User Manual

dataFEED Secure Integration Server

EN-dataFEED Secure Integration Server1.30

Disclaimer

The information contained in these instructions corresponds to the technical status at the time of printing of it and is passed on with the best of our knowledge. The information in these instructions is in no event a basis for warranty claims or contractual agreements concerning the described products, and may especially not be deemed as warranty concerning the quality and durability pursuant to Sec. 443 German Civil Code. We reserve the right to make any alterations or improvements to these instructions without prior notice. The actual design of products may deviate from the information contained in the instructions if technical alterations and product improvements so require. It may not, in part or in its entirety, be reproduced, copied, or transferred into electronic media.

Softing Industrial Automation GmbH

Richard-Reitzner-Allee 6
85540 Haar / Germany
https://data-intelligence.softing.com

☎ + 49 89 4 56 56-0
info.idi@softing.com
support.automation@softing.com
✉ https://data-intelligence.softing.com/support/

The latest version of this manual is available in the Softing download area at:
http://industrial.softing.com/en/downloads.html

Table of Contents

1 Introduction

This manual is the complete reference to the configuration, management and operation of the dataFEED Secure Integration Server version 1.30, and includes detailed descriptions of the configuration and management operations.

1.1 About dataFEED Secure Integration Server

dataFEED Secure Integration Server is a highly secured OPC UA aggregation solution supporting a wide variety of configuration options.

1.2 About this manual

This User Manual explains the usage of dataFEED Secure Integration Server and shall emphasize on the configuration.

Read this manual before starting. For damages due to improper operation Softing Industrial Automation GmbH refuses any liability according to our existing guarantee obligations.

1.3 Disclaimer

The information contained in these instructions corresponds to the technical status at the time of printing of it and is passed on with the best of our knowledge. The information in these instructions is in no event a basis for warranty claims or contractual agreements concerning the described products, and may especially not be deemed as warranty concerning the quality and durability pursuant to Sec. 443 German Civil Code. We reserve the right to make any alterations or improvements to these instructions without prior notice. The actual design of products may deviate from the information contained in the instructions if technical alterations and product improvements so require. It may not, in part or in its entirety, be reproduced, copied, or transferred into electronic media.

1.4 Typographic conventions

The following typographic conventions are used throughout Softing Industrial Automation GmbH customer documentation:

Keys, buttons, menu items, commands and other elements involving user interaction are set in bold font and menu sequences are separated by an arrow	Open **Start** -> **Control Panel** -> **Programs**
Buttons from the user interface are enclosed in brackets and set to bold typeface	Press **[Start**] to start the application Press **[Users**] main navigation entry
Symbolic entries or button images in the user interface shall be presented to allow easy identification	Press ⬇ to start an address space
Filenames and directories are written in italic	Device description files are located in *C:\<Application name>\delivery\software\Device Description files*

CAUTION

CAUTION indicates a potentially hazardous or misleading situation which, if not avoided, may result in data loss or unintended system behaviour.

Note

This symbol is used to call attention to notable information that should be followed during installation, use, or servicing of this device.

2 General Information

2.1 Supported Operating Systems

dataFEED Secure Integration Server 1.30 supported operating systems are listed in the table below. It is strongly advised to have the system up to date before proceeding to install dataFEED Secure Integration Server 1.30.

Operating system	Type
Windows 7	64 bit
Windows 8	64 bit
Windows 8.1	64 bit
Windows Embedded 8.1 Industry	64 bit
Windows 10	64 bit
Windows Server 2012	64 bit
Windows Server 2012 R2	64 bit
Windows Server 2016	64 bit
Windows 10 IoT Enterprise	64 bit
Windows Server 2019	64 bit

Table: Supported Operating Systems

Note

For Windows installations, in some special situations (eg: older, not updated Windows versions) , the Microsoft Universal C Runtime installation will silently fail. The issue is identified when the dataFEED Secure Integration Server 1.30 fails at launch with the following error:

The program can't start because api-ms-win-crt-runtime-l1-1-0.dll is missing from your computer. Try reinstalling the program to fix this problem.

To fix the issue an update outlined in KB2999226 (Update for Universal C Runtime in Windows) is provided by Microsoft.

2.2 Hardware Requirements

Minimum requirements:

Processor	Intel Pentium (minimum 2 cores)
Memory	4 GB
Hard disk	120 GB
Operating System	see Supported operating systems 9
Web Browser (*)	Chrome 60, Firefox 50, Internet Explorer 11

Table: Hardware Requirements

(*) used to access the configuration web based interface

3 Installation

Detailed installation instruction shall guide you through the installation process. Please refer to this information 12 whenever needed.

Upgrade information

dataFEED Secure Integration Server upgrades shall be applied gradually (eg: v1.00 to v1.01) or else uninstall the existing version and install a newer one.

Installed (From)	Upgrade (To)	Upgrade notes:
V1.01.0	V1.02.0	Upgrade not supported.
V1.02.0	V1.10.0	Upgrade supported. Existing V1.02.0 configuration is preserved and re-used by the newly installed V1.10.0 Known Issues: • Address space filters from v1.02 are preserved. Inherited filters modifications are not recommended due to the new filter features introduced (service based filtering, automatic browse path filter creation), instead a filters re-creation with the new changes is recommended.

Upgrade best practice

Before accessing the newly upgraded *dataFEED Secure Integration Server* configuration web page it is strongly advised to either reload the configuration page (***CTRL + F5*** or ***SHIFT + F5*** are supported by most web browsers) or to delete the web browser cached data.

3.1 Setup

dataFEED Secure Integration Server is delivered as an automatic installation setup on all Windows based operating systems. Please ensure that the operating system version and features match the operating system requirements 9.

On Windows operating systems dataFEED Secure Integration Server is delivered as a set of services:

Service Name	Details
dataFEEDSISsvc	the main service providing all the runtime and configuration backend functionality
dataFEEDSIS_nginx	an nginx web server service instance used to provide access to the dataFEED Secure Integration Server web based configuration interface

Table: Installation, Setup Components

3.1.1 Delivered Features

Following applications are delivered as part of the dataFEED Secure Integration Server installation:

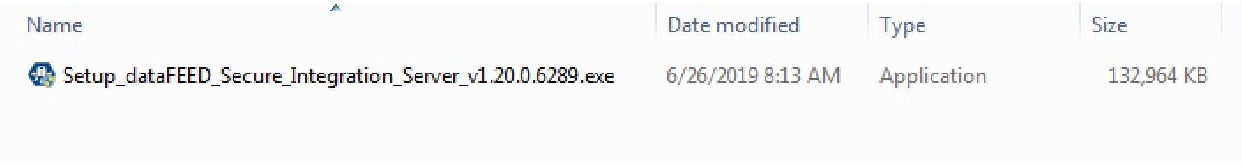
Feature	**Version**	**Details**
dataFEED Secure Integration Server	1.30	dataFEED Secure Integration Server OpcUa aggregation solution main deliverables
dataFEED OPC UA Client	1.47.0.7600	Softing Industrial Automation GmbH's generic OpcUa client
dataFEED OPC UA Demo Server	1.47.0.7600	Softing Industrial Automation GmbH's generic OpcUa server

Table: Installation, Setup , Delivered Features

3.1.2 Guided Installation

1. Start installation

Double click on the provided executable file named **Setup_dataFEED_Secure_Integration_Server_v**1.10.0.5634**.exe**. Please note that the red colour highlighted part **1.20.0.6289** might differ from the provided example.

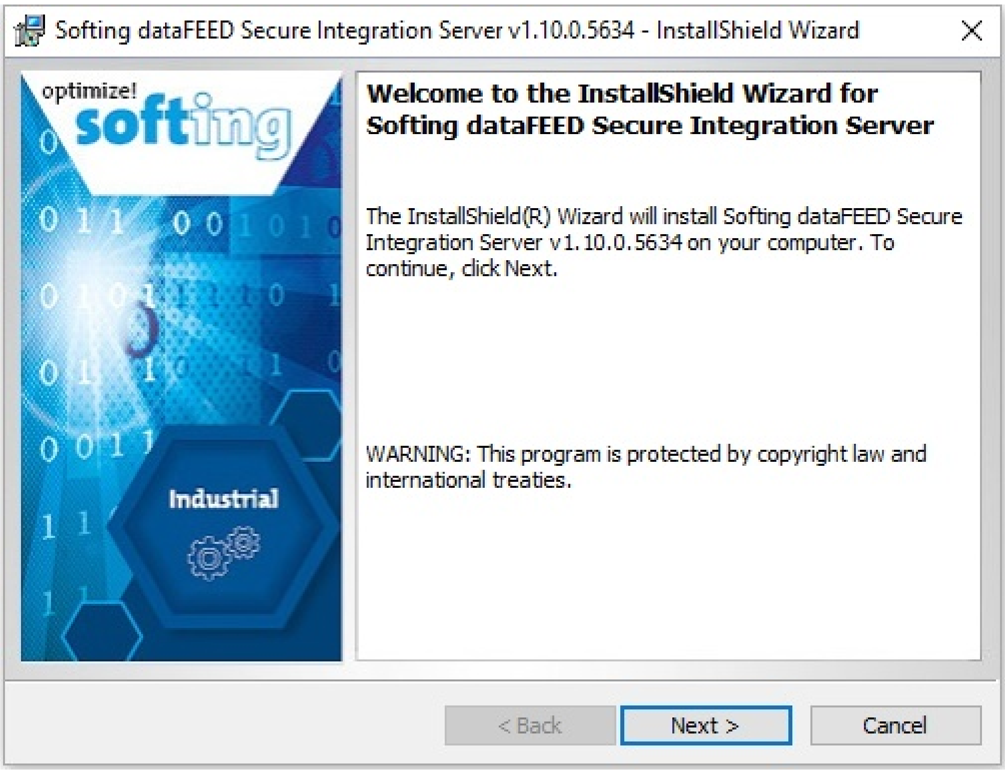


Name	Date modified	Type	Size
Setup_dataFEED_Secure_Integration_Server_v1.20.0.6289.exe	6/26/2019 8:13 AM	Application	132,964 KB

Figure: Installation, Setup Installer

2. Welcome screen

The first interaction with the installation setup is the welcome screen, please select next to continue the installation.


Softing dataFEED Secure Integration Server v1.10.0.5634 - InstallShield Wizard

Welcome to the InstallShield Wizard for Softing dataFEED Secure Integration Server

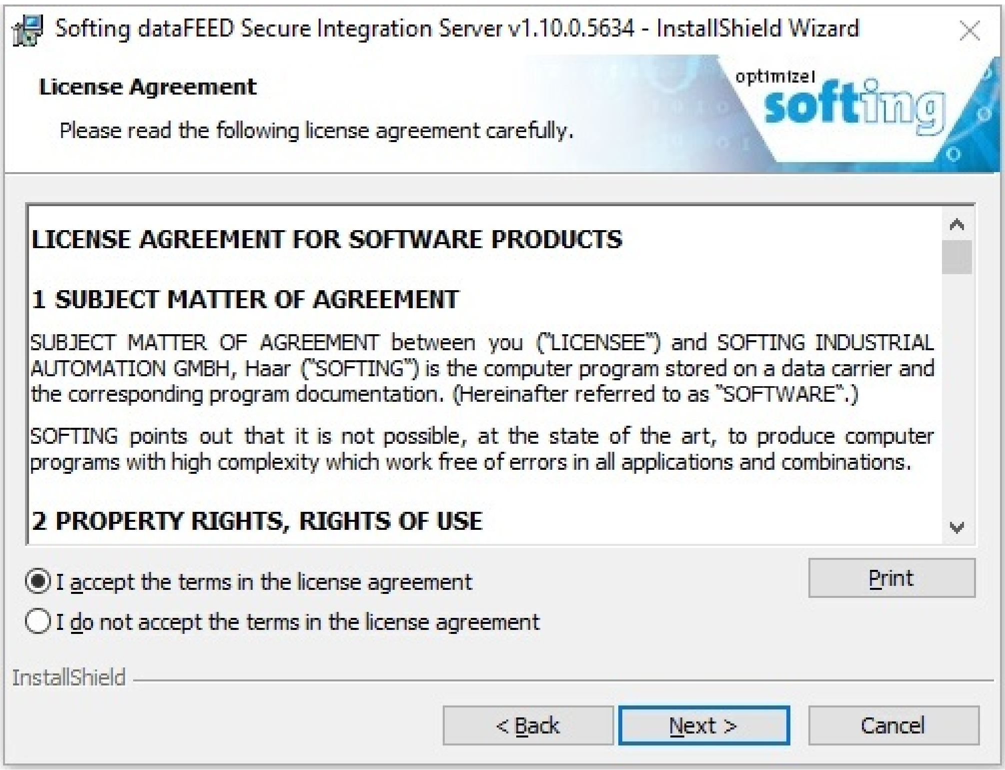
The InstallShield(R) Wizard will install Softing dataFEED Secure Integration Server v1.10.0.5634 on your computer. To continue, click Next.

WARNING: This program is protected by copyright law and international treaties.

Figure: Installation, Setup Welcome Screen

3. License agreement

In order to continue the installation it is mandatory to read the presented license agreement and accept it by selecting the radio button labeled [**I accept the terms in the license agreement]** then select **[Next]**.



Softing dataFEED Secure Integration Server v1.10.0.5634 - InstallShield Wizard

License Agreement

Please read the following license agreement carefully.

LICENSE AGREEMENT FOR SOFTWARE PRODUCTS

1 SUBJECT MATTER OF AGREEMENT

SUBJECT MATTER OF AGREEMENT between you ("LICENSEE") and SOFTING INDUSTRIAL AUTOMATION GMBH, Haar ("SOFTING") is the computer program stored on a data carrier and the corresponding program documentation. (Hereinafter referred to as "SOFTWARE".)

SOFTING points out that it is not possible, at the state of the art, to produce computer programs with high complexity which work free of errors in all applications and combinations.

2 PROPERTY RIGHTS, RIGHTS OF USE

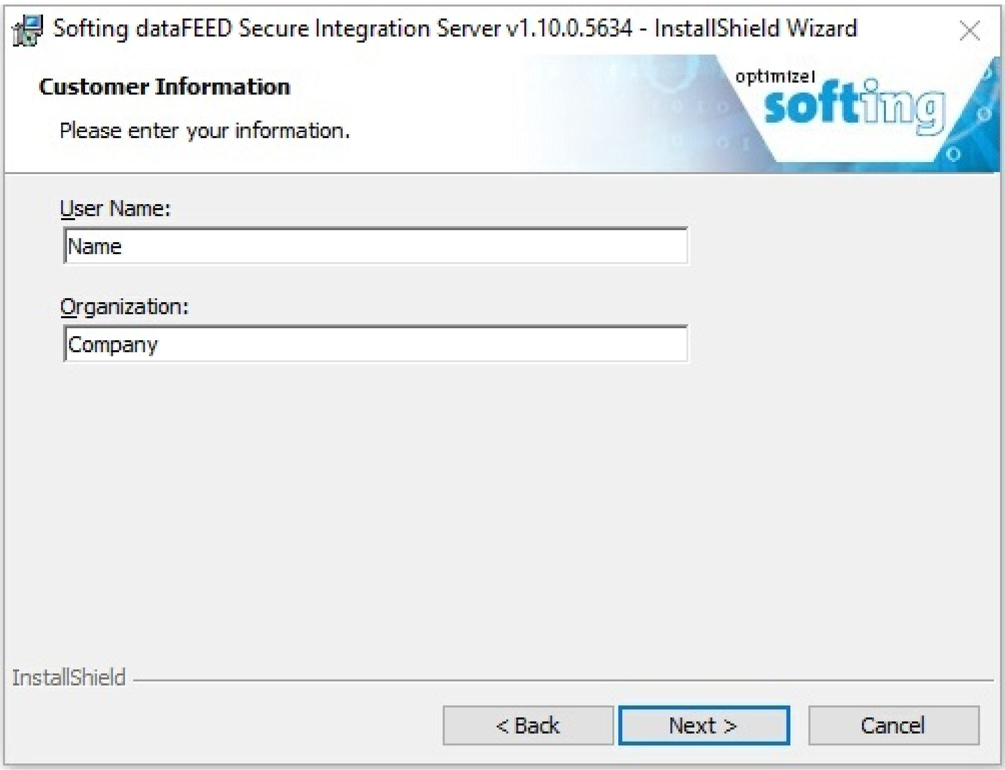
● I accept the terms in the license agreement

○ I do not accept the terms in the license agreement

Figure: Installation, Setup License Agreement

4. Customer Information

Third step requires the customer information to be filled in. After making sure the information is correct please select next.



Softing dataFEED Secure Integration Server v1.10.0.5634 - InstallShield Wizard

Customer Information

Please enter your information.

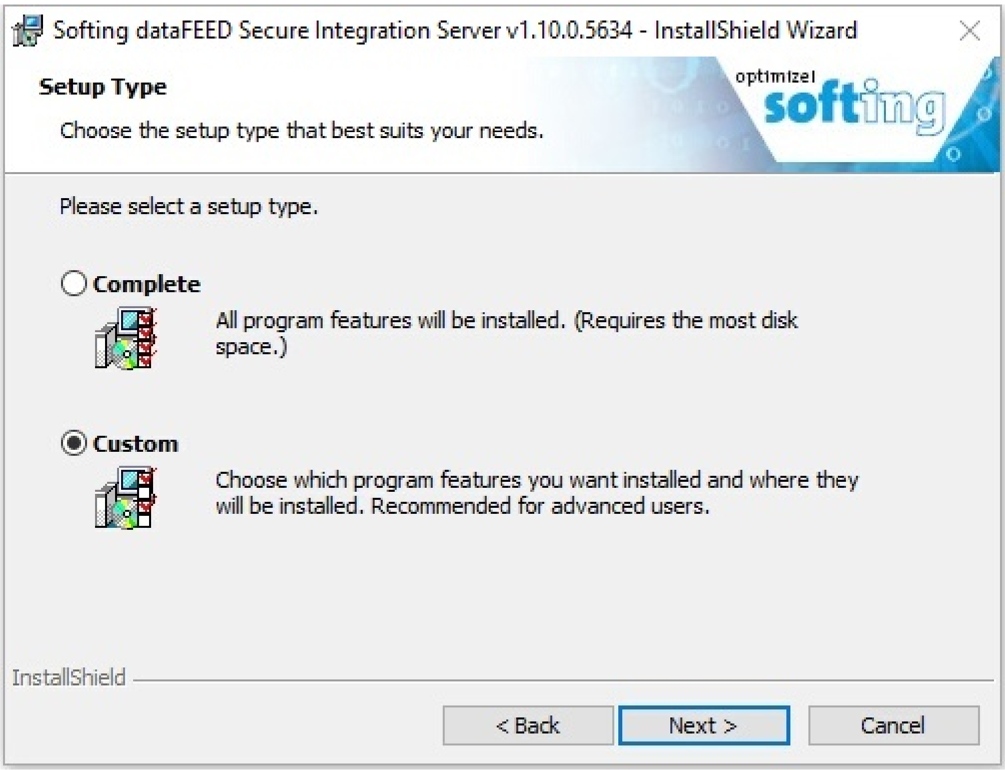
User Name: Name

Organization: Company

Figure: Installation, Setup Customer Information

5. Setup Type

Selecting a complete setup will speed up the configuration process and will install all the additional tools required for dataFEED Secure Integration Server to run. In order to provide further details on the installation of additional tools the guided setup information shall continue with a custom setup selection.



Softing dataFEED Secure Integration Server v1.10.0.5634 - InstallShield Wizard

Setup Type

Choose the setup type that best suits your needs.

Please select a setup type.

○ **Complete**

All program features will be installed. (Requires the most disk space.)

● **Custom**

Choose which program features you want installed and where they will be installed. Recommended for advanced users.

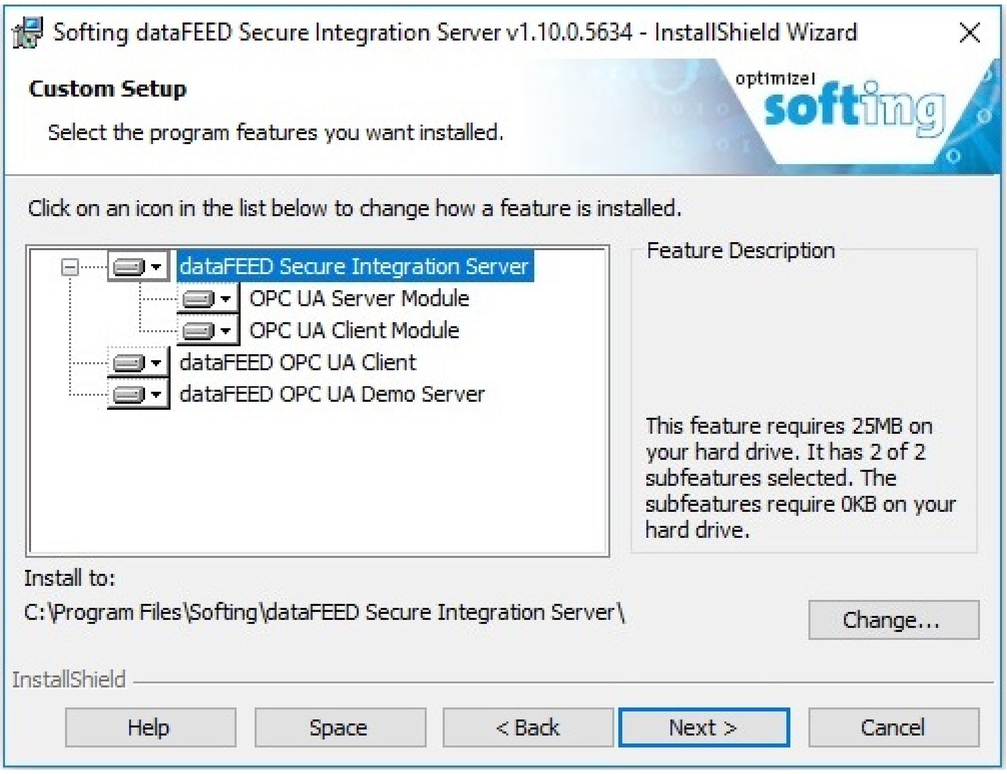
Figure: Installation, Setup Choose Type

6. Custom setup

Installation paths and delivered features can be changed in the custom setup installation step. Please refer to the delivered features 12 for details. When all changes are in place select next to continue.

Correct operation of the dataFEED Secure Integration Server requires installation of both its component modules:

- **OPC UA Server Module**
- **OPC UA Client Module**


Softing dataFEED Secure Integration Server v1.10.0.5634 - InstallShield Wizard

Custom Setup

Select the program features you want installed.

Click on an icon in the list below to change how a feature is installed.

- dataFEED Secure Integration Server
  - OPC UA Server Module
  - OPC UA Client Module
- dataFEED OPC UA Client
- dataFEED OPC UA Demo Server

Feature Description

This feature requires 25MB on your hard drive. It has 2 of 2 subfeatures selected. The subfeatures require 0KB on your hard drive.

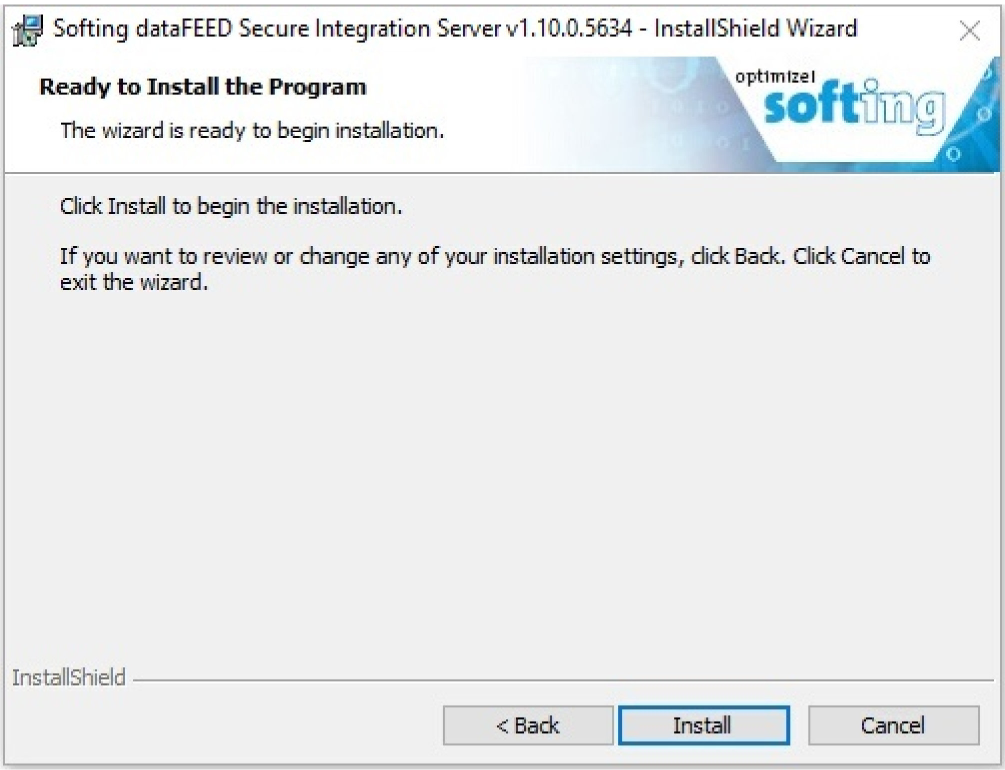
Install to:

C:\Program Files\Softing\dataFEED Secure Integration Server\

Figure: Installation, Setup Customization

7. Ready to install

Press **[Install]** to start the installation process. During the installation a progress bar shall provide feedback about the installation status.


Softing dataFEED Secure Integration Server v1.10.0.5634 - InstallShield Wizard

Ready to Install the Program

The wizard is ready to begin installation.

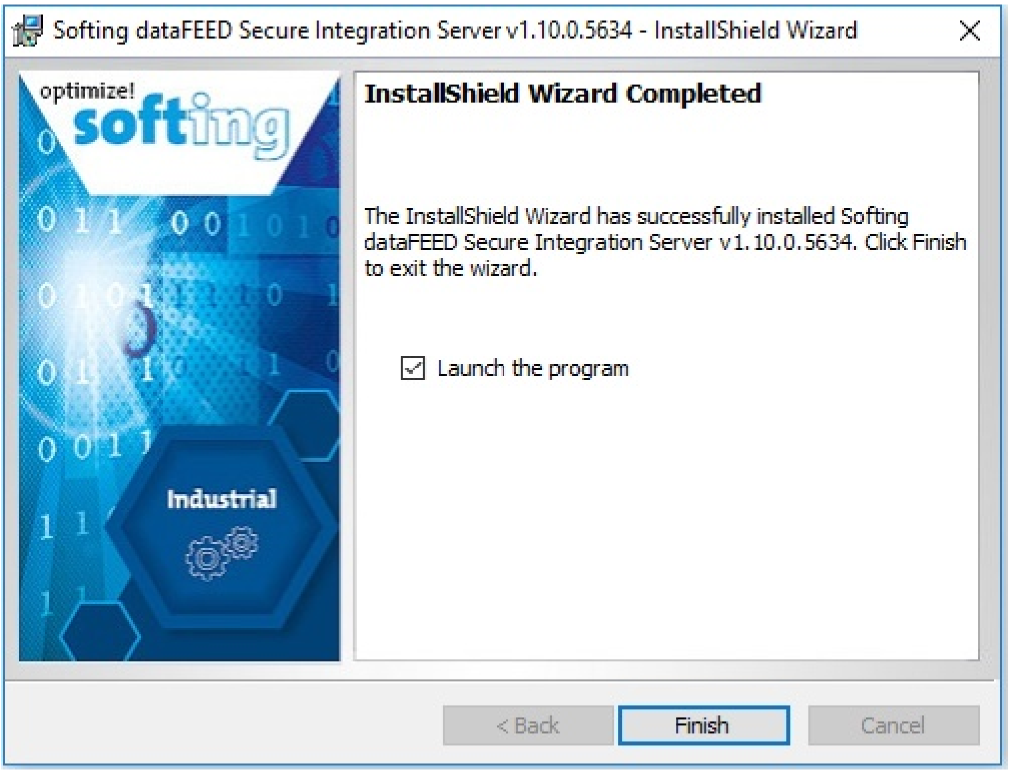
Click Install to begin the installation.

If you want to review or change any of your installation settings, click Back. Click Cancel to exit the wizard.

Figure: Installation, Proceed With Setup Installation

8. Finalizing installation

Last installation step requires the approval to start the dataFEED Secure Integration Server delivered services. The services were already registered; not choosing to start them at this step would require a manual start later. For details on manual actions refer to service starting and stopping chapter 18.



Softing dataFEED Secure Integration Server v1.10.0.5634 - InstallShield Wizard

InstallShield Wizard Completed

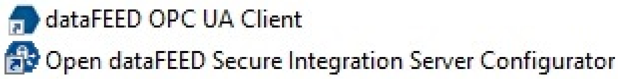
The InstallShield Wizard has successfully installed Softing dataFEED Secure Integration Server v1.10.0.5634. Click Finish to exit the wizard.

☑ Launch the program

Figure: Installation, Finalize Setup Installation

9. Start menu entries and shortcuts

After installation, the following shortcuts shall be accessible on the desktop:



dataFEED OPC UA Client

Open dataFEED Secure Integration Server Configurator

Shortcut	Details
dataFEED OPC UA Client	Shortcut to the delivered Softing dataFEED OPC UA Client
Open dataFEED Secure Integration Server Configurator	Shortcut to dataFEED Secure Integration Server configuration web interface. **Note:** Shall open with the default web browser, ensure it is supported 10.

Tabel: Installation, Finalize Setup Installation

3.1.3 Starting and Stopping

During installation, the dataFEED Secure Integration Server is being deployed as a set of Windows services which are automatically started 17 by default after the installation setup. In order to manually change the state of the services a few guided steps must be followed:

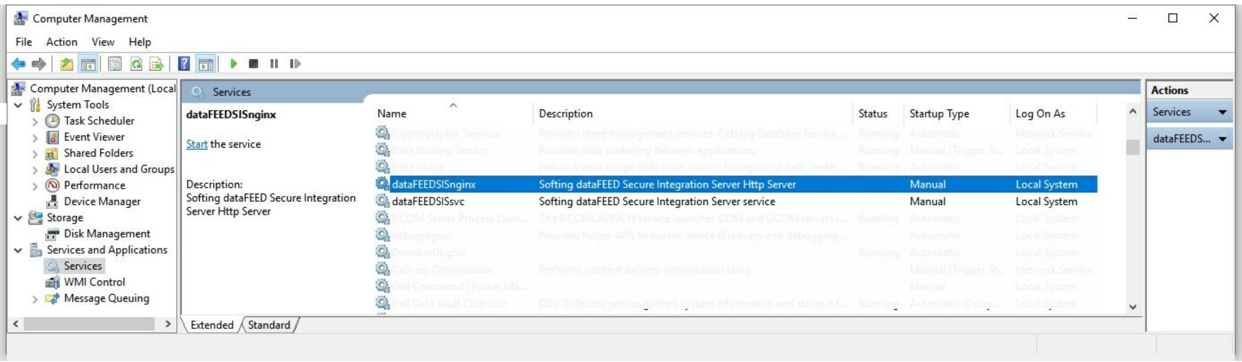
1. Query Services

In order to operate the services, either start or stop them, one has to ensure the services were properly registered during installation. There are two possibilities to achieve this:

1.1. Windows Computer Management

Open **Computer Management** and navigate to **Computer Management -> Services and Applications -> Services.** On the right side view all the system's services are listed. Order by name and search for **dataFEEDSISsvc** and **dataFEEDSISnginx**. Detailed information about the service state and start-up type are visible by checking:

- **Status** column informing about the service's current state (possible states: RUNNING, PAUSED or STOPPED if empty)
- **Startup Type** column indicates the service start-up type (possible types: Automatic, Manual or Disabled)



dataFEEDSISnginx

Start the service

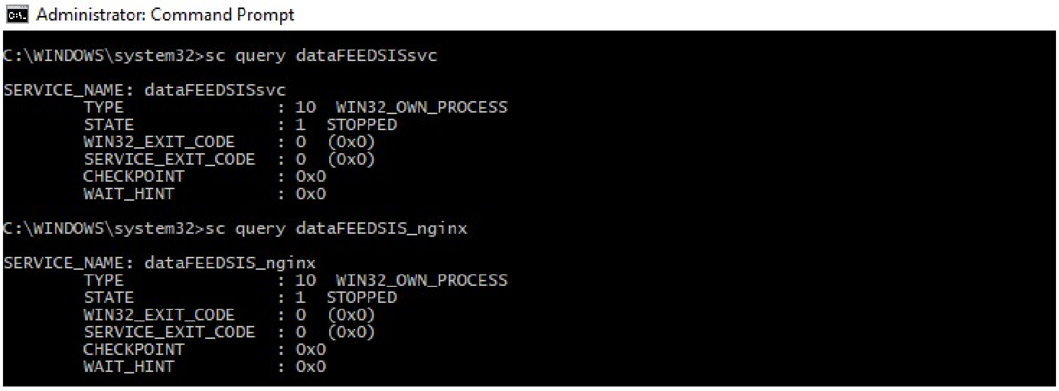
Description:
Softing dataFEED Secure Integration Server Http Server

Name	Description	Status	Startup Type	Log On As
Cryptographic Services	Provides three management services: Catalog Database Service,...	Running	Automatic	Network Service
Data Sharing Service	Provides data brokering between applications.	Running	Manual (Trigger St...	Local System
Data Usage	Network data usage, data limit, restrict background data, meter...	Running	Automatic	Local Service
dataFEEDSISnginx	Softing dataFEED Secure Integration Server Http Server		Manual	Local System
dataFEEDSISsvc	Softing dataFEED Secure Integration Server service		Manual	Local System
DCOM Server Process Laun...	The DCOMLAUNCH service launches COM and DCOM servers i...	Running	Automatic	Local System
debugregsvc	Provides helper APIs to enable device discovery and debugging...		Automatic	Local System
DeleakerDbgSrv		Running	Automatic	Local System
Delivery Optimization	Performs content delivery optimization tasks		Manual (Trigger St...	Network Service
Dell Command | Power Ma...			Manual	Local System
Dell Data Vault Collector	DDV Collector service gathers system information and stores it f...	Running	Automatic (Delay...	Local System

Figure: Installation, Setup, Start Services

1.2. Command Line.

Open a command prompt with administrative rights and issue the following commands: **sc query dataFEEDSISsvc** and ***sc query dataFEEDSIS_nginx***. When the services are not started the displayed **STATE** property will have the value **1 STOPPED.**



```
C:\WINDOWS\system32>sc query dataFEEDSISsvc

SERVICE_NAME: dataFEEDSISsvc
        TYPE               : 10  WIN32_OWN_PROCESS
        STATE              : 1  STOPPED
        WIN32_EXIT_CODE    : 0  (0x0)
        SERVICE_EXIT_CODE  : 0  (0x0)
        CHECKPOINT         : 0x0
        WAIT_HINT          : 0x0

C:\WINDOWS\system32>sc query dataFEEDSIS_nginx

SERVICE_NAME: dataFEEDSIS_nginx
        TYPE               : 10  WIN32_OWN_PROCESS
        STATE              : 1  STOPPED
        WIN32_EXIT_CODE    : 0  (0x0)
        SERVICE_EXIT_CODE  : 0  (0x0)
        CHECKPOINT         : 0x0
        WAIT_HINT          : 0x0
```

Figure: Installation, Setup, Start Services, Query Services From Command Prompt

2. Start Services

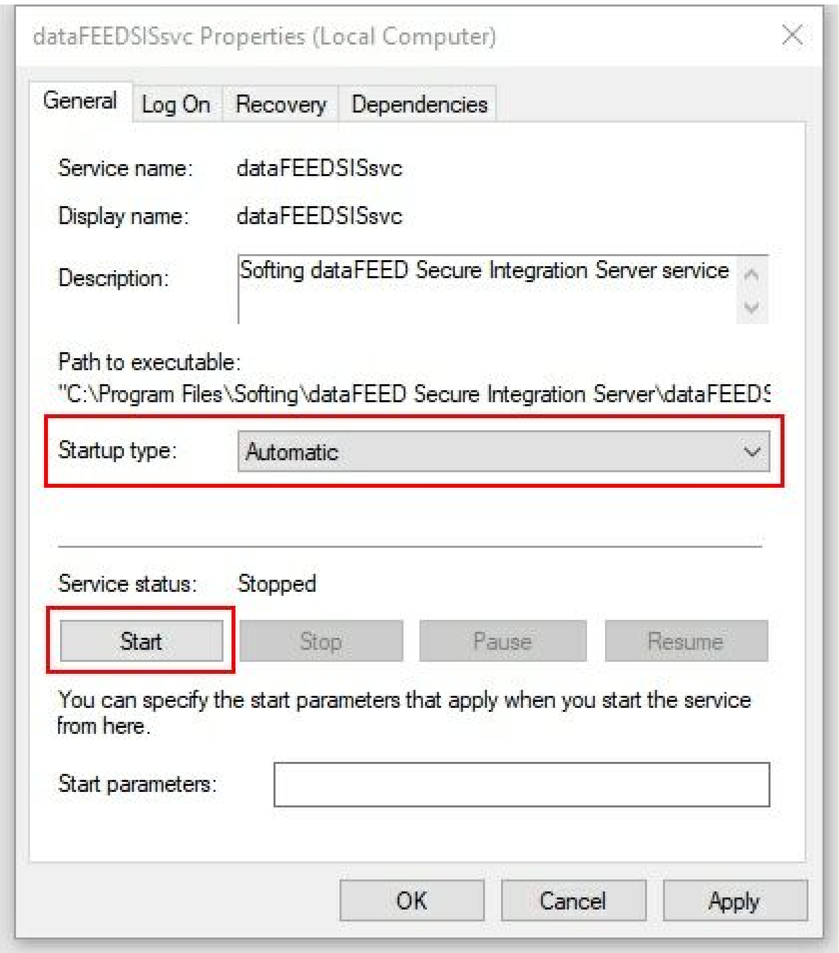
When the services were correctly deployed and registered, but were not started during the installation, use one of the following approaches to start them:

2.1. Windows Computer Management.

Open **Computer Management** and navigate to **Computer Management -> Services and Applications -> Services**. On the right side view all the system's services are listed. Order by name and search for **dataFEEDSISsvc** and **dataFEEDSISnginx**.

For each service proceed as follows:

- Double click on the service entry to open the service properties window
- Click the **[Start]** button on the properties window to start the service
- Change the Startup type from **Manual** to **Automatic** to automatically start the service at system start-up.



dataFEEDSISsvc Properties (Local Computer)

Service name: dataFEEDSISsvc

Display name: dataFEEDSISsvc

Description: Softing dataFEED Secure Integration Server service

Path to executable:
"C:\Program Files\Softing\dataFEED Secure Integration Server\dataFEEDS

Startup type: Automatic

Service status: Stopped

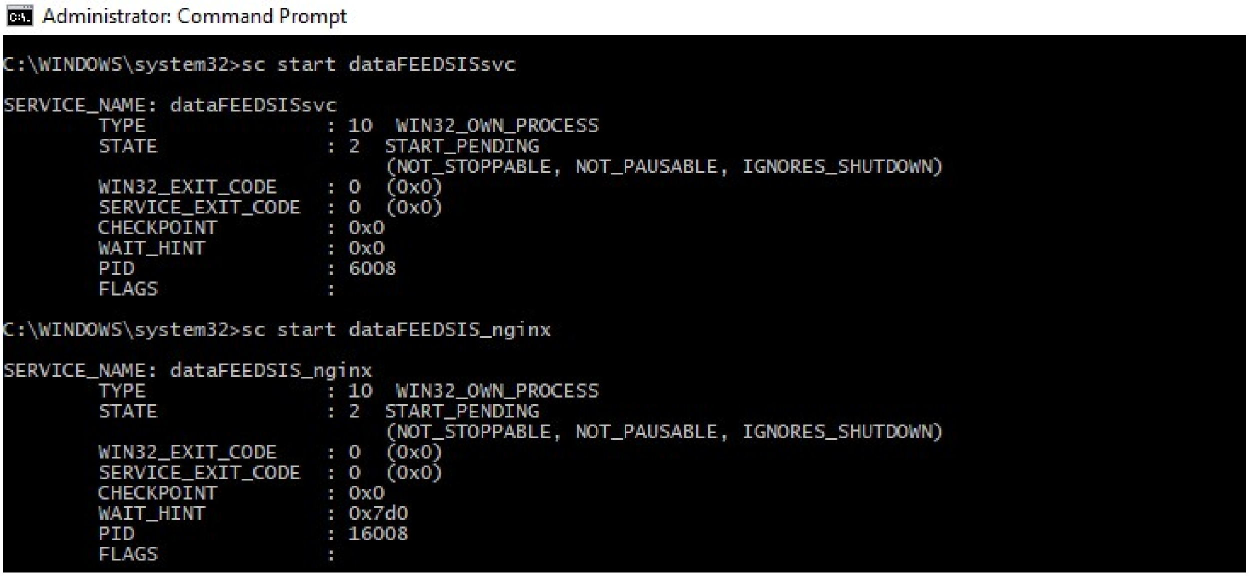
You can specify the start parameters that apply when you start the service from here.

Start parameters:

Figure: Installation, Setup, Start Services, Service Properties

2.2. Command Line.

Open a command prompt with administrative rights and issue the following commands: **sc start dataFEEDSISsvc** and **sc start dataFEEDSIS_nginx**. The services shall change their **STATE** value to **2 START_PENDING.** When the services startup process was finalized querying them again, as described in the previous step, shall show the **STATE** new value as **4 RUNNING**.



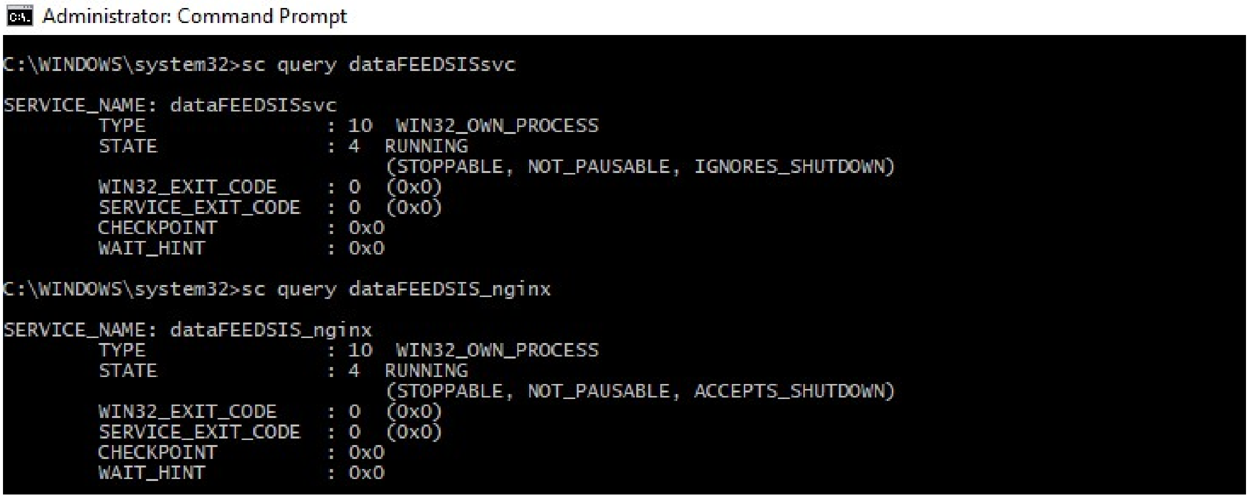
```
C:\WINDOWS\system32>sc start dataFEEDSISsvc

SERVICE_NAME: dataFEEDSISsvc
        TYPE               : 10  WIN32_OWN_PROCESS
        STATE              : 2  START_PENDING
                                (NOT_STOPPABLE, NOT_PAUSABLE, IGNORES_SHUTDOWN)
        WIN32_EXIT_CODE    : 0  (0x0)
        SERVICE_EXIT_CODE  : 0  (0x0)
        CHECKPOINT         : 0x0
        WAIT_HINT          : 0x0
        PID                : 6008
        FLAGS              :

C:\WINDOWS\system32>sc start dataFEEDSIS_nginx

SERVICE_NAME: dataFEEDSIS_nginx
        TYPE               : 10  WIN32_OWN_PROCESS
        STATE              : 2  START_PENDING
                                (NOT_STOPPABLE, NOT_PAUSABLE, IGNORES_SHUTDOWN)
        WIN32_EXIT_CODE    : 0  (0x0)
        SERVICE_EXIT_CODE  : 0  (0x0)
        CHECKPOINT         : 0x0
        WAIT_HINT          : 0x7d0
        PID                : 16008
        FLAGS              :
```

Figure: Installation, Setup, Start Services, Start Services From Command Prompt



```
C:\WINDOWS\system32>sc query dataFEEDSISsvc

SERVICE_NAME: dataFEEDSISsvc
        TYPE               : 10  WIN32_OWN_PROCESS
        STATE              : 4  RUNNING
                                (STOPPABLE, NOT_PAUSABLE, IGNORES_SHUTDOWN)
        WIN32_EXIT_CODE    : 0  (0x0)
        SERVICE_EXIT_CODE  : 0  (0x0)
        CHECKPOINT         : 0x0
        WAIT_HINT          : 0x0

C:\WINDOWS\system32>sc query dataFEEDSIS_nginx

SERVICE_NAME: dataFEEDSIS_nginx
        TYPE               : 10  WIN32_OWN_PROCESS
        STATE              : 4  RUNNING
                                (STOPPABLE, NOT_PAUSABLE, ACCEPTS_SHUTDOWN)
        WIN32_EXIT_CODE    : 0  (0x0)
        SERVICE_EXIT_CODE  : 0  (0x0)
        CHECKPOINT         : 0x0
        WAIT_HINT          : 0x0
```

Figure: Installation, Setup, Start Services, Validate By Querying Services From Command Prompt

3. Stop Services

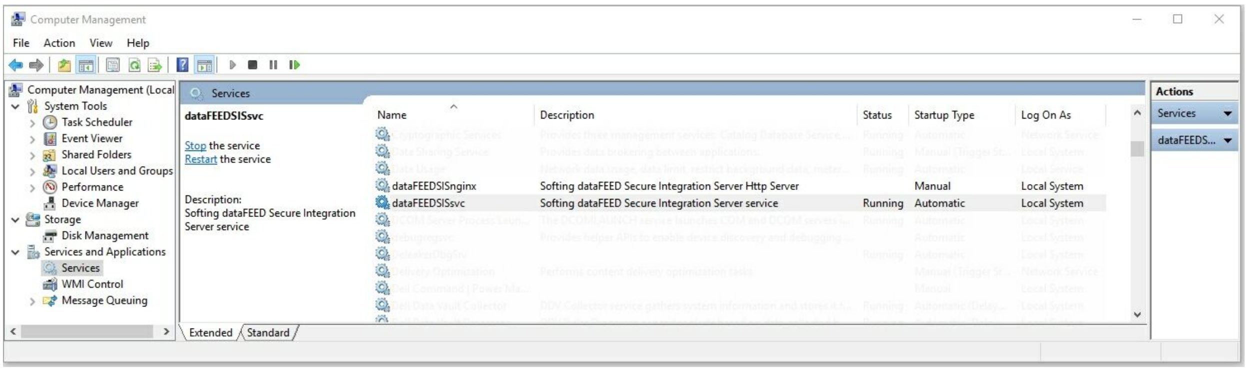
Once the system is up and running it might be required at some point to stop and restart it. In order to stop the running system two possibilities are explained below:

3.1. Windows Computer Management

Open **Computer Management** and navigate to **Computer Management -> Services and Applications -> Services.** On the right side view all the system's services are listed. Order by name and search for **dataFEEDSISsvc** and **dataFEEDSISnginx**.

For each service, while the service is running, proceed as follows:

- Double click on the service entry to open the service properties window.



Computer Management

dataFEEDSISsvc

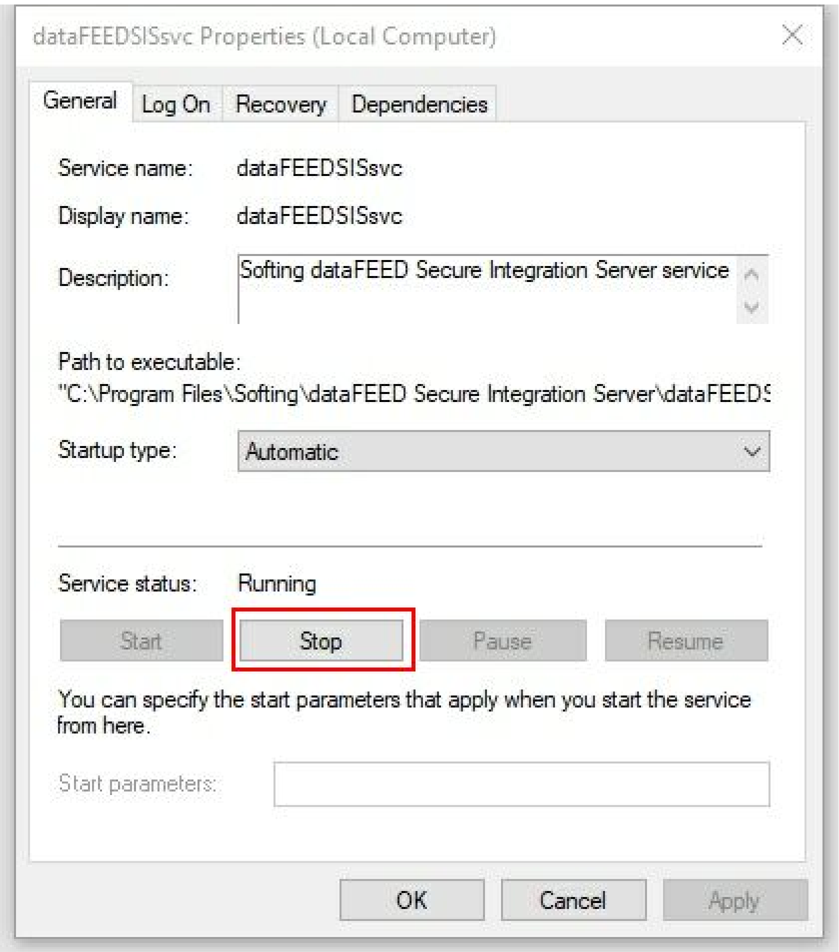
Stop the service
Restart the service

Description:
Softing dataFEED Secure Integration Server service

Name	Description	Status	Startup Type	Log On As
Cryptographic Services	Provides three management services: Catalog Database Service,...	Running	Automatic	Network Service
Data Sharing Service	Provides data brokering between applications.	Running	Manual (Trigger St...	Local System
Data Usage	Network data usage, data limit, restrict background data, meter...	Running	Automatic	Local Service
dataFEEDSISnginx	Softing dataFEED Secure Integration Server Http Server		Manual	Local System
dataFEEDSISsvc	Softing dataFEED Secure Integration Server service	Running	Automatic	Local System
DCOM Server Process Laun...	The DCOMLAUNCH service launches COM and DCOM servers i...	Running	Automatic	Local System
debugregsvc	Provides helper APIs to enable device discovery and debugging ...		Automatic	Local System
DeleakerDbgSrv		Running	Automatic	Local System
Delivery Optimization	Performs content delivery optimization tasks		Manual (Trigger St...	Network Service
Dell Command | Power Ma...			Manual	Local System
Dell Data Vault Collector	DDV Collector service gathers system information and stores it f...	Running	Automatic (Delay...	Local System

Figure: Installation, Setup, Stop Services

- Click the **[Stop]** button on the properties window to stop the service.
- Change the Startup type from Manual to Automatic to automatically start the service at system start-up.



dataFEEDSISsvc Properties (Local Computer)

Service name: dataFEEDSISsvc

Display name: dataFEEDSISsvc

Description: Softing dataFEED Secure Integration Server service

Path to executable:
"C:\Program Files\Softing\dataFEED Secure Integration Server\dataFEEDS

Startup type: Automatic

Service status: Running

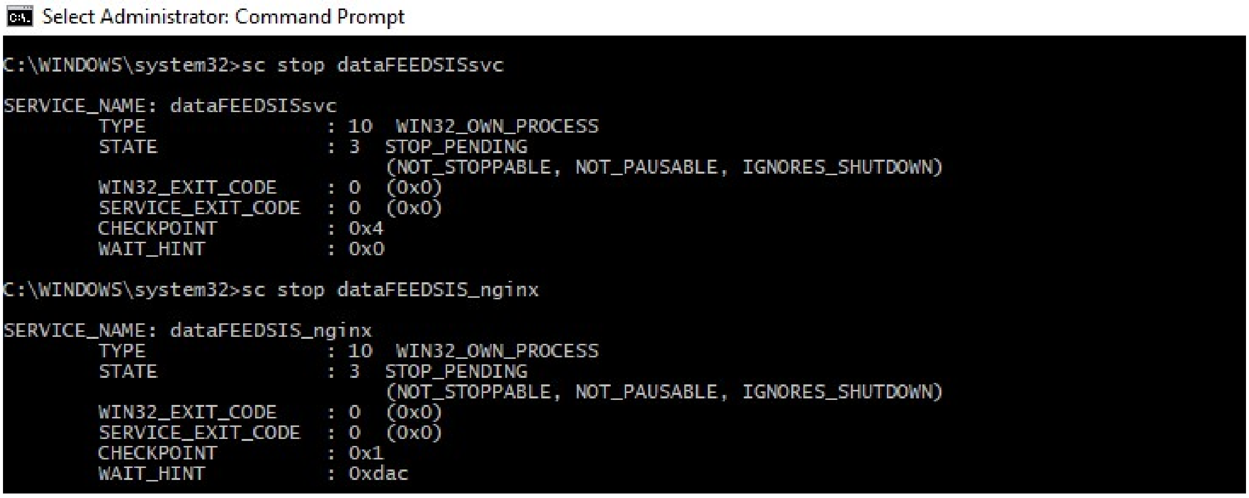
You can specify the start parameters that apply when you start the service from here.

Start parameters:

Figure: Installation, Setup, Stop Services, Service Properties

3.2. Command Line

Open a command prompt with administrative rights and issue the following commands: **sc stop dataFEEDSISsvc** and **sc stop dataFEEDSIS_nginx**. The services shall change their **STATE** value to **3 STOP_PENDING**. When the services have successfully stopped, querying them again as described in the first step, shall display their new state values as **1 STOPPED**.



```
C:\WINDOWS\system32>sc stop dataFEEDSISsvc

SERVICE_NAME: dataFEEDSISsvc
        TYPE               : 10  WIN32_OWN_PROCESS
        STATE              : 3  STOP_PENDING
                                (NOT_STOPPABLE, NOT_PAUSABLE, IGNORES_SHUTDOWN)
        WIN32_EXIT_CODE    : 0  (0x0)
        SERVICE_EXIT_CODE  : 0  (0x0)
        CHECKPOINT         : 0x4
        WAIT_HINT          : 0x0

C:\WINDOWS\system32>sc stop dataFEEDSIS_nginx

SERVICE_NAME: dataFEEDSIS_nginx
        TYPE               : 10  WIN32_OWN_PROCESS
        STATE              : 3  STOP_PENDING
                                (NOT_STOPPABLE, NOT_PAUSABLE, IGNORES_SHUTDOWN)
        WIN32_EXIT_CODE    : 0  (0x0)
        SERVICE_EXIT_CODE  : 0  (0x0)
        CHECKPOINT         : 0x1
        WAIT_HINT          : 0xdac
```

Figure: Installation, Setup, Start Services, Stop Services From Command Prompt

4 Configuration

The current chapter shall provide information which allows proper access, configuration and maintenance of the dataFEED Secure Integration Server in a production environment. Details from accessing the configuration interface, creation and changing user information, changing system states to defining OPC UA client connections, creation of OPC UA server endpoints and address space operations are covered.

4.1 Contact

The default view after logging in is the **Contact & Help** page which provides information for contacting customer support at Softing Industrial Automation GmbH.

4.2 License Agreement

The license agreement section accessible by navigating to **Information -> License Agreements** provides a link listing the license for all free domain software components used by the dataFEED Secure Integration Server.

4.3 Version

Navigating to **Information -> Version** should provide information about the dataFEED Secure Integration Server version currently running on the computer. The version information will be required while contacting Softing Industrial Automation GmbH customer support.

4.4 Introduction

dataFEED Secure Integration Server provides an online accessible web interface for configuration purposes. It requires network access to the machine running the dataFEED Secure Integration Server and a compatible web browser 10.

Access to the configuration web pages is provided by the high performance nginx web server delivered as a service 18 by the dataFEED Secure Integration Server installation package.

Please note that the configuration information herein assumes following:

- usage of Chrome (version 64.0.3282.167 64-bit) for accessing the web pages
- accessing dataFEED Secure Integration Server configuration interface is performed locally (web browser and the dataFEED Secure Integration Server services are on the same machine)

The configuration web interface provides easy and simple access to various configuration areas such as:

- user management: adding, removing or changing user permissions
- interrogating licenses state
- setting logging limits or accessing logs
- configuration backup, restore and factory reset
- change system state (start, restart or stop)

- OPC UA client connections and server endpoints setup with enhanced security features like **IP filtering, access protection or address space filters**
- Address space management (add, remove or reassignment)
- a built-in address space browser

4.4.1 Web Interface Operation

The web server supports both secure (HTTPS) and non-secure (HTTP) access, however using the HTTPS secured channel access requires an extra step of trusting the provided certificate.

Web access Quick reference:

Access URL	Default Username	Default Password	Notes
http://localhost:8099	**admin**	**admin**	Non secure access. Ready to use.
https://localhost:443	**admin**	**admin**	Secure access. Might require additional configuration to entrust the provided security certificate.

Table: Web Interface Operation, Quick reference

1. Accessing Main Page

There are two options to access the main web page:

- Non secured version

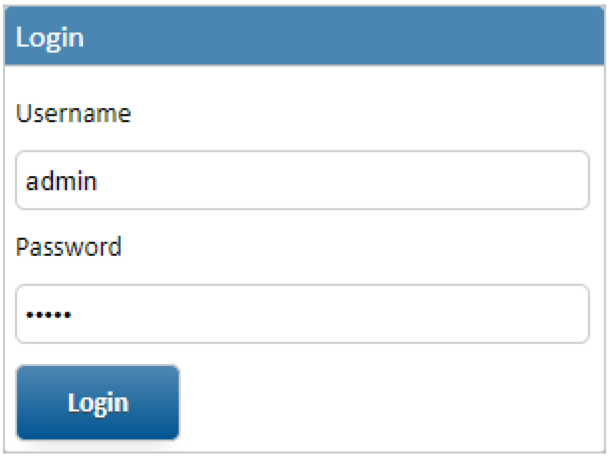
To access the non secured (HTTP) configuration web pages, open the web browser and navigate to **http://localhost:8099**. A login page should now be displayed

- Secured Version

To access the secured (HTTPS) configuration web pages, open the web browser and navigate to **https://localhost:443**. The browser should acknowledge that the connection is not trusted. In order to fix this the web server's SSL certificate needs to be entrusted.

2. Login

First login requires to: fill in the default username (**admin**) and password (**admin**) and to click the **[Login]** button. After logging in, a password change option and other user related operations shall be available for optional use.



Username

admin

Password

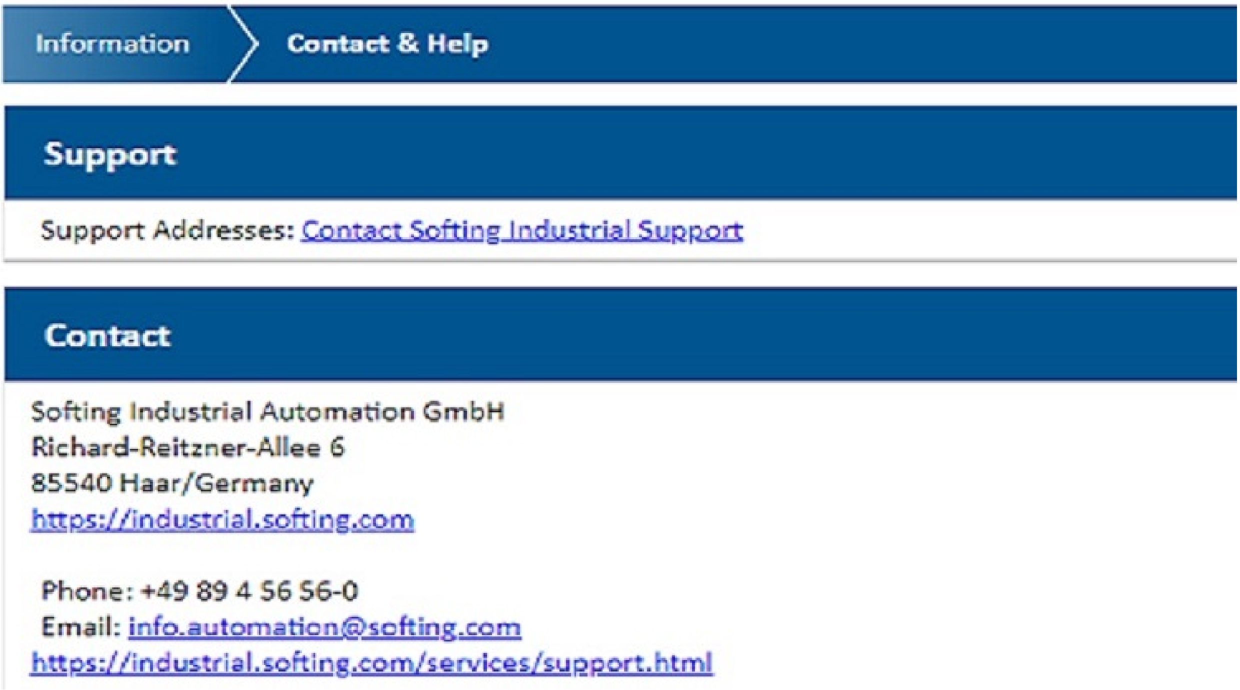
•••••

Figure: Web Interface Operation, Login

3. Page layout

The layout conforms to a single-page application style hence we can identify the following parts:

- **Header** - red area
- **Navigation tree** - blue area
- **Content** - green area



Support

Support Addresses: Contact Softing Industrial Support

Contact

Softing Industrial Automation GmbH
Richard-Reitzner-Allee 6
85540 Haar/Germany
https://industrial.softing.com

Phone: +49 89 4 56 56-0
Email: info.automation@softing.com
https://industrial.softing.com/services/support.html

Figure: Web Interface Operation, Page Layout

4. Header Area

The header provides information about the logged in user and two buttons , global accessible, on the right side.

Global accessible buttons:

Button	Action
Logout	Clicking the **[Logout]** button, the configuration session in progress shall be terminated.
Help	Provides access to the contextual, online browsable, *dataFEED Secure Integration Server* help pages. Click the **[Help]** button to open the help information page associated with the current content.

Table: Web Interface Operation,Header Area

5. Navigation Area

The navigation area allows easy navigation across the various configuration options. A fully expanded navigation tree preview is available below and should provide an overview of the possible configuration options.

The navigation menu is a tree which can be expanded or collapsed by clicking on the displayed labels. The navigation bar will preserve its state once collapsed or expanded.

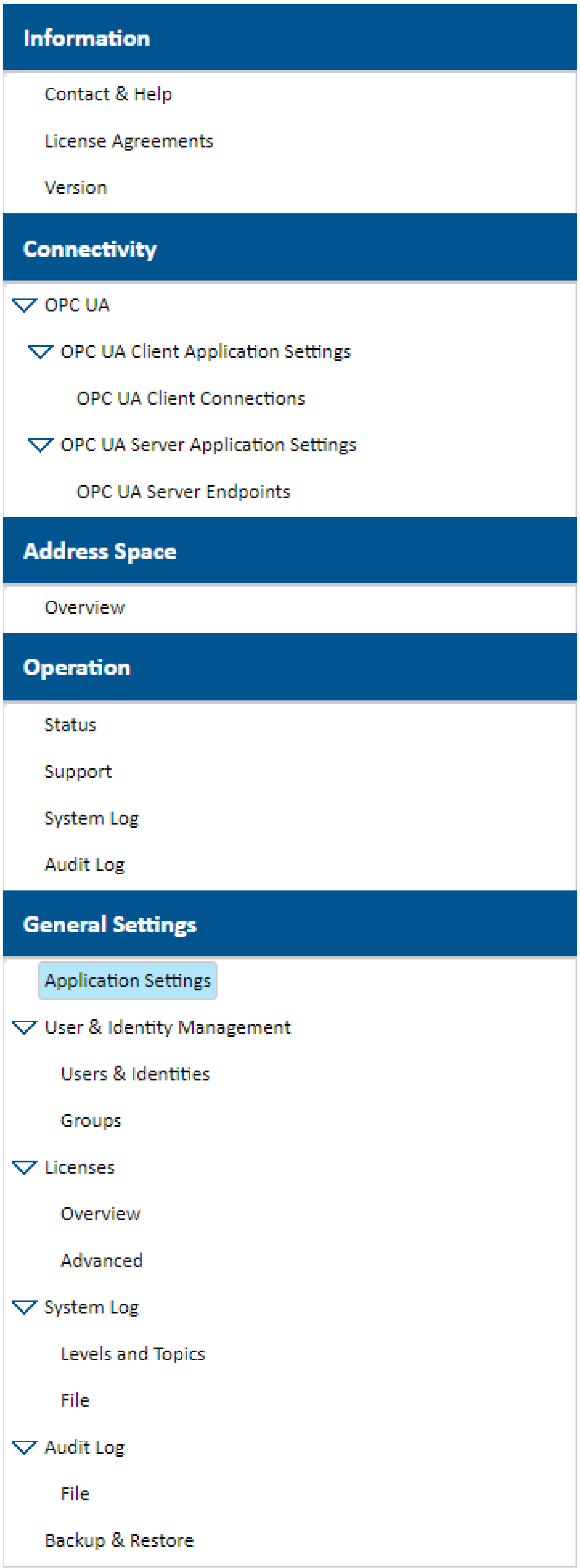


Figure: Web Interface Operation, Navigation Area

6. Content Area

Area used to interact with the user and perform the configuration and visualization operations.

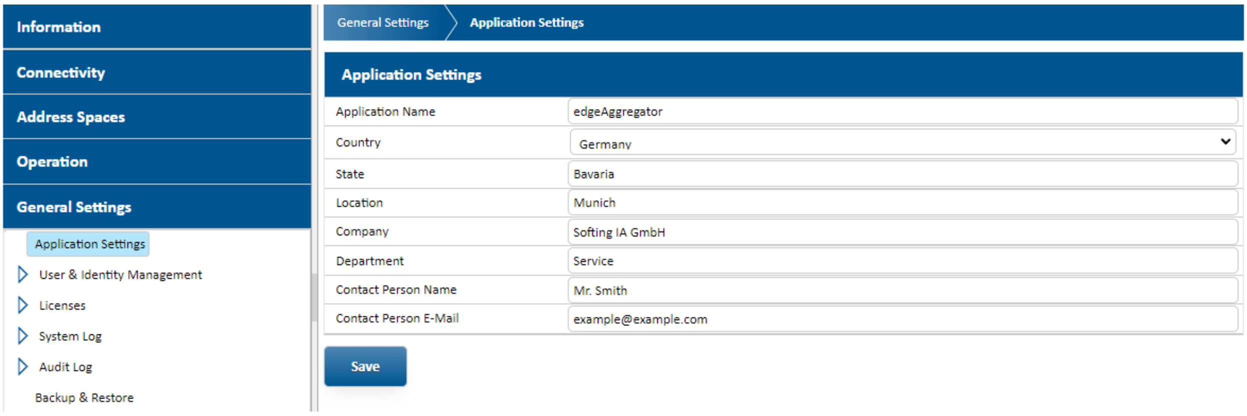
4.5 General Settings

General settings chapter groups information on generic system related configuration operations for user management, logging and configuration backup and restore.

4.5.1 Application Settings

Application settings allows the user to add and customize the dataFEED Secure Integration Server running instance identification information. In larger systems, where several dataFEED Secure Integration Server instances are running, the application settings identification information is valuable by allowing any authorized user to easily identify specific information about the system such as: application name, responsible person and contact information, or location.

Navigate to **General Settings->Application Settings** to access the application setting's page. Application default values are predefined at installation time; it is recommended to customize the application settings after installation during the first configuration session.



Application Settings

Application Name	edgeAggregator
Country	Germany
State	Bavaria
Location	Munich
Company	Softing IA GmbH
Department	Service
Contact Person Name	Mr. Smith
Contact Person E-Mail	example@example.com

Figure: Application Settings page

Bottom page buttons functionality:

Button	Action
Save	Changes in the application settings are applied clicking the **[Save]** button. Saved information is persistent.

Table: Application Settings, buttons functionality

The application identification information, available for user manipulation in the application settings page, is described in the following table:

Parameter name	Default Value	Details
Application name	**edgeAggregator**	Identifies the dataFEED Secure Integration Server running instance.
Country	**Germany**	Identifies the dataFEED Secure Integration Server running instance country.
State	**Bavaria**	Identifies the dataFEED Secure Integration Server running instance state.
Location	**Munich**	Identifies the dataFEED Secure Integration Server running instance location.
Company	**Softing IA GmbH**	Identifies the company running the dataFEED Secure Integration Server instance.
Department	**Service**	Identifies the department running the dataFEED Secure Integration Server instance.
Contact Person Name	**Mr. Smith**	Identified the person responsible for the running instance.
Contact Person E-Mail	**example@example.com**	Identified the responsible's person e-mail for the running instance.

Table: Application Settings, field descriptions

4.5.2 User & Identity Management

User & Identity Management is the configuration section under which the following configuration topics are handled:

- **User & Identities -** by means of which the following operations can be performed on the dataFEED Secure Integration Server users:
  - Modify operations per user:
    - Add, Edit and Delete users
    - Creation (Generation), Assignment and Deletion of user certificates 41.
  - Views per user:
    - Overview of the user Certificate 41 statuses
    - Overview of the Groups to which the user is assigned
    - Overview of the context under which a certain user operates, such as the client connections or server endpoints configured to use the user
- **Groups -** by means of which the the following operations can be performed on the dataFEED Secure Integration Server groups:
  - Modify operations per group:
    - Add and remove user groups
  - Views per group:
    - Number of users belonging to the group
    - Details of the users belonging to the group, such as Name and Description

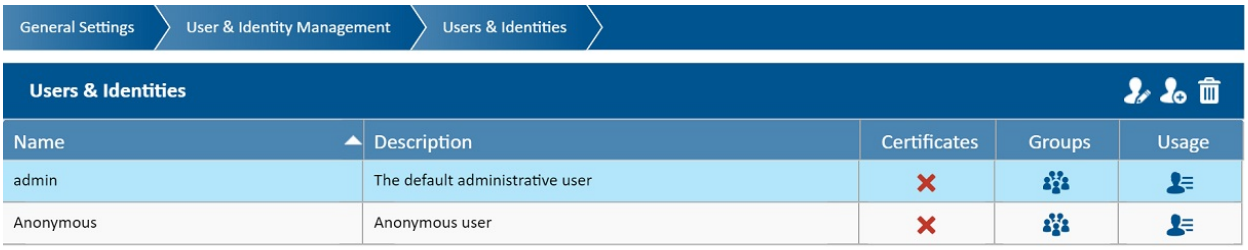
4.5.2.1 Users & Identities

The first access to the configuration GUI requires that the default user name (**admin**) and password (**admin**) are provided, hence it is strongly recommended to change the password after the first log-in.

To change user related configuration options navigate to **General Settings -> User & Identity Management -> Users & Identities,** double click admin user, expand the Change Password control and insert the desired password.

1. General Description

The user is presented with the following page:



General Settings > User & Identity Management > Users & Identities

Users & Identities

Name	Description	Certificates	Groups	Usage
admin	The default administrative user	✗	👥	👤
Anonymous	Anonymous user	✗	👥	👤

Figure: User & Identities main view

Doubleclicking the line of a user results in displaying the according **Settings** page.

Predefined Users

The dataFEED Secure Integration Server is configured to support the following predefined users:

Username	Password	Group name	Details
admin	admin	Administrators	Default administrative user, shall be used for first login.
Anonymous	<none>	OPC UA Users	User restricted to OPC UA connectivity operations only. No user operations are available for this user.

Table: User & Identities, Predefined users

From this page, the following actions can be initiated:

The Users & Identities menu icons trigger by **single-click** the following actions:

Button	Action
👤	**Add user.**
👤	**Edit existing user**
🗑	**Delete existing user and it's user certificates**

Table: User & Identities, Menu Icons

The **Group** and **Usage** icons trigger by **single-click** the following actions:

Button	Action
👥	**Choose groups** to which the user belongs
👤	**Show usage** context in which the selected user is used.

Table: User & Identities, Groups and Usage icons

The application user can easily be aware of the user certificate status by interpreting the **Certificate** column icons.

In order to interpret the **Certificate** icons, check the Certificate icon interpretation 187 in the **Certificate** table entry.

2. Typical use cases

1. Add a new user

This use case can be performed by the following steps:

1. Click **Add user** button and the user Settings 36 page will be displayed
2. Fill in the fields as described in the user Settings 36 page

2. Change existing user configuration parameters

This use case can be performed by the following steps:

1. Click **Edit existing user** button while the desired user row is selected or double-click the row corresponding to the desired user and the user Settings 36 page will be displayed
2. Change the fields as described in the user Settings 36 page

3. Delete existing user

This use case can be performed by the following steps:

1. Click the row corresponding to the desired user and the row shall be selected as a result

2. Click **Delete existing user** 🗑 button and the user will be deleted if it is not already in use. For example in an OPC UA Client Connection authentication 163 or OPC UA server endpoint users list 211.

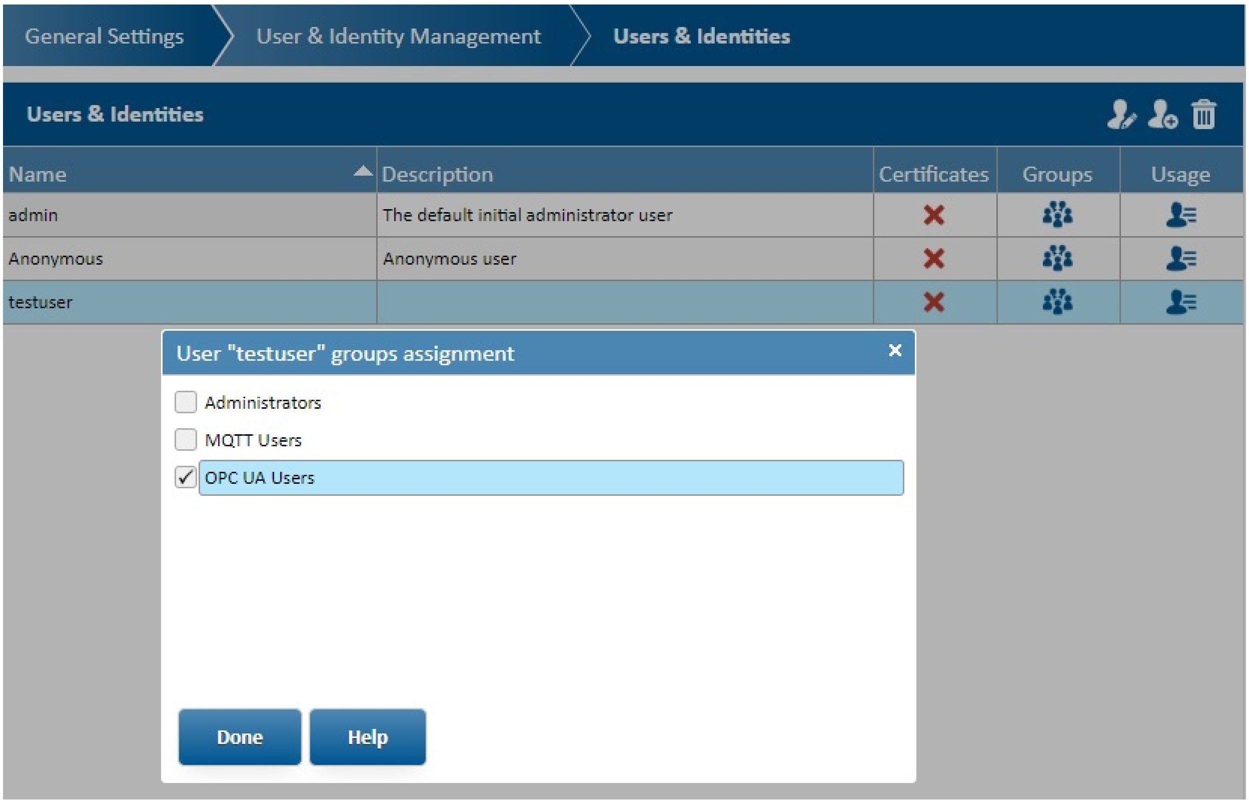
⚠ Before deleting a user from the application one has to ensure that the user is not part of any client Connection Settings 164 or OPC UA server endpoint users list 211.

⚠ Deleting a user has as a consequence the deletion of all it's associated user Certificates 41.

4. Change or view the groups to which the user belongs to

This use case can be performed by the following steps, starting from the context of this page:

1. Click **Choose groups** corresponding to the desired user and the following pop-up shall be displayed:



Name	Description	Certificates	Groups	Usage
admin	The default initial administrator user	✗		
Anonymous	Anonymous user	✗		
testuser		✗		

User "testuser" groups assignment

□ Administrators
□ MQTT Users
☑ OPC UA Users

Figure: User & Identities, User groups assignment

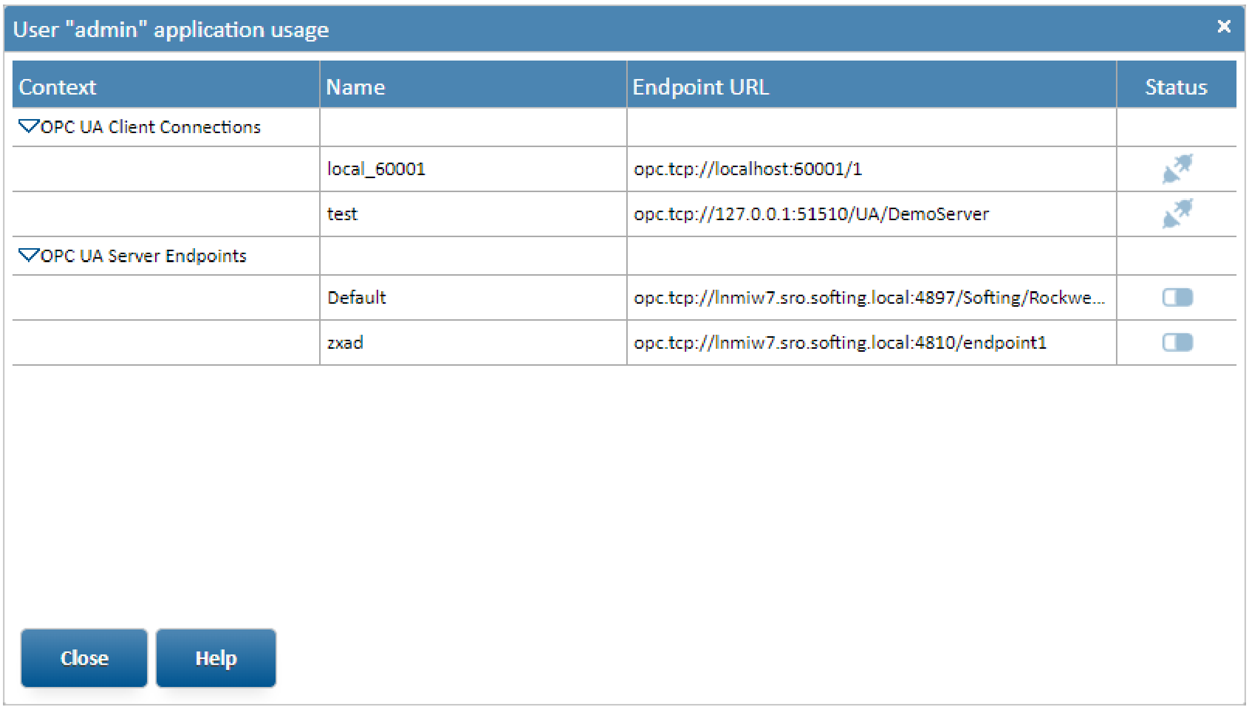
2. Select or deselect the groups in which the user belongs to
3. Press **Done** button to apply the selection

Changing groups alternative

Changing the groups to which the user belongs, can be performed also from the context of operating changes in the user Settings 36 page

5. Visualize user usage context

To visualize a user usage context, which can either be an OPC UA client connection or an OPC UA server endpoint context, click the **User usage** corresponding to the desired user and the following pop-up shall be displayed:



User "admin" application usage

Context	Name	Endpoint URL	Status
▽OPC UA Client Connections			
	local_60001	opc.tcp://localhost:60001/1	🔌
	test	opc.tcp://127.0.0.1:51510/UA/DemoServer	🔌
▽OPC UA Server Endpoints			
	Default	opc.tcp://lnmiw7.sro.softing.local:4897/Softing/Rockwe...	⬭
	zxad	opc.tcp://lnmiw7.sro.softing.local:4810/endpoint1	⬭

Figure: User usage

Information presented in Figure: User usage provides a simple way of identifying the OPC UA client connection or server endpoint which are using the selected user, also providing additional information such as the connection endpoint URL and status information.

6. Generate, upload or remove user certificates

A user can have one or more associated certificates, also known as user certificates, from which one can be selected to authenticate with. This is only possible if the "Certificate" radio button is selected in the "Authentication Settings" presented in "OPC UA Client Connections->Connection Settings" tab, see also Client Connections 161 figure and Authentication Settings description 163.

As described in user Certificates 41 page, one or more multiple user certificates can be generated, uploaded or deleted.

To execute the previously mentioned actions one has to switch over to the user Certificates 41 page accessible at the right side of the user Settings 36 page tab.

4.5.2.1.1 Settings

1. Settings for a New User:

The user settings page enables the parametrization of a user and can be accessed in the following contexts:

1. Through the **General Settings -> User & Identity Management -> Add User** button 31

This is the **main** designed direct path to manage users in the the dataFEED Secure Integration Server

2. Through the **Connectivity -> OPC UA Client Application Settings -> OPC UA Client Connections -> Connection Details ->** Create New User button 162

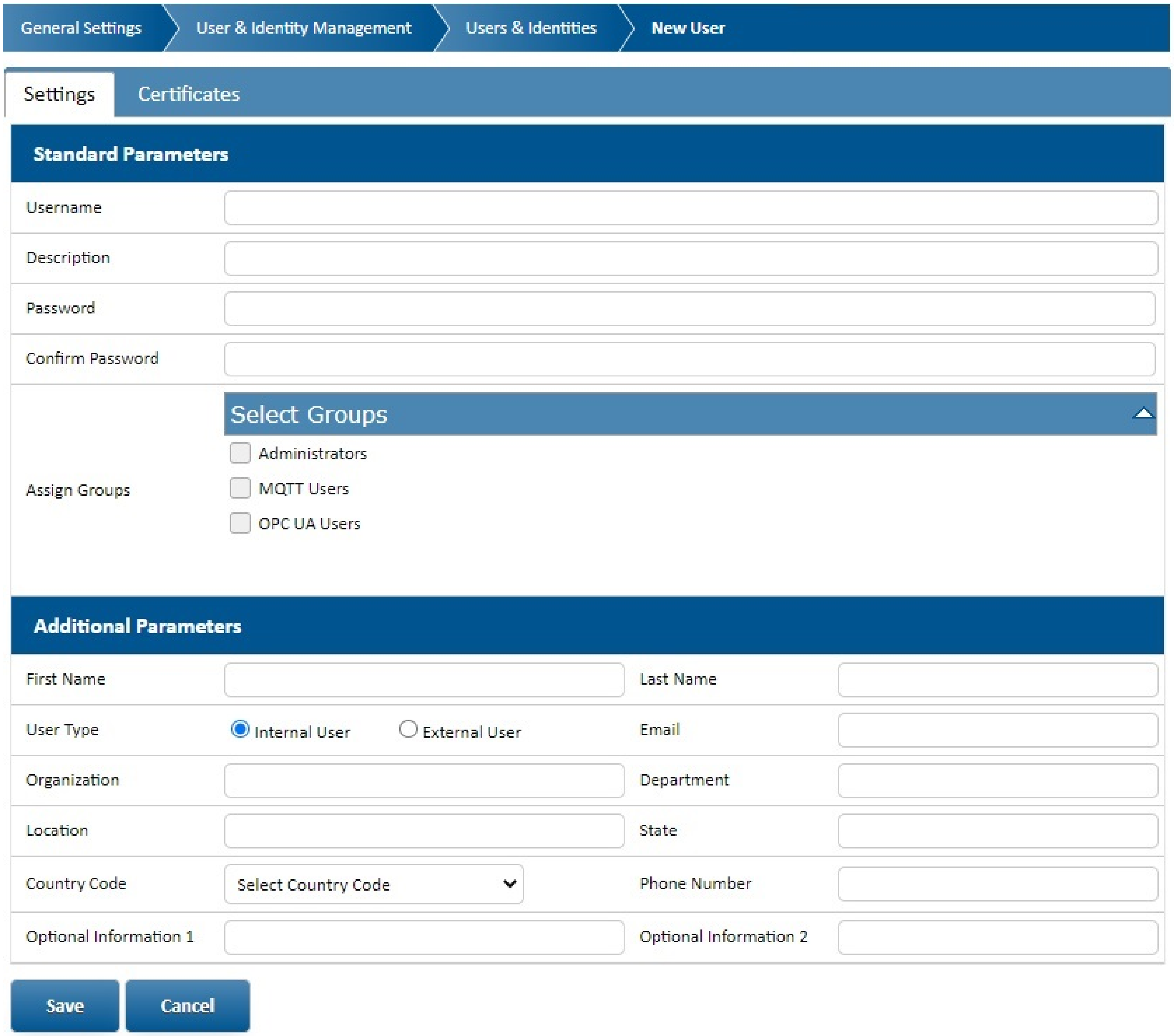
This is a **convenience** designed path to manage users in the the dataFEED Secure Integration Server

3. Through the **Connectivity -> OPC UA Server Application Settings -> OPC UA Server Endpoints ->Endpoint Users - Identities -> Add Endpoint User** **button->** Create New User button 212

This is a **convenience** designed path to manage users in the the dataFEED Secure Integration Server

2. Settings for a New User:

When a new user is added the following user settings page is displayed:



General Settings > User & Identity Management > Users & Identities > New User

Settings | Certificates

Standard Parameters

Username

Description

Password

Confirm Password

Assign Groups: Select Groups

□ Administrators

□ MQTT Users

□ OPC UA Users

Additional Parameters

First Name		Last Name	
User Type	● Internal User ○ External User	Email	
Organization		Department	
Location		State	
Country Code	Select Country Code	Phone Number	
Optional Information 1		Optional Information 2	

Figure: User & Identities, Settings for New User

3. Settings Fields description:

Parameter name	Mandatory	Details
Username	YES	The unique user name which identifies the user in the dataFEED Secure Integration Server instance.
Description	YES	A description associated with the user. Note that the pair *Username/Description* must be unique among all the defined users, otherwise an error will be raised. See warning Figure: User & Identities, Username/Description already exists 39.

Password	YES	The password attached to the user in conjunction with the user groups assignment provides the following permissions: - it allows the user to login on the configuration web page when the user is part of the **Administrators** group - it allows the user to be used as a OPC UA client connection user when it is part of the **OPC UA** Users group
Assign Groups	NO	Drop-down list with the existing configured groups. The user can be assigned to multiple groups by checking their corresponding check-box. It is by this means that the user gains or looses access to certain dataFEED Secure Integration Server user rights.
First Name	NO	The users first name.
Last Name	NO	The users last name.
User Type	YES(implicit)	Radio button implicitly set on "Internal User". The user might be considered as "External User" and selected accordingly.
Organization	NO	The organization that the user belong to.
Department	NO	The department that the user belong to.
Location	NO	The location that the user is in.
State	NO	The state that the user resides in.
Country Code	NO	Drop-down list with the countries from which to choose, in which the user resides.
Phone Number	NO	The phone number or multiple ones separated by convenient characters (ex ; or ,), at which the user can be contacted.
Email	NO	Single email address at which the user can be contacted.
Optional Information 1	NO	Additional associated information.
Optional Information 2	NO	Additional associated information.

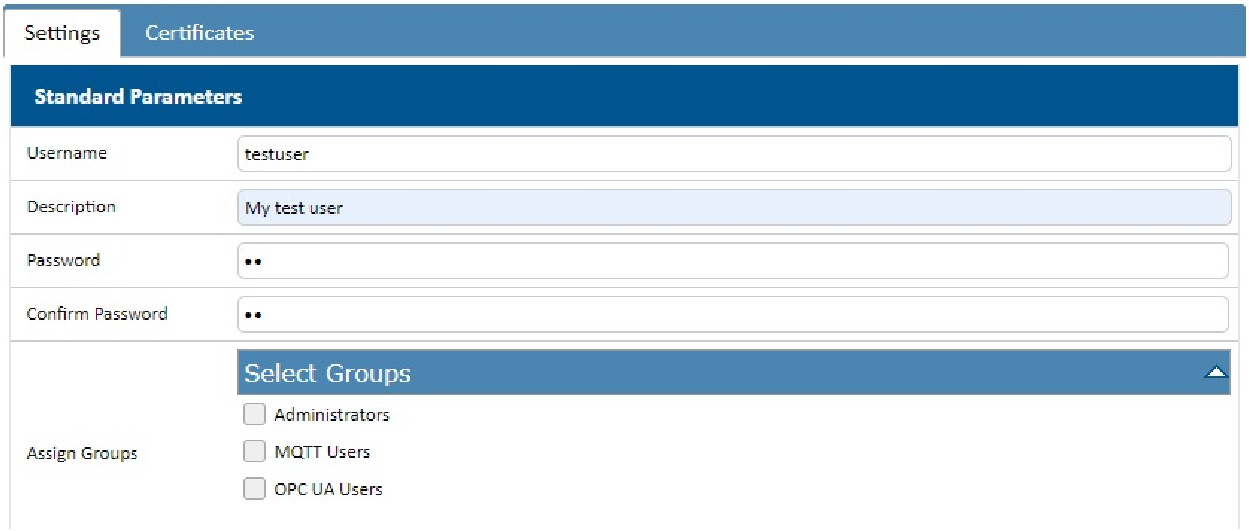
Table: User & Identities, Settings Fields

4. Typical use cases:

1. Quick user setup

By providing the values from the mandatory fields a user can be easily inserted into the dataFEED Secure Integration Server instance.

The user can expand the "Select Groups" drop-down menu in-order to be able to check the groups to which it belongs, as presented in the following picture:

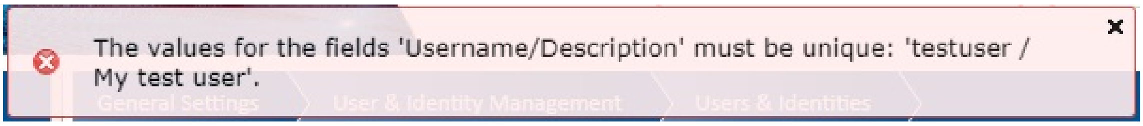


Standard Parameters

Username	testuser
Description	My test user
Password	••
Confirm Password	••
Assign Groups	Select Groups □ Administrators □ MQTT Users □ OPC UA Users

Figure: User & Identities, Settings Standard Parameters

Ensure that the **Username/Description** pair is not already in use, otherwise the following message will be presented when Save button is pressed:



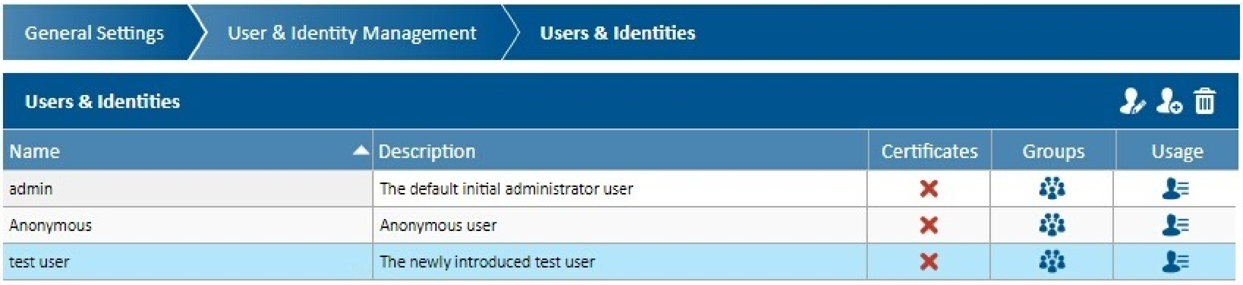
The values for the fields 'Username/Description' must be unique: 'testuser / My test user'.

Figure: User & Identities, Username/Description already exists

By default the group selection is empty and the user can save it's groups settings in this state and change them afterward.

If the newly introduced user shall have the possibility to authenticate using an associated user certificate, than the process of creating user certificates has to be performed by switching to the user Certificates 41 tab.

The New User adding step is completed when the **Save** button action completes and the page context switches back to the **User&Identities** page:

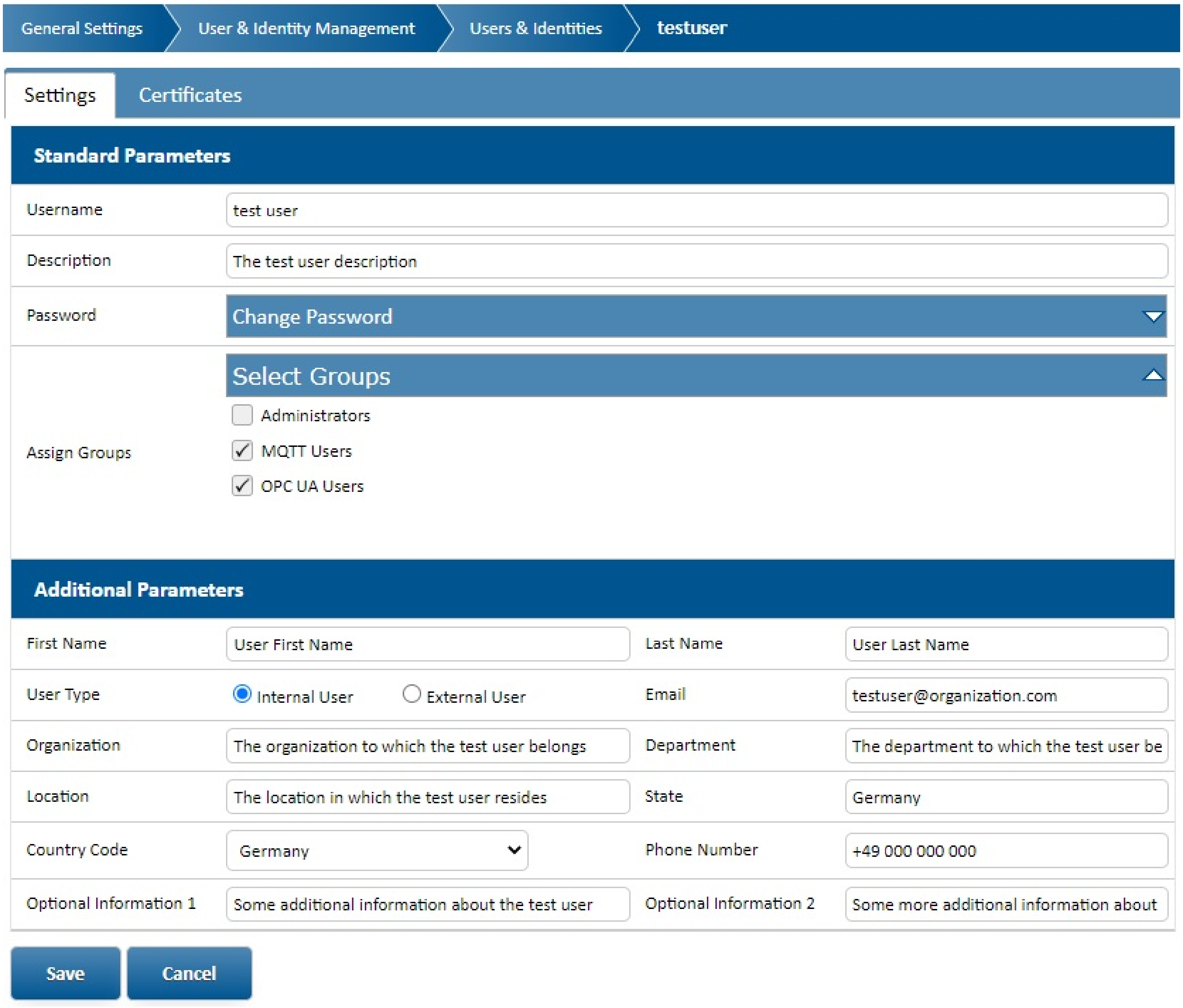


Name	Description	Certificates	Groups	Usage
admin	The default initial administrator user	✗		
Anonymous	Anonymous user	✗		
test user	The newly introduced test user	✗		

Figure: User & Identities, New User is added

5. Settings for an existing user:

When an existing user's settings are modified the following settings page is displayed:



Standard Parameters

Username	test user
Description	The test user description
Password	Change Password
Assign Groups	Select Groups □ Administrators ☑ MQTT Users ☑ OPC UA Users

Additional Parameters

First Name	User First Name	Last Name	User Last Name
User Type	● Internal User ○ External User	Email	testuser@organization.com
Organization	The organization to which the test user belongs	Department	The department to which the test user be
Location	The location in which the test user resides	State	Germany
Country Code	Germany	Phone Number	+49 000 000 000
Optional Information 1	Some additional information about the test user	Optional Information 2	Some more additional information about

Figure: User & Identities, Settings for existing user

The presented fields are identical with the fields from Figure: User & Identities, Settings for New User 37, except that the "Password" and "Confirm Password" fields are now embedded in the expandable "Password" field.

