M2M GPRS Gateway – Control Panel

User Manual

Version 3.20.1

* * * * THIS PAGE IS INTENTIONALLY LEFT BLANK * * *

Table of contents

1. Introduction

The **GPRS Gateway** is a middleware solution that allows easy communication and access to remote units connected by using TCP/IP communication technology. The product works in any network architecture and constitutes a backbone in the communication between RTCU units and back-end/client applications.

The term “**RTCU**” stands for **R**emote **T**erminal **C**ontrol **U**nit and constitutes a unique combination of a programmable control-unit with the possibility of both digital- and analog I/O plus GSM / GPRS or 3G communication.

The **GPRS Gateway** fully supports the advanced **RTCU Deployment Server (RDS)** which is available as a free add-on.

The features include:

- Advanced server architecture that supports thousands of clients and massive traffic.
- It runs as a Windows service. This means that the gateway service will start without Windows log-on and can also be managed remotely as a service.
- Available in a 32-bit and a high-performance 64-bit version.
- Support for up to 32 separately configurable and isolated gateway instances.
- Remote access via the included "Monitor" tool client.
- Full password protection for remote access.
- Up to 10 client keys are supported for more flexible password management.
- Disconnect timeout for inactive clients.
- Advanced filtering feature which allows monitoring/logging on a specific client and/or logging level.
- Encrypted traffic for safer communication.
- Compressed traffic. This reduces the cost of communication.
- Time service for centralized client time management (local/UTC).
- Up to 10 monitor tool clients can be connected simultaneously.
- Plug-in architecture for extending functionality and integration to backbone applications.
- Plug-in developers kit available for free.
- A license must be purchased for clients (100, 250, 500, 1000 clients).

System Requirements

Operating system:	Windows 8/Windows 7/Vista/2003 Server/2008 Server/2010 Server.
Memory:	200 MB + 4 kB per client.
Hard disk space:	3 MB. Additional space required for log-to files.
Other:	Network card. TCP/IP network protocol. (Permanent Internet connection with fixed IP address is recommended.)

Large Packet Support

Large Packet Support (**LPS**) supports the transmission of extended size data-packets over the **GPRS Gateway**.

The standard packet-size over the GPRS Gateway is 480 bytes and by using LPS this is increased to 4064 bytes.

M2M Control IDE / RACP operations such as transfer or large files or applications to/from the device automatically take advantage of the LPS functionality when available. The application can take advantage of LPS by using gwSendPacket / gwReceivePacket. Please consult the M2M Control IDE documentation.

Limitations:

- Supported by all NX32 architecture devices.
- Requires firmware V4.40 or later.
- Requires GPRS Gateway V3.20 or later.

Time Service

The GPRS Gateway 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 M2M Control IDE online documentation and the "GPRS Gateway Configuration" section.

License

Licenses of 100, 250, 500 and 1000 clients can be ordered. Please contact M2M Control for more information.

2. The GPRS Gateway Architecture

The GPRS Gateway is a middleware solution which is used for communicating with remote RTCU units by using any TCP/IP-enabled communication media (e.g. GPRS, UMTS, HSDPA or LAN).

One of the most important function of the GPRS Gateway is to allow access to connected units 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 gateway clients.

The GPRS Gateway also includes:

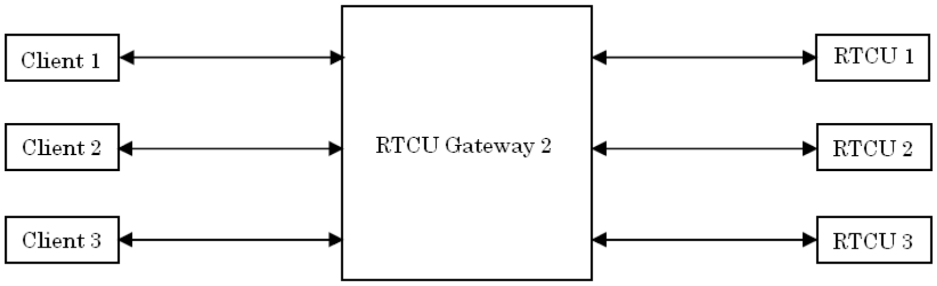
- Security functions.
- Local/remote maintenance.
- Logging features.
- Unit recovery after application failure.

The merging of SMS and TCP/IP technology is made possible with the M2M Control 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 GPRS Gateway 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 units 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.

M2M Control offers a 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 GPRS Gateway architecture can be illustrated like this:



The client is communicating with the GPRS Gateway by using the RACP2 protocol. The message that has been sent from the client to the gateway will be forwarded to the RTCU unit by using the TCP/IP connection (again by using the RACP2 protocol). The response sent from the RTCU unit 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 units is also possible by using the GPRS Gateway.

To use the GPRS Gateway, the client and the RTCU unit need to be supplied with the IP address, port number, and password of the GPRS Gateway.

The GPRS Gateway runs as a Windows service and therefore it runs independently of user logon.

