RTCP

RTCP User Manual

Version 2.0 - 01-12-2020

Table of contents

1 Introduction

The Real-Time Communication Platform enables the management of gateways and endpoints and their real-time communication flows. An important component of the platform is the management portal. The goal of this user guide is to explain its features and its interaction with the gateways.

It is imperative that the business processes and the technical requirements are well understood for the correct interpretation of this user manual. Therefore, preliminary reading of aFRR balancing services - Explanatory and technical guide for gateway management is required.

2 User and access management

2.1 Introduction

The Real-Time Communication Portal has foreseen a setup with company accounts that can contain multiple users, with different potential permission profiles.

To setup your account, you need to register a company account and subsequently register additional users to this account, if needed.

When requesting an account for your organization, the information of the initial 'main user' will be requested. When the account registration is successful, this main user is simultaneously created with the account and will have an admin permission profile allowing the administration of additional users.

Different types of users can be managed with different permissions. In the following matrix, the permission profiles and corresponding permissions are shown:

		Gateway Manager		
	Admin (A) / Normal (N) / Read-only (R)	A	N	R
Section	**Permission**			
My Account	**UI - Account subtab**			
	Edit account			
	Add user			
	Edit personal user information (except 2FA & Profile)			
	Edit personal user information (2FA & Profile)			
	UI - User subtab			
	Edit user (other)			
	Deactivate user			
	Reactivate user			
Platform Accounts	**UI - Account subtab**			
	Edit account			
	Manage users			
	Manage account request			
	Deactivate account			
	UI - User subtab			
	Edit user			
	Deactivate user			
	Reactivate user			
Data Sources	**UI - Gateway subtab**			

	Add gateway			
	Modify gateway information			
	Request certificate token			
	Test connection			
	Retrieve encryption key			
	Deactivate gateway			
	Reactivate gateway			
	UI - Model subtab			
	Add a GW model			
	Edit a GW model			
	Consult documentation (not update)			
	Consult documentation (update)			
	Deactivate model			
	Reactivate model			
	UI - Endpoint subtab			
	Add endpoint			
	Takeover and endpoint			
	Edit an endpoint			
	Link endpoint to gateway			
	Decouple from gateway			
	Replace gateway			
	Deactivate an endpoint			
Communication	**UI - Message log**			
	UI - Message format			

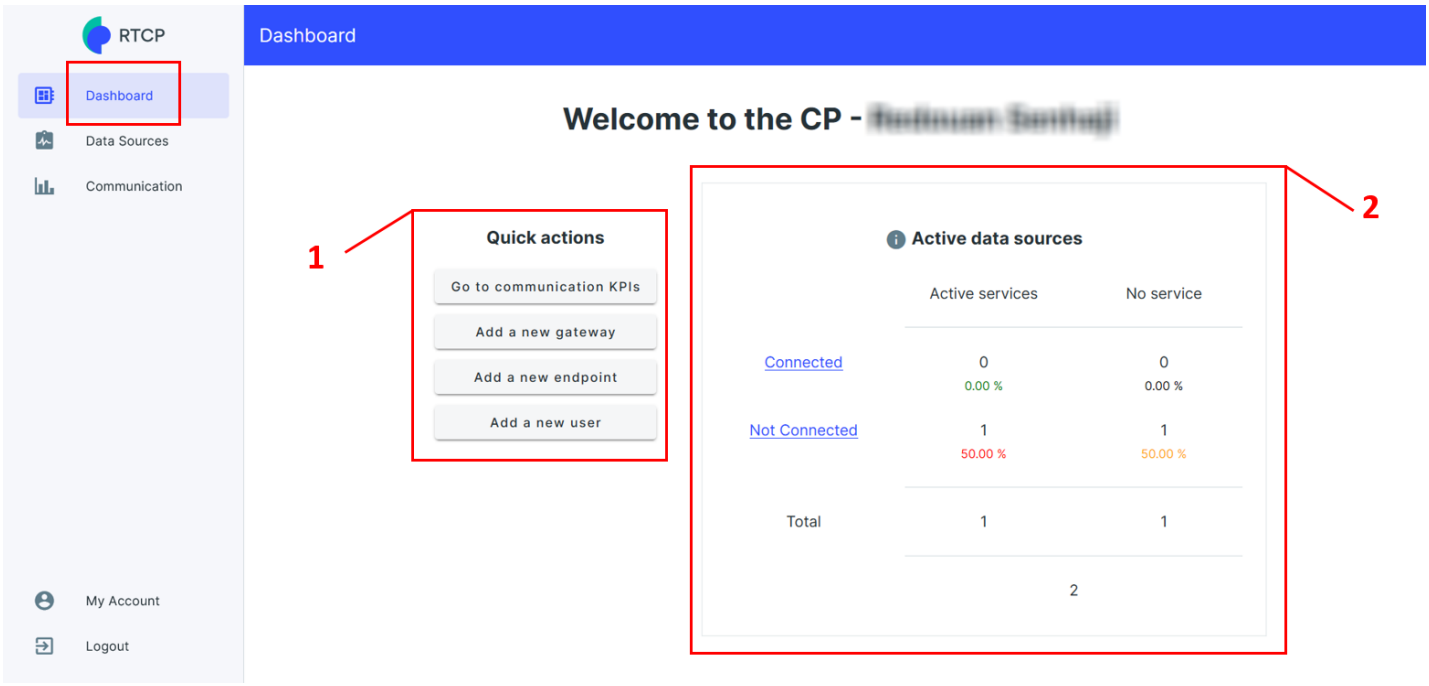
In the following sections, we will discuss:

- User interface
- How to manage an account
- How to manage a user

2.2 User Interface

- The section Dashboard

The user will land on the dashboard page after logging in where access to quick actions and KPIs on the data source portfolio are provided.



