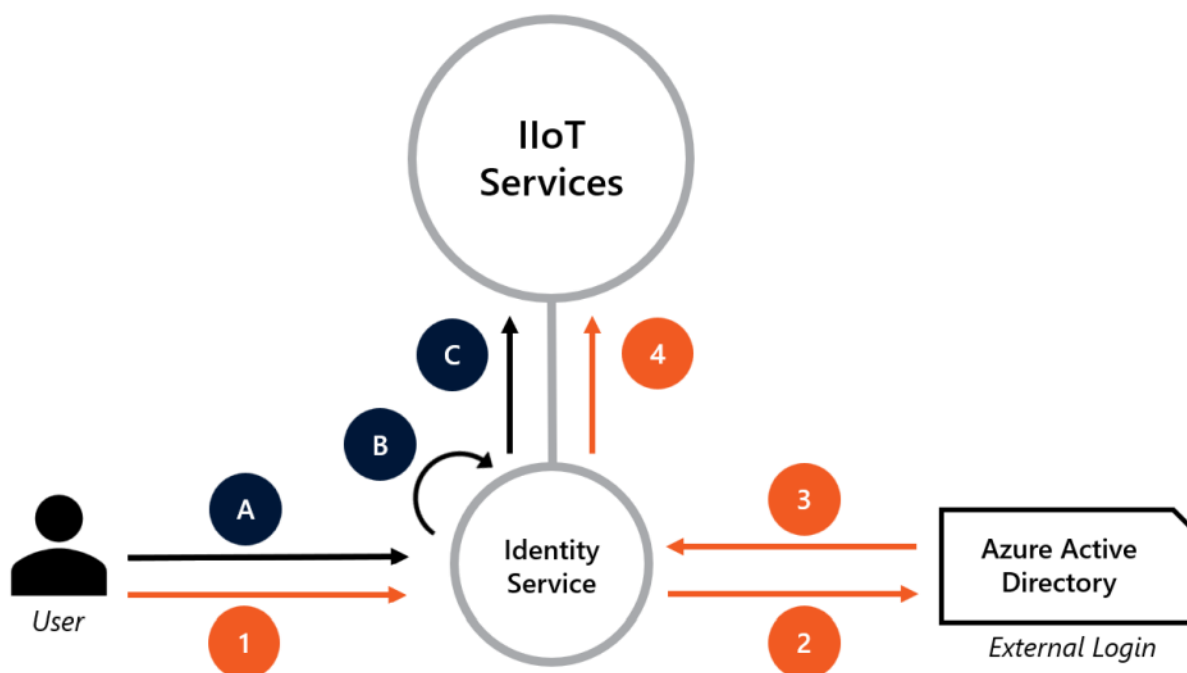
Each failed attempt to log in will be counted. The block is only temporary.

#### Attempts to log in include for example:

- ▶ Entering a password
- ▶ Two-factor authentication via an authenticator app
- ▶ Entering a recovery code for two-factor authentication

The temporary block of a user account lasts 5 minutes. After this time has elapsed, it is possible to log in again.

### 11.2.1.1 Logins: Internal vs. External



In the case of internal login (A,B,C), users log in directly to Identity Service. In the case of external login (1,2,3,4), users log in to Identity Service via an external identity provider.

**Identity Service** supports several user login options. The table below contains definitions and short names of the different login options.

Short name	Description	Administration
<p><b>Internal login</b></p>	<p>Direct login to <b>Identity Service</b> (without external login).</p> <p>The integrated user administration of <b>Identity Service</b> verifies the user’s login credentials.</p> <p>This is the default setting in <b>Identity Service</b>.</p>	<p>In Service Configuration Studio in the <b>Identity Management</b> node via the following menu item:</p> <ul style="list-style-type: none"> <li>▶ <b>Users</b></li> </ul> <p>These are the <b>internal user accounts</b> of <b>Identity Service</b>.</p> <p><b>Note:</b> Each external login is assigned an internal user account. These assigned user accounts are also displayed here.</p>
<p><b>External login</b></p>	<p>Log in to <b>Identity Service</b> via an external login.</p> <p>An external <b>Identity Provider</b> (for instance, <b>Azure Active Directory</b>) verifies the user’s login credentials for <b>Identity Service</b>.</p> <p>External logins must be configured manually.</p>	<p>Using the administration tools of the respective <b>Identity Provider</b>.</p> <p><b>Example:</b> User accounts in <b>Azure Active Directory</b> are administered via the <b>Azure Portal</b>.</p> <p>From the point of view of <b>Identity Service</b>, these are <b>external user accounts</b>.</p>
<p><b>Login</b></p>	<p>If the login to <b>Identity Service</b> is not specified further, it always refers to both options (<b>internal login</b> and <b>external login</b>).</p>	<p>See specific logins.</p>

**Hint:**

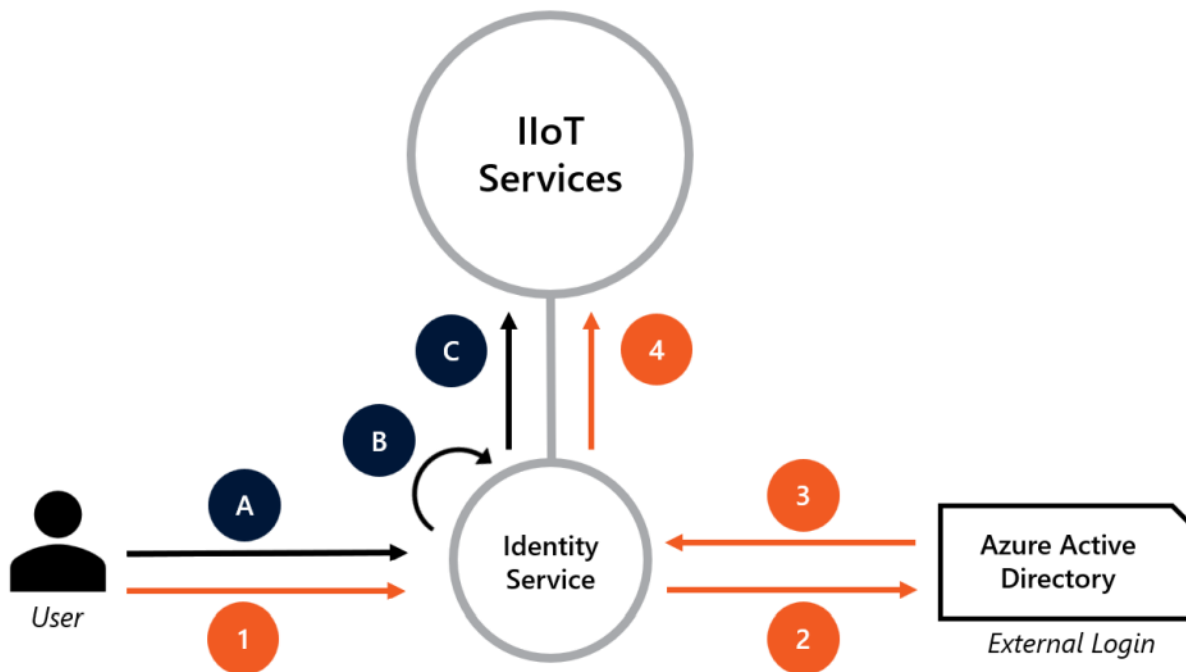
**Login processes in detail**

The login processes to **Identity Service** are documented in detail for each login option:

- ▶ External login (on page 207): Login via external identity provider (for instance, Microsoft Active Directory)
- ▶ Internal login (on page 175): Direct login (without external login)

Each time users log in, they can choose between all login options with which their user account in **Identity Service** is linked at the time of logging in.

**11.2.1.2 External login**



Every user that logs in via an external login (1,2,3,4) can alternatively also log in via an internal login (A,B,C) to Identity Service.

Logging in to the web interface of **Identity Service** with the user account of an external **Identity Provider** requires that the **external user account** is linked with an **internal user account**. There are two possibilities when using **External logins**.

- ▶ The user already has an account in the Identity Service:  
The user can **manually** link their internal user account with **External logins** (on page 160). External logins are provided by the Administrator.
- ▶ The user does not have an account in Identity Service yet:  
An internal user is **automatically** created and linked in **Identity Service** when logging in via an external **Identity Provider** for the first time. The user can only log in by default via **External login** with the user's login credentials. However, users can use **Change password** in **Identity Service** at any time to create access themselves for logging in directly to **Identity Service**.

Every user who logs in via an external login can alternatively log in via an internal login (or create this access themselves at any time).

### Attention

#### External login: Correct way to block user access

To block a user account for an **external login** for **Identity Service**, you must deactivate the user account in **Identity Management**.

It is not enough just to deactivate the account via the external **Identity Provider**.

### 11.2.1.3 User login via external login

Carry out the following steps to log in to an external provider:

1. Open the login page in the **Identity Service**.  
To do this, enter the corresponding URL in a web browser:  
For example `https://mycomputer.testenv.local:9443/identity-service/`
2. Click on the button of the desired identity provider.
3. You will then be redirected in the web interface to the login page of the external identity provider.  
**Note:** The method of redirection depends on the identity provider selected (see the table).
4. Authenticate yourself by entering your user credentials.
5. You are sent back to **Identity Service**.

### REDIRECTION FOR EXTERNAL LOGINS

The type of forwarding on login and the entry of user credentials depends on the respective identity provider.

Identity provider	Redirection	User credentials
<b>Azure Active Directory</b>	To external website of <b>Azure Active Directory</b> : <i>https://login.microsoftonline.com</i>	Input to an external web page of the identity provider.
<b>Microsoft Active Directory</b>	To internal website of <b>Identity Service</b> .	Input to an internal web page of the Identity Service.
<b>OpenLDAP</b>	To internal website of <b>Identity Service</b> .	Input to an internal web page of the Identity Service.
<b>RADIUS</b>	To internal website of <b>Identity Service</b> .	Input to an internal web page of the Identity Service.
<b>OpenID Connect</b>	To external website of <b>OpenID Connect</b> : <i>https://myopenidconnect.com</i>	Input to an external web page of the identity provider.
<b>Keycloak</b>	To external website of <b>Keycloak</b> : <i>https://my-keycloak.com/auth/realms/master</i>	Input to an external web page of the identity provider.

## 11.2.2 User role: Identity Administrator

### ROLE DEFINITION

The *Identity Administrator* is the only user role that can log into both the **Identity Service** (as a normal user) and **Identity Management** (as an administrator). This user role can also be assigned to several users. An Identity Administrator can administrate, in **Identity Management**, all settings that concern other **Users**, **Groups**, **Clients** and external **Identity Providers**.

### INITIAL CONFIGURATION

The initial user account in **Identity Service** is automatically assigned the role of *Identity Administrator*.

#### Proceed as follows:

1. Open the web interface for **Identity Service**.
2. If a user has not been defined yet, open an input screen where you can define a user.



3. Enter the desired **User name**.
4. Enter the desired password under **New Password**.  
Important: The password must meet the minimum password requirements.
5. Confirm the selected password under **Confirm new password**.
6. Close the process by clicking on the **Create** button.

You have thus created the initial user account in **Identity Service**.

**Tip**

You can further configure the user account you created in **Identity Management** under **Users**.

There you can also configure the following data fields:

- ▶ **First name**
- ▶ **Last name**
- ▶ **Email**
- ▶ **Description**

You can overwrite existing default settings.

### 11.2.3 Identity Service - user interface

In the web-based interface, information and configurations for the last logged-in user are provided.

#### HEADER

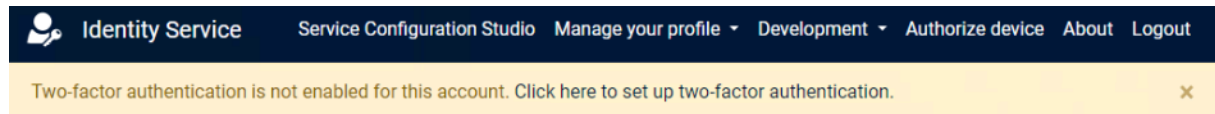


In the header, there are linkings for the administration of functionality of the logged-in user profile for the logged-in user. In addition, under the navigation bar, the activation of **Two-factor authentication** is offered if this has not already been activated.

Option	Description
<b>Service Configuration Studio</b>	Linking to Service Configuration Studio for the administration of all installed IIoT Services.  Login to Service Configuration Studio is carried out with the same user that is already logged in to the Identity Service.

Option	Description
<b>Manage your profile</b> (on page 159)	<p>User interface for the administration of the logged-in user's own user profile.</p> <p>Select from drop-down list:</p> <ul style="list-style-type: none"> <li>▶ <i>Profile information</i> Visualizes the information about the current logged-in user. In addition, links to further configuration options are offered.</li> <li>▶ <i>External logins</i> Shows an overview of the external logins for the logged-in user. In addition, the external logins are visualized with a link.</li> <li>▶ <i>Change password</i> Opens the dialog to change the password for the current logged-in user.</li> <li>▶ Application grants</li> <li>▶ <i>Two-factor authentication</i> Opens the configuration to set parameters for two-factor authentication for the logged-in user.</li> </ul>
<b>Development</b>	<p>Select from drop-down list:</p> <ul style="list-style-type: none"> <li>▶ <i>API documentation</i> Opens the <b>Identity Service</b> API documentation.</li> <li>▶ <i>Diagnostics</i> Opens a view with technical information for the logged-in user.</li> <li>▶ <i>OAuth2 discovery document</i> Opens a new tab in the web browser with information for OAuth authentication.</li> </ul>
<b>Authorize device</b> (on page 173)	<p>Opens the dialog for authentication on devices or software components that do not have a graphical user interface.</p>
<b>About</b>	<p>Shows the license status and the version of <b>Identity Service</b>.</p>
<b>Logout</b>	<p>Logs out the current logged-in user. The login page is displayed in the browser.</p>

## CURRENT STATE OF TWO-FACTOR AUTHENTICATION



This view shows the information under the menu bar if two-factor authentication has been deactivated. Click on the text "Click here to set up two-factor authentication" to activate two-factor authentication and the corresponding configuration is shown.

The display of the notice is deactivated by clicking on the **X** button.

### 11.2.3.1 Manage your profile

In this menu item, the logged in user can manage their own user profile.

#### 11.2.3.1.1 Profile information

Displays information about the user currently logged in

#### PROFILE INFORMATION

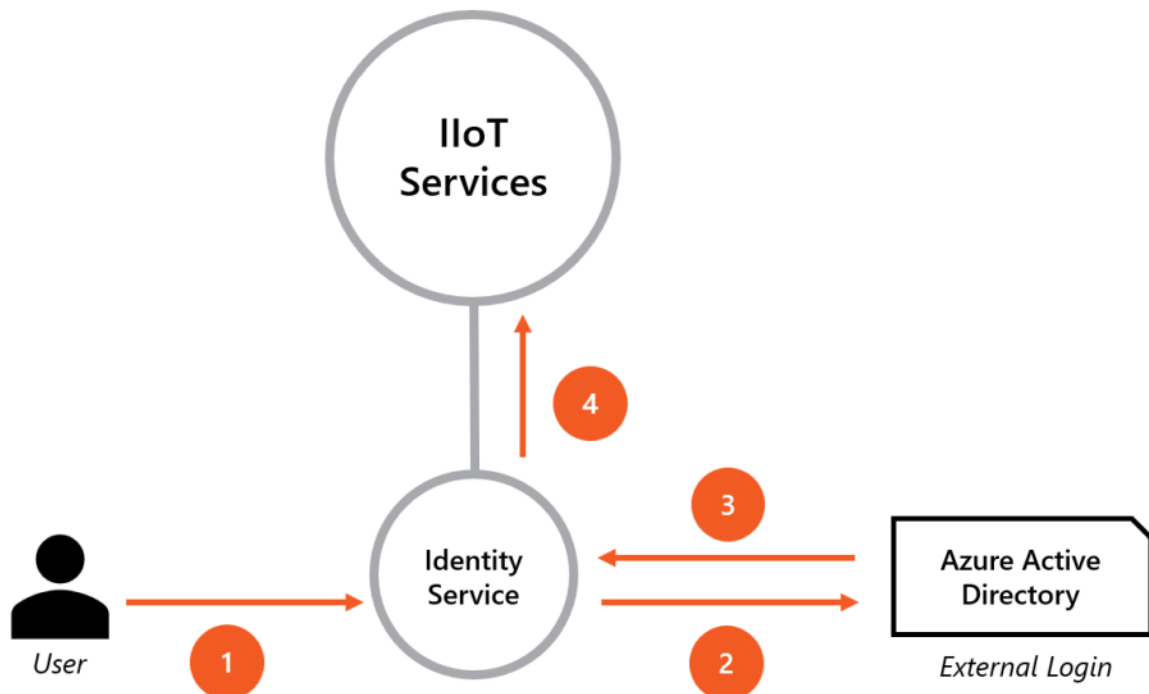
Option	Description
<b>ID</b>	Unique ID of the current logged-in user. This is automatically issued when the user is created.
<b>User name</b>	Configured user name of the logged-in user.
<b>First name</b>	The first name of the user.
<b>Last Name</b>	The last name of the user.
<b>Email</b>	The email address of the user.
<b>Failed login attempts</b>	Number of failed login attempts for the current logged-in user.
<b>Two-factor authentication</b>	Information about the type of two-factor authentication for the logged-in user.

#### QUICK LINKS

Option	Description
<b>Manage logins (n present)</b>	Shows an overview of the external logins for the logged-in user. In addition, the external logins are visualized with a link.

Option	Description
<b>Change password</b>	Opens the dialog to change the password for the current logged-in user.
<b>Grants</b>	
<b>Authorize device</b>	Opens the dialog for the authentication of devices. This is necessary if the authentication of devices is not possible on the client directly.
<b>Two-factor authentication</b>	Opens the configuration to set parameters for two-factor authentication for the logged-in user.

### 11.2.3.1.2 External logins



In the case of external login, users log in to Identity Service via a user account of an external identity provider.

Here users can link their existing user account from **Identity Service** with an external login.

#### EXAMPLE: USE DOMAIN USER ACCOUNT FOR IDENTITY SERVICE

Users already have two different user accounts:

- ▶ A user account in **Identity Service**. Users use this user account to log in to IIoT Services.
- ▶ A domain user account in **Microsoft Active Directory**. Users use this account to log in to their workstation in the domain.

### **Problem:**

Users must remember separate user names and separate passwords for IIoT Services and the domains.

### **Solution:**

Users link their **Identity Service** user account with their user account from **Microsoft Active Directory**. This way users can log in to both systems with the User Credentials from **Microsoft Active Directory**

## LINKING OF EXTERNAL LOGINS

### **The following applies for the linking of external logins with an existing user account:**

- ▶ You as the user can only link external logins if the respective **Identity Providers** have already been configured in **Identity Management** (on page 207) by the administrator.
- ▶ Each user also needs their own user account in **Identity Service**.
- ▶ Despite an existing link to an external login, you can still log in via the internal login. During each login, you have the choice to log in via the internal login or an external login.

A link to an external login can be removed at any time. The internal login is nevertheless always possible.

### 11.2.3.1.3 Change password (for internal login only)

**Change password** allows users to change the password for their user account in **Identity Service** (internal login).

- ▶ A password change in **Identity Service** does not affect the user account of an external identity provider (external login).
- ▶ If you are logged in via an external login, you can use a password change in **Identity Service** to gain access via an internal login (provided it does not exist yet) (on page 154).

Passwords for external logins can only be changed directly via the external **Identity Provider**.

## CHANGE PASSWORD

In this dialog, you change the password for the current logged-in user.

### Change password

Current password



New password

Confirm new password

CHANGE PASSWORD

Option	Description
<b>Current password</b>	The current password for the user.
<b>New password</b>	The new password for the user.
<b>Confirm new password</b>	Confirmation of the new password, as already entered in the <b>New password</b> option.
Change password	Changes the password according to the entry.

Incorrect entries are visualized with a corresponding warning notice in red.

 Invalid user name or password 

### Information

Password changes always required the minimum requirements for a password (on page 238).

### 11.2.3.1.4 Application grants

Here, the user can find an overview of the applications with which they are logged into IloT Services. This is the case, for example, if external client applications are connected via OAuth 2.0. These authorizations can be removed by the user at any time by clicking on the **Revoke Access** button.

### 11.2.3.1.5 Two-factor authentication

The optional two-factor authentication increases the security of a user login to **Identity Service**. The combination of two independent factors effectively secures login processes.

## TWO-FACTOR AUTHENTICATION WITH IDENTITY SERVICE

The following applies for two-factor authentication in the Identity Service:

- ▶ It applies for all login procedures to **Identity Service**.
- ▶ It doesn't matter whether the user logs in via an internal login or an external login (on page 152).
- ▶ Each user configures the two-factor authentication for their own user account in the web interface of **Identity Service**.
- ▶ The administrator can disable two-factor authentication for individual users (on page 178) in **Identity Management**.
- ▶ Configuration of two-factor authentication is only possible if two-factor authentication has also been activated for the user.

### Manage two-factor authentication

#### Authenticator app

Add authenticator app

#### Two-factor authentication

Generate new recovery codes

Disable

Configuration dialog with two-factor authentication activated.

Before you activate two-factor authentication in the Identity Service, you must check the compatibility for the planned use case (on page 165).

## TWO-FACTOR AUTHENTICATION WITH AN EXTERNAL IDENTITY PROVIDER

Some external identity providers offer their own two-factor authentication. This is completely independent of **Identity Service**. The two-factor authentication of an external identity provider is configured in the administration tools of the external identity provider.

**Tip**

Client logins work with Client ID and Secret and are usually automated. Manual entry of login credentials by a human user is not expected here. Therefore, client logins do not support two-factor authentication.

### 11.2.3.1.6 Terminology

The following terms are used in this node:

Term	Description	Practical application
<b>Authenticator App</b>	An app for two-factor authentication that is installed on an authenticator device.	This is usually a mobile device app.  Suitable apps are, for example, Microsoft Authenticator (Windows Phone, Android, iOS) or Google Authenticator (Android, iOS).
<b>Authenticator Device</b>	The device on which the authenticator app is installed.	This is usually a mobile device, generally a smartphone.
<b>Authenticator Key</b>	This static key is generated in <b>Identity Service</b> and is linked long term to a specific user account in <b>Identity Service</b> .  All verification keys generated by the authenticator app are based on this authenticator key.	The authenticator key is transferred from the web interface of <b>Identity Service</b> to the authenticator app via a QR code or manually.  You need this key to configure a user account in the authenticator app of a mobile device.
<b>Recovery Code</b>	If two-factor authentication is enabled, you can log in using your user credentials and a recovery code.  Recovery codes are only used if you do not have access to an authenticator device.  It is a fallback mechanism.	Recovery codes are automatically generated in various configurations of <b>Identity Service</b> and are then displayed once.  <ul style="list-style-type: none"> <li>▶ Recovery codes cannot be displayed again afterwards.</li> <li>▶ Each recovery code can only be used once.</li> </ul>
<b>Verification Code</b>	Verification codes are one-time passwords. They are generated	You need verification codes for different scenarios:



Term	Description	Practical application
	<p>dynamically in the authenticator app and are valid each time for only 30 seconds.</p> <p>All verification codes are based on an authenticator key.</p>	<ul style="list-style-type: none"> <li>▶ First-time enabling of two-factor authentication</li> <li>▶ Reactivating of a disabled two-factor authentication</li> <li>▶ Adding an additional authenticator app</li> <li>▶ Each user login (if two-factor authentication has been enabled)</li> </ul>

### 11.2.3.17 Use of two-factor authentication

Two-factor authentication is only supported for certain use cases in IIoT Services.

You should therefore only use two-factor authentication for a user account if the use case you require is compatible with two-factor authentication. This must be checked for each user account and for each use case.

Important restrictions of two-factor authentication: Users cannot log in to Service Engine.

You can find all information on the compatibility of the different login variants in the **Identity Service:** (on page 148) node **Central authentication service** (on page 148).

### 11.2.3.18 Manage two-factor authentication

You configure two-factor authentication in this dialog.

#### Manage two-factor authentication

##### Authenticator app

Add authenticator app

##### Two-factor authentication

Generate new recovery codes

Disable

Option	Description
<b>Add authenticator app</b>	Opens the dialog to set up an additional two-factor authenticator app.
<b>Generate new recovery codes</b>	Generates new recovery codes for a user account in <b>Identity Service</b> . Previous recovery codes are thus invalid. <b>Note:</b> Only visible if two-factor authentication has been activated.
<b>Disable</b>	Deactivates two-factor authentication. At the same time, the earlier authenticator key loses its validity.

### 11.2.3.1.9 Enable Two-factor authenticaton

The setup of the authenticator app comprises the following actions:

- ▶ It automatically generates a new authenticator key.
- ▶ The authenticator key is registered in an authenticator app.
- ▶ Two-factor authentication is enabled for the **Identity Service** user account.

## SETTING PARAMETERS

### Configure authenticator app for two-factor authentication

Perform the following steps to use an authenticator app:

1. Install a two-factor authenticator app on your mobile device. Use for example Microsoft Authenticator (Windows Phone, Android, iOS) or Google Authenticator (Android, iOS).
2. Scan the QR code or enter this authenticator key in your authenticator app: `5sfa`  
`1ks5 g2t5 g5i5 a4ks enqe c2us tw3y` Spaces and casing can be ignored.



3. The authenticator app will provide you with a unique code. Enter the code in the input field below and enable two-factor authentication.

Verification Code

**ENABLE TWO-FACTOR AUTHENTICATION**

Carry out the following steps to activate two-factor authentication:

1. Go in the web interface of **Identity Service** to the **Manage your profile\Two-factor authentication.** subpage
2. Click on the **Enable Two-factor authentication** button. This opens a configuration dialog.
3. Install an authenticator app on your mobile device. Suitable apps are, for example, Microsoft Authenticator (Windows Phone, Android, iOS) or Google Authenticator (Android, iOS).
4. Scan the QR code in the web interface using the app. Alternatively, you can also enter the key manually.  
**Note:** This way you transfer the authenticator key from **Identity Service** to the app.
5. The app then automatically generates verification codes. Each code is valid for 30 seconds.
6. Enter the currently valid verification code from the app in the appropriate input field in the web interface.
7. Confirm your configuration with the **Enable Two-factor Authentication** button.
8. Save the displayed recovery codes in a safe place.
9. Confirm that the recovery codes have been saved with the **I have stored the codes in a safe place** button.

You have thus enabled two-factor authentication for your user account and have configured the first authenticator device with the first authenticator app.

### 11.2.3.1.10 Recovery codes

Recovery codes allow you to also log in to **Identity Service** without an authenticator app. This is an emergency mechanism in case you can no longer log in via the authenticator app.

#### Your recovery codes

**Store your recovery codes in a safe place and ensure that you can access the codes in the future.**

These are the recovery codes for two-factor authentication of your user account. You will need these codes in case you lose access to your mobile device or authenticator app. Each recovery code can be used only once.

431177c8 892addc8  
2e93d780 40689e74  
d79e27b3 4602564e  
3faa765c f2b078da  
f809d15e a9747d4d

I have stored the codes in a safe place

The following is applicable for recovery codes:

- ▶ Only one set of recovery codes is valid for each user account in **Identity Service**.
- ▶ New recovery codes automatically overwrite older recovery codes. Older recovery codes are thus invalid immediately.
- ▶ The system will show you newly generated recovery codes once. It is not possible to display existing recovery codes again afterwards.
- ▶ Certain configurations in the Identity Service automatically generate new recovery codes.
- ▶ As a logged-in user, you can regenerate Recovery Codes at any time.

Recommendation: When you are shown recovery codes, you should always save them immediately.

### Generate new recovery codes

If you regenerate new recovery codes, the already existing recovery codes are voided.

You can use recovery codes to log into your account in case you have lost access to your authenticator app. You will still need your username and password.

GENERATE NEW RECOVERY CODES

Confirmation dialog when generating new recovery codes.

### 11.2.3.11 User login - authenticator code

If two-factor authentication is enabled, the user logs in to the Identity Service in two steps:

1. Manual entry of user name and password
2. Entry of a verification code

The verification code is generated by an appropriately configured authenticator app. You must read off this code in the app and then manually enter it in the appropriate input field in **Identity Service**.

### authenticator\_code\_header

Two-factor authentication is enabled. Enter the verification code displayed by your authenticator app.

---

Code

Remember device

**LOGIN**

You do not have access to your authenticator device?  
[Click here to log in with a recovery code.](#)

#### CHECKBOX: REMEMBER DEVICE

If the **Remember device** checkbox is activated, you can also log in to a certain device without entering a verification code.

**The following applies here:**

- ▶ In this context, a device is a specific browser installation.
- ▶ If you are using several browsers on the same computer, each browser is considered to be a separate device.
- ▶ You can enable **Remember device** on every device through which you can log in to **Identity Service**.
- ▶ You can use **Forget device** to remove (on page 171) the **Remember device** again.

You should only use the **Remember device** function on devices which are protected against unauthorized access.

### 11.2.3.12 Add authenticator app

This option is only shown if two-factor authentication is enabled.

You can use **Add authenticator app** to configure additional authenticator apps for a user account. The GUI of this configuration dialog is identical with the dialog of **Enable Two-factor authentication** (on page 166).

With "Add authenticator app", there are the following differences in how it works:

1. No new authenticator key is created.
2. All recovery codes, however, are newly generated. Therefore, all previously generated recovery codes lose their validity.
3. Two-factor authentication has already been enabled.

You can set up and simultaneously use as many additional authenticator apps as you want using this configuration dialog. You can thus use several authenticator devices, for example.

**Note:** Since all apps then work with the same authenticator key, they simultaneously display identical verification codes.

### 11.2.3.13 Disable

This option is only shown if two-factor authentication is enabled.

You can thus deactivate two-factor authentication.

This has the following consequences:

- ▶ The existing authenticator key is deleted.
- ▶ All authenticator apps that have been set up with this authenticator key lose access permanently.
- ▶ Two-factor authentication is disabled for your user account.

Afterwards, the only way you can log in is via user name and password in **Identity Service**.

The following applies for the deleted authenticator key:

- ▶ The deleted authenticator key cannot be restored.
- ▶ To reactivate two-factor authentication, you must set up two-factor authentication again. In the process, a new authenticator key is created.

Once the authenticator key has been newly created, you must configure each connected authenticator app again.

### 11.2.3.1.14 Forget device

This option is only shown on devices on which you have activated the **Remember device** checkbox for user login (on page 169).

#### The following applies here:

- ▶ If the **Remember device** option is enabled, you do not have to enter a verification code during user login via a certain device.
- ▶ You can use **Forget device** to disable **Remember device**. You must once again enter a verification code each time during user login.

The **Forget device** option is only offered on devices on which you originally performed **Remember device**.

#### Tip

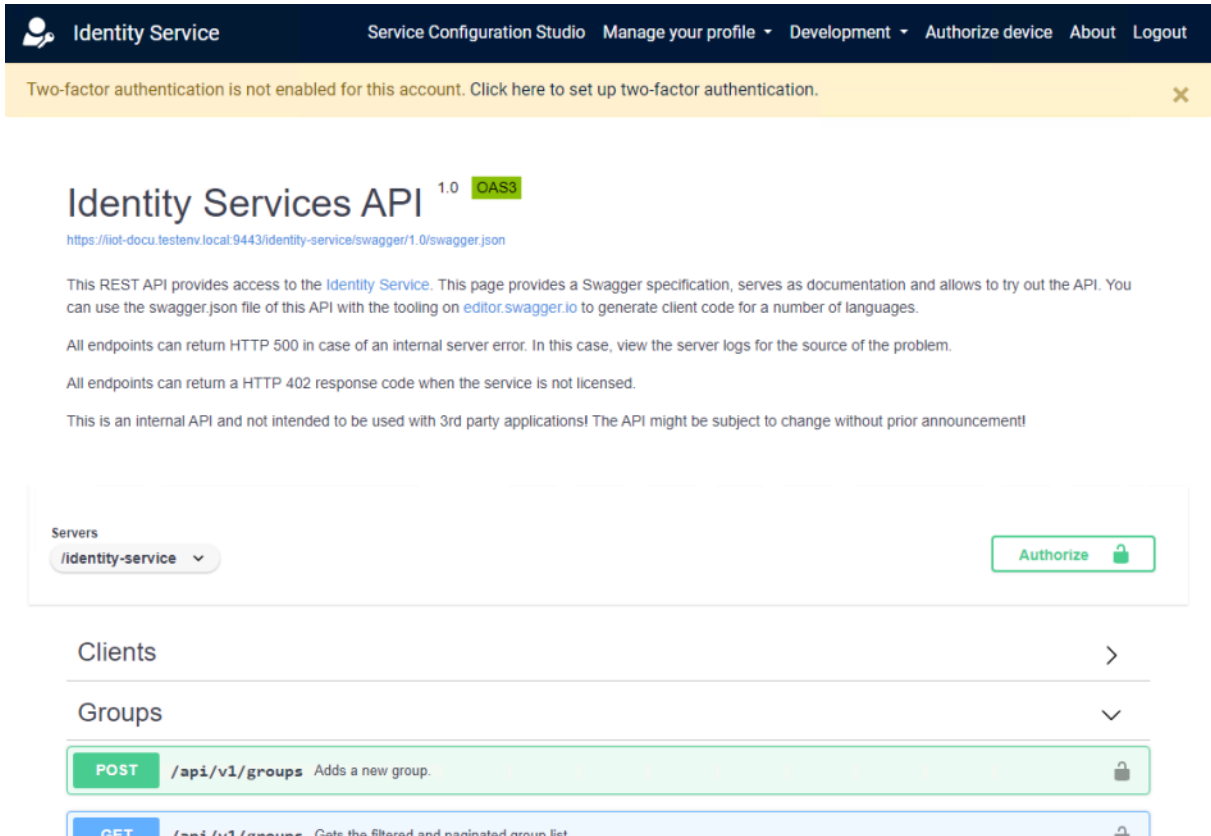
Forget several devices:

If you have selected the **Remember device** option for several devices, you must log in separately via each device and perform **Forget device**.

### 11.2.3.2 Development

In this node, you can find technical information for the logged-in user.

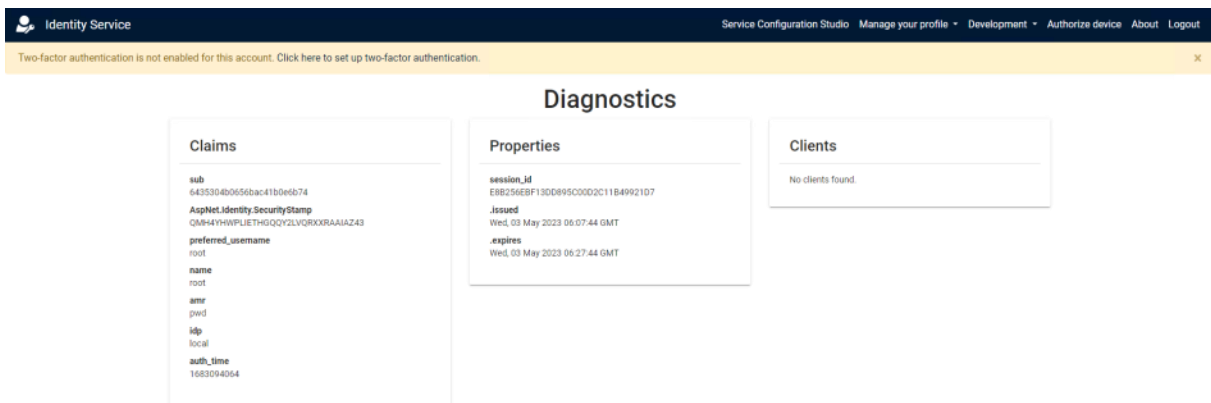
### 11.2.3.2.1 API documentation



The **Identity Service** Swagger documentation is opened in this window.

The **Identity Service** API is an internal API. This API is continually enhanced and adjusted.

### 11.2.3.2.2 Diagnostics



In this view, you can find technical information about the logged-in user. This information is helpful, for example, if external applications from third-party providers are connected to IIoT Services.



### 11.2.3.2.3 OAuth2 discovery document

In this section, you can find information on OAuth authentication.

The OpenID configuration is a standard method for OpenID Connect providers to publish their authorization and token end points together with other configuration details.

This information is always visualized in a new tab in the web browser.

### 11.2.3.3 Authorize device

This menu item is for application scenarios in which applications or devices are to authenticate with the **Identity Service** without a graphical user interface. Here, it may be necessary to implement this via the Device Flow.

To authorize a Device , you must enter its **User code**. The code is displayed on the device. By entering the codes and confirming by clicking on the **SUBMIT** button, the device is authorized for communication with IIoT Services.

**Note:** You can find the **User code** on the device or in its user interface.

### 11.2.3.4 About

This dialog shows the **Identity Service** license status and version information.

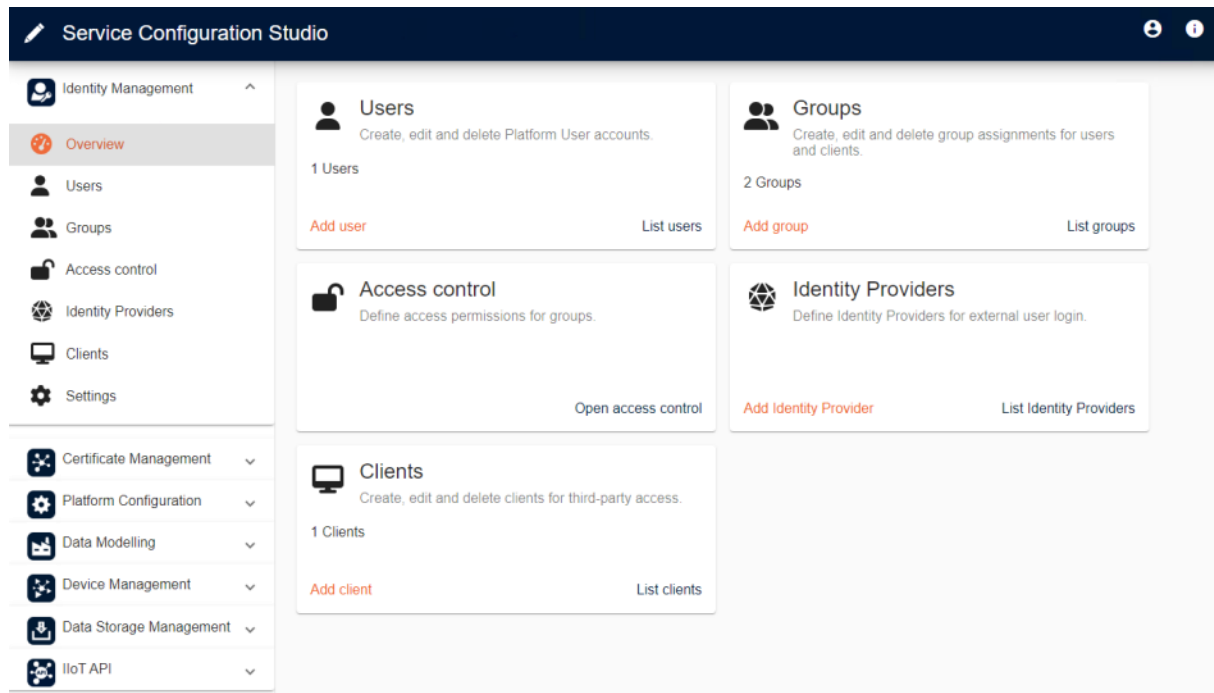
### 11.2.3.5 Logout

**Logout** allows you to log out centrally (Single Sign Out).

**This concerns the following services:**

- ▶ **Identity Service** web interface
- ▶ **Identity Management** web interface

## 11.3 Identity Management



Via the homepage (overview) of Identity Management, you can navigate to all the subpages of this service.

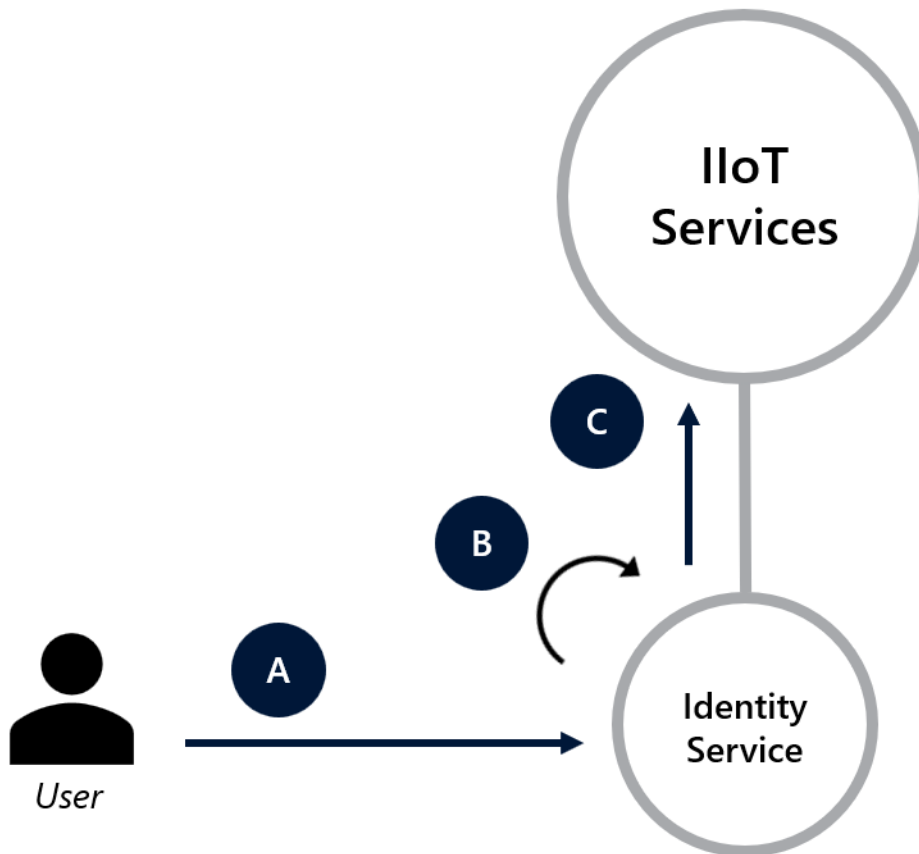
**Identity Management** is the web interface for the comprehensive administration of **Identity Service**.

