

Secure Remote Access

Contents

1	Symbols Used.....	4
2	Quick Start	5
3	Configuring Remote Access Router Hardware.....	6
3.1	Electrical Connection	6
3.1.1	Wiring the RAR	6
3.1.2	Optional Hardware Switch for VPN Management	7
3.2	Prepare Hardware with Optional Interface	9
3.2.1	Mobile phone 3G/4G	9
3.2.2	WIFI	9
3.2.3	Using WIFI RAR as an Access Point (AP)	10
3.3	LED Status Display	13
3.3.1	 Signal LED.....	13
3.3.2	ACT Signal LED.....	14
4	Embedded Remote Access Setup	15
4.1	Requirements.....	15
4.2	Setup	15
5	Remote Access Platform (RAP)	21
5.1	Account Setup.....	21
5.2	RAP Cloud Interface	23

5.2.1	Apps Menu	24
5.2.2	Account Menu.....	24
5.2.3	Two-factor Authentication	25
5.3	Registering a Remote Product	27
5.3.1	Restoring Factory Settings	27
5.3.2	Remote Access Router via Ethernet WAN	28
5.3.3	Router for Remote Access via WIFI WAN	34
5.3.4	Remote Access Router with 3G/4G WAN.....	35
5.3.5	Embedded Remote Access	37
5.4	Additional Network Settings (RAR only)	39
5.5	Additional Network Settings (RAE only)	41
5.6	Configuring Remote Services	43
5.6.1	Creating a VPN Connection.....	43
5.6.2	VNC via VPN	44
5.7	Data collection and Storage	48
5.7.1	Configuring Data Sources	48
5.7.2	Cloud Logging	59
5.7.3	Creating a page for Data Display.....	63
5.7.4	Cloud Notifications.....	78
5.8	User Administration	84
5.8.1	Adding a new user	90
6	Example Solutions.....	93
6.1	Solutions Based on the Remote Access Router (RAR)	93
6.1.1	Example 1: RAR Wired, One-CPU Solution	95
6.1.2	Example 2: RAR Wired, Two-CPU Solution	96

6.1.3	Example 3: RAR + WIFI, One-CPU Solution	97
6.1.4	Example 4 RAR + WIFI, Two-CPU Solution	98
6.1.5	Example 5: RAR + Mobile Network, One-CPU solution	99
6.1.6	Example 6: RAR + Mobile Network, Two-CPU Solution	100
6.2	Embedded Remote Access Solutions (RAE)	101
6.2.1	Example 7: RAE100 One-CPU Solution	101
6.2.2	Example 8: RAE100 Two-CPU Solution	102
6.2.3	Example 9: RAE100 as a Gateway	103
6.3	User Administration.....	105
6.3.1	Example 10: Remote Access Service	105
7	Installation iOS App	107
7.1	Start Menu and App Store.....	107
7.2	App Store – Sigmatek App.....	108
7.3	Install App.....	109
7.4	Sigmatek Login and Home Screen.....	110
8	Installation Android App.....	111
8.1	Startmenü und Play Store	111
8.2	Play Store – Sigmatek App	112
8.3	Install App.....	113
8.4	Sigmatek Login and Home Screen.....	114

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 steps essential for remotely connecting a computer with the SIGMATEK Remote Access Platform (RAP) consist of:

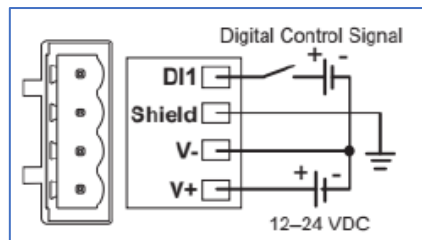
1. For the initial use, register for an RAP business/user account, s5.1.
2. Configure the remote product as needed:
 - a. RAR Hardware, s3
 - b. RAE application, s4 (not required for RAR)
3. Register the device during the initial use.
 - a. RAR via Ethernet, s5.3.2
 - b. RAR via WIFI, s5.3.3.
 - c. RAR via mobile services 3G/4G, s5.3.4.
 - d. RAE application, s5.3.5.
4. Connect control with the RAP. Examples are provided:
 - a. RAR, s6.1
 - b. RAE, s6.2
5. Add remote services:
 - a. VNC, s5.6.2
 - b. Port-forward for IP services, s5.4
 - c. Data recording, s5.7

3 Configuring Remote Access Router Hardware

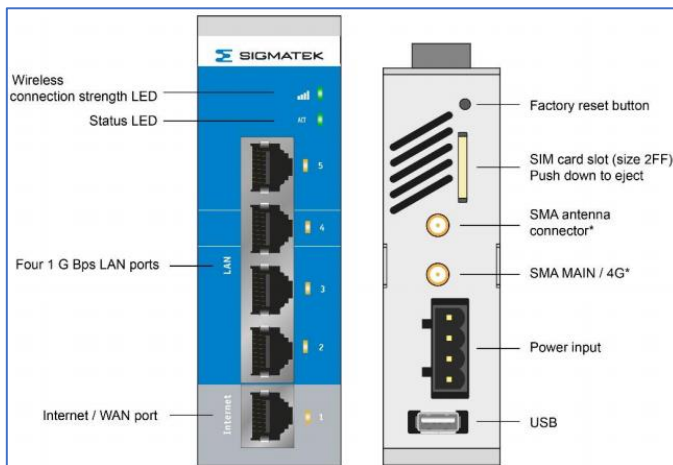
3.1 Electrical Connection

3.1.1 Wiring the RAR

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



Screenshot 1 Supply input connector pin layouts.



Screenshot 2 RAR diagram.

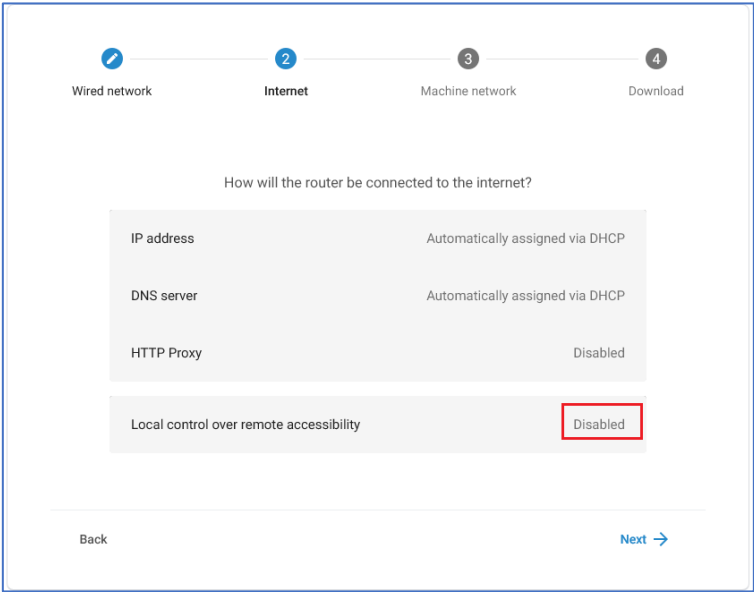
3.1.2 Optional Hardware Switch for VPN Management

The digital input DI1 can be used to deactivate the VPN, this option must be activated via the RAP.

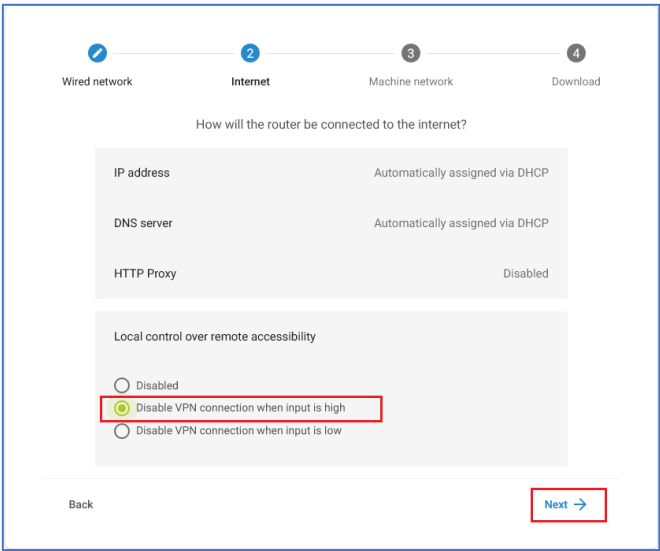
1. Ensure that the electrical wiring of the device is complete (Screenshot 3) and logged into the RAP. See section 0 for registration.
2. In the process of creating a configuration file in section 0, select the option “Select control over remote accessibility” (Screenshot 4)
3. A new controller element with the name “digital input” is displayed (Screenshot 5), select one of the options:
 - a. deactivated [digital input inactive],
 - b. deactivate VPN , if[digital] input low,
 - c. deactivate VPN , if[digital] input high,
4. Proceed with Router config file.



Screenshot 3 Installed RAR with switch at digital input 1.



Screenshot 4 Select local control over the VPN connection.



Screenshot 5 Select the action for the digital input.

3.2 Prepare Hardware with Optional Interface

3.2.1 Mobile phone 3G/4G

While turned off:

1. Then insert the SIM card into the SIM card slot (Screenshot 6).
2. Screw the antenna onto the SMA connector with the label "MAIN" (Screenshot 7).



Screenshot 6 RAR with SIM card marked with red



Screenshot 7 RAR with mobile phone option: 3G/4G antenna installed on the SMA connector of the mobile device.

3.2.2 WIFI

With the device turned off: Connect the WIFI antenna via the SMA connection labeled "DIV".

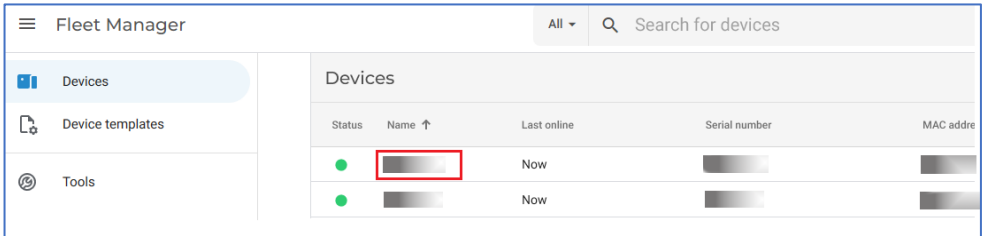


Screenshot 8 RAR with WIFI antenna installed on the SMA connector for the 2.4 GHz signal.

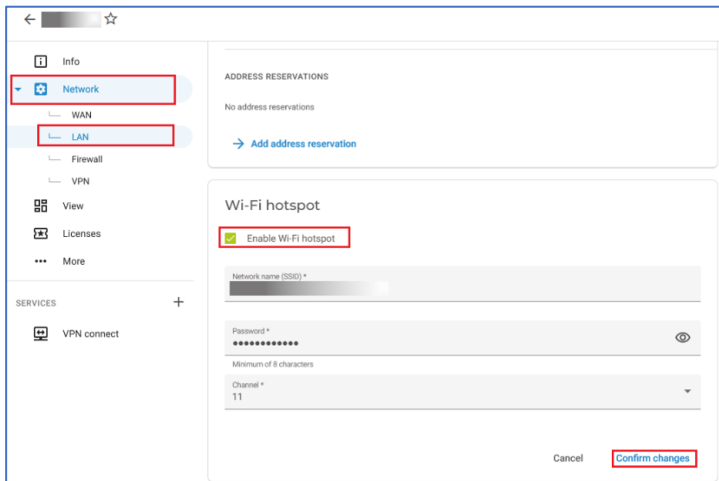
3.2.3 Using WIFI RAR as an Access Point (AP)

An Access Point (AP) is configured in the RAR via the RAP as follows:

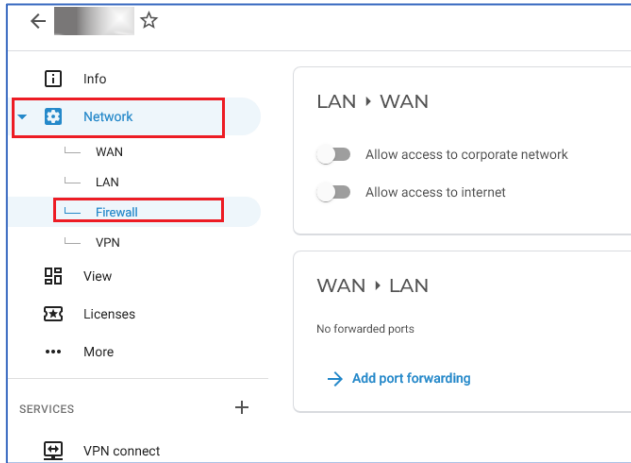
1. Ensure that the electrical wiring of the device is complete (Screenshot 3) and Logged into the RAP. See section 0 for registration.
2. In the RAP, select APPS Menu -> Fleet Manager, and choose the device to configure (Screenshot 9).
3. From Device Menu select Network->Lan for adapting the LAN settings (Screenshot 10).
4. Tick "Enable Wi-Fi-Hotspot"
5. Assign the SSID and password as needed.
6. Click on "Confirm", to save the settings.
7. Select "Push Config to Device". This will sync the changes with the current configuration on the device (Screenshot 12).
8. Via the firewall settings from the Device Menu->Network->Firewall, it is also possible to restrict or allow access to the Internet or host network (Screenshot 11).



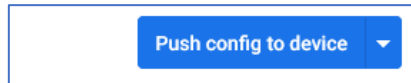
Screenshot 9 Select the Device from the Fleet Manager Menu.



Screenshot 10 Adjust the firewall settings to configure the access to the Internet and host network via the AP.



Screenshot 11 Adjust the firewall settings to configure the access to the Internet and host network via the AP.



Screenshot 12 Configuration changes must always be loaded into the RAR, to be enabled.

3.3 LED Status Display

3.3.1 Signal LED

	Blinks blue	Mobile phone module initializing
	Blinks red 1 pulse	No reception or unable to connect to network (APN or SSID may be wrong)
	Blinks red 2 pulses	PIN invalid or PUK required (To unlock the SIM card with the PUK, a phone is required)
	Blinks red 4 Pulses	SIM card is invalid or missing
	Constant red	Connected, weak reception
	Constant Violet	Connected, medium reception
	Constant Blue	Connected, good reception

3.3.2 ACT Signal LED

	Constant red	Start-up (may take 1-2 min) or not yet registered
	Blinks red 1 pulse	Waiting for internet access
	Blinks red 3 Pulses	LAN/WAN conflict (conflicting subnets)
	Blinks red 4 Pulses	Removed from the platform RAR must be reconfigured and newly logged in
	Blinks red 5 Pulses	Previously logged into RAP (remove from the RAP and log in again)
	Blinks blue 1 pulse	Establishing a connection with RAP
	Blinks blue 2 pulses	Initializing the VPN connection
	Constant blue	Active VPN connection

4 Embedded Remote Access Setup

4.1 Requirements

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

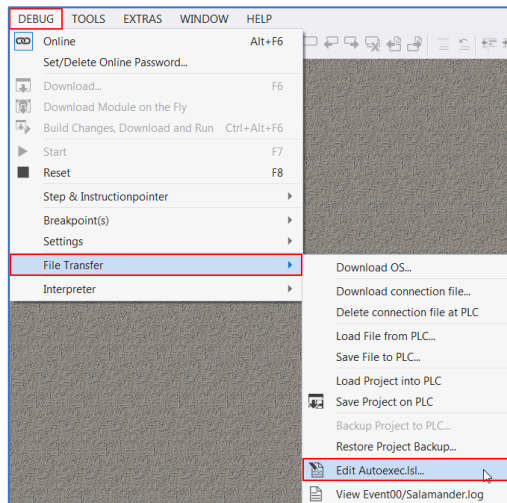
- To install RAE in the SIGMATEK control, the following operating system version is required:
 - Salamander 09.03.102 or higher
- The SIGMATEK Control, into which the RAE100 is installed, must have a valid IP configuration with Internet access.

4.2 Setup

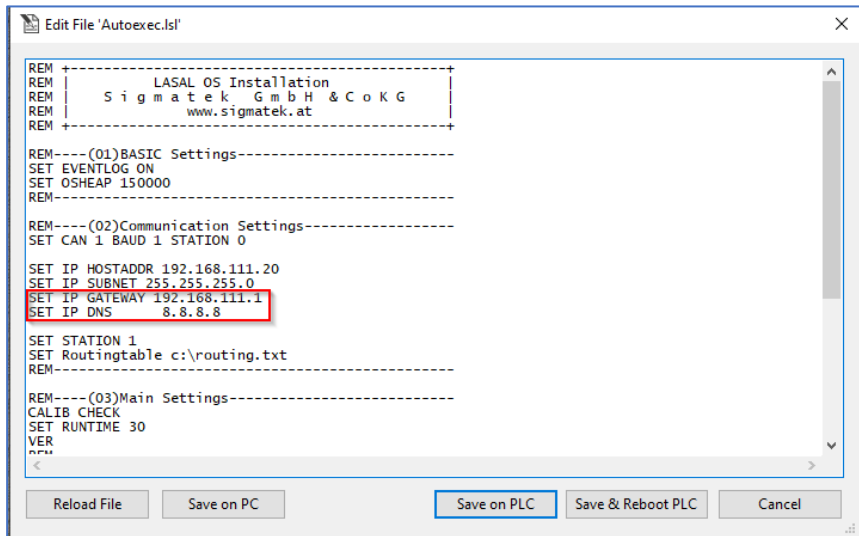
This process describes the testing process for preparing a SIGMATEK control with RAE. The remote product must be registered after configuration.

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 Screenshot 13.
3. Use the settings currently valid for LAN (Screenshot 14):
 - a. IP address
 - b. IP subnet
 - c. IP gateway: IP address of the router used for Internet access
 - d. IP DNS: IP address of a DNS server, which can be reached from the current location. Several server addresses are listed below.
 - i. Cloudflare 1.1.1.1
 - ii. Google 4.4.4.4 or 8.8.8.8
4. With the PLCDiag tool File Commander, under "Tools Advanced Debug Tool → File Commander", create the folder "C:\lsys\packages" if it does not already exist.
 - a. To create a folder, use "MAKE DIR". (Screenshot 15, Screenshot 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" below (Screenshot 17).
5. To install RAE, enter the command in the Command Line Interface.

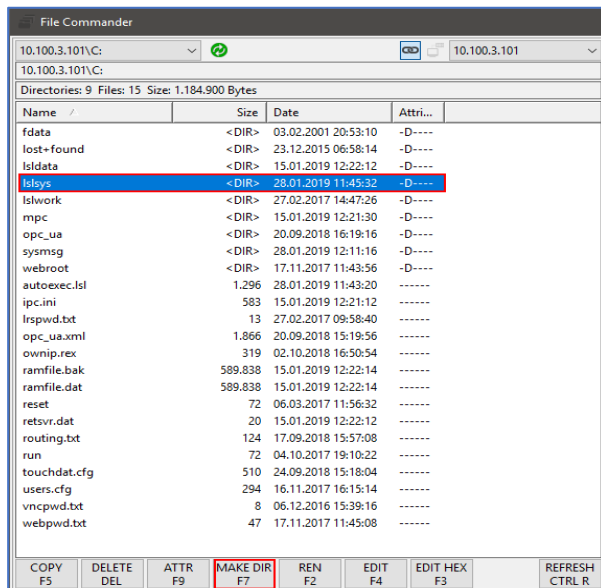
- a. Open the Remote CLI under "Tools" → Advanced Debug Tools → Remote CLI" (Screenshot 18).
- b. To check the internet connection, enter the command "ping www.google.com" (or a site accessible from your region) in the command line and press the enter key or "Execute". If the computer can access the internet, a latency value is registered for the ping command.
- c. Enter the command "PACKAGE INSTALL ixagent" in the command line and press Enter or "Execute" (Screenshot 19). Installation may take some time. Wait for the return (Screenshot 20).
- d. After RAE is installed, it must be enabled with the command "ixagent start" (Screenshot 19). Wait for the return (Screenshot 20).
- e. The RAE application must be started after installation:
 - i. The "ixagent start" command can be run via the remote CLI as needed (Screenshot 21).
 - ii. To automatically start with the machine, the same "ixagent start" command should be attached to the Autoexec.IsI (Screenshot 22).



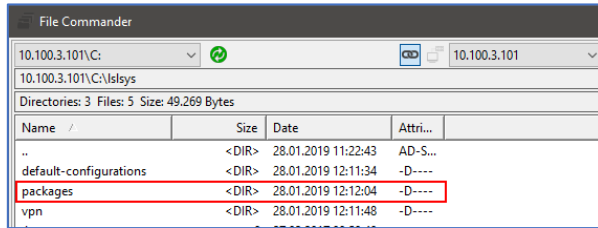
Screenshot 13 Processing the Autoexec.IsI from Class 2.



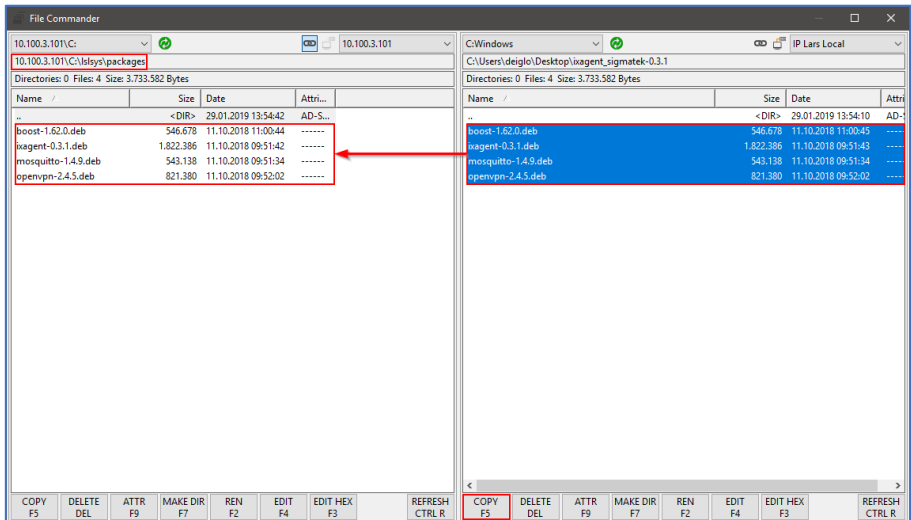
Screenshot 14 Processing the IP configuration



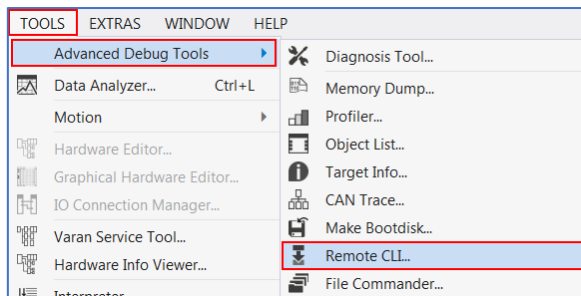
Screenshot 15 File Commander interface - Make Dir Button marked.