1. These buttons allows you to perform quick actions:
   - Go to communication KPIs
   - Add a new gateway
   - Add a new endpoint
   - Add a new user

2. This dashboard gives you an overview of the active data sources (gateways that are linked to endpoints) with the possibility to drill to those sections with applied filters.
   a. Connected = gateway is in connected state
   b. Not connected = gateway is not in connected state
   c. Active service = endpoint has an active routing service
   d. No active service = endpoint has no active service

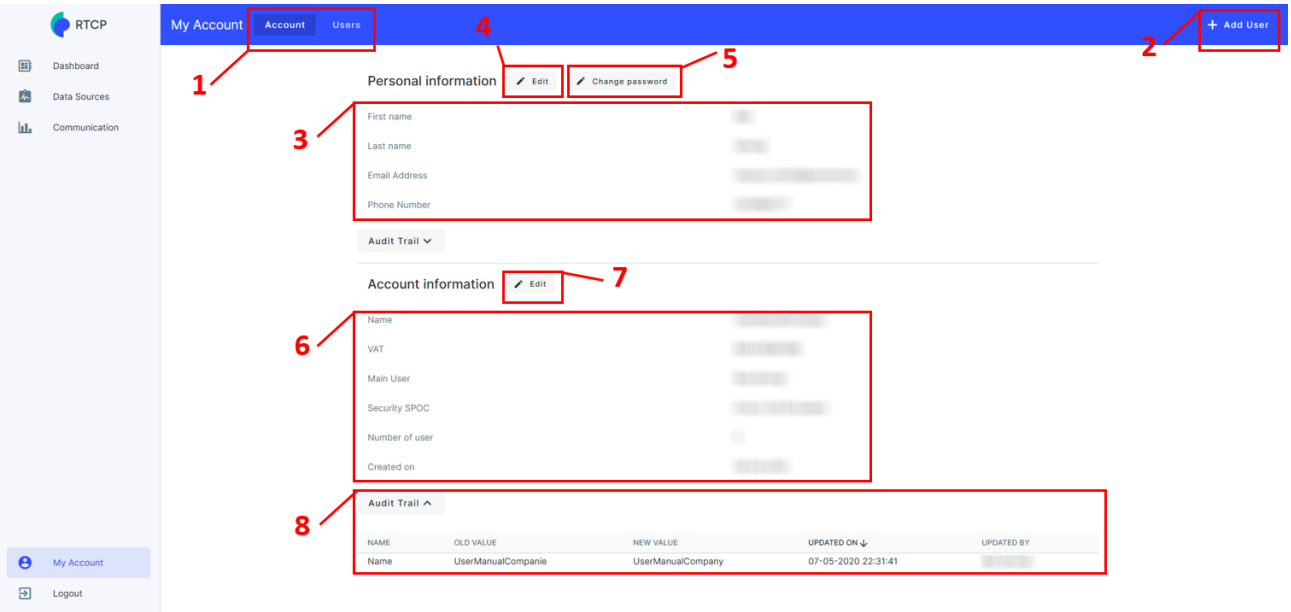
   The colors indicate the degree of possible issues. It is expected that the gateway is in a connected state when it is linked to an endpoint with an active service as recurrent heartbeats are sent in that case.

2.2.1 Account

The section My Account allows you to manage your account and users and it consists of two tabs:

- The tab Account
- The tab Users

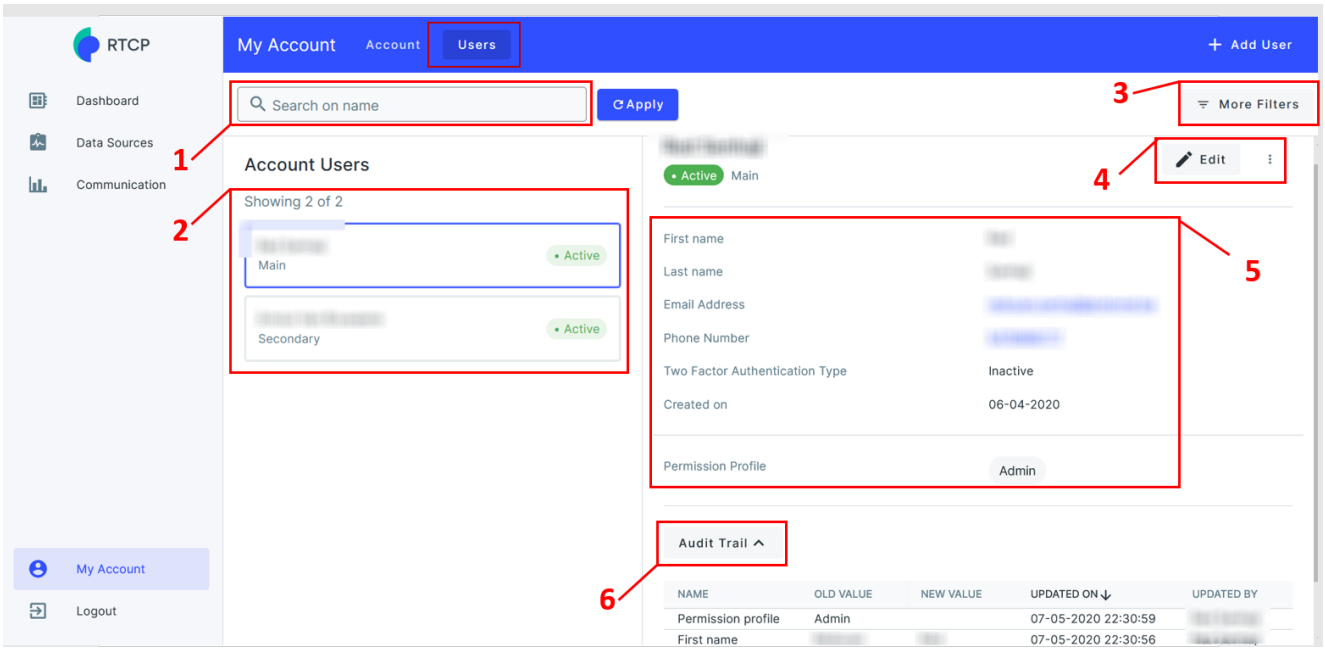
The tab **Account** consists of the following sections:



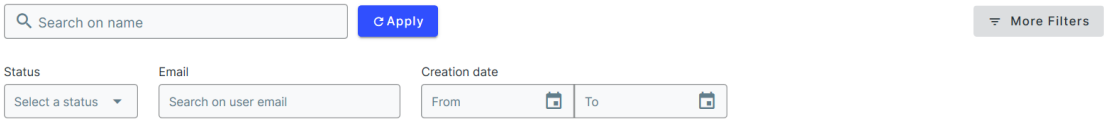
1. A **section** typically consists of different section **tabs**. The two tabs under the section **My Account** are:
   - Account
   - Users
2. The tab action **Add User** to register an additional user
3. In the **Personal Information**, you can consult personal details of the logged in user
4. The button **Edit** in the subsection **Personal information** allows you to modify the user information
5. The button **Change Password** allows you to modify the current user password
6. In the subsection **Account information**, you can consult the account details of your company
7. The button **Edit** in the **Account information** subsection allows you to modify information of your account as well as the main user and security SPOC
8. In the subsection **Audit Trail**, you can consult the updates of the entity you have modified as well as the most important relationship changes this entity has with another entity.