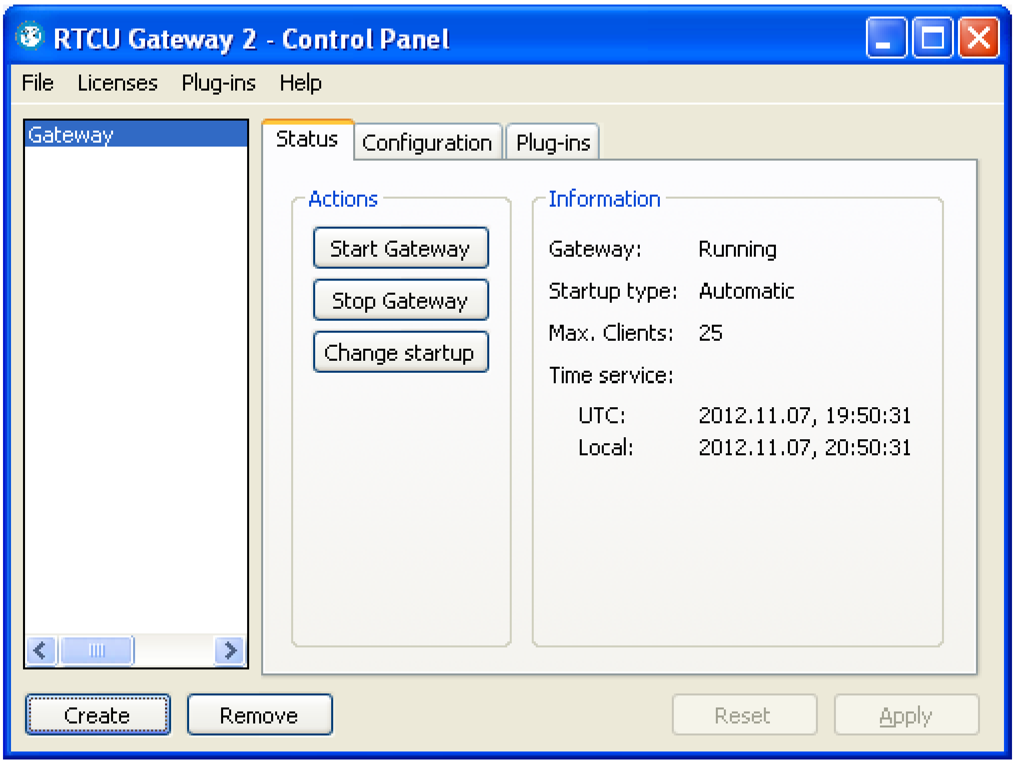
A complete GPRS Gateway setup consist of:

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

3. Control Panel

The "GPRS Gateway - Control Panel" is where the gateways are managed.

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

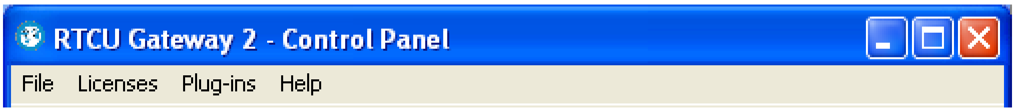


Gateway: Running
Startup type: Automatic
Max. Clients: 25
Time service:
UTC: 2012.11.07, 19:50:31
Local: 2012.11.07, 20:50:31

The interface can basically be split into two areas - the Gateway list and the Gateway management areas.

3.1. Menuitems

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



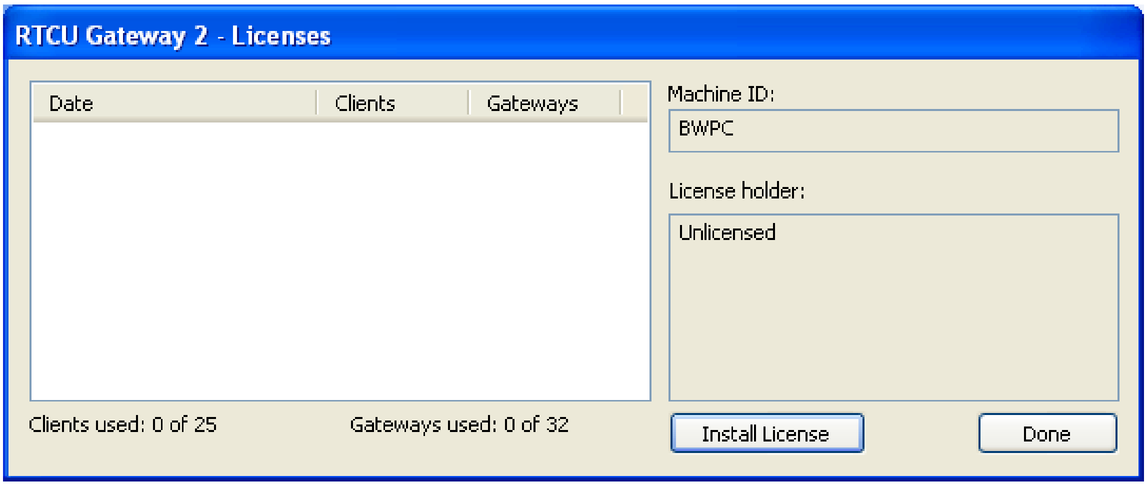
- File
- Licenses
- Plug-ins
- Help

3.1.1. Menu item: File

The "Exit" command ends the Control Panel program.

3.1.2. Menu item: Licenses

The "Licenses" dialog shows the licenses that are installed on the server.
When no license is installed, the GPRS Gateway accepts 25 clients on a maximum of 32 gateways.
For example, it is possible to create one gateway with all 25 clients or two gateways - one with 15 clients and one with 10 clients.



Date	Clients	Gateways

Machine ID: BWPC

License holder: Unlicensed

Clients used: 0 of 25

Gateways used: 0 of 32

Additional licenses can be ordered from M2M Control to support more clients and gateways.
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 M2M Control, follow these steps:

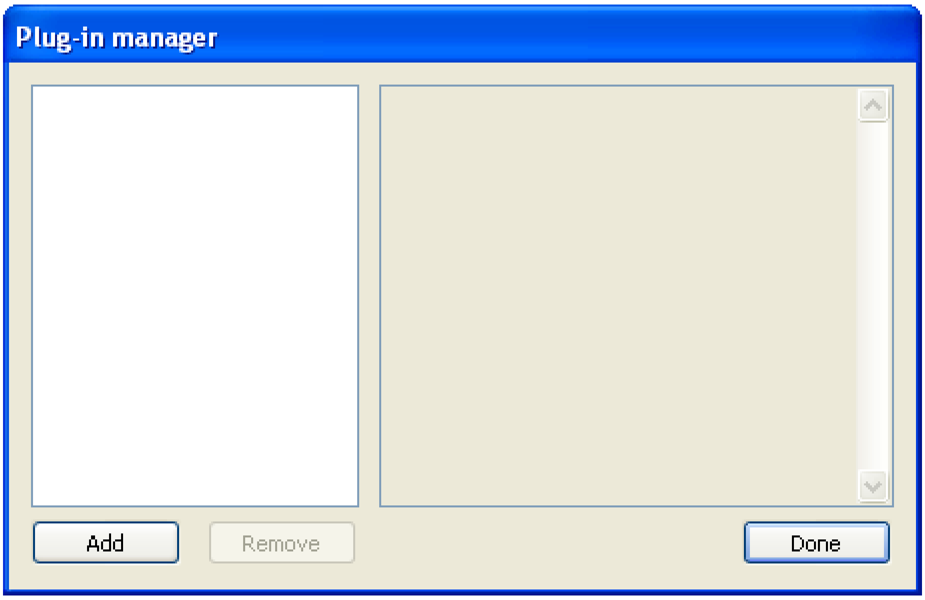
1. Open the Control Panel.
2. Go to the Licenses dialog.
3. Press the "Install License" button.
4. Select the license file in the file dialog.

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

3.1.3. Menu item: Plug-ins

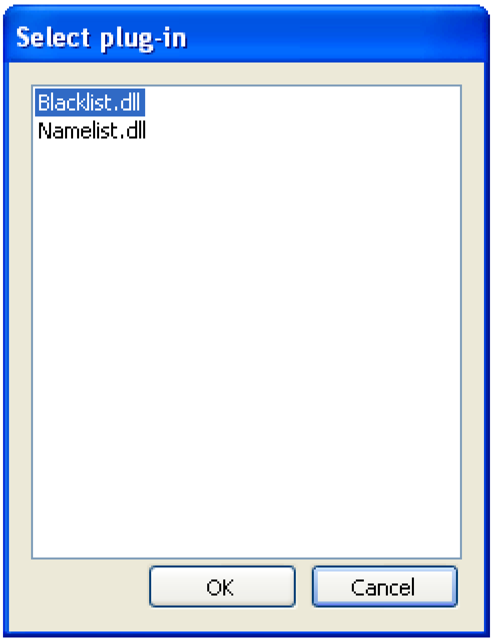
Plug-ins are DLL libraries that can be installed dynamically to extend the functionality of the GPRS Gateway.
A plug-in can be developed by using the free GPRS Gateway plug-in developers kit.

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

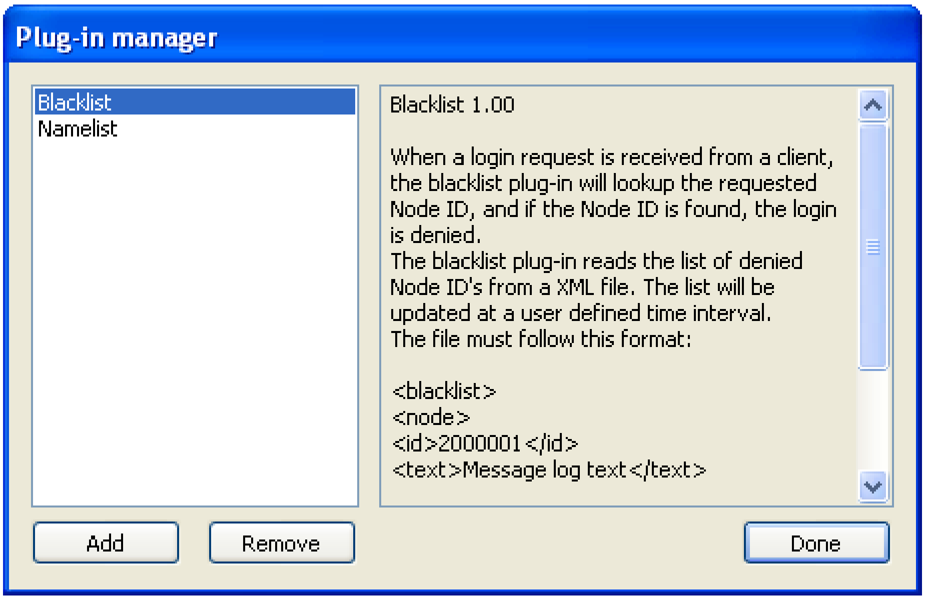


To add a plug-in, follow these steps:

1. Copy the plug-in DLL to the "Plugins" folder in the Gateway install directory.
   (This step is not necessary for the standard plug-ins that come installed with the GPRS Gateway.)
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.



Blacklist 1.00

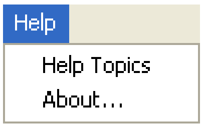
When a login request is received from a client, the blacklist plug-in will lookup the requested Node ID, and if the Node ID is found, the login is denied.
The blacklist plug-in reads the list of denied Node ID's from a XML file. The list will be updated at a user defined time interval.
The file must follow this format:

```
<blacklist>
<node>
<id>2000001</id>
<text>Message log text</text>
```

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

3.1.4. Menu item: Help

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



The individual items:

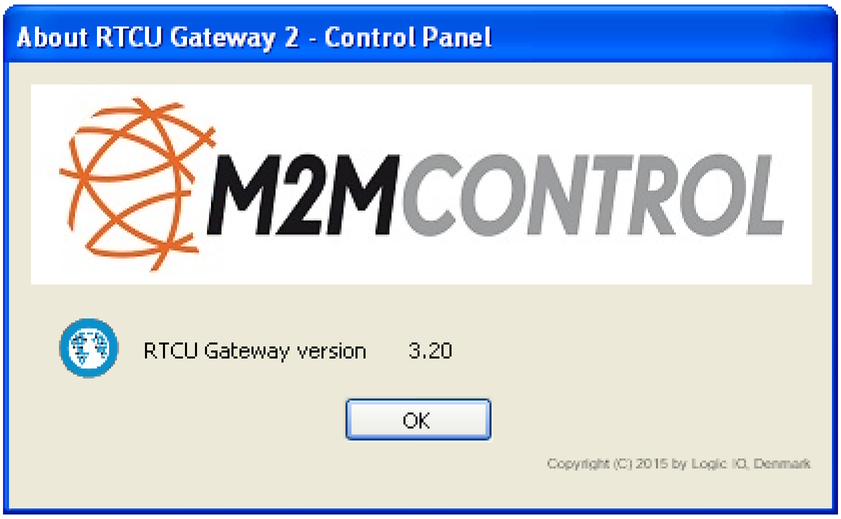
- Help topics
- About

3.1.4.1. Help - Help topics

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

3.1.4.2. Help – About

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

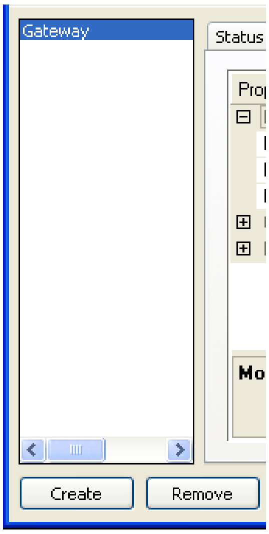

About RTCU Gateway 2 - Control Panel

RTCU Gateway version 3.20

Copyright (C) 2015 by Logic IO, Denmark

3.2. Gateway List

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

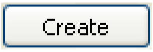


To manage a gateway instance, select it in the list and use the gateway management pages to configure it.

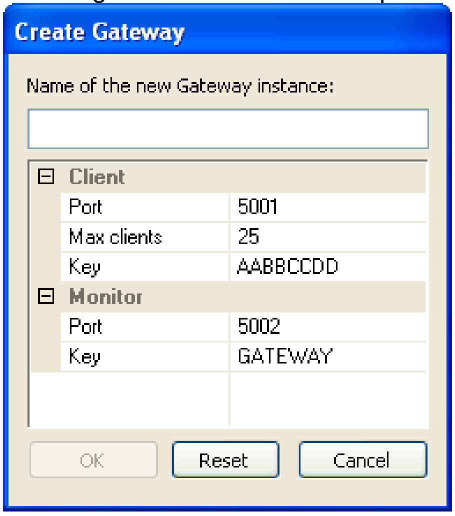
A new gateway can be created with the "Create" button if there are gateway licenses left.

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

3.2.1. Create gateway



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



Create Gateway

Name of the new Gateway instance:

⊟ Client	
Port	5001
Max clients	25
Key	AABBCCDD
⊟ Monitor	
Port	5002
Key	GATEWAY

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

Name of the Gateway Instance
The name of the gateway 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 "Gateway (5001)".

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

- Client parameters
- Monitor parameters

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

3.2.2. Remove gateway

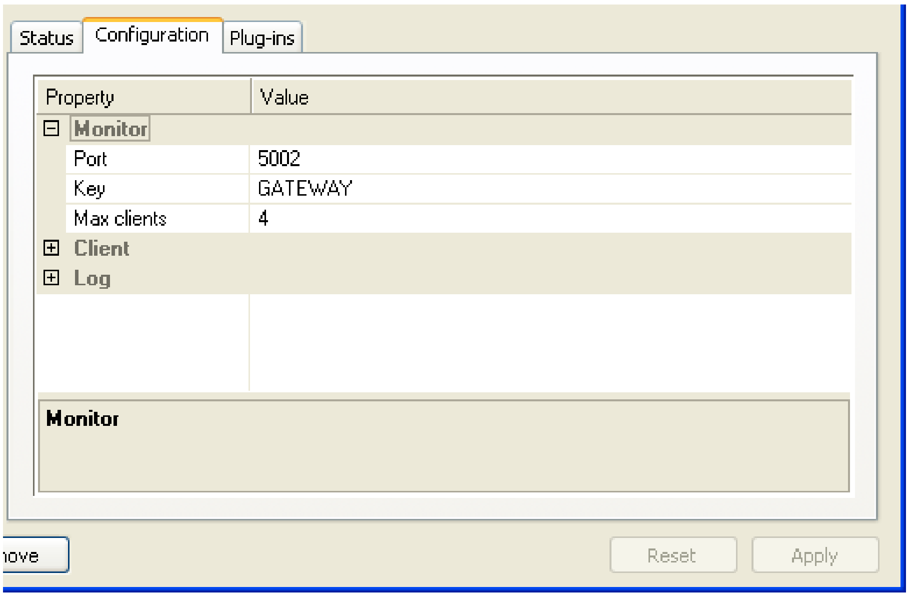
Pressing the above button will completely remove a gateway instance from the server. The service will be removed, including its configuration, and the maximum number of clients will be freed for the other gateway instances.
The log files will not be removed.

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

The gateway instance must be stopped before removing it.