4.5.2.1.2 Certificates

Each application user can authenticate to remote OPC UA servers using an user name security token, which uses the username/password pair to authenticate, or an X509 security token, which requires as a prerequisite for the authentication creating or attaching an associated user certificate, as described in the current chapter.

1. General description:

The configuration of such certificates is done through the user Certificates page:

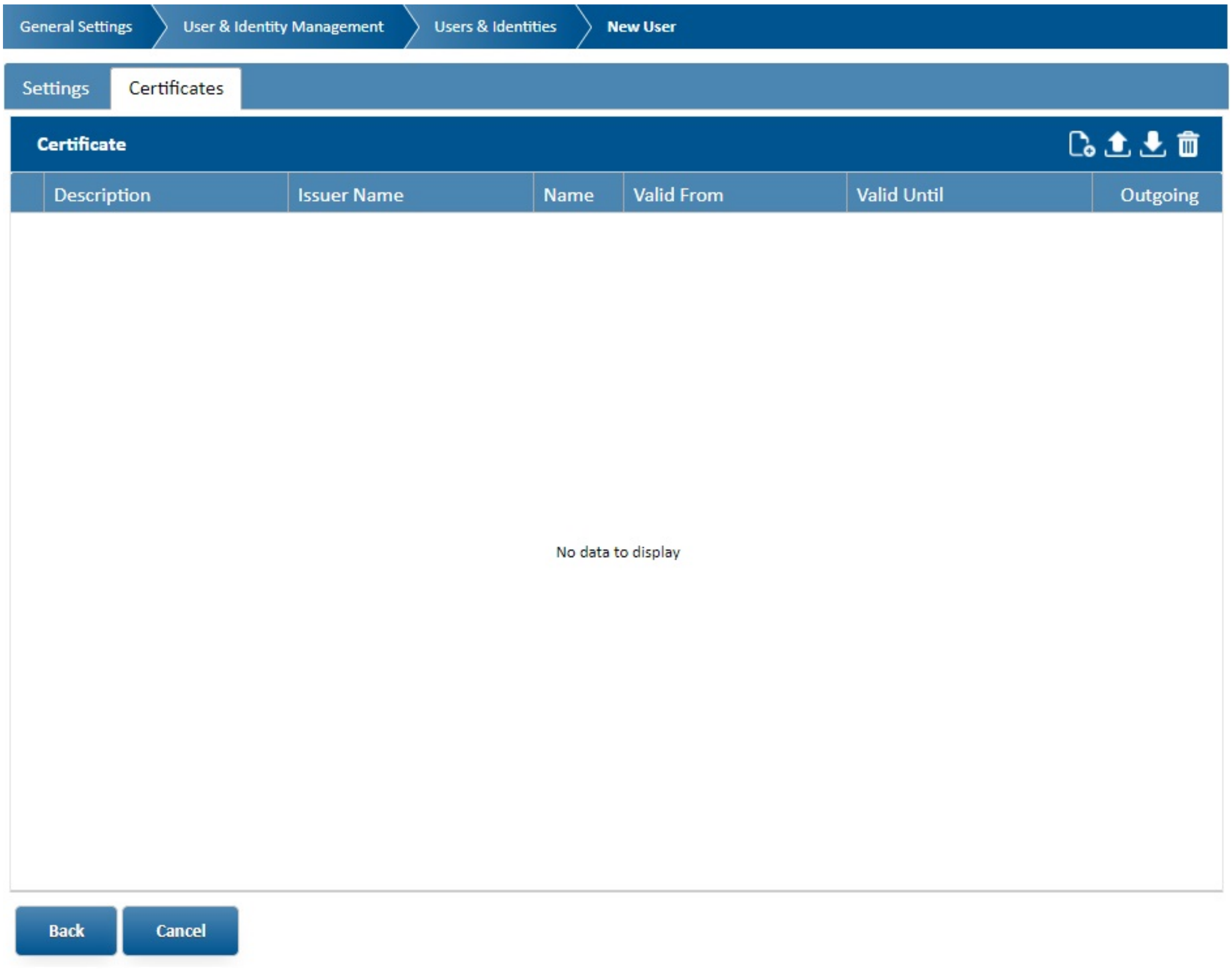


Figure: User & Identities, User Certificates Page

For a newly added user no certificates created in advance are shown.

Clicking the **Generate certificate** button creates a new user certificate and adds this.

Clicking the **Upload Certificate** button uploads an existing user certificate.

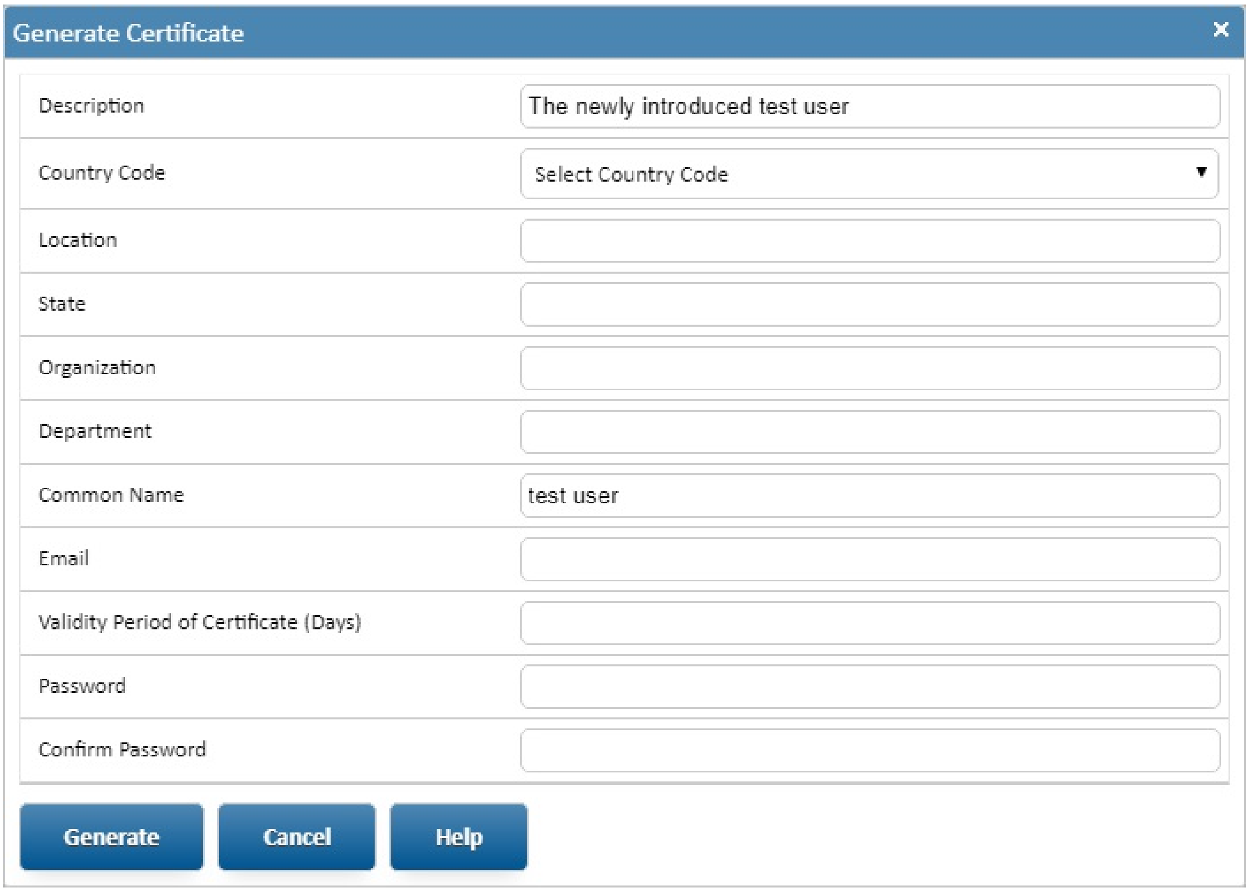
Clicking the **Download Certificate** button downloads the selected existing user certificate.

Clicking the **Delete User Certificate** button deletes the selected existing user certificate.

2. Typical use cases:

1. Generate a new user certificate:

To generate a new user certificate, click on the **Generate certificate** button and the following window will pop up:



Generate Certificate

Description	The newly introduced test user
Country Code	Select Country Code
Location	
State	
Organization	
Department	
Common Name	test user
Email	
Validity Period of Certificate (Days)	
Password	
Confirm Password	

Figure: User & Identities, Generate Certificate

By hovering over the input text fields, a Tool-tip will appear to inform about the mandatory state of the field with regards to the generation of the Certificate.

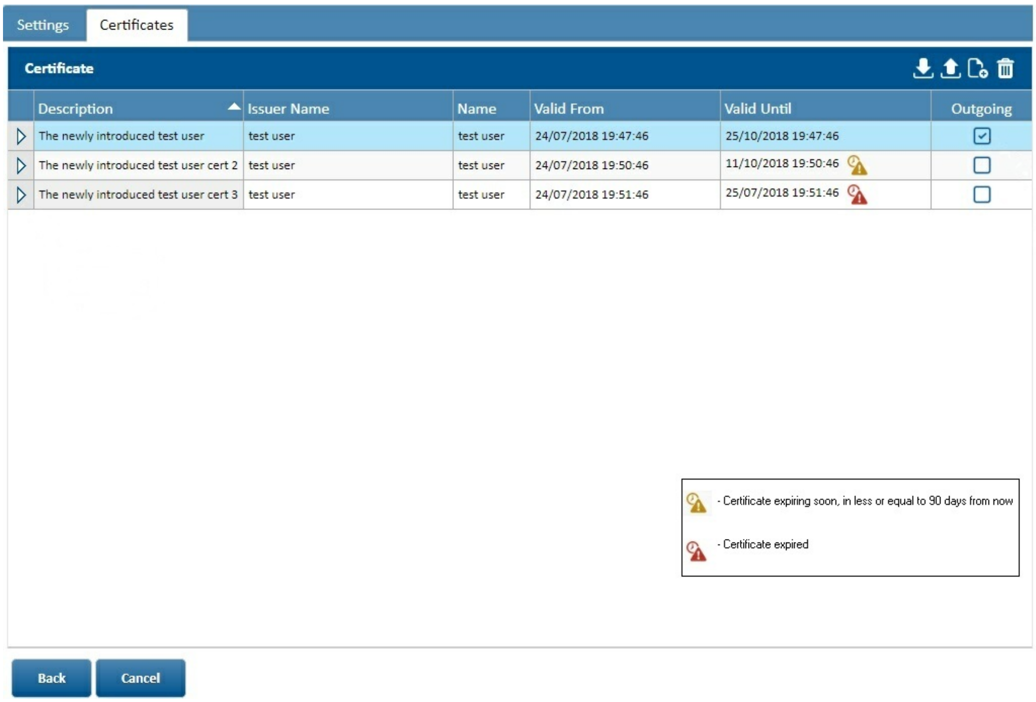
Certificate generation fields description:

Parameter name	Mandatory	X509 field name	Details
Description	**YES**		Certificate description, used for informative purposes.
Country Code	**NO**	**C**	Country Name as ISO3166 two character country code
Location	**YES**	**L**	Locality name, generally city
State	**YES**	**ST**	State or Province Name

Organization	**YES**	**O**	Organization Name
Department	**YES**	**OU**	Organizational Unit Name
Common Name	**YES**	**CN**	Common Name
Email	**NO**		Email Address
Validity Period	**YES**		Validity period starting at the time of generation
Password	**NO**		Password for protecting the certificate's attached private key.

Table: User & Identities, Certificate Generation Fields

Press the Generate button to generate and add the certificate to the associated user certificates list:



Description	Issuer Name	Name	Valid From	Valid Until	Outgoing
The newly introduced test user	test user	test user	24/07/2018 19:47:46	25/10/2018 19:47:46	☑
The newly introduced test user cert 2	test user	test user	24/07/2018 19:50:46	11/10/2018 19:50:46 ⚠	□
The newly introduced test user cert 3	test user	test user	24/07/2018 19:51:46	25/07/2018 19:51:46 ⚠	□

⚠ - Certificate expiring soon, in less or equal to 90 days from now

⚠ - Certificate expired

Figure: User & Identities, User Certificates

Clicking the extension icon on the left will display all the details of the user certificate.

Selecting the check box in the **Outgoing** column enables the associated user certificate for use in the user certificate authentication scenario.

It is worth mentioning that the **Outgoing** check-box is exclusive in the user certificates table, that means only one or none certificates can be selected to be used as the active user certificate at one time.

The expiry date of each user certificate is visually signaled as in **Figure: User & Identities, User Certificates:**

- Certificates that don't expire within 90 days from current time are not marked
- Certificates that expire within 90 days from the current time are marked with the yellow icon ⚠
- Certificates that are already expired are marked with the red icon ⚠

At any time the user can cancel the process of generating a new user certificate by clicking the Cancel button.

To save the newly generated certificate press the Back button to switch to the Settings page and click the Save button.

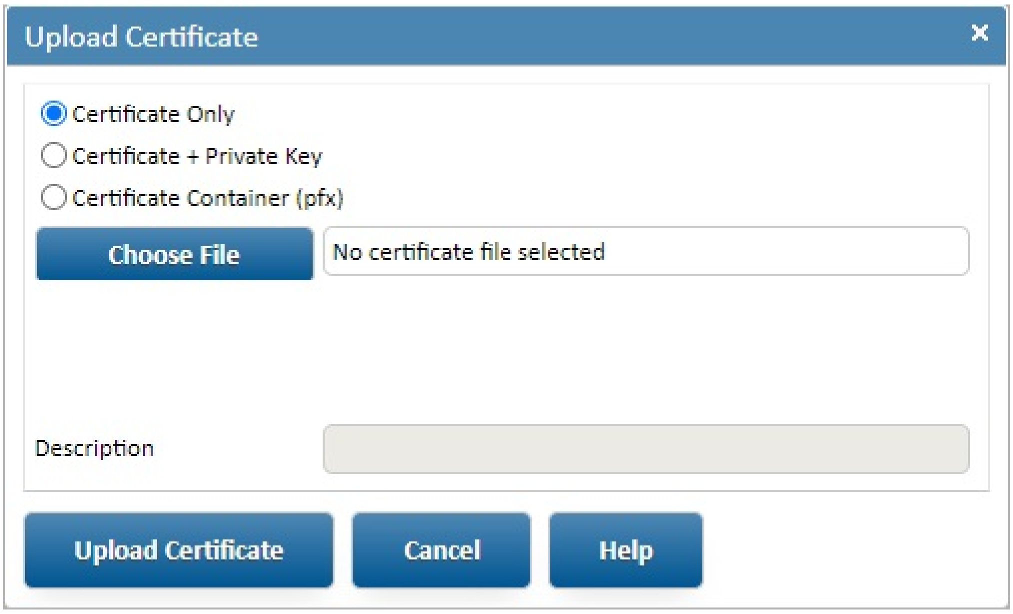
⚠ **The newly generated user certificate is persisted only if the Save button from the Settings page is clicked.**

2. Upload an existing user certificate:

To upload an existing certificate and use it as a user certificate click the **Upload Certificate** ⬆ button and new window will pop up.

There are 3 possible options to upload the certificate, as follows:

- **A. Certificate Only**



Upload Certificate ×

● Certificate Only
○ Certificate + Private Key
○ Certificate Container (pfx)

Choose File | No certificate file selected

Description

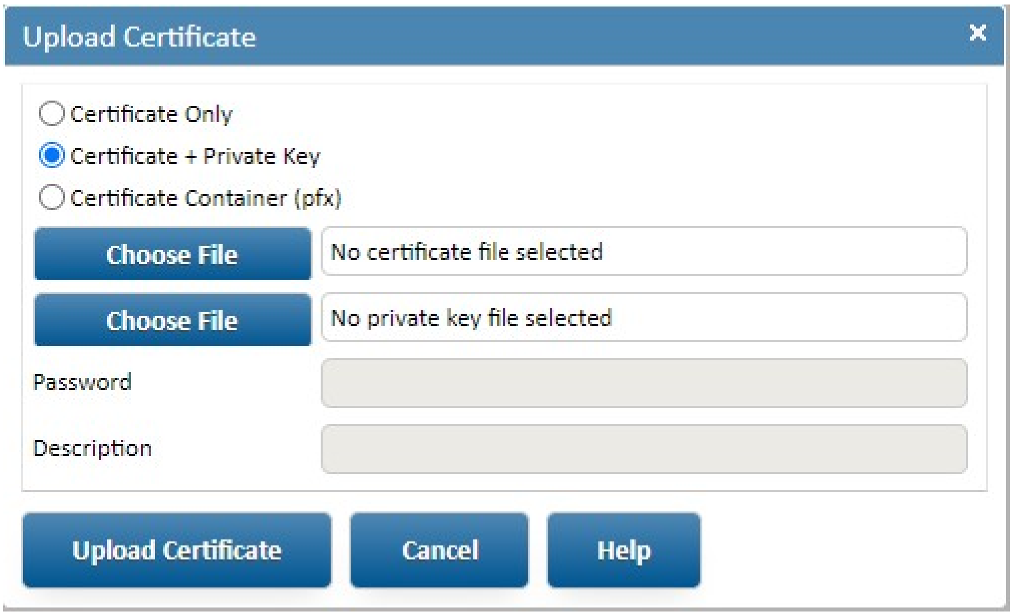
Figure: User & Identities, Upload Certificate, Certificate Only

1. Click the **Choose File** button and select a certificate in DER or PEM format, from the desired location

The **Description** field is used to describe the imported certificate and can be modified at this time as desired. As a consequence a certificate's **Description** can be modified by downloading it (as described at step 3) and uploading it with a different **Description** value, since the previously associated user certificate will be **overwritten** in this case.

2. Click the **Upload Certificate** button to upload the selected certificate (and to overwrite it if an existing user certificate was downloaded and selected in this process).

- **B. Certificate + Private Key**



Upload Certificate

○ Certificate Only
● Certificate + Private Key
○ Certificate Container (pfx)

No certificate file selected

No private key file selected

Password:

Description:

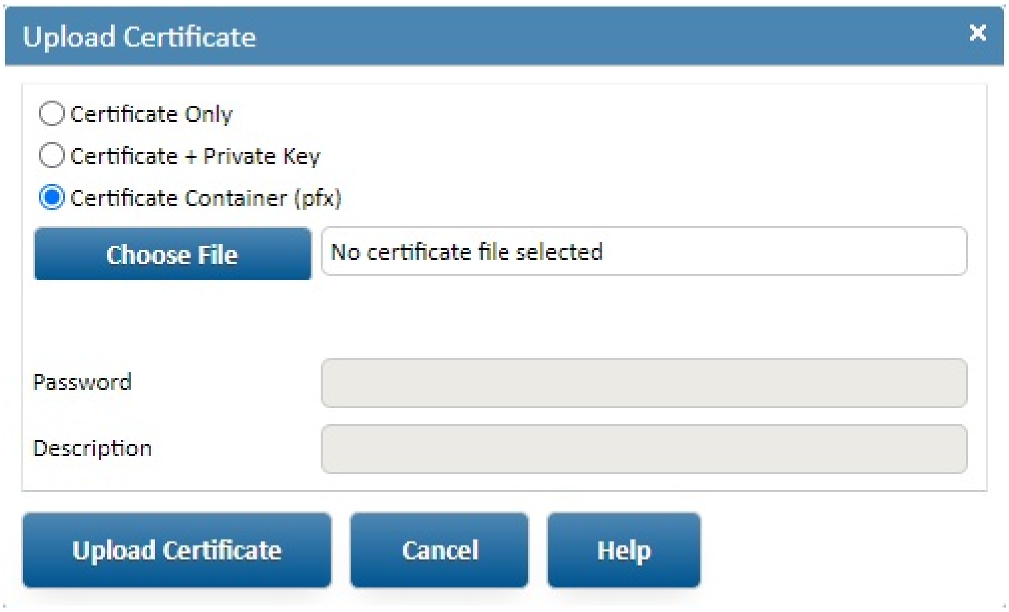
Figure: User & Identities, Upload Certificate, Certificate + Private Key

1. Click the first **Choose File** button and select a certificate in DER or PEM format, from the desired location
2. Click the second **Choose File** button and select the certificate's private key in DER or PEM format, from the desired location

The **Password** field can be used to provide the certificate's private key password, if it is the case.

The **Description** field is used to describe the imported certificate and can be modified at this time as desired. As a consequence a certificate's **Description** can be modified by downloading it (as described at step 3) and uploading it with a different **Description** value, since the previously associated user certificate will be **overwritten** in this case.

- **C. Certificate Container (pfx)**


Upload Certificate

○ Certificate Only
○ Certificate + Private Key
● Certificate Container (pfx)

Choose File | No certificate file selected

Password

Description

Figure: User & Identities, Upload Certificate, Certificate Container

1. Click the **Choose File** button and select a pfx file, containing both the certificate and the matching private key.

The **Password** field can be used to provide the pfx certificate's password, if it is the case.

The **Description** field is used to describe the imported certificate and can be modified at this time as desired. As a consequence a certificate's **Description** can be modified by downloading it (as described at step 3) and uploading it with a different **Description** value, since the previously associated user certificate will be **overwritten** in this case.

2. Click the **Upload Certificate** button to upload the selected certificate (and to overwrite it if an existing user certificate was downloaded and selected in this process).

The newly uploaded user certificate is persisted only if the Save button from the Settings page is clicked.

The options *Certificate + Private Key* and *Certificate Container* allow uploading a chain of certificates.

If so is the case, all the certificates extracted from the chain will be saved.

3. Download an existing selected user certificate:

To download an existing certificate click **Download Certificate** ⬇ button and the certificate will be downloaded using the web browser's file download default behaviour.

4. Delete an existing selected user certificate:

To delete an existing certificate click **Delete User Certificate** 🗑 button and the certificate will be deleted from the Certificates page but the operation will not be persisted until the Save button from the Settings page is clicked.

The deletion of a user certificate is persisted only if the Save button from the Settings page is clicked.

5. Change an existing selected user certificate Description:

Follow the steps described at **Download an existing selected user certificate** and use the same certificate with changed Description field at the steps described in **Upload an existing user certificate.**

4.5.2.2 User Groups

To change user groups related configuration options navigate to **General Settings -> User & Identity Management -> Groups.** The accessed page shall provide the means for creating new or remove existing user groups.

After creating a new user, it is strongly advised to assign it to a group.

Users of the two, predefined and non removable, standard groups have special permissions:

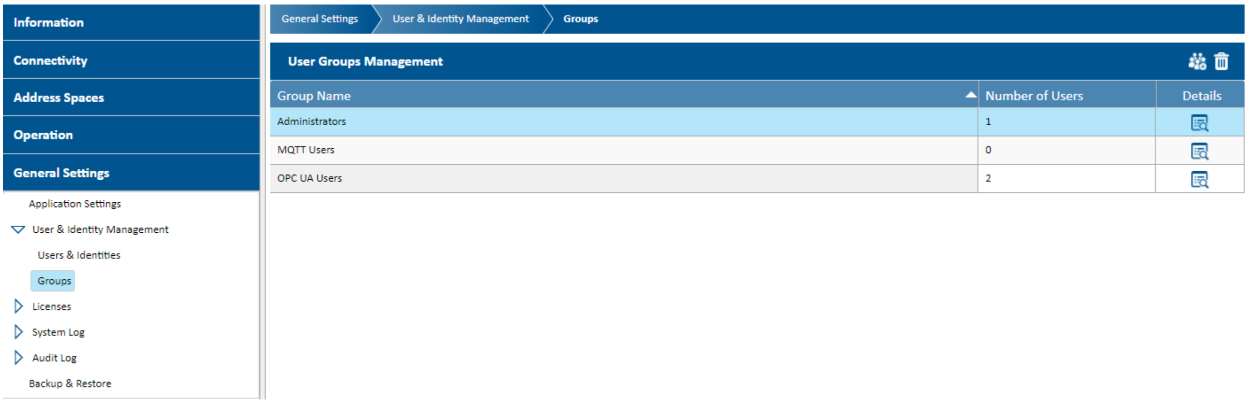
Standard group name	Details
Administrators	Group for users with administrative rights. Only members of this group can access the web interface and perform configuration changes.
OPC UA Users	Group restricted to OPC UA connectivity operations only. Only users members of this group can be assigned as OPC UA server endpoints users.

Table: User & Identities, User Groups

The two standard (predefined) groups: **Administrators** and **OPC UA Users** cannot be deleted.

1. General description

User groups page lists all existing groups as seen bellow:



Information

Connectivity

Address Spaces

Operation

General Settings

- Application Settings
- User & Identity Management
  - Users & Identities
  - Groups
- Licenses
- System Log
- Audit Log
- Backup & Restore

General Settings > User & Identity Management > Groups

User Groups Management

Group Name	Number of Users	Details
Administrators	1	🔍
MQTT Users	0	🔍
OPC UA Users	2	🔍

Groups overview page

Figure: User & Identities, Groups Overview

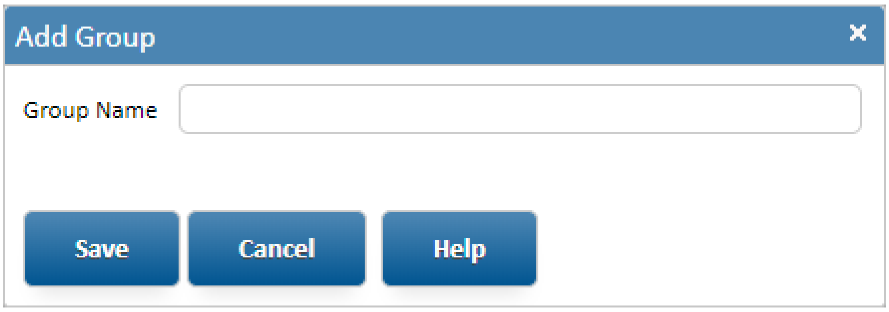
Following actions are possible from this page:

Button	Action
👥	**Add new group.**
🗑	**Delete selected group.**
🔍	**View all users assigned to the group.**

Table: User & Identities, Groups Overview Buttons

2. Add group

To create a new group click the **Add Group** 👥 button and the following pop-up shall be displayed:



Add Group

Group Name

Add new group

Figure: User & Identities, Add Group

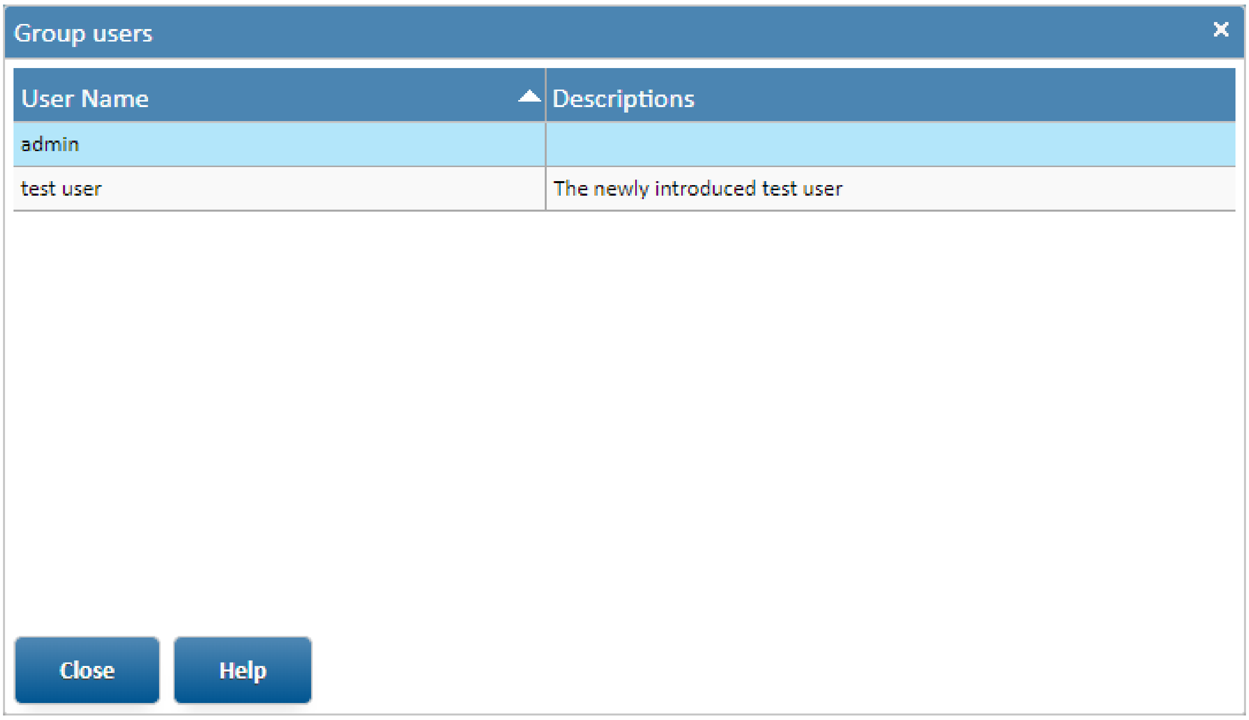
Fill in the desired group name (input validation is performed, while entering not supported character the text box will highlight it) and click the **Save** button.

3. Remove Group

To delete an existing group, select the desired group and click **Delete Group** 🗑. The deleted group will automatically disappear from the groups table.

4. Group Details

To visualize all users assigned to a group, click the **User usage** 🔍 and the following pop-up shall be displayed:



User Name	Descriptions
admin	
test user	The newly introduced test user

Group users detailed information

Figure: User & Identities, Group Users

4.5.2.3 LDAP

Information about the supported LDAP operations and the available application settings.

After changing the LDAP server configuration to one that points to a valid LDAP server that has some users already created, the log in operation in the application will be possible using the LDAP users. Possible cases for log in are:

- using the common name
- using the email
- using the user name (uid, not uidNumber)

User Validation & Fallback mechanism

When an LDAP user is used to log into the application user validation is done. First its credentials are validated in the main server (searched for and then logging in the server with its password). If the user isn't found or its password doesn't match, then the backup server is used for the same checks.

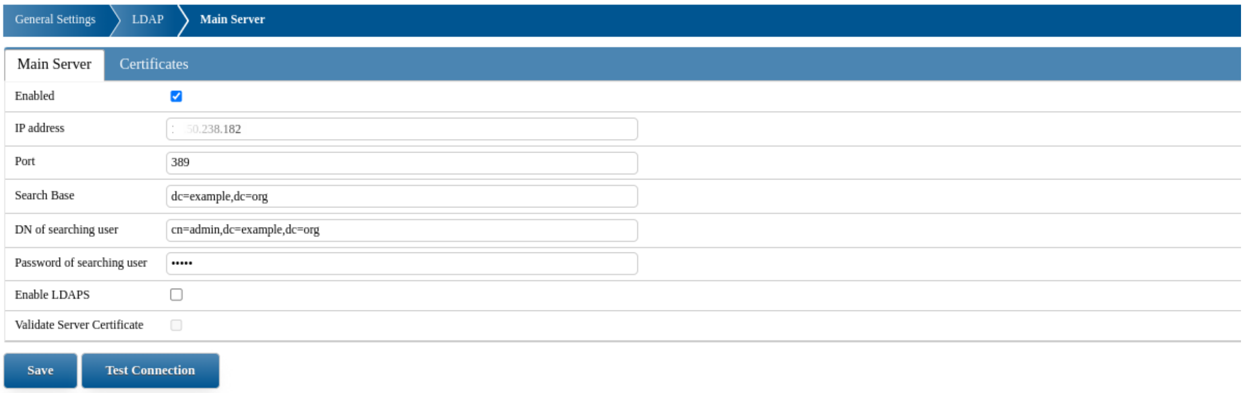
Only the enabled server configurations are used. If neither is enabled, then the logged in user is validated against the applications local users.

4.5.2.3.1 LDAP Server Settings

Configuration Page

The **Main Server and Backup Server** pages shows the settings used by the application to connect to an LDAP server. A main and a backup server can be configured. The server input fields are the same for both servers. If the main server connection fails, the application will try to connect to the backup server, as a fallback mechanism.

Note: The default timeout to a ldap server is 15 seconds. Please make sure you are able to fulfill this condition, otherwise the ldap connection will not be made.



Enabled	☑
IP address	[illegible]50.238.182
Port	389
Search Base	dc=example,dc=org
DN of searching user	cn=admin,dc=example,dc=org
Password of searching user	•••••
Enable LDAPS	☐
Validate Server Certificate	☐

Configuration fields:

- Enabled - checkbox that determines if the setting should be used when attempting to connect to a LDAP server
- IP Address - address of the LDAP server to connect to
- Port - the port that the LDAP server is available at
- Search base - the object in the LDAP under which to search
- DN of searching user - distinguished name representing the querying user
- Password of searching user - the password of the user described by the field above
- Enable LDAPS - checkbox to enable a secure connection to the LDAP server, using client certificates
- Validate Server Certificate - checkbox to enable the validation of the server certificate, using a CA certificate

Certificates Page

This tab enables the upload of a set of client certificates to make the connection to the LDAP server secure.
The upload will allow only specific file formats (PEM + KEY or PFX formats).

Once uploaded a certificate can be deleted or downloaded. Their private keys will be stored encrypted by adding password information, otherwise unencrypted.

To save the uploaded certificates go back to the configuration page and press Save. Otherwise the uploaded certificates will be discarded (same as with the Cancel button) and the previously uploaded ones will be used (if any).

Restrictions:

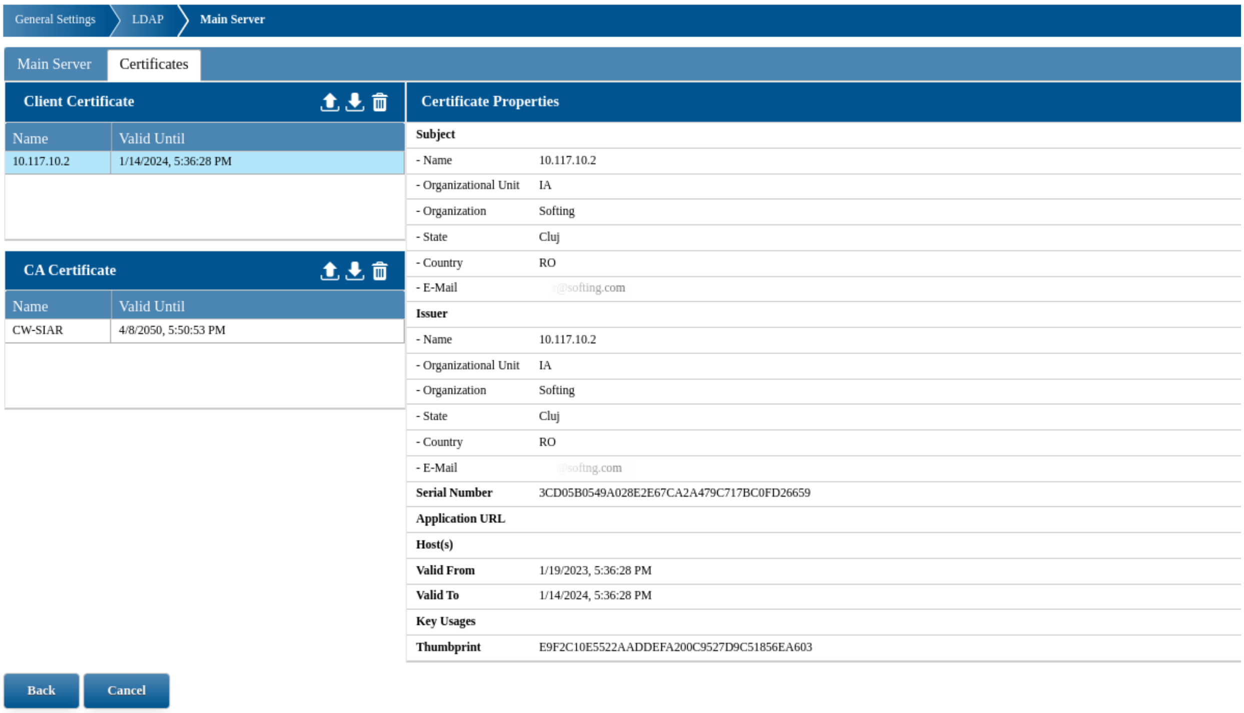
- When checking the **Enable LDAPS** check box on the configuration page, the configuration can only be saved if client certificate has been uploaded. That will be used to connect to the secure server
- When checking the **Enable LDAPS and the** Validate server certificate check box on the configuration page, the configuration can only be saved if a CA certificate has been uploaded. That will be used to validate the Server's own/application certificate

Downloading existing certificates

When downloading the client certificate, select it and press the Download button. This will result in three files being downloaded, a .DER, .PEM and .PFX file (encrypted with the original password, containing the private key as well).

The CA certificate will be donwloaded only in the first two formats.

To view information about a certificate select it in the left side tables.



Client Certificate

Name	Valid Until
10.117.10.2	1/14/2024, 5:36:28 PM

CA Certificate

Name	Valid Until
CW-SIAR	4/8/2050, 5:50:53 PM

Certificate Properties

Subject	
- Name	10.117.10.2
- Organizational Unit	IA
- Organization	Softing
- State	Cluj
- Country	RO
- E-Mail	[redacted]@softing.com
Issuer	
- Name	10.117.10.2
- Organizational Unit	IA
- Organization	Softing
- State	Cluj
- Country	RO
- E-Mail	[redacted]@softng.com
Serial Number	3CD05B0549A028E2E67CA2A479C717BC0FD26659
Application URL	
Host(s)	
Valid From	1/19/2023, 5:36:28 PM
Valid To	1/14/2024, 5:36:28 PM
Key Usages	
Thumbprint	E9F2C10E5522AADDEFA200C9527D9C51856EA603

Available certificate information fields when selecting:

For both Subject and Issuer:

- Name
- Organizational Unit
- Organization
- State
- Country
- E-mail

Other certificate information:

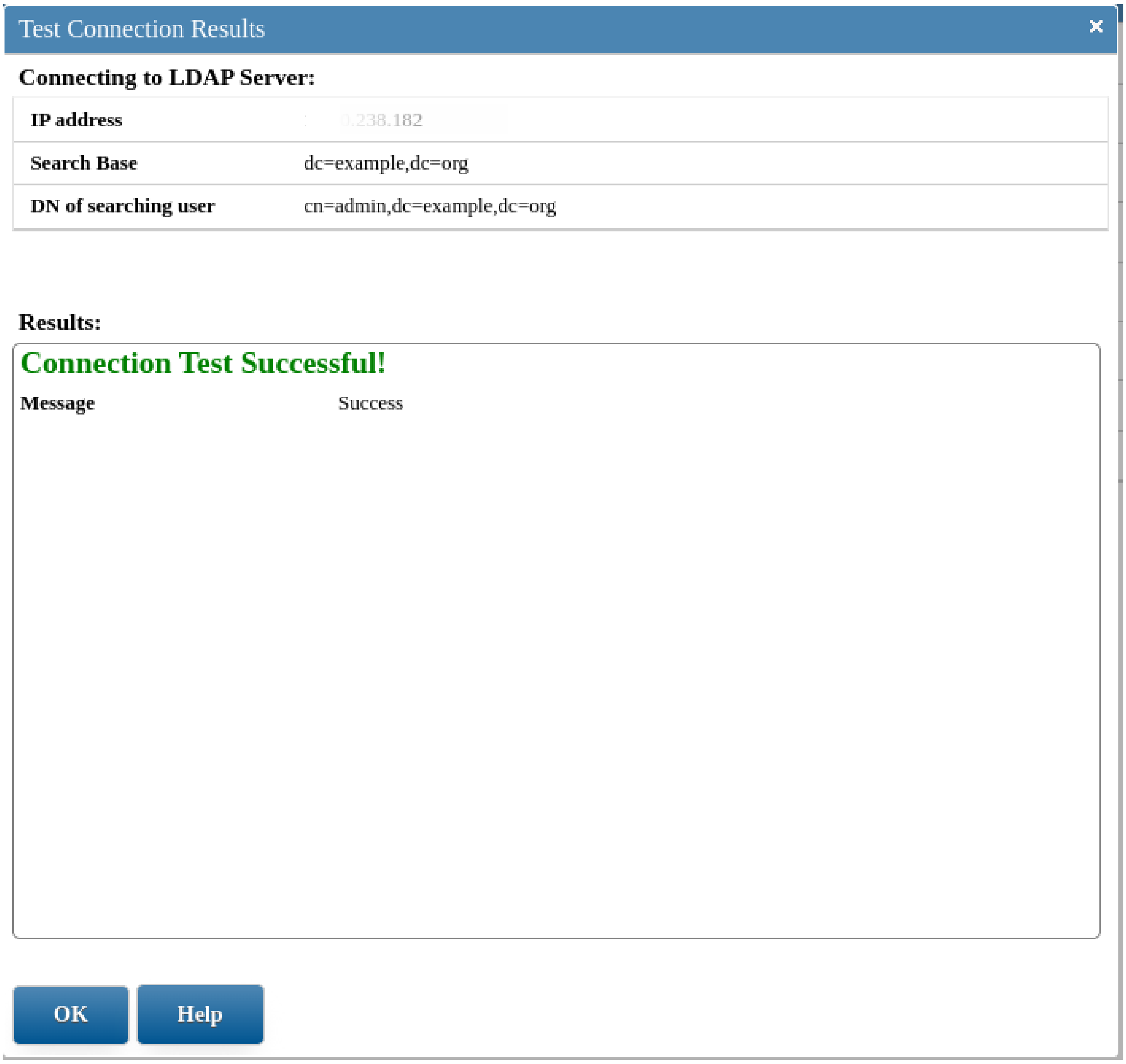
- Serial Number
- Application URL
- Host(s)
- Valid From
- Valid To
- Key Usages
- Thumbprint

4.5.2.3.2 Test Connection

By pressing the test button bellow the configuration a test connection can be made with the values entered in the form. The test can be made without saving the current configuration.

After pressing **Test Connection** the connection will be made with the configuration in the selected tab (e.g. Main Server tab). To test with the configuration made in the other tab it needs to be selected(e.g. Backup server tab).

Successful connection test



Test Connection Results

Connecting to LDAP Server:

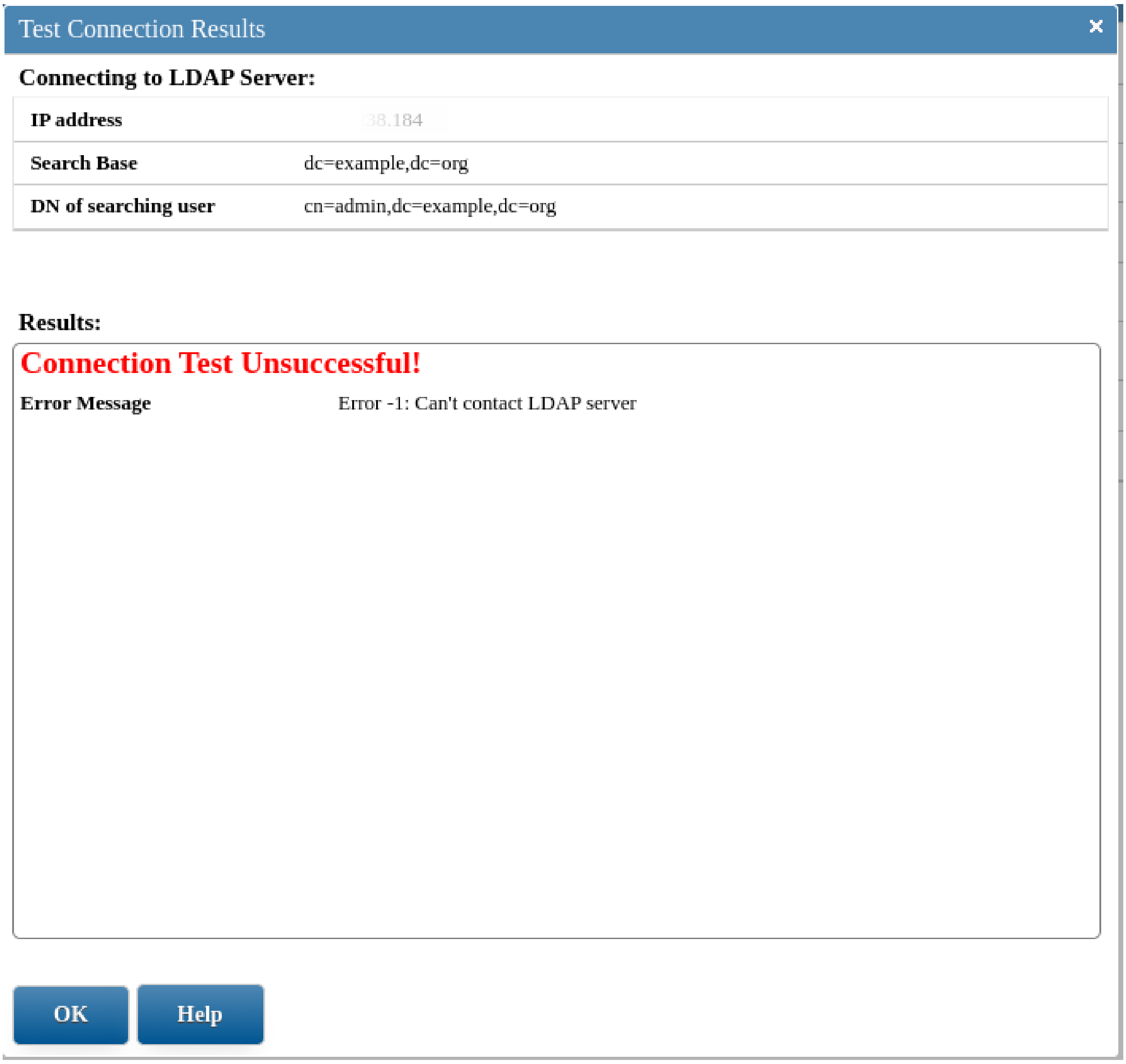
IP address	[redacted].238.182
Search Base	dc=example,dc=org
DN of searching user	cn=admin,dc=example,dc=org

Results:

Connection Test Successful!

Message	Success

The window for an unsuccessful connection will show an error message describing the issue. Depending on the error severity and server behavior more or less information may be provided in the **Error Message** section. Check also server logs for more information, if needed.



Connecting to LDAP Server:

IP address	[redacted]38.184
Search Base	dc=example,dc=org
DN of searching user	cn=admin,dc=example,dc=org

Results:

Connection Test Unsuccessful!

Error Message Error -1: Can't contact LDAP server

4.5.3 Licenses

dataFEED Secure Integration Server can be started and configured without any available or valid licenses installed, however in order to use the OPC UA services a valid license needs to be acquired and activated 58.

dataFEED Secure Integration Server 1.30 allows licenses activation directly in the configuration web interface, using the Licenses Overview 56 page.

Additional license related operations are provided by the Licenses Advanced 58 page.

If no license is installed on the local computer dataFEED Secure Integration Server runs for 72 hours in a limited **demonstration mode**.

All dataFEED Secure Integration Server features are enabled, however the number of *OPC UA Connections* is limited to 10 and the number of *Mapped/Companion Address Spaces* is limited to 5.

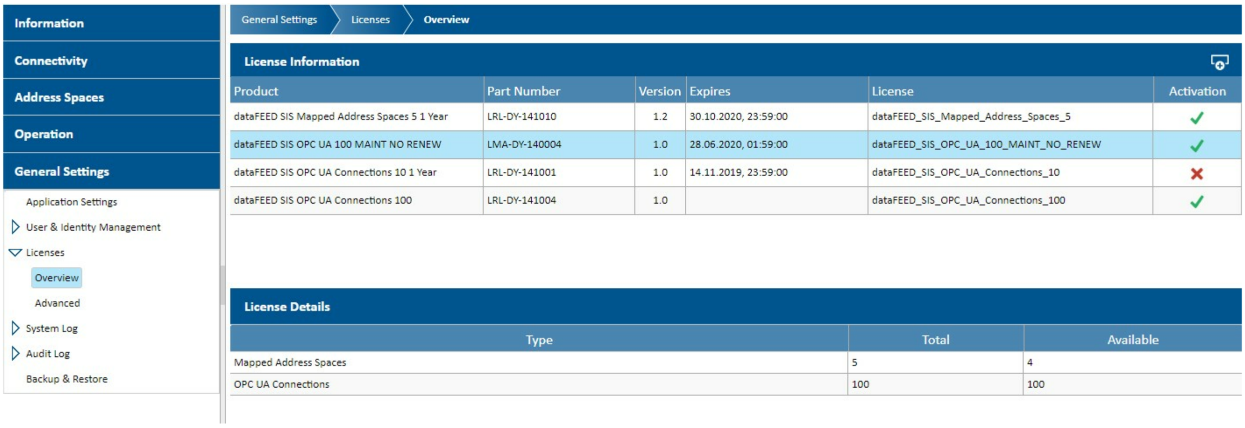
When the demonstration period ends after 72 hours, dataFEED Secure Integration Server stops all functionalities.

Restarting dataFEED Secure Integration Server will start a new 72-hours demonstration period.

- The machine running dataFEED Secure Integration Server 1.30 requires internet connection for license activation.
- Before proceeding, please ensure that you have already purchased a valid license key in the following format: **XXXXX-XXXXX-XXXXX-XXXXX.**
- The demonstration mode is only available if no licenses are installed on the corresponding computer.
- **Installing at least one license key will disable the demonstration mode completely!**

4.5.3.1 Overview

Information about the already licensed features is directly available on the web interface. To access it log into the web interface 24 and navigate to **Licenses->Overview** page.



License Information

Product	Part Number	Version	Expires	License	Activation
dataFEED SIS Mapped Address Spaces 5 1 Year	LRL-DY-141010	1.2	30.10.2020, 23:59:00	dataFEED_SIS_Mapped_Address_Spaces_5	✓
dataFEED SIS OPC UA 100 MAINT NO RENEW	LMA-DY-140004	1.0	28.06.2020, 01:59:00	dataFEED_SIS_OPC_UA_100_MAINT_NO_RENEW	✓
dataFEED SIS OPC UA Connections 10 1 Year	LRL-DY-141001	1.0	14.11.2019, 23:59:00	dataFEED_SIS_OPC_UA_Connections_10	✗
dataFEED SIS OPC UA Connections 100	LRL-DY-141004	1.0		dataFEED_SIS_OPC_UA_Connections_100	✓

License Details

Type	Total	Available
Mapped Address Spaces	5	4
OPC UA Connections	100	100

Figure: Licenses Overview page

There are two views presenting details about the licenses:

1. License Information

Provides the list with the dataFEED Secure Integration Server licenses found on the system; the Activation column is of great interest as it shows the current state of the license:

Symbol	Details
✓	License correctly activated and processed by the running instance of the dataFEED Secure Integration Server.
✗	License not activated. Possible reason are an expired license or an invalid license file.

Table: Licensing activation state

The header of this table provides the **[Add License]** button. Use this button to activate a new license 58.

2. License Details

The information present in this view is refreshed each time the **General Settings -> Licenses** page is loaded and shall reflect the current internal state of the licensed features .

Feature	Details
Type	**OPC UA Connections** - Provides information on the total number of licensed OPC UA connections and the number of connections currently available (either for OPC UA Client Connection or OPC UA Server Endpoints usage). **Mapped Address Spaces** - Provides information on the total number and the number of currently available licensed Mapped/Companion Address Spaces.
Total	The number of license slots provided by the active licenses.
Available	The number of license slots currently available to be used.

Table: License Details

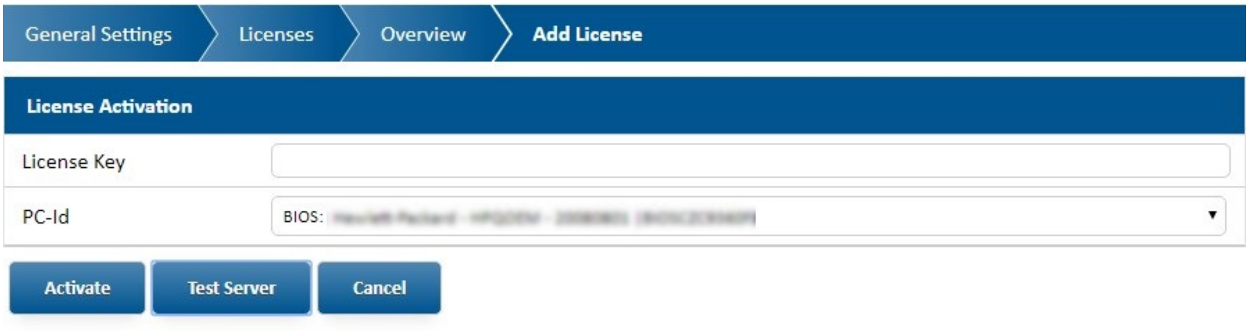
An OPC UA Connection is:

- any connection established by an external OPC UA client to an OPC UA server endpoint defined in the currently running instance of the dataFEED Secure Integration Server
- any successfully created and licensed OPC UA Client Connection in the currently running instance of the dataFEED Secure Integration Server. Please note that the connection does not need to be **Connected** to use a license slot and even if the remote server is not responding or it was misconfigured it will still use a license slot !

A Mapped/Companion Address Spaces:

- can be configured and managed in the *Address Spaces -> Mapped/Companion Address Spaces* configuration page of the dataFEED Secure Integration Server
- uses a license slot as long as it is Active and even if it was not correctly started because it was misconfigured.

4.5.3.2 Activate license



License Activation

License Key	
PC-Id	BIOS: [redacted]

Figure: Activate license

This page provides an easy possibility to activate a new license for dataFEED Secure Integration Server.

The steps needed for this operation are:

1. Fill in the License Key input field with a valid license key (format: XXXXX-XXXXX-XXXXX-XXXXX).

2. Select a PC-Id from the corresponding drop-down list.

3. Click on the **[Activate]** button.

- The machine running dataFEED Secure Integration Server 1.30 requires internet connection for license activation.
- Before proceeding please ensure that you already purchased a valid license key in the foll

Bottom page buttons actions:

Button	Action
Activate	Activate the license key inserted in the corresponding text input filed with the currently selected PC-Id.
Test Server	Test the connection to the Softing licensing server.
Cancel	Cancel the operation and return to the Licenses Overview 56 page.

Table: Activate license

4.5.3.3 Advanced

The **Licenses->Advanced** page provides following collapsible sections, each of them allowing specific operations:

- License Import

- PC-Ids Export
- License Proxy Settings

1. License Import

A valid license file (having extension .lic),previously generated using a correct license key for a PC Id corresponding to the machine the dataFEED Secure Integration Server instance runs on, can be imported using this section.

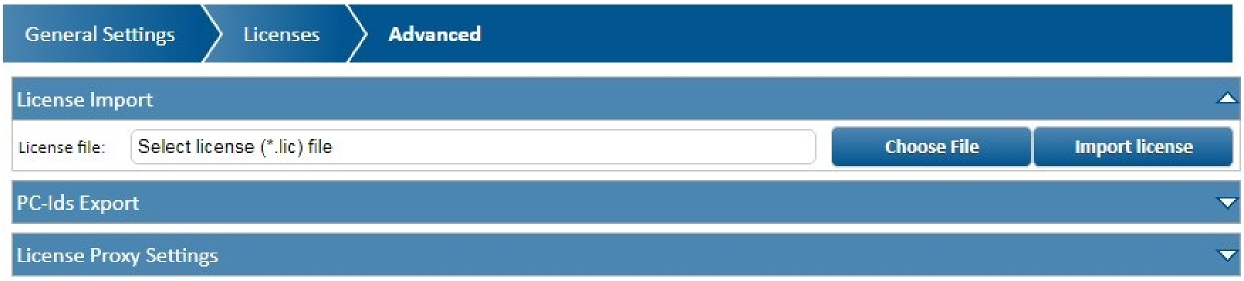


Figure: License import

To perform a license import, follow the steps:

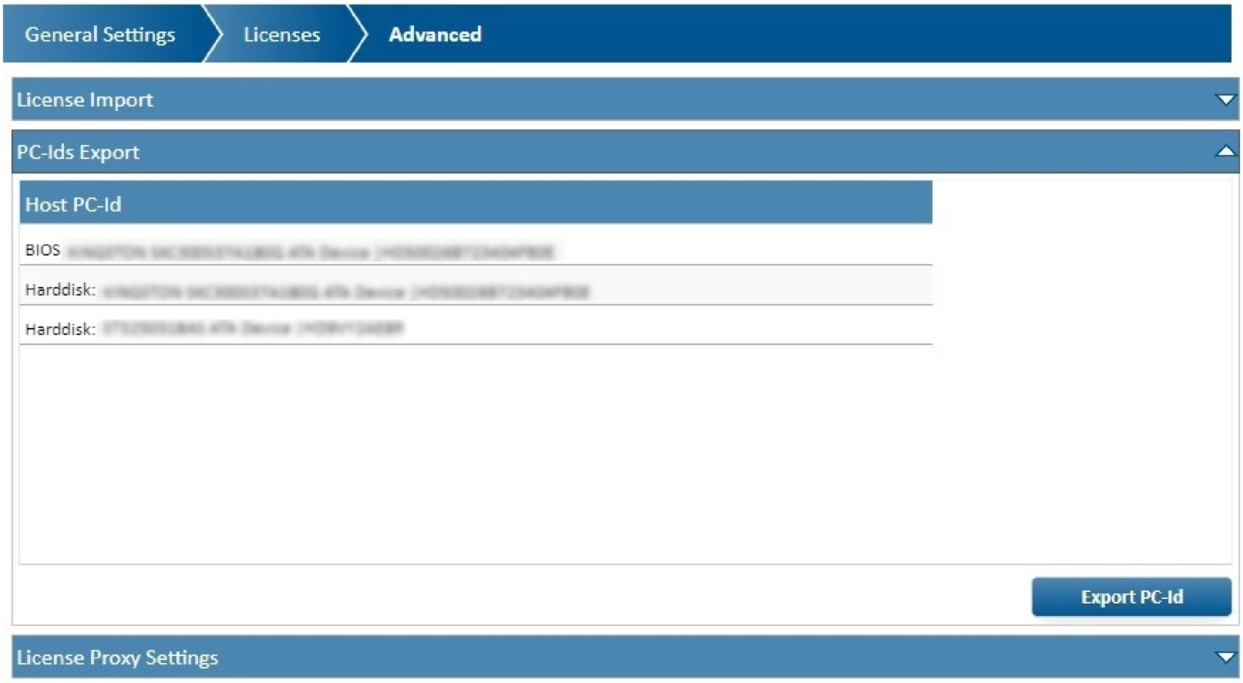
a) Click the **[Choose File]** button and select the the lic file to be imported.

b) Click the **[Import license]** button.

2. PC-Ids Export

This section provides the possibility to retrieve the available PC-Ids of the machine currently running the dataFEED Secure Integration Server instance, with the goal to use them in an remote license activation scenario.

A list with the Ids is presented; the user has the possibility to copy the text from the table or to export the selected PC-Id in a file, selecting the corresponding table row and pressing the **[Export PC-Id]** button.



Host PC-Id

BIOS [redacted]

Harddisk: [redacted]

Harddisk: [redacted]

Figure: PC-Ids export

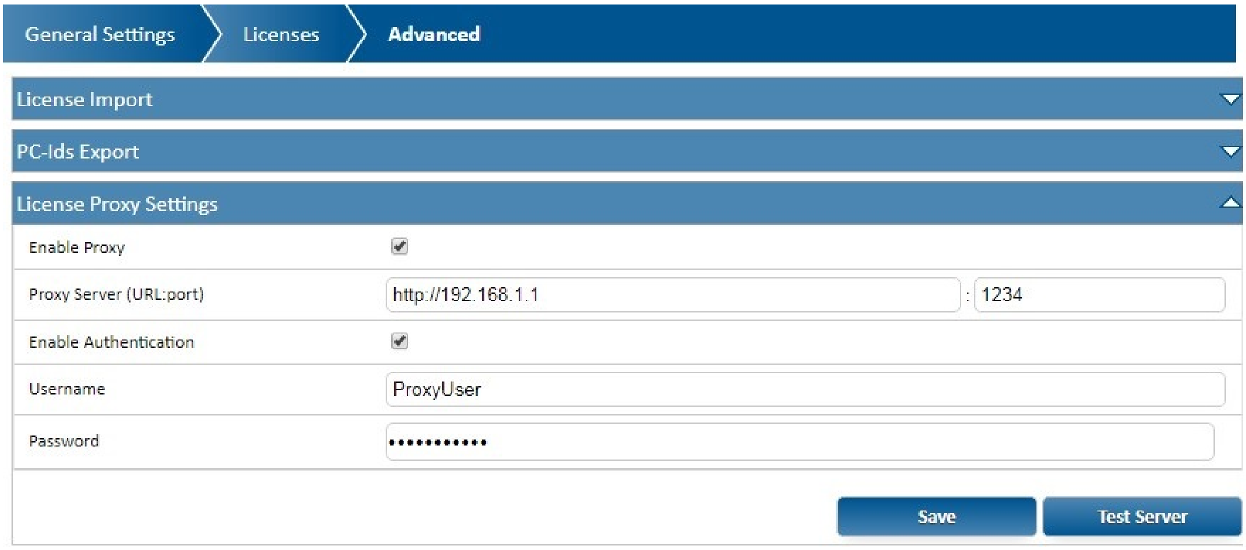
3. License Proxy Settings

This configuration section provides the possibility to specify a proxy to be used when the dataFEED Secure Integration Server instance performs the internet calls towards the Softing license activation server.

Once the needed details are filled in, pressing **[Save]** button will persist the new settings.

Pressing **[Test Server]** button provides an easy way to check if the currently specified settings are valid, by performing a try to access the Softing licensing server.

Note that if the machine running the dataFEED Secure Integration Server instance already specifies a global proxy, it will be automatically used. The settings specified in this section override the global system-wide internet proxy settings.



Enable Proxy ☑

Proxy Server (URL:port) http://192.168.1.1 : 1234

Enable Authentication ☑

Username ProxyUser

Password ••••••••••••

Figure: License proxy settings

4.5.3.4 No Internet Access Licensing

In some cases, due to security or infrastructure reasons, Internet access might not be available on computers running the dataFEED Secure Integration Server; therefore imposing a different approach on activating the provided licenses.

Installing a license for dataFEED Secure Integration Server 1.30 in this case, involves an external standalone tool, the Softing License Manager V4, for licenses activation.

In order for the solution to work it is required to have access to the following:

- a computer with an already installed and running dataFEED Secure Integration Server instance
- Softing License Manager V4 installed on a computer with Internet access
- the previously exported PC-Id files on the computer running the dataFEED Secure Integration Server instance

The following example will guide you step by step to solve the activation issues on a computer without Internet connectivity:

1. Install Softing License Manager V4 on a computer with Internet access

2. Use the web configuration interface to the dataFEED Secure Integration Server instance and export a PC-Id. See Licenses->Advanced->PC-Ids Export 59 section

3. Use the Softing License Manager V4 to *Generate license file for remote PC*

Fill in a valid License Key (in format XXXXX-XXXXX-XXXXX-XXXXX) and the PC-Id (from the step 2 above).

Click on **[Generate and export license file...]** and save the received .lic file.

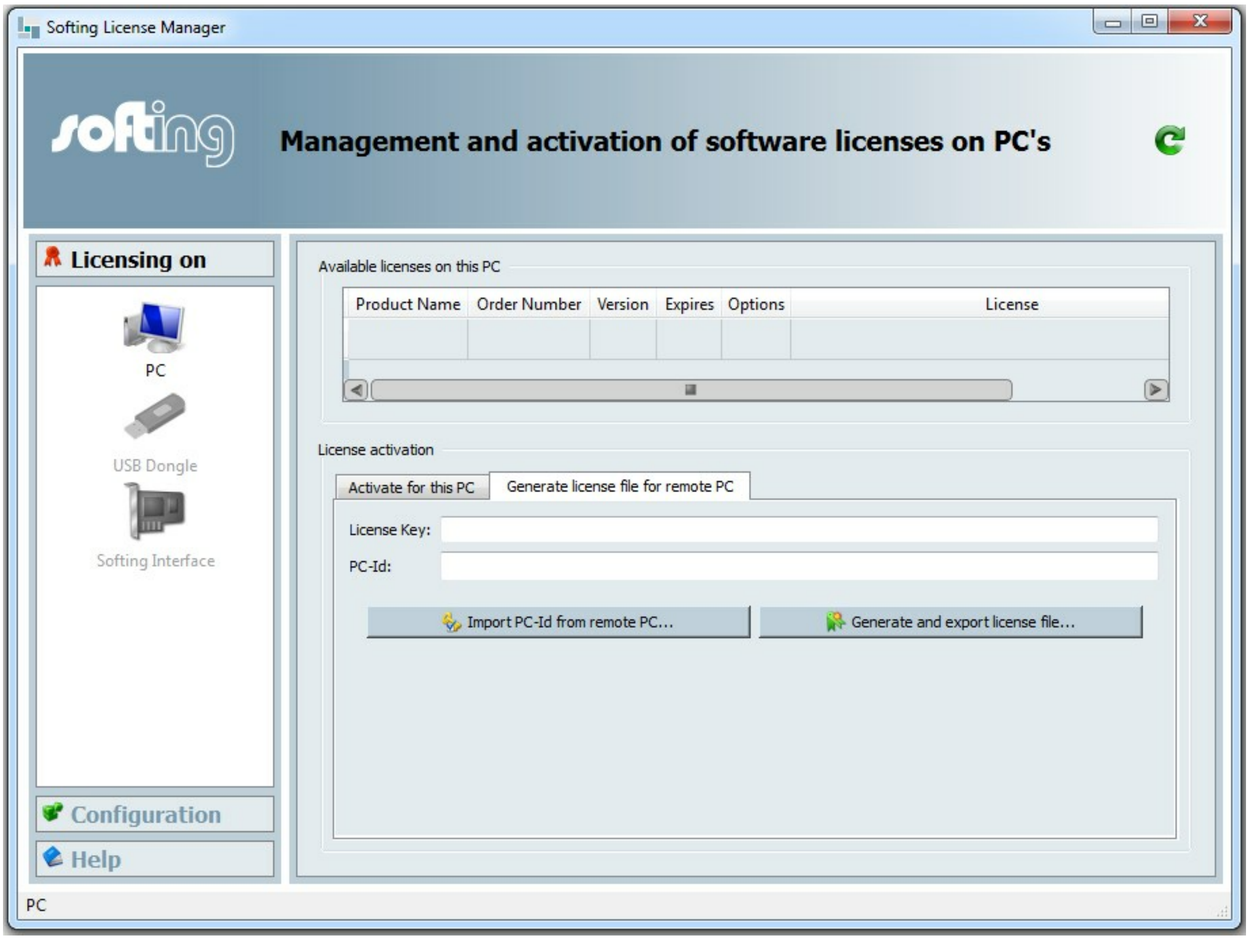


Figure: Generating license file for remote PC using Softing License Manager

4. Use the web configuration interface of the dataFEED Secure Integration Server instance and import the .lic file generated at previous step. See Licenses->Advanced->License Import 59 section.

Once the license file has been successfully imported, a corresponding license feature row shall appear in the *License Information* table of the Licenses->Overview 56 page.

4.5.4 Notifications

This chapter describes the Alert Notifications functionality provided by the dataFEED Secure Integration Server.

dataFEED Secure Integration Server can be configured to generate various Alert Notifications to be sent when events of interest occur during run-time.

This area provides information about how to configure various related settings like: selection of the run-time events which generate Alert Notification, the details of the Alert Events Messages being sent, settings of the Alert Notification communication path, the recipients for the Alert Events, etc.

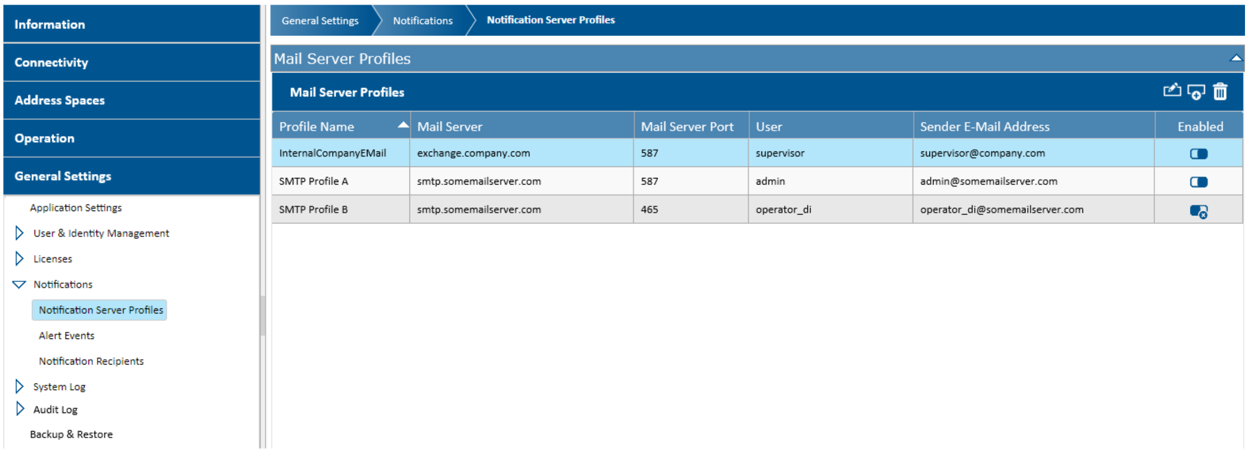
4.5.4.1 Notification Server Profiles

To send Alert Notifications, dataFEED Secure Integration Server requires access to a mail server (SMTP protocol). It is possible to define multiple Notification Server Profiles.

This page is used to manage the Notification Server Profiles, as explained below.

1. Overview

Navigate to **General Settings -> Notifications -> Notification Server Profiles** to access overview page of the the currently configured Mail Server Profiles.



Profile Name	Mail Server	Mail Server Port	User	Sender E-Mail Address	Enabled
InternalCompanyEMail	exchange.company.com	587	supervisor	supervisor@company.com	●
SMTP Profile A	smtp.somemailserver.com	587	admin	admin@somemailserver.com	●
SMTP Profile B	smtp.somemailserver.com	465	operator_di	operator_di@somemailserver.com	⊗

Figure: Notification Server Profiles Overview page

The configured Mail Server Profiles are presented in a table format, each row represents a profile and the information in the table is sortable by clicking the table header. The table header information is described in the following table:

Column name	Information details
Profile Name	Mail Server Profile name as defined at creation time.
Mail Server	The hostname/URL/IP Address of the SMTP server.
Mail Server Port	The port used to communicate with the SMTP server
User	The user name needed to connected to the SMTP server.
Sender E-Mail Address	Email address from which the emails will be sent.
Enabled	Describes the configuration state of the Mail Server Profile. Possible values are **Enabled** ● or **Disabled** ⊗. Note: Clicking on the current configuration state icon would trigger a state toggle:

	• **Enabled** -> **Disabled** • **Disabled** -> **Enabled**

Table: Mail Server Profiles table fields

2. Mail Server Profiles Operations

Mail Server Profiles

Figure: Mail Server Profiles Menu Bar

The **Mail Server Profiles** operations bar provides three buttons with following functionality:

Button	Action
✎	Edit selected Mail Server Profile
⊕	Add a new Mail Server Profile
🗑	Delete selected Mail Server Profile

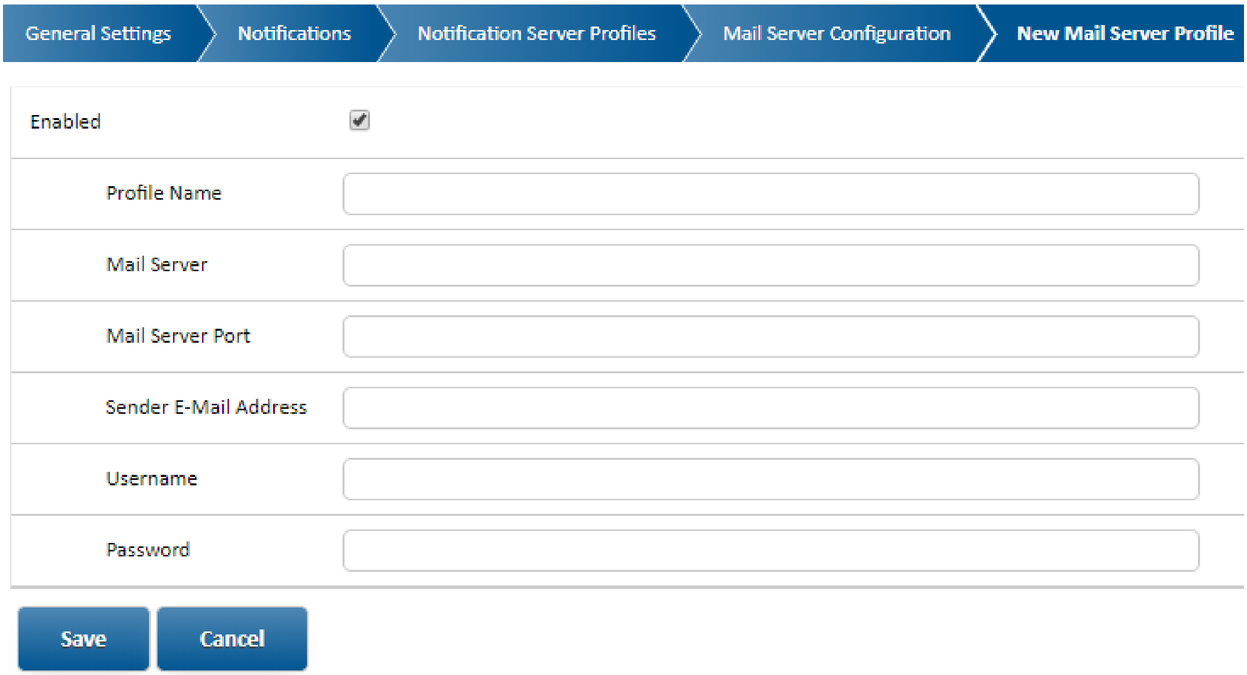
Table: Mail Server Profiles Actions

3. Add/Edit Mail Server Profiles

To create a new Mail Server Profile, navigate to **General Settings -> Notifications -> Notification Server Profiles** and click the **[Add Profile]** ⊕ button on the information bar.

To edit an existing Mail Server Profile, navigate to **General Settings -> Notifications -> Notification Server Profiles** and click the **[Edit Profile]** ✎ button on the information bar.

The following page will be displayed:



General Settings > Notifications > Notification Server Profiles > Mail Server Configuration > **New Mail Server Profile**

Enabled	☑
Profile Name	
Mail Server	
Mail Server Port	
Sender E-Mail Address	
Username	
Password	

Figure: Add new Mail Server Profile

The fields description is presented in the following table:

Column name	Information details
Enabled	The enabled status of the Mail Server Profile. At run-time, the Notifications will be sent over only through the *enabled profiles.*
Profile Name	Mail Server Profile name; it must uniquely identify a Mail Server Profile.
Mail Server	The hostname/URL/IP Address of the SMTP server.
Mail Server Port	The port used to communicate with the SMTP server.
Sender E-Mail Address	Email address from which the emails will be sent.
Username	The username needed to connected to the SMTP server; for some SMTP servers this is an email address.
Password	The password for the username above used to connect to the SMTP server.

Table: Mail Server Profiles fields

Editing an already existent Mail Server Profile is similar to adding, with the remark that the Profile Name cannot be changed.

The creation of a new Mail Server Profile can also be performed directly from the configuration page where a Mail Server Profile can be used at the definition of a Notification Recipient 77.

4. Deleting a Mail Server Profile

To delete a Mail Server Profile, navigate to **General Settings -> Notifications -> Notification Server Profiles** and click the **[Delete Profile]** 🗑 button on the information bar.

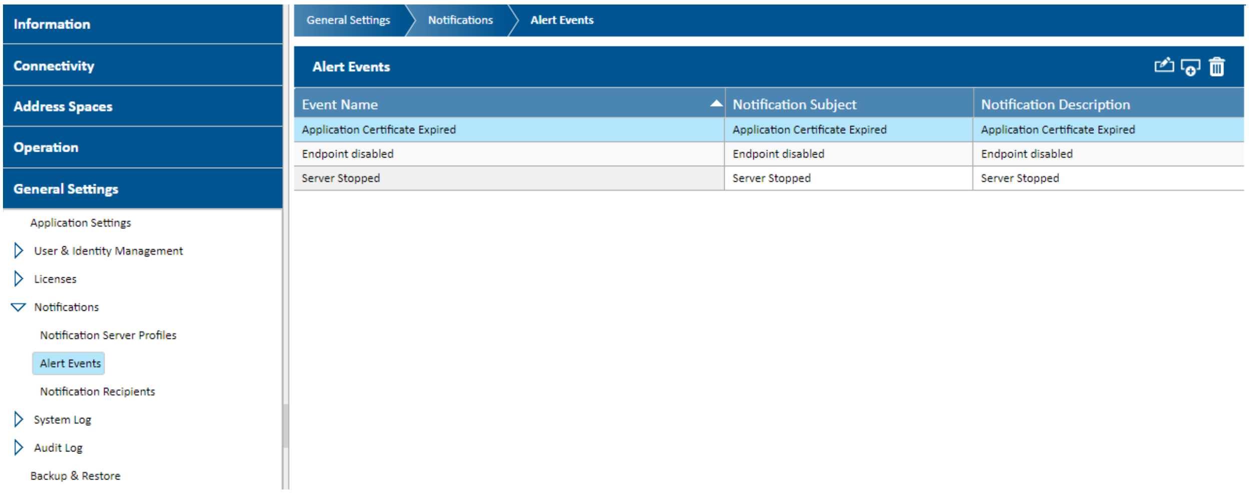
A Mail Server Profile cannot be deleted if it used by a Notification Recipient 72 definition.

4.5.4.2 Alert Events

This configuration section provides the possibility to select from a predefined list, events which generate Alert Events and configure the details of the Notifications being sent.

1. Overview

Navigate to **General Settings -> Notifications -> Alert Events** to access the overview page of the currently configured Alert Events. The default configuration is empty, therefore no Alert Events will be shown. A pre-populated sample of the Alert Events overview is pictured below:



Event Name	Notification Subject	Notification Description
Application Certificate Expired	Application Certificate Expired	Application Certificate Expired
Endpoint disabled	Endpoint disabled	Endpoint disabled
Server Stopped	Server Stopped	Server Stopped

Figure: Alert Events Overview

The Alert Events are presented in a table format, each row represents an Alert Event and the information in the table is sortable by clicking the table header. The table header information is described in the following table:

Column name	Information details
Event Name	Alert Event name as defined at creation time (unique).
Notification Subject	Alert Notification Subject, user defined, max 64 characters.
Notification Description	Alert Notification Description,user defined, max 128 characters.

Table: Alert Events table fields

From this page, the following actions can be initiated:

The Alert Events menu icons trigger by **single-click** the following actions:

Button	Action
⊕	**Add Alert Event**
✎	**Edit existing Alert Event**
🗑	**Delete existing Alert Event**

Table: Alert Events actions

2. Typical use cases

1. Add a new Alert Notification

This use case can be performed by the following steps:

1. Click **Add Alert Event** button and the Alert Event page 69 will be displayed

2. Fill in the fields as described in the Alert Events Settings page 69

2. Change Alert Events configuration parameters

This use case can be performed by the following steps:

1. Click **Edit Alert Event** button while the desired Alert Event row is selected or double-click the row corresponding to the desired Alert Event and the edit Alert Event page 71 will be displayed

2. Change the fields as described in the Alert Events Settings page 69

3. Delete existing Alert Event

This use case can be performed by the following steps:

1. Click the row corresponding to the desired Alert Event and the row shall be selected as a result

2. Click **Delete Alert Event** button

⚠ An Alert Event cannot be deleted if it used by a Notification Recipient 72 definition.

4.5.4.2.1 Alert Events Settings

1. Settings for an Alert Event:

The Alert Events settings page enables the parametrization of an Alert Events and can be accessed in the following contexts:

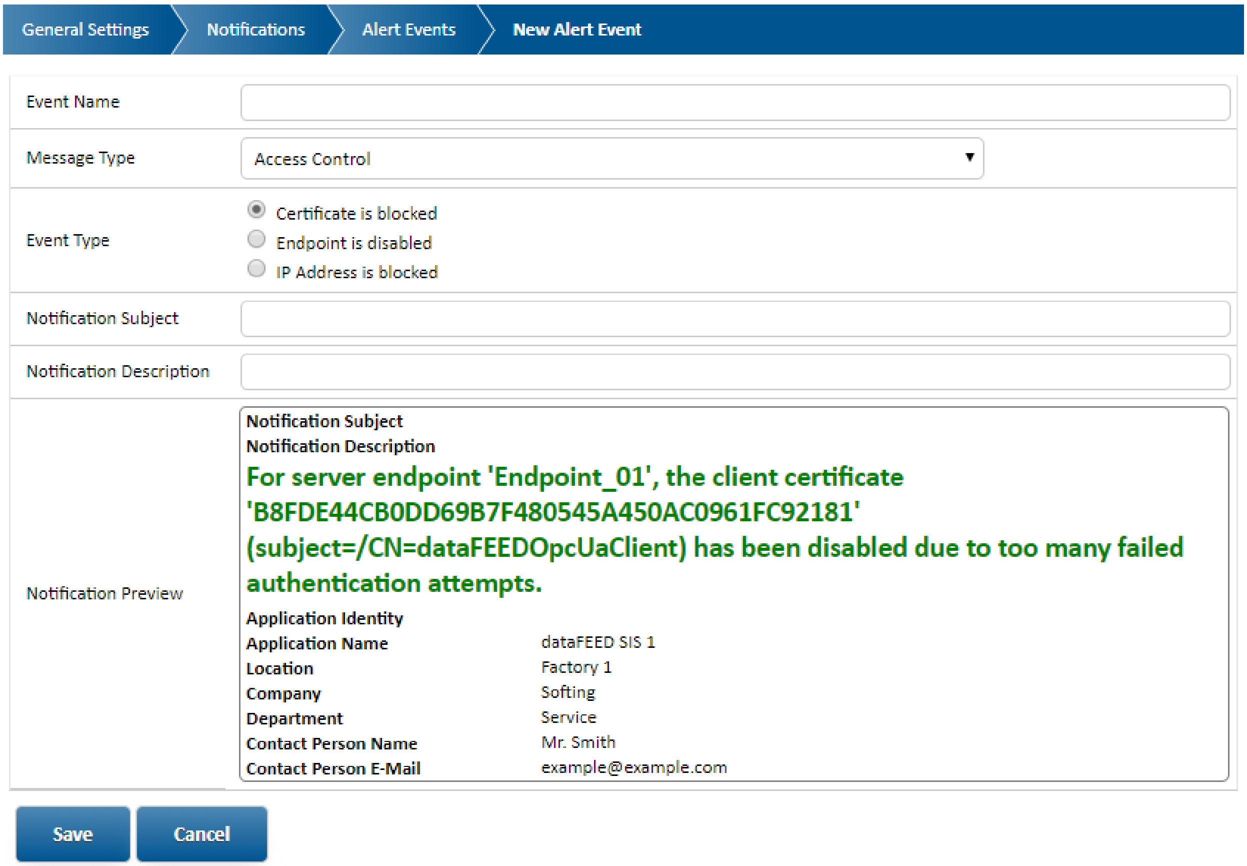
1. Through the **General Settings -> Notifications -> Alert Events -> Add Alert Event** button 67

This is the **main** designed direct path to manage Notification Recipients in the dataFEED Secure Integration Server

2. Through the Notification Recipients Settings page 77, at the time a Notification Recipient is created/edited.

2. Settings for a New Alert Event:

When a new Alert Event is added the following settings page is displayed:



Event Name	
Message Type	Access Control ▾
Event Type	● Certificate is blocked ○ Endpoint is disabled ○ IP Address is blocked
Notification Subject	
Notification Description	
Notification Preview	**Notification Subject** **Notification Description** **For server endpoint 'Endpoint_01', the client certificate 'B8FDE44CB0DD69B7F480545A450AC0961FC92181' (subject=/CN=dataFEEDOpcUaClient) has been disabled due to too many failed authentication attempts.** **Application Identity** **Application Name** dataFEED SIS 1 **Location** Factory 1 **Company** Softing **Department** Service **Contact Person Name** Mr. Smith **Contact Person E-Mail** example@example.com

Figure: New Alert Event settings page

3. Alert Event fields description:

Parameter name	Mandatory	Details
Event Name	YES	The unique Event name which identifies the alert event in the dataFEED Secure Integration Server instance. See warning Figure: Alert Event already exists 71

Message Type	YES	The message type is predefined drop-down list with the existing configured events: - event list can not be modified from the user interface. - by default the first event in the list is selected. - the value of this field will be automatically displayed in the Notification Preview.
Event Type	YES	Radio buttons list with the existing configured events. The user can select the Event Type that will trigger the Notification Alert: - by default the first button in the list is selected. - the value of this field will be automatically displayed in the Notification Preview.
Notification Subject	YES	The subject of the notification message.
Notification Description	YES	The description of the notification message.
Notification Preview	YES	This field is automatically prepopulated with values set in previous fields. It provides a sample of the notification which will be sent at run-time, based on the selection and input of the user.

Table: Alert Event Settings

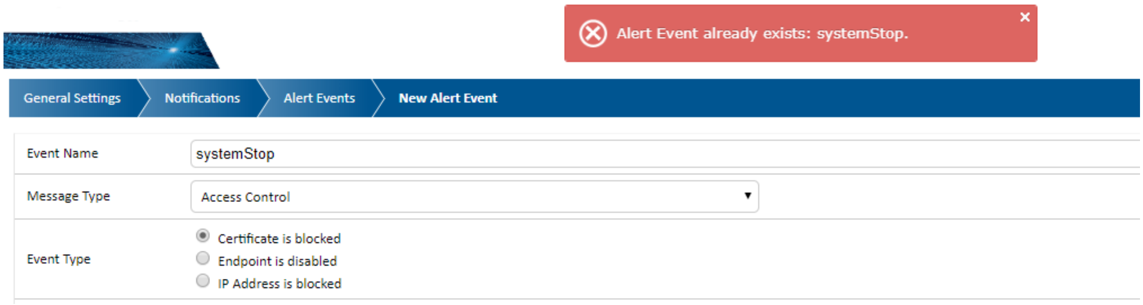
4. Typical use cases:

1. Quick Alert Event setup

By providing the values for the mandatory fields an Alert Event can be easily inserted into the dataFEED Secure Integration Server instance.

Once created the Alert Event can be used to send notifications about system events that are configured in the system:

Ensure that the **Alert Event Name** value is not already in use, otherwise the following message will be presented when Save button is pressed:



Alert Event already exists: systemStop.

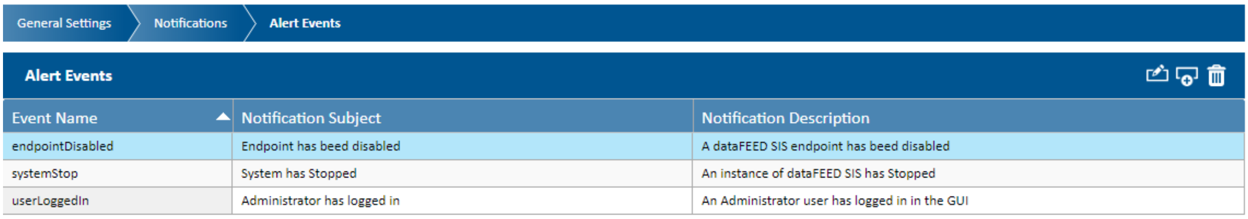
Event Name: systemStop

Message Type: Access Control

Event Type:
● Certificate is blocked
○ Endpoint is disabled
○ IP Address is blocked

Figure: Alert Event already exists

The New Alert Event adding step is completed when the **Save** button action completes and the page context switches back to the **Alert Events** page:

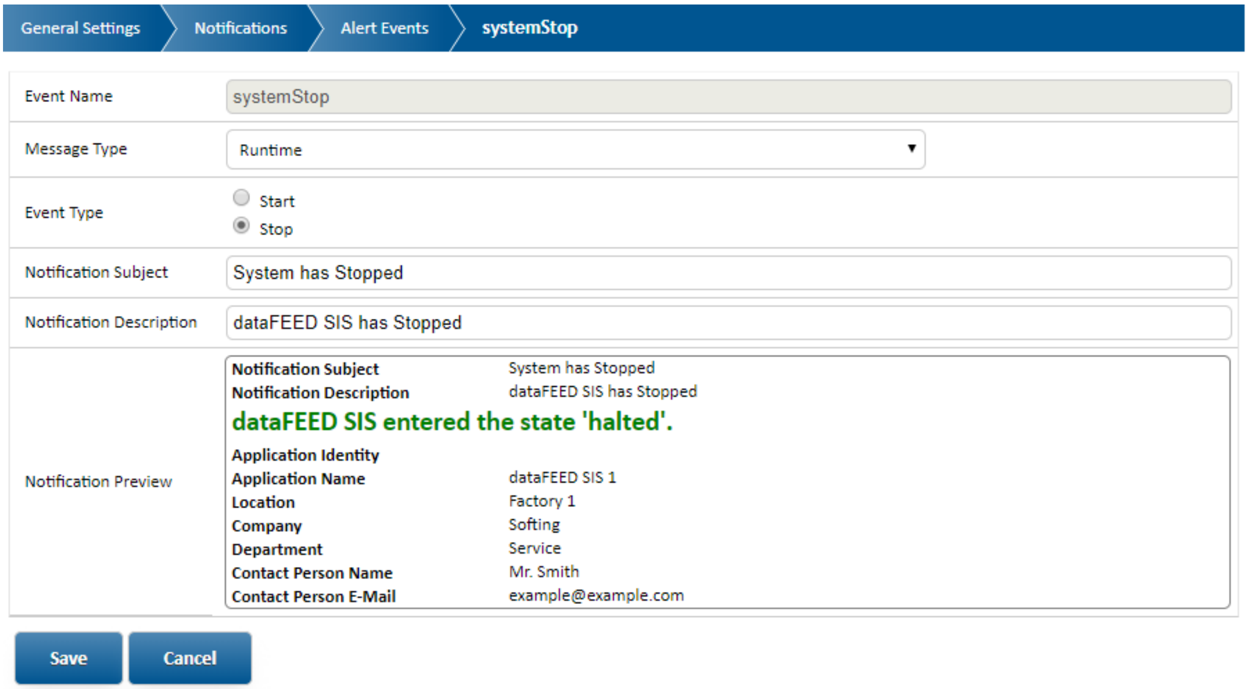


Event Name	Notification Subject	Notification Description
endpointDisabled	Endpoint has beed disabled	A dataFEED SIS endpoint has beed disabled
systemStop	System has Stopped	An instance of dataFEED SIS has Stopped
userLoggedIn	Administrator has logged in	An Administrator user has logged in in the GUI

Figure: New Alert Events is added

5. Settings for an existing Alert Event:

When an existing Alert Event settings are modified, the following settings page is displayed:



Event Name	systemStop
Message Type	Runtime
Event Type	○ Start ● Stop
Notification Subject	System has Stopped
Notification Description	dataFEED SIS has Stopped

Notification Preview

Notification Subject	System has Stopped
Notification Description	dataFEED SIS has Stopped

dataFEED SIS entered the state 'halted'.

Application Identity	
Application Name	dataFEED SIS 1
Location	Factory 1
Company	Softing
Department	Service
Contact Person Name	Mr. Smith
Contact Person E-Mail	example@example.com

Figure: Edit Alert Events settings page

The presented fields are identical with the fields from Figure: Settings for New Alert Event 69, except that the "Event Name" is now grayed out and can not be modified.

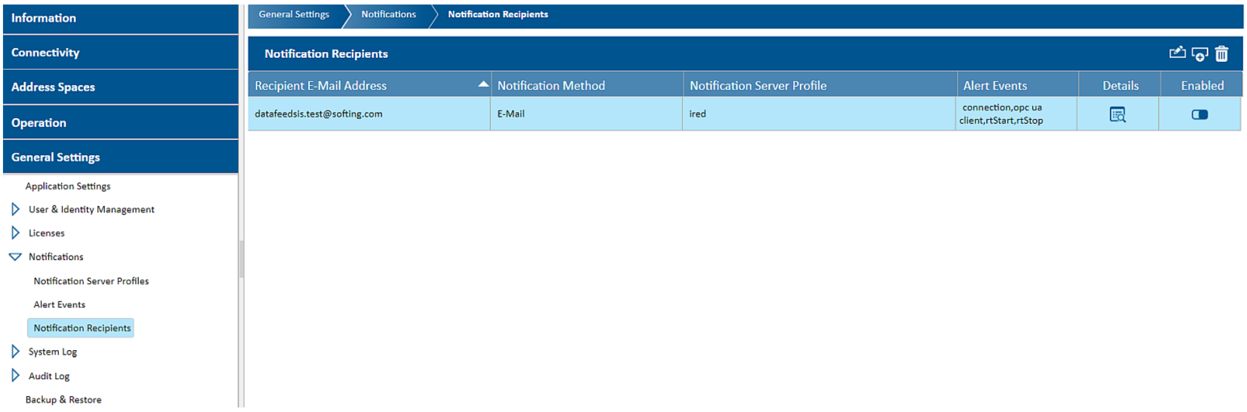
4.5.4.3 Notification Recipients

This page is the final step in configuring a Notification Recipient. In this section the user will link all previously set up components into a ready to use Notification by selecting a: Recipient E-Mail Address, a Notification Server Profile and one or more Alert Events.

Once this step is completed any one of the configured Alert Events will trigger and E-Mail Notification to be sent.

1. Overview

Navigate to **General Settings -> Notifications -> Notification Recipients** to access the overview page of the currently configured Notification Recipients. The default configuration is empty, therefore no Notification Recipients will be shown. A pre-populated sample of the Notification Recipients overview is pictured below:



Notification Recipients

Recipient E-Mail Address	Notification Method	Notification Server Profile	Alert Events	Details	Enabled
datafeedsis.test@softing.com	E-Mail	ired	connection,opc ua client,rtStart,rtStop		

Figure: Notification Recipients Overview page

The Notification Recipients are presented in a table format, each row represents a **Notification Recipient** and the information in the table is sortable by clicking the table header. The table header information is described in the following table:

Column name	Information details
Recipient E-Mail Address	Shows the email address to which the Notification will be sent.
Notification Method	Type of configured delivery method(eg: email) .
Notification Server Profile	Show Mail Server Profile selected for delivery.
Alert Events	Provides a list of selected Alert Events.
Details	Details icon when clicked a Pop-up window with details of the configured Alert Events for the current Notification Recipient.
Enable	Describes the configuration state of the Notification Recipient. Possible values are **Enabled** or **Disabled** . Note: Clicking on the current configuration state icon would trigger a state toggle: • **Enabled** **-> Disabled** • **Disabled** **-> Enabled**

Table: Notification Recipients table fields

From this page, the following actions can be initiated:

The Notification Recipients icons trigger by **single-click** the following actions:

Button	Action
⊕	**Add Notification Recipient**
✎	**Edit existing Notification Recipient**
🗑	**Delete existing Notification Recipient**
🔍	**Details pop-up window**
◐	**Enable/Disable Notification Recipient**

Table: Notification Recipient actions

2. Typical use cases

1. Add a new Notification Recipient

This use case can be performed by the following steps:

1. Click **Add Notification Recipient** ⊕ button and the New Notification Recipient page 76 will be displayed.
2. Fill in the fields as described in the Notification Recipient Settings page 76.

2. Change configuration parameters for exiting Notification Recipient

This use case can be performed by the following steps:

1. Click **Edit Notification Recipient** ✎ button while the desired Notification Recipient row is selected or double-click the row corresponding to the desired Notification Recipient and the Edit Notification Recipient page 77 will be displayed.
2. Change the fields as described in the Notification Recipient Settings page 76.

