

Sicherer Fernzugriff

Inhalt

1	Verwendete Symbole	4
2	Schnellstart.....	5
3	Fernzugriffsrouter Hardware Einrichtung	6
3.1	Elektrischer Anschluss	6
3.1.1	Verdrahtung der RAR	6
3.1.2	Optionale Hardware-Schaltung zur VPN-Verwaltung.....	7
3.2	Hardware mit optionalen Schnittstellen vorbereiten	10
3.2.1	Mobiltelefon 3G/4G	10
3.2.2	WIFI	10
3.2.3	Verwendung von WIFI RAR als Access Point (AP).....	11
3.3	LED Zustandsanzeige	14
3.3.1	 Signal-LED.....	14
3.3.2	ACT Signal LED.....	15
4	Eingebetteter Fernzugriff-Setup.....	16
4.1	Anforderungen	16
4.2	Einrichtung	16
5	Remote Access Plattform (RAP)	23
5.1	Kontoeinrichtung	23
5.2	RAP Cloud-Schnittstelle	25

5.2.1	Apps Menü	26
5.2.2	Account Menü.....	26
5.2.3	Zwei-Faktor-Authentifizierung.....	27
5.3	Registrierung eines Fernprodukts.....	29
5.3.1	Auf Werkseinstellungen zurücksetzen.....	29
5.3.2	Fernzugriffsrouter über Ethernet WAN	30
5.3.3	Router für Fernzugriff über WIFI WAN	36
5.3.4	Fernzugriffsrouter mit 3G/4G WAN.....	37
5.3.5	Eingebettete Fernzugriff	39
5.4	Zusätzliche Netzwerkeinstellungen (nur RAR).....	41
5.5	Zusätzliche Netzwerkeinstellungen (nur RAE).....	43
5.6	Remotedienste einrichten.....	45
5.6.1	Herstellung einer VPN-Verbindung.....	45
5.6.2	VNC über VPN	46
5.7	Datenerfassung und -aufbewahrung	50
5.7.1	Einrichten von Datenquellen.....	50
5.7.2	Cloud Logging	61
5.7.3	Eine Seite zur Datenanzeige erstellen.....	65
5.7.4	Cloud-Benachrichtigungen	80
5.8	Benutzerverwaltung	86
5.8.1	Erstellen eines neuen Benutzers	92
6	Beispiellösungen	95
6.1	Lösungen auf Basis von Fernzugriffsrouter (RAR).....	95
6.1.1	Beispiel 1: RAR verkabelt, Einzel-CPU-Lösung.....	98
6.1.2	Beispiel 2: RAR verkabelt, Zwei-CPU-Lösung.....	99

6.1.3	Beispiel 3: RAR + WIFI, Einzel-CPU-Lösung.....	100
6.1.4	Beispiel 4 RAR + WIFI, Zwei-CPU-Lösung	101
6.1.5	Beispiel 5: RAR + Mobilfunk, Einzel-CPU-Lösung	102
6.1.6	Beispiel 6: RAR + Mobilfunk, Zwei-CPU-Lösung	103
6.2	Eingebettete Fernzugriffslösungen (RAE)	104
6.2.1	Beispiel 7: RAE100 Einzel-CPU-Lösung.....	104
6.2.2	Beispiel 8: RAE100 Zwei-CPU Lösung	105
6.2.3	Beispiel 9: RAE100 als Gateway	106
6.3	Verwaltung von Benutzern	108
6.3.1	Beispiel 10: Remote-Access-Service	108
7	Installation iOS App	110
7.1	Startmenü und App Store	110
7.2	App Store – Sigmatek App.....	111
7.3	App installieren	112
7.4	Sigmatek Login und Startbildschirm	113
8	Installation Android App.....	114
8.1	Startmenü und Play Store	114
8.2	Play Store – Sigmatek App	115
8.3	App installieren	116
8.4	Sigmatek Login und Startbildschirm	117

1 Verwendete Symbole

Um das Arbeiten mit der Schulungsunterlage so einfach und komfortabel wie möglich zu gestalten, wurden 3 verschiedene Symbole verwendet. Diese sollen das Navigieren durch die Dokumentation erleichtern, Zusatzinformationen liefern, wichtige Abschnitte hervorheben und Beispiele ankündigen. Die Bedeutung der 3 Symbole wird wie folgt erklärt:



Achtung

Stoßen Sie in der Hilfe auf dieses Symbol, sollten Sie den folgenden Zeilen Ihre ganze Aufmerksamkeit schenken. Diese Informationen sind sehr wichtig und zu BEACHTEN. Es wird empfohlen den Absatz neben diesem Symbol sehr gründlich durchzulesen.



Tipp:

Der aufzeigende Daumen ist das Symbol für einen hilfreichen Tipp, wie Sie etwas schneller oder besser erledigen können.



Beispiel

Dieses Symbol zeigt den Beginn eines Beispiels an.

2 Schnellstart

Die wesentlichen Schritte für die Fernverbindung eines Rechners mit der SIGMATEK-Remote Access Plattform (RAP) bestehen aus:

1. Registrieren Sie sich bei der ersten Nutzung für ein RAP-Unternehmen/Benutzerkonto, s5.1.
2. Remote Produkt als benötigt einrichten:
 - a. RAR Hardware, s3
 - b. RAE Applikation, s4 (nicht nötig für RAR)
3. Das Gerät bei der ersten Verwendung registrieren.
 - a. RAR über Ethernet, s5.3.2
 - b. RAR über WIFI, s5.3.3.
 - c. RAR über Mobilfunkdienste 3G/4G, s5.3.4.
 - d. RAE Applikation, s5.3.5.
4. Steuerung mit der RAP verbinden. Beispiele werden vorgelegt:
 - a. RAR, s6.1
 - b. RAE, s6.2
5. Ferndienste hinzufügen:
 - a. VNC, s5.6.2
 - b. Port-forward für IP-Dienste, s5.4
 - c. Datenaufzeichnung, s5.7

3 Fernzugriffsrouter Hardware Einrichtung

3.1 Elektrischer Anschluss

3.1.1 Verdrahtung der RAR

- Der RAR muss mit 12–24 V Spannung versorgt werden, indem die Versorgungsspannung angeschlossen wird.
- Die Schirmung sollte auf einem Schutzleiter (PE) angelegt werden.
- Verlegen Sie die Kabel mit Aderendhülsen, um die Belastung der Drähte zu verringern.
- Ein digitaler Eingang ist für Hardware-basierte Verwaltung der VPN-Verbindung verfügbar
 - Standardmäßig ist der Digitaleingang nicht konfiguriert und muss nicht verdrahtet werden.

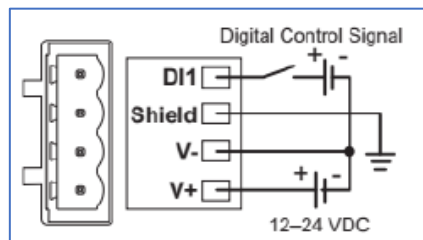


Abb. 1 Versorgungseingangsstecker Pin-Bezeichnungen.

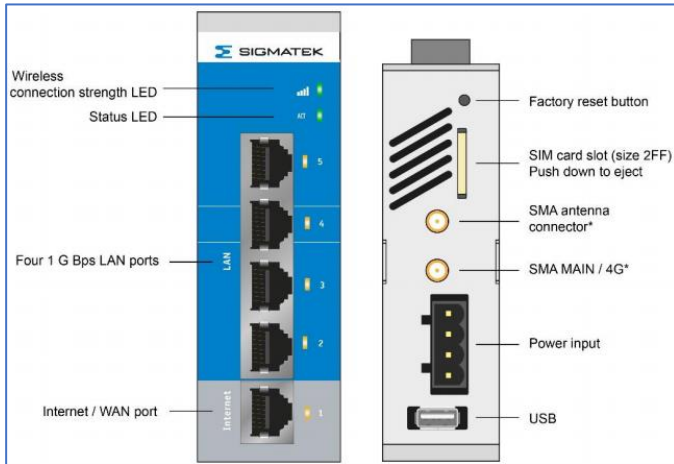


Abb. 2 Diagramm des RARs.

3.1.2 Optionale Hardware-Schaltung zur VPN-Verwaltung

Der digitale Eingang DI1 kann zur Deaktivierung des VPN verwendet werden; diese Option muss über den RAP aktiviert werden:

1. Sicherstellen, dass die elektrische Verkabelung des Geräts vollständig ist (Abb. 3) und im RAP registriert wurde. Zur Registrierung siehe Abschnitt 0.
2. Wählen Sie bei der Erstellung einer Konfigurationsdatei in Abschnitt 0 die Option „Select control over remote accessibility“ (Abb. 4).
3. Es wird ein neues Steuerelement mit der Bezeichnung "digitaler Eingang" angezeigt (Abb. 5); wählen Sie eine der Optionen:
 - a. deaktiviert [digitaler Eingang inaktiv],
 - b. VPN deaktivieren, wenn [digitaler] Eingang niedrig,
 - c. VPN deaktivieren, wenn [digitaler] Eingang hoch,
4. Fahren Sie mit der Router-Konfigurationsdatei fort.



Abb. 3 eingebaute RAR mit installiertem Schalter am digitalen Eingang 1.

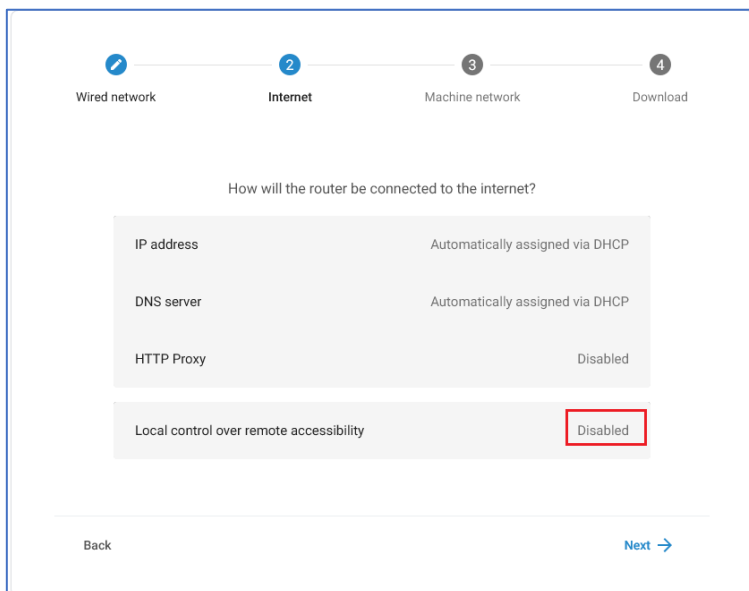


Abb. 4 Wählen Sie die lokale Kontrolle über die VPN-Verbindung.

1 2 3 4
Wired network Internet Machine network Download

How will the router be connected to the internet?

IP address	Automatically assigned via DHCP
DNS server	Automatically assigned via DHCP
HTTP Proxy	Disabled

Local control over remote accessibility

☐ Disabled
☒ Disable VPN connection when input is high
☐ Disable VPN connection when input is low

Back
Next →

Abb. 5 Auswahl der Aktion des digitalen Eingangs in der VPN-Verwaltung.

3.2 Hardware mit optionalen Schnittstellen vorbereiten

3.2.1 Mobiltelefon 3G/4G

Im ausgeschalteten Zustand:

1. Stecken Sie die SIM-Karte in den SIM-Kartenschlitz (Abb. 6).
2. Schrauben Sie die Antenne auf den SMA-Anschluss mit der Bezeichnung "MAIN" (Abb. 7).



Abb. 6 RAR mit rot markierter Sim-Karte



Abb. 7 RAR mit Mobilfunk Option: 3G/4G-Antenne auf dem SMA-Anschluss des Mobilfunkgeräts installiert.

3.2.2 WIFI

Bei ausgeschaltetem Gerät: Schließen Sie die WIFI-Antenne über den mit "DIV" gekennzeichneten SMA-Anschluss an den RAR an.



Abb. 8 RAR mit installierter WIFI-Antenne am SMA-Anschluss für den 2,4-GHz Funk.

3.2.3 Verwendung von WIFI RAR als Access Point (AP)

So richten Sie einen Access Point (AP) auf dem RAR über RAP ein:

1. Sicherstellen, dass die elektrische Verkabelung des Geräts vollständig ist (Abb. 3) und im RAP registriert wurde. Zur Registrierung siehe Abschnitt 0.
2. Im RAP unter APPS Menu -> Fleet Manager, wählen Sie das zu konfigurierende Gerät aus (Abb. 9).
3. Wählen Sie im Gerät-Menü den Punkt Netzwerk->LAN, um die LAN-Einstellungen anzupassen (Abb. 10).
4. „Enable Wi-Fi-Hotspot“ ankreuzen
5. Weisen Sie die SSID und das Passwort nach Bedarf zu.
6. Klicken Sie auf „Bestätigen“, um die Einstellungen zu speichern.
7. Wählen „Push Config to Device“ aus. Dadurch werden die Änderungen mit der aktuellen Konfiguration des Geräts synchronisiert (REF _Ref103776152 \h Abb. Abb. 12).
8. Über die Firewall-Einstellungen ist es außerdem möglich, aus dem Device Menu->Network->Firewall, den Zugang zum Internet bzw. zum Host-Netzwerk zu beschränken oder zu erlauben (Abb. 11).

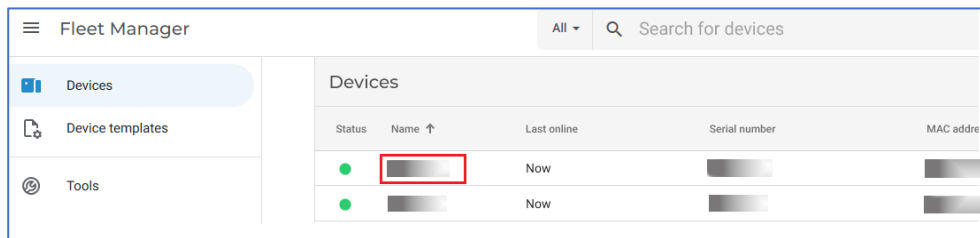


Abb. 9 Wählen Sie das Gerät aus dem Fleet-Manager Menü.

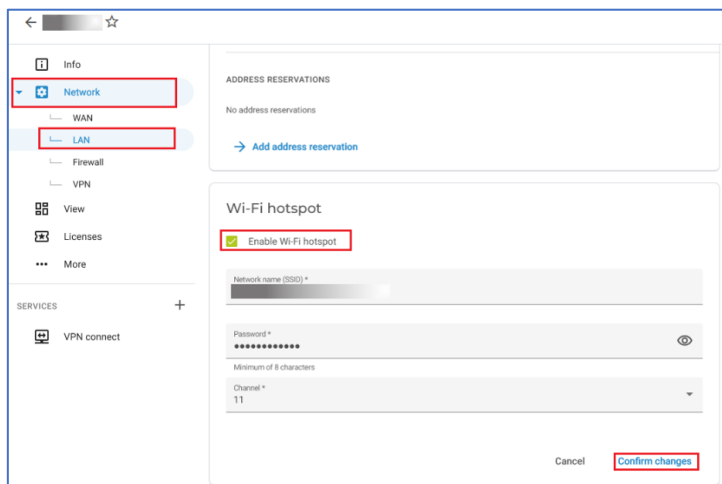


Abb. 10 Passen Sie die Firewall-Einstellungen an, um den Zugriff über den AP auf das Internet und die Host-Netzwerke zu konfigurieren.

