RTCU Communication Hub
Users Manual

Version 1.04

logic IO
The M2M Enabler

Table of Contents

Introduction

1 Introduction

The **RTCU Communication Hub (RCH)** is a managed middleware service that enables reliable and secure bi-directional communication between RTCU devices installed in the field and the application back-end infrastructure.

The **RCH** works over any TCP/IP based communication channel, whether it is behind a NAT firewall or a dynamic IP address schema. For full flexibility, it can be installed on-premises or in the cloud.

The **RCH** offers several layers of security, including X.509 TLS secured communication with full certificate management. Automatic data compression is supported for lower communication cost and reduced latency.

The **RCH** supports the **RTCU Deployment Server (RDS)** that has been designed for automatic over-the-air (OTA) upgrade of a large number of installed RTCU devices. The RDS tool is available as a free extension to the RCH.

The main features of the RTCU Communication Hub:

- Advanced 64-bit server architecture supporting thousands of clients and massive traffic.
- Runs as a Microsoft Windows service. The service will start without user log-on and can also be managed remotely.
- Support for up to 32 separately configurable and isolated hub instances on the same server.
- Remote manageable using the "Monitor" tool client utility. Up to 10 simultaneous clients.
- Password protected remote access.
- Comprehensive logging functionality.
- Advanced filtering feature which allows monitoring/logging on a specific client and/or logging level.
- Graphical diagnostic tool.
- Secure TLS socket communication.
- Full X.509 certificate management.
- Automatic data compression for lower communication costs and reduced latency.
- Automatic fallback and recovery.
- Plug-in architecture for extending functionality and integration to backbone applications.
- Plug-in developers kit is available for free.
- Integrated device time service.
- Open-source integration libraries.
- Support the **RTCU Deployment Server** and the **RTCU IDE**.
- Backward compatible with the **RTCU Gateway 2**.
- Free for up to 25 clients. A license must be purchased for additional clients.

System Requirements

Operating system:	Microsoft Windows 10/Windows 8/2008 Server/2010 Server.
Memory:	500 MB + 4 kB per client (standard connection) or + 400 kB per client (Secure connection).
Hard disk space:	10 MB. Additional space required for log-to files.
Other:	Network card. TCP/IP network protocol. (Permanent Internet connection with a fixed IP address is recommended.)

Time Service

The RTCU Communication Hub has an inbuilt Time Service which allows central synchronization of the real-time clock for connected clients. The clients can request the local time or the UTC time for a truly universal time synchronization service. For more information, please consult the RTCU IDE online documentation and the "RTCU Communication Hub Configuration" section.

Heartbeat Service

The RTCU Communication Hub has an inbuilt Heartbeat Service which monitors the heartbeat of clients, and notifies the plug-ins of "heartbeat online" and "heartbeat offline" events.
Using the Heartbeat functionality allows for very fast detection of a device that goes offline/online, for example when the quality of the cellular connection is suboptimal.
The RCH comes with an example plug-in that logs the status. See the Heartbeat plug-in for more details.

License

The RTCU Communication Hub supports 25 clients as default. To allow additional clients, further licenses must be ordered.
Please contact Logic IO for more information.

The RTCU Communication Hub Architecture

2 The RTCU Communication Hub Architecture

The RTCU Communication Hub is a middleware solution which is used for communicating with remote RTCU devices by using any TCP/IP-enabled communication media, such as cellular, WLAN, LAN etc.

One of the most important function of the RTCU Communication Hub is to allow access to connected devices that operate with a private and/or dynamic IP address by mapping the private IP address of a unit to a global IP address that is accessible by other clients.

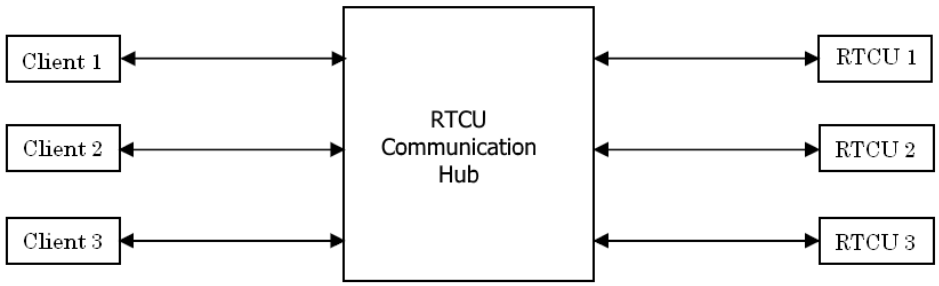
The RTCU Communication Hub also includes:
- Security functions.
- Local/remote maintenance.
- Logging features.
- Device recovery after application failure.

The merging of SMS and TCP/IP technology is made possible with the Logic IO proprietary VSMS (Virtual SMS) technology which allows any RTCU application that uses SMS messages to transparently send/receive messages by using either SMS, TCP/IP, data call, or a cable connection without any changes to the software already developed.

The RTCU Communication Hub defined protocol is named "RACP2" (Remote Access Communication Protocol REV 2) and is based on the RACP protocol that is used for communicating with RTCU devices by using a serial line connection (please see the separate document that describes the RACP and RACP2 protocols). By using a standard TCP/IP socket interface, the protocol is made extremely simple and easy to implement by the clients.

Logic IO offers a free software library (DLL) that implements the client side of the RACP2 protocol for use in a Microsoft Windows environment. The source code (written in C) can also be supplied.

By using the RACP2 protocol, the RTCU Communication Hub architecture can be illustrated like this:



The client is communicating with the RTCU Communication Hub by using the RACP2 protocol. The message that has been sent from the client to the RCH will be forwarded to the RTCU device by using the TCP/IP connection (again by using the RACP2 protocol). The response sent from the RTCU device to the client will be forwarded back to the client in the same way.

It should be noted that communication between two clients and two RTCU devices is also possible by using the RTCU Communication Hub.

To use the RTCU Communication Hub, the client and the RTCU device need to be supplied with the IP address, port number, and password of the RTCU Communication Hub.

The RTCU Communication Hub runs as a Windows service and therefore it runs independently of user logon.

6 The RTCU Communication Hub Architecture

A complete RTCU Communication Hub setup consists of:

- RTCU Communication Hub service for managing the message routing and logging-to file system on the server.
- RTCU Communication Hub guard service whose only task is to restart the service if it stops unexpectedly.
- RTCU Communication Hub - Control Panel which handles the creation and management of RTCU Communication Hub services.

Migration

3 Migration

The RTCU Communication Hub (RCH) is the successor to the RTCU Gateway 2 and operates in a similar way and is also 100% backward compatible.

Please be aware that the new license file is required for the RCH. It can not use the former license file format from the RTCU Gateway 2.

The RCH configuration is not compatible with the configuration of the RTCU Gateway 2 and must be migrated manually.

Please follow the following steps when migrating from the RTCU Gateway 2 to the RCH:

1. Write down the configuration for the server instances from the RTCU Gateway 2 Control Panel.

2. Uninstall the RTCU Gateway 2 server.
The RCH cannot be installed on a server where the RTCU Gateway 2 is already present.

3. Install the RCH.

4. Install any new license files(s) in the Control Panel.

5. Install plug-ins
The plug-in mechanism is not changed from RTCU Gateway 2, so former plug-ins will still work.

6. Recreate the server instances from the configuration notes from step 1.
The first thing to note, is that there are more options than in the gateway.

It is recommended that secure connections are not included during the migration to avoid any disruption in already existing installations, when familiarizing with the new settings.
Instead secure connections should be kept in a separate instance until it is ready for deployment.

The Monitor Tool uses secure connection to communicate with the server, and requires the new options to be filled out.
The RCH comes with a server certificate, which is used by default, so so the Monitor Tool can be used without having to get a certificate yourself.
Please note that the default certificate is part of the RCH, both server and monitor tool and therefor available to anyone downloading the installers.

7. Start the server instances.

The server instances are now migrated from the RTCU Gateway 2 to the RCH.