The following applies for Identity Management:

- ▶ Logged-in users can administer **all user accounts** of the Identity Service.
- ▶ An admin user is created on initial installation.
- ▶ Only users that belong to the *Administrators* group can log in to the web interface of **Identity Management**.
- ▶ The initial user created in the IIoT Services automatically belongs to the *Administrators* group.

Other users can subsequently be granted permission to log in to **Identity Management**.

### 11.3.1 Users (internal login)



Via internal login, users log in to Identity Service as follows:

- A. The user enters their internal login credentials in Identity Service.
- B. Identity Service compares the credentials with the existing user accounts.
- C. The authenticated user has access to IloT Services.

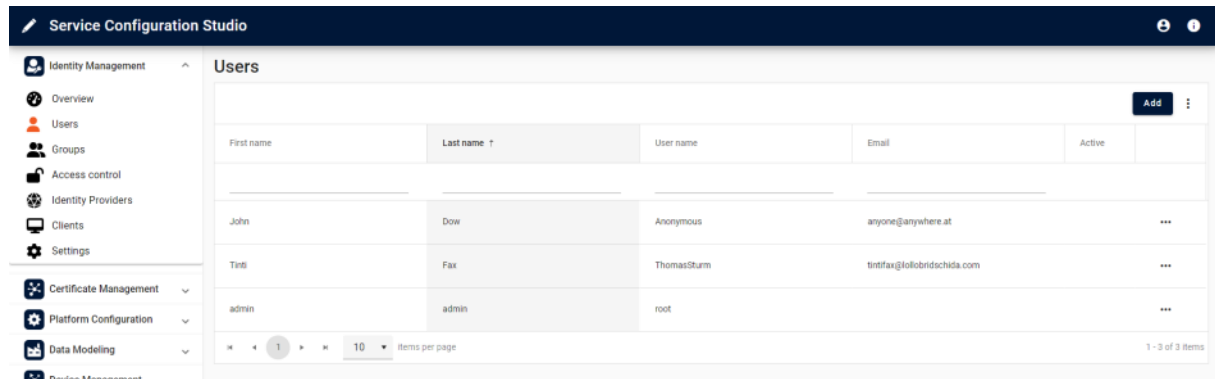
Here you can centrally administer all internal user accounts of **Identity Service**. Every user who wants to log in to the web interfaces of IloT Services needs a user account in the **Identity Service**.

Using the login information defined here, the user authenticates themselves directly to **Identity Service** (**internal login**).

#### **Hint**

External login: You can also optionally link user accounts of **Identity Service** with **external logins** (on page 160).

## USER INTERFACE IN SERVICE CONFIGURATION STUDIO



The configured users are displayed in a list in Service Configuration Studio. The following is applicable for this list:

- ▶ The list can be sorted by clicking on a column heading.
- ▶ Another click on a column heading reverses the sorting order.
- ▶ The column according to which sorting is carried out and the sorting sequence is visualized with an arrow.
- ▶ The number of displayed entries is configured in a footer.
- ▶ It is possible to scroll forward or backward in the list using the arrow keys in the footer.

## CONTEXT MENU

The following menu entries are available when the ... Button is clicked on:

Menu entry	Description
<b>Edit</b>	Opens the confirmation dialog (on page 178) for the selected element.
<b>Change password</b>	Opens the dialog to enter a new password.
<b>Reset lockout</b>	Unlocks the automatic locking of a user. Note: only available if the selected user is locked.
<b>Delete</b>	Deletes the selected entry. A request to confirm this action is made before it is deleted.

### 11.3.1.1 Create new user

You create a new User for **Identity Service** with the **ADD** button.  
 An **internal user** is thus created. This User can log in via the internal login.

#### Add user

---

---

---

---

---

---

Require password change on next login

---

\* This field is mandatory.

Option	Description
<b>First name</b>	The first name of the user.
<b>Last name</b>	The last name of the user.
<b>User name</b>	The user name of the user. The user name cannot be changed afterwards.
<b>Email</b>	The email address of the user.
<b>Password</b>	The password for the user.
<b>Confirm password</b>	You reenter the password here.
<b>Require password change on next login</b>	If you activate this checkbox, the user must change their password the next time they log in.

Option	Description
Description	You can add a description here.

### 11.3.1.2 Edit user

You change a user’s configuration in this dialog.

#### Edit local user

First name\*  
Tinti

Last name\*  
Fax

Email  
tintifax@projectx.at

Active     Allow login linking of Identity Providers

Description

\* This field is mandatory.

Cancel

Submit

#### You can edit an existing user as follows:

1. Click on the ... symbol in the user's line
2. Click on Edit.

Option	Description
First name	The first name of the user.
Last name	The last name of the user.
Email	The email address of the user.
Active	By deactivating the checkbox, the user is deactivated. Every new user is active by default.
Allow login linking of Identity Providers	User-specific option for the possibility to link external providers to the local user. In addition, this

Option	Description
	<p>option stipulates whether the user can change their local password.</p> <ul style="list-style-type: none"> <li>▶ <i>Active</i>: The user can link their login to external providers.</li> <li>▶ <i>Inactive</i>: The user cannot use their login with external providers (on page 207).</li> </ul> <p>Default: depending on the configuration of the <b>Default option for login linking of new users</b> option in the <b>Settings</b> (on page 238) dialog.</p>
Description	Text field for a description.

**Note:** You cannot edit the **User name** afterwards.

## CHANGE PASSWORD

### You can reset a user's password as follows:

1. Click on the ... symbol in the user's line
2. Click on **Change password**.

### A window with the following properties then opens:

Option	Description
<b>Password</b>	The password for the user.
<b>Confirm password</b>	You reenter the password here.
<b>Require password change on next login</b>	If you activate this checkbox, the user must change their password the next time they log in.

## DISABLE TWO-FACTOR AUTHENTICATION

This menu item is only displayed if the respective user has enabled two-factor authentication for their user account.

### This option is intended for the following use case:

- ▶ The user has enabled two-factor authentication for their user account.
- ▶ The user does not have access to their authenticator device and therefore cannot generate a verification code.
- ▶ The user does not have access to their recovery codes.

If the administrator disables two-factor authentication for the user concerned, the user can log in again to Identity Service.

**You as the administrator can disable the two-factor authentication of a user as follows:**

1. Click on the ... symbol in the user's line
2. Click on the **Disable two-factor authentication** menu item.
3. Confirm your configuration by clicking on the **Disable two-factor authentication** button.

You have thus disabled the two-factor authentication for this user. The user can log in again without a verification code.

 **Tip**

Re-enable two-factor authentication:

Every user logged in to **Identity Service** has the option to re-enable two-factor authentication (on page 163) for their user account at any time.

### 11.3.1.3 Deactivate users

Newly created users of the **Identity Service** are by default in the *Active* status.

You can deactivate a user as follows:

1. Go to **Users** in the **Identity Management**.
2. Click on the ... symbol next to the user.
3. Select the **Edit** option.  
A pop-up then opens with the editable properties of this user.
4. Uncheck the **Active** checkbox.
5. Confirm the action by clicking on the **Submit** button.

You have now deactivated the user.



### Info

Deactivated users cannot:

- ▶ Log in directly to the **Identity Service**
- ▶ Log in to the **Identity Service** via external logins
- ▶ Be assigned to groups

Deactivated users are hidden by default in the overview table of **Identity Management\Users**. You can also display deactivated users in the table using the **Show inactive user accounts** option.

#### 11.3.1.4 Activate users

You can reactivate a deactivated user as follows:

1. Go to **Users** in the **Identity Management**.  
Deactivated users are not displayed by default.
2. Click on the ... button in the header of the table.
3. Activate the **Show inactive user accounts** checkbox.  
The table now displays deactivated users too.
4. Click on the ... button next to the deactivated user in the header of the table.
5. Select the **Edit** option.  
A pop-up then opens with the editable properties of this user.
6. Activate the **Active** checkbox
7. Confirm the action with **Submit**.

You have now reactivated the user.

#### 11.3.1.5 Pre-defined users

No users are pre-configured for IIoT Services by default. You must create the initial user when you log in to the web interface of the **Identity Service** for the first time (on page 156).

### 11.3.2 Groups

You administer groups for the **Identity Service** in the **Groups** node.


#### Groups can contain:

- ▶ **Users**
- ▶ **Clients**
- ▶ Supported **Identity Providers**  
*Keycloak, Microsoft Active Directory, Radius*

The main page of **Groups** shows an overview in table form.

**Here you can:**

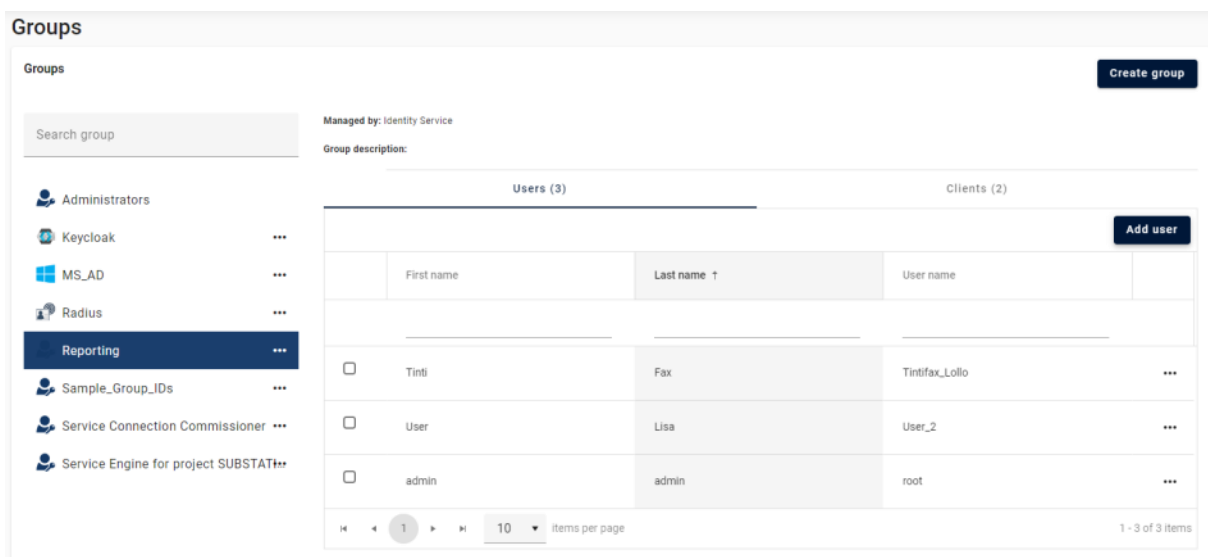
- ▶ Create new groups
- ▶ Edit groups
- ▶ Administer group affiliations (for users and clients)
- ▶ **Note:** Groups of identity providers get their affiliations from the respective provider
- ▶ Delete existing groups

 **Information**

You can only administer user groups of non-supported, external Identity Providers with the administration tools from the respective Identity Provider.

### 11.3.2.1 Groups - overview

You administer groups for the **Identity Service** in the **Groups** node.



Option	Description
<b>Create Group</b>	Opens the dialog to create a new group (on page 185).

Option	Description
<b>Search list</b>	Input field for the filtering of the displayed groups.
<b>Managed by:</b>	Type of user assignment. <ul style="list-style-type: none"> <li>▶ <i>Identity Service</i> User and client assignment for the group are configured in Identity Management.</li> <li>▶ <i>External provider</i> User assignment is taken from external provider.</li> </ul>
<b>Group description</b>	Brief description of the group..
<i>List of the configured groups</i>	List of all configured groups.  Click on the ... button to open the dialog to edit the group (on page 185).
<b>Users</b>	List of all assigned users of the selected group. The number of assigned users is displayed in brackets.  The list can be sorted by clicking on the column heading. Another click reverses the sorting order. The sorted column and the sorting sequence are visualized graphically.  A user can be removed from the group by clicking on the ... button in the context menu.  <b>Note:</b> The removal of a user from a group is only possible if the group is not an <i>external provider</i> type.
<b>Add User</b>	Add new user to the group.  Click on the button to open the dialog for user assignment (on page 190).
<b>Clients</b>	List of all assigned clients of the selected group. The number of assigned clients is displayed in brackets.  The list can be sorted by clicking on the column heading. Another click reverses the sorting order. The sorted column and the sorting sequence are visualized graphically.  A client can also be removed from the group by clicking on the ... button in the context menu.

Option	Description
	<b>Note:</b> Only visible if the group is not an <i>external provider</i> type.

## NAVIGATION AND STATUS BAR

Items per page: 10 ▾ 1 – 3 of 3 |< < > >|

The status bar allows you to customize the view of the respective page and to navigate in the list view.

Option/symbol	Description
<b>Items per page</b>	Number of items shown per page. Selection from a drop-down list.
<b>[a] - [b] of [c]</b>	Sum of all available items and information on the items shown: <ul style="list-style-type: none"> <li>▶ <i>[a]</i>: Number of the first item shown</li> <li>▶ <i>[b]</i>: Number of the last item shown</li> <li>▶ <i>[c]</i>: Sum of all items</li> </ul>
<b>Zur ersten Seite (  &lt; )</b>	Jumps to first page of the list view.
<b>Vorherige Seite (&lt;)</b>	Jumps to previous page of the list view. <b>Note:</b> Not available on the first page.
<b>Nächste Seite (&gt;)</b>	Jumps to the next page of the list view. <b>Note:</b> Not available on the last page.
<b>Zur letzten Seite (&gt; )</b>	Jumps to the last page of the list view.

### 11.3.2.2 Administer groups


Identity Management groups are configured in the **Create Group** dialog.

#### Create group

Group name\*

---

Managed by\* ▼

 Identity Service

Group description

Cancel
Add

Option	Description
<b>Group name</b>	Name of the group.
<b>Manged by</b>	<p>Type of administration of groups and users.</p> <p>Select from drop-down list. The drop-down list contains the selection <b>Identity Service</b> and also the previously-configured external provider.</p> <ul style="list-style-type: none"> <li>▶ <i>Identity Service</i> User and client assignment for the group are configured in Identity Management.</li> <li>▶ External provider User assignment is taken from external provider.</li> </ul> <p><b>Attention:</b> This option cannot be changed after creation.</p> <p>Default: <i>Identity Service</i></p>
<b>LDAP Group DN</b>	<p><b>Distinguished Name (DN)</b> of the LDAP group.</p> <p>Configuration of the complete distinguished name of the MS Active Directory group that is used as a basis for the assignment of the MS AD user to <b>Identity Management</b> groups.</p>

Option	Description
	You can find detailed information about the available parameters on the Microsoft website ( <a href="https://learn.microsoft.com/en-us/previous-versions/windows/desktop/ldap/distinguished-names">https://learn.microsoft.com/en-us/previous-versions/windows/desktop/ldap/distinguished-names</a> ).  <b>Note:</b> This option is only available for the identity provider Microsoft Active Directory.
<b>Group description</b>	Field for the entry of an optional text with the description of the group.
<b>Cancel</b>	Discards all changes and closes the dialog.
<b>Add</b>	Applies settings and closes the dialog.

### CREATE GROUP

Carry out the following steps to create a new group:

- ▶ Click on the **Create Group** button
- ▶ Enter the **Group name** and the **Description** into the detail window
- ▶ In the **Managed by** option, select whether the group dependencies are to be administered by the **Identity Service** or by an external identity provider.
- ▶ Click on the **Add** button.

The group is thus created.

### EDIT GROUPS

Carry out the following steps to edit an existing group:

- ▶ Click on the ... button of the desired group
- ▶ Select the *Edit* option
- ▶ You can now edit the properties **Group name** and **Description** .  
**Note:** The **Group name** must be unique.
- ▶ Confirm your changes by clicking on the **Submit** button

Your changes are thus saved.

### DELETE GROUP

Carry out the following steps to delete a group:

- ▶ Click on the ... button for the group
- ▶ Select the **Delete** option  
A corresponding confirmation dialog will now open.  
**Caution:** The deletion of a group cannot be undone.
- ▶ Enter the name of the group to be deleted under **Enter group name**. This is a request for confirmation to prevent unintended deletion of the group.
- ▶ Deletion is only possible if the entry corresponds to the group name exactly. The entry is case sensitive.
- ▶ Confirm by clicking on the **Delete** button.



### Information

The assigned user accounts of a deleted group are retained. They are not deleted with the group.

#### 11.3.2.2.1 Automatic allocation of users to groups when logging in via identity provider

The following rules apply for the automatic assignment of users of identity providers to **Identity Management** groups:

- ▶ For the automatic assignment of users to **Identity Management** groups, a corresponding Identity Provider must be linked to the groups in the **Managed by** option. This **Identity Provider** must already be configured in the **Identity Management** for the configuration of the group.
- ▶ Note the restriction for hierarchical groups from the identity providers *Keycloak* and *Microsoft Active Directory*. **Identity Management** does **not** support group hierarchies. It uses a flat group structure. All groups are located on the same hierarchical level. The hierarchical group structures of Keycloak are converted by **Identity Management** into flat group structures.
- ▶ How users are assigned to a group in **Identity Management** with automatic allocation based on an identity provider depends on the identity provider. The following identity providers support the automatic allocation of users to groups in **Identity Management**:
  - ▶ **RADIUS**  
via names. A user that logs on to the **Identity Service** via *RADIUS* is automatically added to all **Identity Management** groups that match one of the external group names of the Identity Provider *RADIUS*. The requirement for this is that the group name in *RADIUS* matches **Identity Management** group name exactly and that the **Managed by** option is set correctly. This also includes the capitalization of the group names.

**Note:** Additional information on the necessary configurations for the identity provider *RADIUS* can be found in the chapter **Automatic allocation of RADIUS users to Identity Management groups** (on page 213).

▶ **Keycloak**

via names. A user that logs on to the **Identity Service** via *Keycloak*, is automatically added to all **Identity Management** groups that match one of the external group names of the Identity Provider *Keycloak*. The requirement for this is that the group name in *Keycloak* matches **Identity Management** group name exactly and that the **Managed by** option is set correctly. This also includes the capitalization of the group names.

**Note:** Additional information on the necessary configurations for the identity provider *Keycloak* can be found in the chapter **Automatic allocation of Keycloak users to Identity Management groups** (on page 216).

▶ **Microsoft Active Directory**

via Distinguished Name

▶ Group naming for identity providers

To ensure correct allocation, group names in the configuration of the respective identity provider must not contain ',' (comma) or '@' (at symbol).

- ▶ The automatic allocation of a user to an **Identity Management** group occurs the first time the user logs on to the **Identity Service** via **Identity Provider**. The user is only assigned to those groups that have selected the respective provider in the **Managed by** (on page 185) option.
- ▶ If a user already assigned to the identity provider is deleted, this user remains assigned to the group in **Identity Management**. This user can no longer log on via **Identity Service**. Manually remove the user from the group in **Identity Management**. Select the group and the user to be deleted from the list of assigned users. Click on the ... Button to open the context menu. Select Remove. The user is removed from the group after confirming the warning dialog.
- ▶ Additionally, users from Identity Providers can be added manually to **Identity Management** if the **Managed by** option with the *Identity Service* entry is selected for the **Identity Management** group. These manually assigned users remain in the respective identity provider even after group changes.



**👍 Hint:****Group administrators in Identity Service**

The administrative users in IloT Services are part of the *Administrators* group in the **Identity Management**. At least one user of the **Identity Management** must be part of the *Administrators* group at all times to ensure administrative access to IloT Services.

**This is ensured by the following protective functions:**






- ▶ In **Identity Management**, the last user cannot be removed manually from the *Administrators* group in **Identity Service**.
- ▶ The group assignments automatically obtained from Keycloak also cannot remove the last user from the *Administrators* group.

This ensures that administrative access to IloT Services is also guaranteed when group assignments are obtained via Keycloak.

### 11.3.2.3 Administer users in groups

Existing users are added to or removed from groups in the **Add users** dialog.

**Add users**

	Tinti Fax	<input checked="" type="checkbox"/>
	User John	<input type="checkbox"/>
	User Lisa	<input checked="" type="checkbox"/>
	thomas Sturm thomas.sturm@copadata.com	<input type="checkbox"/>
	admin admin	<input type="checkbox"/>

Selected: 2

Cancel
Add

Option	Description
<b>Search list</b>	Input field for the filtering of the displayed users.
<i>Client list</i>	List of the users configured in Identity Service. <b>Note:</b> The list contains all clients that are not already assigned to the group.
<b>Selected:</b>	Information about the number of selected users.
<b>Cancel</b>	Discards all changes and closes the dialog.
<b>Add</b>	Applies settings and closes the dialog.

## ADDING USERS TO GROUPS

### Proceed as follows:

1. Select a group and highlight it by clicking the mouse.
2. Switch to the **Users** tab.
3. Click on the **Add user** button.
4. In the **Add users** dialog, select one or more users from the list.  
**Note:** You can filter the list by user names.
5. Apply the selected users by clicking on the **Add** button.

The selected users thus become members of the corresponding group.



### Information

No users can be added to groups for external providers. Users are automatically added to the group if they log in with this external identity provider.

## REMOVE USERS FROM A GROUP

You only remove the user from the group at this point. The user's account continues to exist regardless of group affiliation.

### Proceed as follows:

1. Highlight the group with a mouse click.
2. Switch to the **Users** tab.
3. Select the user and click on the ... button for the user.
4. Click on **Remove**.
5. Confirm the request for confirmation again with **Remove**.

The user is thus deleted from the group.



### Information

The last-assigned user of the pre-defined **Administrators** group cannot be deleted from the group.

### 11.3.2.4 Administering clients in groups

Existing **clients** are added to or removed from groups in the **Add** dialog.

#### Add clients

<input type="checkbox"/>	HTML Engine Client	<input type="checkbox"/>
	<small>HTML Engine</small>	
<input type="checkbox"/>	Report Engine Client	<input checked="" type="checkbox"/>
	<small>Report Engine</small>	
<input type="checkbox"/>	Service Engine Client	<input type="checkbox"/>
	<small>Service Engine</small>	
<input type="checkbox"/>	Service Engine for project SUBSTATION_HMI_Z12	<input checked="" type="checkbox"/>
	<small>SE_556B2FD8-ED1E-4096-960B-1F2D8CF6C6A9</small>	

Selected: 2

Cancel
Add

Option	Description
<b>Search list</b>	Input field for the filtering of the displayed clients.
<i>Client list</i>	List of the clients configured in the Identity Service. <b>Note:</b> The list contains all clients that are not already assigned to the group.
<b>Selected:</b>	Information about the number of selected clients.
<b>Cancel</b>	Discards all changes and closes the dialog.
<b>Add</b>	Applies settings and closes the dialog.

## ADDING CLIENTS TO GROUPS

Proceed as follows:

1. Select a group and highlight it by clicking the mouse.
2. Switch to to the Clients tab.
3. Click on the Add Client button.
4. In the add clients dialog, select one or more clients from the list.  
Note: You can filter the list by client names.
5. Apply the selected clients by clicking on the Add button.

The selected clients thus become members of the corresponding group.

## REMOVE CLIENT FROM A GROUP

You only remove the client from the group at this point. The client's account continues to exist regardless of group affiliation.

Proceed as follows:

1. Highlight the group with a mouse click.
2. Switch to to the Clients tab.
3. Select the client and click on the ... button.
4. Click on **Remove**.
5. Confirm the request for confirmation again with **Remove**.

The client is thus deleted from the group.

### 11.3.2.5 Pre-defined groups

The *Administrators* system group is pre-configured for IloT Services.

The following applies for the Administrators system group:

- ▶ Members of this group can administer IloT Services in Service Configuration Studio in the **Identity Management**.
- ▶ The *Administrators* system group cannot be deleted or renamed.
- ▶ At least one user must always be assigned to the group. This is ensured by corresponding protective functions in IloT Services. The last user cannot be deleted from the group.

It is thus ensured that an administrator has access to IloT Services at all times.

### 11.3.3 Access control

You administer authorizations for **Groups** in **Access control**.

- ▶ Authorizations are issued via resources and roles.
- ▶ Only the combination of resource and role results in the authorization. It is not possible to assign a resource without a role.

The authorizations result from the group affiliations (**Groups**) of users (**User**) and applications (**Clients**).

#### BASIC PROCEDURE

The basic principle of assigning an authorization is as follows:

1. You select an **Group**
2. You add a resource to the **Group**.
3. You assign a role to the resource.

You have now assigned an authorization to the group.

#### 11.3.3.1 Add resources

Resources in IloT Services are, for example:

- ▶ Self-created Service Engine projects
- ▶ Pre-defined resources such as **Infrastructure**

You add resources as follows:

1. Select a group.
2. Click on the **Add resources** button.
3. Select the checkboxes for the desired resources from the list.
4. Confirm your selection by clicking on the **Add** button.

You have thus assigned resources to a **Group**. You must now assign each resource at least one role.

#### Attention

The selection of a resource is only saved if a role has been assigned. A resource without role assignment is not saved.

### 11.3.3.2 Adding roles to the resource

You must add at least one role after adding a resource.

You add a role as follows:

1. Click on the ... button in the resource.
2. Select **Manage roles** from the menu.
3. Highlight the checkbox of the desired role.
4. Apply the change by clicking on the **Submit** button.

You have thus assigned the role. Now the authorization – the combination of resource and role – is active.

### 11.3.3.3 Removing resources

You remove a resource as follows:

1. Please select a group.
2. Click on the ... button for the resource that you want to remove.
3. Select the **Remove resource** option in the context menu.
4. Confirm your selection by clicking on the **Remove** button.

You have thus removed the resource from the group.



#### Information

You cannot remove the **Infrastructure** resource from the pre-defined **Service Grid Administrator** group.

### 11.3.3.4 Pre-defined resources and roles

The following resources with the corresponding roles have been pre-configured in IIoT Services:

Pre-defined resources	Pre-defined roles	Description
<b>Infrastructure</b>	<i>Identity Administrator</i>	<p>Only users with the <i>Identity Administrator</i> role have access to <b>Identity Management</b>. This assignment between role and resource is pre-defined and cannot be unassigned.</p> <p>The role is assigned by default to the <i>Administrators</i></p>

Pre-defined resources	Pre-defined roles	Description
		group.
<b>Infrastructure</b>	<i>Certificate Management Administrator</i>	Only users with this role have access to <b>Certificate Management</b> . The role is assigned by default to the <i>Administrators</i> group.
<b>Infrastructure</b>	<i>Platform Configuration Administrator</i>	Only users with this role have access to <b>Platform Configuration</b> . The role is assigned by default to the <i>Administrators</i> group.
<b>Infrastructure</b>	<i>Device Management Administrator</i>	Only users with this role have access to <b>Device Management</b> . The role is assigned by default to the <i>Administrators</i> group.
<b>Infrastructure</b>	<i>Device Management Agent</i>	System role for device agents. Is not envisaged as a user role.
<b>Infrastructure</b>	<i>Service Connection Commissioner</i>	This role can be used for the connection of a Service Engine to the <b>Ilot Services Connection Wizard</b> and for the registration of the <b>Device Agent</b> with <b>Device Management</b> .
<b>Infrastructure</b>	<i>Data Storage Administrator</i>	This role can manage and fully administer <b>Data Storage Management</b> in Service Configuration Studio. This role is necessary to clean up data or to delete it.
<b>Infrastructure</b>	<i>Data Modeling Administrator</i>	This role serves as administrator of <b>Data Modeling</b> in Service Configuration Studio. In this role, as an example, <b>Tenants</b> are administered and <b>Construction Kit Libraries</b> are imported or deleted, in <b>Data Modeling</b> .
<b>Infrastructure</b>	<i>Service Connection Commissioner</i>	With this role, it is only possible for a client to call up new or current Certificate Bundles. All device agents communicate in this role. Old agents get the new role through migration.



Pre-defined resources	Pre-defined roles	Description
<b>Infrastructure</b>	<i>IloT Services Client</i>	<p>With this role, the Service Engine user administration can be used with the <b>Identity Service</b> of IloT Services.</p> <p>This role can only read users and groups. Configuration of the <b>Identity Service</b> cannot be edited by this role.</p>
<b>Dashboard Service</b>	<i>Viewer, Editor, Manager, Administrator</i>	<p>Only users with one of these roles have access to <b>Dashboard Service</b>.</p> <p>The <i>Dashboard Administrator</i> role is assigned by default to the <i>Administrators</i> group.</p>
<b>Report Engine Server</b>	<i>IloT API – Reporting Read</i>	<p>This role can, in this resource, query all reports on this Report Engine Server via the <b>IloT API</b>.</p>
<b>Report</b>	<i>IloT API – Reporting Read</i>	<p>Users in this role can, in this resource, query the report or the reports precisely via the <b>IloT API</b>.</p> <p>The following is applicable here:</p> <ul style="list-style-type: none"> <li>▶ Each report is a subordination of precisely one Report Engine Server.</li> <li>▶ Each Report Engine Server has 0 - n subordinate reports.</li> </ul>
"zenon project name"	<i>Data Read</i>	<p>Enables read access to unlocked project variables via the IloT API as well as the reading of data from <b>Data Storage</b>.</p>
"zenon project name"	<i>Data Write</i>	<p>Enables write access to unlocked project variables via the IloT API as well as the writing of data to <b>Data Storage</b>.</p>
"zenon Projektname"	<i>Acknowledge Alarms</i>	<p>Allows the confirmation of alarm messages for this project, for example via the IloT API.</p>
<b>Data Modeling</b>	<i>Data Modeling Admin</i>	<p>Administrative access to <b>Data Modeling</b> including <b>Tenants</b>.</p>
<b>Data Modeling</b>	<i>Data Modeling Write</i>	<p>Access to <b>Tenants</b> and write access to <b>Data Modeling</b>.</p>
<b>Data Modeling</b>	<i>Data Modeling</i>	<p>Access to <b>Tenants</b> and read access to <b>Data</b></p>

Pre-defined resources	Pre-defined roles	Description
	<i>Read</i>	<b>Modeling.</b>
<b>Tenant</b>	<i>Tenant Admin</i>	Administrative access to <b>Tenants</b> . Only available if no role has been defined for <b>Data Modeling</b> .
<b>Tenant</b>	<i>Tenant Write</i>	Write access to <b>Tenants</b> . Only available if no role has been defined for <b>Data Modeling</b> .
<b>Tenant</b>	<i>Tenant Read</i>	Read access to <b>Tenants</b> . Only available if no role has been defined for <b>Data Modeling</b> .

## ZENON PROJECT AS A RESOURCE

**A zenon project is only available as a resource if the following conditions are met:**

- ▶ The project has been configured for IIoT Services using Engineering Studio and the **IIoT Services Connection Wizard**.
- ▶ Service Engine must be started.
- ▶ There must be a network connection with IIoT Services.

If even only one condition is not met, you will not have access to the project via IIoT Services.

### 11.3.3.5 Reserve - to be deleted

The following resources with the corresponding roles have been pre-configured in IIoT Services:

Pre-defined resources	Pre-defined roles	Description
<b>"zenon project name"</b>	<i>IIoT API – Data Read</i>	Enables read access to unlocked project variables via the IIoT API as well as the reading of data from <b>Data Storage</b> .
<b>"zenon project name"</b>	<i>IIoT API – Data Write</i>	Allows write access to enabled variables of the project via the IIoT API.
<b>"zenon project name"</b>	<i>IIoT API – Acknowledge</i>	Allows confirmation of alarm messages for this project via the IIoT API.

Pre-defined resources	Pre-defined roles	Description
	<i>Alarms</i>	
"zenon project name"	<i>Data Storage – Data Read</i>	Allows data to be read from <b>Data Storage</b> .
"zenon project name"	<i>Data Storage – Data Write</i>	Allows data to be written from <b>Data Storage</b> .

### 11.3.4 Report permissions

Here you can configure the availability and the access permissions for reports and Custom Report Items via the IIoT API.

#### REPORT ENGINES MENU

Option	Description
<i>Search</i>	Searches the existing instances of Report Engine.  String input. The search starts when the first character is entered. All instances of Report Engine are found that contain the string. The list is limited to search hits.
<b>Report Engines</b>	List of available instances of Report Engine.
<b>Detail display</b>	Displays all the properties of the selected Report Engine and allows you to configure them.
<b>Assign group permissions Symbol</b>	Clicking on the symbol opens the dialog Dialog (on page 205) for assigning group permissions.  Only available if an instance of Report Engine has been selected.

### 11.3.4.1 Report

Option	Description
<b>Search</b>	Searches the available items for name and alias.  String input. The search starts when the first character is entered. All items are found that contain the string. The list of items is limited to the items found during the search.
<b>Last update time</b>	Displays the date and the time of the last update of the table, such as: Last time the table was displayed, last time the content was updated, last time the content was saved.
<b>Update symbol</b>	Clicking on the button updates the data in the table for the IIoT Services.
<b>List of reports</b>	List of available reports. Their names and properties are displayed. Users can: <ul style="list-style-type: none"> <li>▶ Edit an alias</li> <li>▶ Publish or withdraw individual reports</li> </ul>
<b>Name</b>	Name of the report.
<b>Description</b>	Description of the report.  Clicking on the description opens a window that displays the complete description.
<b>Alias</b>	Name of the alias. This can be changed for the respective action via the symbol.  Permitted characters: Alphanumeric characters and underscores  <b>Note:</b> The assigned alias must be unique throughout all configured Report Engine instances for each item type.
<b>Published</b>	Displays whether the report has been published.
<b>Actions</b>	Available actions: <ul style="list-style-type: none"> <li>▶ Edit an item: Allows you to Change an alias (on page</li> </ul>

Option	Description
	203). <ul style="list-style-type: none"> <li>▶ Publish an item: Opens the Publishing dialog (on page 204) of an item.</li> </ul>
<b>Navigation</b>	Enables you to navigate in the list. <ul style="list-style-type: none"> <li>▶  &lt;: Displays the first page.</li> <li>▶ &lt;: Displays the previous page.</li> <li>▶ <b>Number</b>: Displays the current page and selection of another page.</li> <li>▶ &gt;: Displays the next page.</li> <li>▶ &gt; : Displays the last page.</li> <li>▶ <b>Items per page</b>: Configuration of the lines per page to be displayed. Select from drop-down list.</li> <li>▶ <b>Items displayed</b>: Shows how many items are currently being displayed and how many in total are available. Filters are taken into account.</li> <li>▶ <b>Update</b> symbol: Clicking on the button updates the displayed data with the current data of the system.</li> </ul>

### 11.3.4.2 SQL element

List of the available SQL elements. The SQL functionality of Report Engine can thus be made available via the IIoT API in the form of Stored Procedures and User-defined Functions. These can be checked here and provided with an alias as well as published and withdrawn.

**The following options are available:**

Option	Description
<b>Search</b>	Searches the available items for name and alias.  String input. The search starts when the first character is entered. All items are found that contain the string. The list of items is limited to the items found during the search.

Option	Description
<b>Last update time</b>	Displays the date and the time of the last update of the table, such as: Last time the table was displayed, last time the content was updated, last time the content was saved.
<b>Update symbol</b>	Clicking on the button updates the data in the table for the IIoT Services.
<b>List of SQL elements</b>	List of the available SQL elements. Their names and properties are displayed. Users can: <ul style="list-style-type: none"> <li>▶ Edit an alias</li> <li>▶ Publish or withdraw individual SQL elements</li> </ul>
<b>Name</b>	Name of the SQL element.
<b>Description</b>	Description of the SQL element. Clicking on the description opens a window that displays the complete description.
<b>Alias</b>	Name of the alias. This can be changed for the respective action via the symbol.  Permitted characters: Alphanumeric characters and underscores  <b>Note:</b> The assigned alias must be unique throughout all configured Report Engine instances for each item type.
<b>Published</b>	Displays whether the SQL element has been published.
<b>Actions</b>	Available actions: <ul style="list-style-type: none"> <li>▶ Edit an item: Allows you to Change an alias (on page 203).</li> <li>▶ Publish an item: Opens the Publishing dialog (on page 204) of an item.</li> </ul>
<b>Navigation</b>	Enables you to navigate in the list. <ul style="list-style-type: none"> <li>▶  &lt;: Displays the first page.</li> <li>▶ &lt;: Displays the previous page.</li> <li>▶ <b>Number</b>: Displays the current page and selection</li> </ul>

Option	Description
	<p>of another page.</p> <ul style="list-style-type: none"> <li>▶ &gt;: Displays the next page.</li> <li>▶ &gt; : Displays the last page.</li> <li>▶ <b>Items per page</b>: Configuration of the lines per page to be displayed. Select from drop-down list.</li> <li>▶ <b>Items displayed</b>: Shows how many items are currently being displayed and how many in total are available. Filters are taken into account.</li> <li>▶ <b>Update</b> symbol: Clicking on the button updates the displayed data with the current data of the system.</li> </ul>

### 11.3.4.3 Edit an alias

Aliases can be created, edited and deleted directly in the lists or in the Publishing dialog (on page 204).

## CREATING OR EDITING AN ALIAS

### To edit an alias:

1. Click on the **Pencil** symbol in the Actions column.  
The input field opens in the Alias column.
2. Enter the desired alias.  
Note: The assigned alias must be unique for all configured instances of Report Engine for each element type.  
Click on the **Apply** symbol (check mark):  
To leave the field without making changes, click on the **Discard** symbol.
3. The alias is entered into the list.

The alias has thus been edited.

## DELETE AN ALIAS

### To delete an alias:

1. Click on the **Pencil** symbol in the Actions column.  
The input field opens in the Alias column. An **X** symbol is displayed next to the alias.

2. Click on the **X**.  
The text is deleted.
3. Click on the **Apply** symbol (check mark):  
To leave the field without making changes, click on the **Discard** symbol.

The alias has thus been deleted.

### 11.3.4.4 Publish

This dialog is opened if you click on the **Publish** button of an element of a Report Engine.

*Published* means that the respective element can be reached via the IIoT API using the selected alias.

#### To publish or withdraw the publishing:

1. Select the desired item.
2. Configure the options of the detail view.  
These are different for individual items and parameters.

For parameters, you receive a list of available items in the detail view. Select the desired items by means of the checkboxes. Clicking on the button affects all the selected parameters.

3. Click on the **Publish selected** or **Unpublish selected** button.

### ITEM DIALOG

Option	Description
<b>Tree view Additional filter</b>	Project filter. Selection of an item from the tree view. Detailed configuration takes place in the detail window.  <b>Symbols:</b> <ul style="list-style-type: none"> <li>▶ Red triangle: There is a problem in this node.</li> <li>▶ Yellow triangle: There is a problem in the nesting of this node.</li> </ul>
<b>Detail view</b>	Configuration of the selected item from the tree view.
<b>Alias</b>	Alias of the item.  <b>Note:</b> The assigned alias must be unique throughout all configured Report Engines for each item type.



Option	Description
<b>Published</b>	Displays the status of the item via a checkbox: <ul style="list-style-type: none"> <li>▶ <i>active</i>: published</li> <li>▶ <i>inactive</i>: unpublished</li> </ul>
<b>Unpublish</b>	Clicking on the button opens the confirmation dialog.  If this is confirmed, the selected, already published item is reset to unpublished. Thus, the item is no longer accessible via the REST interface.
<b>Publish</b>	Clicking on the button opens the confirmation dialog.  If this is confirmed, the selected item is published.

### 11.3.4.5 Assign permissions

Here you can configure which item is to be available in which permissions group. You can configure or copy assignments.

#### **To assign an item to a permissions group:**

1. Select the permissions group in the group list.
2. Highlight the items you would like to allow in the tree view.
3. Press the **Save** button.

#### **To copy an assignment from one permissions group to another:**

1. Click on the **Copy assignment from group to group** button.  
The dialog to assign groups is opened.
2. Select the source group.
3. Select the target group.
4. Click on **Copy**.  
The rights granted in the source group are copied to the target group.