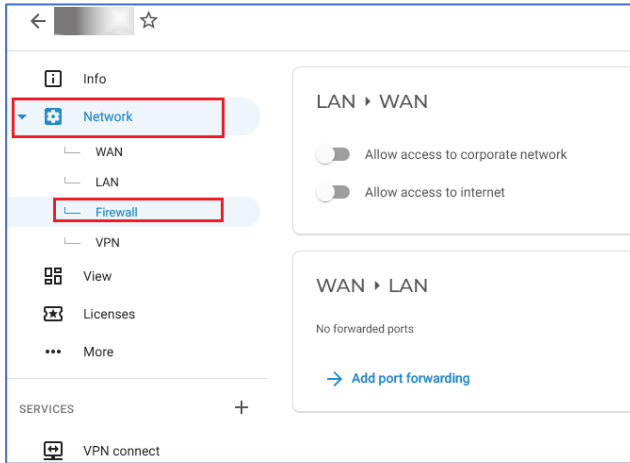


Abb. 11 Passen Sie die Firewall-Einstellungen an, um den Zugriff über den AP auf das Internet und die Host-Netzwerke zu konfigurieren.

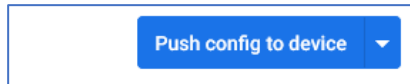


Abb. 12 Konfigurationsänderungen müssen immer in den RAR übertragen werden, um übernommen zu werden.

3.3 LED Zustandsanzeige

3.3.1 Signal-LED

	Blau blinkend	Initialisierung des Mobilfunkmoduls
	Rot blinkend 1 Impuls	Kein Empfang oder keine Verbindung zum Netzwerk möglich (APN oder SSID kann falsch sein)
	Rot blinkend 2 Impulse	PIN ungültig oder PUK erforderlich (Zum Entsperren der SIM-Karte mit PUK ist ein Telefon erforderlich)
	Rot blinkend 4 Impulse	Die SIM-Karte ist ungültig oder fehlt.
	Konstantes Rot	Verbunden, schwacher Empfang
	Konstantes Violett	Verbunden, mittlerer Empfang
	Konstantes Blau	Verbunden, guter Empfang

3.3.2 ACT Signal LED

	Konstantes Rot	Das Hochfahren (kann 1-2 Minuten dauern) oder noch nicht registriert
	Rot blinkend 1 Impuls	Warten auf den Internetzugang
	Rot blinkend 3 Impulse	LAN/WAN-Konflikt (widersprüchliche Subnetze)
	Rot blinkend 4 Impulse	Von der Plattform entfernt RAR muss neu konfiguriert und registriert werden
	Rot blinkend 5 Impulse	Zuvor bei RAP angemeldet (aus dem RAP entfernen und erneut registrieren)
	Blau blinkend 1 Impuls	Herstellung der Verbindung mit RAP
	Blau blinkend 2 Impulse	Initialisierung der VPN-Verbindung
	Konstantes Blau	Aktive VPN-Verbindung

4 Eingebetteter Fernzugriff-Setup

4.1 Anforderungen

Das RAE Package wurde speziell für das Betriebssystem Salamander entwickelt, welches die Voraussetzung für die Software-Lösung ist.

- Um RAE auf der SIGMATEK-Steuerung installieren zu können ist die folgende Betriebssystemversion nötig:
 - Ab Salamander 09.03.102
- Die SIGMATEK-Steuerung, auf der RAE100 installiert ist, muss über eine gültige IP-Konfiguration mit Internetzugang verfügen.

4.2 Einrichtung

Dieser Prozess beschreibt das Testverfahren zur Vorbereitung einer SIGMATEK-Steuerung mit RAE. Das Remote-Produkt muss nach der Einrichtung registriert werden.

1. Öffnen Sie LASAL CLASS 2 und stellen Sie eine Verbindung zum HMI her.
2. Die IP-Konfiguration kann über LASAL CLASS 2 eingestellt werden: "Debug → File Transfer → Edit Autoexec.lsl" wie in Abb. 13 gezeigt.
3. Verwenden der für das aktuelle LAN gültigen Einstellungen (Abb. 14):
 - a. IP Adresse
 - b. IP Subnet
 - c. IP Gateway: IP-Adresse des für den Internetzugang verwendeten Routers
 - d. IP DNS: IP-Adresse eines DNS-Servers, der vom aktuellen Standort aus erreichbar ist; einige Serveradressen sind unten angegeben:
 - i. Cloudflare 1.1.1.1
 - ii. Google 4.4.4.4 oder 8.8.8.8
4. Erstellen Sie mit dem PLCDiag-Tool File Commander unter "Tools → Advanced Debug Tools → File Commander" den Ordner "C:\lsys\packages" auf dem Rechner, falls er noch nicht vorhanden ist.
 - a. Um einen Ordner zu erstellen, verwenden Sie "MAKE DIR". (Abb. 15, Abb. 16).
 - b. Kopieren Sie den RAE in den Packages Ordner. Dazu navigieren Sie auf der rechten Seite des File Commanders zu dem Paket und klicken unten auf „COPY“ (Abb. 17).

5. Um den RAE zu installieren, müssen Sie dazu in der Command Line Interface den Befehl eingeben.
 - a. Dazu öffnen sie das Remote CLI unter „Tools → Advanced Debug Tools → Remote CLI“ (Abb. 18).
 - b. Um die Internetverbindung zu überprüfen, geben Sie über die Remote-CLI den Befehl "ping www.google.com" (oder eine von Ihrer Region aus erreichbarer Seite) in die Befehlszeile ein und drücken Sie die Eingabetaste oder "Execute". Wenn der Rechner das Internet erreichen kann, wird ein Latenzwert für den Ping-Befehl gemeldet.
 - c. Geben Sie den Befehl „PACKAGE INSTALL ixagent“ in der Command Line ein und drücken Enter oder „Execute“ (Abb. 19). Das Installieren kann einige Zeit beanspruchen. Auf die Rückmeldung warten (Abb. 20).
 - d. Nachdem RAE installiert worden ist, muss es mit dem Befehl „ixagent start“ aktiviert werden (Abb. 19). Auf die Rückmeldung warten (Abb. 20).
 - e. Die RAE-Anwendung muss nach der Installation gestartet werden:
 - i. Bei Bedarf kann der Befehl "ixagent start" über die Remote-CLI ausgeführt werden (Abb. 21).
 - ii. Für den automatischen Start mit der Maschine sollte der gleiche Befehl "ixagent start" an die Autoexec.lsl angehängt werden (Abb. 22).

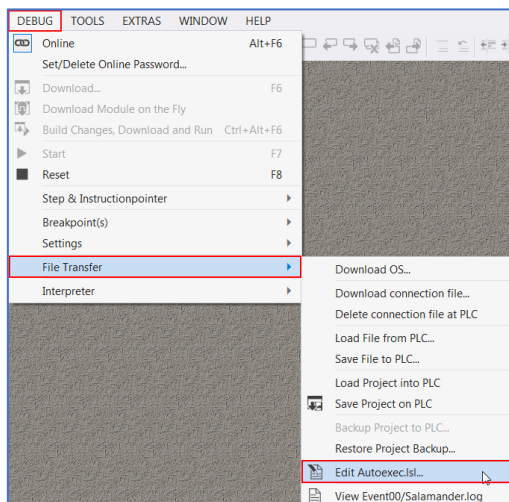


Abb. 13 Bearbeitung der Autoexec.Is1 aus CLASS 2.

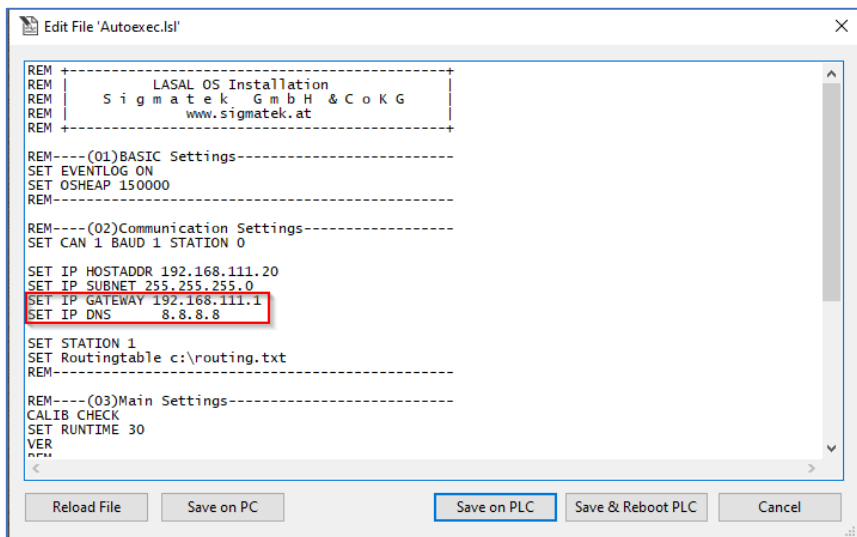


Abb. 14 Bearbeitung der IP-Konfiguration.

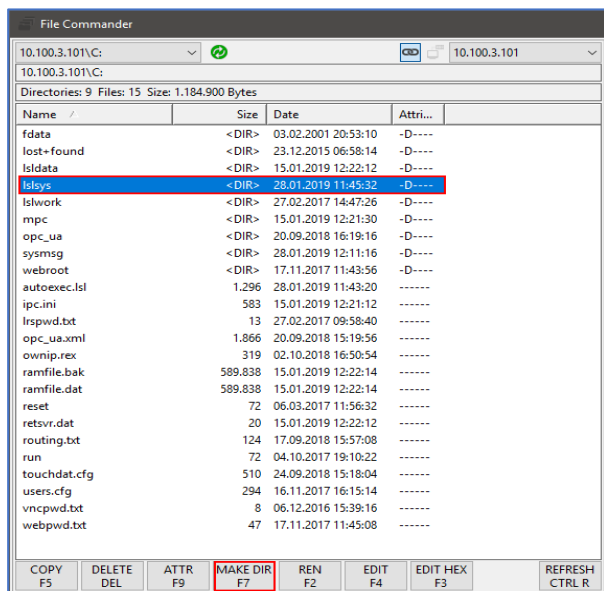


Abb. 15 File Commander interface - Make Dir Button markiert.

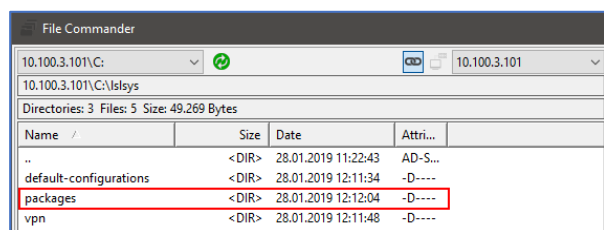


Abb. 16 Packages Ordner in C:\lsysys

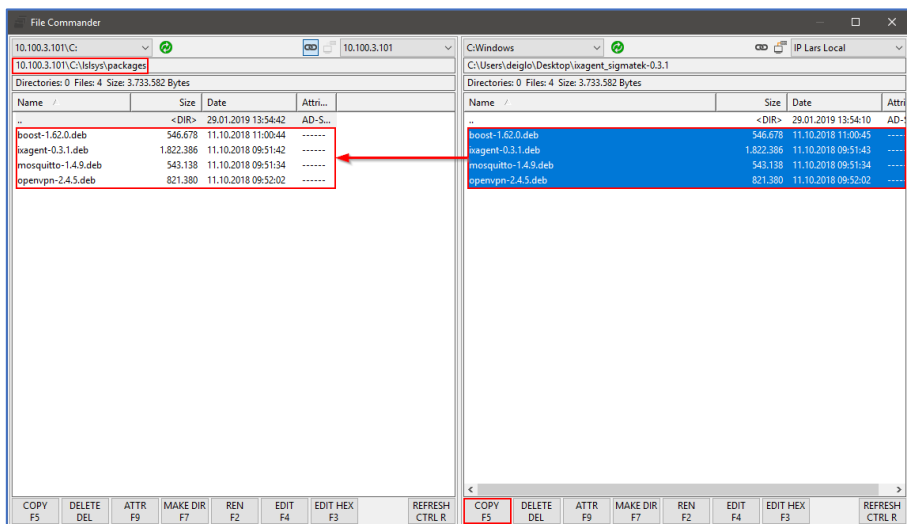


Abb. 17 Kopieren der Packages auf die Maschine.

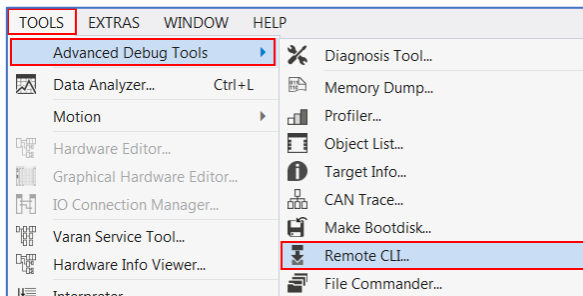


Abb. 18 Öffnen des Remote CLI Tools.

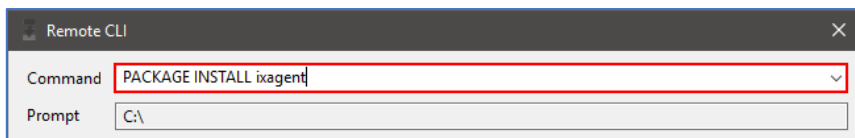


Abb. 19 Ausführen des Befehls zur Installation der RAE-Anwendung über die CLI.

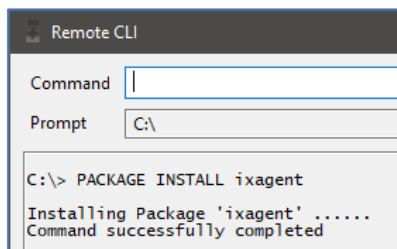


Abb. 20 Installation erfolgreich bestätigt.

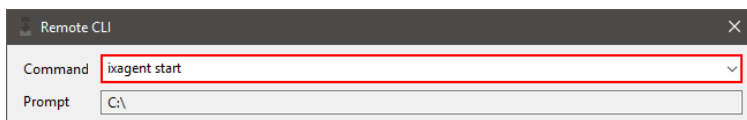


Abb. 21 Starten der RAE-Anwendung.