2.2.2 Users

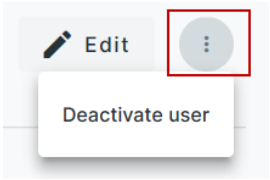
The tab **Users** consists of the following subsections:



1. The **search bar** where you can search the users you have created
2. A list containing the users you created
3. The button **More Filters** which allows you to add more filters



4. The button **Edit** which allows you to edit the information of the selected user. Next to the button Edit, the **3 dotted button** allows you to perform additional actions:



5. In this subsection, you can consult the **details** of the selected user
6. In the subsection **Audit Trail**, you can consult the updates of the entity you have modified as well as the most important relationship changes this entity has with another entity.

2.3 How to manage an account

In this chapter, we will discuss the following topics:

- How to add a new user
- How to change a main user and Security SPOC

2.3.1 How to add a new user

To add a new user:

1. Go to the section **My Account**
2. Click on the button **Add User**

The system opens a pop-up screen for user registration

3. Enter the necessary details
4. Click on the button **Edit** to select the Permission Profile
5. Select the **Permission Profile** of your choice and click on Back
6. Once all the fields are filled in, click on **Submit**

Once you have clicked on Submit, the system will send an email to the added user to finalize the user creation by confirming the email address. An email with a temporary password will subsequently be sent for logging in.

Note:

Only users with an admin profile can add new users.

2.3.2 How to change a main user and security SPOC

A main user must always have the 'admin' permission profile and he can never be deactivated. The main user can be changed, but only by a user that also has admin rights.

To be able to register a gateway model, a security SPOC must first be assigned. This user can be contacted in case of security related questions.

To change a main user and security SPOC,

1. Go to the section **My Account**
2. Click on the button **Edit** in the subsection **Account Information**
3. Select the main user of your choice in the field **Main User**
4. Select the Security SPOC of your choice in the field **Security SPOC**
5. Click on **Save**

2.4 How to manage a user

In this chapter, we will discuss the following topics:

- How to change your password
- How to modify the two factor authentication (2fa)
- How to modify the user permission profile
- How to deactivate/reactivate a user

2.4.1 How to change your password

To change the password of a user,

1. Go to the section **My Account**
2. Click on the button **Change password** in the subsection Personal Information
3. As a result, the system opens a pop-up window where you have to enter a new password and confirm your new password
4. Click finally on **Continue** to confirm

2.4.2 How to modify the two-factor authentication

The system allows the activation of different types of two-factor authentication. This can be applied to users of your organization by admin users. Note that this is only possible when the user is in an active status.

The two-factor authentication is a method of confirming users' claimed identities by using a combination of two different factors.

The platform provides the option to have a code sent to your mobile phone or to your e-mail address.

To modify the two-factor authentication:

1. Go to the section **My Account**
2. Click on the button **Edit** in the subsection Personal Information
3. Click on the button **Edit** in the field 2FA
4. Select the option of your choice:
   - **Inactive**: this means there is no two-factor authentication upon signing in
   - **SMS**: If you select this option, you have to enter your mobile phone number in order to receive the code when logging in
   - **Email**: If you select this option, you have to enter your e-mail address in order to receive the code when logging in
5. Click on **Back** and then on **Submit**

2.4.3 How to modify the user permission profile

To modify the user permission profile:

1. Go to the section **My Account**
2. Click on the button **Edit** in the subsection Personal Information
3. Click on the button **Edit** in the field Permission profile(s)
4. Select the option of your choice:
   - **Admin**: An admin user can read and edit all relevant information for his company including full account and user management.
   - **Normal**: A normal user can read and edit most relevant information for his company.
   - **Read-only**: A read-only user can read all relevant information for his company. No write operation are allowed except for own user information modifications.
5. Click on **Back** and then on **Submit**

Note: The change will take effect upon (re)logging in with the concerned account.

2.4.4 How to deactivate/reactivate a user

To deactivate a user:

1. Go to the section **My Account**
2. Go to the tab **Users** on top of the screen
3. Select the user you want to deactivate/reactivate
4. Click on the **dots** on the right side of the button Edit
5. If the user is activated click on **Deactivate user**
   If the user is deactivated then click on **Activate user**

When confirming a deactivation, the user's account will be blocked from accessing the portal.

3 Data Source management

3.1 Introduction

This section enables the user to setup gateways and endpoints that will form the data source that should send the metering data to the platform. A data source is formed when a gateway is linked to an endpoint, which is the digital representation of the delivery point where the gateway is installed.

The system foresees separate communication channels for gateway only (heartbeat & encryption messages) and for the full data source (metering communication). More on communication in the next chapter.