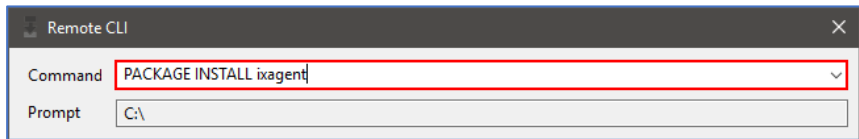
Screenshot 16 Packages folder in C:\lsys



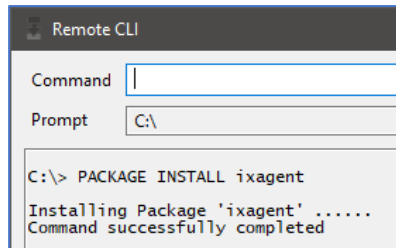
Screenshot 17 Copy packages to the machine.



Screenshot 18 Open the Remote CLI Tool.



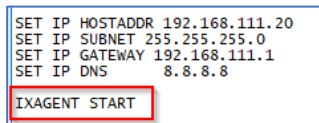
Screenshot 19 Run the command for installing the RAE application via the CLI.



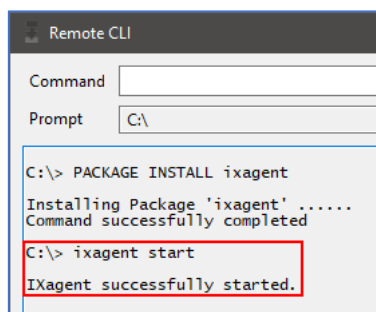
Screenshot 20 Successful installation confirmed.



Screenshot 21 Start the RAE application.



Screenshot 22 Attaching the command for starting the RAE application to the Autoexec.lsl file.



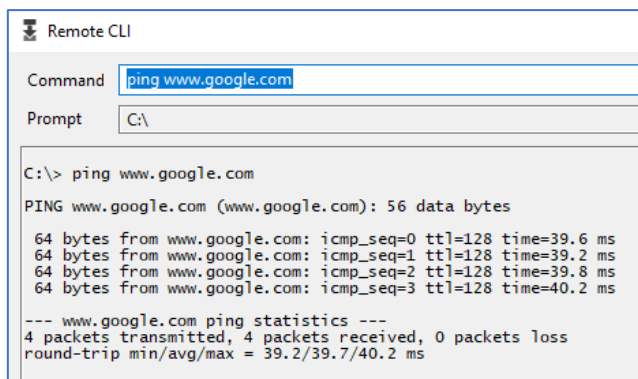
```
Remote CLI

Command
Prompt C:\

C:\> PACKAGE INSTALL ixagent
Installing Package 'ixagent' .....
Command successfully completed

C:\> ixagent start
IXagent successfully started.
```

Screenshot 23 Message confirming that the RAE application was successfully started.



```
Remote CLI

Command ping www.google.com
Prompt C:\

C:\> ping www.google.com
PING www.google.com (www.google.com): 56 data bytes
 64 bytes from www.google.com: icmp_seq=0 ttl=128 time=39.6 ms
 64 bytes from www.google.com: icmp_seq=1 ttl=128 time=39.2 ms
 64 bytes from www.google.com: icmp_seq=2 ttl=128 time=39.8 ms
 64 bytes from www.google.com: icmp_seq=3 ttl=128 time=40.2 ms

--- www.google.com ping statistics ---
 4 packets transmitted, 4 packets received, 0 packets loss
round-trip min/avg/max = 39.2/39.7/40.2 ms
```

Screenshot 24 Running the PING command to a domain with a web server that supports ICMP Echo Response.

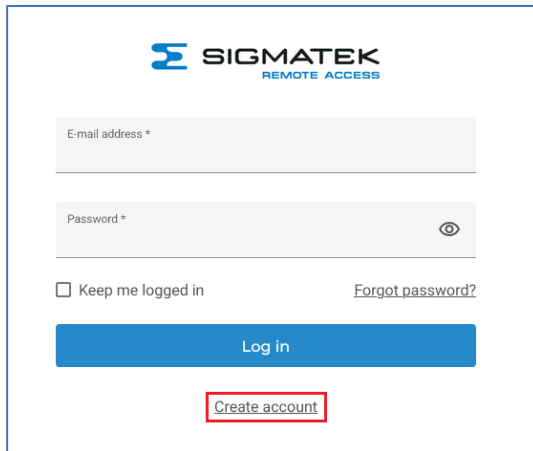
5 Remote Access Platform (RAP)

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

5.1 Account Setup

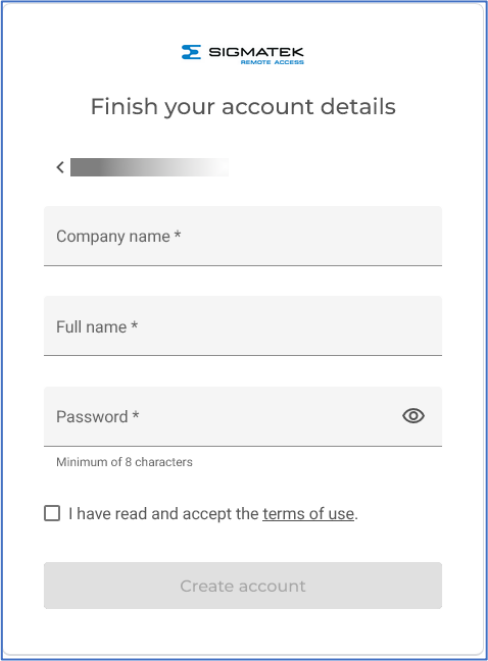
If you have not yet created a company account, please register with the Remote Access Platform.

1. Open the RAP main page: <https://www.sigmatek-connect2.com>. To register, click the link "Create account" (Screenshot 25).
2. Enter the required data and confirm the conditions to proceed (Screenshot 26).
3. If the registration is successful, an e-mail is sent to the registered address. This link must be clicked to activate the account (Screenshot 27).



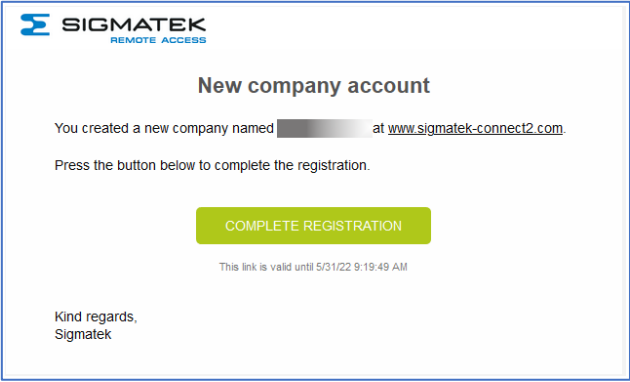
The screenshot shows the SIGMATEK Remote Access Platform login and registration interface. At the top is the SIGMATEK logo with "REMOTE ACCESS" underneath. Below the logo are two input fields: "E-mail address *" and "Password *". The password field has an eye icon for toggling visibility. Below the password field is a checkbox labeled "Keep me logged in" and a link "Forgot password?". A large blue button labeled "Log in" is positioned below these elements. At the bottom, a red-bordered button labeled "Create account" is highlighted.

Screenshot 25 Registering a new company account.



The screenshot shows a web form titled "Finish your account details" with the Sigmatek Remote Access logo at the top. Below the title is a back arrow and a blurred input field. The form contains three main input sections: "Company name *" with a light gray background, "Full name *" with a light gray background, and "Password *" with a light gray background and a toggle eye icon. Below the password field is the text "Minimum of 8 characters". At the bottom, there is a checkbox labeled "I have read and accept the [terms of use](#)." and a large gray button labeled "Create account".

Screenshot 26 Entering the required data.



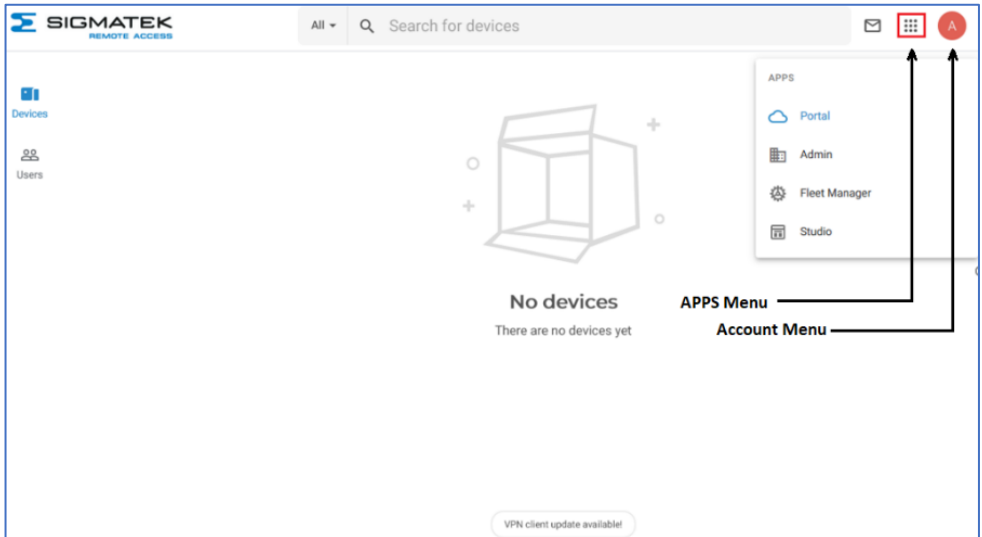
The screenshot shows an email template titled "New company account" with the Sigmatek Remote Access logo. The text reads: "You created a new company named [blurred] at www.sigmatek-connect2.com." Below this, it says "Press the button below to complete the registration." and features a prominent green button labeled "COMPLETE REGISTRATION". Under the button, it states "This link is valid until 5/31/22 9:19:49 AM". At the bottom left, it says "Kind regards, Sigmatek".

Screenshot 27 Complete the registration by clicking the link in the e-mail.

5.2 RAP Cloud Interface

To log onto the platform:

1. go to the main page <https://www.sigmatek-connect2.com>.
2. After entering the log-in data, click on "LOG IN".
3. If more than one company is available select one. This is required for displaying and registering new devices.
4. The RAP main interface is then displayed (Screenshot 28). It displays the List of configured Devices and Users. The Apps Menu and Account Menu can be expanded and are placed on the top-right corner of the screen (Screenshot 28).



Screenshot 28 main interface for a selected company with the Apps menu expanded

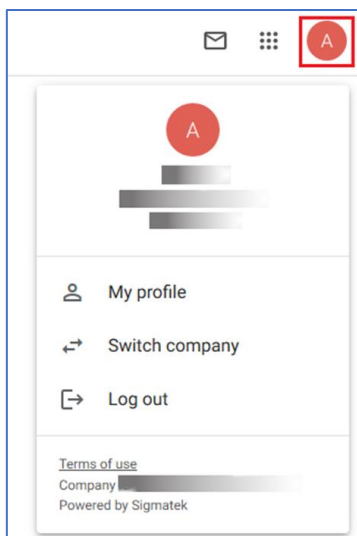
5.2.1 Apps Menu

- Portal, Use your device's services and invite users
- Admin, Manage your company
- Fleet Manager, Manage your fleet of devices
- Studio, Create custom pages so you only see what you need to see

5.2.2 Account Menu

Open the Account Menu by clicking on the Red Circle (Screenshot 29). It provides access to:

- Profile settings - localization, e-mail address, security and viewing rights
- Change companies - when managing multiple companies with a single user account



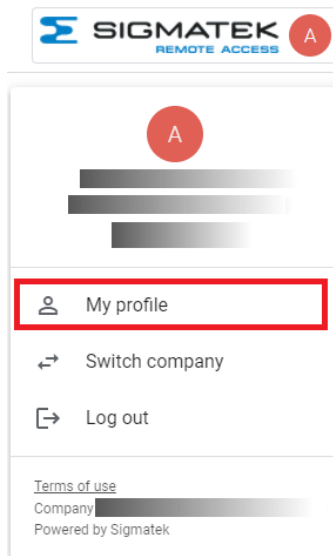
Screenshot 29 Open Account settings via the main interface.

5.2.3 Two-factor Authentication

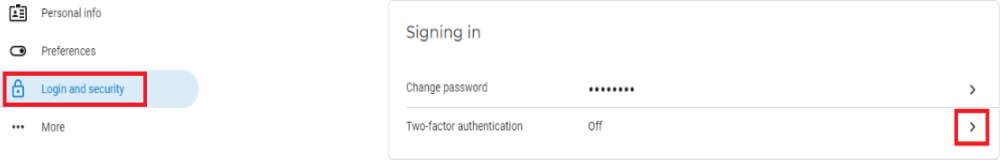
Two-factor authentication (2FA) is an additional security measure used to strengthen an account and prevent others from accessing it.

To enable two-factor authentication:

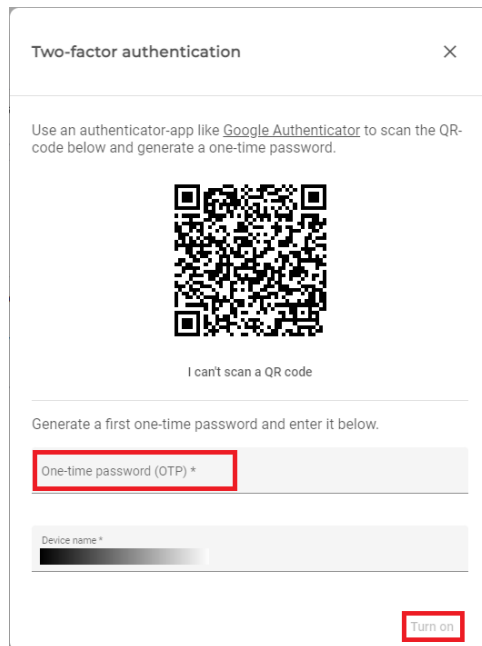
1. Open the personal profile settings. (Screenshot 30)
2. Under the Login and security menu item, click the right arrow to activate two-factor authentication. (Screenshot 31)
3. Then you can scan the QR code with the help of an authentication app such as Google Authenticator. The generated one-time password (OTP) can now be entered. (Screenshot 32)
4. If it is not possible to scan the QR code, it is possible to register in the authentication app using a code and generate a one-time password.



Screenshot 30 Opening the personal profile



Screenshot 31 Under the menu item Login and security click Two-factor authentication.



Screenshot 32 Scan the QR code using an "authentication app" and then enter the one-time password below it.

5.3 Registering a Remote Product

So that the RAR can connect to the cloud, it must first be configured: A configuration file is created and downloaded onto the RAR.

5.3.1 Restoring Factory Settings

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.



Caution: with a **factory reset**, the router **configuration** is **deleted**. This includes WAN/LAN settings, port forwarding, IP services and data upload. Ensure that the old configuration is no longer needed.

When the RAR is turned on, press the small button on the router for 5 seconds until the ACT LED starts blinking from blue to red

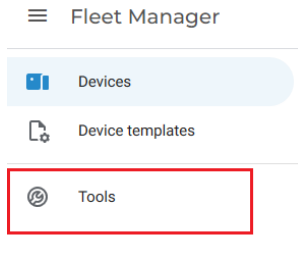


Screenshot 30 Position of the reset button

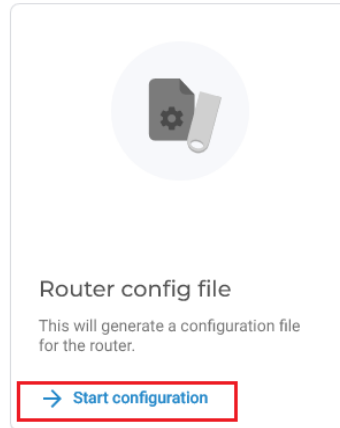
5.3.2 Remote Access Router via Ethernet WAN

From the RAP Apps menu:

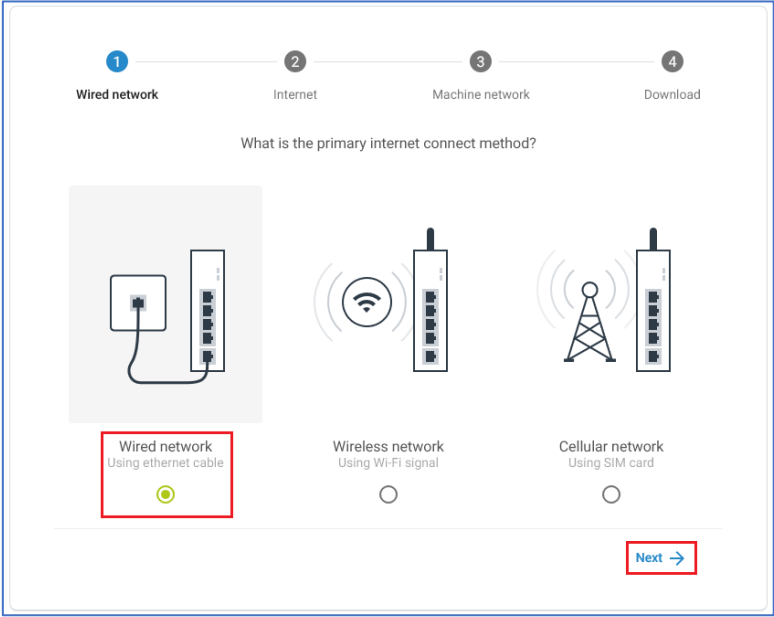
1. Open the Fleet Manager Menu and Click on the Tools option (Screenshot 31).
2. Under “Router config file”, click on “Start Configuration” (Screenshot 32).
3. Select the Internet connection type: wired via Ethernet cable (Screenshot 33).
4. Accept the default WAN configuration or define the settings (Screenshot 34). The settings can be changed after the device is registered.
5. Specify the router address to use in the Router LAN(Screenshot 35).
 - a. Example: The SIGMATEK control has an IP address of 192.168.111.20 and a subnet mask of 255.255.255.0, the router address should be specified in the range 192.168.111.x
 - b. Additional LAN networks can be added later.
6. Download the RAR configuration file (Screenshot 36). With most Windows-based browsers, the file (ixrouter.conf) is stored in the user’s download directory.
7. Copy the configuration file into the main directory of a USB drive.
8. Turn the RAR on, ensure that the WAN interface is connected. Insert the USB drive into the USB connector of the RAR.
9. The ACT LED flashes blue, and the configuration is complete when the LED is no longer flashing; the drive can be removed.
10. The new device is displayed in Fleet Manager area of the RAP with a highlighted background. Left click on the New device (Screenshot 37).
11. Tick the box, choose a name and “Activate the device” to complete the device registration (Screenshot 38).
12. The device is now automatically displayed in the RAP until it is logged off (Screenshot 39).



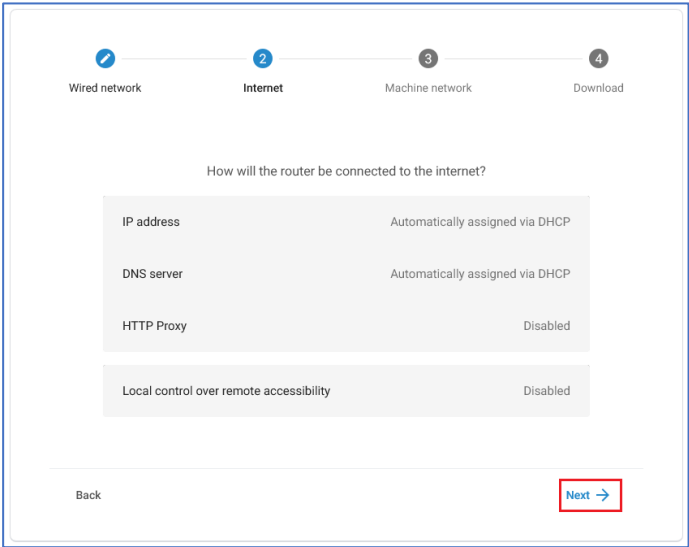
Screenshot 31 Select Tools from the Fleet Manager main menu.



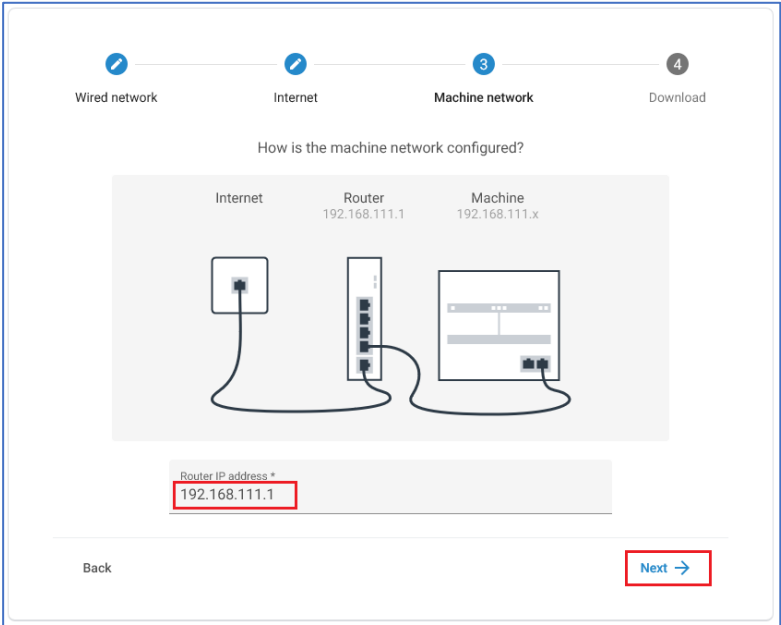
Screenshot 32 Select the option for starting the configuration.



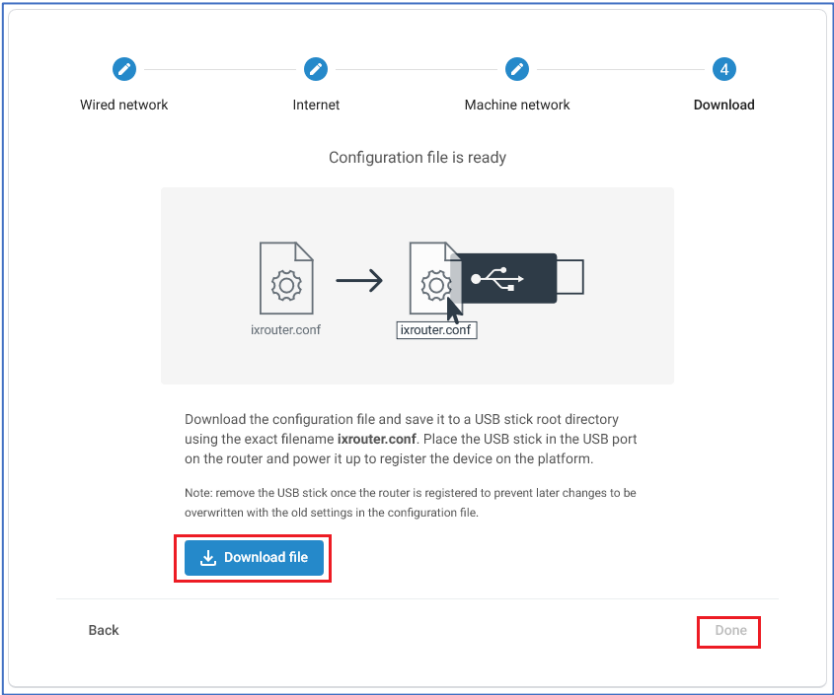
Screenshot 33 Select the WAN interface.