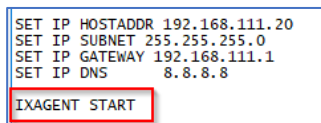


Abb. 22 Anhängen des Befehls zum Starten der RAE-Anwendung an die Datei Autoexec.lsl

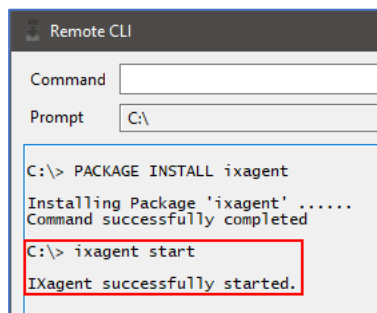
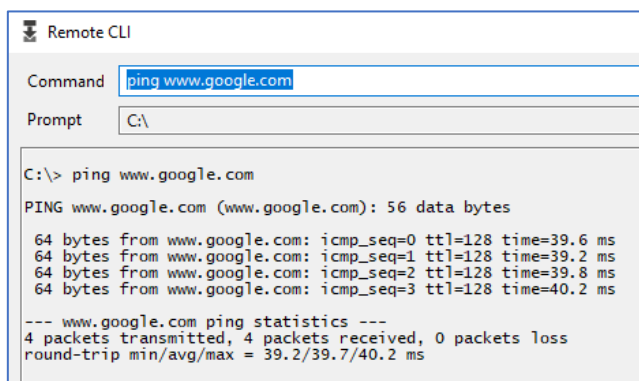


Abb 23 Bestätigungsmeldung, dass die RAE-Anwendung erfolgreich gestartet wurde.



```
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
```

Abb. 24 Ausführen des PING-Befehls auf eine Domäne mit einem Webserver, der ICMP Echo Response unterstützt.

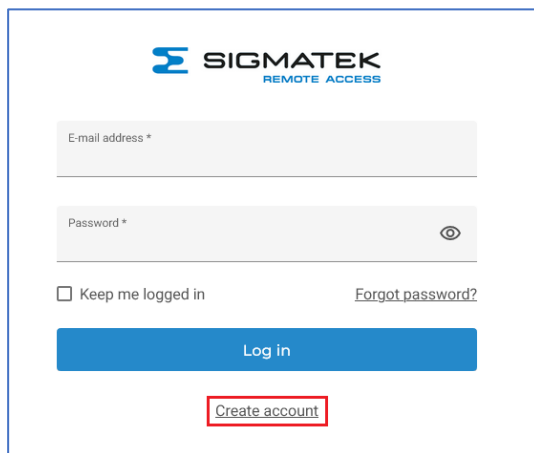
5 Remote Access Plattform (RAP)

Die Fernzugriffsplattform ist die Benutzerschnittstelle für die SIGMATEK Router und Anwendungsprodukte. Für die Registrierung neuer Geräte und den Fernzugriff auf Daten ist ein Benutzerkonto erforderlich.

5.1 Kontoeinrichtung

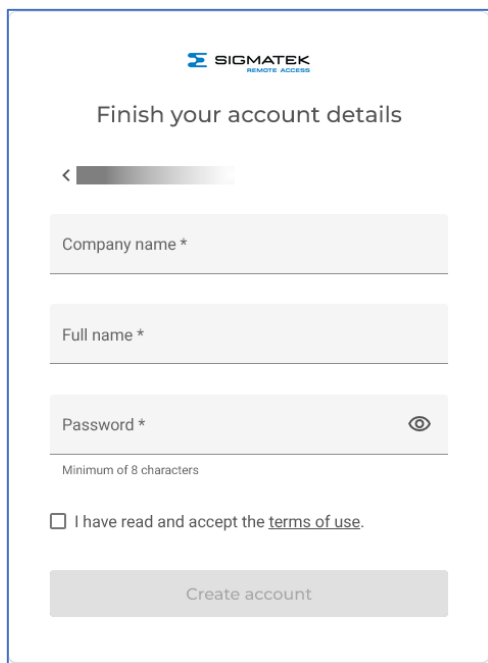
Falls Sie noch keinen Firmenaccount angelegt haben, registrieren Sie sich bei der Remote Access Plattform.

1. Öffnen Sie die RAP Hauptseite: <https://www.sigmatek-connect2.com> Um sich anzumelden, klicken Sie auf den Link "Don't have an account? Register" (Abb. 25).
2. Geben Sie die erforderlichen Daten ein und bestätigen Sie die Annahme der Bedingungen um fortzufahren (Abb. 26).
3. Ist die Registrierung erfolgreich, wird eine E-Mail an die registrierte Adresse gesendet. Dieser Link muss zur Freischaltung des Benutzerkontos angeklickt werden (Abb. 27).



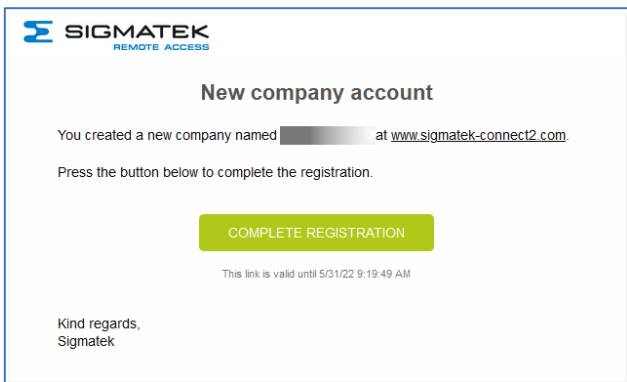
The screenshot shows the SIGMATEK Remote Access login and registration interface. At the top is the SIGMATEK logo with 'REMOTE ACCESS' underneath. Below the logo are two input fields: 'E-mail address *' and 'Password *'. The password field has an eye icon for toggling visibility. Below these fields is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

Abb. 25 Registrierung für ein neues Firmenkonto.



The screenshot shows a registration form titled "Finish your account details" with the Sigmatek Remote Access logo at the top. Below the title is a back arrow and a greyed-out field. The form contains three input fields: "Company name *", "Full name *", and "Password *". The password field has a toggle icon and a note "Minimum of 8 characters". Below these fields is a checkbox with the text "I have read and accept the [terms of use](#).". At the bottom is a "Create account" button.

Abb. 26 Eingabe der angeforderten Daten.



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

Abb. 27 Vervollständigen Sie die Registrierung durch Klicken auf den Link in der E-Mail.

5.2 RAP Cloud-Schnittstelle

Um sich bei der Plattform anzumelden:

1. gehen Sie auf die Hauptseite <https://www.sigmatek-connect2.com>.
2. Nach Eingabe der Anmeldedaten klicken Sie auf "LOG IN".
3. Wenn mehr als ein Unternehmen verfügbar ist, wählen Sie eines aus. Dies ist zur Anzeige und Registrierung neuer Geräte nötig.
4. Der RAP Hauptschnittstelle wird dann angezeigt (Abb. 28). Angezeigt wird die Liste der konfigurierten Geräte und Benutzer. Das Apps-Menü und das Kontomenü können erweitert werden und befinden sich in der oberen rechten Ecke des Bildschirms (Abb. 28).

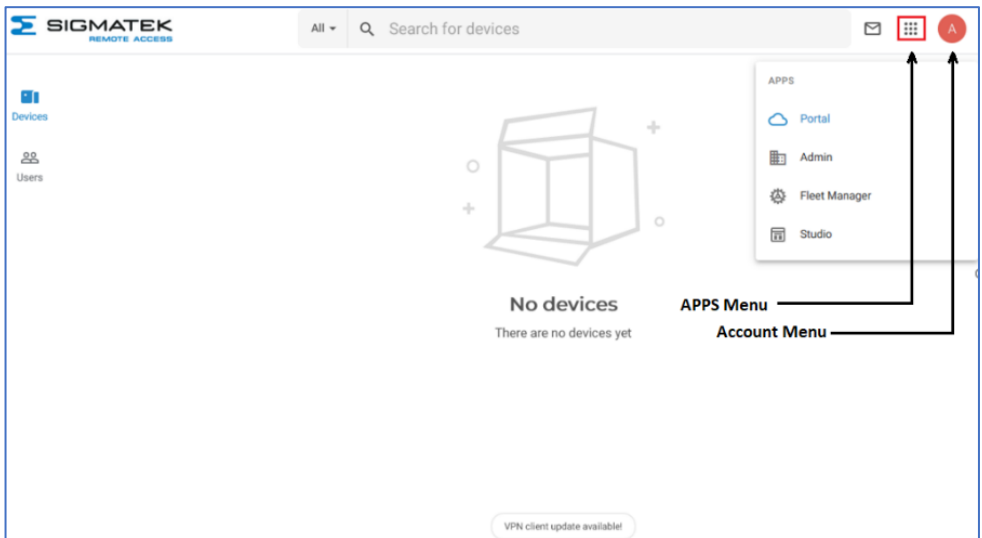


Abb. 28 Hauptschnittstelle für ein ausgewähltes Unternehmen mit aufgeklapptem Apps-Menü.

5.2.1 Apps Menü

- Portal, Verwenden Sie die Dienste Ihres Geräts und laden Sie Benutzer ein
- Admin, Ihre Unternehmen verwalten
- Fleet Manager, Ihre Geräteflotte verwalten
- Studio, Benutzerdefinierte Seiten erstellen, damit Sie nur sehen, was Sie brauchen

5.2.2 Account Menü

Öffnen Sie das Kontomenü, indem Sie auf den roten Kreis klicken (Abb.29). Er bietet Zugang zu:

- Profileinstellungen - Lokalisierung, E-Mail-Adresse, Sicherheit und Ansichtsberechtigungen
- Firmen wechseln - bei der Verwaltung mehrerer Unternehmen über ein einziges Benutzerkonto

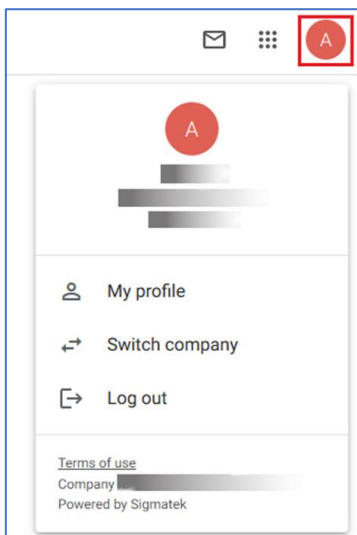


Abb.29 Öffnen der Account-Einstellungen über die Hauptschnittstelle.

5.2.3 Zwei-Faktor-Authentifizierung

Die Zwei-Faktor-Authentifizierung (2FA) ist eine zusätzliche Sicherheitsmaßnahme, die dazu dient, ein Konto zu stärken und zu verhindern, dass andere darauf zugreifen.

Um die Zwei-Faktor-Authentifizierung zu aktivieren:

1. Öffnen Sie die persönlichen Profil Einstellungen. (Abb. 30)
2. Unter dem Menüpunkt Login und Sicherheit klicken Sie auf den Pfeil nach rechts, um die Zwei-Faktor-Authentifikation zu aktivieren. (Abb. 31)
3. Anschließend können Sie mit Hilfe einer Authentifizierungs-App wie z.B. Google Authenticator den QR-Code scannen. Das erzeugte One-time Passwort (OTP) kann nun eingegeben werden. (Abb. 32)
4. Ist das Scannen des QR-Codes nicht möglich besteht die Möglichkeit sich mithilfe eines Codes in der Authentifizierungs-App zu registrieren und ein One-Time Passwort zu erzeugen.

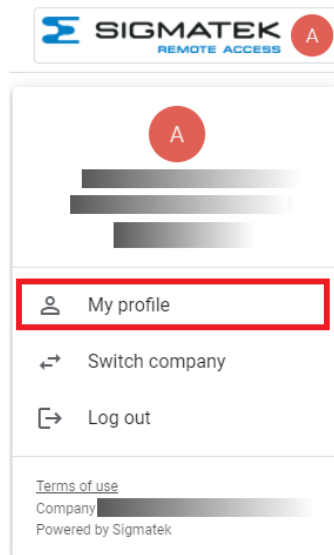


Abb. 30 Das persönliche Profil öffnen.

 Personal info Preferences Login and security More

Signing in

Change password

>

Two-factor authentication Off

>

Abb. 31 Klicken Sie unter dem Menüpunkt Login and security auf Two-factor authentication.

Two-factor authentication

×

Use an authenticator-app like [Google Authenticator](#) to scan the QR-code below and generate a one-time password.



I can't scan a QR code

Generate a first one-time password and enter it below.

One-time password (OTP) *

Device name *

Turn on

Abb. 32 Scannen Sie den QR-Code mithilfe einer „Authentifizierungs-App“ und geben Sie anschließend das One-time Passwort darunter ein.

5.3 Registrierung eines Fernprodukts

Damit das RAR eine Verbindung zur Cloud herstellen kann, muss er konfiguriert werden: Eine Konfigurationsdatei wird erstellt und auf das RAR heruntergeladen.

5.3.1 Auf Werkseinstellungen zurücksetzen

Um den Router zu konfigurieren muss eine Config Datei erstellt werden. Bevor die Config Datei auf den Router übertragen wird, sollte ein Factory Reset gemacht werden, wenn der Router zuvor schon einmal registriert wurde.



Achtung beim Factory Reset wird die Konfiguration des Routers gelöscht.

Dazu gehören WAN/LAN-Einstellungen, Port-Weiterleitung, IP-Dienste und Daten-Upload.

Stellen Sie sicher, dass die alte Konfiguration nicht mehr benötigt wird.

Drücken Sie bei eingeschaltetem RAR die kleine Taste am Router 5 Sekunden lang, bis die ACT-LED blau-rot zu blinken beginnt.



Abb. 30 Position der Reset-Taste

5.3.2 Fernzugriffsrouter über Ethernet WAN

Vom RAP Apps Menü

1. Das Fleet Manager Menü öffnen und auf die Tools-Option klicken (Abb. 31).
2. Klicken Sie auf "Konfiguration starten" unter „Router config file“ (**Fehler! Verweisquelle konnte nicht gefunden werden.**).
3. Wählen Sie den Internetverbindungstyp: verkabelt über Ethernet-Kabel (Abb. 32).
4. Akzeptieren Sie die Standard-WAN-Konfiguration oder legen Sie Einstellungen fest (Abb. 33). Die Einstellungen können geändert werden, nachdem das Gerät registriert wurde.
5. Geben Sie die Router-Adresse an, die im Router-LAN (Abb. 34) verwendet werden soll.
 - a. Beispiel: die SIGMATEK-Steuerung hat eine IP-Adresse von 192.168.111.20 und eine Subnetzmaske von 255.255.255.0; die Router-Adresse sollte im Bereich 192.168.111.x angegeben werden
 - b. Weitere LAN-Netzwerke können später hinzugefügt werden.
6. Laden Sie die RAR-Konfigurationsdatei herunter (Abb. 35); bei den meisten Windows-basierten Browsern wird die Datei (ixrouter.conf) im Download-Verzeichnis des Benutzers gespeichert.
7. Kopieren Sie die Konfigurationsdatei in das Stammverzeichnis eines USB-Laufwerks.
8. Schalten Sie den RAR ein; stellen Sie sicher, dass die WAN-Schnittstelle angeschlossen ist. Stecken Sie das USB-Laufwerk in den USB-Anschluss von RAR.
9. Die LED ACT blinkt blau. Sobald sie nicht mehr blinkt, ist die Konfiguration abgeschlossen und das Laufwerk kann entfernt werden.
10. Das neue Gerät wird in der Fleet Manager Bereich der RAP mit einem hervorgehobenen Hintergrund angezeigt. Klicken Sie mit der linken Maustaste auf das neue Gerät (Abb. 36).
11. Kreuzen Sie das Kästchen an, wählen Sie einen Namen und "Aktivieren Sie das Gerät", um die Registrierung des Geräts abzuschließen (Abb.37).
12. Das Gerät wird nun automatisch im RAP angezeigt, bis es abgemeldet wird. (Abb. 38).

