Secure Remote Access

Contents

1 Symbols Used

To make working with the training manual easier and more comfortable, 3 different symbols are used. These symbols should simplify navigating through the documentation, provide additional information, highlight important sections, and introduce examples. The meanings of the 3 symbols are as follows:

Attention

This symbol means that the information directly following requires your complete attention. The information here is VERY IMPORTANT and should be NOTED. It is recommended that the paragraph next to this symbol be thoroughly read.

Tip

The thumb symbol identifies a help tip that explains how something can be done faster or better.

Example

This symbol indicates the beginning of an example.

2 Quick Start

The essential steps for remotely connecting a machine using the SIGMATEK Remote Access Platform (RAP) consists of:

1. Register for an RAP company/user account on first-use, p21
2. Setup the remote product as relevant:
    a. RAR hardware, p6
    b. RAE application, p15 (not required for RAR)
3. Register the device on first use.
    a. RAR using ethernet, p26
    b. RAR using WIFI, p29
    c. RAR using cellular services 3G/4G, p31
    d. RAE application, p32
4. Connect controls to the RAP. Examples are presented:
    a. RAR, p65
    b. RAE, p73
5. Add remote services:
    a. VNC, p39
    b. Port forward for IP services, p33
    c. Data logging, p43

3 Remote Access Router Hardware Setup

3.1 Electrical Connection

3.1.1 Wiring the RAR

- The RAR must be supplied with 12-24 V voltage by connecting the supply voltage.
- Shielding should be connected to the protective earth (PE).
- Install cables using ferrules to reduce strain on the wires.
- A digital input is available for hardware-based management of the VPN connection
    - By default, the digital input is not configured and does not need to be wired.

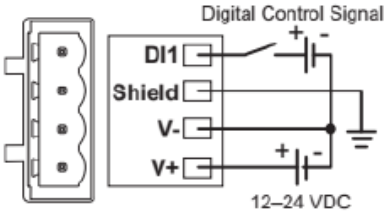


Figure 3.1 Power input connector pin designations.

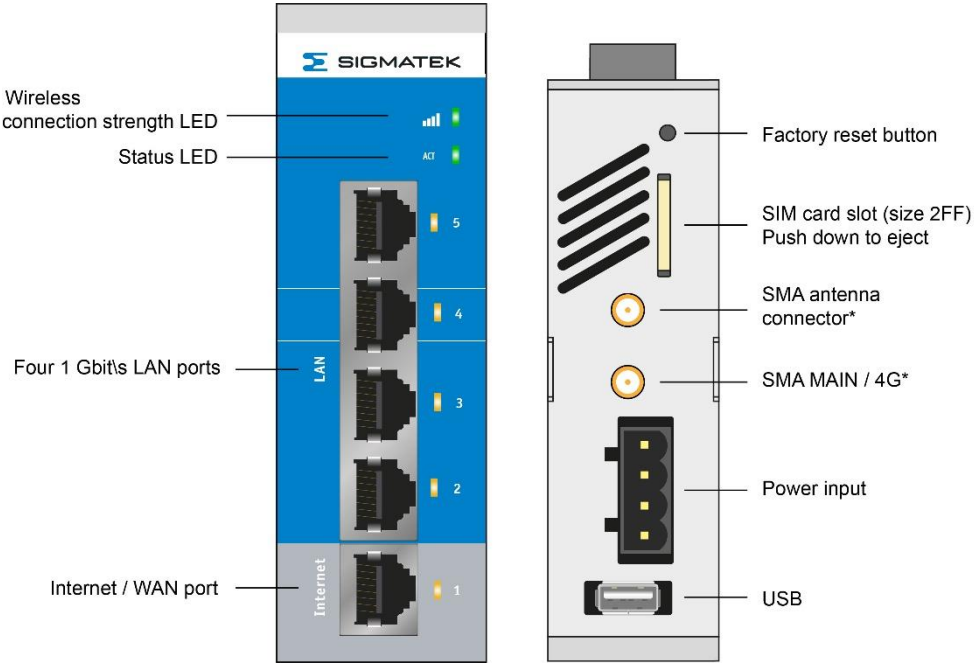


Figure 3.2 Diagram of the RAR.

3.1.2 Optional hardware switch for VPN management

The digital input DI1 may be used to disable the VPN; this option must be enabled via the RAP:

1. Ensure the device electrical wiring is complete (Figure 3.3) and it has been registered with the RAP. Refer to section 5.3 for registration.
2. On the RAP, select the device to be configured.
3. Locate the WAN settings; click “show more” (Figure 3.4).
4. A new control labelled “digital input” will be displayed (Figure 3.5); select one of the options:
    a. disabled [digital input inactive],
    b. disable VPN when [digital] input low,
    c. disable VPN when [digital] input high.
5. Store and apply the configuration to the device.

Figure 3.3 RAR with switch installed on digital input 1.

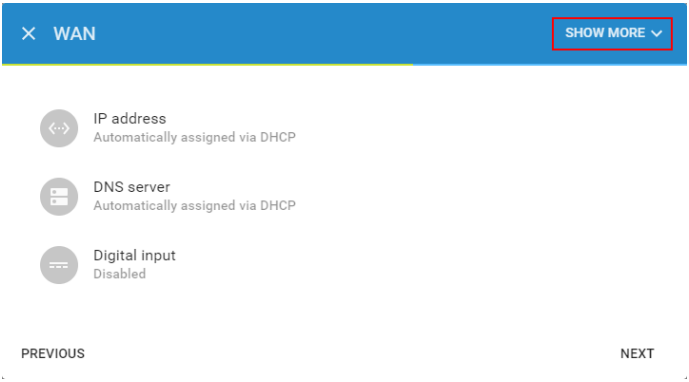


Figure 3.4 WAN settings in the RAP.

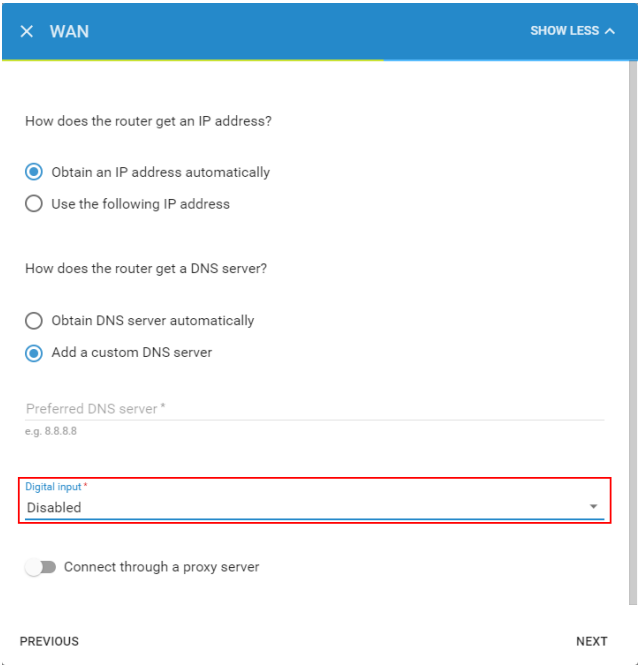


Figure 3.5 Selecting the action, on the VPN management, of the digital input.

3.2 Preparing Hardware with Optional Interfaces

3.2.1 Cellular – 3G/4G

With power off:

1. Insert the SIM card into the SIM card slot (Figure 3.6).
2. Screw the antenna onto the SMA connector marked “MAIN” (Figure 3.7).

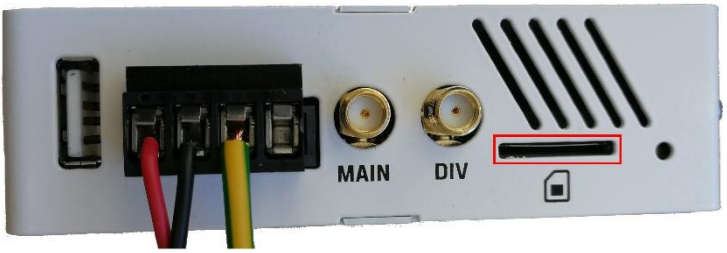


Figure 3.6 RAR with sim card marked red.

Figure 3.7 RAR with cellular option: 3G/4G antenna installed on the SMA connector for the cellular radio.

3.2.2 WIFI

With power off: connect the WIFI antenna to the RAR using the SMA connector marked “DIV”.

Figure 3.8 RAR with WIFI antenna installed on the SMA connector for the 2.4 GHz radio.

3.2.3 Using WIFI RAR as an Access Point (AP)

To setup an access point (AP) on the RAR using RAP:

1. Ensure the device electrical wiring is complete (Figure 3.3) and it has been registered with the RAP. Refer to section 5.3 for registration.
2. On the RAP, select the device to be configured.
3. On the config page, edit the LAN settings.
4. Click on the slide switch labelled “Enable Wi-Fi hotspot”.
5. Assign the SSID and password as required.
6. Click “confirm” to store the settings.
7. Additionally, via the firewall settings it is possible to restrict or permit access to the internet and/or the host network.
8. Push changes to the router to activate the new configuration.

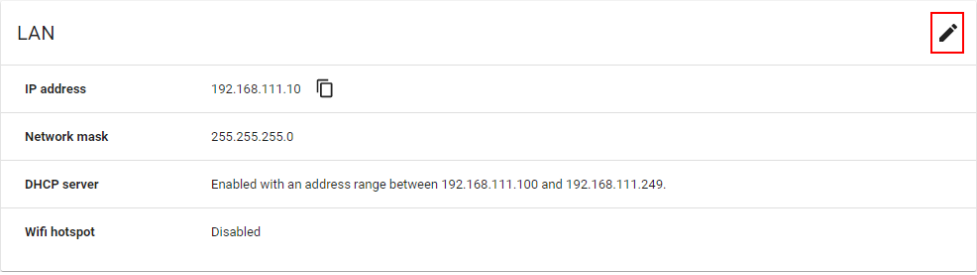


Figure 3.9 Edit the LAN settings.

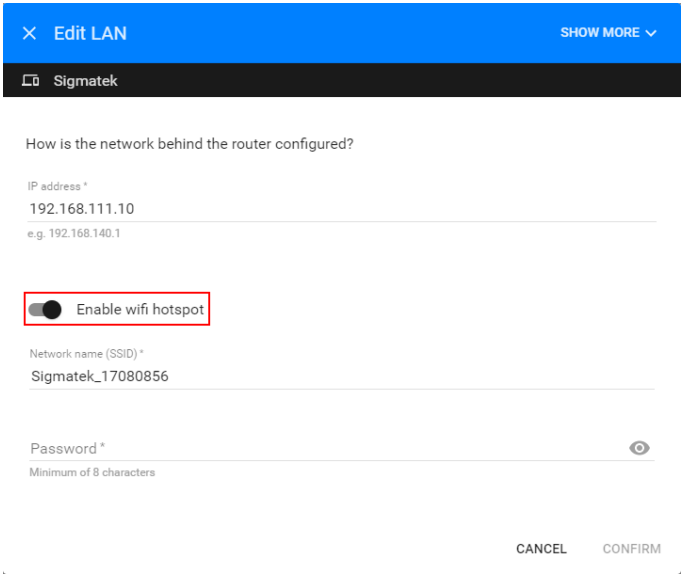


Figure 3.10 LAN settings: enable and configure the wifi hotspot (AP).

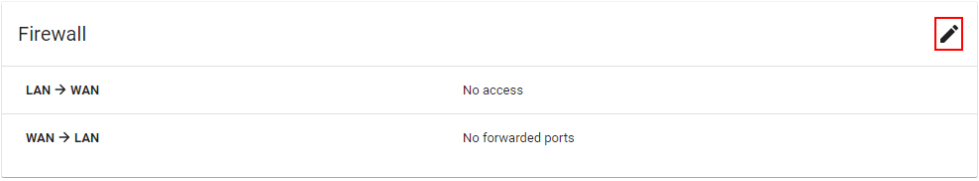


Figure 3.11 Edit the firewall settings to configure access via the AP to the internet and host networks.

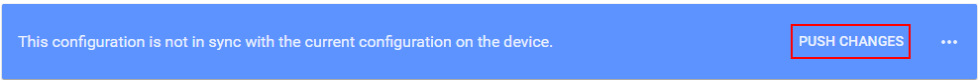


Figure 3.12 Configuration changes must always be pushed to the RAR to take effect.

3.3 LED Status Display

3.3.1 Signal LED

	Blue blinking	Initializing the mobile radio module
	Red blinking 1 pulse	No receive or no connection to the network possible (APN or SSID may be wrong)
	Red blinking 2 pulses	PIN invalid or PUK required (A phone is required to unlock the SIM card with PUK)
	Red blinking 4 pulses	SIM card is invalid or missing
	Constant red	Connected, poor signal
	Constant violet	Connected, medium signal
	Constant blue	Connected, good signal

3.3.2 ACT Signal LED

	Constant red	**Boots (can take 1-2 minutes) or not yet registered**
	Red blinking 1 pulse	Waiting for Internet access
	Red blinking 3 pulses	LAN/WAN conflict (conflicting subnets)
	Red blinking 4 pulses	Removed from the platform RAR must be re-configured and registered
	Red blinking 5 pulses	Previously registered at RAP (remove from RAP and register again)
	Blue blinking 1 pulse	Establishing connection with RAP
	Blue blinking 2 pulses	Initialising VPN connection
	Constant blue	Active VPN connection

4 Remote Access Embedded Setup

4.1 Requirements

The RAE package was developed especially for the operating system Salamander, which is the prerequisite for the software solution.

- To install RAE on the SIGMATEK control, the OS version must be:
  - Salamander >= 09.03.102.
- The SIGMATEK control on which RAE100 is installed must have a valid IP configuration with access to the Internet.

4.2 Setup

This process describes the test procedure for preparing a SIGMATEK control with RAE.
The remote product must be registered after setup.

1. Open LASAL Class 2 and establish a connection to the HMI.
2. The IP configuration can be set via LASAL CLASS 2: "Debug → File Transfer → Edit Autoexec.lsl" as shown in Figure 4.13.
3. Apply settings valid for the current LAN (Figure 4.14):
   a. IP address
   b. IP subnet
   c. IP gateway: IP address of the router used to access the internet
   d. IP DNS: IP address of a DNS server reachable from the current location, some server addresses are given below:
      i. Cloudflare 1.1.1.1
      ii. Google 4.4.4.4 or 8.8.8.8
4. Using the PLCDiag tool File Commander under "Tools → Advanced Debug Tools → File Commander" create the folder "C:\lslsys\packages" on the machine if it does not already exist.
   a. To create a folder use "MAKE DIR" (Figure 4.15, Figure 4.16).
   b. Copy the RAE to the packages folder. To do this, navigate to the package on the right side of the File Commander and click on "COPY" (Figure 4.17).
5. To install RAE, enter the command in the Command Line Interface.
   a. Open the Remote CLI under "Tools → Advanced Debug Tools → Remote CLI" (Figure 4.18).

b. Enter the command "PACKAGE INSTALL ixagent" in the command line and press Enter or "Execute" (Figure 4.19). Installation may take some time. Wait for the return (Figure 4.20).

c. After RAE is installed, it must be enabled with the command "ixagent start" (Figure 4.19). Wait for the return (Figure 4.20).

d. To check internet connection, via the Remote CLI enter the command "ping www.google.com" (or a site accessible from your region) in the command line and press Enter or "Execute". If the machine can reach the internet a latency value will be reported for the ping command.

e. The RAE application must be started after installation:

   i. On-demand the command “ixagent start” may be executed from the Remote CLI (Figure 4.21).

   ii. For automatic start-up with the machine, the same command “ixagent start” should be appended to the Autoexec.lsl (Figure 4.22).

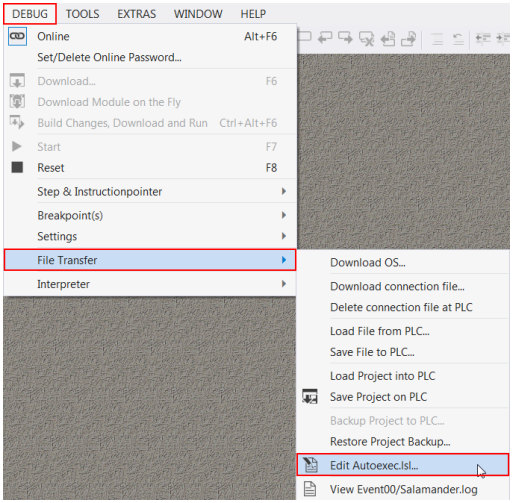


Figure 4.13 Editing the Autoexec.lsl from Class 2.

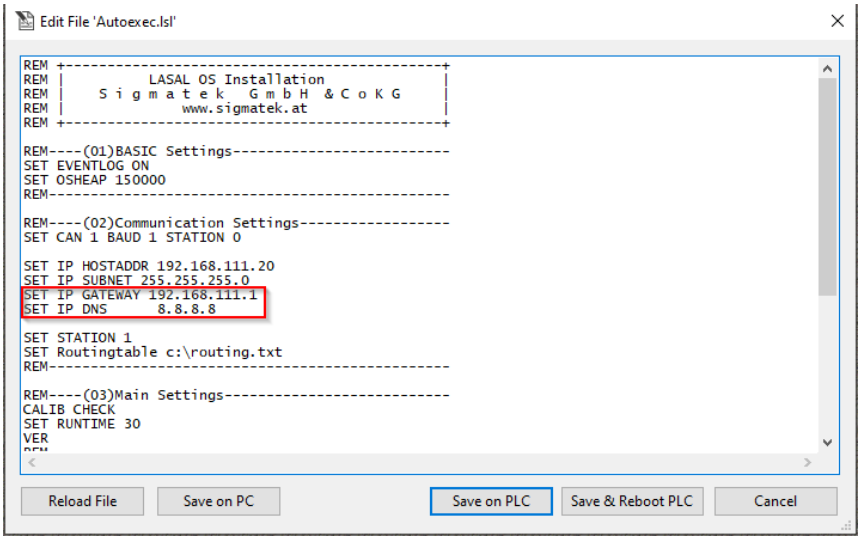


Figure 4.14 Editing the IP configuration.