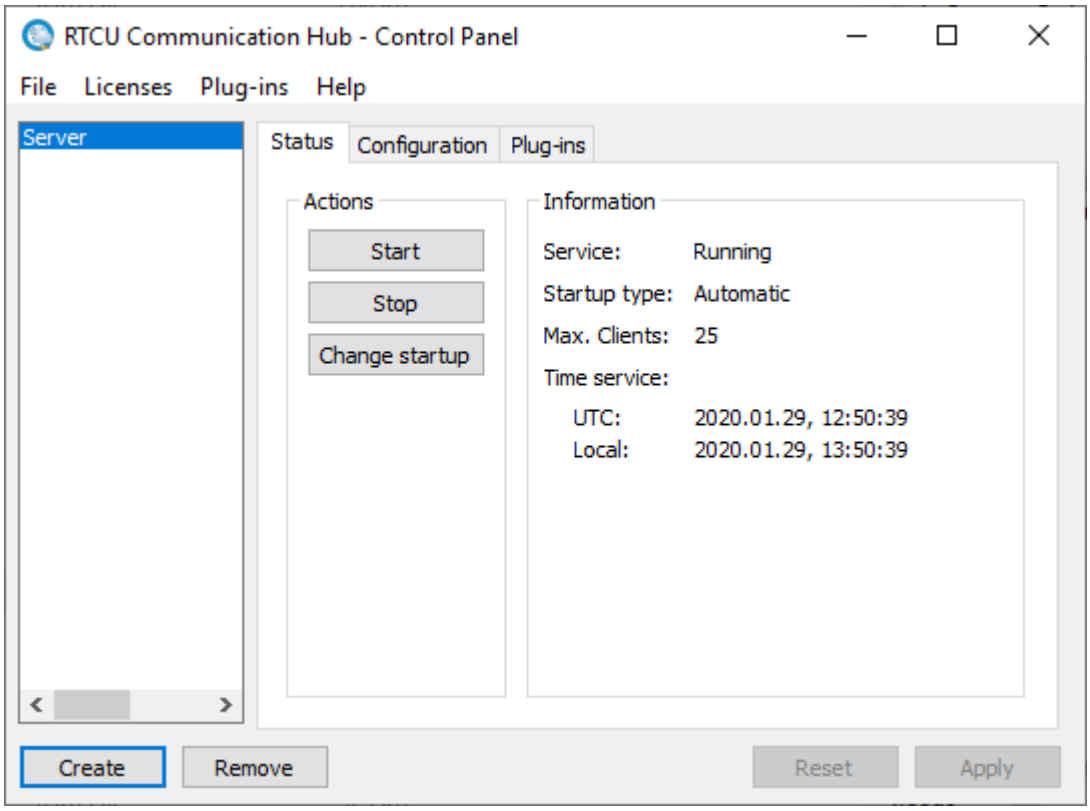
8. (optionally) Create a new server instance to test out the new secure connections.
This allows trying secure connection without interfering in the production server setup.

Control Panel

4 Control Panel

The "RTCU Communication Hub - Control Panel" is where the server instances are managed.

All configuration of the instances must be done through this interface.



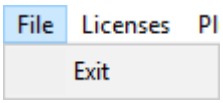
The interface can basically be split into tree areas - the Menuitems, the Instance list and the Instance management areas.

4.1 Menuitems

The following pages describe all the different menu items that are available in the Control Panel.

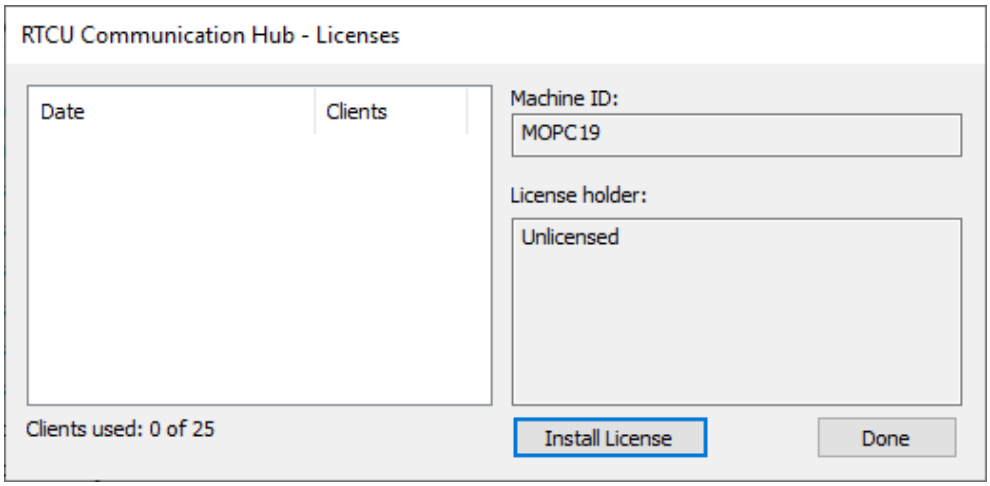
4.1.1 Menu item: File

The "Exit" command ends the Control Panel program.



4.1.2 Menu item: Licenses

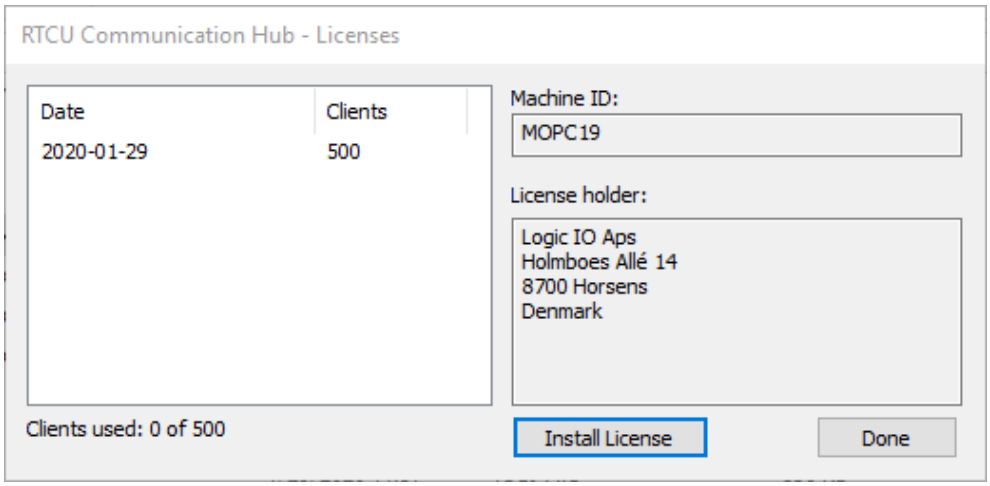
The "Licenses" dialog shows the licenses that are installed on the server.
When no license is installed, the RTCU Communication Hub accepts 25 clients.
For example, it is possible to create one instance with all 25 clients or two instances - one with 15 clients and one with 10 clients.



Additional licenses can be ordered from Logic IO to support more clients.
Each license is bound to the Machine ID of the server. This information is therefore required when ordering.

To use the license file received from Logic IO, follow these steps:

1. Open the Control Panel.
2. Go to the Licenses dialog.
3. Press the "Install License" button.
4. Select the license file in the file dialog.



It is now possible to change the maximum number of clients in the Instance configuration.

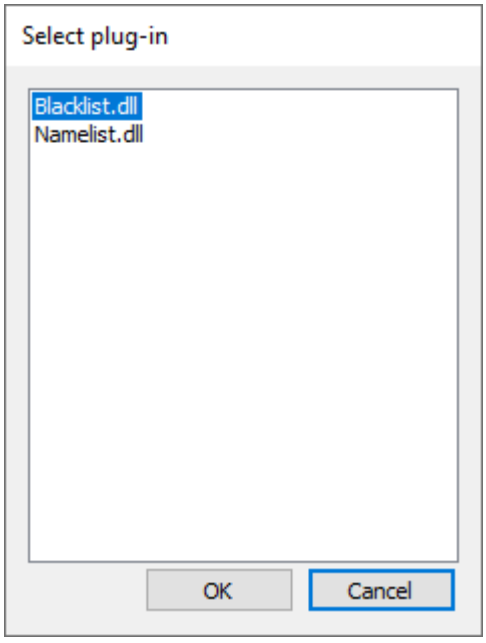
4.1.3 Menu item: Plug-ins

Plug-ins are DLL libraries that can be installed dynamically to extend the functionality of the RTCU Communication Hub.
A plug-in can be developed by using the free RTCU Communication Hub plug-in developers kit.