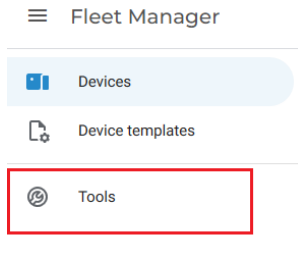


Abb. 31 Wählen Sie
Tools aus dem
Hauptmenü des Fleet
Managers.

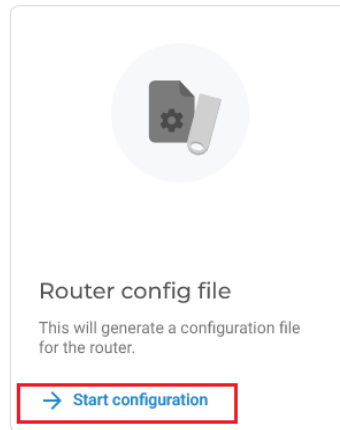


Abb. SEQ Screenshot *
ARABIC 32 SEQ Screenshot
* ARABIC Wählen Sie die
Option zum Starten der
Konfiguration.

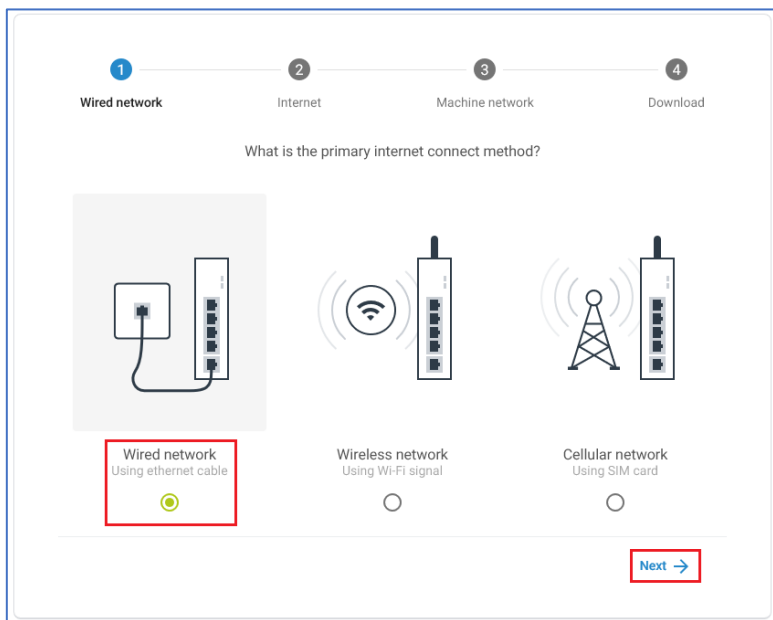
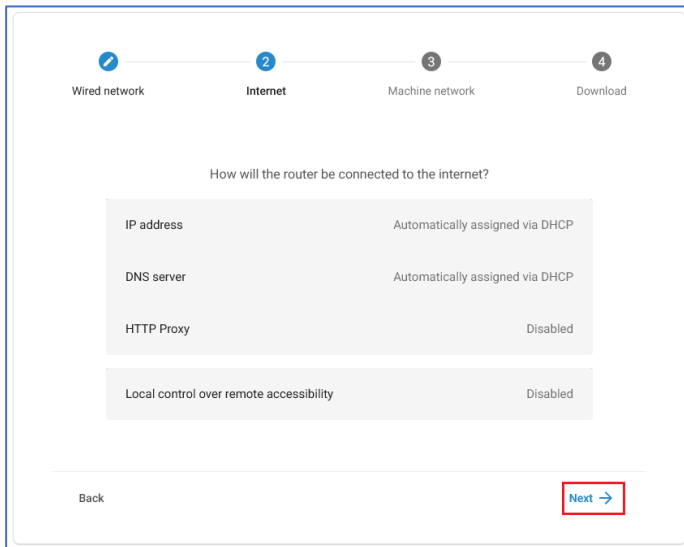


Abb. 32 Wählen Sie die WAN-Schnittstelle aus.



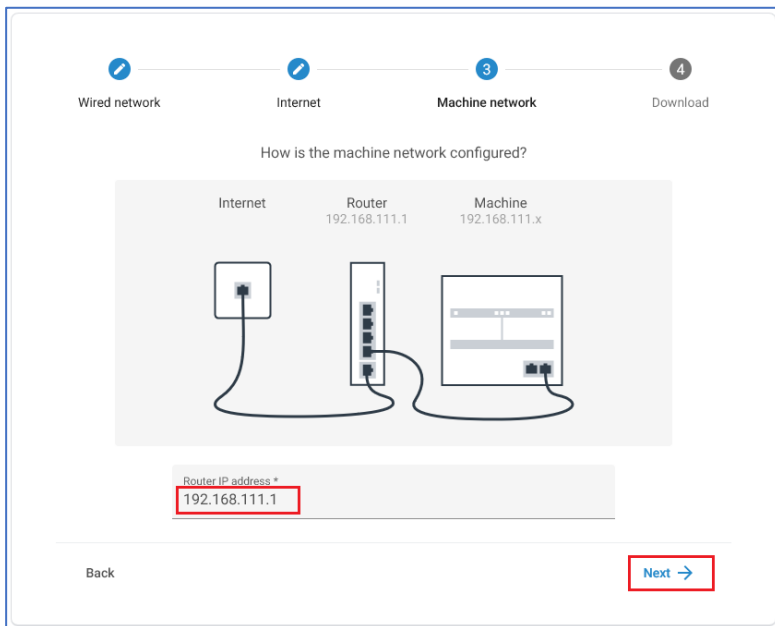
Wired network Internet Machine network Download

How will the router be connected to the internet?

IP address	Automatically assigned via DHCP
DNS server	Automatically assigned via DHCP
HTTP Proxy	Disabled
Local control over remote accessibility	Disabled

Back Next →

Abb. 33 Übernehmen/Ändern Sie die Einstellungen der WAN-Schnittstelle.



Wired network Internet Machine network Download

How is the machine network configured?

Internet Router 192.168.111.1 Machine 192.168.111.x

Router IP address *

192.168.111.1

Back Next →

Abb. 34 Konfiguration der LAN-Schnittstelle.

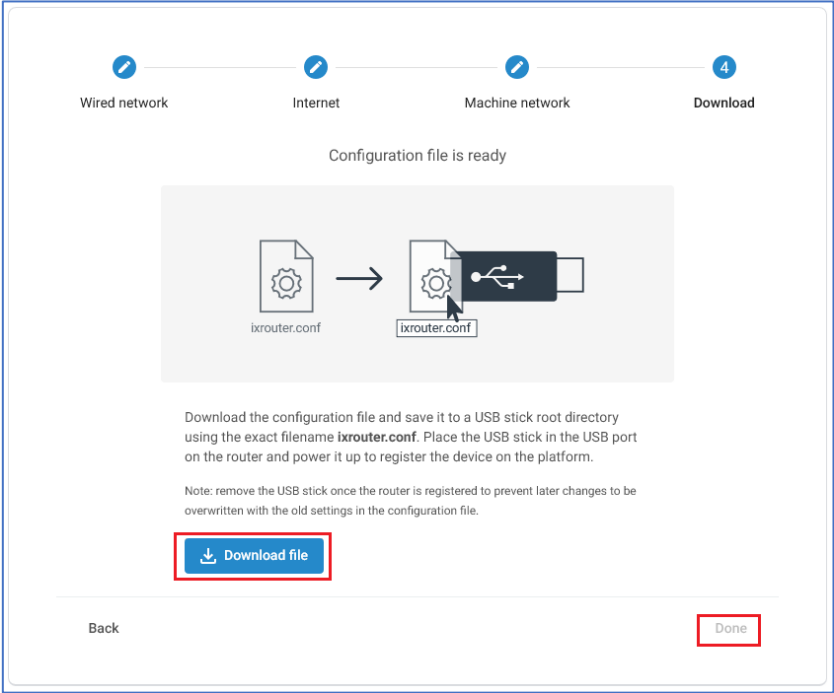


Abb. 35 Laden Sie die RAR-Konfigurationsdatei herunter.

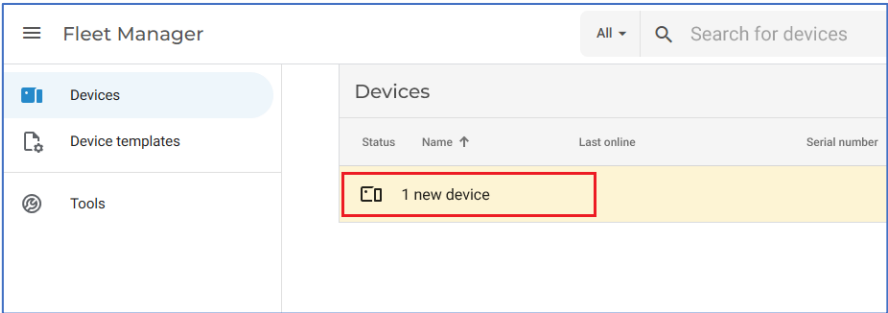


Abb. 36 Klicken Sie mit der linken Maustaste auf New Device

Activate new devices

Search

New devices	Name	Template	Groups
 C0:D3:91:31:BB:4B - 17079280 Remote Access Router	Name * 	Template ▼	Groups ⋮

Cancel

Activate device

Abb.37 Aktivieren Sie das neue Gerät über den RAP.

Fleet Manager

All ▼
 Search for devices





Devices

Device templates

Tools

Devices

Status	Name ↑	Last online	Serial number	MAC address	Firmware version	
●	RAR Ken	Now	17079280	C0:D3:91:31:BB:4B	3.21.1	 Connect

Abb. 38 Nach der Registrierung des Geräts wird der aktuelle VPN-Status des Geräts in der RAP-Hauptschnittstelle angezeigt.

5.3.3 Router für Fernzugriff über WIFI WAN

Siehe Verfahren in 5.3.2.

- Wählen Sie in Schritt 3 (die Art der Internetverbindung auswählen) "Drahtloses Netzwerk" als Methode für den Internetzugang (Abb. 39).
- Geben Sie die SSID und das Passwort des WIFI ein, das den Internetzugang bereitstellen soll (Abb. 40).
- Einrichtungsverfahren vervollständigen gemäß Abschnitt 5.3.2.

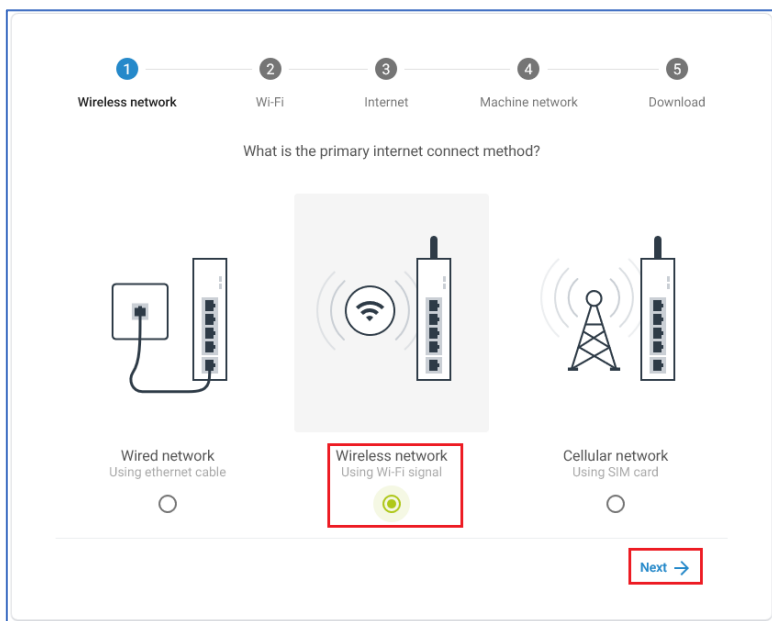
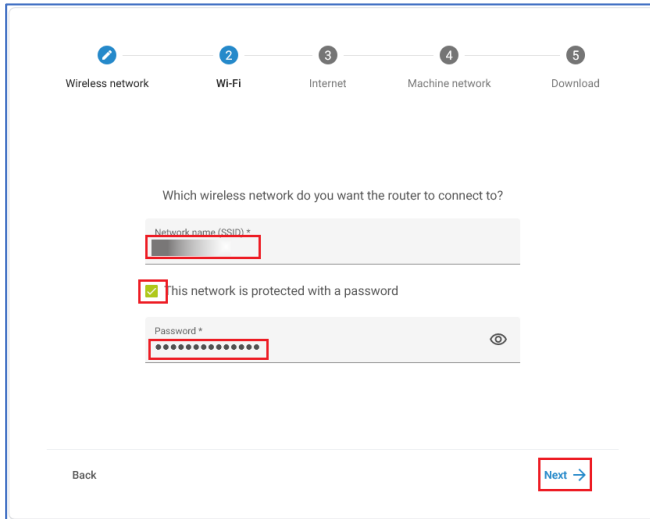


Abb. 39 Wählen Sie die Internetverbindungsmethode aus: „Drahtlos“.



The screenshot shows a five-step progress bar at the top: 1. Wireless network (blue), 2. Wi-Fi (blue), 3. Internet (grey), 4. Machine network (grey), 5. Download (grey). Below the progress bar, the text reads: "Which wireless network do you want the router to connect to?". There are two input fields: "Network name (SSID) *" and "Password *". The "Network name" field contains a redacted value. Below the "Network name" field, there is a checkbox with a green checkmark and the text "This network is protected with a password". The "Password" field contains a redacted value. At the bottom left, there is a "Back" button. At the bottom right, there is a "Next →" button.

Abb. 40 Geben Sie die WIFI-Zugangsdaten für das Host-Netzwerk an.

5.3.4 Fernzugriffsrouter mit 3G/4G WAN

Siehe Verfahren in Abschnitt 5.3.2.

- Wählen Sie in Schritt 3 (die Art der Internetverbindung auswählen) „Mobilfunknetz“ als Methode für den Internetzugang (Abb. 41).
- Geben Sie die „SIM Karte APN“ und den „SIM Karte PIN code“ ein. Diese Angaben können beim Netzbetreiber angefordert werden (Abb. 42).
- Einrichtungsverfahren vervollständigen gemäß Abschnitt 5.3.2.