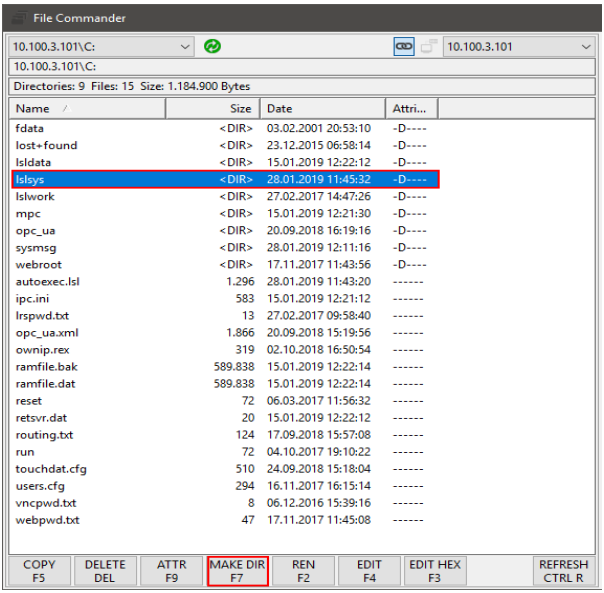


Figure 4.15 File Commander interface - Make Dir button highlighted.

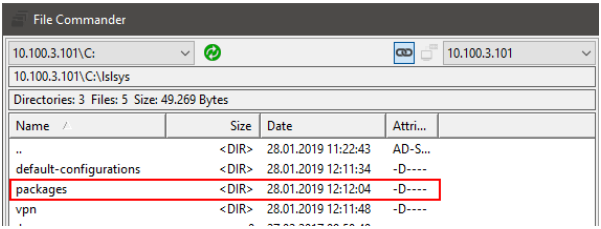


Figure 4.16 Packages folder within C:\lslsys

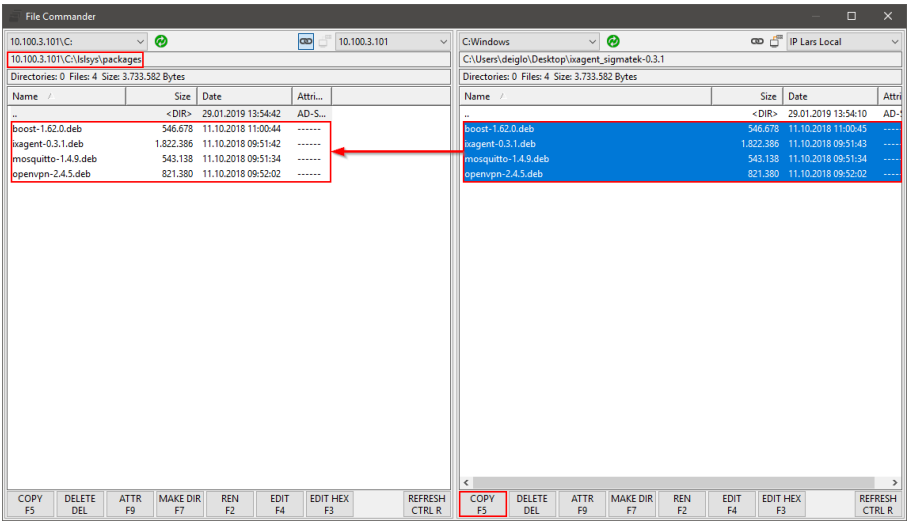


Figure 4.17 Copying the packages to the machine.

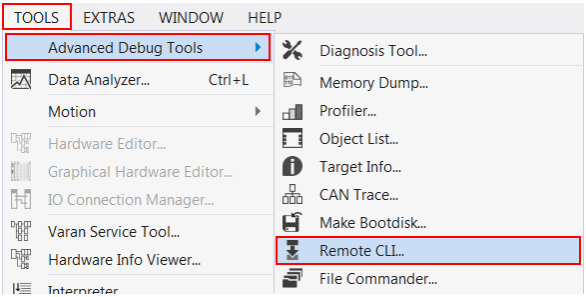


Figure 4.18 Opening the Remote CLI tool.

Figure 4.19 Executing the RAE application install command via the CLI.

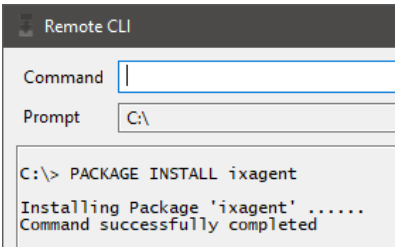


Figure 4.20 Installation successful confirmation.

Figure 4.21 Starting the RAE application.

```
SET IP HOSTADDR 192.168.111.20
SET IP SUBNET 255.255.255.0
SET IP GATEWAY 192.168.111.1
SET IP DNS      8.8.8.8

IXAGENT START
```

Figure 4.22 Appending the RAE application start command to the Autoexec.lsl

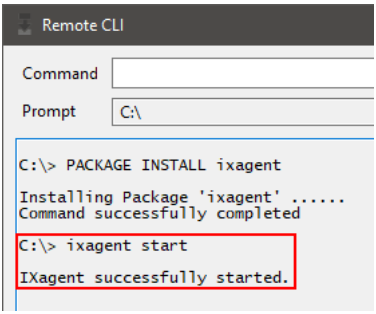


Figure 4.23 Confirmation message that the RAE application started successfully.

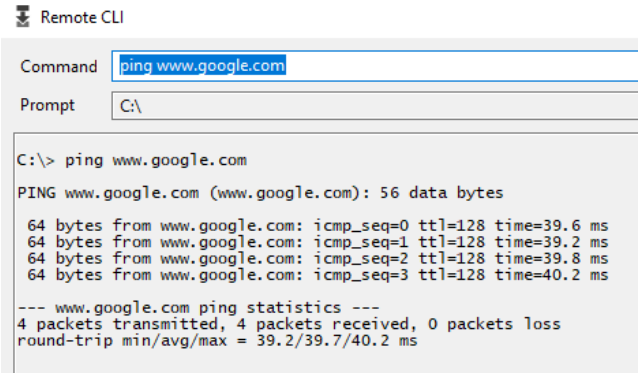


Figure 4.24 Executing the PING command against a domain with web server supporting ICMP echo response.

5 Remote Access Platform (RAP)

The remote access platform is the user interface for the SIGMATEK router and application products. A user account is required to register new devices and remotely access data.

5.1 Account Setup

If you have not yet created a company account, please register with the Remote Access Platform.

1. Open the RAP main page: https://www.sigmatek-connect.com. To register, click on the link labelled “Don’t have an account? Register” (Figure 5.25).
2. Enter requested details and confirm acceptance of the terms to proceed (Figure 5.26).
3. If registration is successful an email will be sent to the registered address. The link must be clicked to activate the user account (Figure 5.27).

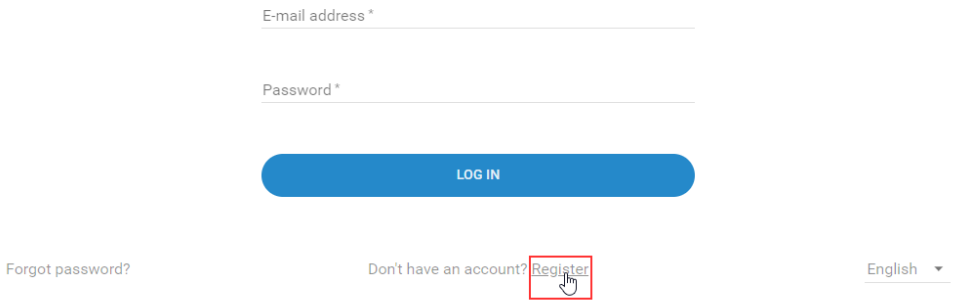


Figure 5.25 RAP: registering for a new company account.

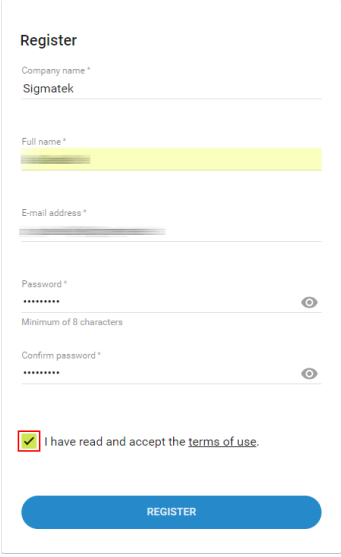


Figure 5.26 RAP: entering requested details.

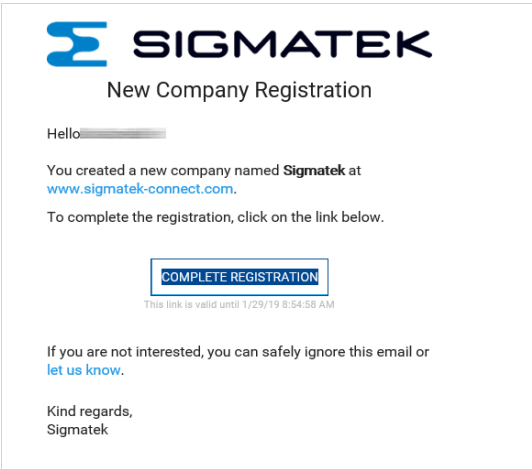


Figure 5.27 RAP: complete the registration by clicking on the button sent via email.

5.2 RAP Cloud Interface

To log in to the platform:

1. Go to the main page https://www.sigmatek-connect.com.
2. After entering login data click on "LOG IN".
3. Select the company required to view and register new devices.

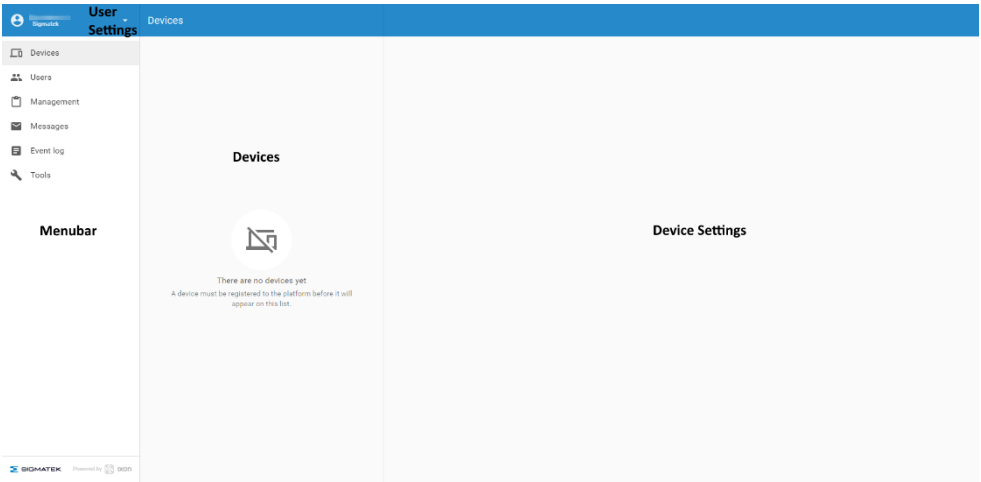


Figure 5.28 RAP main interface for a selected company.

5.2.1 Main Menu

- Devices – view registered devices and change their settings.
- Management - device management.
- Messages - alarms related to the "Notification System".
- Event log – displays all events of users, devices, and settings.
- Tools – device registration.

5.2.2 User Settings

The User Settings can be opened by clicking on the white arrow (Figure 5.29); it provides access to:

- Profile Settings – localisation, email address, security, and view permissions
- Company Settings – add sub-companies and RAP branding
- Billing information
- Switch company – when managing multiple companies from a single user account

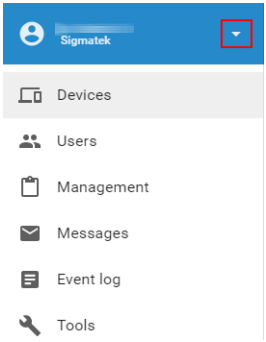


Figure 5.29 Opening the User Settings from the main interface.

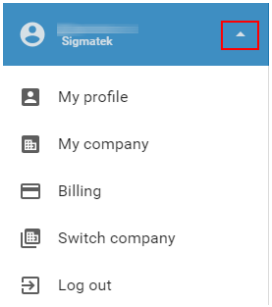


Figure 5.30 User Settings menu

5.3

5.4 Registering a remote product

For the RAR to establish a connection to the cloud, it must be configured: a config file is created and downloaded.

5.4.1 Factory Reset

A config file must be created to configure the router. Before the config file is transferred to the router, a factory reset should be performed if the router has already been registered before.

Attention The **factory reset deletes** the router **configurations**. This includes WAN/LAN settings, port forwarding, IP services and data upload.

Ensure that the old configuration is no longer required.

With the RAR powered, press the small button on the router for 5 seconds until the ACT LED starts flashing blue-red.

Figure 5.31 Location of the reset button

5.4.2 Remote Access Router using ethernet WAN

From the RAP main menu:

1. Click on the Tools option.
2. Click on “Start Configuration” under Configuration file (Figure 5.32).
3. Select a company to register the device with (Figure 5.33).
4. Select the type of internet connection: wired using ethernet cable (Figure 5.34).
5. Accept the default WAN configuration or specify settings (Figure 5.35). Settings may be altered after the device is registered.
6. Specify the router address to be used on the router LAN.
    a. Example: the SIGMATEK control will have an IP address of 192.168.111.20 and subnet mask of 255.255.255.0; the router address should be specified in the range 192.168.111.x
    b. Additional LAN networks may be added later.
7. Download the RAR configuration file (Figure 5.37); on most Windows-based browsers the file (ixrouter.conf) will be stored in the users Download directory.
8. Copy the configuration file to the root of a USB drive.
9. Power on the RAR; ensure the WAN interface is connected. Insert the USB drive into the RAR USB port.
10. The ACT LED will blink blue; once it has stopped blinking the configuration is complete and the drive may be removed.
11. The new device will be displayed in the RAP main interface with a highlighted background. Click on the “…” symbol and select “Activate” to finalise registration of the device (Figure 5.38).
12. Enter a name for the device.
13. The device will now automatically appear in the RAP until it is de-registered (Figure 5.39).

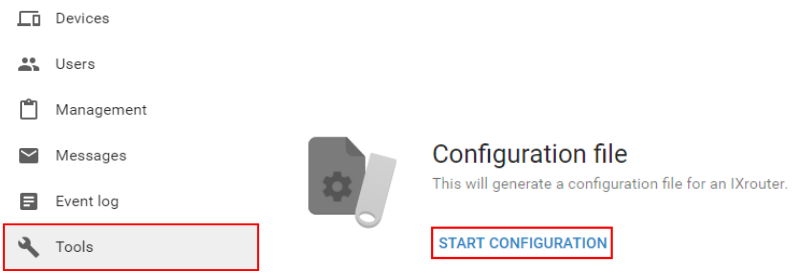


Figure 5.32

Left: select Tools from the RAP main menu.

Right: choose the option to start configuration.

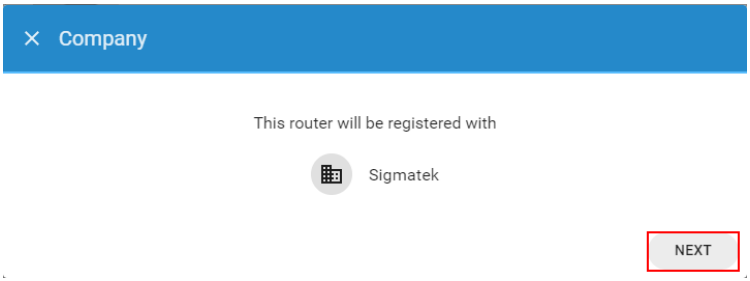


Figure 5.33 Select the company the device should be registered to.

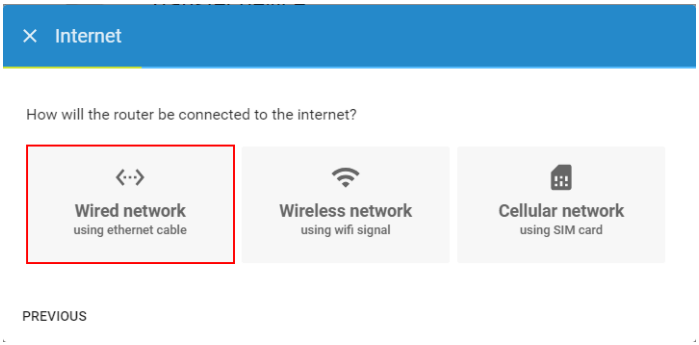


Figure 5.34 Select the WAN interface.

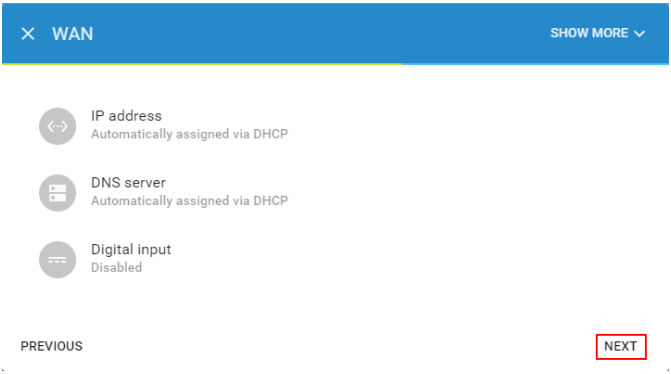


Figure 5.35 Accept/edit the WAN interface settings.