3. Delete existing Notification Recipient

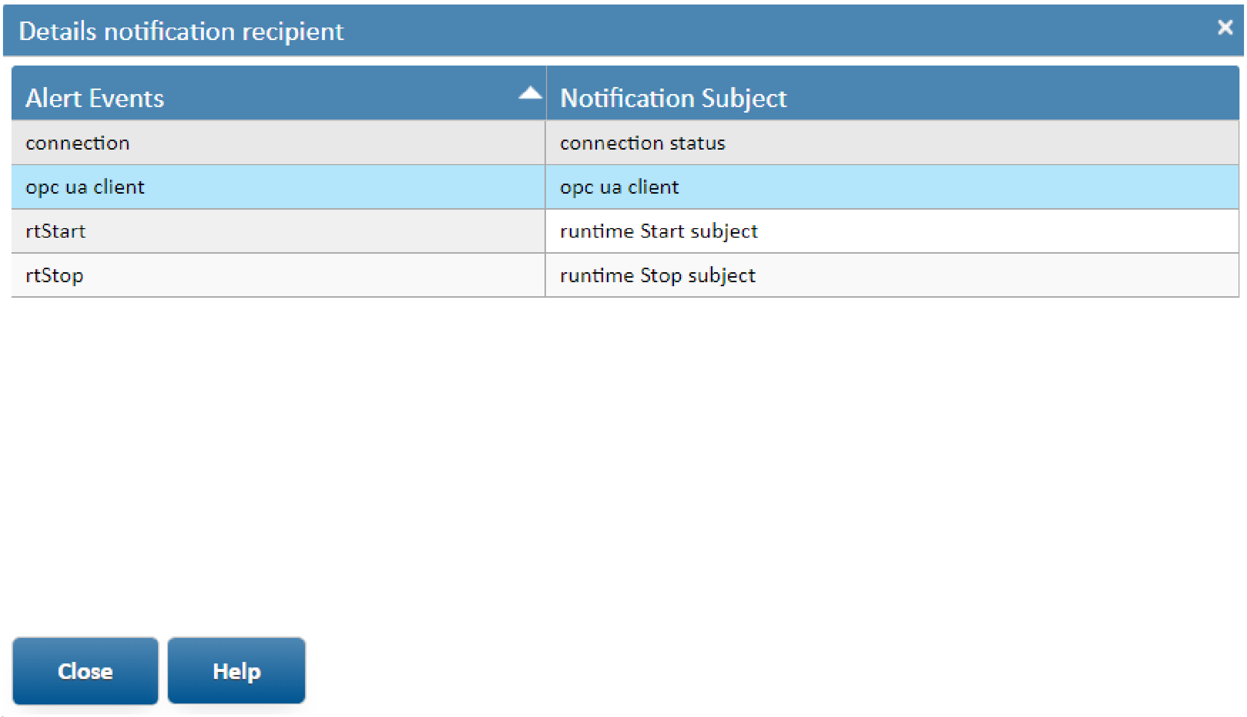
This use case can be performed by the following steps:

1. Click the row corresponding to the desired Notification Recipient and the row shall be selected as a result.

2. Click **Delete Notification Recipient** button and the Notification Recipient will be deleted.

Details notification recipient dialog

To visualize the details of Alert Events that are configured for a Recipient, click the and the following pop-up shall be displayed:



Alert Events	Notification Subject
connection	connection status
opc ua client	opc ua client
rtStart	runtime Start subject
rtStop	runtime Stop subject

Figure: Notification Recipients, Details window

4.5.4.3.1 Notification Recipients Settings

1. Settings for a Notification Recipient:

The Notification Recipient settings page allows the configuration of a notification that will be automatically sent to the recipient once the trigger conditions are met:

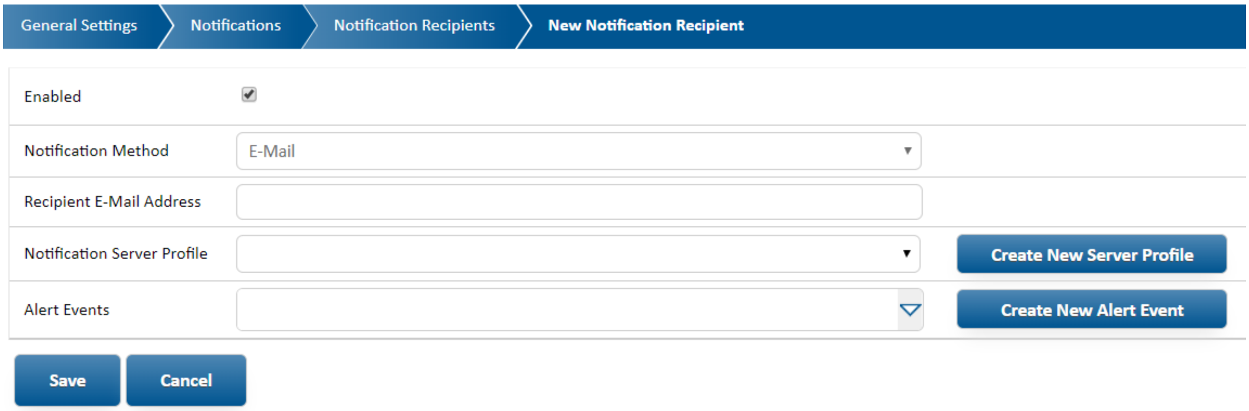
1. Through the **General Settings -> Notifications -> Notification Recipients -> Add Recipient** button 74

This is the **main** designed direct path to manage Alert Events in the dataFEED Secure Integration Server

2. Through editing and existent Notification Recipient

2. Settings for a New Notification Recipient:

When a new Notification Recipient is added the following settings page is displayed:



General Settings > Notifications > Notification Recipients > New Notification Recipient

Enabled ☑

Notification Method: E-Mail

Recipient E-Mail Address:

Notification Server Profile:

Alert Events:

Figure: New Notification Recipient, settings page

3. Notification Recipients fields description:

Parameter name	Mandatory	Details
Enabled	YES	Displays the status of the Notification Recipient
Notification Method	YES	only E-Mail is available
Recipient E-Mail Address	YES	Displays the configured email address of the recipient
Notification Server Profile	YES	Drop down list with Notification Server Profiles available for use
Alert Events	YES	Multiple selection list with Alert Events available for use

Table: Alert Event Settings

From this page, the following actions can be initiated:

The Notification Recipients icons trigger by **single-click** the following actions:

Button	Action
Create New Server Profile	**Create New Server Profile**
Create New Alert Event	**Create New Alert Event**

Table: Notification Recipient actions

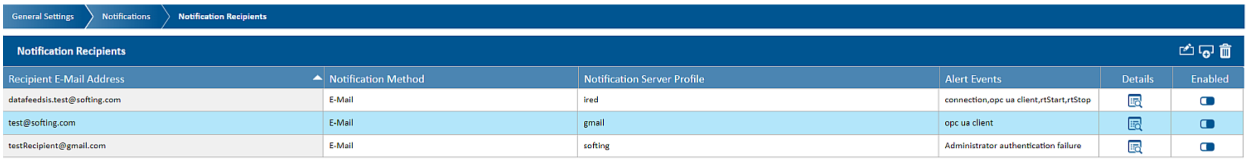
4. Typical use cases:

1. Quick Notification Recipient setup

By providing the values for the mandatory fields an Notification Recipient can be easily inserted into the dataFEED Secure Integration Server instance.

Required components for a notification can be created from configuration, using the **Create New Server Profile** 64 and **Create New Alert Event** 69 buttons.

The New Recipient Notification adding step is completed when the **Save** button action completes and the page context switches back to the **Notification Recipients** overview page:



General Settings > Notifications > Notification Recipients

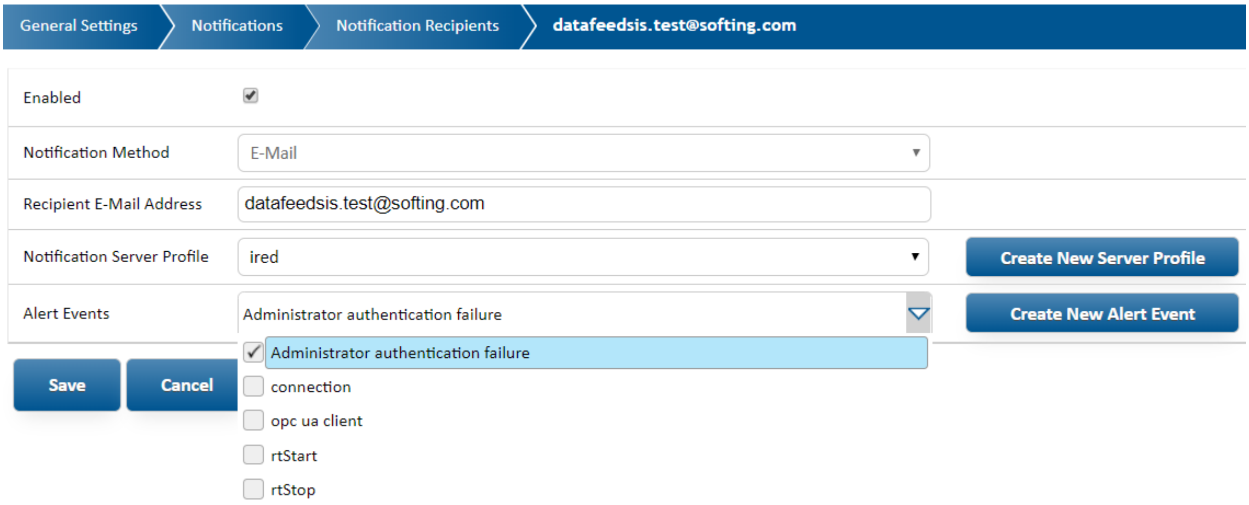
Notification Recipients

Recipient E-Mail Address	Notification Method	Notification Server Profile	Alert Events	Details	Enabled
datafeedsis.test@softing.com	E-Mail	ired	connection,opc ua client,rtStart,rtStop		
test@softing.com	E-Mail	gmail	opc ua client		
testRecipient@gmail.com	E-Mail	softing	Administrator authentication failure		

Figure: New Notification Recipient is added

5. Settings for an existing Alert Event:

When an existing Notification Recipient settings are modified, the following settings page is displayed:



Enabled	☑
Notification Method	E-Mail
Recipient E-Mail Address	datafeedsis.test@softing.com
Notification Server Profile	ired
Alert Events	Administrator authentication failure

☑ Administrator authentication failure
☐ connection
☐ opc ua client
☐ rtStart
☐ rtStop

Figure: Edit Alert Events settings page

The presented fields are identical with the fields from Figure: New Notification Recipient, settings page , except that the "E-Mail" is now grayed out and can not be modified. All other fields can be changed by the user. Step is completed when the **Save** button action completes and the page context switches back to the **Notification Recipients** overview page.

4.5.5 Logging & Metrics

This chapter describes the logging and metrics facility provided by the dataFEED Secure Integration Server.

When multiple software modules operate simultaneously, with complex interactions between modules, processing large amounts of information it is often difficult to determine exactly what is happening
“inside” when something appears not to be operating correctly, or what was happening when problems occur. The logging facility handles the generation, processing and storage of log messages used to identify and troubleshoot such situations.

4.5.5.1 Logging & Metrics

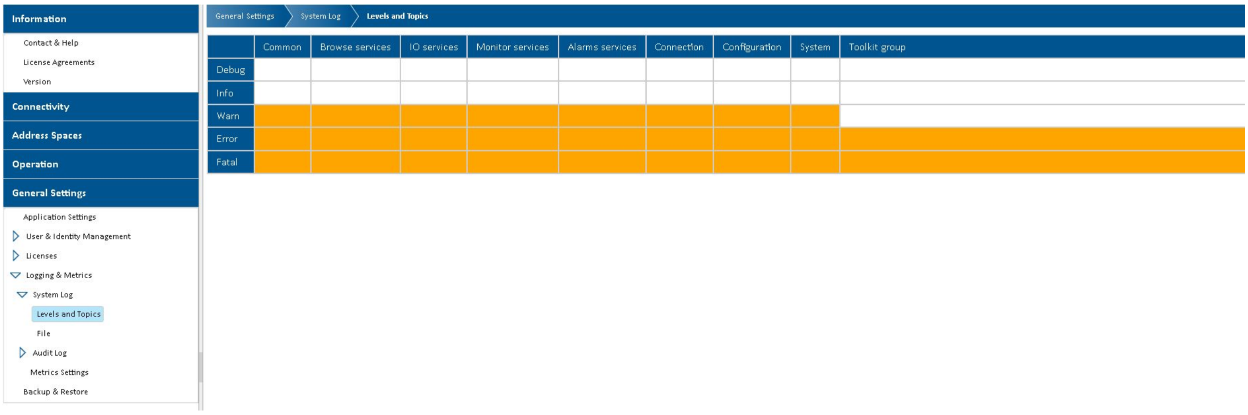
System logging facilities in the dataFEED Secure Integration Server is useful for diagnostics and support. Correctly setting up the logging facilities in a production environment provides improved performance and fast support response times.

4.5.5.1.1 Levels and Topics

The logging mechanism implemented in the dataFEED Secure Integration Server is modular and allows enabling different log severity for each component module.

Change Log Severity

To change the logging severity level for a component navigate to **General Settings -> Logging & Metrics -> System Log -> Levels and Topics.** The logging severity matrix shall provide an easy to use solution to change the severity for each component. Clicking on the cell corresponding to the intersection of a module with the severity level will change the module's severity to the value defined by the row label. The Logging severity matrix is presented below:



	Common	Browse services	IO services	Monitor services	Alarms services	Connection	Configuration	System	Toolkit group
Debug									
Info									
Warn	🟧	🟧	🟧	🟧	🟧	🟧	🟧	🟧	
Error	🟧	🟧	🟧	🟧	🟧	🟧	🟧	🟧	🟧
Fatal	🟧	🟧	🟧	🟧	🟧	🟧	🟧	🟧	🟧

Figure: Logging & Metrics, Change System Log Severity

Logging severity levels are defined in the table below:

Severity	Details
Debug	Highest verbosity. Output log contains development related information. **Activating this severity might impact overall performance therefore it is strongly advised not to activate it unless otherwise instructed by Softing Industrial Automation GmbH support staff.**
Info	High verbosity. Output log contains system behaviour detailed information. **Activating this severity might impact overall performance therefore it is strongly advised not to activate it unless otherwise instructed by Softing Industrial Automation GmbH support staff.**
Warn	Output log contains information which might concern the system user. Warning logs are potential issues and have to be coupled with the system behaviour. **This is the default logging severity.**
Error	Output log contains system operation errors. Error logs have to be analyzed as their presence indicates a potential faulty system behaviour.
Fatal	Output log contains system operation fatal errors. Originators of this type of log information are actions that would typically stop the system due to an error which is unrecoverable.

Table: Logging & Metrics, System Log Severity Fields

4.5.5.1.2 File

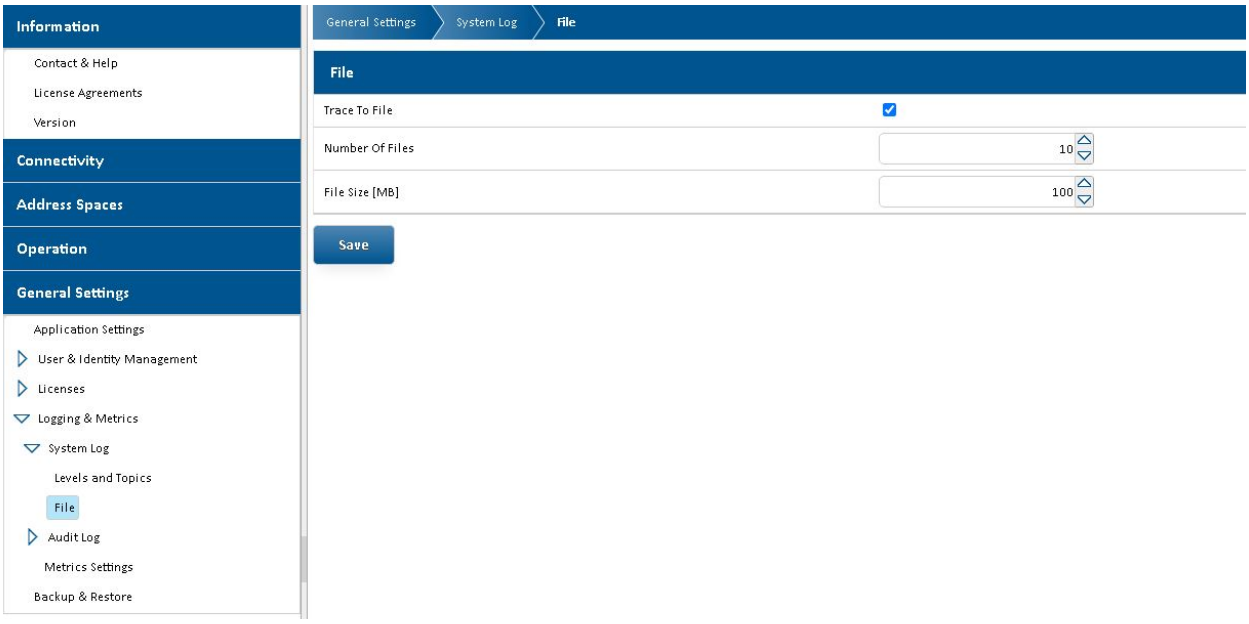
File Settings

A log file rotation solution was implemented in order to reduce the total space required by the logging module. In situations when it might be required to change the default log file settings navigate to **General Settings -> System Log -> File.**

The following options can be adjusted in the system log file configuration page:

Option	Default Value	Details
Trace to File	Enabled	Used to enable or disable system log output to file.
Number of Files	10	Part of the system log file rotate facility. It defines the maximum number of log files to be created. When the limit is surpassed and a new file needs to be created the oldest one shall be discharged (deleted).
File Size	100	Maximum log file size. When the currently used log file reaches the file size the file will be stored (see Number of Files) and logging shall be resumed in a new empty file.

Table: Logging, Log File Settings



File

Trace To File	☑
Number Of Files	10
File Size [MB]	100

Figure: Logging & Metrics, System Log File Page

4.5.5.2 Audit Log

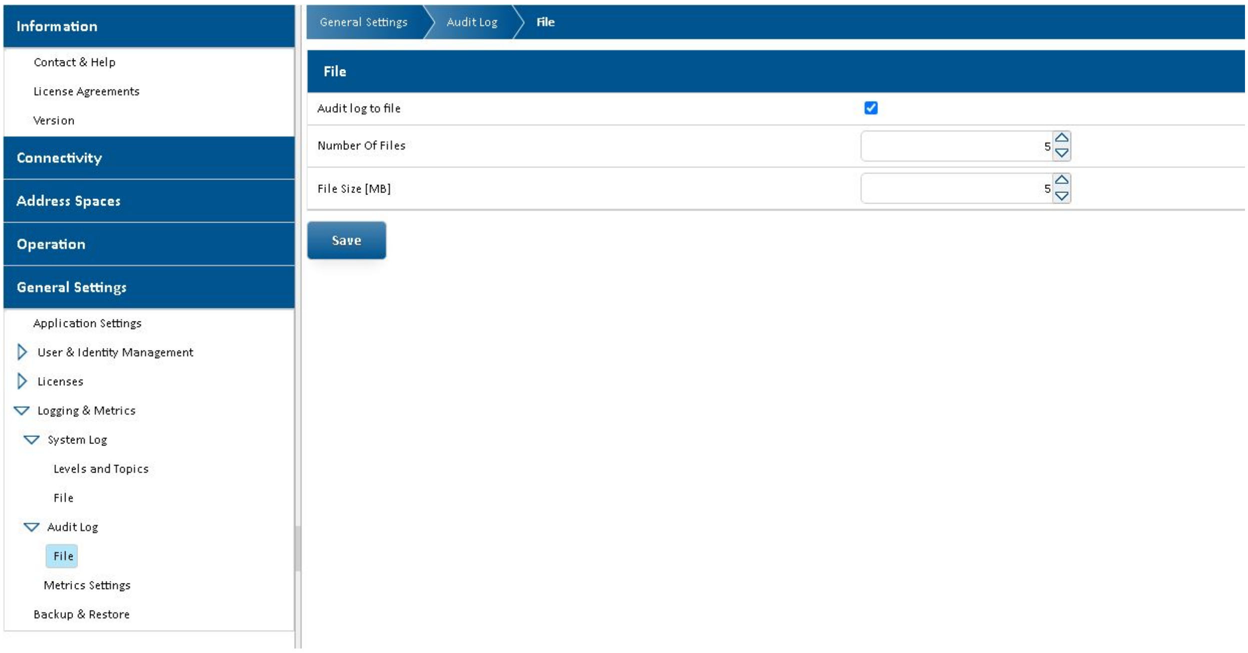
Audit log keeps a trace of all the configuration actions performed from the web interface on the dataFEED Secure Integration Server running instance. To configure the audit log settings navigate to **General Settings -> Logging & Metrics -> Audit Log -> File.**

4.5.5.2.1 File

The following options can be altered in the audit log file configuration page:

Option	Default Value	Details
Audit log to file	Enabled	Used to enable or disable audit log output to file.
Number of Files	5	Part of the audit log file rotate facility. It defines the maximum number of log files to be created. When the limit is surpassed and a new file needs to be created the oldest one shall be discharged (deleted).
File Size	5	Maximum log file size. When the currently used log file reaches the file size the file will be stored (see Number of Files) and logging shall be resumed in a new empty file.

Table: Logging, Audit Log File Settings



File

Audit log to file ☑

Number Of Files 5

File Size [MB] 5

Table: Logging & Metrics, Audit Log File Page

4.5.5.3 Metrics Settings

This chapter provides information about internal system information published to different monitoring solutions.
Currently only Prometheus is supported (See below).

To enable or disable metrics, either use the check box shown in the figure below, or programatically send an HTTP POST request to the **"/runtime/core/metrics-config"** API endpoint of the dataFEED Secure Integration Server.
The request should look like this:

```
curl -X POST -d '{ "enabled": true }' http://<host_name>:<port>/runtime/core/metrics-config
```

to enable, or use '{ "enabled": false }' JSON data to disable it.

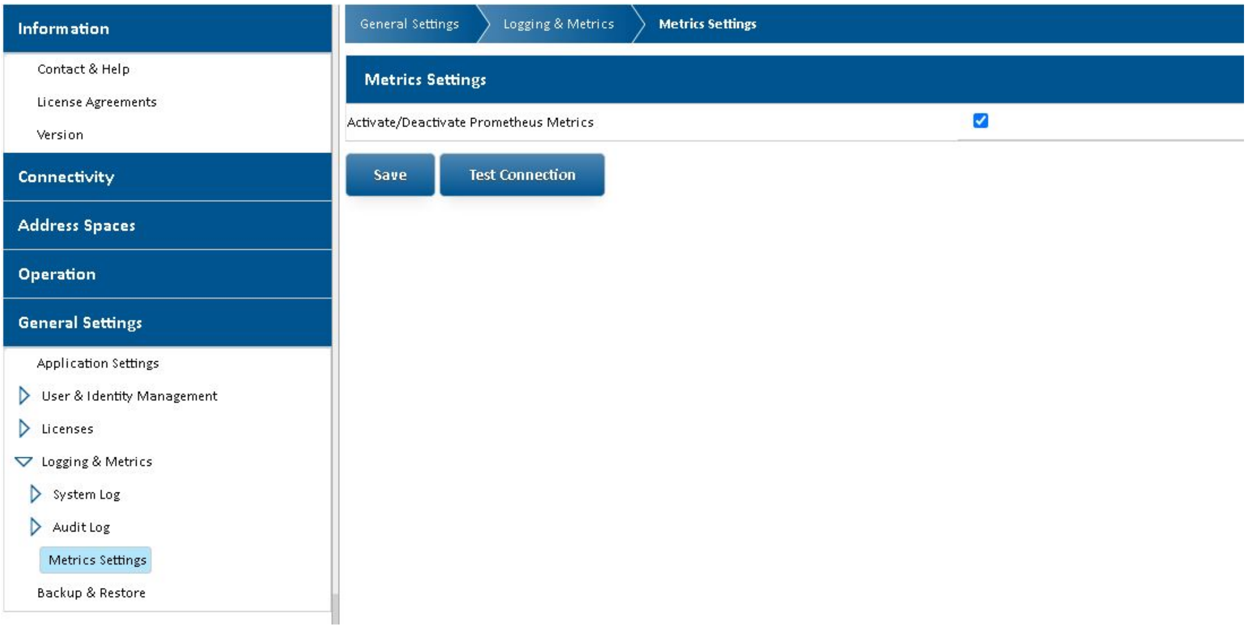
A GET operation on the same endpoint wlll give back the values of the settings, in the same JSON format as above.

On the page shown below there is a dedicated checkbox, which sets the availability of metrics from the user interface.

Prometheus

The following options can be altered in the metrics configuration page:

Option	Default Value	Details
Activate/Deactivate Prometheus Metrics	Disabled	Used to enable or disable the availability of the "/metrics" API endpoint for Prometheus.



Activate/Deactivate Prometheus Metrics ☑

Figure: Logging & Metrics, Metrics Settings page

The "Save" button saves the state to the configuration and the "Test Connection" button make a GET request to the **"/metrics"** endpoint to get the metrics data, similarly to how Prometheus scrapes the same endpoint.
The "/metrics" endpoint is used as by default, as in Prometheus.

The current implementation provides two types of metric families:
 - **status information**: of each connection defined in each module (e.g. Enabled, Connected, etc.) -- these are contained by ***_Connection_metrics** Prometheus families, where '*' is the name of the module
 - **numerical statistics**: like total number of messages received/sent, number of connections that are online/connected -- these are contained by ***_Statistics_metrics** Prometheus families

The Status information-specific metrics are implemented as Prometheus Gauge metric type and the Numerical statistics as Prometheus Counter types, to better represent the meaning of their value types.

Different families and metrics contain different Prometheus Labels.
Metric names are provided in the **"Metric"** labels, the entity for which the metric is provided in stored in the **"Connection"** label (i.e. the name of the connection) and **"Statistics"** label (i.e. the category of connections, or messages)

Pressing the **"Test Connection"** button will open a new browser page with the result of the GET operation on the "/metrics" endpoint. E.g.:

```
# HELP softing_edgeconnector_SiemensS7_Connection_metrics Softing edgeConnector
SiemensS7_Connection Metrics # TYPE
softing_edgeconnector_SiemensS7_Connection_metrics gauge
softing_edgeconnector_SiemensS7_Connection_metrics{Connection="S7-300-
400",Metric="Enabled"} 1
softing_edgeconnector_SiemensS7_Connection_metrics{Connection="S7-300-
400",Metric="Connected"} 1

# HELP softing_edgeconnector_SiemensS7_Statistics_metrics Softing edgeConnector
SiemensS7_Statistics Metrics # TYPE softing_edgeconnector_SiemensS7_Statistics_metrics
counter
softing_edgeconnector_SiemensS7_Statistics_metrics{Metric="TotalNumberOfWriteRequests
",Statistics="S7-840D-PLC"} 2523
softing_edgeconnector_SiemensS7_Statistics_metrics{Metric="TotalNumberOfReadRequests"
,Statistics="S7-840D-PLC"} 5639


# HELP softing_edgeconnector_Mqtt_Connection_metrics Softing edgeConnector
Mqtt_Connection Metrics # TYPE softing_edgeconnector_Mqtt_Connection_metrics gauge
softing_edgeconnector_Mqtt_Connection_metrics{Connection="MQTT_Connection",Metric="
Enabled"} 1
softing_edgeconnector_Mqtt_Connection_metrics{Connection="MQTT_Connection",Metric="
Connected"} 1

# HELP softing_edgeconnector_Mqtt_Statistics_metrics Softing edgeConnector Mqtt_Statistics
Metrics # TYPE softing_edgeconnector_Mqtt_Statistics_metrics counter
softing_edgeconnector_Mqtt_Statistics_metrics{Metric="TotalNumberConnected",Statistics="
Connections"} 1
softing_edgeconnector_Mqtt_Statistics_metrics{Metric="Sent",Statistics="Messages"} 136896
softing_edgeconnector_Mqtt_Statistics_metrics{Metric="Received",Statistics="Messages"}
68448

# HELP softing_edgeconnector_OPCUAServer_Statistics_metrics Softing edgeConnector
OPCUAServer_Statistics Metrics # TYPE
softing_edgeconnector_OPCUAServer_Statistics_metrics counter
softing_edgeconnector_OPCUAServer_Statistics_metrics{Metric="TotalNumberConnectedClie
nts",Statistics="Default"} 1
```

```
# HELP softing_edgeconnector_OPCUAServer_Statistics_metrics Softing edgeConnector
OPCUAServer_Statistics Metrics # TYPE
softing_edgeconnector_OPCUAServer_Statistics_metrics counter
softing_edgeconnector_OPCUAServer_Statistics_metrics{Metric="TotalFailedOpcuaEndpointA
uthentications",Statistics="Default"} 1
```

```
# HELP softing_edgeconnector_OPCUAServer_Statistics_metrics Softing edgeConnector
OPCUAServer_Statistics Metrics # TYPE
softing_edgeconnector_OPCUAServer_Statistics_metrics counter
softing_edgeconnector_OPCUAServer_Statistics_metrics{Metric="TotalNumberSubscriptions",
Statistics="Endpoint1@ns=2;i=1667363375"} 0
softing_edgeconnector_OPCUAServer_Statistics_metrics{Metric="TotalNumberSubscriptions",
Statistics="Default@ns=2;i=3754038848"} 2
softing_edgeconnector_OPCUAServer_Statistics_metrics{Metric="TotalNumberSubscriptions",
Statistics="Default@ns=2;i=1667363375"} 1
```

```
# HELP softing_edgeconnector_OPCUAServer_Connection_metrics Softing edgeConnector
OPCUAServer_Connection Metrics # TYPE
softing_edgeconnector_OPCUAServer_Connection_metrics gauge
softing_edgeconnector_OPCUAServer_Connection_metrics{Connection="Default@ns=2;i=339
3993676",Metric="Enabled"} 1
softing_edgeconnector_OPCUAServer_Connection_metrics{Connection="Default@ns=2;i=339
3993676",Metric="Connected"} 1
```

```
# HELP softing_edgeconnector_Core_Statistics_metrics Softing edgeConnector Core_Statistics
Metrics # TYPE softing_edgeconnector_Core_Statistics_metrics counter
softing_edgeconnector_Core_Statistics_metrics{Metric="TotalFailedRestApiAuthentications",
Statistics="Core"} 1
```

```
# HELP softing_edgeconnector_Core_SystemStatistics_metrics Softing edgeConnector
Core_SystemStatistics Metrics # TYPE softing_edgeconnector_Core_SystemStatistics_metrics
gauge
softing_edgeconnector_Core_SystemStatistics_metrics{Metric="Status",SystemStatistics="Op
eration"} 0
```

Note: The payload above has been formatted with new lines for easier reading.

Below we can find tables with each module's metrics. Each module's metrics are grouped by their connection types.

Mqtt

Metric Name	Metric Type	Family	Category	Values
Connected	Gauge	Connection	Connections	0 or 1 (false or true)
Enabled	Gauge	Connection	Connections	0 or 1 (false or true)
TotalNumberConnected	Counter	Statistics	Statistics/Messages	0 to 18,446,744,073,709, 551,615
Sent	Counter	Statistics	Statistics/Messages	0 to 18,446,744,073,709, 551,615
Received	Counter	Statistics	Statistics/Messages	0 to 18,446,744,073,709, 551,615

PLC Module / Siemens S7 300/400

Metric Name	Metric Type	Family	Category	Value
Connected	Gauge	Connection	Connections	0 or 1 (false or true)
Enabled	Gauge	Connection	Connections	0 or 1 (false or true)
TotalNumberOfReadRequests	Counter	Statistics	Statistics/Messages	0 to 18,446,744,073,709, 551,615
TotalNumberOfWriteRequests	Counter	Statistics	Statistics/Messages	0 to 18,446,744,073,709, 551,615

Note: Metrics TotalNumberOfReadRequests and TotalNumberOfWriteRequests sum up the different non-modifying and modifying PLC requests, respectively, depending on Protocol type.

OPC UA Server

Metric Name	Metric Type	Family	Category	Value
Connected	Gauge	Connection	Connections	0 or 1 (false or true)
Enabled	Gauge	Connection	Connections	0 or 1 (false or true)
TotalNumberConnectedClients	Counter	Statistics	Statistics	0 to 18,446,744,073,709,551,615
TotalNumberSubscriptions	Counter	Statistics	Statistics	0 to 18,446,744,073,709,551,615
TotalFailedOpcuaEndpointAuthentications	Counter	Statistics	Statistics	0 to 18,446,744,073,709,551,615

Note: A connection in the OPC UA Server is uniquely identified by the endpoint name and the session Id of the connected client application. See label in payload example above: Connection="Default@ns=2;i=3393993676"

Core

Metric Name	Metric Type	Family	Category	Value
TotalFailedRestApiAuthenticications	Counter	Statistics	Statistics	0 to 18,446,744,073,709,551,615
Status	Gauge	SystemStatistics	Operation	0 or 1 (false or true)

Note: The metric Status represents the system state with 0 being Halted and 1 being Running.

The Connection status-specific metrics are called **"Connected"** and **"Enabled"** with numeric values, for each of the connection types in the dataFEED Secure Integration Server. The different connection types are "SiemensS7", "SiemensS7_2", "Mqtt" but depending on the module in which a connection is created, there can be more. A Prometheus Family is created per each connection type, and the type of metric published for the families in this example are of type **Gauge** in Prometheus terms. The possible values for the "Connected" metric published from the application are 0 and 1 (0 = not connected, 1 = connected), similarly for "Enabled".

The **"Statistics"** families include metrics with counter-specific values, like total number of received and sent messages, for the MQTT module: **"Received" and "Sent"**, for the OPCUA Server module: **"TotalNumberConnectedClients", "TotalNumberOfReadRequests"** and **"TotalNumberOfWriteRequests"** for PLC protocols. Their values are always increasing as more messages are sent and received by the configured Publisher and Subscriber components.These metrics are of type **Counter**.

4.5.6 Backup and Restore

Backup and restore provides a valuable functionality to save and restore configurations. Once a production environment has been set-up it can be backed up and later used for restore.

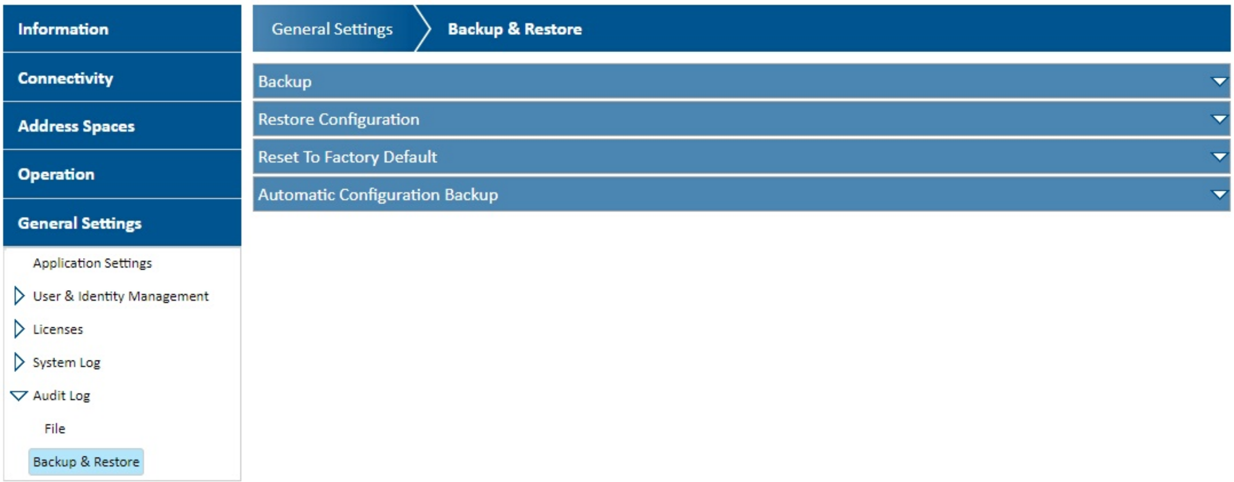


Figure: General Settings, Backup and Restore Main page

1. Backup

Click the **[Backup]** button to download a copy of the current configuration archived and compressed in a zip format file named **config-download.zip.** The file shall contain all the information required to recreate the current configuration state of the system.

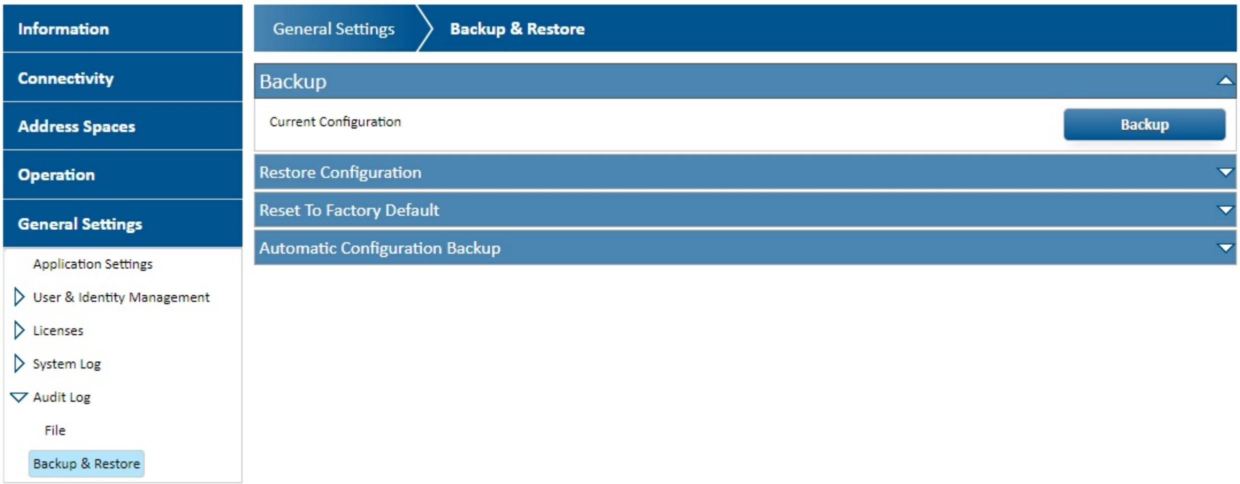


Figure: General Settings, Backup

2. Restore

Restore should be performed on the computer used to create the original backup image !

Although a restore is practically possible on a different computer it is not recommended !

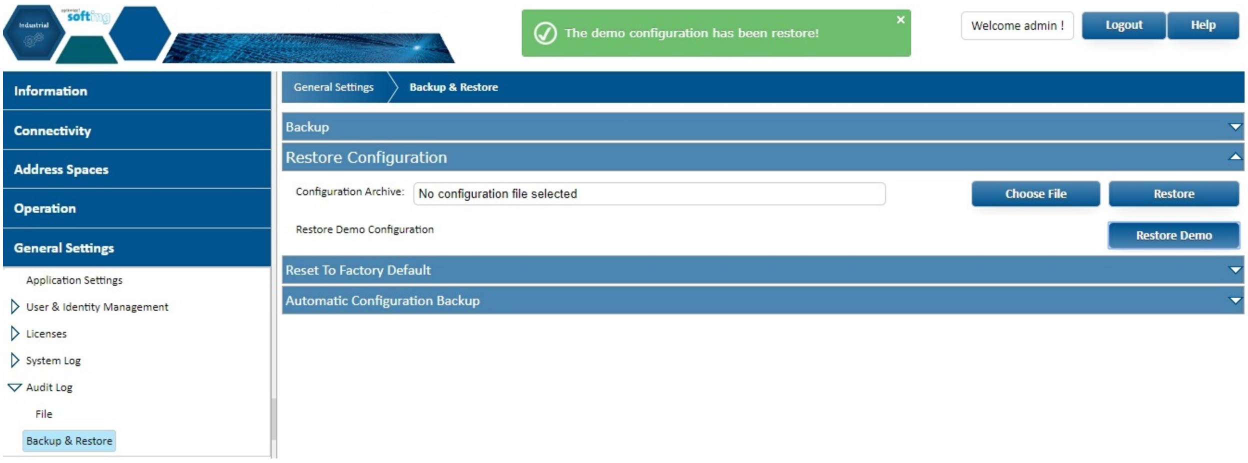
The restore functionality relies on a previously created and stored backup zip file. To start a restore process follow the steps:

a) Change system state to halted mode. Navigate to **Operation -> Status** and click the **[Stop]** button. Details here 240.

b) Click the **[Choose File]** button in the **Restore Configuration** area and select the the zip file containing the configuration to be restored.

c) Click the **[Restore]** button in the **Restore Configuration** area. At this time a busy spinner bar shall be displayed as long as the restore process is running.

- Finalizing the restore process should be notified by a message as seen below.



The demo configuration has been restore!

Configuration Archive: No configuration file selected

Figure: General Settings, Backup and Restore Demo Configuration Finalized

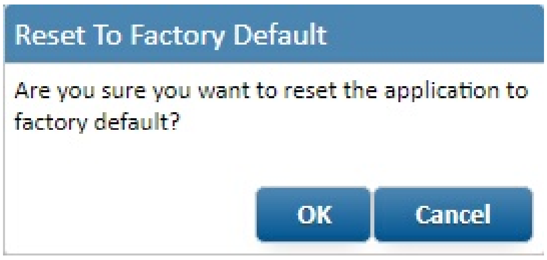
3. Factory Reset

Taking the dataFEED Secure Integration Server to the initially provided configuration is achievable as a built in feature; therefore it does not require any previously stored configurations.

a) Change system state to halted mode. Navigate to **Operation -> Status** and click the **[Stop]** button. Details here 240.

b) Click the **[Reset]** button in the **Reset to Factory Default** region.

c) Acknowledge the pop-up by clicking the **[OK]** button:

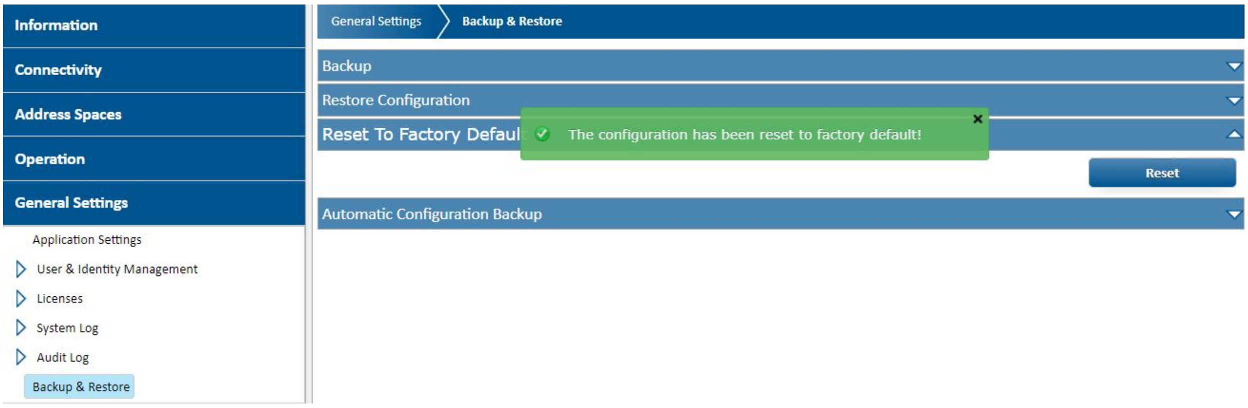


Reset To Factory Default

Are you sure you want to reset the application to factory default?

Figure: General Settings, Acknowledge Reset To Factory Default

- Finalizing the **Factory Reset** process should be notified by a message as seen below. Acknowledge it by clicking the **[OK]** button:



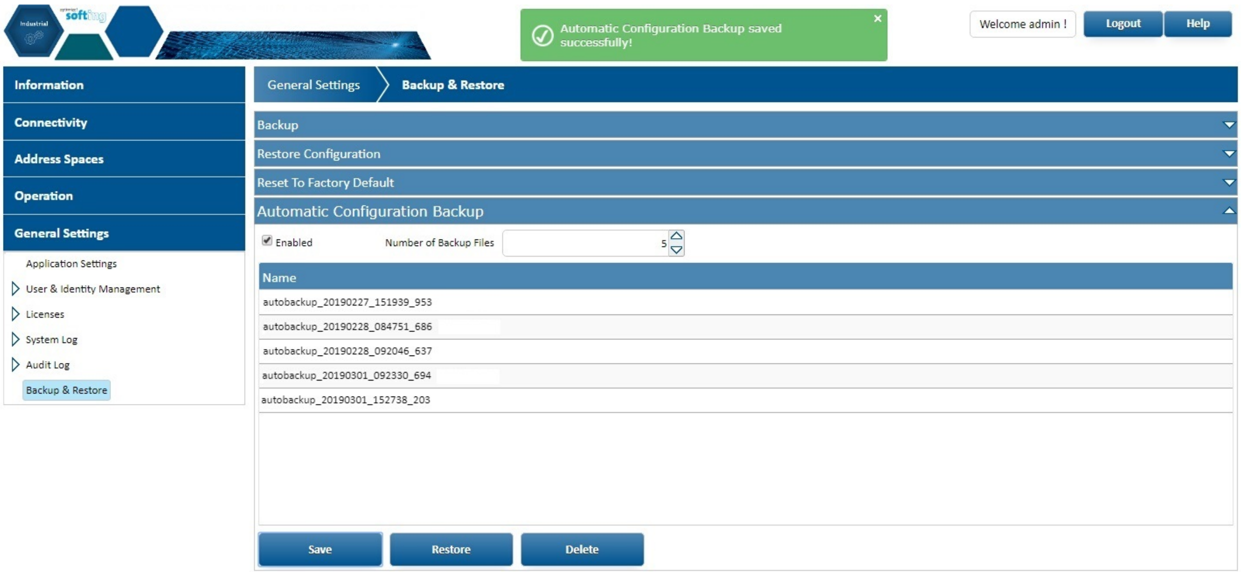
✓ The configuration has been reset to factory default!

Figure: General Settings, Backup and Restore Factory Default Finalized

4. Automatic Configuration Backup

When enable, by checking the [**Enabled**] checkbox, the automatic configuration backup will store all configuration changes conducted during a configuration session in a new backup file identified by a prefix and the timestamp. The maximum number of automatically saved configuration is defined by **Number of Backup Files,** and is configurable. When the limit is reached the oldest saved configuration is discarded.

Apply settings changes by pressing **[Save].** The operation shall be notified by a message as seen below.



✓ Automatic Configuration Backup saved successfully!

☑ Enabled   Number of Backup Files 5

Name
autobackup_20190227_151939_953
autobackup_20190228_084751_686
autobackup_20190228_092046_637
autobackup_20190301_092330_694
autobackup_20190301_152738_203

Figure: General Settings, Backup and Restore, Save Automatic Configuration Backup Settings

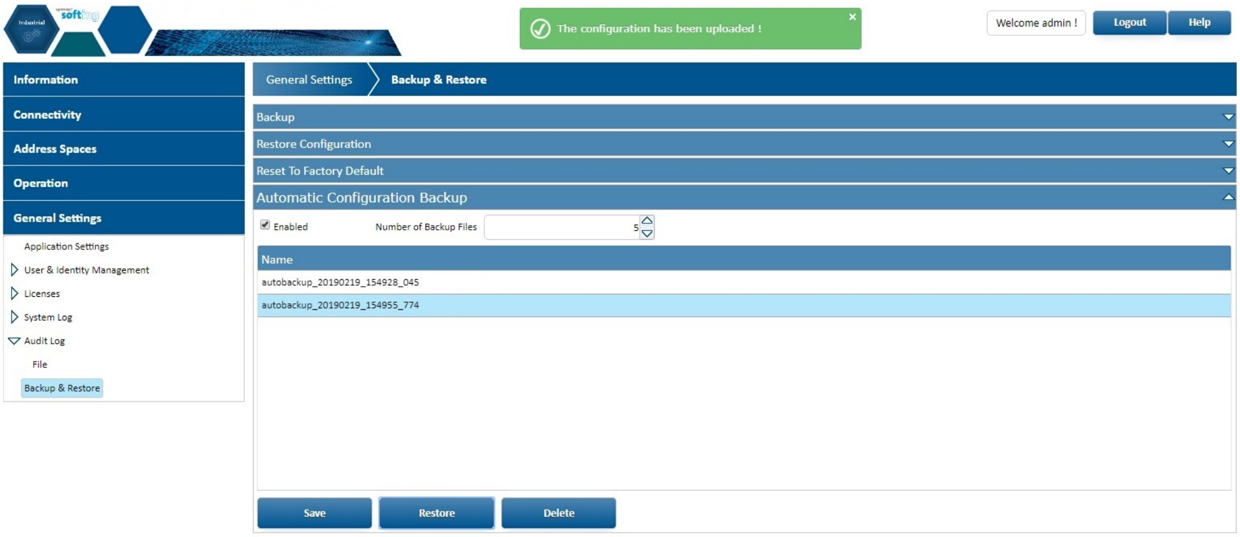
To **restore** the system to previous configuration state follow the steps:

a) Change system state to halted mode. Navigate to **Operation -> Status** and click the **[Stop]** button. Details here 240.

b) Select a backup file containing the configuration to be restored from table in the **Automatic Configuration Backup** area.

c) Click the **[Restore]** button in the **Automatic Configuration Backup** area. At this time a busy spinner bar shall be displayed as long as the restore process is running.

- Finalizing the restore process should be notified by a message as seen below.



The configuration has been uploaded !

☑ Enabled Number of Backup Files 5

Name
autobackup_20190219_154928_045
autobackup_20190219_154955_774

Figure: General Settings, Backup and Restore Automatic Configuration Backup Finalized

To delete a configuration, select the configuration by name and press **[Delete]**.

- The activated licenses of the dataFEED Secure Integration Server 1.30 instance are also subject of Backup/Restore operation.
- A Reset To Factory Defaults operation will remove all existing activated licenses of the dataFEED Secure Integration Server 1.30 instance.
- Refer to the Licenses 55 chapter for more information regarding license related operations.

4.6 MQTT Configuration

MQTT Configuration chapter groups information about MQTT related configuration.

4.6.1 Overview

A key feature of the dataFEED Secure Integration Server are publishing PLC data to MQTT Brokers, as well as subscribing to MQTT brokers to get data into PLC variables.

First is required the definition of the

➢ MQTT Connections 91 (Brokers)

followed by the configuration of the

➢ MQTT Publisher 124 (Client)

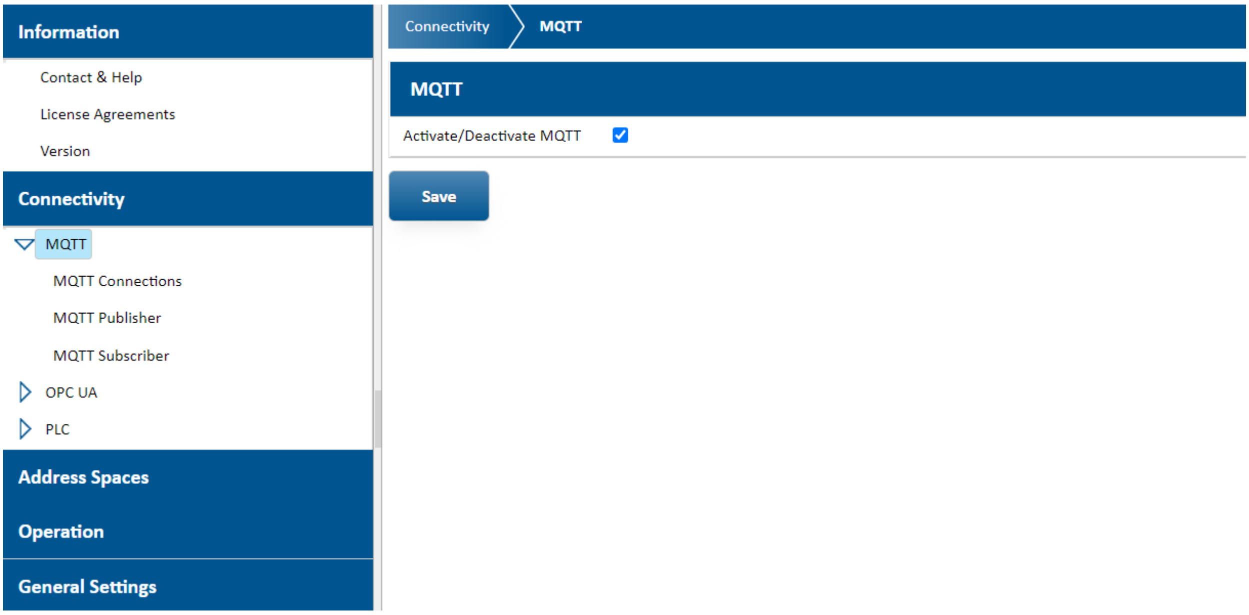
and/or

➢ MQTT Subscriber 144

To enable or disable this functionality, navigate to **Connectivity ->MQTT ,** change the state of the feature by checking/unchecking the **[Activate/Deactivate MQTT]** checkbox and click **[Save]** button.

The checkbox state reflects the actual feature state:

- **checked** ☑ : MQTT enabled
- **unchecked** □ : MQTT disabled



Activate/Deactivate MQTT ☑

Figure: Overview page MQTT connectivity

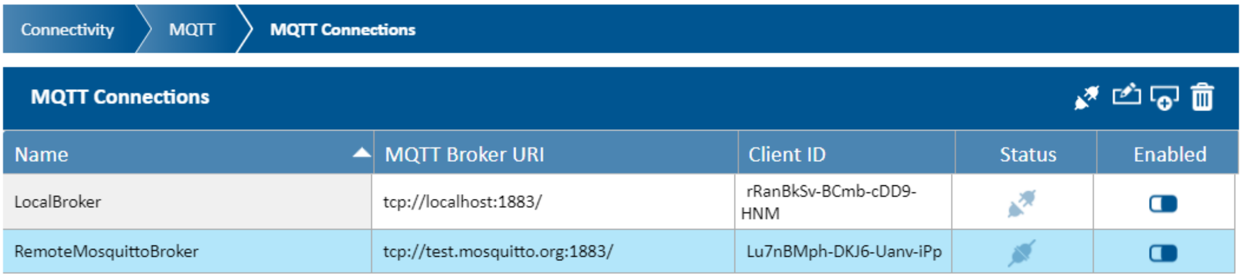
4.6.2 MQTT Connections

The logical sequence for configuring the MQTT connectivity is:

1. definition of MQTT broker connections
2. definition of publishing and/or subscribing jobs

Information about all configured MQTT connections is centralized and accessible by navigating to **Connectivity -> MQTT -> MQTT Connections**.

The page displays the list of defined connections or the message *'No data to display'*.



Name	MQTT Broker URI	Client ID	Status	Enabled
LocalBroker	tcp://localhost:1883/	rRanBkSv-BCmb-cDD9-HNM		
RemoteMosquittoBroker	tcp://test.mosquitto.org:1883/	Lu7nBMph-DKJ6-Uanv-iPp		

Figure: List of defined MQTT connections

The table header information is described below:

Column name	Information details
Name	User defined name of the connection
MQTT Broker URI	The URI (including the scheme) of the MQTT broker
Client ID	User defined unique client ID to connect the broker
Status	Connected or Disconnected. A connection could be disconnected for more reasons (is not enabled, connection parameters are not valid, MQTT feature is disabled, the broker is down). Clicking on the status icon has no effect.
Enabled	Toggle which enable or disable a connection. By disabling it, a connection changes its status to *Disconnected*. By enabling it back, if re-connection is successful, the status become *Connected*. Activating/ Deactivating a connection could be made independently of the status (*Enabled/Disabled*) of the MQTT feature.

Table: Connection list

The **MQTT Connections** information bar provides four buttons with the following functionality:

Button	Action
🔌	Test the selected MQTT connection 106
✎	Modify the selected MQTT connection 105
⊕	Add a new MQTT connection 92
🗑	Remove the selected MQTT connection 105

Table: List of actions for handling the MQTT connections

4.6.2.1 Add connection

By clicking the **[Add MQTT Connection]** button located in the MQTT Connections 91 page**,** the context is switched to the definition of the parameters needed in order to establish a new MQTT connection.

It contains four tab pages, each grouping the following parameter sets:

Connection Settings 93

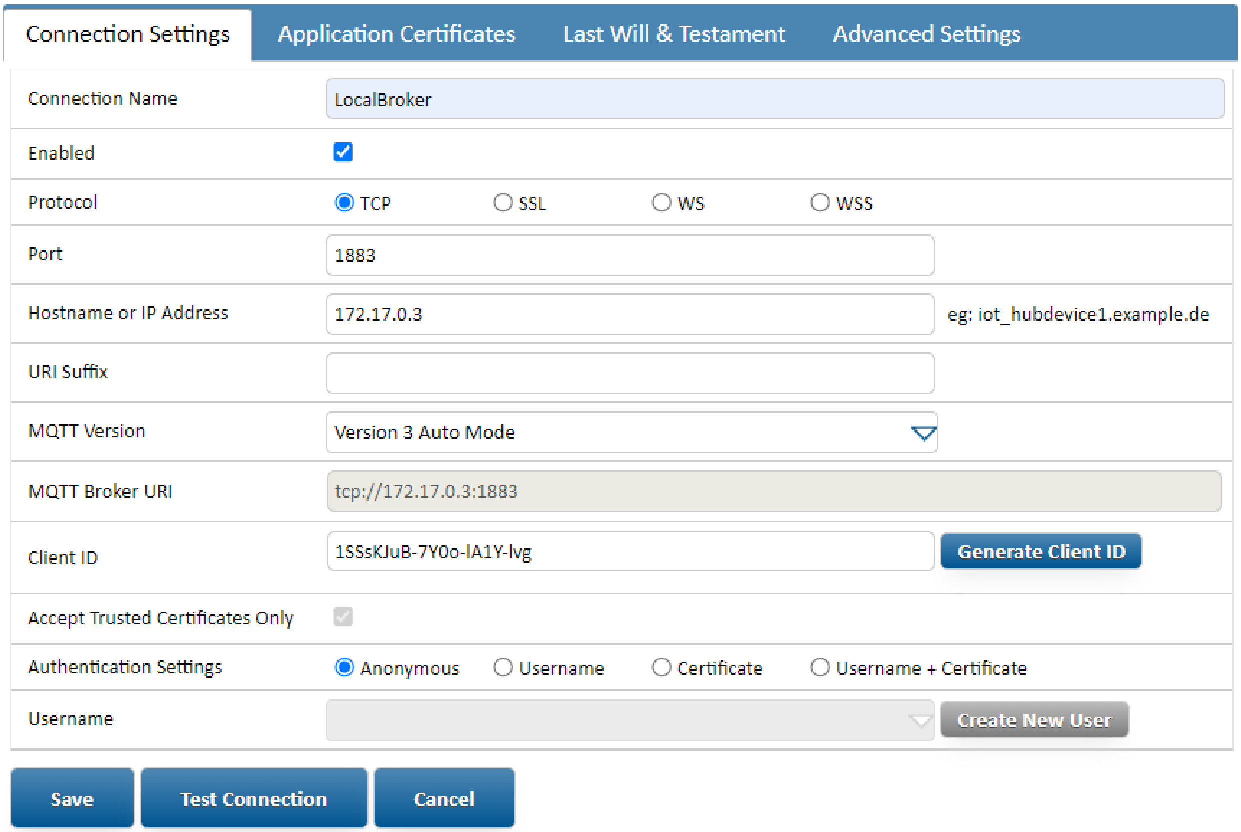
Application Certificates 97

[Last Will & Testament 100]

[Advanced Settings 102]

4.6.2.1.1 Connection settings

The tab page *Connection settings* contains the parameters which are mandatory for any connection.

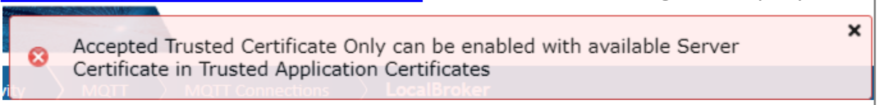
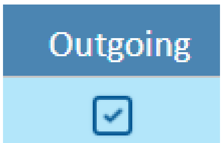


Connection Name	LocalBroker
Enabled	☑
Protocol	● TCP ○ SSL ○ WS ○ WSS
Port	1883
Hostname or IP Address	172.17.0.3 eg: iot_hubdevice1.example.de
URI Suffix	
MQTT Version	Version 3 Auto Mode
MQTT Broker URI	tcp://172.17.0.3:1883
Client ID	1SSsKJuB-7Y0o-lA1Y-lvg
Accept Trusted Certificates Only	☑
Authentication Settings	● Anonymous ○ Username ○ Certificate ○ Username + Certificate
Username	

Figure: Connection settings tab page

Parameter name	Default value	Value description
Connection Name	**empty**	Defines the connection name as it will be displayed in the MQTT Connections overview page. This name will be further referred in the pages for defining the MQTT publishers.
Enabled	**Enabled**	Enable (checked) or disable (unchecked) the currently configured MQTT connection.
Protocol	**TCP**	Radio buttons group containing the following options for the underlying network protocol: *TCP, SSL, WS, WSS*

		- *TCP* for raw TCP/IP connection - *SSL* for TCP/IP with transport level security - *WS* for WebSocket without use of TLS - *WSS* for WebSocket with TLS
Port	**1883**	The port of the MQTT server that is to be used. The default for TCP is 1883. **Note** Port *1883* is the default port setting for the default protocol *TCP*. If other protocols (*SSL*, *WS* or *WSS*) are selected, the default port also changes (*8883*, *8000* or *443* *respectively*).
Hostname or IP address	**empty**	External mqtt server endpoint. Used by the MQTT publisher to establish a new connection. The accepted values are either IPV4, IPV6 addresses or local name/ domain name. ***Note**: The Hostname or IP is automatically validated while filled in. ***Note**: DO NOT fill the URI protocol prefix (Ex tcp://, mqtts://)
URI Suffix	**None**	The suffix part to complete the connection URL. For example use suffix 'mqtt', hostname 'local' and port '1883' to compose the connection URI 'hostname:1883/mqtt'
MQTT Version	**Version 3 Auto Mode**	The MQTT version to use for establishing the new connection. Possible values: - *Version 3 Auto Mode* - Use MQTT v3.1.1 then fall back to MQTT v3.1 - *Version 3.1* - Use MQTT v3.1 - *Version 3.1.1* - Use MQTT v3.1.1 - *Version 5* - Use MQTT v5
MQTT Broker URI	**None**	Read only field which automatically compose the MQTT Broker URI by concatenating the user defined values for parameters: transport protocol, hostname, port and suffix.
Client ID	**randomly generated**	Unique Id to identify on the broker the client connection established by the current application. The value is limited to 23 characters. You can use the “Generate client ID” button or provide one yourself.

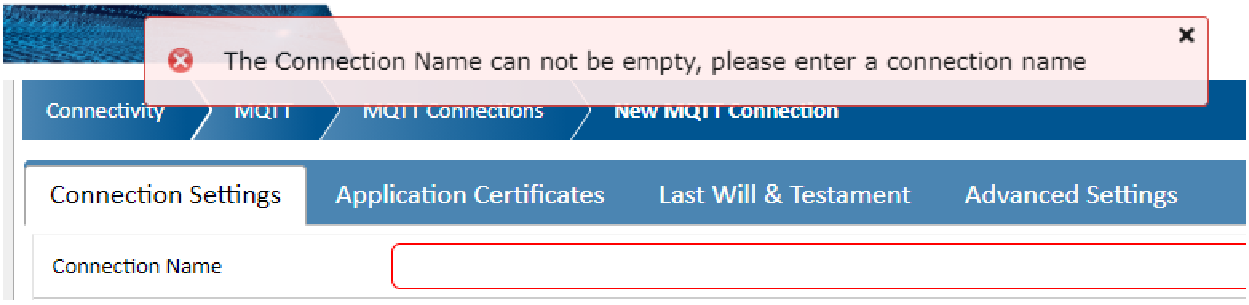
Accept Trusted Certificates Only	**True**	True (checked) or False (unchecked). The check-box has a meaning and is enabled only for the protocols *SSL* and *WSS*. If True and enabled, there are accepted MQTT connections only to brokers with a valid certificate in the Trusted Application Certificate List 97. If True and enabled, but there are no trusted certificates defined in Trusted Application Certificate list 97, an error message is displayed.  Accepted Trusted Certificate Only can be enabled with available Server Certificate in Trusted Application Certificates
Authentication Settings	**Anonymous**	Method for authenticating the client session that will be established against the MQTT Broker. Possible values: • *Anonymous* (the server does not authenticate the client) • *Username* (authentication with username and password) • *Certificate* (authentication using X509 client certificate) • *Username and Certificate* (authentication using both username/ password and client certificate)
Username	**empty**	Enabled only for *Authentication settings : Username or Username and Certificate.* The *Username* can be can be created new from the scratch(by clicking the button **[Create New User])** or selected from a list. If selected the option **[Create New User]**, the flow will continue in the page **General Settings -> User & Identity Management -> Users & Identities -> New User**. The users created by following this flow are placed by default in the group *MQTT Users*. By saving the new user, the *Username* combo box will be filled automatically with the identity of the newly created user. • Case 1 (*Authentication settings : Username)* The user can be selected from the list of users belonging to the group *MQTT Users.* • Case 2 (*Authentication settings: Username and Certificate)* The user can be selected from the list of users which have defined a valid outgoing user certificate and belonging to *MQTT Users* group. ***Note:** A valid outgoing certificate, is a certificate in the validity period which has the flag Outgoing *checked* 

		****Note:** If the selected user outgoing certificate has also the signers chain available, at the connection time, the entire chain of certificates will be passed to the broker for validation.

Table: Connection settings parameters

By clicking **[Test Connection]** it will be tried a connection to the MQTT broker using the current parameters. see Test connection 106.

By Clicking **[Save]** button is triggered a validation of the connection parameters. In case of missing information or errors appropriate messages are displayed.



The Connection Name can not be empty, please enter a connection name

Figure: Error message shown on parameters validation

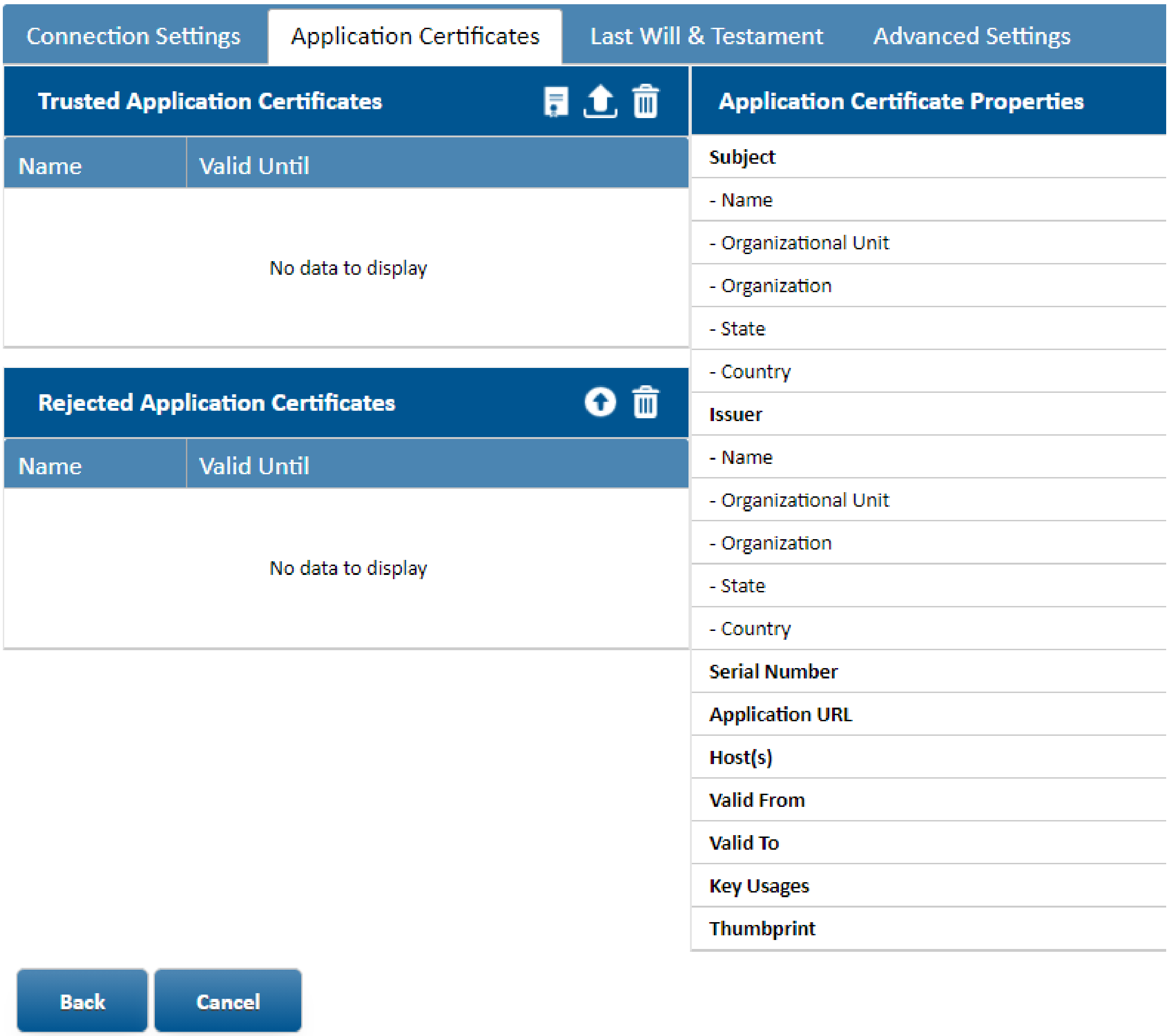
If the validation pass, the connection parameters are persistently stored and the context will be moved to the page showing the MQTT Connections 91 list.

By clicking **[Cancel]** button all changes are discarded and the context will be moved to the page showing the MQTT connections 91 list.

4.6.2.1.2 Application certificates

In this tab page there will be defined the certificates of the MQTT brokers to connect.

If the parameter *Accept Trusted Certificates Only* present in the section Connection settings 93, is checked, the connection is possible only after having the broker's certificate in the *Trusted Application Certificates* list.



Connection Settings | Application Certificates | Last Will & Testament | Advanced Settings

Trusted Application Certificates

Name	Valid Until
No data to display	

Rejected Application Certificates

Name	Valid Until
No data to display	

Application Certificate Properties

Subject
- Name
- Organizational Unit
- Organization
- State
- Country

Issuer
- Name
- Organizational Unit
- Organization
- State
- Country

Serial Number

Application URL

Host(s)

Valid From

Valid To

Key Usages

Thumbprint

Figure: Application certificates tab page

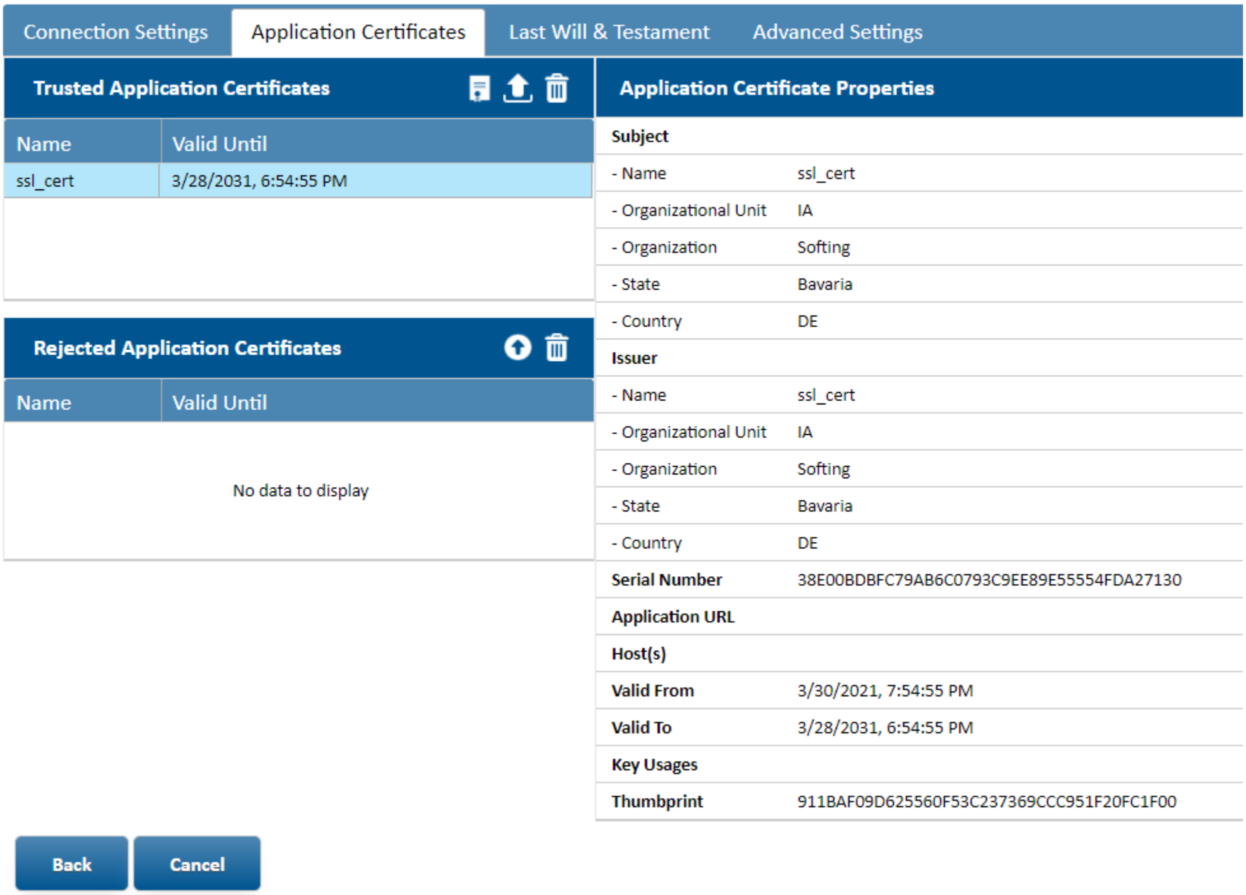
There are three(3) ways to achieve that:

1. By receiving the MQTT broker certificate.

A broker certificate is received only for the secured connections; therefor, verify that the Connection settings 93 section contains valid parameters for Hostname/IP/Port/ClientId and the Protocol is SSL or WSS.

Click the button **[Receive Broker Certificate]**

The certificate of the broker will be retrieved during the TLS handshake and will appear in the *Trusted Application Certificates* list. The table *Application Certificate Properties* on the right side will display the information stored within the certificate.



Trusted Application Certificates

Name	Valid Until
ssl_cert	3/28/2031, 6:54:55 PM

Rejected Application Certificates

Name	Valid Until

No data to display

Application Certificate Properties

Subject	
- Name	ssl_cert
- Organizational Unit	IA
- Organization	Softing
- State	Bavaria
- Country	DE
Issuer	
- Name	ssl_cert
- Organizational Unit	IA
- Organization	Softing
- State	Bavaria
- Country	DE
Serial Number	38E00BDBFC79AB6C0793C9EE89E55554FDA27130
Application URL	
Host(s)	
Valid From	3/30/2021, 7:54:55 PM
Valid To	3/28/2031, 6:54:55 PM
Key Usages	
Thumbprint	911BAF09D625560F53C237369CCC951F20FC1F00

2. By testing the connection in the Connection settings 93 section.

Select the protocol *SSL* or *WSS.*

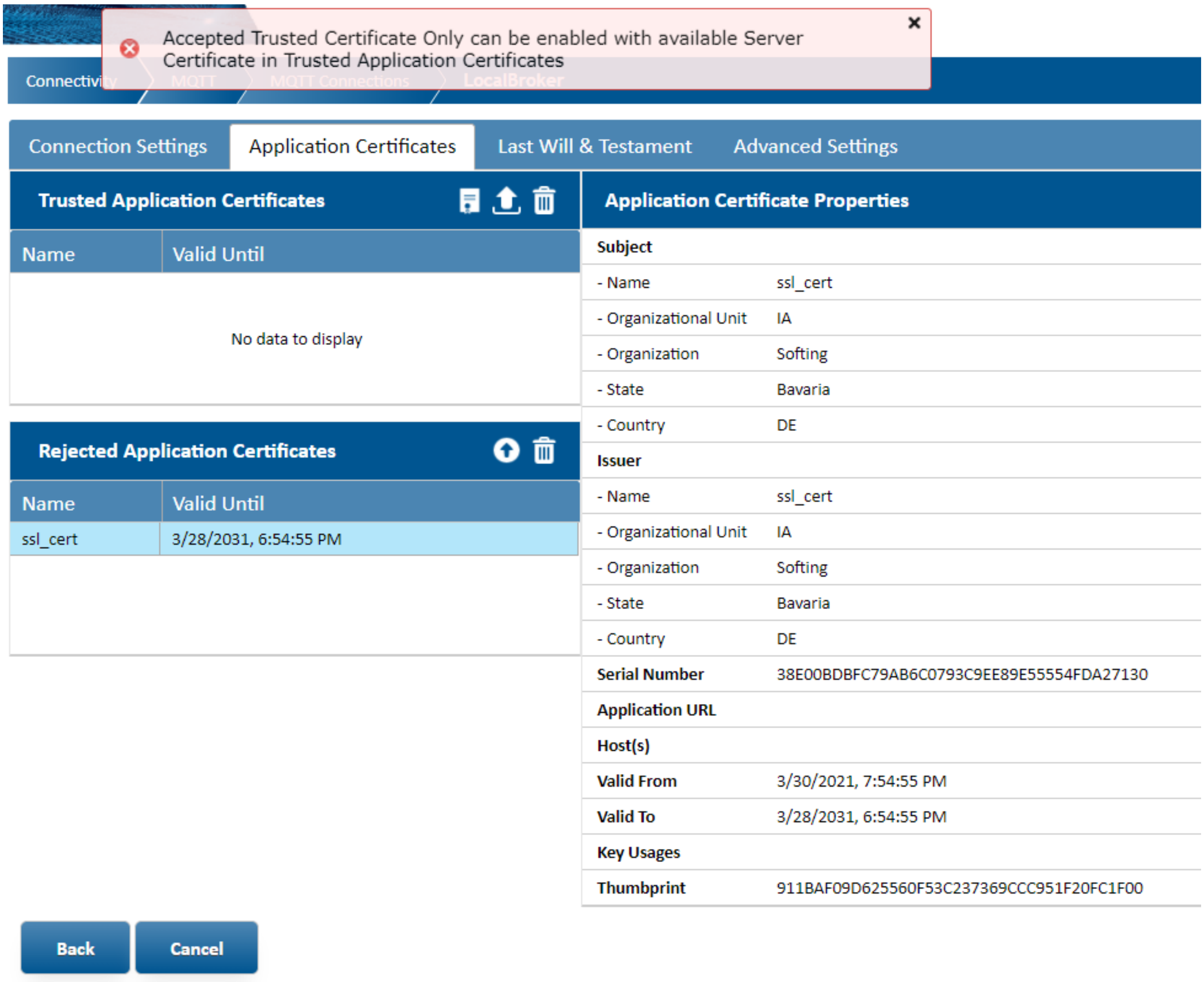
Verify that *Hostname/IP Address* and the *Port* contain valid values.

Check the check-box *Accept Trusted Certificates Only*.

Click the button *Test Connection*.

Even if the connection test is unsuccessful (because there were not defined yet valid certificates for the broker in the list Trusted Application Certificates 97),

the list *Rejected Application Certificates* is containing the certificate of the broker to whom the connection was just tested.



Accepted Trusted Certificate Only can be enabled with available Server Certificate in Trusted Application Certificates

Trusted Application Certificates

Name	Valid Until
No data to display	

Rejected Application Certificates

Name	Valid Until
ssl_cert	3/28/2031, 6:54:55 PM

Application Certificate Properties

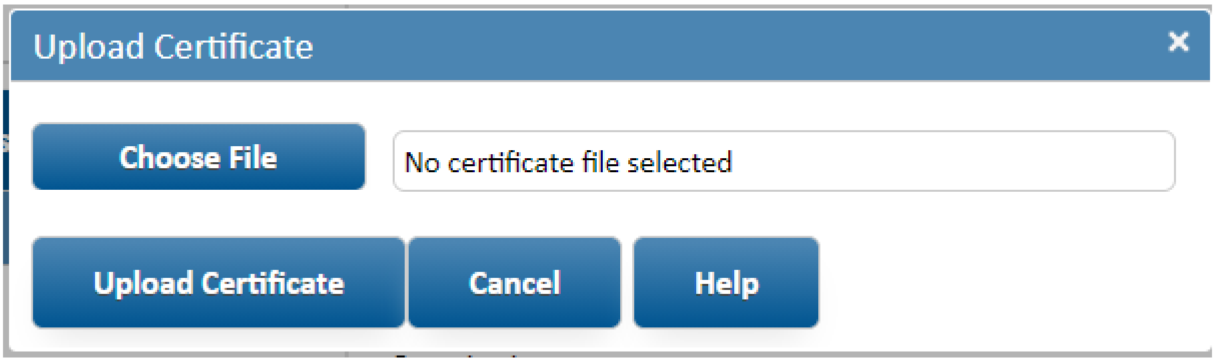
Subject	
- Name	ssl_cert
- Organizational Unit	IA
- Organization	Softing
- State	Bavaria
- Country	DE
Issuer	
- Name	ssl_cert
- Organizational Unit	IA
- Organization	Softing
- State	Bavaria
- Country	DE
Serial Number	38E00BDBFC79AB6C0793C9EE89E55554FDA27130
Application URL	
Host(s)	
Valid From	3/30/2021, 7:54:55 PM
Valid To	3/28/2031, 6:54:55 PM
Key Usages	
Thumbprint	911BAF09D625560F53C237369CCC951F20FC1F00

This certificate can be accepted and move to the trusted list by clicking **[Move to Trusted]** button

3. By uploading the certificate to the trusted list.

Click the button **[Upload Trusted Certificate]**

The dialog below is shown.



Upload Certificate

No certificate file selected

Click **[Chose file]** button to select the certificate. Are allowed certificates with extensions **.pem** and **.crt**.

Click the button **[Upload Certificate]**.

If the certificate file is valid, information about its subject, validity, issuer is displayed in the panel Application Certificate Properties located on the right side of the screen

Once the broker's certificate is in the trusted list, re-trying the test connection will turn to successful.

The **Trusted Applications Certificate toolbar** provides three buttons with the following functionality:

Button	Action
📜	Receive broker certificate. It initiates a TLS handshake protocol to get the certificate of the broker having the settings defined in Connection settings 93 panel. (see Step 1 above)
⬆	Upload trusted certificate. Used to define X.509 certificates of the MQTT brokers to connect. (.pem and .crt formats)
🗑	The currently selected trusted certificate is permanently deleted.

The **Rejected Applications Certificate toolbar** provides two buttons with the following functionality:

Button	Action
⬆	The currently selected certificate is moved from the list of rejected to the trusted list. As result, a connection to a broker having *Accept Trusted Certificates Only = True* become successful.
🗑	The currently selected rejected certificate is permanently deleted.

By Clicking **[Back]** button the context will be moved to the page showing the Connection settings 93.

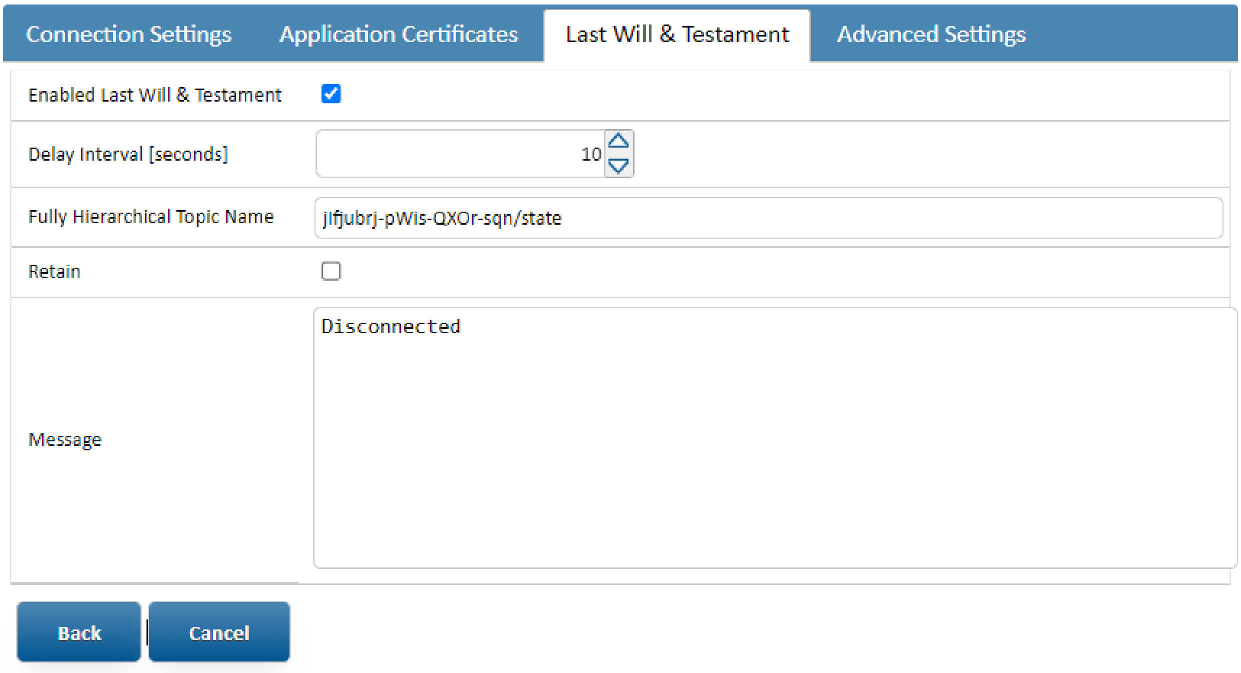
By clicking **[Cancel]** button all changes made to the new connection are discarded and the context will be moved to the page showing the list of MQTT connections.

4.6.2.1.3 Last will & Testament

This is a typical parameter for any MQTT client connection.

If activated, the broker will notify other clients if the connection established in the current application was ungracefully disconnected.

The information about last will & testament is communicated to the MQTT Broker every time the connection to it is established. The last will message is a normal MQTT message with a topic, retained message flag and payload.



Enabled Last Will & Testament	☑
Delay Interval [seconds]	10
Fully Hierarchical Topic Name	jlfjubrj-pWis-QXOr-sqn/state
Retain	□
Message	Disconnected

Figure: Last will and testament parameters

Parameter name	Default value	Value description.
Enabled Last will & Testament	**Disabled**	Enabled (checked) or Disabled (unchecked).
Delay Interval [seconds]	**10**	The seconds broker shall wait until sending the Last Will message after the disconnection is noticed. **Note:** This option is visible only for MQTT v5 connections.
Fully Hierarchical Topic Name	**generated topic name (Ex: rRanBkSv-BCmb-cDD9-HNM/state)**	Enabled if Enabled Last will & Testament is checked. Full path name to the last will topic (where the last will message will be published). The initial default value is generated automatically using the template *<ClientID>/state.*
Retain	**False**	True (checked) or False (unchecked). Keeps other clients up to date about the current status of the application. Clients that subscribe to the topic while the application is offline, receive the LWT retained message from the broker.
Message	**Disconnected**	user defined string informing the MQTT client connection established by the application is disconnected.

By Clicking **[Back]** button all changes made in the current page will be kept until the **[Save]** button is clicked and the context will be moved to the page showing the Connection settings 93.

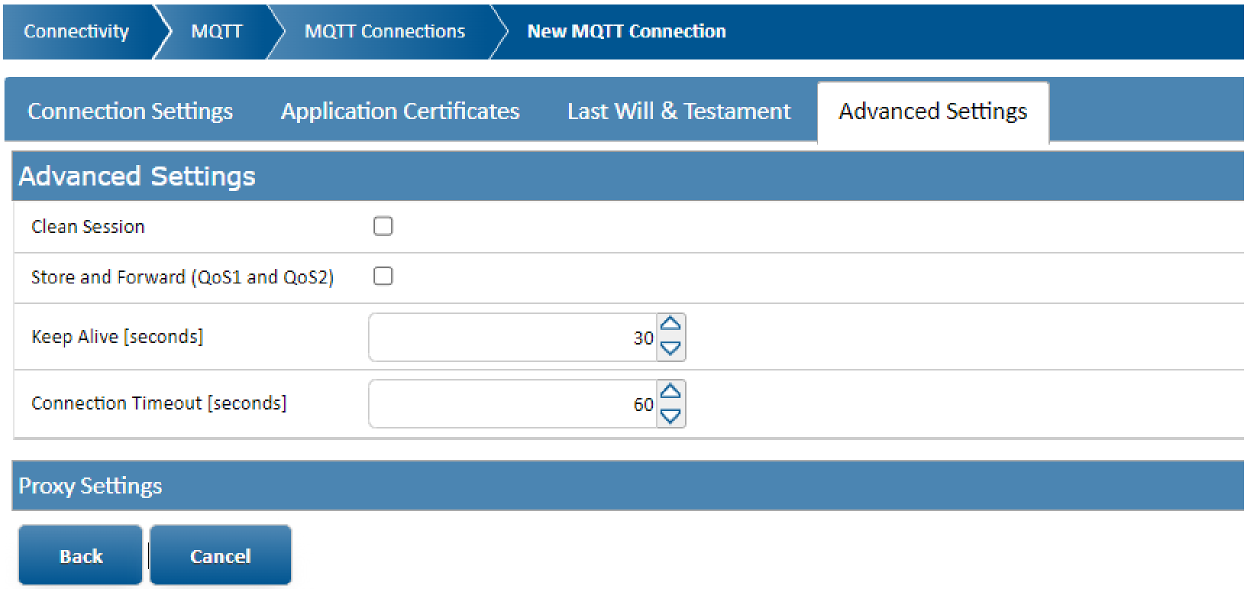
By clicking **[Cancel]** button all changes made to the new connection are discarded and the context will be moved to the page showing the list of MQTT connections 91.

4.6.2.1.4 Advanced settings

The tab page Advanced Settings contains parameters for more advanced tuning of the MQTT connection to the broker.

It is structured on two groups of parameters: *Advanced Settings* and *Proxy Settings*.

For a connection configured to use an MQTT v3x protocol, the *Advanced Settings* group contain the following:



Advanced Settings

Clean Session □

Store and Forward (QoS1 and QoS2) □

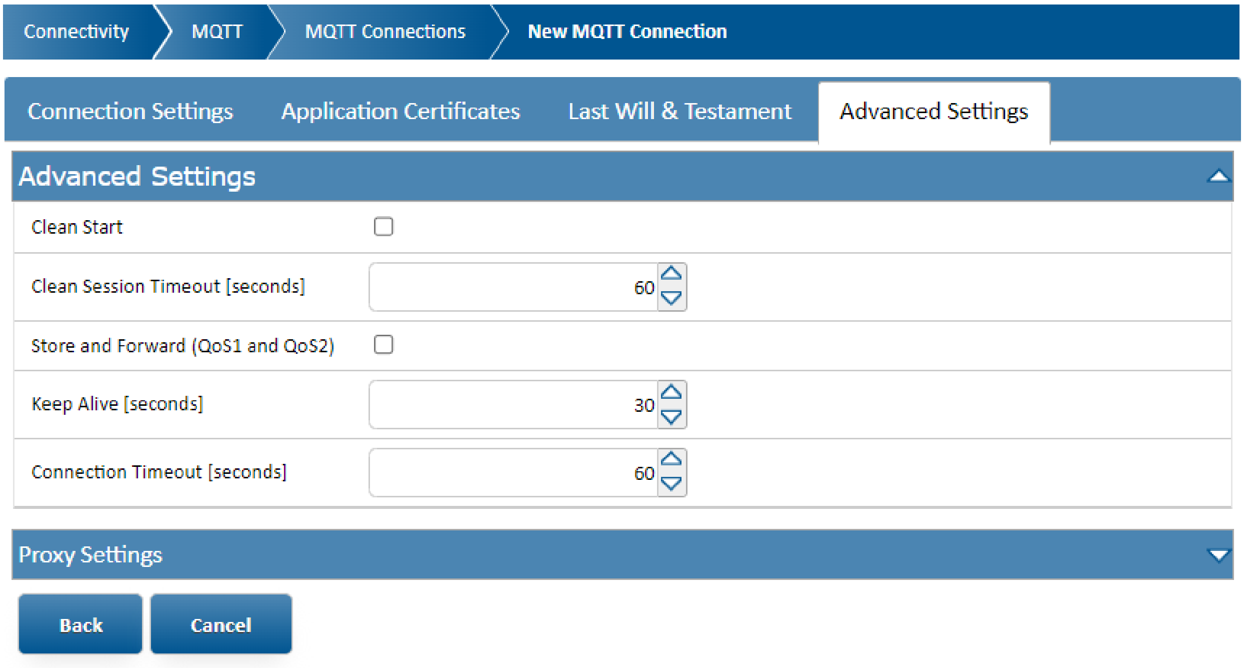
Keep Alive [seconds] 30

Connection Timeout [seconds] 60

Proxy Settings

Figure: Advanced mqtt connection settings for MQTT v3x connections

For an MQTT v5 connection, the *Advanced Settings* group contain the following:



Advanced Settings

Clean Start □

Clean Session Timeout [seconds] 60

Store and Forward (QoS1 and QoS2) □

Keep Alive [seconds] 30

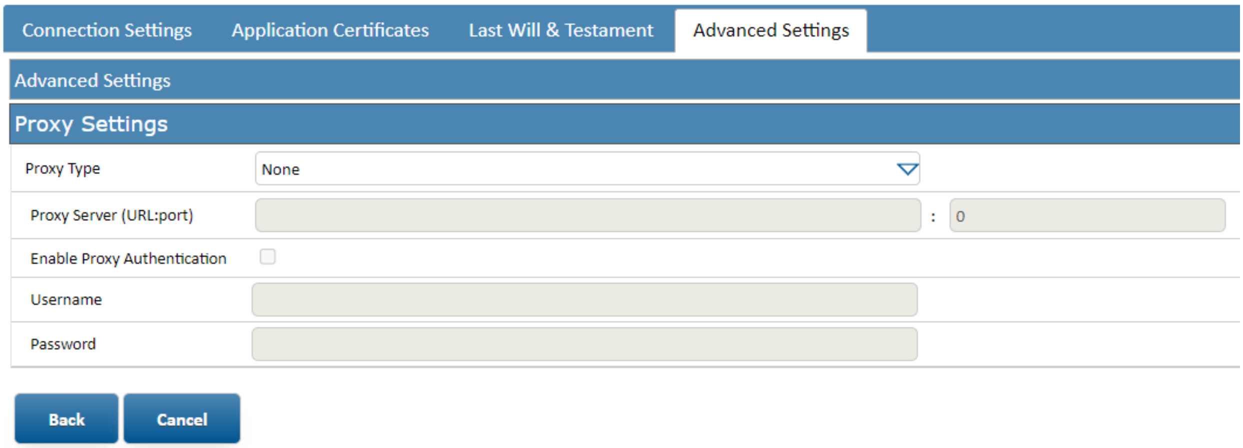
Connection Timeout [seconds] 60

Figure: Advanced mqtt connection settings for MQTT v5 connections

Parameter name	Default value	Value description
Clean session	**Unchecked**	Normally when a MQTT broker receives a message it will deliver it immediately to all clients with matching subscriptions. If there are no subscribers, the message will not be delivered anywhere. In some situations it would make sense to keep the message in the broker and deliver it when a client comes back online. This can be solved by using a *clean session* flag when connecting. If *clean session* flag is set to false (Unchecked) when a client connects, the broker will create a persistent session. When a client with a persistent session disconnects, the broker will keep the information about its subscriptions and will queue QoS 1 and 2 messages until the client re-connects. **Note:** The option described above is present only for the MQTT v3x connections.
Clean Start	**Unchecked**	In MQTTv5 *clean session* is now known as *clean start*, and is used in conjunction with a new feature called the *clean session timeout* (session expiry interval). **Note:** The option is present only for the MQTT v5 connections.
Clean Session Timeout [seconds]	**60**	Even if the *clean start* is set to *unchecked*, the broker will expire the client and clean the session clear its state after the timeout provided here will elapse. **Note:** The option is present only for the MQTT v5 connections.