3.3. Gateway management

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



Property	Value
⊟ Monitor	
Port	5002
Key	GATEWAY
Max clients	4
⊞ Client	
⊞ Log	

Monitor

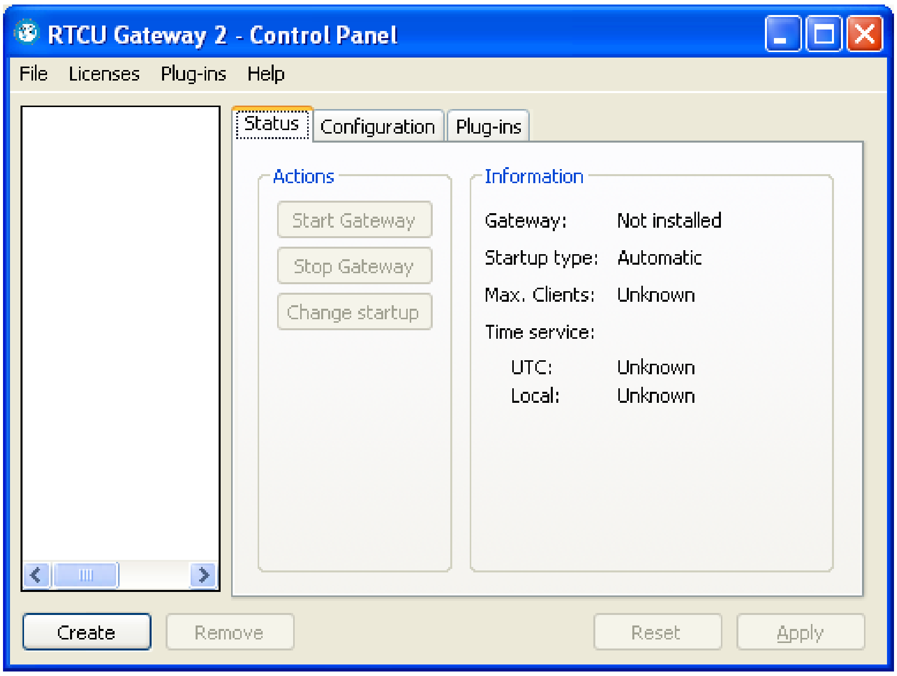
The management pages consist of:

- Gateway Status
- Gateway Configuration
- Gateway plug-ins

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

3.3.1. Gateway Status

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



Gateway: Not installed
Startup type: Automatic
Max. Clients: Unknown
Time service:
UTC: Unknown
Local: Unknown

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

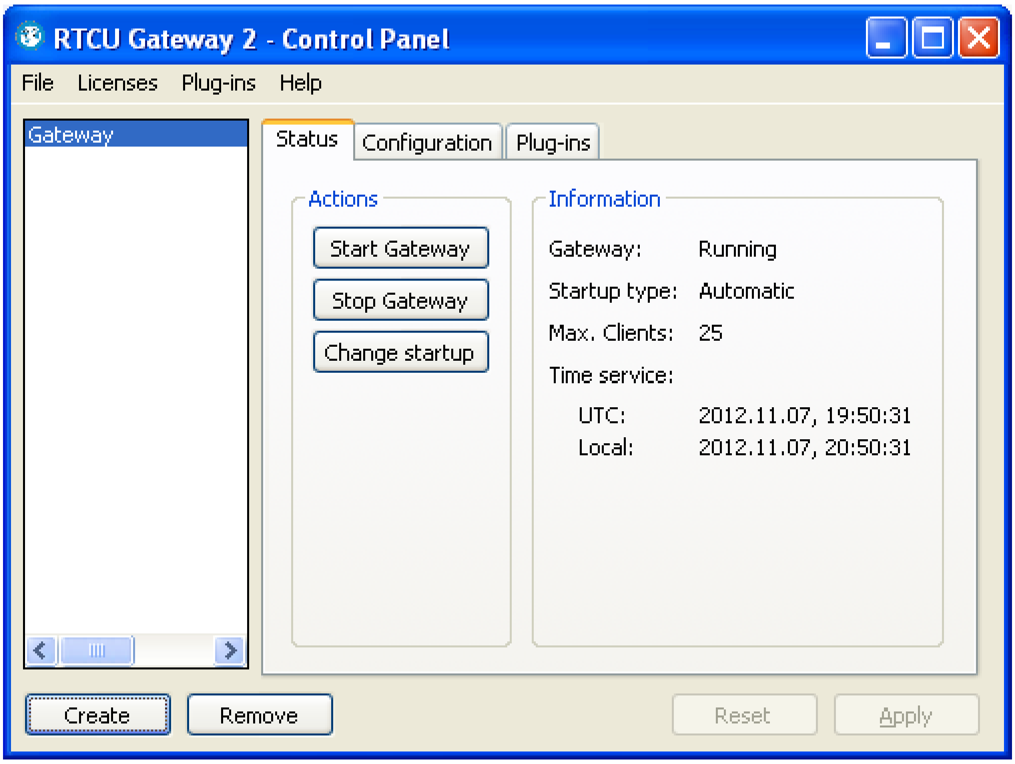
The "Information" group contains the status of the gateway instance.
The items can have the following states:

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

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

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

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

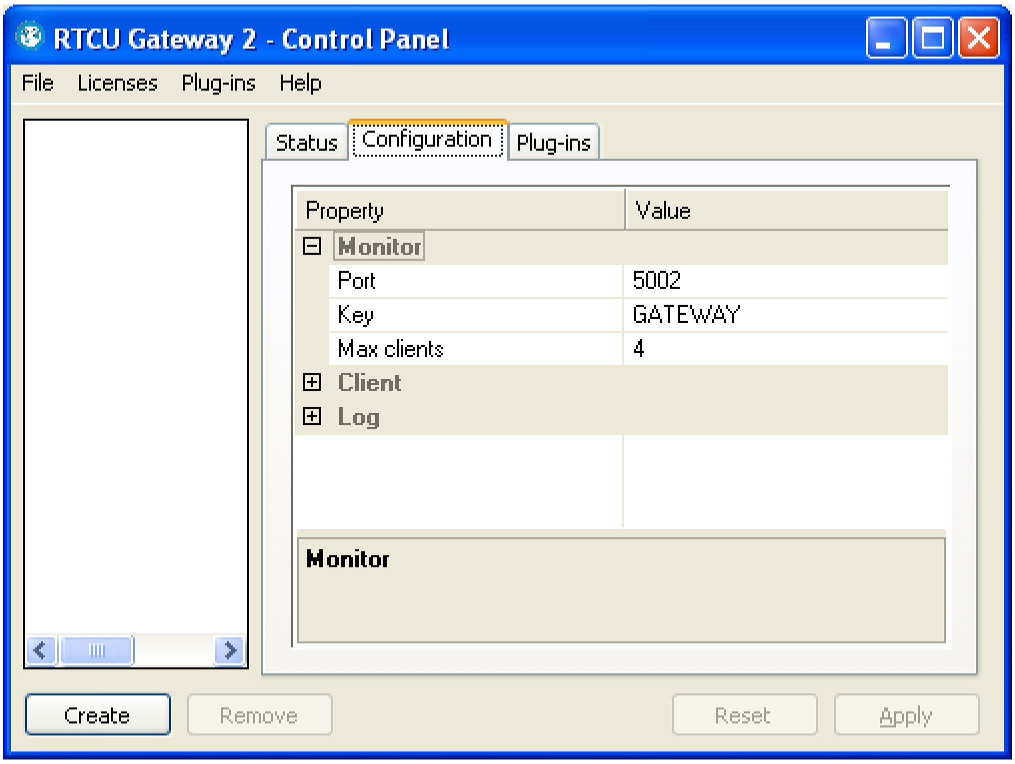


Information

Gateway: Running
Startup type: Automatic
Max. Clients: 25
Time service:
UTC: 2012.11.07, 19:50:31
Local: 2012.11.07, 20:50:31

3.3.2. Gateway Configuration

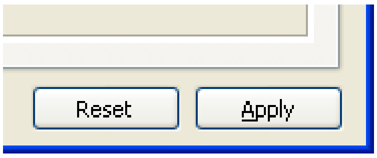
The "Configuration" page is where the configuration of the selected gateway instance is managed.



Property	Value
⊟ Monitor	
Port	5002
Key	GATEWAY
Max clients	4
⊞ Client	
⊞ Log	

Monitor

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

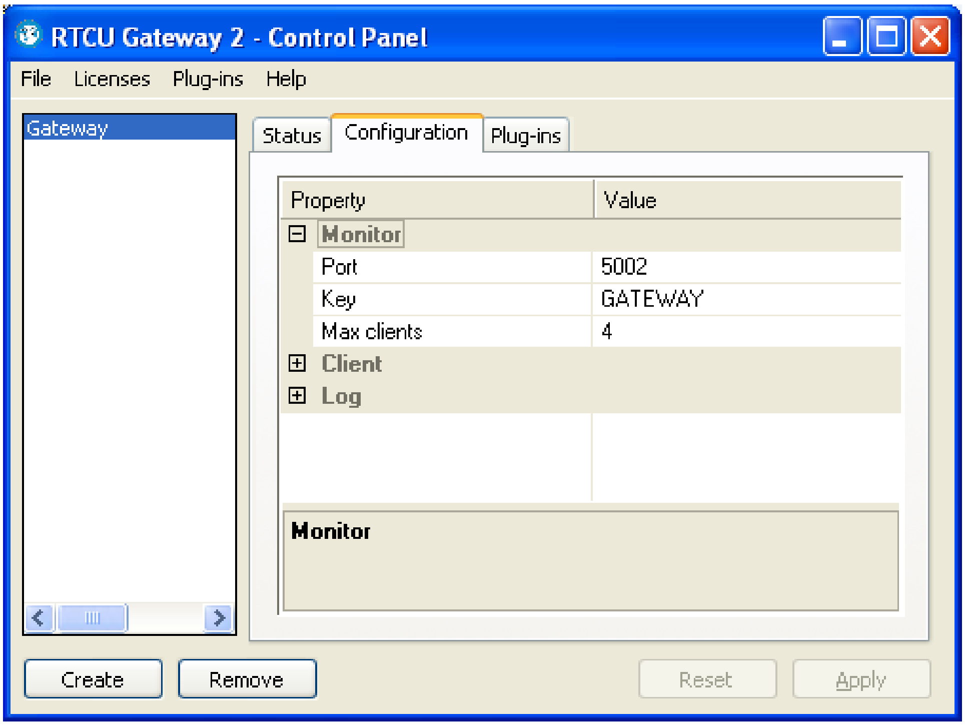


Press the Apply button to save the configuration. The gateway will use the new configuration when it is restarted.
Press the Reset button to clear all changes made to the configuration.

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

- Monitor parameters
- Client parameters
- Log parameters

3.3.2.1. Monitor parameters


RTCU Gateway 2 - Control Panel
File Licenses Plug-ins Help
Gateway
Status Configuration Plug-ins
Create Remove Reset Apply