## ASSIGNMENT OF PERMISSIONS GROUPS TO ITEMS DIALOG

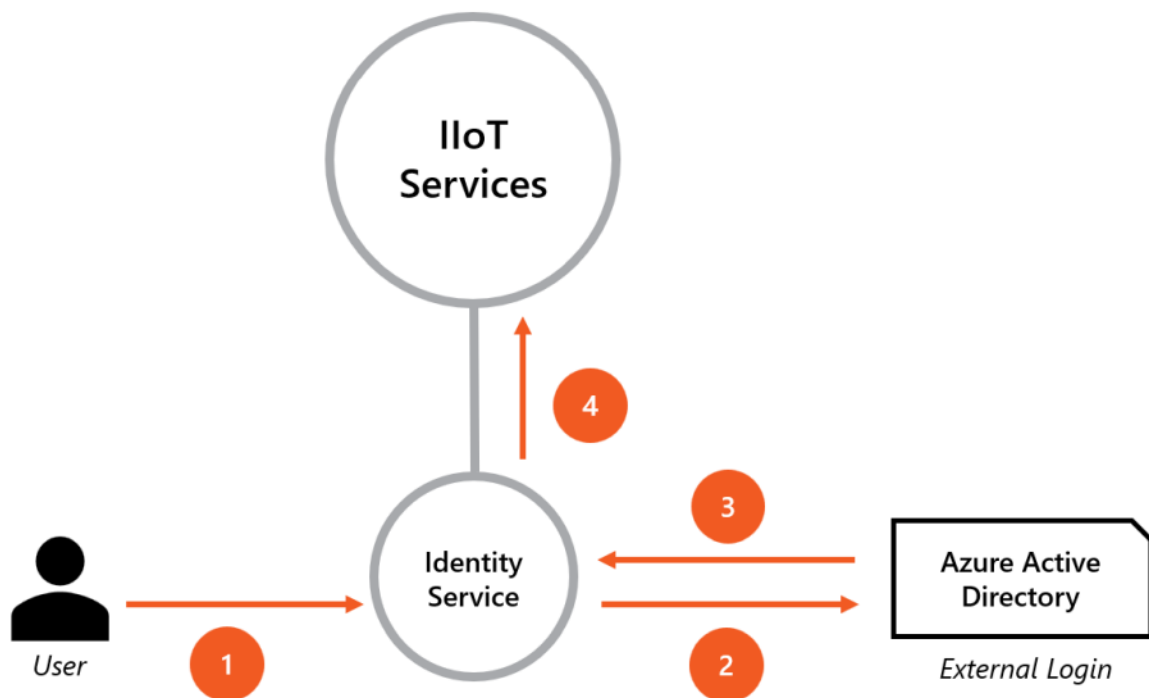
Option	Description
<b>Groups</b>	Displays all the available permissions groups.
<b>Search</b>	Search in the group list. String input. The search starts when the first character is entered. All permissions groups are found that contain the string. The list of groups is limited to the groups found during the search.
<b>Items</b>	Displays all the available items.
<b>Search (Groups)</b>	Search for item name in all items of Report Engine.  String input. The search starts when the first character is entered. All items are found that contain the string. The list of items is limited to the items found during the search.
<b>Search (Items)</b>	Search for item type in all items of Report Engine.  Select from drop-down list. All items are found that match the type. The list of items is limited to the items found during the search.
<b>List of items</b>	Displays the available items. When an entry is made in the search window, the display is limited to the relevant hits.
<b>Copy assignment from group to group</b>	Opens the dialog to copy permissions from one group to another permissions group.
<b>Save</b>	Clicking on the button saves the configuration.

## TRANSFER OF RIGHTS FROM GROUP TO GROUP DIALOG

Option	Description
<b>Search</b>	Search in the group list. String input. The search starts when the first character is entered. All permissions groups are found that contain the string. The list of groups is limited to the groups found during the search.
<b>List of groups</b>	Displays all the available source groups.
<b>Search</b>	Search for item name in all items of Report Engine.

Option	Description
	String input. The search starts when the first character is entered. All items are found that contain the string. The list of items is limited to the items found during the search.
List of groups	Displays all the available target groups.
Copy	Transfers rights from the source group to the target group

### 11.3.5 Identity providers (for external logins)



The process of logging in a user via an external login is as follows:

1. The user clicks on an external login on the login page in the web interface of Identity Service (here: Azure Active Directory).
2. Identity Service redirects the user to the website of Azure Active Directory. The user enters their credentials there.
3. The external identity provider compares the credentials with its user accounts and reports the result to Identity Service.
4. The Identity Service grants the authenticated user access to IIoT Services.

In the **Identity Providers** menu item, you can define external identity providers for **External logins** (on page 160). This therefore allows you to integrate IIoT Services into an existing authentication infrastructure.

**Tip**

How a user name is entered during user login depends on the identity provider.

**Example: Microsoft Active Directory as external identity provider**

- ▶ Full user name:  
*john.doe@microsoft.com*
- ▶ Login to web interface of **Identity Service**:  
*john.doe@microsoft.com*
- ▶ Login to Service Engine:  
*john.doe*

You can find detailed information on this in the **IIoT Services - configuration in Engineering Studio** (on page 307) node in the **Compatibility table**: (on page 316) node **User names** (on page 316).

### 11.3.5.1 Azure Active Directory

Option	Description	Example
<b>Provider Alias</b>	Is needed for unique identification.  The <b>Provider Alias</b> is also used for the login page of the Identity Service. There, the user can select which Identity Provider they want to use for login.	<i>my-azure-ad</i>
<b>Provider description</b>	Optional description of the Identity Provider.	
<b>Tenant ID</b>	A unique identifier that you must look up in your Azure subscription.	<i>e5fa83b7-d261-48f0-8728-524d9b949d52</i>
<b>Authority</b>	URL at which the OpenID Connect Provider can be contacted.	<i>https://login.microsoftonline.com</i>
<b>Client ID</b>	Enter the <b>Client ID</b> defined in the Azure Active Directory. This is required by Identity Service to	<i>07c8b99b-fe15-2587-8e58-c1dc85d4fe17</i>

Option	Description	Example
	authenticate external users.  <b>Note:</b> The <b>Client ID</b> must be registered in the Azure Active Directory.	
<b>Client Secret</b>	<b>Client Secret</b> that is generated in Azure Active Directory and has been assigned to the <b>Client ID</b> .  <b>Note:</b> Azure Active Directory always creates <b>Client ID</b> and <b>Client Secret</b> in pairs. Identity Service uses this specific combination of pairs to authenticate external users.	85NZrL17WRBWWbyn.FDuz_tZ4Yt55. .341

**Tip**

**Configuration in Azure Active Directory**

The configuration dialog displays – adjusted to your system – the following hint:

*Please enter the following redirect URL(s) to your external identity provider:*  
<https://mycomputer.mydomain.com:9443/identity-service/auth/my-azure-ad/signin-callback>

You must save your individual URLs in Azure Portal as valid Redirect URL(s).

**Redirect URL after upgrade**

As of Version 10.1, Identity Service uses different Redirect URLs for authentication with **Azure Active Directory**.

After an upgrade of an older IIoT Services version 10.0 (or older), you must thus reconfigure the updated Redirect URLs of Identity Service in Azure Portal.

**11.3.5.2 Microsoft Active Directory**

There are the following options for configuration with **Microsoft Active Directory**:

Option	Description	Example
<b>Provider Alias</b>	Is used for unique identification if several Identity Provider s have	


Option	Description	Example
	<p>been configured.</p> <p>The <b>Provider Alias</b> is also used for the login page of the Identity Service. There, the user can select which Identity Provider they want to use for login.</p>	
<b>Provider description</b>	Optional description of the Identity Provider.	
<b>Hostname</b>	The Microsoft Active Directory domain controller.	
<b>Port</b>	Port number via which the Microsoft Active Directory is accessible on the host.	636 (TLS active) 389 (TLS inactive)
<b>Apply TLS encryption</b>	<p><i>Active</i>: The communication is TLS encrypted.</p> <p><i>Inactive</i>: Communication is not encrypted.</p> <p>Requirements:</p> <ul style="list-style-type: none"> <li>▶ The matching <b>Port</b> must be selected.</li> <li>▶ The server must provide a matching server certificate.</li> </ul> <p>Default: <i>active</i></p>	<i>active</i>

### 11.3.5.2.1 Automatic allocation of Microsoft Active Directory RADIUS users to Identity Management groups

Execute the following steps to automatically add MS Active Directory users to **Identity Management** groups in **Identity Management**:

1. Configure an identity provider.
2. Create a new group in **Identity Management**.
3. Select the configured identity provider from the drop-down list for this group in the **Managed by** option.

4. Configure the full name of the MS Active Directory group in the **LDAP Group DN** option.

 **Information**

Further information on the automatic allocation of users from Identity Provider to Identity Management groups can be found in the **Groups** (on page 181) chapter **Automatic allocation of users to groups when logging in via identity provider** (on page 187).

### 11.3.5.3 OpenLDAP

There are the following options for configuration with **OpenLDAP**:

Option	Description	Example
<b>Provider Alias</b>	Is used for unique identification if several Identity Provider s have been configured.  The <b>Provider Alias</b> is also used for the login page of the Identity Service. There, the user can select which Identity Provider they want to use for login.	
<b>Provider description</b>	Optional description of the Identity Provider.	
<b>Hostname</b>	Address of the authentication source.	<i>openldap.myserver.com</i>
<b>Port</b>	Port number for the connection.	<i>636 (TLS active) 389 (TLS inactive)</i>
<b>Apply TLS encryption</b>	<i>Active:</i> The communication is TLS encrypted. <i>Inactive:</i> Communication is not encrypted.  Requirements: <ul style="list-style-type: none"> <li>▶ The matching <b>Port</b> must be selected.</li> <li>▶ The server must provide a matching server certificate.</li> </ul>	<i>active</i>

Option	Description	Example
	Default: <i>active</i>	

### 11.3.5.4 RADIUS

RADIUS implementation in the **Identity Service** supports:

- ▶ Client login for applications via IIoT Services
- ▶ User login via Service Engine and Web Engine
- ▶ User login via the Service Configuration Studio of the Identity Service.

Option	Description
<b>Provider Alias</b>	Is needed for unique identification.  The <b>Provider Alias</b> is also used for the login page of the Identity Service. There, the user can select which Identity Provider they want to use for login.  <b>Example:</b> <i>my-radius</i>
<b>Provider description</b>	Optional description of the Identity Provider.
<b>Hostname</b>	The hostname of the RADIUS server.  <b>Example:</b> <i>myradius.mydomain.com</i>
<b>Port</b>	Port number of the RADIUS server.  Default: <i>1812</i>  <b>Note:</b> This option is only visible after a <b>host name</b> has been configured.
<b>Shared Secret</b>	The <b>Shared Secret</b> is used for the encrypted transfer of the user password when logging in to the RADIUS Server.  <b>Example:</b> <i>85NZrL17WRBWVbyn.FDuz_tZ4Yt55..341</i>  (as defined on the Radius server)  <b>Note:</b> This option is only visible after a <b>host name</b> has been configured.
<b>Authentication type</b>	The following authentication methods are supported:



Option	Description
	<ul style="list-style-type: none"> <li>▶ <i>PAP</i></li> <li>▶ <i>CHAP</i></li> </ul> <p>The use of <i>CHAP</i> is recommended.</p> <p>Default: <i>CHAP</i></p> <p><b>Note:</b> This option is only visible after a <b>host name</b> has been configured.</p>
<b>Clear all</b>	All current and unsaved configurations are reset to the default value.
<b>Add new connection</b>	Adds the option to configure a new fallback connection for the configuration dialog.
<b>Add</b>	Applies the configuration and closes the dialog. The configuration is available as a new radius connection for login.

## CONNECTIONS

The first connection for **RADIUS** is the **Primary connection**. This must be configured to use **RADIUS**.

You can also optionally create one or several **Fallback connections**. If the **Primary connection** does not respond to a request, the system attempts to connect via a **Fallback connection**. **Fallback connections** are used in the configured order.

### 11.3.5.4.1 Automatic allocation of RADIUS users to Identity Management groups

Execute the following steps to automatically add RADIUS users to **Identity Management** groups in **Identity Management**:


1. Configure an identity provider.
2. Customize the configuration of the Identity Provider for the allocation of users to Identity Management groups. The RADIUS protocol uses Vendor Specific Attributes to transfer additional information during user login.

The RADIUS server must be configured in such a way that, upon the successful authentication of users, it returns a list of group names to the **Identity Service**. The list of group names must be transferred from the RADIUS server during login using **Vendor Specific Attributes (VSA)**.

The following VSA are supported for RADIUS as the identity provider:

- ▶ **Vendor ID:** 22050

- ▶ **Attribute ID:** 1
  - ▶ **Format of group names:** List with one or more group names (separated by a comma).  
**Examples:** *Group1* or *Administrator,Group2,Group3*
3. Create a new group in **Identity Management**.
  4. Select the configured identity provider from the drop-down list for this group in the **Managed by** option.

 **Information**

Further information on the automatic allocation of users from Identity Provider to Identity Management groups can be found in the **Groups** (on page 181) chapter **Automatic allocation of users to groups when logging in via identity provider** (on page 187).

### 11.3.5.5 OpenID Connect

Option	Description	Example
<b>Provider Alias</b>	Is needed for unique identification.  The <b>Provider Alias</b> is also used for the login page of the Identity Service. There, the user can select which Identity Provider they want to use for login.	
<b>Provider description</b>	Optional description of the Identity Provider.	
<b>Authority</b>	URL at which the OpenID Connect Provider can be contacted.	<i>https://myopenidconnect.com</i>
<b>Client ID</b>	Enter the <b>Client ID</b> defined in the OpenID Connect Provider. This is required by Identity Service to authenticate external users.  <b>Note:</b> The <b>Client ID</b> must be registered in the OpenID Connect Identity Provider .	<b>For example:</b> <i>07c8b99b-fe15-2587-8e58-c1dc85d4fe17</i>  The format of the Client ID depends on the OpenID Connect Provider used.

Option	Description	Example
<b>Client Secret</b>	<p><b>Client Secret</b> that is generated in OpenID Connect and has been assigned to the OpenID Connect <b>Client ID</b>.</p> <p><b>Note:</b> OpenID Connect always creates <b>Client ID</b> and <b>Client Secret</b> in pairs. Identity Service uses this specific combination of pairs to authenticate external users.</p>	<p><b>For example:</b></p> <p><i>85NZrL17WRBWVbyn.FDuz_tZ4Yt55..341</i></p> <p>The format of the Client Secret depends on the OpenID Connect Provider used.</p>

 **Tip**

**Configuration in OpenID Connect**

The configuration dialog displays – adjusted to your system – the following hint:

*Please enter the following redirect URL(s) to your external identity provider:*

*https://mycomputer.mydomain.com:9443/identity-service/auth/my-openid-connect/signin-callback*

*https://mycomputer.mydomain.com:9443/identity-service/auth/my-openid-connect/signout-callback*

You must save your individual URLs in the administration tool of the OpenID Connect Providers as valid Redirect URL(s).

**11.3.5.6 Keycloak**

Option	Description	Example
<b>Provider Alias</b>	<p>Is needed for unique identification.</p> <p>The <b>Provider Alias</b> is also used for the login page of the Identity Service. There, the user can select which Identity Provider they want to use for login.</p>	
<b>Provider description</b>	Optional description of the Identity Provider.	

Option	Description	Example
<b>Authority</b>	The URL which provides Keycloak for user authentication.	<i>https://my-keycloak.com/auth/realms/master</i>
<b>Client ID</b>	Enter the <b>Client ID</b> defined in the Keycloak. This is required by Identity Service to authenticate external users.  <b>Note:</b> The <b>Client ID</b> must be registered in the Keycloak.	<i>identity-service-client</i>  Note: The Client ID is defined by the administrator.
<b>Client Secret</b>	<b>Client Secret</b> that is generated in Keycloak and has been assigned to the <b>Client ID</b> .  <b>Note:</b> <b>Client ID</b> and <b>Client Secret</b> are always required in pairs. <b>Identity Service</b> uses this specific combination of pairs to authenticate external users.	<i>07c8b99b-fe15-2587-8e58-c1dc85d4fe17</i>

### Tip

#### Configuration in Keycloak

The configuration dialog displays – adjusted to your system – the following hint:

*Please enter the following redirect URL(s) to your external identity provider:*

*https://mycomputer.mydomain.com:9443/identity-service/auth/my-keycloak/signin-callback*

*https://mycomputer.mydomain.com:9443/identity-service/auth/my-keycloak/signout-callback*


You must save your individual URLs in the administration tool of Keycloak as valid Redirect URL(s).

### 11.3.5.6.1 Automatic allocation of Keycloak users to Identity Management groups

Execute the following steps to automatically add Keycloak users to **Identity Service** groups in **Identity Management**:

1. Configure an identity provider.

2. Customize the configuration of the Identity Provider for the allocation of users to Identity Management groups.
  - ▶ Customize the **provider-specific configuration** (on page 217).
  - ▶ Configure a **Protocol Mapper on the Keycloak Server** (on page 217).
3. Create a new group in **Identity Management**.
4. Select the configured identity provider from the drop-down list for this group in the **Managed by** option.

 **Information**

Further information on the automatic allocation of users from Identity Provider to Identity Management groups can be found in the **Groups** (on page 181) chapter **Automatic allocation of users to groups when logging in via identity provider** (on page 187).

### 11.3.5.6.2 Provider-specific configuration

Provider-specific configurations for Keycloak:

- ▶ **Access Type** = *confidential*  
**Note:** This settings activates the **Credentials** tab. You require **Client ID** and **Client Secret**.
- ▶ **Implicit Flow Enabled** = *ON*
- ▶ **Standard Flow Enabled** = *ON*
- ▶ **Direct Access Grants** = *ON*

### 11.3.5.6.3 Protocol mapper - configuration of the Keycloak server

You must configure a protocol mapper in the Keycloak server:

1. Go to the administrator console of the Keycloak server that you use.
2. Go to **Clients** -> **Identity-Server** -> **Mappers**.
3. Create a new protocol mapper by clicking **Create**.
4. Configure the protocol mapper with the following settings:

Property	Necessary configuration
<b>Protocol</b>	<i>openid-connect</i> (value is preset)
<b>Name</b>	Enter a name of your choice.

Property	Necessary configuration
	Note: This is an internal name for Keycloak. It is not relevant for <b>Identity Service</b> .
<b>Mapper Type</b>	<i>Group Membership</i>
<b>Token Claim Name</b>	<i>Group</i>
<b>Full group path</b>	<p><i>On or Off</i></p> <p>This setting defines whether, in the case of hierarchically nested groups, the server sends the full group path to <b>Identity Service</b> or only the group names.</p> <p><b>Example:</b></p> <ul style="list-style-type: none"> <li>▶ Group name: <i>Administrators</i></li> <li>▶ Group path: <i>London/Administrators</i></li> </ul> <p>This setting determines which group assignments can be generated (see example (on page 219)).</p>
<b>Add to ID token</b>	Any configuration.
<b>Add to access token</b>	Any configuration.
<b>Add to userinfo</b>	<i>On</i>

You have thus finished configuring the Keycloak server for transferring group assignments to **Identity Management**.



### 11.3.5.6.4 Example: Apply group assignments



Example of the "Full group path -> On" configuration: Identity Service converts the hierarchical group structures of Keycloak into flat group structures.

Case description:



In the Keycloak server, separate administrator groups (*Paris/Administrators* and *London/Administrators*) are defined for the Paris site and the London site.

- ▶ The hierarchical arrangement into the parent groups *Paris* and *London* differentiates the *Administrators* subgroups of the same name. There are two separate subgroups with the same group name.
- ▶ How the two group structures are transferred to **Identity Service** depends on the *Full group path* setting selected in the protocol mapper.

**The configuration options in Keycloak are as follows:**

Keycloak: Group assignments	Keycloak: Configuration	Shared group information	Identity Service: Group assignments
<i>Paris/Administrators;</i> <i>London/Administrators</i>	<b>Full group path</b> -> <i>On</i>  (see graphic)	<i>Paris/Administrators;</i> <i>London/Administrators</i>	<i>Paris;</i> <i>London;</i> <i>Administrators</i>
<i>Paris/Administrators;</i> <i>London/Administrators</i>	<b>Full group path</b> -> <i>Off</i>	<i>Administrators;</i> <i>Administrators</i>	<i>Administrators</i>

**The following applies for the applying of group assignments in this example:**

- ▶ The corresponding group assignment can be made in **Identity Management** for each of the listed Keycloak group assignments.
- ▶ The *Full group path* setting in Keycloak determines which group names are transferred.
- ▶ The hierarchical group structures of Keycloak are converted by **Identity Management** into flat group structures.

The *Administrators* subgroups which are separated in Keycloak are combined into one group with the same name in **Identity Management**.



## 11.3.6 Clients

In the **Clients** menu item, you manage client access to IIoT Services.

**Example:** Third-party applications use the client to connect to IIoT Services via the IIoT API.

### CLIENTS

The table shows the existing client definitions. Only clients that have been created manually are shown there by default.

#### Tip

System clients are created and managed automatically by IIoT Services. They cannot be edited and are hidden in the table by default. You can display the system clients with the **Show system clients** checkbox.

### TABLE

**The table contains the following columns:**

- ▶ Client ID
- ▶ Client name
- ▶ Redirect URLs
- ▶ Grant types
- ▶ Allowed scopes

Each table column offers the option to filter and sort the displayed **Clients**.


**You can do the following in the table:**

- ▶ Add clients (**Add** button, opens the detail view)
- ▶ Edit clients (**Edit** button, opens the detail view)
- ▶ Delete clients (**Delete** button)

### 11.3.6.1 Add new client


In this dialog, you select the type of client that you want to create.

#### Add new client




**Service Engine**

Create a Service Engine client to connect the Service Engine with the Identity Service or Data Storage.




**Report Engine**

Create a Report Engine client to connect the Report Engine with the Identity Service or Data Storage.



**HTML Web Engine**

Create an HTML Web Engine client to connect the HTML Web Engine to the Identity Service.



**Custom OAuth 2.0 client**

Create a custom OAuth 2.0 client to connect to the Identity Service or IIoT API.

Cancel

Option	Description
Service Engine	Opens the configuration dialog for a new Service Engine client.
Report Engine	Opens the configuration dialog for a new Report Engine client.
HTML Web Engine	Opens the configuration dialog for a Web Engine client.
Custom OAuth 2.0 client	Opens the configuration dialog for a new OAuth client.
Cancel	Closes the selection dialog

### 11.3.6.1.1 Service Engine

In this dialog, you configure a new client for logging in to Service Engine.

## Add new client

Client ID \*

ID of the client. Must be unique (3-50 characters)

Client name \*

Name of the client (3-100 characters)

Secret

QLqC/r+uV5leO6tAMjXFrP6JpbzqlG5Jy4MfcQcX9uC75fRoZeVjVR+K7SUdVbtPDyQIn0yhL6haUU/yFDuHA==



Do not forget to copy the Secret. It cannot be viewed again.

\* This field is required.

Cancel

Add

Option	Description
<p><b>Client ID</b></p>	<p>Unique ID of the client. The ID must be unique and can contain numbers, letters, and special characters.</p> <p>If there is already a client with the same ID, the client will not be created and a corresponding warning will be displayed.</p> <p>The required length is at least 3 characters and no more than 50 characters.</p>
<p><b>Client name</b></p>	<p>User-defined name of the client. The name must contain at least 3 characters and may not be longer than 50 characters.</p>
<p><b>Secret</b></p>	<p>The <b>Secret</b> is created automatically by the system. The client application uses the Client ID and the Secret to authenticate itself with the <b>Identity Service</b> successfully.</p> <p><b>Attention:</b> The Secret is only displayed when the entry is initially created. If the entry is edited again at a later time, it is no longer displayed. Ensure that you can also access the Secret later (by saving it as a text file, for example). You need the Secret to configure the client application accordingly.</p> <p>If needed, you can use the dialog to have a new Secret generated.</p>

Option	Description
	<b>Note:</b> only available if an existing client is changed. This symbol is not available during the initial configuration of a client.
<b>Renew Secret (symbol)</b>	Generates a new Secret for the client. Each click generates a new Secret.  <b>Note:</b> This button is only available when editing an already existing client.
<b>Copy to clipboard (symbol)</b>	Copies the Secret to the clipboard.

#### NAVIGATION

Button	Description
<b>Cancel</b>	Discards all inputs and closes the dialog.
<b>Add</b>	Closes the dialog. The client is created with the current configuration.  <b>Note:</b> This button is only active if the dialog has been configured with valid inputs.

### 11.3.6.1.2 Report Engine

In this dialog, you configure a client for Report Engine login for the Identity Service.

#### Add new client

**Client ID\***

ID of the client. Must be unique (3-50 characters)

**Client name\***

Name of the client (3-100 characters)

**Report Engine hostname\***

FQDN of the Report Engine

**GraphQL Interface port\***

50793

Port of the GraphQL interface (default: 50793)

**Secret**

hk6bZfZ/8zSAZljdw9ZbpHCD0+hMYPKpF/nsmNZwxEOtdfyUp1TCzn8WGleR0mOvOPOP3C9v44pHbcB7ETqCjg==

Do not forget to copy the Secret. It cannot be viewed again.

**Advanced options** ^

CORS origin URL +

Allowed URL for CORS access

\* This field is mandatory.

Option	Description
<b>Client ID</b>	<p>Unique ID of the client. The ID must be unique and can contain numbers, letters, and special characters.</p> <p>If there is already a client with the same ID, the client will not be created and a corresponding warning will be displayed.</p> <p>The required length is at least 3 characters and no more than 50 characters.</p>
<b>Client name</b>	<p>User-defined name of the client. The name must contain at least 3 characters and may not be longer than 50 characters.</p>
<b>Report Engine hostname</b>	<p>FQDN of the Report Engine that the client will use for the</p>

Option	Description
	login to the Identity Service.
<b>GraphQL Interface port</b>	Port number for communication to the GraphQL interface.  Default: 50793
<b>Secret</b>	<p>The <b>Secret</b> is created automatically by the system. The client application uses the Client ID and the Secret to authenticate itself with the <b>Identity Service</b> successfully.</p> <p><b>Attention:</b> The Secret is only displayed when the entry is initially created. If the entry is edited again at a later time, it is no longer displayed. Ensure that you can also access the Secret later (by saving it as a text file, for example). You need the Secret to configure the client application accordingly.</p> <p>If needed, you can use the dialog to have a new Secret generated.</p> <p><b>Note:</b> only available if an existing client is changed. This symbol is not available during the initial configuration of a client.</p>
<b>Renew Secret (symbol)</b>	<p>Generates a new Secret for the client. Each click generates a new Secret.</p> <p><b>Note:</b> This button is only available when editing an already existing client.</p>
<b>Copy to clipboard (symbol)</b>	Copies the Secret to the clipboard.

**ADVANCED OPTIONS**

Option	Description
<b>CORS origin URL</b>	<p>URL of the host or domain used to access the <b>GraphQL Interface</b>.</p> <p><b>Example:</b> <i>https://mywebsite.com</i> or for on-premises deployment, <i>https://[FQDN]:12345</i></p> <p>This is the only allowed CORS source to access the <b>Identity Service</b>..</p>
+	Adds a new entry for the configuration of a new CORS URL.

Option	Description
x	Deletes the configuration of the entry.

**NAVIGATION**

Button	Description
Cancel	Discards all inputs and closes the dialog.
Add	<p>Closes the dialog. The client is created with the current configuration.</p> <p><b>Note:</b> This button is only active if the dialog has been configured with valid inputs.</p>

### 11.3.6.1.3 HTML Web Engine

In this dialog, you configure a client for HTML Web Engine login to the **Identity Service**.

#### Add new client

**Client ID\***

---

ID of the client. Must be unique (3-50 characters)

**Client name\***

---

Name of the client (3-100 characters)

**HTML Web Engine URL\***

---

URL of HTML Web Engine (optionally with port)

\* This field is mandatory.

Cancel

Add

Option	Description
Client ID	<p>Unique ID of the client. The ID must be unique and can contain numbers, letters, and special characters.</p> <p>If there is already a client with the same ID, the client will not be created and a corresponding warning will be displayed.</p> <p>The required length is at least 3 characters and no more than 50 characters.</p>

Option	Description
	<p><b>Recommendation:</b> For optimum cooperation with the components of the zenon software platform, it is recommended that this option is configured with the <i>WebEngineClient</i> entry. <i>WebEngineClient</i> is, for example, the default value for authentication via the Identity Service of the Web Visualization Service.</p> <p>The configuration of this option must correspond to the configuration for the <b>HTML Web Engine</b> and the INI entry <b>WebEngineIdentityClient=</b>.</p>
<b>Client name</b>	User-defined name of the client. The name must contain at least 3 characters and may not be longer than 50 characters.
<b>HTML Web Engine URL</b>	<p>FQDN of the HTML Web Engine that the client will use for login to the Identity Service.</p> <p>Optional entry of the port. The URL and port are separated with a colon (:).</p> <p>Default port: 443 (IIS) or 9500 (Docker)</p> <p><b>Example:</b> <i>https://HTMLwebEngineUrl:443</i></p>

**NAVIGATION**

Button	Description
<b>Cancel</b>	Discards all inputs and closes the dialog.
<b>Add</b>	<p>Closes the dialog. The client is created with the current configuration.</p> <p><b>Note:</b> This button is only active if the dialog has been configured with valid inputs.</p>



### 11.3.6.1.4 Custom OAuth 2.0 client

In this dialog, you configure a client for logging in via OAuth.

#### Add new client

Client ID\*

ID of the client. Must be unique (3-50 characters)

Client name\*

Name of the client (3-100 characters)

Grant types\*

ClientCredentials

Allowed authentication flow

Allowed scopes

Predefined or custom-defined scopes

Secret

6MzQWtP88tC2HvixE0XeYuBIVYWhJaUo+dyNPKuFgpCwsxcYkdQ/CM4TL3zYldX28I+9EzKmYpwWFJGpGC4b7Q==

Do not forget to copy the Secret. It cannot be viewed again.

\* This field is mandatory.

Cancel
Add

Option	Description
<b>Client ID</b>	<p>Unique ID of the client. The ID must be unique and can contain numbers, letters, and special characters.</p> <p>If there is already a client with the same ID, the client will not be created and a corresponding warning will be displayed.</p> <p>The required length is at least 3 characters and no more than 50 characters.</p>
<b>Client name</b>	<p>User-defined name of the client. The name must contain at least 3 characters and may not be longer than 50 characters.</p>
<b>Grant types</b>	<p>Client authentication method.</p> <p>Select from drop-down list:</p> <ul style="list-style-type: none"> <li>▶ <i>Implicit</i></li> <li>▶ <i>Code</i></li> <li>▶ <i>ClientCredential</i></li> </ul>

Option	Description
	<ul style="list-style-type: none"> <li>▶ <i>RessourceOwnwerPassword</i></li> <li>▶ <i>DeviceFlow</i></li> <li>▶ <i>CodeAndDeveLogin</i></li> </ul> <p>Default: <i>ClientCredentials</i></p> <p>You can find a detailed overview in the <b>Grant types</b> (on page 235) chapter.</p>
<b>Allowed scopes</b>	<p>Configure the access for access tokens. The scope defines which data a client application can access on behalf of the user.</p> <p>Selection from drop-down list; multiple selection is possible:</p> <ul style="list-style-type: none"> <li>▶ <i>openid</i></li> <li>▶ <i>profile</i></li> <li>▶ <i>email</i></li> <li>▶ <i>role</i></li> <li>▶ <i>groups</i></li> <li>▶ <i>identityAPI.read_only</i></li> <li>▶ <i>identityAPI.full_access</i></li> <li>▶ <i>iiotServicesAPI</i></li> <li>▶ <i>certificateManagementAPI</i></li> <li>▶ <i>platformConfigurationAPI</i></li> <li>▶ <i>dataStorageAPI</i></li> <li>▶ <i>graphQLInterface</i></li> <li>▶ <i>deviceManagementAPI</i></li> <li>▶ <i>dataModelingAPI</i></li> <li>▶ <i>offline_access</i></li> </ul> <p>You can find a detailed overview of the pre-configured scopes in the <b>Allowed scopes</b> chapter.</p>
<b>PCKE required</b>	<p>Only visible if one of the following <b>Grant types</b> has been selected in the <b>Grant types</b> option: <i>Code</i>, <i>CodeAndDeviceLogin</i></p>

Option	Description
<b>Client secret required</b>	Only visible if one of the following <b>Grant types</b> has been selected in the <b>Grant types</b> option: <i>Code, DeviceFlow, CodeAndDeviceLogin</i>
<b>Redirect URL</b>	<p>Defines the URLs to which the <b>Identity Service</b> can forward the user after successful authentication. This is a security feature.</p> <p>Only visible if one of the following <b>Grant types</b> has been selected in the <b>Grant types</b> option: <i>Code, CodeAndDeviceLogin</i></p>
<b>Secret</b>	<p>The <b>Secret</b> is created automatically by the system. The client application uses the Client ID and the Secret to authenticate itself with the <b>Identity Service</b> successfully.</p> <p><b>Attention:</b> The Secret is only displayed when the entry is initially created. If the entry is edited again at a later time, it is no longer displayed. Ensure that you can also access the Secret later (by saving it as a text file, for example). You need the Secret to configure the client application accordingly.</p> <p>If needed, you can use the dialog to have a new Secret generated.</p> <p><b>Note:</b> only available if an existing client is changed. This symbol is not available during the initial configuration of a client.</p>
<b>Renew Secret (symbol)</b>	<p>Generates a new Secret for the client. Each click generates a new Secret.</p> <p><b>Note:</b> This button is only available when editing an already existing client.</p>
<b>Copy to clipboard (symbol)</b>	Copies the Secret to the clipboard.
<b>Allow access tokens via browser</b>	<p>Here you stipulate whether access tokens are permitted for browser access or not.</p> <p><b>Hint:</b> This option must be activated for browser access or Webview.</p> <p>Only visible if one of the following <b>Grant types</b> has been selected in the <b>Grant types</b> option: <i>Implicit, Code,</i></p>

Option	Description
	<i>CodeAndDeveLogin, DeviceFlow</i>

### ADVANCED OPTIONS

The display of this option depends on the configuration of the **Allowed scopes** option.

Option	Description
<b>Allowed URL for CORS access</b>	<p>URL of the host or domain used to access the <b>GraphQL Interface</b>.</p> <p><b>Example:</b> <i>https://mywebsite.com</i> or for on-premises deployment, <i>https://[FQDN]:12345</i></p> <p>This is the only allowed CORS source to access the <b>Identity Service</b>..</p> <p>Only visible if one of the following <b>Grant types</b> has been selected in the <b>Grant types</b> option:<i>Implicit, Code, DeviceFlow, CodeAndDeviceLogin</i></p>
<b>Logout notification Type</b>	<p>This defines the type and manner in which a client signs out the user from <b>Identity Service</b> in accordance with OpenID Connect.</p> <p>There are three options in the drop-down menu:</p> <ul style="list-style-type: none"> <li>▶ <i>None</i> (default setting)</li> <li>▶ <i>Frontchannel</i></li> <li>▶ <i>Backchannel</i></li> </ul> <p>Only visible if one of the following <b>Grant types</b> has been selected in the <b>Grant types</b> option:<i>Implicit, Code, DeviceFlow, CodeAndDeviceLogin</i></p>
<b>Allowed post logout redirect URL</b>	<p>Defines the URLs to which the <b>Identity Service</b> can forward the user after being logged out successfully. This is a security feature.</p> <p>Only visible if one of the following <b>Grant types</b> has been selected in the <b>Grant types</b> option:<i>Implicit, Code, DeviceFlow, CodeAndDeviceLogin</i></p>
<b>+</b>	Adds a new entry for the configuration of an additional option.
<b>x</b>	Deletes the configuration of the entry.

**NAVIGATION**

Button	Description
Cancel	Discards all inputs and closes the dialog.
Add	<p>Closes the dialog. The client is created with the current configuration.</p> <p><b>Note:</b> This button is only active if the dialog has been configured with valid inputs.</p>

### 11.3.6.2 Allowed scopes

**Allowed scopes** define the access for access tokens. The scope defines which data a client application can access on behalf of the user.

#### A) SELF-DEFINED SCOPES

You can also define your own scopes. To do this, enter the name of the scope into the text field directly and confirm the process with the **Enter** key.

#### B) PRE-DEFINED SCOPES

**Important:** The pre-defined **Allowed scopes** only work in conjunction with certain **Grant types**. Only use permitted combinations of **Allowed scopes** and **Grant types** (on page 237).

Scope	User context*	Description
<b>openid</b>	yes	<p>You need this scope if you want to log in via OpenID. The <i>openid</i> scope shows that the application uses OpenID to verify the identity of the user.</p> <p>This scope is also used for authentication in Service Engine, Report Engine, access via GraphQL interface and the HTML Web Engine with IIoT Services.</p>
<b>profile</b>	yes	<p>The application can request the user's profile information with the <i>profile</i> scope.</p> <p>This scope is also used for authentication in Service Engine, Report Engine, access via GraphQL interface and the HTML Web Engine with IIoT Services.</p>
<b>email</b>	yes	The application can request the user's email address

Scope	User context*	Description
		with the <i>email</i> scope.
<b>offline_access</b>	yes	<p>The application can request refresh tokens (on page 235) with the <i>offline_access</i> scope.</p> <p>This scope is also used for authentication in Service Engine, Report Engine, access via GraphQL interface and the HTML Web Engine with IIoT Services.</p> <p><b>Note:</b> The client application can only access IIoT Services online. The name <i>offline_access</i> for the scope is misleading in this respect.</p>
<b>iiotServicesAPI</b>	no	The application can access the IIoT API with the <i>iiotServicesAPI</i> scope. The application can thus query variables from < NAME_SERVICE_ENGINE > (on page 295), for example.
<b>identityAPI.full_access</b>	no	The <i>identityAPI.full_access</i> scope is reserved for system-related purposes.
<b>identityAPI.read_only</b>	no	The <i>identityAPI.read_only</i> scope is reserved for system-related purposes.
<b>dataStorageAPI</b>	no	<p>The application may access the data storage with the <i>dataStorageAPI</i> scope.</p> <p>The scope is needed for the client definition of a Service Engine, a Report Engine and queries via GraphQL interface.</p>
<b>role</b>	yes	
<b>groups</b>	yes	With the <i>groups</i> scope, the application can query group dependencies for the logged-in user.
<b>certificateManagementAPI</b>	no	The <i>certificateManagementAPI</i> scope is reserved for system-related purposes.
<b>platformConfigurationAPI</b>	no	The <i>platformConfigurationAPI</i> scope is reserved for system-related purposes.
<b>graphqlInterface</b>	no	<p>The application may access the data storage with the <i>graphqlInterface</i> scope.</p> <p>The scope is required for the client definition of a Service Engine.</p>

Scope	User context*	Description
		When opening the GraphQL interface without authentication data, the user is forwarded to the login page of the <b>Identity Service</b>
<b>deviceManagementAPI</b>	no	The <i>deviceManagementAPI</i> scope is reserved for system-related purposes.
<b>dataModellingAPI</b>	no	The <i>dataModellingAPI</i> scope is reserved for system-related purposes.

\***Grant type** with user context is required

### 11.3.6.2.1 Refresh tokens and offline\_access

An OAuth 2.0 client application can request Refresh Token. The application can remain logged in on a lasting basis with Refresh Token.

## TIME VALIDITY OF ACCESS TOKENS

Access tokens for a client application always have a time limit. The application logs out automatically after this time period. The client application can avoid this automatic logout if it requests a new access token by means of a refresh token.

## CONFIGURATION OF THE CLIENT

### To configure a client application for the Refresh Token request:

1. Create the client in **Identity Management**.
2. Enter the following for the **Allowed scopes** option: *offline\_access*.

The client application can thus request Refresh Token.

### 11.3.6.3 Grant types

You determine which authentication flow the client uses in the **Grant types**.

Important: The **Grant types** only work in conjunction with certain **Allowed scopes**. Only use permitted combinations of **Allowed scopes** and **Grant types** (on page 237).

Grant type	User context	Description
<i>Implicit</i>	yes	Interactive authentication: Is required if the client implements the authentication using a

Grant type	User context	Description
		browser.
<i>Code</i>	yes	Authorization code according to <i>OAuth 2.0</i> specification.
<i>ClientCredentials</i>	no	Authentication of the client by means of <b>Client ID</b> and <b>Secret</b> .
<i>ResourceOwnerPassword</i>	yes	Authentication via user name and password. They are also sent in the authentication request.
<i>DeviceFlow</i>	yes	The <i>DeviceFlow</i> option can also be used to enable devices without a browser or with otherwise limited input possibilities to request an Access Token.  Is also used for the client definition in Service Engine or Report Engine.
<i>CodeAndPkce</i>	yes	Combination: <i>Code</i> and <i>Pkce</i> .  <i>Pkce</i> is the abbreviation for <i>Proof Key for Code Exchange</i> . The use of <i>Pkce</i> increases security in certain cases.
<i>ServiceEngineFlow</i>	yes	Combination of the types <i>ClientCredentials</i> and <i>ResourceOwnerPassword</i> . Is used in the client definition of a Service Engine.
<i>ReportEngineFlow</i>	yes	Combination of the types <i>dataStorageAPI</i> , <i>openid</i> , <i>graphqlInterface</i> .  Is used with the client definition for a Report Engine as well as for queries via GraphQL interface.
<i>WebEngineFlow</i>	yes	Combination of the types <i>CodeAndPkce</i> and <i>ResourceOwnerPassword</i> .  Is used in the client definition of a Service Engine.