Store and Forward (QoS1 and QoS2)	**Unchecked**	If *clean session* flag is set to false (Unchecked) and this is checked, then the QoS1 and 2 messages are stored in the filesystem until confirmed by the MQTT broker.
Keep Alive	**30**	The keep alive is the time interval (in seconds) in which the client sends a ping to the broker if no other MQTT packets are sent during this period of time. It is used to determine if the connection is still up. Disable *Keep Alive* by setting the parameter to zero (0).
Connection Timeout	**60**	This value, measured in seconds, defines the maximum time interval the client will wait for the network connection to the MQTT server to be established. A value of 0 disables timeout processing meaning the client will wait until the network connection is made successfully or fails.

The Proxy *Settings* group contain the following:



Advanced Settings

Proxy Settings

Proxy Type: None

Proxy Server (URL:port): : 0

Enable Proxy Authentication: □

Username

Password

Figure: Mqtt connection proxy settings

Parameter name	Default value	Value description
Proxy type	**None**	Two possible values (*None* and *HTTPS*) *Note: If HTTPS proxy type is chosen, the Host name and port shall not be empty
Proxy server	**empty**	separate fields for URL (Host name or IP address) respectively the port. *Note: Exclude the protocol scheme from the Host name.
Enable proxy authentication	**Unchecked**	Checked for True and Unchecked for False *Note: If True, the *Username* and *Password* parameters shall not be empty.
Username	**empty**	name of the user (only if *Enable proxy authentication* = True)
Password	**empty**	password (only if *Enable proxy authentication* = True)

By Clicking **[Back]** button all changes made in the current page will be kept until the **[Save]** button is clicked and the context will be moved to the page showing the Connection settings 93.

By clicking **[Cancel]** button all changes made to the new connection are discarded and the context will be moved to the page showing the list of MQTT connections 91.

4.6.2.2 Modify connection

By clicking the [**Edit MQTT Connection]** button located in the MQTT Connections 91 page**,** the context is switched to the modification of the currently selected MQTT connection.

The following groups of parameters can be edited:

Connection Settings 93

Application Certificates 97

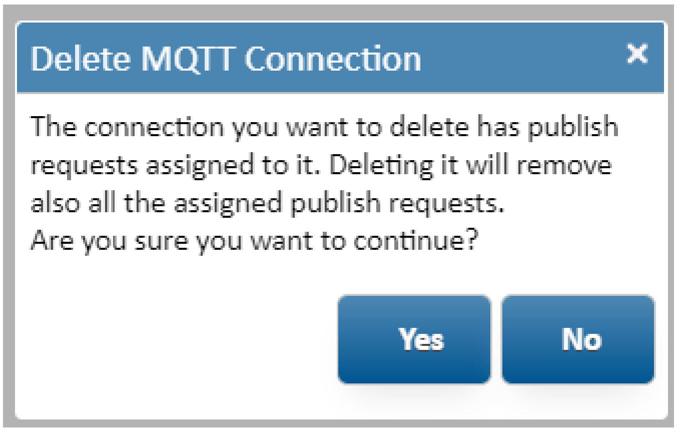
Last will & Testament 100

Advanced Settings 102

4.6.2.3 Delete connection

By clicking the [**Delete MQTT Connection]** button located in the MQTT Connections 91 page**,** the currently selected MQTT connection is deleted.

***Warning**: There is no additional confirmation requested before deleting the connection except the case when there is a publisher configured to use that connection.



Delete MQTT Connection

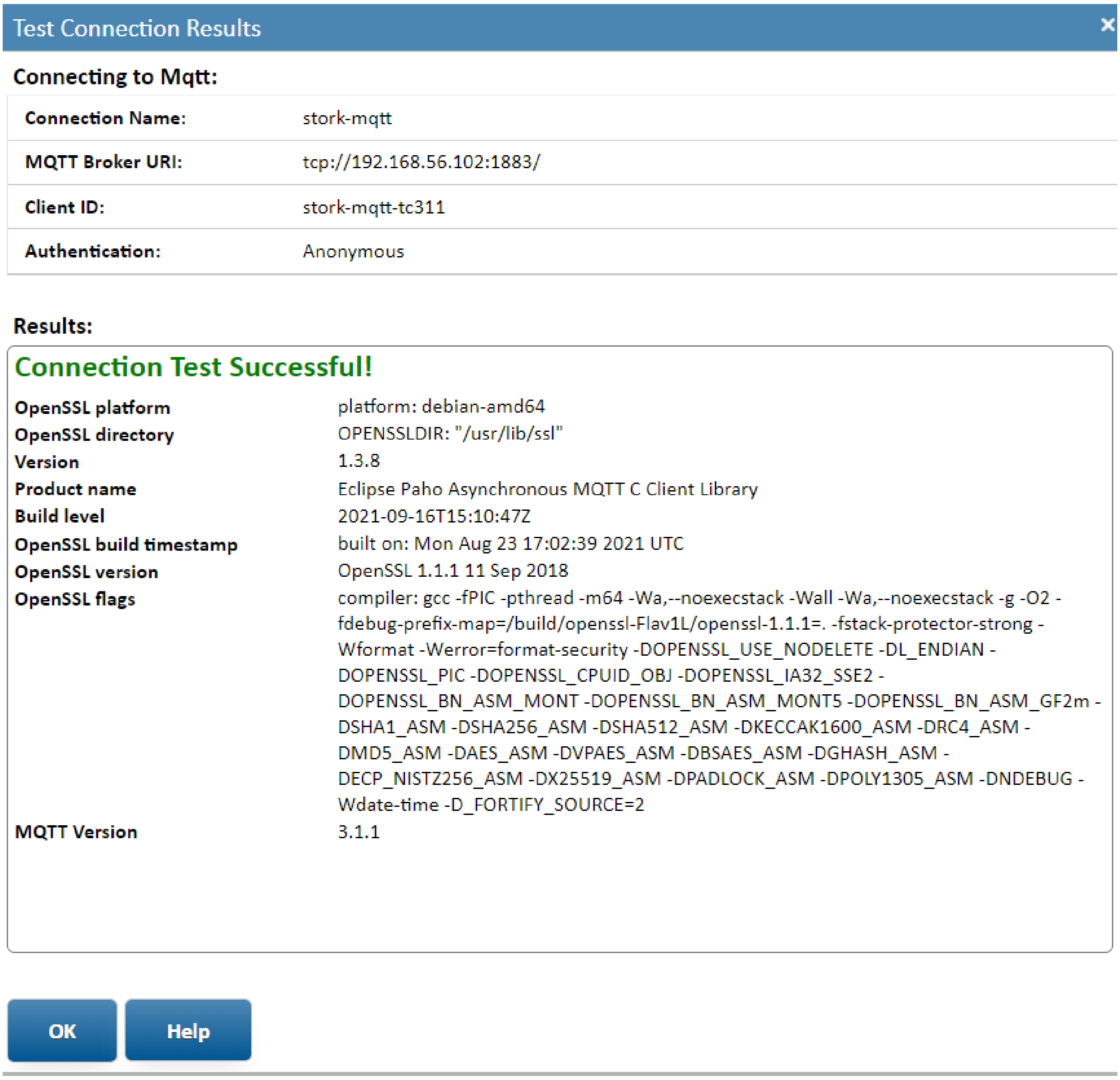
The connection you want to delete has publish requests assigned to it. Deleting it will remove also all the assigned publish requests.
Are you sure you want to continue?

In case of affirmative answer, besides the connection will be deleted also the MQTT Publishers which are using it.

4.6.2.4 Test connection

The test of the current selection is performed using the actual connection parameters.

If the connection is successful, it is displayed a pop-up window similar to the one below.



Test Connection Results

Connecting to Mqtt:

Connection Name:	stork-mqtt
MQTT Broker URI:	tcp://192.168.56.102:1883/
Client ID:	stork-mqtt-tc311
Authentication:	Anonymous

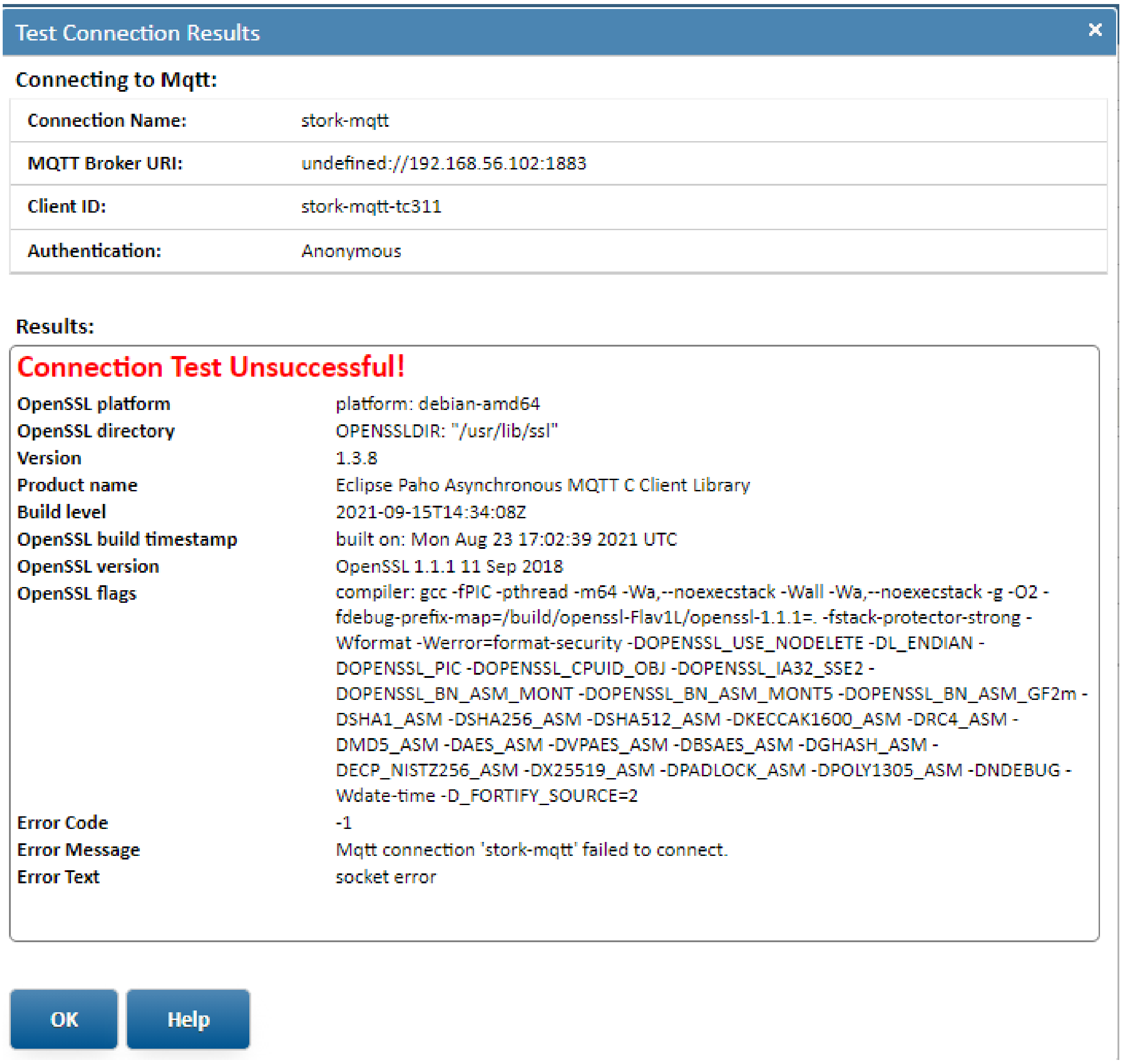
Results:

Connection Test Successful!

OpenSSL platform	platform: debian-amd64
OpenSSL directory	OPENSSLDIR: "/usr/lib/ssl"
Version	1.3.8
Product name	Eclipse Paho Asynchronous MQTT C Client Library
Build level	2021-09-16T15:10:47Z
OpenSSL build timestamp	built on: Mon Aug 23 17:02:39 2021 UTC
OpenSSL version	OpenSSL 1.1.1 11 Sep 2018
OpenSSL flags	compiler: gcc -fPIC -pthread -m64 -Wa,--noexecstack -Wall -Wa,--noexecstack -g -O2 -fdebug-prefix-map=/build/openssl-Flav1L/openssl-1.1.1=. -fstack-protector-strong -Wformat -Werror=format-security -DOPENSSL_USE_NODELETE -DL_ENDIAN -DOPENSSL_PIC -DOPENSSL_CPUID_OBJ -DOPENSSL_IA32_SSE2 -DOPENSSL_BN_ASM_MONT -DOPENSSL_BN_ASM_MONT5 -DOPENSSL_BN_ASM_GF2m -DSHA1_ASM -DSHA256_ASM -DSHA512_ASM -DKECCAK1600_ASM -DRC4_ASM -DMD5_ASM -DAES_ASM -DVPAES_ASM -DBSAES_ASM -DGHASH_ASM -DECP_NISTZ256_ASM -DX25519_ASM -DPADLOCK_ASM -DPOLY1305_ASM -DNDEBUG -Wdate-time -D_FORTIFY_SOURCE=2
MQTT Version	3.1.1

Figure: pop-up dialog shown on successful validation

If the connection is unsuccessful, the pop-up window will contain indication about the error.



Test Connection Results

Connecting to Mqtt:

Connection Name:	stork-mqtt
MQTT Broker URI:	undefined://192.168.56.102:1883
Client ID:	stork-mqtt-tc311
Authentication:	Anonymous

Results:

Connection Test Unsuccessful!

OpenSSL platform	platform: debian-amd64
OpenSSL directory	OPENSSLDIR: "/usr/lib/ssl"
Version	1.3.8
Product name	Eclipse Paho Asynchronous MQTT C Client Library
Build level	2021-09-15T14:34:08Z
OpenSSL build timestamp	built on: Mon Aug 23 17:02:39 2021 UTC
OpenSSL version	OpenSSL 1.1.1 11 Sep 2018
OpenSSL flags	compiler: gcc -fPIC -pthread -m64 -Wa,--noexecstack -Wall -Wa,--noexecstack -g -O2 -fdebug-prefix-map=/build/openssl-Flav1L/openssl-1.1.1=. -fstack-protector-strong -Wformat -Werror=format-security -DOPENSSL_USE_NODELETE -DL_ENDIAN -DOPENSSL_PIC -DOPENSSL_CPUID_OBJ -DOPENSSL_IA32_SSE2 -DOPENSSL_BN_ASM_MONT -DOPENSSL_BN_ASM_MONT5 -DOPENSSL_BN_ASM_GF2m -DSHA1_ASM -DSHA256_ASM -DSHA512_ASM -DKECCAK1600_ASM -DRC4_ASM -DMD5_ASM -DAES_ASM -DVPAES_ASM -DBSAES_ASM -DGHASH_ASM -DECP_NISTZ256_ASM -DX25519_ASM -DPADLOCK_ASM -DPOLY1305_ASM -DNDEBUG -Wdate-time -D_FORTIFY_SOURCE=2
Error Code	-1
Error Message	Mqtt connection 'stork-mqtt' failed to connect.
Error Text	socket error

Figure: pop-up dialog shown on validation with errors

***Warning**: If the connection to be validated is in *Connected* status, the validation will fail because is not possible to connect to the MQTT broker with same *Client ID* if another connection is still active. If for this reason the connection validation fail, it could be re-tried with another *Client ID*.

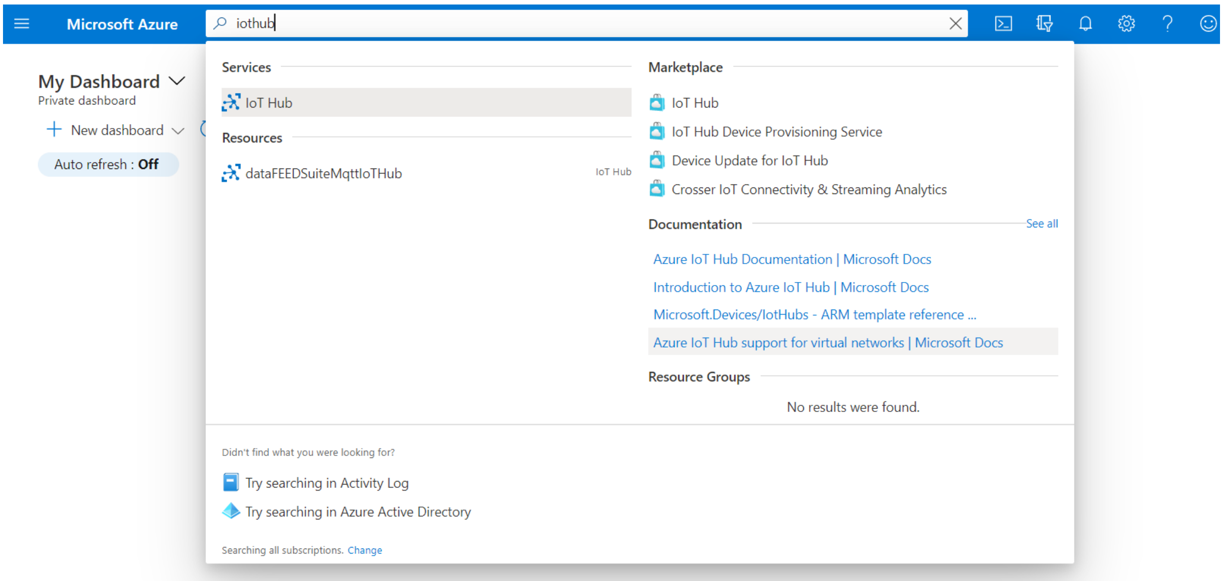
4.6.2.5 Connect to Azure IoT Hub via SSL and WSS

dataFEED Secure Integration Server application supports connections with *Azure IoT Hub*. The steps below are describing the configuration needed in order to create such a connection.

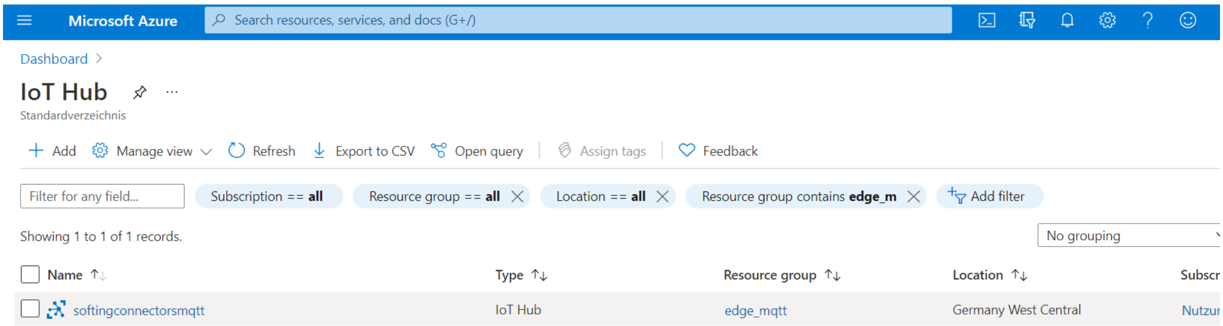
1. Download *Device Explorer* tool. The latest released can be found at: https://github.com/Azure/azure-iot-explorer/releases

2. Connect *Device Explorer* to *Azure IoT Hub*.

- In Microsoft Azure portal search for IoT Hub.


Microsoft Azure
iothub
My Dashboard
Private dashboard
New dashboard
Auto refresh : Off
Services
IoT Hub
Resources
dataFEEDSuiteMqttIoTHub
IoT Hub
Marketplace
IoT Hub
IoT Hub Device Provisioning Service
Device Update for IoT Hub
Crosser IoT Connectivity & Streaming Analytics
Documentation
See all
Azure IoT Hub Documentation | Microsoft Docs
Introduction to Azure IoT Hub | Microsoft Docs
Microsoft.Devices/IotHubs - ARM template reference ...
Azure IoT Hub support for virtual networks | Microsoft Docs
Resource Groups
No results were found.
Didn't find what you were looking for?
Try searching in Activity Log
Try searching in Azure Active Directory
Searching all subscriptions. Change

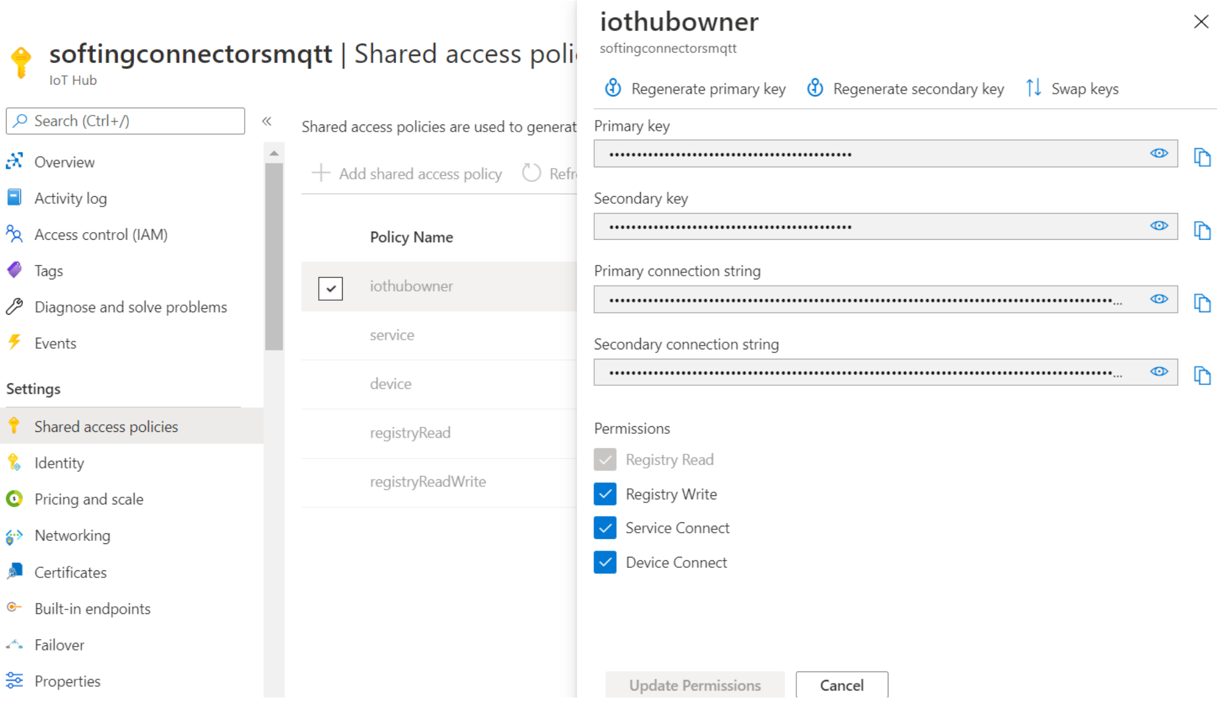
- Select an *IoT Hub* to be connected or select a new one.



Showing 1 to 1 of 1 records.

Name	Type	Resource group	Location	Subscr
softingconnectorsmqtt	IoT Hub	edge_mqtt	Germany West Central	Nutzur

- Select *Shared access policies* Settings



Primary key: ••

Secondary key: ••

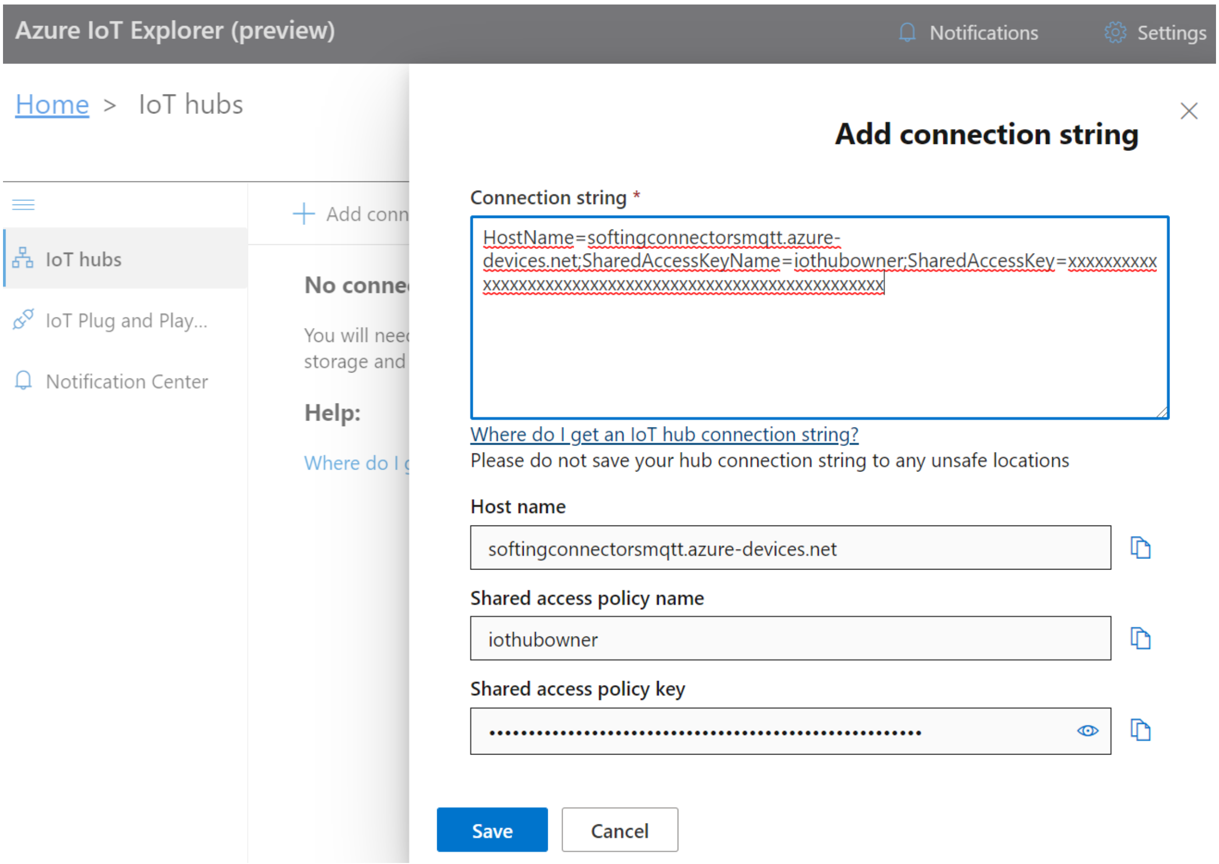
Primary connection string: ••...

Secondary connection string: ••...

Permissions

- ☑ Registry Read
- ☑ Registry Write
- ☑ Service Connect
- ☑ Device Connect

- Select ***iothubowner*** *Policy and copy Connection string - primary key*
- In *Device Explorer*, paste connection string to *IoT Hub Connection String* field and press *Save* button



Connection string *

HostName=softingconnectorsmqtt.azure-devices.net;SharedAccessKeyName=iothubowner;SharedAccessKey=xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx

Where do I get an IoT hub connection string?

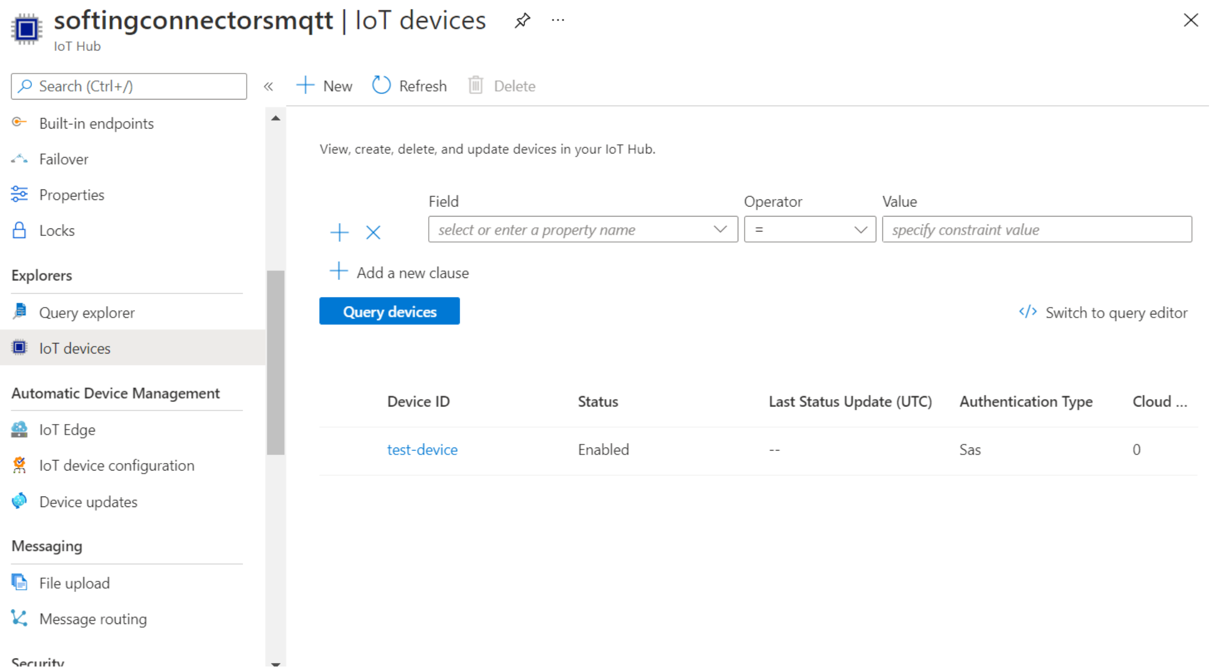
Please do not save your hub connection string to any unsafe locations

Host name: softingconnectorsmqtt.azure-devices.net

Shared access policy name: iothubowner

Shared access policy key: ••

- In *Azure Iot Hub* select *IoT devices* and *Add* a new device



softingconnectorsmqtt | IoT devices

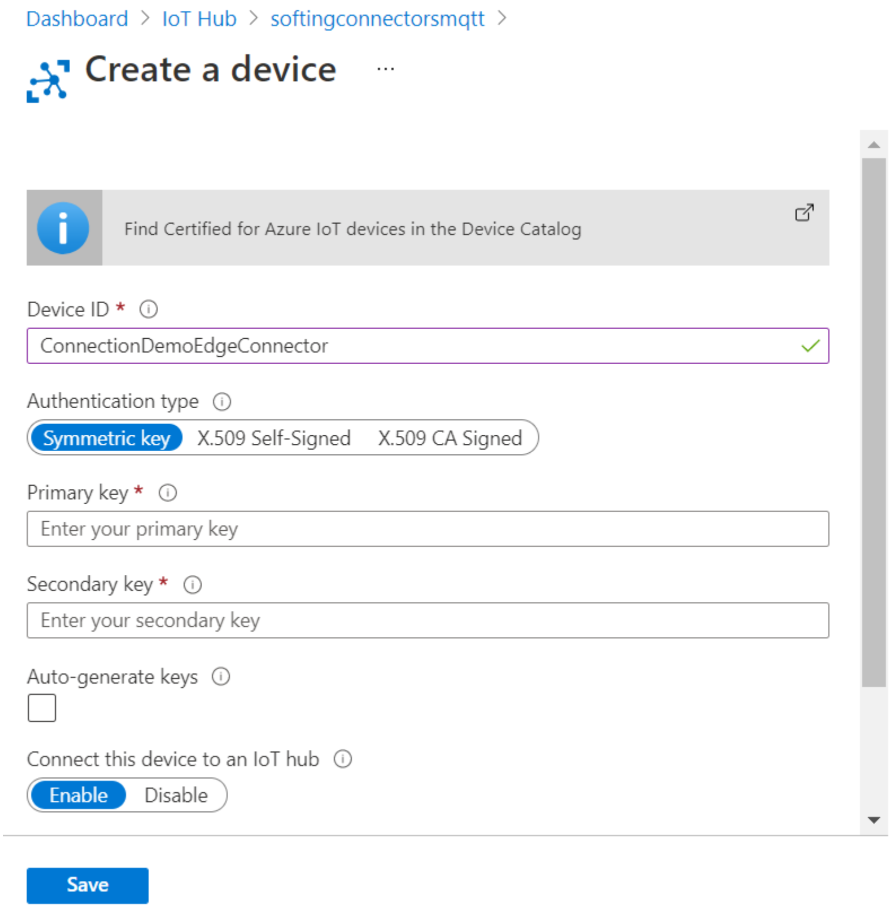
IoT Hub

View, create, delete, and update devices in your IoT Hub.

Field	Operator	Value
select or enter a property name	=	specify constraint value

Device ID	Status	Last Status Update (UTC)	Authentication Type	Cloud ...
test-device	Enabled	--	Sas	0

- Define unique *Device ID* (23 characters maximum)
- Do not modify default settings for rest of the fields and press *Save* button



Dashboard > IoT Hub > softingconnectorsmqtt >

Create a device ...

Find Certified for Azure IoT devices in the Device Catalog

Device ID *
ConnectionDemoEdgeConnector

Authentication type
[✓ Symmetric key] X.509 Self-Signed X.509 CA Signed

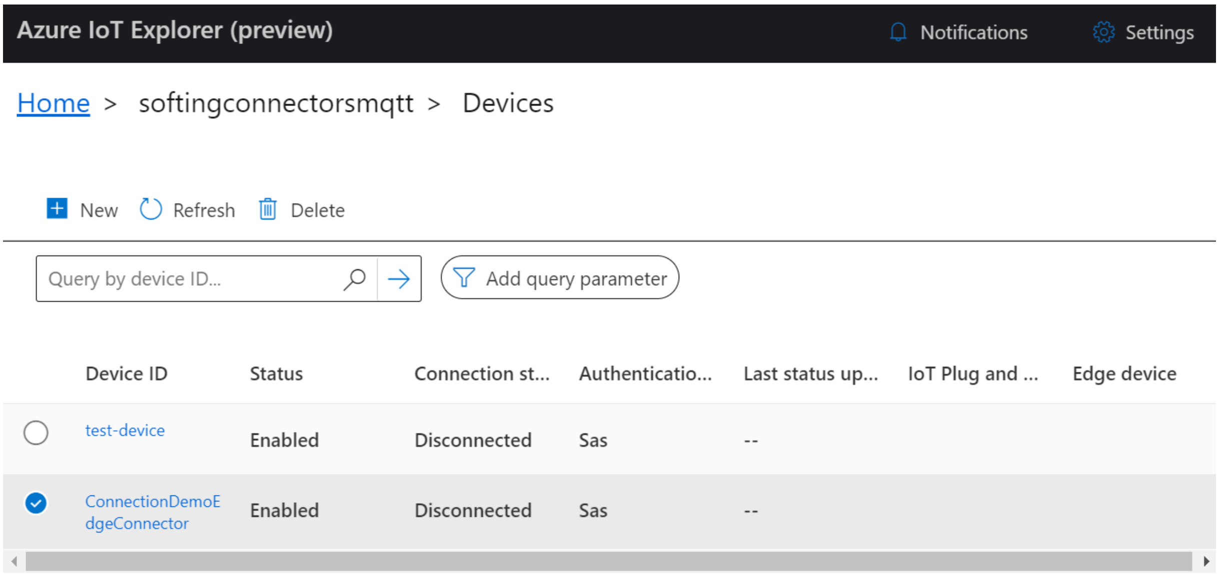
Primary key *
Enter your primary key

Secondary key *
Enter your secondary key

Auto-generate keys
□

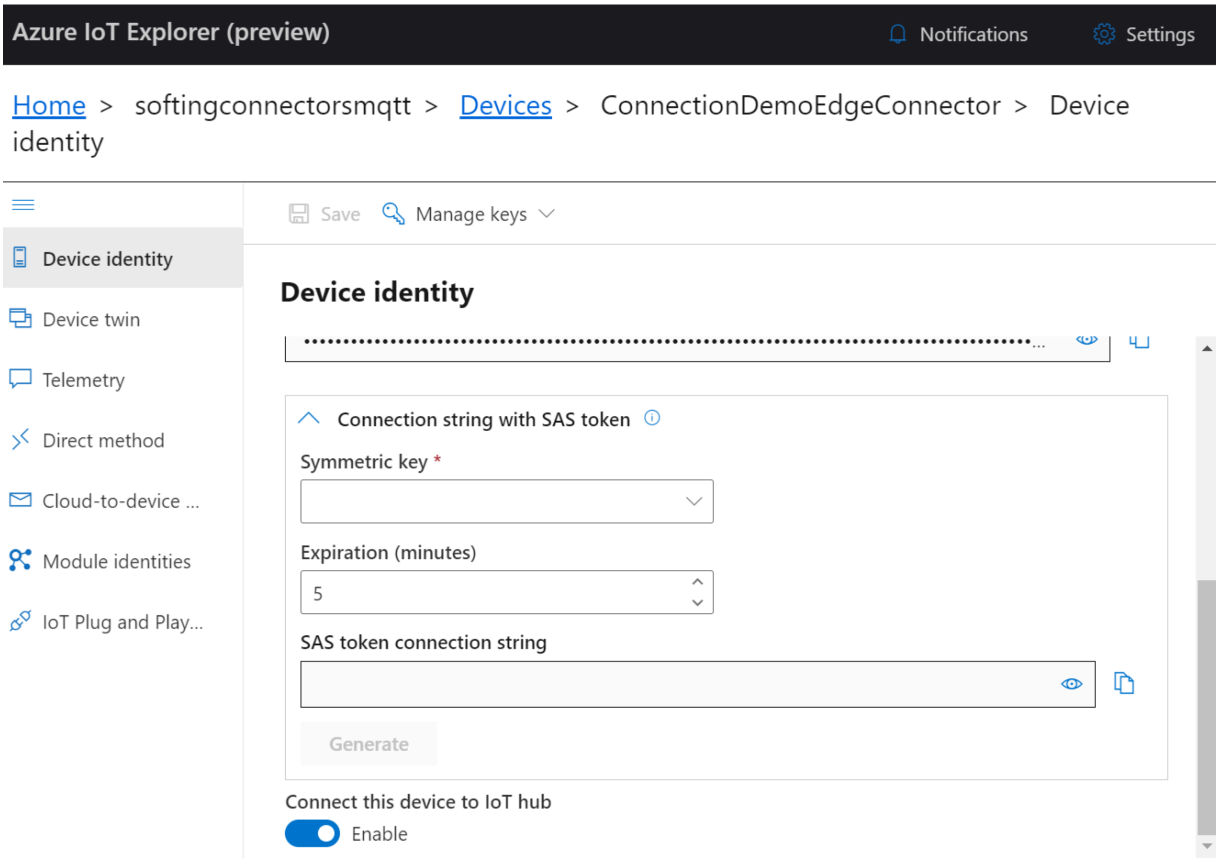
Connect this device to an IoT hub
[✓ Enable] Disable

- The added device will appear in *Device Explorer*



	Device ID	Status	Connection st...	Authenticatio...	Last status up...	IoT Plug and ...	Edge device
○	test-device	Enabled	Disconnected	Sas	--		
●	ConnectionDemoEdgeConnector	Enabled	Disconnected	Sas	--		

- Select the device
- Chose *Device Identity* tab page and expand option *Connection string with SAS token*



Symmetric key *

Expiration (minutes): 5

SAS token connection string

Connect this device to IoT hub: Enable

- Define *SAS token expiration* (e.g. 35 min)
- Chose *Symmetric key* = "Primary key"
- Press *Generate* button
- Copy generated *SAS token* string for later use

3. Connect the Edge connector to *Azure IoT Hub*

- Create new MQTT Connection

○ Enter connection name in Connection Name field

○ Set the hostname of the broker to *<IoT Hub Name>.azure-devices.net*

○ Uncheck *Accept Trusted Certificates Only*

○ Enter *device ID* of created Azure IoT Hub device in *Client ID* field

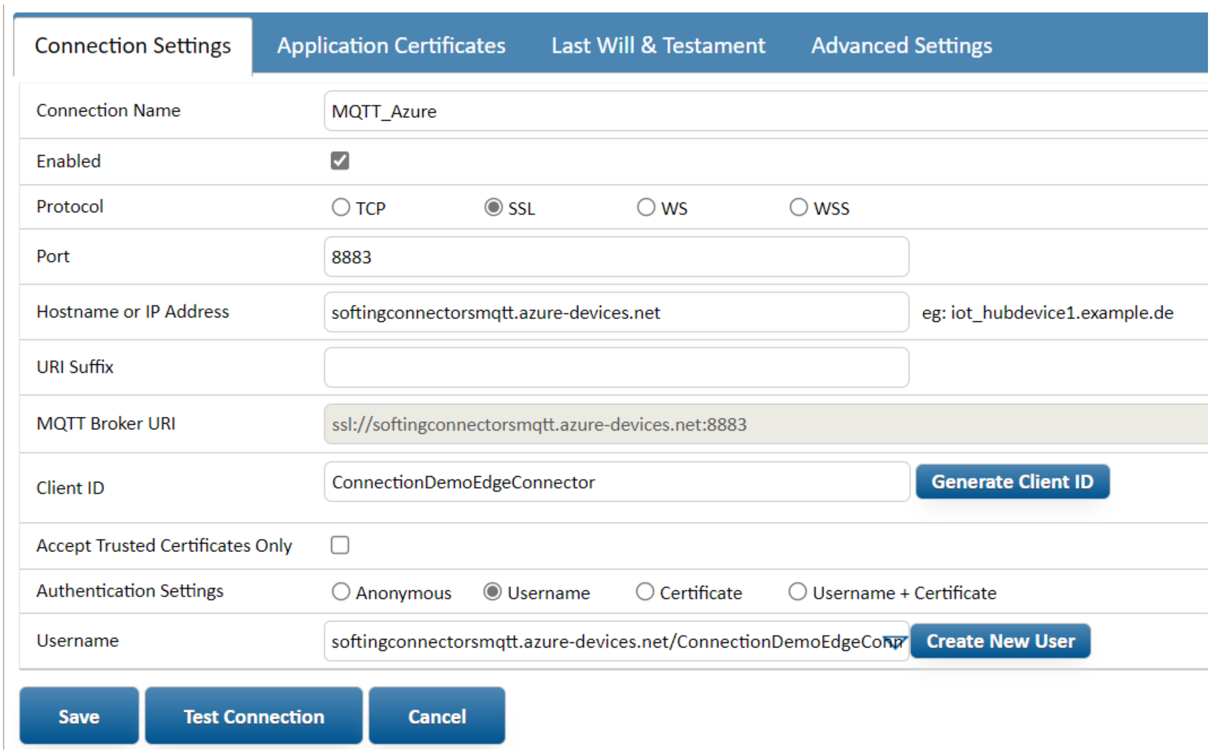
○ Select *SSL* protocol

○ Chose *Authentication settings: Username*

○ Click the button **[New User]**

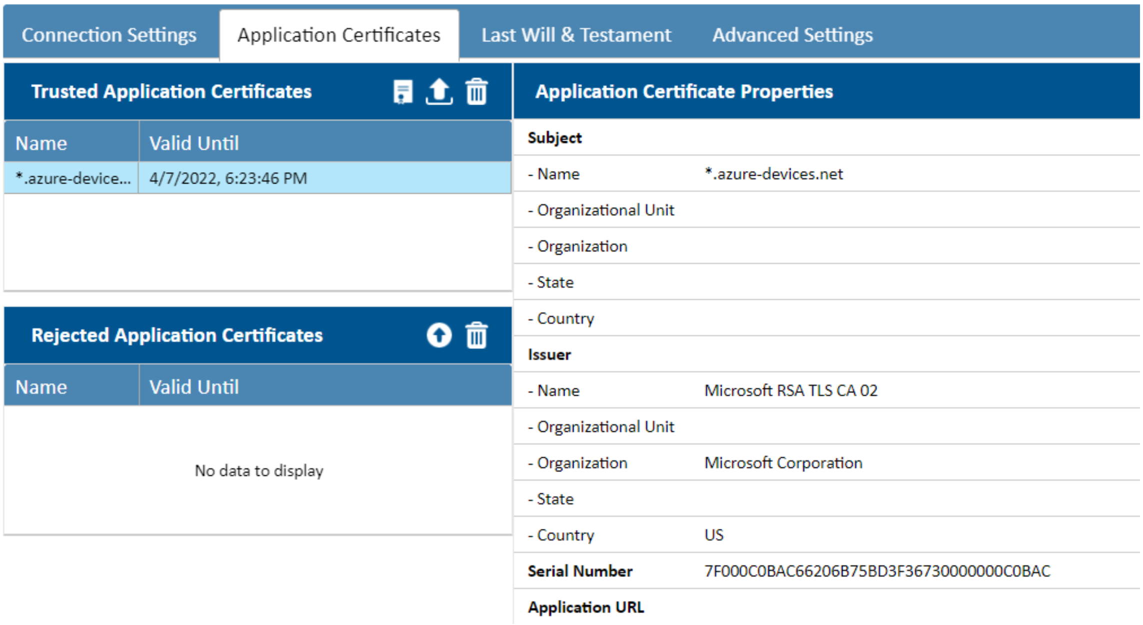
○ Set *Username* in *Authentication Settings* to *<IoT Hub Name>.azure-devices.net/<DeviceID>*

○ Set *Password* in *Authentication Settings* to part of generated *SAS Token* after *SharedAccessSignature=string* (e.g. string beginning with *SharedAccessSignature sr=softingconnectorsmqtt.azure-devices.net*)



Connection Name	MQTT_Azure	
Enabled	☑	
Protocol	○ TCP ● SSL ○ WS ○ WSS	
Port	8883	
Hostname or IP Address	softingconnectorsmqtt.azure-devices.net	eg: iot_hubdevice1.example.de
URI Suffix		
MQTT Broker URI	ssl://softingconnectorsmqtt.azure-devices.net:8883	
Client ID	ConnectionDemoEdgeConnector	
Accept Trusted Certificates Only	□	
Authentication Settings	○ Anonymous ● Username ○ Certificate ○ Username + Certificate	
Username	softingconnectorsmqtt.azure-devices.net/ConnectionDemoEdgeConn	

- Go to tab page Application certificates and press button **[Receive Broker Certificate]**



Trusted Application Certificates

Name	Valid Until
*.azure-device...	4/7/2022, 6:23:46 PM

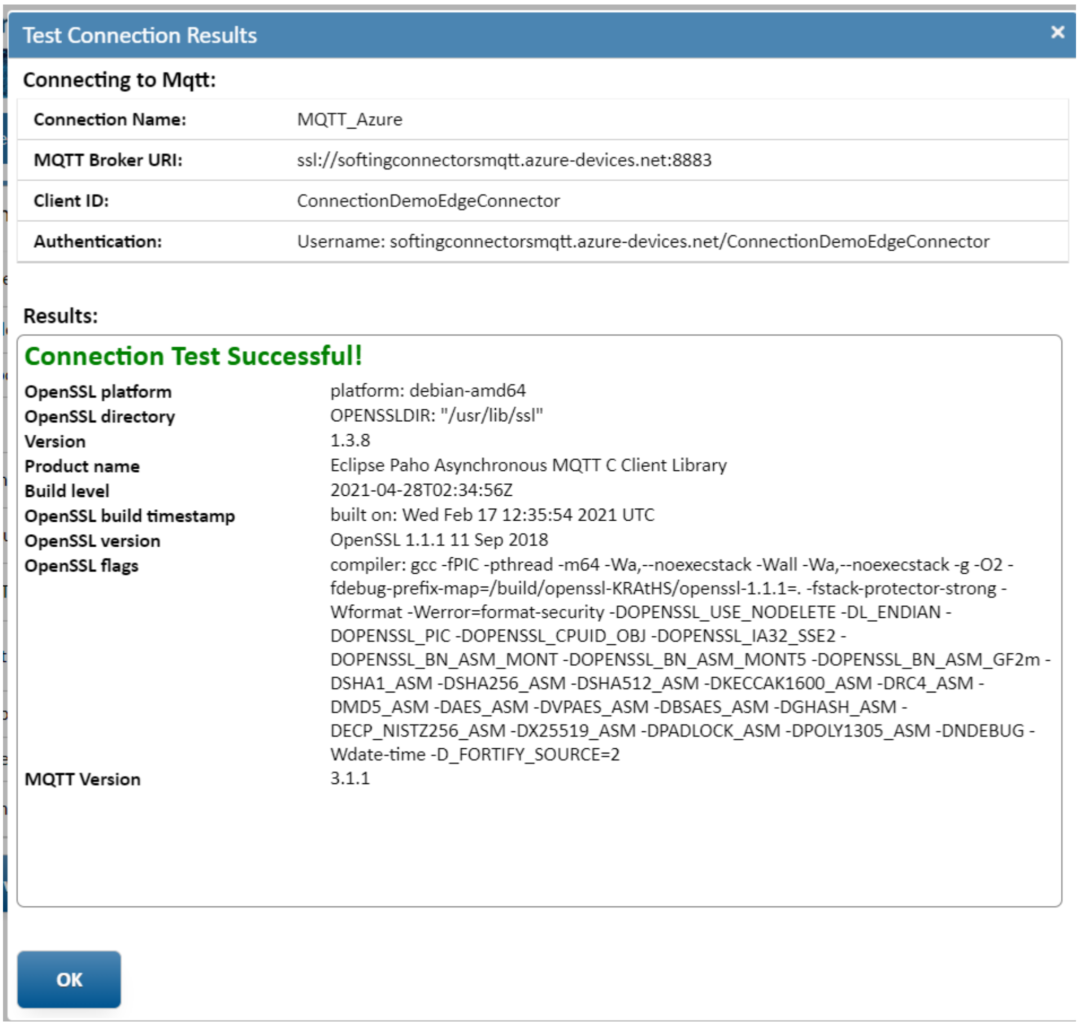
Rejected Application Certificates

Name	Valid Until
No data to display	

Application Certificate Properties

Subject	
- Name	*.azure-devices.net
- Organizational Unit	
- Organization	
- State	
- Country	
Issuer	
- Name	Microsoft RSA TLS CA 02
- Organizational Unit	
- Organization	Microsoft Corporation
- State	
- Country	US
Serial Number	7F000C0BAC66206B75BD3F36730000000C0BAC
Application URL	

- Press **[Test Connection]** button to verify the connection



Connecting to Mqtt:

Connection Name:	MQTT_Azure
MQTT Broker URI:	ssl://softingconnectorsmqtt.azure-devices.net:8883
Client ID:	ConnectionDemoEdgeConnector
Authentication:	Username: softingconnectorsmqtt.azure-devices.net/ConnectionDemoEdgeConnector

Results:

Connection Test Successful!

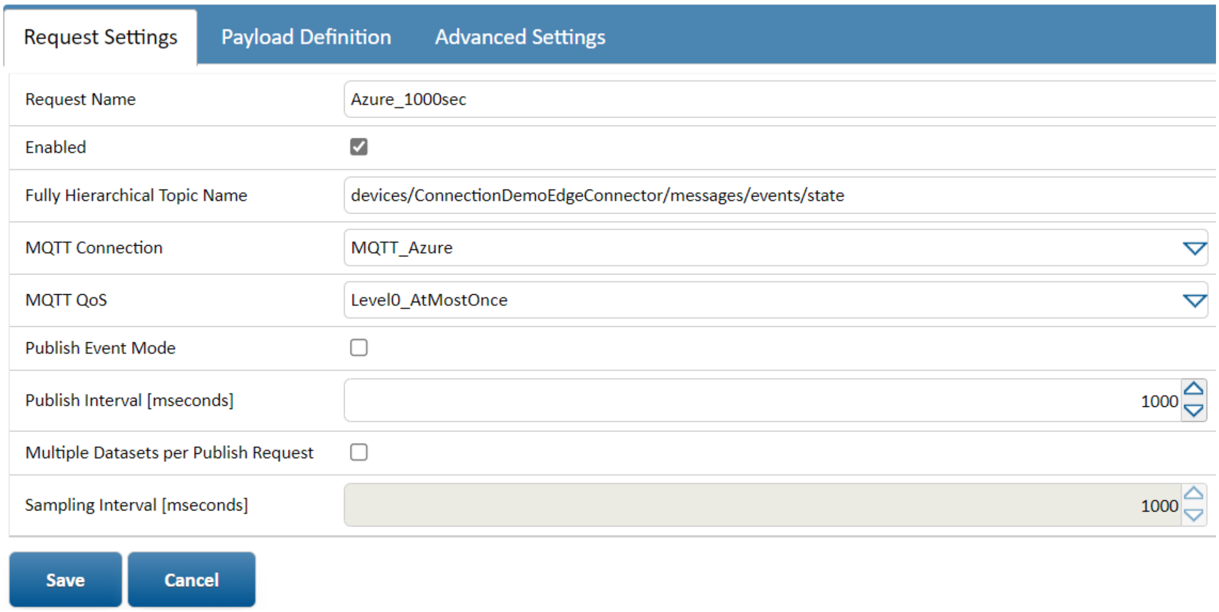
OpenSSL platform	platform: debian-amd64
OpenSSL directory	OPENSSLDIR: "/usr/lib/ssl"
Version	1.3.8
Product name	Eclipse Paho Asynchronous MQTT C Client Library
Build level	2021-04-28T02:34:56Z
OpenSSL build timestamp	built on: Wed Feb 17 12:35:54 2021 UTC
OpenSSL version	OpenSSL 1.1.1 11 Sep 2018
OpenSSL flags	compiler: gcc -fPIC -pthread -m64 -Wa,--noexecstack -Wall -Wa,--noexecstack -g -O2 -fdebug-prefix-map=/build/openssl-KRAtHS/openssl-1.1.1=. -fstack-protector-strong -Wformat -Werror=format-security -DOPENSSL_USE_NODELETE -DL_ENDIAN -DOPENSSL_PIC -DOPENSSL_CPUID_OBJ -DOPENSSL_IA32_SSE2 -DOPENSSL_BN_ASM_MONT -DOPENSSL_BN_ASM_MONT5 -DOPENSSL_BN_ASM_GF2m -DSHA1_ASM -DSHA256_ASM -DSHA512_ASM -DKECCAK1600_ASM -DRC4_ASM -DMD5_ASM -DAES_ASM -DVPAES_ASM -DBSAES_ASM -DGHASH_ASM -DECP_NISTZ256_ASM -DX25519_ASM -DPADLOCK_ASM -DPOLY1305_ASM -DNDEBUG -Wdate-time -D_FORTIFY_SOURCE=2
MQTT Version	3.1.1

*__Note__: If is configured a connection with the protocol WSS, use *URI Suffix=* ***$iothub/websocket***

- Save the connection by pressing **[Save]** button

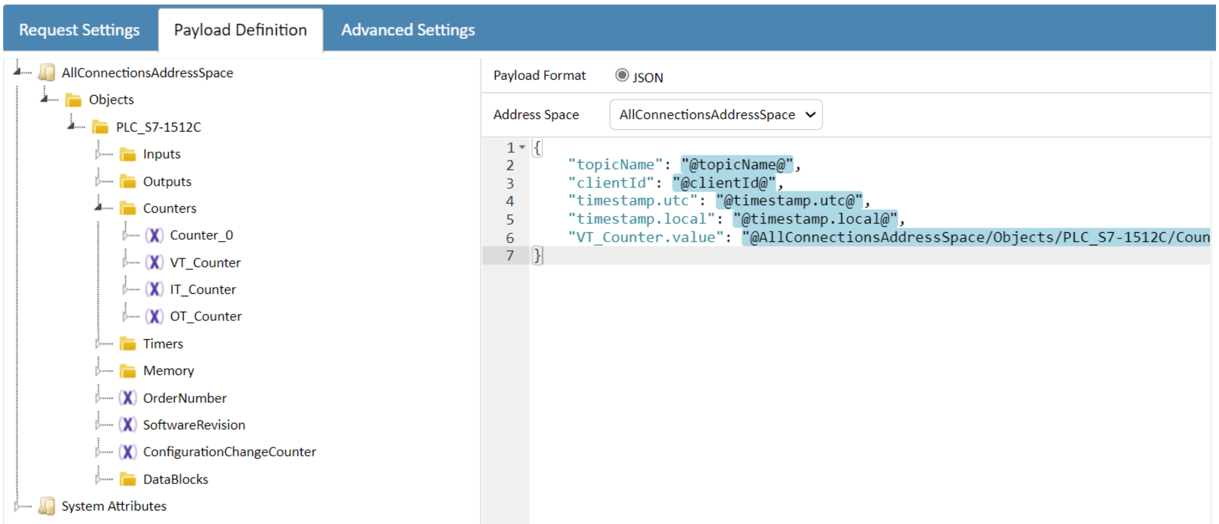
4. Define an MQTT Publisher

- Go to **Connectivity -> MQTT -> MQTT Publisher** and click the button **[Add MQTT Publisher]**
- Give a name to the publisher request
- select the *MQTT Connection* previously created (e.g. MQTT_Azure)
- Enter ***devices/<Device ID>/messages/events/state*** in *Fully Hierarchical Topic Name* field (e.g. devices/ConnectionDemoEdgeConnector/messages/event/state)
- Select *QoS* = ***Level0_AtMostOnce*** and *Publish Interval* = ***1000 ms***



Request Name	Azure_1000sec
Enabled	☑
Fully Hierarchical Topic Name	devices/ConnectionDemoEdgeConnector/messages/events/state
MQTT Connection	MQTT_Azure
MQTT QoS	Level0_AtMostOnce
Publish Event Mode	☐
Publish Interval [mseconds]	1000
Multiple Datasets per Publish Request	☐
Sampling Interval [mseconds]	1000

- Select the payload in tab page *Payload Definition*



Payload Format ● JSON

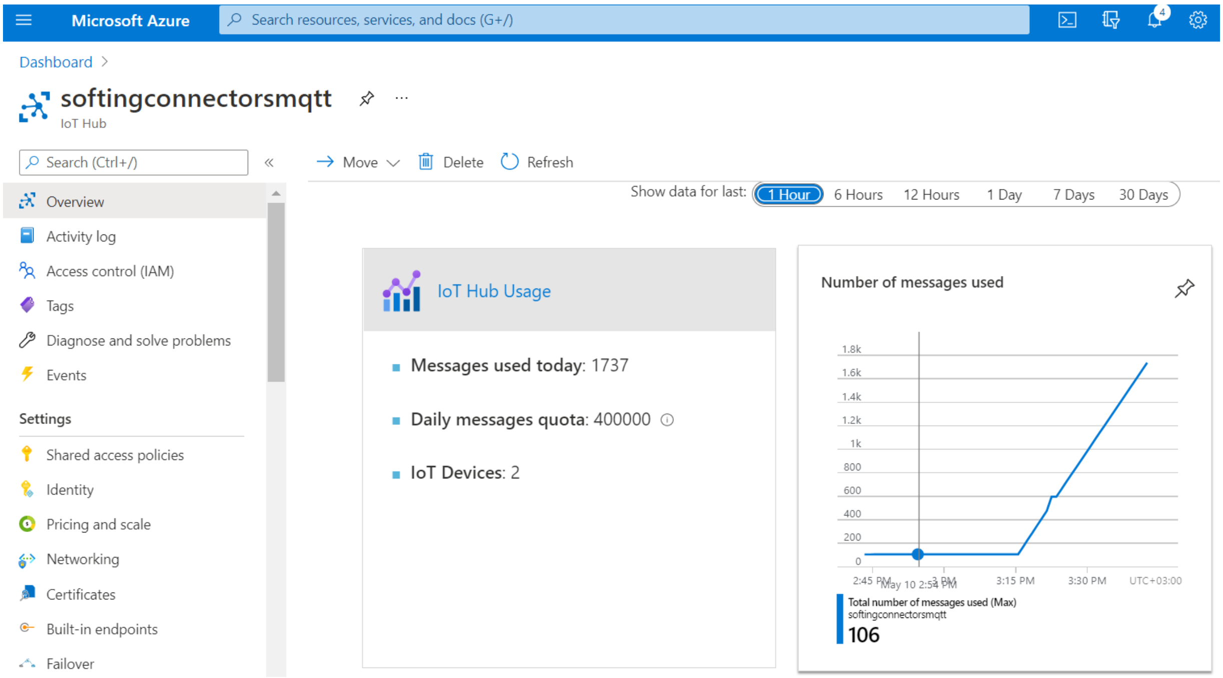
Address Space AllConnectionsAddressSpace

```
{
    "topicName": "@topicName@",
    "clientId": "@clientId@",
    "timestamp.utc": "@timestamp.utc@",
    "timestamp.local": "@timestamp.local@",
    "VT_Counter.value": "@AllConnectionsAddressSpace/Objects/PLC_S7-1512C/Coun
}
```

- Save the publisher request

5. Test the MQTT connection

- check the IoT Hub usage in Azure portal

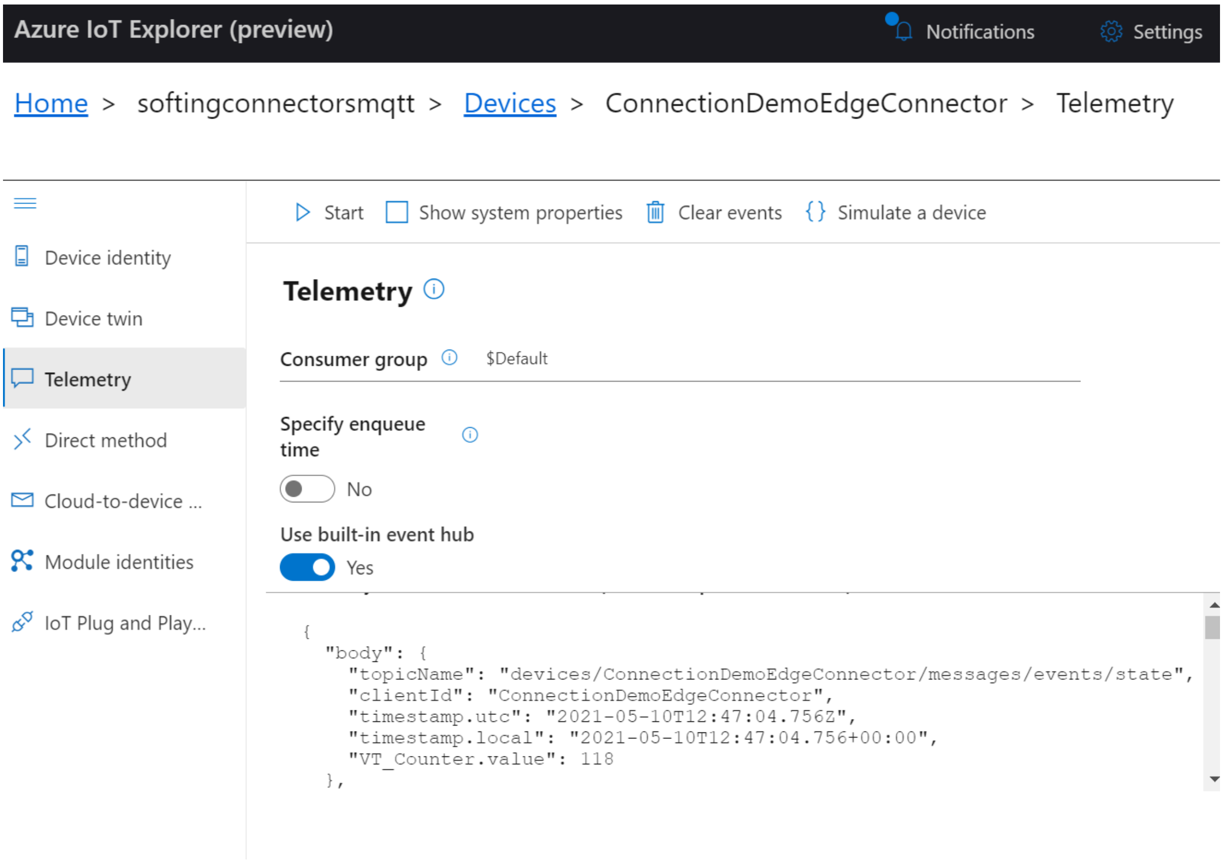


Messages used today: 1737

Daily messages quota: 400000

IoT Devices: 2

- or, in *Azure IoT Explorer*, chose tab page *Telemetry*, click *Start* button and see the received events



Consumer group $Default

Specify enqueue time

No

Use built-in event hub

Yes

```
{
  "body": {
    "topicName": "devices/ConnectionDemoEdgeConnector/messages/events/state",
    "clientId": "ConnectionDemoEdgeConnector",
    "timestamp.utc": "2021-05-10T12:47:04.756Z",
    "timestamp.local": "2021-05-10T12:47:04.756+00:00",
    "VT_Counter.value": 118
  },
```

- click *Stop* button to stop monitoring events.

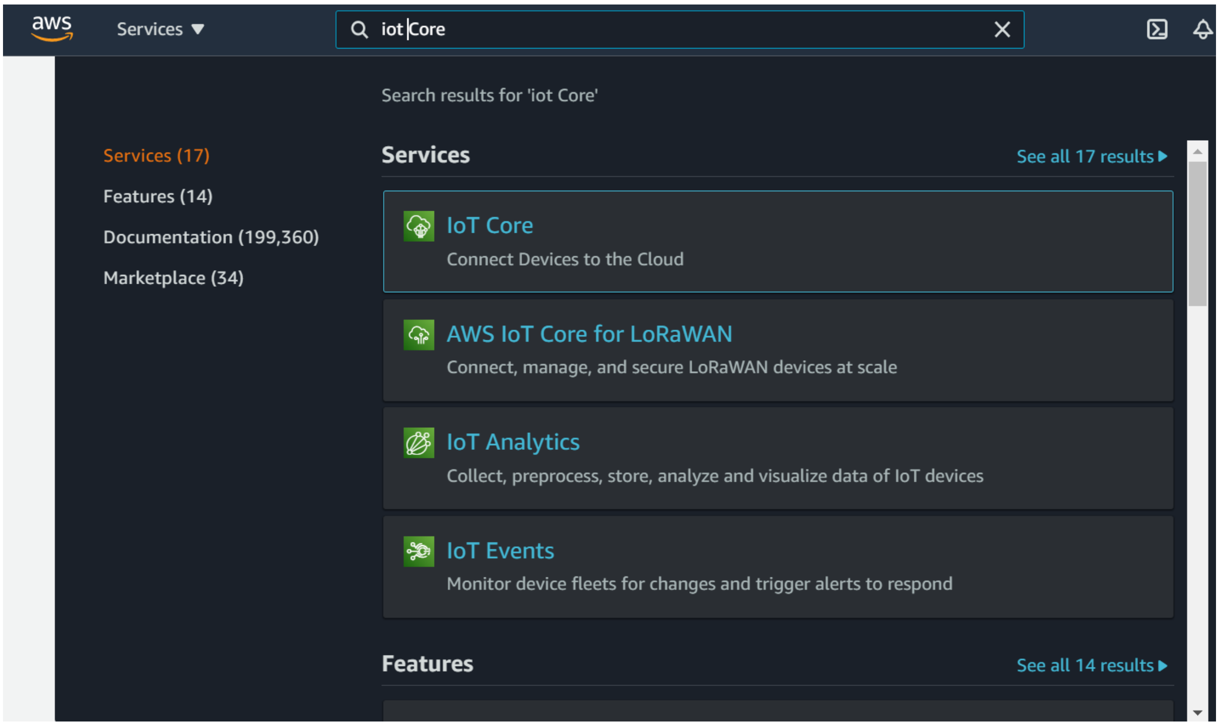
4.6.2.6 Connect to AWS IoT device via SSL

The dataFEED Secure Integration Server application supports connections with *AWS IoT Device*. This topic describes how to configure dataFEED Secure Integration Server as *AWS IoT* device (*"Thing"*).

From the *AWS IoT* point of view dataFEED Secure Integration Server is referred to in this manual as *gateway*. It is based on the the *AWS Developer Guide*, from: https://docs.aws.amazon.com/iot/latest/developerguide/what-is-aws-iot.html.

1. AWS preparation steps

- Go to Amazon AWS Console (https://console.aws.amazon.com/console/home)
- search *IOT Core* service



Search results for 'iot Core'

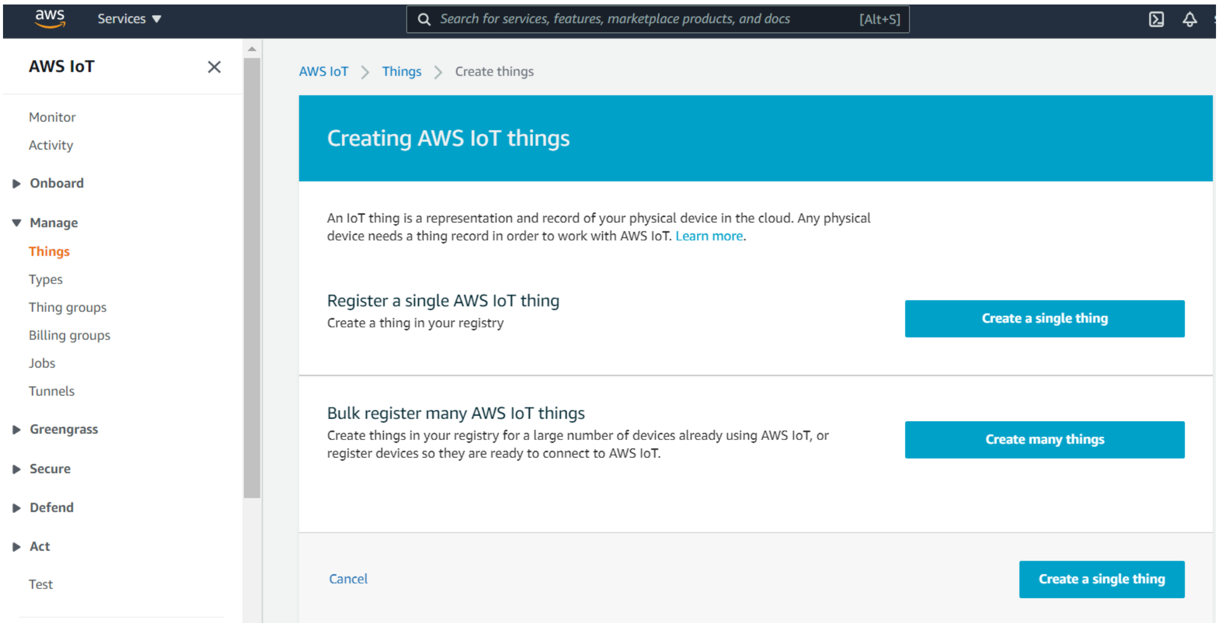
IoT Core
Connect Devices to the Cloud

AWS IoT Core for LoRaWAN
Connect, manage, and secure LoRaWAN devices at scale

IoT Analytics
Collect, preprocess, store, analyze and visualize data of IoT devices

IoT Events
Monitor device fleets for changes and trigger alerts to respond

- Open *IOT Core* service
- Go to option *Manage -> Things* and click *Create* button.



Creating AWS IoT things

An IoT thing is a representation and record of your physical device in the cloud. Any physical device needs a thing record in order to work with AWS IoT. Learn more.

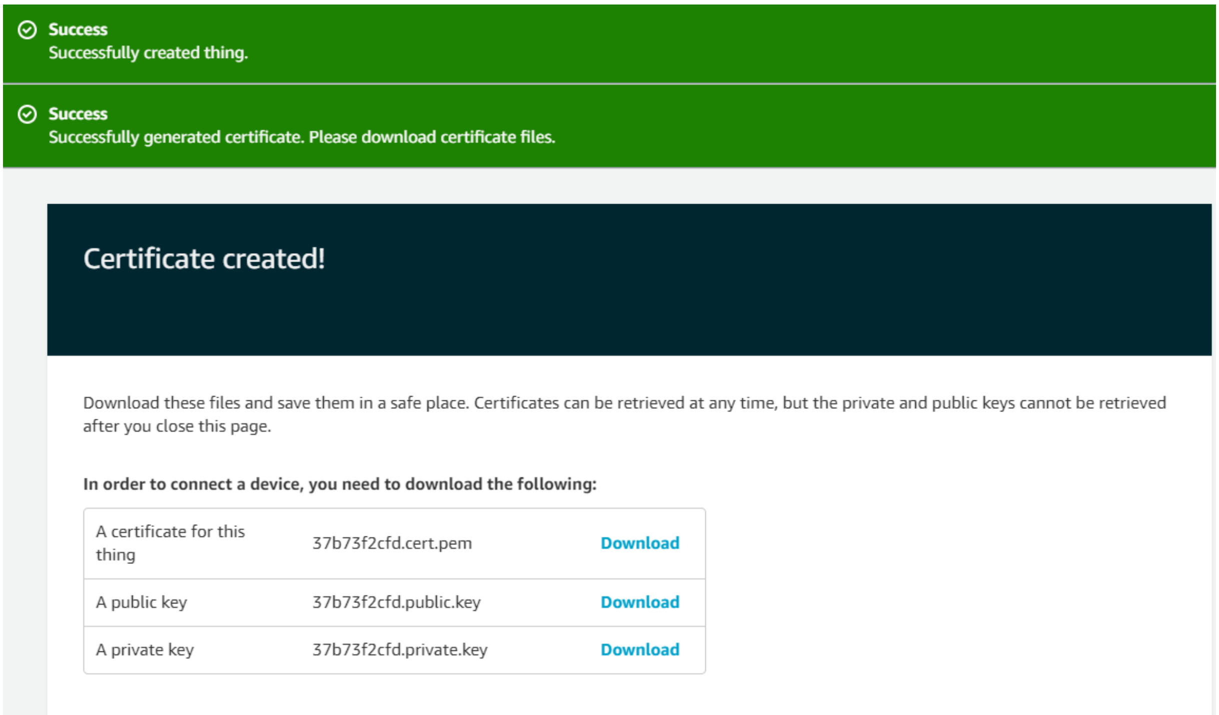
Register a single AWS IoT thing

Create a thing in your registry

Bulk register many AWS IoT things

Create things in your registry for a large number of devices already using AWS IoT, or register devices so they are ready to connect to AWS IoT.

- Click on *Create a single thing*. It will be opened a form for registering the thing/device. In our case our thing/device is the edge connector.
- Give your thing/device a name (e.g. MqttEdgeConnector) and click *Next* for the next page. A new page will be opened for the definition of the certificate associated to the device/thing. Click on *Create certificate* button.
- It will be shown the generated certificates. Download and securely store the certificates for later use.



Success
Successfully created thing.

Success
Successfully generated certificate. Please download certificate files.

Certificate created!

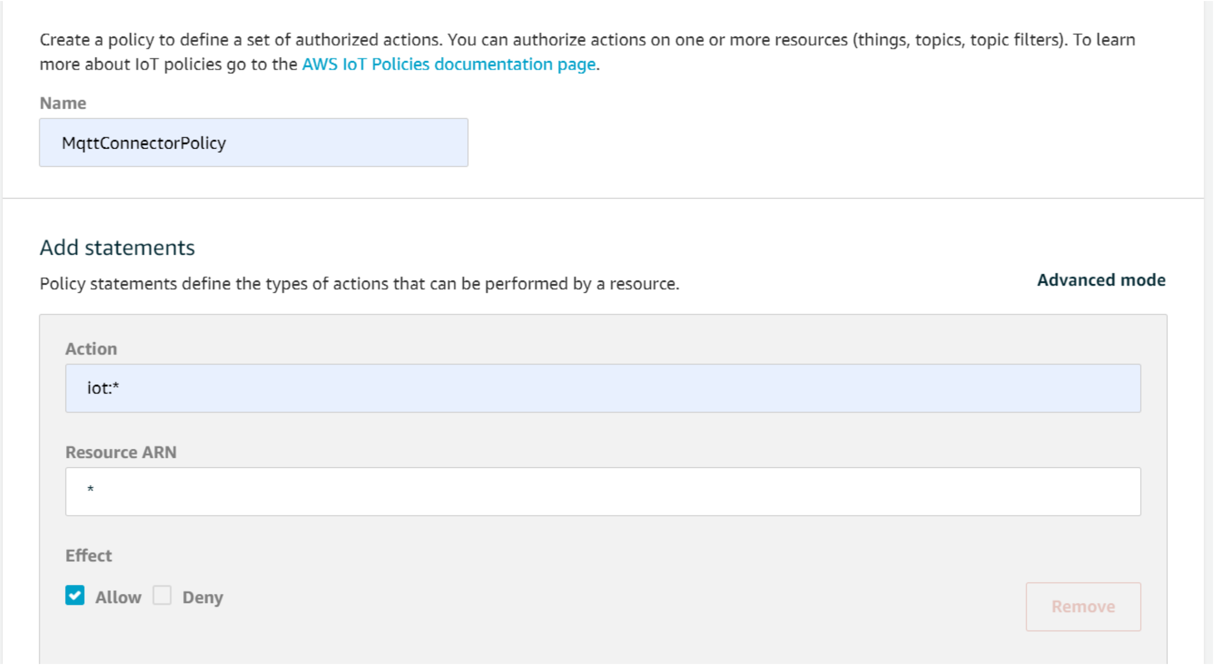
Download these files and save them in a safe place. Certificates can be retrieved at any time, but the private and public keys cannot be retrieved after you close this page.

In order to connect a device, you need to download the following:

A certificate for this thing	37b73f2cfd.cert.pem	Download
A public key	37b73f2cfd.public.key	Download
A private key	37b73f2cfd.private.key	Download

- Click *Done* for completing the creation of the device.
- Next go to menu option *Secure* - > *Policies* and click *Create* button. It will be opened a page for defining the policy to be attached to the certificate.
- Create a new policy, give it a name (e.g. MqttConnectorPolicy) and define the resources and

allowed/denied actions.



Create a policy to define a set of authorized actions. You can authorize actions on one or more resources (things, topics, topic filters). To learn more about IoT policies go to the AWS IoT Policies documentation page.

Name: MqttConnectorPolicy

Add statements

Policy statements define the types of actions that can be performed by a resource.

Action: iot:*

Resource ARN: *

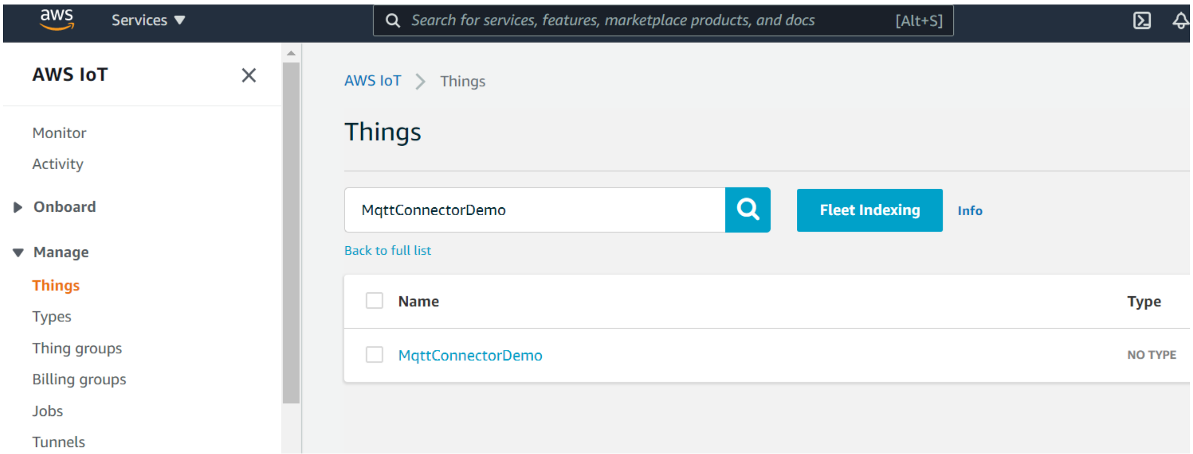
Effect: ☑ Allow □ Deny

- Click on *Create* button.

***Note**: in your real policy statement **be more restrictive**. Using *iot:** for *Action* and * for *Resource ARN* as in the sample above is granting any action to any resource!

- Assign the created policy (or another existing one) to the certificate of the device/thing.

○ search the newly created device

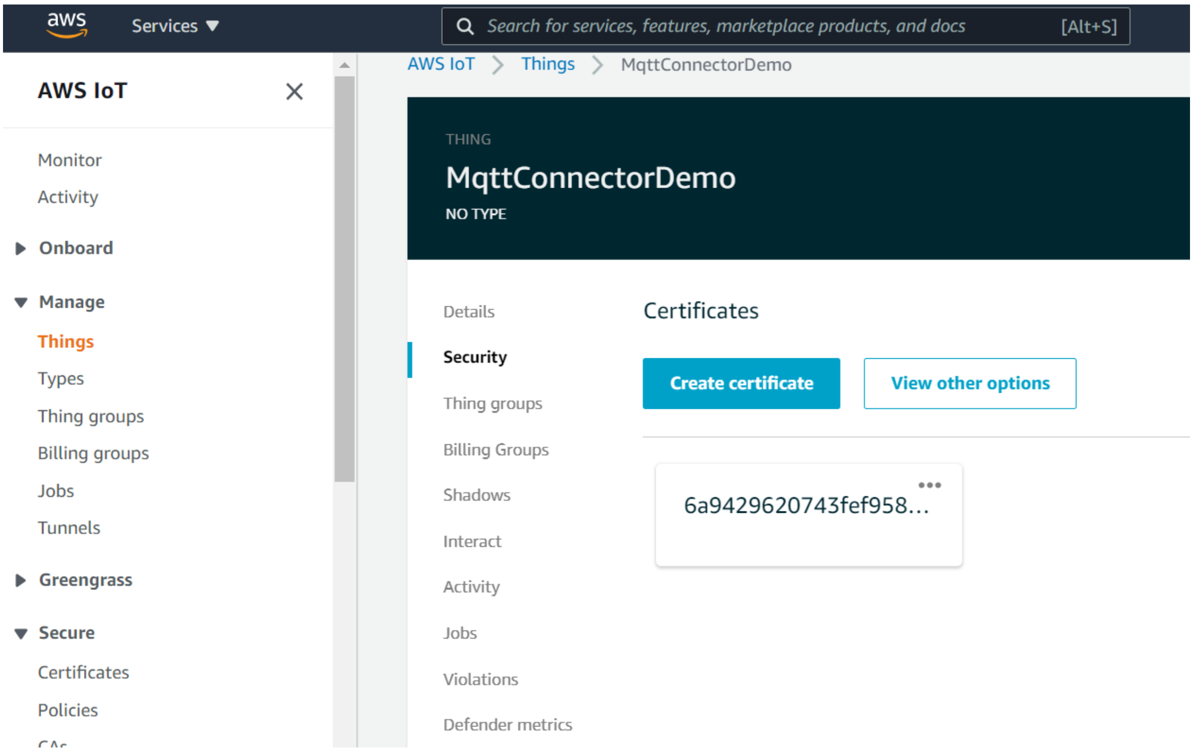


MqttConnectorDemo

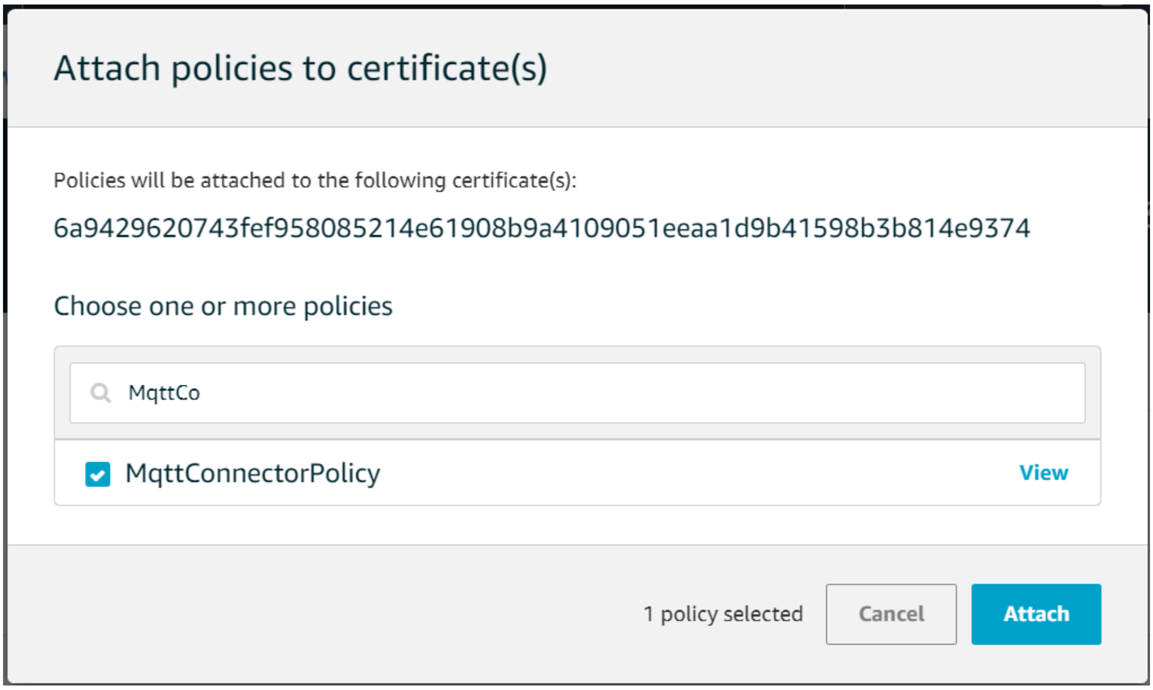
Name	Type
□ MqttConnectorDemo	NO TYPE

○ Click its name

○ Chose from the menu *Security* and visualize the certificate



- ○ Click on the certificate and chose *Policies* from the menu
- ○ Attach to the certificate the created policy (or another existing one)



Attach policies to certificate(s)

Policies will be attached to the following certificate(s):

6a9429620743fef958085214e61908b9a4109051eeaa1d9b41598b3b814e9374

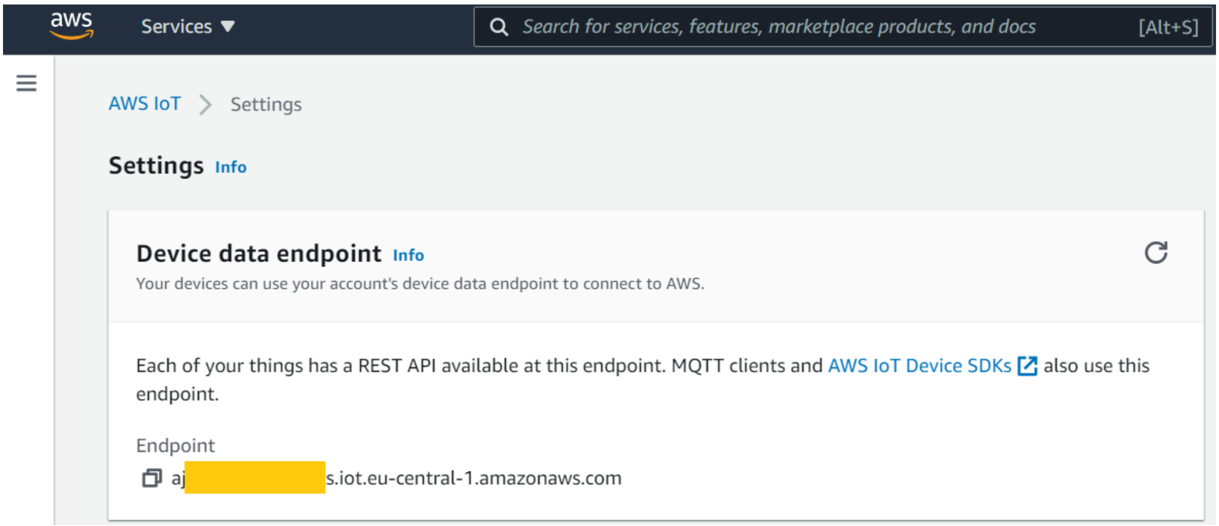
Choose one or more policies

MqttCo

☑ MqttConnectorPolicy View

1 policy selected Cancel Attach

- Go to your AWS IoT Service Settings page and copy the MQTT endpoint URL.



aws
Services ▼
Search for services, features, marketplace products, and docs [Alt+S]
AWS IoT > Settings

Settings Info

Device data endpoint Info

Your devices can use your account's device data endpoint to connect to AWS.

Each of your things has a REST API available at this endpoint. MQTT clients and AWS IoT Device SDKs also use this endpoint.

Endpoint

aj[redacted]s.iot.eu-central-1.amazonaws.com

2. Configure the MQTT Connection.

- Open the configuration application of dataFEED Secure Integration Server .
- In the navigation menu go to **Connectivity -> MQTT -> MQTT Connections**
- Click the toolbar button **[Add MQTT Connection]** and fill the following connection parameters:

○ Connection Name

○ Enabled = *True*

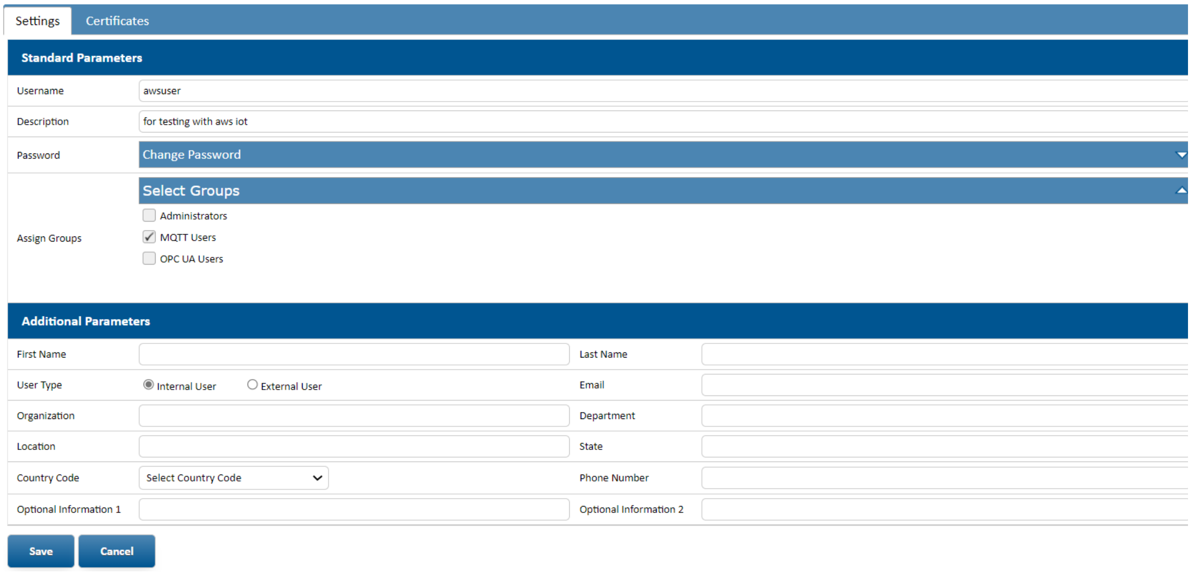
○ Protocol = *SSL*

○ Hostname = <the url copied in AWS IoT Settings page> (see above)

○ Authentication settings = *Certificate*

○ Accept trusted certificates only = *False*

○ Click on **[Create new User]** and create a user with some fake data



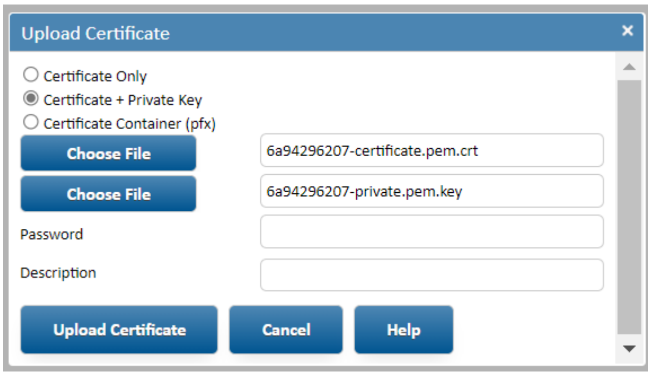
Standard Parameters

Username	awsuser
Description	for testing with aws iot
Password	Change Password
Assign Groups	Select Groups □ Administrators ☑ MQTT Users □ OPC UA Users

Additional Parameters

First Name		Last Name	
User Type	● Internal User ○ External User	Email	
Organization		Department	
Location		State	
Country Code	Select Country Code	Phone Number	
Optional Information 1		Optional Information 2	

○ Go to the *Certificates* tab page of the new user and upload the certificates belonging to the IoT Device/Thing.