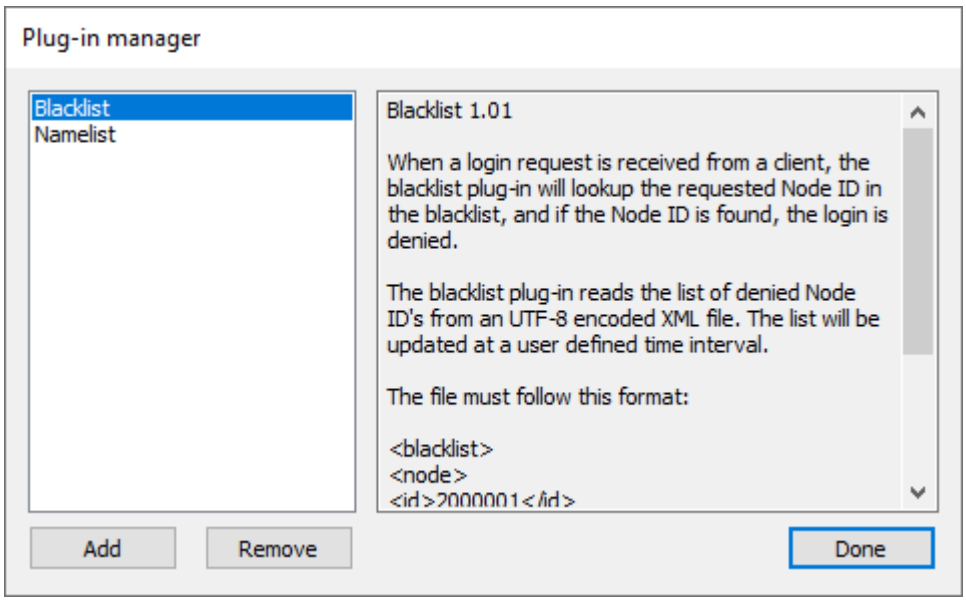
The "Plug-In Manager" dialog is where available plug-ins are added and removed.

To add a plug-in, follow these steps:

1. Copy the plug-in DLL to the "Plugins" folder in the RTCU Communication Hub install directory. (This step is not necessary for the standard plug-ins that come installed with the RTCU Communication Hub.)
2. Open the Control Panel.
3. Go to the Plug-Ins Manager dialog.
4. Press the "Add" button and select the plug-in DLL in the pop-up list.



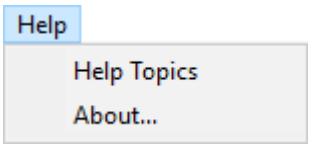
When a plug-in is added, the Plug-In Manager displays the available information about it.



When removing a plug-in (with the "Remove" button), it is removed from the configuration of the instances but not from the hard drive.
Any running instances will continue to use the plug-in until they are restarted.

4.1.4 Menu item: Help

By using the "Help" menu, it is possible to receive help regarding specific items.



The individual items:

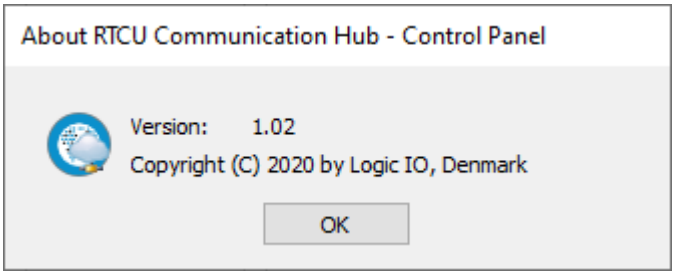
- Help topics
- About

4.1.4.1 Help - Help topics

This command will start the "Windows Help" system. You will be presented with the contents of the Control Panel help manual.

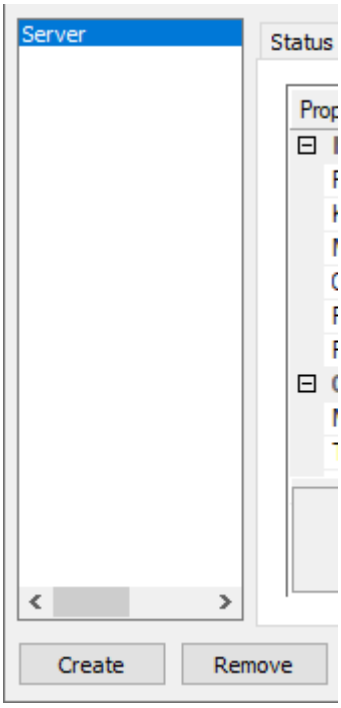
4.1.4.2 Help - About

This command shows the current version number of the Control Panel program and a copyright notice.



4.2 Instance List

The list on the left side of the Control Panel contains all installed instances.



To manage an instance, select it in the list and use the Instance management pages to configure it.

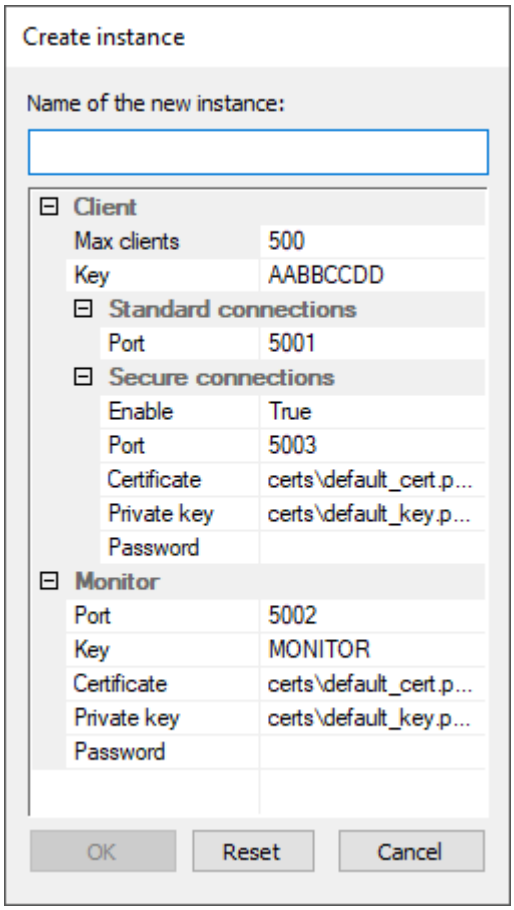
A new instance can be created with the "Create" button if there are licenses left.

To remove an instance, select it a press the "Remove" button.

4.2.1 Create instance

Create

Pressing the above button will open a dialog to create a new instance on the server.



Press the "OK" button to create the instance.
Press the "Reset" button to reset the configuration back to default values.
Press the "Cancel" button to abort creating the instance.

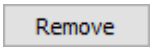
Name of the instance
The name of the instance is used to identify the instances and differentiate them from each other - both for the server and the administrator.
The name is a Unicode string that can be up to 30 characters long. For example "Communication Hub (5001)".

Configuration
The description of the configuration parameters (and additional options) for client and monitor can be found here:

- Client parameters
- Standard connection parameters
- Secure connection parameters
- Monitor parameters

The parameters that are not included in this dialog will hold default values and cannot be changed until after creation.