### 11.3.6.4 Permitted combinations: "Allowed scopes" and "Grant types"

A functional client configuration needs **Allowed scopes** and **Grant types** to suit one another. During configuration, it is necessary to check whether the selected **Grant type** has a user context or not.

#### Hint

You can find out whether a **Grant type** has a user context from the corresponding table (on page 235).

### GRANT TYPES WITH USER CONTEXT

You can combine **Grant types** with a user context (such as *Implicit*, *Code*, *DeviceFlow* for example) with desired **Allowed scopes**.

You can also expressly combine **Grant types** that have user context with **Allowed scopes** that do not have user context.

### GRANT TYPES WITHOUT USER CONTEXT

You can only combine **Grant types** without user context (*ClientCredentials* for example) with **Allowed scopes** without user context (*serviceGridAPI*, *identityAPI.full\_access* for example).

#### Attention

It is technically possible to configure a client with a non-permitted combination of **Allowed scopes** and **Grant types**. This leads to authorization problems when accessing the IIoT API however.

### 11.3.7 Settings

You can configure the password requirements in this dialog.

#### Settings

Password requirements

Minimum length\*  
 8

Uppercase letters\*  
 1

Lowercase letters\*  
 1

Digits\*  
 1

Special characters\*  
 1

Reset all to defaults
Undo
Apply

#### PASSWORD REQUIREMENTS

In this option group, you can configure the minimum requirements for a password.

Option	Description
<b>Minimum length</b>	Minimum number of characters, numbers or special characters that a password must contain in order to be valid.  Default: 8
<b>Uppercase letters</b>	Minimum number of upper-case letters that a password must contain in order to be valid.  Default: 1
<b>Lowercase letters</b>	Minimum number of lower-case letters that a password must contain in order to be valid.  Default: 1
<b>Digits</b>	Minimum number of numbers that a password must contain in order to be valid.  Default: 1
<b>Special characters</b>	Minimum number of special characters that a password must contain in order to be valid.



Option	Description
	<ul style="list-style-type: none"> <li>▶ <i>Inactive</i>: No additional configurations for the validity of a password or the notification before expiry.</li> </ul> <p>Default: <i>inactive</i></p>
<b>Minimum lifetime in days</b>	<p>Number of days for the minimum validity of a password. The user can configure a new password here at the earliest after expiry of the value configured here.</p> <p>Default: <i>0 (= unlimited)</i></p> <p><b>Note:</b> This button is only available if the <b>Enforce password lifetime</b> option has been activated.</p>
<b>Maximum lifetime in days</b>	<p>Number of days for the maximum validity of a password. The user must configure a new password at the latest on expiry of the value configured here.</p> <p>Default: <i>90</i></p> <p><b>Note:</b> This button is only available if the <b>Enforce password lifetime</b> option has been activated.</p>
<b>Notification before expiration of password in days</b>	<p>Number of days for the notification of expiry of a password. The notification (on page 243) is visualized on login to the Identity Service.</p> <p>Default: <i>14</i></p> <p><b>Note:</b> This button is only available if the <b>Enforce password lifetime</b> option has been activated.</p>

## LOGIN RULES

Additional setting for the locking of the login.

**Note:** You can also combat attacks and interventions from outside with the settings in this group. This can however lead to a user being locked without the user knowing why they are locked. In this case, the user was probably locked due to a brute force attack with too many invalid login attempts.

**Login rules**

Max. login tries before block\* i  
3

User block duration in minutes\* i  
1

**User settings**

Default option for login linking of new users\*  
Not allowed ▼

Option	Description
<b>Max. login tries before block</b>	Number of incorrect login attempts. The user is locked out of login when the configured number is reached. The duration of the lock is configured in the <b>User block duration in minutes</b> option.  Default: 3
<b>User block duration in minutes</b>	Time duration in minutes that a user must wait after an automatic lock of their login before the lock is rescinded and the user can log in again.  Default: 1

**USER SETTINGS**

**User settings**

Default option for login linking of new users\*  
Not allowed ▼

Option	Description
<b>Default option for login linking of new users</b>	Option for configuring the global default setting for the linking of external <b>identity providers</b> when creating new users.  Select from drop-down list: <ul style="list-style-type: none"> <li>▶ <i>Allowed:</i> The user can link their login to external providers.</li> </ul> <b>Note:</b> In order for the user to be able to use external providers, the <b>Allow login linking of Identity Providers</b> option must be activated for the

Option	Description
	user in the <b>Edit local User</b> (on page 178) dialog. <ul style="list-style-type: none"> <li>▶ <i>Not allowed</i>: The user cannot use their login with external providers (on page 207).</li> </ul> Default: <i>Not allowed</i>

## BUTTONS

Buttons for the configuration of the settings.

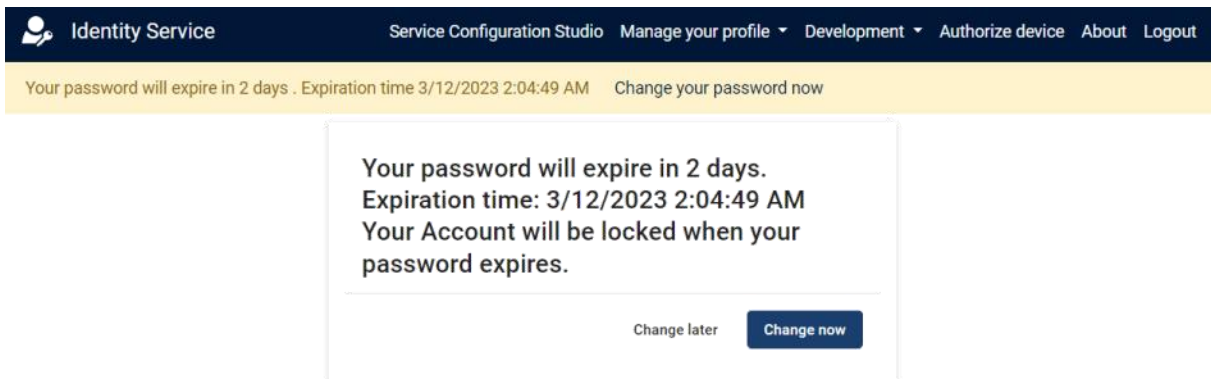
Button	Description
<b>Reset all to defaults</b>	Resets all the configurations for this dialog back to the respective default values. <b>Note:</b> Only active if at least one default value has been changed.
<b>Undo</b>	Resets all current and unsaved changes to the configuration back to the respective default value. <b>Note:</b> Only active if at least one default value has been changed.
<b>Apply Changes</b>	Applies the current configurations. <b>Note:</b> Only active if at least one default value has been changed. In addition, this button is only active if there is no incorrect configuration.



### Information

The password complexity is applicable to Identity Service users. Users for external providers are subject to the password stipulations of the respective provider.

### 11.3.7.1 Password renewal - visualization



This display shows the notification for an expired password.

Option	Description
Change your password now	Opens the dialog to enter a new password.
Change later	Ignores the current notification. The user continues to use the existing password.
Change now	Opens the dialog to enter a new password.

### 11.3.8 Navigation bar

The buttons in the navigation bar offer the following options:

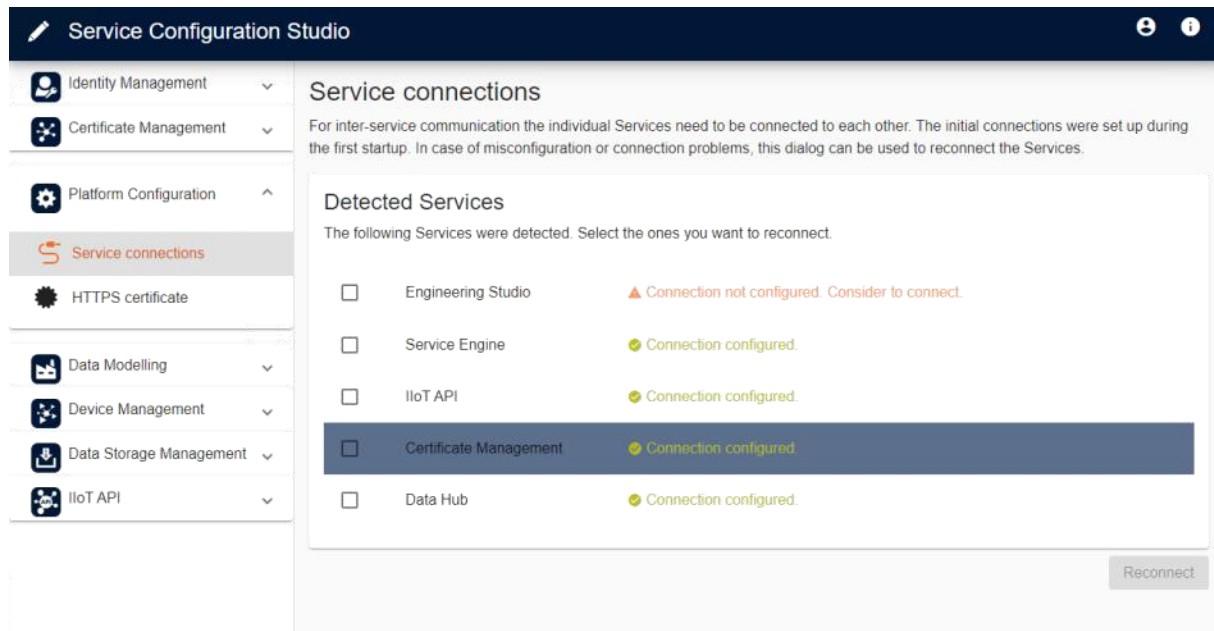
- ▶ **User profile:** Directs the logged-in user to their profile page in the **Identity Service** (on page 159).
- ▶ **Logout:** Logs out of **Identity Service** (on page 173)
- ▶ **About:** Displays the installed version of the **Identity Service** and the license status.

## 12 Platform configuration

The platform configuration supports the following configurations:

- ▶ Reconfiguration of existing connections to IIoT Services.
- ▶ Configuration of self-signed or externally-provided HTTPS certificates.

## 12.1 Service connections



This page lists the IIoT Services found that connect to the **Data Hub**.

### ⚠ Attention

If a new connection for the **Data Hub** is configured, it may take up to a maximum of 60 seconds until the **Data Hub** has applied the changes and properly allows connections to other services again.

### LIST OF CONNECTIONS FOUND

All IIoT Services that were found during the initial installation of IIoT Services on the system are listed.

### CONNECTION STATE

The state of each of the individual connections is shown in text and color.

- ▶ *Connection configured* (in green)  
Configured and valid connections.
- ▶ *Connection not configured. Consider to connect* (in orange)  
Connections that were found but were not connected.
- ▶ *Connection expired at [date of expiration]* (in red)  
Configured, valid connections whose validity will expire shortly. This display is shown three months before expiry.



## RECONNECT BUTTON

This button reconnects existing connections.

**Note:** Only active if at least one connection has been selected.

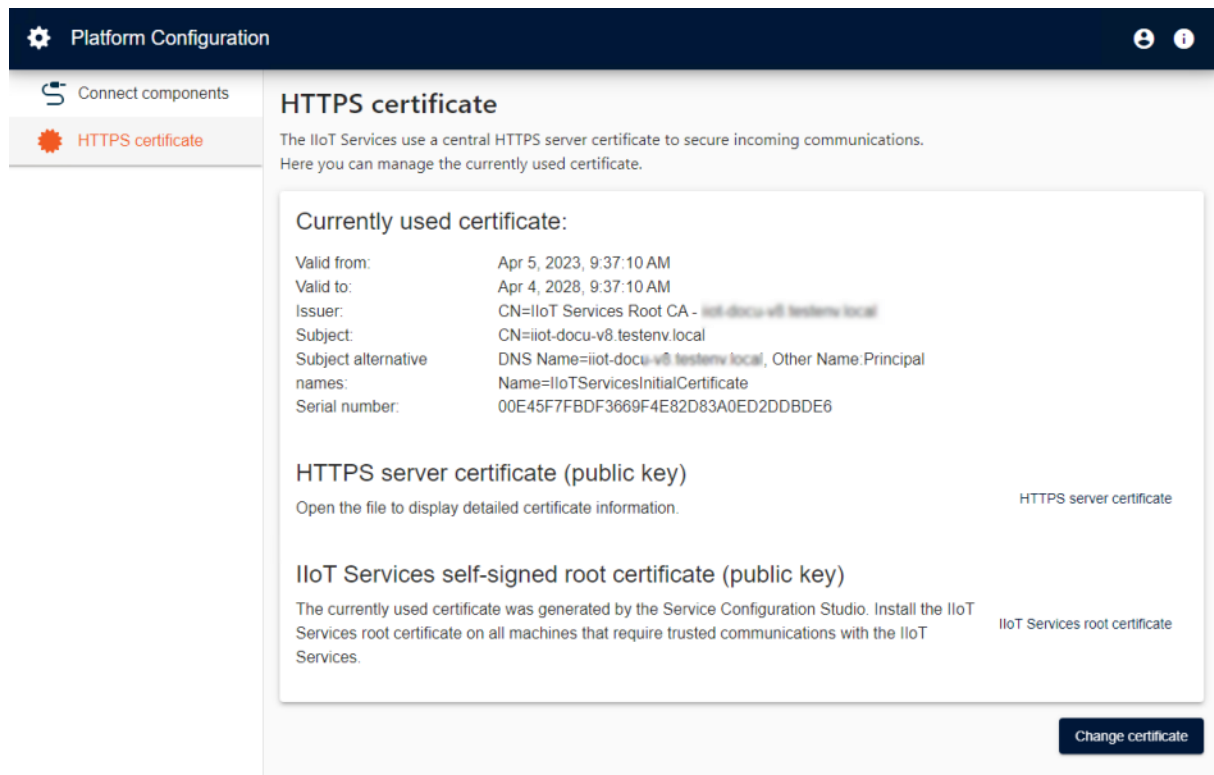
## LINK NEW CONNECTION

Carry out the following steps if you want to link a new connection.

1. Activate the checkbox for the desired connection.  
Note: Multiple selection is possible.
- ▶ Click on the **Reconnect** button.  
The connection is reconnected and the state adjusted accordingly.

## 12.2 HTTPS certificate

In this section, you can make changes to the configuration of the HTTPS certificate used.



The screenshot shows the 'Platform Configuration' interface with a sidebar on the left containing 'Connect components' and 'HTTPS certificate'. The main content area is titled 'HTTPS certificate' and contains the following information:

The IIoT Services use a central HTTPS server certificate to secure incoming communications. Here you can manage the currently used certificate.

**Currently used certificate:**

Valid from:	Apr 5, 2023, 9:37:10 AM
Valid to:	Apr 4, 2028, 9:37:10 AM
Issuer:	CN=IIoT Services Root CA - iiot-docu-v8 testenv.local
Subject:	CN=iiot-docu-v8.testenv.local
Subject alternative names:	DNS Name=iiot-docu-v8.testenv.local, Other Name:Principal
Serial number:	00E45F7FBDF3669F4E82D83A0ED2DDBDE6

**HTTPS server certificate (public key)**  
Open the file to display detailed certificate information. [HTTPS server certificate](#)

**IIoT Services self-signed root certificate (public key)**  
The currently used certificate was generated by the Service Configuration Studio. Install the IIoT Services root certificate on all machines that require trusted communications with the IIoT Services. [IIoT Services root certificate](#)

[Change certificate](#)

The initial certificate is created by default the first time the **IIoT Services** are started.

## HTTPS CERTIFICATE

The following actions are available for the HTTPS certificate:

- ▶ Create and use a new IIoT Services Self-signed HTTPS Certificate

- ▶ Import and use a Third-party HTTPS Certificate

Certificate files for a third-party certificate must meet the following requirements:

- ▶ File format: PFX and P12 are permitted
- ▶ Contains private key and public key
- ▶ Supports server authentication (1.3.6.1.5.5.7.3.1)
- ▶ Certificate must be valid

A certificate with or without password protection can be used. If a certificate file is imported without password protection, you must leave the password field empty.

### CURRENTLY USED CERTIFICATE

This section shows information about the HTTPS certificate currently being used.

Option	Description
<b>Valid from:</b>	Start date of the validity of the certificate.
<b>Valid to:</b>	End date of the validity of the certificate.
<b>Issuer</b>	Name of the certificate issuer, certification instance and FQDN.  Default: <i>IloT Services Root CA - [FQDN]</i>
<b>Subject</b>	FQDN of the certificate owner.
<b>Subject alternative names</b>	Alternative names of certificate holder, for example, additional domains.
<b>Serial number</b>	Unique number for identifying the certificate.

### HTTPS SERVER CERTIFICATE (PUBLIC KEY)

You can download the server certificate in this section.

Button	Description
<b>HTTPS server certificate</b>	Downloads the HTTPS server certificate currently being used.

### IloT SERVICES SELF-SIGNED ROOT CERTIFICATE (PUBLIC KEY)

You can download the IloT Services root certificate in this section.

This section is only displayed if the currently-used HTTPS certificate is a self-signed HTTPS certificate and was created by IloT Services.

This certificate must be installed for successful trust with IIoT Services. You can find further information on this in the **Trust** (on page 259) node and in the **Configure trust** (on page 261) node.

Button	Description
IIoT Services root certificate	Downloads the server certificate currently present.

## CHANGE CERTIFICATE

Button to replace the certificate used. Click on Change Certificate to open the **dialog to configure certificates** (on page 247).

### 12.2.1 Change HTTPS certificate

In this area, you can change the HTTPS certificate used. A new certificate with changed parameters can be created or an existing certificate can be uploaded. The input fields depend on the option selected.

**Change certificate**
x

Select an option from the drop-down list.

Create self-signed certificate
▼

---

The Service Configuration Studio generates a new self-signed HTTPS server certificate. This will replace the currently used certificate.

**Trust**  
To establish trusted communications with the IIoT Services, you need to install the root certificate on any machine that communicates with the IIoT Services.

**Note:** The root certificate remains the same, even if you create a new self-signed HTTPS server certificate.

**Domain names**  
Provide all domains applicable to this IIoT Services installation.

Domain \*
x

iiot-docu-v8.testenv.local

Add domain

Configure

Option	Description
X	Closes the configuration dialog. <b>Caution:</b> all unsaved changes are lost.

Option	Description
<b>Certificate type</b>	<p>Selection of the certificate type that is to be edited or uploaded</p> <ul style="list-style-type: none"> <li>▶ <i>Create self-signed certificate</i> Creates a new self-signed certificate</li> <li>▶ <i>Use custom certificate</i> Uploads an existing certificate. If the certificate used is encrypted, the corresponding password for successful use must be saved in the <b>Password (optional)</b> option.</li> </ul>
<b>Domain</b>	<p>This value is used as the certificate owner in the certificate to be created.</p> <p>Enter the domain name with which IIoT Services can be reached by other computers.</p> <p><b>Note:</b> Only available if <i>Create self-signed certificate</i> is selected as the certificate type.</p>
<b>Add domain</b>	<p>Add an input field to configure an additional domain.</p> <p><b>Note:</b> Only available if <i>Create self-signed certificate</i> is selected as the certificate type.</p>
<b>X</b>	<p>Removes the selected domain entry.</p> <p><b>Note:</b> Only available if <i>Create self-signed certificate</i> is selected as the certificate type.</p>
<b>Import</b>  <b>Drag &amp; Drop the certificate here or click to browse</b>	<p>Field to upload an already existing certificate:</p> <ul style="list-style-type: none"> <li>▶ Clicking on this area opens the file selection dialog to upload an existing certificate file.</li> <li>▶ Dragging and dropping a certificate file in this area uploads the certificate.</li> </ul> <p>Please check the requirements for a certificate in the <b>Certificates</b> section.</p> <p><b>Note:</b> Only available if <i>Use custom certificate</i> is selected as the certificate type.</p>

Option	Description
<b>Password (optional)</b>	Entry of the certificate password if the uploaded certificate is encrypted with a password. The display is masked and validated. In the case of errors, this is displayed with a red bar under the password entry.  <b>Note:</b> Only available if <i>Use custom certificate</i> is selected as the certificate type.
<b>Eye icon</b>	Shows the password for verification in plain text.  <b>Note:</b> Only available if <i>Use custom certificate</i> is selected as the certificate type.
<b>Configure</b>	Applies the configured settings.  With the <i>Create self-signed certificate</i> option: Creates the new HTTPS certificate with the parameters entered.  With the <i>Use custom certificate</i> option: Applies the HTTPS certificate supplied.  A confirmation dialog is shown when clicking on the button.

## CONFIRMATION DIALOG

Dialog to apply or discard the new certificate settings.

Configure new certificate

Do you want to replace the currently used HTTPS certificate with the configured option?

Cancel

Option	Description
<b>Cancel</b>	Discards all changes and closes the dialog.
<b>Configure</b>	Applies settings and closes the dialog.

## DIALOG - DOWNLOAD NEW CERTIFICATE

A dialog is also shown after changing a certificate and confirming this with Configure. In this dialog, you can download the newly-used certificate.

### ⚠ Attention

Only download the newly-generated HTTPS certificate if you need it for your storage or data archive. This file contains the private certificate key and must therefore be treated with extreme caution due to security concerns. Loss or unintended publication of this file can lead to considerable security problems in IIoT Services and to potential attacks on your IIoT Services as well as your complete infrastructure.

#### HTTPS server certificate (.pfx)

Download and store the self-signed HTTPS certificate if required. It contains the private key and must therefore be protected from unauthorized access. A leaked private key will compromise the security of the system.

**Attention: Download the certificate only if you absolutely need it. You will not be able to access the certificate afterwards.**

Download HTTPS certificate as PFX

Option	Description
Download HTTPS certificate as PFX	The newly-created certificate, including the private key, is downloaded.

## 12.2.2 Change "Issued by" for custom certificate

The issuer of the certificate is generated with *IIoT Services Root CA* by default. The suffix (= issued by) is created as with - *[FQDN]* by default.

This suffix can be configured in a Docker environment with the help of an environment variable for the **Platform Configuration Service**. This is not included in the docker compose YAML file by default.

Carry out the following configuration in the `docker-compose.yml` file in order to configure the suffix using the environment variable:

1. Open the `docker-compose.yml` file.
2. Add the following entry for the environment variable in the section for the platform configuration service:  
**'PLATFORM\_CONFIGURATION\_Certificate\_RootCertificateCustomText=[desired text for issued by]'**

### Example

```

...
platform-configuration:
...
-
'PLATFORM_CONFIGURATION_Certificate__RootCertificateCustomText=xycvxvc

```

## APPSETTINGS FILE IN WINDOWS

Alternatively, in Windows, the suffix/issued by can also be adjusted with a custom definition in the Appsettings file:

```

{
  ...
  ,
  "CertificateOptions": {
    "RootCertificateCustomText": "user-defined text for Issued by]"
  }
}

```

### 12.2.3 Certificates

The entire communication between the IloT Servicess and clients is encrypted with certificates for security reasons.

#### Examples for clients of IloT Servicess:

- ▶ Internal services of the IloT Servicess
- ▶ zenon applications (e.g. Service Engine)
- ▶ 3rd party applications that are connected via the IloT API
- ▶ Browser access to the web interfaces of the IloT Servicess

Each client connection to the IloT Servicess must be encrypted. It is not possible to establish an unencrypted connection.

The IloT Servicess need the following certificates:

- ▶ For HTTPS connections: a central HTTPS Server Certificate
- ▶ For Certificate Bundles (CB): each CB has an individual Client Certificate

You have the option to integrate your own HTTPS certificates.

### 12.2.3.1 Terminology

The following attributes and names are used for certificates in the IIoT Services:

Term	Definition
(Digital) Certificate	<p>All connections are encrypted with digital certificates in the IIoT Services. Certificates are issued and signed by a Certification Authority (CA).</p> <p>The complete key pair for a certificate consists of a Private Key and a Public Key.</p>
Third-party Certificate	Certificate that has not been created and signed by IIoT Services.
Certificate Expiration	Certificates are issued with a defined period of validity. After the period of validity expires, the certificate can no longer be used to establish an encrypted connection.
Certificate Holder	The holder of a certificate. The holder is the only one who may have access to the Private Key.
Certification Authority (CA)	A certification authority creates and signs certificates. The term is often used synonymously with Trusted Third-party Certification Authority.
CA-signed Certificate	A certificate that has been issued and signed by a Certification Authority (CA). The term is often used synonymously for certificates that have been created by a Trusted Third-party Certification Authority.
HTTPS (Server) Certificate	The HTTPS server uses this central certificate to encrypt connections to HTTPS clients.
Private Key	<p>The private part of the key pair for a digital certificate. The Private Key must provide effective protection against unauthorized access. Only the Certificate Holder may have access to the Private Key.</p> <p>If unauthorized persons gain possession of the Private Key, the certificate is compromised and must be replaced.</p>
Public Key	The public part of the key pair. The Public Key can be published without any restrictions.
Root Certificate	<p>Other certificates are derived from this certificate.</p> <p>A trust relationship to IIoT Services Root Certificate applies for all certificates derived from it.</p>
(IIoT Services) Self-signed	<p>Certificate that has been issued and signed by the IIoT Services.</p> <p>No client has a trust relationship to this certificate by default. The trust</p>

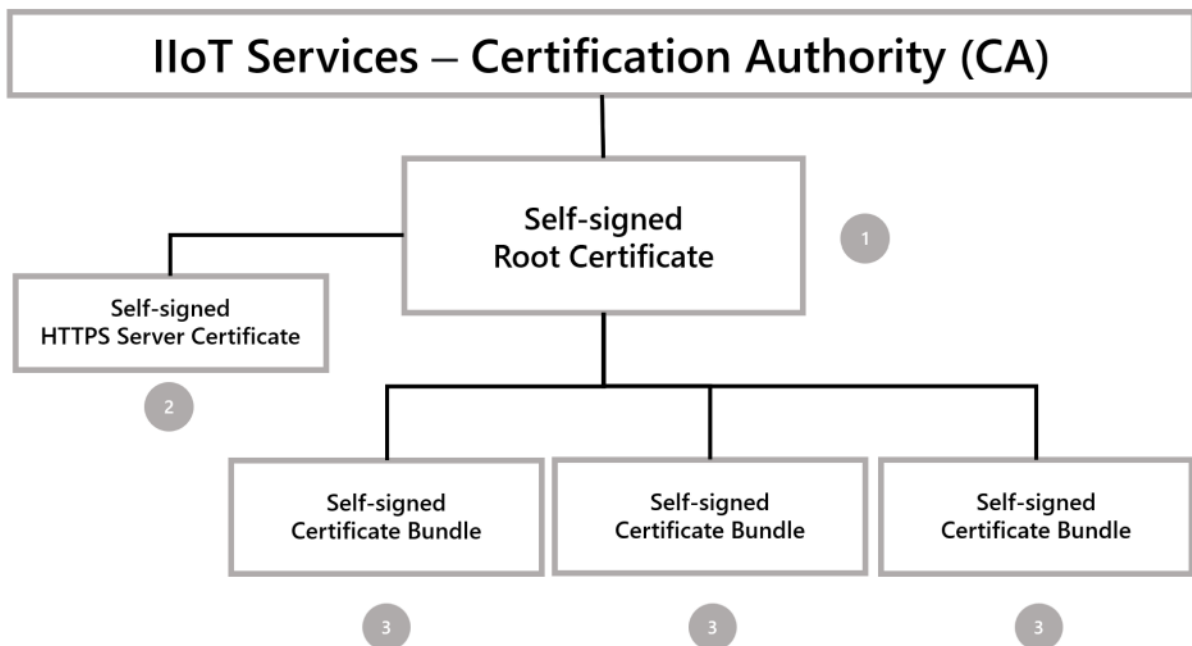


Term	Definition
Certificate	relationships must be configured manually for each client.
Trust	The basis of an encrypted connection is a trust relationship between the client and the certificate of the server. The client must be able to verify the issuer of the certificate and trust the issuer.
Trusted Third-party Certificate	Certificate that has been issued and signed by a Trusted Third-party Certification Authority.  All clients with common operating systems have a trust relationship to this certificate by default.
Trusted Third-party Certification Authority	A Certification Authority (CA) whose Root Certificate is already preinstalled in common operating systems.

### 12.2.3.2 Certificate hierarchy

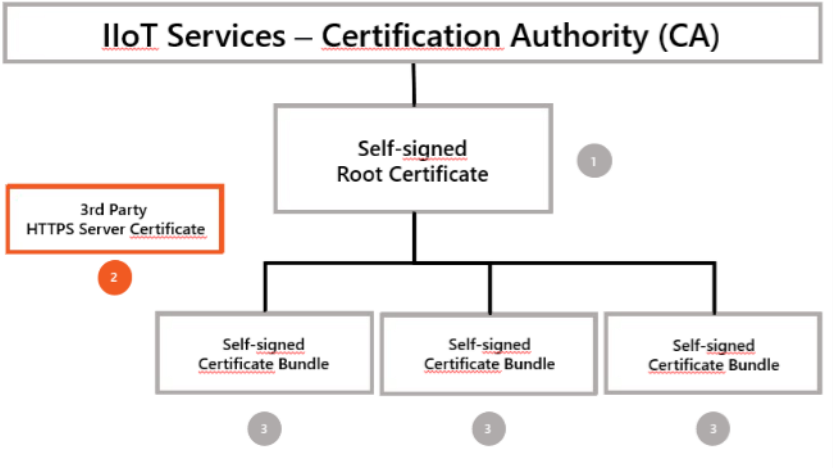
The IIoT Services have their own Certification Authority (CA) integrated. It is independent of third parties to secure the communication. The certificate hierarchy depends on the configuration selected.

#### DEFAULT: SELF-SIGNED CERTIFICATES FOR HTTPS AND CB



IIoT Services create all required certificates themselves by default. Both the "HTTPS Server Certificate" (2) and the "Certificate Bundles" (3) are derived from the same Root Certificate (1).

### OPTIONAL: THIRD-PARTY CERTIFICATE FOR HTTPS AND SELF-SIGNED CERTIFICATES FOR CB



You replace the preconfigured "Self-signed HTTPS Server Certificate" with an imported "Third-party HTTPS Server Certificate" (2). The other certificates (1 and 3) remain unchanged.

### 12.2.3.3 Certificate files

The IIoT Services use the following certificate files:

	IIoTServices.pfx	Imported certificate file (* .pfx or *.p12)	ca.crt	IIoTServices.crt
<b>Label</b>	IIoT Services Self-signed HTTPS Server Certificate	3rd party HTTPS Server Certificate	IIoT Services Self-signed Root Certificate	Option A) IIoT Services Self-signed HTTPS Server Certificate (by default) Option B) 3rd party HTTPS Server Certificate (optional)
<b>Content</b>	Public Key Private Key	Public Key Private Key	Public Key	Public Key
<b>Certification Authority (CA)</b>	IIoT Services Root CA - [FQDN]	3rd party CA	IIoT Services Root CA - [FQDN]	Option A) IIoT Services Root CA - [FQDN] Option B) 3rd party CA
<b>Period of validity</b>	<i>5 years</i> Renewal via <b>Platform Configuration.</b>	Period of validity as defined by 3rd party Certification Authority.  Renewal via 3rd party Certification Authority.	<i>30 years</i> No renewal possible.	Option A) <i>5 years.</i> Renewal via <b>Platform Configuration.</b>  Option B) Period of validity as defined by 3rd party Certification Authority.



	IloTServices.pfx	Imported certificate file (*.pfx or *.p12)	ca.crt	IloTServices.crt
				Renewal via 3rd party Certification Authority.
<b>GUI</b>	<p>Download in Service Configuration Studio:  <b>Service Configuration Studio\Platform Configuration\Certificates</b></p> <p><b><u>Important:</u></b></p> <p>This certificate file can only be downloaded directly after the certificate has been created. It cannot be downloaded at a later point in time.</p>	<p>Import in Service Configuration Studio:  <b>Service Configuration Studio\Platform Configuration\Certificates</b></p>	<p>Download in Service Configuration Studio:  <b>Service Configuration Studio\Certificate Management\Certificates</b></p>	<p>Download in Service Configuration Studio:  <b>Service Configuration Studio\Platform Configuration\Certificates</b></p>
<b>Example</b>	<p>You are analyzing data from the IloT Services in a test environment using a web-based 3rd party application. The web interface of the</p>	<p>You replace the preconfigured IloT Services Self-signed HTTPS Certificate with the 3rd party HTTPS Certificate in a productive environment.</p> <p>This ensures that IloT Services</p>	<p>Configuration of a trust relationship between client computers and the IloT Services Self-signed HTTPS</p>	<p>Reading out the entire specification of the HTTPS Server Certificate used by the IloT Services.</p>



	IloTServices.pfx	Imported certificate file (*.pfx or *.p12)	ca.crt	IloTServices.crt
	3rd party application is to be secured using the same "IloT Services Self-signed HTTPS Certificate".	HTTPS communication is encrypted with the 3rd party HTTPS Certificate.	Certificate in a test environment.	
<b>Example:Configuration</b>	In the 3rd party application, configure the <i>IloTServices.pfx</i> file as the certificate to be used.	Import the certificate file into the IloT Services.	Import ca.crt onto the client computer in the certificate manager of the operating system.	Open the properties of the certificate. Just double-click on <i>IloTServices.crt</i> under Windows.

### 12.2.3.4 HTTPS certificate options

In the IIoT Services, you can choose between the following certificates for the HTTPS certificate:

- ▶ IIoT Services Self-signed HTTPS Certificate (by default)
- ▶ Third-party HTTPS Certificate (optional)

There are different options for third-party certificates:

- ▶ Trusted Third-party HTTPS Certificates: These certificates are created by a recognized external certification authority. These are certification authorities such as Let's Encrypt, GoDaddy or VeriSign.
- ▶ Third-party Certificates: These certificates are created by an unspecified Certification Authority outside of the IIoT Services. This is typically the case if you are operating your own certificate infrastructure in your company.

It is possible to operate your own certificate infrastructure in many different forms and requires that the administrator possess the appropriate knowledge. The IIoT Services Help therefore only documents the use of Trusted Third-party HTTPS Certificates.

#### **There are basic differences between the certificates:**

	IIoT Services Self-signed HTTPS certificate	Trusted third-party HTTPS certificate
Certification Authority (CA)	IIoT Services Root CA - [FQDN]	Trusted Third-party Certification Authority
Configuration of the certificate	This certificate is created automatically during the installation of IIoT Services.  No manual configurations are required for the IIoT Services.	This certificate is created by an external Certification Authority – i.e. outside of IIoT Services.  These are typically well-known certification authorities such as Let's Encrypt, GoDaddy or VeriSign.  The administrator manually imports the certificate file into the IIoT Services.
Client's trust relationship	Must be configured by the administrator manually or with group policies for each client.  Reason: The IIoT Services Root Certificate is not preinstalled in the operating system.	Is provided automatically.  Reason: The Root Certificates of these certificate authorities are preinstalled in common operating systems.

	IloT Services Self-signed HTTPS certificate	Trusted third-party HTTPS certificate
Certificate renewal	The administrator can create a new HTTPS Certificate in Service Configuration Studio.	Same as the initial configuration.
Recommendation	This certificate is only recommended for small-scale test environments.  Reason: The trust relationship to the certificate must be set up separately for each client. This requires a lot of time and effort in environments with many clients and/or a heterogeneous system landscape.	This certificate is recommended for test environments and productive environments of all sizes.  This includes heterogeneous system landscapes with different client operating systems.

### 12.2.3.5 Trust relationships

All clients require trust relationships for connections to the IloT Services.

IloT Services support two connection types:

- ▶ Connections with Certificate Bundle (CB)
- ▶ Connections with HTTPS

The trust relationship must be configured separately for each connection type.

The following applies for connections with Certificate Bundle:

- ▶ Only certain zenon applications and services require a CB.
- ▶ Each client requires its own Certificate Bundle with an individual Certificate.
- ▶ Each Certificate is based on the IloT Services Self-signed Root Certificate.

Certificate Bundles are configured using the **IloT Services Connection Wizard**.

The following applies for connections with HTTPS:

- ▶ All IloT Services clients can establish a HTTPS connection  
**Important:** This also applies to zenon applications and services that connect with CB.
- ▶ Each HTTPS client requires a trust relationship for the HTTPS Certificate used.
- ▶ IloT Services use a central HTTPS Server Certificate.
- ▶ A IloT Services Self-signed HTTPS Certificate is preinstalled by default.
- ▶ The preinstalled certificate can be replaced optionally by a Third-party HTTPS Certificate.

How you must configure the trust relationship depends on the HTTPS Certificate used.

### 12.2.3.5.1 IIoT Services Connection Wizard

From version 12, the **Service Node Configuration Tool** is no longer supported and is also not included in the setup:

- ▶ The connections of zenon components are configured with the **IIoT Services Connection Wizard**.
- ▶ From version 14, certificates are transferred from the connected IIoT Services on execution of the wizard and can be installed on the Engineering Studio computer during the course of the wizard.



#### Information

The **Service Node Configuration Tool (SNCT)** was used in previous versions of zenon up to and including 11.2 for the generation of Certificate Bundles (CB) for clients.

### 12.2.3.5.2 HTTPS trust relationship

It is only possible to establish an HTTPS connection if there is a trust relationship between the client and the HTTPS Certificate of the IIoT Services.

#### HTTPS CLIENTS

Each client connected to the IIoT Services requires a trust relationship with the HTTPS Certificate.

#### **You must set up trust relationships, for example, for the following client computers:**

- ▶ Clients that access Service Configuration Studio with a browser
- ▶ Clients that access the IIoT API with a Third-party Application
- ▶ zenon components and applications that connect with the IIoT Services
- ▶ The host computer on which the IIoT Services are installed.

#### **IIoT Services HTTPS certificates frequently used are:**

- ▶ IIoT Services Self-signed HTTPS Server Certificate
- ▶ Trusted Third-party HTTPS Server Certificate

The configuration of the trust relationship depends on the certificate selected.



### 12.2.3.5.3 Configure trust relationship

The configuration of a trust relationship depends on the certificate selected.

#### SELF-SIGNED HTTPS SERVER CERTIFICATE

You must configure trust relationships for all client computers.

To configure a client:

1. Load the ca.crt certificate file for the IIoT Services Self-signed Root Certificate from this web interface:  
Service Configuration Studio\Certificate Management\Certificates
2. Import the certificate file manually into the certificate store of the respective operating system. For example: In the Windows operating system, you must import the certificate file into the *Trusted root Certification Authorities* folder via the certificate store of the local computer.

**Note:** You can automate this procedure by using group policies.

You have thus configured the trust relationship.

#### TRUSTED THIRD-PARTY HTTPS SERVER CERTIFICATE

In general, you do not have to manually configure any trust relationship for this certificate.

Reason: Root Certificates for Trusted Third-party Certification Authorities are already preinstalled in common operating systems. Thus a trust relationship exists by default.

### 12.2.3.5.4 Trust relationship with multiple certificates (Docker only)

It is possible to install additional trustworthy certificates for the IIoT Services. This is necessary, for example, if the services have to communicate with third-party systems that use self-signed certificates. An example of this is communication between the **Identity Service** and **Identity Provider** (e.g. OpenLDAP or Keycloak).

#### INSTALLATION

In Windows, the IIoT Services automatically use the certificates of the certificate store to verify certificates. In a Docker environment, these additional certificates that have to be trusted must be stored manually in the services.

Carry out the following steps in order to add additional certificates to the trusted certificates of the container:

1. Create a folder and place the certificates there (with the folder name "certs" for example).
2. Include the certificates in each Docker service that is to trust the certificate. Carry out this inclusion for each service.

Add a row in the **volumes** section of the respective service in the *docker-compose.yml* file.