Property	Value
⊟ Monitor	
Port	5002
Key	GATEWAY
Max clients	4
⊞ Client	
⊞ Log	

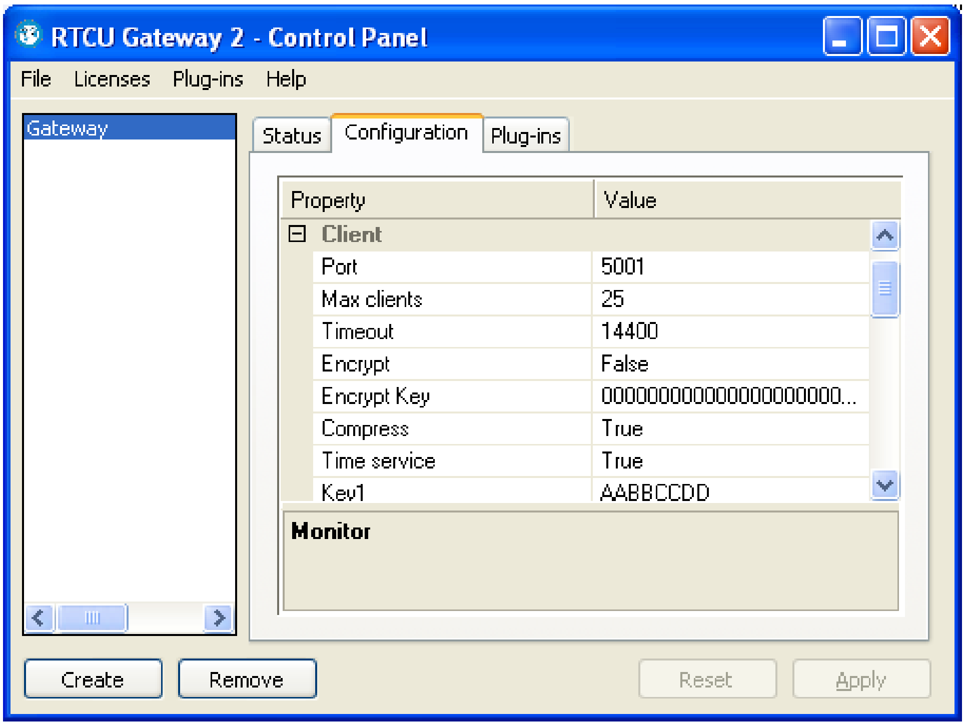
Monitor

Port — The IP port where the gateway 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 gateway instance. The default is 4 clients but up to 10 is supported.

3.3.2.2. Client parameters



Property	Value
⊟ **Client**	
Port	5001
Max clients	25
Timeout	14400
Encrypt	False
Encrypt Key	000000000000000000000...
Compress	True
Time service	True
Key1	AABBCCDD

Port
The IP port where the gateway instance will listen for clients.

Maximum clients
The maximum number of clients that are allowed to connect to the gateway instance.
This number is dictated by the license.

Timeout
The time without transactions before the gateway 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.

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.

Time service
Enables/disables the "Time" service.
Enabling the Time service will allow clients to request the local or UTC time from the gateway 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 gateway instance clients.

Key2
The access key #2 for the gateway instance clients.

Key3
The access key #3 for the gateway instance clients.

Key4
The access key #4 for the gateway instance clients.

Key5 The access key #5 for the gateway instance clients.

Key6 The access key #6 for the gateway instance clients.

Key7 The access key #7 for the gateway instance clients.

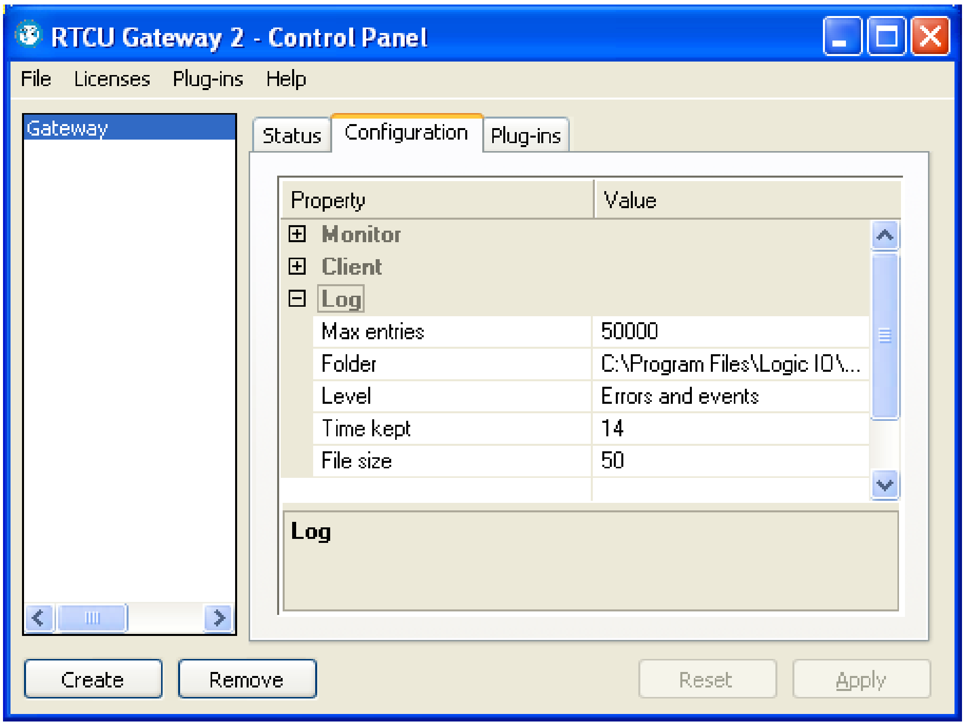
Key8 The access key #8 for the gateway instance clients.

Key9 The access key #9 for the gateway instance clients.

Key10 The access key #10 for the gateway instance clients.

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

3.3.2.3. Log parameters



Property	Value
⊞ Monitor	
⊞ Client	
⊟ Log	
Max entries	50000
Folder	C:\Program Files\Logic IO\...
Level	Errors and events
Time kept	14
File size	50

Log

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 gateway instance.

Folder The directory path the gateway instance uses when logging to files. The gateway instance will create a folder with the gateway name in this directory, and in this a folder for each day is created.
The log files are stored in <folder>\<gateway name>\<date>\.
For example: C:\Logs\Gateway\2012-08-24\file001.log.