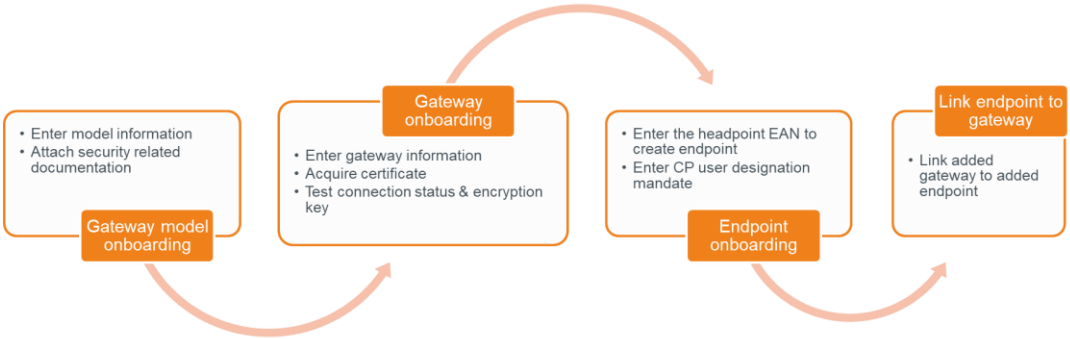
To setup a data source, there are multiple processes to go through:

1. Setting up a functioning gateway
    a. Onboard a gateway model
    b. Onboard a gateway
    c. Acquire and configure the digital certificate of your gateway
    d. Test its connection to see if it is able to respond to a heartbeat message
    e. Test the retrieval of a dummy encryption key
2. Setting up an endpoint
    a. Sign the CP user designation with the grid user
    b. Onboard the endpoint and attach the CP user designation

Note that there is no specific sequence imposed in setting up either the gateway or the endpoint. When both of these data source elements (gateway and endpoint) are setup, we can link them together to form an active data source:

3. Link endpoint to gateway
    a. Install the gateway at the delivery point
    b. Select the delivery point's respective endpoint and link it to the gateway

See summary of applicative steps to undertake in the image below:

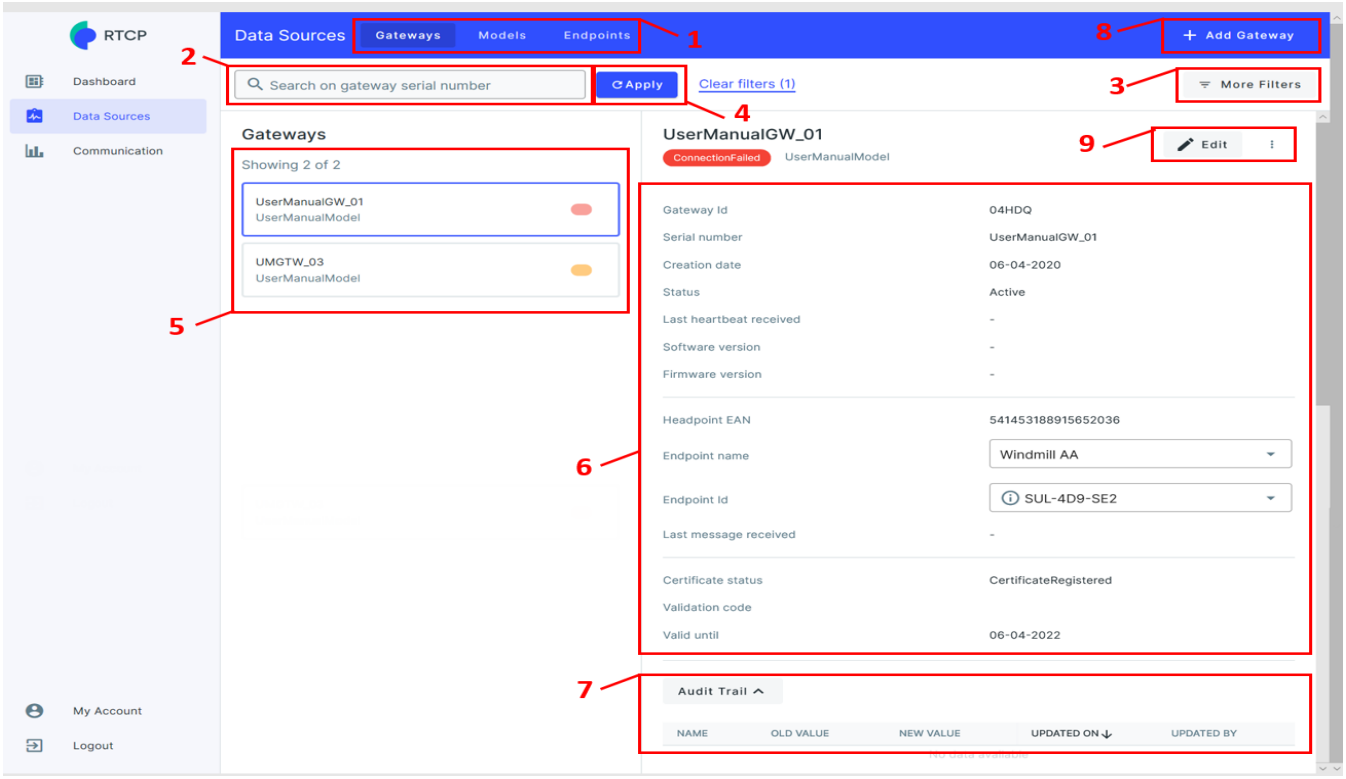


In the following chapter, we will discuss the following topics:

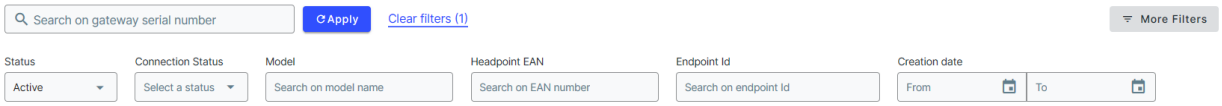
- User interface
- How to manage a model
- How to manage a gateway
- How to manage an endpoint

3.2 User Interface

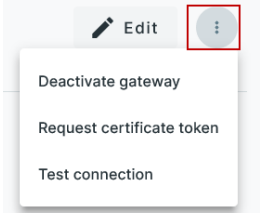
The Data Sources section opens immediately on the Gateways tab. The data source tabs share the same screen composition and will always show following elements:



1. The **section** consists of different section **tabs**.
   - Gateways
   - Models
   - Endpoints
2. The basic **search bar** to query on data source Ids
3. The button **More Filters** which allows you to add more filters:



4. The button **Apply** allows you to run the query with applied filters and can also be used to refresh all the data in the tab
5. The queried result list
6. In this information window you can see the **details** of the **selected record**
7. In the **Audit Trail**, you can consult the history of updates done on the entity as well as the most important relationship changes this record has with another entity.
8. **Tab actions** can be executed without focusing on a certain record
9. **Record based actions** are performed on the selected record in the result list. Besides editing, the 3 dotted button allows you to perform additional actions:



3.3 How to manage a Model

In this chapter, we will discuss the following topics:

- How to add a model
- How to modify a model
- How to modify deactivate/reactivate a model

3.3.1 How to add a Model

It is required to first assign a security SPOC for your account who will be contacted in case of questions on gateway models and security related issues in order to add a model.