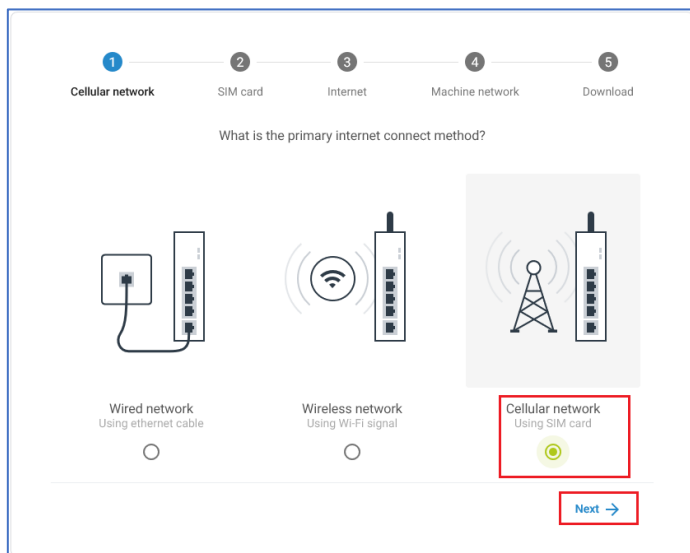


Abb. 41 Wählen Sie die Internetverbindungsmethode: „Mobilfunknetz“.

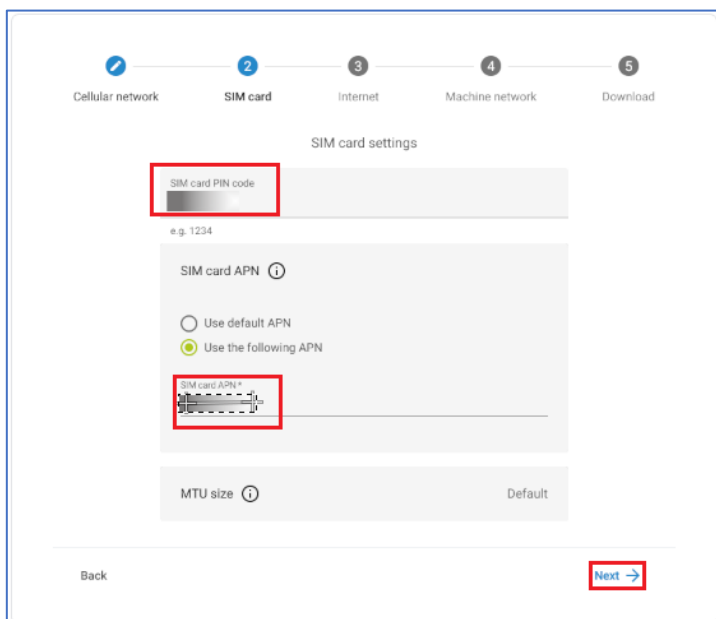


Abb. 42 Geben Sie die Daten der SIM-Karte ein.

5.3.5 Eingebettete Fernzugriff

Dieser Abschnitt gilt nur für die eingebettete Softwarelösung RAE100. Der RAE100 muss zuvor installiert worden sein; dieses Verfahren wird im Abschnitt 4 beschrieben.

Bei der ersten Verwendung muss die RAE-fähige Steuerung bei RAP registriert werden:

1. Führen Sie über die Remote-CLI den Befehl "ixagent Register companyID" aus Abb. 43). Die RAP-Firmen-ID finden Sie auf der RAP-Oberfläche unter „Identity“. APPS Menü -> Admin-> Identity (Abb. 44).
2. Die erfolgreiche Registrierung wird durch eine Rückmeldung im Command Line Feedback bestätigt (Abb. 45).
3. Das neue Gerät wird dann in der Fleet Manager-Hauptschnittstelle mit einem hervorgehobenen Hintergrund angezeigt. Klicken Sie mit der linken Maustaste auf das neue Gerät (Abb. 36).
4. Kreuzen Sie das Kästchen an, wählen Sie einen Namen und "Aktivieren Sie das Gerät", um die Registrierung des Geräts abzuschließen (Abb.37).
5. Für ein RAE-Gerät wird ein Aktivierungscode benötigt (Abb. 46).



Einen Aktivierungscode können Sie von Ihrem SIGMATEK-Vertreter erwerben.

6. Das Gerät wird nun automatisch im RAP angezeigt, bis es abgemeldet wird. (Abb. 38).



Sollte es nicht möglich sein gewisse Dienste wie eine VNC-Verbindung hinzuzufügen, muss man unter dem Menüpunkt ‚Network‘ im Bereich ‚LAN‘ eine IP-Adresse und Netzwerkmaske hinzufügen. Diese sind frei wählbar.

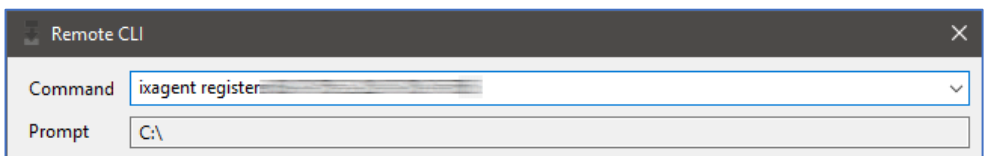


Abb. 43 Ausführen des Register Befehls im Remote-CLI.

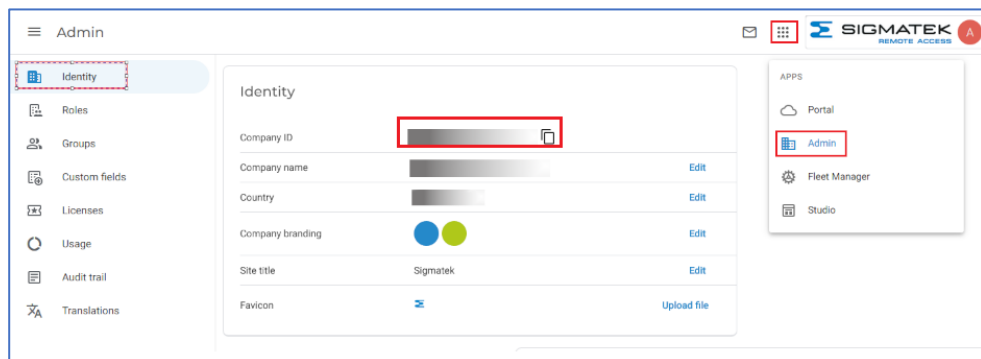


Abb. 44 Die Firmen-ID wird unter RAP>Benutzer>Mein Unternehmen angezeigt.

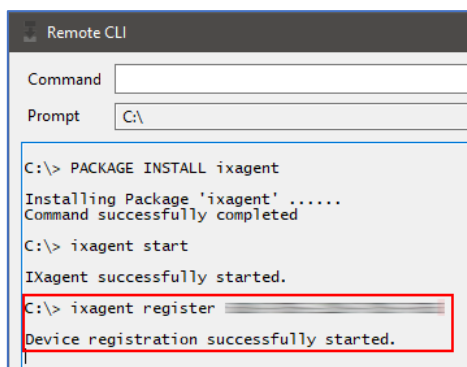


Abb. 45 Bestätigung der erfolgreichen Registrierung.

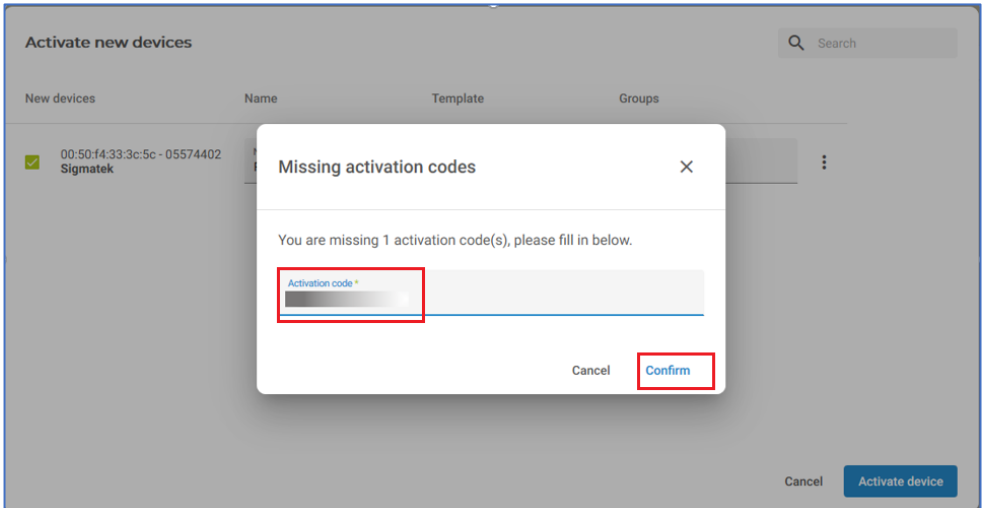


Abb. 46 Aktivierungscode für RAE benötigt

5.4 Zusätzliche Netzwerkeinstellungen (nur RAR)

Durch Klicken auf ein RAR-Gerät, das im APPs-Menü -> Fleet Manager aufgelistet ist, sind mehrere Netzwerkoptionen verfügbar.

In der RAR LAN-Konfiguration ist es möglich:

- Ein zusätzliches Subnet hinzufügen
- Statische IP-Leases zuweisen
- Ändern des IP-Adresszuweisungspools des DHCP-Servers
- Quell NAT aktivieren/deaktivieren

Beispiel: um dem Router eine zusätzliche Subnetzmaske zuzuweisen:

1. Im Fleet Manager des RAPS, wählen Sie ein RAR-Gerät aus. Die Gerätekonfigurationsseite wird dann geöffnet (Abb. 47).
2. Gehen Sie im RAR-Menü auf Network->LAN und wählen Sie auf dem Bildschirm rechts „Add additional subnet“ (Abb. 48).
3. Es öffnet sich ein neues Fenster (Abb. 49) für die neuen LAN-Einstellungen. In der Regel ist das Gateway die LAN-IP-Adresse des RAR-Routers. Geben Sie die gewünschten Subnet-Einstellungen ein und klicken Sie auf "ADD".

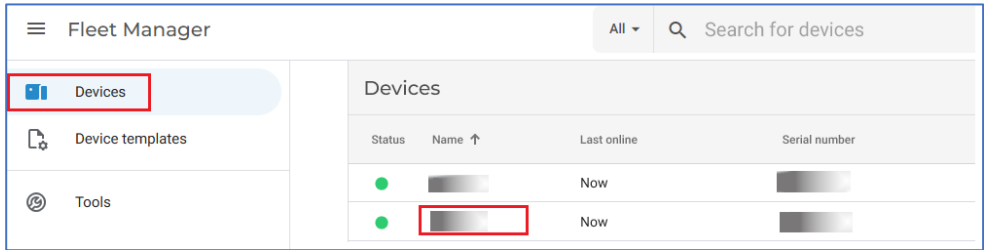


Abb. 47 Öffnen Sie die Seite Gerätekonfiguration.

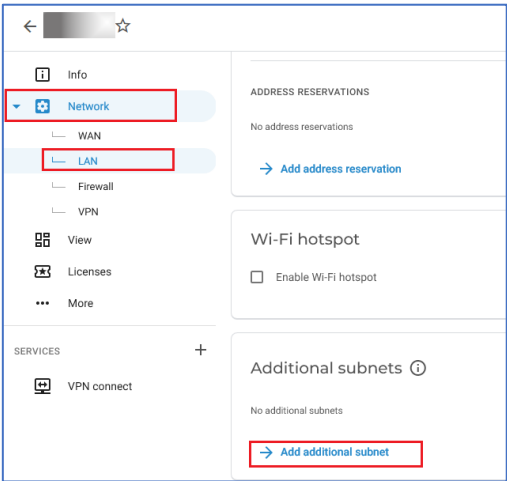


Abb. 48 Bearbeiten Sie die LAN-Konfiguration.

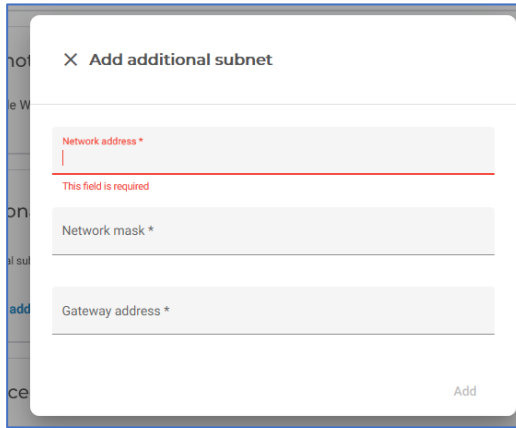


Abb. 49 LAN-Konfigurationseinstellungen bearbeiten

5.5 Zusätzliche Netzwerkeinstellungen (nur RAE)

In einigen Konfigurationen kann es erwünscht sein, einen Fernzugriff auf Steuerungen zu ermöglichen, die mit der Steuerung verbunden sind, auf der RAE läuft.

- Für den Fernzugriff auf die anderen Steuerelemente ist es erforderlich, eine Port-Weiterleitung über die Firewall einzurichten (Abb. 50).
 - Firewall wird von Salamander OS ab 09.03.141 unterstützt. Firewall-Befehle sind in der Lasal OS Dokumentation beschrieben.
1. Verbindung zur Steuerung über LASAL CLASS 2.
 2. Öffnen Sie die Datei Autoexec.lsl mit CLASS 2: DEBUG > FILE TRANSFER > EDIT AUTOEXEC.LSL... Fügen Sie Firewall-Befehle hinzu, um die Weiterleitung und NAT an nachgeschaltete Geräte zu verwalten.
 - a. Beispiel: Die Steuerung mit der IP-Adresse 10.100.3.3 ist mit der Steuerung verbunden, auf der RAE mit der IP-Adresse 192.168.111.20 läuft. Die folgenden Zeilen müssen hinzugefügt werden, um eine VNC-Verbindung weiterzuleiten:
 - 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. Speichern Sie die Änderungen und starten Sie die Steuerung neu.

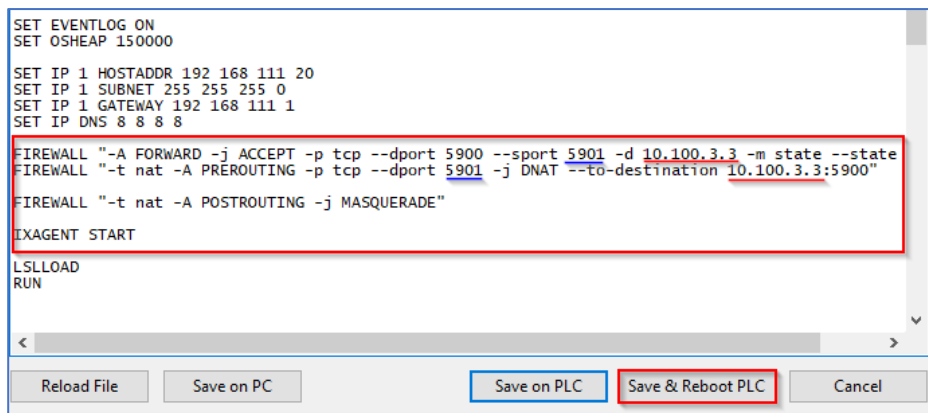


Abb. 50 Autoexec mit Portweiterleitungsbefehlen.