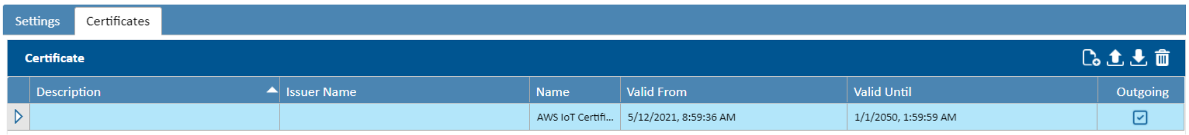


Upload Certificate

○ Certificate Only
● Certificate + Private Key
○ Certificate Container (pfx)

Choose File	6a94296207-certificate.pem.crt
Choose File	6a94296207-private.pem.key
Password	
Description	

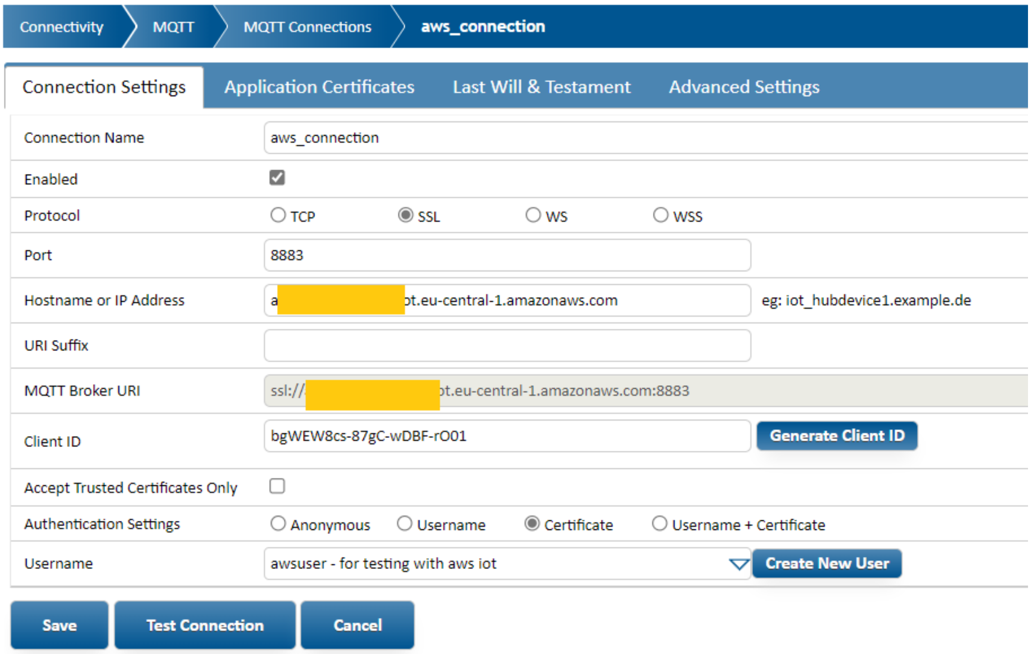
○ Set the *Outgoing* flag of the new certificate to *True*



Certificate

Description	Issuer Name	Name	Valid From	Valid Until	Outgoing
		AWS IoT Certifi...	5/12/2021, 8:59:36 AM	1/1/2050, 1:59:59 AM	☑

○ Test and Save the connection



Connection Name	aws_connection	
Enabled	☑	
Protocol	○ TCP ● SSL ○ WS ○ WSS	
Port	8883	
Hostname or IP Address	a[redacted]t.eu-central-1.amazonaws.com	eg: iot_hubdevice1.example.de
URI Suffix		
MQTT Broker URI	ssl://[redacted]t.eu-central-1.amazonaws.com:8883	
Client ID	bgWEW8cs-87gC-wDBF-rO01	Generate Client ID
Accept Trusted Certificates Only	□	
Authentication Settings	○ Anonymous ○ Username ● Certificate ○ Username + Certificate	
Username	awsuser - for testing with aws iot	Create New User

3. Configure an *MQTT Publisher* using previously created MQTT Connection

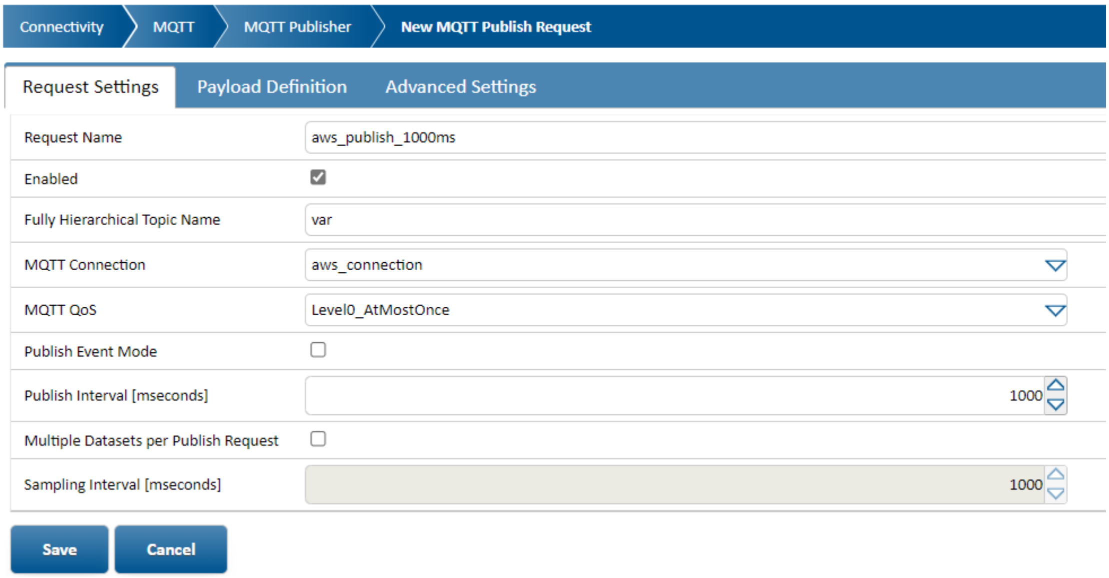
- Open the configuration application of dataFEED Secure Integration Server .
- In the navigation menu go to **Connectivity -> MQTT -> MQTT Publisher**
- Click the toolbar button **[Add MQTT Publisher]** and fill the following connection parameters:

○ The *Request Name*

○ *Enabled* = True

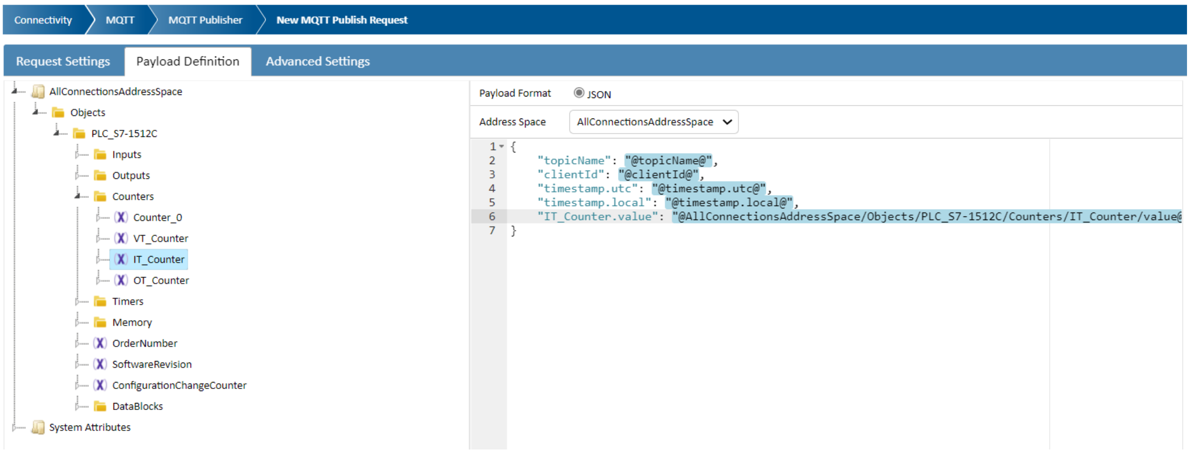
○ *MQTT Connection* = <the MQTT connection configured in step 2> (E.G. aws_connection)

○ *Fully Hierarchical Topic Name* = <the path of the topic to write messages>



Request Name	aws_publish_1000ms
Enabled	☑
Fully Hierarchical Topic Name	var
MQTT Connection	aws_connection
MQTT QoS	Level0_AtMostOnce
Publish Event Mode	□
Publish Interval [mseconds]	1000
Multiple Datasets per Publish Request	□
Sampling Interval [mseconds]	1000

- ○ Chose in the payload of the publisher a variable having dynamic value



Payload Format ● JSON

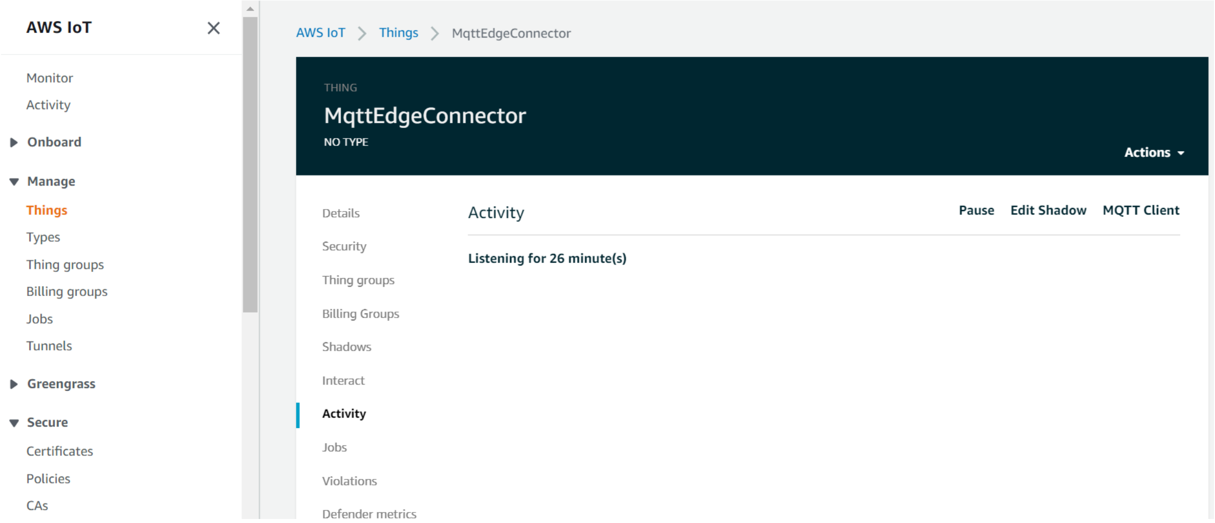
Address Space: AllConnectionsAddressSpace

```
{
    "topicName": "@topicName@",
    "clientId": "@clientId@",
    "timestamp.utc": "@timestamp.utc@",
    "timestamp.local": "@timestamp.local@",
    "IT_Counter.value": "@AllConnectionsAddressSpace/Objects/PLC_S7-1512C/Counters/IT_Counter/value@
}
```

- ○ *Save* the publisher configuration

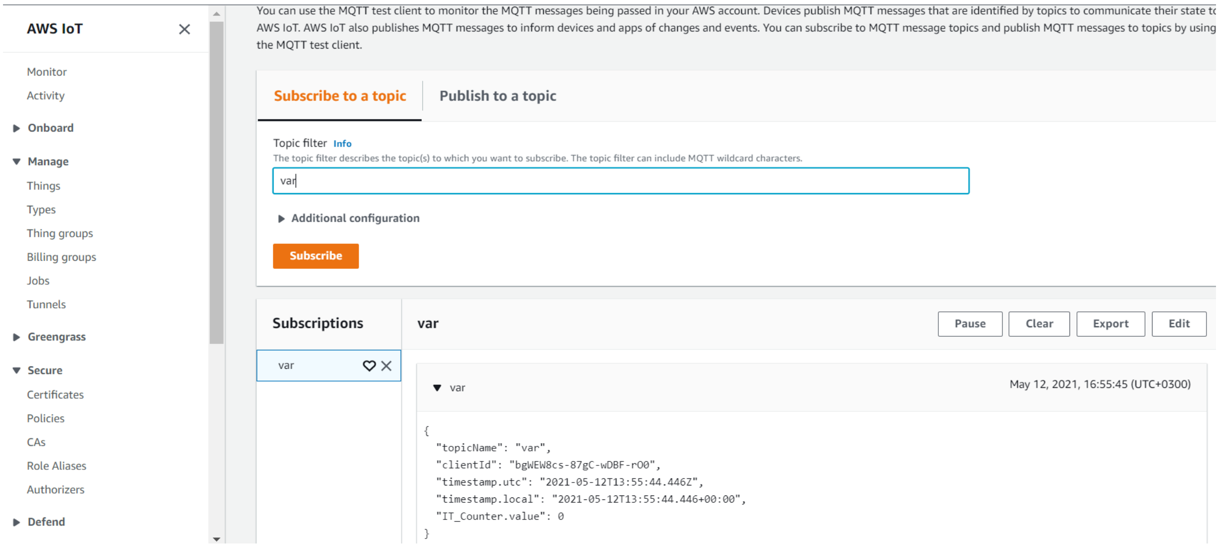
4. Test message publishing

- Go to Amazon AWS Console (https://console.aws.amazon.com/console/home)
- Search the device corresponding to the Edge connector in AWS IoT Services and go to *Activity* tab page



Listening for 26 minute(s)

- Chose option *MQTT Client* and visualize the messages incoming on the topic configured in the MQTT Publisher (e.g. var)



You can use the MQTT test client to monitor the MQTT messages being passed in your AWS account. Devices publish MQTT messages that are identified by topics to communicate their state to AWS IoT. AWS IoT also publishes MQTT messages to inform devices and apps of changes and events. You can subscribe to MQTT message topics and publish MQTT messages to topics by using the MQTT test client.

Topic filter Info

The topic filter describes the topic(s) to which you want to subscribe. The topic filter can include MQTT wildcard characters.

var

var

var

May 12, 2021, 16:55:45 (UTC+0300)

```
{
  "topicName": "var",
  "clientId": "bgWEW8cs-87gC-wDBF-rO0",
  "timestamp.utc": "2021-05-12T13:55:44.446Z",
  "timestamp.local": "2021-05-12T13:55:44.446+00:00",
  "IT_Counter.value": 0
}
```

- check the payload content

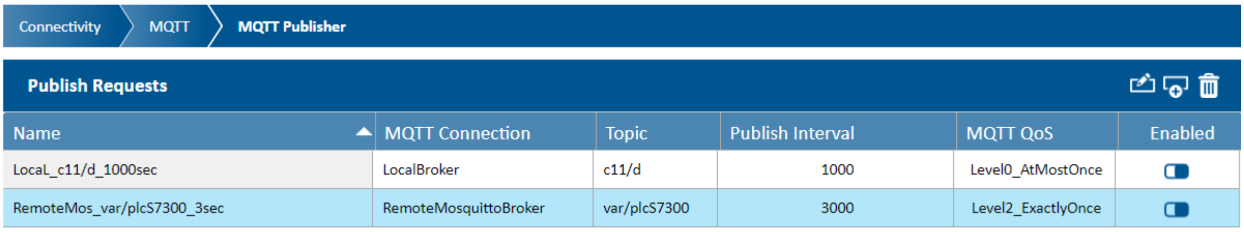
4.6.3 MQTT Publisher

The logical sequence for configuring the MQTT connectivity is:

1. definition of MQTT broker connections
2. definition of publishing jobs

Information about all configured MQTT publisher jobs is centralized and accessible by navigating to **Connectivity -> MQTT -> MQTT Publisher**.

The page displays the list of defined connections or the message *'No data to display'*.



Connectivity > MQTT > MQTT Publisher

Publish Requests

Name	MQTT Connection	Topic	Publish Interval	MQTT QoS	Enabled
Local_c11/d_1000sec	LocalBroker	c11/d	1000	Level0_AtMostOnce	●
RemoteMos_var/plcS7300_3sec	RemoteMosquittoBroker	var/plcS7300	3000	Level2_ExactlyOnce	●

Figure: List of configured MQTT publisher jobs

The table header information is described below:

Column name	Information details
Name	User defined name of the publishing job
MQTT Connection	The MQTT Connection used by the publishing job. see MQTT Connections 91.
Topic	MQTT Topic to publish to.
Publish Interval	Value in milliseconds of the time interval between successive publish operations. ***Note:** For the publish requests configured with *Data Point Triggered* Mode, the displayed value is "*N/A*".
MQTT QoS	Quality of Service level of the published messages.
Enabled	Toggle which enable or disable a publisher job. By disabling it, the publisher is stopping sending messages. It is not sufficient that the publisher job is enabled in order to send messages to the broker. It is needed also that the connection which is used by the publishing job to be enabled too. By disabling an MQTT connection (see Modify Connection 105), all publishers which are using it are stopping sending messages. By enabling an MQTT connection (see Modify Connection 105), all publishers which are using it and are in *Enabled* state, are re-starting to send messages.

Table: Publisher jobs list

The **Publish Requests** information bar provides four buttons with the following functionality:

Button	Action
⊕	Add new publishing job
✎	Modify the selected publishing job
🗑	Delete the selected publishing job

Table: List of actions for handling the MQTT publishing jobs

***Note**: Throughout the rest of the documentation the notions *MQTT Publisher*, *publisher job* or *publisher request* are equivalent.

4.6.3.1 Add publish request

By clicking the **[Add MQTT Publisher]** ⊕ button located in the MQTT Publisher 124 page**,** the context is switched to the definition of the parameters needed to create a new publisher job.

It contains three tab pages, each grouping the following parameter sets:

Request Settings 125

Payload definition 132

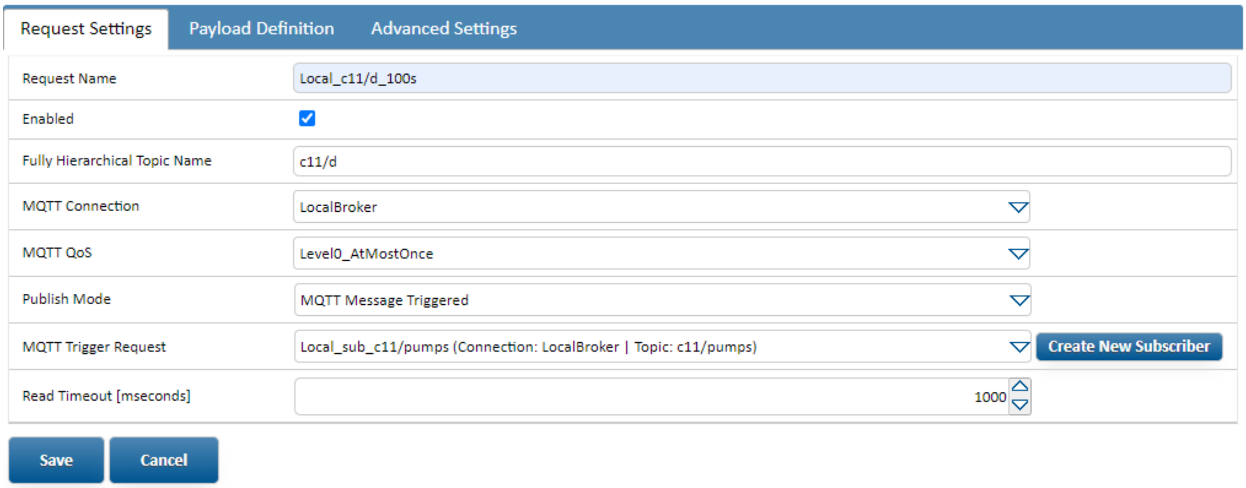
Advanced Settings 137

Advanced Trigger 142

Note: A maximum number of 100 publish requests per connection is allowed.

4.6.3.1.1 Request Settings

The tab page *Request Settings* contains the parameters which are mandatory for any publisher request.



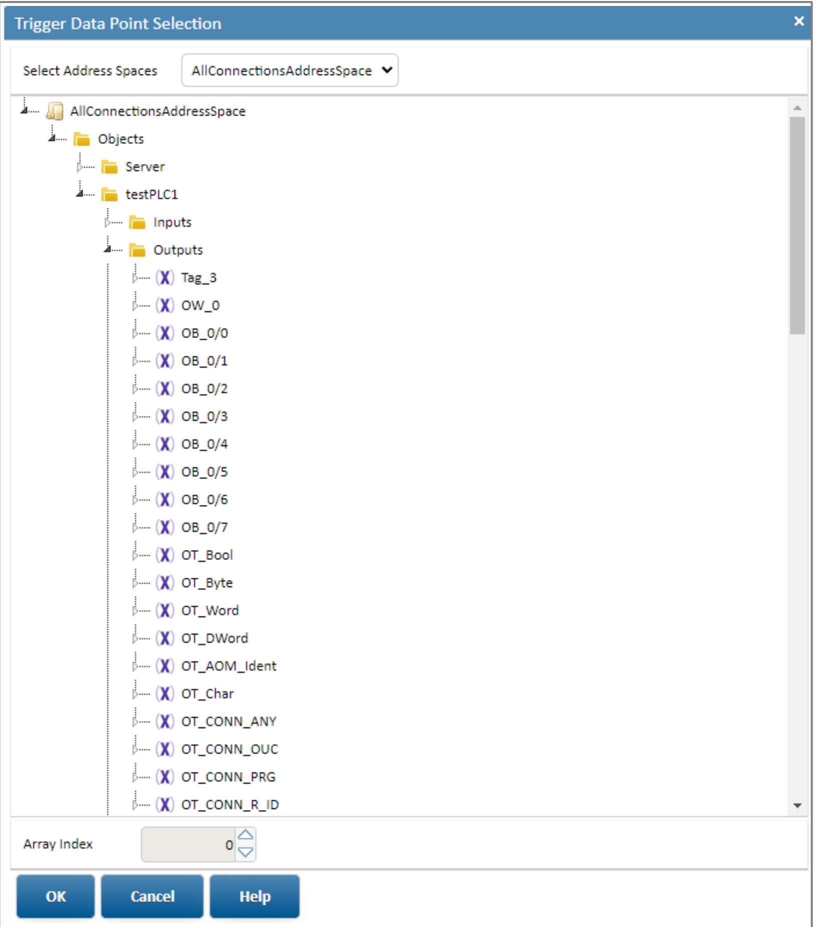
Request Name	Local_c11/d_100s
Enabled	☑
Fully Hierarchical Topic Name	c11/d
MQTT Connection	LocalBroker
MQTT QoS	Level0_AtMostOnce
Publish Mode	MQTT Message Triggered
MQTT Trigger Request	Local_sub_c11/pumps (Connection: LocalBroker | Topic: c11/pumps)
Read Timeout [mseconds]	1000

Figure: Request Settings tab page

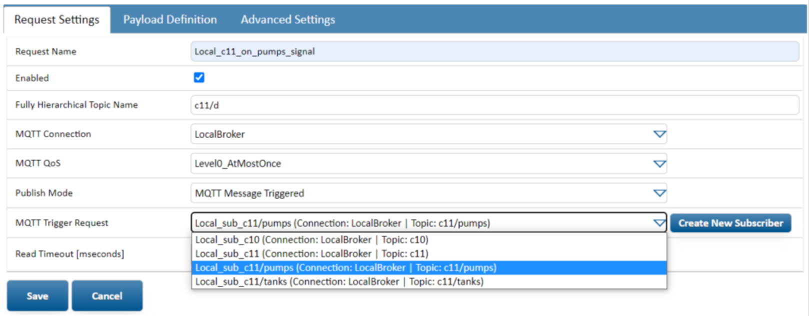
Parameter name	Default value	Value description
Request Name	**empty**	Defines the publisher request name as it will be displayed in the MQTT Publisher overview page.
Enabled	**Enabled**	Enable (checked) or disable (unchecked) the currently configured publisher request. If disabled, the publisher is stopping sending messages. It is not sufficient that the publisher job is enabled in order to send messages to the broker. It is needed also that the connection which is used by the publishing job to be enabled too. By disabling an MQTT connection (see Modify Connection 105), all publishers which are using it are stopping sending messages. By enabling an MQTT connection (see Modify Connection 105), all publishers which are using it and are in *Enabled* state, are re-starting to send messages.
Fully Hierarchical Topic Name	**empty**	The topics are described in the MQTT specification and define where the messages will be published. MQTT Topics are structured in a hierarchy similar to folders and files in a file system using the forward slash (/)as a delimiter. ***Note**: topics are: • Case sensitive • use UTF-8 strings. • Must consist of at least one character to be valid.
MQTT Connection	**First in the list of defined connections**	Combo-box to select the MQTT Connection used for the publish request.

MQTT QoS	**Level0_AtMostOnce**	Quality of Service level of the published messages. Possible values: • Level0_AtMostOnce • Level1_AtLeastOnce • Level2_ExactlyOnce These levels are described in the MQTT specification and defines the guarantee of delivery for a specific message.
Publish Mode	**Standard**	Application specific parameter, represented by the following selections in the drop-down list: ⦿ *Standard* ⦿*Data Point Enabled* ⦿ *Data Point Triggered* ⦿*MQTT Message Triggered* ⦿*Advanced Trigger* ⦿ *Event* *Publish Mode* defines the sampling type for the data to be sent. ➢ If *Publish Standard Mode*, MQTT message will be sampled and published (even if there are no data changes of the items selected in the payload definition) with a frequency defined by the *Publish Interval.* ➢ If *Data Point Enabled Mode*, the mechanism is similar with *Publish Mode Standard,* but the entire process is enabled/ disabled based on the Boolean value of the specified *Data Point Trigger* (enabled if the actual value is identical to value specified in *Trigger Value* field, disabled otherwise). ➢ If *Data Point Triggered* Mode, an MQTT message will be published only once, with data collected at the time the monitored *Data Point Trigger* receives a value which fulfills the condition imposed by the parameter *Trigger Value:* o *False to True (leading edge)* - the mechanism will fire up when a data change from *False* to *True* is detected for the Boolean value of the *Data Point Trigger* o *True to False (falling edge)* - the mechanism will fire up when data change from *True* to *False* is detected for the Boolean value of the *Data Point Trigger*

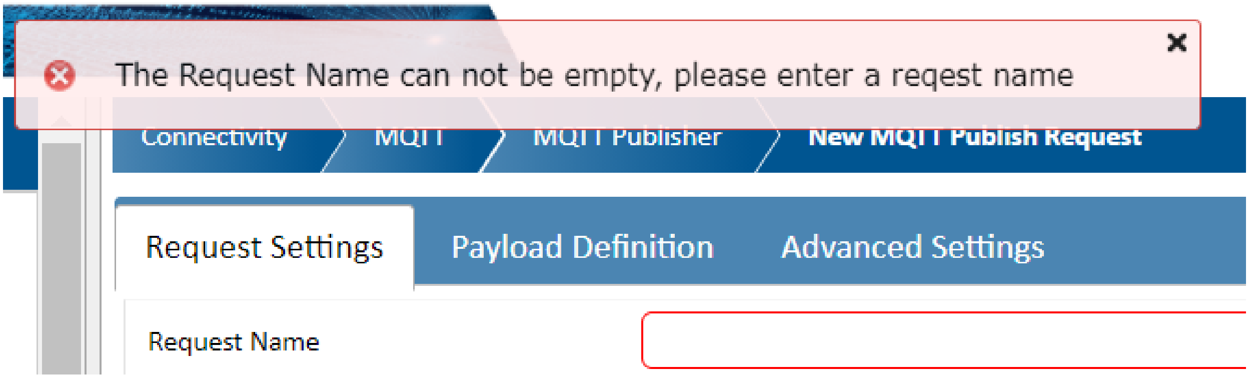
		○ *Changed* - the mechanism will fire up when any change is detected for the Boolean or Integer-based value of the *Data Point Trigger* ➢ If *MQTT Message Triggered Mode* - the mechanism will fire up when a message is received on the topic defined by the indicated subscriber request. Multiple publisher requests can use the same subscriber request as a trigger. ➢ If *Publish Event Mode* (*Publish Mode Event* radio button enabled) , MQTT message will be sampled and published only when a data change occurs on any of the items selected in the message payload definition. In order to avoid the stress of the MQTT Broker, the occurrence of publishing will not happen sooner than the time interval specified in the *Publish Interval*. The message payload will contain ALL data changes available within the *Publish Interval*. ➢ If *Advanced Trigger* Publish Mode is used, user has the possibility to use one ore more data items in a custom defined algorithm which defines whether the message is to sent or not. The value of the data items used in the algorithm is monitored with the configured *Trigger Sampling Interval.* The algorithm is provided using the LUA editor available in the Advanced Trigger 142 tab.
Data Point Trigger	**empty**	Application specific parameter, represented by a selection list, available only for *Publish Modes Data Point Enabled* and *Data Point Triggered*. If the [*Select*] button is pressed, a new window is opened and the user has the possibility to choose the address space together with a variable of data type Boolean (for *Data Point Enabled* mode) or Boolean/Integer-based (for *Data Point Triggered* mode), which will be monitored, in order to trigger the collecting of data and publishing MQTT message. The browsing tree only displays the variables with selectable data types (Boolean/Integer-based) as well as Scalar and One Dimension Array. In case an array variable is selected, the *Array Index* spin-box control becomes enabled and a value can be inserted, specifying the index in the selected array for which the value is to be evaluated.

		 Trigger Data Point Selection Select Address Spaces: AllConnectionsAddressSpace Array Index: 0 AllConnectionsAddressSpace Objects Server testPLC1 Inputs Outputs Tag_3 OW_0 OB_0/0 OB_0/1 OB_0/2 OB_0/3 OB_0/4 OB_0/5 OB_0/6 OB_0/7 OT_Bool OT_Byte OT_Word OT_DWord OT_AOM_Ident OT_Char OT_CONN_ANY OT_CONN_OUC OT_CONN_PRG OT_CONN_R_ID OK Cancel Help
Trigger Value	**true**	Application specific parameter, represented by a combo box, available only in *Data Point Enabled* and *Data Point Triggered Publish Modes.* The possible values and meaning is depending on the selected *Publish Mode:* ➢ *Data Point Enabled Mode :* The collecting of data and publishing of MQTT messages is enabled as long as the current value of the triggered item is the same as the value of the *Trigger Value* field. Selectable values of the *Trigger Value* parameter are Boolean values: *true/false*. ➢ If *Data Point Enabled Triggered* Mode: The collecting of data and publishing of MQTT message will take place only once, at the time the monitored *Data Point Trigger* receives a value which fulfills the condition imposed by the selected value*:* ○ *False to True (leading edge)* - the mechanism will fire up when a data change from *False* to *True* is detected for the Boolean value of the *Data Point Trigger*

		○ *True to False (falling edge)* - the mechanism will fire up when data change from *True* to *False* is detected for the Boolean value of the *Data Point Trigger* ○ *Changed* - the mechanism will fire up when any change is detected for the Boolean or Integer-based value of the *Data Point Trigger*
Trigger Sampling Interval [mseconds]	**1000**	Application specific parameter, available only in *Data Point Triggered Publish Mode.* Possible values between 10 and 100 000 000. The value (in milliseconds) represents the frequency of collecting the data for for the triggered item specified in *Data Point Triggered* list.
Publish Interval[mseconds]	**1000**	Application specific parameter with possible values between 10 and 100 000 000. The value (in milliseconds) represents the time interval between successive publish operations. ***Note**: The *Publish Interval* cannot be smaller than the *Sampling Interval.* ****Note**: The *Publish Interval* is not displayed for the *Data Point Triggered Publish Mode.*
Multiple Datasets per Publish Request	**Unchecked**	Application specific parameter, represented by a check box. Enabled only for *Standard Publish Mode* and *Data Point Enabled Publish Mode* If **checked/true**, the payload of the MQTT message will contain multiple data sets, each timestamped according to the time the values were sampled. The time interval between successive sampling of values is depending on *Sampling Interval [mseconds]* parameter. E.g.: for Publish Interval = 1000 and Sampling Interval = 100, the payload will contain 10 data sets (in some cases 9).
Sampling Interval [mseconds]	**1000**	Application specific parameter with possible values between 10 and 100 000 000. The value (in milliseconds) represents the frequency of collecting the data for publishing. The parameter has a meaning only if *Multiple Datasets per Publish Request* = True ***Note:** The *Sampling Interval* cannot be greater than the *Publish Interval.*
MQTT Trigger Request	**empty**	Application specific parameter, represented by a drop down list from where an already defined subscriber request can be selected, available only in *MQTT Message Triggered Mode.* The existing subscriber requests are listed with their request names and following details: • the connection the subscriber request belongs to • the topic name defined for the subscriber request

		If the [*Create New Subscriber*] button is pressed, have the possibility to add new subscriber in the publisher request page for MQTT Trigger Request  Request Settings | Payload Definition | Advanced Settings Request Name: Local_c11_on_pumps_signal Enabled: ☑ Fully Hierarchical Topic Name: c11/d MQTT Connection: LocalBroker MQTT QoS: Level0_AtMostOnce Publish Mode: MQTT Message Triggered MQTT Trigger Request: Local_sub_c11/pumps (Connection: LocalBroker | Topic: c11/pumps) [Create New Subscriber] Local_sub_c10 (Connection: LocalBroker | Topic: c10) Local_sub_c11 (Connection: LocalBroker | Topic: c11) Local_sub_c11/pumps (Connection: LocalBroker | Topic: c11/pumps) Local_sub_c11/tanks (Connection: LocalBroker | Topic: c11/tanks) Read Timeout [mseconds] [Save] [Cancel] ***Note**: Multiple MQTT Message Triggered publish requests can be triggered by the same subscribe request.
Read Time Out [mseconds]	**1000**	Application specific parameter with possible values between 10 and 100 000 000. The value (in milliseconds) defines the timeout for collecting the values for all defined data points for publishing when using the *Publish Mode Data Point Triggered, MQTT Message Triggered* or *Advanced Trigger Mode*. Once the specified time has elapsed, a publish message will be sent, even if the values for all defined data points had not been collected completely.

By Clicking **[Save]** button is triggered a validation of the publisher parameters. In case of missing information or errors appropriate messages are displayed.



The Request Name can not be empty, please enter a reqest name

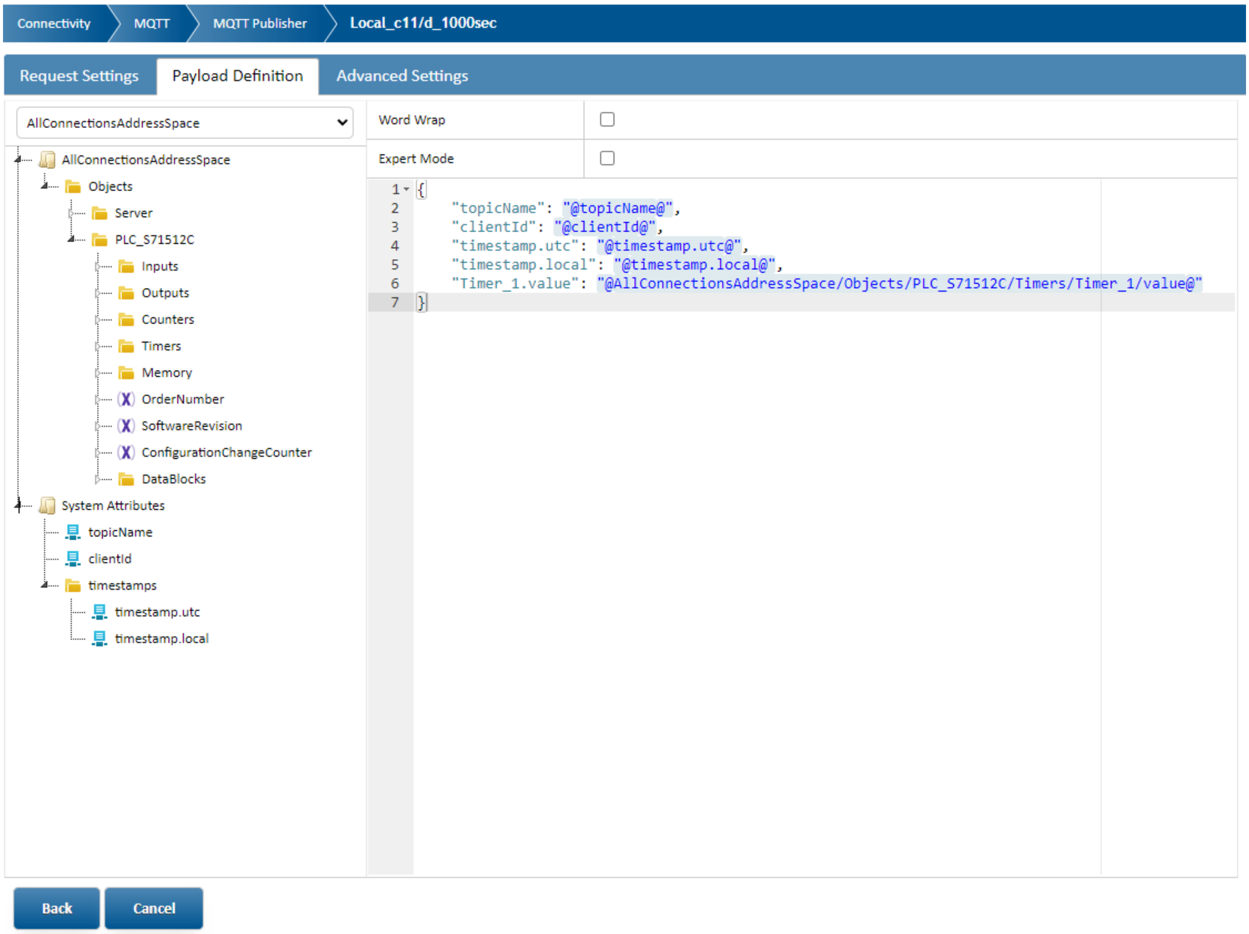
If the validation pass, the publisher parameters are persistently stored and the context will be moved to the page showing the MQTT Publisher 124 list.

If the publisher was *Enabled* it will start immediately to send messages.

By clicking **[Cancel]** button all changes are discarded and the context will be moved to the page showing the MQTT Publisher 124 list.

4.6.3.1.2 Payload Definition

The tab page *Payload definition* holds the definition of publisher's message payload .



Word Wrap □

Expert Mode □

```
{
    "topicName": "@topicName@",
    "clientId": "@clientId@",
    "timestamp.utc": "@timestamp.utc@",
    "timestamp.local": "@timestamp.local@",
    "Timer_1.value": "@AllConnectionsAddressSpace/Objects/PLC_S71512C/Timers/Timer_1/value@"
}
```

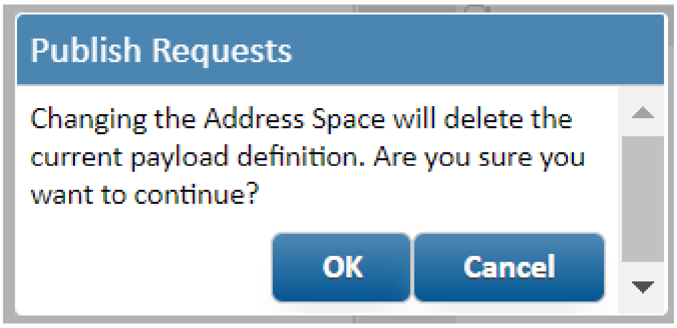
Figure: Tab page for the definition of the MQTT message payload

The page has two sides:

- the right side contains an editor, where is defined the structure of the message.
- the left side contains a combo-box for the selection of the internal address space which is holding the variables to insert in the payload; the main control is a tree based structure which displays both system information variables and the internal address spaces selected on the combo-box.

First thing to do is select the address space where the variables will be picked from.

***Warning**: in the current version is possible to select variables only from one address space. By switching between address spaces, the payload definition will be reset. The user is asked for confirmation before performing this operation.



Publish Requests

Changing the Address Space will delete the current payload definition. Are you sure you want to continue?

Figure: Pop-up for confirming address space switch

After selecting the address space to work on, the left side tree will be re-populated with the folders, variables and attributes which is containing it.

The navigation in the tree is possible by expanding and collapsing the folders and variables (click on the tree node icons).

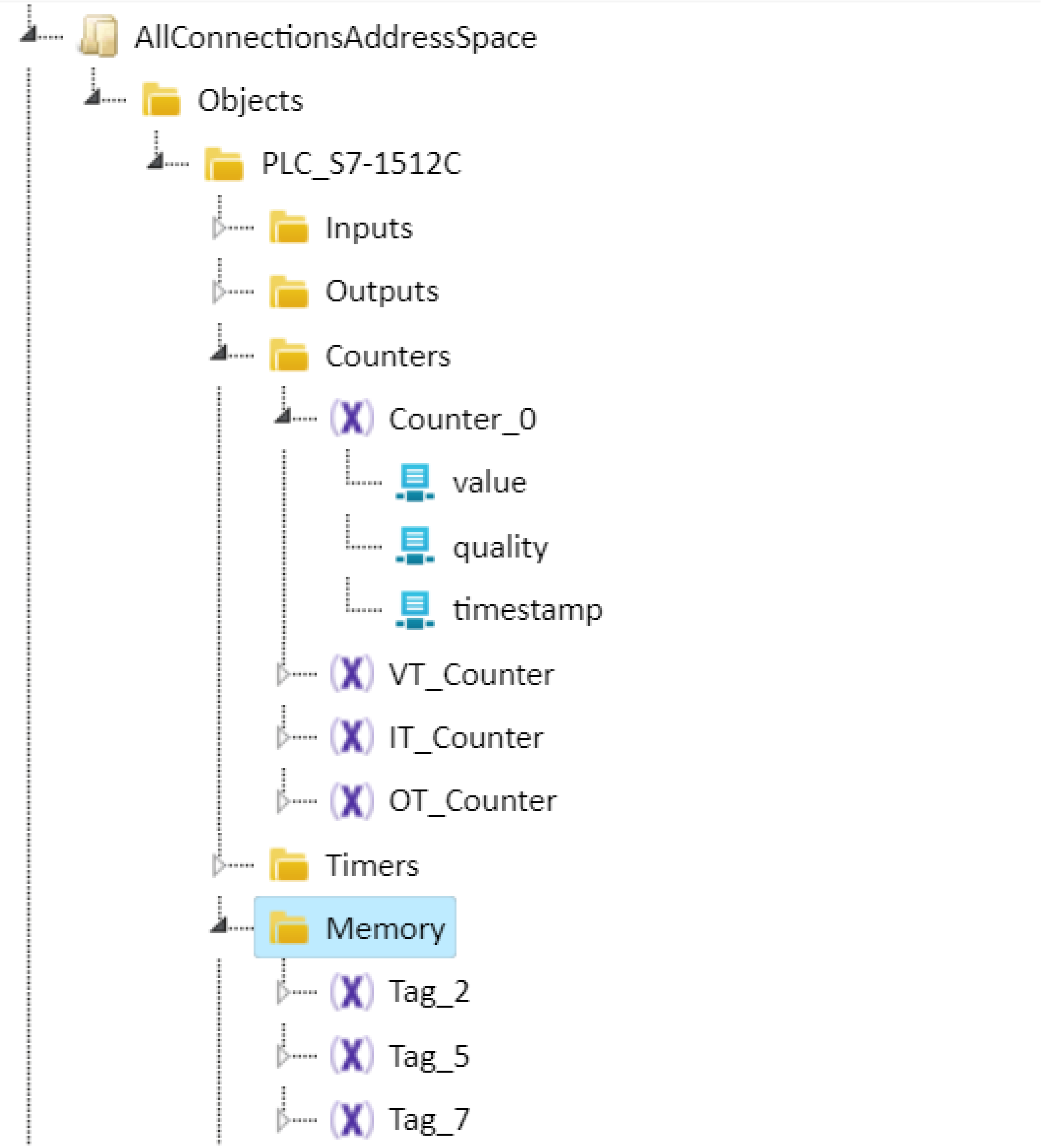


Figure: Navigating the address space

The selection of the variables to be inserted in the payload can be done in two ways:

- By dragging and dropping the node from the left side to the payload editor.
- By double clicking the node.

It is possible to select folders, variables and attributes. Folders are identified by node icon 📁 , variables by node icon (X) and attributes by 🖧 .

If folders 📁 are selected, ALL contained variables are added to the payload.

- By double-clicking it, the contained variables are added as flat JSON fields at the end of the payload.
- By dragging and dropping it, the user is asked whether the variables will be dropped as flat fields or respecting the structure of the folder in the address space. While the confirmation pop-up message is shown, the operation can be canceled by pressing the **[Esc]** keyboard button. The variables are inserted in the payload respecting the cursor position at the moment of dropping.

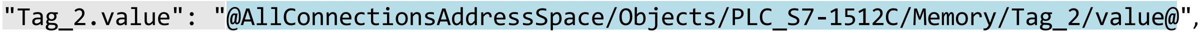
***Warning**: selecting large folders could require long time to execute.

If variables (X) are selected, in the payload will be inserted their value attribute.

The attributes 🖧 are of the following kinds: *value*, *timestamp* and *quality*.

Once the variables and attributes are added, they are present in the JSON payload as fields. The fields are containing as values strings for unique node identification in the address space.

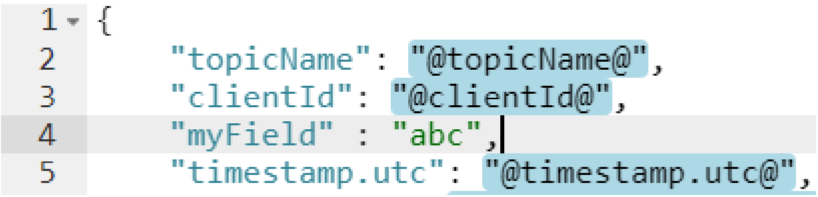
Example



```
"Tag_2.value": "@AllConnectionsAddressSpace/Objects/PLC_S7-1512C/Memory/Tag_2/value@",
```

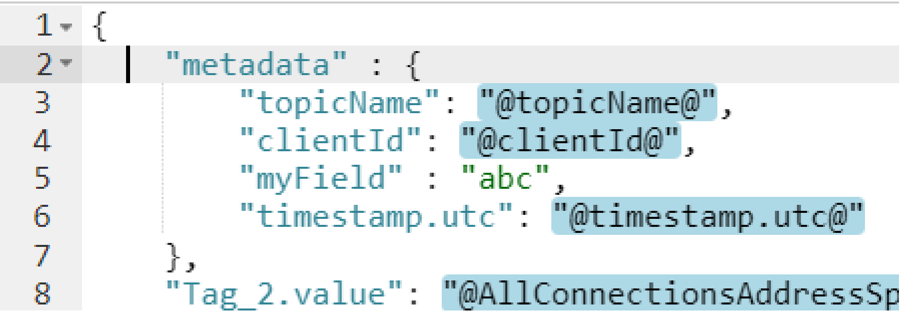
The payload can be edited manually by:

- Adding manually additional JSON fields with static values



```
{
     "topicName": "@topicName@",
     "clientId": "@clientId@",
     "myField" : "abc",
     "timestamp.utc": "@timestamp.utc@",
```

- Re-organizing content by grouping variables in sub-objects or arrays.



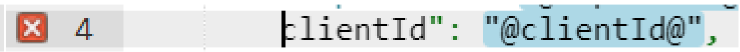
```
{
    "metadata" : {
        "topicName": "@topicName@",
        "clientId": "@clientId@",
        "myField" : "abc",
        "timestamp.utc": "@timestamp.utc@"
    },
    "Tag_2.value": "@AllConnectionsAddressSp
```

- Deleting fields (**[Delete],[Backspace]** keyboard buttons]

While editing the payload there are performed some JSON validations:

- Duplicate field names
- Unquoted field names
- The content is well formed (use of single quotes, unescaped double quotes, missing commas to separate fields, etc)
- Missing opening and closing brackets
- other syntax errors which may produce invalid content

These errors are immediately shown.



```
☒ 4        clientId": "@clientId@",
```

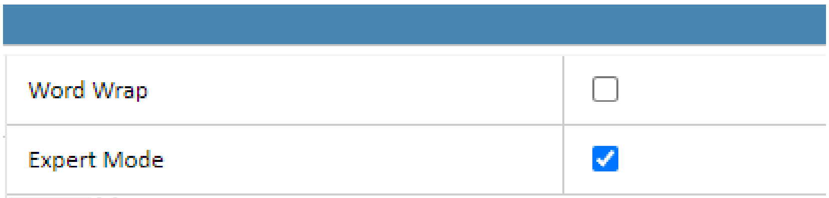
By hovering the mouse over the icon ☒ is is displayed a message indicating the source of the error.

It is shown only one error at a time; by fixing it, the editor will position the error icon in front of the next one.

***Warning:** In default/normal editing mode (*Expert Mode* check-box disabled*)* the value of a field which represents a unique node identification (i.e the string between @@ characters) cannot be changed or removed. It could be removed instead the whole field by selecting it and pressing **[Delete] or [Backspace]** keyboard buttons.

Expert Mode editor

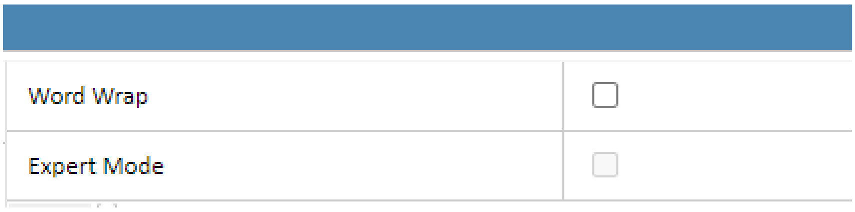
For the *MQTT Message Triggered* Publish Mode, user can activate the *Expert Mode* for the payload definition editor by checking the *Expert Mode* check-box.



Word Wrap	□
Expert Mode	☑

Figure: Activating Expert Mode on the payload definition tab

For any other publish mode , the *Expert Mode* editing is disabled and cannot be activated.



Word Wrap	□
Expert Mode	□

Figure: Disabled Expert Mode

While the *Expert Mode* is active user is allowed to edit also the unique node identification fields (i.e the string between @@ characters).

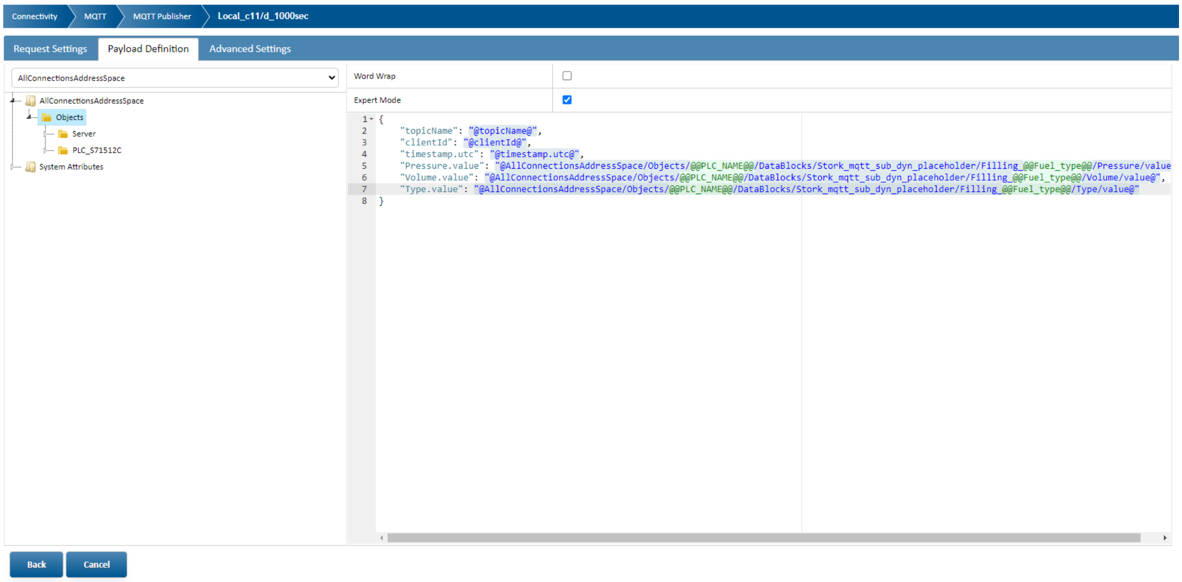
User can freely edit the content, but, in order to point out to an existing variable the editing should comply to the following rule: the content should be a string representing a list of the display names of the nodes used to navigate to the desired node, in the address space hierarchy, tokens (the different hierarchical levels) being separated by *slash* character: **/.**

The real value of this mode is achieved when the so called '*placeholders*' are used in the definition of a unique node identification field.

A *placeholder* is a sub-string in a unique node identification field, guarded by a double *at* sign (@@), which replaces a hierarchical level entirely or partially.

At run-time, if the triggering MQTT message (received on the the subscriber request configured to trigger the current publish request) contains in the root of the JSON object members having as key the *placeholder* name and with string values, the string value will be used to replace the *placeholder* in the definition of the unique node identification field, resulting in a dynamically built identification of an address space node. If the unique node identification points out to a readble variable , the variable will be used as source for reading the value.

The screen-shot below illustrates such a configuration.



Word Wrap □

Expert Mode ☑

```
{
    "topicName": "@topicName@",
    "clientId": "@clientId@",
    "timestamp.utc": "@timestamp.utc@",
    "Pressure.value": "@AllConnectionsAddressSpace/Objects/@@PLC_NAME@@/DataBlocks/Stork_mqtt_sub_dyn_placeholder/Filling_@@Fuel_type@@/Pressure/value
    "Volume.value": "@AllConnectionsAddressSpace/Objects/@@PLC_NAME@@/DataBlocks/Stork_mqtt_sub_dyn_placeholder/Filling_@@Fuel_type@@/Volume/value@",
    "Type.value": "@AllConnectionsAddressSpace/Objects/@@PLC_NAME@@/DataBlocks/Stork_mqtt_sub_dyn_placeholder/Filling_@@Fuel_type@@/Type/value@"
}
```

Figure: Tab page for the definition of the MQTT message payload using placeholders

If the received triggering MQTT message does not provide actual values (of type string) for ALL the placeholders used in the payload definition of the publish request, the publish request will NOT be triggered.

However, if all placeholders are identified in the received triggering MQTT message, but based on the provided values some of the unique node identification fields in the publish request payload cannot be resolved to valid readable variables in the address space, the publish will be triggered, providing for the corresponding keys a *null* value.

By Clicking **[Back]** button the context will be moved to the page showing the Request settings 125 page.

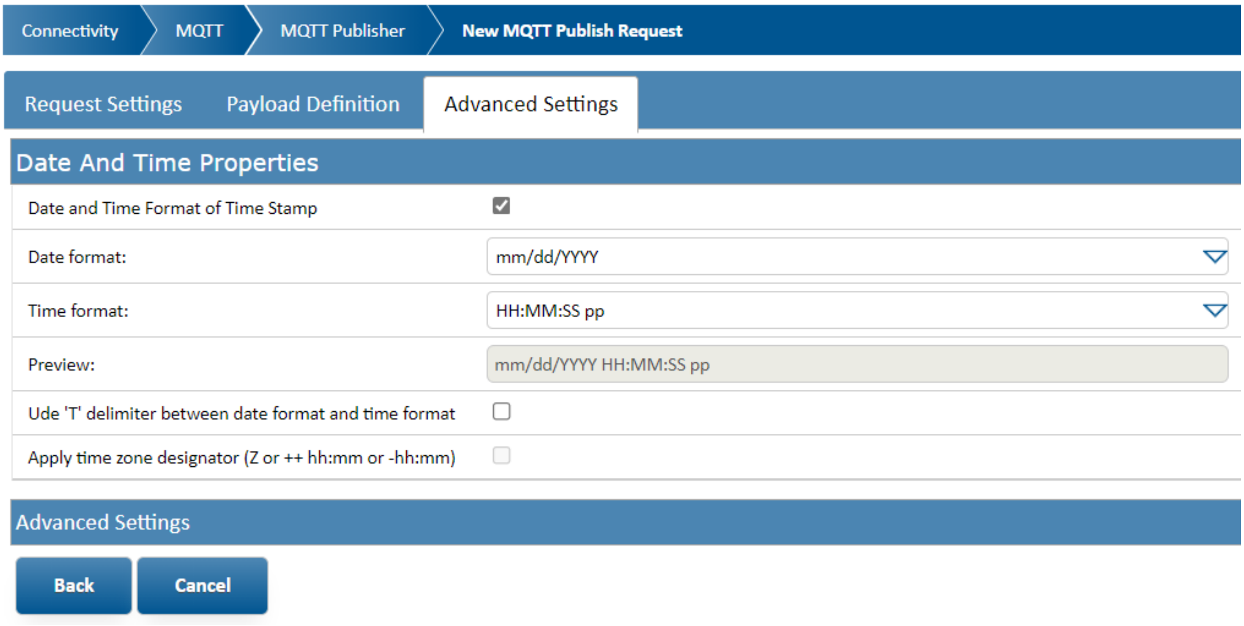
By clicking **[Cancel]** button all changes made to the new publisher are discarded and the context will be moved to the page showing the list of MQTT publisher 124 requests

4.6.3.1.3 Advanced Settings

The tab page *Advanced Settings* holds additional parameters related to the publisher request .

It has two expandable/collapsible sections.

The first (**Date and Time Properties**) holds parameters for tuning the date and time formats in the messages payload.



Date And Time Properties

Date and Time Format of Time Stamp	☑
Date format:	mm/dd/YYYY
Time format:	HH:MM:SS pp
Preview:	mm/dd/YYYY HH:MM:SS pp
Ude 'T' delimiter between date format and time format	□
Apply time zone designator (Z or ++ hh:mm or -hh:mm)	□

Advanced Settings

Figure: Date and Time Properties tab page

Parameter name	Default value	Value description
Date and Time format on Timestamp	**Checked**	**True**(checked) or **False**(unchecked). By setting it to **True**, the format of the *timestamp* field in the JSON payload can be customized. The customization is specified using the parameters below. If **False** is selected, the implicit format for serializing the *timestamp* is: *YYYY-mm-ddTHH:MM:SS.FFFZ*
Date format	**mm/dd/YYYY**	Pattern string used to format the date part of the *timestamp* field in the message payload. Values can be selected from a combo-box having the following options: • **mm/dd/YYYY** • **dd-mm-YYYY** • **dd.mm.YYYY** • **dd/mm/YYYY** • **YYYY-mm-dd** • **mm-dd-YYYY** Where: • dd- day of the month (00-31) • mm - month of the year (01-12)

		• YYYY - four digit year If no default option fits, own formatting can be inserted. The characters used for date formatting are: d, m, Y according to ISO 8601. It is supported an empty *date format*, but only it *time format* is not empty. All allowed *date format* symbols are: **AAA, aaa, BBB, bbb, ccc, dd, jjj ,mm, UU, ww, xxx, yy, YYYY** (see the table below). For separating different fractions the following characters can be used: . - / |
Time format	**HH:MM:SS pp**	Pattern string used to format the time part of the *timestamp* field in the message payload Values can be selected from a combo-box having the following options: • **HH:MM:SS** • **HH:MM:SS pp** • **HH:MM:SS.FFF pp** • **HH:MM:SS.FFF** Where: • HH - (00-23) hour in 24 hour format (if pp is not present) or (00-12) in 12 hour format. • MM - minutes (00-59) • SS - seconds (00-59) • pp - AM or PM in 12 hour format • FFF - milliseconds fraction (000-999**)** If no default option fits, own formatting can be inserted. It is supported an empty *time format*, but only it *date format* is not empty. All allowed time *format* symbols are: **II, HH, MM, SS, pp, XXX, FFFFFF, FFFFF, FFFF, FFF ,FF, F** (see the table below). For separating different fractions the following characters can be used: . - : /

Preview	**mm/dd/YYYY HH:MM:SS pp**	(disabled) field which shows the composition of the date and time fractions to form the *timestamp* string field in the message payload.
Use 'T' delimiter between date format and time format	**Unchecked**	in some formats **T** is a literal to separate the date from the time.
Apply zone designator (Z or ++hh:mm or -hh:mm)	**Unchecked**	**Z** stands for 'zero hour offset' or UTC time in ISO 8601.

***Note:** The options above for datetime serialization are valid only for the *timestamp* field of the JSON payload.

Datetime symbol (specifier)	Replaces	Example
aaa	Abbreviated weekday name *	Thu
AAA	Full weekday name *	Thursday
bbb	Abbreviated month name *	Aug
BBB	Full month name *	August
ccc	Date and time representation *	Thu Aug 23 14:55:02 2001
dd	Day of the month, zero-padded (01-31)	23
HH	Hour in 24h format (00-23)	14
II	Hour in 12h format (01-12)	02
jjj	Day of the year (001-366)	235
mm	Month as a decimal number (01-12)	08
MM	Minute (00-59)	55
pp	AM or PM designation	PM
SS	Second (00-61)	02
UU	Week number with the first Sunday as the first day of week one (00-53)	33
xxx	Date representation *	08/23/01
XXX	Time representation *	14:55:02
yy	Year, last two digits (00-99)	01
YY	Year	2001
F	Milliseconds, one digit	1

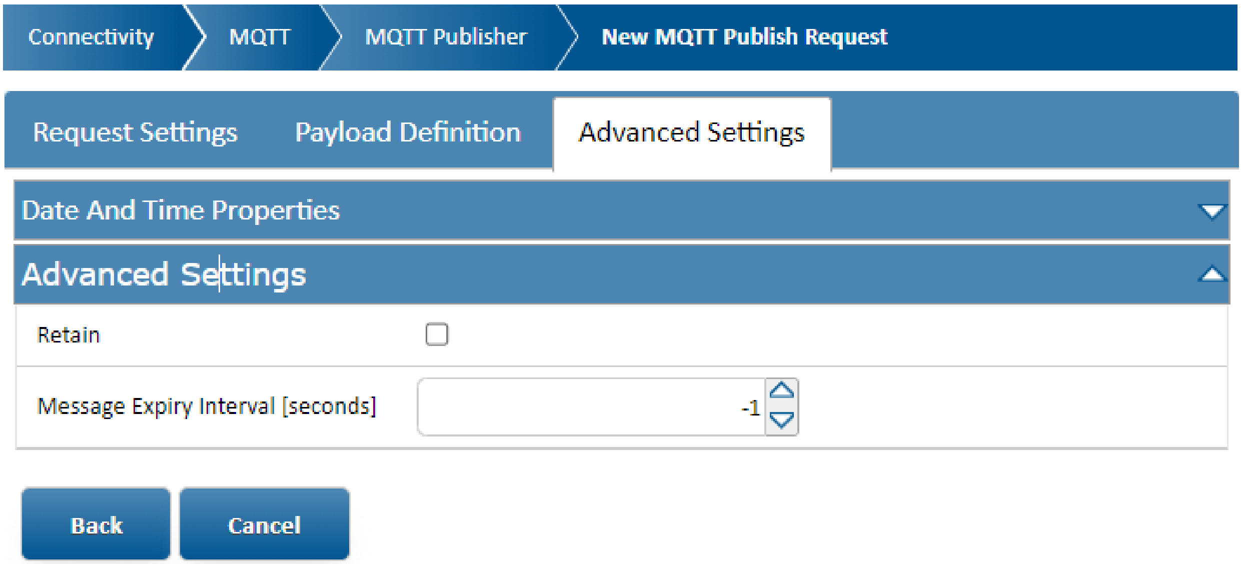
FF	Milliseconds, two digits	15
FFF	Milliseconds, three digits	152
FFFF	Milliseconds, four digits	1520
FFFFF	Milliseconds, five digits	15200
FFFFFF	Milliseconds, six digits	152000

Table: Datetime format symbols

Available delimiters: *".", ":", "/", ",", "\", "|", ";", " ", "\t", "-"*

The second tab page (Advanced Settings) holds the following parameters:

Parameter name	Default value	Value description
Retain	**Unchecked**	True (checked) or False (unchecked). It is an MQTT specific flag. A retained message is available immediately for new subscribers.It eliminates the wait for the publishing clients to send the next update. The broker stores only the last retained message for a specific topic.
Message Expiry Interval [seconds]	**-1**	This interval defines the period of time that the broker stores the PUBLISH message for any matching subscribers that are not currently connected. When no message expiry interval is set (*value -1)*, the broker must store the message for matching subscribers indefinitely. When the *retain* option is set, this interval also defines how long a message is retained on a topic. **Note:** The option is present only for publishers attached to an MQTT v5 connection.



Retain □

Message Expiry Interval [seconds] -1

Figure: Retain parameter in Advanced Settings section

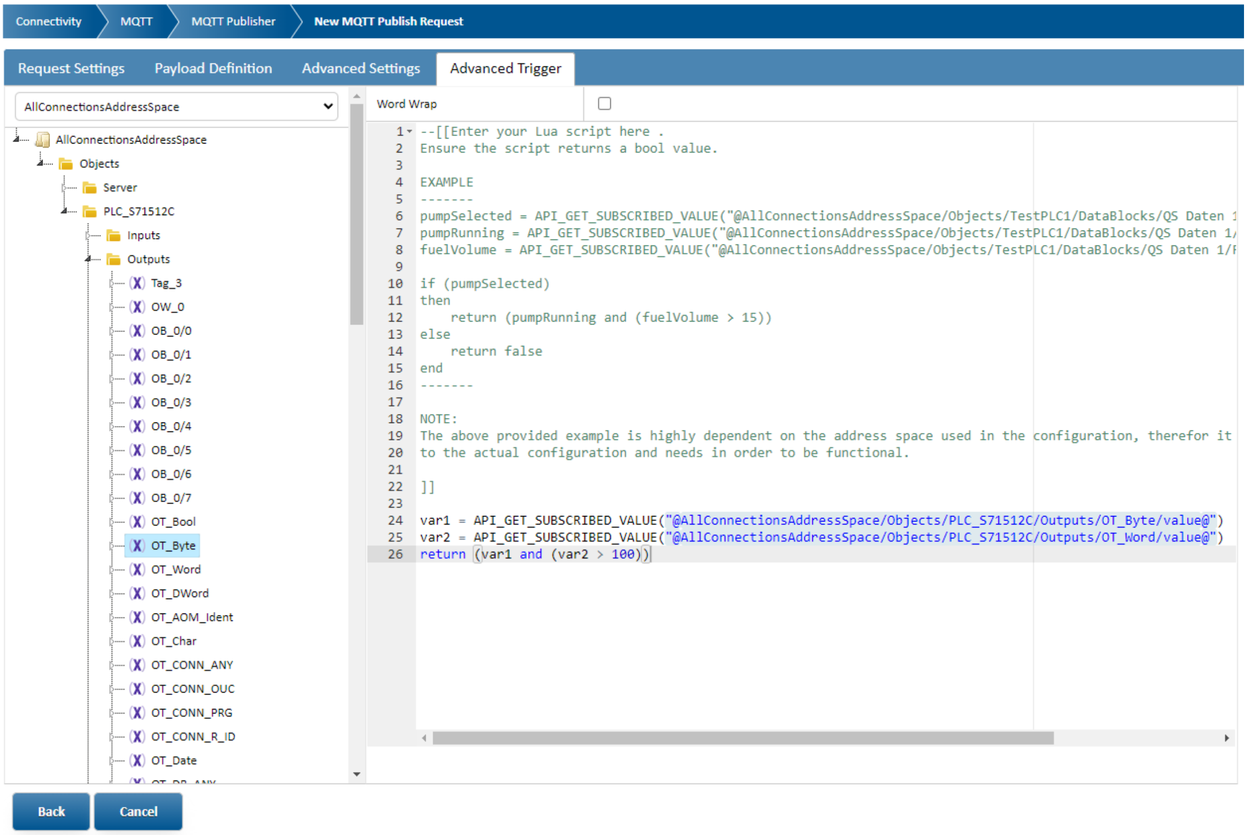
By Clicking **[Back]** button the context will be moved to the page showing the Request settings 125 page.

By clicking **[Cancel]** button all changes made to the new publisher are discarded and the context will be moved to the page showing the list of MQTT publisher 124 requests

4.6.3.1.4 Advanced Trigger

The tab page *Advanced Trigger* holds the definition of the algorithm used by the publishers configured with *Advanced Trigger* publish mode.

The tab is visible only for the MQTT Publishers with Advanced Trigger publish mode.



```
--[[Enter your Lua script here .
Ensure the script returns a bool value.

EXAMPLE
-------
pumpSelected = API_GET_SUBSCRIBED_VALUE("@AllConnectionsAddressSpace/Objects/TestPLC1/DataBlocks/QS Daten 1
pumpRunning = API_GET_SUBSCRIBED_VALUE("@AllConnectionsAddressSpace/Objects/TestPLC1/DataBlocks/QS Daten 1/
fuelVolume = API_GET_SUBSCRIBED_VALUE("@AllConnectionsAddressSpace/Objects/TestPLC1/DataBlocks/QS Daten 1/F

if (pumpSelected)
then
    return (pumpRunning and (fuelVolume > 15))
else
    return false
end
-------

NOTE:
The above provided example is highly dependent on the address space used in the configuration, therefor it
to the actual configuration and needs in order to be functional.

]]

var1 = API_GET_SUBSCRIBED_VALUE("@AllConnectionsAddressSpace/Objects/PLC_S71512C/Outputs/OT_Byte/value@")
var2 = API_GET_SUBSCRIBED_VALUE("@AllConnectionsAddressSpace/Objects/PLC_S71512C/Outputs/OT_Word/value@")
return (var1 and (var2 > 100))
```

The page has two sides:

- the left side contains a combo-box for the selection of the internal address space which is holding the variables to use in the triggering logic; the main control is a tree based structure which displays the internal address space selected on the combo-box.
- the right side contains an editor, where user can define the triggering logic as a LUA algorithm.

Script is standard LUA script. Read more about LUA Syntax at LUA Reference Manual page.

The standard LUA *string* and *maths* libraries are available.

The script should provide a boolean value as a return. In case a *True* value is returned, the trigger will fire-up (the associated message will be sent), otherwise, no message will be sent. Any other return type would NOT fire the trigger (therefor, no message will be sent).

A custom defined function **API_GET_SUBSCRIBED_VALUE** is available. It shall be used with a unique node identification (i.e the string between @@ characters) as a parameter. Such a unique node identification is generated by drag&drop data items from the left side address space tree.

The script is executed each time at least one of the used variables changes its value. Note that they are sampled with the defined *Trigger Sampling Interval.*

At least one data item should be used; otherwise, the algorithm will be never run and trigger will never fire.

In case on any error at the execution time, the result will be equivalent to *False*.

If the running of the scripts takes more than 2 seconds, the execution will be interrupted and the result will be will be equivalent to *False*.

By Clicking **[Back]** button the context will be moved to the page showing the Request settings 125 page.

By clicking **[Cancel]** button all changes made to the new publisher are discarded and the context will be moved to the page showing the list of MQTT publisher 124 requests

4.6.3.2 Modify publish request

By clicking the **[Edit MQTT Publisher]** button located in the MQTT Publisher 124 page**,** the context is switched to the modification of the currently selected MQTT publisher.

The following groups of parameters can be edited:

Request Settings 125

Payload Definition 132

Advanced Settings 137

4.6.3.3 Delete publish request

By clicking the [**Delete MQTT Publisher]** button located in the MQTT Publisher 124 page**,** the currently selected MQTT publisher is deleted.

***Warning**: There is no additional confirmation requested, before deleting the publisher .

4.6.4 MQTT Subscriber

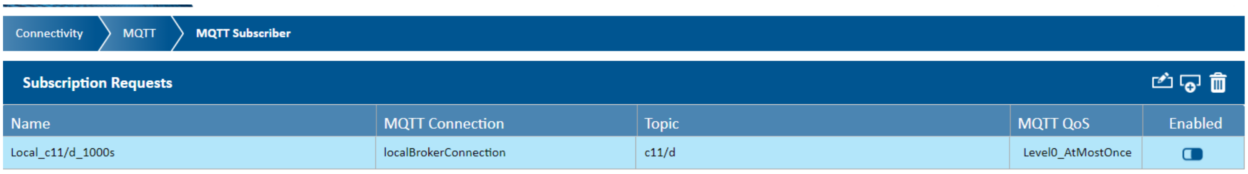
The logical sequence for configuring the MQTT Subscriber connectivity is:

1. Definition of MQTT broker connections

2. Definition of subscription requests/jobs

Information about all configured MQTT subscription jobs is centralized and accessible by navigating to **Connectivity -> MQTT -> MQTT Subscriber**.

The page displays the list of defined subscription requests/jobs or the message *'No data to display'*.



Connectivity > MQTT > MQTT Subscriber

Subscription Requests

Name	MQTT Connection	Topic	MQTT QoS	Enabled
Local_c11/d_1000s	localBrokerConnection	c11/d	Level0_AtMostOnce	

Figure: List of configured MQTT subscriber job

The table header information is described below:

Column name	Information details
Name	User defined name of the subscription job
MQTT Connection	The MQTT Connection used by the subscription job. see MQTT Connections 91.
Topic	MQTT Topic to subscribe to.
MQTT QoS	Quality of Service level for the subscription.
Enabled	Toggle which enable or disable a subscriber job. By disabling it, the subscriber stops processing incoming MQTT messages. It is not sufficient that the subscriber job is enabled in order to process messages from the broker, but it is needed also that the connection which is used by the subscription job to be enabled, too. By disabling an MQTT connection (see Modify Connection 105), all subscribers which are using it are stopped and they can't process messages anymore. By enabling an MQTT connection (see Modify Connection 105), all subscribers which are using it and are in *Enabled* state, are re-starting to process messages.

Table: Subscriber jobs list

The **Subscription Requests** information bar provides three buttons, with the following functionality:

Button	Action
⊕	Add MQTT Subscriber
✎	Edit MQTT Subscriber
🗑	Delete MQTT Subscriber

Table: List of actions for handling the MQTT subscriber jobs

***Note**: Throughout the rest of the documentation the notions *MQTT Subscriber*, *subscriber job* or *subscriber request* are equivalent.

4.6.4.1 Add subscription request

By clicking the **[Add MQTT Subscriber]** ⊕ button located in the MQTT Subscriber 144 page**,** the context is switched to the definition of the parameters needed to create a new subscriber job.

It contains two tab pages, each grouping the following parameter sets:

Request Settings 145

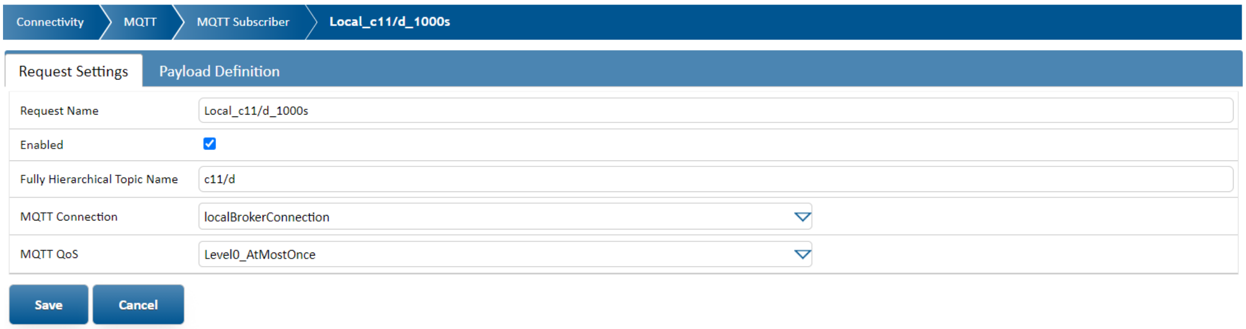
Payload definition 148

Advanced Settings (only for Subscribers attached to an MQTT v5 connection)

Note: A maximum number of 100 subscription requests per connection is allowed.

4.6.4.1.1 Request Settings

The tab page *Request Settings* contains the parameters which are mandatory for any subscription request.



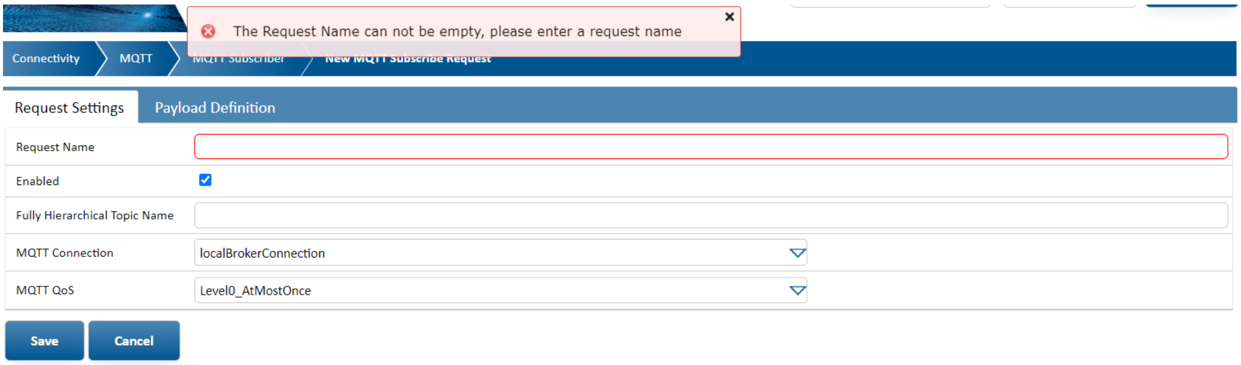
Request Name	Local_c11/d_1000s
Enabled	☑
Fully Hierarchical Topic Name	c11/d
MQTT Connection	localBrokerConnection
MQTT QoS	Level0_AtMostOnce

Figure: Request Settings tab page

Parameter name	Default value	Value description
Request Name	**empty**	Defines the subscriber request name as it will be displayed in the MQTT Subscriber overview page.
Enabled	**Enabled**	Enable (checked) or disable (unchecked) the currently configured subscriber request. If disabled, the subscriber is stopping processing messages. It is not sufficient that the subscriber job is enabled in order to process messages from the broker. It is needed also that the connection which is used by the subscription job to be enabled too. By disabling an MQTT connection (see Modify Connection 105), all subscribers which are using it are stopping processing messages. By enabling an MQTT connection (see Modify Connection 105), all subscribers which are using it and are in *Enabled* state, are re-started to process messages.
Fully Hierarchical Topic Name	**empty**	The topics are described in the MQTT specification and define from where the messages will be received and processed. MQTT Topics are structured in a hierarchy similar to folders and files in a file system using the forward slash (/)as a delimiter. ***Note1**: topics are: • Case sensitive • use UTF-8 strings. • Must consist of at least one character to be valid. ***Note2**: Be aware that it is not possible to create two subscription requests with the same topic name.

MQTT Connection	**First in the list of defined connections**	Combo-box to select the MQTT Connection used for the subscription request.
MQTT QoS	**Level0_AtMostOnce**	Quality of Service level of the messages. Possible values: • Level0_AtMostOnce • Level1_AtLeastOnce • Level2_ExactlyOnce These levels are described in the MQTT specification and defines the guarantee of delivery for a specific message.

By Clicking **[Save]** button is triggered a validation of the subscriber parameters. In case of missing information or errors, appropriate messages are displayed.



The Request Name can not be empty, please enter a request name

Request Name	
Enabled	☑
Fully Hierarchical Topic Name	
MQTT Connection	localBrokerConnection
MQTT QoS	Level0_AtMostOnce

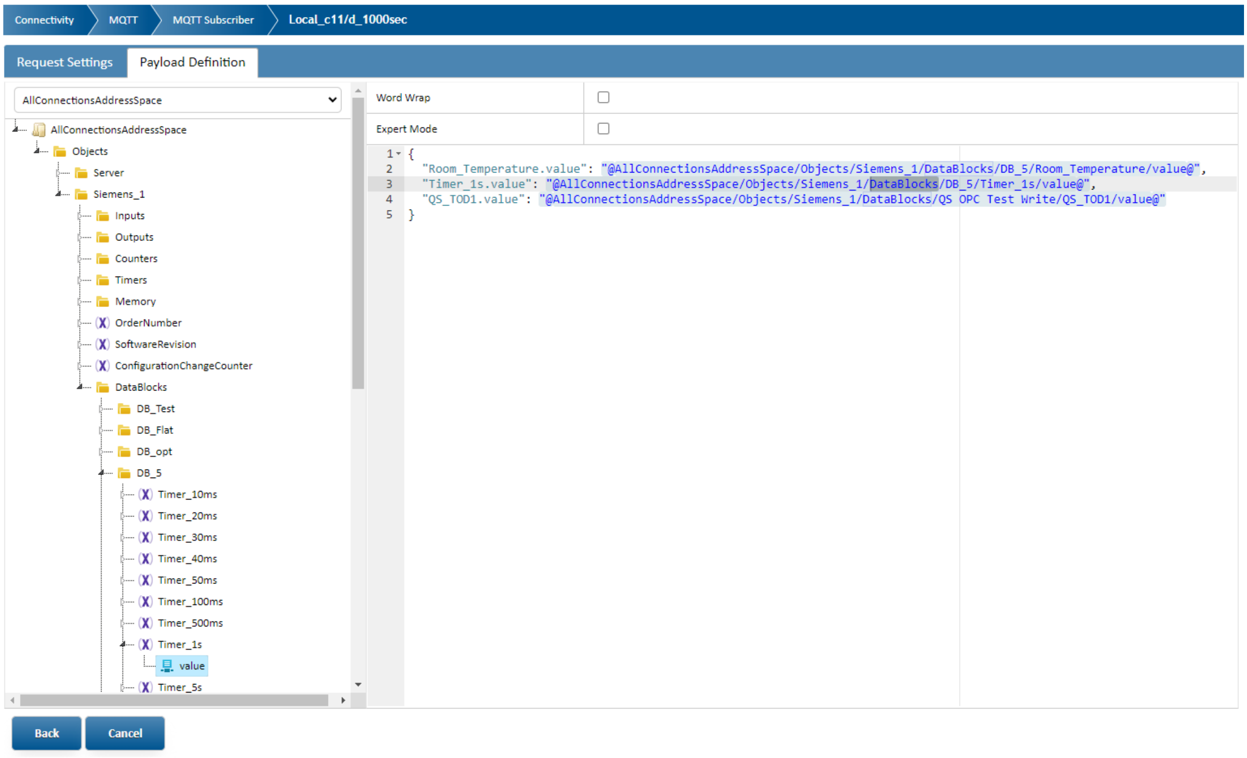
If the validation pass, the subscriber parameters are persistently stored and the context will be moved to the page showing the MQTT Subscriber 144 list.

If the subscriber was *Enabled,* it will start immediately to process messages.

By clicking **[Cancel]** button, all changes are discarded and the context will be moved to the page showing the MQTT Subscriber 144 list.

4.6.4.1.2 Payload Definition

The tab page *Payload definition* holds the definition of expected message payload .



Word Wrap ☐

Expert Mode ☐

```
{
  "Room_Temperature.value": "@AllConnectionsAddressSpace/Objects/Siemens_1/DataBlocks/DB_5/Room_Temperature/value@",
  "Timer_1s.value": "@AllConnectionsAddressSpace/Objects/Siemens_1/DataBlocks/DB_5/Timer_1s/value@",
  "QS_TOD1.value": "@AllConnectionsAddressSpace/Objects/Siemens_1/DataBlocks/QS OPC Test Write/QS_TOD1/value@"
}
```

Figure: Tab page for the definition of the MQTT message payload

The page has two sides:

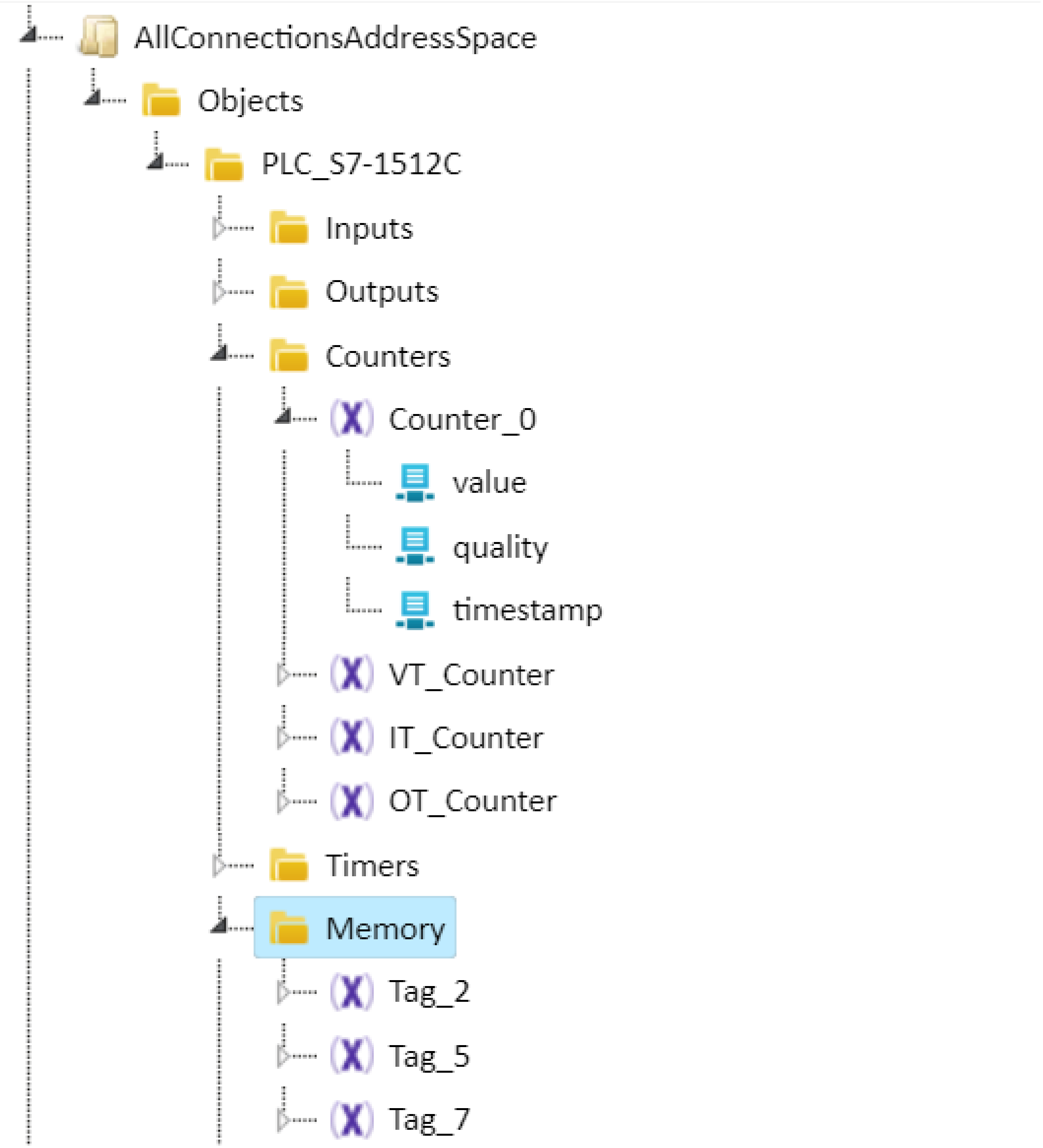
- the right side contains an editor, where is defined the structure of the message, together with some editing options.
- the left side contains a combo-box for the selection of the internal address space which is holding the variables to write, with values from the actual MQTT message payload; the main control is a tree based structure which displays the internal address spaces, selected on the combo-box.

First thing to do is select the address space where the variables will be picked from.

***Warning**: In the current version it is possible to select variables only from one address space. By switching between address spaces, the payload definition will be reset. The user is asked for confirmation before performing this operation.

After selecting the address space to work on, the left side tree will be re-populated with the folders, variables and attributes which are contained in it.

The navigation in the tree is possible by expanding and collapsing the folders and variables (click on the tree node icons).



- AllConnectionsAddressSpace
  - Objects
    - PLC_S7-1512C
      - Inputs
      - Outputs
      - Counters
        - Counter_0
          - value
          - quality
          - timestamp
        - VT_Counter
        - IT_Counter
        - OT_Counter
      - Timers
      - Memory
        - Tag_2
        - Tag_5
        - Tag_7

Figure: Navigating the address space

The selection of the variables to be inserted in the payload can be done in two ways:

- By dragging and dropping the node from the left side to the payload editor.
- By double clicking the node.

It is possible to select

- folders
- variables
- attributes

If folders are selected, all contained variables are added to the payload.

  - By double-clicking it, the contained variables are added as flat JSON fields at the end of the payload.
  - By dragging and dropping it, the user is asked whether the variables will be dropped as flat fields or respecting the structure of the folder in the address space. While the confirmation pop-up message is shown, the operation can be canceled by pressing the **[Esc]** keyboard button. The variables are inserted in the payload respecting the cursor position at the moment of dropping.

  ***Warning**: Selecting large folders could require long time to execute.

If variables (X) are selected, in the payload will be inserted their value attribute.

The attributes are of the following kinds: *value.*

Once the variables and attributes are added, they are present in the JSON payload as fields.

The fields contain unique node identification, from the address space, like in the example below:

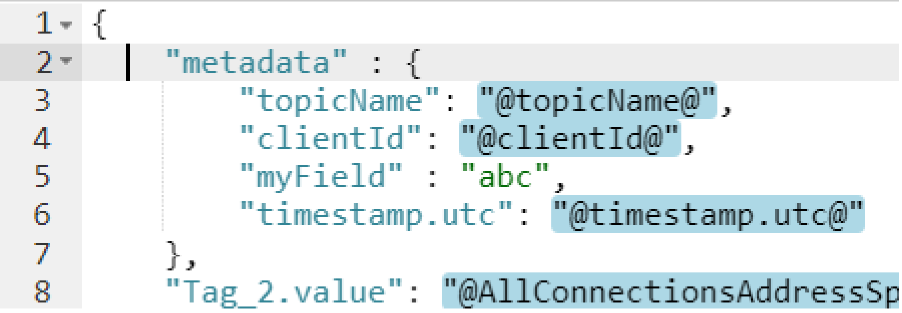
```
"Tag_2.value": "@AllConnectionsAddressSpace/Objects/PLC_S7-1512C/Memory/Tag_2/value@",
```

The mapping between the received payload and the data points in the address space is done as described below:

  - in the received payload, by drag&dropping a node over a key, the node value will take the value of the received key;

The payload can be also, manually edited by:

- Re-organizing content by grouping variables in sub-objects or arrays.



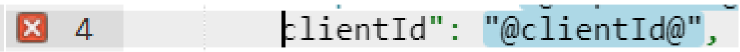
```
{
    "metadata" : {
        "topicName": "@topicName@",
        "clientId": "@clientId@",
        "myField" : "abc",
        "timestamp.utc": "@timestamp.utc@"
    },
    "Tag_2.value": "@AllConnectionsAddressSp
```

- Deleting fields (**[Delete],[Backspace]** keyboard buttons]

While editing the payload, there are performed some JSON validations:

- Duplicate field names
- Unquoted field names
- The content is well formed (use of single quotes, unescaped double quotes, missing commas to separate fields, etc.)
- Missing opening and closing brackets
- other syntax errors which may produce invalid content

These errors are immediately shown.



```
clientId": "@clientId@",
```

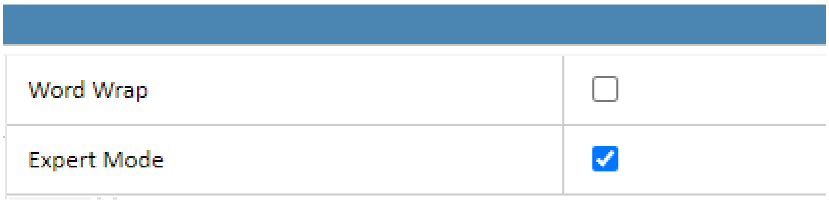
By hovering the mouse over the icon ☒ is is displayed a message indicating the source of the error.

It is shown only one error at a time; by fixing it, the editor will position the error icon in front of the next one.

***Warning**: In default/normal editing mode (*Expert Mode* check-box disabled*)* the value of a field which represents a unique node identification (i.e the string between @@ characters) cannot be changed or removed. It could be removed instead the whole field by selecting it and pressing **[Delete] or [Backspace]** keyboard buttons.

Expert Mode editor

User can enable the *Expert Mode* for the payload definition editor by checking the *Expert Mode* check-box.



Word Wrap ☐

Expert Mode ☑

Enabling Expert Mode on the payload definition tab

This mode allows the user to edit also the unique node identification fields (i.e the string between @@ characters).

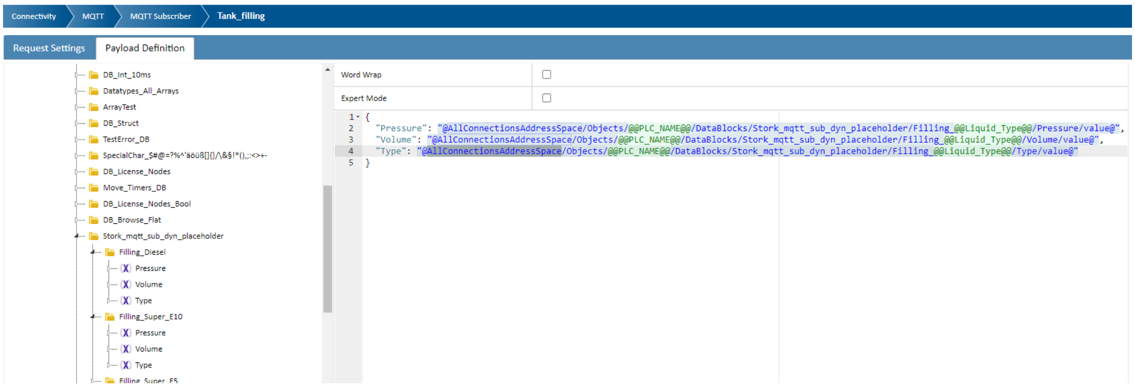
User can freely edit the content, but, in order to point out to an existing variable the editing should comply to the following rule: the content should be a string representing a list of the display names of the nodes used to navigate to the desired node, in the address space hierarchy, tokens (the different hierarchical levels) being separated by *slash* character: **/.**

The real value of this mode is achieved when the so called '*placeholders'* are used in the definition of a unique node identification field.

A *placeholder* is a sub-string in a unique node identification field, guarded by a double *at* sign (@@), which replaces a hierarchical level entirely or partially.

At run-time, if the MQTT message contains in the root of the JSON object members having as key the *placeholder* name and with string values, the string value will be used to replace the *placeholder* in the definition of the unique node identification field, resulting in a dynamically built identification of an address space node. If the unique node identification points out to a writable variable of a corresponding data type, the variable will be used as destination for writing the received value, as described above.

The screen-shot below illustrates such a configuration.



Word Wrap ☐

Expert Mode ☐

```
{
  "Pressure": "@AllConnectionsAddressSpace/Objects/@@PLC_NAME@@/DataBlocks/Stork_mqtt_sub_dyn_placeholder/Filling_@@Liquid_Type@@/Pressure/value@",
  "Volume": "@AllConnectionsAddressSpace/Objects/@@PLC_NAME@@/DataBlocks/Stork_mqtt_sub_dyn_placeholder/Filling_@@Liquid_Type@@/Volume/value@",
  "Type": "@AllConnectionsAddressSpace/Objects/@@PLC_NAME@@/DataBlocks/Stork_mqtt_sub_dyn_placeholder/Filling_@@Liquid_Type@@/Type/value@"
}
```

Figure: Tab page for the definition of the MQTT message payload

In this example, a possible valid MQTT message which would result in valid writing of the variables could be:

```
{
    "Pressure" : 12.25,
    "Volume" : 4000,
    "Type" : 3,
    "PLC_NAME" : "PLC_S71512C",
    "Liquid_Type" : "Diesel"
}
```

In a positive scenario, the result would be writing the values *12.25, 4000, 3* into the variables, defined by the following unique identifications (correspondingly):

- "@AllConnectionsAddressSpace/Objects/PLC_S71512C/DataBlocks/Stork_mqtt_sub_dyn_placeholder/Filling_Diesel/Pressure/value@"
- "@AllConnectionsAddressSpace/Objects/PLC_S71512C/DataBlocks/Stork_mqtt_sub_dyn_placeholder/Filling_Diesel/Volume/value@"
- "@AllConnectionsAddressSpace/Objects/PLC_S71512C/DataBlocks/Stork_mqtt_sub_dyn_placeholder/Filling_Diesel/Type/value@"

By Clicking **[Back]** button, the context will be moved to the page showing the Request settings 145 page.

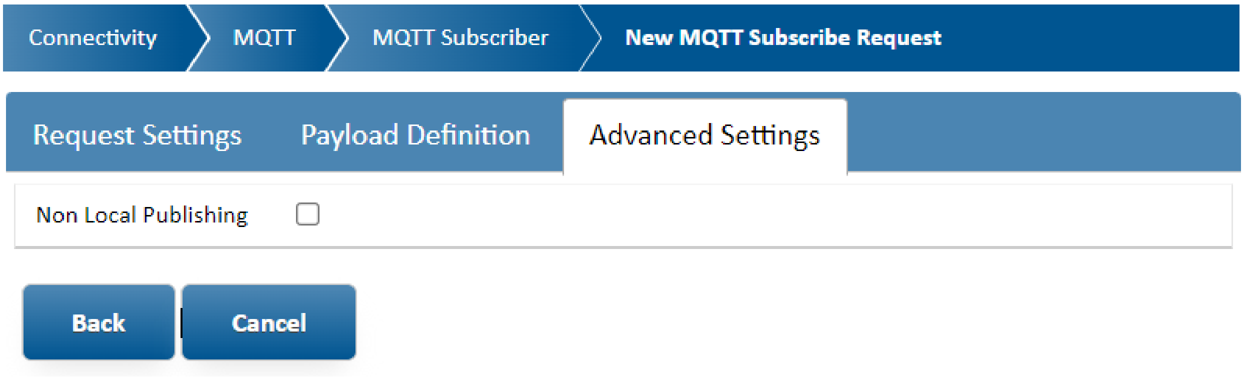
By clicking **[Cancel]** button, all changes made to the new subscriber are discarded and the context will be moved to the page showing the list of MQTT subscriber 144 requests

4.6.4.1.3 Advanced Settings

The tab page *Advanced Settings* holds additional parameters related to the subscriber request .

This tab page is visible only for the subscriber currently attached to an MQTT v5 connection.

The *Advanced Settings* contain the following:



Non Local Publishing ☐

Figure: Advanced mqtt subscriber settings

Parameter name	Default value	Value description
Non Local Publishing	**Unchecked**	In MQTTv3.1.1, if one subscribes to the same topic as the connection also publishes on, then all of the messages that connection publishes will be also received. In MQTT v5 by using the *Non Local Publishing* option the broker will not send any messages that were published from the same connection. **Note:** The option described above is present only for the subscribers attached to an MQTT v5 connections.

By Clicking **[Back]** button the context will be moved to the page showing the Payload Definition 148 page.

By clicking **[Cancel]** button all changes made to the new publisher are discarded and the context will be moved to the page showing the list of MQTT subscriber 144 requests.

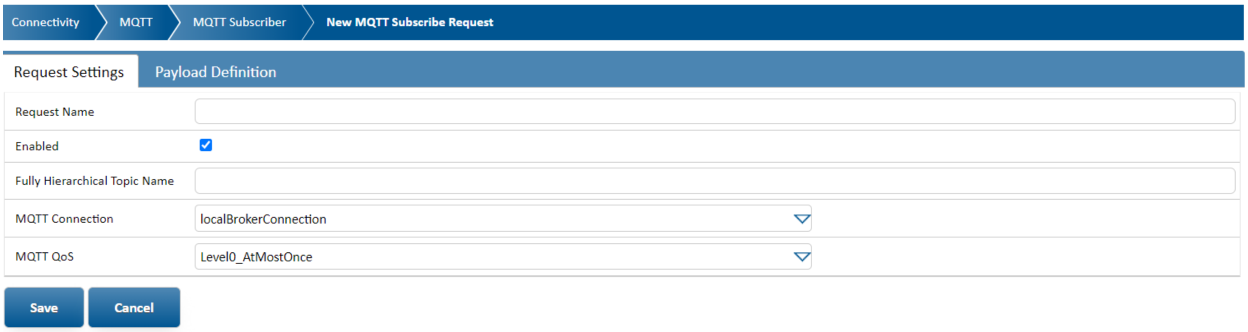
4.6.4.2 Modify subscription request

By clicking the [**Edit MQTT Subscriber]** ✎ button located in the MQTT Subscriber 144 page**,** the context is switched to the modification of the currently selected MQTT subscriber.

The following groups of parameters can be edited:

Request Settings 145

Payload Definition 148



Connectivity > MQTT > MQTT Subscriber > New MQTT Subscribe Request

Request Name	
Enabled	☑
Fully Hierarchical Topic Name	
MQTT Connection	localBrokerConnection
MQTT QoS	Level0_AtMostOnce

Figure: Sample window for modifying the parameters of a MQTT subscription

4.6.4.3 Delete subscription request

By clicking the [**Delete MQTT Subscriber]** button, located in the MQTT Subscriber 144 page**,** the currently selected MQTT subscription is deleted.