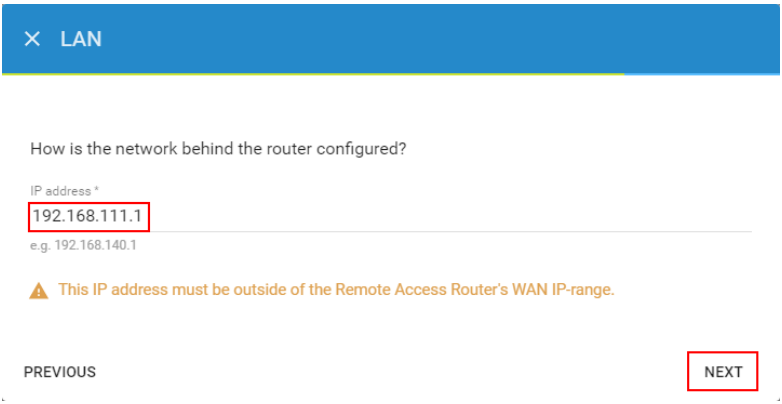


Figure 5.36 LAN interface configuration.

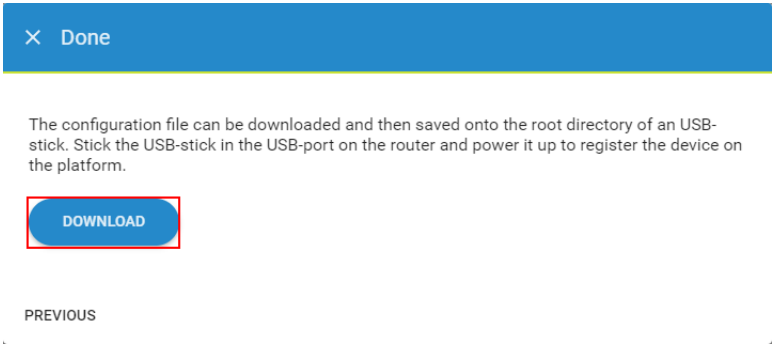


Figure 5.37 Download the RAR configuration file.

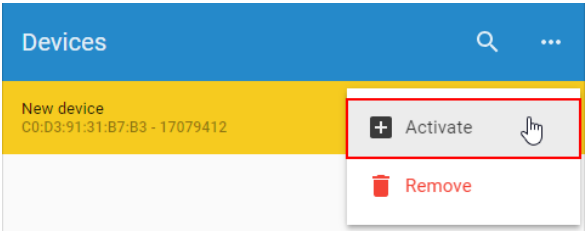


Figure 5.38 Activate the new device from the RAP.

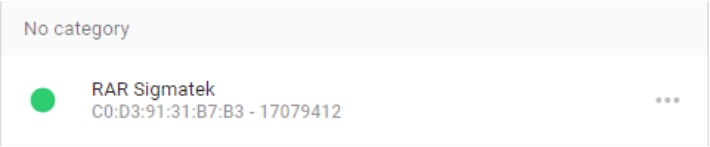


Figure 5.39 After device registration the actual VPN status of the device is displayed in the RAP main interface.

5.4.3 Remote Access Router using WIFI WAN

Refer to the procedure in section 0, p26.

- At step 4 (select the type of internet connection), select “wireless network” as the method of accessing the internet (Figure 5.40).
- Enter the SSID and password of the WIFI that will provide internet access (Figure 5.41).
- Complete the setup procedure as per section 0.

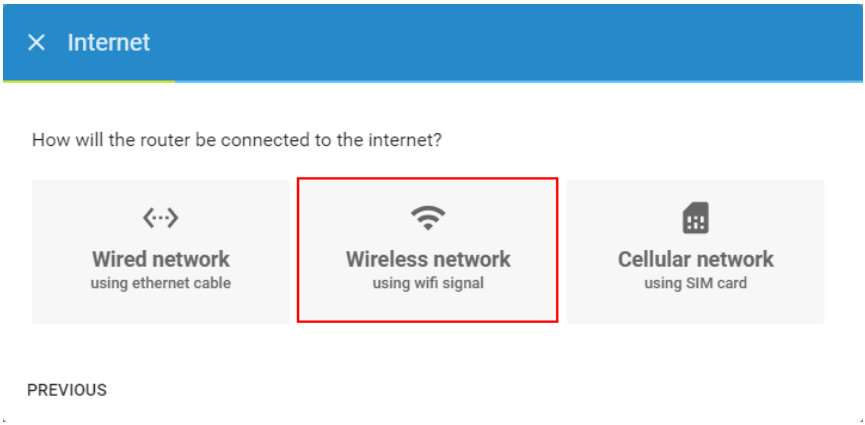


Figure 5.40 Select the internet connection method: “wireless”.

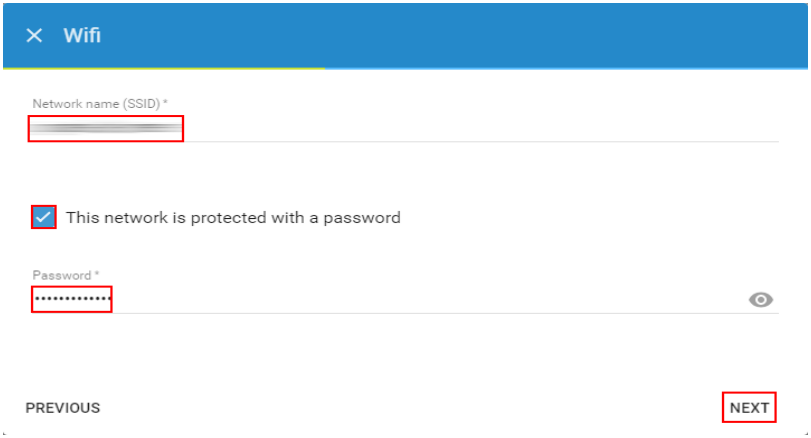


Figure 5.41 Provide the host network WIFI credentials.

5.4.4 Remote Access Router with 3G/4G WAN

Refer to the procedure in section 0, p26.

- At step 4 (select the type of internet connection), select “cellular network” as the method of accessing the internet (Figure 5.42).
- Enter the SIM card APN and SIM card PIN code. These details may be obtained from the network provider (Figure 5.43).
- Complete the setup procedure as per section 0.

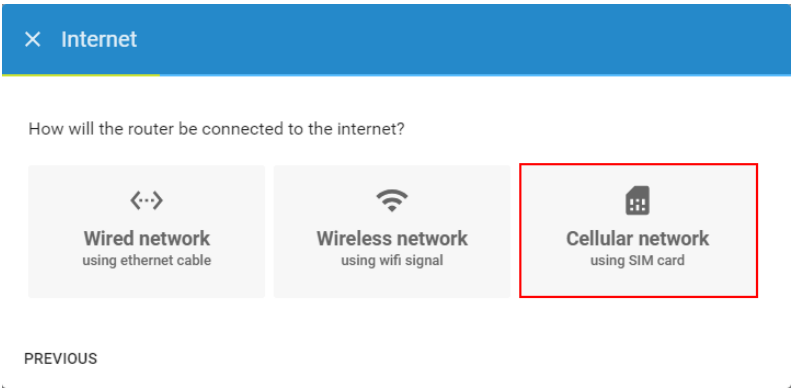


Figure 5.42 Select the internet connection method: “cellular network”.

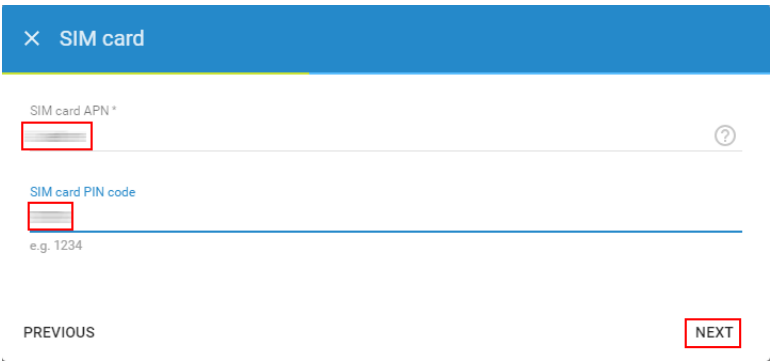


Figure 5.43 Enter the SIM card details.

5.4.5 Remote Access Embedded

This section applies only to the embedded software solution, RAE100. The RAE100 must have been previously installed; this procedure is defined in section 4.

On first use the RAE enabled control must be registered with RAP:

1. Using the Remote CLI, execute the command “ixagent register companyID” (Figure 5.44). The RAP company ID may be found from the RAP interface under “My Company” (Figure 5.45).
2. Successful registration will be confirmed in the command line feedback (Figure 5.46).
3. Complete the setup procedure as per section 0 (step 11, p26), activating the RAE device via the RAP interface.

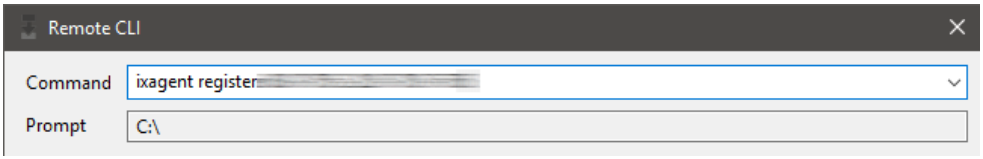


Figure 5.44 Executing the register command in the Remote CLI.

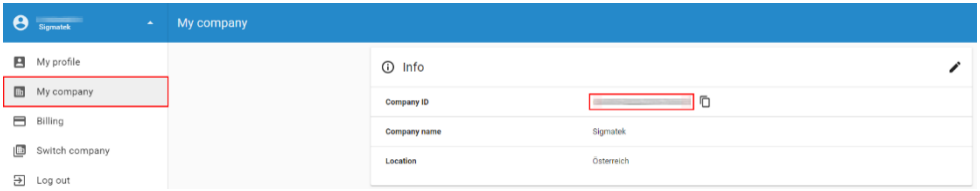


Figure 5.45 Company ID is displayed on RAP>User>My company.

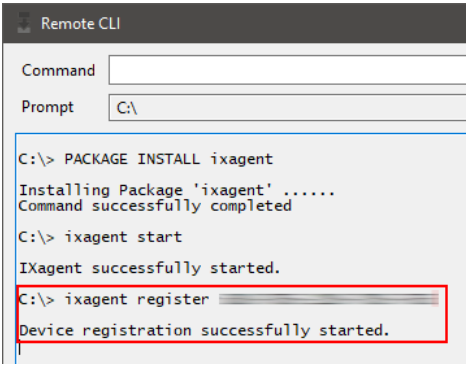


Figure 5.46 Confirmation of the successful registration.

5.5 Additional network settings (RAR only)

In the RAR LAN configuration it is possible to:

- Add an additional subnet
- Assign static IP leases
- Change the DHCP server IP address allocation pool
- Enable/disable source NAT

Example: to assign an additional subnet mask to the router:

1. On the RAP go to "CONFIG" (Figure 5.47).
2. On the LAN panel, click the pencil symbol to edit settings (Figure 5.48).
3. At the top right, click “show more” to reveal the option to add an additional subnet.
4. The new field is revealed in the panel (Figure 5.49). Typically, the gateway will be the LAN IP address of the RAR router. Enter the required subnet settings and click “ADD”.

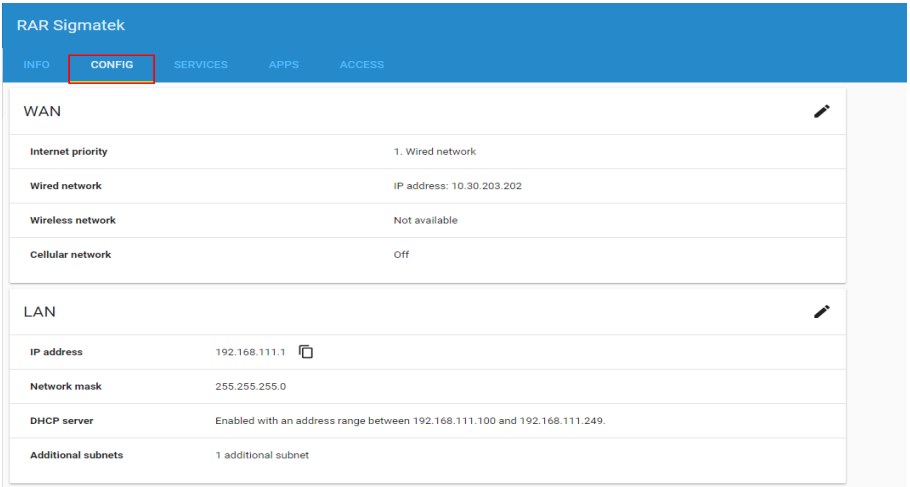


Figure 5.47 Open the Device config page.

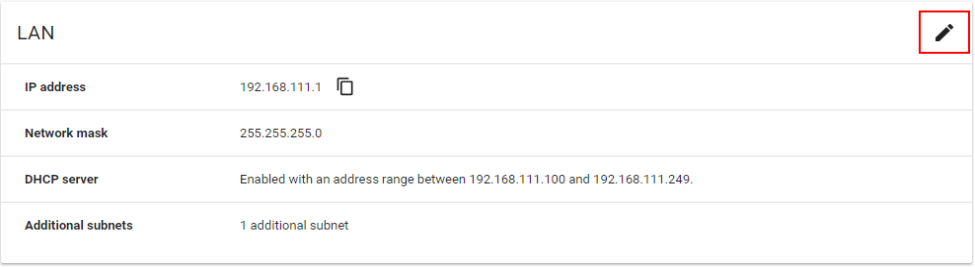


Figure 5.48 Edit the LAN configuration.

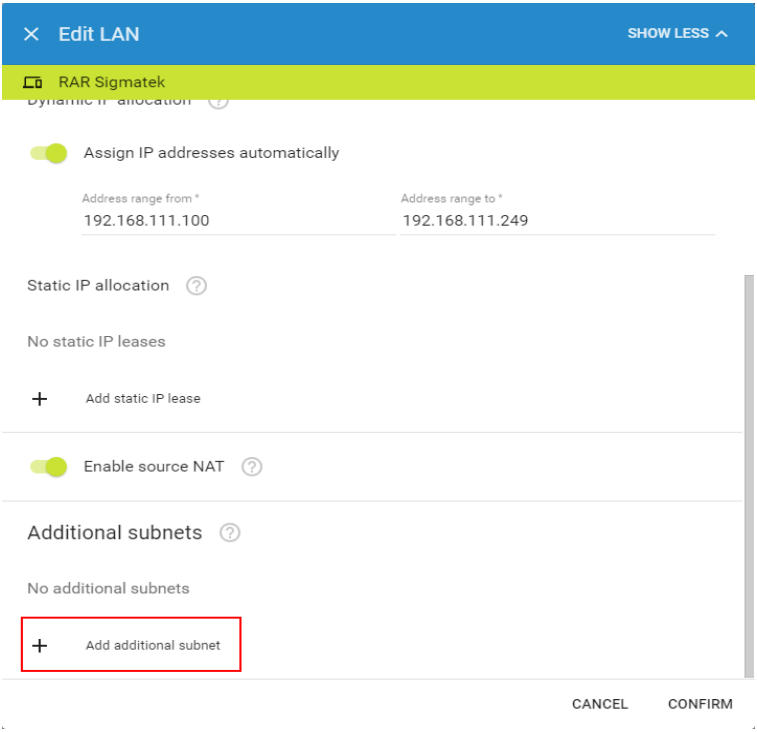


Figure 5.49 LAN configuration: after clicking “show more” the “add additional subnet” option is revealed.

5.6 Additional network settings (RAE only)

In some configurations it may be desired to provide remote access to controls connected to the control running RAE.

- To remotely access the other controls, it is required to setup port forwarding using the firewall.
- Firewall is supported on Salamander OS >= 09.03.141. Firewall commands are described in the Lasal OS documentation.

1. Connect to the control via LASAL CLASS 2.
2. Open the Autoexec.lsl using Class 2: Debug > File Transfer > Edit Autoexec.lsl. Add firewall commands to handle the forwarding and NAT to downstream devices.
    a. Example: control with IP address 10.100.3.3 is connected to the control running RAE with IP address of 192.168.111.20. The following lines must be added to forward a VNC connection:
        i. FIREWALL “-A FORWARD -j ACCEPT -p tcp --dport 5900 --sport 5901 -d 10.100.3.3 -m state --state”
        ii. FIREWALL “-t nat -A PREROUTING -p tcp --dport 5901 -j DNAT --to-destination 10.100.3.3:5900”
        iii. FIREWALL “-t nat -A POSTROUTING -j MASQUERADE”
3. Save the changes and reboot the control.

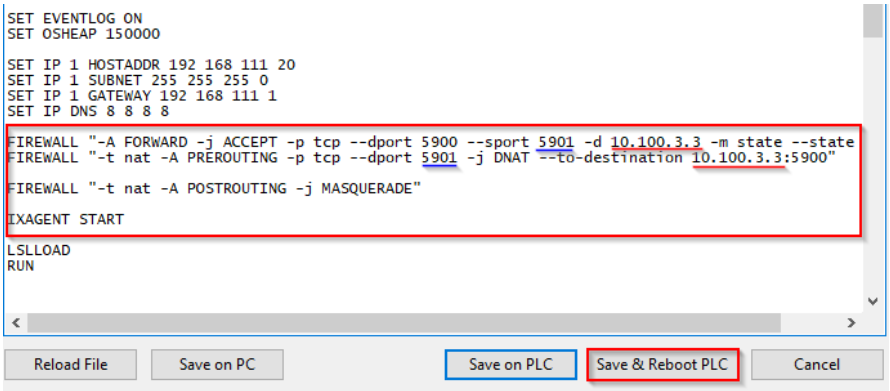


Figure 5.50 Autoexec with port forward commands.

5.7 Setup of remote services

Before configuring remote services, the device must have been registered with RAP.