- a) Configure the path and the folder in which your certificates are located. This can be an absolute or relative path entered.  
For example: - *./certs:/certs/*

1. Restart the container.

```
Example

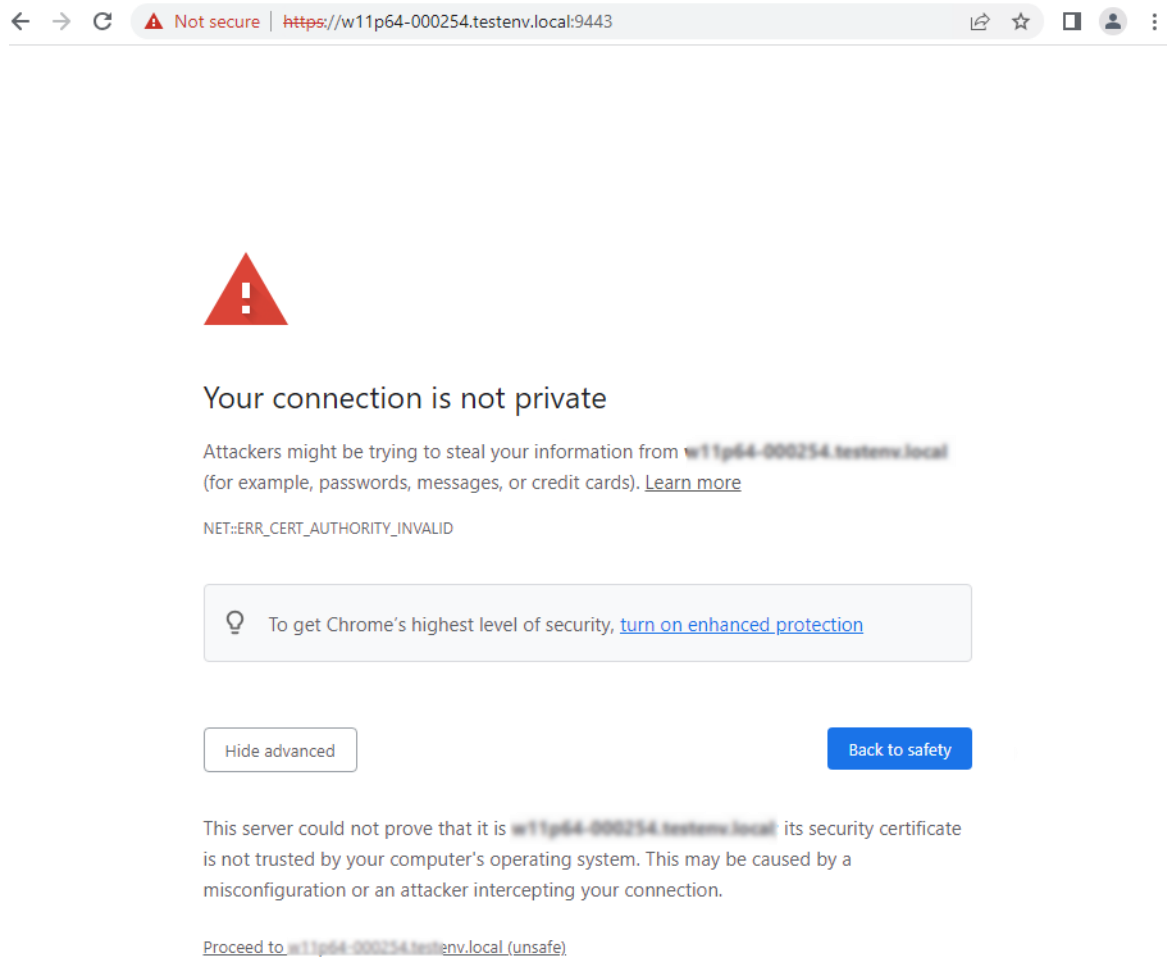
identity-service:
  ...
  networks:
    - iiot-services-network
  volumes:
    - iiot-services-data:/var/iiot-services-data/
    - ./certs:/certs/ <-- add this line
```

The following is applicable here:


- ▶ The certificates are loaded each time the container is started.
- ▶ The newly-added certificates are loaded each time the container is started.
- ▶ Certificates that are removed from the folder are not uninstalled during operation.
- ▶ Deletion and recreation of the respective container resets all previously-installed certificates and only then installs the certificates currently present in the folder.

### 12.2.3.5.5 HTTPS certificate warnings

You may receive an HTTPS certificate warning when establishing an HTTPS connection between a client and IIoT Services.




← → ↻ ⚠ Not secure | https://w11p64-000254.testenv.local:9443



### Your connection is not private

Attackers might be trying to steal your information from [w11p64-000254.testenv.local](https://w11p64-000254.testenv.local) (for example, passwords, messages, or credit cards). [Learn more](#)

NET:ERR\_CERT\_AUTHORITY\_INVALID

 To get Chrome's highest level of security, [turn on enhanced protection](#)

[Hide advanced](#) [Back to safety](#)

This server could not prove that it is [w11p64-000254.testenv.local](https://w11p64-000254.testenv.local) its security certificate is not trusted by your computer's operating system. This may be caused by a misconfiguration or an attacker intercepting your connection.

[Proceed to w11p64-000254.testenv.local \(unsafe\)](#)

The following applies for certificate warnings:

- ▶ They make the user aware that there is no trust relationship between the client and the HTTPS Certificate of the HTTPS connection.
- ▶ You must then check the certificate used by this HTTPS connection.

The certificate and thus the identity of the HTTPS server must be clearly verified. This prevents attacks over the HTTPS connection like Man-in-the-middle attacks.

#### **The following applications issue certificate warnings:**

- ▶ Browser: When you attempt to open a IIoT Services web interface.
- ▶ Engineering Studio during configuration with the **IIoT Services Connection Wizard**.

The user can manually establish the HTTPS connection after a positive check of the certificate warning.

**The following applications do not issue certificate warnings:**

- ▶ Service Engine: When you attempt to connect to IloT Services via HTTPS.
- ▶ Report Engine: When you attempt to connect to IloT Services via HTTPS.

The user cannot establish these HTTPS connections manually. In these cases, the trust relationship must be configured before establishing the connection.

**Note:** In the **Diagnosis Viewer**, you can find logs of failed connection attempts of zenon applications.

The following applies for certificate warnings when accessing via the IloT API:

- ▶ User access via Service Configuration Studio: The browser issues a certificate warning.
- ▶ Client access to the IloT API for a third-party application: The third-party application decides here how it handles HTTPS connections. The third-party application can also issue certificate warnings if configured accordingly.

Third-party applications are generally to be configured in such a way that there is a trust relationship to the HTTPS Certificate.

**To avoid certificate warnings:**

- ▶ Make sure that a trust relationship has been established with the HTTPS Certificate of the IloT Services for all clients before establishing the connection.

You should not receive any more certificate warnings after successful initialization of IloT Services and the correct configuration of all clients.

### 12.2.3.5.6 HTTPS certificate check

The basic principle is: After a HTTPS certificate warning, the HTTPS Certificate must be checked by the user. How the certificate check is actually done depends on the context of the certificate check.

## CERTIFICATE WARNINGS DURING INSTALLATION

Certificate warnings are unavoidable during initialization of the IloT Services. At this stage, you need not and cannot verify the certificate.

## CERTIFICATE WARNINGS DURING OPERATION

In a fully configured IloT Services environment, all required HTTPS trust relationships should be established. Therefore there should not be any HTTPS certificate warnings during operation. Certificate warnings in this context are thus unavoidable and must be checked very carefully.

To check the certificate:

- ▶ Preparation: Save the *IloTServices.crt* certificate file during the installation of IloT Services. You have thus made sure that you always have access to the HTTPS Server Certificate configured for IloT Services even in the case of a compromised HTTPS connection. This certificate should be used for the HTTPS connection.
- ▶ When the certificate warning is displayed: extract the certificate shown. This certificate is actually used for the HTTPS connection.
- ▶ Compare the two certificates with each other.

Both certificates must match. If this is not the case, the HTTPS connection has been compromised.

### 12.2.3.6 Period of validity

The validity of certificates is checked before the connection is established. A connection is then only established if the certificate is valid at the time of connection.

**The period of validity of IloT Services self-signed certificates is:**

- ▶ Root Certificate (CA): *30 years*
- ▶ HTTPS Server Certificate: *5 years*
- ▶ Client Certificates for Certificate Bundles (CB): *5 years*

**The period of validity of third-party certificates is:**

- ▶ Freely definable by the respective Certification Authority.

The administrator must continuously monitor the terms of all certificates. Certificates must be replaced in time before the end of the period of validity.

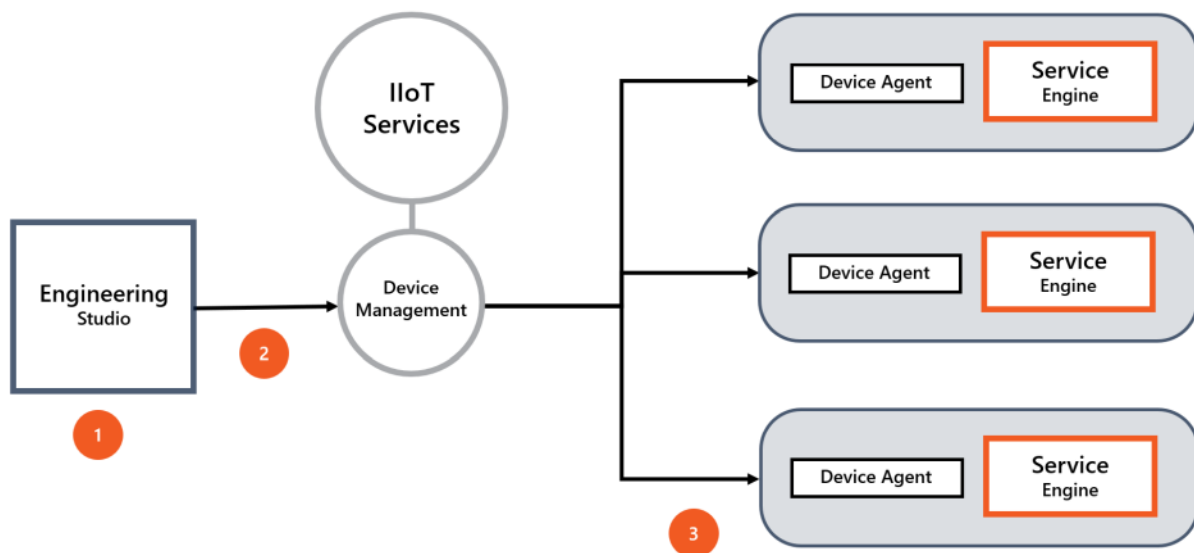
## MONITOR THE PERIOD OF VALIDITY

**To monitor the periods of validity of certificates:**

Certificate	Where the period of validity is displayed
IloT Services Root Certificate	In the properties of the <i>ca.crt</i> certificate file.
HTTPS Server Certificate	In the properties of the <i>IloTServices.crt</i> certificate file.
Client Certificates for Certificate Bundles (CB)	<p><b><u>Service Configuration Studio web interface:</u></b></p> <ul style="list-style-type: none"> <li>▶ Service Configuration Studio\Certificate Management\Certificates</li> </ul> <p>Each CB contains an individual Client Certificate</p>

Certificate	Where the period of validity is displayed
	and must therefore be monitored separately.  Hint: You can sort the column view by the period of validity of the certificates.

## 13 Device Management



You can use Device Management to centrally manage connected client computers.

**Device Management** is a service for monitoring and software deployment in the zenon Software Platform.

**The following applies for Device Management:**

- ▶ Each device requires an installed **Device Agent**.
- ▶ When executing a deployment task, a check is carried out to ensure that an appropriate Certificate Bundle has been configured on the device if the project has been configured for IIoT Services.
- ▶ The software deployment supports updates and configurations for Service Engine.
- ▶ The software deployment can be done manually or scheduled.

**To deploy software using Device Management:**

1. Create and configure a zenon project in Engineering Studio.

2. Upload the project from Engineering Studio to **Device Management**. This creates a deployable software package.
3. The software package can be deployed on any number of Service Engine instances.

**Device Management** also allows you to efficiently manage large environments.

## 13.1 General

**Device Management** is used to supply Service Engine files for Service Engine on devices.

1. Create and configure a zenon project in Engineering Studio. These projects are prepared as software packages using a wizard and are transferred to **Device Management** of the IIoT Services for distribution.
2. The software package can be deployed on any number of Service Engine instances. You use the **Device Management** service in Service Configuration Studio to configure the deployment to the devices.  
This deployment can also be done scheduled.  
Device Management offers a user interface and an overview of the available devices and software packages as well as a configuration interface for the listing and planning of the deployment.
3. An appropriate service is registered on the devices to make the devices accessible to **Device Management**. Both Windows operating systems as well as Linux and Raspberry are supported as devices.  
**Note:** You can find a list of supported operating systems in the **Installation and updates** node in the **Linux** node.

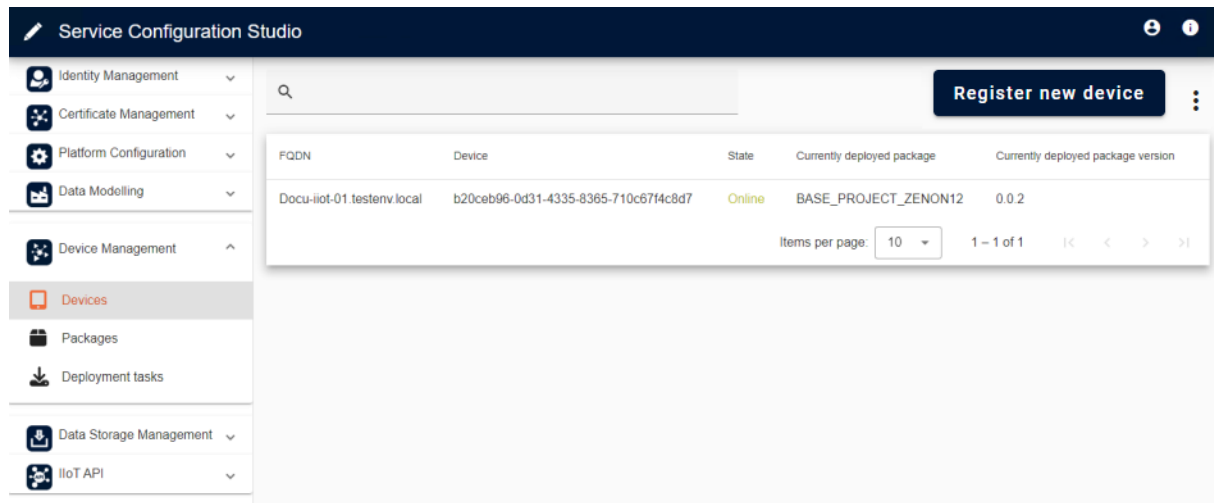
### PROCEDURE

The following steps are carried out on the device when executing a **Deployment task**:

1. Software packages are transferred to a device with a **Deployment Task**. The project packages are saved on the device in the Default folder for zenon projects.
  - ▶ Windows default folder: *C:\Users\Public\Documents\zenon\_Projects*.
  - ▶ Linux default folder: */etc/copa-data*
2. Any Service Engine running on the device is stopped.
3. The current deployment task project is installed on the device and set as a start project.
4. Service Engine is started again.  
**Note:** If Service Engine had not yet been started before execution of the deployment task, Service Engine is started after successful transfer.

## 13.2 Devices

List of all registered devices for **Device Management** on the IIoT Services.



Option	Description
<b>Search list</b>	Filtering of the list. Entry of the filter criteria for the display of the list as a text.
<b>Register new device</b>	Opens a dialog with a property help to show how you set up a device for Device Management. In doing so, it is possible to switch between instructions for Windows or Linux operating systems. The notes contain context-dependent information that can be used for installation on the device by copying to the clipboard.
...	Additional actions for Device Management: <ul style="list-style-type: none"> <li>► <i>Show removed devices</i> The list display also contains devices that have been removed from Device Management.</li> </ul>

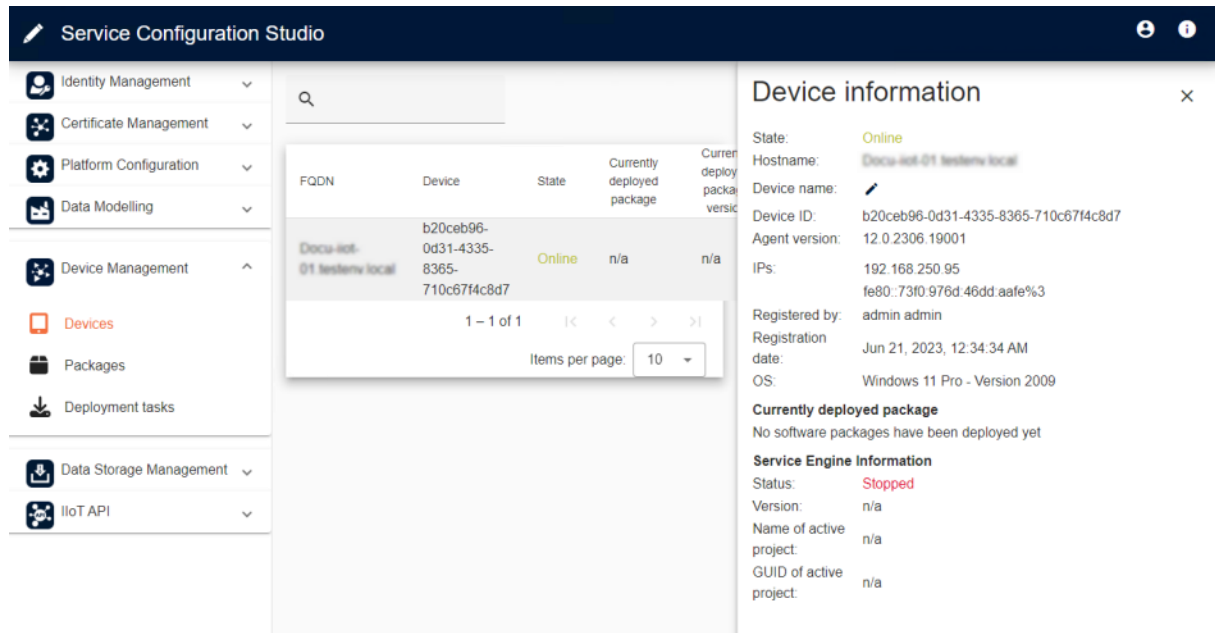
The items of this list can be sorted by clicking on the column heading.

Option	Description
<b>FQDN</b>	FQDN of the device. Is applied by the device when registering the <b>Device Agent</b> .
<b>Device</b>	Unique ID of the client on IIoT Services. Is created automatically on the device when registering the <b>Device Agent</b> .  The display depends on the configuration of the device (on page 271):

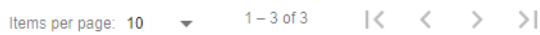


Option	Description
	<ul style="list-style-type: none"> <li>▶ Device Name: If a corresponding device name has been configured, this is displayed in the list.</li> <li>▶ Device ID: If no corresponding device name has been configured, the automatically generated device ID is displayed in the list.</li> </ul>
<b>State</b>	<p>State of the device. The state is visualized as text and with colors.</p> <ul style="list-style-type: none"> <li>▶ <i>InRegistration</i> (black) Device has just been configured for <b>Device Management</b> and is in initial establishment of a connection. It cannot currently receive any deployment tasks.</li> <li>▶ <i>Offline</i> (red) Device cannot be reached.</li> <li>▶ <i>Online</i> (green) Device can be reached; Service Engine service for <b>Device Management</b> is running.</li> <li>▶ <i>Online (Marked for removal)</i> (green) Device is contactable; it has however been marked for removal; Service Engine service for <b>Device Management</b> is running.</li> <li>▶ <i>Removed</i> (black) Device has been removed from Device Management.</li> </ul>
<b>Currently deployed package</b>	<p>Name of the package that is currently installed on the device.</p> <p><b>Note:</b> If no deployment task has been executed on the device yet, the entry <i>n/a</i> is shown.</p>
<b>Currently deployed package Version</b>	<p>Version of the package that is currently installed on the device.</p> <p><b>Note:</b> If no deployment task has been executed on the device yet, the entry <i>n/a</i> is shown.</p>

Clicking on the item opens a tab with detailed information.



### NAVIGATION AND STATUS BAR



The status bar allows you to customize the view of the respective page and to navigate in the list view.

Option/symbol	Description
Items per page	Number of items shown per page. Selection from a drop-down list.
[a] - [b] of [c]	Sum of all available items and information on the items shown: <ul style="list-style-type: none"> <li>▶ [a]: Number of the first item shown</li> <li>▶ [b]: Number of the last item shown</li> <li>▶ [c]: Sum of all items</li> </ul>
Zur ersten Seite (  < )	Jumps to first page of the list view.
Vorherige Seite (<)	Jumps to previous page of the list view. <b>Note:</b> Not available on the first page.
Nächste Seite (>)	Jumps to the next page of the list view.

Option/symbol	Description
	<b>Note:</b> Not available on the last page.
Zur letzten Seite (> )	Jumps to the last page of the list view.


### 13.2.1 Detail view - Devices

The detail view provides you with additional information about the device.

#### Device information ×

State: Online

Hostname: TS-WI1x04\_L1.testenv.local

Device name: 

Device ID: e50741f0-f55a-4631-8a28-7a2809730ae6

Agent version: 14.0.2401.31003

IPs: 10.43.192.147  
fe80::7298:defb:41fa:4ec4%4

Registered by: admin admin

Registration date: Feb 7, 2024, 1:28:09 PM

OS: Windows 11 Pro - Version 2009

**Currently deployed package**

No software packages have been deployed yet

**Service Engine Information**

Status: Stopped

Version: 14.0.0.199903 BETA

Name of active project: BASE\_PROJECT\_ZENON12

GUID of active project: 6f525322-603d-4b6d-90fa-4dc7b6d10943

[Remove device](#)

Option	Description
State	<p>State of the device. The state is visualized as text and with colors.</p> <ul style="list-style-type: none"> <li>▶ <i>InRegistration</i> (black) Device has just been configured for <b>Device Management</b> and is in initial establishment of a connection. It cannot currently receive any deployment tasks.</li> <li>▶ <i>Offline</i> (red) Device cannot be reached.</li> <li>▶ <i>Online</i> (green)</li> </ul>

Option	Description
	<p>Device can be reached; Service Engine service for <b>Device Management</b> is running.</p> <ul style="list-style-type: none"> <li>▶ <i>Online (Marked for removal)</i> (green) Device is contactable; it has however been marked for removal; Service Engine service for <b>Device Management</b> is running.</li> <li>▶ <i>Removed</i> (black) Device has been removed from Device Management.</li> </ul>
<b>Hostname</b>	FQDN of the device. Is applied by the device when registering the <b>Device Agent</b> .
<b>Device Name</b>	<p>Optional entry of a custom device name. Click on the pen symbol to open the dialog for entering a name.</p> <p>Default: <i>empty</i></p>
<b>Device ID</b>	Unique ID of the client on IIoT Services. Is created automatically on the device when registering the <b>Device Agent</b> .
<b>Agent version</b>	Version of the <b>Device Agent</b> service that is installed on the device.
<b>Upgrade</b>	<p>This button is displayed if an older version of the <b>Device Agent</b> is installed on the device.</p> <p>Clicking on the button automatically creates a deployment task that updates the <b>Device Agent</b>.</p> <p>This task is then listed in the list with the detail view of the deployment task (on page 292). This task is named by default with the <i>Upgrade_Device_Agent</i> package name.</p> <p><b>Note:</b> If the current version is installed on the device, this button is hidden.</p>
<b>IPs</b>	IP address of the client. Is applied by the device when registering the <b>Device Agent</b> .
<b>Registered by</b>	User name of the user who has registered the service on Device Management.
<b>Registration date</b>	Date of registration on Device Management with the current Device Management service.
<b>OS</b>	Operating system of the client. Is applied by the device when

Option	Description
	registering the <b>Device Agent</b> .

**CURRENTLY-DEPLOYED PACKAGE**

Option	Description
<b>Currently deployed package</b>	<p>Information on the current software package provided:</p> <ul style="list-style-type: none"> <li>▶ Name of the software package which has been delivered most recently to the client.</li> <li>▶ If no software package has been transferred to the client yet, a corresponding message is displayed: <i>No software packages have been deployed yet</i></li> </ul>

**SERVICE ENGINE INFORMATION**

Option	Description
<b>Status</b>	<p>State of the Service Engine on the device. The state is visualized as text and with colors.</p> <ul style="list-style-type: none"> <li>▶ <i>running</i> (green) Service Engine is installed and running on the device.</li> <li>▶ <i>stopped</i> (red) Service Engine is installed on the device but has not been started.</li> <li>▶ <i>No Service Engine installed</i> (red) No valid installation of Service Engine has been found on the device.</li> </ul>
<b>Version</b>	Version of Service Engine on the device.
<b>Name of active project</b>	Name of the active project that is running in Service Engine on the device.
<b>GUID of active project.</b>	GUID of the project that is running in Service Engine on the device.
<b>Remove Device</b>	<p>Removes the device from Device Management. Removal must be confirmed by means of a dialog.</p> <p>Procedure:</p>

Option	Description
	<ul style="list-style-type: none"> <li>▶ The confirmation dialog is opened and must be confirmed.</li> <li>▶ The device gets the status "<i>Marked for removal</i>".</li> <li>▶ A <b>Deployment task</b> is created for the device for the removal of the device.</li> <li>▶ The installed software packages and the <b>Device Agent</b> are deleted on the device as soon as the deployment task has been supplied to the device and executed.</li> <li>▶ The device then has the status "<i>Removed</i>" and is hidden in the list of devices.</li> </ul>
<b>Force remove</b>	<p>Button for the forced removal of a device. <b>Note:</b> This button is only visible if a device has already been pre-marked for removal with <b>Marked for removal</b>.</p> <p>Forced removal can be applied for example if a device is offline but is to be removed from <b>Device Management</b> immediately. In addition, it can be used to remove devices with which communication is no longer possible.</p> <p>Additional process:</p> <ul style="list-style-type: none"> <li>▶ The device is removed from <b>Device Management</b> immediately.</li> <li>▶ All open <b>Deployment tasks</b> for the device are ended immediately.</li> <li>▶ The device and its access data are immediately blocked for any future access. The device is immediately changed to the state of <i>Removed</i>.</li> </ul>

**NAVIGATION - CLOSE DIALOG**

Button	Description
X	Closes the detail view.

### 13.2.1.1 Device name configuration dialog

In this dialog, you configure the custom name of the device for the view in **Device Management**.

#### Device name

Device name

HelloWorld

The entered device name is already used by another device.

The entry is validated to ensure that the name is unique. In the event of an error, a corresponding warning message is displayed.

Navigation

Button	Description
Cancel	Discards all changes and closes the dialog.
Submit	Applies settings and closes the dialog.

### 13.2.1.2 "Remove Device" confirmation dialog

With this dialog, you confirm the removal of a device from Device Management.

Do you want to remove this device?

The device will be marked for removal and will be permanently removed.

Device  
|

Enter the device name: 'TS-W11x64\_1.testenv.local'

Option	Description
Device	Input field for the device to be removed. The configured device name is to be entered, or the FQDN of the device if no device name has been configured.  <b>Note:</b> An input proposal, depending on configuration, is shown as text under the input field.
Cancel	Cancels the removal and closes the dialog.

Option	Description
Delete	Confirms the removal, carries out the next steps and closes the dialog

### 13.2.2 Configure device for Device Management

In order for software packages to be deployed for a device, an appropriate IIoT Services service must be registered and running on the device. Name of the service:

#### **CopaData.ServiceGrid.DeviceManagement.Agent.**

- ▶ The service must be registered on the device.  
The destination address of the Device Agent service must be configured during registration. After correct registration, the device is visible in **Device Management** on the **Devices** page.  
**Note:** Note that it may take some time until the newly-registered device is displayed in the device overview (on page 271).
- ▶ The service must run on the device.  
The service must be running on the device to deploy or deliver a software package.



#### **Information**

**Device Management** contains contextual installation instructions. Clicking on the **Register new device** button in the **Devices** node brings up a dialog with brief installation instructions Service Configuration Studio. The commands to be executed on the target client can be copied from the instructions directly.

#### 13.2.2.1 Install device agent for Windows (Windows)

Carry out the following steps in order to install and register the service:

1. Ensure that there is appropriate trust between the device and IIoT Services.
2. Register the required service.
  - ▶ Go to `C:\Programs\Common Files\COPA-DATA\ServiceGridCli\14_0>`.
  - ▶ Start the Windows **PowerShell** application as administrator.
  - ▶ Enter the following command. If you also want to register the name of the device, supplement the command with the the option `-n`.  
`.\CopaData.ServiceGrid.DeviceManagement.Agent.exe -u [URL to the IIoT Services]:Port -n [Name of the device]`  
The name of the device is optional. If the command is entered without a device name,



the pre-configured CLI client is used for the connection (= *DeviceManagementAgentCliClientId*).

**Example:** `.\CopaData.ServiceGrid.DeviceManagement.CLI.exe setup-agent -u https://iiot-docu-v8.testenv.local:9443 -n LinuxDevice`

### 3. Authenticate yourself with the **Identity Service**.

#### a) When authenticating via web browser:

Enter user name and password if the web browser opens with the login page.

**Note:** This step does not take place if you are already logged in to **Identity Service**.

#### b) When authenticating on another client:

Enter the following command during installation, if web access is not possible on the device on which you want to install the device agent:

```
C:\Program Files\Common Files\COPA-DATA\ServiceGridCli\12_0>
.\CopaData.ServiceGrid.DeviceManagement.CLI.exe setup-agent -u
https://iiot-docu-v8.testenv.local:9443 -n LinuxDevice --use-device-code
```

Authorization is carried out by means of Identity Service in Service Configuration Studio (on page 279). The installation on the client will be completed after successful authorization.

After successful registration, the device is listed in the overview of devices.

**Note:** When updating the state in Device Management, there can be delays of several minutes.

#### **Hint**

If the *CopaData.ServiceGrid.DeviceManagement.CLI.exe* is started in the command line without parameters, an appropriate help text is displayed in the **Command Line Interface**.

## 13.2.2.2 Install Device Agent for Linux

The **Device Agent** is installed together with the IIoT command line interface.

#### **Attention**

**Device Management** is not available for Service Engine in Docker environments.

You can find detailed instructions for installation on Linux systems in the **Service Engine on Linux** section.

Carry out the following steps to install the service for **Device Management** (= **Device Agent**) on a Linux device:

1. Update the list of the zenon software packages available. Execute the following command:  
`sudo apt update`
2. Install the command line interface on the Linux device. Execute the following command:  
`sudo apt install iiot-cli-14-0`
3. Carry out the installation of the Device Agent service. To do this, enter the following command:
  - a) If you have web access for authentication on the Linux device:  
`iiot-cli setup-agent -u [URL to the IIoT Services]:Port -n [Name of the device]`  
The name of the device is optional. If the command is entered without a device name, the pre-configured CLI client is used for the connection (= `DeviceManagementAgentCliClientId`).  
**Example:** `iiot-cli setup-agent -u https://iiot-docu-v8.testenv.local:9443 -n LinuxDevice`
  - b) If you do not have web access for authentication on the Linux device:  
`iiot-cli setup-agentsetup-agent -u https://iiot-docu-v8.testenv.local:9443 -n LinuxDevice --use-device-code`  
  
The **--use-device-code** command tag is used for authorization via the Identity Service in Service Configuration Studio (on page 279).  
The URL and code for this authorization is visualized in the command line.  
After successful authorization, installation on the Linux device will be complete.
4. If you have installed more than one version of IIoT-CLI , you can switch between the versions. To do this, execute the following command:  
`sudo update-alternatives --config iiot-cli`  
Then follow the instructions of CLI.
5. Check the status of the device agent:
  - ▶ Check the connection status of the device in the user interface of **Device Management** (on page 271) device administration in Service Configuration Studio. The Linux device must display the status Online.
  - ▶ On the Linux computer, the status of the device agent is checked with the following command:  
`sudo systemctl status device-agent.service`

 **Information**

Ensure that the following language settings (**Locales**) are installed on your system:

- `en_US.UTF-8`

- `UTF-8/en_US.UTF-8`

- `UTF-8`

If these **Locales** are missing, it can happen that the Device Agent is closed with the following error message:

*terminate called without an active exception Aborted*

### 13.2.2.3 Authorization via Identity Service

When installing services on devices without web access, authentication can be carried out on another computer or device (a smartphone for example).

Carry out the following steps to authorize devices:

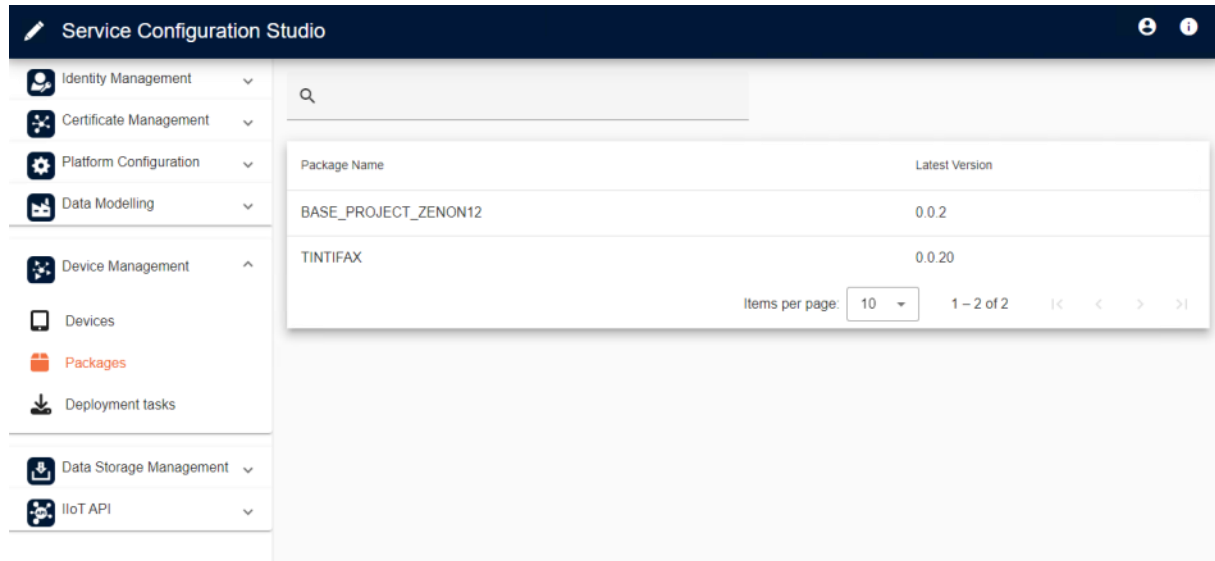
- a) Open the URL as stated in the command line of the CLI.

**Example:** "To login please go to  
'<https://iiot-docu-v8.testenv.local:9443/identity-service/device>' and enter the code:  
'539083363' to login."

- b) Log in to the Identity Service in Service Configuration Studio.
- c) Enter the code, as stated in the command line interface, into the authorization dialog.
- d) Confirm your input by clicking on the Send button.
- e) After confirmation, the installation of the device agent on the device will be continued automatically.

### 13.3 Packages

List of all available software packages for **Device Management** on the IIoT Services.

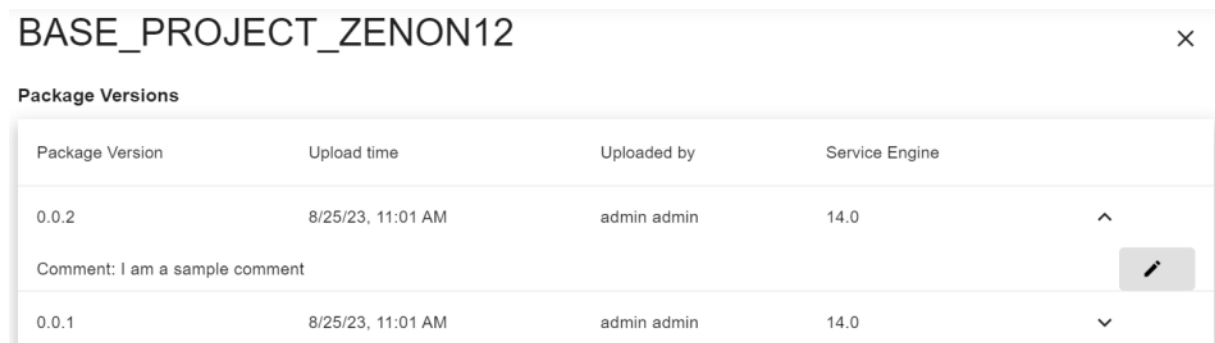


The items of this list can be sorted by clicking on the column heading.

Option	Description
<b>Package Name</b>	Name of the software package.
<b>Latest Version</b>	Number of the latest version of the software package.

#### PROJECT - DETAILED INFORMATION

Clicking on the item opens a tab with detailed information.



Option	Description
<b>Package name</b>	Name of the software package.
<b>Package Version</b>	Version of the zenon project. The version number is based on the <b>Versioning active</b> project property in Engineering Studio. This must be

Option	Description
	activated in order to be able to send valid package versions.  You can find detailed information on this in the <b>Project backup</b> node in the <b>Versioning</b> node.
<b>Upload time</b>	Timestamp from when the package of the Engineering Studio was transferred with the wizard.
<b>Uploaded by</b>	<b>Identity Service</b> user who transferred the project of the Engineering Studio with the wizard.
<b>Service Engine</b>	Version of the Service Engine files. Corresponds to the configuration of the <b>Create Service Engine files for</b> property in Engineering Studio when creating the package.  <b>Note:</b> If this information is unknown, no value is displayed.
<b>Comment</b>	Comment for the zenon project package. This comment can be entered in Engineering Studio when creating a package in the wizard (on page 324) in the option package comment. The comment can also be changed in Device Management.
[pencil_symbol]	Opens the dialog to edit a comment.

### NAVIGATION AND STATUS BAR

Items per page: 10 ▾ 1 – 3 of 3 |< < > >|

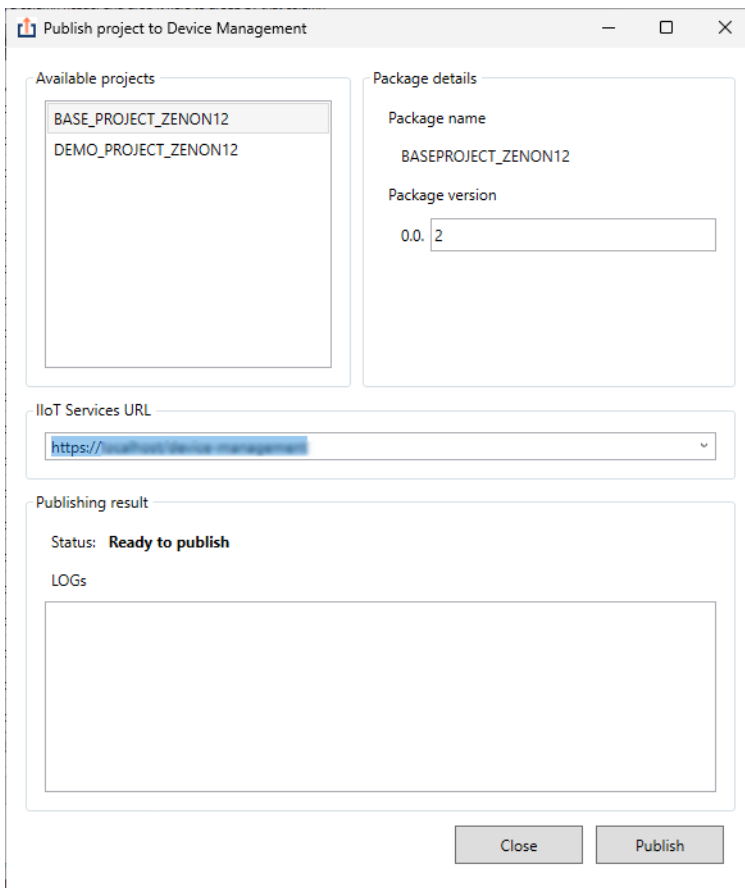
The status bar allows you to customize the view of the respective page and to navigate in the list view.

Option/symbol	Description
<b>Items per page</b>	Number of items shown per page. Selection from a drop-down list.
<b>[a] - [b] of [c]</b>	Sum of all available items and information on the items shown: <ul style="list-style-type: none"> <li>▶ <i>[a]</i>: Number of the first item shown</li> <li>▶ <i>[b]</i>: Number of the last item shown</li> <li>▶ <i>[c]</i>: Sum of all items</li> </ul>

Option/symbol	Description
Zur ersten Seite (  < )	Jumps to first page of the list view.
Vorherige Seite (<)	Jumps to previous page of the list view. <b>Note:</b> Not available on the first page.
Nächste Seite (>)	Jumps to the next page of the list view. <b>Note:</b> Not available on the last page.
Zur letzten Seite (> )	Jumps to the last page of the list view.

### 13.3.1 Deploying zenon projects for Device Management

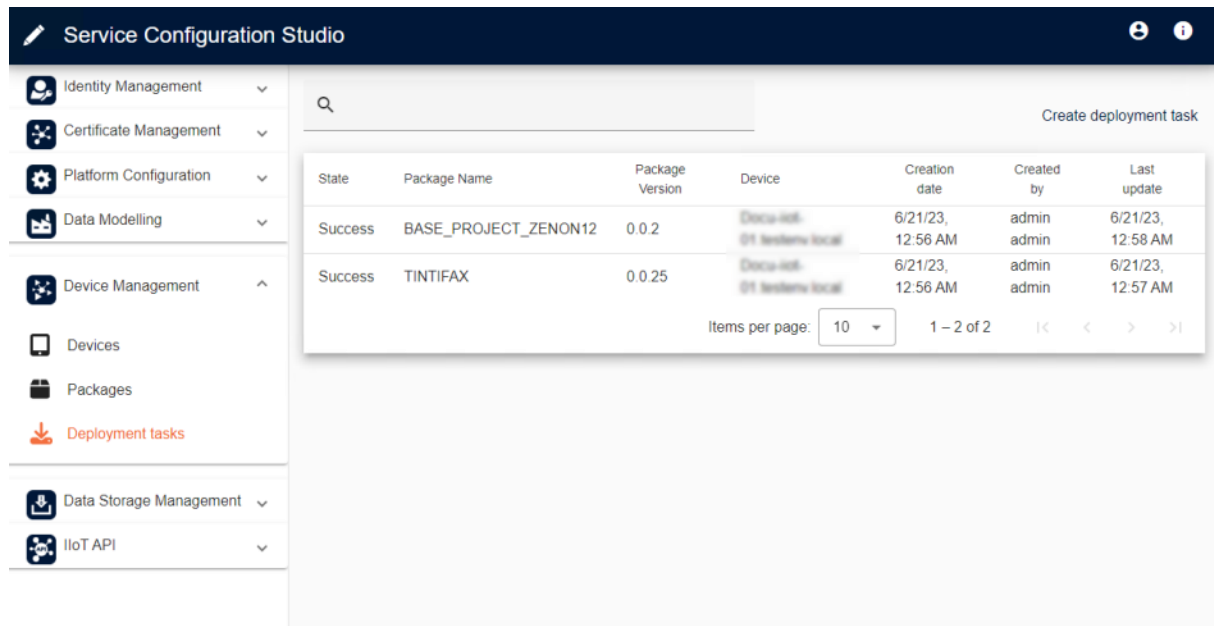
The deployment of packages is implemented in Engineering Studio with a wizard.