To add a model,

1. Go to the section **Data Sources**
2. Go to the tab **Models** on top of the screen
3. Click on the button **Add Model**
4. Enter the **Model Name** and **Manufacturer**
5. Click on **Submit**
6. The model is now created and will have a state **Documentation required**.
7. Add all required security related documentation
8. Click **Submit**

As a result, a new active model will be added to the list of models and can be used to create gateways.

Note:

When not all documentation is uploaded at once, the already uploaded documentation will remain saved and the model is in 'Documentation required' state until all documents are uploaded.

3.3.2 How to modify a Model

To modify a model,

1. Go to the section **Data Sources**
2. Go to the tab **Models** on top of the screen
3. Select the model you want to modify
4. Click on the button **Edit**
5. Modify the necessary information
6. Click on **Confirm**

3.3.3 How to deactivate/reactivate a Model

To deactivate/reactivate a model,

1. Go to the section **Data Sources**
2. Go to the tab **Models** on top of the screen
3. Select the model you want to modify
4. Click on the **dots** on the right side of the button **Edit**
5. If the model is activated click on **Deactivate model**

   If the model is deactivated then click on **Activate model**
6. In the pop-up, click on **Yes** to confirm your choice

Note:

1. A model can only be deactivated when there are no active gateways of that model
2. When deactivating a model, no new gateway of that model can be created

3.4 How to manage a Gateway

In this chapter, we will discuss the following topics:

- How to create a gateway
- How to modify a gateway
- How to request a certificate token
- How to test the gateway connection
- How to retrieve an encryption key
- How to deactivate/reactivate gateway

3.4.1 How to create a Gateway

To create a gateway,

1. Go to the section **Data Sources**
2. Go to the tab **Gateways** on top of the screen
3. Click on the button **Add Gateway**
4. Enter the **Serial Number** and chose an **active Model**
5. Click on **Submit**

As a result, a new gateway will be added to your list of gateways.

Note:

Before you can create a gateway, you should first have a model in an active state.

3.4.2 How to modify a Gateway

To modify a gateway,

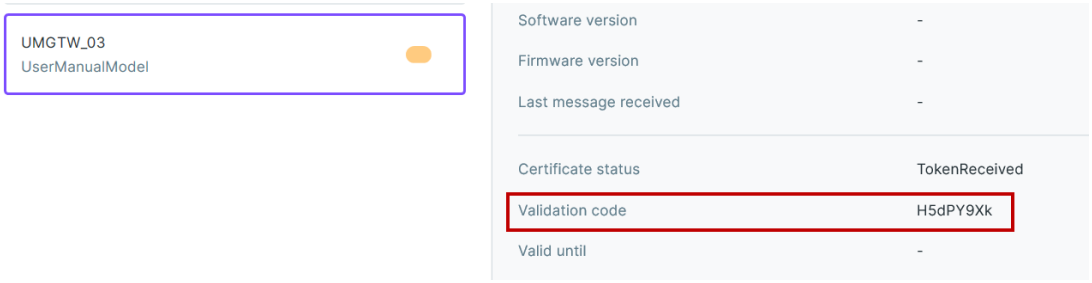
1. Go to the section **Data Sources**
2. Go to the tab **Gateways** on top of the screen
3. Select the gateway you want to modify
4. Click on the button **Edit**
5. Modify the fields of your choice
6. Click on **Submit**

3.4.3 How to request a certificate token

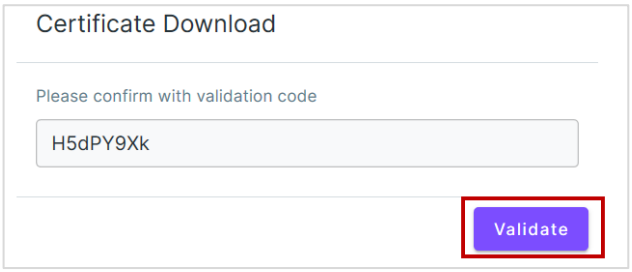
To request a certificate token,

1. Go to the section **Data Sources**
2. Go to the tab **Gateways** on top of the screen
3. Select the gateway for which you want to request a certificate token
4. Click on the **3 dotted button** and click on **Request certificate token**
5. An email will be sent and the certificate status is set to **TokenReceived**
6. The next step is to **download the certificate** token which is made available through a link in the e-mail you just received

Once you have clicked on this link, the system will open a new window where you have to enter the **validation code** made available in the information screen of the gateway:



7. Enter the validation code and click on **Validate**



Once you have clicked on Validate, a message will indicate that the download is ongoing. Once the download is finished, you can install the certificate.

Once the certificate is acquired, you will see the Certificate status of the gateway change to **CertificateRegistered**.

Tip:

You can see the status of your request in the information screen of the gateway:

Following states will be visible:

- TokenRequested – token is requested to the Public Key Infrastructure
- TokenReceived – email with token link is sent to the user
- TokenRejected – download failed (5 faulty attempts)
- CertificateRegistered – download succesful

3.4.4 How to test the Gateway connection

More context on this and the next subchapter can be found in the introduction of the communication chapter.

Once you have required the certificate token for your gateway, you can test the gateway connection.

To do so,

1. Go to the section **Data Sources**
2. Go to the tab **Gateways** on top of the screen
3. Select the gateway for which you want to test the connection
4. Click on the **3 dotted button** and click on **Test connection**

Once you have clicked on it, a pop-up indicates you that the request of testing the connection has been sent. A heartbeat message was sent from the platform on the message queue where the gateway can pick it up and put its reply on.

Tip:

Refresh the webpage to see the status change.

If the connection test **failed**, the label on top of the screen will be **red** with the text **ConnectionFailed**. This will happen when no answer is received after 90 seconds.

If the connection test **succeeded**, the label on top of the screen will be **green** with the text **Connected**.