5.7.1 Establishing a VPN Connection

A VPN connection requires that the RAR/RAE is powered and has an internet connection.
Available devices have a green dot against their label in the RAP interface.
To establish a VPN connection between the RAR/RAE and the current pc:

1. The VPN TUN adapter driver must be installed.
    a. This can be downloaded from RAP > Tools >" VPN Client" (Figure 5.51).
    b. There are optional settings available by clicking the gear icon from the Tools page:
        i. Client log mode
        ii. Stealth mode: support for restrictive networks. Data is obscured in addition to encryption. Most firewalls are then unable to identify the type of traffic.
        iii. Proxy server
2. Select the device from the RAP main interface.
3. From the "info" page, click "connect" under the VPN tab (Figure 5.52).
4. Once connected the device has a blue status indicator (Figure 5.53).
5. Windows and software can now communicate by TCP/IP to devices, such as SIGMATEK controls, connected to the RAR.

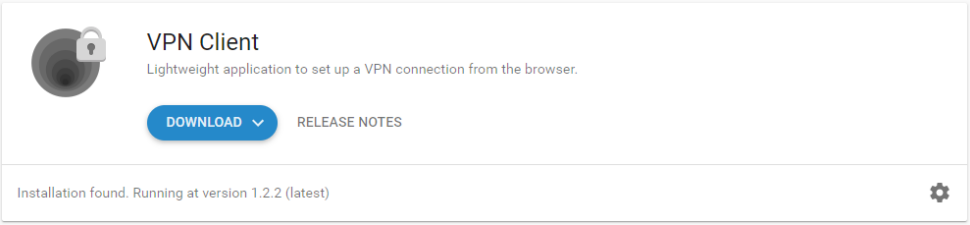


Figure 5.51 The cloud VPN client can be download from the RAP>Tools page.

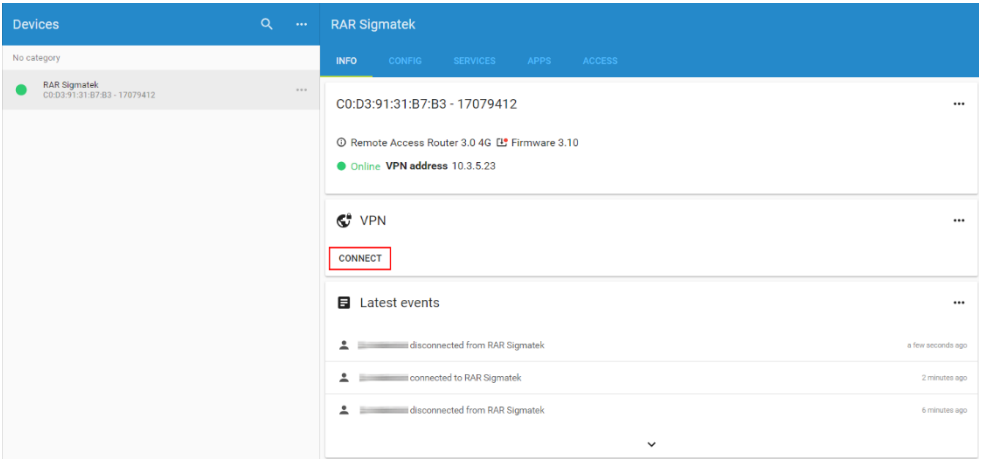


Figure 5.52 Each device has a VPN connect button to establish secure communications.

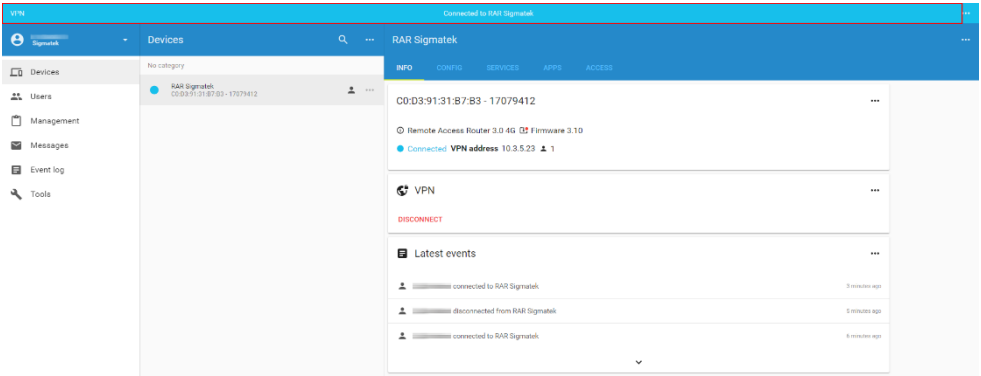


Figure 5.53 After establishing a VPN connection the device status indicator turns blue.

5.7.2 VNC over VPN

Using a VNC viewer, it is possible to directly access and interact with the HMI screen.

Activation of the VNC service on a SIGMATEK control is described in the training document, LASAL REMOTE SERVICES.

Once VNC is enabled on the control it should be tested via a local connection. When it is confirmed operational follow the guide for enabling the VNC Viewer service in the Remote Access Platform.

5.7.2.1 VNC Setup

1. From the RAP main menu, select Devices and click on the relevant remote device (Figure 5.54).
2. Click on the “Services” tab and click the “+” button (Figure 5.55).
3. Assign a name for the device service and specify the IP address of the target (Figure 5.57). For the RAE, the IP address is automatically specified as “localhost”.
4. Select VNC as the service (Figure 5.56).
5. Activate the checkbox labelled “This device is protected with a password” and enter the password (Figure 5.57). If required, change the port to match the actual setup.
6. Complete the process:
    a. RAR:
        i. Click ADD.
        ii. From the “Config” tab, *push* the configuration changes.
    b. RAE: click ADD; the change is effective immediately.

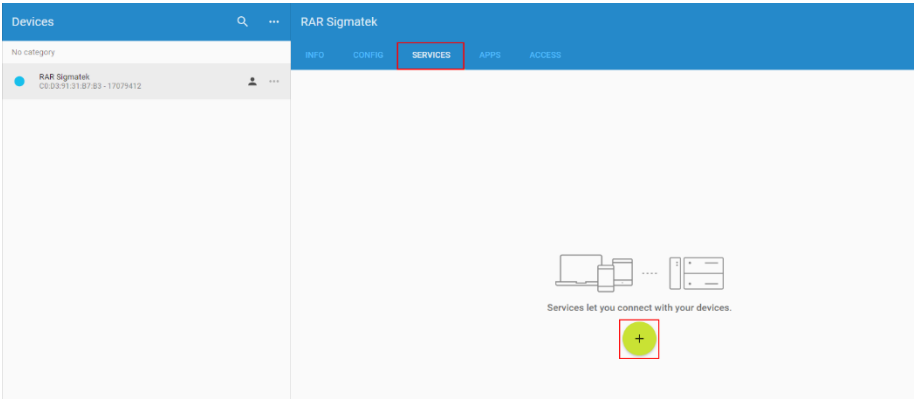


Figure 5.54 Adding a new service to the device.

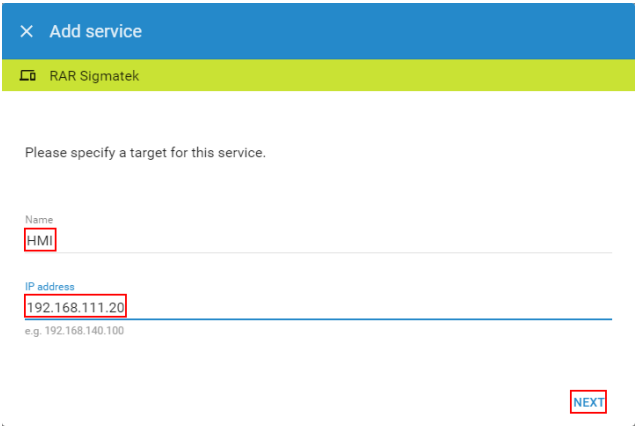


Figure 5.55 Setting the service target by IP address.

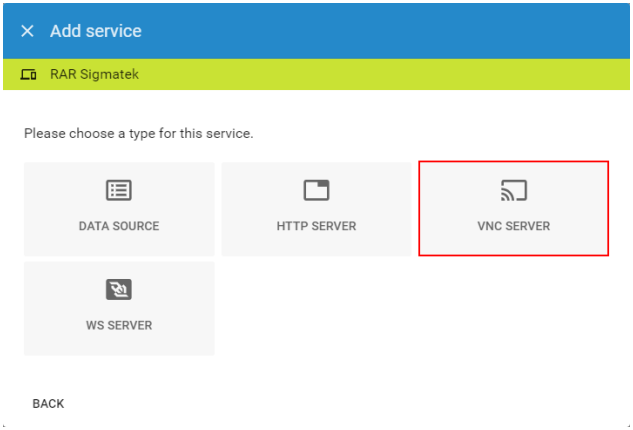


Figure 5.56 Select “VNC Server” as the service.

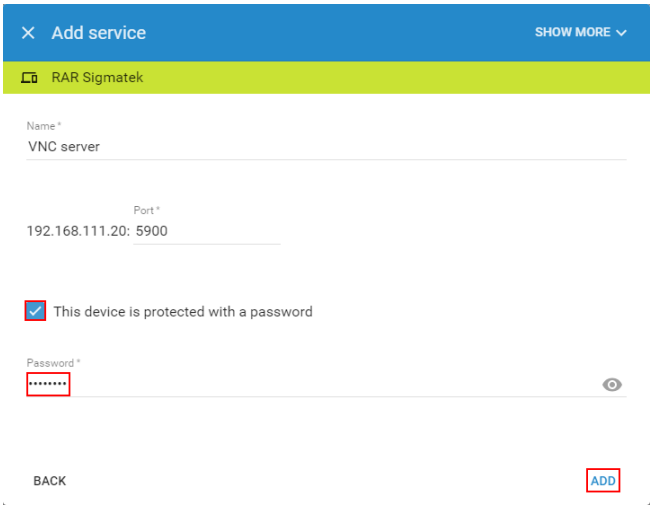


Figure 5.57 Set the VNC server port and password.

5.7.2.2 Connect to VNC

1. From the Device page, select the “Info” tab.
2. Under services, select the required VNC. Click on “VNC Server” (Figure 5.58).
3. The viewer will be opened in the same window; to return to the “info” tab click on the “x” in the left corner (Figure 5.59).

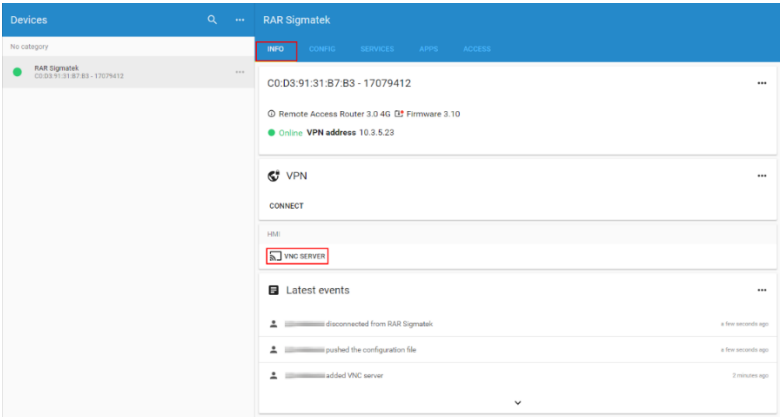


Figure 5.58 Select “VNC server” from the “Info” tab on the relevant device.

Figure 5.59 To exit the VNC viewer, click on the “x”.

5.8 Data Acquisition and Retention

5.8.1 Setting up Data Sources

Each control configured on a remote device may have one data source; the supported protocols for SIGMATEK controls are OPC UA and Modbus TCP.

1. From the RAP main menu, select the Device and open the “Services” tab. Click on the “+” button to add a new service (Figure 5.60).
2. Specify the control target that will provide the data source (Figure 5.61).
3. Click “Next” and in the following dialogue click “Data source” (Figure 5.62).
4. Enter the details for the data source:
    a. From the presented list select the relevant data source type, e.g. OPC UA or Modbus TCP.
    b. Set the server port.
    c. Set the authentication credentials if supported/required.
    d. Click “Add”.
5. The data source configurator will automatically open. Click on the “+” button to add a variable.
6. Refer to the following sections for adding variables using the respective source type.

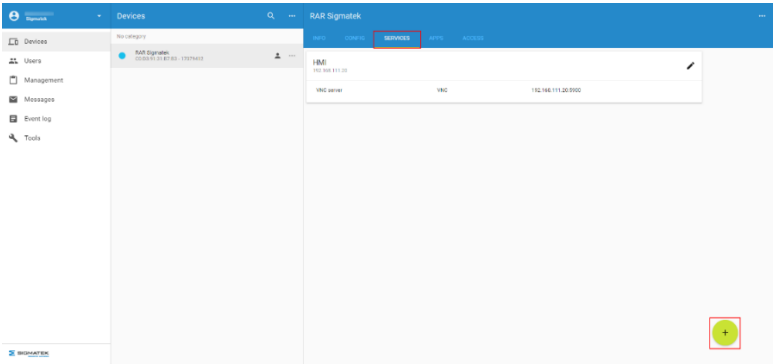


Figure 5.60 Add a new service to the remote device via the RAP > Device > Services tab.

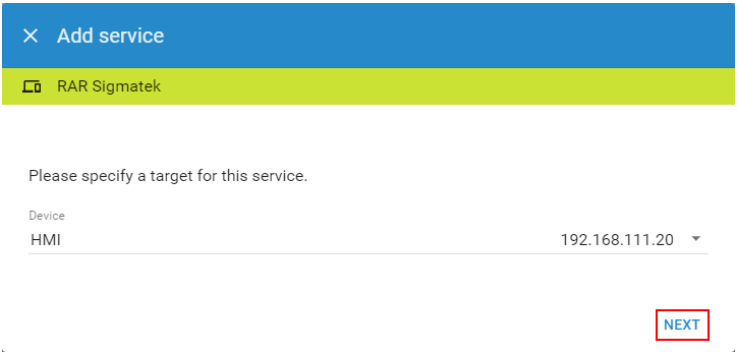


Figure 5.61 For the service specify the target.

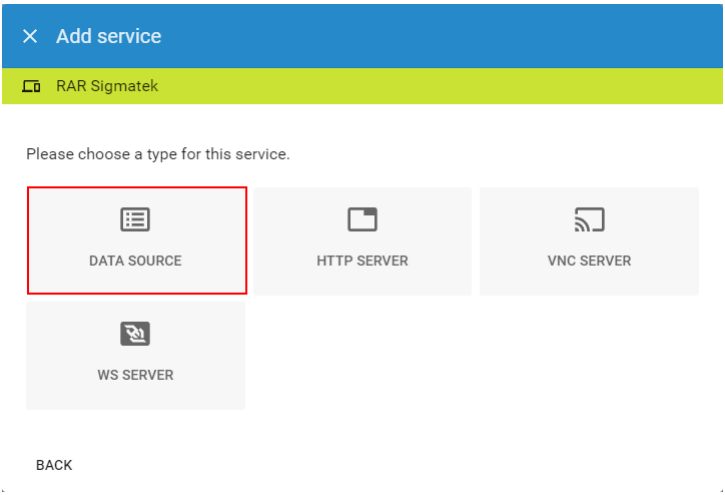


Figure 5.62 Select “Data Source” as the type of service.

5.8.1.1 OPC UA

To be able to record or utilize control data, the control must make data available to the RAP.

- Contact your SIGMATEK representative to obtain the OPC UA server and licence.
- Setup of OPC UA is described in the respective documentation.

To make an OPC UA data source available to the RAP:

1. Consider using a utility, such as UaExpert, to create the data map.
    a. Add the servers to be used in Cloud Logging or Cloud Notify; the “Node Id” and datatype are required.
2. See section 5.8.1 for adding an OPC UA data source.
3. To enable this data source service, go to RAP > Device > CONFIG and click on "PUSH CHANGES".
4. To add variables:
    a. From RAP > Device > Services click on the pencil icon of the relevant control (Figure 5.63).
    b. Select the "Data Source" service (Figure 5.64).
    c. Click on "OPEN CONFIGURATOR" (Figure 5.65).
    d. Click on the “+” symbol in the Data Configurator to provide data for recording (Figure 5.66).
    e. Go to "Add new variable".
    f. Assign the name of the variable. Specify the data type and address of the variable. These values may be obtained from the OPC UA map or using software such as UA Expert (Figure 5.67). An example of the address is shown in Figure 5.68. A factor and unit may also be applied. Click on “ADD”.
    g. Click on "SYNC" in the configurator header line.
    h. After sync is complete begin a test of the data server connection and variable acquisition by clicking on "RUN TEST".

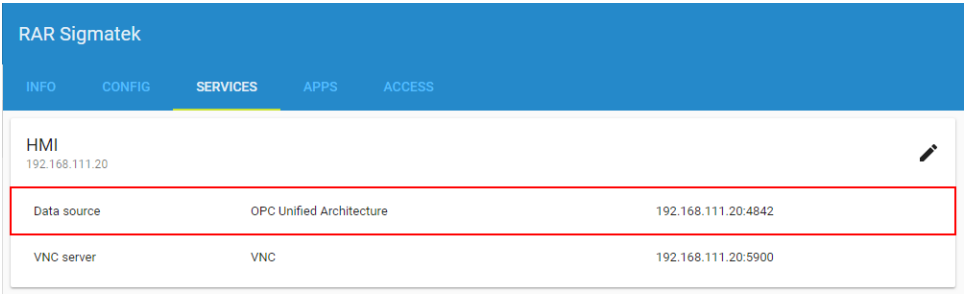


Figure 5.63 From the RAP > Devices > Services tab, click on the edit button of the station with the data source to add variables.