You can find detailed information for the transfer of a project from Engineering Studio in the **Device Management** (on page 323) node in the **IIoT Services - configuration in Engineering Studio** (on page 307) node.

## 13.4 Deployment task

List of all **Device Management** deployment tasks on IIoT Services.



State	Package Name	Package Version	Device	Creation date	Created by	Last update
Success	BASE_PROJECT_ZENON12	0.0.2	Device-101-01 (zenon-101)	6/21/23, 12:56 AM	admin	6/21/23, 12:58 AM
Success	TINTIFAX	0.0.25	Device-101-01 (zenon-101)	6/21/23, 12:56 AM	admin	6/21/23, 12:57 AM

### BUTTON: CREATE DEPLOYMENT TASK

Opens the tab for configuring a new deployment task.

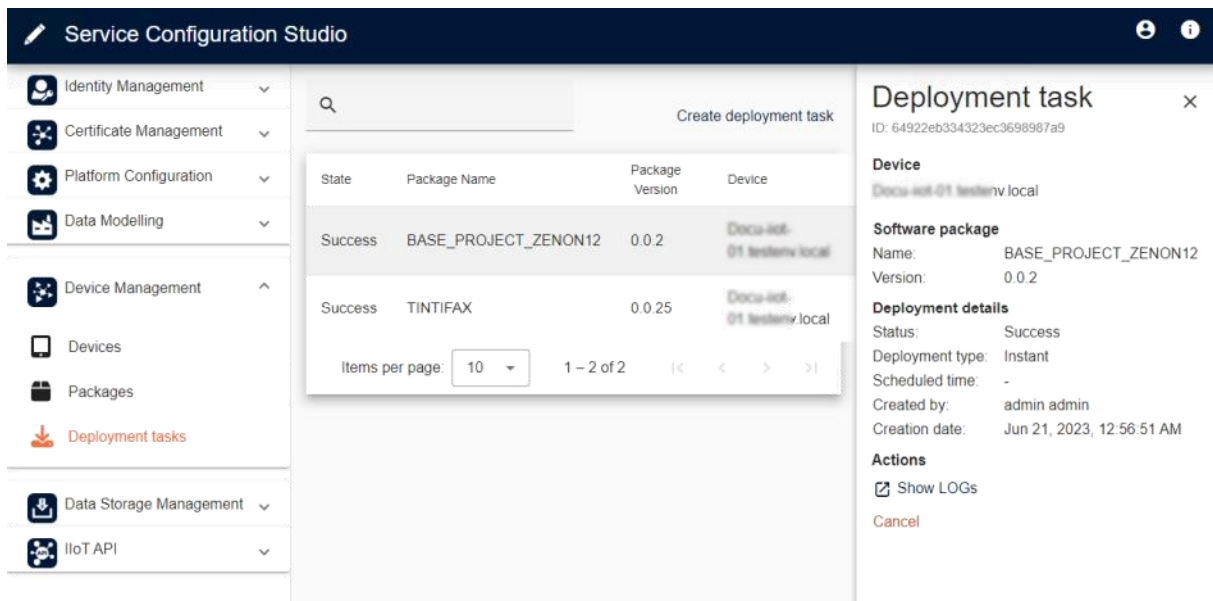
### LIST: DEPLOYMENT TASKS

The items of this list can be sorted by clicking on the column heading.

Option	Description
<b>State</b>	<p>Current state of the deployment task. The state is visualized as text and with colors.</p> <ul style="list-style-type: none"> <li>▶ <i>Success</i> (green) The deployment task was performed successfully. The software package has been transferred to the device.</li> <li>▶ <i>Failed</i> (red) The deployment task failed and was not performed successfully. No software package was transferred to the device.</li> <li>▶ <i>Pending</i> The deployment task is planned but has not been successfully performed yet.</li> </ul>

Option	Description
	<ul style="list-style-type: none"> <li>▶ <i>Canceling</i> A planned deployment task which has not been performed yet (previous state was pending) is canceled.</li> <li>▶ <i>Canceled (orange)</i> A previously-planned deployment task has been successfully canceled.</li> </ul>
<b>Package Name</b>	Name of the software package.
<b>Package Version</b>	Version of the software package which is delivered to the device by the deployment task.
<b>Device</b>	FQDN of the target device to which the software package is delivered.
<b>Creation date</b>	Timestamp of the creation of the deployment task.
<b>Created by</b>	User name of the user who has created the deployment task.
<b>Last update</b>	Timestamp of the latest update of the deployment task.

Clicking on the item opens a tab with detailed information.



The screenshot shows the Service Configuration Studio interface. On the left is a navigation menu with categories like Identity Management, Certificate Management, Platform Configuration, Data Modelling, Device Management, Devices, Packages, Deployment tasks, Data Storage Management, and IIoT API. The main area displays a table of deployment tasks with columns for State, Package Name, Package Version, and Device. Two tasks are visible: one for 'BASE\_PROJECT\_ZENON12' (version 0.0.2) and one for 'TINTIFAX' (version 0.0.25), both in 'Success' state and targeting 'Docu-let-01 testenv local'. A 'Create deployment task' button is at the top right of the table. A detailed panel for the selected task is open on the right, showing its ID, device, software package name and version, deployment details (Status: Success, Deployment type: Instant, Scheduled time: -, Created by: admin admin, Creation date: Jun 21, 2023, 12:56:51 AM), and actions like 'Show LOGS' and 'Cancel'.



### 13.4.1 Create deployment tasks

You can configure the transfer (=deployment) of software packages on this page. The options correspond to existing project configurations:

- ▶ Selection of devices corresponds to the list on the **Device** page.
- ▶ Selection of the software packages to be deployed corresponds to the list on the **Software Package** page.

Clicking on the **Create deployment task** button opens the tab for configuring a deployment task.

**Create a new deployment task**

Device  
 aanv-w10x64-v6.testenv.local ▼

---

Software Package  
 PROJECT\_2 ▼

---

Package Version  
**#** 0.0.50 (latest) ▼

---

Use device-specific Project ID

---

Deployment type  
 Instant ▼

---

Option	Description
<b>Device</b>	List of all available devices. Select from drop-down list.  The display depends on the configuration of the device (on page 271): <ul style="list-style-type: none"> <li>▶ Device Name: If a corresponding device name has been configured, this is displayed in the list.</li> <li>▶ Device ID: If no corresponding device name has been configured, the automatically generated device ID is displayed in the list.</li> </ul>
<b>Software Package</b>	List of all available software packages. Select from drop-down list. The list also contains the information on which version of Service Engine the Service Engine files were created.  <b>Note:</b> Only available if a <b>Device</b> has been selected.
<b>Package Version</b>	List of versions of the selected software package. Select from

Option	Description
	<p>drop-down list.</p> <p>The latest version is marked with the additional text <b>(latest)</b>. Corresponds to the configuration of the <b>Create Service Engine files for</b> property in Engineering Studio when creating the package.</p> <p><b>Note:</b> Only available if a <b>Software Package</b> has been selected.</p>
<p><b>Use device-specific Project ID</b></p>	<p>Option for the automatic generation of a unique GUID for the deployment task.</p> <ul style="list-style-type: none"> <li>▶ <i>Active:</i> Generates a new, device-specific, unique GUID. This GUID is used as the project GUID. If the same project is distributed to several devices and these devices connect to IIoT Services, this GUID is used for unique identification. If this option has been activated, it ensures that several devices with the same project do not overwrite their data on the Data Storage or, in the event of communication with the Data Hub, transfer contradictory variable values. Activate this option to minimize the danger of overwriting and if you use IIoT Services primarily for the evacuation of variable values to the Data Storage or for data queries via API.</li> <li>▶ <i>Inactive:</i> No new, device-specific, unique GUID is generated. The GUID of the zenon project is used. As a result, it is ensured that full functionality of all zenon services in Service Engine is supported. However, if this option is deactivated, it must be ensured that client-specific project data is not overwritten by the current project data.</li> </ul> <p>Default: <i>activated</i></p> <p><b>Attention:</b> The updating of the Project GUID is not possible in all parts of the project for the device agent for technical reasons. As a result, it may happen that, if the option is activated, zenon project data is no longer referenced correctly and complete functionality is not available on the client/device.</p> <p>The following rule is applicable as orientation:</p> <ul style="list-style-type: none"> <li>▶ Activate this option if you use IIoT Services to evacuate data and variable values to the Data Hub. With queries via the IIoT API, it is also recommended that this option is</li> </ul>

Option	Description
	activated. <ul style="list-style-type: none"> <li>▶ Deactivate this option if you want to use the full functionality of Service Engine with all services. In this case you must ensure that, when using Data Storage and Data Hub communication, the recorded data from the different instances do not overwrite each other.</li> </ul>
<b>Deployment type</b>	Type of deployment. Select from drop-down list. <ul style="list-style-type: none"> <li>▶ <i>Instant</i> Software package is transferred immediately to the selected devices.</li> <li>▶ <i>Scheduled</i> Software package is transferred based on a schedule. If this deployment type is selected, additional configuration options are displayed for configuring the schedule.</li> </ul>
<b>Note on compatibility</b>	Compatibility note for the Service Engine installed on the device.  This text displays the compatibility of the package with the Service Engine installed on the device.

### CONFIGURATION OPTIONS WITH “SCHEDULED” DEPLOYMENT TYPE

If the Scheduled deployment type is selected, additional options are displayed.

**Create a new deployment task**

Device  
 aanv-w10x64-v6.testenv.local ▼

Software Package  
 PROJECT\_2 ▼

Package Version  
 # 0.0.50 (latest) ▼

Use device-specific Project ID

Deployment type  
 Scheduled ▼

Date  Time

Select timezone  
 Vienna (UTC+02:00) ▼

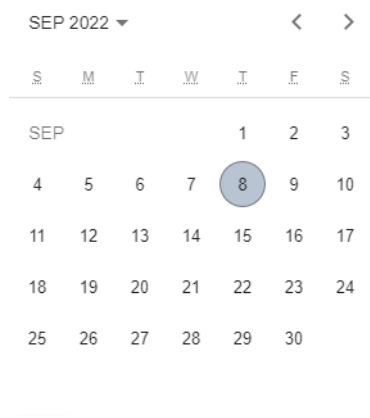
Option	Description
<b>Date</b>	Date on which the deployment task is to be performed. Selection in a calendar dialog.
<b>Time</b>	Time when the deployment task is to be performed. Selection in a clock dialog.
<b>Select timezone</b>	Selection of the time zone that applies for the date and time. The deployment task is performed on the device on the configured date at the configured time using the time zone selected here.  Select from drop-down list.

**NAVIGATION**

Option	Description
<b>Cancel</b>	Discards the set configurations and closes the configuration.
<b>Create deployment task</b>	Applies the configuration and creates a new deployment task.  <b>Note:</b> This button is only available if the deployment task has been completely configured and all options have been configured.

### 13.4.1.1 Select date in the calendar display

You can configure the date on which the deployment task is to be performed in a calendar display. This view is opened automatically by the **Date** option. In the header of the dialog, you can click to switch between the month and year view.



Month view for selecting the date on which the deployment task is to be performed.

- ▶ The current date is displayed with a light blue circle.
- ▶ The date on which the task is to be performed is displayed with a dark blue circle.

Option	Description
<b>Year view/month view</b>	<p>Depending on the current view, the years or months of the selected year are displayed. After selecting a year, the view automatically switches to the month view.</p> <ul style="list-style-type: none"> <li>▶ <i>Year view:</i> After selecting the year, all months of that year are displayed for selection.</li> <li>▶ <i>Month view:</i> Calendar month view for selecting the execution date.</li> </ul> <p>Click to switch between the views.</p>
<b>Left arrow (symbol &lt;)</b>	Switches to the previous month in the month view.
<b>Right arrow (symbol &gt;)</b>	Switches to the following month in the month view.

#### CLOSE DIALOG

Option	Description
<b>OK</b>	Applies settings and closes the dialog.

Option	Description
Cancel	Discards all changes and closes the dialog.

### 13.4.1.2 Select time in the clock display

You can configure the time when the deployment task is to be performed in a clock display. This view is opened automatically by the **Time** option. In the header of the dialog, you can click to switch between the hours and minutes. If the hour is selected first, the display will automatically switch to the minute view.



Select the hour by clicking on the clock display. In the case of a 24-hour format, select the afternoon hours in the inner circle.



Select the minutes by clicking on the clock display.

**CLOSE DIALOG**

Option	Description
OK	Applies settings and closes the dialog.
Cancel	Discards all changes and closes the dialog.

### 13.4.2 Detail view - Deployment task

The detail view provides you with additional information about the deployment task.


**Deployment task** ✕

ID: 631879308335bce216f2bea5

**Device**  
aanv-w10x64-v6.testenv.local

**Software package**  
Name: PROJECT\_2  
Version: 0.0.50

**Deployment details**  
Status: Success  
Deployment type: Instant  
Scheduled time: -  
Created by: admin admin  
Creation date: Sep 7, 2022, 12:57:52 PM

**Actions**  
[Show LOGs](#)   
[Cancel](#)

#### DEPLOYMENT TASK

The ID of the deployment task is shown as a header of the detail view.

#### DEVICE

ID of the target device to which the software package contained in the deployment task is delivered.

#### SOFTWARE PACKAGE

Option	Description
<b>Name</b>	Name of the software package delivered by the deployment task.
<b>Version</b>	Version number of the software package delivered by the deployment task.

#### DEPLOYMENT DETAILS

Option	Description
<b>Status</b>	Current state of the deployment task. The state is visualized as text and with colors.



Option	Description
	<ul style="list-style-type: none"> <li>▶ <i>Success</i> (green) The deployment task was performed successfully. The software package has been transferred to the device.</li> <li>▶ <i>Failed</i> (red) The deployment task failed and was not performed successfully. No software package was transferred to the device.</li> <li>▶ <i>Pending</i> The deployment task is planned but has not been successfully performed yet.</li> <li>▶ <i>Cancelling</i> A planned deployment task which has not been performed yet (previous state was pending) is canceled.</li> <li>▶ <i>Canceled</i> (orange) A previously-planned deployment task has been successfully canceled.</li> </ul>
<b>Cancellation date</b>	Timestamp of the cancellation of the deployment task.  <b>Note:</b> This option is only visible if the deployment task has been canceled.
<b>Canceled by</b>	User name of the user who canceled the deployment task.  <b>Note:</b> This option is only visible if the deployment task has been canceled.
<b>Cancellation comment</b>	<b>Note:</b> This option is only visible if the deployment task has been canceled.
<b>Deployment type</b>	Type of delivery: <ul style="list-style-type: none"> <li>▶ <i>Instant:</i> The deployment task is performed immediately. The selected software package is delivered to the device immediately after the deployment task is created.</li> <li>▶ <i>Scheduled:</i> The deployment task is performed at a configured time.</li> </ul>

Option	Description
Scheduled time	Timestamp of the planned execution of the deployment task.  <b>Note:</b> This information is not available for the Instant deployment type. This is displayed with a hyphen (-).
Created by	User name of the user who has created the deployment task.
Creation date	Timestamp of the creation of the deployment task.

### ACTIONS

Option	Description
Show LOGs	Opens a new window with all LOG entries for the deployment task.
Cancel	Button to cancel an existing deployment task. When the button is clicked on, a corresponding confirmation dialog is opened.

### SHOW LOGS - DETAIL VIEW

**Deployment Task Log**  
631879308335bce216f2bea5  
Package: PROJECT\_2 Version: 0.0.50

×

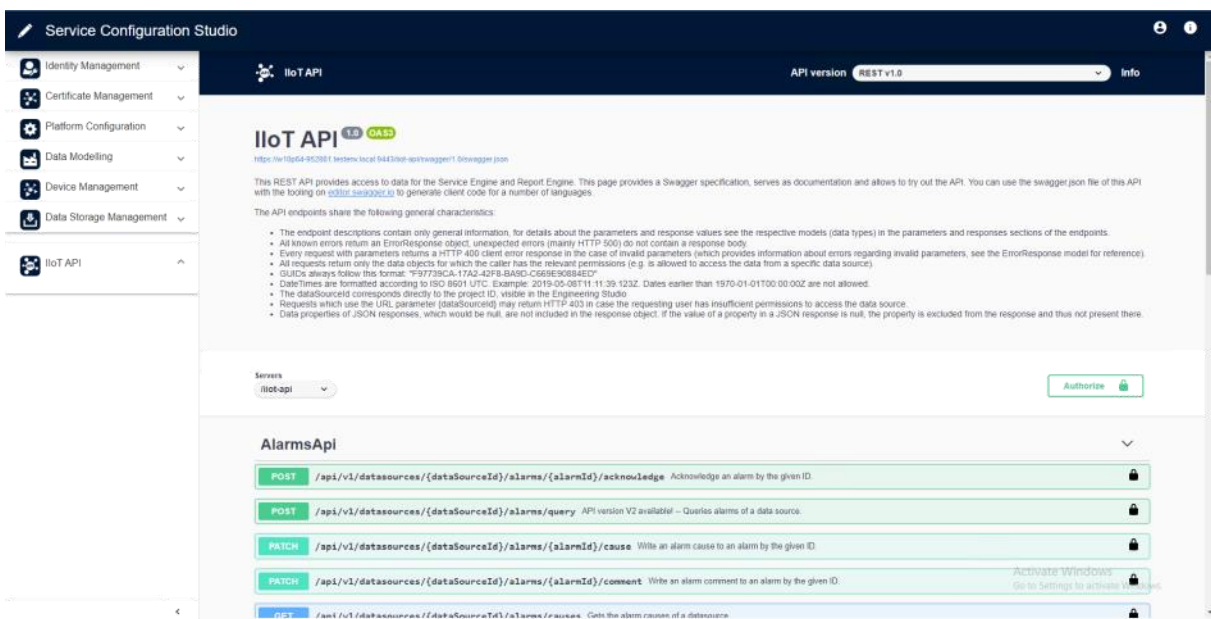
```
[INFO] [2022-09-07 12:57:52]: Task added by user or client with id: 63174b2e920fa02c53997f5e
[INFO] [2022-09-07 12:58:15]: Start processing HTTP request GET https://aanv-w10x64-v6.testenv.local:9415/api/agent/v1/packages
[INFO] [2022-09-07 12:58:15]: Sending HTTP request GET https://aanv-w10x64-v6.testenv.local:9415/api/agent/v1/packages/PROJECT_2
[INFO] [2022-09-07 12:58:15]: Received HTTP response headers after 35.4385ms - 200
[INFO] [2022-09-07 12:58:15]: End processing HTTP request after 35.6962ms - 200
[INFO] [2022-09-07 12:58:16]: Downloaded package for task 631879308335bce216f2bea5 successfully. Package PROJECT_2 Version 0.0.50
[INFO] [2022-09-07 12:58:16]: Start executing deployment task for package PROJECT_2 : 0.0.50
[INFO] [2022-09-07 12:58:19]: Plugin [CopaData.ServiceGrid.DeviceManagement.Plugin.Plugins.PublishZenonProject.PublishZenonProject]
[INFO] [2022-09-07 12:58:19]: Plugin [CopaData.ServiceGrid.DeviceManagement.Plugin.Plugins.PublishZenonProject.PublishZenonProject]
[INFO] [2022-09-07 12:58:19]: Plugin [CopaData.ServiceGrid.DeviceManagement.Plugin.Plugins.PublishZenonProject.PublishZenonProject]
[INFO] [2022-09-07 12:58:19]: Plugin [CopaData.ServiceGrid.DeviceManagement.Plugin.Plugins.PublishZenonProject.PublishZenonProject]
[INFO] [2022-09-07 12:58:19]: Plugin [CopaData.ServiceGrid.DeviceManagement.Plugin.Plugins.PublishZenonProject.PublishZenonProject]
[INFO] [2022-09-07 12:58:19]: Plugin [CopaData.ServiceGrid.DeviceManagement.Plugin.Plugins.PublishZenonProject.PublishZenonProject]
[INFO] [2022-09-07 12:58:19]: Plugin [CopaData.ServiceGrid.DeviceManagement.Plugin.Plugins.PublishZenonProject.PublishZenonProject]
[INFO] [2022-09-07 12:58:34]: Plugin [CopaData.ServiceGrid.DeviceManagement.Plugin.Plugins.PublishZenonProject.PublishZenonProject]
[INFO] [2022-09-07 12:58:35]: Executing deployment task 631879308335bce216f2bea5 finished, status is Success
```

Copy all logs
Close

## NAVIGATION

Button	Description
Copy all LOGs	Copies all LOG entries of the LOG window to the clipboard.
Close	Closes the LOG window.

## 14 IIoT API



The IIoT API allows you to easily connect external **Clients** to the zenon Software Platform using the REST API.

### Clients include for example:

- ▶ Mobile Apps
- ▶ Web applications
- ▶ Manufacturing Execution Systems (MES)
- ▶ Enterprise Resource Planning Systems (ERP)

You can integrate any application into your zenon network via IIoT Services. For clients to be able to access project data, for example, you must grant relevant permissions in **Access control** (on page 194).

## FUNCTIONALITIES AND DOCUMENTATION

The IloT API currently supports the following functionalities:

### Service Engine

- ▶ Querying and writing of real-time data
- ▶ Querying of archive data
- ▶ Querying and confirmation of alarms including equipment groups (as JSON array) as well as resources label.
- ▶ Querying of chronological events including equipment groups (as JSON array) as well as resources label.

### Report Engine

- ▶ Triggering and querying of Reports
- ▶ Triggering and querying of SQL elements

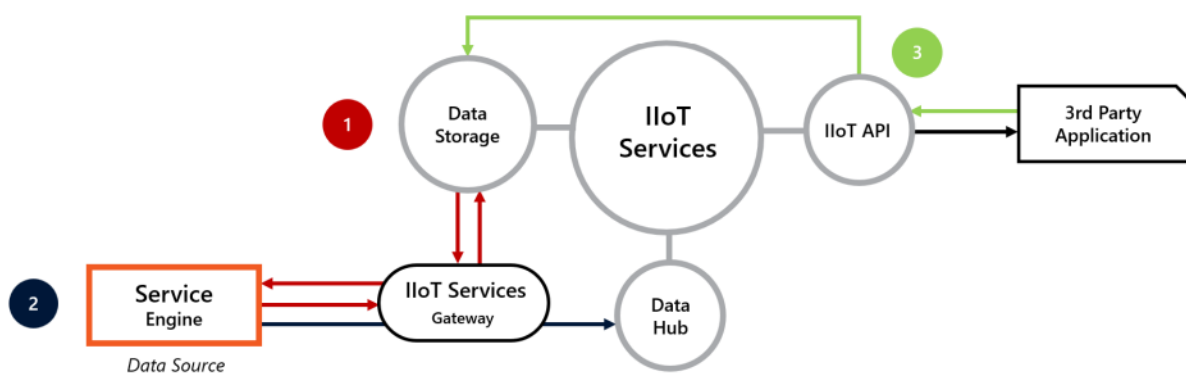
### Data Storage

- ▶ Querying of archive data

All IloT API functions are documented in detail in the Swagger help of Service Configuration Studio.

As of version 14, this documentation has been supplemented with the differences from API version 1 to API version 2.

## 14.1 Service Engine - third-party application: Provide process data



Process data entered into the IloT Services can be processed by any third-party application via the IloT API.

The IloT API allows the connection of third-party applications. Third-party applications are applications that are not part of the zenon software platform.

Third-party applications can process data from one or more Service Engine instances using the IloT API.

## AREA OF APPLICATION

### Third-party applications include for example:

- ▶ Mobile Apps
- ▶ Web applications
- ▶ Manufacturing Execution Systems (MES)
- ▶ Enterprise Resource Planning Systems (ERP)

You can in principle connect any interfaceable application to the IloT API.

## SUPPORTED DATA ACTIONS

### The IloT API supports the following data actions in Service Engine:

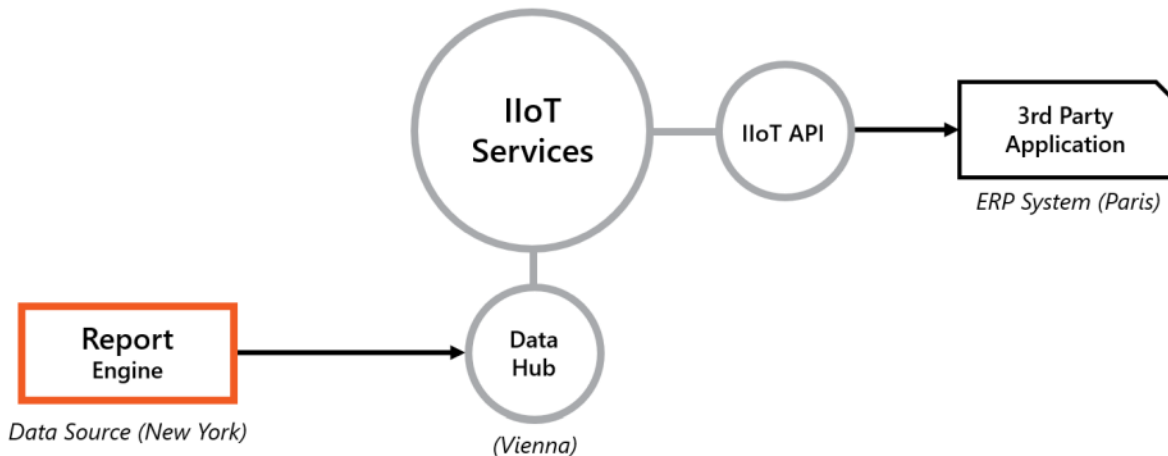
Supported data action	Variable access authorization*
Read alarms	<i>Read only</i>
Acknowledge alarms	<i>Read-write</i>
Comment on alarms	<i>Read-write</i>
Set causes of alarms	<i>Read-write</i>
Variables** - read	<i>Read only</i>
Variables** - write	<i>Read-write</i>
Read archive data	<i>Read only</i>
Read events	<i>Read-only***</i>
Comment on events	<i>Read-write</i>

\* Required access authorization in Service Engine (data source).

\*\* \* Simple variable type (no structure variables, no arrays).

\*\*\* No access authorization is required for system events.

## 14.2 Report Engine > third-party application: Provide report data



The IloT API allows you to enable third-party applications to access the data of Report Engine.

Report Engine can provide report data for third-party applications via IloT Services. Third-party applications access resources in IloT Services via **REST Interface**.

### AREA OF APPLICATION

The IloT API allows you to access the data of Report Engine using any third-party application.

#### Third-party applications include for example:

- ▶ Mobile Apps
- ▶ Web applications
- ▶ Manufacturing Execution Systems (MES)
- ▶ Enterprise Resource Planning Systems (ERP)

You can in principle connect any interfaceable application to the IloT API.

### SUPPORTED DATA ACTIONS

The IloT API allows you to perform various data actions in Report Engine.

Supported data actions:

- ▶ Reports - execute
- ▶ Reports - read results

- ▶ Database queries - execute
- ▶ Database queries - read results

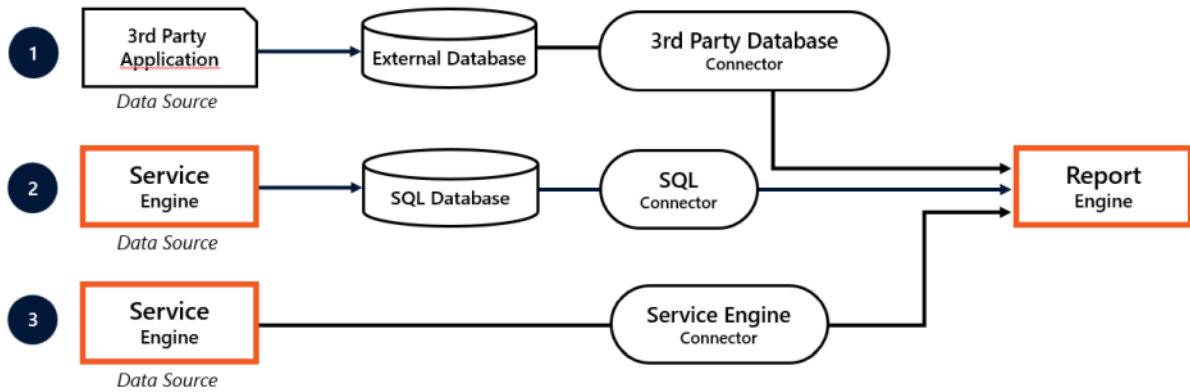
## CONFIGURATIONS

**The following configurations are required for reports and database queries:**

- ▶ Reporting Studio: Configuration in the **Service Node Interface** dialog
- ▶ Service Configuration Studio: Configuration of the **Report Permissions**

It is thus ensured that IIoT Services can access Report Engine reports and databases.

### 14.2.1 Data sources for Report Engine

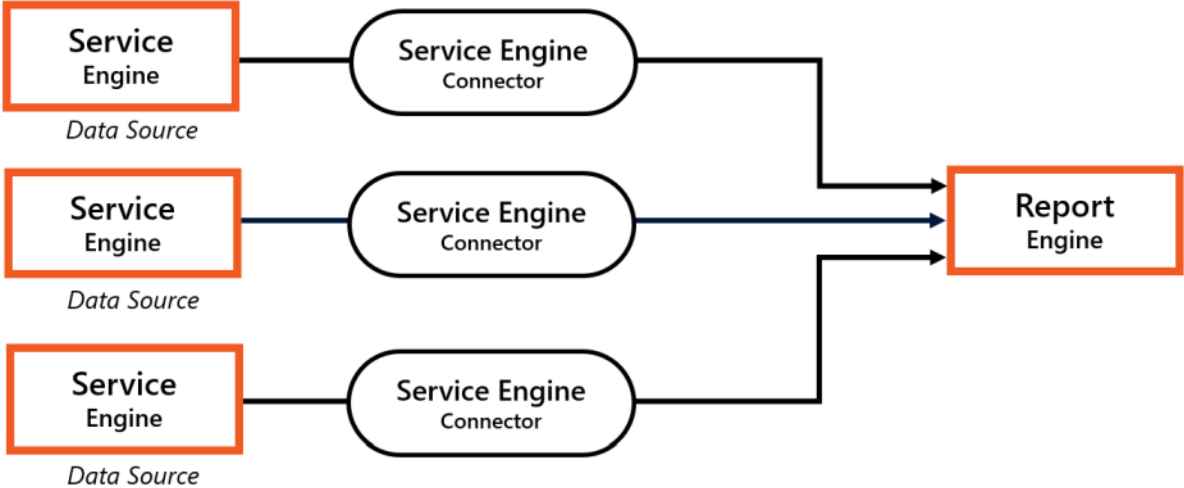


- Report Engine can evaluate the following data sources:
- 1) Data from third-party applications from an external database.
  - 2) Process data of a Service Engine from a SQL database.
  - 3) Process data of a Service Engine (without an intermediate database).

Report Engine can read and evaluate data from different sources. The connectors necessary for the connection depend on the particular use case.



### 14.2.2 Multiple Service Engine instances



Report Engine can collect and evaluate data from different Service Engine instances.

Report Engine allows you to collect data from different sources and evaluate it centrally. Thus, for instance, it is possible to connect multiple instances of Service Engine with Report Engine.

## 14.3 IIoT API

You can test the API using the interactive Swagger API documentation. The documentation contains all necessary information for use of the API.

The user must be logged on to **Identity Service** in order to use the interactive documentation.

The commands are summarized in groups. The respective commands in the list are shown or hidden by clicking on the arrow key.

## 14.4 Login to Swagger API documentation

Carry out the following steps to log in to the IIoT API:

- ▶ Click on the **Authorize** button.
- ▶ In the **Login** dialog process, the access token for access to the API is fetched and, in the case of HTTPS requests, sent to the API.
- ▶ You can now use the API.
- ▶ Clicking on **Logout** revokes the access permission again.

### **Hint**

Activate – if not yet set – the checkbox for the **iiotServicesAPI** and **dataStorageAPI** options in the authorization dialog.

## 14.5 Status bits for variables

When variable values are read, all status bits are returned. In addition, the selected set of status bits is also output as a JSON object.

When variable values are written, only values are written. Timestamp or status are not passed along.

### **Information**

You can find detailed information on this in the **Status processing** section.

## 14.6 Navigation bar

The navigation bar in the IIoT API offers the following options:

- ▶ **API Version:** Allows you to switch between the available API versions. By default, *Version 2* is selected. It is strongly recommended that you no longer use API *Version 1*, as of version 14.
- ▶ **Info:** Displays the installed version of the IloT API and the license status.

## 15 IloT Services Gateway

The **IloT Services Gateway** connects IloT Services to zenon applications. It also ensures compatibility between different release versions.



### Information

Recommendation: Generally speaking, you should always use the version of **IloT Services Gateway** that corresponds to the installed version of IloT Services.

### VERSION CHECK

Different versions of IloT Services and **IloT Services Gateway** can communicate with one another on the basis of a common protocol.

For communication, a check is carried out to see which version of the protocol is used by the individual components. The check is successful if all components use the same major version of the protocol. Minor versions can be different. If the major version is different for a component, communication is no longer possible.

#### Example:

- ▶ Components with *20.00* can communicate with *20.10*.
- ▶ Components with *20.10* cannot communicate with *30.10*



### Information

Valid major version for IloT Services 14: *20*

**Note:** For versions of the zenon Software Platform prior to version 14, all components must correspond exactly. This also includes the minor version.

## 15.1 Installation

For the connection between zenon applications and IIoT Services, the appropriate version of the **IIoT Services Gateway** must be selected and installed.

The following applications use the **IIoT Services Gateway**:

- ▶ Service Engine
- ▶ Engineering Studio
- ▶ Report Engine
- ▶ Reporting Studio

**Important:** You must always execute both installers (x86 and x64) on each client. This way, you ensure that these clients can connect to the IIoT Services.

### Tip

Check the installation:

Under **Apps and features**, the Windows operating system shows a separate entry for each installed version of the **IIoT Services Gateway**.

## 15.2 Configuration

### PRIOR CONSIDERATIONS

Several versions of the **IIoT Services Gateway** can be installed on a computer at the same time. The system cannot use these versions at the same time however. Only one version of the **IIoT Services Gateway** can ever be centrally configured and used.

These processes can install a **IIoT Services Gateway**:

- ▶ Installation of zenon applications via the platform setup.
- ▶ Build update of installed zenon applications.
- ▶ Installation of the **IIoT Services Gateway** via two separate installers (x64 and x86).

In practice, several versions of the **IIoT Services Gateway** are typically installed on a computer at the same time.

 **Hint**

Use several versions alternately:

You can use several versions of the **IIoT Services Gateway** alternately on one computer. For each change, you must configure the respective required version of the **IIoT Services Gateway** manually in *zenon6.ini*.

## DEFAULT CONFIGURATION

By default, zenon applications always connect to IIoT Services via the most-recently-installed version of the **IIoT Services Gateway**.

The default configuration covers the usual application purposes and therefore does not generally need to be adjusted manually by the user.

## MANUAL CONFIGURATION

Manual configuration of the **IIoT Services Gateway** by the user is only required in a few cases.

You can use manual configuration to stipulate to the system which version of the **IIoT Services Gateway** zenon applications connect to the IIoT Services.

### General requirement:

Several versions of the **IIoT Services Gateway** are installed on the computer.

### Manual configuration can, for example, be necessary in the following cases:

- ▶ Subsequent downgrade of a zenon installation
- ▶ Parallel installations of different zenon versions on one computer
- ▶ Connection from zenon applications to different versions of the IIoT Services
- ▶ The zenon version used does not support the latest version of the **IIoT Services Gateway**.
- ▶ The connection should be established with a current **IIoT Services Gateway** to the IIoT Services of an older version.

 **Hint**

Restart applications and services:

You must restart the following components after manual configuration of the **IIoT Services Gateway**:

- ▶ All zenon apps connected to the IIoT Services: Service Engine, Engineering Studio and Reporting Studio
- ▶ The Windows service for the Report Engine service node (if you are using Report Engine): *zanMQTTClientxxxx*

The new configuration is only effective after restarting these applications and services.

## 15.2.1 Configuration in zenon6.ini

The **IIoT Services Gateway** is configured centrally in the *%cd\_system%\zenon6.ini* file. This setting is applicable for all zenon applications installed on the computer.

The default configuration is as follows:

### [ServiceGridGateway]

*Version=LAST*

In this configuration, zenon applications connect to the most recent version of the **IIoT Services Gateway** that is installed on the computer.

### Example of configuration for version 11.0:

### [ServiceGridGateway]

*Version=11\_0*

In this example, zenon applications connect to **IIoT Services Gateway 11**.

## SYNTAX

The syntax for manual configuration of the version is "**MM\_N**". The first two figures "**MM**" define the version number of the major release. The last figure "**N**" defines the minor release.

 **Hint**

Configure the figure for the minor release:

The last figure must always be given, including for major releases, such as **IIoT Services Gateway** 11 for example. In this case, you must configure the value "11\_0".

## 16 IIoT Services - configurations in Engineering Studio

In Engineering Studio, you can undertake different configurations for connections between zenon apps and services of the IIoT Services.

### 16.1 Trust

Establishing trust is important for secure communication with the respective IIoT Services. Trust is established via a trusted HTTPS certificate or root certificate.

You can find further information on this in the **Trust** (on page 259) node and in the **Configure trust** (on page 261) node.

### 16.2 IIoT Services

The Service Engine communicates with services of the IIoT Services.

Supported IIoT Services:

- ▶ **Data Hub:** Data transfer of live data and archive data between apps.
- ▶ **Identity Service:** User authentication via IIoT Services.
- ▶ **Data Storage:** Evacuation and reading back of archive data, alarm data and event data.
- ▶ **Device Management:** Monitoring and software distribution in the zenon software platform

In general, the following applies:

- ▶ Multiple instances of **Data Hub** can be available in a network.
- ▶ Each IIoT Services instance provides only one **Data Hub**.
- ▶ **Data Hub** must be configured separately for each project.
- ▶ For the communication of Service Engine with the IIoT Services and for configuration in Engineering Studio, trust has to have been established on the computer.

- ▶ on the respective computer a **Certificate Bundle** has to be installed. This can be installed with the **IIoT Services Connection Wizard**.

## 16.2.1 Connection to IIoT Services

A zenon project communicates with IIoT Services, if the corresponding connections exist. Connections are configured with the **IIoT Services Connection Wizard**.

### Hint

If you use Report Engine and the **Metadata Synchronizer** for reporting, the following procedure is recommended:

First establish a connection to IIoT Services for Report Engine. As a result of this, the reporting can be configured via Report Engine when executing the **IIoT Services Connection Wizard** in the **Report Engine Connection settings** wizard dialog. The wizard then automatically carries out the necessary connection configuration.

## CONFIGURATION IN ENGINEERING STUDIO

Follow the steps below to get the Engineering Studio to start the **IIoT Services Connection Wizard** and to configure a connection to the IIoT Services:

1. Highlight or activate a project in Engineering Studio.
2. Go to the **Network** node in the project properties.
3. Go to property group **IIoT Services**.
4. Activate the **Activate IIoT Services** checkbox.  
This activates the configuration of the property **Connection settings** as well as the button ....
5. Click on the .... button.  
This starts the **IIoT Services Connection Wizard**.
6. Configure the options in the wizard dialogs.
7. After successfully configuring the **IIoT Services Connection Wizard** find the **IIoT Service URL** used and the **Client-ID** in the input field of **Connection settings**.

### Attention

If you use the **IIoT Services Connection Wizard** to configure the **Connection settings** for a global project, then only the **IIoT Service URL** is displayed. The **Client-ID** is not displayed.



## 16.2.2 Access permission for variables

For communication between Service Engine and IIoT Services, the variables whose values are exchanged must be configured with the corresponding access permission. You can configure this access permission for a variable in Engineering Studio.

Further information on this can be found in the **External settings** node in the **IIoT Services** node.

### Attention

Only variables with **simple data type** are suitable for this. Structure variables and root variables of arrays are not available in IIoT Services.