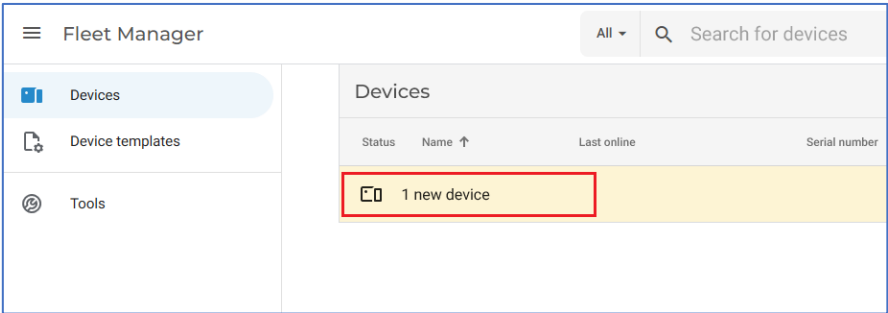
Screenshot 34 Accept/change the WAN interface settings.



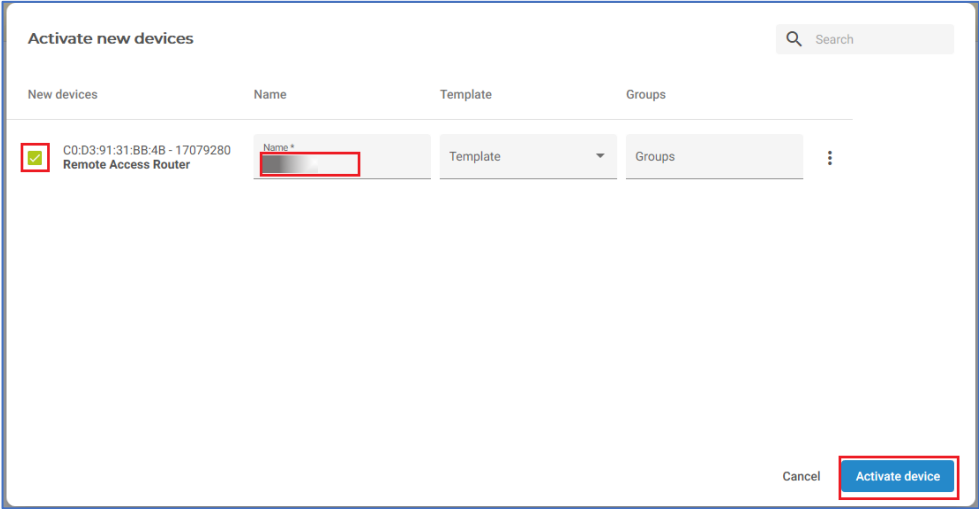
Screenshot 35 LAN interface configuration.



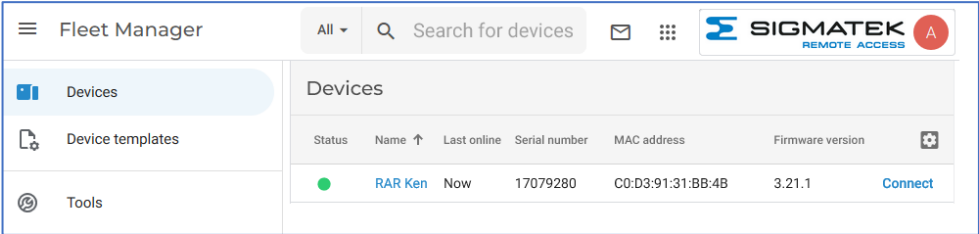
Screenshot 36 Download the RAR configuration file.



Screenshot 37 Left Click on New Device



Screenshot 38 Activate the new device via the RAP.

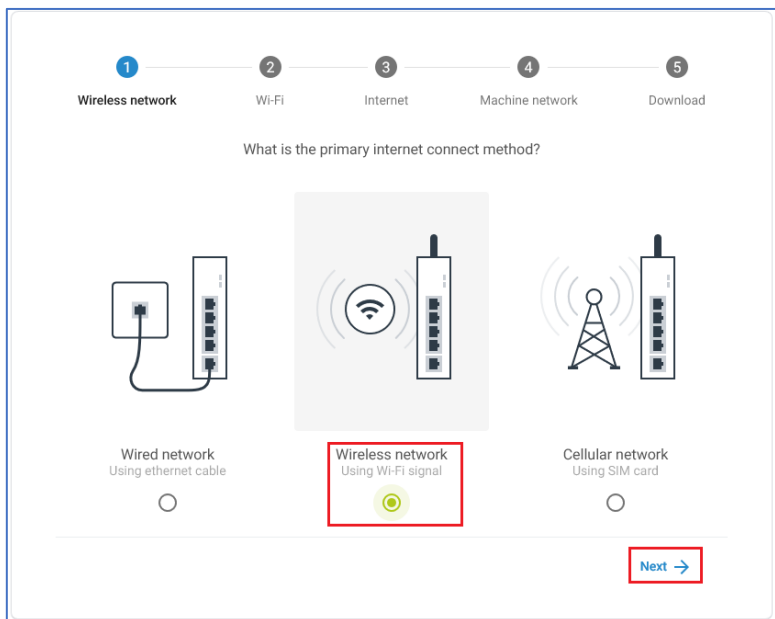


Screenshot 39 After registering the device, the current VPN status of the device is displayed in the main interface of the RAP.

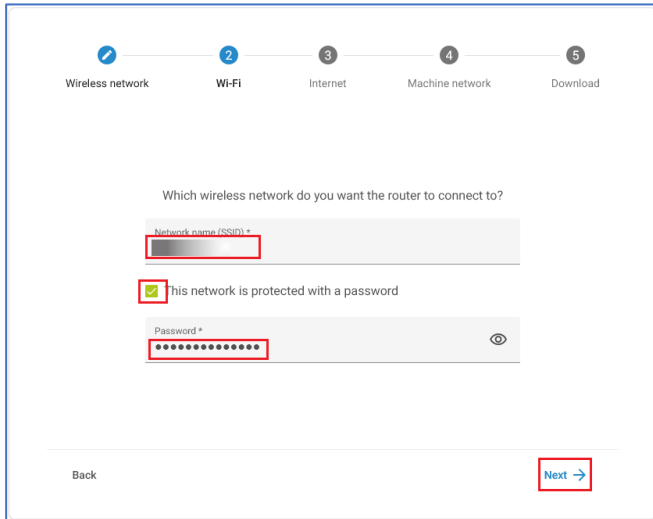
5.3.3 Router for Remote Access via WIFI WAN

See process in 5.3.2.

- In step 3 (selecting the internet connection type), select “Wireless Network” as the method for internet access (Screenshot 40).
- Enter the WIFI SSID and password to provide Internet access (Screenshot 41).
- Complete set-up according to section 5.3.2.



Screenshot 40 Select the Internet connection method: “Wireless”.



Wireless network **Wi-Fi** Internet Machine network Download

Which wireless network do you want the router to connect to?

Network name (SSID) *

☒ This network is protected with a password

Password *

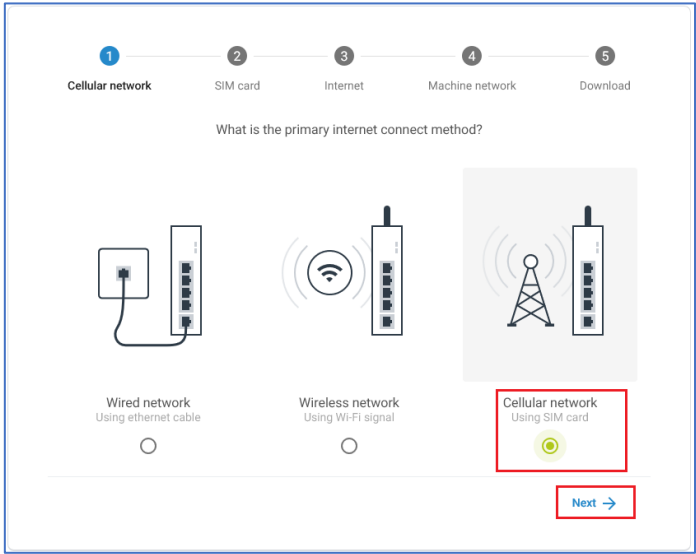
Back Next →

Screenshot 41 Enter the WIFI access data for the host network.

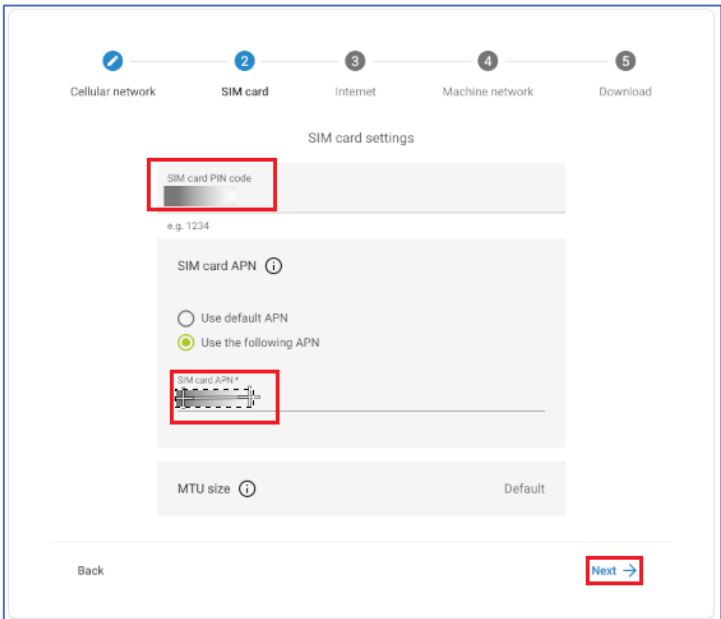
5.3.4 Remote Access Router with 3G/4G WAN

See process in section 5.3.2.

- In step 3 (selecting the internet connection type), select “Mobile Network” as the method for internet access (Screenshot 42).
- Enter the "SIM card APN" and the "SIM card PIN code". These data can be requested by the network (Screenshot 43).
- Complete set-up according to section 5.3.2..



Screenshot 42 Select the Internet connection method: “Cellular Network”.



Screenshot 43 Enter the SIM card data.

5.3.5 Embedded Remote Access

This section applies to the embedded software solution RAE100. The RAE100 must first be installed. This process is described in Section 4.

When used for the first time, The RAE-capable control must be registered in the RAP:

1. Via the remote CLI, run the "ixagent register companyID" command (Screenshot 44). The RAP company ID can be found in the RAP interface under "Identity". APPS Menu -> Admin-> Identity (Screenshot 45).
2. Successful registration is confirmed by a return message in the Command Line Feedback (Screenshot 46).
3. The new device is then displayed in Fleet Manager area of the RAP with a highlighted background. Left click on the new device (Screenshot 37).
4. Tick the box, choose a name and "Activate the device" to complete the device registration (Screenshot 38).
5. For a RAE device an activation code is required (Screenshot 47).

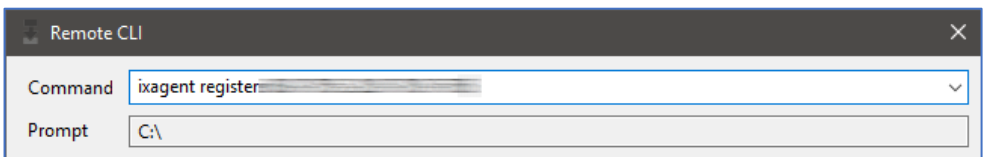


Acquire a RAE device activation code from your SIGMATEK representative.

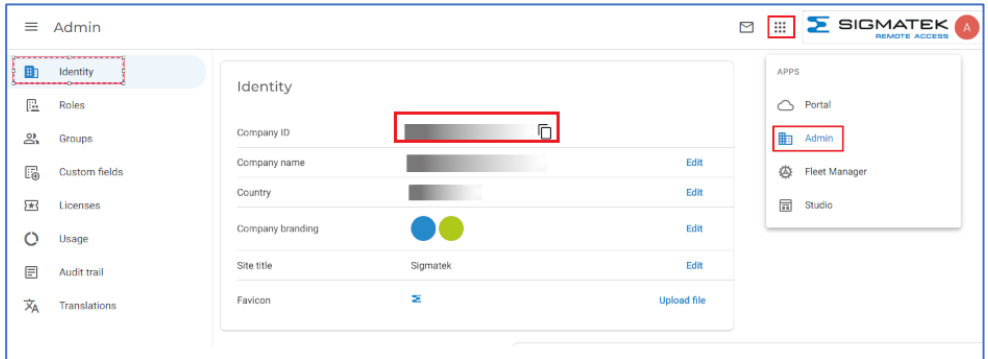
6. The device is now automatically displayed in the RAP until it is logged off (Screenshot 39).



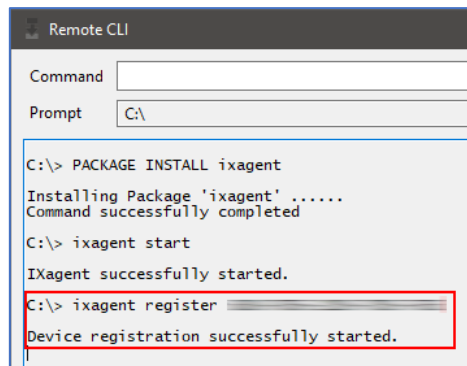
If it is not possible to add certain services like a VNC connection, you have to add an IP address and network mask under the menu item 'Network' in the 'LAN' section. These are freely selectable.



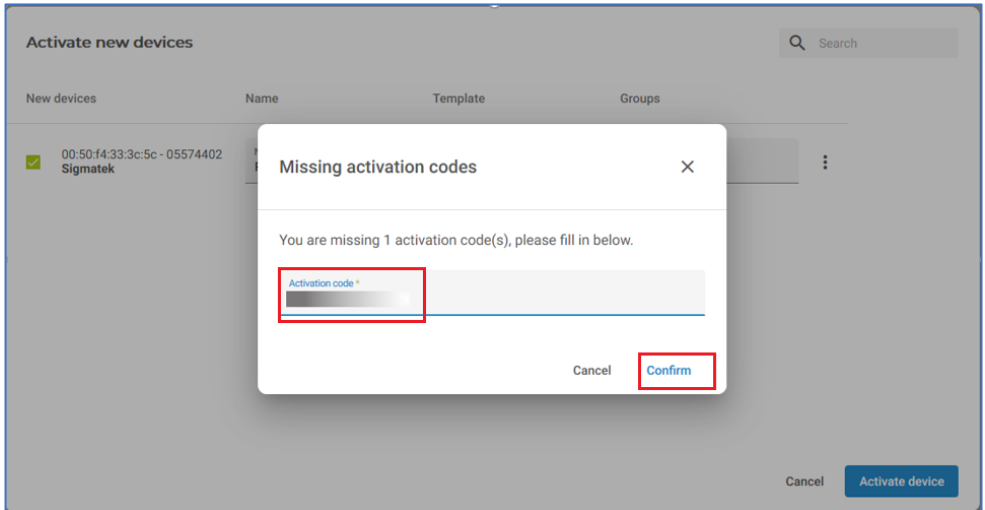
Screenshot 44 Running the register command in the Remote-CLI.



Screenshot 45 The company ID is displayed under APPS Menu -> Admin-> Identity.



Screenshot 46 Successful registration confirmed.



Screenshot 47 Activation code is required for RAE

5.4 Additional Network Settings (RAR only)

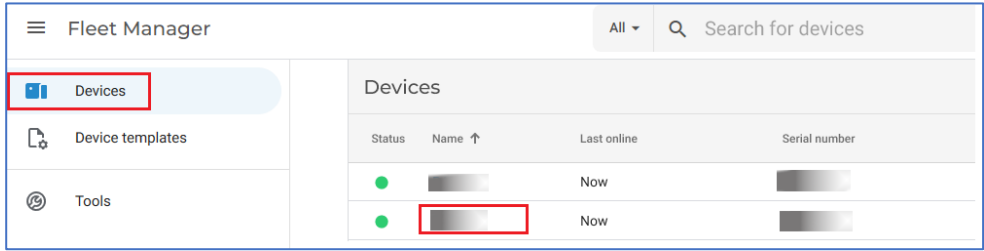
By Clicking on a RAR Device listed on APPs Menu -> Fleet Manager, several Network options are available

In the RAR LAN configuration, it's possible to:

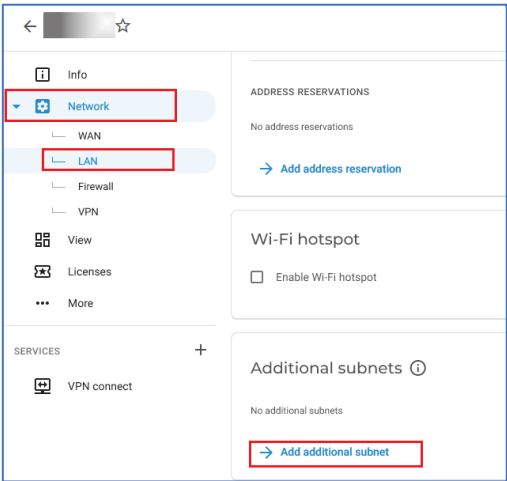
- add an additional subnet
- Assign static IP leases
- Change the IP address assignment pool of the DHCP server
- Enable/disable source NAT

Example: to assign the router an additional subnet mask:

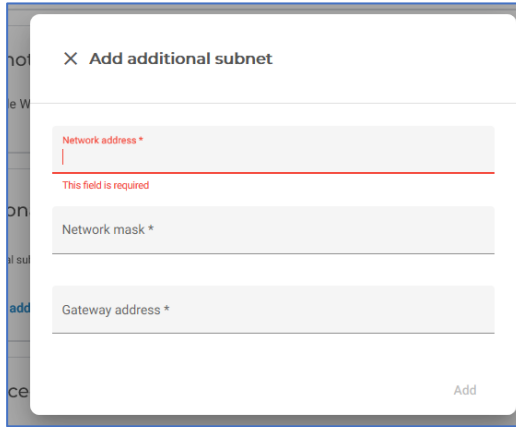
1. In the RAP's Fleet Manager select a RAR device. This opens the device configuration page (Screenshot 48).
2. In the RAR menu go to Network->LAN and from the screen on the right select "Add additional subnet" (Screenshot 49).
3. A new window pops-up (Screenshot 50) for the new Lan settings. Normally, the gateway is the LAN IP address of the RAR router. Enter the desired subnet settings and click "ADD".



Screenshot 48 Open the device configuration page.



Screenshot 49 Edit the LAN configuration.



Screenshot 50 LAN configuration settings

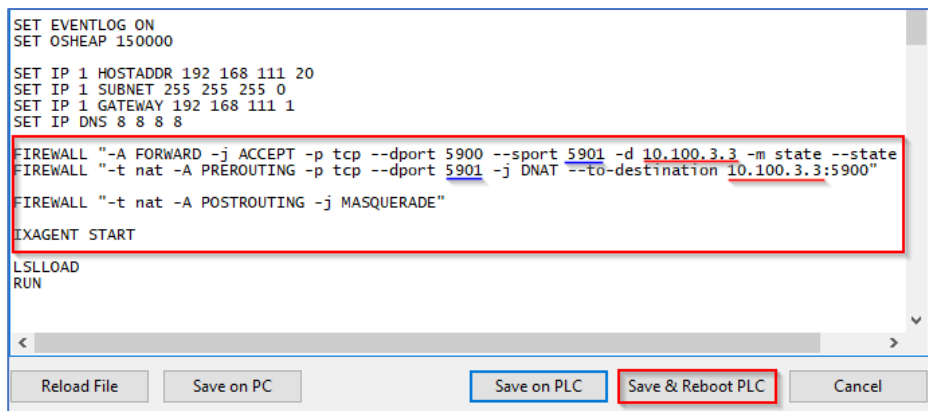
5.5 Additional Network Settings (RAE only)

In some configurations, remote access to controllers connected to the controller running RAE may be desired.

- For remote access, to the other control elements, port-forwarding must be configured via the firewall (Screenshot 51).
- Firewall is supported by Salamander OS 09.03.141 or higher. Firewall commands are described in the Lasal OS documentation.

1. Connection to the control via LASAL Class 2.
2. Open the Autoexec.lsl file with Class 2: DEBUG > FILE TRANSFER > EDIT AUTOEXEC.LSL... Add firewall commands to manage forwarding and NAT to connected devices.
 - a. Example: The control with the IP address 10.100.3.3 is connected with the control in which the RAE with the IP address 192.168.111.20 is running. The following lines must be added in order to forward a VNC connection:
 - i. FIREWALL “-A FORWARD -j ACCEPT -p tcp --dport 5900 --sport 5901 -d 10.100.3.3 -m 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 restart the control.



Screenshot 51 Autoexec with port-forwarding commands.

5.6 Configuring Remote Services

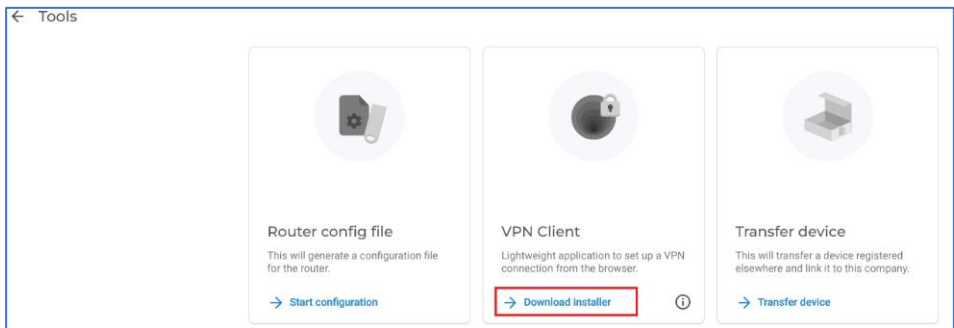
Before configuring remote services, the device must first be registered in the RAP.

5.6.1 Creating a VPN Connection

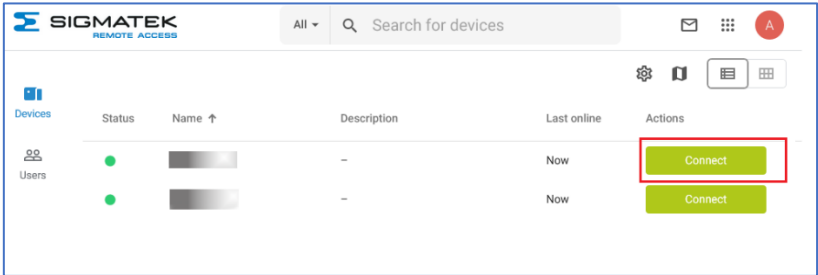
A VPN connection requires that the RAR/RAE powered and connected to the Internet. Available devices are identified in the RAP interface with a green dot next to their name.