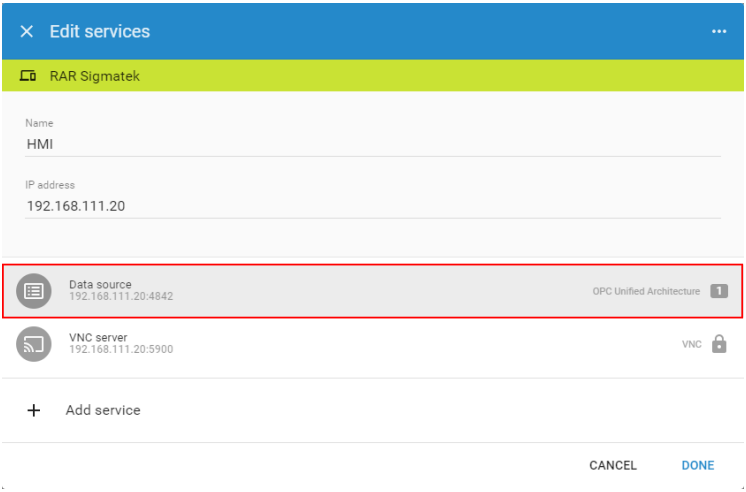


Figure 5.64 Click on the data source to edit the data source configuration.

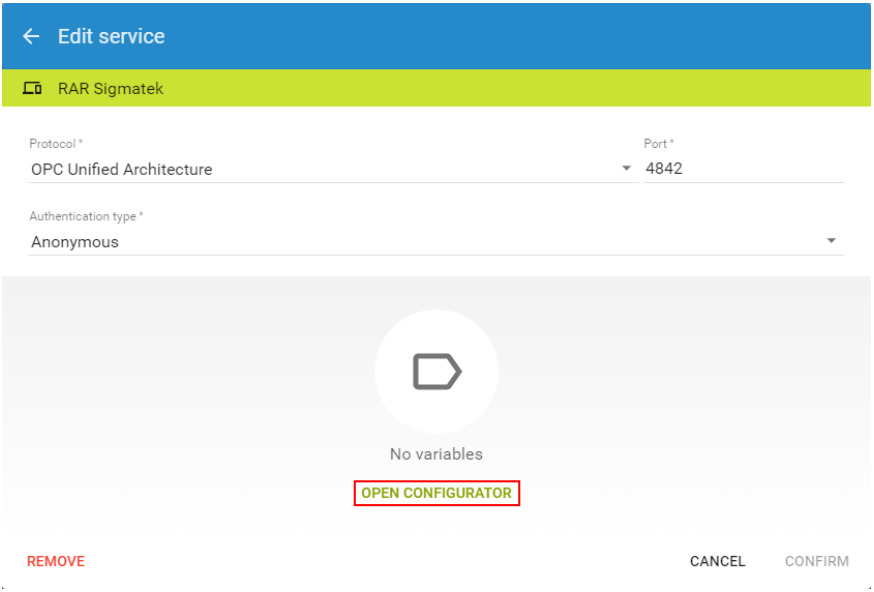


Figure 5.65 The “Open Configurator” button provides access to edit the variables.

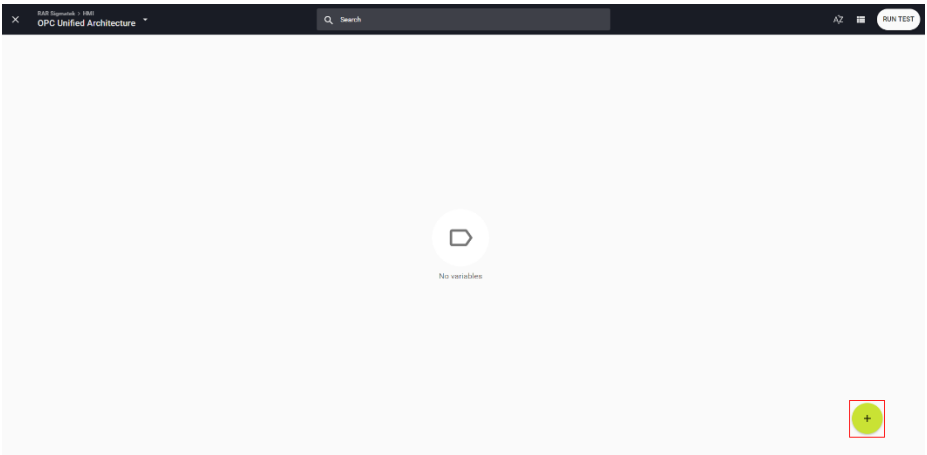


Figure 5.66 Data Configuration interface.

#	Server	Node Id	Display Name	Value	Datatype	Source Timestamp	Server Timestamp	Statuscode
1	OPC-UA Embedded Server	NS2|Numeric|20001	OPC_ST1V.V1_DINT	0	Int32	13:38:30.684	13:38:30.684	Good
2	OPC-UA Embedded Server	NS2|Numeric|20004	OPC_ST1V.V2_DINT	0	Int32	13:38:30.685	13:38:30.685	Good

Figure 5.67 Locating the node id and data type from the UaExpert data access view.

Namespace index	Identifier type	Identifier	Address for RAP variable
2	String	Vartemp	ns=2;s=vartemp
2	Numeric	20001	ns=2;i=20001

Figure 5.68 Example of creating the RAP variable identifier.

5.8.1.2 Modbus TCP

To be able to record or utilize control data, the control must make data available to the RAP.

- Further information on the Modbus slave is available in the class documentation.

The Modbus slave must be added to the control that is the data source:

1. Add the ModbusTCPSlave class. Note the port number for the RAP configuration ().
2. Setup the data sources in the ModbusTableBase class. This class assigns a server to a Modbus register (Figure 5.70).
3. See section 5.8.1 for adding a Modbus data source. When applying Modbus settings (Figure 5.71), note the following:
    a. Slave number = 1
    b. Byte order = ABCD
4. To enable this data source service, go to RAP > Device > CONFIG and click on "PUSH CHANGES".
5. To add variables:
    a. From RAP > Device > Services click on the pencil icon of the relevant control.
    b. Select the "Data Source" service.
    c. Click on "OPEN CONFIGURATOR".
    d. Click on the “+” symbol in the Data Configurator to provide data for recording (Figure 5.72).

e. Go to "Add new variable".

f. Assign the name of the variable. Specify the data type and address of the variable (Figure 5.73). A factor and unit may also be applied. Click on “ADD”.

g. Click on "SYNC" in the configurator header line.

6. After sync is complete begin a test of the data server connection and variable acquisition by clicking on "RUN TEST".

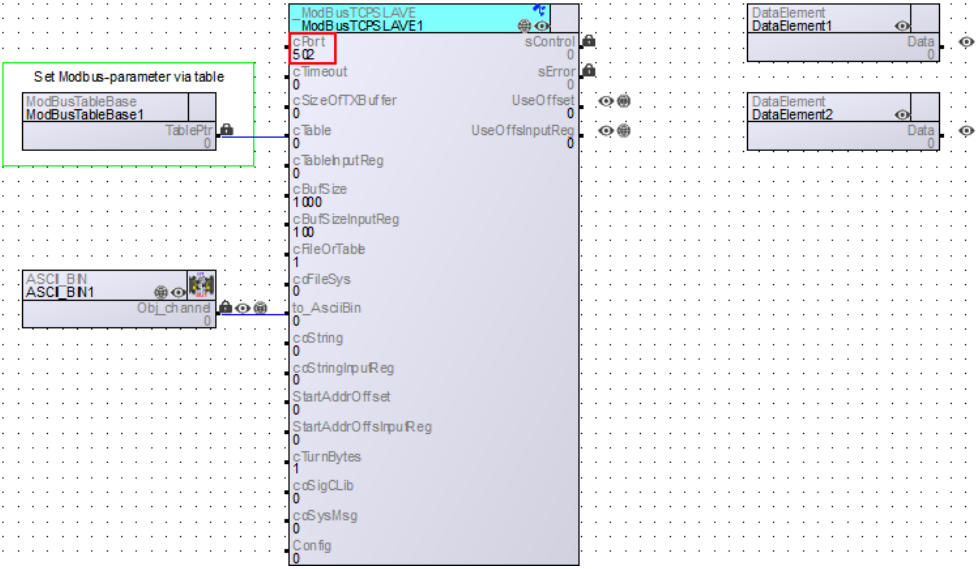


Figure 5.69 Overview of a ModbusTcpSlave network with example data sources, DataElement1.Data and DataElement2.Data.

```
FUNCTION TAB ModBusTableBase::Table

  // Modbus-Adress,  Register-Count,   Access Restriction,          "Objectname.Servername",
     100 $uint,        2 $usint,       MODBUSTABLE_ACCESS_RW $usint, "DataElement1.Data",
     200 $uint,        2 $usint,       MODBUSTABLE_ACCESS_RW $usint, "DataElement2.Data",

END_FUNCTION
```

Figure 5.70 In ModbusTableBase::Table the data sources from DataElement objects are assigned to Modbus registers.

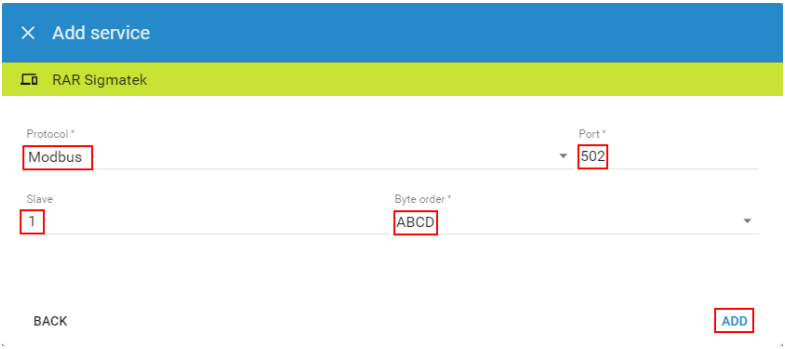


Figure 5.71 Configuring the data source settings for Modbus.

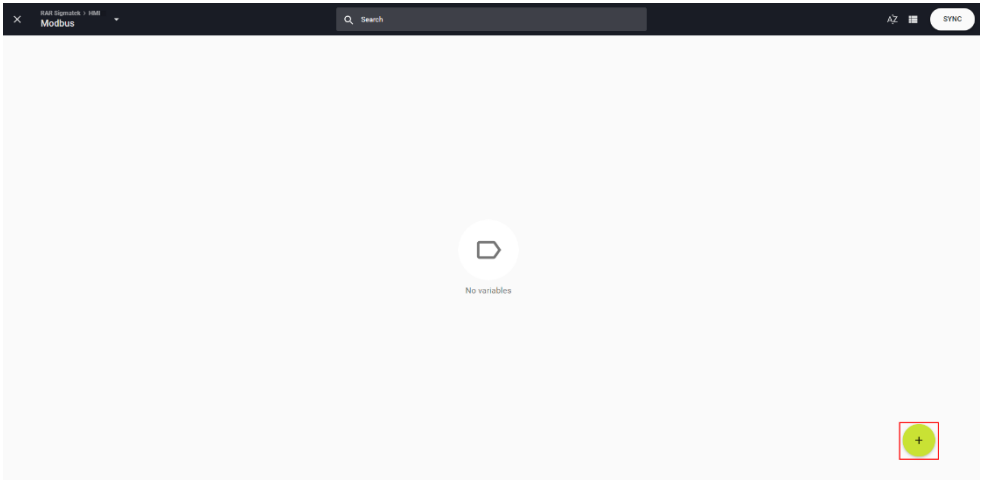


Figure 5.72 Data Configurator interface.

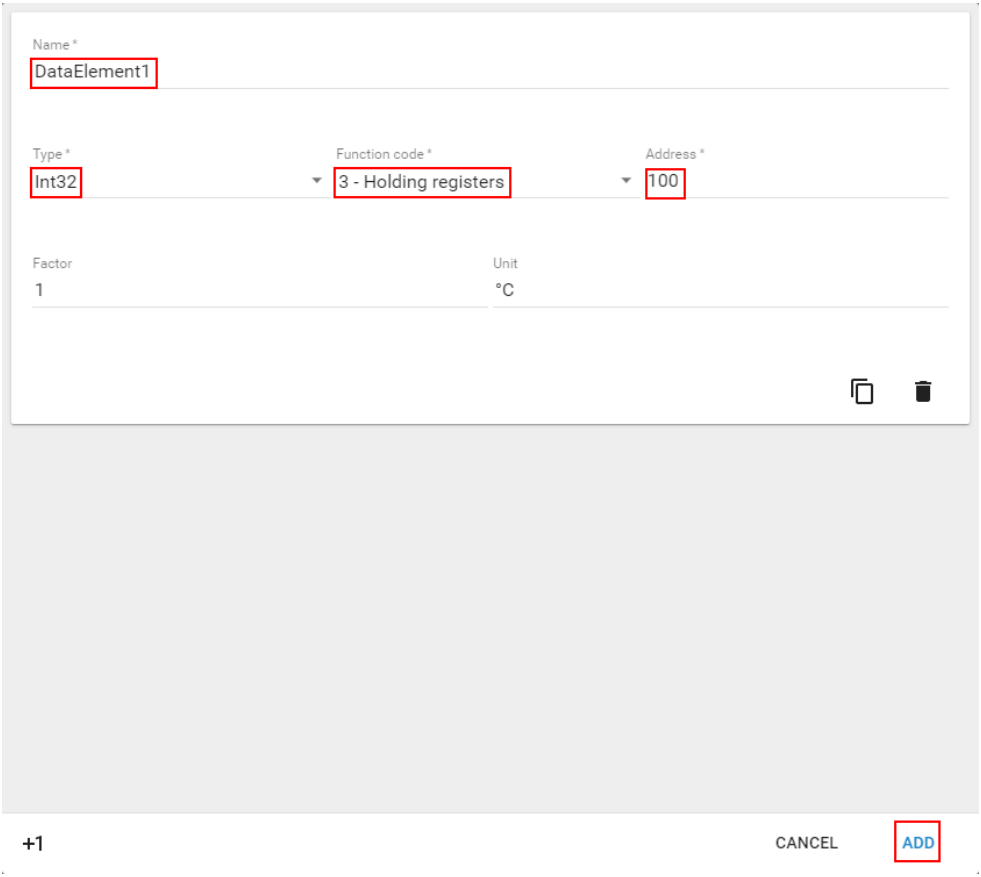


Figure 5.73 Adding a variable from a Modbus data source.

5.8.2 Cloud Logging

Cloud logging offers the possibility of recording data from the control. This data can be viewed as reports or as a live view. Cloud logging requires a licence; available licences are displayed under Billing (Figure 5.74).

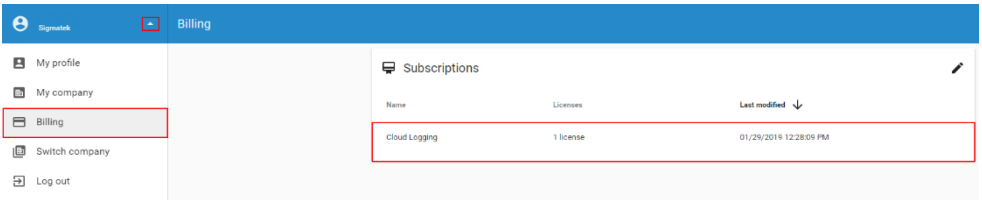


Figure 5.74 RAP billing page displaying the cloud logging licence.

5.8.2.1 Enable Cloud Logging

1. Obtain a licence from your SIGMATEK representative.
2. To record data to the cloud: on RAP go to the device. Click on the “APPS” tab (Figure 5.75).
3. Activate “cloud logging”.
4. Select the licence (Figure 5.76).

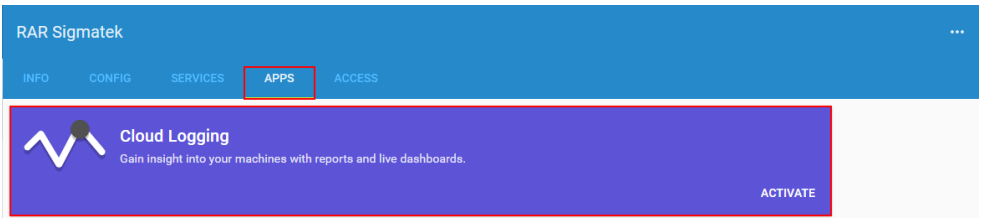


Figure 5.75 APPS tab with cloud logging activation.

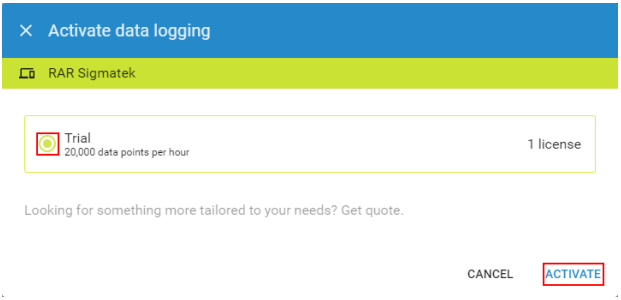


Figure 5.76 Select the type of data logging licence to activate.

5.8.2.2 Add data sources to Cloud Logging

1. After activation open the Cloud Logging (Figure 5.77).
2. From the Cloud Logging menu, click on “tags”.
3. Click on the “+” button to add a tag (Figure 5.78).
4. In the tag editor: enter a data source, select the logging interval and data retention policy (Figure 5.79).
5. Click “Add”; tags will be listed (Figure 5.80). Repeat process for all required data sources.

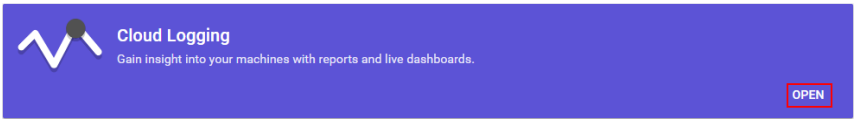


Figure 5.77 After activation the Cloud Logging interface is available.