4.2.2 Remove instance



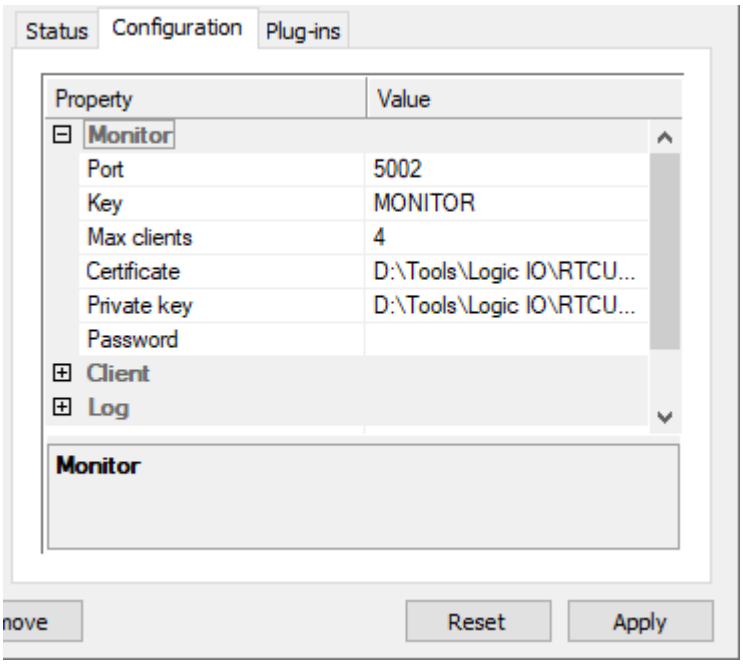
Pressing the above button will completely remove an instance from the server. The service will be removed, including its configuration, and the maximum number of clients will be freed for the other instances.
The log files will not be removed.

To ensure that no instance is removed accidentally, a pop-up dialog is shown which asks for verification.

The instance must be stopped before removing it.

4.3 Instance management

The right side of the control panel contains the management pages.



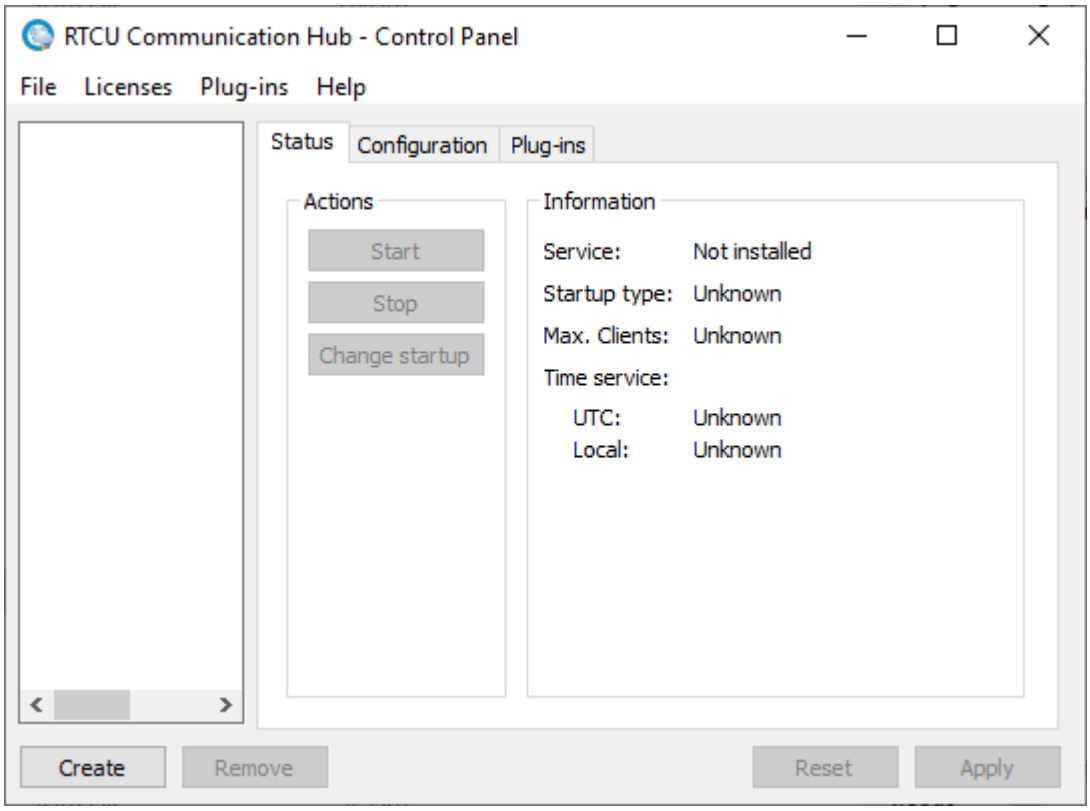
The management pages consist of:

- Instance Status
- Instance Configuration
- Instance plug-ins

Any change made on these pages will be committed to the current selected instance in the Instance list.

4.3.1 Instance Status

The "Status" page is where the instances are controlled and monitored.



The "Actions" group contains options for changing the status of the selected instance.
The actions supported include starting and stopping the instance and changing the startup type.

The "Information" group contains the status of the instance.
The items can have the following states:

Service

Running	The instance has been started and is running.
Stopping ...	The instance is currently stopping.
Stopped	The instance is not running.
Not installed	No instances are installed.

Startup Type

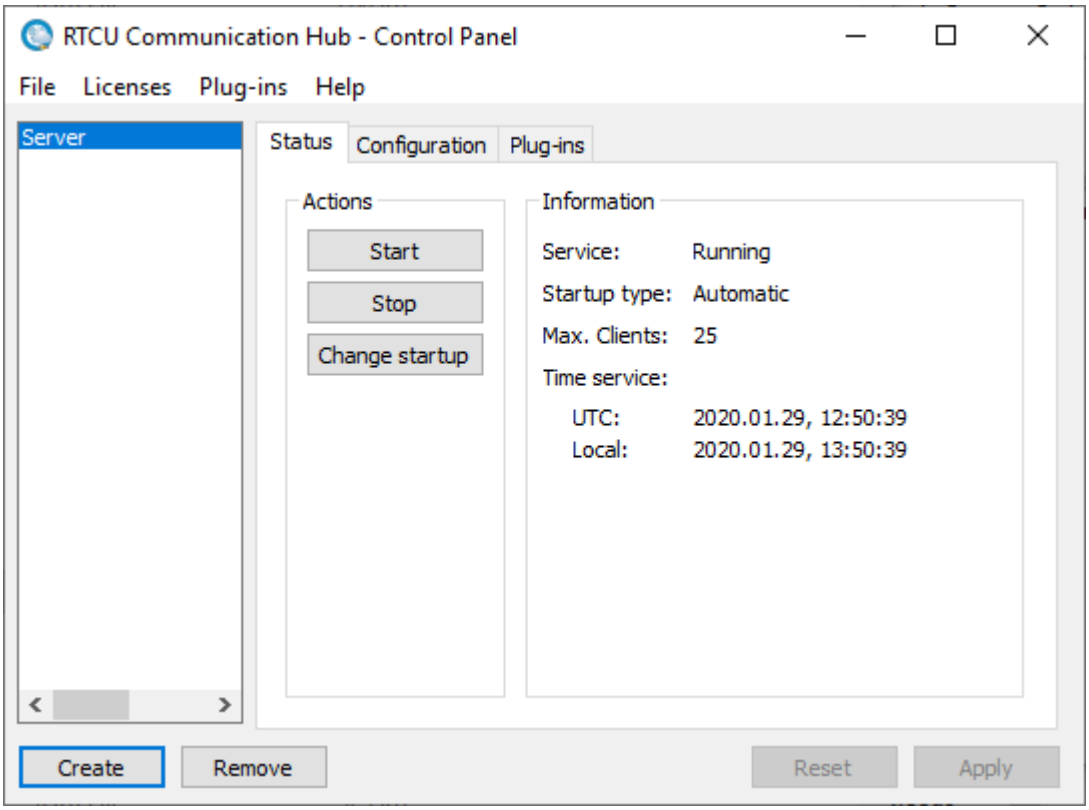
Automatic	The instance starts automatically with Windows.
Manual	The instance must be started manually from the Control Panel.
Unknown	No instances are installed.

Maximum Clients

Clients	The maximum number of clients that can connect to the instance.
Unknown	The instance is not running.