To create a connection between the RAR/RAE and the current PC:

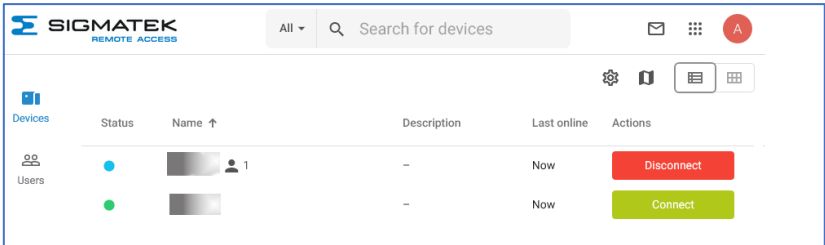
1. The VPN TUN adapter driver must be installed.
 - a. This can be downloaded via Fleet Manager → Tools → "VPN Client" (Screenshot 52).
 - b. Also via RAR configuration page under Network->VPN optional settings are available:
 - i. Client protocol mode
 - ii. Stealth mode: Support for restrictive networks. In addition to encryption, the data is made unrecognizable. Most firewalls are then unable to recognize the type of data traffic.
 - iii. Proxyserver
2. Select the RAR device from either the "Fleet Manager" page or the "Portal" main interface.
3. Click on "Connect" (Screenshot 53).
4. As soon as the device is connected, a blue status indicator lights (Screenshot 54).
5. Windows and software can now communicate via TCP/IP with devices, such as SIGMATEK controls that are connected to the RAR.



Screenshot 52 The cloud VPN can be downloaded from the RAP>Tools page.



Screenshot 53 Each device has a VPN connection button to establish secure communication.



Screenshot 54 After creating a VPN connection, the device status indicator lights blue.

5.6.2 VNC via VPN

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



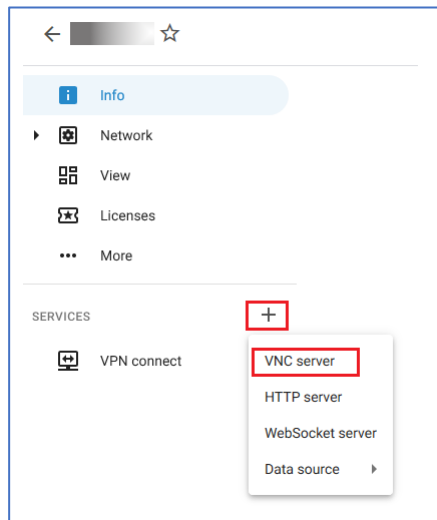
Activating the VNC service in a SIGMATEK control is described in the LASAL REMOTE SERVICES training manual.

As soon as the VNC is activated in the control, it should be tested over a local connection. If the ready status is confirmed, follow the instructions for activating the VNC Viewer Service in the Remote Access Platform.

5.6.2.1 VNC Configuration

- 1. From the APPs Menu → Fleet Manager and clicking the appropriate remote device
- 2. Click on the “+” button next “Services” (Screenshot 55).

3. Assign a name to the device service and specify the IP address of the destination (Screenshot 56). For the RAE, the IP address is automatically defined as “localhost”.
4. Change the connection as needed to adapt the actual configuration.
5. A new VNC service is now listed under the Services tab (Screenshot 57).
6. Complete the process:
 - a. RAR
 - i. Click ADD.
 - ii. Push config to Device for synchronization (Screenshot 58).
 - b. RAE: click on ADD; the change is immediately in effect.



Screenshot 55 Adding a new service to the device.

VNC server

Name *

HMI

IP address

192.168.111.20

Port *

5900

☒

 Requires a password

Password *



Access category *

Category A

☐

 Use read-only mode

Encoding

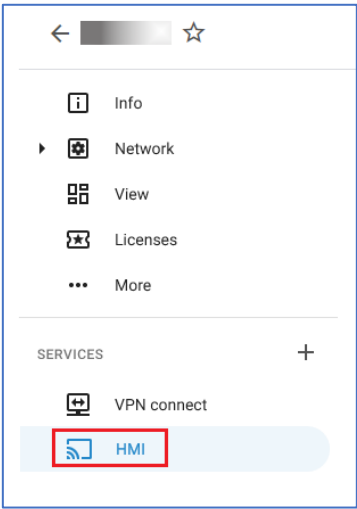
Automatically (recommended)

Color depth

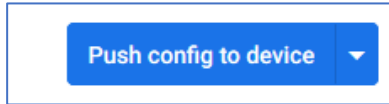
Automatically (recommended)

Add

Screenshot 56 Setting the service destination by IP address.



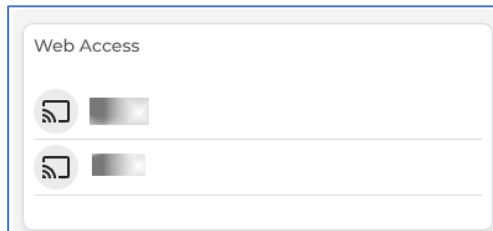
Screenshot 57 New VNC Service is listed



Screenshot 58 Push config to Device for synchronization.

5.6.2.2 Connecting with the VNC

1. Select your Device from the Device list on the Portal page.
2. Under Web Access select the desired VNC (Screenshot 59).
3. The viewer is opened in the same window. To return to the "Info" tab, click the "x" in the left corner (Screenshot 60).



Screenshot 59 select the desired VNC under Web Access



Screenshot 60 To end the VNC Viewer, click the "x".

5.7 Data collection and Storage

5.7.1 Configuring Data Sources

Each control configured on a remote device can have a data source. The supported protocols for SIGMATEK controls are OPC UA and Modbus TCP.

In the following sections, adding variables for both protocols are described.

5.7.1.1 OPC UA

To record or utilize control data, the control must first provide the data to the RAP.

- Contact your SIGMATEK representative to acquire the OPC UA and license.
- The configuration of OPC UA is described in the corresponding documentation.

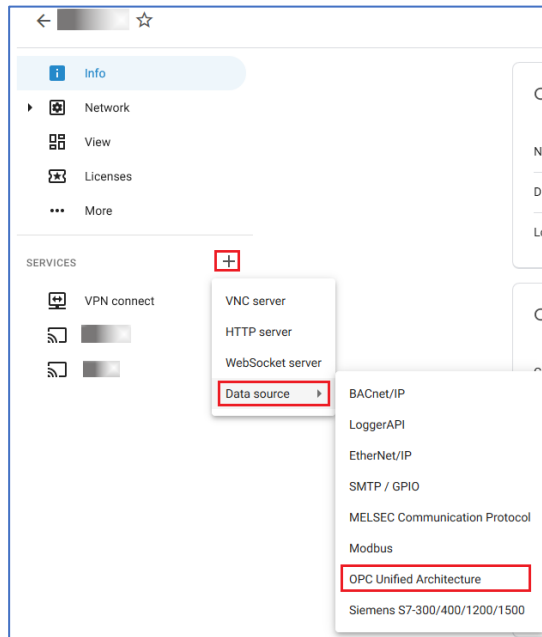
To provide an OPC UA data source for the RAP:

1. To create the data card, consider using a utility program such as UaExpert (Screenshot 66).
 - a. Add the server to use in Cloud Logging or Cloud Notify. The “Node ID” and data type are required.
2. On the RAP add a OPC UA DataSource Service (Screenshot 61).
 - a. “Fleet manager” -> select Device ->. Click the “+” button to add a new service .
 - b. Select Datasource and OPC UA Protocol.
 - c. Enter the target control that should provide the data source (Screenshot 62).
 - i. IP Address of Sigmatek control
 - ii. Define the server port. (e.g 4842)
 - iii. Click “ADD”.
 - d. The new OPC UA data source configuration menu is now listed under services and can be expanded (Screenshot 63).
3. Click on the “Add new variable” button to add a variable (Screenshot 64).
 - a. Assign a name to the variable, specify the data type and address of the variable (Screenshot 65). These values can be retrieved from the OPC UA card or suing such software as UA Expert (Screenshot 66). An example for the address can be found in Screenshot 67. A size and unit can also be used. Click on “ADD”.

- b. In the header of the configuration, click “Push Config to Device”.
- c. After the sync is complete, click “TESTRUN” to test the data server connection and the variable capture (Screenshot 68).



“Push Config to Device” and “Run Test” are only allowed after activating a licence. This is explained in section 5.7.2.



Screenshot 61 Add a new service to the remote device.

Data source

OPC Unified Architecture

Name *

Identifier *

CP112_opc

IP address

192.168.2.100

Port *

4842

Authentication type *

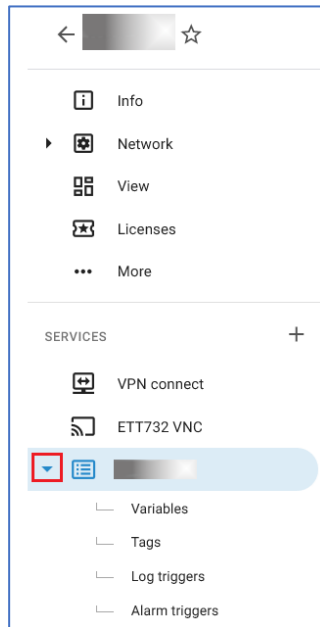
Anonymous

Polling sleep time

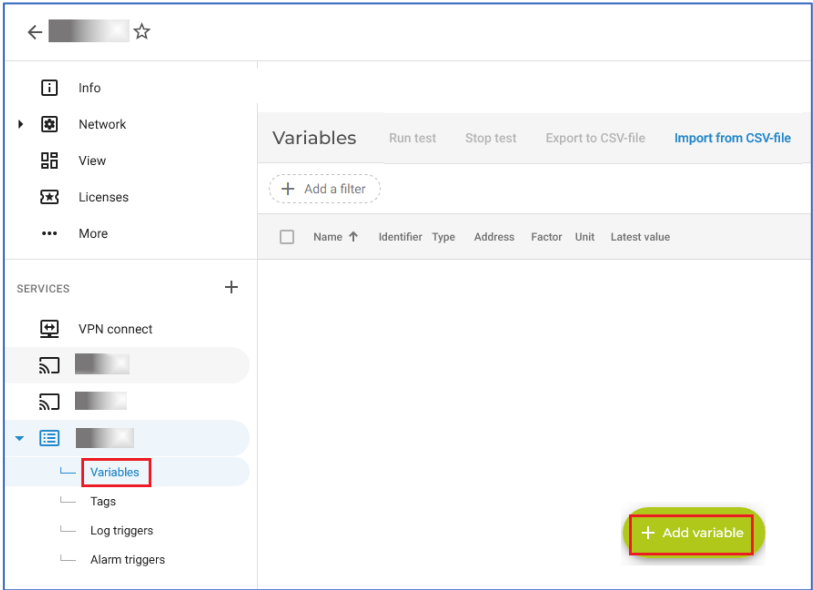
100 milliseconds (recommended)

Add

Screenshot 62 Enter the destination for the service.



Screenshot 63 New OPCUA data source is listed under services



Screenshot 64 Data source configuration menu allows to add variables

Edit variable

Name *

Identifier *

Note: name identifier

Type

Namespace *

Identifier type *

Identifier value *

Note: OPC-UA identifier

Factor

Unit

Remove

Cancel

Confirm

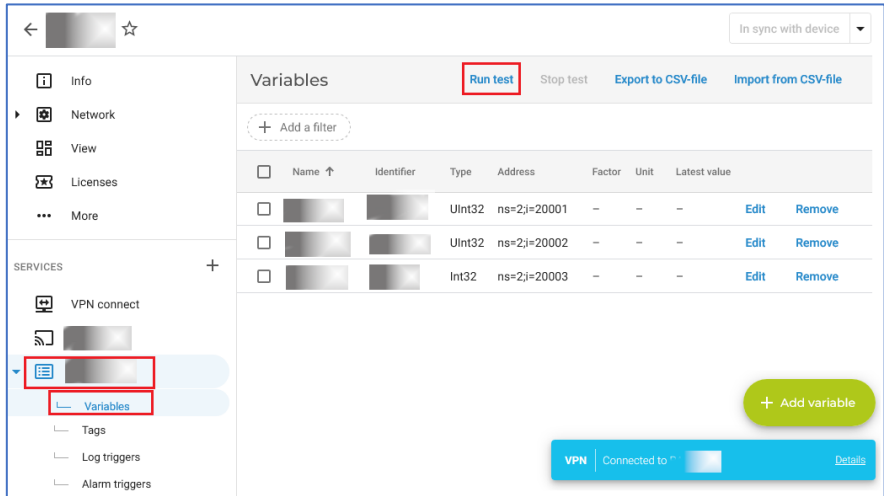
Screenshot 65 Specify the data type and address of the variable.

#	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

Screenshot 66 Locating the node ID and data type in 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

Screenshot 67 Example for creating the RAP variable identifiers.



Screenshot 68 “Run test” to test the data server connection and the variable capture.

5.7.1.2 Modbus TCP

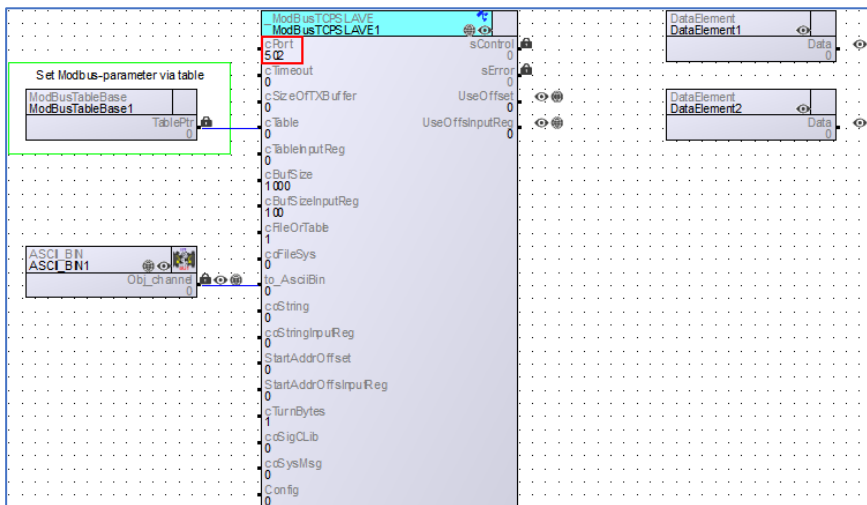
To record or utilize control data, the control must first provide the data to the RAP.

- More information on the Modbus slave can be found in the class documentation.

The Modbus slave must be added to the control defined as the data source:

1. Add the ModbusTCPSlave. Note the port number for the RAP configuration (Screenshot 69).
2. Configure the data sources in the ModbusTableBase class. The class assigns a server to a Modbus register (Screenshot 70).
3. On the RAP add a modbus DataSource Service (Screenshot 71).
4. When configuring the Modbus settings (Screenshot 72), the following must be noted:
 - a. Slave number = 1
 - b. Byte order = ABCD
5. “Push Config to Device” for Synchronization (Screenshot 73).
6. To add variables:

- a. Open Fleet Manager → Modbus DataSource → Variables → Click “+Add variable” (Screenshot 74).
 - b. Assign the name to the variable. Specify the data type and address of the variable (Screenshot 75). A size and unit can also be used. Click on “ADD”.
 - c. In the header of the configuration, click “Push Config to Device”.
7. After the sync is complete, click “TESTRUN” to test the data server connection and the variable capture.



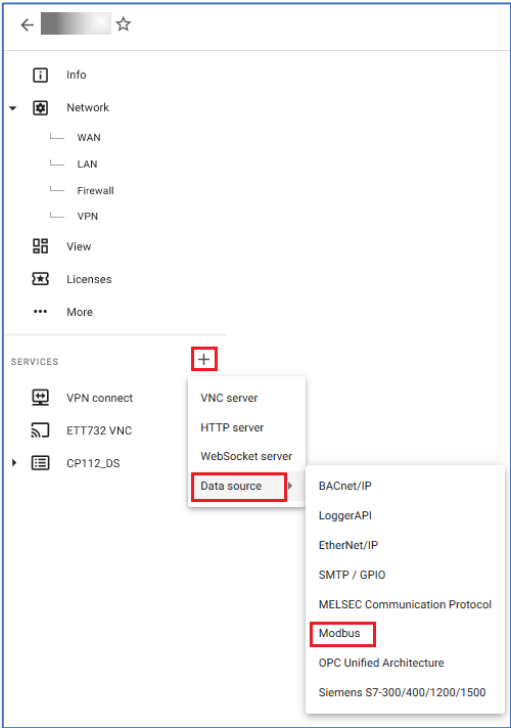
Screenshot 69 Overview of a ModbusTcpSlave network with example-data sources DataElement1.Data and DataElement2.Data.

```

FUNCTION TAB ModbusTableBase::Table
// Modbus-Adress, Register-Count, Access Restriction, "objectname.Servername",
100 $uint, 2 $uint, MODBUSTABLE_ACCESS_RW $uint, "DataElement1.Data",
200 $uint, 2 $uint, MODBUSTABLE_ACCESS_RW $uint, "DataElement2.Data",
END_FUNCTION

```

Screenshot 70 In ModbusTableBase::Table, the data sources of the DataElement objects are assigned to the Modbus registers.



Screenshot 71 Add a Datasource Modbus service

Data source
Modbus

Name *

Identifier *

IP address

Port *
502

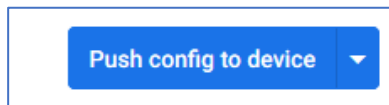
Slave
1

Byte order *
ABCD

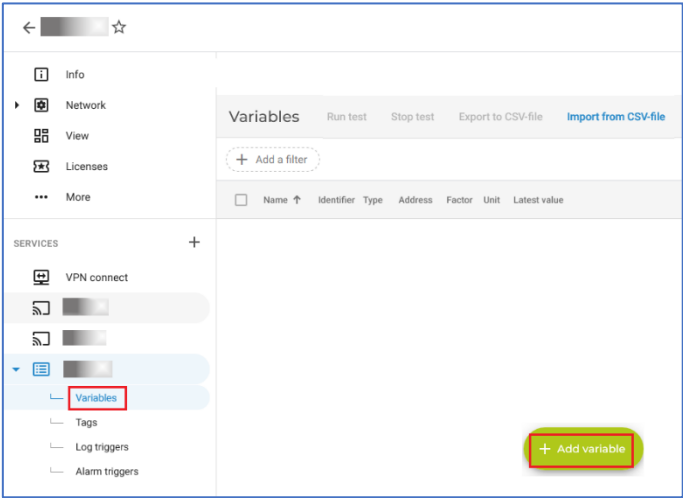
Polling sleep time
100 milliseconds (recommended)

Add

Screenshot 72 Configuration of the data source settings for the Modbus.



Screenshot 73 Push Config to Device for Synchronization.



Screenshot 74 Add a variable to the Modbus Datasource.

Add variable

Name *

DataElement1

Identifier *

data-element-1

Type *

Int32

Function code *

3 - Holding registers

Address *

100

Factor

1

Unit

Celsius

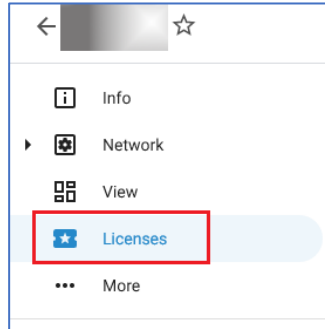
Cancel

Add

Screenshot 75 Configuring a ModBus variable.

5.7.2 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. For cloud logging, a license is required. Active licenses are displayed in Fleet Manager → Device page → Licenses (Screenshot 76).

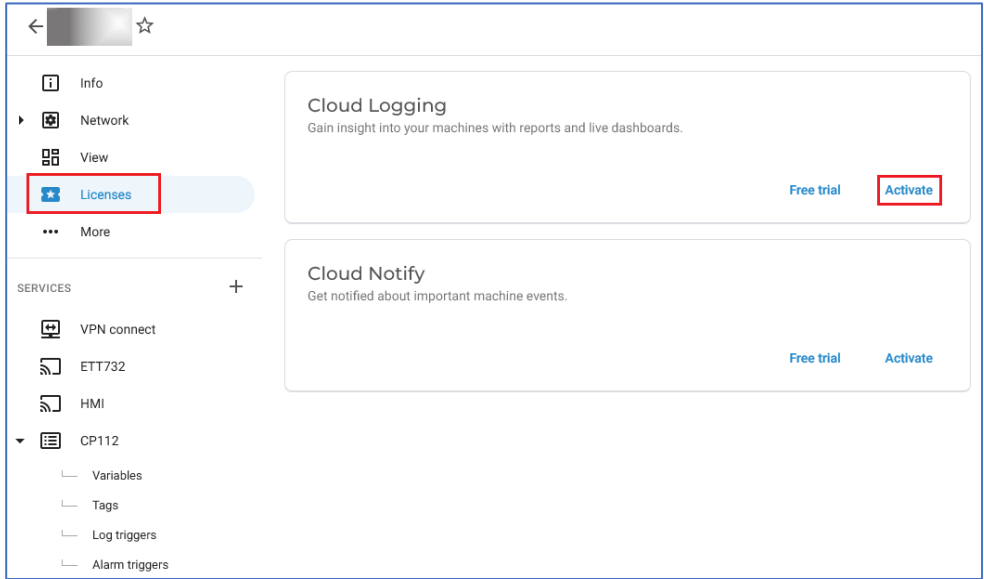


Screenshot 76 Licences for Cloud logging on Fleet Manager → Device Page.

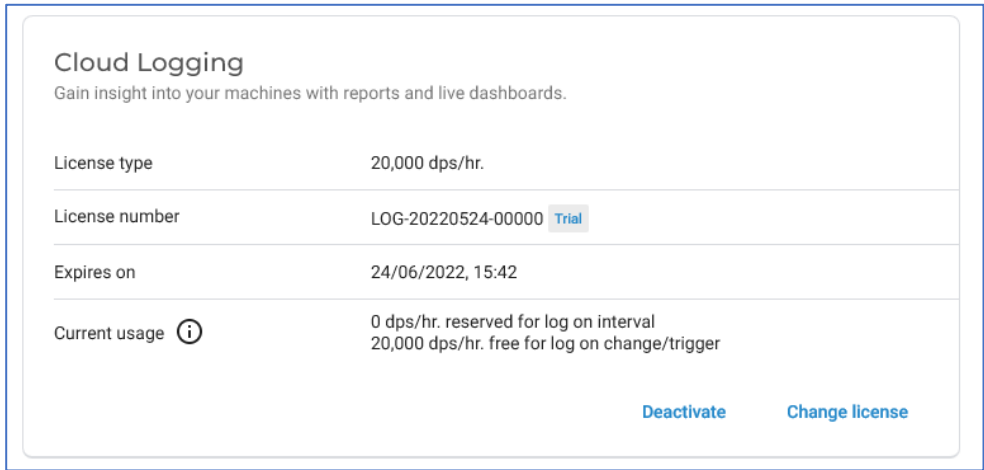
1. Acquire a license from your SIGMATEK representative.
2. Activate “Cloud Logging”.
3. Select the license (Screenshot 77).
4. New Active Licence is now displayed (Screenshot 78).