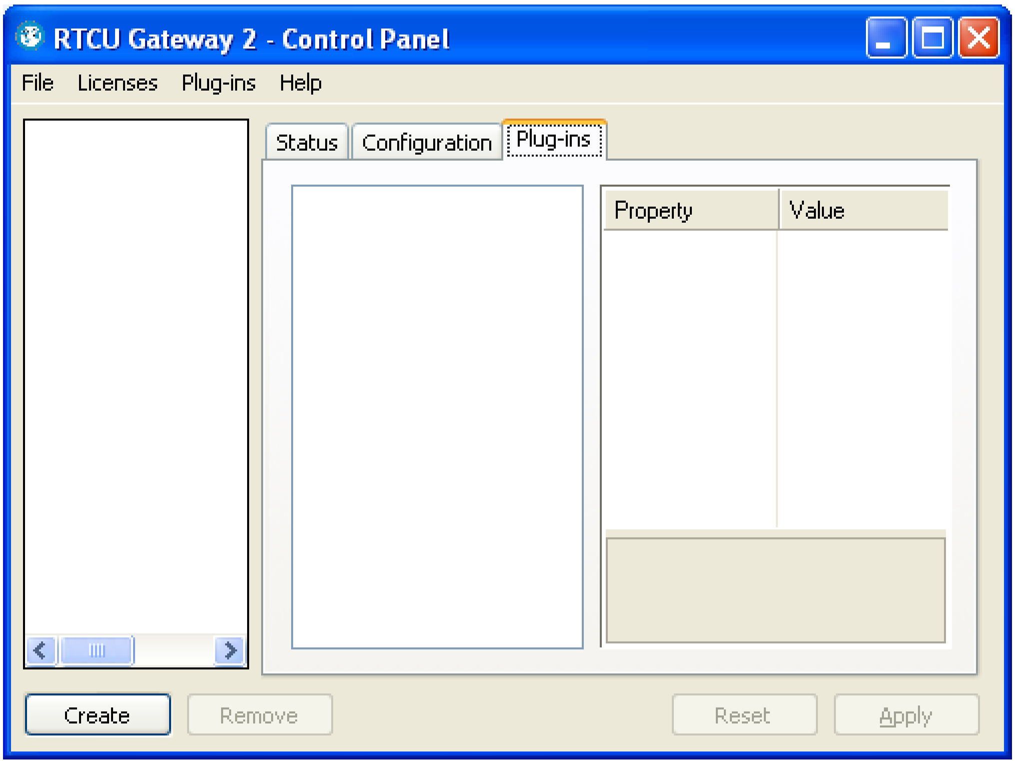
Level The level of logging that is used by the gateway instance for the log files.

Time kept The number of days the log files are stored on the server before being deleted.

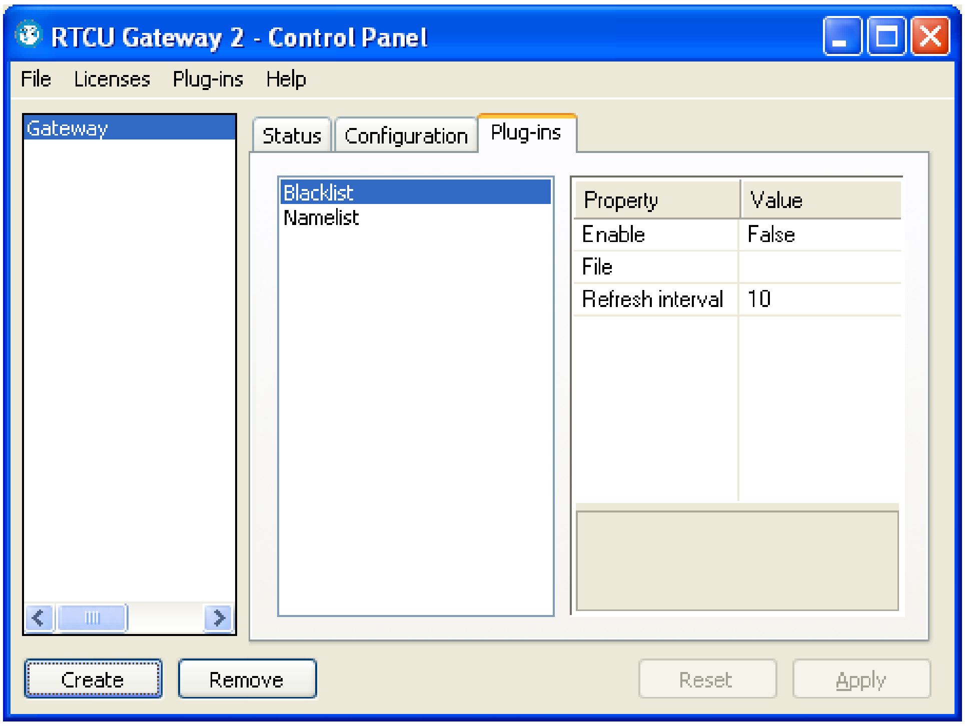
File size The maximum size of a log file before the gateway starts on a new file. The size is given in MB.

3.3.3. Gateway plug-ins

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



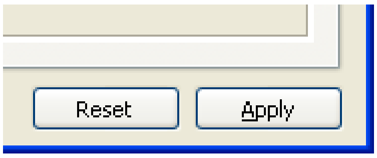
On the left side of the page, a list of the plug-ins added in the Plug-in Manager can be seen. On the right of the page, the available properties for the selected plug-in can be seen.



Property	Value
Enable	False
File	
Refresh interval	10

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 gateway instance. A disabled plug-in will not be loaded by the gateway service.

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



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

4. Standard Plug-ins

The GPRS Gateway includes a plug-in framework for easy extension of the gateway functionality.

The following standard plug-ins are included in the GPRS Gateway server installation:

- Blacklist This plug-in will prevent clients from connecting to the gateway based on their Node ID.
- 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 "GPRS Gateway Plug-In Developers Kit" that also includes the full source code to the above plug-ins.

4.1. Blacklist

The "Blacklist" plug-in will compare the Node IDs of all clients that try to log on to the gateway 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 gateway instance.

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>
```

4.2. 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 gateway instance.

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>
```

5. Trouble Shooting 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 gateway. 2. Connection block by firewall.	Possible solutions: 1. Check your gateway configuration. 2. Check your firewall configuration .

Infranet Technologies GmbH
Tempowerkring 19
21079 Hamburg
Germany

Fon: +49 40 696 47 – 260