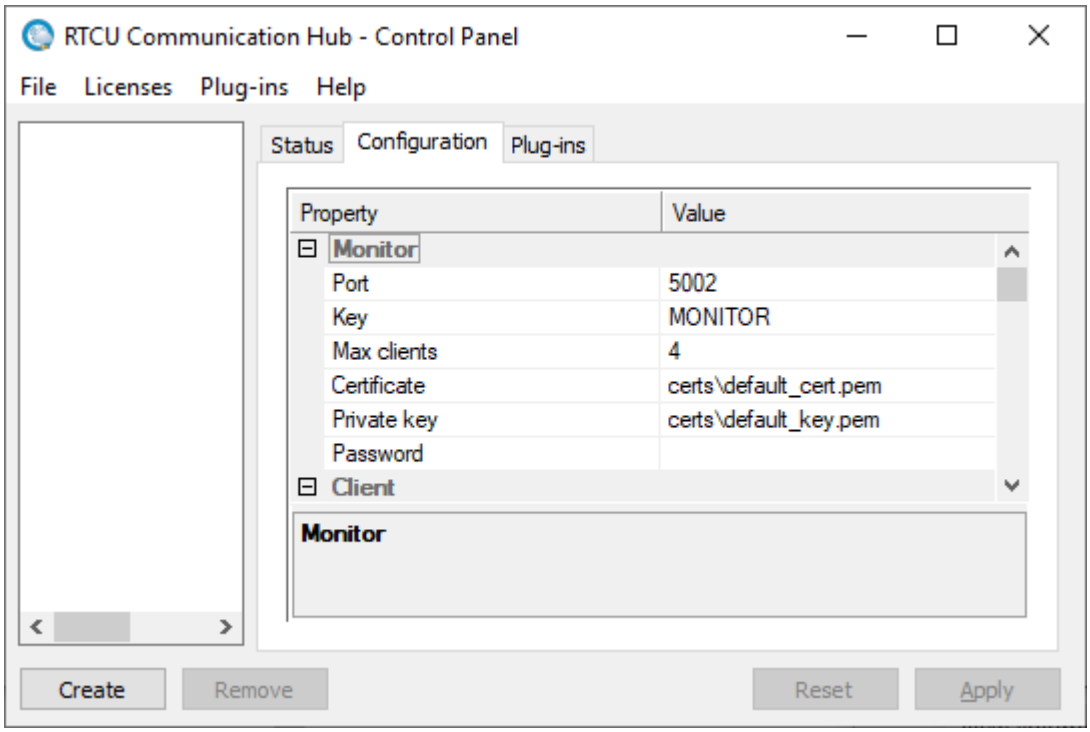
Time Service

Time	The current time of the instance - shown in both UTC and local time. "(DST)" is added if Daylight Saving Time is in effect.
Unknown	The instance is not running and/or no time information is available.
Disabled	The time service is disabled for the instance.

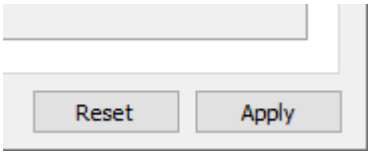


4.3.2 Instance Configuration

The "Configuration" page is where the configuration of the selected instance is managed.



When the configuration is changed, the "Apply" and "Reset" buttons are enabled.

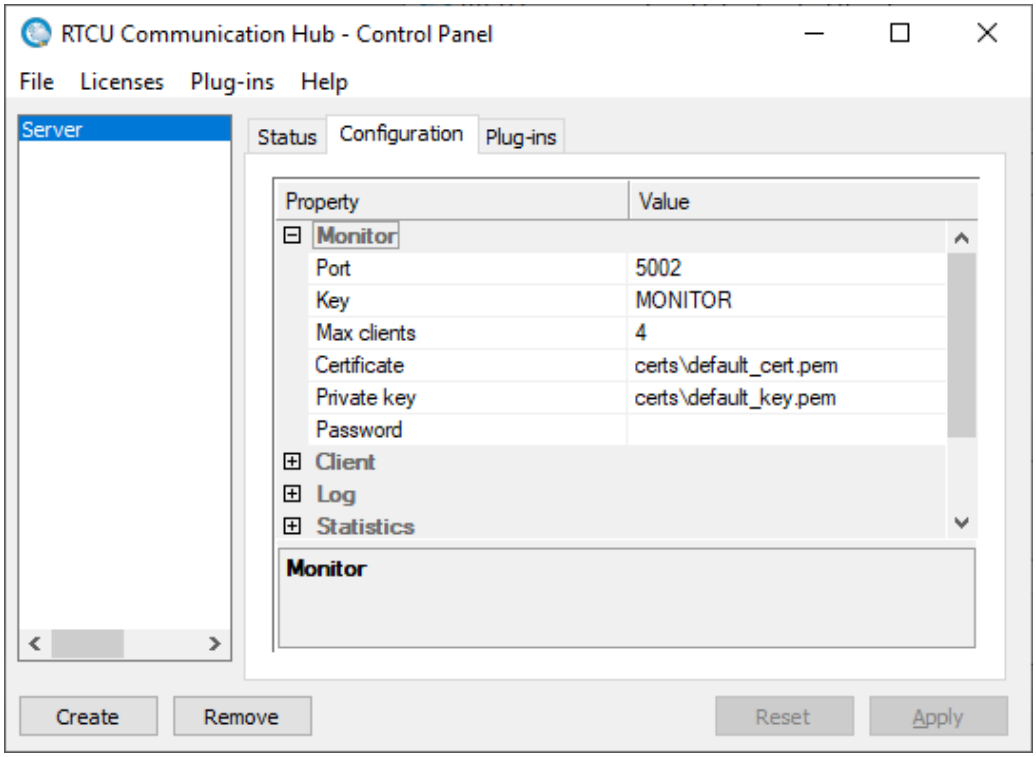


Press the Apply button to save the configuration. The instance will use the new configuration when it is restarted.
Press the Reset button to clear all changes made to the configuration.

For a description of the individual parameters, follow the links below:

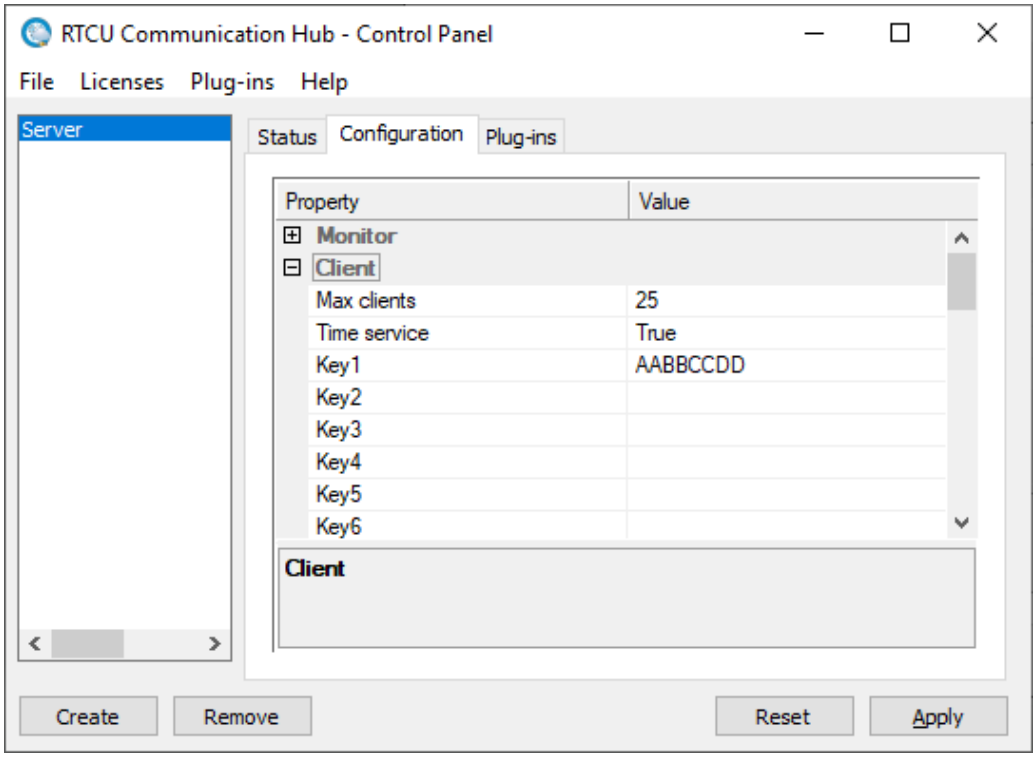
- Monitor parameters
- Client parameters
- Standard connection parameters
- Secure connection parameters
- Log parameters
- Statistics parameters

4.3.2.1 Monitor parameters



Port	The IP port where the instance listens for any monitor tool clients.
Key	The access key for the monitor tool clients.
Maximum clients	The maximum number of monitor tool clients that are allowed to connect to the instance. The default is 4 clients but up to 10 is supported.
Certificate	The PEM file containing a X509 certificate, used to secure the connection to the monitor.
Private key	The PEM file containing the private key for the certificate
Password	The password of the private key. Leave empty if the private key do not require password.