A 30-day Cloud Logging trial is an option and can be activated.
It can only be used for a single device in your company.



Screenshot 77 Active Licenses for the selected Device

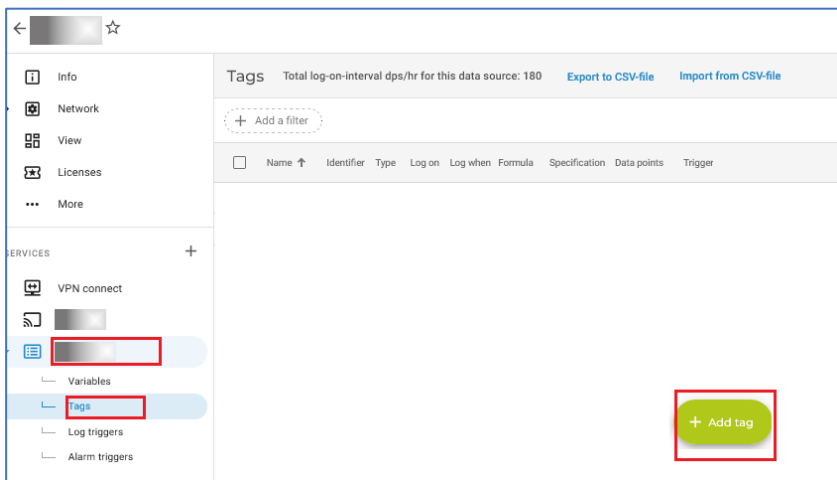


Screenshot 78 New Active Licence is now displayed.

5.7.2.1 Adding Data Sources to Cloud-Logging

Data tags describe how you wish to log your variables. You can choose to log them at a static interval (100ms - 1 hour), when their value changes, or on a custom trigger. Additionally, you define how long the data should be stored (retention policy).

1. After Cloud Logging activation, open tags from Fleet Manager → Device page → Data source menu → Tags. Click “Add Tag” (Screenshot 79).
2. In the tag editor fill-in the Data source input, logging interval selection and the data retention guidelines (Screenshot 80).
3. Click “Add”. The tags are then listed (Screenshot 81). Repeat the process for all required data sources.



Screenshot 79 Add Tags for Cloud Logging

Add tag

Variable *

Name *

Identifier *

Log on *
Interval

Interval *
Every minute

Formula

Retention policy *
5 years

Cancel

Add

Screenshot 80 Tag editor interface

Tags

Total log-on-interval dps/hr for this data source: 180

[Export to CSV-file](#)

[Import from CSV-file](#)

+ Add a filter

☐	Name ↑	Identifier	Type	Log on	Log when	Formula	Specification	Data points	Trigger
☐			UInt32	Interval	Every minute	LAST	-	60 dps/hr.	- Edit Remove
☐			Int32	Interval	Every 30 seconds	LAST	-	120 dps/hr.	- Edit Remove

+ Add tag

Screenshot 81 The available tags are listed.

5.7.3 Creating a page for Data Display

You can Create Your own custom device page in the Cloud studio to visualize your data. There are two ways to visualize your data: Through data reports that show historical data and through live monitoring that shows real-time machine data.

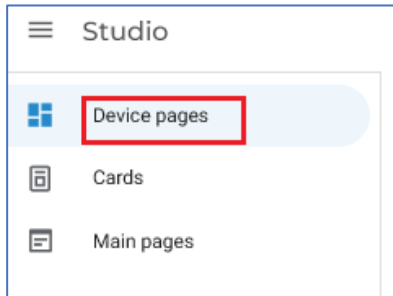


Historical and live display of data requires at least a pre-configured Data source service with variables for Live data and Tags for historical display, as configured in section 5.7.1 and section 5.7.2.

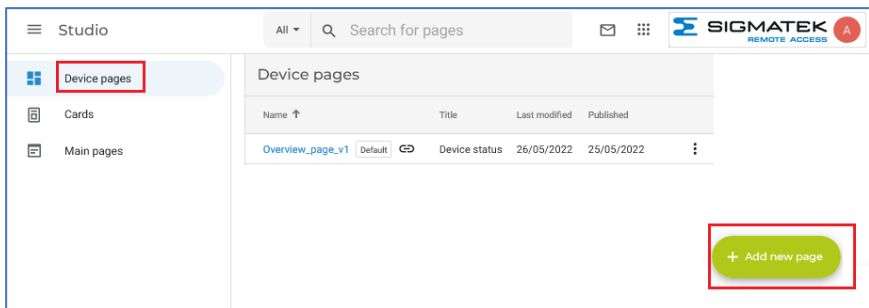
1. Open the Studio Menu from APPS Menu → Studio.
2. Open the Devices pages option (Screenshot 82).
3. Click the "+ Add new page" button to create a new device page (Screenshot 83). Enter Name and title for the page.
4. Open the newly created page or alternatively an already existing page can be open and edited (Screenshot 84).
5. Select device and component to be added (Screenshot 85).
 - a. There are eleven components for historical metrics
 - b. There are five components for Live Metrics
6. Examples (two live Metrics and two historical Metrics):
 - a. Live Value component: a Live data value display (Screenshot 86).
 - i. Add Live value component from the available list of components (Screenshot 87).
 - ii. Click on the newly added live value component and add component details: Title, Subtitle and click edit on Data source (Screenshot 88).
 - iii. Click the folder option on the Input screen (Screenshot 89).
 - iv. Select Data source and variable from the available lists previously configured in section 5.7.1 (Screenshot 90).
 - b. Live Gauge component: an analog display of Live data values (Screenshot 91).
 - i. Add Live gauge component from the available list of components (Screenshot 85).

- ii. Click on the newly added live gauge component and add component details: Title, Subtitle and click edit on Data source (Screenshot 88).
 - iii. Add Gauge range and click the folder option on the Input screen (Screenshot 92).
 - iv. Select Data source and variable from the previously configured Device data source service created in section 5.7.1 (Screenshot 90).
 - c. Line Graph component: displays trends in a data source (Screenshot 93).
 - i. Add Line Graph component from the available list of components (Screenshot 85).
 - ii. Click on the newly added line Graph component and add component details: Title, Subtitle, axis range and click Add Line (Screenshot 94).
 - iii. Add Line Details and Click on Tag (Screenshot 95).
 - iv. Select Data source and Tag from the previously configured Device data source service created in section 5.7.2.1 (Screenshot 96).
 - d. Period Bar Chart: Bar chart for data in a specific interval (Screenshot 97).
 - i. Add Period Bar Chart component from the available list of components (Screenshot 85).
 - ii. Click on the newly added Period Bar chart component and add component details: Title, Subtitle, Y-axis range, recording interval, bar style and click Add Bar (Screenshot 98).
 - iii. Add Line Details and add Tag (Screenshot 99).
 - iv. Select data source service and add Tag as configured in section 5.7.2.1 (Screenshot 96).
 - e. Layout example (Screenshot 100).
- 7. After the configuration is complete, the changes must be loaded into the device by clicking "Publish" tab. Discarding a draft is also possible by clicking the three dots and selecting "Revert to a Published version" (Screenshot 101).
- 8. To add a page to the device, go to Fleet Manager → Device → View → "Add page" (Screenshot 102).

9. Select page and Category and click add (Screenshot 103).
10. The new Page is now displayed online on Portal → Device. Navigation in-between pages is also allowed from the device page in Portal (Screenshot 104).



Screenshot 82 “Studio → Device pages” to create data reports and live monitoring for devices in the cloud.



Screenshot 83 Create a new page by clicking the “+” button.

All ▾

Search for pages

Device pages			
Name ↑	Title	Last modified	Published
Main Page Draft	Main Dashboard	26/05/2022	-
Overview_page_v1 Default GD	Device status	26/05/2022	25/05/2022

Screenshot 84 Select a page to add Data reports or Live Data

← Main Page

First Dashboard

Select device for preview ▾

+

Add a component ▾

Info

Cloud Connection St...

Device Info

Event Log

Remote Access

VPN Connect

Web Access

Historical Metrics

Data Export

Line Graph

Period Barchart

Statusbar

Data Table

Multiple Status

Single Value

Tank

Gauge

Multiple Values

Status

Live Metrics

Live Gauge

Live Multiple Values

Live Value

Live Line Graph

Live Status

Live Multiple Status

Live Tank

Layout

Image

Text Note

Screenshot 85 Data reports (historic) or Live Monitor can be added for a specific device

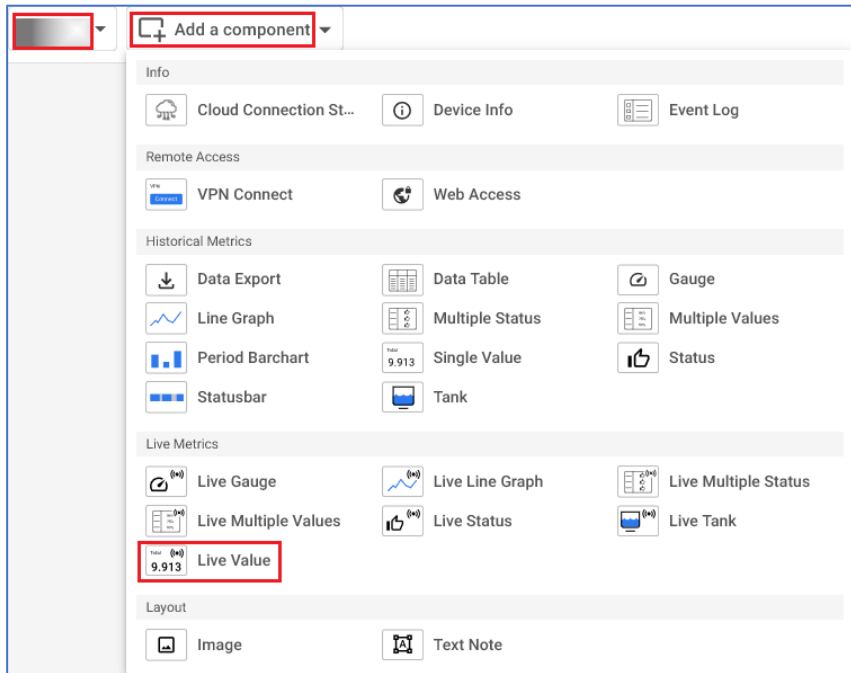
Page 66

07.08.2023

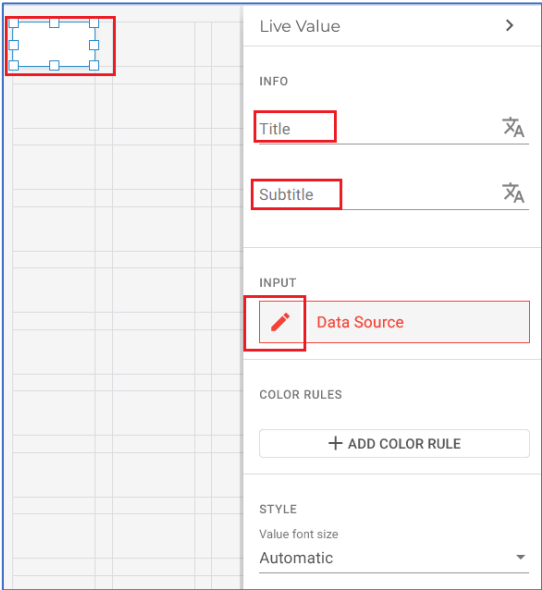
Counter

8,263,710

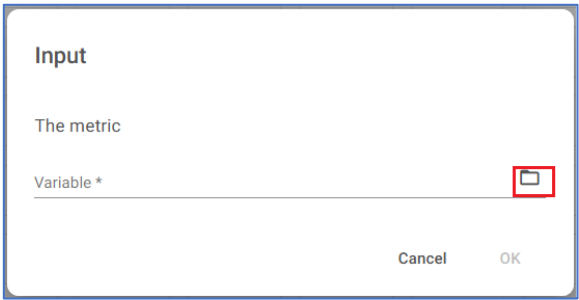
Screenshot 86 Live Value component example.



Screenshot 87 Add a component -> Live value



Screenshot 88 Add Live Value details



Screenshot 89 click the folder for editing Data Source

Data source *

Variable *

Cancel

Screenshot 90 Add data source and variable



Screenshot 91 Live Gauge component example.

Input

Metric

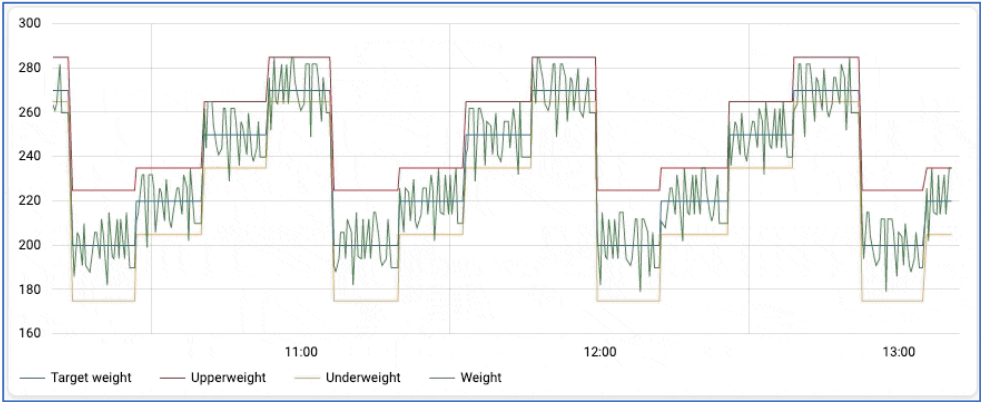
Variable

Min *

Max *

CancelOK

Screenshot 92 Add Live Gauge range values and data source variable



Screenshot 93 Line Graph component example.

Line Graph >

INFO

Title

✖A

Subtitle

✖A

LINES

+ ADD LINE

LEFT Y-AXIS

Min

⬆⬇⬆

Max

⬆⬇⬆

RIGHT Y-AXIS

Min

⬆⬇⬆

Max

⬆⬇⬆

REFERENCE LINES

+ ADD STATIC LINE

+ ADD DYNAMIC LINE

LEGEND

☐ Show legend

☒ Allow data export to CSV

Screenshot 94 Add Line Graph details, axis values and Add Line

Line

Name *

✖A

Color *



This field is required

Y-Axis *

Left

Metric

Tag *

Aggregator *

Type *

Line

Cancel

OK

Screenshot 95 Configure Line details and add Tag

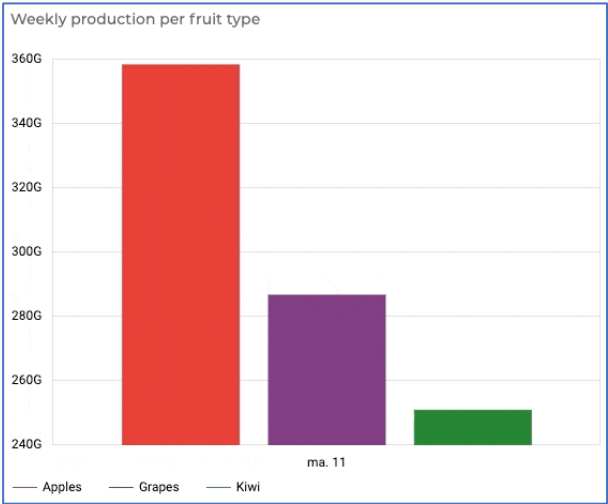
Data source *

Tag

Cancel

OK

Screenshot 96 Add data source and Tag



Screenshot 97 Period Bar Chart example

Period Barchart >

INFO

Title 

Subtitle 

BARS

+ ADD BAR

Interval 

STYLE

Bar style 

Y-AXIS

Min 

Max 

REFERENCE LINES

+ ADD STATIC LINE

+ ADD DYNAMIC LINE

LEGEND

☐ Show legend

☒ Allow data export to CSV

Screenshot 98 Period Bar Chart details

Bar

Name *

Color *

This field is required

Metric

Tag *

Aggregator *

Cancel

OK

Screenshot 99 Configure Bar details and add Tag

300

280

260

240

220

200

180

160

11:00

11:41:00

12:00

13:00

— Target weight

— Upperweight

— Underweight

— Weight

Upperweight

235 kg

Underweight

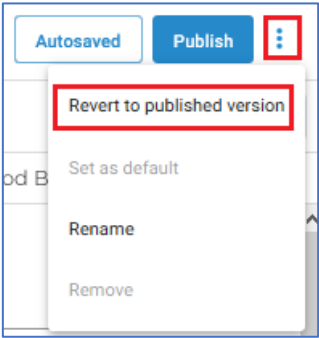
205 kg

Time	Recipe	Setpoint	Underweight	Weight	Upperweight
11-01-2021 13:40:07	4	220 kg	205 kg	235 kg	235 kg
11-01-2021 13:39:37	4	220 kg	205 kg	214 kg	235 kg
11-01-2021 13:39:07	4	220 kg	205 kg	232 kg	235 kg
11-01-2021 13:38:37	4	220 kg	205 kg	214 kg	235 kg
11-01-2021 13:38:07	4	220 kg	205 kg	232 kg	235 kg
11-01-2021 13:37:37	4	220 kg	205 kg	214 kg	235 kg
11-01-2021 13:37:07	4	220 kg	205 kg	215 kg	235 kg

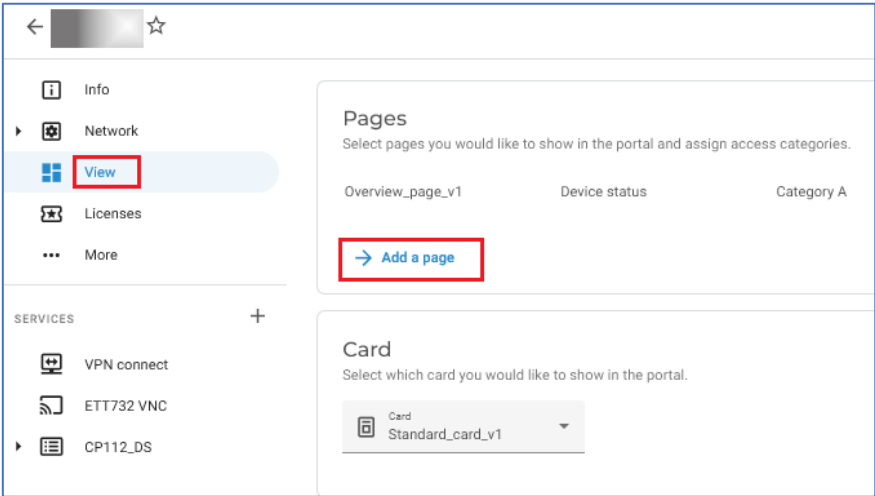
Screenshot 100 Monitoring page example with components line graph, value and data table

07.08.2023

Page 75



Screenshot 101 Revert to a published version is an option available



Screenshot 102 Fleet Manager → Device → View → “Add page” to add page to device.

X Add a page

Page *

Access category *
Category A

Cancel Add

Screenshot 103 Add Device Page

Device status
First Dashboard


SIGMATEK

Web Access
ETT732 VNC

Torque
100 150 200 250

Cloud connection status
Status Logbook VPN data usage
VPN connection AM08
Configuration connection AM04
Data logging connection AM04

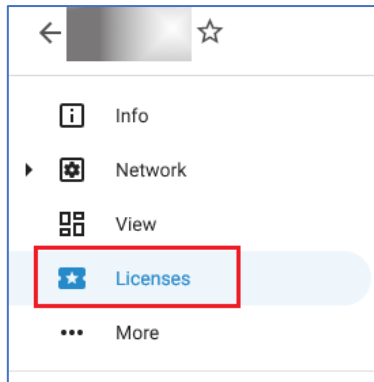
Cloud connection status
Status Logbook VPN data usage
VPN connection AM08
Configuration connection AM04

Screenshot 104 Navigation in-between pages is allowed from Portal->Device.

5.7.4 Cloud Notifications

The Cloud Notifications offers the possibility to record notifications about important machine events and to send them via e-mail.

For cloud notifications, a license is required. Active and available licenses are displayed in Apps menu → Fleet Manager → Device → Licenses (Screenshot 105).



Screenshot 105 Click Licenses for Device Licenses page.

5.7.4.1 Activating Cloud Notifications

1. Acquire a license from your SIGMATEK representative.
2. Activate Cloud Notify via Licenses (Screenshot 106).
3. Insert Activation code and click Activate (Screenshot 107).
4. Add Notification via Fleet Manager → Device → More(...) → Add notification (Screenshot 108).
5. Select the concerning connection, enter the alarms details and press Add (Screenshot 109).

Cloud Logging

Gain insight into your machines with reports and live dashboards.

License type	20,000 dps/hr.
License number	LOG-20220524-00000 Trial
Expires on	24/06/2022, 15:42
Current usage ⓘ	180 dps/hr. reserved for log on interval 19,820 dps/hr. free for log on change/trigger

Deactivate
Change license

Cloud Notify

Get notified about important machine events.

Free trial
Activate

Screenshot 106 Activate Cloud Notify via Licenses.