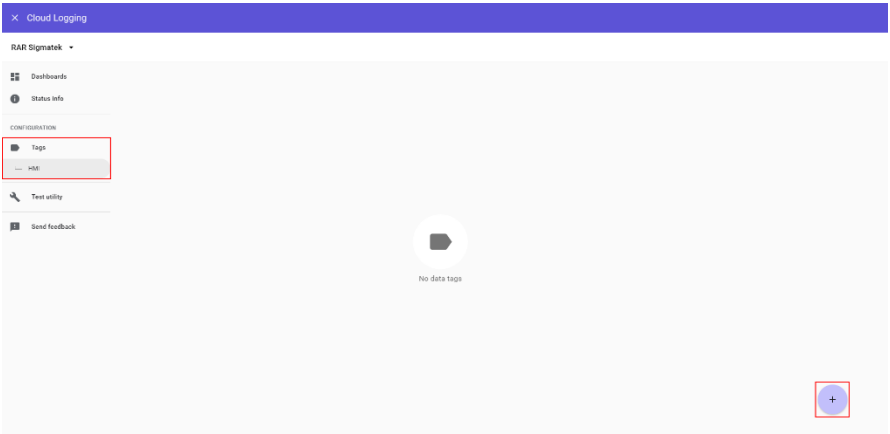


Figure 5.78 Cloud Logging interface; the “+” button is used to add new tags.

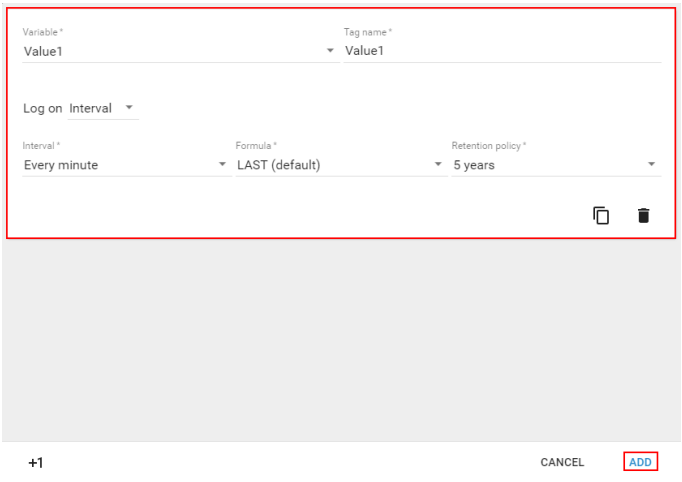


Figure 5.79 Tag editor interface.

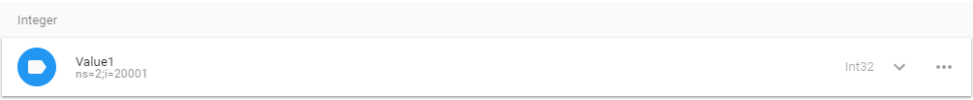


Figure 5.80 Available tags are listed.

5.8.2.3 Create a data display dashboard

1. From the Cloud Logging menu, click on “Dashboards”.
2. Click on the “+” button to create a new dashboard (Figure 5.81). Dashboards may be imported from file or created from scratch.
3. From the options, select data report (historical) or live monitor (Figure 5.82).
4. Assign a name to the dashboard and select the design theme (Figure 5.83). Click “Add” to move to the design step.
5. Dashboard widgets can be selected, and tags assigned to each widget in the Dashboard designer (Figure 5.84).
    a. Value widget: a data value display (Figure 5.86).
    b. Status widget: an indicator dependent upon one or more conditions (Figure 5.87).
    c. Gauge widget: an analogue style data value display (Figure 5.88).
    d. Graph widget: for trending a data source (Figure 5.89).
6. After configuration is complete, the changes must be pushed to the device from the device “Config” tab. The dashboard can be viewed from the “Info” tab (Figure 5.85).

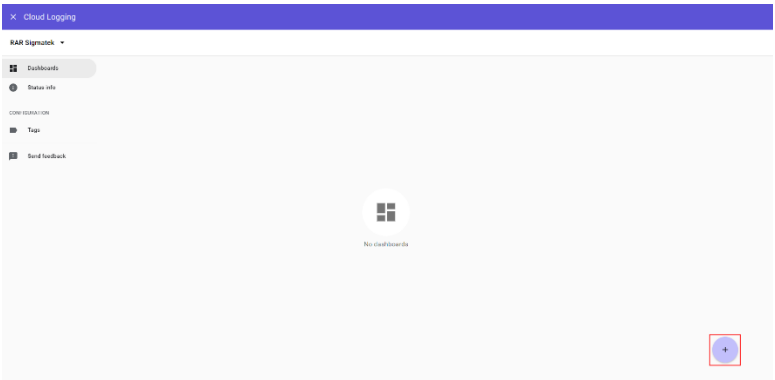


Figure 5.81 Create a new dashboard by clicking the “+” button.

Figure 5.82 Select a dashboard type: report or live.

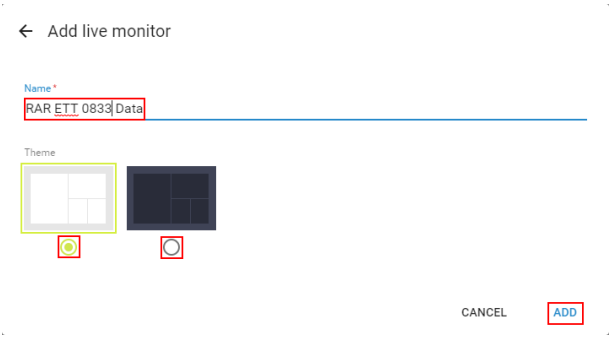


Figure 5.83 Assign a dashboard name and select theme.

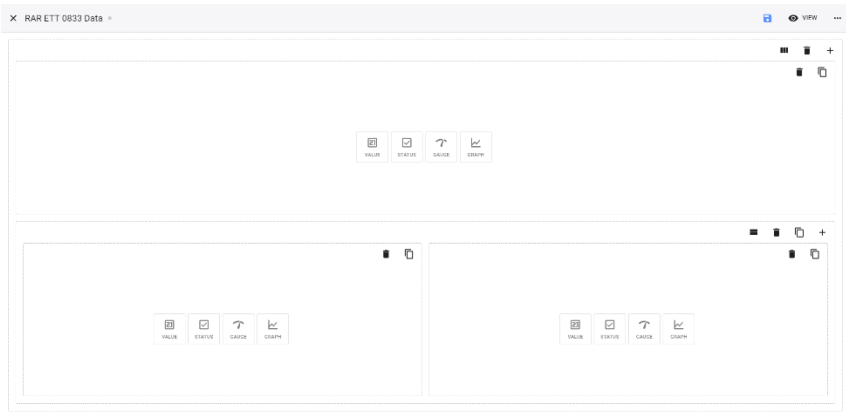


Figure 5.84 Example Dashboard layout.

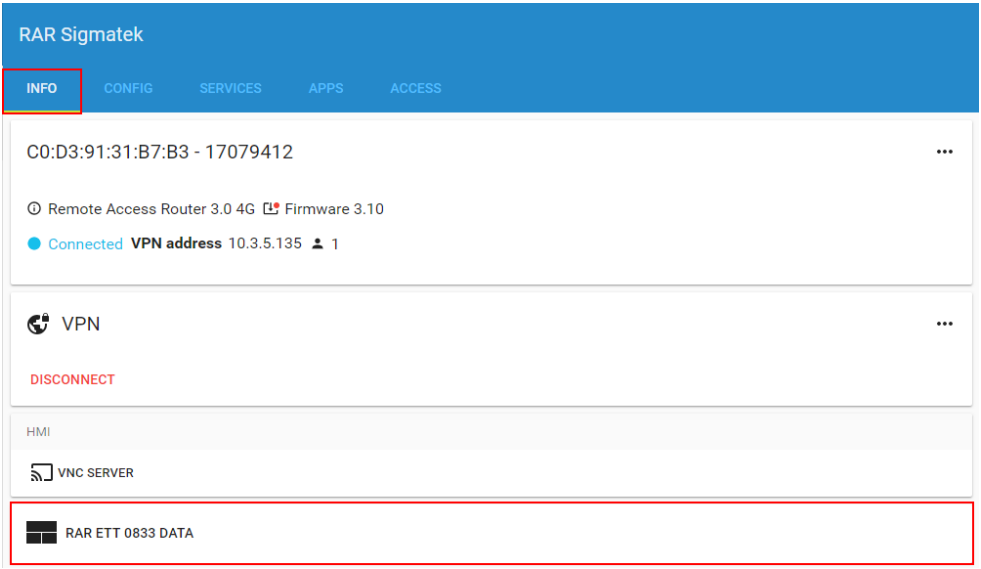


Figure 5.85 Dashboards are accessed from RAP > Device > Info.

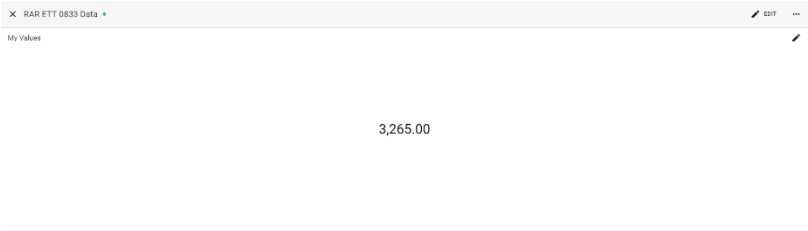


Figure 5.86 Value widget on a live dashboard.

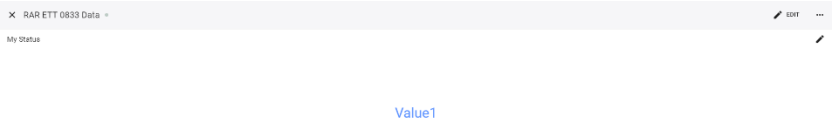


Figure 5.87 Status widget on a live dashboard.

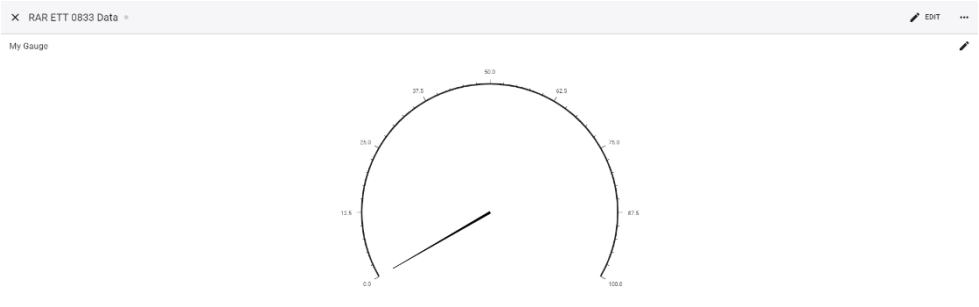


Figure 5.88 Gauge widget on a live dashboard.

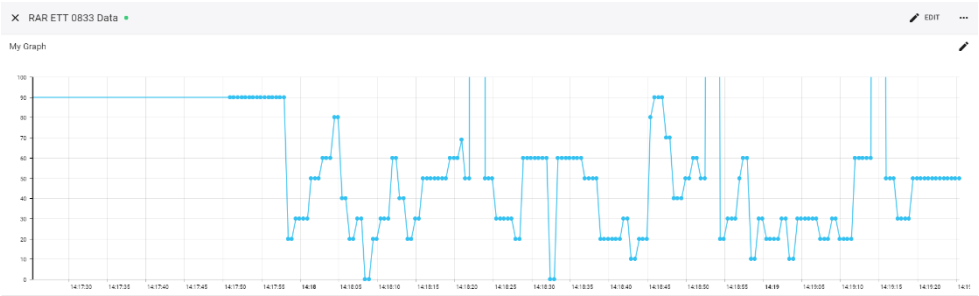


Figure 5.89 Graph widget on a live dashboard.

5.8.3 Cloud Notification

The Cloud Notification offers the possibility to record notifications about important machine events and to send them via e-mail.
A licence is required for Cloud Notification; available licences are displayed under Billing ().

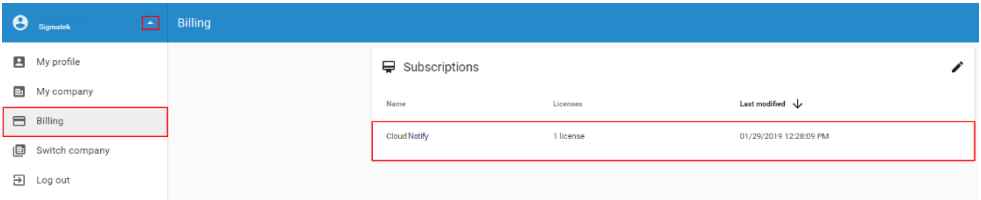


Figure 5.90 RAP billing page displaying the Cloud Notify licence.

5.8.3.1 Enable Cloud Notification

1. Obtain a licence from your SIGMATEK representative.
2. To record data to the cloud: on RAP go to the device. Click on the “APPS” tab (Figure 5.91).
3. Activate “cloud logging”.
4. Select the licence (Figure 5.92).

Figure 5.91 Activate Cloud Notify from the APPS.

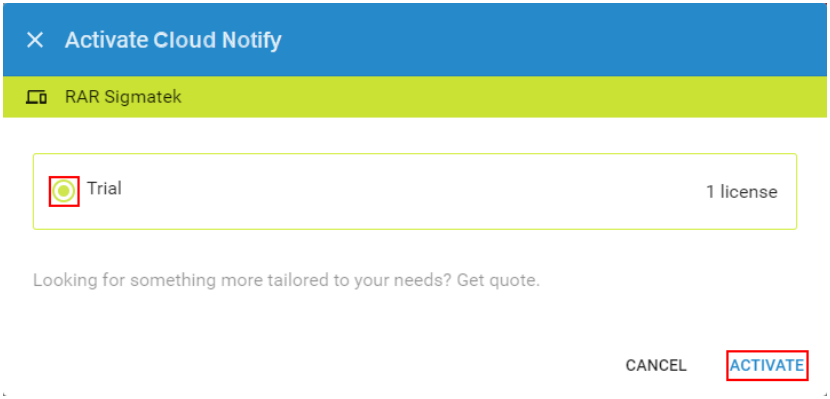


Figure 5.92 Select the licence to be used for the Cloud Notify App.

5.8.3.2 Setup Cloud Notification

1. Setup tags: refer to section 5.8.1 for setting up data sources.
2. Setup alarms:
    a. From the Cloud Notify interface, click the “+” button (Figure 5.93).
    b. Click on “add new alarm” (Figure 5.94).
    c. Select the variable that will be used as the basis of the notification.
    d. Set the alarm parameters (Figure 5.95):
        i. Name
        ii. Severity
        iii. Trigger conditions (value, operator)
        iv. Instructions for alarm resolution
    e. Click “Add” to store the new alarm.
    f. From the RAP main menu, select the device and from the “Info” page click on “push” to send the new configuration to the remote device.
3. Setup recipients from the alarms (Figure 5.96):
    a. Recipients must be registered as device users.
    b. From the Cloud Notify interface, click on “Alarm receivers”.
    c. Choose the users that receive alarms by severity level: click on the relevant severity level to apply the setting.

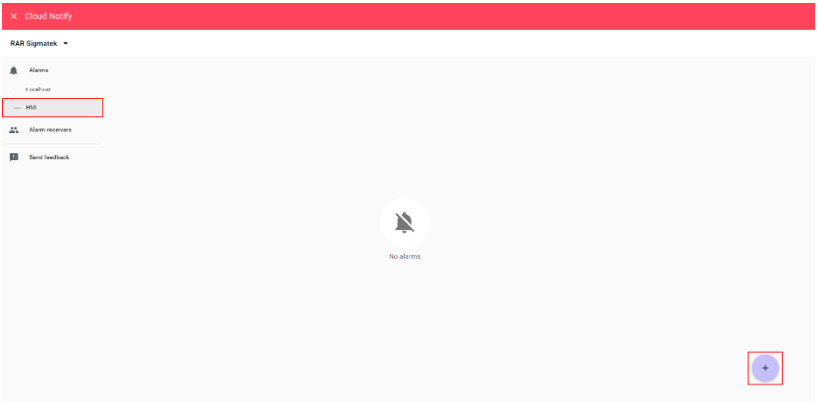


Figure 5.93 Add tags using the Cloud Notify interface.

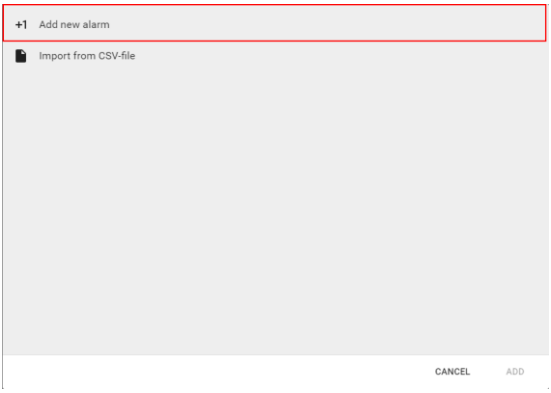


Figure 5.94 Create alarms as the basis of notifications.

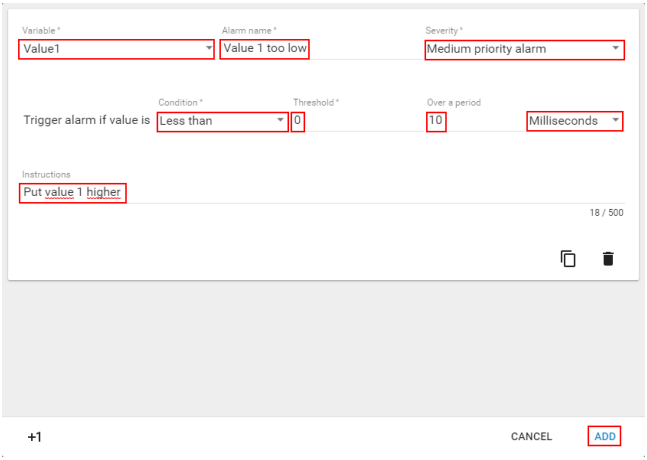


Figure 5.95 Setting the source and parameters for the cloud alarm.