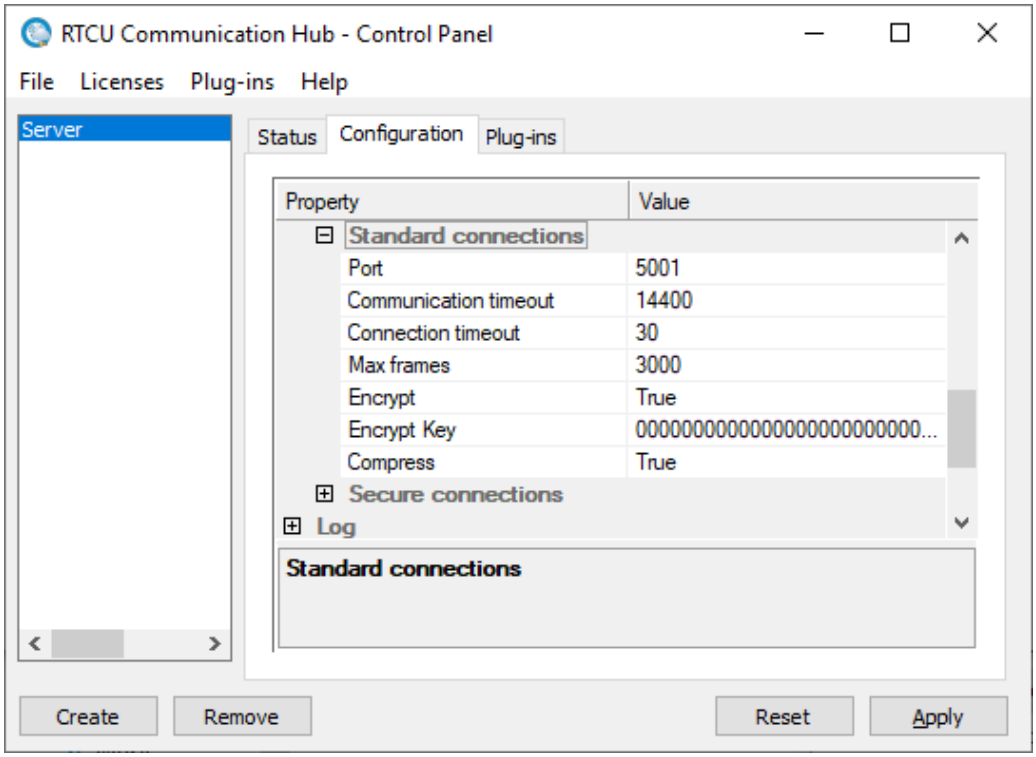
4.3.2.2 Client parameters



Maximum clients	The maximum number of clients that are allowed to connect to the instance. This number is dictated by the license.
Time service	Enables/disables the "Time" service. Enabling the Time service will allow clients to request the local or UTC time from the instance by using the gwTimeGet() function. Disabling the Time service will return zero to the clients requesting the time.
Key1	The access key #1 for the instance clients.
Key2	The access key #2 for the instance clients.
Key3	The access key #3 for the instance clients.
Key4	The access key #4 for the instance clients.
Key5	The access key #5 for the instance clients.
Key6	The access key #6 for the instance clients.
Key7	The access key #7 for the instance clients.
Key8	The access key #8 for the instance clients.
Key9	The access key #9 for the instance clients.
Key10	The access key #10 for the instance clients.

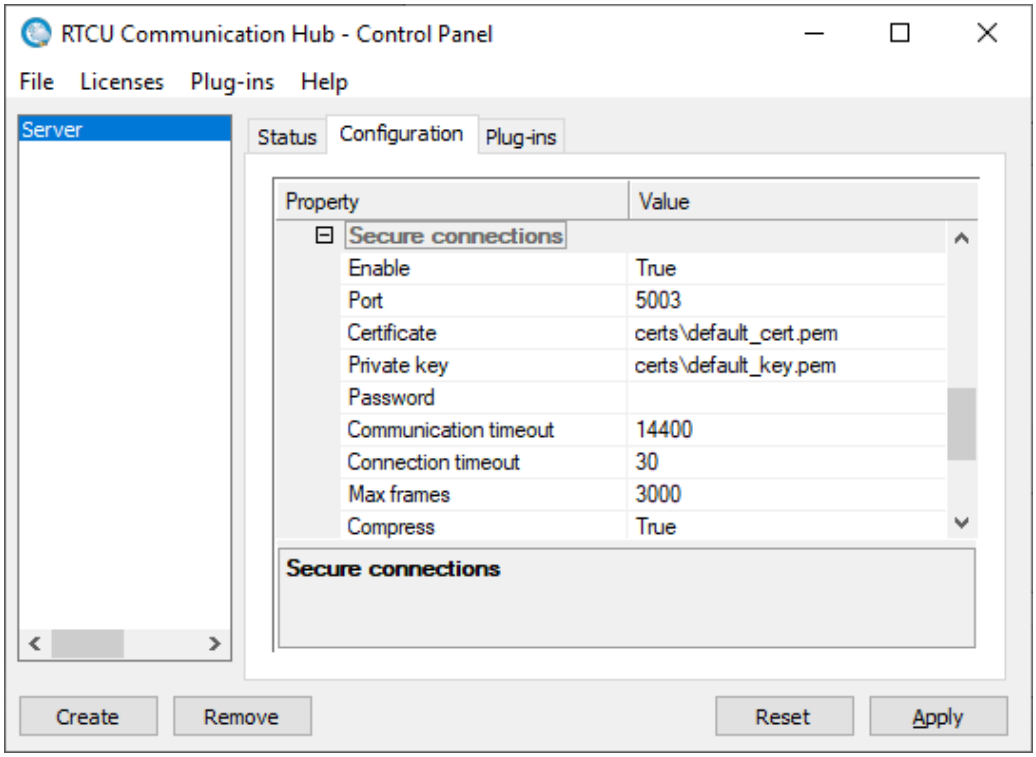
All access keys are equal and work similarly, and up to 10 available keys can conveniently be managed.