3.4.5 How to retrieve an encryption key

In order to make sure the gateway has the correct logic to interpret encryption key messages and encrypt a message body with the received encryption key, an action on gateway level is provided.

Here you can either request the latest encryption keys (only for GWs linked to endpoints with active services) or a dummy encryption key that can be used for a standalone gateway.

1. Go to the section **Data Sources**
2. Go to the tab **Gateways** on top of the screen
3. Select the gateway for which you want to test the connection
4. Click on the **3 dotted button** and click on **Retrieve encryption key**
5. Select the desired option and confirm

An encryption key message will be sent by the platform to the concerning gateway(s) and chosen encryption key version.

3.4.6 How to deactivate/reactivate a Gateway

To deactivate/reactivate a gateway,

1. Go to the section **Data Sources**
2. Go to the tab **Gateways** on top of the screen
3. Select the gateway you want to deactivate/reactivate
4. Click on the **dots** on the right side of the button **Edit**
5. If the gateway is activated click on **Deactivate gateway**
   If the model is deactivated then click on **Activate gateway**
6. In the pop-up, click on **Yes** to confirm your choice

3.5 How to manage an Endpoint

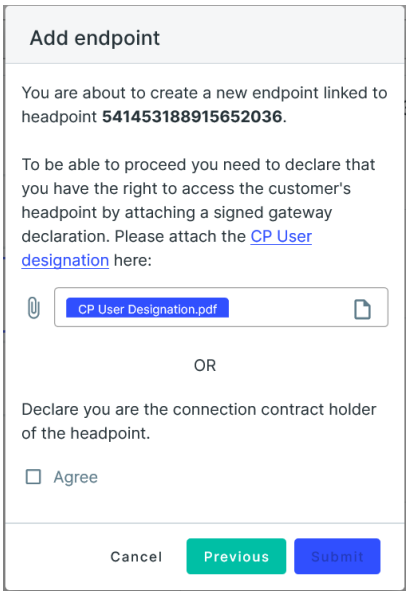
In this chapter, we will discuss the following topics:

- How to add an endpoint
- How to modify an endpoint
- How to deactivate/reactivate an endpoint
- How to move an endpoint
- How to link an endpoint to a gateway
- How to decouple an endpoint from a gateway
- How to replace a gateway

3.5.1 How to add an Endpoint

To add an endpoint,

1. Go to the section **Data Sources**
2. Go to the tab **Endpoints** on top of the screen
3. Click on the button **Add Endpoint**
4. Enter the **Headpoint EAN** and the **Endpoint friendly name** and chose the concerned system operator
5. Click on **Next**
6. Add the **CP User Designation Document** or declare that you are the connection contract holder of the headpoint by ticking the checkbox **Agree**



7. Click finally on **Submit** to confirm your choice

As a result, the CP user designation is sent to the concerning system operator for review. The endpoint is immediately added to the list and can be used.

3.5.2 How to modify an Endpoint

To modify a model,

1. Go to the section **Data Sources**
2. Go to the tab **Endpoints** on top of the screen
3. Select the endpoint you want to modify
4. Click on the button **Edit**
5. Modify the necessary information
6. Click on **Confirm**

3.5.3 How to deactivate/reactivate an Endpoint

To deactivate/reactivate an endpoint,

1. Go to the section **Data Sources**
2. Go to the tab **Endpoints** on top of the screen
3. Select the endpoint you want to deactivate/reactivate
4. Click on the **dots** on the right side of the button **Edit**
5. If the endpoint is activated click on **Deactivate endpoint**

   If the endpoint is deactivated then click on **Activate endpoint**
6. In the pop-up, click on **Yes** to confirm your choice

3.5.4 How to move an Endpoint

An Endpoint can be moved to another Headpoint in case it has mistakenly been added to a certain headpoint. Endpoints that are already use cannot be moved.

1. Go to the section **Data Sources**
2. Go to the tab **Endpoints** on top of the screen
3. Select the endpoint you want to move
4. Click on the **dots** on the right side of the button **Edit**
5. Click on **Move endpoint**
6. Enter the EAN of your choice and click on **Next**
7. Add the CP User Designation Document or declare that you are the connection contract holder of the headpoint by ticking the checkbox **Agree**
8. Click finally on **Submit** to confirm your choice

3.5.5 How to link an Endpoint to a Gateway

To link an Endpoint to a Gateway,

1. Go to the section **Data Sources**
2. Go to the tab **Endpoints** on top of the screen
3. Select the endpoint you want to link
4. Click on the **dots** on the right side of the button **Edit**
5. Click on **Link to gateway**
6. Tick the checkbox on top of the pop-up if you want to use a gateway already installed at the same Headpoint
   If not, select the gateway of your choice in the list and click on **Next**
7. Click on **Submit** to confirm your choice

Note:

A Gateway can only be installed on one Headpoint.

3.5.6 How to decouple an endpoint from a Gateway

To decouple an endpoint from a Gateway,

1. Go to the section **Data Sources**
2. Go to the tab **Endpoints** on top of the screen
3. Select the endpoint you want to decouple
4. Click on the **dots** on the right side of the button **Edit**
5. Click on **Decouple from gateway**
6. Use the date picker to **enter the date** on which the gateway will be decoupled
   Note: when today is entered, the gateway will immediately be decoupled
7. Click on **Next**
8. Read the notification and click on **Submit** to confirm your choice

As a result, a pop-up will appear confirming your choice.

3.5.7 How to replace a gateway on an Endpoint

To replace a gateway,

1. Go to the section **Data Sources**
2. Go to the tab **Endpoints** on top of the screen
3. Select the endpoint for which you want to replace the gateway
4. Click on the **dots** on the right side of the button **Edit**
5. Click on **Replace gateway**
6. Select the new gateway you want to link
7. Click on **Submit** to confirm your choice

As a result, a pop-up will appear confirming your choice.

4 Communication

4.1 Introduction

Multiple communication streams with the Communication Platform have to be managed by the gateway:

4.1.1 Metering communication

The gateway and the endpoint will form the data source of aFRR messages that must be sent with a frequency of 4 seconds, towards the Communication Platform. The Communication Platform will authenticate the gateway (for all communication) and subsequently validate whether all conditions for data routing are present (for metering communication).