***Warning**: There is no additional confirmation requested, before deleting the subscription .

4.7 OPC UA Configuration

4.7.1 Overview

Being the central topic in the dataFEED Secure Integration Server architecture the OPC UA configuration is an essential part of the entire system. As depicted in the block diagram below the dataFEED Secure Integration Server provides important functionalities to the user such as:

- **data aggregation** - OPC UA data collected by the integrated OPC UA client is transparently routed to the OPC UA server endpoints and made available to the external OPC UA clients
- **address space filtering** - Collected data exposed to external OPC UA clients is configurable by enabling the filtering functionality which restricts or allows OPC UA user to access the existing address spaces partially or totally
- **access control** - The **enhanced security** provided by the dataFEED Secure Integration Server is composed of: **IP Access Filter** used to either whitelist trusted machines or blacklist untrusted machines and **Access Protection** providing enhanced connection control to protect against possible harmful applications

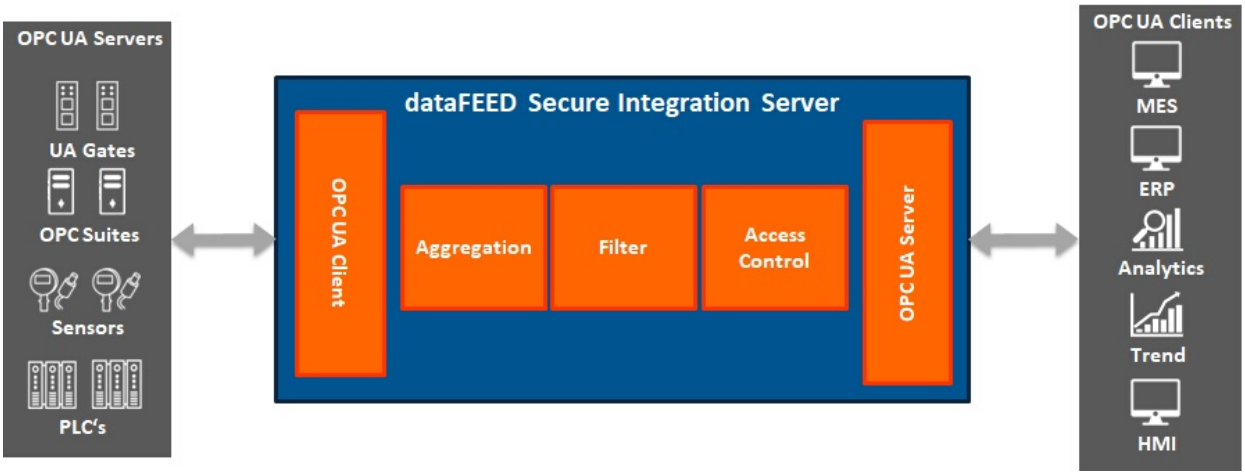
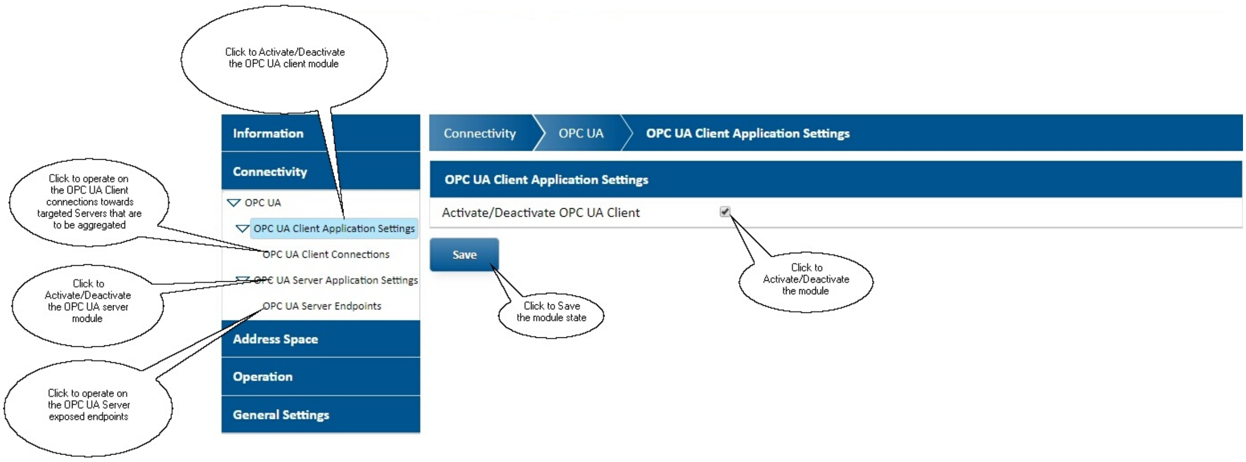


Figure: OPC UA Configuration, Concept Overview

The user is offered the following GUI interface:


Click to Activate/Deactivate the OPC UA client module
Click to operate on the OPC UA Client connections towards targeted Servers that are to be aggregated
Click to Activate/Deactivate the OPC UA server module
Click to operate on the OPC UA Server exposed endpoints
Information
Connectivity
OPC UA
OPC UA Client Application Settings
OPC UA Client Connections
OPC UA Server Application Settings
OPC UA Server Endpoints
Address Space
Operation
General Settings
Connectivity
OPC UA
OPC UA Client Application Settings
Save
Click to Save the module state
Click to Activate/Deactivate the module

OPC UA Client Application Settings

Activate/Deactivate OPC UA Client ☑

Figure: OPC UA Configuration,GUI Overview

The OPC UA Client Application Settings and OPC UA Server Application Settings pages give the possibility to enable or disable the entire OPC UA Client and Server functionality provided through dataFEED Secure Integration Server by activating or deactivating their corresponding modules.

4.7.2 OPC UA Client

4.7.2.1 OPC UA Client Module

The OPC UA Client Module allows the dataFEED Secure Integration Server to create OPC UA client instances which are used to connect to external OPC UA servers. The information retrieved from the external server through the OPC UA client connection is then aggregated into the existing internal address spaces and exposed on the configured OPC UA server endpoints to be accessed by external OPC UA clients .

Each connection to an external OPC UA server requires one OPC UA client connection configured and shall use one OPC UA connection license slot.

OPC UA client connection supported features:

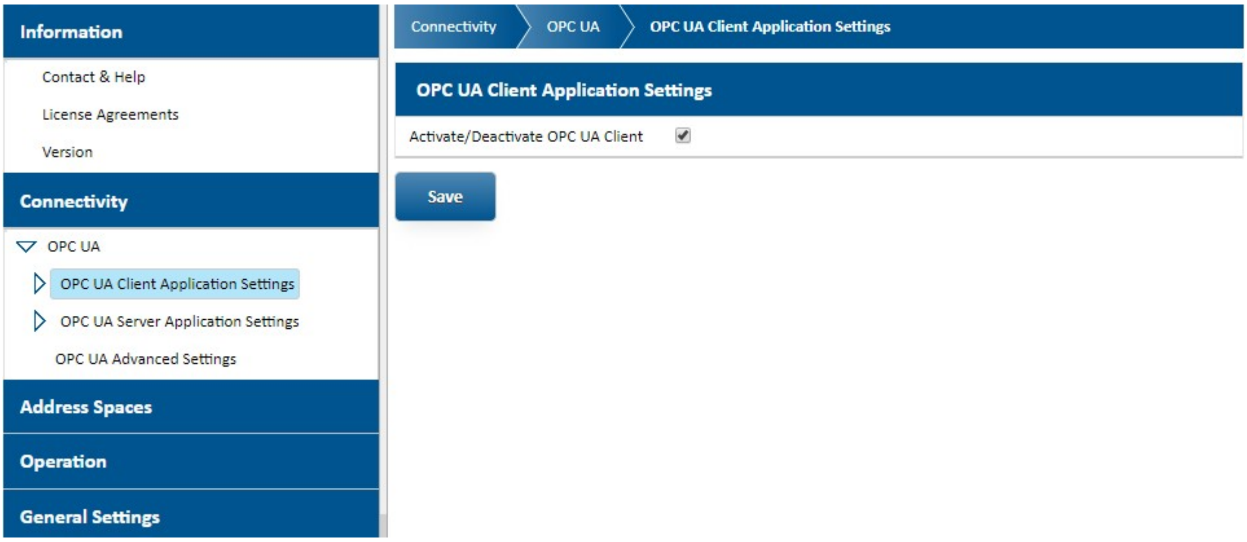
Parameter name	Supported features
transport protocol	• **opc.tcp** • **https**
message encoding	• **binary (serialized byte array)**
security modes	• **None** • **Sign** • **SignAndEncrypt**
security policy (depends on security mode)	• **None** • **Basic256** • **Basic256Sha256** • **Basic128Rsa15** • **Aes128_Sha256_RsaOaep** • **Aes256_Sha256_RsaPss**
authentication mechanism	• **Anonymous** • **username and password** • **certificate**

Table: OPC UA Client, Supported Features

Enabling/Disabling OPC UA Client Module

To enable or disable the OPC UA client module, navigate to **Connectivity -> OPC UA -> OPC UA Client Application Settings** and change the state of the module by checking/unchecking the **[Activate/ Deactivate OPC UA Client]** checkbox. The checkbox state reflects the module state:

- **checked** ☑ : OPC UA client module enabled
- **unchecked** □ : OPC UA client module disabled

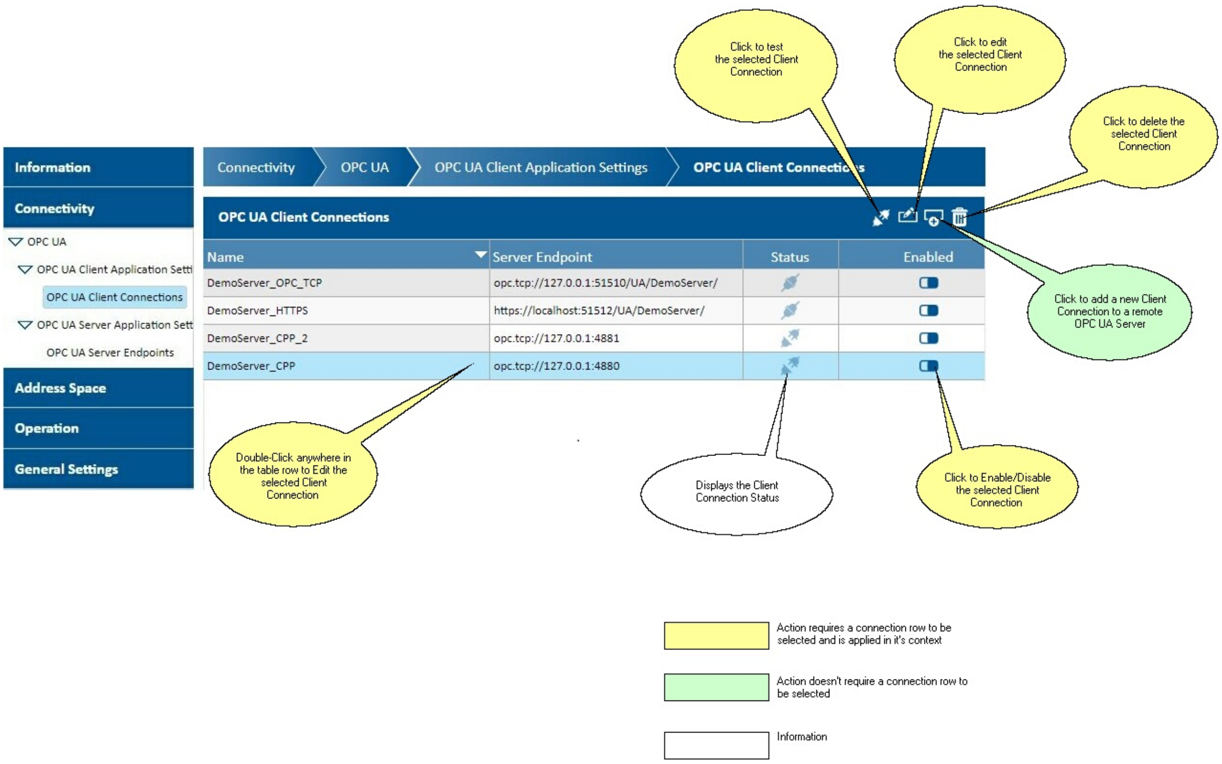


Activate/Deactivate OPC UA Client ☑

Figure: OPC UA Client Application Settings

4.7.2.2 Client Connections

All configured OPC UA client connection area easily accessible by navigating to **Connectivity -> OPC UA -> OPC UA Client Application Settings -> OPC UA Client Connections**. The default configuration is empty, therefore no OPC UA client connections will be shown. A pre-populated sample of the OPC UA client connections overview is pictured below:


Click to test the selected Client Connection
Click to edit the selected Client Connection
Click to delete the selected Client Connection
Click to add a new Client Connection to a remote OPC UA Server
Double-Click anywhere in the table row to Edit the selected Client Connection
Displays the Client Connection Status
Click to Enable/Disable the selected Client Connection
Information
Connectivity
OPC UA
OPC UA Client Application Setti
OPC UA Client Connections
OPC UA Server Application Sett
OPC UA Server Endpoints
Address Space
Operation
General Settings
Connectivity
OPC UA
OPC UA Client Application Settings
OPC UA Client Connectios
Action requires a connection row to be selected and is applied in it's context
Action doesn't require a connection row to be selected
Information

OPC UA Client Connections

Name	Server Endpoint	Status	Enabled
DemoServer_OPC_TCP	opc.tcp://127.0.0.1:51510/UA/DemoServer/		
DemoServer_HTTPS	https://localhost:51512/UA/DemoServer/		
DemoServer_CPP_2	opc.tcp://127.0.0.1:4881		
DemoServer_CPP	opc.tcp://127.0.0.1:4880		

Figure: OPC UA Client, Client Connections Overview

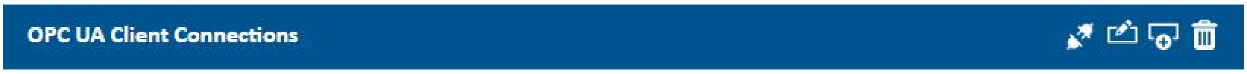
The OPC UA client connections are presented in a table format, each row represents a connection and the information in the table is sortable by clicking the table header. The table header information is described in the following table:

Column name	Information details
Name	Connection name as defined at creation time.
Server Endpoint	The remote OPC UA server endpoints URL.
Status	Describes the **state of the OPC UA connection;** can be either **Connected** when the OPC UA client connection is connected to the remote OPC UA server or **Disconnected** when the OPC UA client connection is not connected to the remote OPC UA server**.** Connection status is dynamically updated each 2 seconds.
Enabled	Describes the configuration state of the OPC UA client connection. Possible values are **Enabled** or **Disabled** .

	Note: Clicking on the current configuration state icon would trigger a state toggle: • **Enabled** ◐ **-> Disabled** ⊗ • **Disabled** ⊗ **-> Enabled** ◐

Table: OPC UA Client, Connection Fields

4.7.2.3 Client Connection Creation



Information bar

Figure: OPC UA Client, Client Connections Information Menu Bar

The **OPC UA Client Connection** information bar provides four buttons with following functionality:

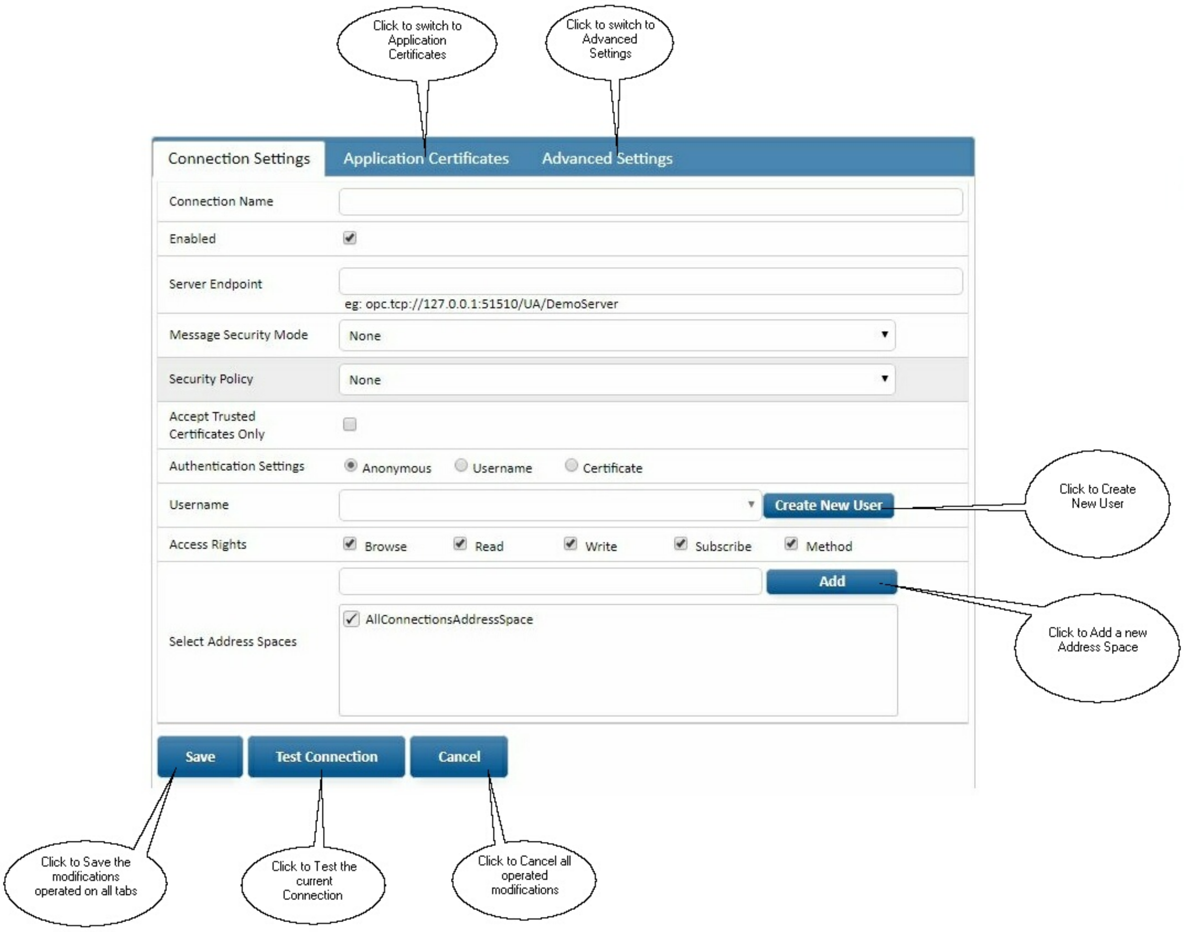
Button	Action
🔌	Test existing OPC UA client connection.
✎	Edit existing OPC UA client connection.
⊕	Add new OPC UA client connection.
🗑	Delete existing OPC UA client connection.

Figure: OPC UA Client, Buttons

To create a new OPC UA client connection, navigate to **Connectivity -> OPC UA -> OPC UA Client Application Settings -> OPC UA Client Connections** and click the **[Add new connection]** ⊕ button on the information bar. The OPC UA client connection configuration page shows up and contains three different configuration tabs: **Connection settings, Certificates** and **Advanced Settings.**

4.7.2.3.1 Connection Settings

Connection Settings is the main view in the OPC UA client connection configuration page and provides a simple and intuitive interface for configuring a new or editing an existing OPC UA Client connection.



Click to switch to Application Certificates

Click to switch to Advanced Settings

Connection Settings | Application Certificates | Advanced Settings

Connection Name	
Enabled	☑
Server Endpoint	eg: opc.tcp://127.0.0.1:51510/UA/DemoServer
Message Security Mode	None ▾
Security Policy	None ▾
Accept Trusted Certificates Only	□
Authentication Settings	● Anonymous ○ Username ○ Certificate
Username	▾ Create New User
Access Rights	☑ Browse ☑ Read ☑ Write ☑ Subscribe ☑ Method
Select Address Spaces	Add ☑ AllConnectionsAddressSpace

Save | Test Connection | Cancel

Click to Create New User

Click to Add a new Address Space

Click to Save the modifications operated on all tabs

Click to Test the current Connection

Click to Cancel all operated modifications

Figure: OPC UA Client, Client Connection Creation, Connection Settings

Actions provided by the page buttons:

Button	Action
Create New User	Convenient way to create a new user in this context. The user Settings 36 page will become active as a consequence of pressing this button.
Add	Convenient way to add a new address-space as a new option to the Address Space selection.
Save	Once the connection settings 160, certificates 164 and advanced setting 172 configurations are finalized the **[Save]** button shall apply the newly configured/modified OPC UA client connection. Connections changes are applied immediatly at runtime.
Test Connection	After finalizing connection settings 160 (also, optionally, certificates 164 and advanced setting 172 configurations) the **[Test Connection]** button shall provide a fast way for testing the connection. The results of the test 179 will be provided in a separate pop-up dialog.
Cancel	Cancel the current client connection configuration session. **Beware all changes shall be lost !**

Table: OPC UA Client, Client Connection Creation, Connection Settings Actions

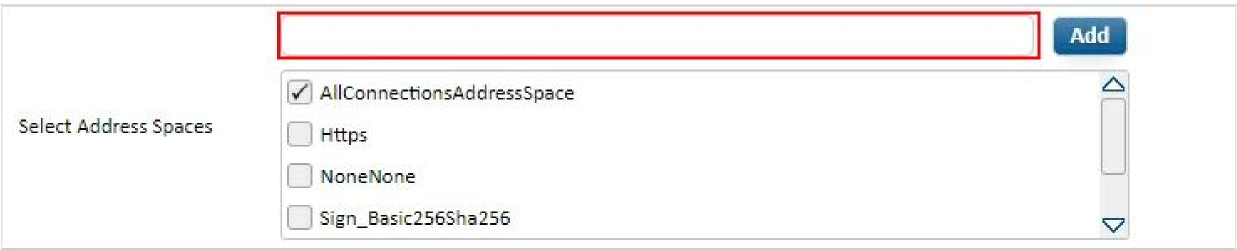
Configuration parameters are described in the following table:

Parameter name	Default value	Value description
Connection Name	**empty**	Defines the connection name as it will show up in the OPC UA client connection overview page. This name shall also be used by the OPC Client when connecting to an external OPC UA server ***Note**: Characters not supported in this field: **# ^ < > / $**
Enable	**Enabled**	Instructs the dataFEED Secure Integration Server to either enable (checked) or disable (unchecked) the currently configured OPC UA Client connection.
Server endpoint	**empty**	External OPC UA server endpoint. USed by the OPC UA client connection to establish a new connection. ***Supported transport protocols: opc.tcp, https** ***Note**: The URL is automatically validated while filled in.
Message Security Mode	**None**	Defines the message security mode used by the OPC UA client connection. ***Supported message security modes: None, Sign, SignAndEncrypt**
Security Policy	**None**	Defines the security policy used by the OPC UA client connection and it Specifies the encryption algorithm applied to the messages.

		***Supported security policies: None, Basic256, Basic256Sha256, Basic128Rsa15**
Accept Trusted Certificates Only	**Disabled**	Instructs the configured OPC UA client connection to accept only trusted certificates. ***Note:** Requires additional manual setup 170 to configure the OPC UA server trusted certificates.
Authentication Settings	**Anonymous**	Defines and sets up the required authentication mechanism. If **Anonymous radio button** is selected, than the client connection is configured to be executed using the Anonymous user. To avoid confusion, a distinction has to be emphasized between the **Username radio button** at this level and the **Username drop-down** list below it. **Relation with the Username drop-down list:** If **Username radio button** is selected, than the **Username drop-down** list will present the configured available user names, from which one has to be chosen, in order to be used in the client authentication process. If the **Certificate** radio button is selected than the user, identified by the **Username drop-down** list value, has to have an associated active(selected) "Outgoing" client certificate(see use case 5 from Users & Identities 35 for more details). Further on, the client authentication mechanism will use the respective active "Outgoing" client certificate to authenticate. In case there is no "Outgoing" client certificate associated to the user the **Username drop-down** list will not permit selecting the Username identifier associated to the user since it will be grayed out.
Username drop-down	**empty**	Username used to connect to the external OPC UA server. See description in **Authentication Settings,** for more details with regards to it's behavior and it's relation with **Authentication Settings.**
Access Rights	**All**	Configures all permitted services on the OPC UA client connection. Enable the service by checking the appropriate service checkbox. **Supported services: Browse, Read, Write, Subscribe, Method**
Select Address Spaces		Defines the destination aggregation address space used to store the external OPC UA server's address space. **Default aggregation address space name**: **AllConnectionsAddressSpace**

Table: OPC UA Client, Client Connection Creation, Connection Settings Parameters

Creating additional aggregation address spaces



Select Address Spaces

☑ AllConnectionsAddressSpace

□ Https

□ NoneNone

□ Sign_Basic256Sha256

Figure: OPC UA Client, Client Connection Creation, Connection Settings Add Address Space

It is possible to create additional aggregation address spaces by filling in the desired address space name in the red highlighted input field and clicking on the **[Add]** button. All available address spaces are visible in a list and can be selected as destination address space for the OPC UA client connection by checking the corresponding checkbox.

Notes on parameters change operations:

A restart of the client connection leading to closing the associated session to the server is triggered if any of the following parameters is changed :

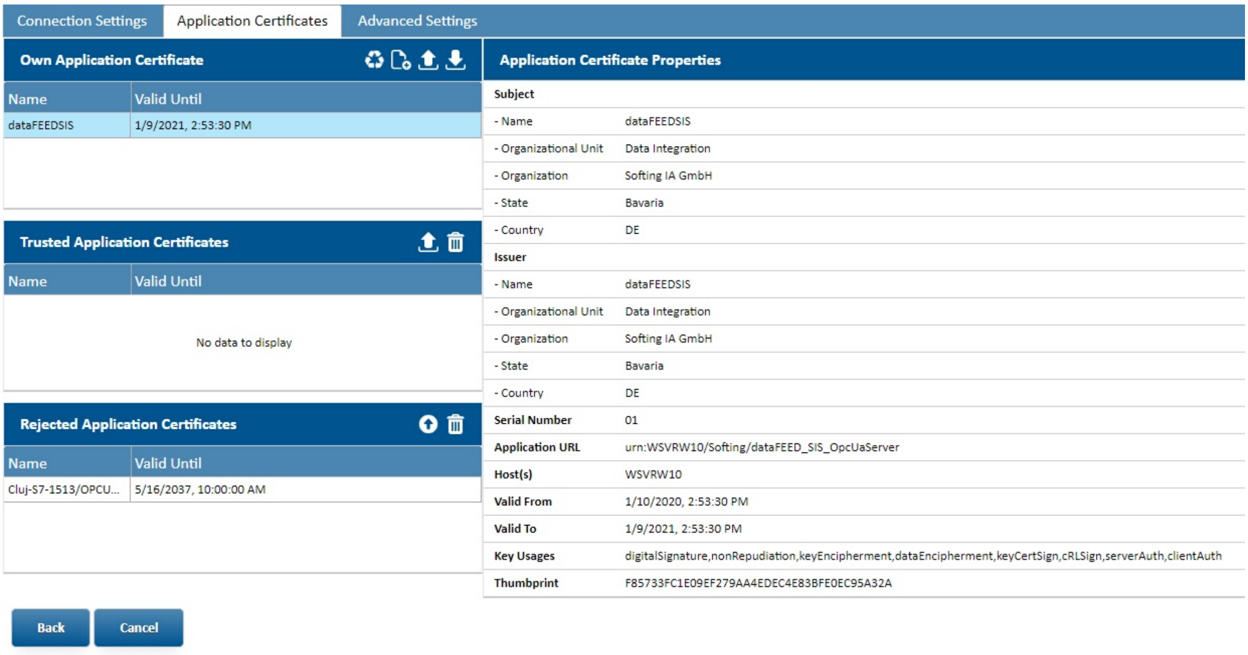
- **Server endpoint**
- **Enabled**
- **Authentication Settings**
- **Username**
- **Message Security Mode**
- **Security Policy**
- **the own application certificate**

Changing access rights has immediate effect upon existing sessions – subsequent UA request will be allowed or denied according to the new rules, and existing subscriptions will stop or resume receiving notifications.

4.7.2.3.2 Certificates

- **Managing the SSL application instance certificates is necessary if the security mode is Sign or SignAndEncrypt or for https connections.**
- **dataFEED Secure Integration Server uses separate PKI stores for each OPC UA client connection, therefore SSL certificates have to be managed for each connection independently.**
- **All certificates generated by the dataFEED Secure Integration Server are self signed**

The certificates page provides an interface for managing the SSL certificates stored in the connection's PKI store.



Own Application Certificate

Name	Valid Until
dataFEEDSIS	1/9/2021, 2:53:30 PM

Trusted Application Certificates

Name	Valid Until
No data to display	

Rejected Application Certificates

Name	Valid Until
Cluj-S7-1513/OPCU...	5/16/2037, 10:00:00 AM

Application Certificate Properties

Subject	
- Name	dataFEEDSIS
- Organizational Unit	Data Integration
- Organization	Softing IA GmbH
- State	Bavaria
- Country	DE
Issuer	
- Name	dataFEEDSIS
- Organizational Unit	Data Integration
- Organization	Softing IA GmbH
- State	Bavaria
- Country	DE
Serial Number	01
Application URL	urn:WSVRW10/Softing/dataFEED_SIS_OpcUaServer
Host(s)	WSVRW10
Valid From	1/10/2020, 2:53:30 PM
Valid To	1/9/2021, 2:53:30 PM
Key Usages	digitalSignature,nonRepudiation,keyEncipherment,dataEncipherment,keyCertSign,cRLSign,serverAuth,clientAuth
Thumbprint	F85733FC1E09EF279AA4EDEC4E83BFE0EC95A32A

Figure: OPC UA Client, Client Connection Creation, Application Certificates

Bottom page buttons actions:

Button	Action
Back	Navigate to the connection settings 160 page
Cancel	Cancel the current client connection configuration session. **Beware all changes shall be lost !**

Table: OPC UA Client, Client Connection Creation, Application Certificates Buttons

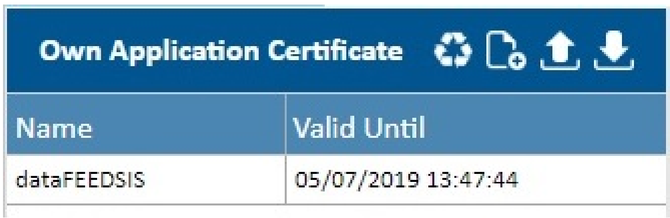
There are four highlighted sections on the certificates page:

Area	Colour	Details
Own application certificates	Blue	Lists the certificate used to identify the dataFEED Secure Integration Server connection application instance. This certificate is uniquely created for each OPC UA client connection.
Trusted application certificates	Green	Contains certificates identifying other OPC UA application instances which are being trusted by the current OPC UA connection instance. When secured connections are created OPC UA connections can be established only when both involved parties trust each others application certificates.
Rejected application certificates	Red	Contains all certificates which were rejected during the connection establishment phase. No OPC UA connections can be established to the corresponding OPC UA application instance unless the certificates are moved into the trusted certificates folder.
Application certificates properties	Yellow	Information about the selected certificate on any of the three certificates folders (Own, Trusted, Rejected) is visible in the application certificates properties area.

Table: OPC UA Client, Client Connection Creation, Application Certificates Sections

1. Own Application Certificate

Only one certificate should be visible in the own certificate area. This is the certificate which is used by the running OPC UA application to identify itself.



Own Application Certificate

Name	Valid Until
dataFEEDSIS	05/07/2019 13:47:44

Figure: OPC UA Client, Client Connection Creation, Own Application Certificate

Several operations are accessible using the buttons placed top right:

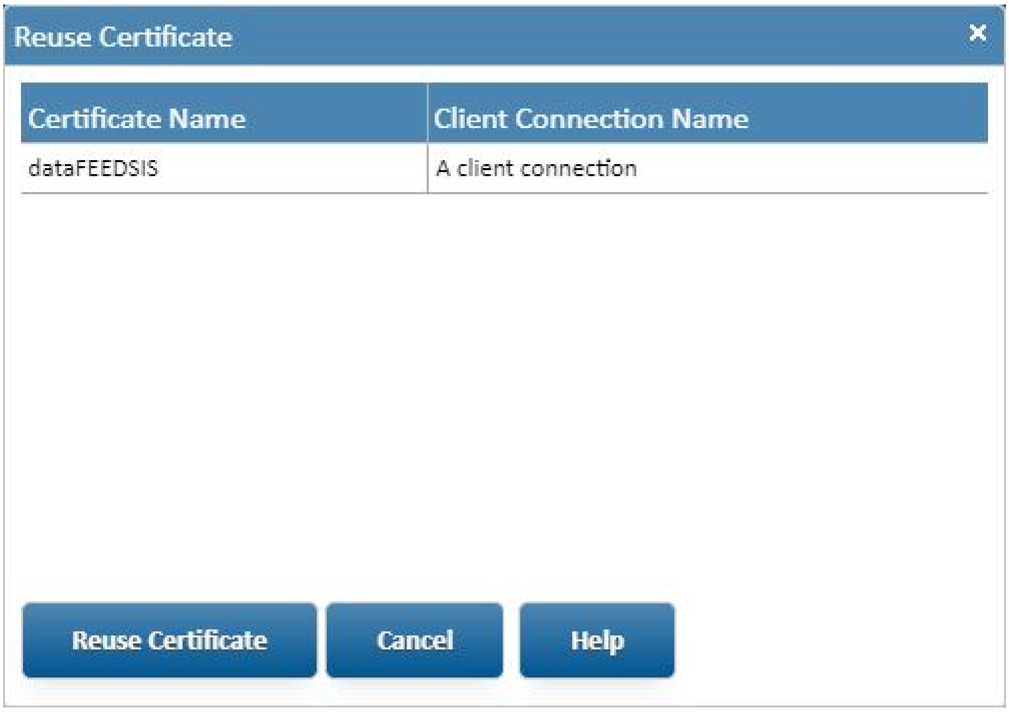
Button	Action
♻	Reuse application certificate
🗋	Generate application certificate
⬆	Upload application certificate
⬇	Download application certificate

Table: OPC UA Client, Client Connection Creation, Own Application Certificate Buttons

a. Reuse application certificate

Provides the possibility to reuse a certificate which is already in use, to identify a different configured OPC UA client connection. Clicking the **[Reuse certificate]** button brings up a window which lists the available client connection.

To reuse the certificate of an existing connection, select the connection in the list and click the **[Reuse Certificate]** Reuse Certificate labeled button.



Certificate Name	Client Connection Name
dataFEEDSIS	A client connection

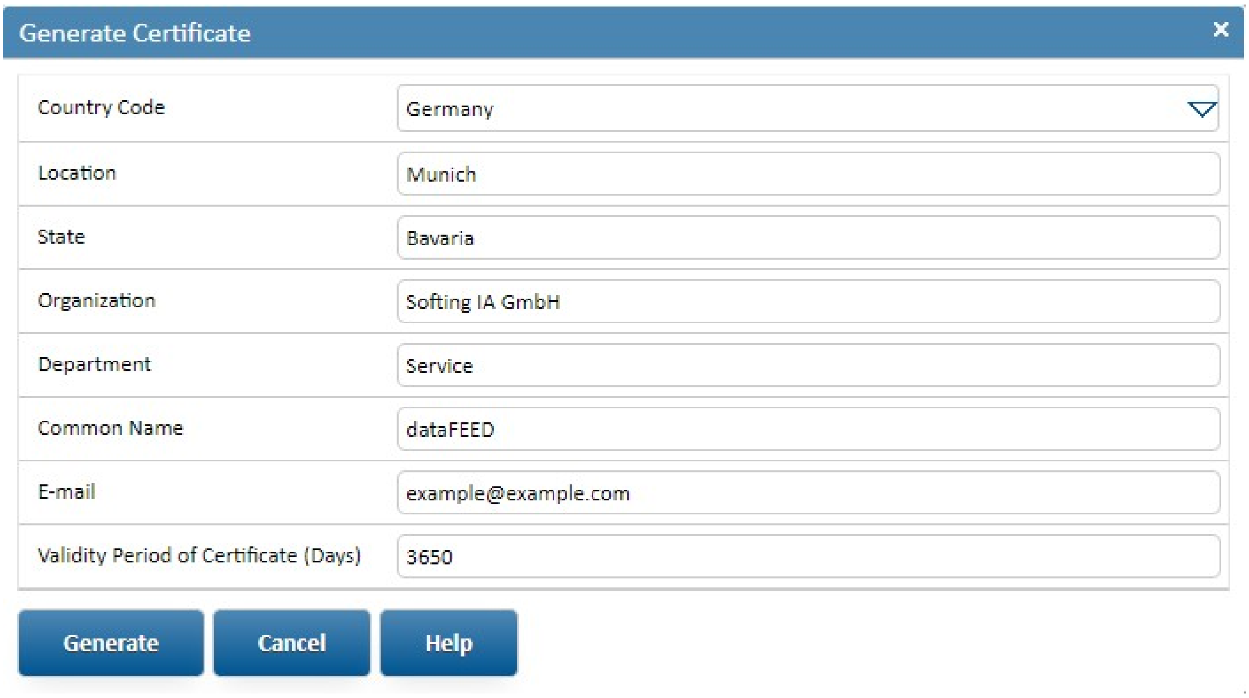
Reuse certificate window

Figure: OPC UA Client, Client Connection Creation, Reuse Certificate

b. Generate application certificate

Will create a new replacement certificate for the current own certificate.

To generate a new application certificate, click on the **Generate certificate** button and the following window will pop up:



Country Code	Germany
Location	Munich
State	Bavaria
Organization	Softing IA GmbH
Department	Service
Common Name	dataFEED
E-mail	example@example.com
Validity Period of Certificate (Days)	3650

Figure: User & Identities, Generate Certificate

The fields are populated with some proposed values, according to the corresponding values defined in the Application Settings 28 page.

By hovering over the input text fields, a Tool-tip will appear to inform about the mandatory state of the field with regards to the generation of the Certificate.

Certificate generation fields description:

Parameter name	Mandatory	X509 field name	Details
Country Code	**NO**	**C**	Country Name as ISO3166 two character country code
Location	**YES**	**L**	Locality name, generally city
State	**YES**	**ST**	State or Province Name
Organization	**YES**	**O**	Organization Name
Department	**YES**	**OU**	Organizational Unit Name
Common Name	**YES**	**CN**	Common Name
Email	**NO**		Email Address
Validity Period	**YES**		Validity period starting at the time of generation

Table: Connection Certificate, Certificate Generation Fields

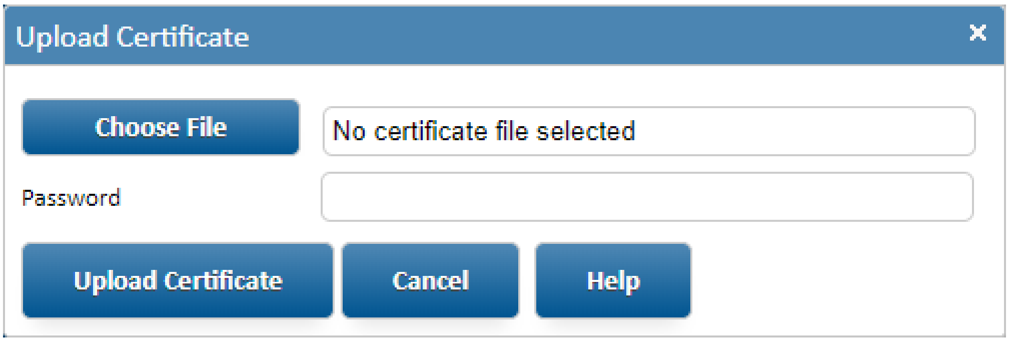
Press the Generate button to generate and add the certificate own application certificate list:

⚠ **After regeneration, the existing applications trust relationships will be voided.**

c. Upload application certificate

Provides a simple way to replace the currently used application identification certificate with an already existing certificate. The upload certificate windows opens by clicking the **[Upload certificate]** button. In this view the new certificate file shall be selected by pressing the **[Choose File]** button.

If the certificate requires a password, the corresponding password input field is to be used, otherwise the field should be left empty.



Upload Certificate

No certificate file selected

Password

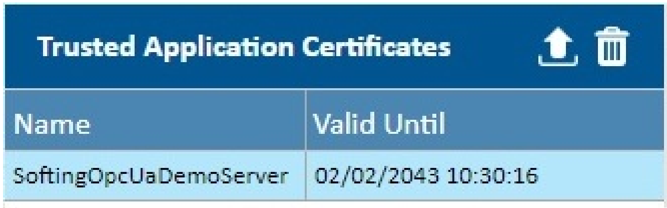
Figure: OPC UA Client, Client Connection Creation, Upload Certificate

d. Download application certificate

Provides a way to download the current own certificate. The download will start automatically and the filename format is **SoftingOpcUaConnection[*thumbprint*].der** where ***thumbprint*** is the actual thumbprint of the downloaded certificate.

2. Trusted Application Certificates

Allows manipulation and information retrieval on the current connection's trusted certificates. All remote OPC UA application instances whose certificates are listed in this view have a trust relationship established with the current connection.



Trusted Application Certificates

Name	Valid Until
SoftingOpcUaDemoServer	02/02/2043 10:30:16

Figure: OPC UA Client, Client Connection Creation, Trusted Certificates

Several operations are accessible using the buttons placed top right:

Button	Action
⬆	Upload certificate
🗑	Delete certificate

Figure: OPC UA Client, Client Connection Creation, Trusted Certificates Buttons

a. Upload certificate

Uploading a trusted certificate is required:

- When an OPC UA client connection has the **Accept Trusted Certificates Only** option enabled. In this case the external OPC UA server's certificate needs to be uploaded in the client connection trusted certificates section.

An alternative solution for the above scenario is to entrust an already rejected certificate 170.

Provides a way to add a pre-owned certificate, locally stored, to the trusted folder. After clicking the **[Upload Certificate]** button a new view, where the new certificate file shall be selected by pressing the **[Choose file]** button, opens. To finalize the action press the **[Upload Certificate]** button as described in **Figure: OPC UA Client, Client Connection Creation, Upload Certificate.**

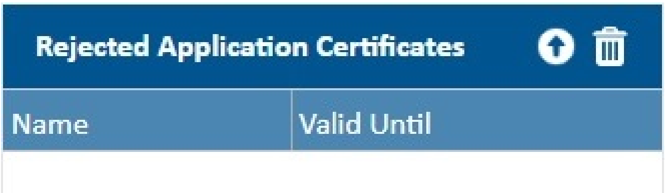
b. Delete certificate

Deletes the currently selected certificate from the trusted certificates folder. After deletion the trust relationship with the deleted certificate owner application will be invalidated.

3. Rejected Application Certificates

dataFEED Secure Integration Server does not automatically trust remote OPC UA application instance certificates therefore secured connection attempts may result in remote certificates automatically stored in the Rejected certificates folder.

All remote OPC UA application instance certificates whose connection establishment to the current OPC UA connection failed due to trust relationship condition should be listed under the rejected certificates view.



Rejected Application Certificates ⬆ 🗑

Name	Valid Until

Figure: OPC UA Client, Client Connection Creation, Rejected Application Certificates

Several operations are accessible using the buttons placed top right:

Button	Action
⬆	Move to Trusted
🗑	Delete certificate

Table: OPC UA Client, Client Connection Creation, Rejected Application Certificates Buttons

a. Move to Trusted

Provides the functionality needed to trust an alredy rejected OPC UA application instance by moving its rejected certificate into the trusted certificates folder. Clicking the **[Move to Trusted]** button will move the selected rejected certificate into the trusted certificates folder. The result of this action is visible in the configuration page and the previously rejected certificate shall now be visible only under the trusted certificates list.

This is an important manual step required:

- To enable a configured OPC UA client connection, having the **Accept Trusted Certificates Only** option enabled, connect the external OPC UA server.

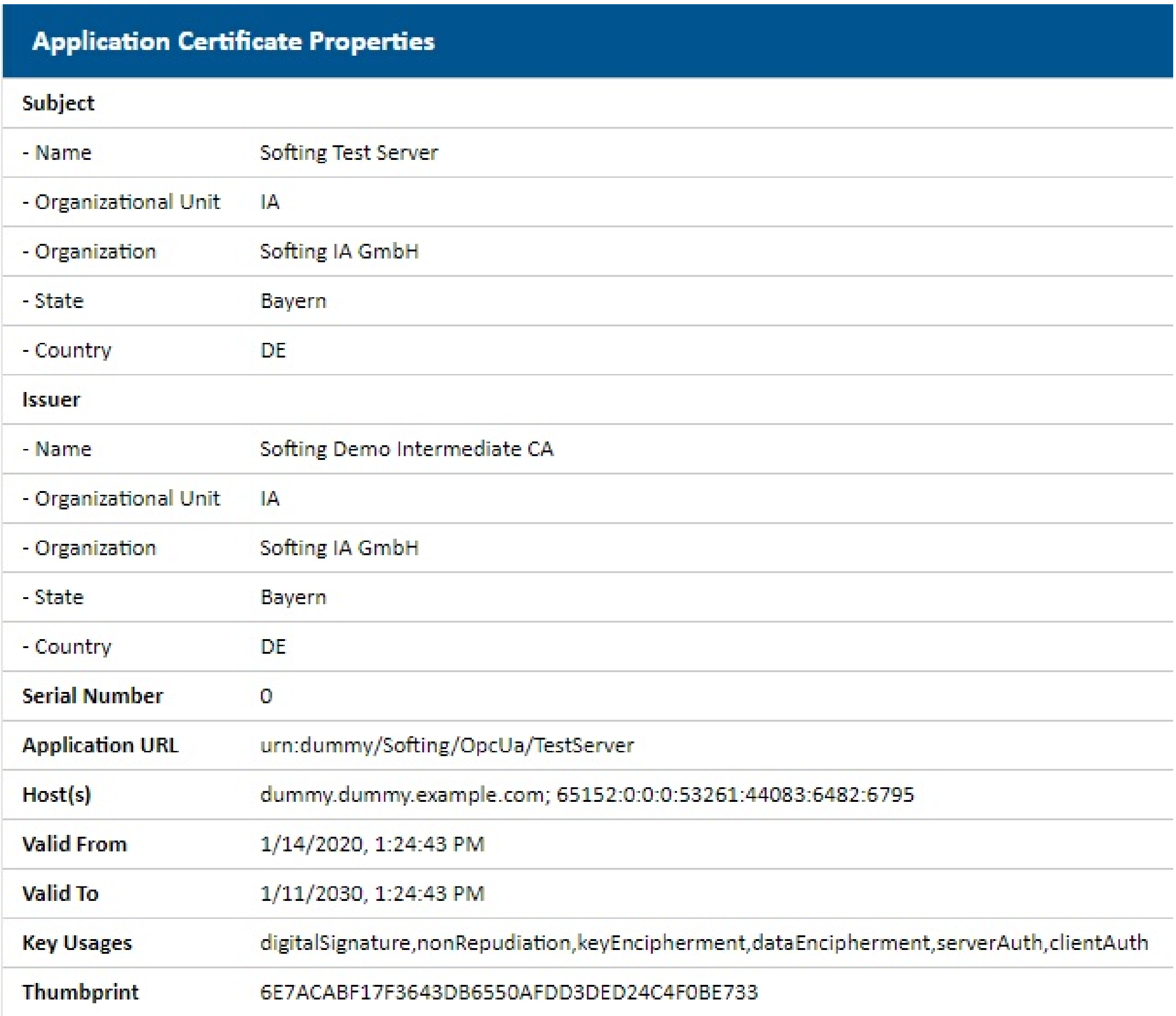
Any previously trust-related failed connection attempts, will subsequently succeed after moving the certificates to the trusted application certificates folder.

b. Delete Certificate

Deletes the currently selected certificate from the rejected certificates folder.

4. Application Certificates Properties

Information about the selected certificate is available in the certificates properties area.



Application Certificate Properties

Subject	
- Name	Softing Test Server
- Organizational Unit	IA
- Organization	Softing IA GmbH
- State	Bayern
- Country	DE
Issuer	
- Name	Softing Demo Intermediate CA
- Organizational Unit	IA
- Organization	Softing IA GmbH
- State	Bayern
- Country	DE
Serial Number	0
Application URL	urn:dummy/Softing/OpcUa/TestServer
Host(s)	dummy.dummy.example.com; 65152:0:0:0:53261:44083:6482:6795
Valid From	1/14/2020, 1:24:43 PM
Valid To	1/11/2030, 1:24:43 PM
Key Usages	digitalSignature,nonRepudiation,keyEncipherment,dataEncipherment,serverAuth,clientAuth
Thumbprint	6E7ACABF17F3643DB6550AFDD3DED24C4F0BE733

Figure: OPC UA Client, Client Connection Creation, Application Certificates Properties

4.7.2.3.3 Advanced Settings

The advanced settings page provides the interface to adjust some OPC UA sensitive communication parameters, in order to handle various types of external OPC UA servers and their specific behaviour (eg: different response times during session creation) . By correctly configuring these advanced parameters based on the targeted OPC UA server capabilities and resources the overall connection reliability and availability could improve .

Changing the advanced settings presented herein might cause unreliable connections or data exchange problems; therefore thorough knowledge of each parameter's meaning it required and the possible consequences resulting from its change !

Advanced parameters changes on an active connection shall trigger a connection restart.

To access the advanced settings page click on the **[Advanced Settings]** tab in the client connection creation main view. The tab is split in four, exculsively collapsible, sections; **[Service Settings]** section is expanded by default.

Bottom page buttons actions:

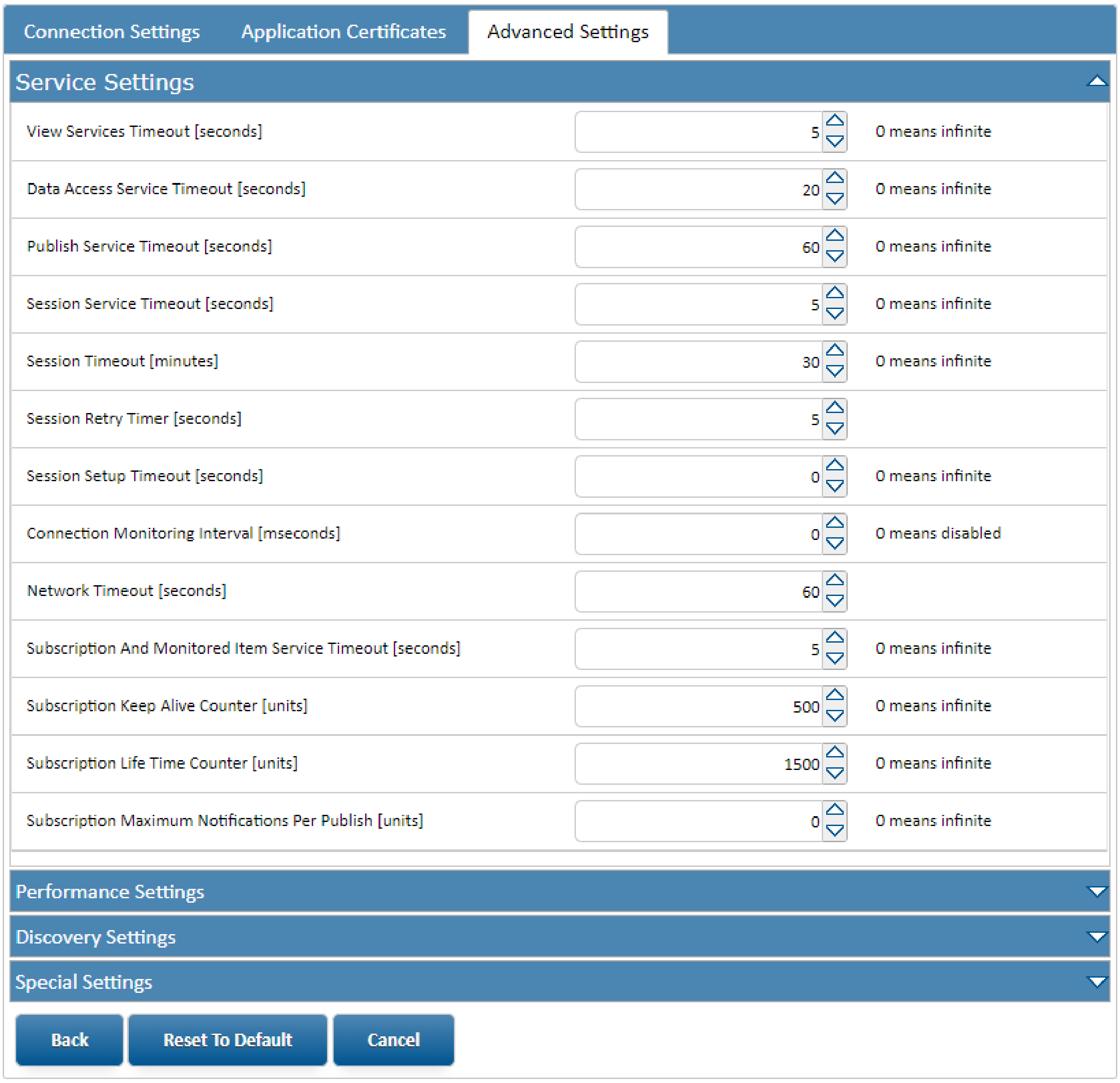
Button	Action
	Navigate to the connection settings 160 page
	If present, it resets all parameters in the current, expanded, advanced settings page section to their default values 173.
	Cancel the current client connection configuration session. ***Note: all changes shall be lost !**

Figure: OPC UA Client, Client Connection Creation, Advanced Settings Buttons

To change any parameter value either select the appropriate input field and type in the desired value. Note that automatic range checking applies for each field, or use the spin buttons ⇕ to adjust the values by increasing or decreasing them.

1. Service Settings

Allows access to a set of OPC UA communication related parameters which can be adjusted to change the OPC UA client's behaviour.



Parameter	Value	
View Services Timeout [seconds]	5	0 means infinite
Data Access Service Timeout [seconds]	20	0 means infinite
Publish Service Timeout [seconds]	60	0 means infinite
Session Service Timeout [seconds]	5	0 means infinite
Session Timeout [minutes]	30	0 means infinite
Session Retry Timer [seconds]	5	
Session Setup Timeout [seconds]	0	0 means infinite
Connection Monitoring Interval [mseconds]	0	0 means disabled
Network Timeout [seconds]	60	
Subscription And Monitored Item Service Timeout [seconds]	5	0 means infinite
Subscription Keep Alive Counter [units]	500	0 means infinite
Subscription Life Time Counter [units]	1500	0 means infinite
Subscription Maximum Notifications Per Publish [units]	0	0 means infinite

Figure: OPC UA Client, Client Connection Creation, Advanced Settings, Service Settings Section

All available parameters with details and unit information are described in the table below:

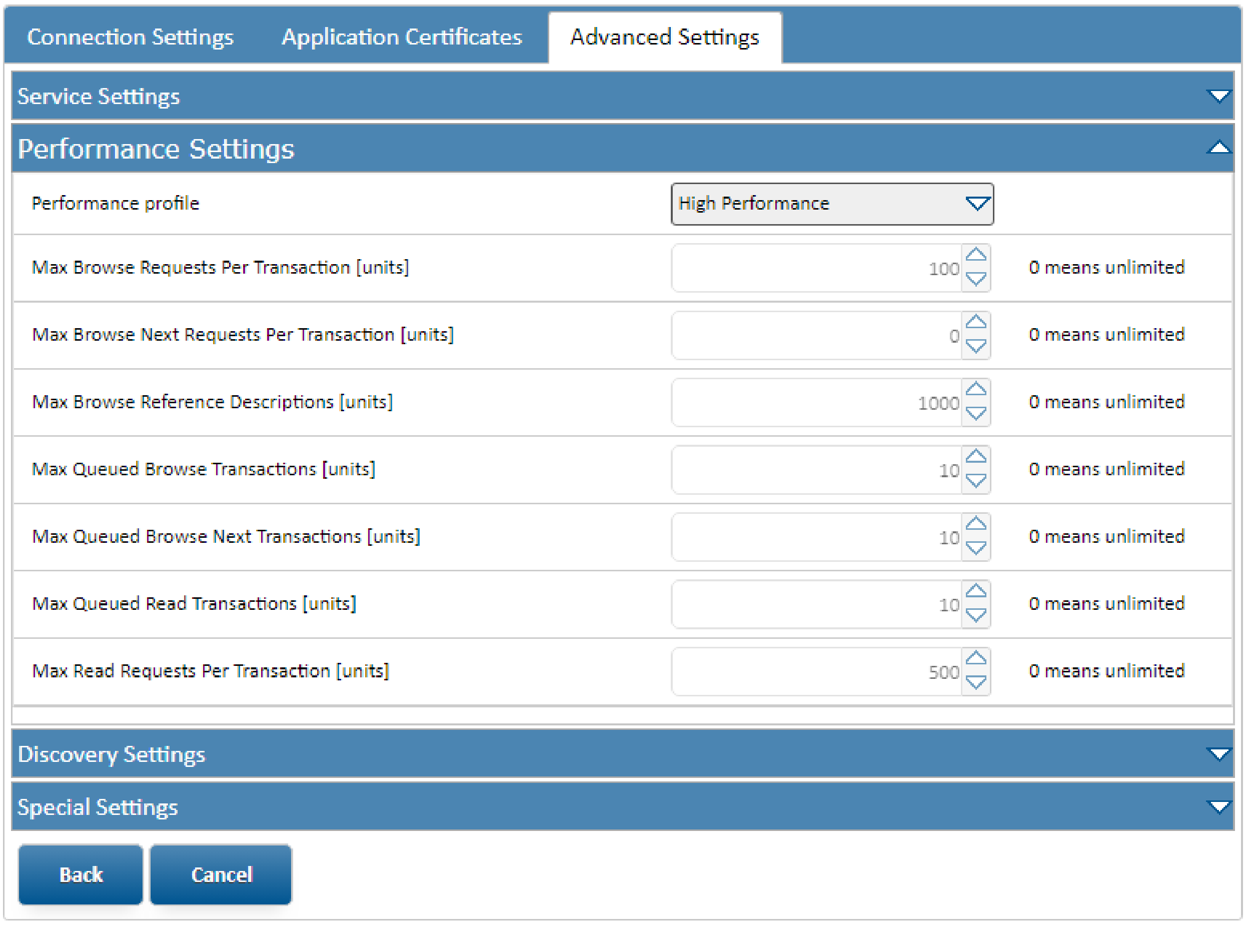
Parameter name	Default Value	Unit	Details
View Services Timeout	**5**	**seconds**	Timeout for browse service related requests. eg: Instructs the OPC UA Client how long to wait for a browse request.
Data Access Service Timeout	**20**	**seconds**	Timeout for read service and write service related requests. eg: Instructs the OPC UA Client how long to wait for a read or write request.

Publish Service Timeout	**60**	**seconds**	Timeout for publish service related requests.
Session Service Timeout	**5**	**seconds**	The timeout for the session service related requests.
Session Timeout	**30**	**minutes**	Maximum number of milliseconds that a session should remain open without activity. If the client fails to communicate within this interval, then the server shall automatically terminate the session. Any further communication using this session is no longer possible until client re-connects the session.
Session Retry Timer	**5**	**seconds**	Sets the interval in which the OPC UA client tries to re-connect a broken session and/or subscription.
Session Setup Timeout	**0**	**seconds**	This parameter specifies the maximum amount of time allowed for application to connect to the external server.
Connection Monitoring Interval	**0**	**miliseconds**	Sets the interval for verifying the health of the connection to the server. *By default the functionality is disabled.
Network Timeout	**60**	**seconds**	Timeout to use when trying to establish a network connection. A value greater than 0 has to be provided.
Subscription And Monitored Item Service Timeout	**5**	**seconds**	Timeout for subscription service and monitor item related requests.
Subscription Keep Alive Counter	**500**	**units**	Sets the subscription's keep alive counter threshold used to send keep alive notification messages.
Subscription Life Time Counter	**1500**	**units**	Sets the threshold for the subscription's life timer counter. Whenever the life time counter reaches the provided threshold, the server deletes she Subscription.
Subscription Maximum Notifications Per Publish	**0 (infinte)**	**units**	Sets the maximum number of notifications that a client wishes to receive per publish response. If the client does not want to impose restrictions on the message size of the publish response, this parameter should be set to 0.

Table: OPC UA Client, Client Connection Creation, Advanced Settings Fields

2. Performance Settings

Allows access to a set of OPC UA client specific, performance related, parameters predefined profiles used to increase or decrease, according to the OPC UA server performance, OPC UA read and browse communication throughput.



Performance profile	High Performance	
Max Browse Requests Per Transaction [units]	100	0 means unlimited
Max Browse Next Requests Per Transaction [units]	0	0 means unlimited
Max Browse Reference Descriptions [units]	1000	0 means unlimited
Max Queued Browse Transactions [units]	10	0 means unlimited
Max Queued Browse Next Transactions [units]	10	0 means unlimited
Max Queued Read Transactions [units]	10	0 means unlimited
Max Read Requests Per Transaction [units]	500	0 means unlimited

Figure: OPC UA Client, Client Connection Creation, Advanced Settings, Performance Settings Section

The four performance profile available are described below. Switch between profiles using the **[Profile type]** selection list.

Performance Profile	Description
Low Performance	Predefined, non changeable, profile. shall be selected when low resource/ performance servers are to be connected.
Medium Performance	Predefined, non changeable, profile. Most used servers are to be connected.
High Performance	Predefined, non changeable, profile. shall be selected when high resource/ performance servers are to be connected.
Custom Profile	User customizable profile.

Table: OPC UA client connection performance profiles description

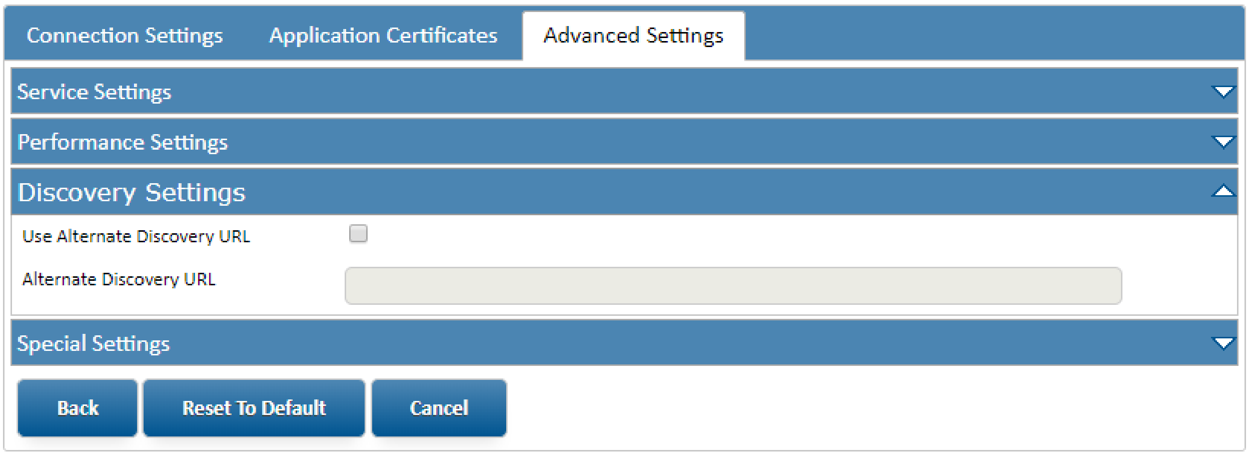
Performance parameters are detailed in the table below:

Parameter name	Performance Profile Default Values	Details

	Low	Standard	High	
Max Browse Requests Per Transaction	**1**	**10**	**100**	Maximum browse requests to be included in one transaction targeting the external OPC UA server. **Note**: A value of 0 used in a custom profile will not limit the number of requests to be included in one transaction.
Max Browse Next Requests Per Transaction	**1**	**0**	**0**	Maximum browse next requests to be included in one transaction targeting the external OPC UA server. **Note**: A value of 0 used in a custom profile will not limit the number of requests to be included in one transaction
Max Browse Reference Descriptions	**100**	**1000**	**1000**	Maximum browse reference descriprions to be included in one request targeting the external OPC UA server. **Note**: A value of 0 used in a custom profile will not limit the number of references to be included in one request
Max Queued Browse Transactions	**1**	**10**	**10**	Browse transaction queue size. The queue is used to handle concurrent browse transactions targeting the external OPC UA server. **Note**: A value of 0 used in a custom profile will not limit the queue size
Max Queued Browse Next Transactions	**20**	**500**	**500**	Browse next transaction queue size. The queue is used to handle concurrent browse next transactions targeting the external OPC UA server. **Note**: A value of 0 used in a custom profile will not limit the queue size
Max Queued Read Transactions	**1**	**10**	**10**	Read transaction queue size. The queue is used to handle concurrent read transactions targeting the external OPC UA server. **Note**: A value of 0 used in a custom profile will not limit the queue size
Max Read Requests Per Transaction	**20**	**500**	**500**	Maximum read requests to be included in one transaction targeting the external OPC UA server. **Note**: A value of 0 used in a custom profile will not limit the number of requests to be included in one transaction

Table: OPC UA client connection performance parameters description

3. Discovery Settings



Use Alternate Discovery URL □

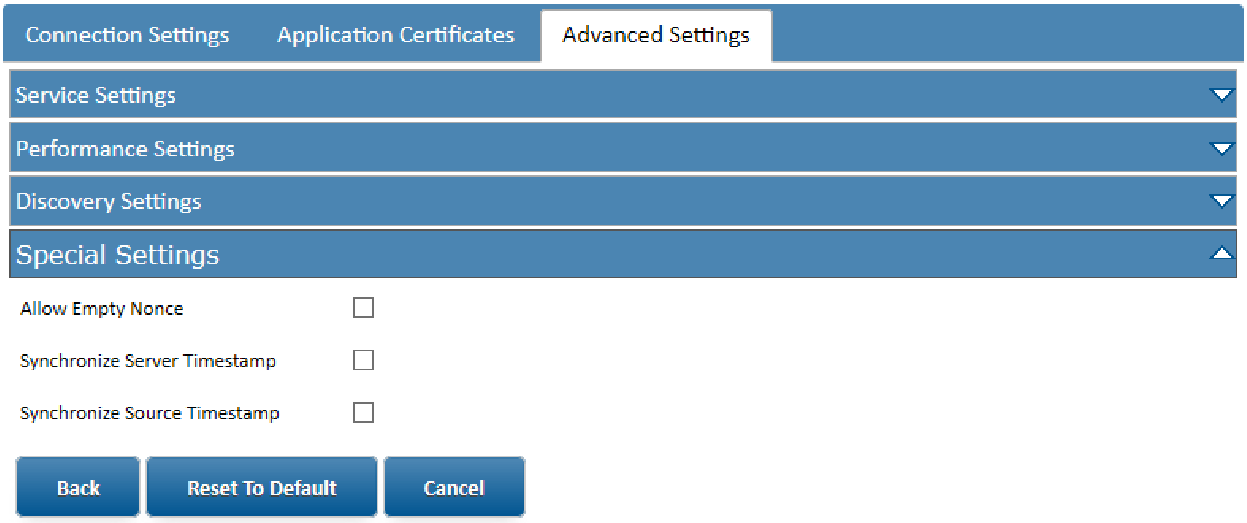
Alternate Discovery URL

Figure: OPC UA Client, Client Connection Creation, Advanced Settings, Discovery Settings Section

- **Use Alternate Discovery URL**:
  - To be used when an OPC-UA server exposes a dedicated non secure endpoint other than the one used by the OPC-UA communication for invoking the "GetEndpoints" service on it. It is a different URL than the one provided in the "Connection Settings -> Endpoint" used to first establish an unsecured connection with, and then invoke the "GetEndpoints" service on it.
  - The input URL has to be specified under the "Alternate Discovery URL" field.

4. Special Settings

Parameters defined in this section are highly specialized and particular to some OPC UA Server implementation. Due to this reasons all parameters in the section are explained more detailed.



Allow Empty Nonce □

Synchronize Server Timestamp □

Synchronize Source Timestamp □

Figure: OPC UA Client, Client Connection Creation, Advanced Settings, Special Settings Section

- **Allow Empty Nonce**:

  - Nonce: A randomly generated value used to defeat "playback" attacks. One party randomly generates a nonce and sends it to the other party. The receiver encrypts it using the agreed upon secret key and returns it to the sender. Because the nonce was randomly generated by the sender this defeats playback attacks because the re-player can't know in advance the nonce the sender will generate. The receiver denies connections that do not have the correctly encrypted nonce.
  - By checking the corresponding check-box, a secure communication channel can be established with servers which do not provide a valid Nonce in the handshake phase of the encrypted communication. If such a Nonce is provided by the external server targeted by the encrypted connection while the check-box is selected the Nonce is used, making this option selection ineffective.
  - Use this option with caution since it might cause a security risk.

- **Synchronize Server Timestamp**:
  - By checking this check-box, the Server Timestamp attribute of the DataValues retrieved from the corresponding OPC UA Client Connection is set to the current time of the dataFEED Secure Integration Server.
  - This setting is applied live for all the DataValues retrieved from the moment of saving the configuration, without the need to restart the OPC UA Client Connection.

- **Synchronize Source Timestamp**:
  - By checking this check-box, the Source Timestamp attribute of the DataValues retrieved from the corresponding OPC UA Client Connection is set to the current time of the dataFEED Secure Integration Server.
  - This setting is applied live for all the DataValues retrieved from the moment of saving the configuration, without the need to restart the OPC UA Client Connection.
  - Note that this setting can be checked only if the *Synchronize Server Timestamp* is also checked.

4.7.2.4 Edit Existing Client Connection

To edit an existing OPC UA client connection navigate to **Connectivity -> OPC UA -> OPC UA Client Application Settings -> OPC UA Client Connections,** select the appropriate endpoint entry in the list and click the **[Edit connection]** ✎ button on the information bar. Editing the existing connection is similar to creating a new connection 160 with some of the fields being grayed out as they are not changeable after creation (eg: Connection Name).

4.7.2.5 Test Existing Client Connection

To perform a test on an existing OPC UA client connection navigate to **Connectivity -> OPC UA -> OPC UA Client Application Settings -> OPC UA Client Connections,** select the appropriate endpoint entry in the list and click the **[Test connection]** button on the information bar.

Testing a connection is also possible within the Connection Settings 160 page, at the time a new connection is created or while editing an existent connection.

Connection test is possible only while the system is in running state (see the System States 240 page for more details) and the OPC UA Client Module is enabled (find more details here 157).

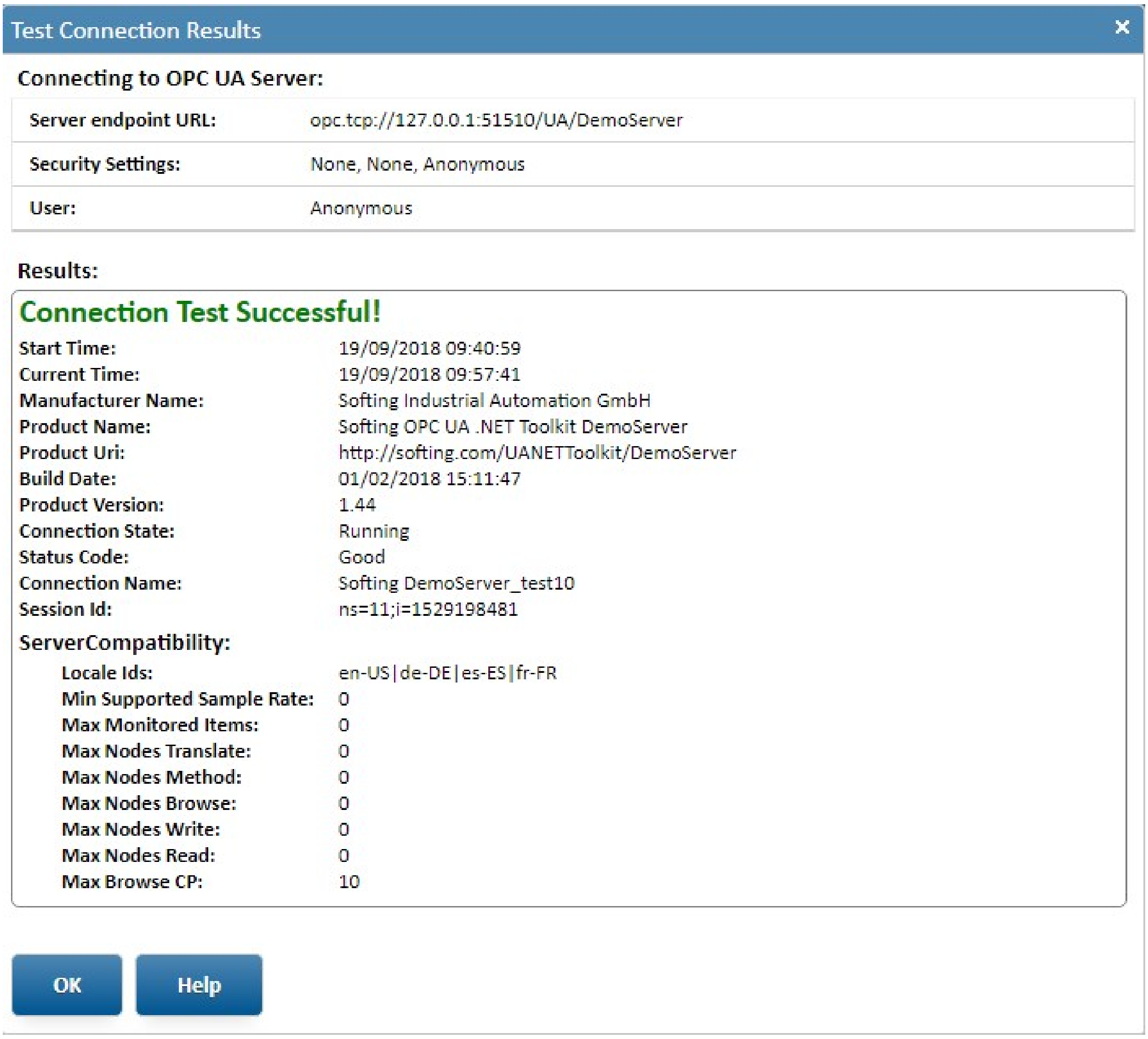
The connection test feature also requires an available license slot 57 in order to work.

The test connection cannot be canceled. In some cases it may take up to Network Timeout parameter defined for the connection being tested (default 60 seconds).

Test Connection Results

The results of a connection test are presented in a separate pop-up dialog.

In case of a successful test, additional information retrieved from the external server is displayed.



Test Connection Results

Connecting to OPC UA Server:

Server endpoint URL:	opc.tcp://127.0.0.1:51510/UA/DemoServer
Security Settings:	None, None, Anonymous
User:	Anonymous

Results:

Connection Test Successful!

Start Time:	19/09/2018 09:40:59
Current Time:	19/09/2018 09:57:41
Manufacturer Name:	Softing Industrial Automation GmbH
Product Name:	Softing OPC UA .NET Toolkit DemoServer
Product Uri:	http://softing.com/UANETToolkit/DemoServer
Build Date:	01/02/2018 15:11:47
Product Version:	1.44
Connection State:	Running
Status Code:	Good
Connection Name:	Softing DemoServer_test10
Session Id:	ns=11;i=1529198481

ServerCompatibility:

Locale Ids:	en-US|de-DE|es-ES|fr-FR
Min Supported Sample Rate:	0
Max Monitored Items:	0
Max Nodes Translate:	0
Max Nodes Method:	0
Max Nodes Browse:	0
Max Nodes Write:	0
Max Nodes Read:	0
Max Browse CP:	10

Figure: OPC UA Client, Test Client Connection

Column name	Information details
Start Time	The time external server was started at. Read from *StartTime* component of the *ServerStatus* object variable of the external server address space (i=2256). The value is displayed in the local time zone of the browser.
Current Time	The current time external server provides. Read from *CurrentTime* component of the *ServerStatus* object variable of the external server address space (i=2256). The value is displayed in the local time zone of the browser.
Manufacturer Name	The manufacturer name of the external server. Read from component *BuildInfo\ManufacturerName* of the *ServerStatus* object variable of the external server address space (i=2256).

Product Name	The product name of the external server. Read from component *BuildInfo\ProductName* of the *ServerStatus* object variable of the external server address space (i=2256).
Product Uri	The product URI of the external server. Read from component *BuildInfo\ManufacturerName* of the *ServerStatus* object variable of the external server address space (i=2256).
Build Date	The build date of the external server. Read from component *BuildInfo \BuildDate* of the *ServerStatus* object variable of the external server address space (i=2256).
Product Version	The software version of the external server. Read from component *BuildInfo\SoftwareVersion* of the *ServerStatus* object variable of the external server address space (i=2256).
Connection State	The current state of the external server. Read from component *State* of the *ServerStatus* object variable of the external server address space (i=2256).
Status Code	The OPC UA Status Code of the called services. If all services were called with success, the value will be *Good.* Otherwise, it will display the status code returned by the first erroneously service call.
Connection Name	The name of the test connection on the dataFEED Secure Integration Server side. It is the connection name defined by the user, post-fixed with a string to recognize it as a test connection.
Session Id	The session Id as assigned by the external server.
Locale Ids	The Locale Ids supported by the external server. Read from variable node *LocaleIdArray* of the external server address space (i=2271).
Min Supported Sample Rate	The minimum supported sample rate, as claimed by the external server. Read from variable node *MinSupportedSampleRate* of the external server address space (i=2272). A value of 0 means there is no limit set.
Max Monitored Items	The maximum number of monitored items accepted on service calls belonging to *Monitored Items Service Set*. Read from variable node *MinSupportedSampleRate* of the external server address space (i=11714). A value of 0 means there is no limit set.
Max Nodes Translate	The maximum number of nodes accepted on *Translate Browse Paths To Node Ids* service calls. Read from variable node *MaxNodesPerTranslateBrowsePathsToNodeIds* of the external server address space (i=11712). A value of 0 means there is no limit set.
Max Nodes Method	The maximum number of nodes accepted on *Method Call* service. Read from variable node *MaxNodesPerMethodCall* of the external server address space (i=11709). A value of 0 means there is no limit set.

Max Nodes Browse	The maximum number of nodes accepted on *Browse/Browse Next* service calls. Read from variable node *MaxNodesPerBrowse* of the external server address space (i=11710). A value of 0 means there is no limit set.
Max Nodes Write	The maximum number of nodes accepted on *Write* service calls. Read from variable node *MaxNodesPerWrite* of the external server address space (i=11707). A value of 0 means there is no limit set.
Max Nodes Read	The maximum number of nodes accepted on *Read* service calls. Read from variable node *MaxNodesPerRead* of the external server address space (i=11705). A value of 0 means there is no limit set.
Max Browse CP	The maximum number of *Browse Continuation Points* the external server is able to handle at a time. Read from variable node *MaxBrowseContinuationPoints* of the external server address space (i=2735). A value of 0 means there is no limit set.

Figure: OPC UA Client, Test Client Connection Fields

4.7.3 OPC UA Server

4.7.3.1 OPC UA Server Module

The OPC UA server module allows the dataFEED Secure Integration Server to create OPC UA server endpoints used by external OPC UA clients to access the external OPC UA server aggregated data.

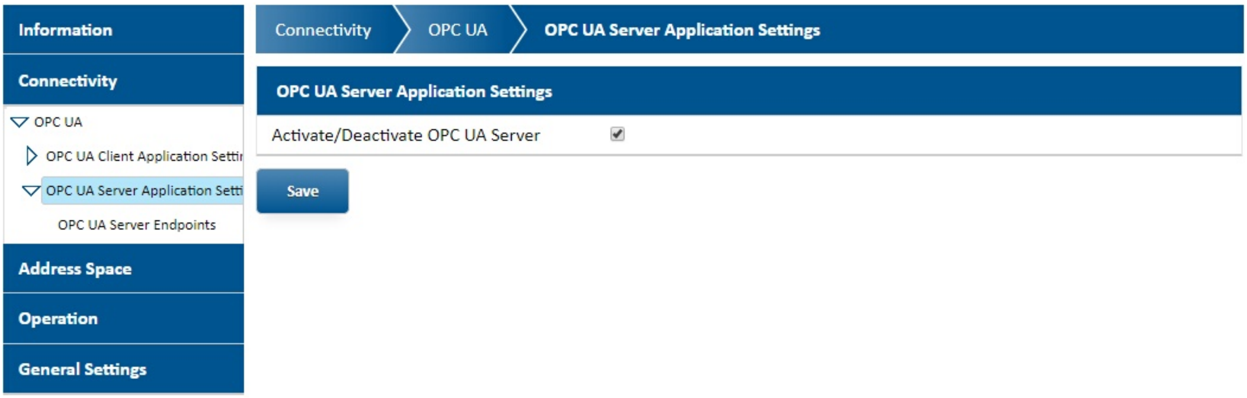
Key features of the OPC UA server module:

- **transport protocols supported: opc.tcp and https**
- **configuration of the OPC UA services**
- **per endpoint IP access filtering provides a simple solution to restrict OPC clients access**
- **advanced access protection**

Enabling/Disabling OPC UA Server Module

To enable or disable the OPC UA client module navigate to **Connectivity -> OPC UA -> OPC UA Server Application Settings** and change the state of the module by checking/unchecking the **[Activate/ Deactivate OPC UA Server]** checkbox. The checkbox state reflects the module state:

- **checked** ☑ : OPC UA server module enabled
- **unchecked** □ : OPC UA server module disabled



OPC UA Server Application Settings

Activate/Deactivate OPC UA Server ☑

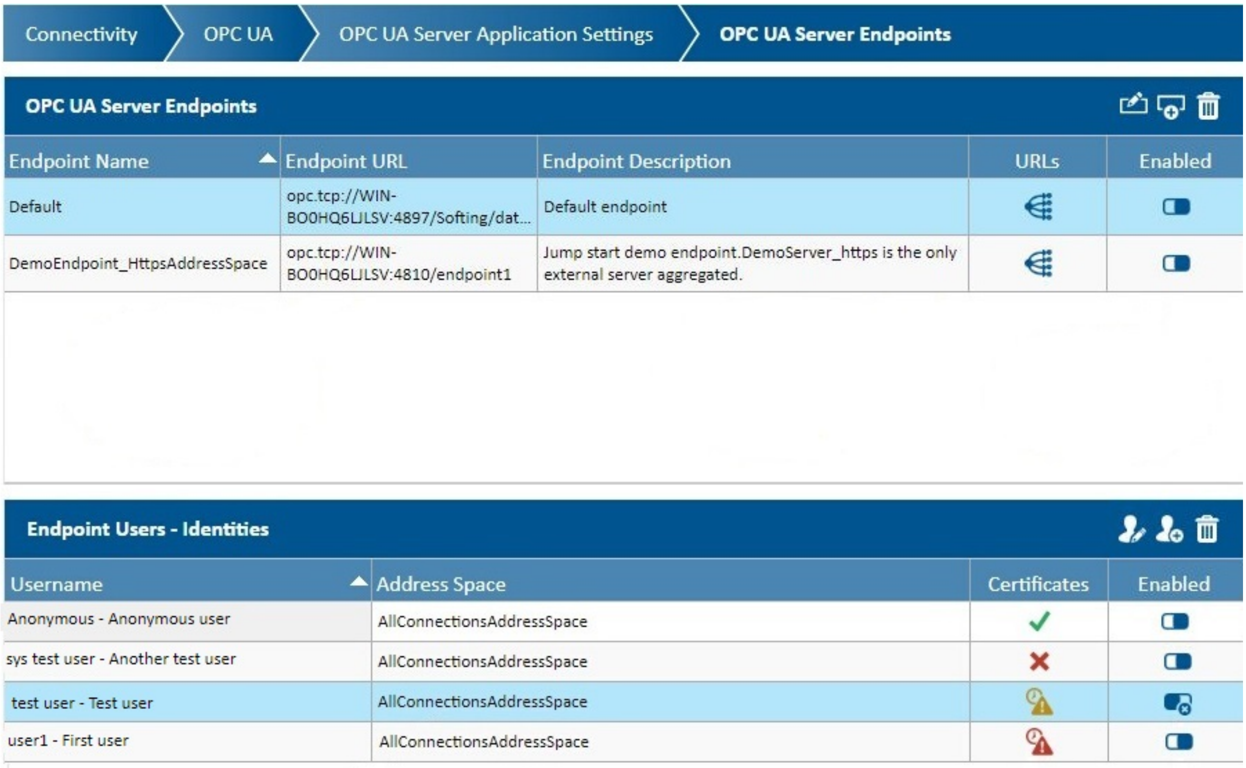
Figure: OPC UA Server, OPC UA Server Application Settings

4.7.3.2 Server Endpoints

Information about all configured server endpoints is centralized and accessible by navigating to **Connectivity -> OPC UA -> OPC UA Server Application Settings -> OPC UA Server Endpoints**.

Configured endpoints:

- **are bound to all network interfaces available on the computer**
- **support both internet protocol v4 and v6**



OPC UA Server Endpoints

Endpoint Name	Endpoint URL	Endpoint Description	URLs	Enabled
Default	opc.tcp://WIN-BO0HQ6LJLSV:4897/Softing/dat...	Default endpoint		
DemoEndpoint_HttpsAddressSpace	opc.tcp://WIN-BO0HQ6LJLSV:4810/endpoint1	Jump start demo endpoint.DemoServer_https is the only external server aggregated.		

Endpoint Users - Identities

Username	Address Space	Certificates	Enabled
Anonymous - Anonymous user	AllConnectionsAddressSpace	✓	
sys test user - Another test user	AllConnectionsAddressSpace	✗	
test user - Test user	AllConnectionsAddressSpace	⚠	
user1 - First user	AllConnectionsAddressSpace	⚠	

Figure: OPC UA Server, Server Endpoints Overview

Selecting an OPC UA Server Endpoint and clicking the menu symbol (Edit Endpoint) opens a window for editing this OPC UA Server Endpoint.

Clicking the menu symbol (Add Endpoint) adds a new OPC UA Server Endpoint.

Selecting an OPC UA Server Endpoint and clicking the menu symbol (Delete Endpoint) deletes this OPC UA Server Endpoint.

Doubleclicking an OPC UA Server Endpoint opens a window for editing this OPC UA Server Endpoint.

Clicking the symbol (Available Endpoint URLs) in the line of a specific OPC UA Server Endpoint shows a list of all URLs, which can be reached via this OPC UA Server Endpoint.

Clicking the symbol (Enabled, click to disable) resp. (Disabled, click to enable) in the line of a specific OPC UA Server Endpoint switches the activation state of this OPC UA Server Endpoint.

Selecting an identity of an OPC UA Server Endpoint user and clicking the menu symbol (Edit Endpoint User) opens a window for editing this OPC UA Server Endpoint user.

Clicking the menu symbol (Add Endpoint User) adds a new OPC UA Server Endpoint user.

Selecting an identity of an OPC UA Server Endpoint user and clicking the menu symbol (Delete Endpoint User) deletes this OPC UA Server Endpoint user.

Doubleclicking the identity of an OPC UA Server Endpoint user opens a window for editing this OPC UA Server Endpoint user.

The column Ceriticates of the table of the identitiesy of an OPC UA Server Endpoint user displays the current certiticate status of this OPC UA Server Endpoint user.

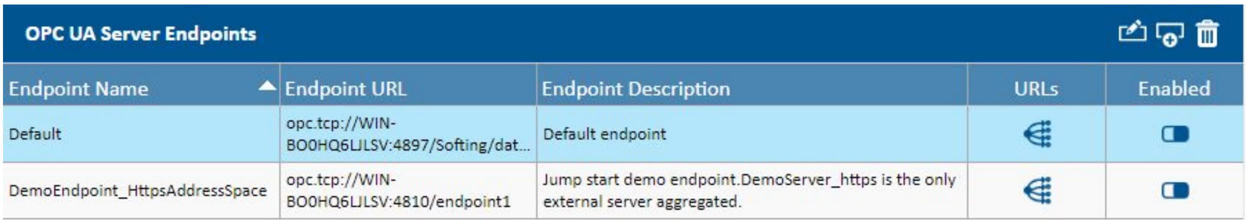
Clicking the symbol (Enabled, click to disable) resp. (Disabled, click to enable) in the line of the identity of an OPC UA Server Endpoint user switches the activation state of this OPC UA Server Endpoint user.

The page consist of two areas:

1. **OPC UA Server Endpoints**

In the **OPC UA Server Endpoints** table, all configured OPC UA server endpoints are displayed, each row representing a connection. The information in the table is sortable by clicking the table header. The sample shows two configured server endpoints.

The dataFEED Secure Integration Server configuration is delivered with a default sample endpoint named "Default" accessible by opc.tcp on port 4897 and assigned user "Anonymous".



OPC UA Server Endpoints

Endpoint Name	Endpoint URL	Endpoint Description	URLs	Enabled
Default	opc.tcp://WIN-BO0HQ6LJLSV:4897/Softing/dat...	Default endpoint		
DemoEndpoint_HttpsAddressSpace	opc.tcp://WIN-BO0HQ6LJLSV:4810/endpoint1	Jump start demo endpoint.DemoServer_https is the only external server aggregated.		

Figure: OPC UA Server, Server Endpoints

The table header information is described in the following table:

Column name	Information details
Endpoint Name	User defined endpoint name.
Endpoint URL	The endpoint URL as resulted based on : • user defined transport protocol (opc.tcp or https) • the fully qualified domain name of the computer running the dataFEED Secure Integration Server • user defined port • user defined url-path
Endpoint Description	User defined endpoint description text. It can be used to include additional information or remarks about the endpoint.
Enabled	Describes the configuration state of the OPC UA server endpoint. **Disabled**, **Enabled**, **Enabled**, **Access Protection temporarily or permanently disabled**, **Access protection IPs or certificates prevented authentication** Please see the table below (**OPC UA Server Endpoint Enabled State**) for details on the endpoint enabled column.
URLs	Provides a list with all possible URLs which can be used to access the configured endpoint (includes URLs created with computer name, FQDN and IPV4 and IPv6 address) **Beware, based on the network architecture and existing constraints not all endpoint URLs might work as expected.** By clicking on URLs row entry image ( ) a window listing all possible valid URLs directing to the configured endpoint will show:

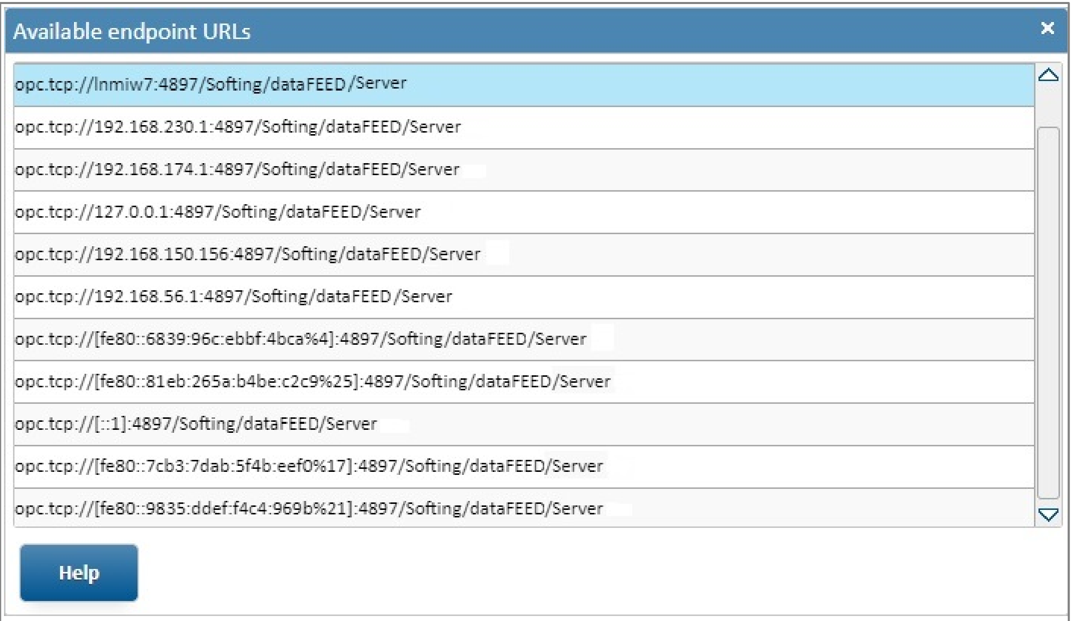
	 Available endpoint URLs opc.tcp://lnmiw7:4897/Softing/dataFEED/Server opc.tcp://192.168.230.1:4897/Softing/dataFEED/Server opc.tcp://192.168.174.1:4897/Softing/dataFEED/Server opc.tcp://127.0.0.1:4897/Softing/dataFEED/Server opc.tcp://192.168.150.156:4897/Softing/dataFEED/Server opc.tcp://192.168.56.1:4897/Softing/dataFEED/Server opc.tcp://[fe80::6839:96c:ebbf:4bca%4]:4897/Softing/dataFEED/Server opc.tcp://[fe80::81eb:265a:b4be:c2c9%25]:4897/Softing/dataFEED/Server opc.tcp://[::1]:4897/Softing/dataFEED/Server opc.tcp://[fe80::7cb3:7dab:5f4b:eef0%17]:4897/Softing/dataFEED/Server opc.tcp://[fe80::9835:ddef:f4c4:969b%21]:4897/Softing/dataFEED/Server Help

Table: OPC UA Server, Server Endpoints Overview

Endpoint State	Icon	Details
Disabled	◧⊗	The endpoint is **configured as disabled** therefore it is inaccessible by any OPC UA client. Clicking on the current configuration state icon would trigger a state toggle: • **Disabled** ◧⊗ -> **Enabled** ◧
Enabled	◧	The endpoint is **configured as enabled,** it is accessible and shall be able to accept incoming connection requests if other environmental conditions are met (e.g.: license slots are available). Clicking on the current configuration state icon would trigger a state toggle: • **Enabled** ◧ **-> Disabled** ◧⊗
Access Protection temporarily or permanently disabled	◧⚠	The endpoint is **configured as enabled**, but it was **disabled by the access protection** feature because the configured access protection restrictions where met. Checking the access protection applied settings it can be found if the endpoint is temporarily or permanently disabled. Clicking on the current configuration state icon would trigger a state toggle resetting the current access protection state and re-enabling the endpoint • **Access Protection temporarily or permanently disabled** ◧⚠ **-> Enabled** ◧

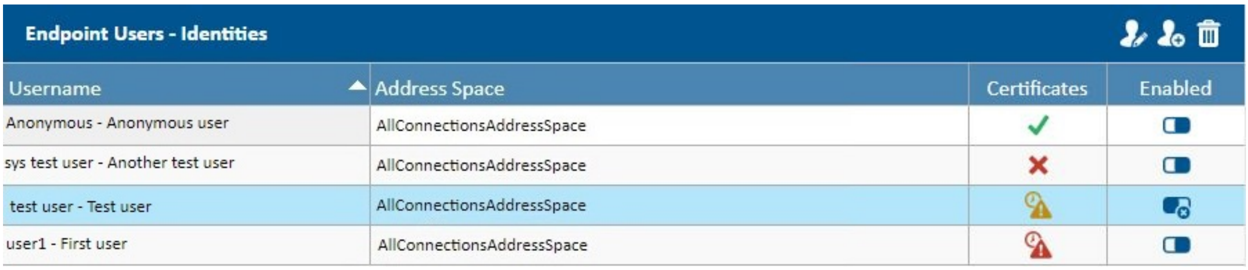
Access protection IPs or certificates prevented authentication	⚠	The endpoint is **configured as enabled**, it is accessible and shall be able to accept incoming connection requests, but it rejects some connections attempts based on IPs or certificates as resulted from the access protection configuration. This state can be manually reset by accessing the access protection settings 202 and disabling/enabling the authentication restrictions for remote IPs and certificates. Clicking on the current configuration state icon would trigger a state toggle, but it **shall not reset** the access protection state. • **Access protection IPs or certificates prevented authentication** ⚠ **-> Disabled** ⊗

Table: OPC UA Server Endpoint Enabled State

See Server Endpoints Creation 188 chapter and sub-chapters for more details on the actions.

2. **Endpoint Users - Identities**

In the **Endpoint Users - Identities** table, details about the users assigned to the currently selected endpoint are provided. Sample below shows the users assigned to the "Default" server endpoint.



Endpoint Users - Identities

Username	Address Space	Certificates	Enabled
Anonymous - Anonymous user	AllConnectionsAddressSpace	✓	●
sys test user - Another test user	AllConnectionsAddressSpace	✗	●
test user - Test user	AllConnectionsAddressSpace	⚠	⊗
user1 - First user	AllConnectionsAddressSpace	⚠	●

Figure: OPC UA Server, Endpoint Users Identities

The table header information is described in the following table:

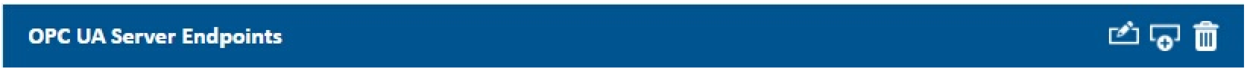
Column name	Information details
Username	Name and description of the user
Address Space	Address space exposed to the OPC UA client connection to the selected endpoint and authenticated with the current
Certificate	Highlights the validity status of the certificates attached to the user or the absence of any certificate Possible values are: • Certificates were found and all are fine: ✓

	• At least one certificate will expire soon: ⚠ • At least one certificate is already expired: ⚠ • No certificates are attached to the current user: ✖
Enabled	Describes the configuration state of the assignment of the current user to the selected OPC UA server endpoint. Possible values are **Enabled** or **Disabled** . Note: Clicking on the current configuration state icon would trigger a state toggle: • **Enabled -> Disabled** • **Disabled -> Enabled**

Table: OPC UA Server, Endpoint Users Identities

See Users Assignment 211 chapter and sub-chapters for more details on the actions.