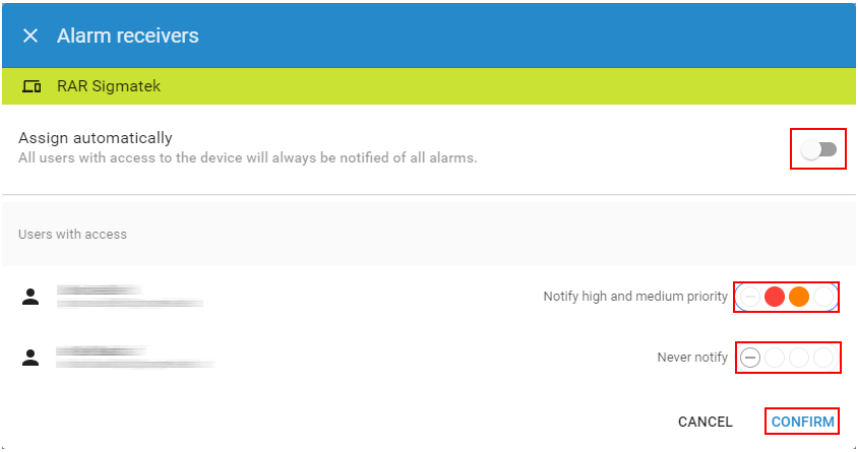


Figure 5.96 Specifying the alarm severity levels sent to the users.

5.9 User Management

5.9.1 New Users

Users may be assigned different rights within RAP: from the main menu select “Users” (Figure 5.30).

- New user:
  - Click the “+” icon to invite a new user with specific permissions.
  - Invited users are displayed under “pending invites”.
  - The invited user receives an email with a login link.

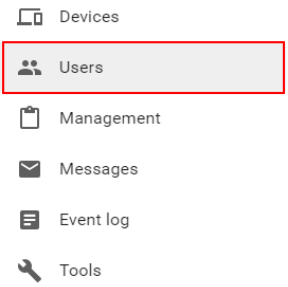


Figure 5.97 Main menu: Users

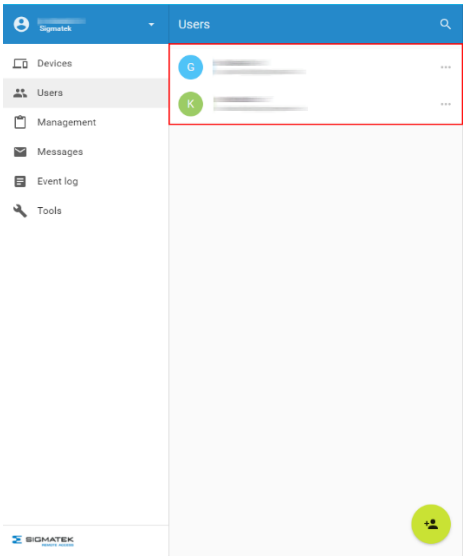


Figure 5.98 Users page displaying all registered users within the currently selected company.

5.9.2 Assigning user access to a device

Assuming both device and user have completed registration:

1. From the RAP main interface, click on the device to be assigned access.
2. Click on the “access” tab (Figure 5.99).
3. Click on the edit icon to add/remove access to this device by user (Figure 5.100).
4. From the same interface, access to all devices in the company may be granted to a specific user.

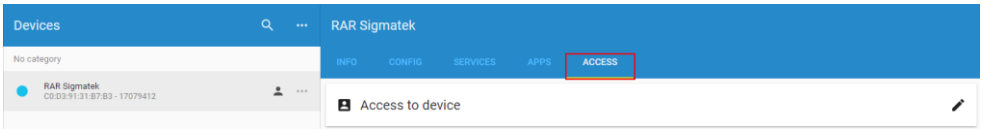


Figure 5.99 The Access tab is available for each device.

Figure 5.100 The edit icon for configuring device access

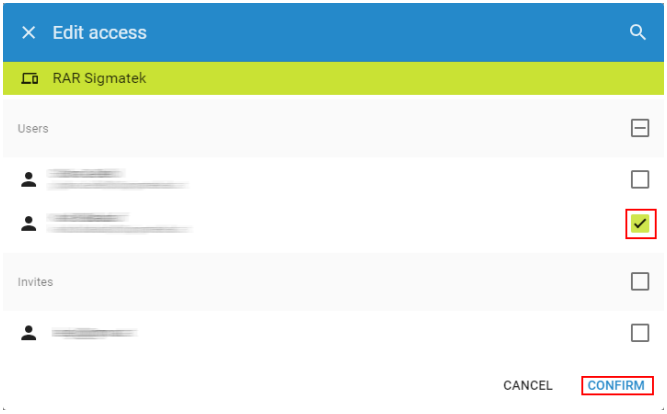


Figure 5.101 Assigning device access to a specific user.

6 Example Solutions

This section presents several universal remote access configurations.

- An exemplary step-by-step guide is presented for the first solution.
- For all solutions a set of suggested configurations are provided in the format of a diagram that illustrates the necessary connections and interface setup.

6.1 Remote Access Router (RAR) Based Solutions

Exemplary setup procedure based on Example 1:

1. Open LASAL CLASS 2 and establish an online connection to the HMI.
2. To access the HMI via the RAR, the default gateway must be changed to the IP address of the RAR (Figure 6.102).
    a. Open the Autoexec.lsl editor from Debug > File Transfer > Edit Autoexec.lsl
    b. Set the gateway to the router IP address (Figure 6.103). This can be found via the RAP main interface > Device > Info > LAN.
    c. Reboot the control to apply the new IP configuration.
3. Connect the HMI to the RAR using an Ethernet cable (Figure 6.104).

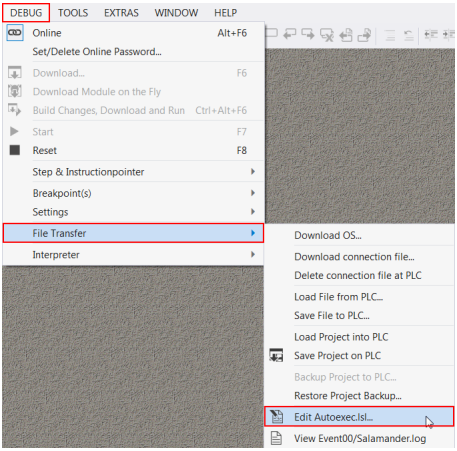


Figure 6.102 Opening the Autoexec.lsl editor from within LASAL CLASS 2.

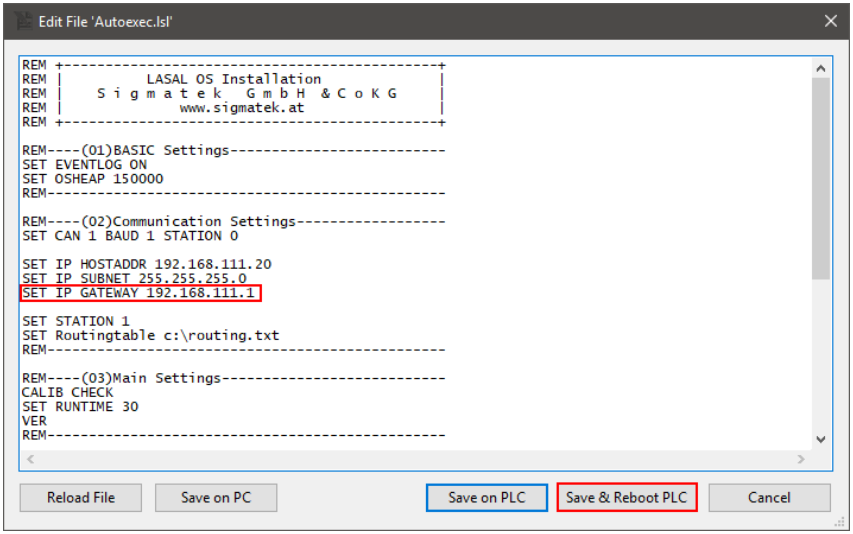


Figure 6.103 Entering the IP gateway into the Autoexec.lsl.

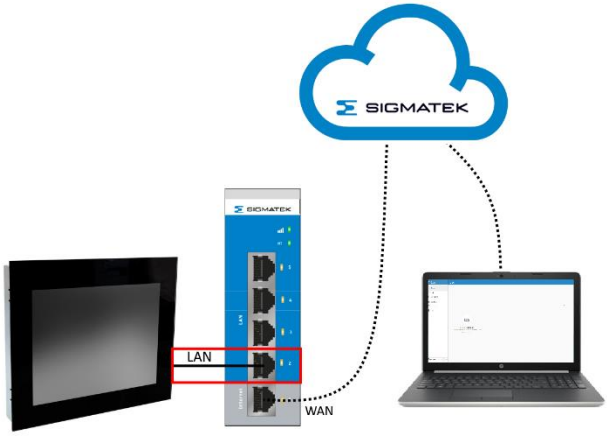
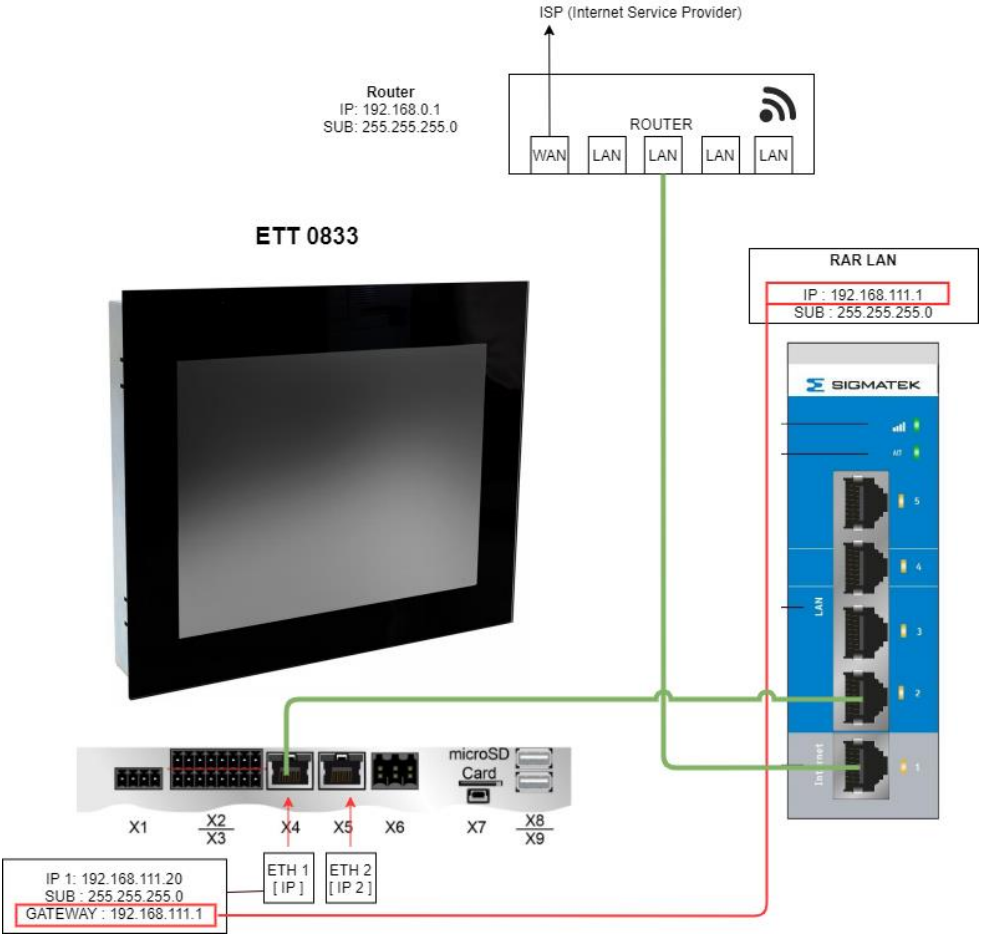
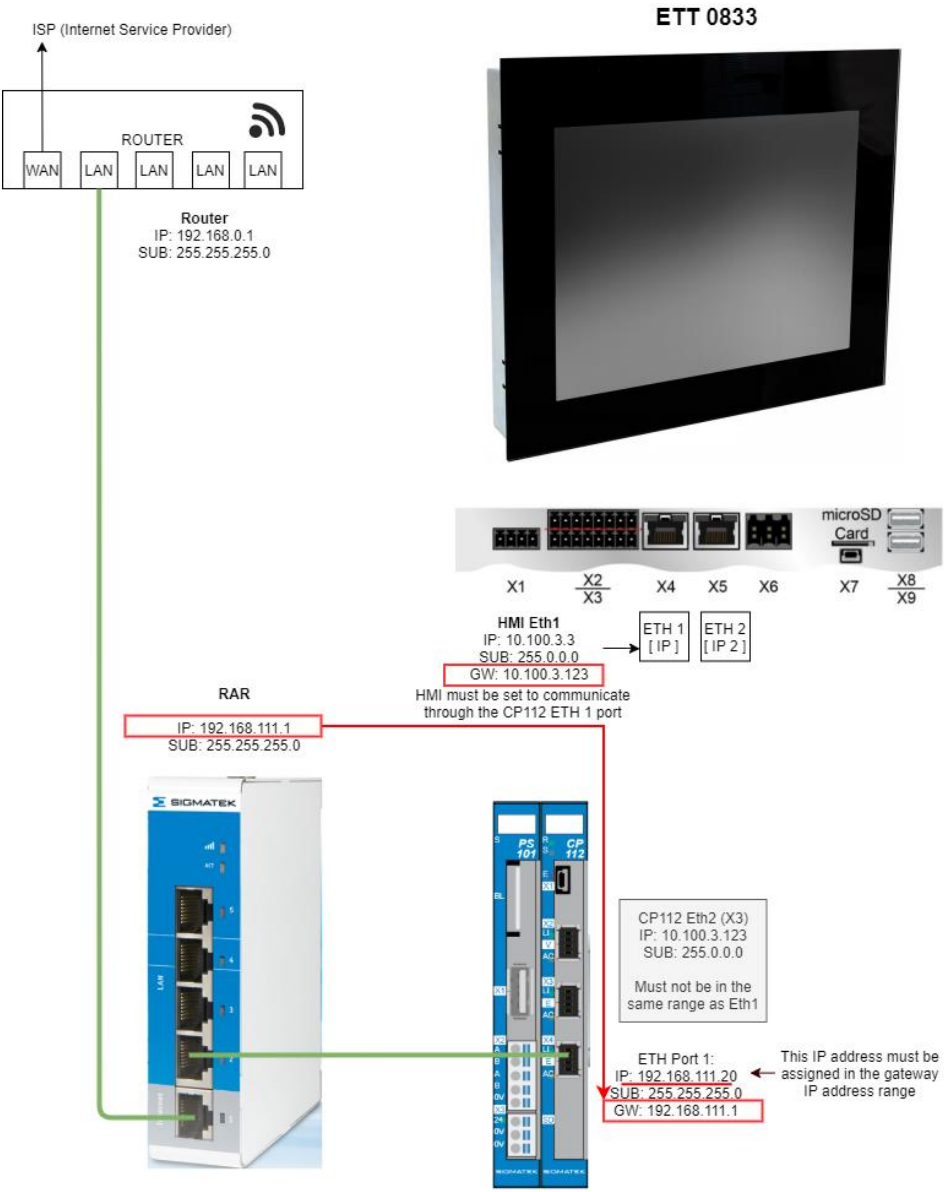


Figure 6.104 HMI connected to the RAR may be accessed securely via the RAP.