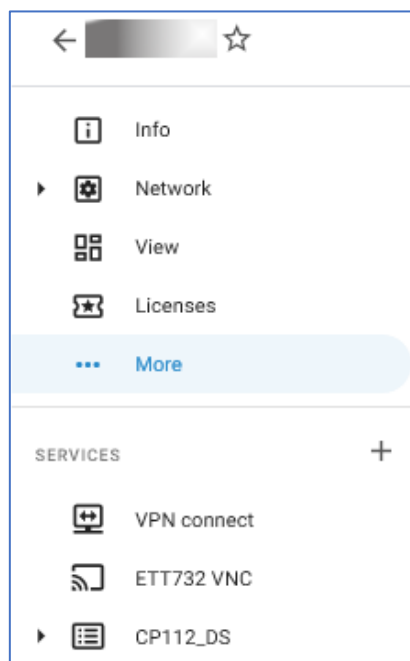
Activate Cloud Notify

Activation code *

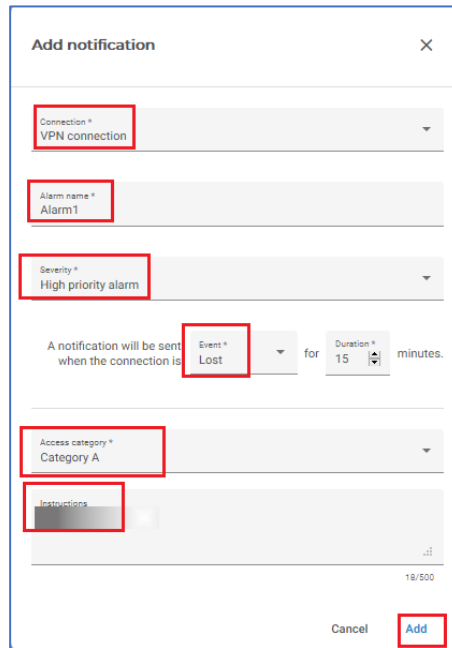
This field is required

Cancel
Activate

Screenshot 107 Insert Activation code and click Activate



Screenshot 108 Add Notification via Fleet Manager → Device → More (...) →
Add notification

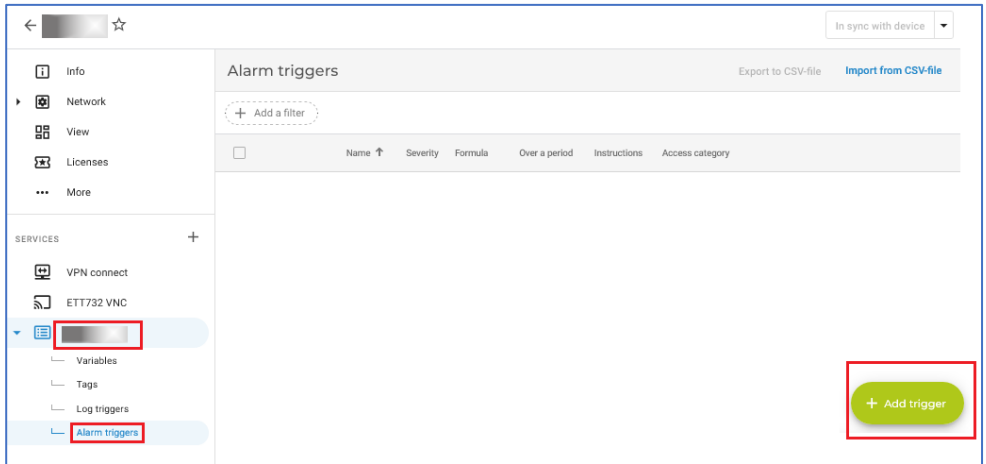


Screenshot 109 Fill-in notification details

5.7.4.2 Configuring Cloud Notifications

1. Setup Datasource service: see section 5.7.1.
2. Configure alarms:
 - a. In Fleet Manager → Select device → Data Service → Alarm triggers → Add trigger (Screenshot 110).
 - b. Set the source and parameters for the Alarm trigger and click add (Screenshot 111);
 - i. Name
 - ii. Severity
 - iii. Condition
 - iv. Threshold or variable
 - v. Period
 - vi. Instructions
 - vii. Access Category

- c. The New Alarm trigger is displayed in Fleet Manager → Select device → Data Service → Alarm triggers. Click “Push config to device” (Screenshot 112).
3. Configuring receivers from the alarms (Screenshot 113):
 - a. The receivers must be registered as device users.
 - b. From the Apps menu → Admin → roles → click add category access.



Screenshot 110 Adding a trigger via the Data source menu.

Add trigger

Variable *

Name *

Severity *

High priority alarm

Condition *

Greater than

Threshold type *

Variable

Variable *

Over a period

10

Milliseconds

Instructions

Access category *

Category A

Cancel

Add

Screenshot 111 Setting the source and parameters for the Alarm trigger.

Push config to device

Alarm triggers

Export to CSV-file

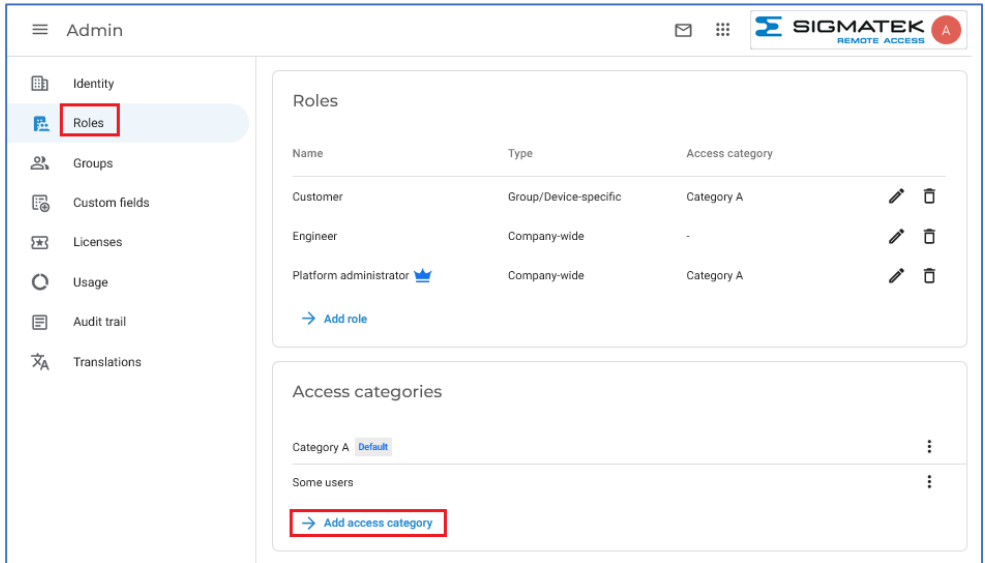
Import from CSV-file

+ Add a filter

☐	Name ↑	Severity	Formula	Over a period	Instructions	Access category	
☐		High priority alarm		10 milliseconds		Category A	Edit Remove

+ Add trigger

Screenshot 112 "Push Config to device" to sync with device



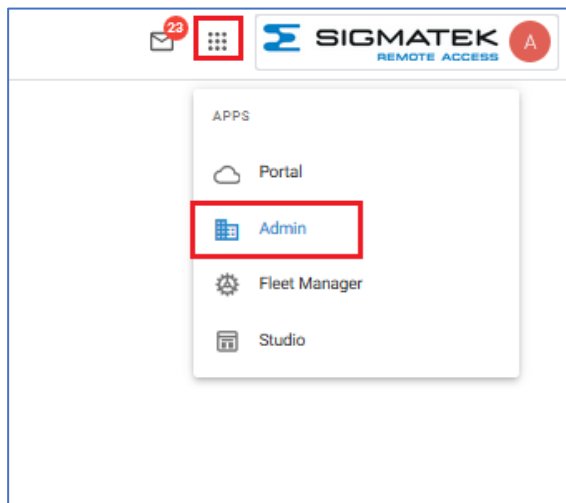
Screenshot 113 Edit users Access category for receiving notifications for specific alarms

5.8 User Administration

Under Admin via APP menu → Admin (Screenshot 114) users and its device permissions can be managed. The core components of managing users are Roles, access categories and groups:

- Roles – is a selection of admin or device permissions the user will have on the RAP cloud. They are of two types:
 - A “Company-wide role” allows to select a wider range of admin options for this user.
 - A “Group/Device specific” limits the user to group specific or device specific permissions.
 - Adding a new Role is via Admin page and clicking Roles→ Add Role (Screenshot 115).
 - Edit permissions and click add (Screenshot 116).
 - Default Roles Customer, Engineer and Platform Administrator are available and can also be edited.

- Access categories – are a selection of pages and services.
 - The diagram in the Screenshot 117 below shows how access categories work. An access category is added when a specific service is configured as previously configured in sections 5.6.2.1, 5.7.3, 5.7.4.2 for a VNC server, a device page and cloud notifications respectively.
 - A new access category can be created via the Admin page, Roles → Add access category (Screenshot 118).
 - Add a name to the new access category (Screenshot 119).
- Groups - Selection of devices and users.
 - A group is assigned to users that are not assigned a “Company wide role”.
 - Groups can be organized in listings of group types for a more structured approach, if many groups exist (e.g. Customer, machine type, region).
 - To make a device visible for users that are not assigned a “Company wide role add the device to a group via Fleet manager → Select Device to edit → info → Groups → edit (Screenshot 120).
 - Creating a new Group is via the Admin page and Groups → Select Group type → “+ Add new group” (Screenshot 121).



Screenshot 114 APP menu → Admin for managing permissions

Admin

Identity

Roles

Groups

Custom fields

Licenses

Usage

Audit trail

Translations

Roles

Name	Type	Access category		
Customer	Group/Device-specific	Category A		
Engineer	Company-wide	-		
New Role	Group/Device-specific	Category C		
Platform administrator	Company-wide	Category A		

→ Add role

Access categories

Category A

Default

Category B

Category C

Some users

→ Add access category

Screenshot 115 Adding a new role via the Admin page

Add new role

Name*
New Role

☒ Company-wide role
User has access to all devices, groups and templates

☐ Group-specific or Device-specific role
User has limited access, only to a specific group or a specific device

ADMIN

Configure company identity

View audit trail

View licenses

Manage roles, access categories, group types and custom fields

Manage groups

Manage pages and cards

Manage users ⓘ

DEVICES

Manage devices

Manage device templates

Services, pages and notifications linked to - Category A

Services, pages and notifications linked to - Category B

Services, pages and notifications linked to - Category C

Services, pages and notifications linked to - Category D

Services, pages and notifications linked to - Some users

NOTIFICATIONS

Expiring licenses

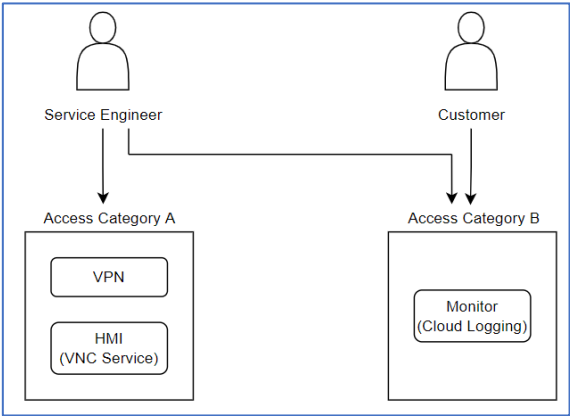
LOG IN

Enforce two-factor authentication ⓘ

Cancel

Add

Screenshot 116 Editing permissions



Screenshot 117 Access Category diagram

Admin

Identity

Roles

Groups

Custom fields

Licenses

Usage

Audit trail

Translations

Roles

Name	Type	Access category	
Customer	Group/Device-specific	Category A	 
Engineer	Company-wide	-	 
New Role	Group/Device-specific	Category C	 
Platform administrator 	Company-wide	Category A	 

→ Add role

Access categories

Category A Default

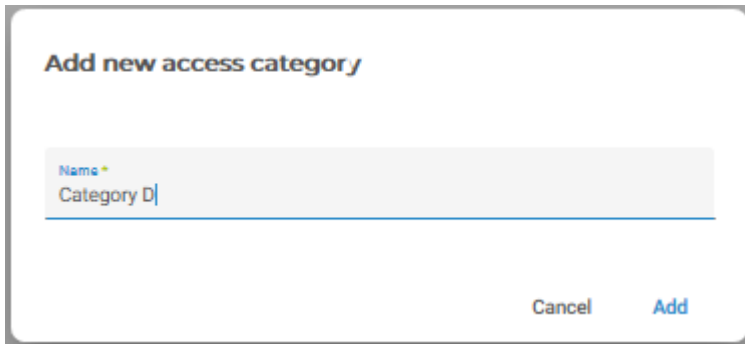
Category B

Category C

Some users

→ Add access category

Screenshot 118 Adding a new access category



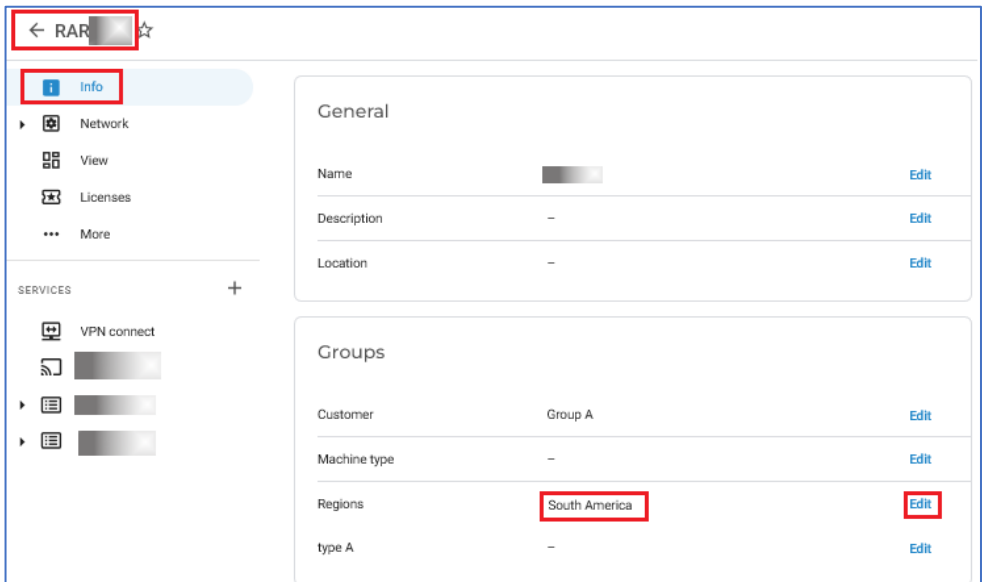
Add new access category

Name *

Category D

Cancel Add

Screenshot 119 Adding a name to the new access category



← RAR [Device Icon] ☆

Info

- Network
- View
- Licenses
- More

SERVICES +

- VPN connect
- [Service Icon]
- [Service Icon]
- [Service Icon]

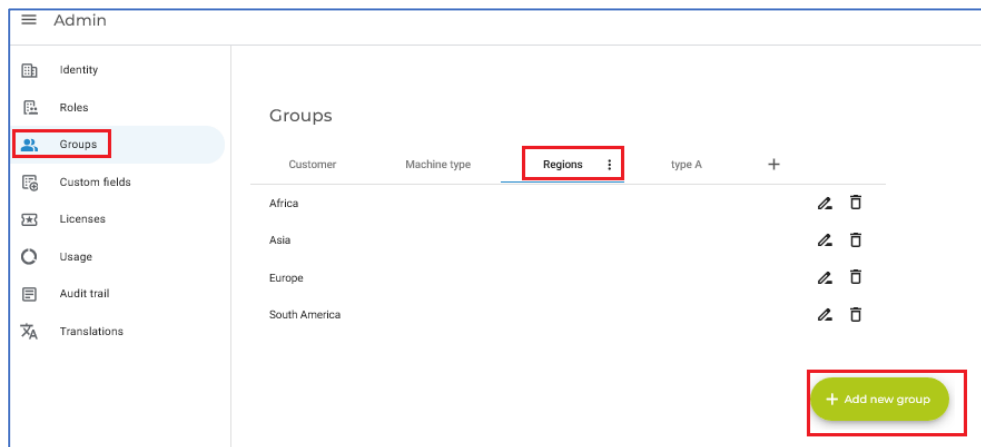
General

Name	[Redacted]	Edit
Description	–	Edit
Location	–	Edit

Groups

Customer	Group A	Edit
Machine type	–	Edit
Regions	South America	Edit
type A	–	Edit

Screenshot 120 Adding RAR Device to group “South America” from Group type “Regions”



Screenshot 121 Adding a new group to group type “Regions”

5.8.1 Adding a new user

A new User can be assigned different roles with the RAP. A complete list of all the users for a company can be accessed via the Portal page from APPS menu → Portal → select Users (Screenshot 122).

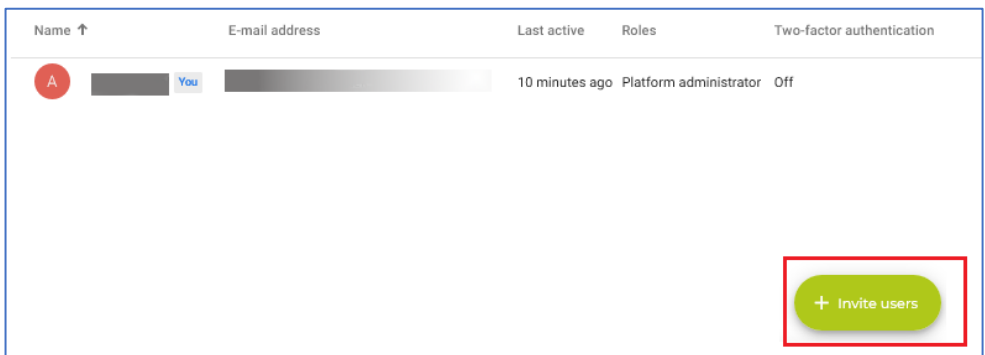
- Add a new User:
 - Click the “+ invite users” icon at APPS menu → Portal → select Users (Screenshot 122)
 - Fill-in the details including the new user’s email and Access level (Screenshot 124).
 - Access Level – You must choose whether you want the role to be applicable to all devices and users in your company, to a group of devices and users or only to one device.
 - Role – Each role is a combination of permissions and thus determines what a user can and cannot do. Roles can be managed via Apps Menu → Admin → roles.
 - Group/device – The user will have access to all devices in this group and the selected roles is limited to this group. With device-specific access, you can select one device to which you can gain

access. Roles can be managed via Apps Menu → Admin → Roles.

- Pending invites are shown with a blue icon (Screenshot 125).
- The invited user receives an e-mail with a registration link.



Screenshot 122 Access to list of users is via the Portal Menu



Screenshot 123 Invite new users via the Portal menu → users.

Invite users

Add more e-mail addresses...

Invitation message

Access level

Company-wide

Group-specific

Device-specific

Device

Role *

Customer

Temporary access

By inviting the user(s) to the group(s) they will get access to the following 1 device(s):

RAR Ken

Cancel

Send invite

Screenshot 124 Fill-in the details for the new user’s email and Access level.

Name ↑	E-mail address	Last active	Roles	Two-factor authentication
 Invited user Expires in 14 days		—	Customer at	—
 You		2 hours ago	Platform administrator	Off

Screenshot 125 pending invites are shown in blue.

6 Example Solutions

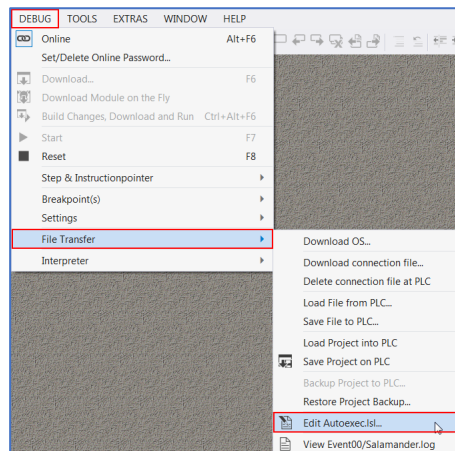
In this section, several universal remote-access configurations are presented.

- Using an example, a step-by-step guide is provided for the first solution.
- For all solutions, a diagram is used provide a series of suggested configurations to illustrate the required connections and interface settings.

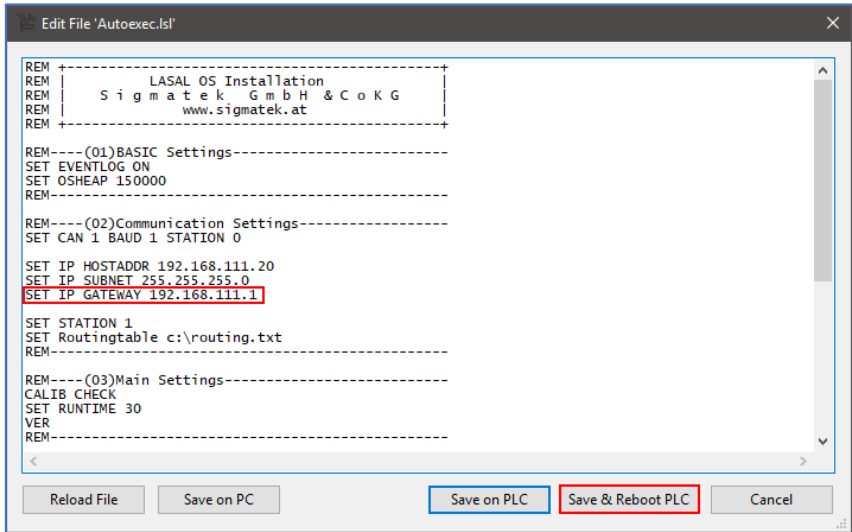
6.1 Solutions Based on the Remote Access Router (RAR)

Set-up example based on example 1:

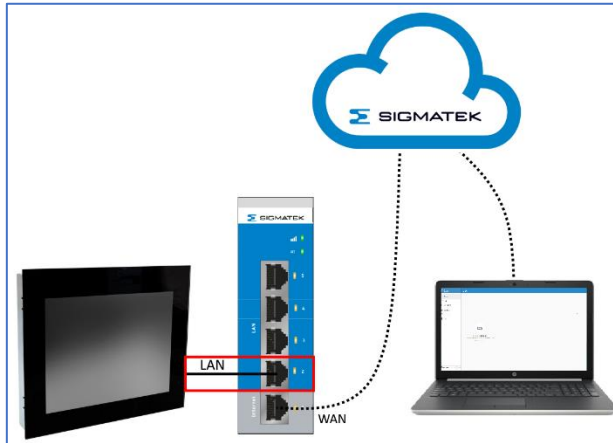
1. Open LASAL CLASS 2 and create an online connection to the HMI.
2. To access the HMI via the RAR, the default gateway must be changed to the IP address of the RAR (Screenshot 126).
 - a. Open the editor Autoexec.IsI via Debug > File Transfer > Edit Autoexec.IsI (Screenshot 126).
 - b. Set the gateway to the router IP address (Screenshot 127). This is located via the RAP Fleet Manager menu → Devices → Network → Lan → Router Lan IP.
 - c. Restart the control to enable the new IP configuration.
3. Connect the HMI to the RAR using an Ethernet cable (Screenshot 128).



Screenshot 126 Opening the editor Autoexec.IsI from LASAL CLASS 2.