Important conditions for a correct routing are required master data elements:

1. Fully active data source
    - Onboarded gateway that can authenticate with a digital certificate
    - Onboarded endpoint
    - Active link between gateway and endpoint
2. Activated routing service on the endpoint
    - This is the result of a successful onboarding process in the Flexhub.

Other conditions that must be met to enable correct routing are functional and technical correctness of the header parameters. The message log described in the next sections shows the following exceptions, in sequence, in case certain conditions are not met.

Condition	Exception text
Technical validity of message	
Valid message type	Message type is unknown
Valid header version	Header version is incorrect
Valid body version	Body version is incorrect
Valid encryption key version (dummy or valid)	Encryption key version is incorrect
Valid encryption key version (valid)	Dummy encryption key version used
Unknown gateway Id	GW Id is not known
Master data elements are correctly configured (see 1 & 2 above)	Data source with active service not found

Header and body versions start at 1 and can evolve in time, in which case CP users will be notified. The only known message type at the moment is ‘aFRR’.

The endpoint information will always show the ‘Last message received’ datetime which will be updated every couple of minutes.

4.1.2 Encryption keys

The gateways need to encrypt the metering communication message bodies. Therefore they will receive the necessary encryption keys and corresponding version from the Communication Platform.

Three different triggers can push a valid encryption key to the gateways:

1. Insertion of a data source in the routing table
    a. Either an active data source (GW linked to EP) gets a routing service activation
    b. Either an EP with an active routing service is linked to a GW

2. The KMS will push a new encryption key every 24h to gateways that are linked to an endpoint with an active service

3. Manually triggered via the **Retrieve encryption key** action (see How to retrieve an encryption key)

4. Gateway request, see technical guide.

4.1.3 Heartbeat

The heartbeat message has two distinct triggers:

1. Manually triggered via the **Test connection** action (see How to test the Gateway connection)
2. A heartbeat message will be activated and sent every 5 minutes once an insertion of a data source in the routing table takes place
    a. Either an active data source (GW linked to EP) gets a routing service activation
    b. Either an EP with an active routing service is linked to a GW

- Heartbeat types
    - Ping : simple heartbeat message used to ping the gateway
    - Time sync : simple heartbeat message enriched with a time synchronization request
    - Version sync : simple heartbeat message with a request to send software and firmware versions
    - Full sync : heartbeat message enriched with both previous sync requests

In all cases, when the heartbeat is not replied to, the gateway connection status will change to 'connection failed'. In the gateway information screen, you will always see the last received heartbeat message timestamp.

The communication section described in this chapter is created to give the user insights and tools that can help to setup and monitor the GW and its communication with the platform.

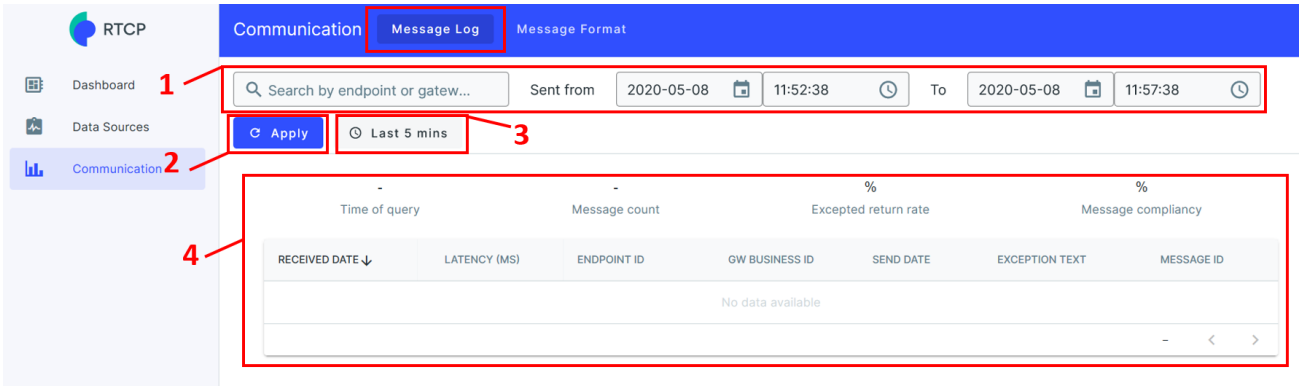
4.2 User Interface

The section Communication consists of the tabs:

- Message Log
- Message Format

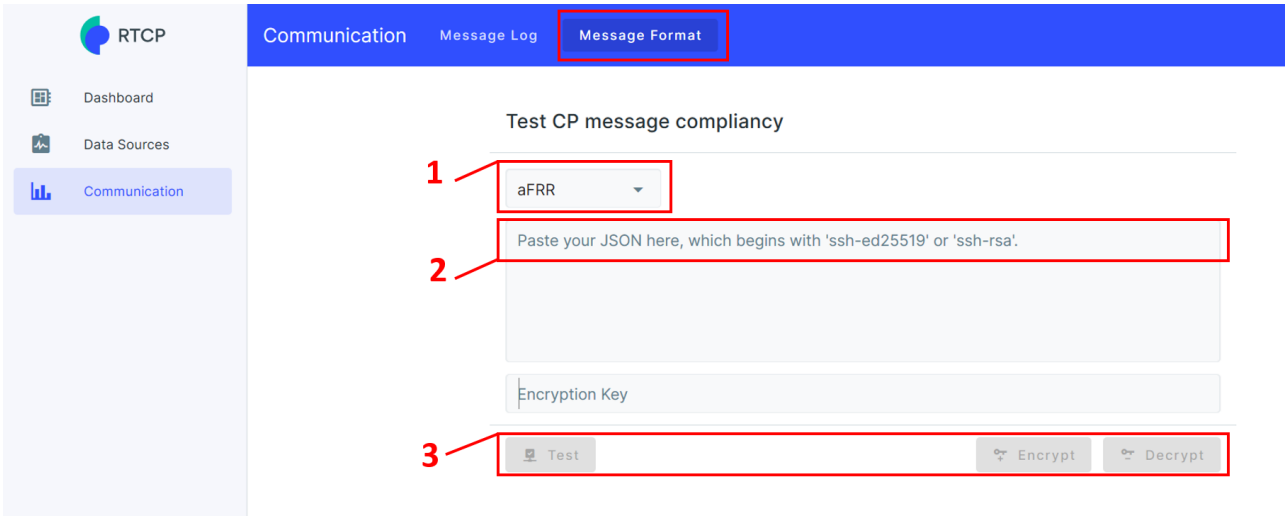
4.2.1 Message Log

The message log allows the user to see the messages processed by the Real-Time Communication Platform for a specific time interval. Also non routed messages will be found here, with the exception text indicating which conditions are not met.