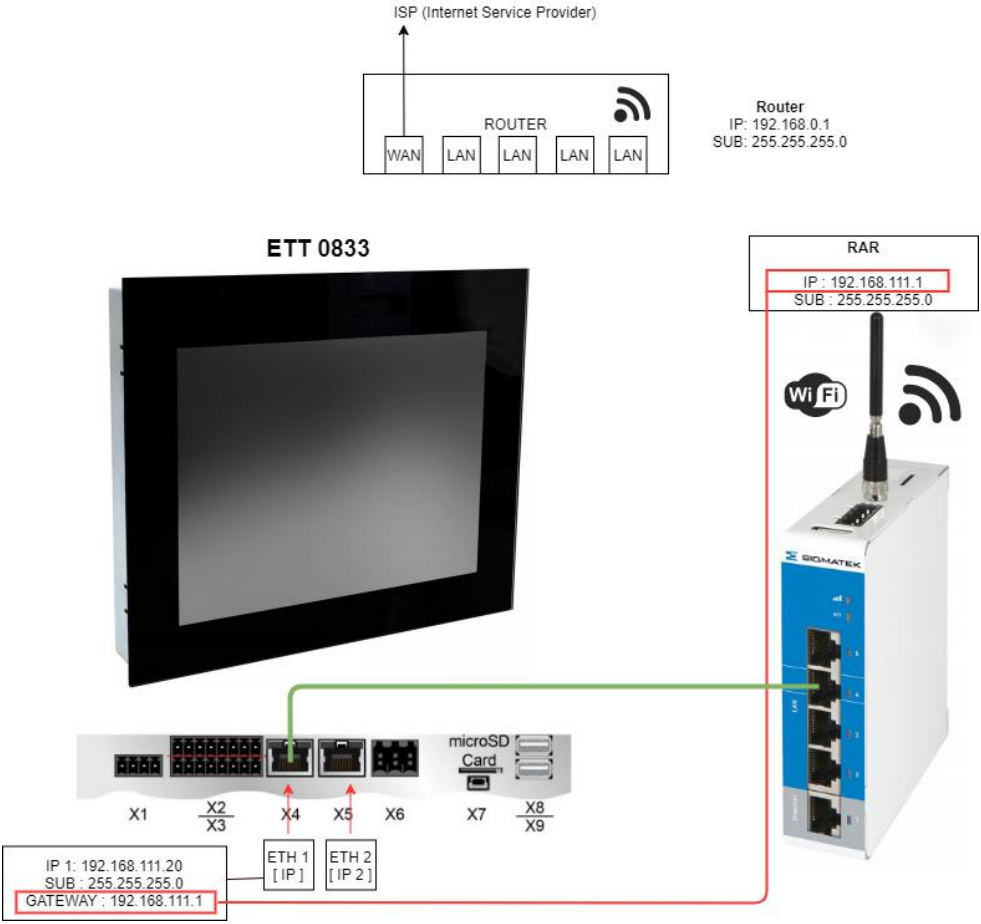
6.1.1 Example 1: RAR wired, single CPU solution



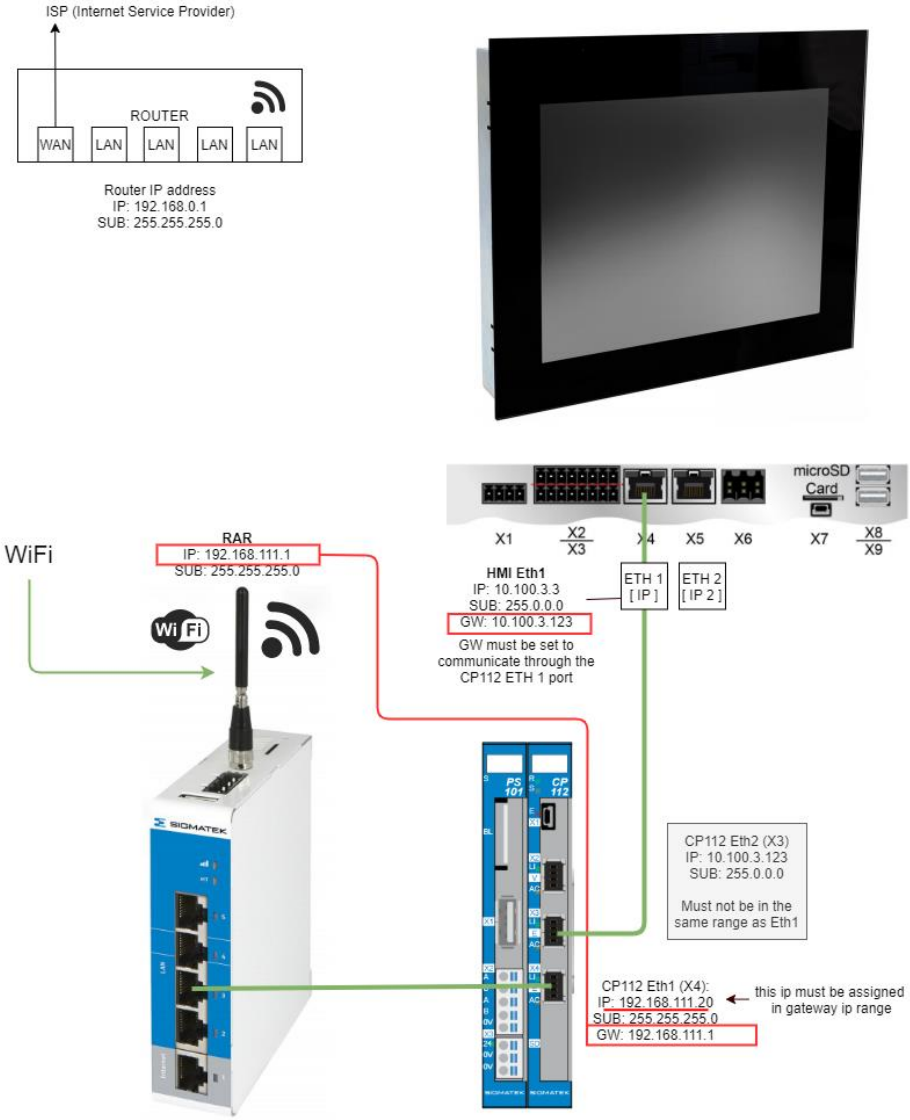
6.1.2 Example 2: RAR wired, dual CPU solution



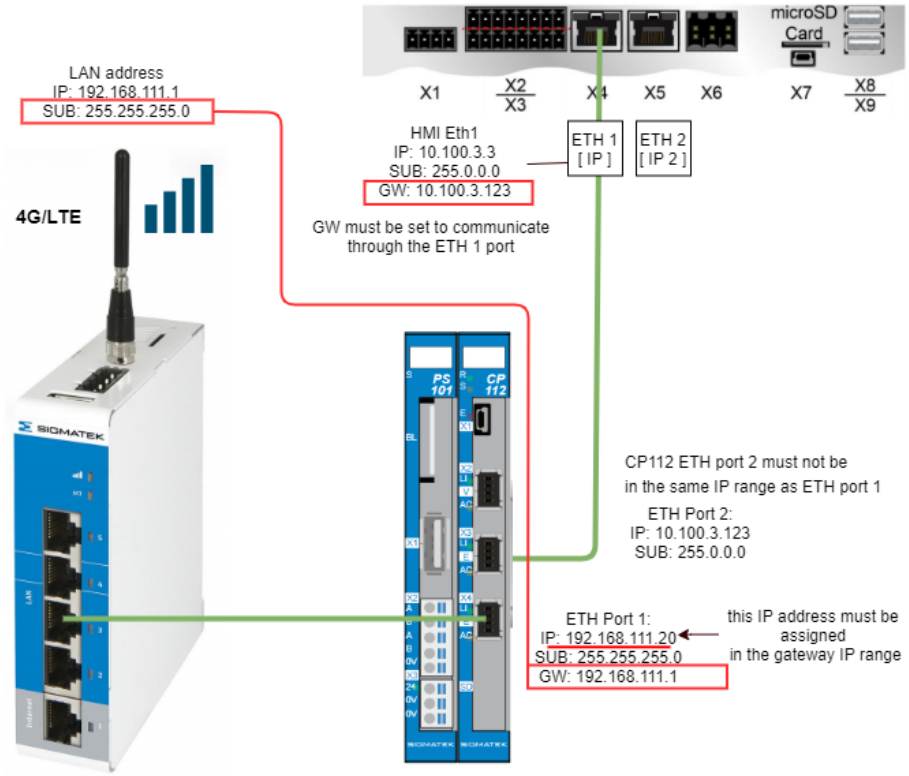
6.1.3 Example 3: RAR + WIFI, single CPU solution



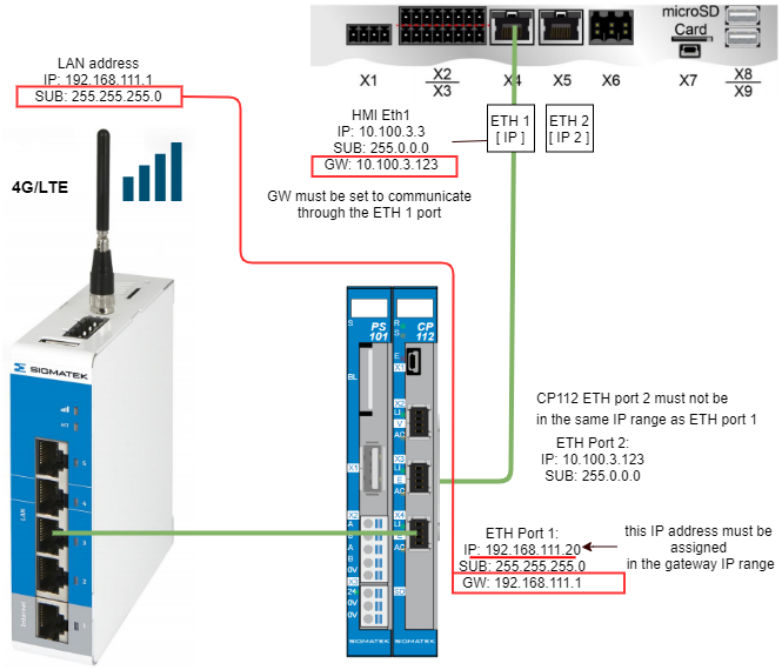
6.1.4 Example 4: RAR + WIFI, dual CPU solution



6.1.5 Example 5: RAR + cellular, single CPU solution

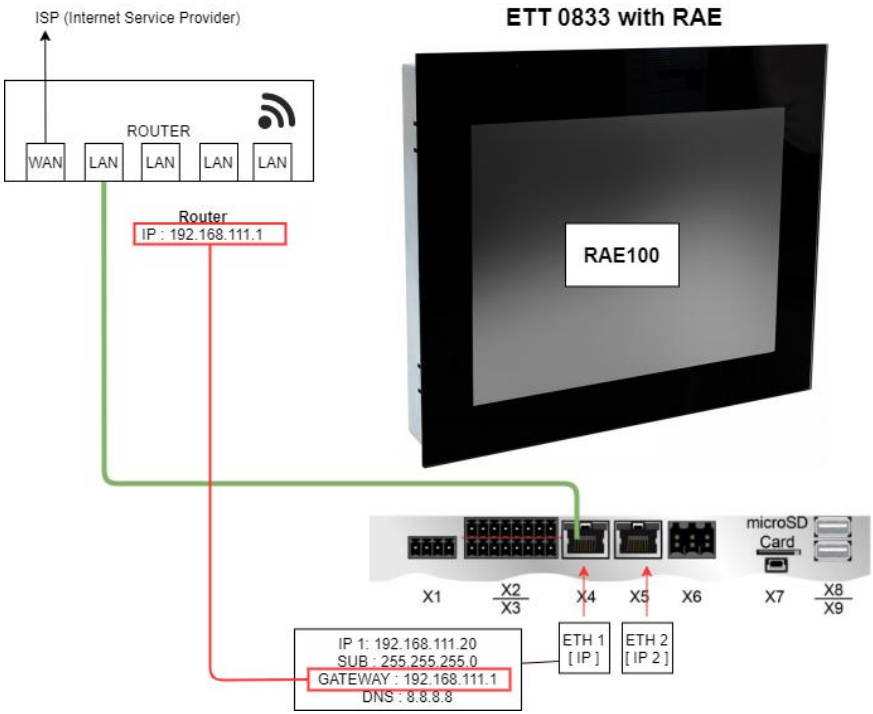


6.1.6 Example 6: RAR + cellular, dual CPU solution



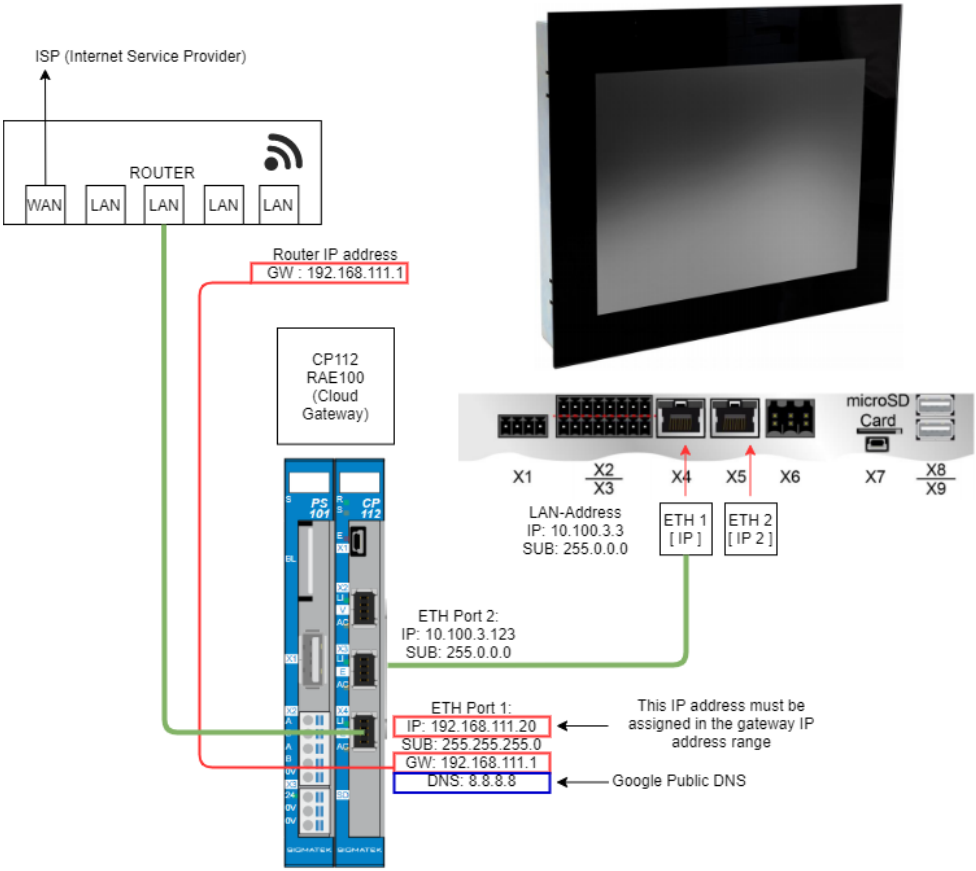
6.2 Remote Access Embedded (RAE) Solutions

6.2.1 Example 7: RAE100 single CPU solution

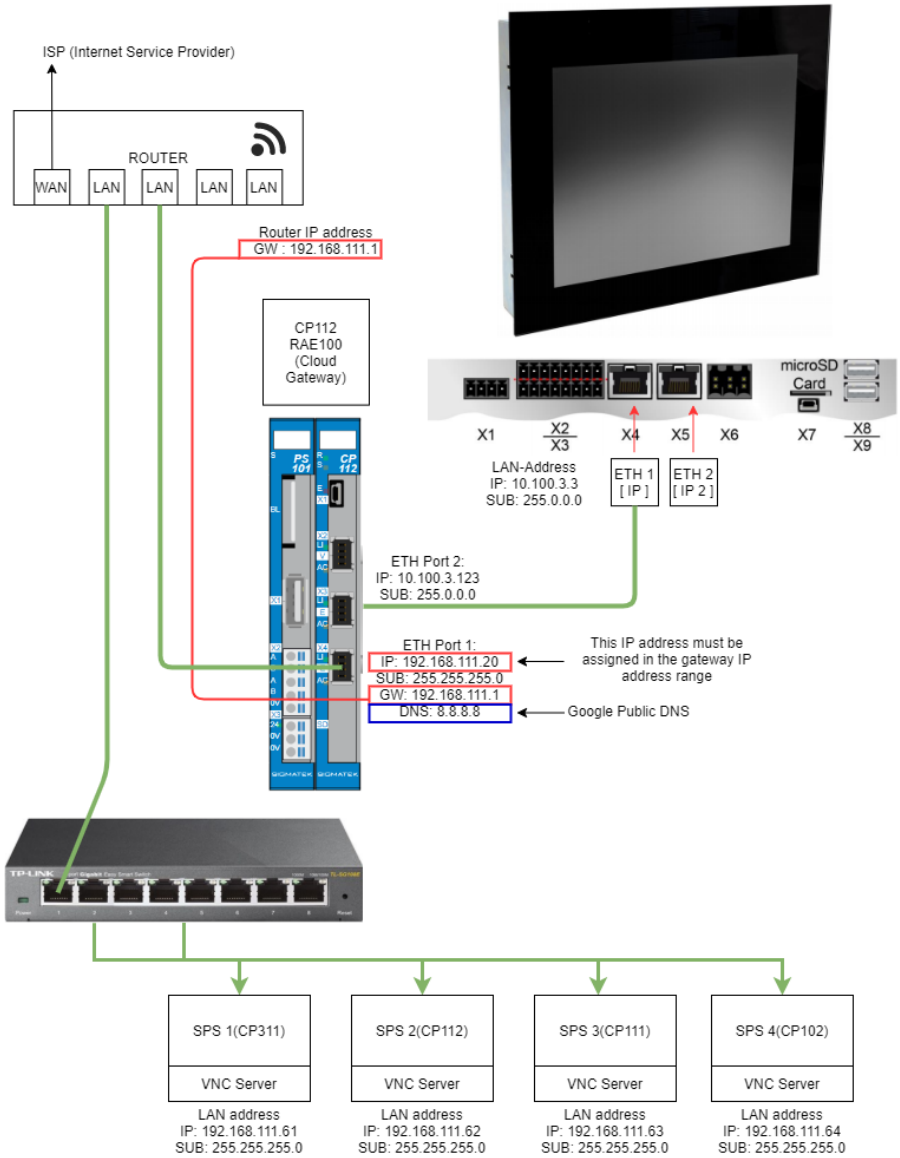


6.2.2 Example 8: RAE100 dual CPU solution

Additional setup is required to enable this solution, in the form of port forwarding on the control running RAE. Refer to section 0.



6.2.3 Example 9: RAE100 As Gateway



Example Autoexec.lsl

```
REM Ethernet interfaces
SET IP HOSTADDR 192 168 111 10
SET IP SUBNET 255 255 255 0
SET IP GATEWAY 192 168 111 1
SET IP DNS 8 8 8 8
SET IP 2 HOSTADDR 10 100 3 123
SET IP 2 SUBNET 255 0 0 0

REM Port forwarding to access CPxxx VNC from RAP
FIREWALL "-A FORWARD -j ACCEPT -p tcp --dport 5900 --sport 5901 -d
192.168.111.61 -m state --state NEW"
FIREWALL "-t nat -A PREROUTING -p tcp --dport 5901 -j DNAT --to-destination
192.168.111.61:5900"

FIREWALL "-A FORWARD -j ACCEPT -p tcp --dport 5900 --sport 5902 -d
192.168.111.62 -m state --state NEW"
FIREWALL "-t nat -A PREROUTING -p tcp --dport 5902 -j DNAT --to-destination
192.168.111.62:5900"

FIREWALL "-A FORWARD -j ACCEPT -p tcp --dport 5900 --sport 5903 -d
192.168.111.63 -m state --state NEW"
FIREWALL "-t nat -A PREROUTING -p tcp --dport 5903 -j DNAT --to-destination
192.168.111.63:5900"

FIREWALL "-A FORWARD -j ACCEPT -p tcp --dport 5900 --sport 5904 -d
192.168.111.64 -m state --state NEW"
FIREWALL "-t nat -A PREROUTING -p tcp --dport 5904 -j DNAT --to-destination
192.168.111.64:5900"

FIREWALL "-t nat -A POSTROUTING -j MASQUERADE"

IXAGENT START

LSLLOAD
RUN
```