5.6 Remotedienste einrichten

Vor der Konfiguration von Remote Services muss das Gerät bei RAP registriert werden.

5.6.1 Herstellung einer VPN-Verbindung

Eine VPN-Verbindung setzt voraus, dass der RAR/RAE mit Strom versorgt wird und eine Internetverbindung besteht. Verfügbare Geräte sind in der RAP-Schnittstelle mit einem grünen Punkt neben ihrer Bezeichnung gekennzeichnet.

Um eine VPN-Verbindung zwischen dem RAR/RAE und dem aktuellen PC herzustellen:

1. Der VPN TUN-Adaptertreiber muss installiert sein.
 - a. Dies kann über Fleet Manager → Tools → "VPN Client" heruntergeladen werden (Abb. 51).
 - b. Optionale Einstellungen sind auch über die RAR-Konfigurationsseite unter Network->VPN verfügbar:
 - i. Client-Protokollmodus
 - ii. Stealth-Modus: Unterstützung für restriktive Netze. Zusätzlich zur Verschlüsselung werden die Daten unkenntlich gemacht. Die meisten Firewalls sind dann nicht in der Lage, die Art des Datenverkehrs zu erkennen.
 - iii. Proxyserver
2. Wählen Sie das RAR Gerät entweder aus die „Fleet Manager“ Seite oder der Hauptschnittstelle der „Portal“.
3. „Connect“ klicken (Abb. 52).
4. Sobald das Gerät angeschlossen ist, leuchtet eine blaue Statusanzeige (Abb. 53).
5. Windows und Software können nun über TCP/IP mit Geräten, wie z. B. SIGMATEK-Steuerungen, die an den RAR angeschlossen sind, kommunizieren.

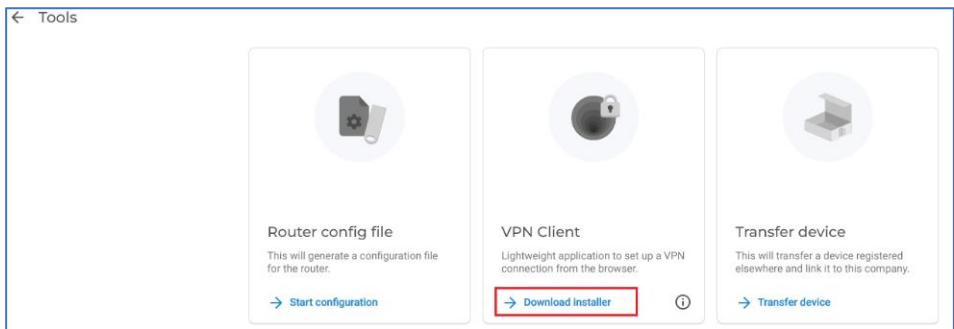


Abb. 51 Der Cloud-VPN-Client kann von der Seite RAP>Tools heruntergeladen werden.

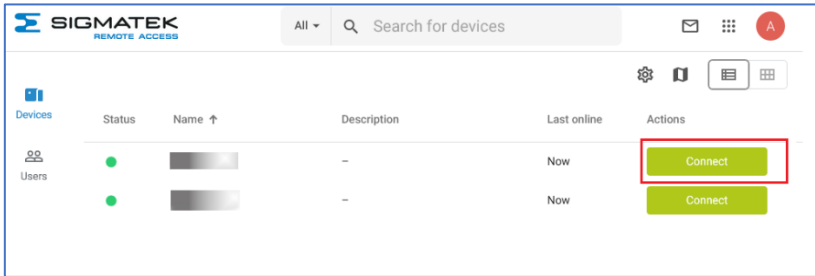


Abb. 52 Jedes Gerät verfügt über eine VPN-Verbindungstaste, um eine sichere Kommunikation herzustellen.

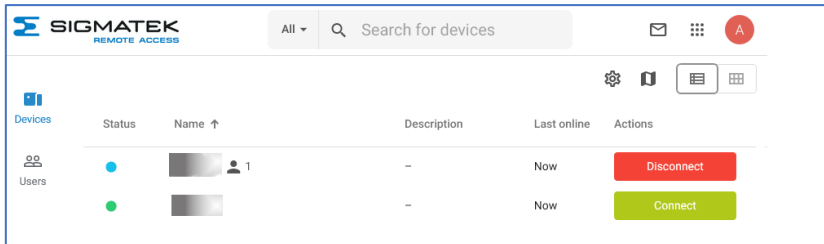


Abb. 53 Nach dem Aufbau einer VPN-Verbindung leuchtet die Gerätestatusanzeige blau.

5.6.2 VNC über VPN

Mithilfe eines VNC-Viewers ist es möglich direkt auf den Bildschirm des HMI zuzugreifen und mit diesem zu interagieren.



Die Aktivierung des VNC-Dienstes auf einer SIGMATEK-Steuerung wird in der Schulungsunterlage LASAL REMOTE SERVICES beschrieben.

Sobald VNC auf der Steuerung aktiviert ist, sollte es über eine lokale Verbindung getestet werden. Wenn die Betriebsbereitschaft bestätigt ist, folgen Sie der Anleitung zur Aktivierung des VNC-Viewer-Dienstes in der Remote Access Plattform.

5.6.2.1 VNC-Einrichtung

1. Über das APPs-Menü → Fleet Manager und Anklicken des entsprechenden Remote-Geräts
2. Klicken Sie auf die Schaltfläche "+" dann „Services (Abb. 54).
3. Vergeben Sie einen Namen für den Gerätedienst und geben Sie die IP-Adresse des Ziels an (Abb. 55). Für die RAE wird die IP-Adresse automatisch als "localhost" angegeben.
4. Ändern Sie bei Bedarf den Anschluss, um ihn an die tatsächliche Einrichtung anzupassen.
5. Ein neuer VNC-Service ist nun unter der Reiter Services aufgelistet (Abb.56).
6. Schließen Sie den Vorgang ab:
 - a. RAR
 - i. Auf ADD klicken.
 - ii. Push config to Device zur Synchronisation (Abb. 57).
 - b. RAE: klicken Sie auf ADD; die Änderung ist sofort wirksam.

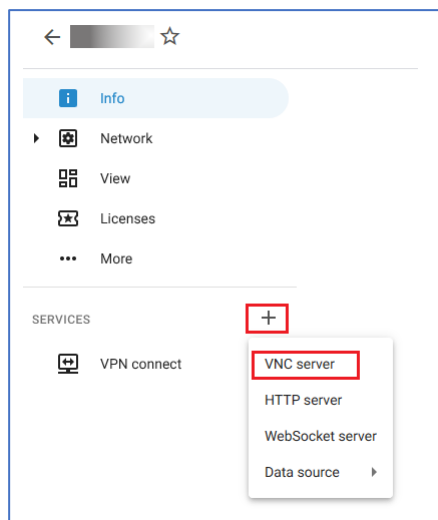


Abb. 54 Hinzufügen eines neuen Dienstes zum Gerät.

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

Abb. 55 Einstellung des Dienstziels nach IP-Adresse.

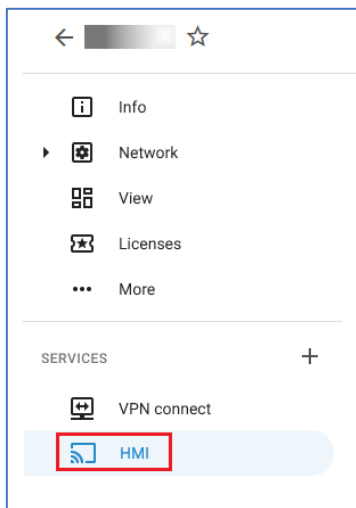


Abb.56 Neue VNC-Service ist gelistet

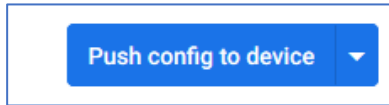


Abb. 57 Push config to device zur Synchronisation (Abb. 58).

5.6.2.2 Mit VNC verbinden

1. Wählen Sie Ihr Gerät aus der Portalseite aus.
2. Wählen Sie unter Web Access das gewünschte VNC aus (Abb. 58).
3. Der Viewer wird im selben Fenster geöffnet; um zur Registerkarte "Info" zurückzukehren, klicken Sie auf das "x" in der linken Ecke (Abb. 59).

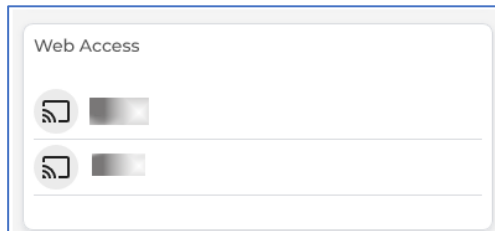


Abb. 58 Das gewünschte VNC unter Web Access auswählen



Abb. 59 Um den VNC-Viewer zu beenden, klicken Sie auf das "x".

5.7 Datenerfassung und -aufbewahrung

5.7.1 Einrichten von Datenquellen

Jede auf einem entfernten Gerät konfigurierte Steuerung kann eine Datenquelle haben; die unterstützten Protokolle für SIGMATEK-Steuerungen sind OPC UA und Modbus TCP.

In den folgenden Abschnitten wird das Hinzufügen von Variablen für beide Protokolle beschrieben.

5.7.1.1 OPC UA

Um nun Daten der Steuerung aufzeichnen oder verwerten zu können muss die Steuerung die Daten der RAP zur Verfügung stellen.

- Wenden Sie sich an Ihren SIGMATEK-Vertreter, um den OPC UA Server und die Lizenz zu erhalten.
- Die Einrichtung von OPC UA wird in der entsprechenden Dokumentation beschrieben.

Um eine OPC UA Datenquelle für den RAP verfügbar zu machen:

1. Zur Erstellung der Datenkarte ziehen Sie die Verwendung eines Dienstprogramms wie UaExpert in Erwägung (Figure 65).
 - a. Fügen Sie die Server hinzu, die in Cloud Logging oder Cloud Notify verwendet werden sollen; die "Node Id" und der Datentyp sind erforderlich.
2. Fügen Sie auf dem RAP einen OPC UA DataSource Service hinzu (Abb. 60).
 - a. "Fleet Manager" -> select Device ->. Klicken Sie auf die Schaltfläche "+" um einen Tag hinzuzufügen.
 - b. Datenquelle und OPC UA auswählen.
 - c. Geben Sie die Zielsteuerung an, die die Datenquelle bereitstellen soll (Abb. 612).
 - i. IP-Adresse der SIGMATEK-Steuerung
 - ii. Legen Sie den Server-Port fest. (Bsp. 4842)
 - iii. Klicken Sie auf „ADD“ (Hinzufügen).
 - d. Das neue Konfigurationsmenü für OPC-UA Datenquellen wird nun unter Dienste aufgelistet und kann erweitert werden (Abb. 62).
3. Klicken Sie auf die Schaltfläche „Add new variable“, um eine Variable hinzuzufügen (Abb. 63)

- a. Der Variable einen Namen zuweisen sowie den Datentyp und die Adresse angeben (Abb. 64). Diese Werte können aus der OPC UA Karte oder mit Hilfe von Software wie UA Expert bezogen werden (Figure 65). Ein Beispiel für die Adresse finden Sie in Abb. 66. Eine Größe und Einheit können auch verwendet werden. Danach klicken Sie auf „ADD“.
- b. Klicken Sie in die Kopfzeile des Konfigurators auf „Push Config to Device“.
- c. Nachdem der Sync abgeschlossen ist, starten Sie einen Test der Datenserververbindung und der Variablenerfassung, indem Sie auf "TESTLAUF" klicken (**Fehler! Verweisquelle konnte nicht gefunden werden.**).



„Push Config to Device“ und „Run Test“ sind nur nach Aktivierung einer Lizenz verfügbar. Dieses Thema wird in Abschnitt 0 erklärt.

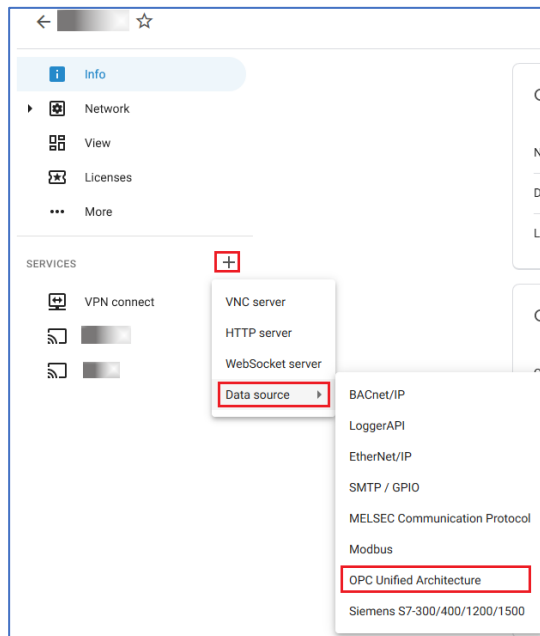


Abb. 60 Fügen Sie dem entfernten Gerät einen neuen Dienst hinzu.

Data source

OPC Unified Architecture

Name *	Identifier *
	CP112_opc

IP address	Port *
192.168.2.100	4842

Authentication type *

Anonymous

Polling sleep time

100 milliseconds (recommended)

Add

Abb. 61 Geben Sie für den Dienst das Ziel an.

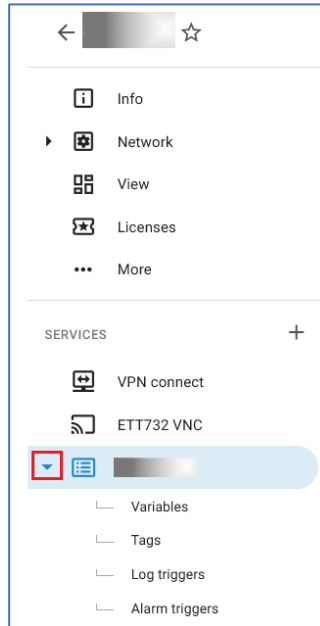


Abb. 62 Die neue OPC UA Datenquelle ist unter Services aufgelistet

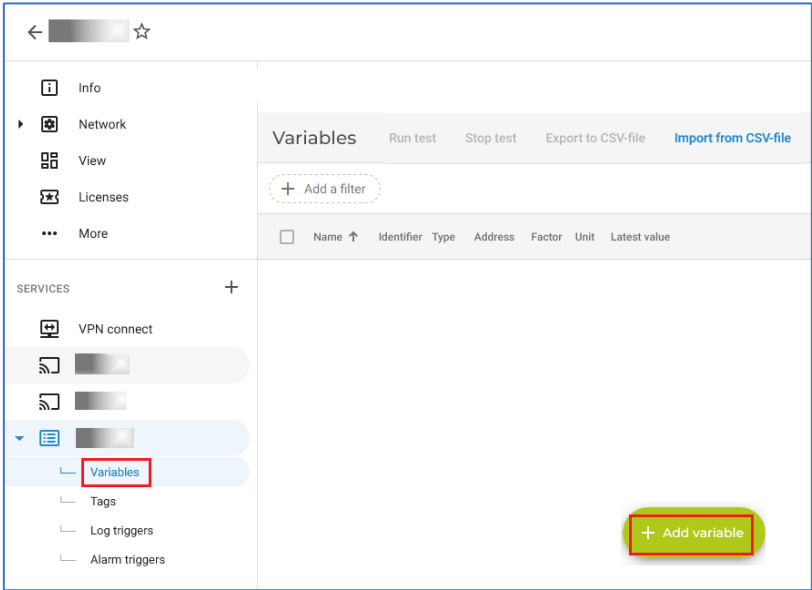


Abb. 63 Das Menü zur Konfiguration der Datenquelle ermöglicht das Hinzufügen von Variablen

Edit variable

Name *

Identifier *

Note: name identifier

Type

Namespace *

Identifier type *

Identifier value *

Note: OPC-UA identifier

Factor

Unit

Remove

Cancel

Confirm

Abb. 64 Geben Sie den Datentyp und die Adresse der Variablen an.