4.7.3.3 Server Endpoints Creation


OPC UA Server Endpoints

Information bar

Figure: OPC UA Server, OPC UA Server Endpoints Menu Bar

The **OPC UA Server Endpoints** information bar provides three buttons with the following functionality:

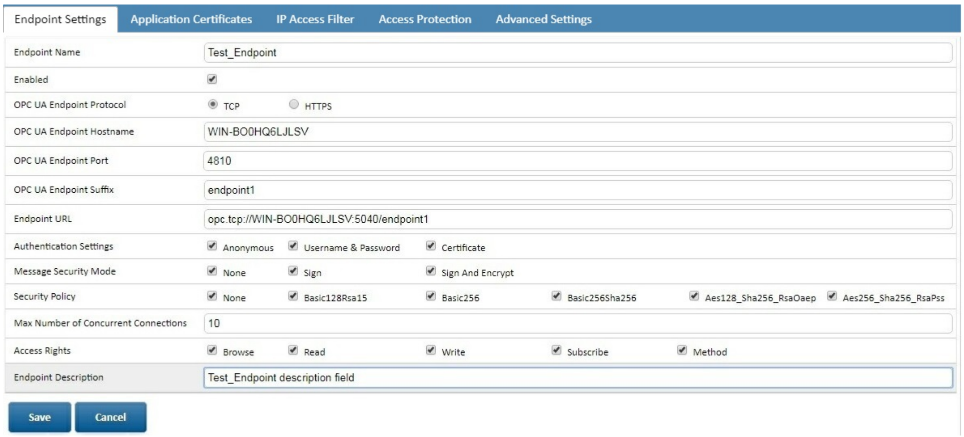
Button	Action
✎	Edit existing OPC UA server endpoint.
⊕	Add new OPC UA server endpoint.
🗑	Delete existing OPC UA server endpoint.

Figure: OPC UA Server, OPC UA Server Endpoints Menu Bar Buttons

To create a new OPC UA server endpoint navigate to **Connectivity -> OPC UA -> OPC UA Server Application Settings -> OPC UA Server Endpoints** and click the **[Add new endpoint]** ⊕ button on the information bar. The OPC UA endpoint configuration page shows up and has three different configuration tabs: **Connection settings, Certificates** and **Advanced Settings.**

4.7.3.3.1 Endpoint Settings

Endpoint Settings is the main view in the OPC UA server endpoint configuration page and provides a simple and intuitive interface for configuring a new or editing an existing OPC UA server endpoint.



Endpoint Name	Test_Endpoint
Enabled	☑
OPC UA Endpoint Protocol	● TCP ○ HTTPS
OPC UA Endpoint Hostname	WIN-BO0HQ6LJLSV
OPC UA Endpoint Port	4810
OPC UA Endpoint Suffix	endpoint1
Endpoint URL	opc.tcp://WIN-BO0HQ6LJLSV:5040/endpoint1
Authentication Settings	☑ Anonymous ☑ Username & Password ☑ Certificate
Message Security Mode	☑ None ☑ Sign ☑ Sign And Encrypt
Security Policy	☑ None ☑ Basic128Rsa15 ☑ Basic256 ☑ Basic256Sha256 ☑ Aes128_Sha256_RsaOaep ☑ Aes256_Sha256_RsaPss
Max Number of Concurrent Connections	10
Access Rights	☑ Browse ☑ Read ☑ Write ☑ Subscribe ☑ Method
Endpoint Description	Test_Endpoint description field

Figure: OPC UA Server, Server Endpoints Creation, Endpoint Settings

Bottom page buttons actions:

Button	Action
Save	Once the configuration is finalized, clicking the **[Save]** button shall apply the newly configured/modified OPC UA server endpoint. Server endpoint changes are applied immediately at runtime.
Cancel	Cancel the current server endpoint configuration session. **Beware all changes shall be lost !**

Table: OPC UA Server, Server Endpoints Creation, Endpoint Settings Buttons

Configuration parameters are described in the following table:

Parameter name	Default value	Value description
Endpoint Name	**empty**	Defines the connection name as it will show up in the OPC UA client connection overview page. This name shall also be used by the OPC Client when connecting to an external OPC UA server ***NOTE**: Characters not supported in this field**: # ^ < > / $**
Enabled	**Enabled**	Instructs the dataFEED Secure Integration Server to either enable (checked) or disable (unchecked) the currently configured OPC UA server endpoint.
OPC UA Endpoint Protocol	**TCP**	The server endpoint transport protocol is configurable by selecting the appropriate radio button.

OPC UA Endpoint Hostname	**Hostname**	Pre-populated, uneditable field, defining the computer's hostname.
OPC UA Endpoint Port	**4810+**	Defines the server port number. Populated with an available port, not assigned to an existing endpoint, starting with **port 4180.** ***NOTE**: Ports under 1024 are not allowed. Field is automatically validated.
OPC UA Endpoint Path	**endpoint 1**	User editable server endpoint URL path. Pre-populated with a string in the form **endpoint[index]** where index might change if the path already exists.
Endpoint URL	**opc.tcp://[hostname]:[port]/[path]**	Configured server endpoint URL based on the selected **transport protocol**, **port number**, **URL path** and the existing **hostname.**
Authentication Settings	**All**	Defines the authentication method supported by the endpoint. Supported settings: **Anonymous, Username & Password** and **Certificate**
Message Security Mode	**All**	Defines the endpoint message security mode (whether signing or encryption is used when exchanging messages). ***NOTE**: Supported message security mode: None, Sign, SignAndEncrypt
Security Policy	**All**	Defines the endpoint security policy (the encryption algorithm applied to the messages). ***NOTE**: Supported security policies: None, Basic256, Basic256Sha256, Basic128Rsa15**,** Aes128_Sha256_RsaOaep and Aes256_Sha256_RsaPss
Max Number of Concurrent Connections	**10**	Specifies the endpoint's maximum supported number of concurrent connection from external OPC UA clients.
Access Rights	**All**	Configures the endpoint's supported services. Enable the service by checking the appropriate service checkbox. ***NOTE**: Supported service: Browse, Read, Write, Subscribe, Method
Endpoint Description	**empty**	User defined endpoint description text. Can be used to include additional information or remarks about the endpoint.

Table: OPC UA Server, Server Endpoints Creation, Endpoint Settings Parameters

Notes on parameters change operations:

A restart of the endpoint – leading to closing all the associated sessions from clients – is triggered if any of the following parameters is changed :

- **Endpoint URL**
- **Enabled**
- **Authentication Settings**
- **Message Security Mode**
- **Security Policy**
- **the own application certificate**

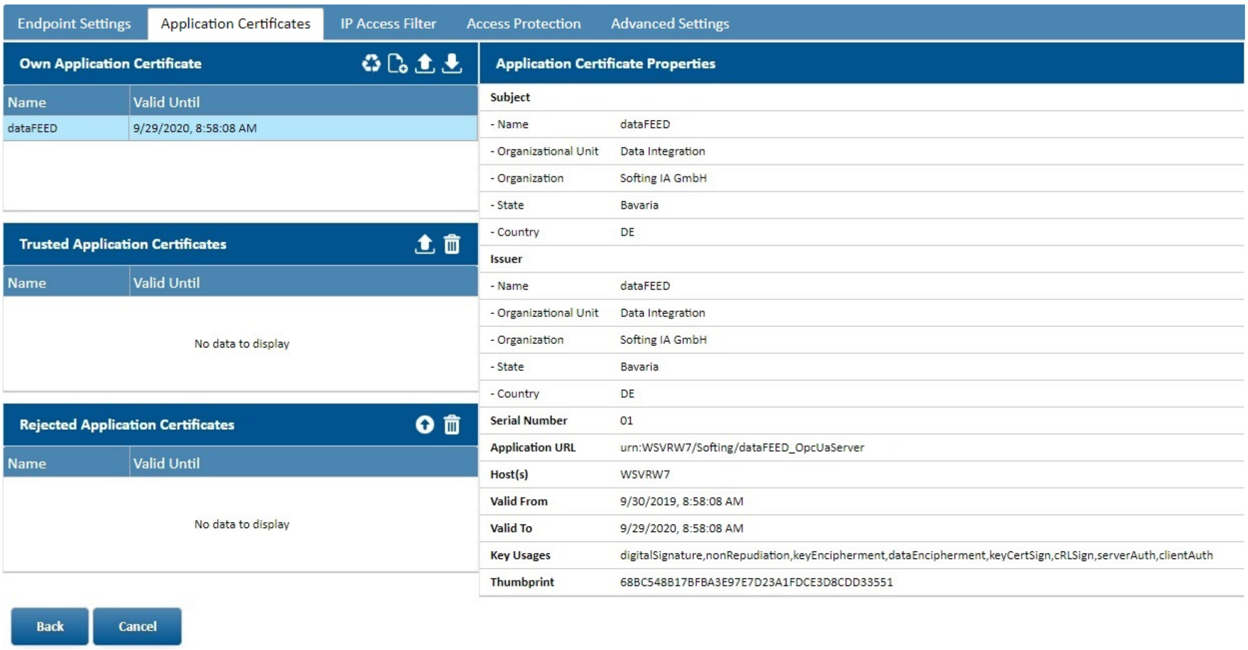
Changing access rights has immediate effect upon existing sessions – subsequent UA request will be allowed or denied according to the new rules, and existing subscriptions will stop or resume receiving notifications.

Changing the maximum number of concurrent connections or changing the trusted certificates will have effect only on future sessions – existing sessions will continue to work even if they would be denied with the new parameters.

4.7.3.3.2 Application Certificates

- **Managing the SSL application instance certificates is necessary if the security mode is Sign or SignAndEncrypt or for https OPC UA server endpoints.**
- **dataFEED Secure Integration Server uses separate PKI stores for each OPC UA server endpoint, therefore SSL certificates have to be managed for each connection independently.**
- **All certificates generated by the dataFEED Secure Integration Server are self signed**

The certificates page provides an interface for managing the SSL certificates stored in the endpoint's PKI store.



Own Application Certificate

Name	Valid Until
dataFEED	9/29/2020, 8:58:08 AM

Trusted Application Certificates

Name	Valid Until

No data to display

Rejected Application Certificates

Name	Valid Until

No data to display

Application Certificate Properties

Subject	
- Name	dataFEED
- Organizational Unit	Data Integration
- Organization	Softing IA GmbH
- State	Bavaria
- Country	DE
Issuer	
- Name	dataFEED
- Organizational Unit	Data Integration
- Organization	Softing IA GmbH
- State	Bavaria
- Country	DE
Serial Number	01
Application URL	urn:WSVRW7/Softing/dataFEED_OpcUaServer
Host(s)	WSVRW7
Valid From	9/30/2019, 8:58:08 AM
Valid To	9/29/2020, 8:58:08 AM
Key Usages	digitalSignature,nonRepudiation,keyEncipherment,dataEncipherment,keyCertSign,cRLSign,serverAuth,clientAuth
Thumbprint	68BC548B17BFBA3E97E7D23A1FDCE3D8CDD33551

Figure: OPC UA Server, Server Endpoints Creation, Application Certificates

Bottom page buttons actions:

Button	Action
Back	Navigate to the endpoint settings 189 page
Cancel	Cancel the current endpoint configuration session. **Beware all changes shall be lost !**

Figure: OPC UA Server, Server Endpoints Creation, Application Certificates Buttons

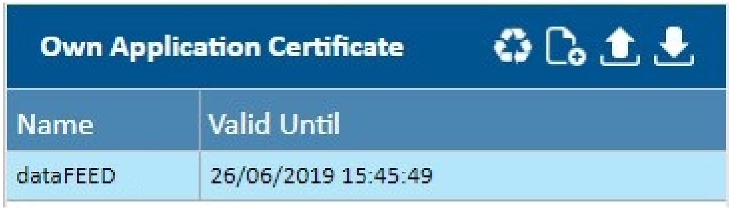
There are four highlighted sections on the certificates page:

Area	Colour	Details
Own application certificates	Blue	Lists the certificate used to identify the dataFEED Secure Integration Server endpoint application instance. This certificate is uniquely created for each OPC UA server endpoint.
Trusted application certificates	Green	Contains certificates identifying other OPC UA application instances which are being trusted by the current OPC UA server endpoint instance. When secured connections are created OPC UA connections can be established only when both involved parties trust each others application certificates.
Rejected application certificates	Red	Contains all certificates which were rejected during the connection establishment phase. No OPC UA connections can be established to the corresponding OPC UA application instance unless the certificates are moved into the trusted application certificates folder.
Application certificates properties	Yellow	Information about the selected certificate on any of the three application certificates folders (Own, Trusted, Rejected) is visible in the application certificates properties area.

Table: OPC UA Server, Server Endpoints Creation, Application Certificates Sections

1. Own Application Certificate

Only one certificate should be visible in the own certificate area. This is the certificate which is used by the running OPC UA server endpoint to identify itself.



Own Application Certificate

Name	Valid Until
dataFEED	26/06/2019 15:45:49

Figure: OPC UA Server, Server Endpoints Creation, Own Application Certificate

Several operations are accessible using the buttons placed top right:

Button	Action
♻	Reuse application certificate
🗋	Generate application certificate
⬆	Upload application certificate
⬇	Download application certificate

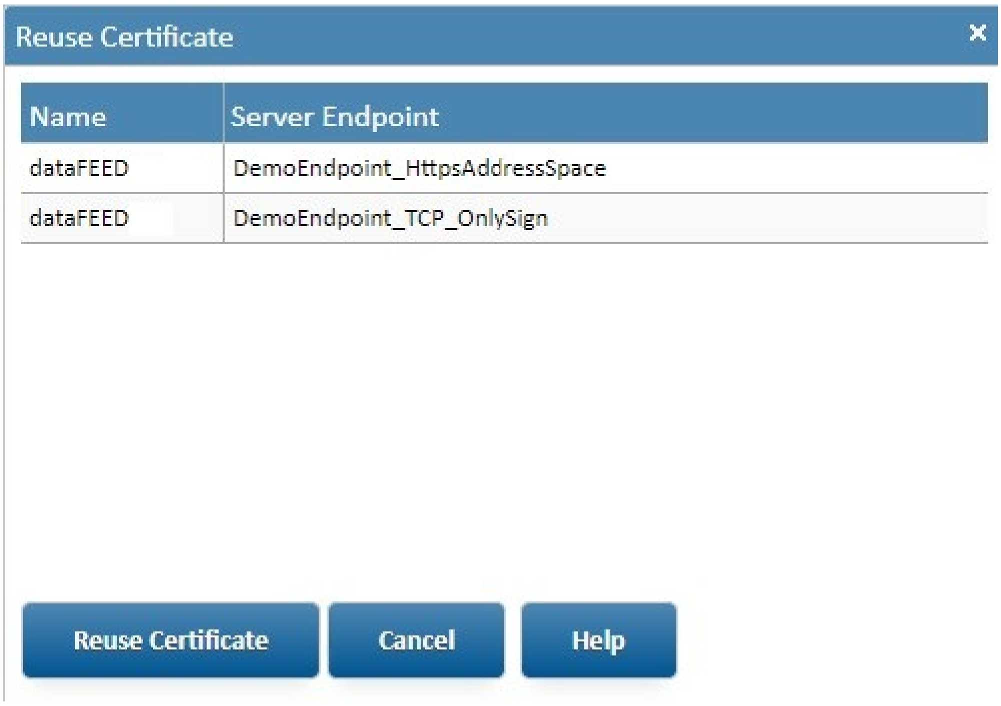
Table: OPC UA Server, Server Endpoints Creation, Own Application Certificate Buttons

Any changes resulting in the replacement of the current own certificate by any of the following actions :reuse, generate or upload will lead the server endpoint restart.

a. Reuse application certificate

Provides the possibility to reuse a certificate which is already in use to identify a different configured OPC UA server endpoint. Clicking the **[Reuse certificate]** button brings up a window which lists the available server endpoints.

To reuse the certificate of an existing endpoint, select the endpoint in the list and click the **[Reuse Certificate]** Reuse Certificate labeled button.



Reuse Certificate

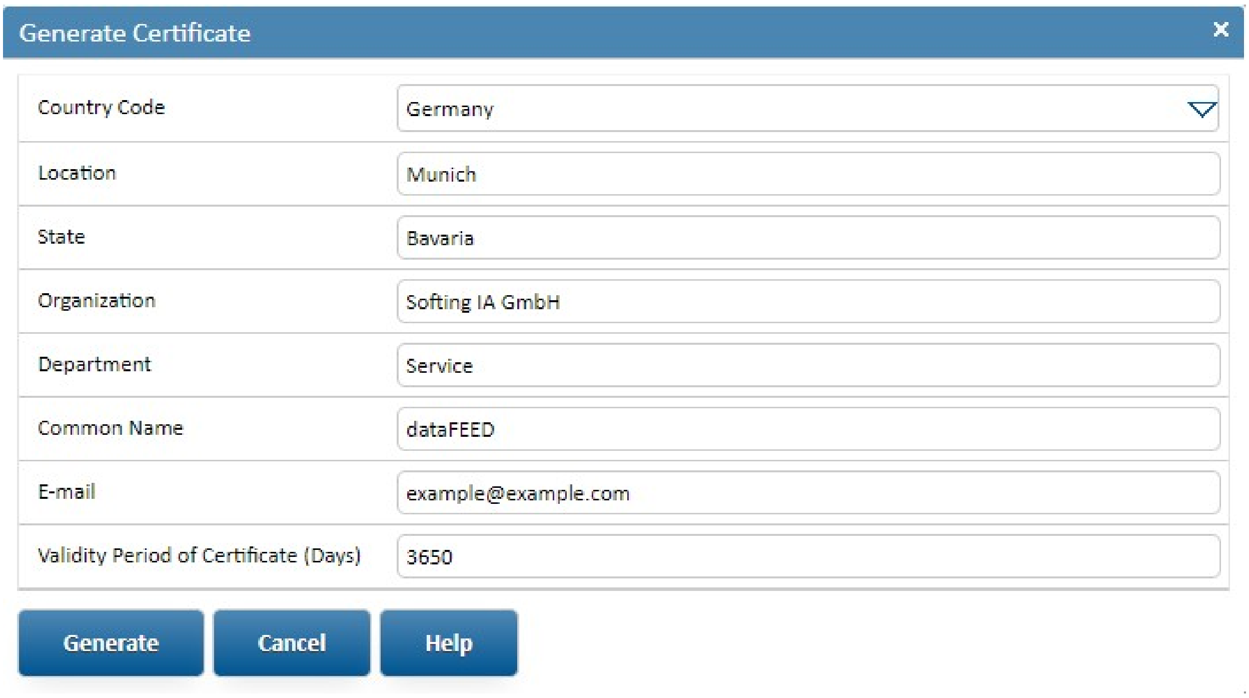
Name	Server Endpoint
dataFEED	DemoEndpoint_HttpsAddressSpace
dataFEED	DemoEndpoint_TCP_OnlySign

Reuse certificate window

Figure: OPC UA Server, Server Endpoints Creation, Reuse Application Certificate

b. Generate application certificate

To generate a new application certificate, click on the **Generate certificate** button and the following window will pop up:



Generate Certificate

Country Code	Germany
Location	Munich
State	Bavaria
Organization	Softing IA GmbH
Department	Service
Common Name	dataFEED
E-mail	example@example.com
Validity Period of Certificate (Days)	3650

Figure: User & Identities, Generate Certificate

The fields are populated with some proposed values, according to the corresponding values defined in the Application Settings 28 page.

By hovering over the input text fields, a Tool-tip will appear to inform about the mandatory state of the field with regards to the generation of the Certificate.

Certificate generation fields description:

Parameter name	Mandatory	X509 field name	Details
Country Code	**NO**	**C**	Country Name as ISO3166 two character country code
Location	**YES**	**L**	Locality name, generally city
State	**YES**	**ST**	State or Province Name
Organization	**YES**	**O**	Organization Name
Department	**YES**	**OU**	Organizational Unit Name
Common Name	**YES**	**CN**	Common Name
Email	**NO**		Email Address
Validity Period	**YES**		Validity period starting at the time of generation

Table: Application Certificate, Certificate Generation Fields

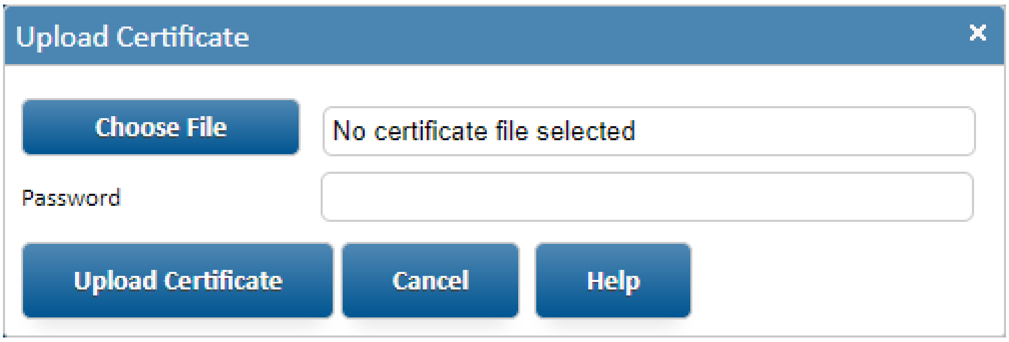
Press the Generate button to generate and add the certificate own application certificate list:

⚠ **After regeneration, the existing applications trust relationships will be voided**

c. Upload application certificate

Provides a simple way to replace the currently used application certificate with an already existing certificate. The upload certificate windows opens by clicking the **[Upload certificate]** button. In this view the new certificate file shall be selected by pressing the **[Choose File]** button.

If the certificate requires a password, the corresponding password input field is to be used, otherwise the field should be left empty.



No certificate file selected

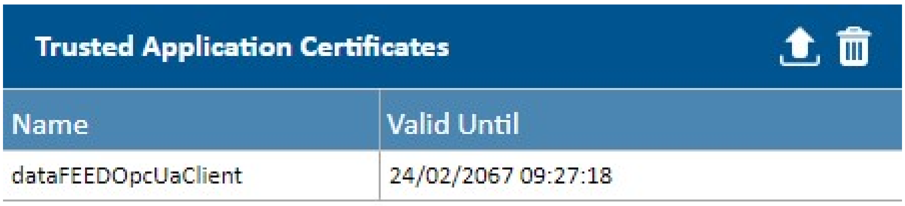
Figure: OPC UA Server, Server Endpoints Creation, Upload Certificate

d. Download application certificate

Provides a way to download the current own certificate. The download will start automatically and the filename format is **SoftingOpcUaEndpoint[*thumbprint*].der** where ***thumbprint*** is the actual thumbprint of the downloaded certificate.

2. Trusted Application Certificates

Allows manipulation and information retrieval on the current server endpoint's trusted certificates. All remote OPC UA client application instances whose certificates are listed in this view have a trust relationship established with the current endpoint.



Name	Valid Until
dataFEEDOpcUaClient	24/02/2067 09:27:18

Figure: OPC UA Server, Server Endpoints Creation, Trusted Application Certificates

Several operations are accessible using the buttons placed top right:

Button	Action
⬆	Upload certificate
🗑	Delete certificate

Table: OPC UA Server, Server Endpoints Creation, Trusted Application Certificates Buttons

a. Upload certificate

Uploading a trusted certificate is required:

- When an external OPC UA client is expected to establish a secure connection to an existing server endpoint. In this case the external OPC UA client's certificate needs to be uploaded in the server endpoint trusted certificates section.

An alternative solution for the above scenario is to entrust an already rejected certificate 198.

Provides a way to add a pre-owned certificate, locally stored, to the trusted folder. After clicking the **[Upload Certificate]** button a new view, where the new certificate file shall be selected by pressing the **[Choose file]** button, opens. To finalize the action press the **[Upload Certificate]** button.

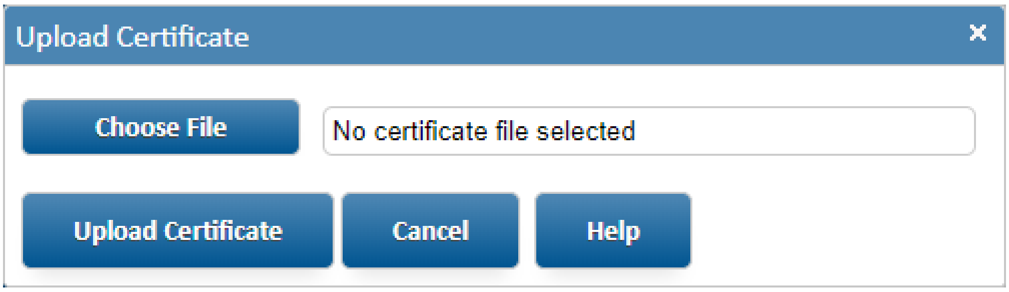


Figure: OPC UA Server, Server Endpoints Creation, Upload Certificate

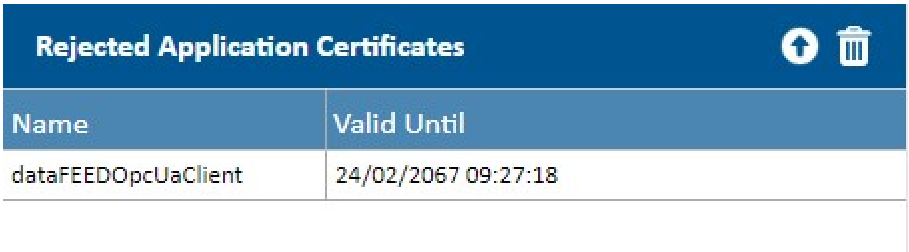
b. Delete certificate

Deletes the currently selected certificate from the trusted certificates folder. After deletion the trust relationship with the deleted certificate owner application will be invalidated.

3. Rejected Application Certificates

dataFEED Secure Integration Server does not automatically trust remote OPC UA application instance certificates therefore secured connection attempts may result in remote certificates automatically stored in the Rejected certificates folder.

All remote OPC UA application instance certificates whose connection establishment to the current OPC UA endpoint failed due to trust relationship condition should be listed under the rejected certificates view.


Rejected Application Certificates

Name	Valid Until
dataFEEDOpcUaClient	24/02/2067 09:27:18

Figure: OPC UA Server, Server Endpoints Creation, Rejected Application Certificates

Several operations are accessible using the buttons placed top right:

Button	Action
⬆	Move to Trusted
🗑	Delete certificate

Table: OPC UA Server, Server Endpoints Creation, Rejected Application Certificates Buttons

a. Move to Trusted

Provides the functionality needed to trust an alredy rejected OPC UA application instance by moving its rejected certificate into the trusted certificates folder. Clicking the **[Move to Trusted]** button will move the selected rejected certificate into the trusted certificates folder. The result of this action is visible in the configuration page and the previously rejected certificate shall now be visible only under the trusted certificates list.

This is an important manual step required:

- To enable external OPC UA clients to connect to a **secured OPC UA server endpoint** connection.

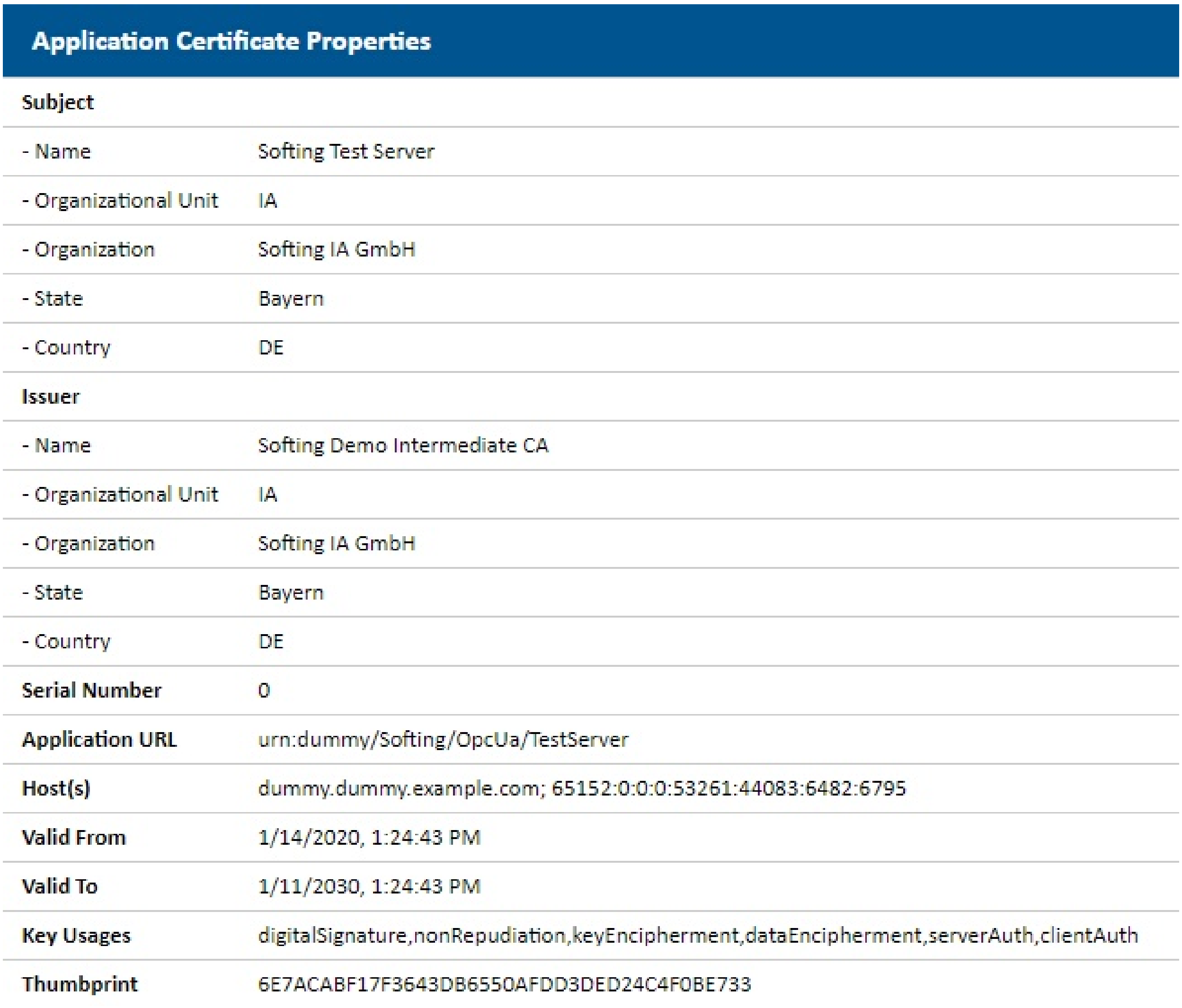
Any previously trust-related failed connection attempts, will subsequently succeed after moving the certificates to the trusted folder.

b. Delete Certificate

Deletes the currently selected certificate from the rejected certificates folder.

4. Application Certificates Properties

Information about the selected certificate is available in the certificates properties area.



Application Certificate Properties

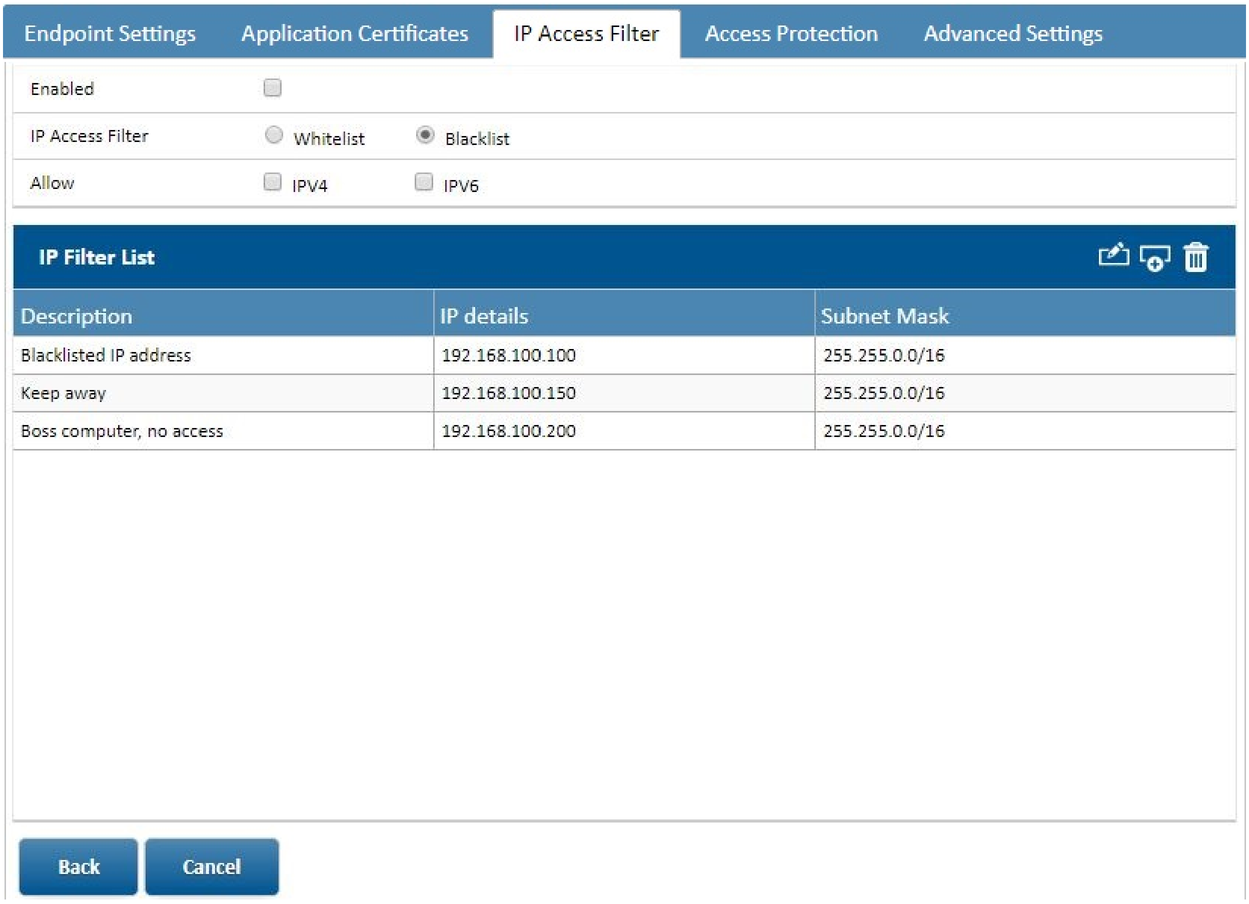
Subject	
- Name	Softing Test Server
- Organizational Unit	IA
- Organization	Softing IA GmbH
- State	Bayern
- Country	DE
Issuer	
- Name	Softing Demo Intermediate CA
- Organizational Unit	IA
- Organization	Softing IA GmbH
- State	Bayern
- Country	DE
Serial Number	0
Application URL	urn:dummy/Softing/OpcUa/TestServer
Host(s)	dummy.dummy.example.com; 65152:0:0:0:53261:44083:6482:6795
Valid From	1/14/2020, 1:24:43 PM
Valid To	1/11/2030, 1:24:43 PM
Key Usages	digitalSignature,nonRepudiation,keyEncipherment,dataEncipherment,serverAuth,clientAuth
Thumbprint	6E7ACABF17F3643DB6550AFDD3DED24C4F0BE733

Figure: OPC UA Server, Server Endpoints Creation, Application Certificates Properties

4.7.3.3.3 IP Access Filter

IP filtering is a simple and effective endpoint IP access filtering functionality, supporting both IPV4 and IPV6. Using whitelisting and blacklisting concepts provides an easy way to configure it.

The main page of an endpoint IP Access filter, enabled and configured to blacklist all IPV4 addresses in the Endpoint IP List (192.168.100.100, 192.168.100.150 and 192.168.100.200), is visible below:



Enabled ☐

IP Access Filter ○ Whitelist ● Blacklist

Allow ☐ IPV4 ☐ IPV6

IP Filter List

Description	IP details	Subnet Mask
Blacklisted IP address	192.168.100.100	255.255.0.0/16
Keep away	192.168.100.150	255.255.0.0/16
Boss computer, no access	192.168.100.200	255.255.0.0/16

Figure: OPC UA Server, Server Endpoints Creation, IP Access Filter

Bottom page buttons actions:

Button	Action
Back	Navigate to the endpoint settings page
Cancel	Cancel the current server endpoint configuration session. **Beware all changes shall be lost !**

Table: OPC UA Server, Server Endpoints Creation, IP Access Filter Buttons

1. General IP Filtering Configuration

The general IP Filtering configuration can be seen on the top half of the IP access filter page and is used to configure the IP access filter working mode. When enabled by checking the **[Enabled]** checkbox a mutually exclusive working mode can be selected based on the following table:

Mode	Icon	Details
Whitelist	● Whitelist	**Permission** based access list, allows only authorized IP addressed to access the server endpoint. Authorized IPs are user defined and shall be listed in the **Endpoint IP List**.
Blacklist	● Blacklist	**Restriction** based list, prevents all unauthorized IP addressed to access the server endpoint. Unauthorized IPs are user defined and shall be listed in the **Endpoint IP List**.

Table: OPC UA Server, Server Endpoints Creation, General IP Filtering Configuration

Selecting the supported IP version is done by checking the desired version in the **Allow** section. Both IP versions can be enabled at the same time :

Version	Icon	Details
IPV4	☑ IPV4	Selecting IPV4 shall apply the filtering on IP version 4 addresses.
IPV6	☑ IPV6	Selecting IPV6 shall apply the filtering on IP version 6 addresses.

Table: OPC UA Server, Server Endpoints Creation, IP Versions

2. IP Filter List

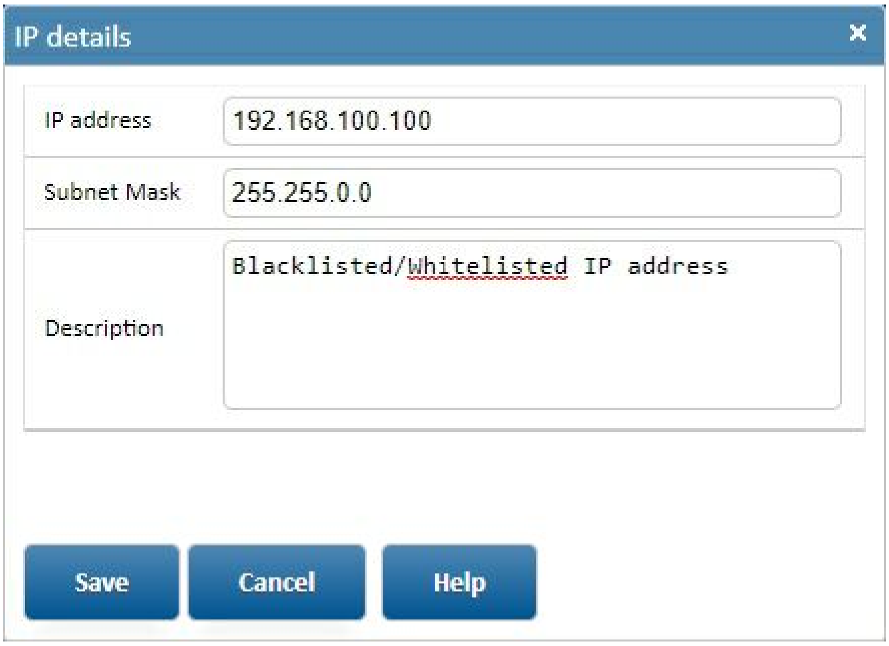
The endpoint IP List area is used to list all IP addresses entered in the current endpoint filtering functionality. Following actions are possible by using the three buttons on the Filter IP list information bar:

Button	Action
✎	Edit existing filter IP entry.
⊕	Add new IP to the filter.
🗑	Delete the currently selected IP from the filter.

Table: OPC UA Server, Server Endpoints Creation, IP Filter List Buttons

a. Add IP Filter

To add a new IP in the list click the **[Add IP Filter]** and a window will show up:



IP address: 192.168.100.100

Subnet Mask: 255.255.0.0

Description: Blacklisted/Whitelisted IP address

Figure: OPC UA Server, Server Endpoints Creation, Add IP Filter

Before finalizing by clicking the **[Save]** button, the following information shall be filled in:

Information	Action
IP address	Remote IP address which needs to be added into the filter.
Subnet mask	The IP address corresponding subnet mask.
Description	Description about the IP filter entry.

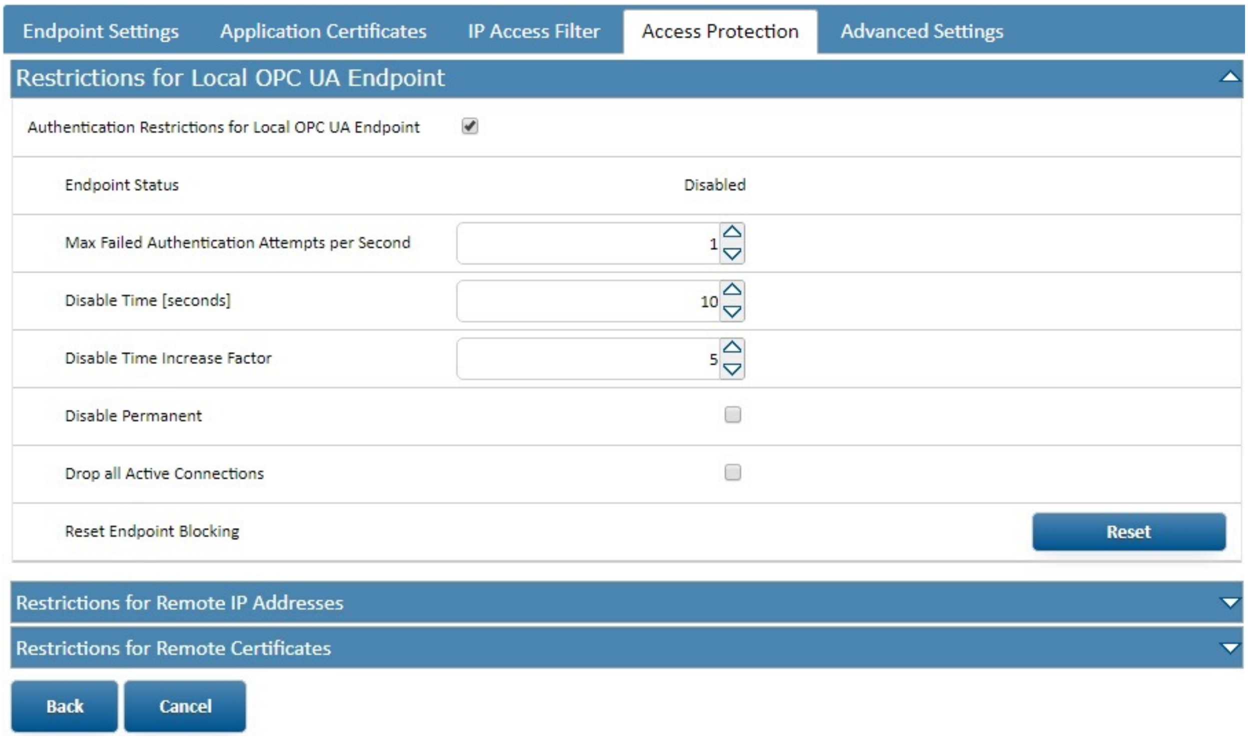
Table: OPC UA Server, Server Endpoints Creation, IP Filter Details

b. Edit Filter IP

To edit an existing IP entry select the appropriate entry in the IP filter list and click the **[Edit IP Filter].** A window similar to the one described for the add IP filter operation will show up. Upon changing the needed information to finalize the operation click the **[Save]** button.

4.7.3.3.4 Access Protection

Access protection provides enhanced control on connections or connection attempts to the endpoint.



Restrictions for Local OPC UA Endpoint

Authentication Restrictions for Local OPC UA Endpoint ☑

Endpoint Status	Disabled
Max Failed Authentication Attempts per Second	1
Disable Time [seconds]	10
Disable Time Increase Factor	5
Disable Permanent	□
Drop all Active Connections	□
Reset Endpoint Blocking	Reset

Restrictions for Remote IP Addresses

Restrictions for Remote Certificates

Figure: OPC UA Server, Server Endpoints Creation, Access Protection

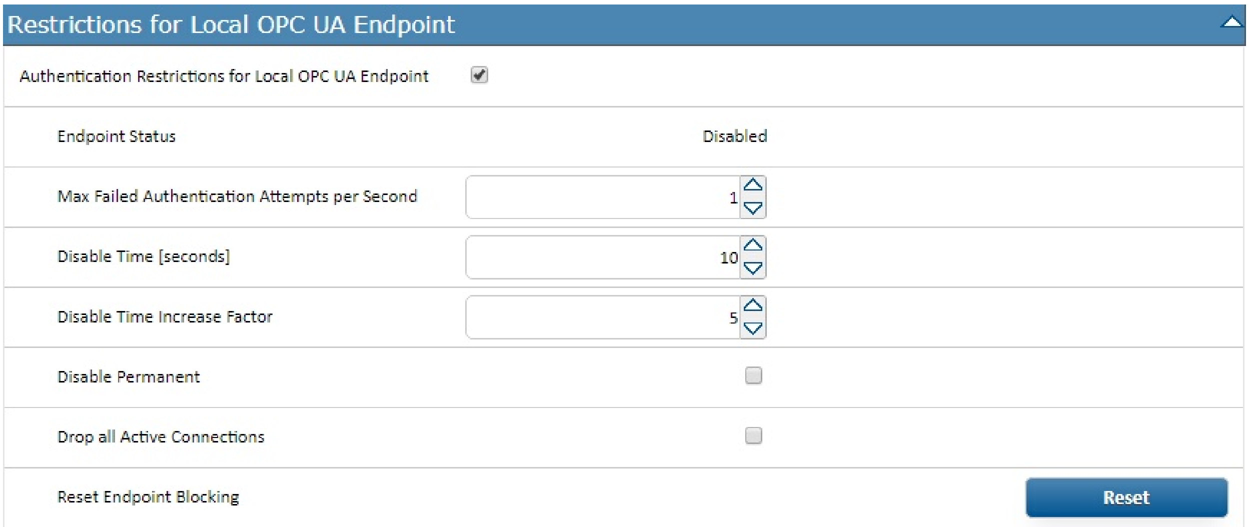
Bottom page buttons actions:

Button	Action
Back	Navigate to the endpoint settings page
Cancel	Cancel the current server endpoint configuration session. **Beware all changes shall be lost !**

Table: OPC UA Server, Server Endpoints Creation, Access Protection Buttons

Access protection restrictions are classified in three distinct and collapsible groups and they target OPC UA clients as a group or individually and are identified either by IP or certificate.

1. Authentication Restrictions for Local OPC UA Endpoint



Restrictions for Local OPC UA Endpoint

Authentication Restrictions for Local OPC UA Endpoint ☑

Endpoint Status	Disabled
Max Failed Authentication Attempts per Second	1
Disable Time [seconds]	10
Disable Time Increase Factor	5
Disable Permanent	☐
Drop all Active Connections	☐
Reset Endpoint Blocking	Reset

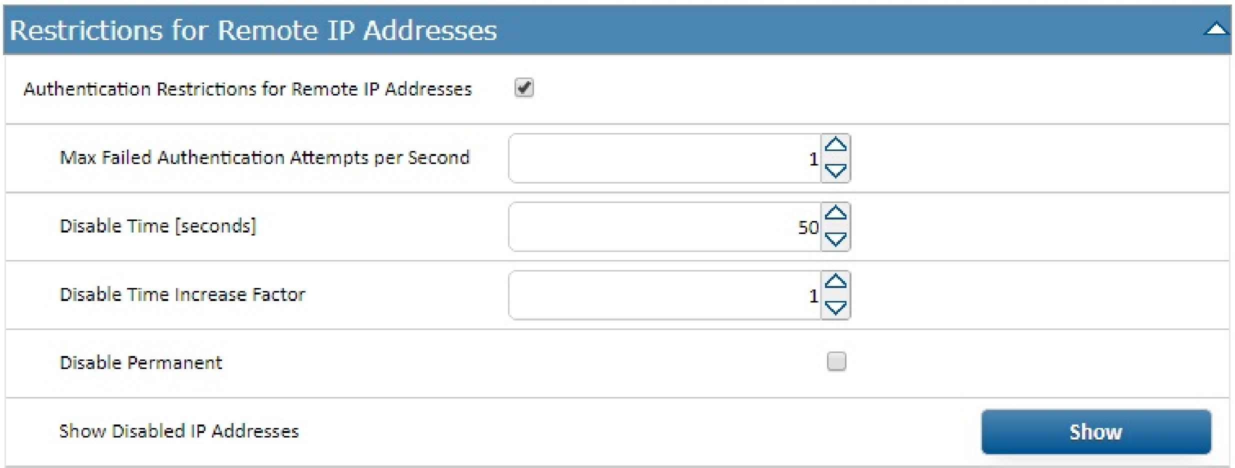
This restriction group **applies on the OPC UA clients** trying to establish a connection to the endpoint **as a group,** the clients are being identified based on their IP address. The restrictions can be seen as a possible consequence of the sum of the actions performed by several OPC UA clients.

Parameter name	Default Value	Unit	Details
Endpoint Status			Disabled, as a consequence of exceeding the maximum number of failed authentication attempts, or Enabled (that is, not Disabled).
Max Failed Authentication Attempts per Second	**10**	**units**	Total number of maximum failed authentications per second. Origin of the authentication attempt can be any OPC UA client.
Disable Time	**10**	**seconds**	Endpoint disable time if the maximum failed authentication attempts limit is reached. Applies on all OPC UA clients.
Disable Time Increase Factor	**5**	**factor**	Endpoint disable increase factor will be used to increase the **Disable Time** in case the maximum failed authentication attempts limit is reached several times consecutively without successful authentication in between. The disable time is increased (multiplied) with a factor of the value of this parameter. Eg: based on the default values the disable time related to the count of consecutive failed authentication attempts

<table>
<tr><td></td><td></td><td></td><td><table><tr><th>Consecutive failed authentications</th><th>Disable time (default values based)</th></tr><tr><td>10</td><td>10 seconds</td></tr><tr><td>20</td><td>50 seconds (5* 10 seconds)</td></tr><tr><td>30</td><td>250 second (5* 50 seconds)</td></tr></table></td></tr>
<tr><td><b>Disable Permanent</b></td><td></td><td></td><td>When selected the option will permanently disable the endpoint if the maximum failed authentication attempts limit is reached.
Manual re-enabling by klicking the <b>[Reset]</b> button is required to revert the effects of this parameter's action.</td></tr>
<tr><td><b>Drop all Active Connections</b></td><td></td><td></td><td>When selected the option will drop all active connection to the endpoint if the maximum failed authentication attempts limit is reached.</td></tr>
<tr><td><b>Reset Endpoint Blocking</b>
Reset</td><td></td><td></td><td>Reset the blocked endpoint</td></tr>
</table>

Table: OPC UA Server, Server Endpoints Creation, Authentication Restrictions For Local OPC UA Endpoint

2. Authentication Restrictions for Remote IP



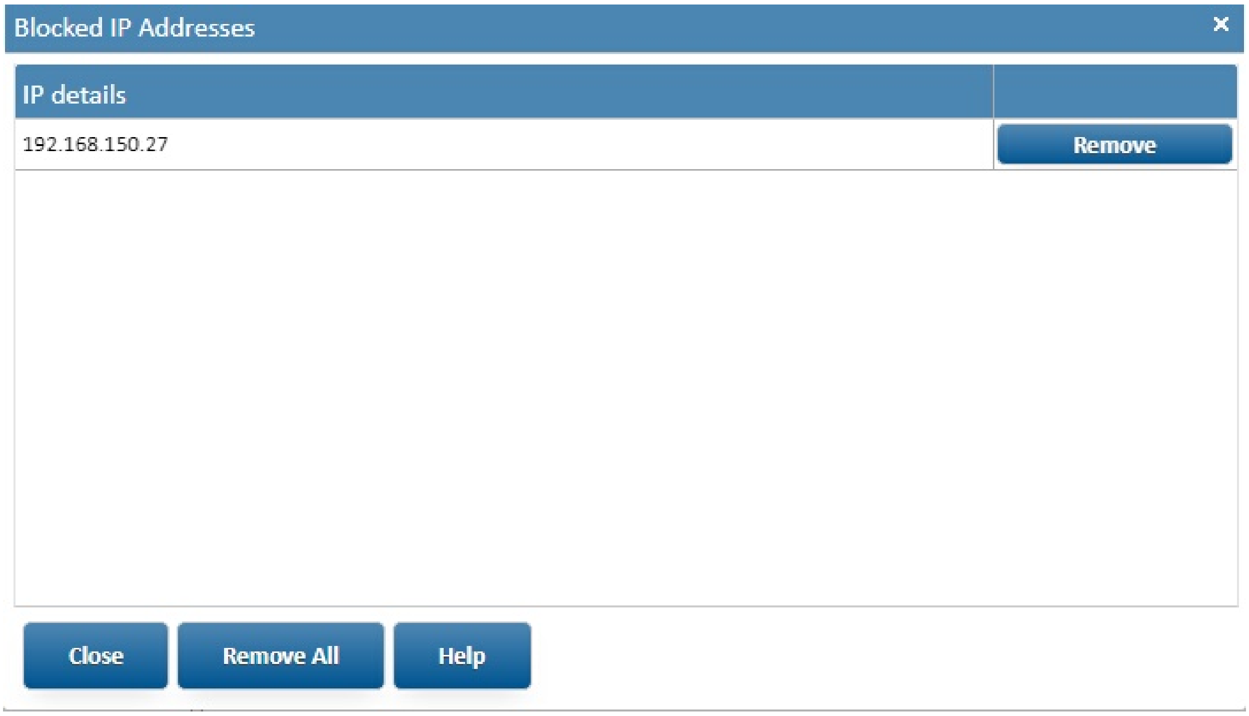
Restrictions for Remote IP Addresses

Authentication Restrictions for Remote IP Addresses	☑
Max Failed Authentication Attempts per Second	1
Disable Time [seconds]	50
Disable Time Increase Factor	1
Disable Permanent	☐
Show Disabled IP Addresses	Show

This restriction group applies **on each possible OPC UA client** trying to establish a connection to the endpoint **individually,** the clients are being identified based on their IP address. The restrictions can be seen as a possible consequence of the actions performed by one OPC UA client and restrictions apply to that client alone.

<table>
<tr><th>Parameter name</th><th>Default Value</th><th>Unit</th><th>Details</th></tr>
<tr><td><b>Max Failed Authentication Attempts per Second</b></td><td><b>10</b></td><td><b>units</b></td><td>Total number of maximum failed authentications per second.
Origin of the authentication attempt must be the same OPC UA client.</td></tr>
<tr><td><b>Disable Time</b></td><td><b>10</b></td><td><b>seconds</b></td><td>IP Address disable time if the maximum failed authentication attempts limit is reached.
IP Address is disabled only for the OPC UA client whose actions triggered the disabling.</td></tr>
<tr><td><b>Disable Time Increase Factor</b></td><td><b>5</b></td><td><b>factor</b></td><td>Endpoint disable increase factor will be used to increase the <b>Disable Time</b> in case the maximum failed authentication attempts limit is reached several times consecutively without successful authentication in between.
The disable time is increased (multiplied) with a factor of the value of this parameter.
Eg: based on the default values the disable time related to the count of consecutive failed authentication attempts
<table>
<tr><th>Consecutive failed authentications</th><th>Disable time (default values based)</th></tr>
<tr><td>5</td><td>10 seconds</td></tr>
<tr><td>10</td><td>50 seconds (5* 10 seconds)</td></tr>
<tr><td>15</td><td>250 second (5* 50 seconds)</td></tr>
</table></td></tr>
<tr><td><b>Disable Permanent</b></td><td></td><td></td><td>When selected the option will permanently disable the endpoint if the maximum failed authentication attempts limit is reached.
Manual re-enabling is required to revert the effects of this parameter's action.
Endpoint is disabled only for the OPC UA client whose actions triggered the disabling</td></tr>
<tr><td><b>Show Disabled IP Addresses</b>
Show</td><td></td><td></td><td>Show Disabled IP Addresses</td></tr>
</table>

To show the list with blocked Addresses click the **[SHOW]** and a window will show up:



Blocked IP Addresses

IP details

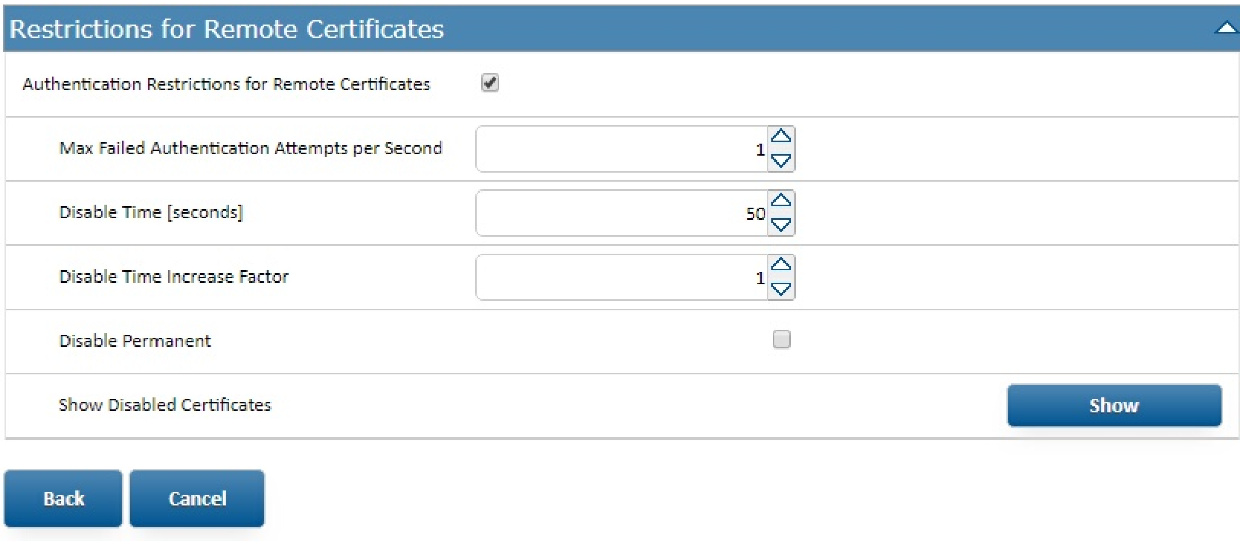
192.168.150.27

Window buttons actions:

Button	Action
Remove	Remove selected ip from Blocked Ip list
Close	Close IP Blocked Addresses window
Remove All	Remove All Blocked IP Addresses
Help	Help

Table: OPC UA Server, Server Endpoints Creation, Authentication Restrictions For Remote IP

3. Authentication Restrictions for Remote Certificates



Restrictions for Remote Certificates

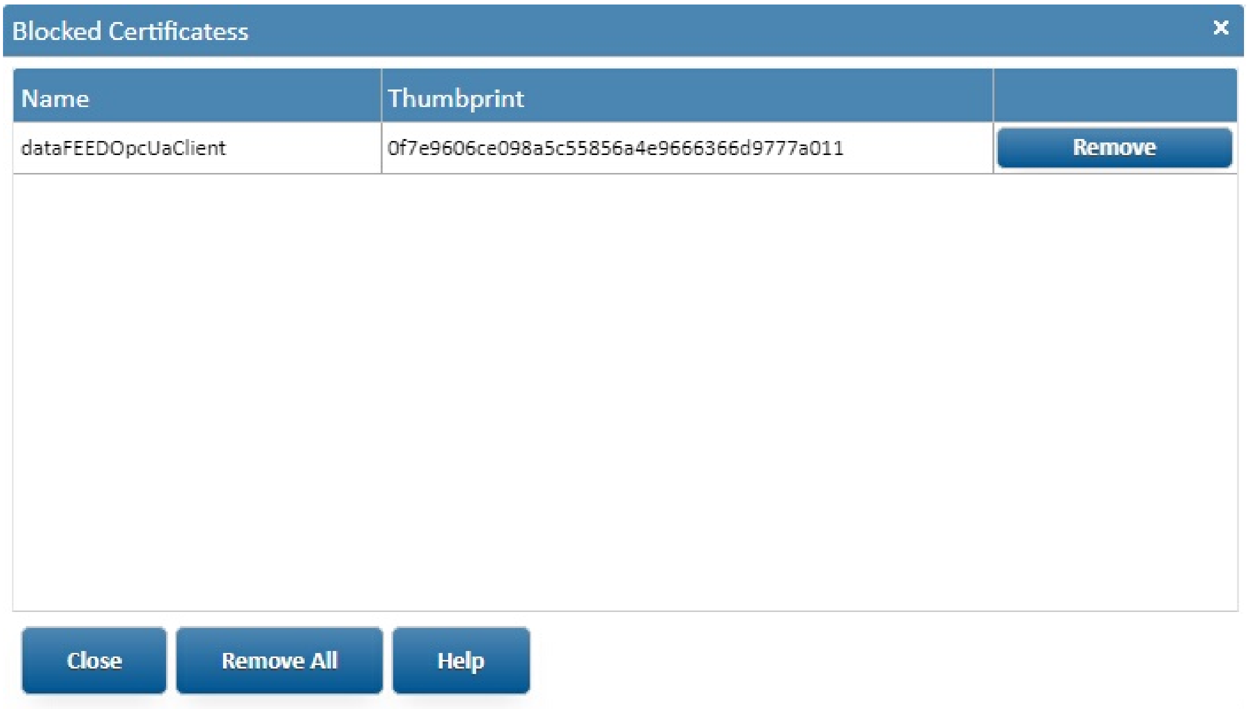
Authentication Restrictions for Remote Certificates	☑
Max Failed Authentication Attempts per Second	1
Disable Time [seconds]	50
Disable Time Increase Factor	1
Disable Permanent	□
Show Disabled Certificates	Show

This restriction group applies **on each possible OPC UA client** trying to establish a connection to the endpoint **individually,** the clients are being identified based on their application certificates. The restrictions can be seen as a possible consequence of the actions performed by one OPC UA client and restrictions apply to that client alone.

Parameter name	Default Value	Unit	Details
Max Failed Authentication Attempts per Second	**5**	**units**	Total number of maximum failed authentications per second. Origin of the authentication attempt must be the same OPC UA client.
Disable Time	**10**	**seconds**	Certificate disable time if the maximum failed authentication attempts limit is reached. Certificate is disabled only for the OPC UA client whose actions triggered the disabling.
Disable Time Increase Factor	**5**	**factor**	Endpoint disable increase factor will be used to increase the **Disable Time** in case the maximum failed authentication attempts limit is reached several times consecutively without successful authentication in between. The disable time is increased (multiplied) with a factor of the value of this parameter. Eg: based on the default values the disable time related to the count of consecutive failed authentication attempts

<table>
<tr><td></td><td></td><td></td><td><table><tr><th>Consecutive failed authentications</th><th>Disable time (default values based)</th></tr><tr><td>5</td><td>10 seconds</td></tr><tr><td>10</td><td>50 seconds (5* 10 seconds)</td></tr><tr><td>15</td><td>250 second (5* 50 seconds)</td></tr></table></td></tr>
<tr><td><b>Disable Permanent</b></td><td></td><td></td><td>When selected the option will permanently disable the endpoint if the maximum failed authentication attempts limit is reached.
Manual re-enabling is required to revert the effects of this parameter's action.
Endpoint is disabled only for the OPC UA client whose actions triggered the disabling</td></tr>
<tr><td><b>Show Blocked Certificates</b>
Show</td><td></td><td></td><td>Show Blocked Certificates</td></tr>
</table>

Table: OPC UA Server, Server Endpoints Creation, Authentication Restrictions For Remote Certificates



Blocked Certificatess

Name	Thumbprint	
dataFEEDOpcUaClient	0f7e9606ce098a5c55856a4e9666366d9777a011	Remove

Window buttons actions:

Button	Action
Remove	Remove selected blocked certificate from Blocked Certificates list
Close	Close Blocked Certificates window
Remove All	Remove All Blocked Certificates
Help	Help

4.7.3.3.5 Advanced Settings

The Advanced Settings page provides more advanced configuration options for the current OPC UA Server Endpoint.

The option **Provide only Endpoint Description of current Endpoint** is used to restrict the endpoint description information exposed by the current OPC UA Server Endpoint.

The default state the option ‘Provide only Endpoint Description of current Endpoint’ is checked, meaning that the current endpoint will provide only the Endpoint Descriptions matching the current endpoint (with the same protocol, hostname and port).

By unchecking the restriction option, the endpoint will provide the Endpoint Descriptions corresponding to all opened OPC UA Server Endpoints.

Note that this option affects the current endpoint only, other endpoints will still expose the

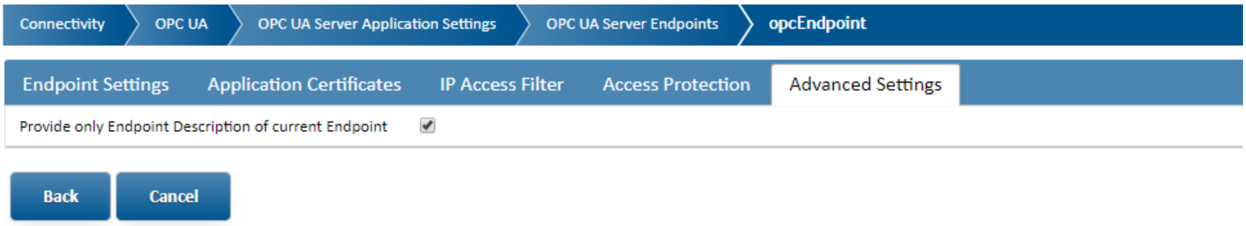
Endpoint Descriptions according to their own configuration.

A change to this option is applied immediately, without requiring the OPC UA Server Endpoint to be

restarted.

To enable or disable this option, navigate to **Connectivity -> OPC UA -> OPC UA Server Application Settings -> OPC UA Server Endpoints -> [opcEndpoint] -> Advanced Settings** and change the state by checking/unchecking the **[Provide only Endpoint Description of current Endpoint]** checkbox. The checkbox state reflects the expose of Endpoint Descriptions behavior:

- **checked** ☑ : Provide only Endpoint Description of current Endpoint enabled
- **unchecked** □ : Provide only Endpoint Description of current Endpoint disabled



Provide only Endpoint Description of current Endpoint ☑

Figure: OPC UA Server, Server Endpoints Creation, Advanced Settings

4.7.3.4 Edit existing Server Endpoints

To edit an existing OPC UA server endpoint navigate to **Connectivity -> OPC UA -> OPC UA Server Application Settings -> OPC UA Server Endpoints** select the appropriate endpoint entry in the list and click the **[Edit connection]** button on the information bar. Editing the existing endpoint is similar to creating a new server endpoint 188 with some of the fields being grayed out as they are not changeable after creation (eg: Endpoint Name).

Changing the endpoint URL will trigger an automatic endpoint restart. Endpoint URL depends on following editable endpoint settings fields:

- **OPC UA Endpoint Protocol**
- **OPC UA Endpoint Port**
- **OPC UA Endpoint Suffix**

4.7.3.5 Users Assignment

Any newly created OPC UA server endpoint requires a user to be assigned before it can be used by external OPC UA clients.

Failing to assign at least one user to a newly created OPC UA server endpoint would make the endpoint non accessible for any external OPC UA client.

All user operations affects the endpoint selected in the OPC UA Server Endpoints list.

The endpoint users information bar provides access to three buttons which can be used to change the selected endpoint users list.

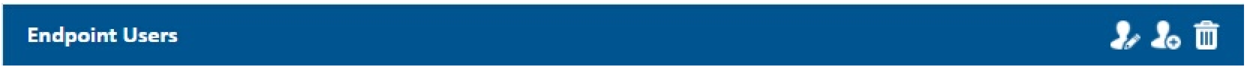


Figure: OPC UA Server, Users Assignment, Endpoint Users Menu Bar

Button	Action
👤✎	Edit endpoint user allows changing the settings for the endpoint users list selected entry.
👤+	Add a new user to the select endpoint.
🗑	Deletes user selected in the endpoint users list.

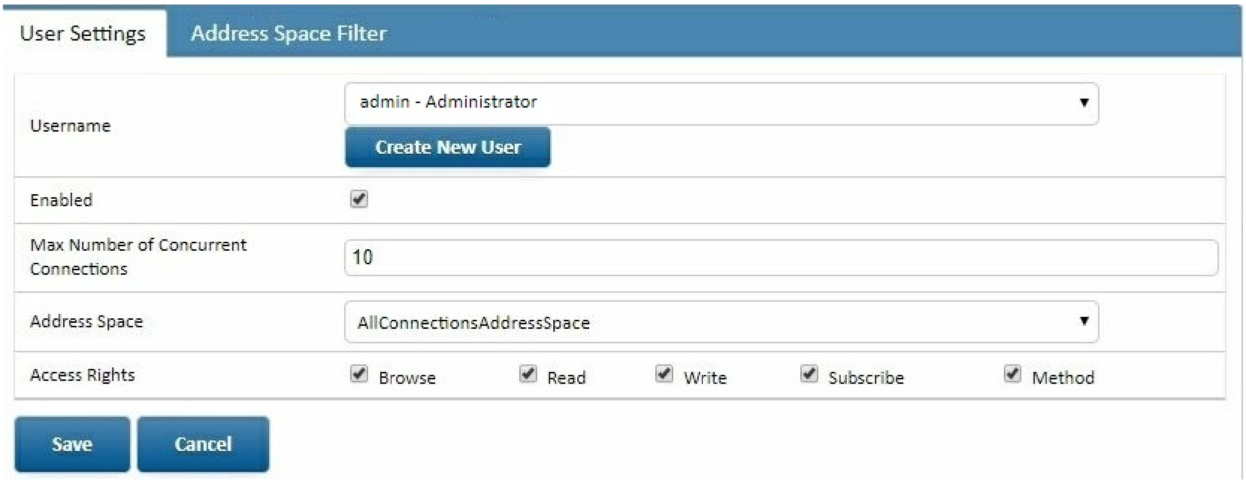
Table: OPC UA Server, Users Assignment, Endpoint Users Menu Bar Buttons

4.7.3.5.1 User Settings

Adding or editing an endpoint user are similar operations with the difference that the edit user will not allow creating a new user or reassigning a new user name to the selected endpoint. To add a new/edit an existing user click the **[Add Endpoint User] / [Edit Endpoint User]** button.

Add Endpoint User:

A new page will show up and a series of options shall be available. When editing an existing user the Username drop down list is deactivated, and also the creation of new users is disabled.



Username: admin - Administrator

Enabled: ☑

Max Number of Concurrent Connections: 10

Address Space: AllConnectionsAddressSpace

Access Rights: ☑ Browse ☑ Read ☑ Write ☑ Subscribe ☑ Method

Figure: OPC UA Server, Users Assignment, User Settings

Page buttons actions:

Button	Action
Create New User	Convenient way to create a new user in this context. The user Settings 36 page will become active as a consequence of pressing this button.
Save	Once the user configuration is finalized clicking the **[Save]** button shall apply the configuration and bind the user and the additional configuration to the selected endpoint.
Cancel	Cancel the current endpoint configuration session.

Table: OPC UA Server, Users Assignment, User Settings Buttons

The user settings configuration tab allows selecting an already existing user by using the **Username** provided drop down list or create a new system user 36 by clicking the **[Create New User]** button. User settings information to be filled in is described in the following table:

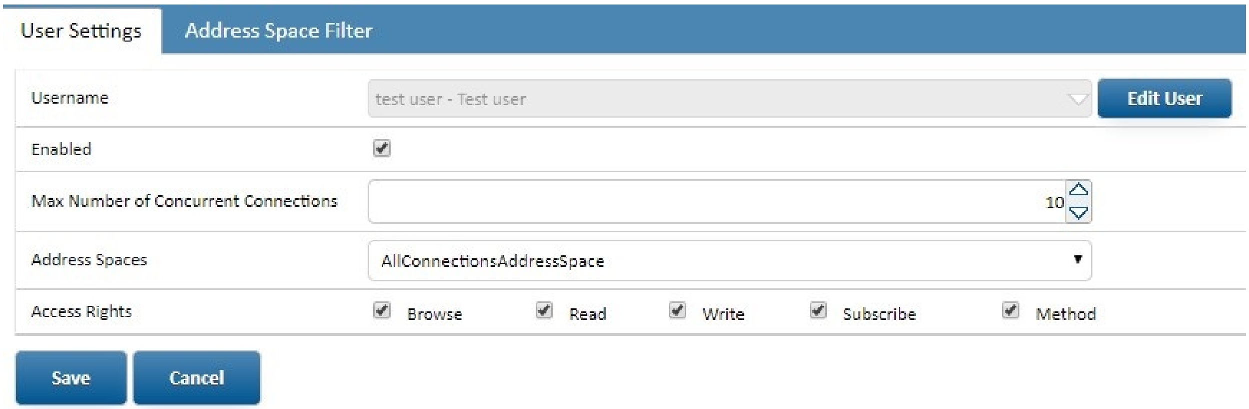
Parameter name	Default Value	Details
Username	**empty**	Defines the endpoint's authorized user.
Enabled	**True**	Controls if the endpoint's authorized user is enabled or disabled. Once disabled the username cannot be used to authenticate while a OPC UA client establishes a connection to the endpoint.
Max Number of Concurrent Connections	**10**	Maximum allowed number of concurrent OPC UA client connections to the selected endpoint being authenticated with the username defined in the **Username** parameter
Address Space	allConnetionsAddressSpace	Address space exposed to the OPC UA client connection to the selected endpoint and authenticated with the username defined in the **Username** parameter
Access Rights	All	Services allowed for the username defined in the **Username** parameter

Table: OPC UA Server, Users Assignment, User Settings Parameters

Edit Endpoint User:

Once a user is assigned to an endpoint, a new option is available to edit user settings directly from the **Endpoint Users – Identities -Edit Endpoint User**.

To edit any user assigned to an endpoint just double click on the user or press the **[Edit Endpoint User]** button from **Endpoint Users – Identities** section. A new **[Edit User]** button is now available in the User Settings page, see the picture below:



Username	test user - Test user
Enabled	☑
Max Number of Concurrent Connections	10
Address Spaces	AllConnectionsAddressSpace
Access Rights	☑ Browse ☑ Read ☑ Write ☑ Subscribe ☑ Method

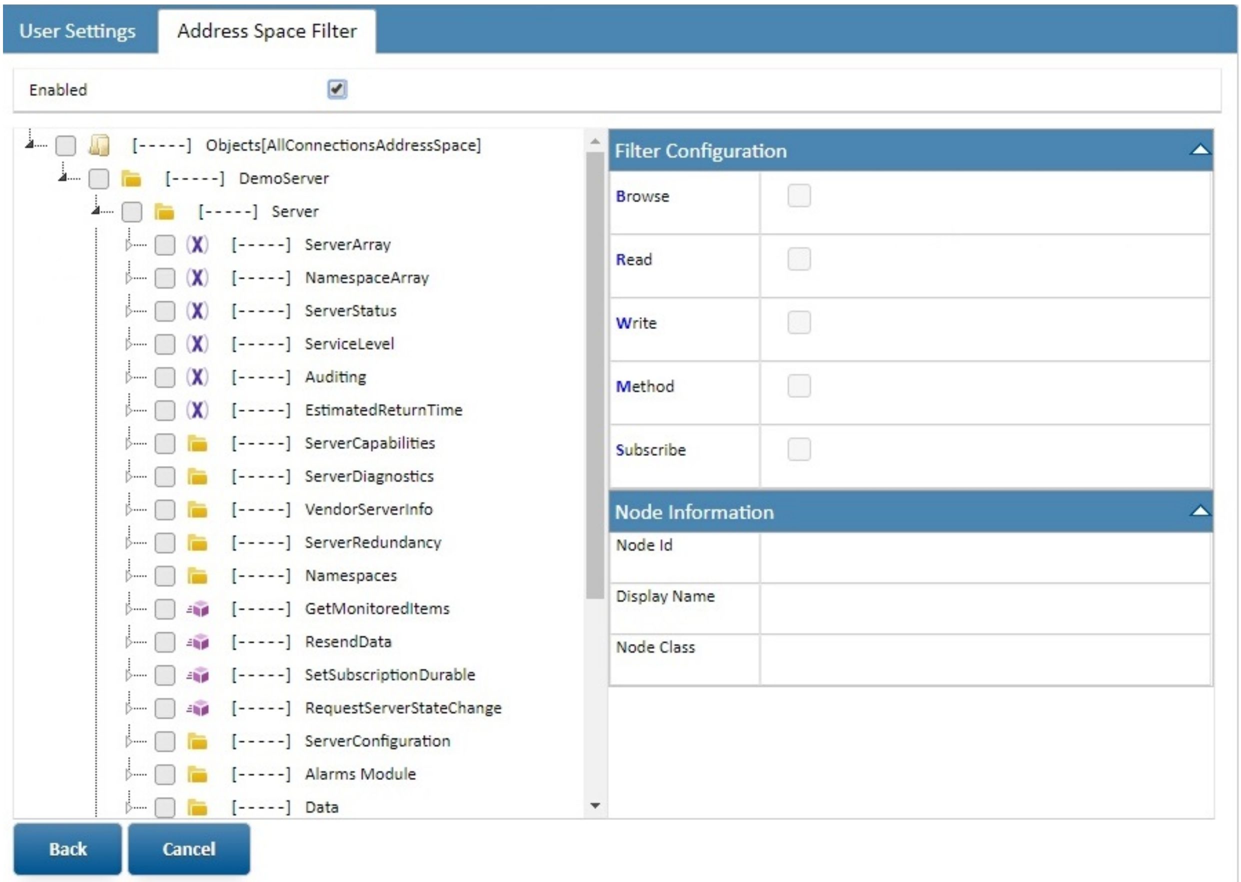
Table: Figure: OPC UA Server, Users Assignment, User Settings

4.7.3.5.2 Address Space Filter

The Address space filter is an additional functionality allowing enhanced user based restrictions to the exposed address space and is applied per **overall OPC-UA service base**.

When enabled, by validating the **[Enabled]** check-box, this functionality allows selecting only the desired address space sub-tree accessible to the currently configured user name together with the desired service filters.

The currently supported service filters are: Browse, Read, Write, Method call and Subscribe.



Enabled ☑

```
□ [-----] Objects[AllConnectionsAddressSpace]
  □ [-----] DemoServer
    □ [-----] Server
      □ (X) [-----] ServerArray
      □ (X) [-----] NamespaceArray
      □ (X) [-----] ServerStatus
      □ (X) [-----] ServiceLevel
      □ (X) [-----] Auditing
      □ (X) [-----] EstimatedReturnTime
      □ [-----] ServerCapabilities
      □ [-----] ServerDiagnostics
      □ [-----] VendorServerInfo
      □ [-----] ServerRedundancy
      □ [-----] Namespaces
      □ [-----] GetMonitoredItems
      □ [-----] ResendData
      □ [-----] SetSubscriptionDurable
      □ [-----] RequestServerStateChange
      □ [-----] ServerConfiguration
      □ [-----] Alarms Module
      □ [-----] Data
```

Filter Configuration	
Browse	□
Read	□
Write	□
Method	□
Subscribe	□

Node Information	
Node Id	
Display Name	
Node Class	

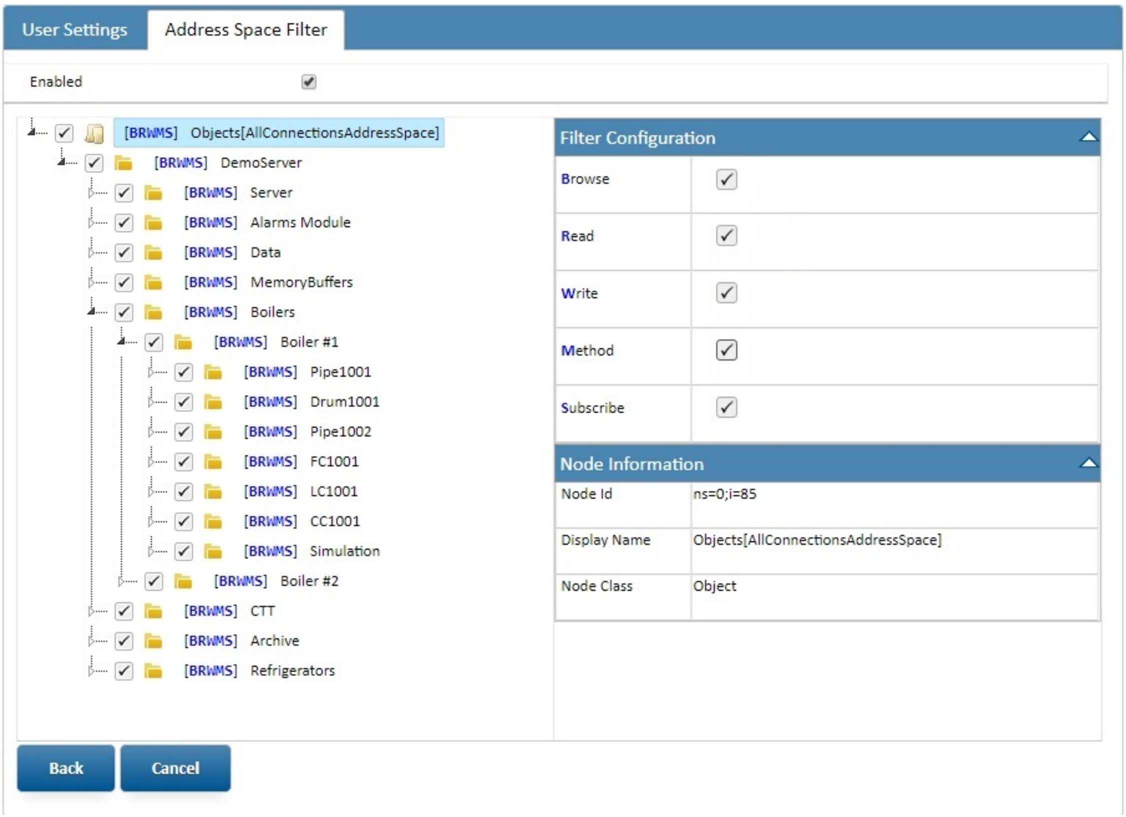
Figure: OPC UA Server, Users Assignment, Address Space Filter

Selecting the sub-tree is easily achievable by navigating the root address space, as defined in the **User Settings** tab in the **Address Space** parameter, and selecting the desired node service filters to be applied as filters for the configured user.

If at least a service filter of a node is selected in the address space's **node hierarchy**, than all the parent nodes are highlighted by a filled check-box, thus signaling that as a visual cue, to aid in pinpointing the node by sequential browsing.

Quick services filtering:

An easy way to apply OPC-UA service filtering on all nodes in the address space is to operate on the Objects node only.



Enabled ☑

- ☑ [BRWMS] Objects[AllConnectionsAddressSpace]
  - ☑ [BRWMS] DemoServer
    - ☑ [BRWMS] Server
    - ☑ [BRWMS] Alarms Module
    - ☑ [BRWMS] Data
    - ☑ [BRWMS] MemoryBuffers
    - ☑ [BRWMS] Boilers
      - ☑ [BRWMS] Boiler #1
        - ☑ [BRWMS] Pipe1001
        - ☑ [BRWMS] Drum1001
        - ☑ [BRWMS] Pipe1002
        - ☑ [BRWMS] FC1001
        - ☑ [BRWMS] LC1001
        - ☑ [BRWMS] CC1001
        - ☑ [BRWMS] Simulation
      - ☑ [BRWMS] Boiler #2
    - ☑ [BRWMS] CTT
    - ☑ [BRWMS] Archive
    - ☑ [BRWMS] Refrigerators

Filter Configuration

Browse	☑
Read	☑
Write	☑
Method	☑
Subscribe	☑

Node Information

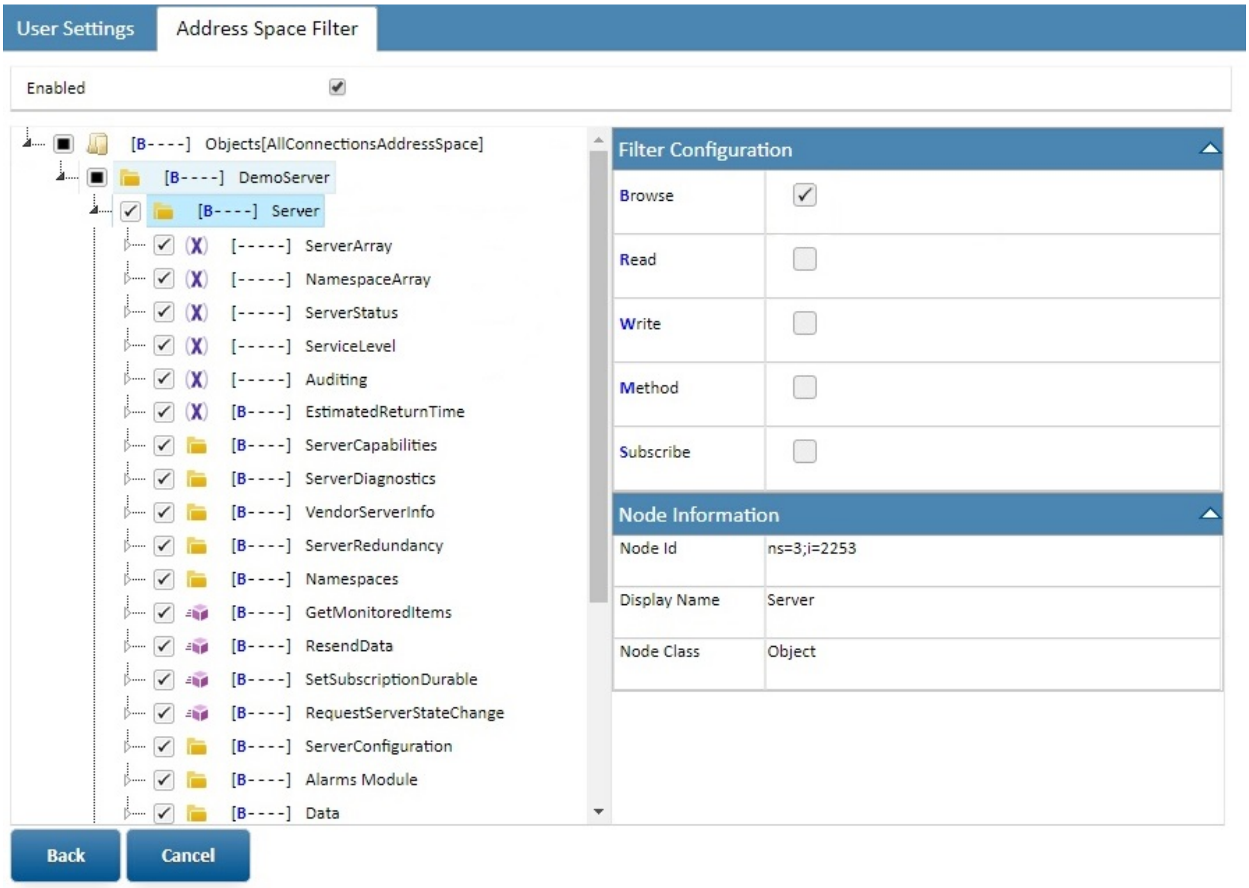
Node Id	ns=0;i=85
Display Name	Objects[AllConnectionsAddressSpace]
Node Class	Object

Figure: OPC UA Server, Users Assignment, Quick Address Space Service Filter

If services are enabled only for child nodes of the Objects node, then no service filters for all parent nodes (including the Objects node) are shown except the Browse service, which is displayed if the Browse service has been selected for a child node.

The service filter selection is applied on a node and on it's child nodes with the following behavior particularities per service base.

Browse Filter Selection:



User Settings | Address Space Filter

Enabled ☑

- ■ [B----] Objects[AllConnectionsAddressSpace]
  - ■ [B----] DemoServer
    - ☑ [B----] Server
      - ☑ [-----] ServerArray
      - ☑ [-----] NamespaceArray
      - ☑ [-----] ServerStatus
      - ☑ [-----] ServiceLevel
      - ☑ [-----] Auditing
      - ☑ [B----] EstimatedReturnTime
      - ☑ [B----] ServerCapabilities
      - ☑ [B----] ServerDiagnostics
      - ☑ [B----] VendorServerInfo
      - ☑ [B----] ServerRedundancy
      - ☑ [B----] Namespaces
      - ☑ [B----] GetMonitoredItems
      - ☑ [B----] ResendData
      - ☑ [B----] SetSubscriptionDurable
      - ☑ [B----] RequestServerStateChange
      - ☑ [B----] ServerConfiguration
      - ☑ [B----] Alarms Module
      - ☑ [B----] Data

Filter Configuration

Browse	☑
Read	□
Write	□
Method	□
Subscribe	□

Node Information

Node Id	ns=3;i=2253
Display Name	Server
Node Class	Object

Figure: OPC UA Server, Users Assignment, Address Space Filter select Browse service filter

Browse service filter selection is automatically propagated both up the **node hierarchy** and down through all the node's **hierarchical children**. The propagation of the selection up the **node hierarchy,** does not hold any longer, if at least one sibling node has the Browse service filter set.

Browse service filter selection on sibling nodes is done independently and it is by this means that the user can further refine the selection at this service level.

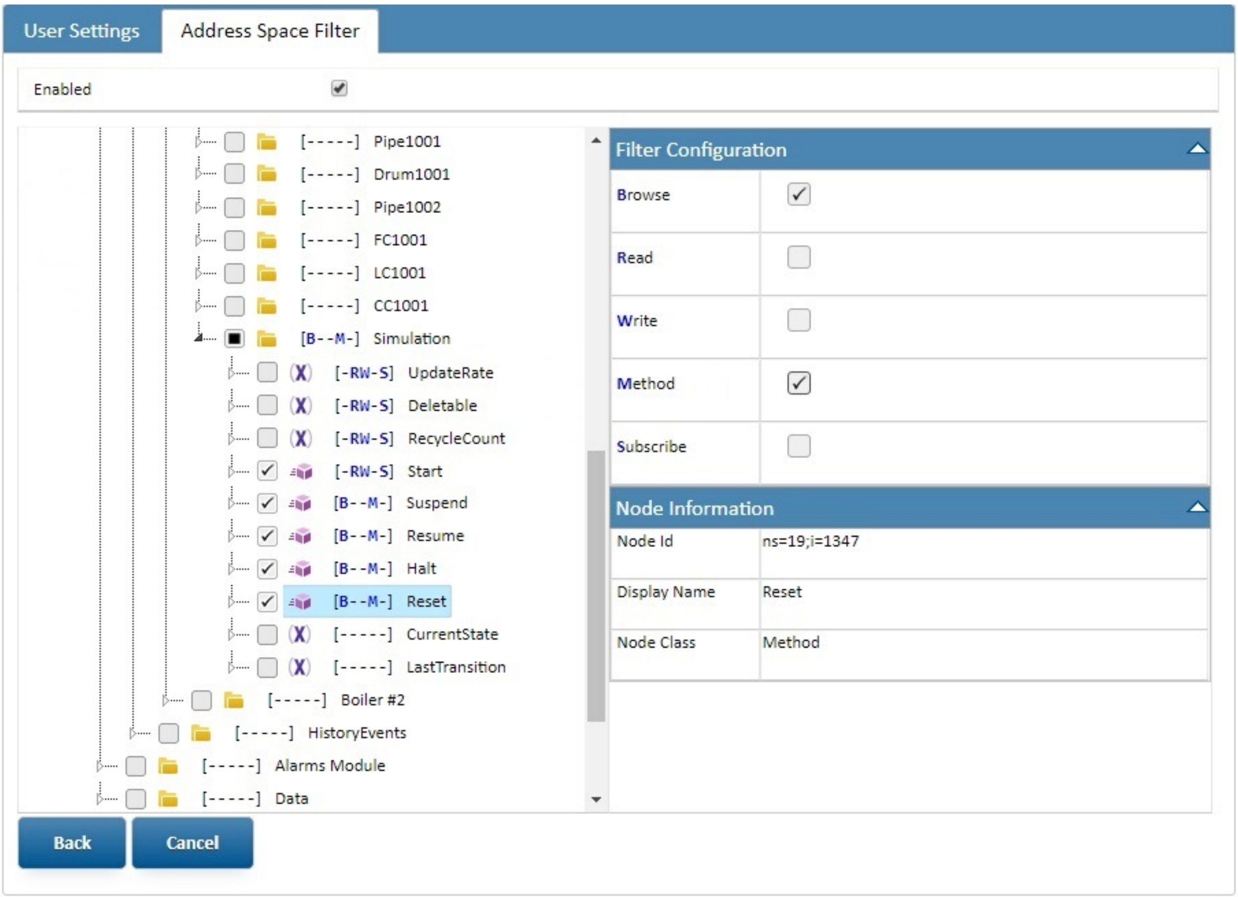
The backward propagation up the **node hierarchy** and down through all the node's **hierarchical children** is automatically maintained as a means to keep "alive" the access via the Browse service to the node which has the Browse service filter set, therefore keeping the Browse service behavior consistent by not allowing such a node to become unreachable.

Method Filter Selection:

Method service filter selection is automatically propagated only in the direction of all the node's **hierarchical children**, but the service filter will be applied only to enable/disable method calls on method nodes.

By enabling Method call service filter on method nodes the user has not yet enabled the method call service on the method nodes. For this to happen, the hierarchical parent on which the method node is to be called, also has to have the Method call service filter set. This is a design particularity, since the OPC-UA method call service requires as input the instance of the object on which the method node is called.

Method call service filter selection on sibling nodes is done independently and it is by this means that the user can further refine the selection at this service level.



Enabled ☑

```
□ [-----] Pipe1001
□ [-----] Drum1001
□ [-----] Pipe1002
□ [-----] FC1001
□ [-----] LC1001
□ [-----] CC1001
■ [B--M-] Simulation
    □ [-RW-S] UpdateRate
    □ [-RW-S] Deletable
    □ [-RW-S] RecycleCount
    ☑ [-RW-S] Start
    ☑ [B--M-] Suspend
    ☑ [B--M-] Resume
    ☑ [B--M-] Halt
    ☑ [B--M-] Reset
    □ [-----] CurrentState
    □ [-----] LastTransition
  □ [-----] Boiler #2
□ [-----] HistoryEvents
□ [-----] Alarms Module
□ [-----] Data
```

Filter Configuration

Browse	☑
Read	□
Write	□
Method	☑
Subscribe	□

Node Information

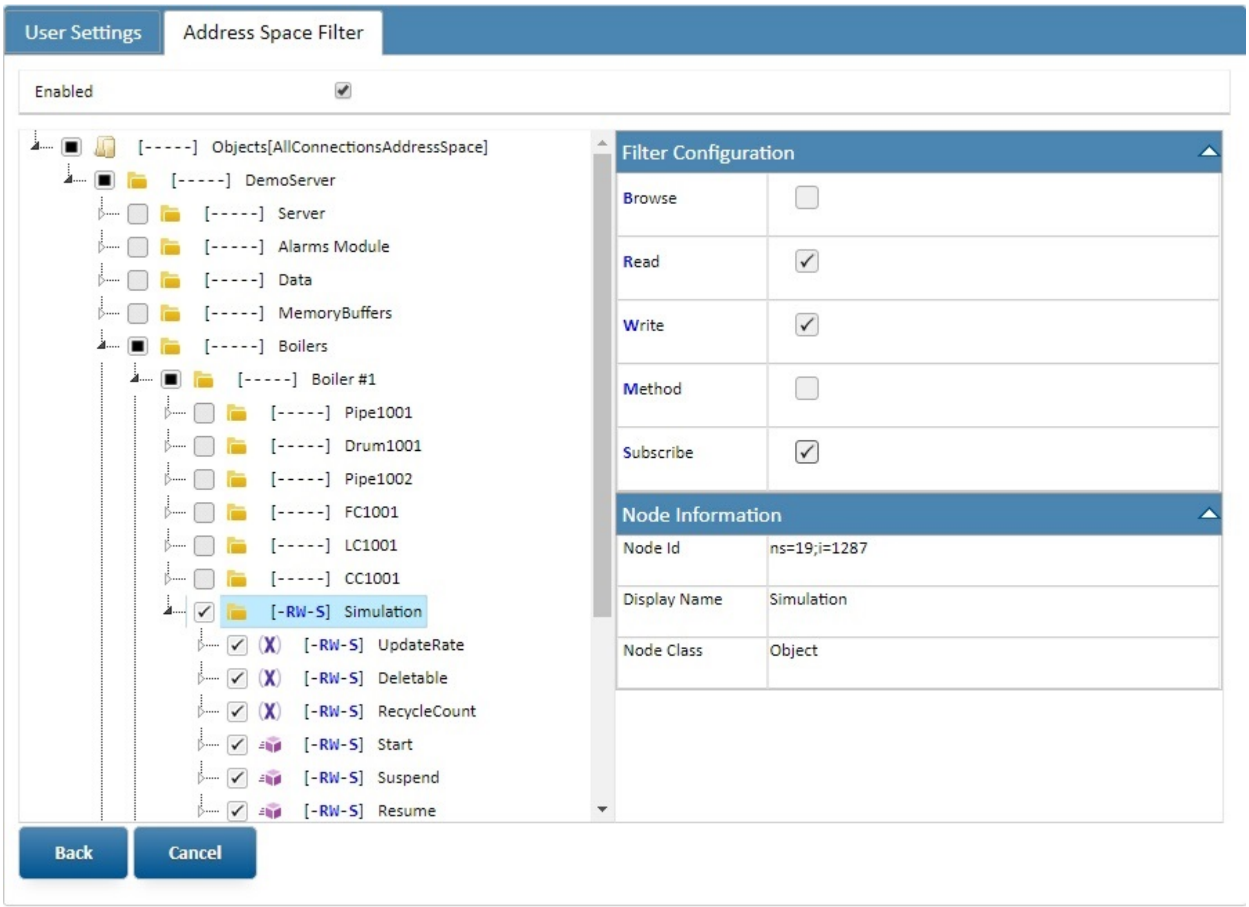
Node Id	ns=19;i=1347
Display Name	Reset
Node Class	Method

Figure: OPC UA Server, Users Assignment, Address Space Filter select Method service filter

Read, Write and Subscribe Filter Selection:

Read, Write and Subscribe service filter selection is automatically propagated only in the direction of all the node's **hierarchical children.**

Read, Write and Subscribe service filter selection on sibling nodes is done independently and it is by this means that the user can further refine the selection at this service level.