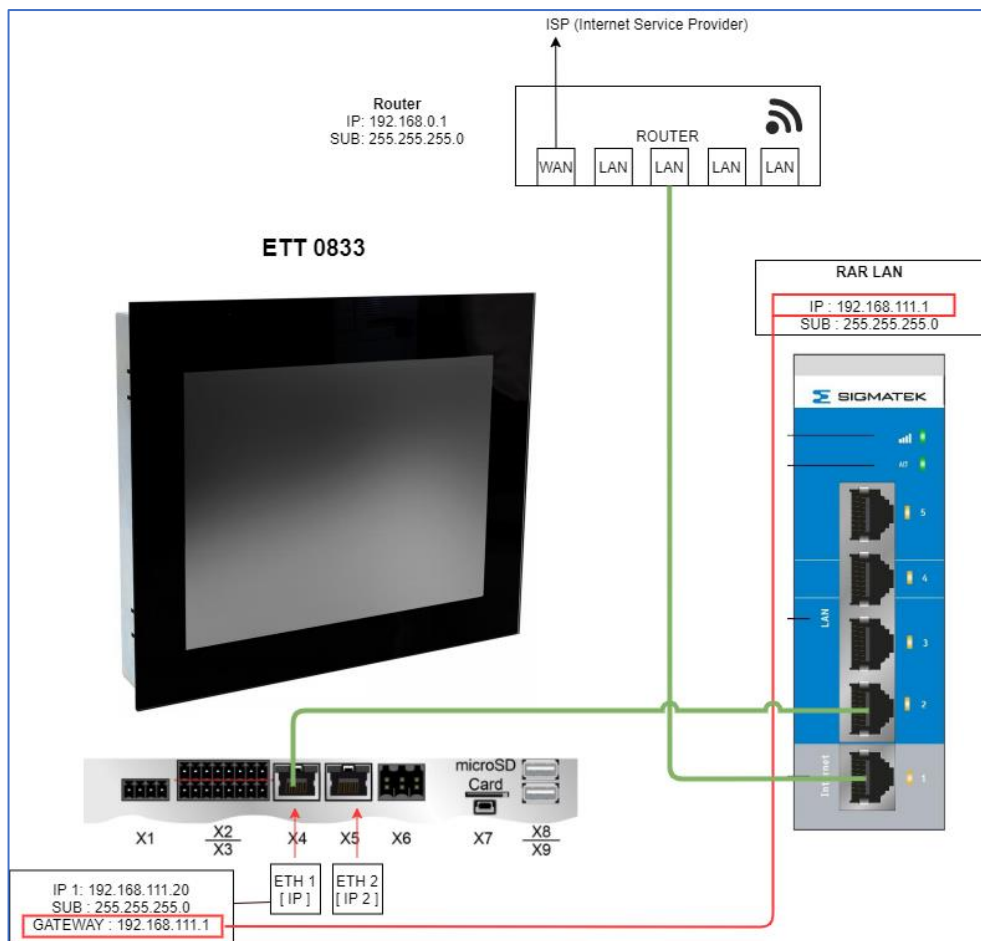


Screenshot 127 Entering the IP gateway into the Autoexec.lsl.

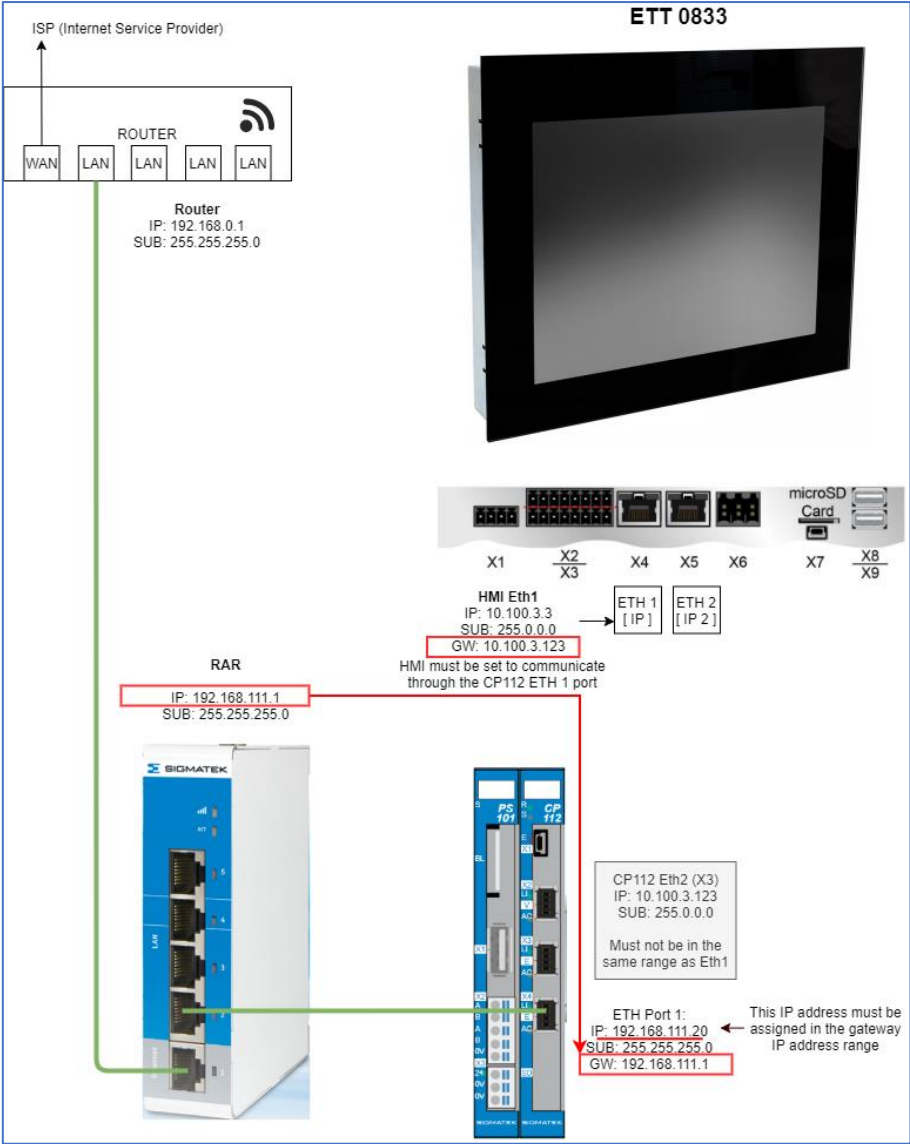


Screenshot 128 The HMI connected to the RAR can be accessed via the RAP.

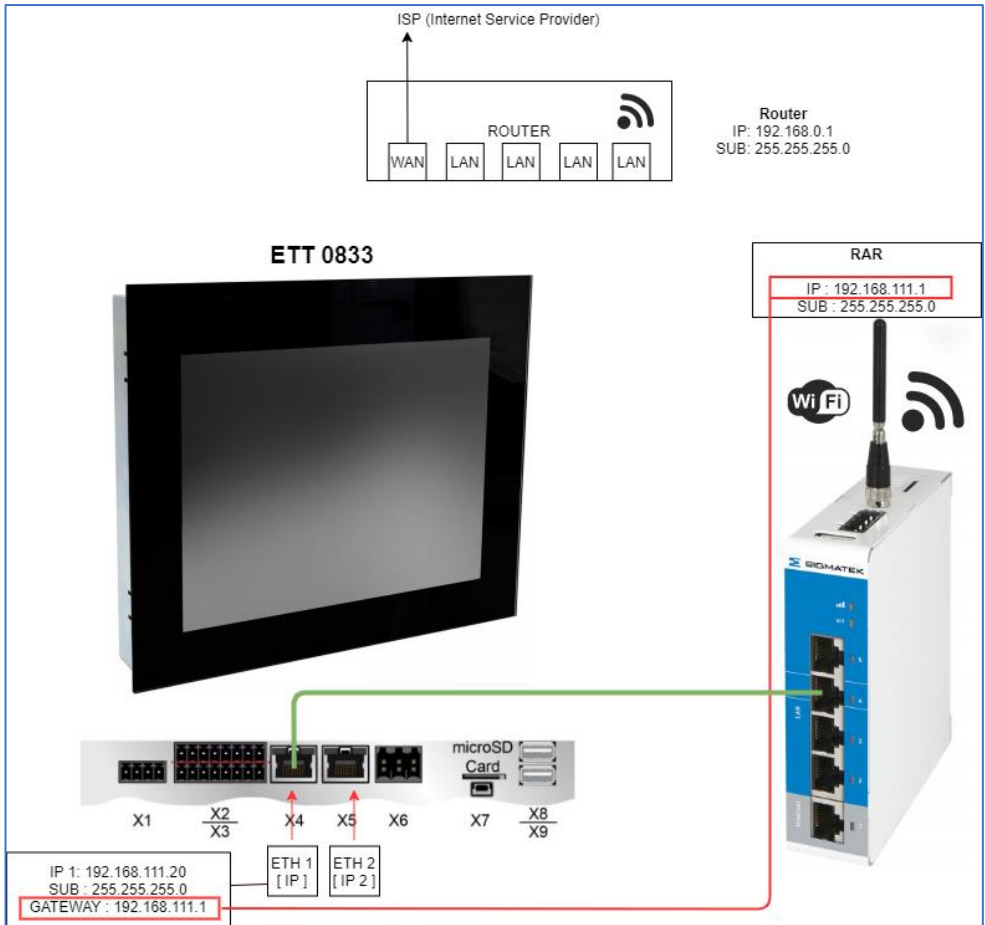
6.1.1 Example 1: RAR Wired, One-CPU Solution



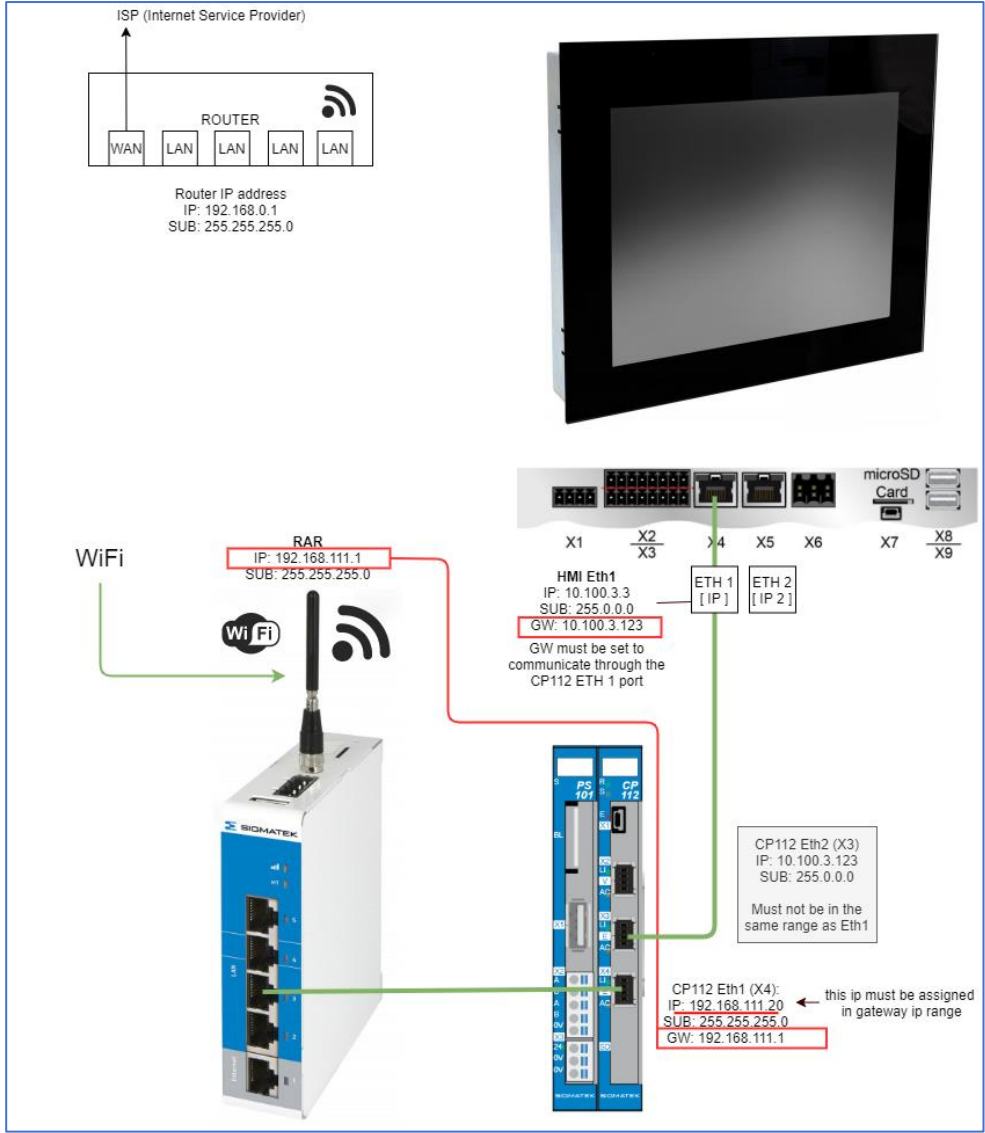
6.1.2 Example 2: RAR Wired, Two-CPU Solution



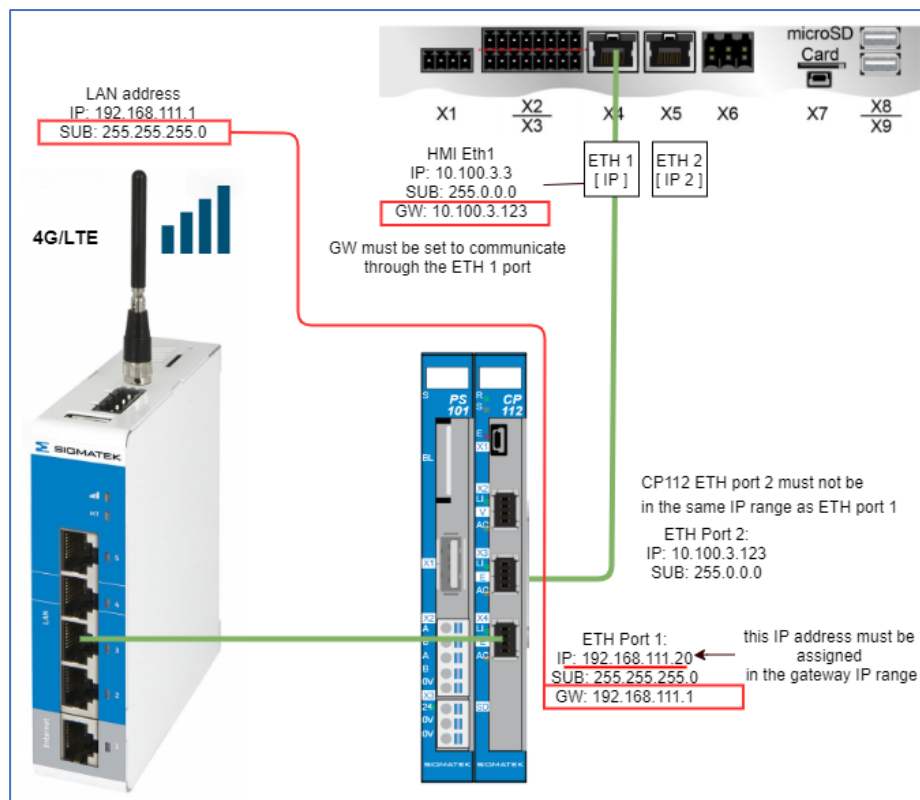
6.1.3 Example 3: RAR + WIFI, One-CPU Solution



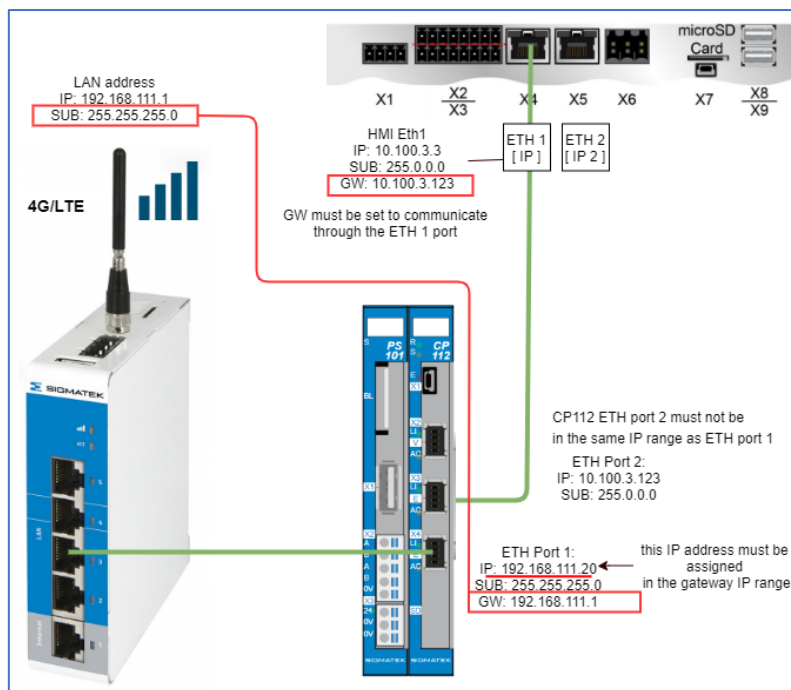
6.1.4 Example 4 RAR + WIFI, Two-CPU Solution



6.1.5 Example 5: RAR + Mobile Network, One-CPU solution

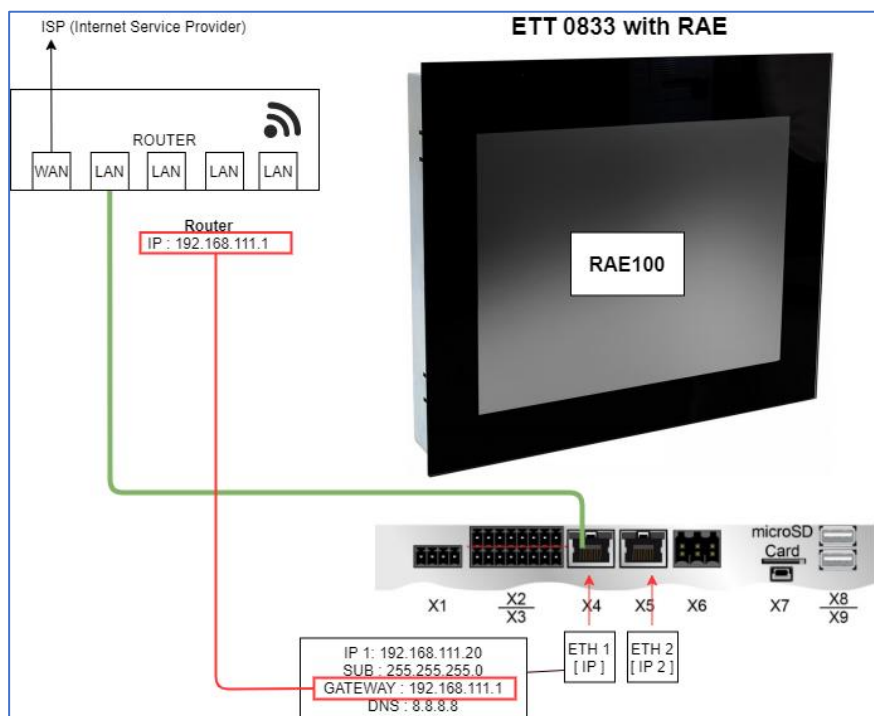


6.1.6 Example 6: RAR + Mobile Network, Two-CPU Solution



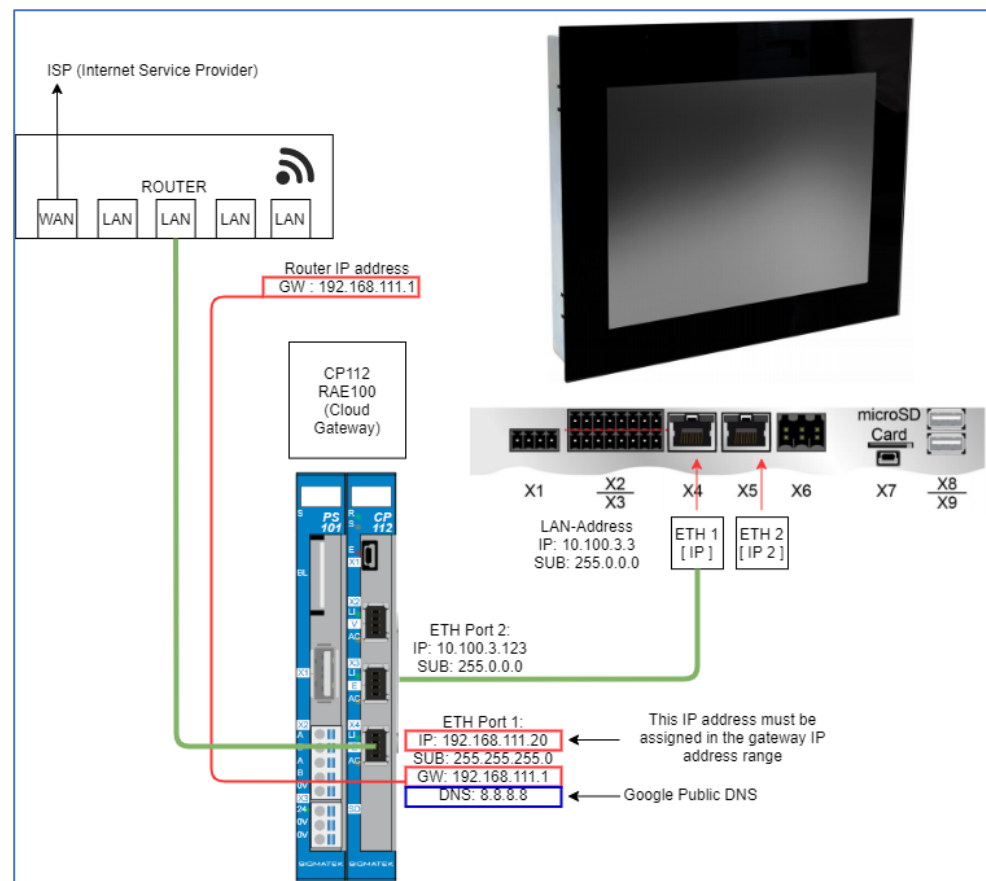
6.2 Embedded Remote Access Solutions (RAE)

6.2.1 Example 7: RAE100 One-CPU Solution

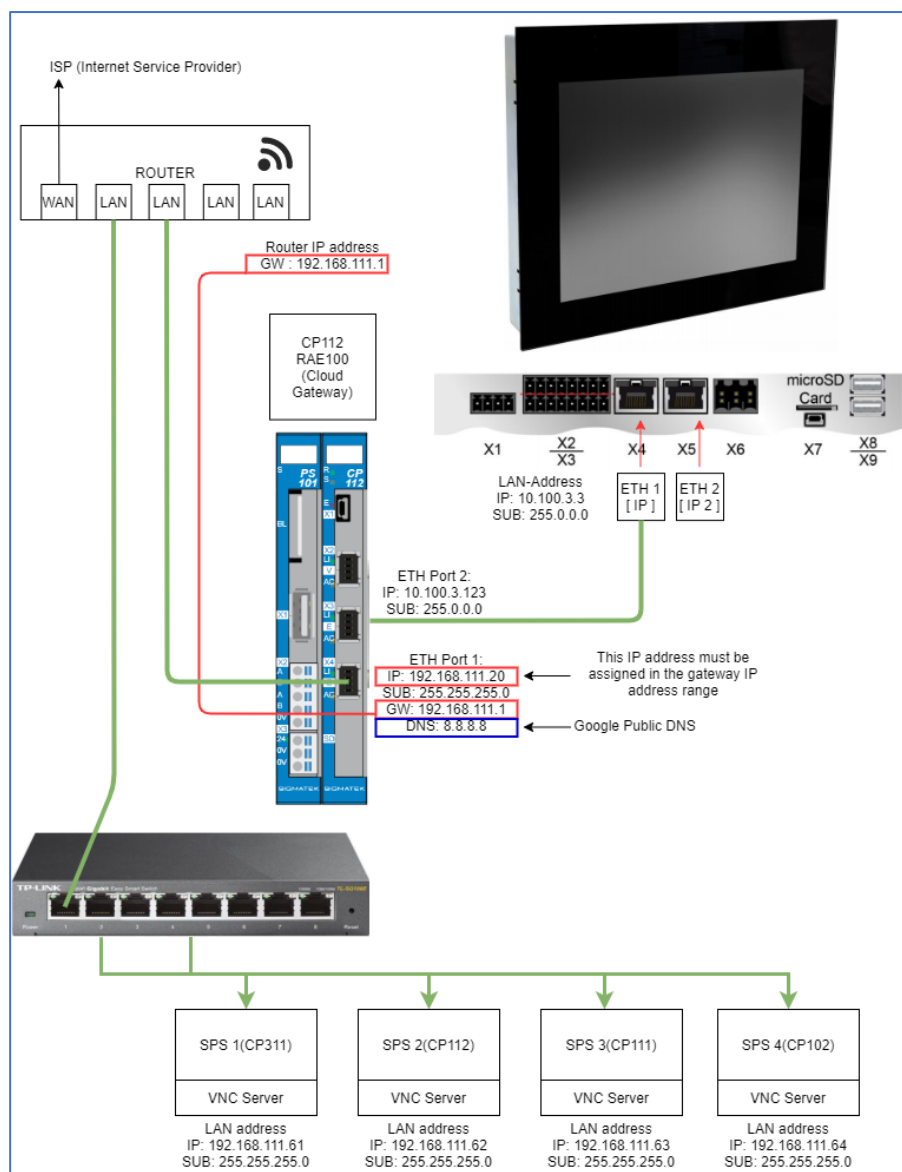


6.2.2 Example 8: RAE100 Two-CPU Solution

To enable this solution, an additional port forwarding configuration is required on the controller running RAE. See section 5.5.