#	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 65 Auffinden der Knoten-ID und des Datentyps in der UaExpert-Datenzugriffsansicht.

Namespace index	Identifizier-Typ	Kennung	Adresse für RAP-Variable
2	Zeichenkette	Vartemp	ns=2;s=vartemp
2	Numerisch	20001	ns=2;i=20001

Abb. 66 Beispiel für die Erstellung des RAP-Variablenbezeichners.

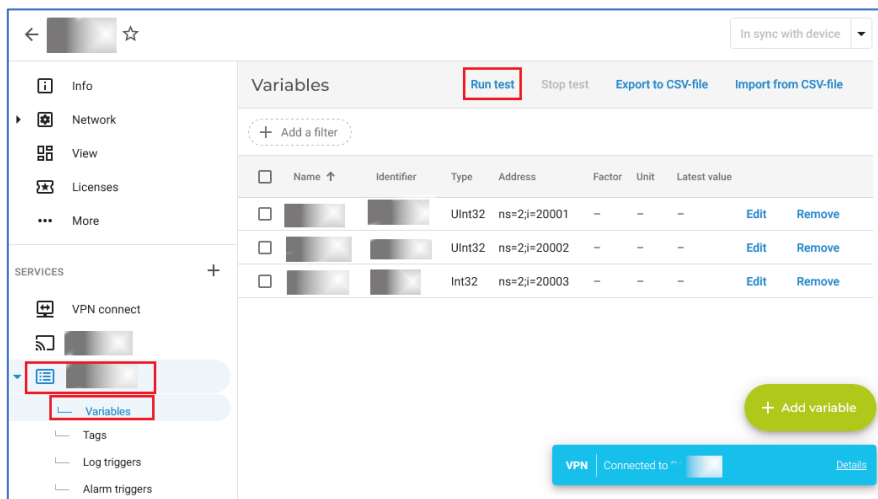


Abb. 68 SEQ Screenshot * ARABIC 68 SEQ Screenshot * ARABIC „Run test“ um die Datenserververbindung und der Variablenerfassung zu testen.

5.7.1.2 Modbus TCP

Um nun Daten der Steuerung aufzeichnen oder verwerten zu können muss die Steuerung die Daten der RAP zur Verfügung stellen.

- Weitere Informationen über den Modbus-Slave finden Sie in der Klassendokumentation.

Der Modbus-Slave muss zu der Steuerung hinzugefügt werden, die die Datenquelle ist:

1. Fügen Sie die Klasse ModbusTCPSlave hinzu. Notieren Sie sich die Portnummer für die RAP-Konfiguration (Abb. 67).
2. Richten Sie die Datenquellen in der Klasse ModbusTableBase ein. Diese Klasse ordnet einen Server einem Modbus-Register zu (Abb. 68).
3. Fügen Sie auf dem RAP einen Modbus DataSource Service hinzu (Abb. 69).
4. Bei der Konfigurierung von Modbus-Einstellungen (Abb. 70 ist Folgendes zu beachten:
 - a. Slave Nummer = 1
 - b. Byte-Reihenfolge = ABCD
5. „Push config to Device“ zur Synchronisation (Abb. 71).

-
- The screenshot displays the 'ModbusTCP Slave' configuration window. The 'cPort' parameter is highlighted with a red box and has a value of 502. Other parameters include 'cTimeout' (0), 'cSizeOfTxBuffer' (0), 'cTable' (0), 'cTableInputReg' (0), 'cBusSize' (1000), 'cBusSizeInputReg' (100), 'cFileOffsetTable' (1), 'cFileSys' (0), 'to_AsciiBin' (0), 'cString' (0), 'cStringInputReg' (0), 'StartAddrOffset' (0), 'StartAddrOffsetInputReg' (0), 'cTurnBytes' (1), 'cSigCLib' (0), 'cSysMsg' (0), and 'Config' (0). The 'DataElement' section shows 'DataElement1' and 'DataElement2' with their respective 'Data' values (0 and 0). The 'Set Modbus-parameter via table' section shows 'ModBusTableBase' and 'ModBusTableBase1' with their respective 'TablePtr' values (0 and 0). The 'ASCII Bin' section shows 'ASCII_Bin1' with its 'Obj_channel' value (0).

```
FUNCTION TAB ModbusTableBase::Table
// Modbus-Address, 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
```

07.08.2023

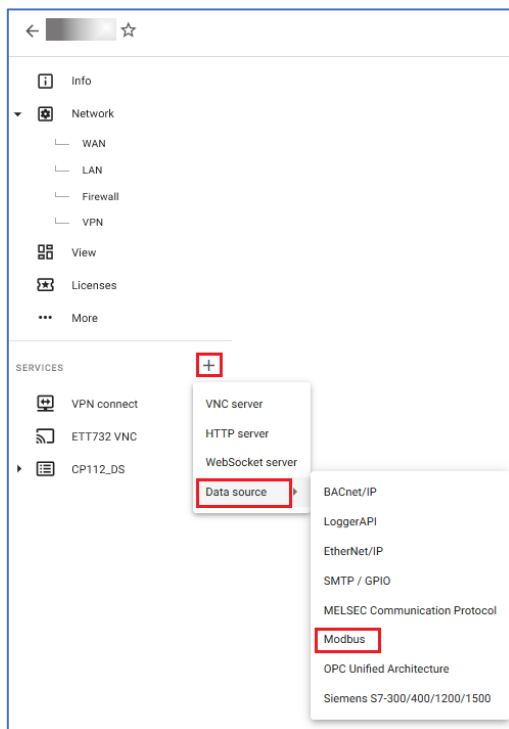


Abb. 69 Einen Datasource Modbus Service hinzufügen

Data source
Modbus

Name *

Identifier *

IP address

Port *
502

Slave
1

Byte order *
ABCD

Polling sleep time
100 milliseconds (recommended)

Add

Abb. 70 Konfigurieren der Datenquelleneinstellungen für Modbus.

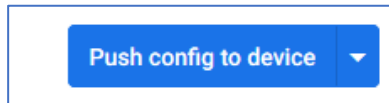


Abb. 71 Push config to device zur Synchronisation.

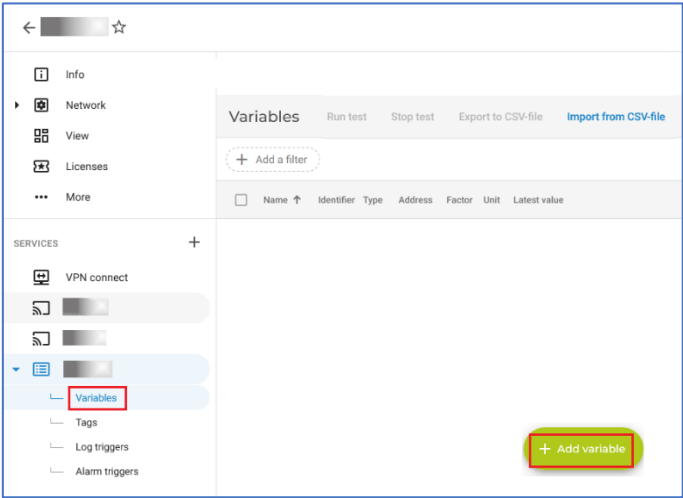
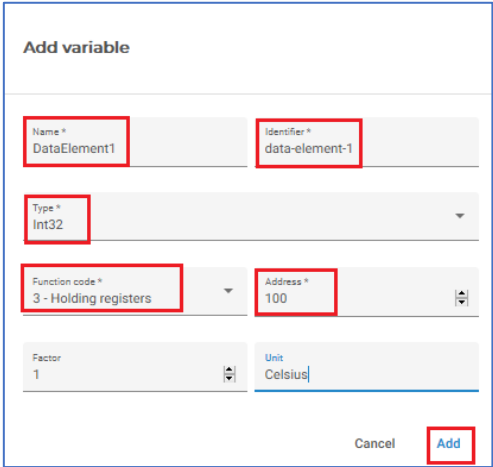


Abb. 72 Variable zur Modbus DataQuelle hinzufügen.



The 'Add variable' dialog box is shown. The following fields are highlighted with red boxes: 'Name *' (DataElement1), 'Identifier *' (data-element-1), 'Type *' (Int32), 'Function code *' (3 - Holding registers), 'Address *' (100), 'Factor' (1), 'Unit' (Celsius), and the 'Add' button.

Abb. 73 Modbus Variable konfigurieren.

5.7.2 Cloud Logging

Das Cloud Logging bietet die Möglichkeit Daten der Steuerung aufzuzeichnen. Diese Daten sind als Reports oder als Live-View einzusehen. Für das Cloud-Logging ist eine Lizenz erforderlich. Aktive Lizenzen werden in Fleet Manager → Device page → Licenses angezeigt (Abb. 74).

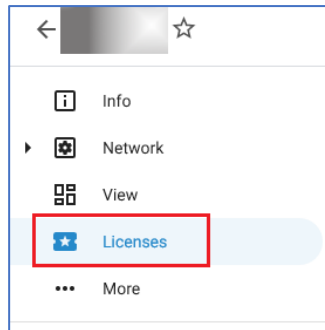


Abb. 74 Lizenzen zum Cloud Logging auf Fleet Manager → Device Page.

1. Eine Lizenz von Ihrem SIGMATEK-Vertreter erwerben.
2. „Cloud Logging“ aktivieren.
3. Wählen Sie die Lizenz (Abb. 75).
4. Neue Aktive Lizenz wird jetzt angezeigt (Abb. 76).



Es gibt die Möglichkeit eine 30-tägige Testversion von Cloud Logging zu aktivieren. Sie kann nur für ein Gerät verwendet werden.

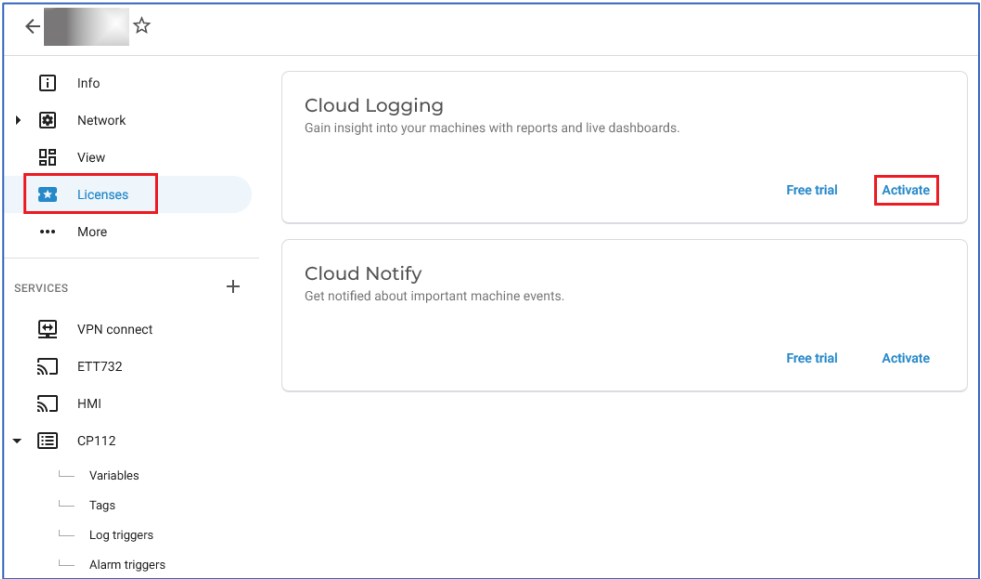


Abb. 75 Aktive Lizenzen für das ausgewählte Gerät

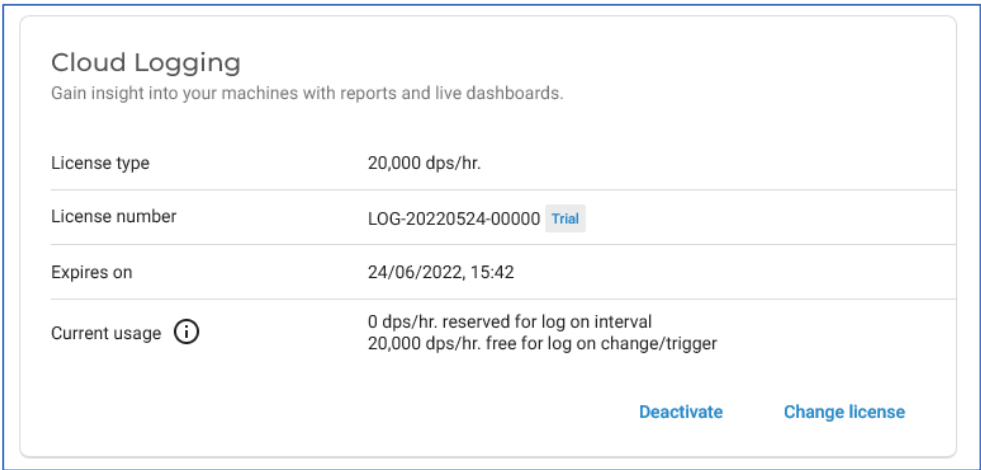


Abb. 76 Die neue aktive Lizenz kann nun angezeigt werden.

5.7.2.1 Datenquellen zu Cloud Logging hinzufügen

Daten-Tags beschreiben, wie Sie Ihre Variablen protokollieren möchten. Sie können sich entschieden, ob die Variablen bei einer Wertänderung in einem statischen Intervall (100 ms - 1 Stunde) aufgezeichnet werden sollen oder mit einem benutzerdefinierten Auslöser. Außerdem definieren Sie, wie lange die Daten gespeichert werden soll.

1. Nach Aktivierung des Cloud-Loggings, öffnen Sie die Tags von Fleet Manager → Device page → Data source menu → Tags. „Add Tag“ klicken (Abb. 77).
2. Geben Sie im Tag-Editor die Datenquelle, das Aufzeichnungsintervall und die Datenaufbewahrungsrichtlinien ein. (Abb. 78).
3. Klicken Sie auf „Add“ (Hinzufügen); die Tags werden dann aufgelistet (Abb. 79). Wiederholen Sie den Vorgang für alle erforderlichen Datenquellen.