## 16.2.3 Data Storage

**Data Storage** can be used for the central storage of archive data, alarms and events.

Generally:

- ▶ The configuration of the data to be stored is carried out in Engineering Studio.
- ▶ The access permission for the variables is defined in the Engineering Studio.
- ▶ The continuous evacuation of data from Service Engine in the **Data Storage** is carried out via the REST interface.

*OAuth 2.0* is used as the authentication method.

### Tip

In Engineering Studio, you only need to configure the connection to **Data Storage** if you want to actually use this service.

If this is not the case, you can leave the respective input fields empty.

## REQUIREMENTS

The following requirements must be met to ensure communication with **Data Storage**:

1. The **IIoT Services Gateway** is licensed.
2. In the Engineering Studio, a connection is configured to the IIoT Services (on page 308).
3. The access permission for the variables are configured correctly.

4. The user permissions to communicate with the **Data Storage** are in **Identity Service** correctly configured.

Detailed information on this service can be found in the **Data Storage** (on page 115) node.

### **Attention**

Project backups can contain security-critical information and data. For example, the client secret of the **Identity Service** for the IIoT Services is part of a project backup.

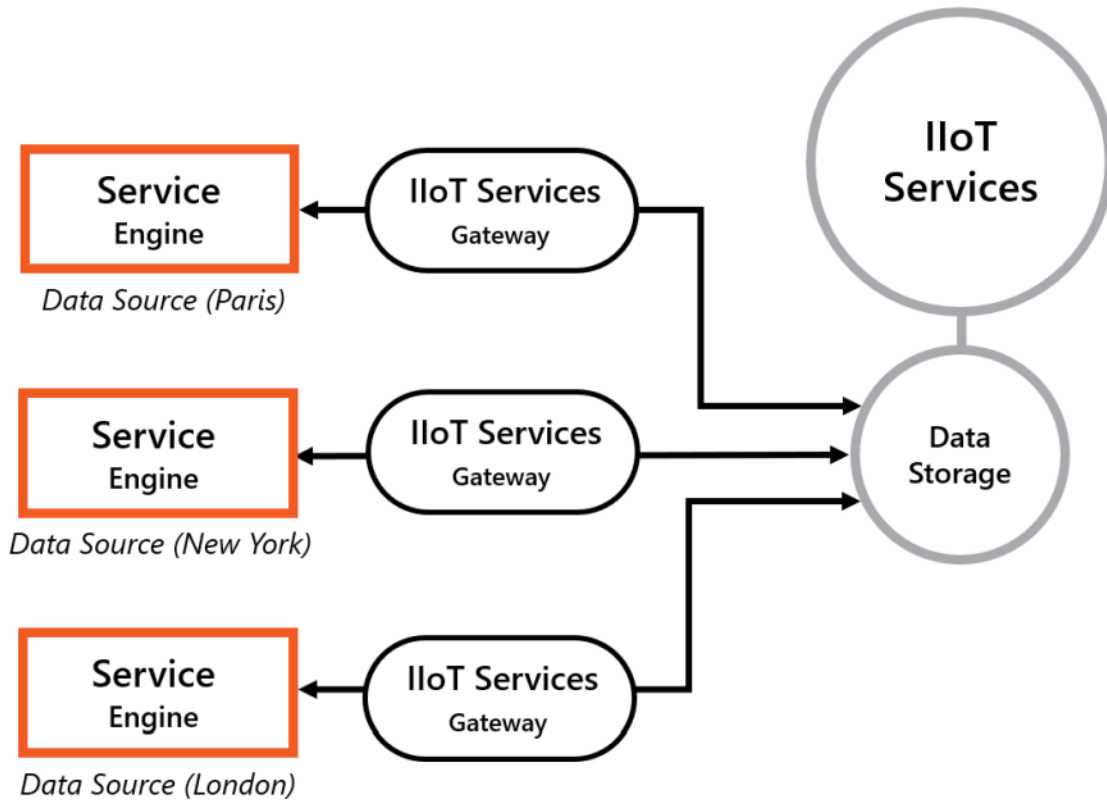
If you pass on a project backup, be sure to remove the Client Secret before creating the project backup. Otherwise, unwanted and unauthorized access to your **Identity Service** or **Data Storage** may occur.

## 16.2.3.1 Configure connection to Data Storage

Carry out the following steps to configure the connection to **Data Storage**:

1. Make sure in advance that the computer on which you are doing your configurations in Engineering Studio has established a corresponding trust (on page 307) to IIoT Services.
2. Configure a connection to the IIoT Services (on page 308).

### 16.2.3.2 Data actions for Data Storage



Each Service Engine can evacuate its own data to Data Storage and restore them from there.

You can evacuate the following data to Data Storage:

- ▶ Archive (historical variable values)
- ▶ Alarms
- ▶ Events

You must configure this data accordingly in Engineering Studio.

The configuration applies for the following data transfers:

- ▶ The evacuation of data from Service Engine to **Data Storage**.
- ▶ Reading back the data from **Data Storage** to Service Engine.

After the configuration is completed, the data transfers are performed automatically as a background service.

## Requirements for using Data Storage

Certain requirements must be met in order to use **Data Storage**:

- ▶ Service EngineVersion 10.0 (or higher): Older versions do not support **Data Storage**.
- ▶ **Data Storage** must be configured (on page 309) in Service Engine.

**Tip**

### Evacuation to SQL database

**Alarms** and **events** can alternatively be evacuated to an SQL database too.

### 16.2.3.2.1 Data evacuation - overview

Depending on the type of data (archive data, alarms or events), data in Service Engine and the Data Storage are handled differently.

Data type	Source data in Service Engine	Evacuated data in Data Storage
<b>Archive data (historical variable values)</b>	After successful evacuation to <b>Data Storage</b> the data are deleted in Service Engine.	Are stored unchanged.  An update is not possible and is also not needed for archive data.
<b>Alarms</b>	Remain stored in Service Engine after a successful evacuation and can be updated.	Can subsequently be updated.  <b>Data Storage</b> automatically synchronizes itself with Service Engine. If the connection is interrupted, the data are buffered.
<b>Events</b>	Remain stored in Service Engine after a successful evacuation and can be updated.	Can subsequently be updated.  <b>Data Storage</b> automatically synchronizes itself with Service Engine. If the connection is interrupted, the data are buffered.

### 16.2.3.2.2 Evacuate Alarms to Data Storage

Carry out the following steps to evacuate alarms to Data Storage:

1. Open the project in Engineering Studio.
2. Make sure that the necessary access rights for all variables are set correctly with the alarms to be evacuated.
3. Go to the **Alarm Message List** node in the project properties.
4. Go to the **Data storage AML** group.
5. Select the *Ring buffer and historic data* entry in the **Save AML data** drop-down menu.
6. Click on the .... button next to the **Storage location** entry.  
This opens the dialog for selecting a storage location.
7. Activate the **Data Storage** checkbox.
8. Close the dialog by clicking the **OK** button.

### 16.2.3.2.3 Evacuate archive to Data Storage

The following applies for archives:

- ▶ Archives only contain historical variable values.
- ▶ Other data types (such as events or alarms) are not supported by archives.
- ▶ Only archives for which **Data Storage** has been configured as an option for evacuation are evacuated to **Data Storage**.

## CONFIGURATION OF THE ARCHIVE

Carry out the following steps to evacuate an archive to **Data Storage**:

1. Make sure in advance that the access permission for all variables in the archive are configured correctly.
2. Open the project in Engineering Studio.
3. Switch in the project tree to the **Historian** node.
4. In the detail view, select the archive that you want to evacuate.
5. Open the **Edit archive** dialog. To do so, select the **Edit archive** command in the toolbar or context menu.
6. Go to the **Save** tab.
7. Activate the **Data Storage** option.

The configuration of the archive is now complete. If a prerequisite is not met, only the option **Do not evacuate** will be shown during the configuration of the archive.

### ⚠ Attention

#### Data loss due to missing permissions

An archive can only be fully evacuated from Service Engine to **Data Storage** if sufficient access permission for the IIoT Services are set for all the variables to be evacuated.

#### Missing access permission have these consequences:

- ▶ The archive data for the affected variables cannot be evacuated to **Data Storage**.
- ▶ The archive data for the affected variables are deleted from Service Engine.

When creating the Service Engine files, you will receive warning messages if the variables are not configured correctly.

#### 16.2.3.2.4 Evacuate events to Data Storage

Carry out the following steps to evacuate the event data to Data Storage:

1. Open the project in Engineering Studio.
2. Make sure that the necessary access rights for all variables are set correctly with the events to be evacuated.
3. Go to the **Chronological Event List** node in the project properties.
4. Go to the **Data storage CEL** group.
5. Select the *Ring buffer and historic data* entry in the **Save CEL data** drop-down menu.
6. Click on the .... button next to the **Storage location** entry.  
This opens the dialog for selecting a storage location.
7. Activate the **Data Storage** checkbox.
8. Close the dialog by clicking the **OK** button.

You have thus configured the evacuation of event data.

#### 16.2.4 Identity Service

As an option for configuring project-specific user administration in Engineering Studio, the **Identity Service** for IIoT Services can also be used to authenticate the user in Service Engine. In addition, the authentication of Service Engine via **Identity Service** is mandatory for the evacuation of data to **Data Storage**. Detailed information on this service can be found in the **Identity Service** (on page 148) node.

### ⚠Attention

Project backups can contain security-critical information and data. For example, the client secret of the **Identity Service** for the IIoT Services is part of a project backup.

If you pass on a project backup, be sure to remove the Client Secret before creating the project backup. Otherwise, unwanted and unauthorized access to your **Identity Service** or **Data Storage** may occur.

You can configure **Identity Service** in the project properties of Engineering Studio.

1. Service Engine uses **Identity Service** to authenticate users.
2. Service Engine evacuates data to **Data Storage** of IIoT Services.

**Note:** For this evacuation, Service Engine must perform authentication via **Identity Service**. Service Engine uses OAuth 2.0 for authentication in **Identity Service** and access to the Data Storage.

### ⚠Attention

Make sure that the computer on which you are doing your configurations in Engineering Studio has established the corresponding trust (on page 307) with IIoT Services.

## 16.2.4.1 Login options for Identity Service

For authentication of a Service Engine user via **Identity Server** the following options are available:

- ▶ Internal login:  
Users log in to **Identity Service** via an internal user account.
- ▶ External login:  
Users log in to **Identity Service** via an external **Identity Provider**.

When using external identity providers, please note the following:

Passwords of user accounts of external identity providers cannot be changed with the **Edit User** screen type of the project-specific user administration in Service Engine.

## 16.2.4.2 Password changes in Service Engine

As the logged in user, you can change your password directly in Service Engine. This is also generally supported if Service Engine authenticates itself to the **Identity Service** for IIoT Services. However, it only works if you use an internal login.

**CASE A) INTERNAL LOGIN:  
IDENTITY SERVICE USES ITS OWN USER ADMINISTRATION**

The password change with Service Engine is supported. If you enter a password change in Service Engine, this change is effective in **Identity Service**. When you login the next time, you must use the new password.

**CASE B) EXTERNAL LOGIN:  
IDENTITY SERVICE USES AN EXTERNAL IDENTITY PROVIDER**

External identity providers are, for example, OpenLDAP or Microsoft Active Directory. A password change with Service Engine is not supported for external logins. You as the logged in user can enter a password change in Service Engine, but it will not be effective. When you login the next time, you must continue to use the old password.

**PASSWORDS OF USER ACCOUNTS OF EXTERNAL LOGINS**

Passwords of user accounts of external logins can only be changed using the administration tools of the respective identity provider. See for this also the node with the login options of Identity Service (on page 152).

**16.2.4.3 Compatibility table: User names**

You can use **Identity Service** for user authentication to Service Engine.

**The following should be noted:**

1. **Identity Service** can work with different identity providers.
2. Each identity provider defines user names differently.
3. The user login to Service Engine might be different than the user login to the web interface of **Identity Service**. This depends on the identity provider selected.
4. The selected user name must meet both the requirements of the identity provider and the requirements of Service Engine.

These points should be considered both for the general definition of user names as well as for the creation of individual user accounts.

**The table below provides further details:**

Identity provider	Requirements Identity provider	Requirements Service Engine	User name and login (Examples)
Internal user administration of Identity Service (on	None.  The user name is	The length is not limited.  To work together with apps from the zenon software platform, such as Service	<ul style="list-style-type: none"> <li>▶ User name (as defin <i>john.doe</i></li> <li>▶ User login to the w</li> </ul>



Identity provider	Requirements Identity provider	Requirements Service Engine	User name and login (Examples)
page 175)	freely definable.	Engine for example, the following process is strongly recommended: <ul style="list-style-type: none"> <li>▶ Length of 20 characters maximum. In the text field with the visualization of the logged-in user, user names with more than 20 characters are not displayed. The display for the complete user name is shown without limitation. With functions of the Service Engine service that use the user names (for example: AML, CEL), this entry remains empty.</li> <li>▶ The special characters '@' and '\' are not allowed in user names.</li> </ul>	<b>Service:</b> <i>john.doe</i>
<b>Azure Active Directory</b>	Email address according to the requirements of Azure Active Directory.	Supported with a <b>IDS Login</b> screen. To work together with apps from the zenon software platform, such as Service Engine for example, the following process is strongly recommended: <ul style="list-style-type: none"> <li>▶ Length of 20 characters maximum. In the text field with the visualization of the logged-in user, user names with more than 20 characters are not displayed. The display for the complete user name is shown without limitation. With functions of the Service Engine service that use the user names (for example: AML, CEL), this entry remains empty.</li> <li>▶ The special characters '@' and '\' are not allowed in user names.</li> </ul>	<ul style="list-style-type: none"> <li>▶ User name (as defined in <b>Directory</b>): <i>john.doe@mydomain.com</i></li> <li>▶ User login to the web application: <b>Service:</b> <i>john.doe@mydomain.com</i></li> </ul>

Identity provider	Requirements Identity provider	Requirements Service Engine	User name and login (Examples)
<p><b>Microsoft Active Directory</b></p>	<p>Email address according to the requirements of Microsoft Active Directory.</p> <p><b>Definition of terms</b></p> <ul style="list-style-type: none"> <li>▶ Email address: <i>john.doe@mydomain.com</i></li> <li>▶ local-part: <i>john.doe</i></li> <li>▶ domain-part: <i>mydomain.com</i></li> </ul>	<p>Supported with a <b>IDS Login</b> screen.</p> <p>To work together with apps from the zenon software platform, such as Service Engine for example, the following process is strongly recommended:</p> <ul style="list-style-type: none"> <li>▶ Length of 20 characters maximum. In the text field with the visualization of the logged-in user, user names with more than 20 characters are not displayed. The display for the complete user name is shown without limitation. With functions of the Service Engine service that use the user names (for example: AML, CEL), this entry remains empty.</li> <li>▶ The special characters '@' and '\' are not allowed in user names.</li> </ul>	<ul style="list-style-type: none"> <li>▶ User name (as defined in <b>Directory</b>): <i>john.doe@mydomain.com</i></li> <li>▶ User login to <b>Identity Service</b>: <i>john.doe@mydomain.com</i></li> </ul>
<p><b>OpenLDAP</b></p>	<p>None.</p> <p>Can be defined by the Distinguished Name Template itself.</p>	<p>Supported with a <b>IDS Login</b> screen.</p> <p>To work together with apps from the zenon software platform, such as Service Engine for example, the following process is strongly recommended:</p> <ul style="list-style-type: none"> <li>▶ Length of 20 characters maximum. In the text field with the visualization of the logged-in user, user names with more than 20 characters are not displayed. The display for the complete user name is shown without limitation. With functions of the Service Engine service that use the user names (for example: AML, CEL), this entry remains empty.</li> <li>▶ The special characters '@' and '\' are not allowed in user names.</li> </ul>	<ul style="list-style-type: none"> <li>▶ User name/distinguished name (<b>OpenLDAP</b>): <i>cn=john.doe,dc=mydomain.com</i></li> <li>▶ Distinguished Name Template placeholder: <i>cn={username},dc=mydomain.com</i></li> <li>▶ User login to the <b>Identity Service</b>: <i>john.doe</i></li> </ul> <p>The user login for Distinguished Name Template with multiple placeholders is described in chapter (on page 211).</p>

Identity provider	Requirements Identity provider	Requirements Service Engine	User name and login (Examples)
<p><b>RADIUS</b></p>	<p>None.</p> <p>User name according to the RADIUS directory used.</p>	<p>Supported with a <b>IDS Login</b> screen.</p> <p>To work together with apps from the zenon software platform, such as Service Engine for example, the following process is strongly recommended:</p> <ul style="list-style-type: none"> <li>▶ Length of 20 characters maximum. In the text field with the visualization of the logged-in user, user names with more than 20 characters are not displayed. The display for the complete user name is shown without limitation. With functions of the Service Engine service that use the user names (for example: AML, CEL), this entry remains empty.</li> <li>▶ The special characters '@' and '\' are not allowed in user names.</li> </ul>	<ul style="list-style-type: none"> <li>▶ User name (as defined): <i>john.doe</i></li> <li>▶ User login to the w <b>Service:</b> <i>john.doe</i></li> </ul>
<p><b>OpenID Connect</b></p>	<p>Depends on the <b>OpenID Connect</b> provider used.</p>	<p>Supported with a <b>IDS Login</b> screen.</p> <p>To work together with apps from the zenon software platform, such as Service Engine for example, the following process is strongly recommended:</p> <ul style="list-style-type: none"> <li>▶ Length of 20 characters maximum. In the text field with the visualization of the logged-in user, user names with more than 20 characters are not displayed. The display for the complete user name is shown without limitation. With functions of the Service Engine service that use the user names (for example: AML, CEL), this entry remains empty.</li> </ul> <p>The special characters '@' and '\' are</p>	<ul style="list-style-type: none"> <li>▶ User name (as defined <b>Provider</b>): <i>john.doe</i></li> <li>▶ User login to the w <b>Service:</b> <i>john.doe</i></li> </ul>

Identity provider	Requirements Identity provider	Requirements Service Engine	User name and login (Examples)
		not allowed in user names.	
<p><b>Keycloak</b></p>	<p>None.</p> <p>The user name is freely definable.</p>	<p>Supported with a <b>IDS Login</b> screen.</p> <p>To work together with apps from the zenon software platform, such as Service Engine for example, the following process is strongly recommended:</p> <ul style="list-style-type: none"> <li>▶ Length of 20 characters maximum. In the text field with the visualization of the logged-in user, user names with more than 20 characters are not displayed. The display for the complete user name is shown without limitation. With functions of the Service Engine service that use the user names (for example: AML, CEL), this entry remains empty.</li> <li>▶ The special characters '@' and '\' are not allowed in user names.</li> </ul>	<ul style="list-style-type: none"> <li>▶ User name (as defined) <i>john.doe</i></li> <li>▶ User login to the <b>Service:</b> <i>john.doe</i></li> </ul>

## 16.2.4.4 Identity Service in Service Engine

You must undertake various configurations both in IIoT Services as well as in Engineering Studio in order to be able to use **Identity Service** for user login.

1. Establish connection to IIoT Services via IIoT Connection Wizard (on page 308).
  - ▶ Note on compatibility:  
For configurations in zenon version 11, the client must still be created manually in Service Configuration Studio (on page 321).
2. Configure user authentication of Service Engine in Engineering Studio (on page 322).

### 16.2.4.4.1 Create client in Service Configuration Studio

As of version 12, the client is created automatically when the **IIoT Services Connection Wizard** (on page 308) is configured in Engineering Studio in **Identity Management**. The wizard automatically assigns the *Service Engine Client* role to the client created.

#### NOTE ON COMPATIBILITY

The following section describes the manual configuration of the client definitions in Service Configuration Studio. The manual client configuration is necessary if you want to connect the configuration in a Engineering Studio in a version <12 with <NAME\_GRID>.



#### Information

If you are working with version 11, you must also configure the connections with the **Service Node Configuration Tool**. You can find further information on this in the Help for the zenon software platform 11.

#### CONFIGURATION IN PREVIOUS VERSIONS

Carry out the following steps to manually configure a corresponding client definition in **Identity Management**.

1. Open the Service Configuration Studio.
2. Go to the **Identity Management** node.
3. Go to the **Clients** menu.
4. Create a client definition for Service Engine. To do so, select the client type **Service Engine**.
5. Configure the options for the new client service:
  - ▶ **Client ID**: freely-defined (e.g. "ServiceEngine-ComputerName")

- ▶ **Client Name:** freely-defined (e.g. "*ServiceEngine-ComputerName*")
  - ▶ **Secret:** Is generated automatically. Make a note of the **Secret** for the following configuration steps.
6. Go to the **Access Control** menu.
  7. Assign the *Service Engine Client* role to the client via a corresponding group assignment.

You have thus created a client definition for Service Engine.

#### 16.2.4.4.2 Special case Keycloak

Additional settings in the **Keycloak** administration interface are necessary to use **Keycloak** as the Identity Provider for Service Engine.

To do this, carry out the following steps:

- ▶ Open the **Keycloak Admin Console**.
- ▶ Go to the **Clients** menu item.
- ▶ Open the Client that you have configured for **Identity Service**.
- ▶ Go to **Settings**.
- ▶ Set the **Direct Access Grants Enabled** property to *ON*.

This setting is only for Keycloak. It is not required for other Identity Providers.

#### 16.2.4.4.3 Configure Identity Service

Here you can configure the connection to the **Identity Service**.

1. Make sure in advance that the computer on which you are doing your configurations in the Engineering Studio has established the corresponding trust (on page 307) with IIoT Services.
2. Configure a connection to the IIoT Services (on page 308).

This way Service Engine can authenticate itself as the client application to **Identity Service**.

#### 16.2.4.4.4 Service Engine user authentication via Identity Service

You can use the following settings to configure Service Engine for user authentication via **Identity Service**.

To do this, carry out the following steps:

1. Highlight the project in the workspace in Engineering Studio.
2. Navigate to the **User Administration** project properties group.

3. Select the *Identity Service* entry in the **Use external users source** property under Property in the drop-down list.
4. Optionally, an external login for the **Identity Service** can be stored in the **Identity Service provider** property with the **Provider Alias** as the default setting.  
**Note:** To do this, an **Identity Provider** (on page 207) (with appropriate **Alias**) must already be configured in **Identity Management** (on page 174). For detailed information, refer to the **Configuring Identity Service** (on page 322) node. If no **Alias** has been configured in Engineering Studio, the integrated (internal) user administration of **Identity Service** will be used automatically.

## 16.2.5 Device Management

In Engineering Studio projects are prepared and transferred with a wizard for Device Management.

### ⚠ Attention

Make sure that the computer on which you are doing your configurations in Engineering Studio has established the corresponding trust (on page 307) with IIoT Services.

Detailed information on this service can be found in the **Device Management** (on page 266) section.

### 16.2.5.1 Generate software package - Engineering Studio Wizard

Software packages are created on the basis of zenon projects in Engineering Studio.

Carry out the following steps to create a software package for **Device Management**:

1. Start <NAME\_ENGINEERING\_STUDO>.
2. In the workspace, activate the project for which you would like to create a software package.  
To do this, select the command **Activate project**. The activated project is displayed in the tree view and marked with the text (**Start project**).
3. Start the **Device Manager Wizard**.
4. To do this, select the **Publish project to Device Management...** menu option in the **Tools** menu bar.  
This launches the **Publish project to Device Management...** wizard.  
**Note:** Please note that starting the wizard can take a short time.
5. Configure the options for the software package.  
You can find detailed information on this in the **Publish project to Device Management** node.

6. Transfer the software package by clicking on the **Publish** button.
7. Login is performed via the **Identity Service**.
8. The software package is transferred to **Device Management**. If the transfer was successful, the package is listed in Service Configuration Studio in the list of packages (on page 280).

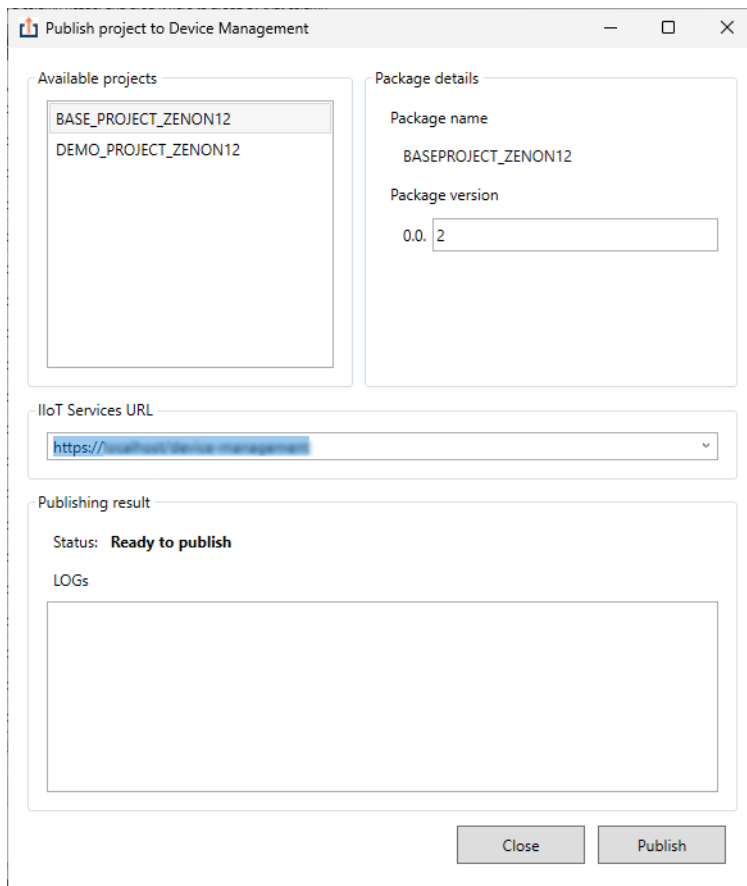
**⚠ Attention**

Make sure that you have generated the Service Engine files before running the wizard. To do this, run either the command **Create all Service Engine files** or generate modified **-Service Engine** files in Engineering Studio before you download a software package for **Device Management**.

### 16.2.5.2 Publish project to Device Management

In this wizard, you configure the software package that you want to transfer to **Device Management**.

This dialog also includes a status bar and an area for LOG messages.





## AVAILABLE PROJECTS

List of all available projects for which a software package can be generated. Selection of the project to be transferred from a list.

**Note:** The list shows the active zenon projects and all projects of the workspace that have been marked with the command **Keep project in memory**.

## PACKAGE DETAILS

Option	Description
<b>Package name</b>	Name of the software package.  The name is the same as the zenon <b>Project name</b> selected and cannot be changed in the wizard.
<b>Package version</b>	Version of the zenon project. The version number is based on the <b>Versioning active</b> project property in Engineering Studio. This must be activated in order to be able to send valid package versions.  You can find detailed information on this in the <b>Project backup</b> node in the <b>Versioning</b> node.
<b>Package comments</b>	Comment field for entry of an optional text. Input in this option field is visualized in <b>Device Management</b> . This comment can optionally be amended in <b>Device Management</b> with the administration of the <b>Packages</b> (on page 280).

## IIOT SERVICES URL

Destination address of the device to which **Device Management** transfers a zenon project as a software package.

The destination address is entered in the input field and must be in the following form:

*https://[URL of IIoT Services]*

**E.g.:** *https://hostname.local*

Connections that have already been configured can be selected again with the drop-down list.

## PUBLISHING RESULT

The status bar visualizes the current execution step or a corresponding status message on the success or failure of creating the software package.

- ▶ *Ready to publish* (font color: black)  
Default text when the wizard is started.
- ▶ *Publishing in progress...* (Font color: black)  
Publishing to **Device Management** is in progress.
- ▶ *Project successfully published.* (Font color: green)  
Software package has been successfully transferred to Device Management.
- ▶ *Publishing failed* (Font color: red)  
.Software package has failed to transfer to Device Management.

## LOGS

This area lists the current steps in publishing a software package. The respective LOG level is prefixed in front of the entry in square brackets [].

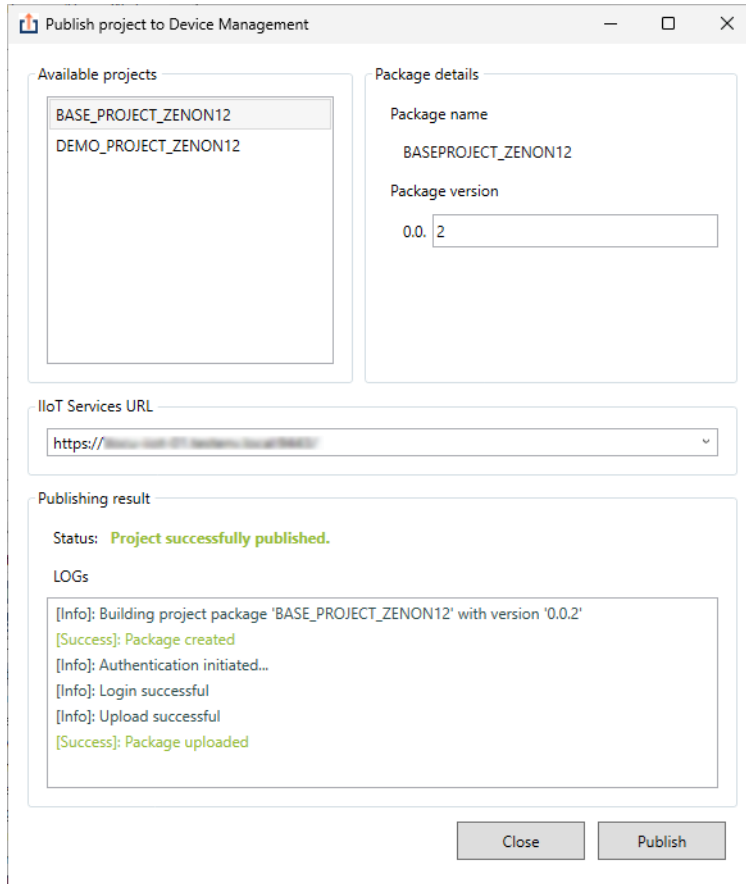
- ▶ **[Info]**: Entries on the execution steps and general information.  
**Example:** *[Info]: Building project package 'NAME' with version '1.0.2'*
- ▶ **[Success]**: Entries for successfully executed steps.  
**Example:** *[Success]: Creating package done*
- ▶ **[Error]**: Error message for one or more execution steps.  
**Example:** *[Error]: There is already a software package with the same name and version existing.*  
*[Error]: Please use a different package version.*

## NAVIGATION

Button	Description
Close	Closes the wizard.
Publish	<p>Creates the software package and transfers it to <b>Device Management</b>.</p> <p><b>Note:</b> You must be logged in to <b>Identity Service</b> for the transfer to be successful. The web browser is opened automatically for this and the <b>Identity Service</b> login page is displayed.</p>

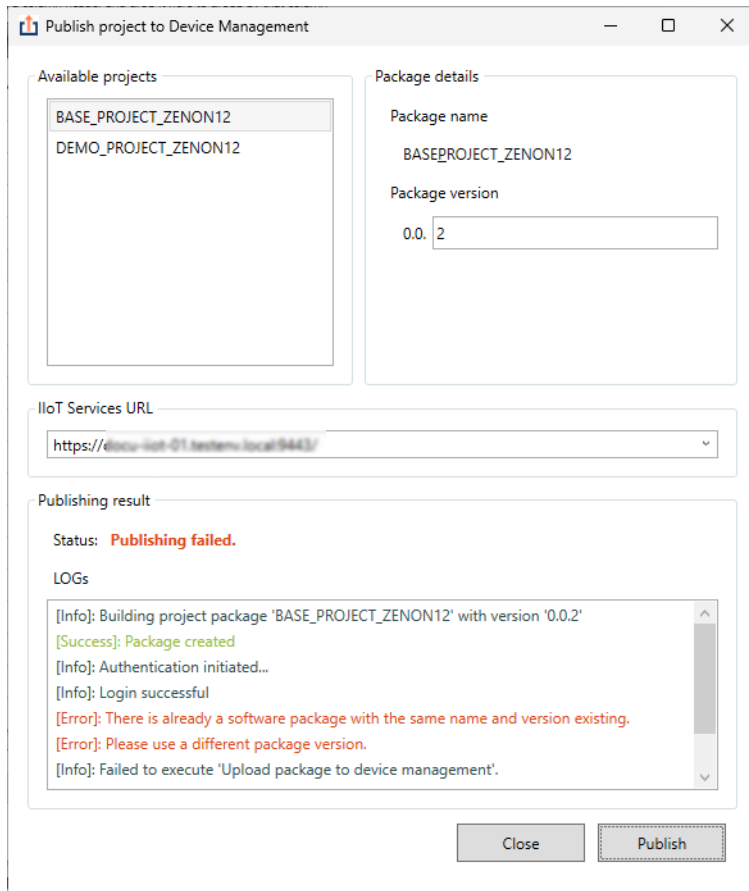
## 16.2.5.2.1 Generate software package - Examples

### EXAMPLE - SOFTWARE PACKAGE HAS BEEN SUCCESSFULLY TRANSFERRED



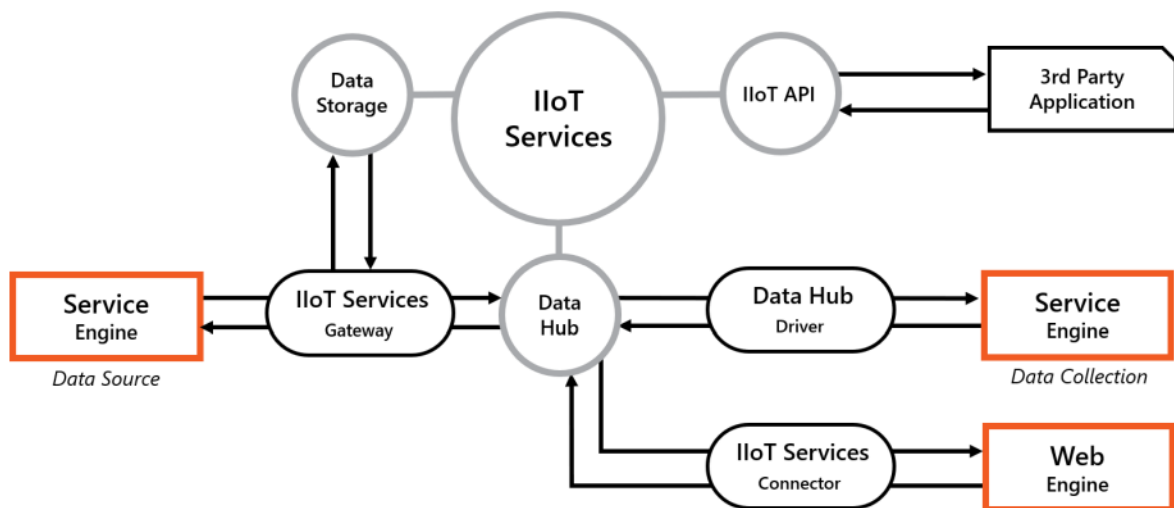
In this example, the software package was created successfully and transferred to Device Management. This software package is listed for Packages detail view.

**EXAMPLE - CREATION OR TRANSFER OF THE SOFTWARE PACKAGE HAS FAILED**



This figure shows a failed creation of the software package. As listed in the LOG entries, the software package already exists on **Device Management** with the configured project version (package version).

**16.3 Data Hub**



Source data of Service Engine can be provided via Data Hub for various destination services.

**Data Hub** allows you to provide data from Service Engine for IloT Services.

The data types supported for source data from Service Engine are:

- ▶ Archive data (historical variable values)
- ▶ Alarms
- ▶ Events
- ▶ Variables

To allow IloT Services to access the various data types, you must set corresponding access permission for variables in Service Engine.

### **Hint:**

#### **System events**

You do not need to configure any special access permission for IloT Services for system events. System events always automatically have read and write permissions for **Data Hub**.

#### **No access to third-party data via Data Hub**

A Service Engine instance can always only enter its own data in **Data Hub**. This also applies if the project aggregates data from several sources (such as in an archive).

### 16.3.1 Connect to Data Hub

Here you can configure the connection to the **Data Hub**.

1. Make sure in advance that the computer on which you are doing your configurations in the Engineering Studio has established the corresponding trust (on page 307) with IloT Services.
2. Configure a connection to the IloT Services (on page 308).

### 16.3.2 Configure variables

In order to use variables in IloT Services, they must be configured for it in Engineering Studio.

Only variables with **simple data type** are suitable for this. Structure variables and root variables of arrays are not available in IloT Services.

### **To configure variables:**

1. Select the desired variable.
2. Open the **Authorization/eSignature** group in the properties.
3. Switch to the **IloT Services settings** subgroup.
4. Configure the variable for use in IloT Services.

### **Configurable properties**

#### **Access permission:**

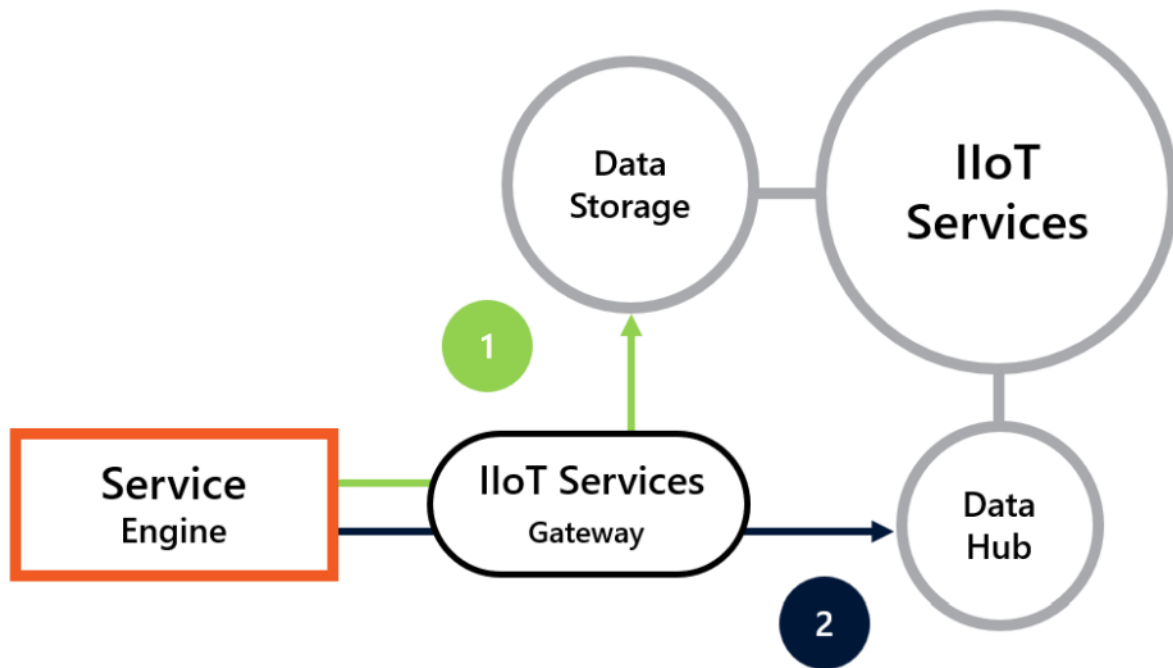
Access right of a variable in IloT Services. Select from drop-down list:

- ▶ *None*: Variable is not available in IloT Services.
- ▶ *Read*: IloT Services has read access to this variable.
- ▶ *Read and write*: IloT Services have read and write access to this variable.  
For reasons of security, access permission should only be set as far as actually necessary for a required data action.

## **16.4 Connectors**

Connectors are used to connect various applications of the zenon software platform with IloT Services.

### 16.4.1 IIoT Services Gateway



The IIoT Services Gateway connects Service Engine with Data Storage (1) and Data Hub (2).

**IIoT Services Gateway** allows you to establish connections between Service Engine and IIoT Services.

#### CONNECTION OPTIONS

Two options are supported for connecting with Service Engine:

- ▶ **Data Hub:** For transferring live data or archive data.
- ▶ **Data Storage:** For transferring archive data.

Each connection option must be configured separately in Engineering Studio.

#### SUPPORTED DATA ACTIONS

For more information about the data actions supported by **IIoT Services Gateway**, see the Possible use cases (on page 17) node.

#### INSTALLATION AND CONFIGURATION

**IIoT Services Gateway** is automatically installed with Service Engine. The **IIoT Services Gateway** must be licensed and configured.

How to license the **IIoT Services Gateway**:

- ▶ If necessary, activate a license for the Service Engine which contains the **IloT Services Gateway**.
- ▶ Enter this license for use.

**IloT Services Gateway** is only shown in the user interface of Engineering Studio after it has been successfully activated.

Enable the Services Gateway as follows:

1. Check beforehand whether the license for **IloT Services Gateway** is valid and active.
2. In project properties, go to the **Network** properties group.
3. Go to the **IloT Services - General** subcategory.
4. Activate the **Execute IloT Services Gateway** checkbox.

**Note:** The checkbox is only shown if **IloT Services Gateway** is correctly licensed.

You have thus activated the **IloT Services Gateway** for this project.

### Tip

A central configuration in the global project with the option to transfer it to the sub-projects is not possible.