6.2.3 Example 9: RAE100 as a Gateway



Example Autoexec.lsl

```
REM Ethernet interface
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 for access to the Cpxxx VNC from the 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"
```

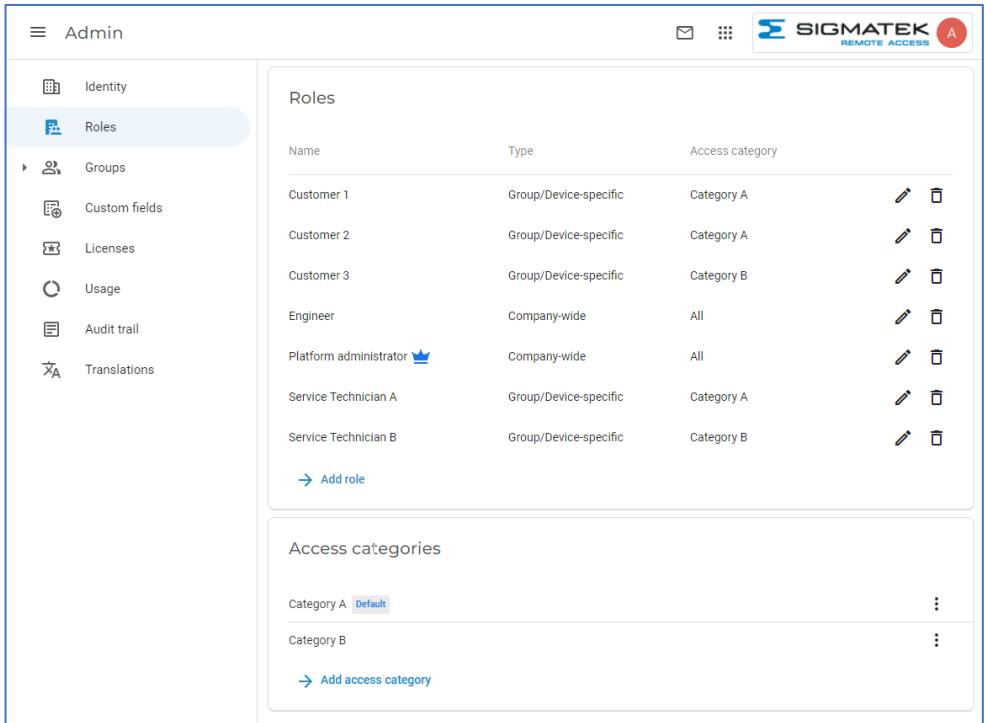
```
IXAGENT START
```

```
LSLLOAD
RUN
```

6.3 User Administration

6.3.1 Example 10: Remote Access Service

Customers are assigned to a category to facilitate maintenance by service technicians. It also ensures that customers can only access the cloud logging service. The service technicians can additionally access VPN and HMI.



The screenshot shows the 'Admin' interface of the Sigmatek Remote Access system. The left sidebar contains a menu with options: Identity, Roles (selected), Groups, Custom fields, Licenses, Usage, Audit trail, and Translations. The main content area is titled 'Roles' and displays a table of roles with columns for Name, Type, and Access category. Below the table is an 'Add role' button. Underneath the roles section is the 'Access categories' section, which lists 'Category A' (marked as Default) and 'Category B', each with a vertical ellipsis menu icon and an 'Add access category' button at the bottom.

Name	Type	Access category	
Customer 1	Group/Device-specific	Category A	
Customer 2	Group/Device-specific	Category A	
Customer 3	Group/Device-specific	Category B	
Engineer	Company-wide	All	
Platform administrator	Company-wide	All	
Service Technician A	Group/Device-specific	Category A	
Service Technician B	Group/Device-specific	Category B	

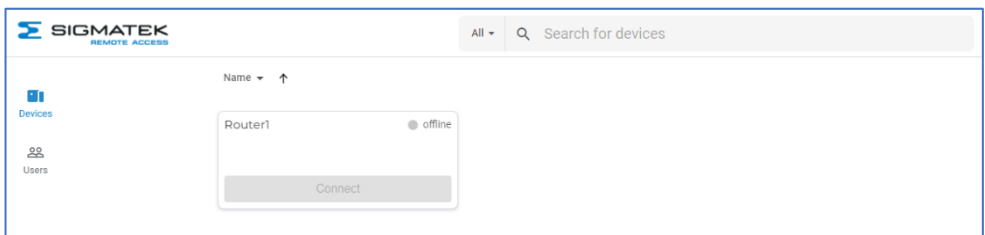
[Add role](#)

Access categories

Category A Default	
Category B	

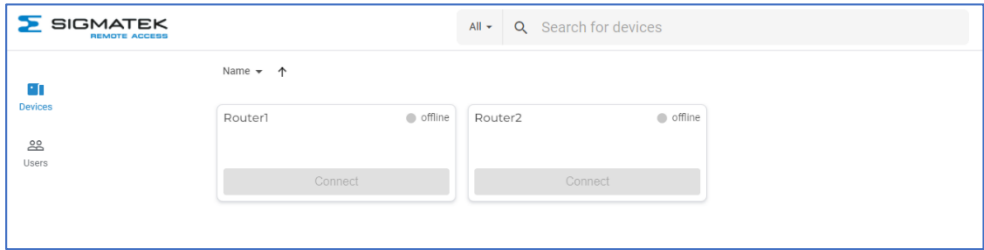
[Add access category](#)

Screenshot 126 User administration menu

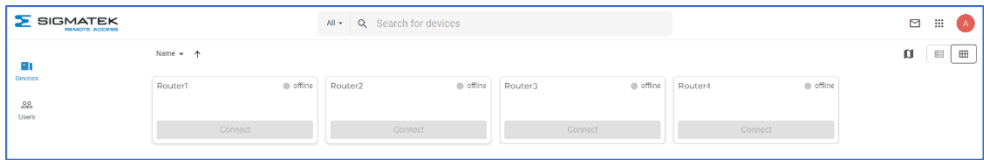


The screenshot shows the Sigmatek Remote Access interface from a customer's perspective. The top bar includes the Sigmatek logo, a filter dropdown set to 'All', and a search bar labeled 'Search for devices'. The left sidebar has 'Devices' (selected) and 'Users'. The main content area displays a single device card for 'Router1', which is marked as 'offline'. Below the device name is a 'Connect' button.

Screenshot 127 The customer only sees his device



Screenshot 128 The service technician can access all devices of category A.



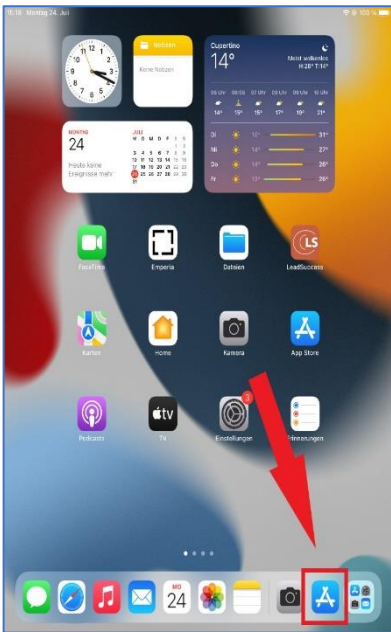
Screenshot 129 Admin and engineer sea all devices in this example

7 Installation iOS App

7.1 Start Menu and App Store

First log in to your device and navigate to the home screen. Search for the App Store on your device. The App Store is marked in red in Screenshot 1. Open the App Store. Now go to step 2.

Note: If the App Store cannot be found on the home screen, wipe from top to bottom on the right side of the home screen. This opens another screen (see Screenshot 2) with a search bar (marked red). Enter App Store there.



Screenshot 1 Home screen

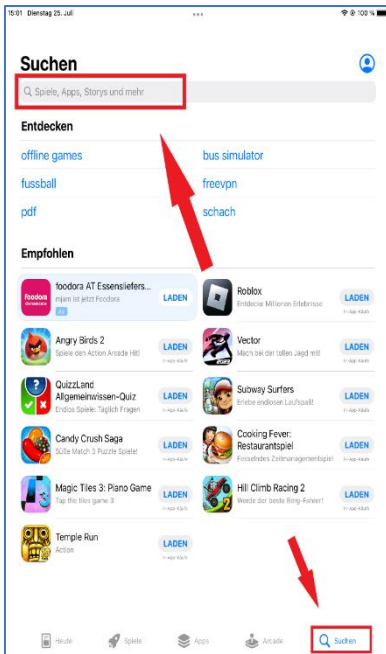


Screenshot 2 Search bar

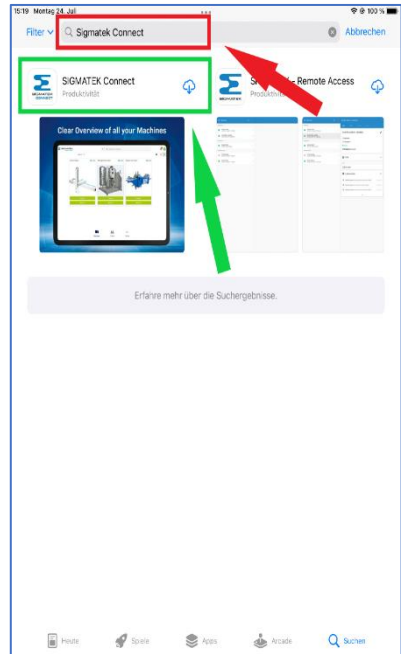
7.2 App Store – Sigmatek App

Once the App Store is open, a window appears with a variety of apps that you can download. But to find "SIGMA TEK Connect" as an app, click on the magnifying glass icon in the bottom right corner (see Screenshot 3). A search bar appears on the screen, enter "Sigmatek Connect" there. The search bar is marked red in Screenshot 3.

You should now see a screen similar to the one shown in Screenshot 4. You will now be provided with several apps to choose from. Please find the "SIGMA TEK Connect" app and click on it. If necessary, scroll down a little to find the app. In Screenshot 4 the App is marked green. Go to step 3.



Screenshot 3 App Store search bar



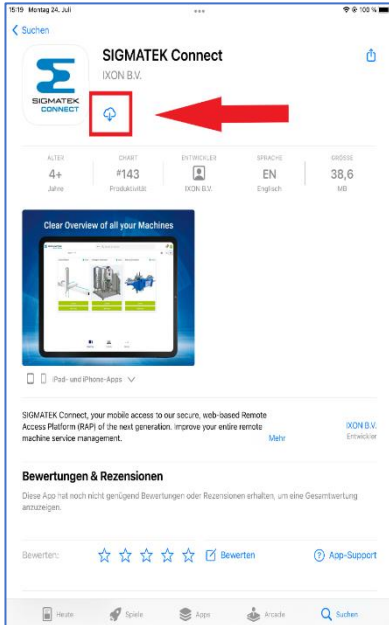
Screenshot 4 Sigmatek – Connect

7.3 Install App

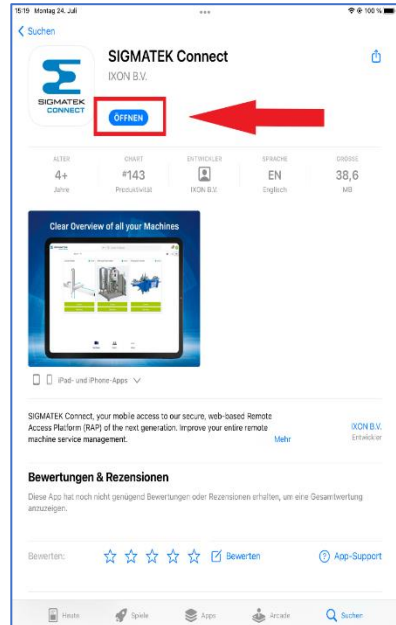
Last but not least, you can install the SIGMATEK Connect App.

To do this, press the clouds icon. The icon is marked red in Screenshot 5. Wait briefly until the installation is complete.

Press Open to start the app. (Screenshot 6, marked red). Go to step 4.



Screenshot 5 Install

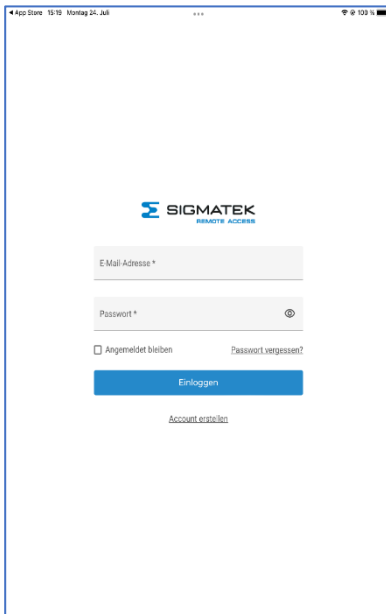


Screenshot 6 Open

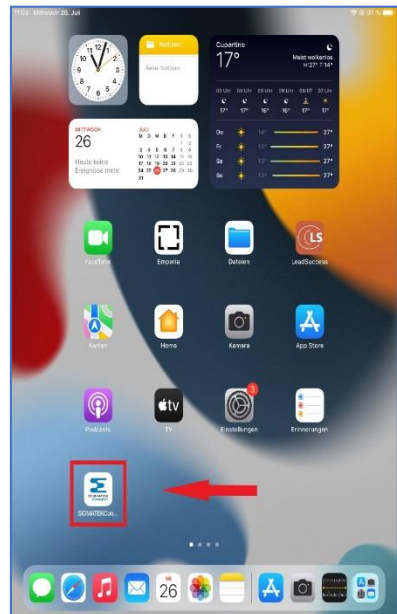
7.4 Sigmatek Login and Home Screen

If you have now opened the app, a login window appears, as shown in Screenshot 7. At the same time, the app is added to your home screen in the background, as shown in red in Screenshot 8. If you do not see the app on your home screen, please check the note in step number 1 again and find the app. Maybe it hides on one of the other screens. Once you have found the app, you can relax and open it when and where you like.

Note: Sometimes it happens that due to memory or other reasons, the app is not linked to the screens of the device. However, you can still open the installed app by going back to the App Store and searching for the app and opening it as shown in Screenshot 6.



Screenshot 7 Login – Platform



Screenshot 8 App – Link on home screen

8 Installation Android App

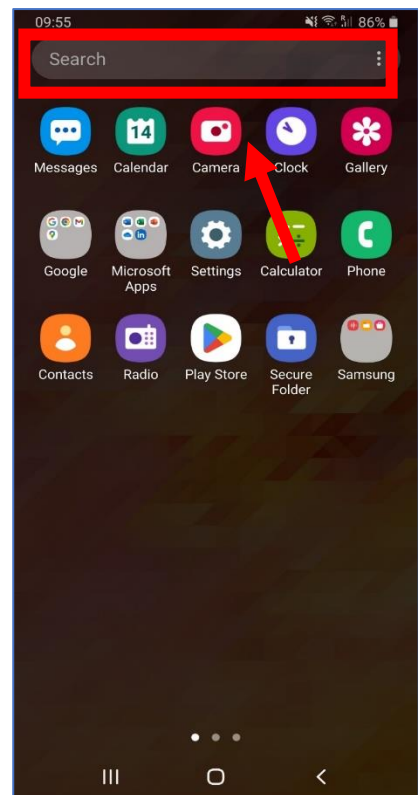
8.1 Startmenü und Play Store

First, log in to your Android device and go to the home screen. Now find the Play Store app of Android on your device. The Play Store is marked red in Screenshot 1. Open the Play Store. Go to step 2.

Note: If the Play Store is not on your home screen, swipe up from the bottom of your home screen. This opens another screen (see Screenshot 2) with a search bar (marked in red). There you enter Play Store.



Screenshot 1 Home screen

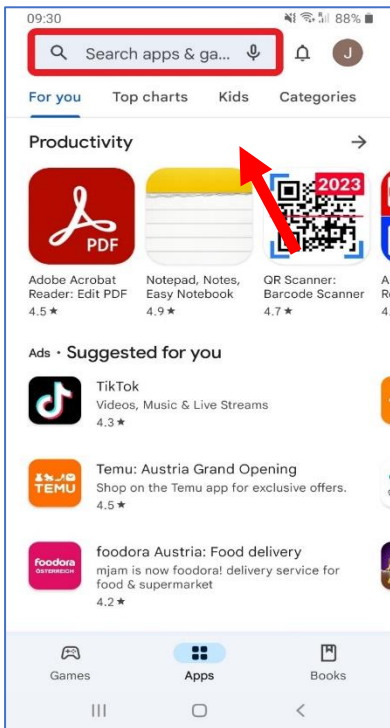


Screenshot 2 Search bar

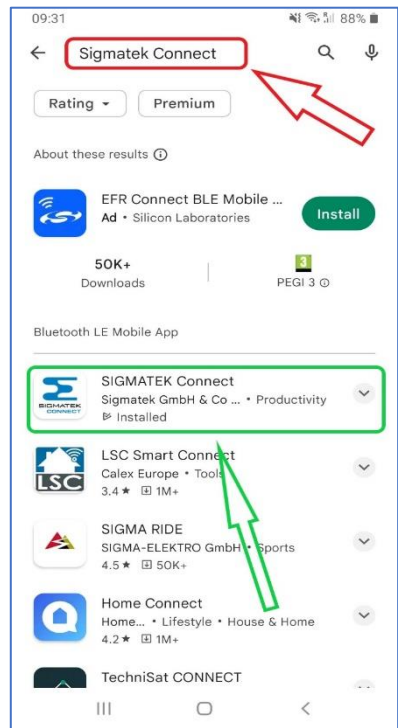
8.2 Play Store – Sigmatek App

Once the Play Store is open, a window appears with quite a few apps that you can download. But to find "SIGMATEK Connect" as an app, click in the search bar at the top and type "**SIGMATEK Connect**". The search bar is highlighted in red in Screenshot 3.

You should now see a screen similar to the one shown in Figure 4. You will now be presented with several apps to choose from. Please find the "**SIGMATEK Connect**" app and click on it. If need be, you will have to scroll down a bit to find the app. In Figure 4, the app is marked with green. Now go to step 3.



Screenshot 3 Play Store search bar



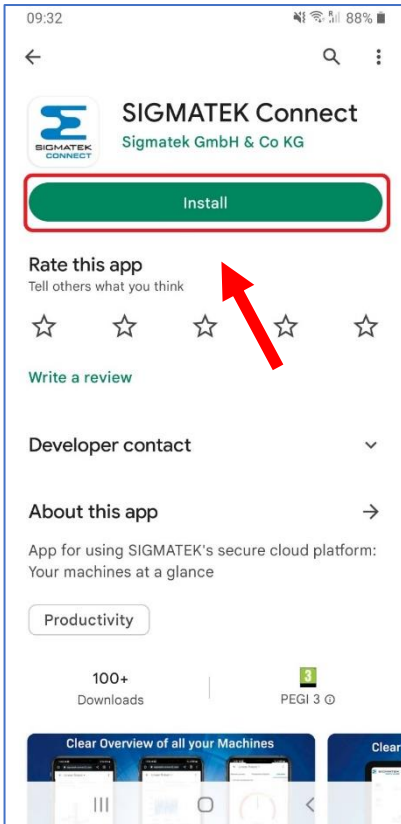
Screenshot 4 SIGMATEK Connect

8.3 Install App

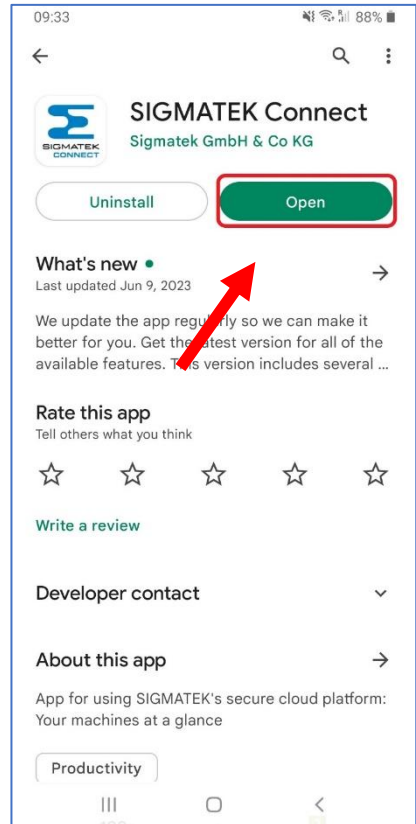
Last but not least, you can install the SIGMATEK Connect App.

To do this, press Install. The Install button is marked red in Figure 5. Wait briefly until the installation is complete.

Press Open to launch the app. (Screenshot 6, marked red). Go to step 4.



Screenshot 5 Install button



Screenshot 6 Open app

8.4 Sigmatek Login and Home Screen

If you have now opened the app, a login window will appear, as shown in Screenshot 7. At the same time, in the background, the app is added to the home screen, as shown in Figure 8, marked in red. If you do not see the app on the home screen, please look at the note at step number 1 again and find the app. Usually it hides on one of the other screen pages. Once you have found the app, you can relax and open it when and where you want.



Screenshot 7 Login - Platform



Screenshot 8 App link