1. Search area to set the interval and the gateway or endpoint Id. When no GW or EP Id is set, the system will query all messages in the interval with a max of 75.
2. The button **Apply** allows you to run the query with applied filters and to refresh all the data in the tab
3. The button **Last 5 mins**, will query the last 5 mins of messages received
4. The list where your results are displayed
    a. KPIs
        i. Time of query
        ii. Message count = count of the amount of messages resulting from the query
        iii. Expected return rate = message count / amount of messages expected within time interval (only relevant for aFRR message where an endpoint Id is set)
        iv. Message compliancy = counted routed messages / message count
    b. List of messages with latency being the difference between the sent timestamp of the GW and the received timestamp by the platform.

4.2.2 Message Format



To test a message format,

1. Go to the section **Communication**
2. Go to the tab **Message Format**
3. Select the **message type** of your choice:
   - aFRR
   - Heartbeat
4. Enter your **message** in the body
5. Click on **Test**

To test a encryption/decryption of an aFRR message,

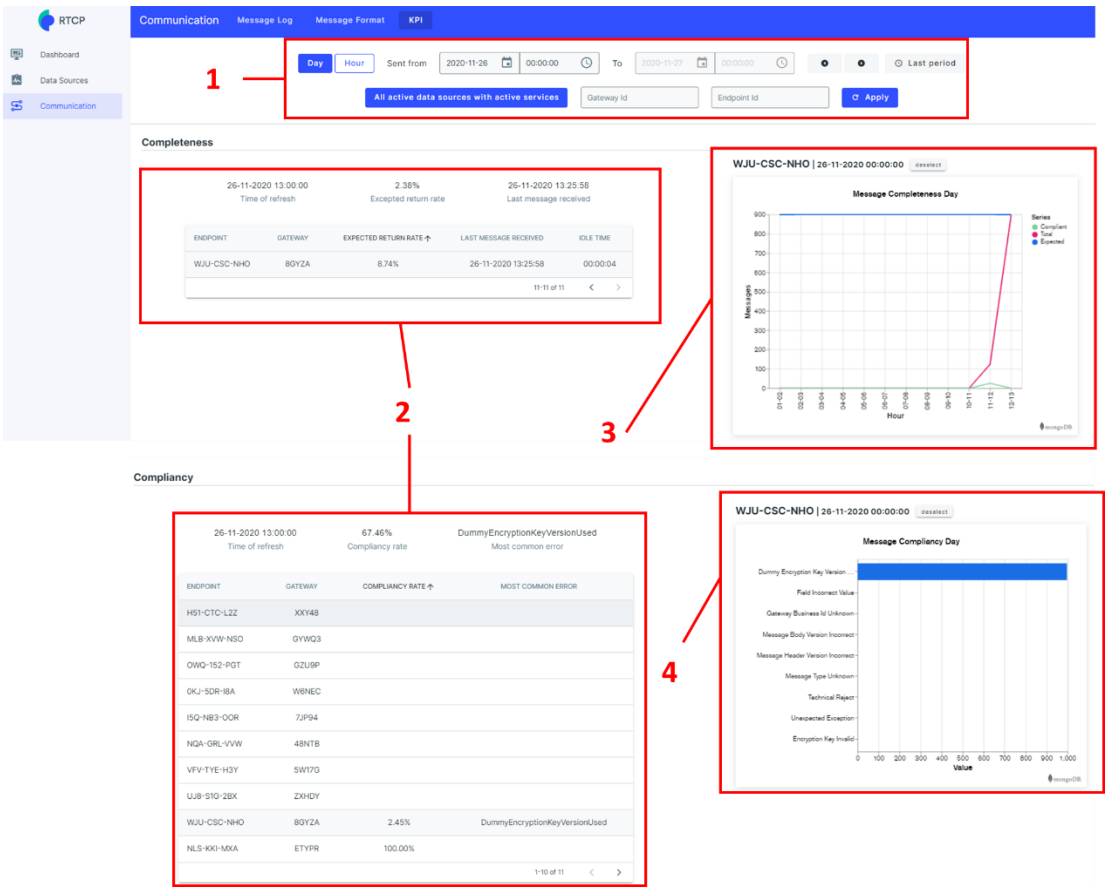
1. Enter a valid encryption key to encrypt/decrypt the message body
2. The system returns the transformed message

4.2.3 KPI

The KPI section allows the user to consult KPIs on a more aggregated level than the message log. The user can select a full day or an hour time interval to view the KPIs and visually consult the counted messages and exceptions by type in the graphs.

Some attention points:

- The KPIs will be **refreshed on the hour** and a history of the **hourly graph** of only **three days** will be kept and **the daily graph** for **thirty days**.
- The **last message received date** and **idle time** will be given only when viewing "last period" until current time and will always give the real-time value, which is different from the other KPIs that are refreshed on the hour.
- **The endpoints are sorted on lowest KPI scores first** as the section is made to allow the user to detect problems. However, all endpoints can be viewed if entered in the EP or GW search field or via the subsequent pages.
- When selecting an endpoint, this will automatically select the endpoint in the other respective section of the screen and inversely (completeness – compliancy).



The screen composition is as follows

1. Search bar to filter on the required period and object.
2. A paged list of Endpoints sorted on lowest KPI score first. Pagination allows to go to next 10 EPs (or use the search on GW or EP ID)
3. The graph showing
    a. Expected amount of messages (blue)
    b. Total amount of messages received (red)
    c. Compliant amount of messages received (green)
4. The graph showing amount of messages by reject reason

5 B2B APIs

There are many REST API calls available to setup and query the data sources and its related communication. Consult the Help section to direct you to the technical documentation of the APIs.