## VERSION CHECK

Different versions of IloT Services and **IloT Services Gateway** can communicate with one another on the basis of a common protocol.

For communication, a check is carried out to see which version of the protocol is used by the individual components. The check is successful if all components use the same major version of the protocol. Minor versions can be different. If the major version is different for a component, communication is no longer possible.

### Example:

- ▶ Components with *20.00* can communicate with *20.10*.
- ▶ Components with *20.10* cannot communicate with *30.10*



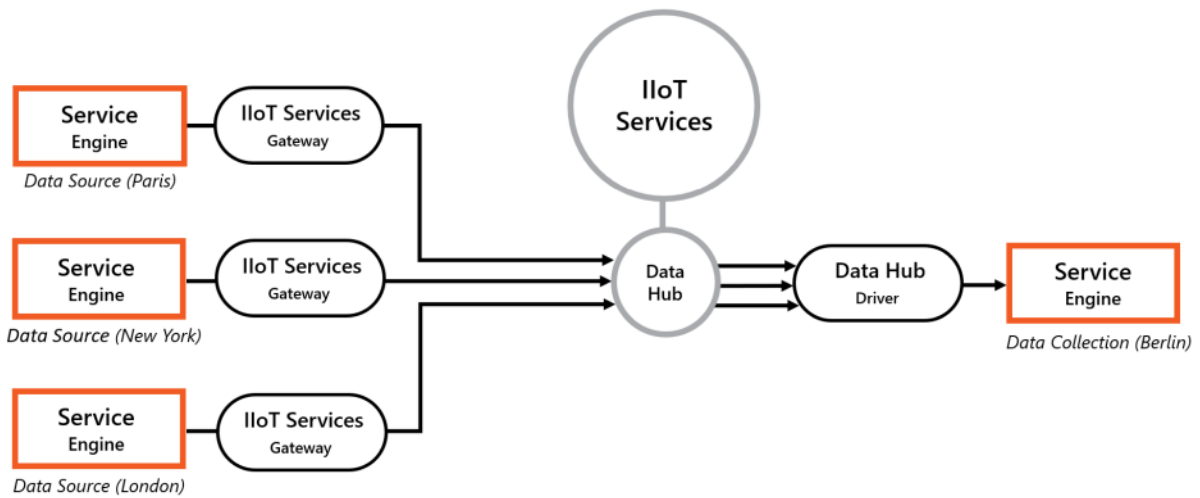
### Information

Valid major version for IloT Services 14: 20

**Note:** For versions of the zenon Software Platform prior to version 14, all components must correspond exactly. This also includes the minor version.



### 16.4.2 Data Hub driver

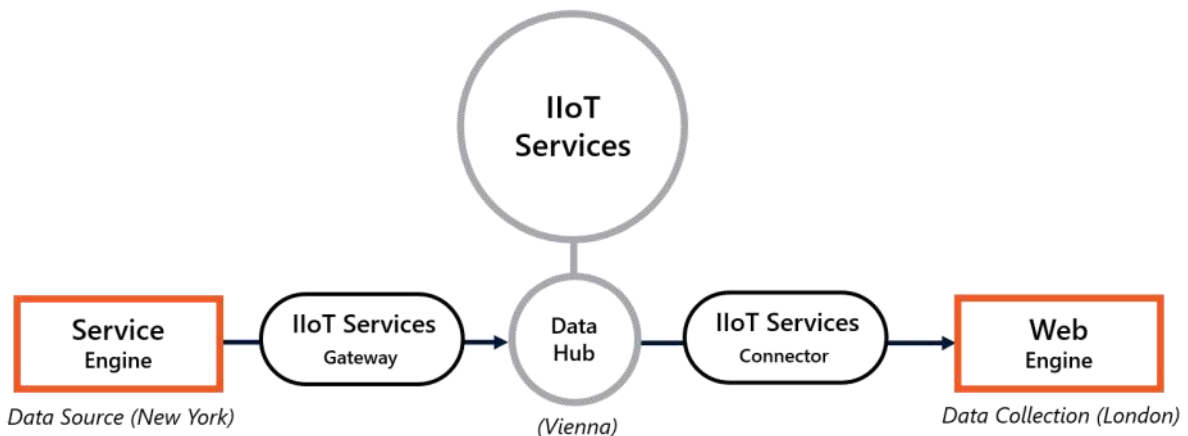


The Data Hub driver transfers source data of multiple Service Engine instances to a central control center.

The Data Hub driver allows you to retrieve data from IloT Services with a Service Engine. The source data is generated by one or more Service Engine instances.

Detailed information about this driver can be found in the **Data Hub driver** node.

### 16.4.3 IloT Services Connector



Service Engine generates process data and then transfers it to IloT Services via Data Hub Gateway. They are transmitted to Web Engine via IloT Services Connector.

IloT Services connector allows you to connect Web Engine with IloT Services.

## INSTALLATION AND CONFIGURATION

IloT Services Connector can be installed together with Web Engine. To do this, the corresponding option in **Web Engine Deployment Tool** must be selected. This configuration is described in the Web Engine documentation.

IloT Services Connector does not have to be licensed separately.

### Info

The connection of the Web Engine to IloT Services via IloT Services connector is supported for zenon 8.20 and higher.

## 16.5 Checklist: Connection between Service Engine and IloT Services

The following is required for a functional connection of Service Engine to IloT Services:

- ▶ For Service Engine, the **IloT Services Connection Wizard** was used to configure a connection to the IloT Services.
- ▶ Your license for Service Engine contains the **IloT Services Gateway** and has been both activated and entered for use.
- ▶ The checkbox for the **Execute IloT Services Gateway** property has been activated.
- ▶ In the project properties, the correct IloT Services instance and installation must be selected.
- ▶ The project is a standalone project or the current Service Engine is the active server for this project in the network.  
The existing connection is closed if another Service Engine takes on the server role during operation.

When the project is reloaded in Service Engine:

- ▶ The connection is closed before reloading.
- ▶ The connection is restarted after reloading.

## 17 Appendices

In this node, you can find further information on IloT Services.

## 17.1 Advanced configurations

You can also, optionally, adjust the IIoT Services by means of advanced configurations. For advanced configuration, edit the corresponding configuration files with a text editor. You only need advanced configuration in a few, very specific usage scenarios.

### Tip

After making changes to configuration files, it is generally a good idea to restart the IIoT Services with all services. You thus ensure that all services work with the current configuration.

### 17.1.1 Installation options

#### **Where you carry out advanced configurations depends on the IIoT Services installation option:**

- ▶ IIoT Services (Docker):  
You can find the file called *docker-compose.yml* in the installation folder. Here you configure all services centrally using corresponding environment variables.
- ▶ IIoT Services (Windows native):  
You can find various *JSON-Dateien* under *%CD\_SYSTEM%\ServiceGrid\*. The JSON file that you have to configure for a particular service is documented in the respective nodes.

You configure the same settings for both installation options in principle. There are however platform-specific differences that are documented in the following nodes.

### Attention

Only configure the documented JSON files! You should not make any changes to JSON files that are not documented.

#### 17.1.1.1 Environment variables (Docker)

In the IIoT Services (Docker) installation version, you edit the *docker-compose.yml* file

In Docker, there is the particular feature that you cannot configure the settings in the container directly. You work with environment variables instead.

**The IIoT Services check whether environment variables are set each time they are started:**

- ▶ Environment variables set:  
The environment variables in *docker-compose.yml* overwrite the corresponding default settings in the Docker containers.
- ▶ No environment variables set:  
Start the IIoT Services with the default settings from the containers.

With self-configured environment variables in *docker-compose.yml*, you ensure that your settings are effective when the services are started.

### 17.1.1.2 JSON (Windows native)

In the IIoT Services (Windows native) installation version, you edit the JSON files of the services for advanced configuration. The IIoT Services load the current respective configuration each time services are restarted.

#### 17.1.1.3 Example: Port change for a service

The ports for all services of the IIoT Services are pre-defined by default. In certain cases – if for example a certain port in a network is already assigned – it can be beneficial to define the port yourself.

##### 17.1.1.3.1 Solution: Configure port change (Docker)

The central port number can be configured in the *.env* file with the **PORT=** entry. If this entry is empty, communication is via port *9443* by default.

If you want to make a change to the port number for the **Proxy Service** (on page 24), save the file with the changed settings and restart all services of the IIoT Services.

##### 17.1.1.3.2 Solution: Configure port change (Windows native)

You configure the port for the **Proxy Service** in the *%CD\_SYSTEM%\ServiceGrid\ProxyService.json* file. If the *ProxyService.json* file is not present on your system, you must create this file yourself.

## RELEVANT SECTIONS IN THE CONFIGURATION FILE

The following sections in the file are relevant:

1. *HostingInformationConfiguration* section  
Here you define the domain names and the port under which the **Proxy Service** is contactable from outside.

## 2. *Kestrel* section

Here you also define the port that the **Proxy Service** will use. The port must be the same as in *HostingInformationConfiguration*

## THE CONFIGURATION IN DETAIL

You must change the port in both sections.

### Code Sample

#### Default configuration (port 9443)

```
{
  "HostingInformationConfiguration": {
    "Uri": "https://[mycomputer.mydomain.com]:9443"
  },
  "Kestrel": {
    "EndPoints": {
      "Https": {
        "Url": "https://*:9443"
      }
    }
  }
}
```

Change both ports from 9443 to 1234.

## Code Sample

### Changed configuration (port 1234)

```
{
  "HostingInformationConfiguration": {
    "Uri": "https://[mycomputer.mydomain.com]:1234"
  },
  "Kestrel": {
    "EndPoints": {
      "Https": {
        "Url": "https://*:1234"
      }
    }
  }
}
```

Save the file with the changed settings and restart all IIoT Services.

**Result:** You have thus changed the port of the **Proxy Service** from *9443* to *1234*. The **Identity Management** is now also available via this port in the Service Configuration Studio.

## 17.1.2 Configurations for individual services

This node contains service-specific configuration details.

### 17.1.2.1 Data Hub

There are no service-specific configurations for the **Data Hub**.

Configurations for the Data Hub are created by default from version 14. Adjustment is possible by means of a configuration file.

- ▶ Save location: *C:\Program Files\Common Files\zenon\DataHub*
- ▶ File name: *CDDataHub.conf*

The respective LOG level can also be adjusted in the *CDDataHub.conf* file. The corresponding entries have the provided configuration file with the corresponding comments.

### 17.1.2.2 Certificate Management

Where you configure **Certificate Management** depends on the installation method of the IIoT Services.

## IIOT SERVICES (DOCKER)

You configure the environment variables in this file:

- ▶ *docker-compose.yml* file (in the installation folder)

Switch to this section in the file:

- ▶ *certificate-management*: section
- ▶ *environment*: subsection

## IIOT SERVICES(WINDOWS NATIVE)

You configure this JSON file:

- ▶ *%CD\_SYSTEM%\ServiceGrid\CertificateManagement.json*

If the file is missing in the installation folder, you must create the *CertificateManagement.json* yourself.

### 17.1.2.2.1 DataHubConfig

You configure the connection between **Certificate Management** and the **Data Hub** here.

Environment variables (Docker)	JSON (Windows native)	Description	Permitted values
<b>CERTIFICATEMANAGEMENT_DataHubConfig__Url=</b> <i>NULL</i>	<i>DataHubConfig</i> ": { "Url": <i>NULL</i> }	The default value is the FQDN of the system. You can optionally also configure a specific URL ( <i>https://myhubcontroller.com</i> for example).	Optional value. Permitted value: Valid URL. Default: <i>NULL</i> (i.e. no URL is defined)
<b>CERTIFICATEMANAGEMENT_DataHubConfig__Port=</b> <i>9411</i>	" <i>DataHubConfig</i> ": { "Port": <i>9411</i> }	You configure the port from the Data Hub here.  The configuration is for the accessibility of the service from external networks.	Mandatory value. Default: <i>9411</i> Permitted values: <i>1 - 65535</i> Recommended ports: <i>1024 - 49151</i>
<b>CERTIFICATEMANAGEMENT</b>	<i>DataHubConfig</i> ":	The default value is	Optional value.

Environment variables (Docker)	JSON (Windows native)	Description	Permitted values
<b>MENT_DataHubConfig__InternalDataHubUrl=</b> <i>localhost</i>	<pre>{   "InternalDataHubUrl": localhost }</pre>	<i>localhost</i> . You can optionally also configure a specific URL ( <i>https://myhubcontroller.com</i> for example).  <b>Note:</b> Bundles for internal IIoT Services, for example IIoT API, get their information from this entry. If this configuration is configured incorrectly, communication with the Data Hub may fail.	Permitted value: Valid URL.  Default: <i>NULL</i> (i.e. no URL is defined)
<b>CERTIFICATEMANAGEMENT_DataHubConfig__InternalDataHubPort=</b> <i>9411</i>	<pre>"DataHubConfig": {   "InternalDataHubPort": 9411 }</pre>	Here you can configure, as an option, the port from the Data Hub for internal communication.  <b>Note:</b> Bundles for internal IIoT Services, for example IIoT API, get their information from this entry. If this configuration is configured incorrectly, communication with the Data Hub may fail.	Mandatory value.  Default: <i>9411</i>  Permitted values: <i>1 - 65535</i>  Recommended ports: <i>1024 - 49151</i>

### 17.1.2.3 Identity Service

Where you configure the **Identity Service** depends on the installation method of the IIoT Services.

#### IIOT SERVICES (DOCKER)

You configure the environment variables in this file:

- ▶ *docker-compose.yml* file (in the installation folder)



**Switch to this section in the file:**

- ▶ *identity-service*: section
- ▶ *environment*: subsection

## IIOT SERVICES (WINDOWS NATIVE)

**You configure this JSON file:**

- ▶ *%CD\_SYSTEM%\ServiceGrid\IdentityService.json*

### 17.1.2.3.1 Radius configuration

Here you can configure the Radius **Identity Provider**.

Environment variables (Docker)	JSON (Windows native)	Description	Permitted values
<b>IDENTITYSERVICE_RadiusConfiguration_AuthenticationTimeoutInMs=3000</b>	<pre>"RadiusConfiguration": {   "AuthenticationTimeoutInMs": 3000 }</pre>	Timeout for requests to the Radius server.  After the timeout expires for the <b>Primary connection</b> , the <b>Identity Service</b> attempts to log in via the configured <b>Fallback connections</b> .	Mandatory value (in milliseconds).  Default: 3000

### 17.1.2.4 Identity Management

There are no service-specific configurations for the **Identity Management**.

### 17.1.2.5 IIoT API

Where you configure the IIoT API depends on the installation method of the IIoT Services.

## IIOT SERVICES (DOCKER)

**You configure environment variables in this file:**

- ▶ *docker-compose.yml* file (in the installation folder)

**Switch to this section in the file:**

- ▶ *iiot-api*: section
- ▶ *environment*: subsection

## IIoT SERVICES (WINDOWS NATIVE)

**You configure this JSON file:**

- ▶ `%CD_SYSTEM%\ServiceGrid\IloTApi.json`

### 17.1.2.5.1 EnableSwaggerDocumentation

You can activate the Swagger documentation here.

The Swagger documentation is used by developers:

- ▶ As a complete interface specification
- ▶ To test certain IIoT Services functions
- ▶ As a reference for self-developed clients

The Swagger documentation is not activated by default.

Environment variables (Docker)	JSON (Windows native)	Description	Permitted values
<b>IIOTAPI_EnableSwaggerDocumentation</b> = <i>true</i>	<code>"EnableSwaggerDocumentation": true</code>	Determines whether the Swagger documentation is available.	Optional value. Permitted values: <ul style="list-style-type: none"> <li>▶ <i>true</i> (activated)</li> <li>▶ <i>false</i> (deactivated)</li> </ul> Default: <i>true</i>

### 17.1.2.5.2 SgIdentityConfiguration

You configure the connection between **IIoT API** and the **Identity Service** here.

Environment variables (Docker)	JSON (Windows native)	Description	Permitted values
<b>IIOTAPI_SgIdentityCon</b>	<code>"SgIdentityConfiguration":</code>	Defines whether	Optional value.

Environment variables (Docker)	JSON (Windows native)	Description	Permitted values
<b>figuration_RequireHttpsMetadata=true</b>	<pre>{   "RequireHttpsMetadata":   true }</pre>	HTTPS is needed for the Discovery Endpoint.	<ul style="list-style-type: none"> <li>▶ <i>true</i> (activated)</li> <li>▶ <i>false</i> (deactivated)</li> </ul> Default value: <i>true</i>

### 17.1.2.5.3 SgApiConfiguration

These settings are relevant for the IIoT API.

Environment variables (Docker)	JSON (Windows native)	Description	Permitted values
<b>IIOTAPI_SgApiConfiguration_VariablesCacheLifetime=300</b>	<pre>"SgApiConfiguration": {   "VariablesCacheLifetime":   300 }</pre>	Time period in seconds of how long variable values are stored in the cache.	<ul style="list-style-type: none"> <li>▶ Minimum: 0</li> <li>▶ Values are not limited in time.</li> <li>▶ Maximum: 2147483647</li> </ul> Default: 300
<b>IIOTAPI_SgApiConfiguration_ReportMaxExecutionTime=1800</b>	<pre>"SgApiConfiguration": {   "ReportMaxExecutionTime":   1800 }</pre>	Time period in seconds of the maximum waiting period for the completion of a report in Report Engine.	<ul style="list-style-type: none"> <li>▶ Minimum: 0</li> <li>▶ Maximum: 2147483647</li> </ul> Default: 1800
<b>IIOTAPI_SgApiConfiguration_ReportCacheLifetime=86400</b>	<pre>"SgApiConfiguration": {   "ReportCacheLifetime":   86400 }</pre>	Time period in seconds of how long the result is available for a report in the IIoT API.  It is discarded once	<ul style="list-style-type: none"> <li>▶ Minimum: 0</li> <li>▶ Maximum: 2147483647</li> </ul> Default: 86400

Environment variables (Docker)	JSON (Windows native)	Description	Permitted values
		the time has run out.	<b>Note:</b> Must be greater than ReportMaxExecutionTime.
<b>IIoTAPI_SgApiConfiguration_SqlElementMaxExecutionTime=1800</b>	<pre>"SgApiConfiguration": {   "SqlElementMaxExecutionTime": 1800 }</pre>	Time period in seconds of the maximum waiting period for the execution of a SQL element.	<ul style="list-style-type: none"> <li>▶ Minimum: 0</li> <li>▶ Maximum: 2147483647</li> </ul> Default: 1800
<b>IIoTAPI_SgApiConfiguration_SqlElementCacheLifetime=86400</b>	<pre>"SgApiConfiguration": {   "SqlElementCacheLifetime": 86400 }</pre>	Time period in seconds of how long the result is available for a SQL call in the IIoT API.  It is discarded once the time has run out.	<ul style="list-style-type: none"> <li>▶ Minimum: 0</li> <li>▶ Maximum: 2147483647</li> </ul> Default: 86400  <b>Note:</b> Must be greater than SqlElementMaxExecutionTime.

### 17.1.3 Configurations for several services (configured centrally)

Where you configure the settings for several services depends on the installation method of the IIoT Services.

#### IIOT SERVICES (DOCKER)

**You configure these settings as environment variables in this file:**

- ▶ .env file (in the installation directory)

#### IIOT SERVICES(WINDOWS NATIVE)

**You configure this JSON file:**

- ▶ %CD\_SYSTEM%/ServiceGrid/common.json

### 17.1.3.1 Incorporating your own database

By default, the IIoT Services create a database as a Persistence Service and configure this database automatically. In this case, no further configuration is necessary.

You can, optionally, install your own MongoDB database and incorporate it into IIoT Services as a Persistence Service. You must configure this connection manually.

Environment variables (Docker)	JSON (Windows native)	Description	Sample values
<b>Persistence_Uri</b> = <i>mongodb://mycomputer.mydomain:27017</i>	<i>"SGSystemConfiguration"</i> { <i>"DatabaseUri":</i> <i>"mongodb://mycomputer.mydomain.com:27017"</i> }	The URL for the Persistence Service.  <b>Note:</b> The Persistence Service is based on a MongoDB.	Mandatory value.  Permitted values: Valid URL.  Example value: <i>mongodb://[mycomputer.mydomain.com]:27017</i>
<b>Persistence_Username</b> = <i>Admin</i>	<i>"SGSystemConfiguration"</i> { <i>"AdminUser": "Admin"</i> }	User name for the Persistence Service. Required if authentication via user name and password is activated.	Mandatory value.  Permitted values: Desired strings (in accordance with MongoDB specification)  Example value: <i>mdb_user</i>
<b>Persistence_Password</b> =	<i>"SGSystemConfiguration"</i> { <i>"AdminUserPassword":</i> <i>"mdb_Changeme123!"</i> }	The password for the administrator.  Required if authentication via user name and password is activated.	Mandatory value.  Permitted values: Must correspond to the password guidelines for IIoT Services.  Example value: <i>mdb_Changeme123!</i>

## 17.1.4 Configurations for several services (configured decentrally)

There are different settings in the IIoT Services, which you have to configure in several services at the same time.

### STATE GENERIC PREFIX

Because the settings documented in this node are not service-specific, we will use, for example, the generic placeholder `<SERVICE_PREFIX>_` for the service-specific prefix (`IIOTAPI_`, for example) in the environment variables.

For each setting in this node, we document the services for which it is relevant. You can then look up the specific information such as the **service prefix** (Docker) and the correct **JSON file** (Windows native) for the respective service.

### LOOK UP SPECIFIC PREFIX

**You can find the required specific information for the respective service here:**

- ▶ Data Hub (on page 338)
- ▶ IIoT API (on page 341)
- ▶ Certificate Management (on page 338)
- ▶ Identity Service (on page 340)

With this information, you can easily create the specific configuration values for each service.

#### 17.1.4.1 Kestrel

Kestrel is the standard web server for projects based on the ASP.NET core.

**These settings are relevant for the following services:**

- ▶ IIoT API
- ▶ Certificate Management
- ▶ Identity Service
- ▶ Identity Management

### GENERAL CONFIGURATION

**You can find the configuration of Kestrel at Microsoft:**

- ▶ <https://docs.microsoft.com/en-us/aspnet/core/fundamentals/servers/kestrel>  
(<https://docs.microsoft.com/en-us/aspnet/core/fundamentals/servers/kestrel>)

## SPECIFIC CONFIGURATION FOR IIOT SERVICES

### You can look up the relevant configurations for the IIoT Services here:

- ▶ Port changes for services (internal and web interface) (on page 336)

### 17.1.5 Adjustments when changing the host name

If a change is made to the host name of the computer on which IIoT Services are installed, the following adjustments must be made manually. These modifications must be carried out for both Windows operating systems as well as Docker installations.

1. Docker installations only:  
Changing the host name in the .env file.
2. Restart IIoT Services services.
3. Log in to the **Platform Configuration** with a IIoT Services administrator account.  
**Note:** A certificate warning might be displayed in the web browser because the host name of the certificate no longer matches with the new host name. If this is the case, the certificate warning must be ignored temporarily in order to access the Service Configuration Studio web interface.
4. Recreate the HTTPS certificate in the **Platform Configuration**.
5. Recreate the certificate bundles for IIoT Services services.
6. Restart IIoT Services services.
7. Renew all service connections (certificate bundles) for all connected zenon services.  
Update the project configurations of all connected zenon services as well, such as Service Engine, Engineering Studio or Report Engine.
8. Modify the configured IIoT Services URLs for the **Identity Service** and the **Data Storage** in the configuration of a Engineering Studio project or in Report Engine.  
You can find this configuration, for example, in Engineering Studio in the **Network active** project properties group under the **Identity Service** properties.  
**Background:** When changing the URL, it may be necessary to create a new **Client Secret** in the **Identity Management**. When configuring a new URL, the existing **Client Secret** will be deleted in the input field of the respective option. If the previous **Secret** is no longer known, a new **Client Secret** must be generated. This new **Secret** must be modified accordingly in the existing project configurations.  
If the previously used **Client Secret** is to be used again for the configuration of a new URL, these changes are unnecessary.

- When using applications from third-party providers:  
Adjustment of the IIoT Services URLs for Identity Service, Data Storage and IIoT API for all applications that connect to the IIoT Services.

## 17.2 IIoT API: Query historic variables

To query archive data from Service Engine via the IIoT API:

- Create an archive in the zenon project.
- Add variables. These variables must be released for the IIoT Services.
- Open the Swagger API documentation of the IIoT API and authenticate yourself.
- To retrieve a list of available archives and their variables, use the following endpoint:  
*/api/v1/datasources/{dataSourceId}/archives*
- To retrieve historic variable values, use this endpoint:  
*/api/v1/datasources/{dataSourceId}/archives/{archiveId}/query*
- Specify the desired **Datasource ID (Projekt-ID)**, archive ID, time filter and variable filter.
- Execute the query and check the result.

You have thus carried out the query.

## 17.3 Docker commands

This node provides you with an overview of Docker commands.

Action	PowerShell command
List all running containers	<code>docker ps</code>
List all containers, including the ones already stopped	<code>docker ps -a</code>
Stop a particular container	<code>docker stop &lt;container-name or container ID&gt;</code>
Stop all running Docker containers*	<code>docker stop \$(docker ps -aq)</code>
Start a stopped container	<code>docker start &lt;container-name or container ID&gt;</code>
Remove a particular container	<code>docker rm &lt;container-name or container ID&gt;</code>
Remove all containers*	<code>docker rm \$(docker ps -aq)</code>
List all volumes	<code>docker volume ls</code>
Remove a particular volume	<code>docker volume rm &lt;volume-name&gt;</code>



Action	PowerShell command
Remove all used volumes*	<code>docker volume rm \$(docker volume ls -q)</code>
List all images	<code>docker image ls</code>
Remove a particular image	<code>docker image rm &lt;image-name or image ID&gt;</code>
Remove all Docker images (containers must be stopped)*	<code>docker image rm \$(docker image ls -q)</code>
<p>With this command, you can reset the entire system.*</p> <p><b>It removes:</b></p> <ul style="list-style-type: none"> <li>▶ all stopped containers</li> <li>▶ all networks that are not used by at least one container</li> <li>▶ all <b>Dangling Images</b></li> <li>▶ the build cache</li> </ul>	<code>docker system prune --all --volumes</code>

\* Commands only for test environments: **Remove** applies to all containers, volumes and images on the computer.

### 17.3.1 Completely delete installation

Sometimes it's a good idea on a test system to completely remove an existing IIoT Services installation and start from scratch.

**To delete a IIoT Services installation:**

1. Stop all running Docker containers with the following command:  
`docker stop $(docker ps -aq)`
2. Remove all running Docker containers with the following command:  
`docker rm $(docker ps -aq)`
3. Remove all volumes with the following command:  
`docker volume rm $(docker volume ls -q)`
4. Remove all Docker images with the following command:  
`docker image rm $(docker image ls -q)`

**To check whether the IIoT Services installation has been deleted:**

1. List all containers (including the stopped ones):  
`docker ps -a`

2. List all volumes:  
`docker volume ls`
3. List all container images:  
`docker image ls`

In all cases, an empty list should be displayed as the output.

### **Attention**

These commands remove all Docker containers and images on the computer. Therefore, they are not suitable for productive systems.

## 17.4 IIoT Services - Diagnosis and LOG messages

LOGs can be used to analyze the behavior of services of the IIoT Services and localize any problems.

The IIoT Services log the following events by default:

- ▶ Standard results (such as the successful start of a service).
- ▶ Error messages (such as a failure to establish a connection).
- ▶ Additional LOG modules for IIoT Services and Linux.
- ▶ LOG messages are sent to the **Diagnosis Server**.

### 17.4.1 IIoT Services (Windows native)

#### IIOT SERVICES (WINDOWS NATIVE)

You can retrieve LOGs for the zenon services in IIoT Services via the GUI using the **Diagnosis Viewer**. LOGs for external services of IIoT Services, such as the Persistence Service, cannot be retrieved using the **Diagnosis Viewer**.

You can find further information on the **Diagnosis Viewer** in the Help in the **Diagnosis Viewer** section.

### 17.4.2 IIoT Services (Docker)

#### IIOT SERVICES (DOCKER)

The following possibilities are available for the LOGs under Docker:

1. **Diagnosis Viewer:**  
LOG messages can be analyzed using the zenon Diagnosis Server.
2. Analysis via Docker logs  
Under Docker, you can retrieve LOGs for all services of the IIoT Services.  
Carry out the following command to call up LOG messages for a service:  
*docker logs <containername>*

**Note:** Replace the placeholder "**<containername>**" with the name of the service.

### 17.4.3 IIoT Services (Docker on Windows)

#### IIOT SERVICES (DOCKER ON WINDOWS)

You can also query the logs using the Docker Dashboard. Clicking on the container opens a properties window with the logs.

### 17.4.4 Activation of zenon logging for Docker

#### ACTIVATION OF ZENON LOGGING FOR DOCKER

zenon logging for Docker installations is not contactable from outside by default. Carry out the following steps to enable connections to the **zenon Logging Server**.

1. Stop the logging service. To do this, carry out the following Docker command in the Docker folder of IIoT Services (c:\iiot-services):  
*docker compose stop zenon-logging-server*
2. Restart the logging service with the port for the zenon Diagnosis Server enabled. To do this, carry out the following command:

```
docker compose -f docker-compose.yml -f docker-compose.expose-logging.yml up  
zenon-logging-server -d
```

**Note:** the port enabling is defined in the *docker-compose.expose-logging.yml* file.

3. Then open the connection to the LOG server in Docker in the Diagnosis Viewer.  
**Note:** In order to be able to establish the connection to the logging server in the Docker environment, the local logging service (**zenLogSrv**) must first be stopped on the computer. This is necessary because both LOG servers use the same port number.
4. Once you have finished your analysis, close the logging service in the Docker environment. To do this, execute the following command:  
*docker compose stop zenon-logging-server*

- Restart the Diagnosis Server in the Docker environment without the port enabled. To do this, execute the following command:

```
docker compose -f docker-compose.yml up zenon-logging-server -d
```

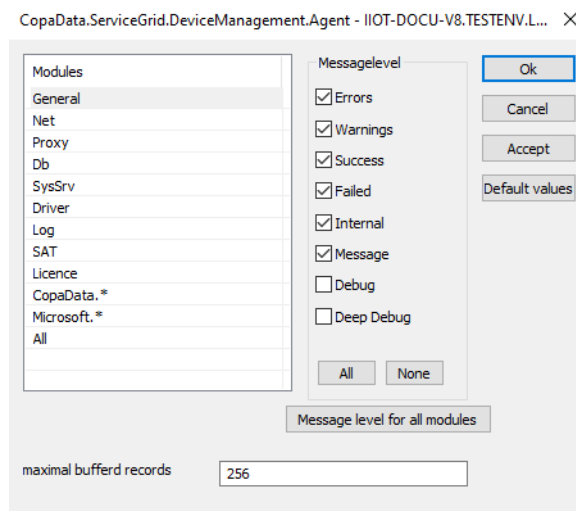
**Note:** If necessary, restart the logging service (**zenLogSrv**) on the local computer that is running the **Diagnosis Viewer**.

**⚠ Attention**

For security reasons, it is recommended that port enabling for the zenon logging server in Docker is only activated temporarily for the duration of the analysis.

### 17.4.5 Additional modules in the Diagnosis Viewer

Services of the IIoT Services have additional entries for module configuration in the **Diagnosis Viewer**.



#### ADDITIONAL LOG MODULES

In general, all zenon components have the same logging modules. However, IIoT Services uses a different technology from that of the zenon **Diagnosis Server**. For IIoT Services, the modules are configured on the basis of namespaces. As a result, the IIoT Services have additional modules that enable more detailed configuration of the Messagelevels.

The logging for IIoT Services uses the following, additional modules.

Module entry	Description
<b>CopaData*</b>	All zenon internal IIoT Services logging modules write their entries to this module.
<b>Microsoft*</b>	If, for example, Microsoft frameworks are used in one of

Module entry	Description
	the IIoT Services, they write your entries to this module.

### MESSAGE LEVEL - MAPPING

All protocol levels that are “higher” than the minimum level are activated automatically in the process.

**Example:** If, in the **Diagnosis Viewer**, only *Messages* have been activated, the levels *Warning* and *Failed* are also active.

zenon message LOG level	IIoT Services LOG level
Errors	Error
Warning	Warning
Success	Not mapped
Failed	Not mapped
Internal	Not mapped
Message	Information
Debug	Debug
Deep Debug	Trace

## 17.5 Troubleshooting

In this node, you can find information on troubleshooting in IIoT Services.

### 17.5.1 Checklist: Verify basic configuration

If you work through this list, you can localize and rectify the most common configuration errors for the IIoT Services.

#### USER NAMES: MAXIMUM LENGTH FOR SERVICE ENGINE

You can also use user names from the **Identity Service** for logging in to Service Engine. However, this also means that the effective length of the user name is no more than 20 characters. This is a limitation of Service Engine.

How you calculate the effective length of a user name (on page 316) is documented separately.

## HOSTNAME: CONTINUOUS LOWERCASE LETTERS

Upper-case letters in host names lead to authentication problems in the IIoT Services. Hostnames must **always** be written with continuous lowercase letters. This is also required if the hostname actually happens to contain uppercase letters.

Please refer to the following table with examples:

Actual hostname	Correct way of writing for the IIoT Services
<i>MyComputer.mydomain.com</i>	<i>mycomputer.mydomain.com</i>
<i>MYCOMPUTER.mydomain.com</i>	<i>mycomputer.mydomain.com</i>
<i>mycomputer.mydomain.com</i>	<i>mycomputer.mydomain.com</i>

If you accidentally entered the host name in upper-case letters when setting up IIoT Services (Docker), you must do the following:

- ▶ Remove the incorrect installation completely (on page 349)
- ▶ Reinstall the IIoT Services (Docker) with the correct host name.

A host name written entirely in lower-case letters is required for proper functioning of the IIoT Services.

## CHECK MINIMUM PASSWORD REQUIREMENTS

Unsuitable passwords lead to authentication problems with the IIoT Services. Only use suitable passwords that meet the minimum password requirements for IIoT Services.

## RESTART SERVICES

If changes to the configuration are made in the IIoT Services, it may be necessary to restart individual services. By restarting all services of the IIoT Services (on page 37), you ensure in all cases that all services can access the current configuration.

After restarting, check all services to see if all relevant services are in the status *Running*. This is a basic requirement for operation of the IIoT Services.

## CONNECTION STATUS IN CERTIFICATE MANAGEMENT

In the web interface of **Certificate Management**, check the connection status to the individual services.

These services must, as a minimum, be in connected state:

- ▶ **Certificate Management**
- ▶ **IIoT API**

**Note:** Due to reconfigurations or expired certificates, it is possible that there are several certificate entries for one service type. In this case, all you need is one certificate entry per service type in the *statusconnected*.

Depending on the application scenario, the following connections may also be required:

- ▶ **Engineering Studio**
- ▶ **Service Engine**
- ▶ **Report Engine**

## CHECK LOG MESSAGES

The LOG messages (on page 350) provide extensive information that can be useful for troubleshooting for the IIoT Services.

## CHECK CONNECTION TO SERVICE ENGINE

### The following requirements must be met:

- ▶ The Service Engine must be configured for IIoT Services. Use the **IIoT Services Connection Wizard** for this.
- ▶ Service Engine must be started.
- ▶ The Service Engine license must include the **Data Hub Gateway**. The license must be activated.
- ▶ Service Engine must be connected to **Certificate Management** (see connection overview (on page 107)).

You can check the status of this connection in **Certificate Management**. If this connection is not provided, you can view the LOGs for Service Engine using the **Diagnosis Viewer**. Here you can get information on establishing connections.

## 17.5.2 Docker

### DATA LOSS DURING UPDATE

In general, an update of Docker does not affect an existing IIoT Services installation. In a few cases, however, data loss can occur during the update.

**Hint:** Before updating the Docker version, back up the Persistence Instance of your IIoT Services installation. That way, even if your Docker update fails, you can still restore the Persistence Instance.

## DATA LOSS DURING SUBSEQUENT CHANGE TO WSL2 (DOCKER ON WINDOWS)

**Docker Desktop for Windows** offers the choice between *Hyper-V* and *WSL2* to execute Docker containers.

The subsequent change from *Hyper-V* to *WSL2* leads to a complete loss of existing IIoT Services installations. You must then reinitialize and set up the IIoT Services.

### **Hint**

When installing **Docker Desktop for Windows**, select the *WSL2* option.

- ▶ **Settings\General\Use the WSL2 based engine**

Only install the IIoT Services afterwards.

## 17.5.3 HSTS problems during new installation

When the digital certificates of the services change due to a complete new installation of the IIoT Services, this can lead to problems. The web browser will not direct you to the website, nor will there be a certificate warning.

This behavior is caused by a browser function called **HSTS (HTTP Strict Transport Security)**.

Carry out the following steps to rectify the problem:

1. Open the **Certificate Management** in Service Configuration Studio:  
*https://[mycomputer.mydomain.com]:9443*
2. Download the **CA Certificate**.
3. Install the **CA Certificate**.
4. Restart the browser.

After restarting the browser, you should be able to access IIoT Services web pages via FQDN again (for example: *https://[mycomputer.mydomain.com]:9443*).

## 17.5.4 Identity Service

The **Identity Service** is the central authentication service of IIoT Services. The problems described below relate to the **Identity Service**.



## ERROR MESSAGE: "UNAUTHORIZED CLIENT"

Clients can authenticate themselves using the **Identity Service**. With correct configuration, the clients can then use the IloT API. The error message "*unauthorized client*" indicates that the client configuration in the **Identity Service** does not match the configuration in the client application.

Solution: Compare the client configuration in the **Identity Service** with the configuration in the client application.

### Check in particular:

- ▶ **Client-ID**
- ▶ **Redirect-URL**
- ▶ **Allowed Scopes**
- ▶ **Grant types**
- ▶ **Secret**

Important: The **Identity Service** also checks the case of the configured URLs. This must match with the URL entered.

## FORGOT PASSWORD. NO LONGER POSSIBLE TO LOG IN

### In the case of a forgotten password, a difference has to be made between different user roles:

1. A user has forgotten their password and can no longer log in to the **Identity Service**.  
**Solution:** Contact the user with the **Identity Administrator** user role. This user can reset the password for each user separately in the **Identity Management**.
2. The user with the *Identity Administrator* user role has forgotten their password. They cannot log in to the **Identity Service** or the **Identity Management**.

Solution: Contact zenon Support. Support can help you reset the user database.

### **Attention**

#### **Reset the user database**

If you reset the user database, configurations for users, groups, clients and **Identity Provider** will be lost, for instance. After resetting the user database, you must reconfigure the IloT Services to a large extent.

## 17.5.5 IloT API: Error codes

In the event of a failed attempt to access the IloT API, one of the following error codes will be output.

### HTTP ERROR CODE 400

- ▶ Cause: Incorrect request of client application.
- ▶ Solution: Check whether the request is formulated correctly and meets the expected data model.

### HTTP ERROR CODE 402

- ▶ Cause: The IIoT API does not have a valid license.
- ▶ Solution: Install a valid license. After installation, the license must be activated. It might be necessary to restart the IIoT Services.

### HTTP ERROR CODE 403

- ▶ Cause: The **User** or **Client** does not have the necessary access permissions.
- ▶ Solution: Configure the access permissions for the **User** or **Client** in the **Identity Management**.

### HTTP ERROR CODE 500

- ▶ Cause: The IIoT API had an internal error while processing a request. This error occurs repeatedly.
- ▶ Solution: Restart the IIoT API service. If the error still continues to occur, contact zenon Support.

### ERROR CONNECTING [...] NO SUCH DEVICE OR ADDRESS

When using the Swagger API documentation, it can happen that the authorization of the user or the client to the IIoT API does not work because the address of the **Identity Service** cannot be resolved.

#### **The error message is displayed in the authorization dialog as follows:**

*Error connecting to*

*https://[mycomputer.myddomain.com]:9443/identity-service/.well-known/openid-configuration: No such device or address*

This error can even occur if the naming resolution generally works and, for instance, if the Service Configuration Studio is displayed.

#### **There are several reasons why the name resolution can fail in this special context.**

- ▶ The host name has been entered incorrectly in the **MACHINE\_HOSTNAME** variable in the .env file. For example, if you used capital letters in this variable, this can lead to authorization problems when using the IIoT API.

**Solution:** Change the hostname in the .env file so that only lower case letters are used for

the entire hostname. Then restart the IIoT Services and reload the website of the IIoT API. Authorize again.

- ▶ The firewall blocks the correct resolution of computer names. To check this, copy the URL specified in the error message and try to open the URL in the browser.

**Solution:** Check the configuration of your firewall.

You can find further information on error codes and their reasons in the Swagger API documentation.

### 17.5.6 Windows hibernation: Different timestamps (Docker on Windows)

Using the **Hibernate** energy-saving option on your computer can lead to problems. The authentication to the Identity Service can fail if the computer is awoken from hibernation mode. This problem occurs when the internal time of Docker after hibernation mode is no longer synchronized automatically with the time of the computer. This results in different timestamps.

Solution: A complete restart of Docker fixes the problem. It is not enough to just restart the services.