4.3.2.3 Standard connection



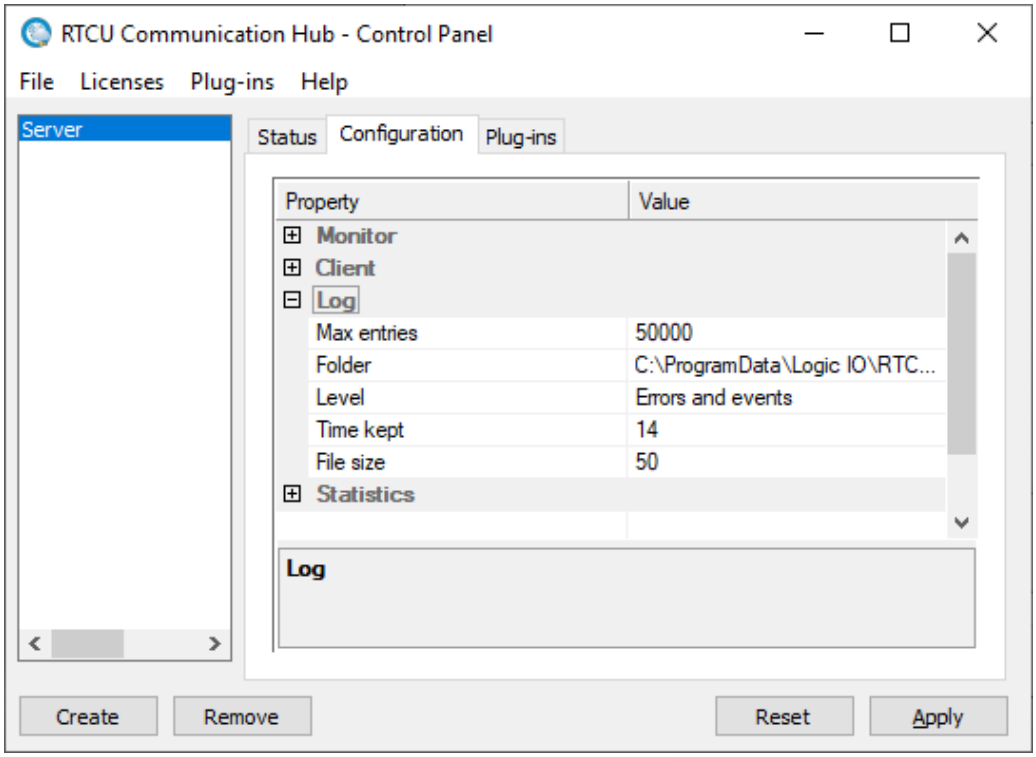
Port	The IP port where the instance will listen for clients with standard connections. This port will also be used for the heartbeat UDP packets.
Communication timeout	The time without transactions before the instance disconnects a client. This is used to clean up inactive connections that for various reasons have not been closed correctly by the network. Time is given in seconds.
Connection timeout	The time without login before the instance disconnects a client. Time is given in seconds.
Maximum frames	The maximum number of messages waiting to be send to a client, before new messages are rejected.
Encrypt	Enables/disables encryption of client communication.
Encrypt Key	The encryption key used to encrypt/decrypt client communication. The key is 16 bytes long and is written in HEX numbers. Note that all 32 characters must be present or the key is rejected.
Compress	Enables/disables compression of client communication.

4.3.2.4 Secure connection



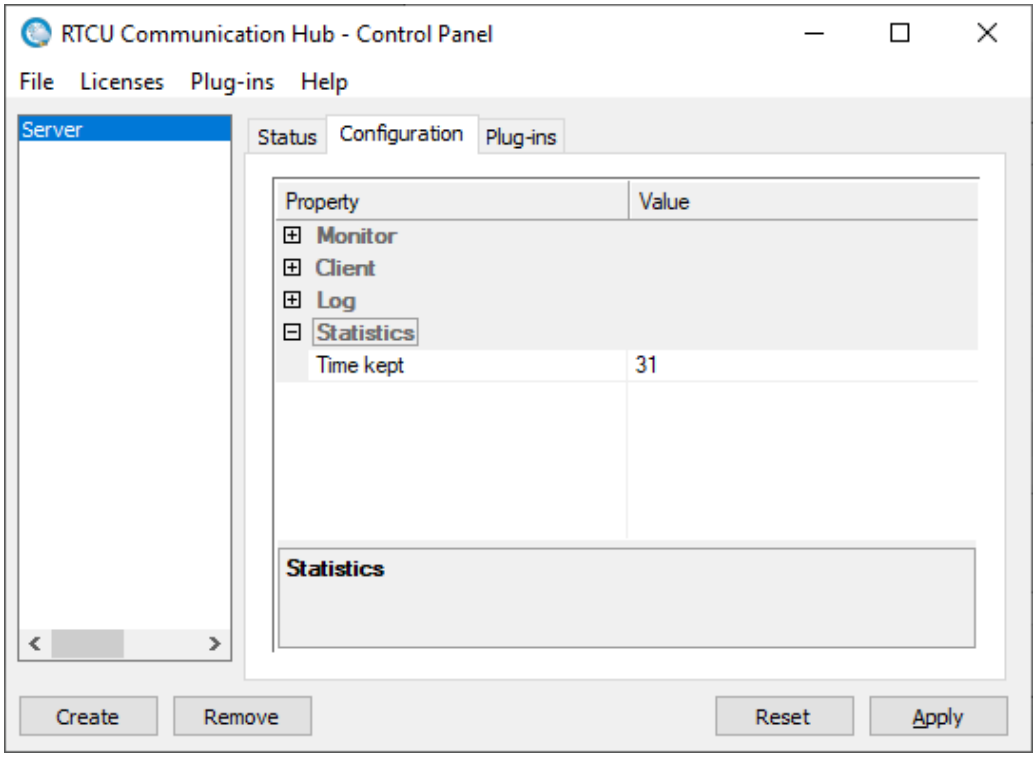
Enable	Enable support for Secure connections in instance.
Port	The IP port where the instance will listen for clients with secure connections.
Certificate	The PEM file containing a X509 certificate, used to secure the connection.
Private key	The PEM file containing the private key for the certificate
Password	The password of the private key. Leave empty if the private key do not require password.
Communication timeout	The time without transactions before the instance disconnects a client. This is used to clean up inactive connections that for various reasons have not been closed correctly by the network. Time is given in seconds.
Connection timeout	The time without login before the instance disconnects a client. Time is given in seconds.
Maximum frames	The maximum number of messages waiting to be send to a client, before new messages are rejected.
Compress	Enables/disables compression of client communication.

4.3.2.5 Log parameters



Maximum entries	The maximum number of log entries that can be held in the server buffer. The server buffer is used by the monitor tool clients to read past log entries. The default is 50,000 entries. Legal values range from 1,000 to 500,000. Increasing this number will also increase the memory footprint of the instance.
Folder	The directory path the instance uses when logging to files. The instance will create a folder with its name in this directory, and in this a folder for each day is created. The log files are stored in <folder>\<instance name>\<date>\. For example: C:\Logs\Server\2020-01-24\file001.log.
Level	The level of logging that is used by the instance for the log files.
Time kept	The number of days the log files are stored on the server before being deleted.
File size	The maximum size of a log file before the instance starts on a new file. The size is given in MB.