Enabled ☑

- ■ [-----] Objects[AllConnectionsAddressSpace]
  - ■ [-----] DemoServer
    - □ [-----] Server
    - □ [-----] Alarms Module
    - □ [-----] Data
    - □ [-----] MemoryBuffers
    - ■ [-----] Boilers
      - ■ [-----] Boiler #1
        - □ [-----] Pipe1001
        - □ [-----] Drum1001
        - □ [-----] Pipe1002
        - □ [-----] FC1001
        - □ [-----] LC1001
        - □ [-----] CC1001
        - ☑ [-RW-S] Simulation
          - ☑ [-RW-S] UpdateRate
          - ☑ [-RW-S] Deletable
          - ☑ [-RW-S] RecycleCount
          - ☑ [-RW-S] Start
          - ☑ [-RW-S] Suspend
          - ☑ [-RW-S] Resume

Filter Configuration

Browse	□
Read	☑
Write	☑
Method	□
Subscribe	☑

Node Information

Node Id	ns=19;i=1287
Display Name	Simulation
Node Class	Object

Figure: OPC UA Server, Users Assignment, Address Space Filter select Read, Write and Subscribe service filters

The service filters are applied only after clicking on the Save button on the "User Settings" tab.

4.7.4 OPC UA Advanced Settings

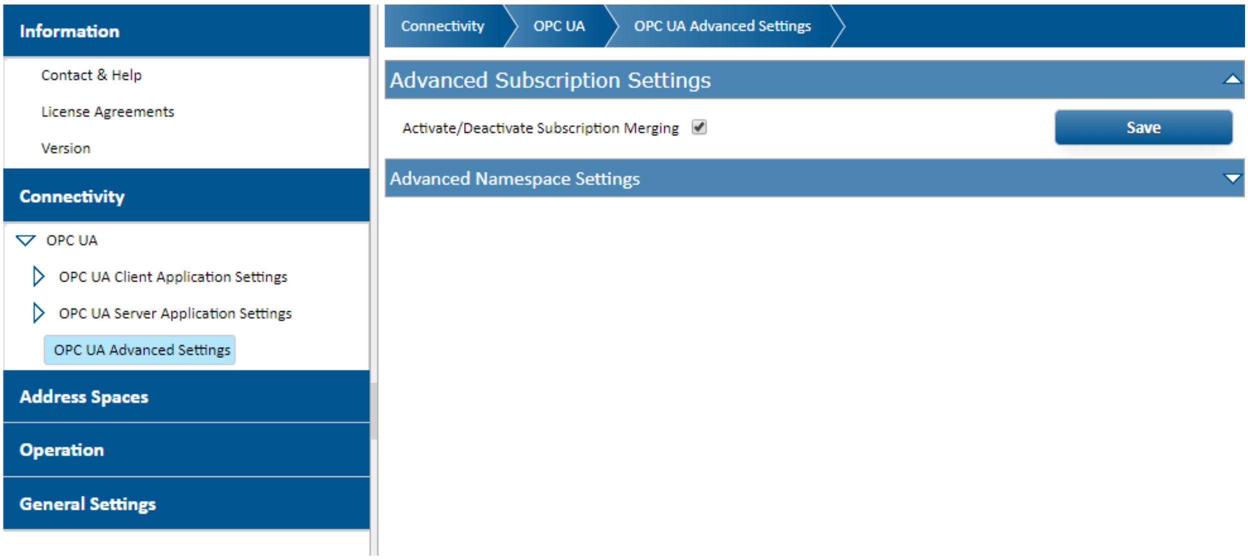
1. Enabling/Disabling Subscription Merging

Note: If performed while in running mode, changing the merging parameter will trigger a restart (going to halted and back to running mode).

To enable or disable the Subscription Merging, navigate to **Connectivity -> OPC UA -> OPC UA Advanced Settings**, expand the **Advanced Subscription Settings** section and change the state of the Subscription Merging, by checking/unchecking the **[Activate/Deactivate Subscription Merging]** checkbox, then click the **[Save]** button.

The checkbox state reflects the subscription merging:

- **checked** ☑ : Subscription Merging enabled
- **unchecked** □ : Subscription Merging disabled



Activate/Deactivate Subscription Merging ☑

Figure: Activate/Deactivate Subscription Merging

2. Reset of the OPC UA Namespace Array

Note: If performed while in running mode, reseting the OPC UA Namespace Array will trigger a restart (going to halted and back to running mode).

While performing connections to external OPC UA Clients, dataFEED Secure Integration Server manipulates the **NamespaceArray** node of the OPC UA address-space (i=2255). The namespace URIs which are found on the configured connections are processed and imported into the own namespace array. Once added, they are persisted at their original index in the array, even after a restart of the dataFEED Secure Integration Server or the removal of the source OPC UA Client connection from the configuration. Sometimes, these persisted namespace URIs might become irrelevant for the current dataFEED Secure Integration Server address-space, therefore there is the option to **Reset the OPC UA Namespace Array**.

By using this option, all persisted data of the OPC UA Namespace Array are discarded and the array is rebuilt by using only URIs provided by the the currently active connections.

To reset the OPC UA Namespace Array, navigate to **Connectivity -> OPC UA -> OPC UA Advanced Settings,** expand the **Advanced Namespace Settings** section and click the **[Reset]** button.

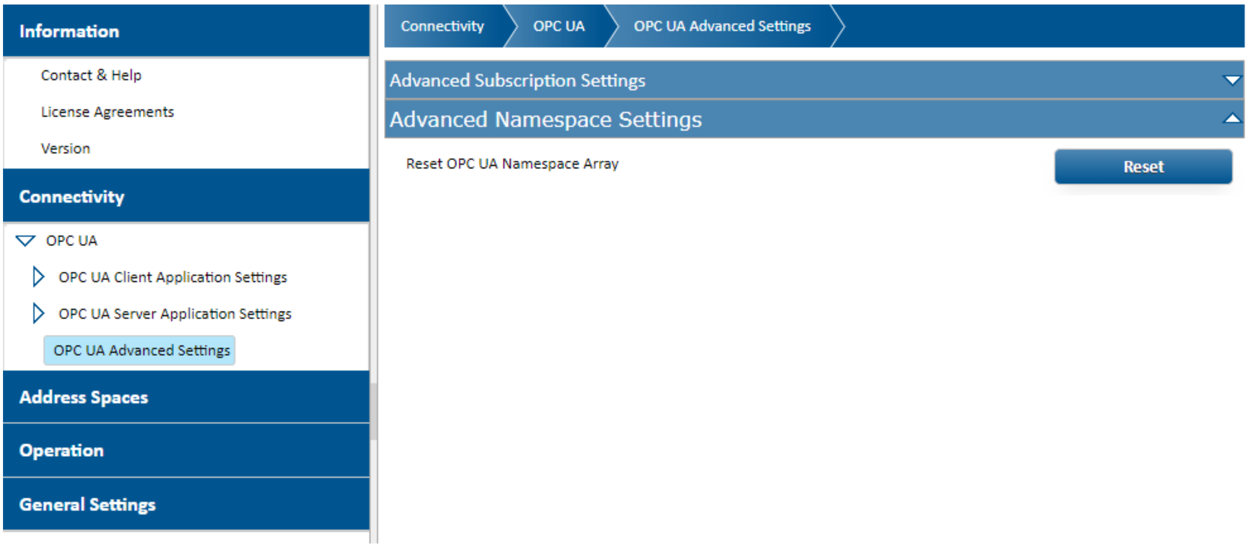


Figure: Reset of the OPC UA Namespace Array

4.7.5 Address Space

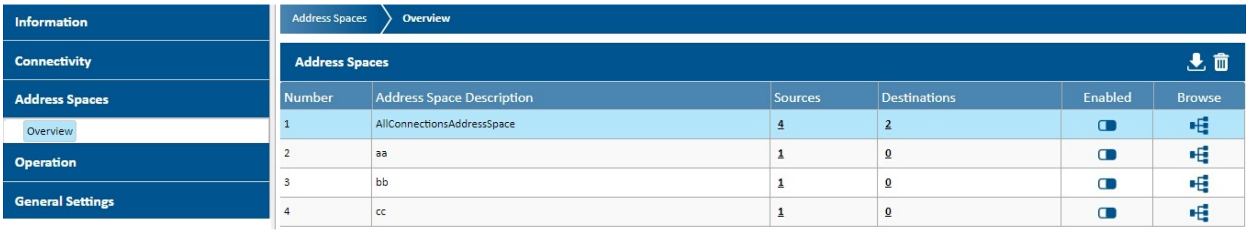
Data aggregated from external OPC UA servers is exposed by the dataFEED Secure Integration Server endpoints in address spaces configurable in the endpoint's user settings. An exposed aggregated address space acts as a single address space as seen from the OPC UA client's point of view.

Address spaces are referenced in the following cases:

- during the configuration of a new or existing OPC UA client connection 164, the connections will be bound to one or more address spaces allowing access to the external OPC UA server address space
- during the configuration of an OPC UA server endpoint user 211 an address space is required to be used as the exposed address space for the OPC UA clients connected to the endpoint and authenticated with the configured user

By default the dataFEED Secure Integration Server defines one address space named **AllConnectionsAddressSpace**

A centralized place to access all defined address spaces is reachable by navigating to **Address Space -> Overview.**



Number	Address Space Description	Sources	Destinations	Enabled	Browse
1	AllConnectionsAddressSpace	4	2	●	☷
2	aa	1	0	●	☷
3	bb	1	0	●	☷
4	cc	1	0	●	☷

Figure: Address Space

The available address spaces are presented in a table format. Each row represents an address space and the information in the table is sortable by clicking the table header. The table header information is described in the table below:

Column name	Information details
Number	Address space table index.
Address Space Description	Address space name as defined when created 164.
Sources	Number of OPC UA client connections defining the current address space.
Destinations	Number of **username**-**endpoint** pairs exposing the address space for OPC UA clients authenticating with the **username** during connection establishment to the **endpoint**.
Status	Describes the configuration state of the address space. Possible values are **Enabled** or **Disabled** . Note: Clicking on the current configuration state icon would trigger a state toggle: • **Enabled** **-> Disabled** • **Disabled** -> **Enabled** **Note: External OPC UA clients will not be able to access data in a server endpoint exposing a disabled address space.**
Browse	Address space browse is possible by clicking on the browse icon in the corresponding address space row.

Table: Address Space Fields

Figure: Address Space Menu Bar

The address space menu bar provides two buttons with the following functionality:

Button	Action
⬇	Export address space.
🗑	Delete the selected address space.

Table: Address Space Menu Bar Buttons

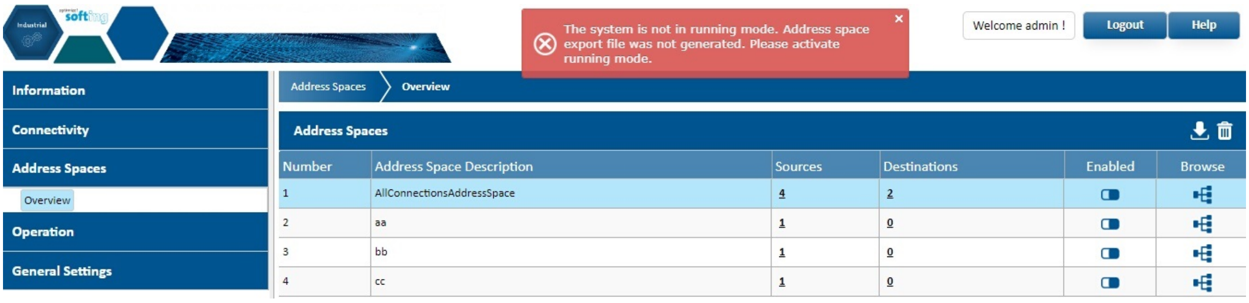
1. Address Space Export

dataFEED Secure Integration Server provides an address space export functionality which creates an OPC UA compliant NodeSet2 XML file describing the address space. To export an existing address space select it in the address space list and click the **[Export Address Space]** button on the information bar. Once the file is available it will be automatically downloaded with the predefined name ***[AddressspaceName]*-export.xml** where ***[AddressspaceName]*** is a placeholder and shall be replaced with the actual exported address space name.

Address space NodeSet2 XML file creation varies depending on various parameters (eg: address space size, network bandwidth etc).

The generated NodeSet2 XML file complies to OPC UA specifications version 1.03

Given the possible high complexity or non-adherence to the OPC UA specifications of some external OPC UA servers, the address space export functionality might fail. In such cases an informative alert window requesting the user's acknowledgement shall pop up:



The system is not in running mode. Address space export file was not generated. Please activate running mode.

Number	Address Space Description	Sources	Destinations	Enabled	Browse
1	AllConnectionsAddressSpace	4	2		
2	aa	1	0		
3	bb	1	0		
4	cc	1	0		

Figure: Address Space, Export Address Space

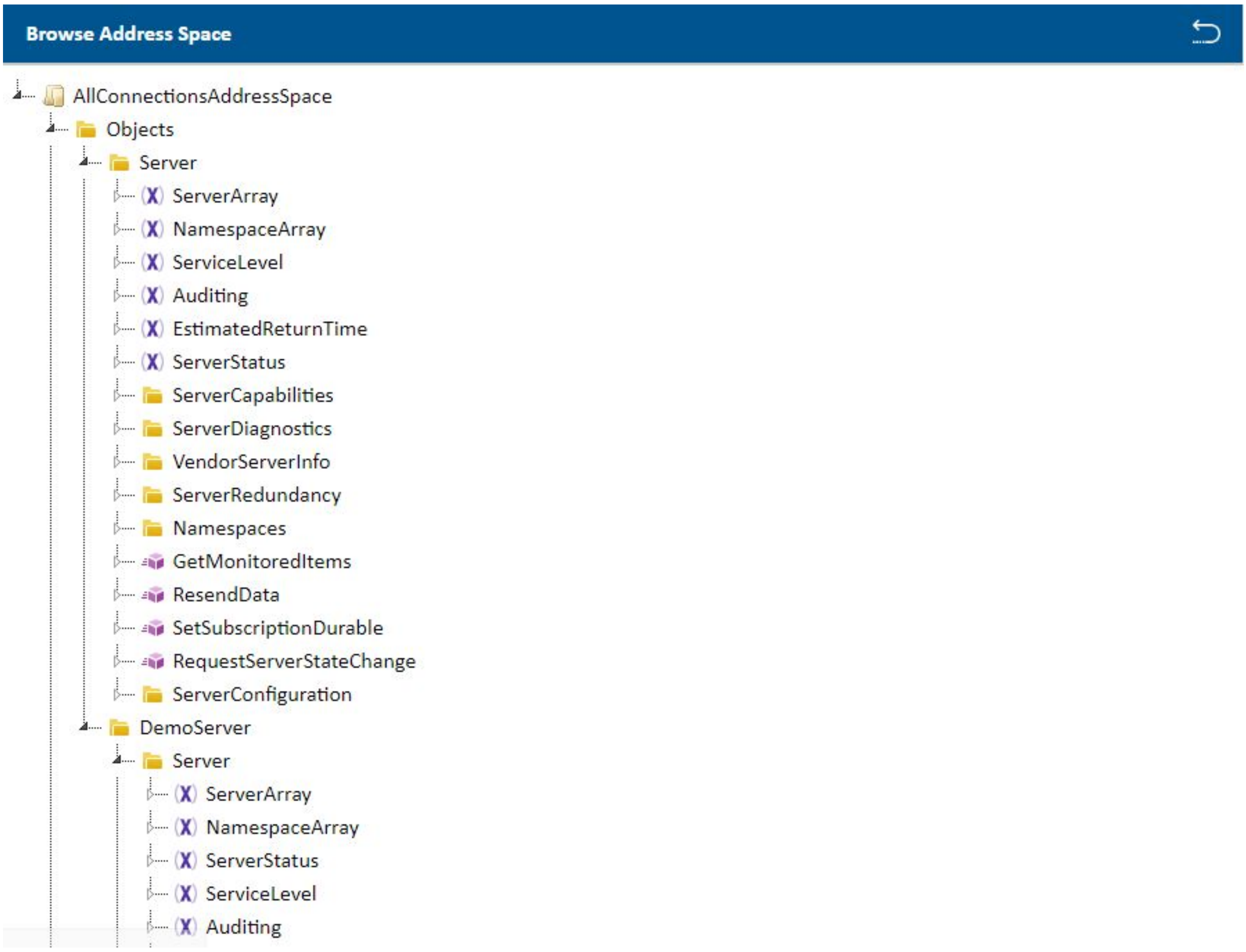
2. Address Space Delete

Prior to deleting an address space it is required that both, the **Sources** and **Destinations,** field values are 0. It essentially means that the address space is not used anymore by any **OPC UA client connection** or by an endpoint attached username (**username-endpoint** pair).

Deletion of an address space is achievable by selecting the desired address space and clicking the **[Delete Address Space]** button.

3. Address Space Browse

It is possible to browse an address space directly in the web browser by clicking the **[Browse Address Space]** browse icon. A new page shall load and will present the OPC UA address space as a tree view:



Browse Address Space

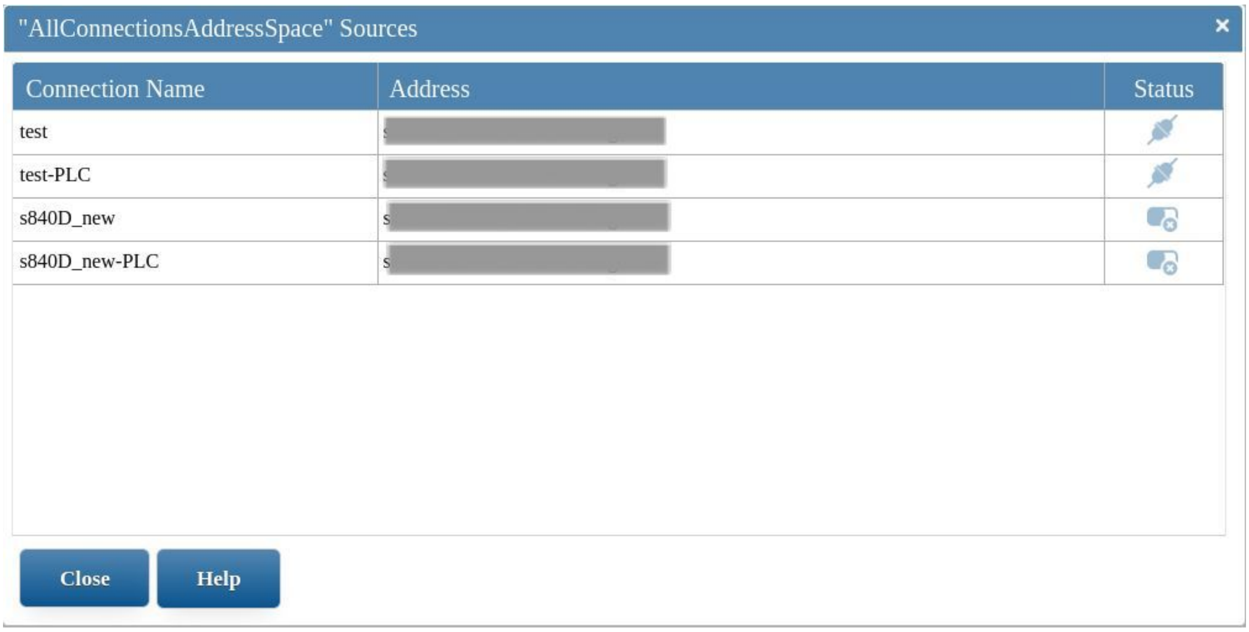
- AllConnectionsAddressSpace
  - Objects
    - Server
      - ServerArray
      - NamespaceArray
      - ServiceLevel
      - Auditing
      - EstimatedReturnTime
      - ServerStatus
      - ServerCapabilities
      - ServerDiagnostics
      - VendorServerInfo
      - ServerRedundancy
      - Namespaces
      - GetMonitoredItems
      - ResendData
      - SetSubscriptionDurable
      - RequestServerStateChange
      - ServerConfiguration
    - DemoServer
      - Server
        - ServerArray
        - NamespaceArray
        - ServerStatus
        - ServiceLevel
        - Auditing

Figure: Address Space, Browse Address Space

Currently the web based OPC UA address space browse functionality is limited to presenting the OPC UA adress space as a tree with the browse name node information attached. To return to the address space overview page click the return button on the Browse address space information bar.

4. Address Space Sources

A list with all connections (sources) using an address space can be opened by clicking the **[Sources]** cell entry of the address space. The detailed information is presented in a new window as shown below (sample from edgeConnector 840D), based on the edgeConnector product type the information might differ:



"AllConnectionsAddressSpace" Sources

Connection Name	Address	Status
test	[redacted]	🔌
test-PLC	[redacted]	🔌
s840D_new	[redacted]	⊗
s840D_new-PLC	[redacted]	⊗

Figure: Address Space Sources

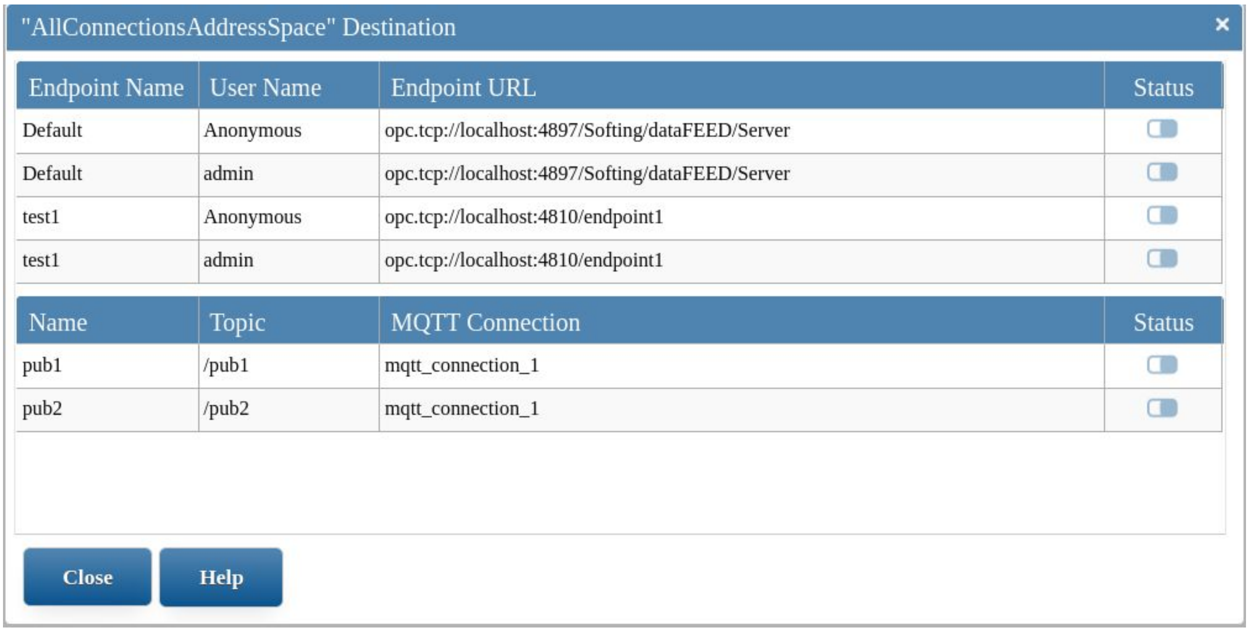
The connections list using the address space as a source is presented in a table with the following information:

Column name	Information details
Connection Name	Source connection name.
Address	Configured source connection address (URL or IP).
Status	Source connection status information: **Connected** 🔌 , **Disconnected** 🔌 **or** **Disabled** ⊗

Table: Address Space Sources Information Fields

5. Address Space Destinations

A list with all the destinations (OPC UA server endpoints or MQTT publish requests) of an address space can be opened by clicking the **[Destinations]** cell entry of the address space. The detailed information is presented in a new window as shown below:



"AllConnectionsAddressSpace" Destination

Endpoint Name	User Name	Endpoint URL	Status
Default	Anonymous	opc.tcp://localhost:4897/Softing/dataFEED/Server	
Default	admin	opc.tcp://localhost:4897/Softing/dataFEED/Server	
test1	Anonymous	opc.tcp://localhost:4810/endpoint1	
test1	admin	opc.tcp://localhost:4810/endpoint1	

Name	Topic	MQTT Connection	Status
pub1	/pub1	mqtt_connection_1	
pub2	/pub2	mqtt_connection_1	

Figure: Address Space, Destinations

Destination OPC UA server endpoints table information:

Column name	Information details
Endpoint Name	Server endpoint name.
Username	Username authorized to access the address space.
Endpoint URL	The server endpoint URL.
Status	Current server endpoint state: **Enabled** or **Disabled** .

Table: Address Space, OPC UA Endpoints Destination Fields

Destination MQTT publisher requests table information:

Column name	Information details
Name	Configured MQTT publisher request name.
Topic	Configured MQTT publisher topic name.
MQTT Connection	The MQTT broker connection used for the publisher request.
Status	Current MQTT publisher request state: **Enabled** or **Disabled** .

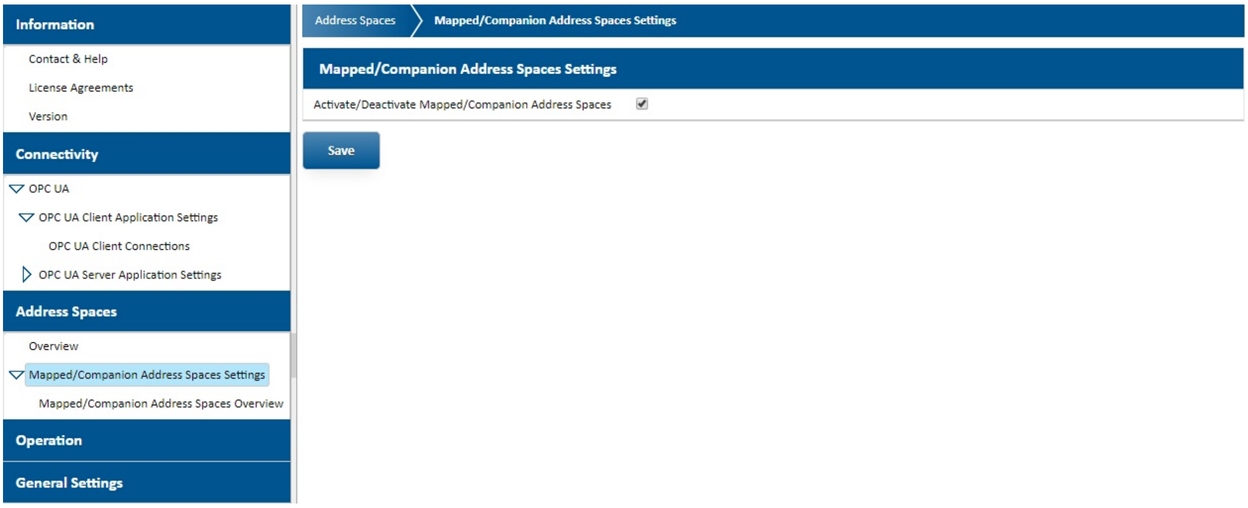
Table: Address Space, MQTT Publisher Requests Destination Fields

4.7.5.1 Mapped/Companion Address Spaces Settings

1. Enabling/Disabling Mapped/Companion Address Spaces

To enable or disable the Mapped/Companion Address Spaces, navigate to **Address Spaces -> Mapped/Companion Address Spaces Settings** and change the state by checking/unchecking the **[Activate/Deactivate Mapped/Companion Address Spaces]** checkbox. The checkbox state reflects the Mapped/Companion Address Spaces state:

- **checked** ☑ : Mapped/Companion Address Spaces enabled
- **unchecked** ☐ : Mapped/Companion Address Spaces disabled


Information
Contact & Help
License Agreements
Version
Connectivity
OPC UA
OPC UA Client Application Settings
OPC UA Client Connections
OPC UA Server Application Settings
Address Spaces
Overview
Mapped/Companion Address Spaces Settings
Mapped/Companion Address Spaces Overview
Operation
General Settings
Address Spaces
Mapped/Companion Address Spaces Settings
Save

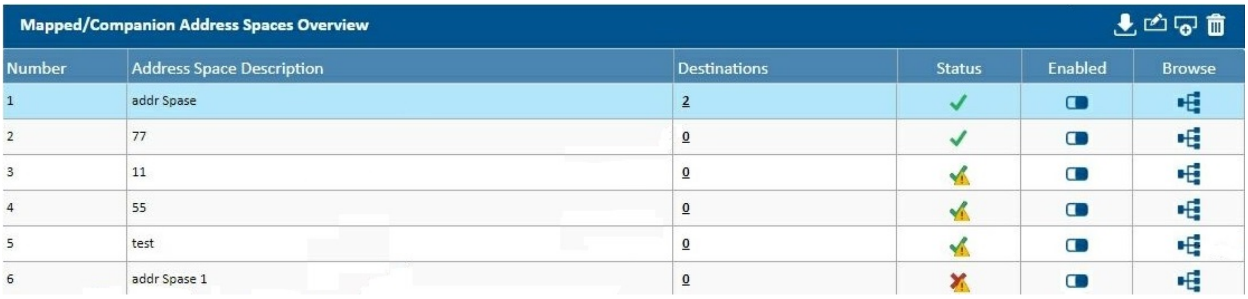
Mapped/Companion Address Spaces Settings

Activate/Deactivate Mapped/Companion Address Spaces ☑

Figure: Mapped/Companion Address Spaces Settings

4.7.5.2 Mapped/Companion Address Spaces Overview

All Mapped/Companion Address Spaces are easily accessible by navigating to **Address Spaces -> Mapped/Companion Address Spaces Settings -> Mapped/Companion Address Spaces Overview**. The default Mapped/Companion Address Spaces is empty, therefore no Mapped/Companion Address Spaces will be shown. A pre-populated sample of the Mapped/Companion Address Spaces overview is pictured below:



Mapped/Companion Address Spaces Overview

Number	Address Space Description	Destinations	Status	Enabled	Browse
1	addr Spase	2	✓	◧	⊞
2	77	0	✓	◧	⊞
3	11	0	⚠	◧	⊞
4	55	0	⚠	◧	⊞
5	test	0	⚠	◧	⊞
6	addr Spase 1	0	✗	◧	⊞

Figure: Mapped/Companion Address Spaces Overview

The Mapped/Companion Address Spaces are presented in a table format, each row represents a Mapped/Companion Address Spaces and the information in the table is sortable by clicking the table header. The table header information is described in the following table:

Button	Action
Number	Address space table index.
Address Space Description	**Address Space Description** as defined at creation time.
Destinations	Number of **username-endpoint** pairs exposing the address space for OPC UA clients authenticating with the **username** during connection establishment to the **endpoint**.
Status	Describes the **state of the Mapped/Companion Address Spaces;** can be: • *good* ✓ – the mapped address space is up and with no issues; • *warning* ✓⚠ – the mapped address space is up, but there were warnings; • *failed* ✗⚠– the mapped address space failed to come up (so, it is unavailable, athough it is enabled); • *off* ✗– the mapped address space is disabled or the module is disabled; • *loading* ⟳ – address space loading is in progress.
Enabled	Describes the state of the **Mapped/Companion Address Spaces**. Possible values are **Enabled** ▭ or **Disabled** ⊗. Note: Clicking on the current configuration state icon would trigger a state toggle: • **Enabled** ▭ **-> Disabled** ⊗ • **Disabled** ⊗ **-> Enabled** ▭
Browse	

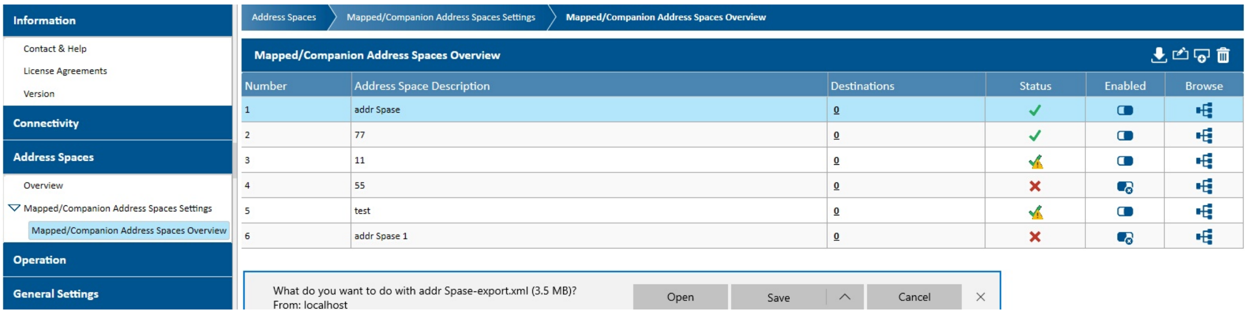
Table: Mapped/Companion Address Spaces Fields

1. Address Space Export

dataFEED Secure Integration Server provides an address space export functionality which creates an OPC UA compliant NodeSet2 XML file describing the address space. To export an existing address space select it in the address space list and click the **[Export Address Space]** button on the information bar. Once the file is available it will be automatically downloaded with the predefined name ***[AddressspaceName]*-export.xml** where ***[AddressspaceName]*** is a placeholder and shall be replaced with the actual exported address space name.

Address space NodeSet2 XML file creation varies depending on various parameters (eg: address space size, network bandwidth etc).

The generated NodeSet2 XML file complies to OPC UA specifications version 1.03



Information
Contact & Help
License Agreements
Version
Connectivity
Address Spaces
Overview
Mapped/Companion Address Spaces Settings
Mapped/Companion Address Spaces Overview
Operation
General Settings
Address Spaces
Mapped/Companion Address Spaces Settings
Mapped/Companion Address Spaces Overview

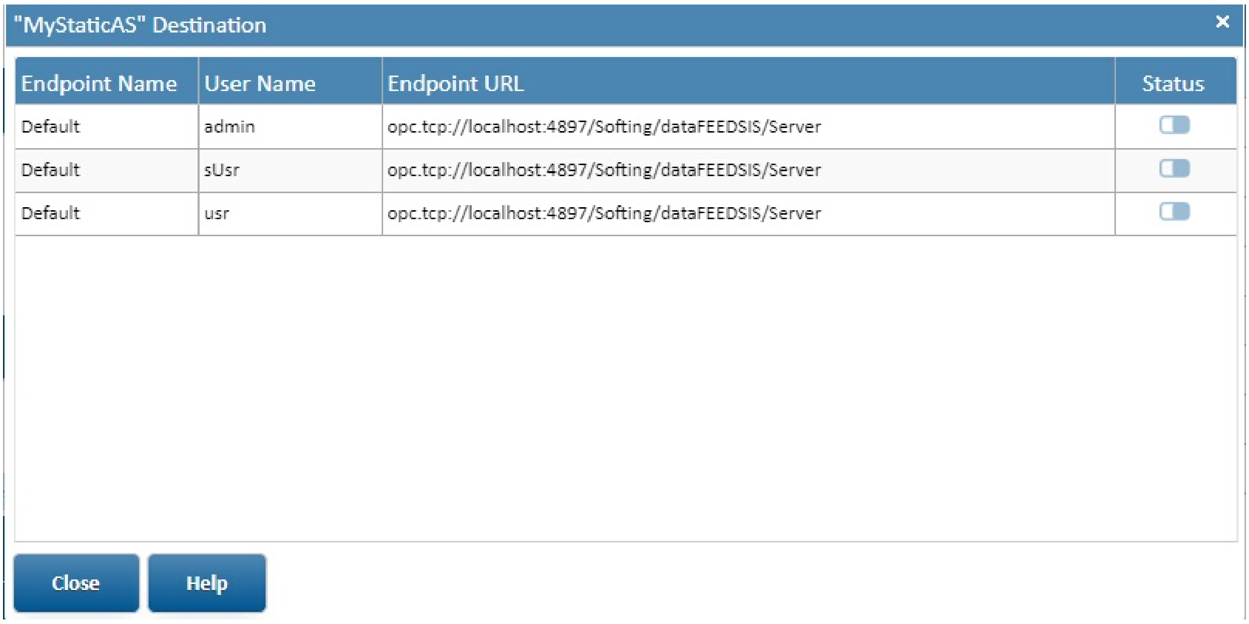
Mapped/Companion Address Spaces Overview

Number	Address Space Description	Destinations	Status	Enabled	Browse
1	addr Spase	0	✓	●	
2	77	0	✓	●	
3	11	0	✓⚠	●	
4	55	0	✗	⊗	
5	test	0	✓⚠	●	
6	addr Spase 1	0	✗	⊗	

What do you want to do with addr Spase-export.xml (3.5 MB)?
From: localhost

Figure: Mapped/Companion Address Spaces Overview - Export selected Mapped/Companion Address Spaces

2. Address Space Destination



"MyStaticAS" Destination

Endpoint Name	User Name	Endpoint URL	Status
Default	admin	opc.tcp://localhost:4897/Softing/dataFEEDSIS/Server	
Default	sUsr	opc.tcp://localhost:4897/Softing/dataFEEDSIS/Server	
Default	usr	opc.tcp://localhost:4897/Softing/dataFEEDSIS/Server	

Figure: Mapped/Companion Address Spaces Overview - Destinations

Button	Action
Endpoint Name	User defined endpoint name.
User Name	Defines the endpoint's authorized user.
Endpoint URL	The endpoint URL as resulted based on : • user defined transport protocol (opc.tcp or https) • the fully qualified domain name of the computer running the dataFEED Secure Integration Server • user defined port • user defined url-path
Status	Describes the state of the endpoint. Possible values are **Enabled** or **Disabled** . Note: Clicking on the current configuration state icon would trigger a state toggle: • **Enabled -> Disabled** • **Disabled -> Enabled**
Browse	

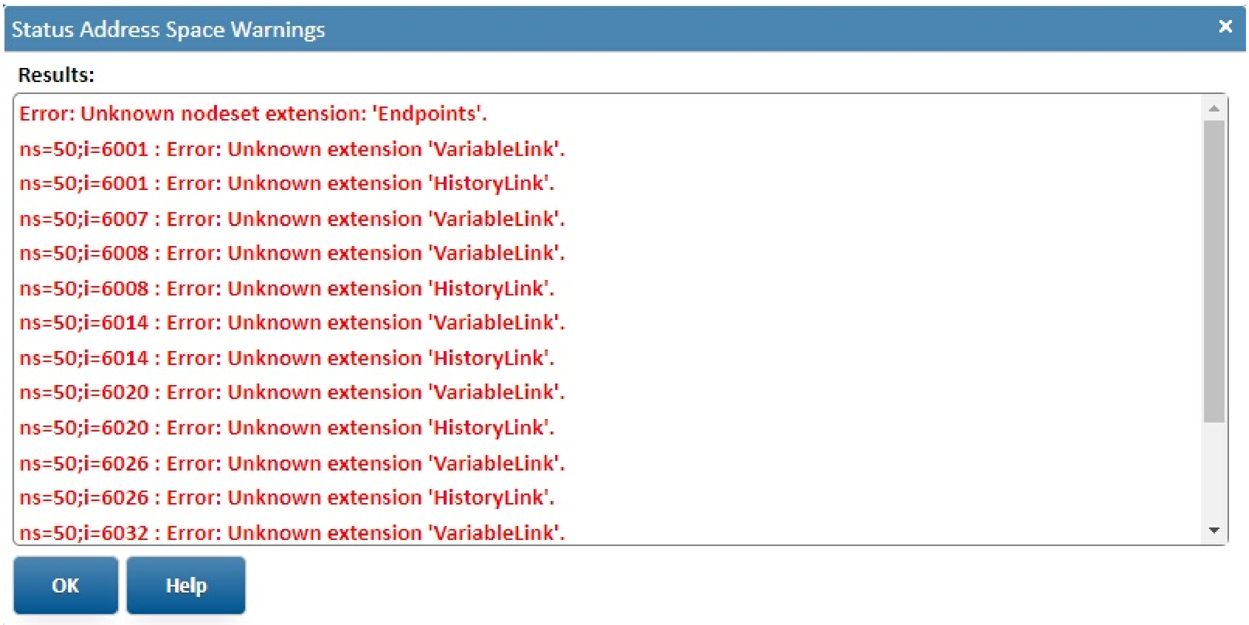
Bottom page buttons actions:

Button	Action
Close	Close Address Space Destination window
Help	Help of the current page.

Table: Buttons Mapped/Companion Address Spaces - Destinations

3. Address Space Status

Describes the **state of the Mapped/Companion Address Spaces**



Status Address Space Warnings

Results:

```
Error: Unknown nodeset extension: 'Endpoints'.
ns=50;i=6001 : Error: Unknown extension 'VariableLink'.
ns=50;i=6001 : Error: Unknown extension 'HistoryLink'.
ns=50;i=6007 : Error: Unknown extension 'VariableLink'.
ns=50;i=6008 : Error: Unknown extension 'VariableLink'.
ns=50;i=6008 : Error: Unknown extension 'HistoryLink'.
ns=50;i=6014 : Error: Unknown extension 'VariableLink'.
ns=50;i=6014 : Error: Unknown extension 'HistoryLink'.
ns=50;i=6020 : Error: Unknown extension 'VariableLink'.
ns=50;i=6020 : Error: Unknown extension 'HistoryLink'.
ns=50;i=6026 : Error: Unknown extension 'VariableLink'.
ns=50;i=6026 : Error: Unknown extension 'HistoryLink'.
ns=50;i=6032 : Error: Unknown extension 'VariableLink'.
```

Bottom page buttons actions:

Button	Action
OK	Close current page.
Help	Help of the current page.

Table: Buttons New Mapped/Companion Address Spaces - Status

4. Address Space Browse

It is possible to browse an address space directly in the web browser by clicking the **[Browse Address Space]** browse icon. A new page shall load and will present the OPC UA address space as a tree view:

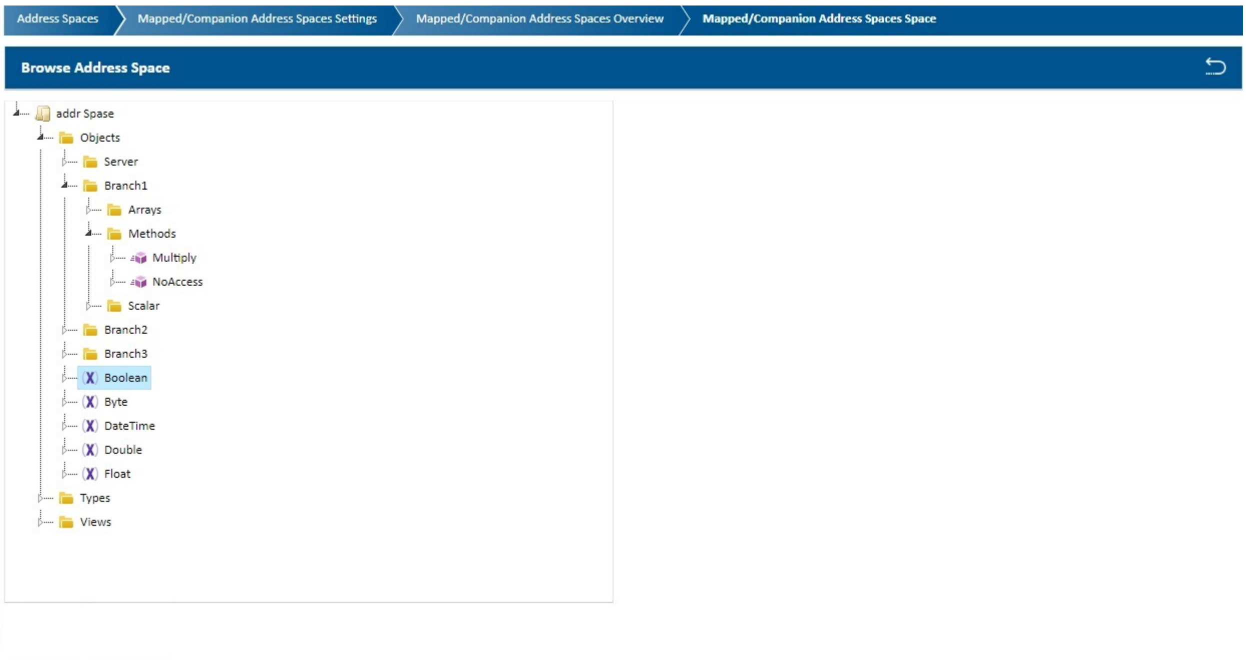


Figure: Mapped/Companion Address Spaces Overview - Browse

4.7.5.3 Mapped/Companion Address Spaces Creation

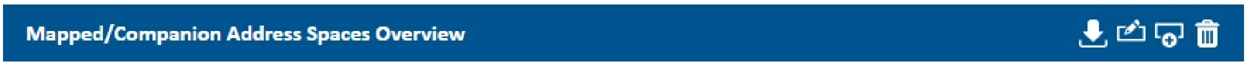


Figure: Mapped/Companion Address Spaces Menu Bar

The **Mapped/Companion Address Spaces** information bar provides four buttons with following functionality:

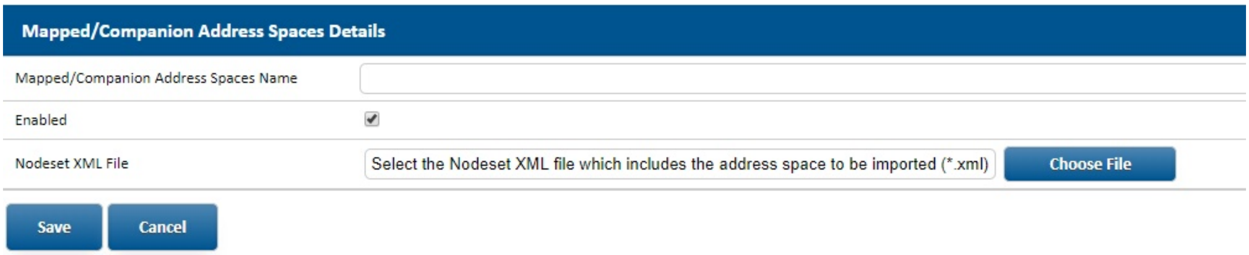
Button	Action
⬇	Export selected Mapped/Companion Address Spaces
✎	Edit selected Mapped/Companion Address Spaces
⊕	Add a new Mapped/Companion Address Spaces
🗑	Delete selected Mapped/Companion Address Spaces

Table: Mapped/Companion Address Spaces Actions

To create a new Mapped/Companion Address Spaces navigate to **Address Spaces -> Mapped/ Companion Address Spaces Settings-> Mapped/Companion Address Spaces Overview** and click the **[Add a new Mapped/Companion Address Spaces]** ⊕ button on the information bar.

4.7.5.3.1 New Mapped/Companion Address Spaces

Mapped/Companion Address Spaces Details is the view in the New Mapped/Companion Address Spaces page and provides a simple and intuitive interface for configuring a new or editing an existing Mapped/Companion Address Spaces.



Mapped/Companion Address Spaces Details

Mapped/Companion Address Spaces Name	
Enabled	☑
Nodeset XML File	Select the Nodeset XML file which includes the address space to be imported (*.xml)

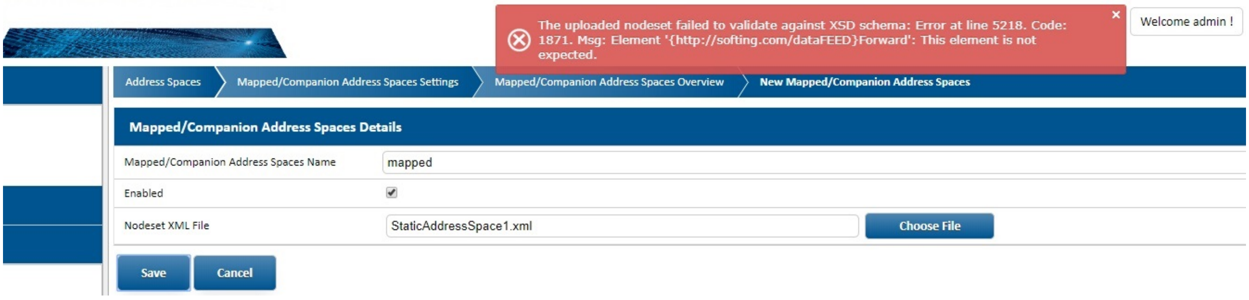
Figure: New Mapped/Companion Address Spaces

Bottom page buttons actions:

Button	Action
Save	Once the configuration is finalized, clicking the **[Save]** button shall apply the newly configured/modified **Mapped/Companion Address Spaces**.
Cancel	Cancel the current **Mapped/Companion Address Spaces** configuration. **Beware all changes shall be lost !**

Table: New Mapped/Companion Address Spaces Buttons

Validation of the nodeset xml file at the import time. After selecting a file, an automatic mechanism checks that the imported file is a valid xml file. If the check fails is should revert the sight creation, and the connection creation. In addition is show a Message Box with an short error description like.



The uploaded nodeset failed to validate against XSD schema: Error at line 5218. Code: 1871. Msg: Element '{http://softing.com/dataFEED}Forward': This element is not expected.

Welcome admin !
Address Spaces
Mapped/Companion Address Spaces Settings
Mapped/Companion Address Spaces Overview
New Mapped/Companion Address Spaces

Mapped/Companion Address Spaces Details

Mapped/Companion Address Spaces Name	mapped
Enabled	☑
Nodeset XML File	StaticAddressSpace1.xml

Figure: New Mapped/Companion Address Spaces Overview - choose nodeset xml file with errors

Configuration parameters are described in the following table:

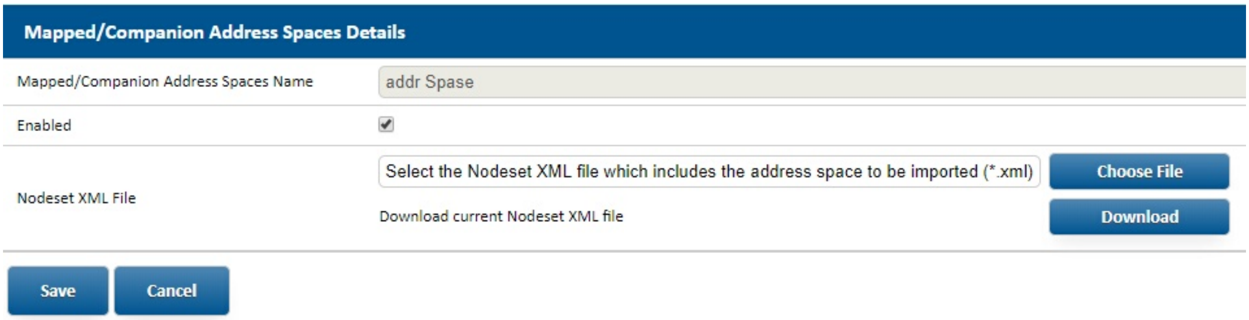
Parameter name	Default value	Value description

Mapped/ Companion Address Spaces Name	**not empty**	Defines the Mapped/Companion Address Spaces name as it will show up in the Mapped/Companion Address Spaces overview page.
Enabled	**Enabled**	Instructs the dataFEED Secure Integration Server to either enable (checked) or disable (unchecked) the currently configured Mapped/ Companion Address Spaces.
Nodeset XML File		One static address space shall be defined by one Nodeset2Xml file 235

Table: New Mapped/Companion Address Spaces Configuration parameters

4.7.5.4 Edit existing Mapped/Companion Address Spaces

Mapped/Companion Address Spaces Details is a view in the New Mapped/Companion Address Spaces page and provides a simple and intuitive interface for configuring a new or editing an existing Mapped/Companion Address Space.



Mapped/Companion Address Spaces Details

Mapped/Companion Address Spaces Name: addr Spase

Enabled: ☑

Nodeset XML File: Select the Nodeset XML file which includes the address space to be imported (*.xml)

Download current Nodeset XML file

Configuration parameters are described in the following table:

Parameter name	Default value	Value description
Mapped/ Companion Address Spaces Name	**not empty**	Defines the Mapped/Companion Address Spaces name as it will show up in the Mapped/Companion Address Spaces overview page.
Enabled	**Enabled**	Instructs the dataFEED Secure Integration Server to either enable (checked) or disable (unchecked) the currently configured Mapped/ Companion Address Spaces.
Nodeset XML File		One static address space shall be defined by one Nodeset2Xml file 235

Table: Edit Mapped/Companion Address Spaces Configuration parameters

Bottom page buttons actions:

Button	Action
Save	Once the configuration is finalized, clicking the **[Save]** button shall apply the newly configured/modified **Mapped/Companion Address Spaces**.
Cancel	Cancel the current **Mapped/Companion Address Spaces** configuration. **Beware all changes shall be lost !**

Table: Edit Mapped/Companion Address Spaces Buttons

4.7.6 Nodeset file

Configuring a Mapped Address Space is done through a Nodeset2 XML file, as defined by the schema at https://opcfoundation.org/UA/2011/03/UANodeSet.xsd, with the addition of a few dataFEED Secure Integration Server defined extensions.

Preparing such a nodeset can be done via a Model Designer tool, or even with a simple text editor.

A starting example can be obtained by downloading the nodeset 234 of the Mapped Address Space from the Demo configuration 87.

The nodeset file contains a description of the nodes in the Mapped Address Space. Each node is described there with its attributes and with the references linking it to other nodes. Compared to a standard Nodeset2 file as defined by OPC Foundation, there are 3 peculiarities that are described in the following sections:

1. Restrictions on namespace usage 235,
2. Forwarding variables 237,
3. Forwarding methods 238.

4.7.6.1 Restrictions on namespace usage

Due to the way UA Types are handled in dataFEED Secure Integration Server, the following restrictions applies all across dataFEED Secure Integration Server:

1. Type nodes and instance nodes cannot co-exist in the same namespace URI.
2. Instance nodes in different Mapped Address Spaces cannot have the same namespace URI.

By *type nodes,* we understand nodes that live somewhere under the Types folder; this include the actual types (VariableType, ObjectType, DataType, ReferenceType), as well as their associated nodes (instance declarations, custom structured data type dictionaries, etc).

By *instance nodes,* we understand the nodes that live somewhere under the Objects folder, and describe an actual instance (they are always nodes of class Variable, Object, or Method).

Restriction 1 means that a node ID of a type node and a node ID of an instance node must have distinct namespace URIs. In other words, any namespace in a dataFEED Secure Integration Server installation must be either a *type namespace*, containing only type nodes, or an *instance namespace*, containing only instance nodes. Restriction 2 means that the instance namespaces of two different Mapped Address Spaces must have distinct namespace URIs.

So, when creating a Mapped Address Space, the design process typically goes as follows:

1. Choose the namespace URIs for the type namespaces. The choice is typically limited here: First, the Companion Specs you may be using will define namespace URIs for their types. Second, if you aggregate underlying servers (through OPC UA Connections 158), all types defined on those servers are automatically imported and so they reserve the corresponding namespace URIs as type namespaces. Third, you can choose additional namespace URIs for the types defined in Mapped Address Space nodesets.
2. Define any types you need in the nodeset files for your Mapped Address Spaces. You can use the same namespace URIs in different Mapped Address Spaces and they may be the same as those used on underlying servers. However, if you use the same node ID in two Mapped Address Spaces or you use in a Mapped Address Space the same node ID as one on an underlying server, they must represent the same thing (the same type, or the same instance declaration, dictionary, etc).
3. For each Mapped Address Space you define, you must choose a set of namespace URIs for the instance nodes in that Mapped Address Space. Those namespace URIs cannot be used for anything else in the dataFEED Secure Integration Server installation.

Example: Looking at the demo configuration, the namespace URIs are:

```
<NamespaceUris>

    <Uri>http://industrial.softing.com/UA/MyMappedAS/Objects</Uri>

    <Uri>http://industrial.softing.com/UA/MyMappedAS/Variables</Uri>

    <Uri>http://industrial.softing.com/UA/MyMappedAS/Methods</Uri>

    <Uri>http://industrial.softing.com/UA/MyMappedAS/Custom</Uri>

    <Uri>http://industrial.softing.com/UA/MyMappedAS/
TypeDefinitions</Uri>

    <Uri>http://industrial.softing.com/UA/Refrigerator</Uri>

</NamespaceUris>
```

Namespace 0 is, as always, the UA namespace.

Namespace 6 (as referred in this nodeset), with URI="`http://industrial.softing.com/UA/Refrigerator`", is a type namespace from the underlying server. No nodes are declared in this namespace in this nodeset; it is legal to declare nodes, but only type nodes, not instances. It needs to be declared in the nodeset because it is referred in a DataType attribute.

Namespace 5, with URI="`http://industrial.softing.com/UA/MyMappedAS/TypeDefinitions`", is used for types declared in this nodeset file. There is an Object Type (LightRefrigeratorType) declared in this namespace, along with all its instance declarations.

Namespaces 1 through 4 are instance namespaces. Their corresponding URIs cannot be used anywhere else in the same dataFEED Secure Integration Server instance. It contains some Objects, Variables, and Methods. If you want to use the same nodeset for a distinct Mapped Address Space, the nodeset for that Mapped Address Space needs to, at the very list, change the URIs for those 4 namespaces to other 4, unique URIs.

4.7.6.2 Forwarding variables

Each variable defined in a Mapped Address Space must represent one variable that exists on some underlying server. That means that reading, writing, or subscribing to the Value of the variable in the Mapped Address Space actually reads, writes, or subscribes to the remote variable, on the underlying server. The mapping between the *local* variable (that in the Mapped Address Space, which is visible to an OPC UA Client) and the *remote* variable (that exist on the underlying server) must be configured in the nodeset2 XML. This is done through the Extension mechanism of the nodeset2.

The local variable definition needs an extension of the form (see full node set in the demo configuration 243):

```
<Extensions>

    <Extension>

        <Forward xmlns="http://softing.com/dataFEED"
nodeId="ns=1;i=10216" />

    </Extension>

</Extensions>
```

The `nodeId` attribute is the node ID of the remote node. However, the namespace index is to be interpreted in the context of a separate namespace URI table, located in the "global" extensions section of the nodeset file itself:

```
<Extensions>

    <Extension>

        <ForwardNamespaceUris xmlns="http://softing.com/dataFEED">

            <Uri>http://softing.com/dataFEEDSIS/nsuri?
conn=NetDemoServerConnection&amp;uri=http://test.org/UA/Data/</Uri>
                                  <!-- Forwarded NS Index = 1 -->

            <Uri>http://softing.com/dataFEEDSIS/nsuri?
conn=NetDemoServerConnection&amp;uri=http://opcfoundation.org/
Quickstarts/ReferenceApplications</Uri>  <!-- Forwarded NS Index = 2
-->

            <Uri>http://softing.com/dataFEEDSIS/nsuri?
conn=NetDemoServerConnection&amp;uri=http://industrial.softing.com/
UA/Refrigerator</Uri>               <!-- Forwarded NS Index = 3 -->


        </ForwardNamespaceUris>

    </Extension>

</Extensions>
```

Therefore, `ns=1;i=10216` is interpreted as the node, on an underlying server, that has the namespace URI `http://softing.com/dataFEEDSIS/nsuri?conn=NetDemoServerConnection&amp;uri=http://test.org/UA/Data/` and the identifier `i=10216`. Given the way the namespace URIs are created for instances on underlying server, this means a node that is located on the underlying server connected via a connection named `NetDemoServerConnection` and having, on that server, the namespace URI `http://test.org/UA/Data/`.

Note that only the Value goes to the underlying server. The designer of the Mapped Address Space has full control over all other attributes, as well as over the references linked to the variable. The designer can thus choose a different BrowseName, DisplayName, Description, as well as a completely different hierarchy of nodes, to be exposed in the Mapped Address Space.

The designer should make sure that the DataType, ValueRank, and ArrayDimensions of the local variable are identical to those attributes of the remote variable. dataFEED Secure Integration Server does not perform any validation on or against those attributes. This means that, if the local variable has DataType=string and the remote variable has DataType=int32, a client reading the Value of the local variable would expect a string and get an int32 instead (the value from the underlying server is forwarded without any check or restriction); in the opposite direction, the client may try to write a string, only to be rejected because the underlying server expected an int32.

Be careful with variables whose values are of type Node ID, Expanded Node ID, or Qualified Name. These values contain (or may contain, in the case of the Expanded Node ID), a namespace index. The meaning of a namespace index is defined only in the context of a known Namespace Array. The underlying server will interpret the namespace index in the context of its own Namespace Array, while the client connected to dataFEED Secure Integration Server will probably interpret the namespace index in the context of dataFEED Secure Integration Server's Namespace Array.

4.7.6.3 Forwarding method calls

Method calls on a *local* method are also forwarded to method calls to a *remote* method on an underlying server.

The configuration for the forwarding mechanism is similar to that for variables, which is described in the previous section.

However, a UA method call has 3 kinds of parameters:

1. the node ID of the actual method to be called;
2. the node ID of the object node on which the method is to be called (normally, this is the parent of the method node);
3. any parameters to the method call.

Therefore:

1. The method node description in the nodeset XML must have an Extension with a Forward element, like in the previous section, pointing to the node ID of the method on the underlying server.
2. The parent object of the method must also have an Extension with a Forward element, pointing to the node ID of the object, on the underlying server, that is the parent of the method.

Example from the demo configuration 243:

The method node itself:

```
<UAMethod NodeId="ns=2;i=14" BrowseName="5:OpenCloseDoor"
ParentNodeId="ns=1;i=1">
    ...
    <Extensions>
        <Extension>
            <Forward xmlns="http://softing.com/dataFEED"
nodeId="ns=3;i=14" />
        </Extension>
    </Extensions>
</UAMethod>
```

The parent node:

```
<UAObject NodeId="ns=1;i=1" BrowseName="5:Light Refrigerator"
ParentNodeId="ns=1;s=MyTestFolder_Refrigerators">
    ...
    <References>
        <Reference ReferenceType="HasComponent">ns=2;i=14</Reference>
        ...
    </References>
    <Extensions>
        <Extension>
            <Forward xmlns="http://softing.com/dataFEED"
nodeId="ns=3;i=1" />
        </Extension>
    </Extensions>
</UAObject>
```

This means any call to the local method *OpenCloseDoor* at node ID ns=2;i=14 (namespace URI="`http://industrial.softing.com/UA/MyMappedAS/Variables`") under *Light Refrigerator* at node ID ns=1;i=1 (namespace URI="`http://industrial.softing.com/UA/MyMappedAS/Objects`") will be forwarded to remote method *OpenCloseDoor* with node ID with namespace URI="`http://test.org/UA/Data/`" and identifier i=14 and with parent object *Refrigerator #1* with node ID on the same namespace URI and with identifier i=1.

By the way, the InputArguments property of the above local method is also forwarded to the InputArguments of the remote method (see the nodeset file for details). This is ok for this case, as all the method arguments are of standard UA types. If at least one argument is of a custom data type, the only way is to give the value is by creating the InputAgruments and/or OutputArguments node with a Value element with ListOfExtensionObject describing the names and types of the method arguments. The reason is that the DataType field is of type NodeId and, as said in the previous section, it is passed without any translation between the underlying server and dataFEED Secure Integration Server. For standard UA types, there is no problem, since their node IDs are all in namespace 0, and namespace 0 always stands for `http://opcfoundation.org/UA/`. With custom data types however, the node ID representing the DataType will live in some other namespace, and it is likely that the namespace will have distinct namespace indexes on dataFEED Secure Integration Server and on the underlying server.

As for the variables, be careful with input and output arguments of types NodeId, ExpandedNodeId, and QualifiedName. The namespace index in such a parameter is passed as-is between dataFEED Secure Integration Server and the underlying server. However, the client and the underlying server will interpret those namespace indexes in the context of distinct namespace arrays.

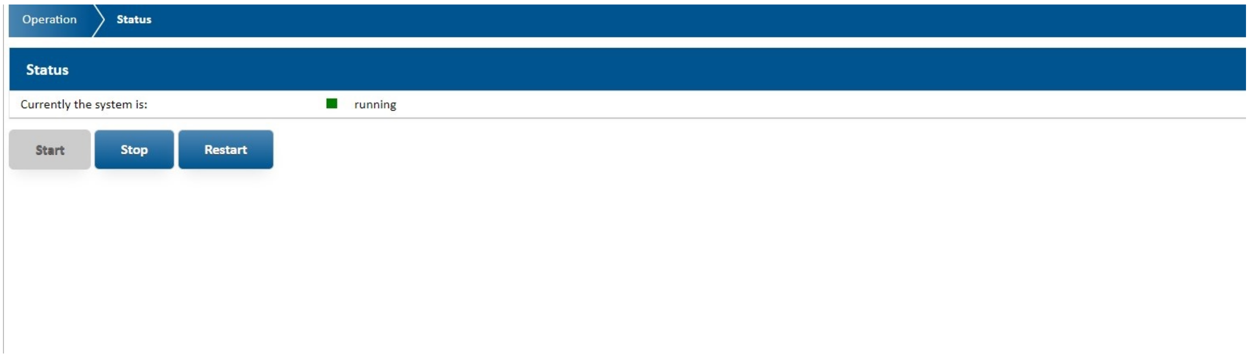
4.8 Operation

System operation menu entry provides a rapid and simple way to access the product logging facilities, files and support data as well as checking and changing the system's operation mode.

4.8.1 System States

1. System Operation Mode

To access system operation mode information or state page navigate to **Operation -> Status**. The user can visualize and change the system's state.



Currently the system is: 🟩 running

Figure: Operation, System Operation Status

In the **Status** area the running dataFEED Secure Integration Server state is visible. There are two stable system states:

State	Details
🟩 running	All component modules are loaded, configured and are running. Configuration is possible and is applied online.
🟥 halted	All component modules are loaded and are stopped. (eg: in care of) Configuration is possible and shall be applied after changing state to running. Some functionalities might not be available (eg: export address space, online browsing) All external data interfaces except the web interface are closed (eg: all OPC UA client and server connection will be stopped)

Table: Operation, System Operation Status

2. Changing System Operation Mode

Same state transitions are not possible, current state button is grayed out, preventing accidental sytem status change transitions.

Changing the system state is possible as described in the following table:

Current State	Desired State	Action Button	Details
🟩 running	🟥 halted	Stop	Stops the system and puts it in the halted state.
🟥 halted	🟩 running	Start	Starts the system and puts it in the running state.
🟩 running	🟩 running	Restart	Restarts the systems. Will create a stop/ start cycle.

Table: Operation, Changing System Operation Mode

4.8.2 Logs and Support

The log 78 files and additional information can be retrieved from the web interface in the **Operation** section.

4.8.2.1 Support Data

Navigating to **Operation -> Support** and clicking the **[Download]** button provides a simple way to fetch the support data for the running instance of the dataFEED Secure Integration Server archived and compressed in a zip format file named **SupportData.zip**.

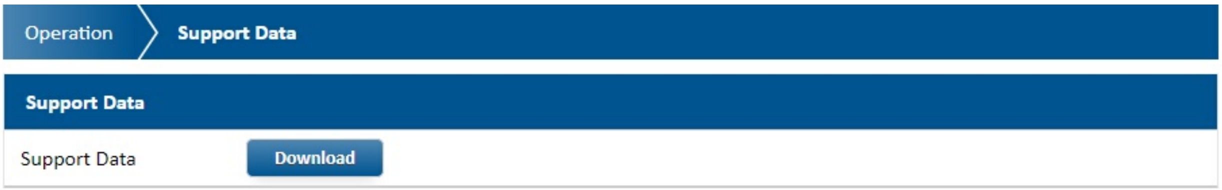
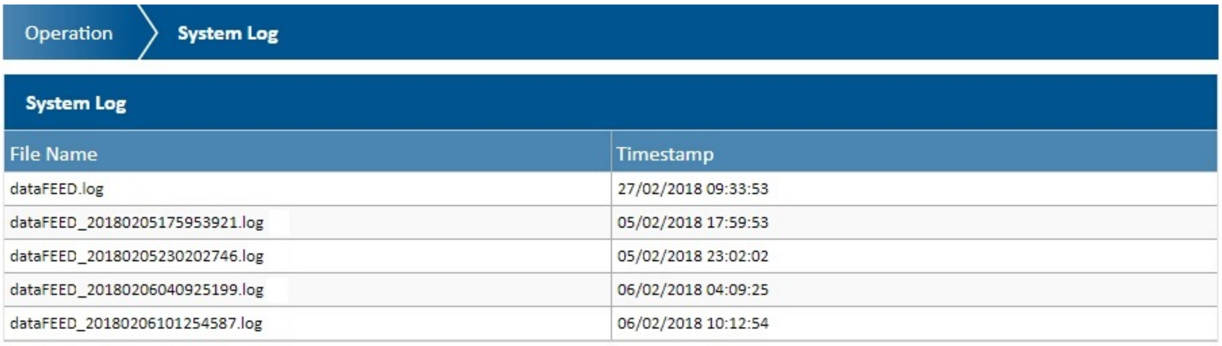


Figure: Operation, Support Data

4.8.2.2 System Log

System log files are available by navigating to **Operation -> System Log**. The page shall display all generated log files (currently used and old, based on the system log rotation configuration 78). Clicking on any row in the table describing the available files will trigger a download of the selected file.

The log file currently in use by the running instance of the dataFEED Secure Integration Server is named **dataFEED.log.** All other files in the form **dataFEED_<timestamp>.log** are older log files produced based on the log rotation configuration.

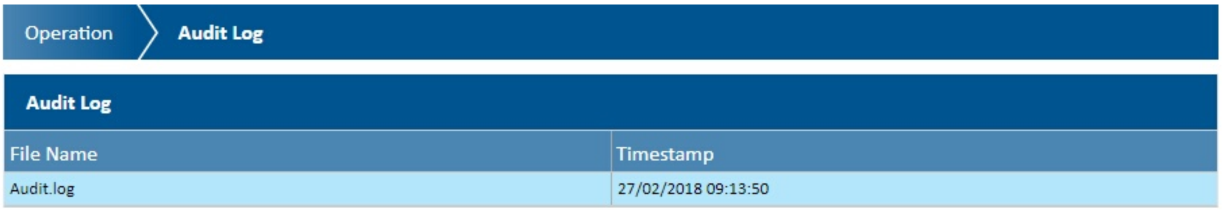


File Name	Timestamp
dataFEED.log	27/02/2018 09:33:53
dataFEED_20180205175953921.log	05/02/2018 17:59:53
dataFEED_20180205230202746.log	05/02/2018 23:02:02
dataFEED_20180206040925199.log	06/02/2018 04:09:25
dataFEED_20180206101254587.log	06/02/2018 10:12:54

Figure: Operation, System Log

4.8.2.3 Audit Log

Audit log produced files are available by navigating to **Opeartion -> Audit Log**. The page shall display all generated log files (currently used and old based on the audit log rotation configuration). Clicking on any row in the table describing the available files will trigger a download of the selected file.



File Name	Timestamp
Audit.log	27/02/2018 09:13:50

Figure: Operation, Audit Log

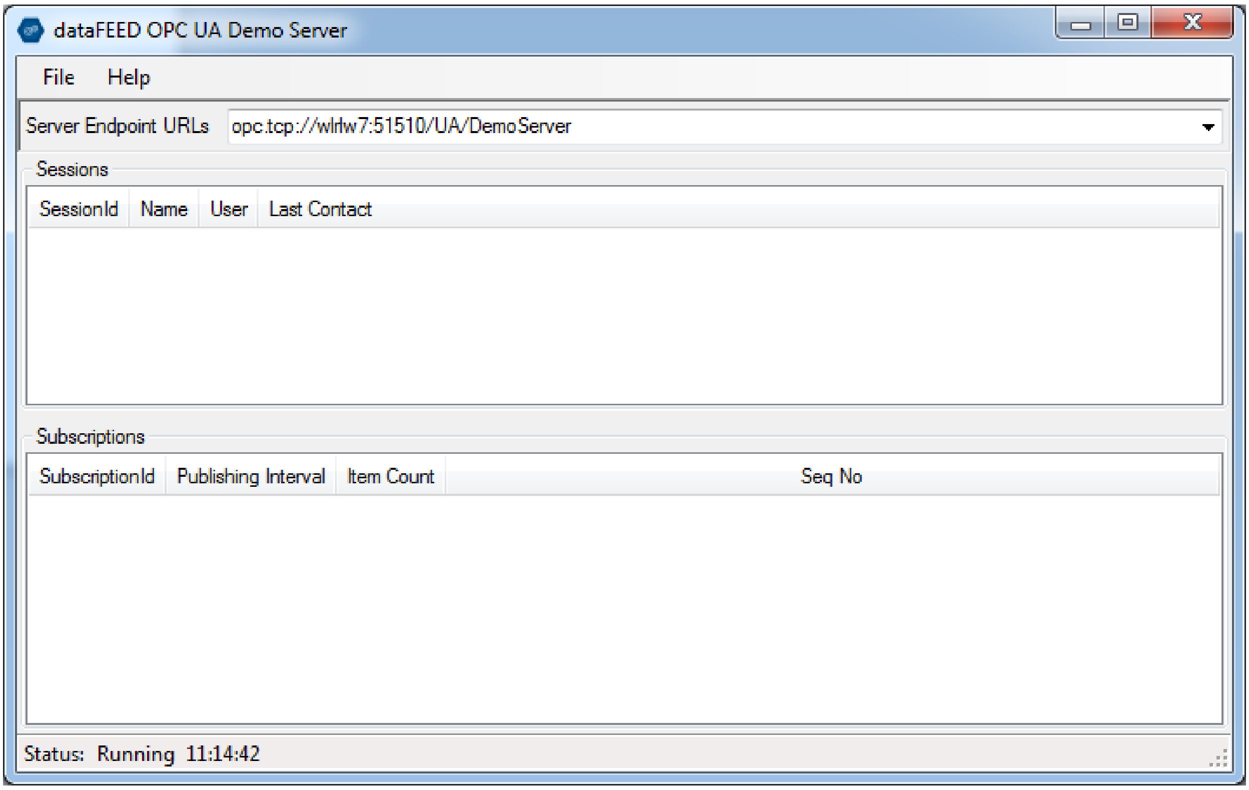
4.9 Demo configuration

This chapter describes a demonstrative configuration that can be loaded into dataFEED Secure Integration Server and demonstrates the basic functionality of the product.

Before proceeding with the information in this chapter please ensure that all the delivered features 12 where installed and a valid license was purchased and activated 55.

1. Start dataFEED OPC UA Demo Server

Locate and start the dataFEED OPC UA Demo Server application by navigating to **Start menu -> Softing -> OPC UA .NET Demo Server -> Softing OPC UA .net Demo Server:**



Server Endpoint URLs: opc.tcp://wlrlw7:51510/UA/DemoServer

SessionId	Name	User	Last Contact

SubscriptionId	Publishing Interval	Item Count	Seq No

Status: Running 11:14:42

Figure: Jump Start, UA Demo Server

Hint: When minimized the dataFEED OPC UA Demo Server can be accessed from the system tray:

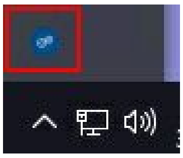


Figure: Jump Start, UA Demo Server Tray Icon

2. Configure dataFEED Secure Integration Server

Steps:

a. Open a supported web browser 10 then navigate to the configuration web page http://localhost:8099 and login using the default credentials (username: **admin** / password:**admin**)

b. Navigate to **Operation -> Status** and click the **[Stop]** button

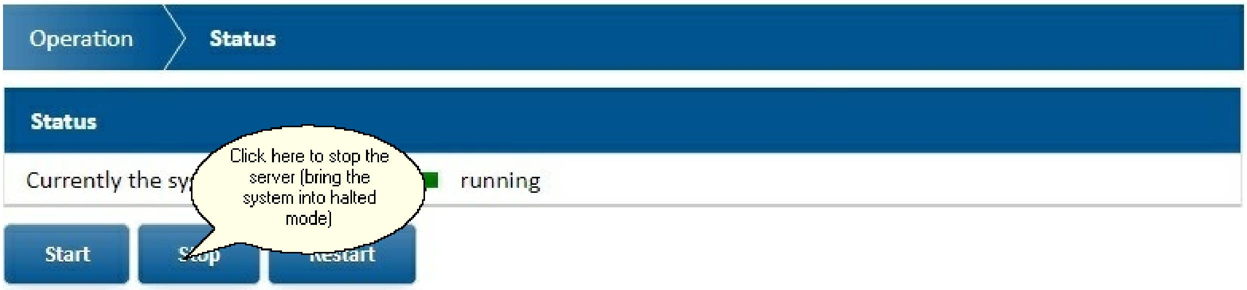

Operation
Status
Status
Currently the sy
running
Click here to stop the server (bring the system into halted mode)
Start
Stop
Restart

Figure: Demo configuration, System Status

c. Navigate to **General Settings -> Backup & Restore** and click the **[Restore Demo]** button in the **Restore Configuration** section

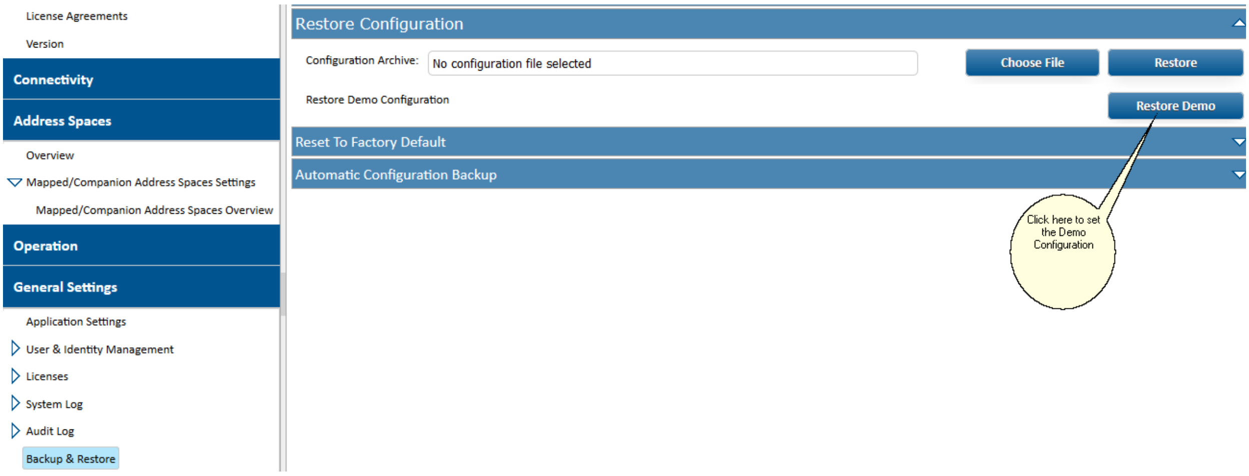
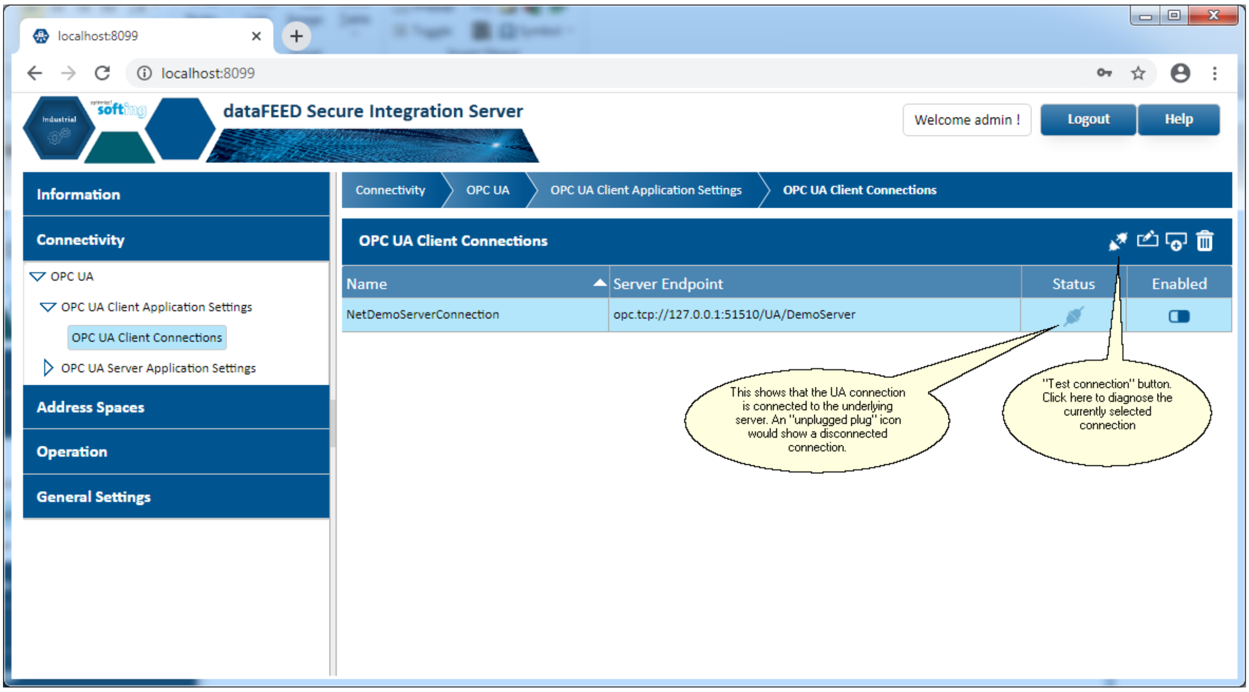


Figure: Jump Start, Backup & Restore

d. Acknowledge the successful restore

e. Navigate back to **Operation -> Status** and click the **[Start]** button

At this time the pre-configured dataFEED Secure Integration Server configuration should be running, and connected to the underlying dataFEED OPC UA Demo Server. To confirm this, navigate to the Connectivity -> OPC UA -> OPC UA Client Application Settings -> OPC UA Client Connections page and look at the Status column for the NetDemoServerConnection. If it shows disconnected, click on the "test connection" button to find out the issue.


localhost:8099
dataFEED Secure Integration Server
Welcome admin !
Logout
Help
Information
Connectivity
OPC UA
OPC UA Client Application Settings
OPC UA Client Connections
OPC UA Server Application Settings
Address Spaces
Operation
General Settings
Connectivity > OPC UA > OPC UA Client Application Settings > OPC UA Client Connections
OPC UA Client Connections

Name	Server Endpoint	Status	Enabled
NetDemoServerConnection	opc.tcp://127.0.0.1:51510/UA/DemoServer		

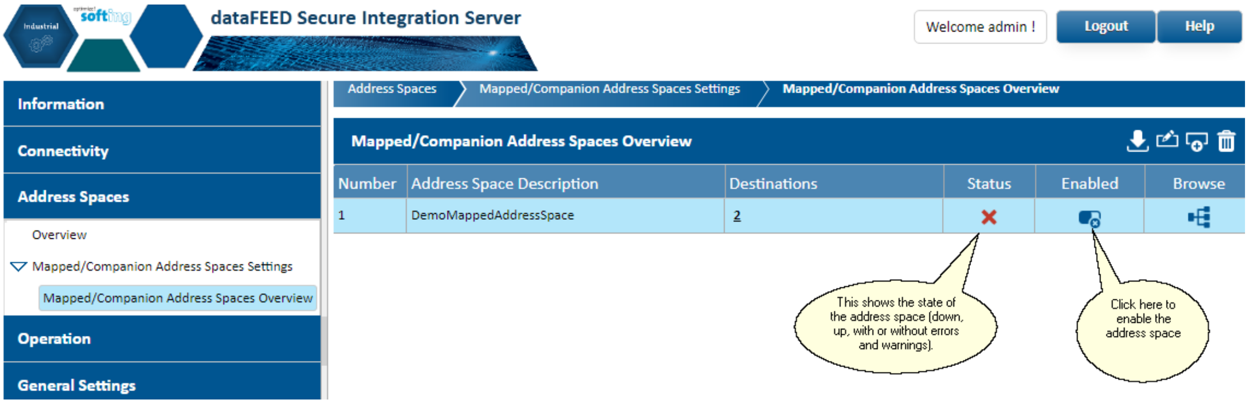
This shows that the UA connection is connected to the underlying server. An "unplugged plug" icon would show a disconnected connection.

"Test connection" button. Click here to diagnose the currently selected connection

Figure: Jump Start, connection to demo underlying server

3. Enable the Mapped Address Space

After having the connection to the underlying demo server up and waiting for a few seconds, it is time to enable the Mapped Address Space functionality. Navigate to Address Spaces->Mapped/ Companion Address Space Settings->Mapped/Companion Address Space Overview and click on the "switch" icon in the Enabled column for DemoMappedAddressSpace


dataFEED Secure Integration Server
Welcome admin !
Logout
Help
Information
Connectivity
Address Spaces
Overview
Mapped/Companion Address Spaces Settings
Mapped/Companion Address Spaces Overview
Operation
General Settings
Address Spaces > Mapped/Companion Address Spaces Settings > Mapped/Companion Address Spaces Overview
Mapped/Companion Address Spaces Overview

Number	Address Space Description	Destinations	Status	Enabled	Browse
1	DemoMappedAddressSpace	2	✗		

This shows the state of the address space (down, up, with or without errors and warnings).

Click here to enable the address space

Figure: Jump Start, enabling mapped address space

Note: if the mapped address space is brought up before the connections to the underlying servers, that are referred in the mapped address space, are up, you can get some warnings and errors. Those complain about nodes and namespace URIs that are not available — that's because those nodes or namespace URIs are on the underlying server. In such a case, disabling and re-enabling the mapped address space resolves those issues.

4. Configure dataFEED OPC UA Client

It is time to setup the endpoints and the dataFEED OPC UA Client to access the content of the dataFEED OPC UA Demo Server.

Steps:

a. Locate and start dataFEED OPC UA Client by navigating to it **Start menu -> Softing -> OPC UA Client -> Softing OPC UA Client.**

b. Double Click the **Project** area to add a new session:

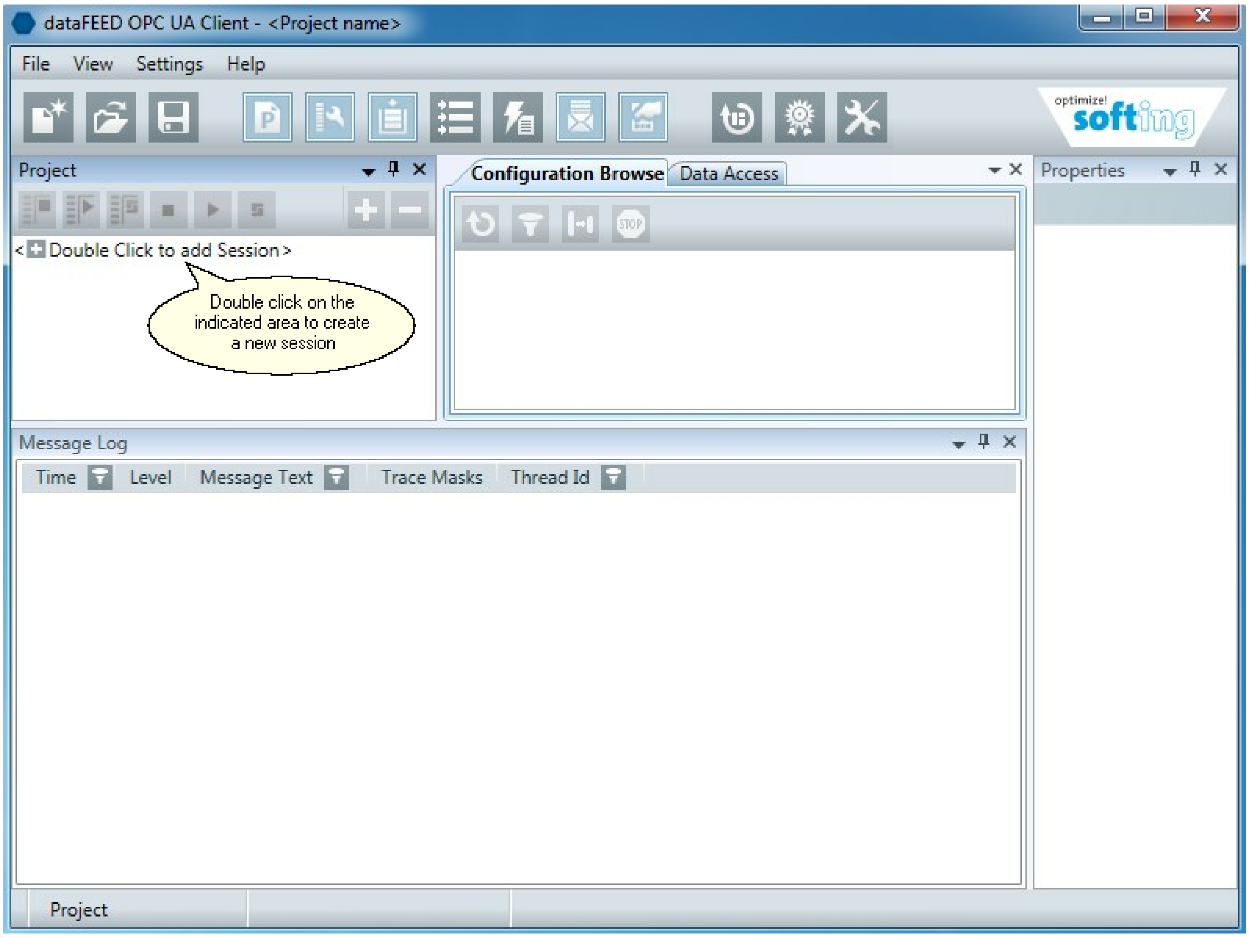
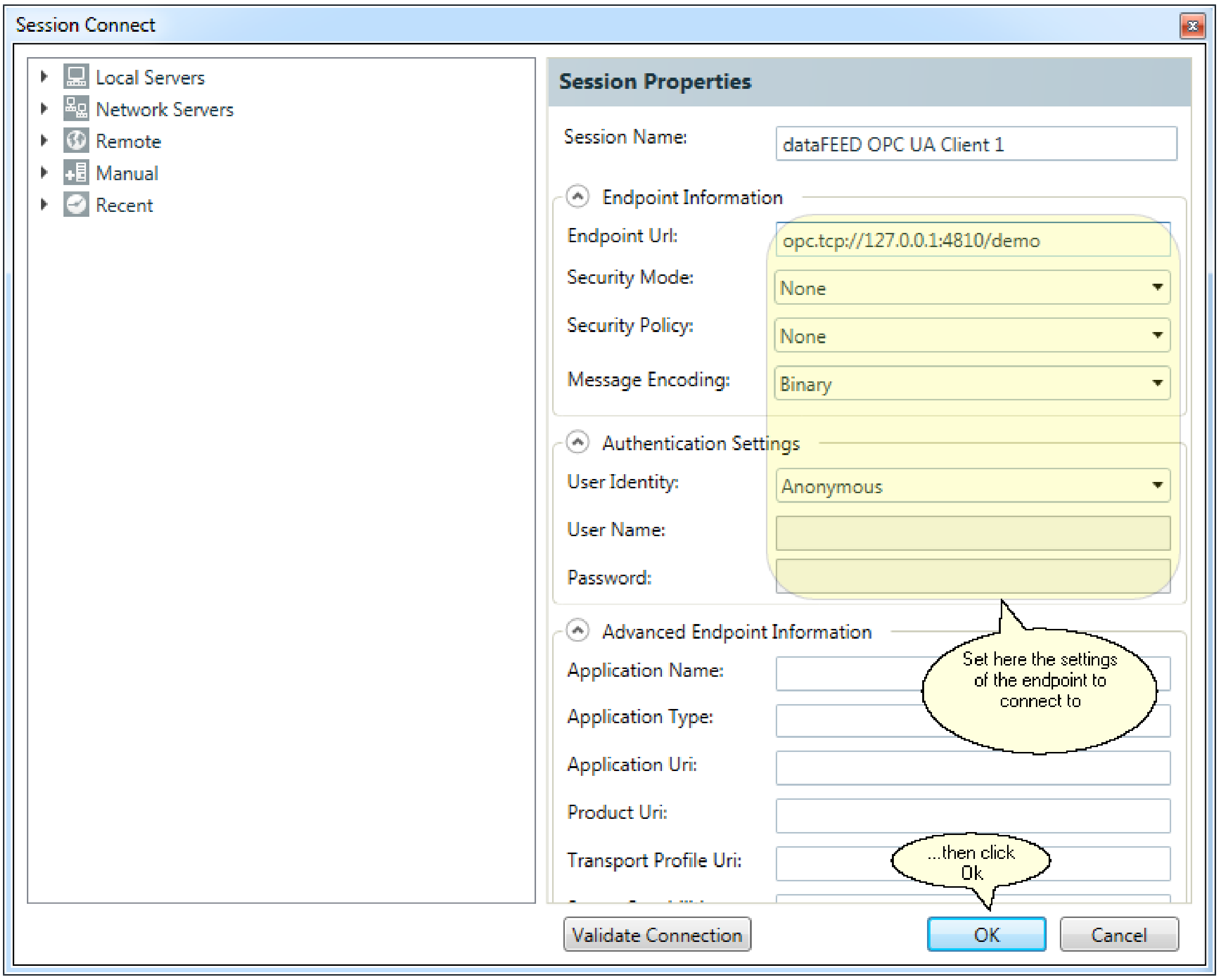


Figure: Jump Start, Softing OPC UA Client

c. Connecting to a dataFEED Secure Integration Server exposed endpoint by filling in the endpoint details in the session connect window:



Session Connect

- Local Servers
- Network Servers
- Remote
- Manual
- Recent

Session Properties

Session Name: dataFEED OPC UA Client 1

Endpoint Information

Endpoint Url: opc.tcp://127.0.0.1:4810/demo

Security Mode: None

Security Policy: None

Message Encoding: Binary

Authentication Settings

User Identity: Anonymous

User Name:

Password:

Advanced Endpoint Information

Application Name:

Application Type:

Application Uri:

Product Uri:

Transport Profile Uri:

Figure: Jump Start, Softing OPC UA Client, Session Properties

Endpoint Information	Example value	Details
Endpoint URL	**opc.tcp://127.0.0.1:4810/ demo**	Local **dataFEED Secure Integration Server** configured endpoint. This endpoint URL matches endpoint named **DemoMappedAddressSpace.**
Security Modes	**None**	*None* (no security) is accepted and shown in the previous screenshot. However, *Sign* and *SignAndEncrypt* are also supported.
Security Policy	**None**	
message encoding	**Binary**	Only binary is supported.

Authentication Settings	Example value	Details
User Identity	**Anonymous**	For this example, we use Anonymous.
User Name		
Password		

Table: Jump Start, Softing OPC UA Client, Session Properties Fields

When all details are filled in correctly click **[OK].**

d. At this stage the dataFEED OPC UA Client should successfully connect to dataFEED Secure Integration Server .

Ready

When all the previous steps are completed, access to the endpoint and its address space is granted. With the aid of the dataFEED OPC UA Client it is easy to perform various actions like browse, read, write or subscribe to nodes.

Softing Industrial Automation GmbH

Richard-Reitzner-Allee 6
85540 Haar / Germany
http://industrial.softing.com

Tel: + 49 89 45 656-0
Fax: + 49 89 45 656-488
info.automation@softing.com