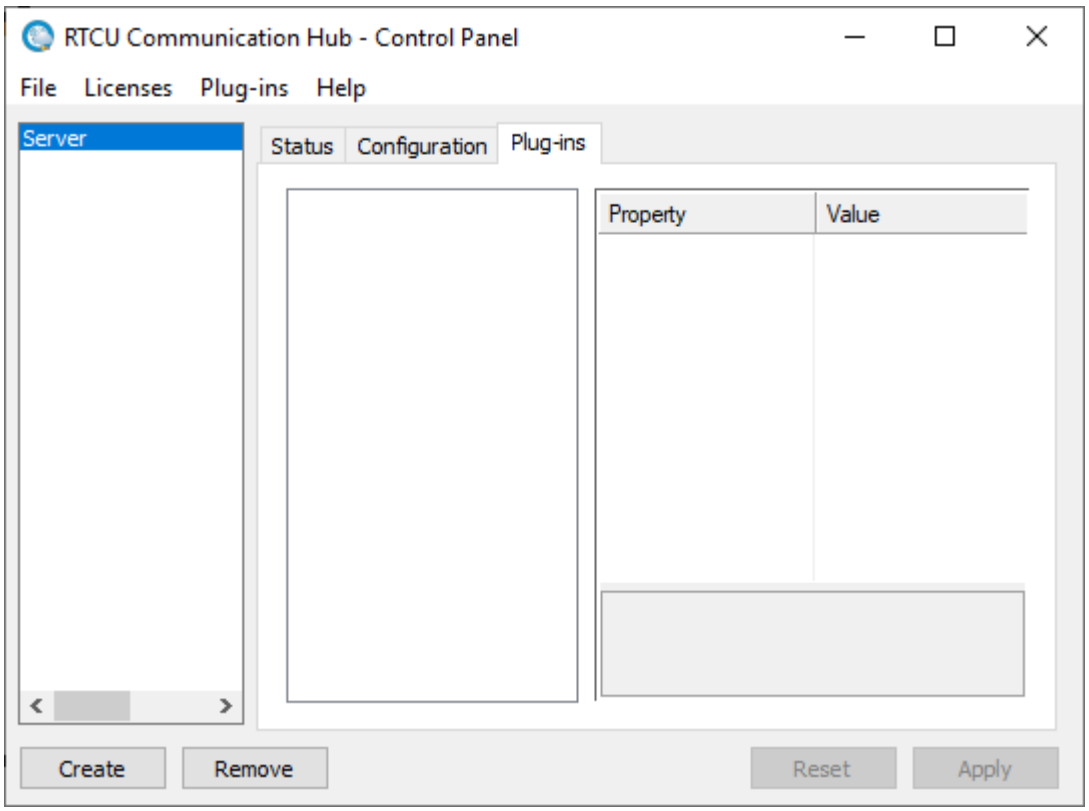
4.3.2.6 Statistics Parameters



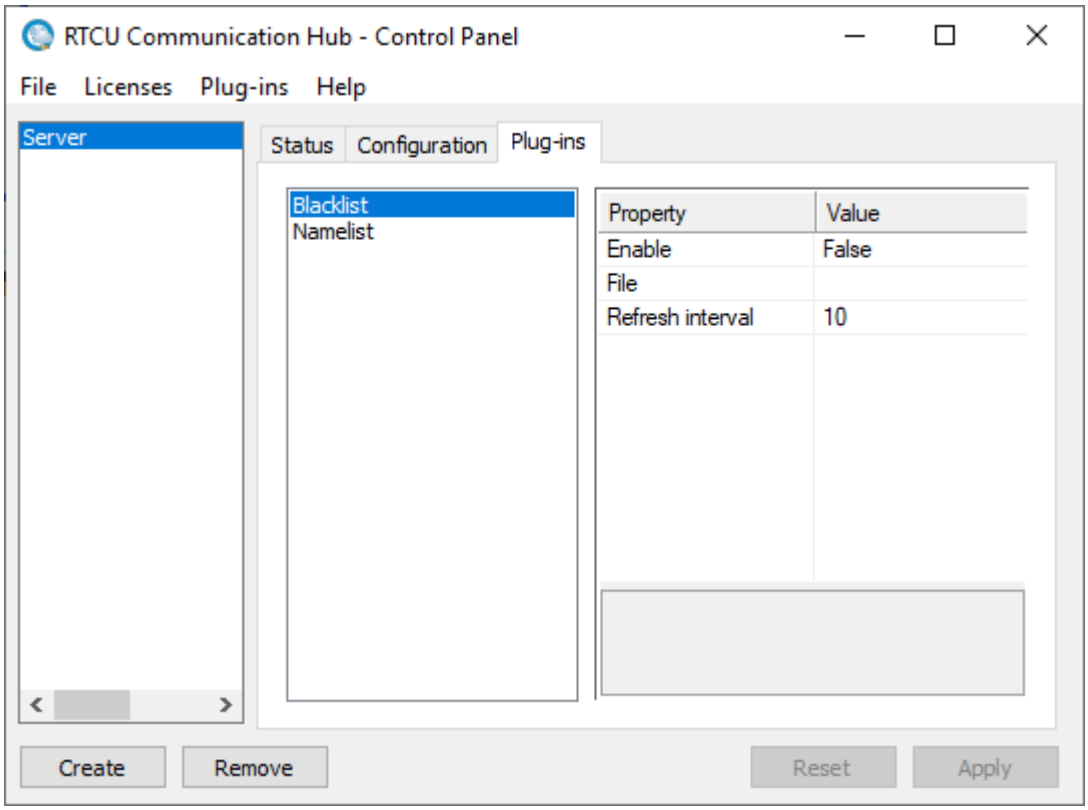
Time kept — The number of days the statistics data is stored on the server before being deleted.

4.3.3 Instance plug-ins

The "Plug-Ins" page is where the plug-ins in the instance are configured.

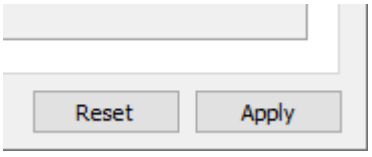


On the left side of the page, a list of the plug-ins added in the Plug-in Manager can be seen. On the right of the page, the available properties for the selected plug-in can be seen.



The actual properties are specific for the individual plug-ins, and the details can be found in the description.
The "Enable" property is used to enable or disable the selected plug-in for the instance. A disabled plug-in will not be loaded by the RTCU Communication Hub service.

When the configuration is changed, the "Apply" and "Reset" buttons are enabled.



Press the Apply button to save the configuration. The instance will use the new configuration when it is restarted.
Press the Reset button to clear all changes made to the configuration.

Standard Plug-ins

5 Standard Plug-ins

The RTCU Communication Hub includes a plug-in framework for easy extension of the functionality.

The following standard plug-ins are included in the RTCU Communication Hub server installation:

- Blacklist — This plug-in will prevent clients from connecting to the RCH based on their Node ID.
- Heartbeat — This plug-in monitors the heartbeat from clients.
- Namelist — This plug-in allows the monitor tool to show a text string instead of the Node ID for clients.

A plug-in can be developed by using the free **RTCU Communication Hub Plug-In Developers Kit** that also includes the full source code to the above plug-ins.

5.1 Blacklist

The "Blacklist" plug-in will compare the Node IDs of all clients that try to log on to the RCH instance with an internal list, and if the Node ID is found on the list, the logon is denied.
The internal list is read from a data file at regular intervals. This ensures that the list of Node IDs that are denied logon can be changed without having to restart the RCH instance.

For details on how to expand this plug-in, see the **RTCU Communication Hub Plug-in Developers Kit**.

Blacklist Configuration

File The name of and the path to the data file.

Refresh interval The number of minutes between the plug-in checks the data file for changes. The default is 10 minutes. This must be a value between 1 and 30 minutes.

Blacklist Data File
The data file used by the Blacklist plug-in is an XML file with the following format:

```
<blacklist>
  <node>
    <id>2000001</id>
    <text>Message shown in log on rejection</text>
  </node>
  <node>
    <id>2000002</id>
    <text />
  </node>
</blacklist>
```

5.2 Heartbeat

The "Heartbeat" plug-in will generate a log entry when notified about a "heartbeat offline" or "heartbeat online" event.
This allows for very fast detection of a device that goes offline/online, for example when the quality of the cellular connection is suboptimal.

When the RCH begins to receive heartbeats from a device, a "heartbeat online" event is generated. When the RCH has not received a heartbeat from the device for a specified time period, a "heartbeat offline" event is generated.
This timeout period is determined by the individual clients, see the **RTCU IDE documentation for rchHeartBeat** for further details.

The heartbeat is sent to the RCH on on the standard connection port as an UDP/IP package that identifies the device that sent it.

For details on how to expand this plug-in and how to use the heartbeat service from other plug-ins, see the **RTCU Communication Hub Plug-in Developers Kit**.

5.3 Namelist

The "Namelist" plug-in allows the monitor tool to show a symbolic name text in the "Clients" list instead of the Node ID.
The Node ID to name mapping is read from a data file at regular intervals. This ensures that the list of names for the Node IDs can be changed without having to restart the instance.

For details on how to expand this plug-in, see the **RTCU Communication Hub Plug-in Developers Kit**.

Namelist Configuration

File The name of and the path to the data file.

Refresh interval The number of minutes between the plug-in checks the data file for changes. The default is 10 minutes. This must be a value between 1 and 30 minutes.

Namelist Data File
The data file used by the Namelist plug-in is an XML file with the following format:

```
<namelist>
  <node>
    <id>11110000</id>
    <name>RDS server</name>
  </node>
  <node>
    <id>11110001</id>
    <name>RDS monitors</name>
  </node>
</namelist>
```

Troubleshooting Guide

6 Troubleshooting Guide

Error	*Reason*	*Solution*
"Server is running low on disk space."	An elevated log level may lead to a huge amount of storage data.	Please check your Log parameters.
"Logging to file failed - buffer overflow."	The log file system cannot keep up. This may be a result of: 1. No more disk space. 2. Slow disk performance. Please note that when this message occurs, the log information will be incomplete as not all messages are saved.	Possible solutions: 1. Remove old log files. 2. Lower the log level in Log parameters.
"Client or monitor cannot connect."	Normally this is the result of: 1. Missing port forwarding in the server. 2. Connection block by firewall.	Possible solutions: 1. Check your server configuration. 2. Check your firewall configuration .

- A -

- C -

- H -

- L -

- M -

- P -

- R -

- S -