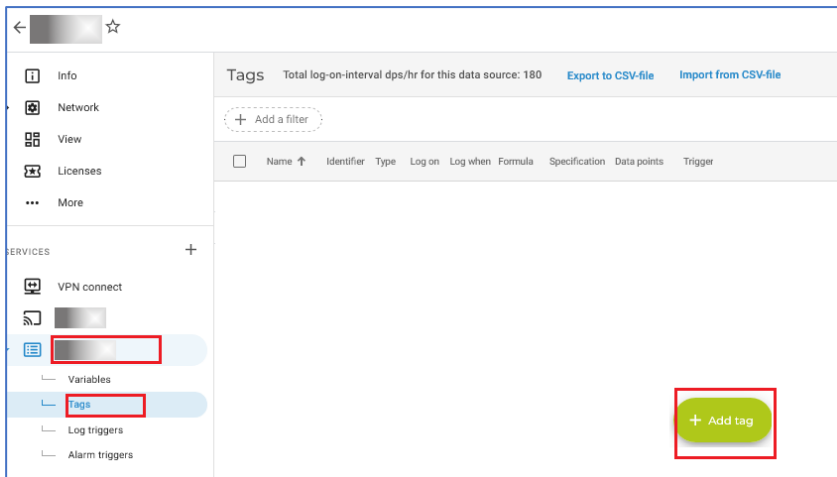


Abb. 77 Tags für Cloud Logging hinzufügen

Add tag

Variable *

Name *

Identifier *

Log on *

Interval

Interval *

Every minute

Formula

Retention policy *

5 years

Cancel

Add

Abb. 78 Schnittstelle zum Tag-Editor.

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

Abb. 79 Die verfügbaren Tags sind aufgelistet.

5.7.3 Eine Seite zur Datenanzeige erstellen

Sie können eine eigene Geräteseite im Cloud Studio anlegen, um Ihren Daten zu visualisieren. Es gibt 2 Möglichkeiten, um Ihre Daten zu visualisieren: Durch Datenberichte, die historische Daten zeigen, und über Live-Überwachung, die Echtzeit-Maschinendaten zeigen.



Die historische und Live-Anzeige von Daten erfordert mindestens einen vorkonfigurierten Datenquellendienst mit Variablen für Live-Daten und Tags für die historische Anzeige, wie in Abschnitt 5.7.1 und Abschnitt 0.

1. Öffnen Sie das Studio-Menü von APPS Menü → Studio.
2. Devices Seiten Option öffnen (Abb. 80).
3. Klicken Sie auf die Schaltfläche "+" um eine neue Geräteseite zu erstellen (Abb. 81). Geben Sie für der Seite einen Namen und Titel.
4. Öffnen Sie die neu erstellte Seite oder eine bereits vorhandene Seite kann geöffnet und bearbeitet werden (Abb. 82).
5. Wählen Sie das Gerät und die Komponente, die hinzugefügt werden sollen (Abb. 83)
 - a. Es gibt elf Komponenten für historische Metriken
 - b. Für Live-Metriken gibt es fünf Komponenten
6. Beispiele (zwei Live-Metriken und zwei historische Metriken):
 - a. Live-Wert Komponente: eine Anzeige der Live-Datenwerte (Abb. 84).
 - i. Eine Live-Wert-Komponente aus der Liste der verfügbaren Komponenten hinzufügen (Abb. 85).
 - ii. Auf die neu hinzugefügte Live-Wert-Komponente klicken und Komponentendetails hinzufügen: Titel, Untertitel und in der Datenquelle klicken Sie auf Bearbeiten (Abb. 86).
 - iii. Auf dem Eingabebildschirm klicken sie auf die Ordneroption (Abb. 87)
 - iv. Wählen Sie die Datenquelle und die Variable aus den verfügbaren Listen aus, wie zuvor im Abschnitt 5.7.1 (Abb. 88).
 - b. Live-Gauge Komponente: eine analoge Anzeige von Live-Datenwerte (Abb. 89).

- i. Wählen Sie die Live-Gauge Komponente aus den verfügbaren Komponentenlisten aus (Abb. 83).
 - ii. Auf die neu hinzugefügte Live-Gauge Komponente klicken und Komponentendetails hinzufügen: Titel, Untertitel und in der Datenquelle klicken Sie auf Bearbeiten (Abb. 86).
 - iii. Gauge-Bereich hinzufügen und auf dem Eingabebildschirm auf die Ordneroption klicken (Abb. 90).
 - iv. Wählen Sie die Datenquelle und die Variable aus, wie zuvor im Abschnitt 5.7.1 konfigurierte Gerätdaten Quelle (Abb. 88).
 - c. Liniendiagramm-Komponente: zur Darstellung von Trends in einer Datenquelle (Abb. 91).
 - i. Fügen der Liniendiagramm Komponente aus der Liste der verfügbaren Komponenten hinzu (Abb. 83).
 - ii. Auf die neu hinzugefügte Liniendiagramm-Komponente klicken und Komponentendetails hinzufügen: Title, Untertitle, Achsbereich und Add Line klicken (Abb. 92).
 - iii. Liniendetails hinzufügen und auf Tag klicken (Abb. 93).
 - iv. Wählen Sie die Datenquelle und die Variable aus den verfügbaren Listen aus, wie zuvor im Abschnitt 5.7.2.1 (Abb. 94).
 - d. Zeitraum-Balkendiagramm: Balkendiagramm für Daten in einem spezifischen Intervall (Abb. 95).
 - i. Fügen Sie das Zeitraum-Balkendiagramm aus der Liste verfügbarer Komponenten (Abb. 83).
 - ii. Auf die neu hinzugefügte Zeitraum-Balkendiagramm Komponente klicken und Komponentendetails hinzufügen: Title, Untertitle, Y-Achsbereich, Aufzeichnungsabstand Balkenstil und auf Add Bar klicken (Screenshot 96).
 - iii. Fügen Sie Liniendetails und Tag hinzu (Abb. 97).
 - iv. Wählen Sie die Datenquelle Dienst und Tag wie sie in Abschnitt 5.7.2.1 (Abb. 94) konfiguriert ist.
 - e. Layout Beispiel (Abb. 98).
7. Nach Abschluss der Konfiguration müssen die Änderungen durch Anklicken der Registerkarte „Publish“ an das Gerät übertragen werden. Sie können einen Entwurf

auch verwerfen, indem Sie auf die drei Punkte klicken und "Revert to a Published version" wählen (Abb. 99).

8. Um dem Gerät eine Seite hinzuzufügen, gehen Sie zu Fleet Manager → Gerät → Ansicht → „Seite hinzufügen“ (Abb. 100).
9. Wählen Sie Seite und Kategorie und klicken auf Hinzufügen (Abb. 101).
10. Die neue Seite wird nun online im Portal → Gerät angezeigt. Die Navigation zwischen den Seiten ist auch über die Geräteseite im Portal möglich (Abb. 102).

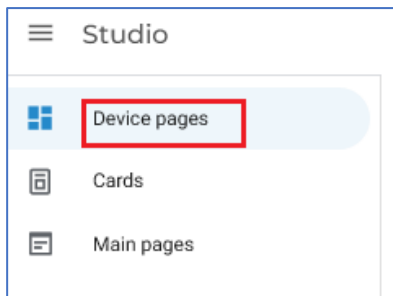


Abb. 80 "Studio → Geräteseiten" um Datenpunkte and Live-Überwachung für Geräte in der Cloud zu erstellen.

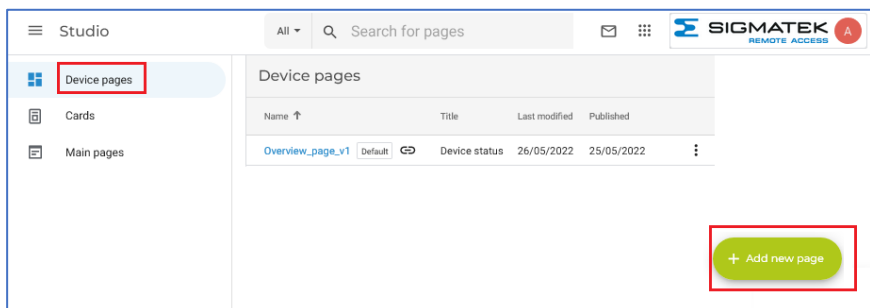


Abb. 81. Erstellen Sie eine neue Seite, indem Sie auf die Schaltfläche "+" klicken.

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

Abb. 82 Wählen Sie eine Seite, um Datenberichte oder Live-Daten hinzuzufügen

← 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

Abb. 83 Datenberichte (historisch) oder Live-Überwachung können für ein bestimmtes Gerät hinzugefügt werden

Seite 68

07.08.2023

Counter
8,263,710

Abb. 84 Beispiel für die Komponente Live-Value.

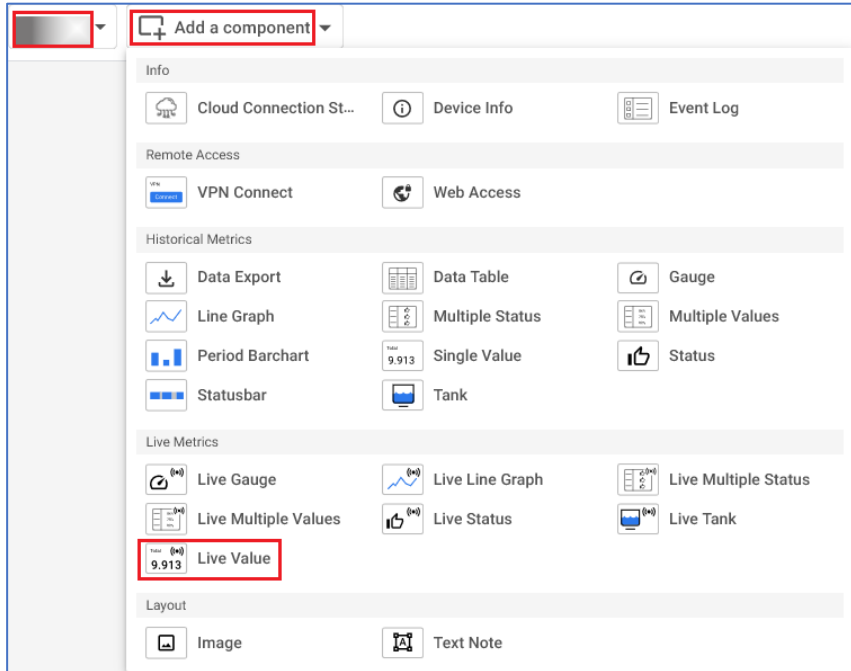


Abb. 85 Eine Komponente hinzufügen -> Live-Value

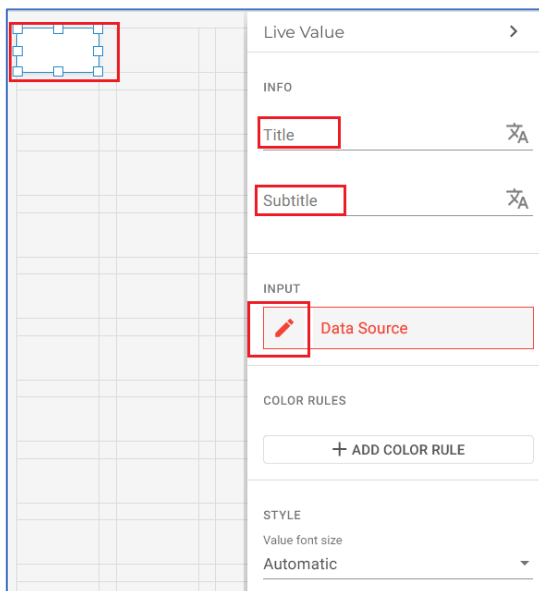


Abb. 86 Live-Value Details hinzufügen

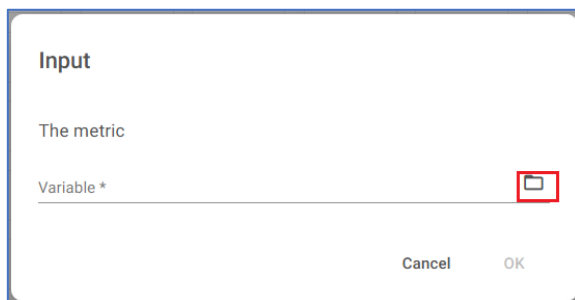


Abb. 87 Ordner zum Bearbeiten der Datenquelle anklicken

A dialog box with a light gray background and a blue border. It contains two input fields, each with a dropdown arrow on the right. The first field is labeled "Data source *" and the second is labeled "Variable *". Both fields have a small gray rectangle to the left of the text. At the bottom right, there are two buttons: "Cancel" and "OK". The "OK" button is highlighted with a red border.

Abb. 88 Datenquelle und Variable hinzufügen

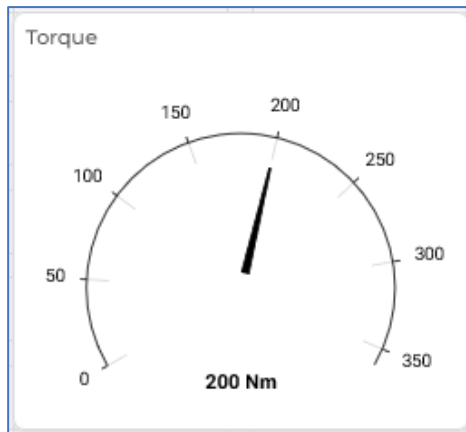


Abb. 89 Beispiel Live-Gauge Komponente.

Input

Metric

Variable

Min *

Max *

CancelOK

Abb. 90 Add Live-Gauge Bereich Werte und Dataquelle Variable

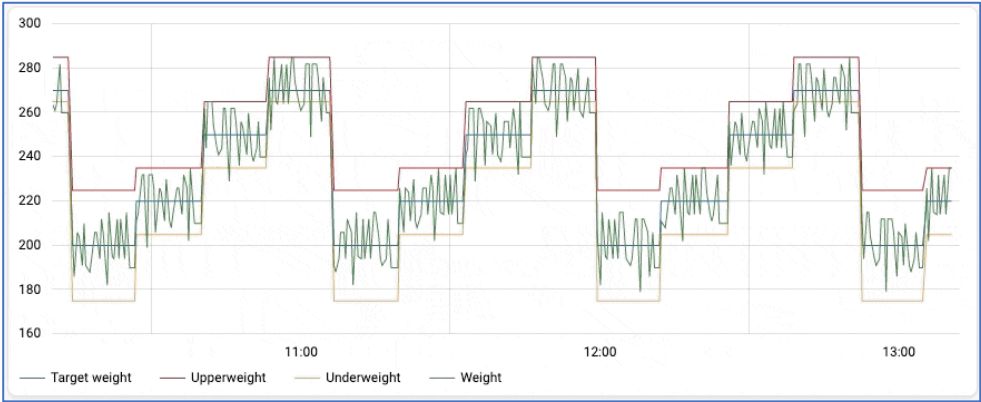


Abb. 91 Beispiel Liniendiagramm Komponente.

Line Graph >

INFO

Title 

Subtitle 

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

Abb. 92 Liniendiagrammdetails, Achsenwerte und Linie hinzufügen

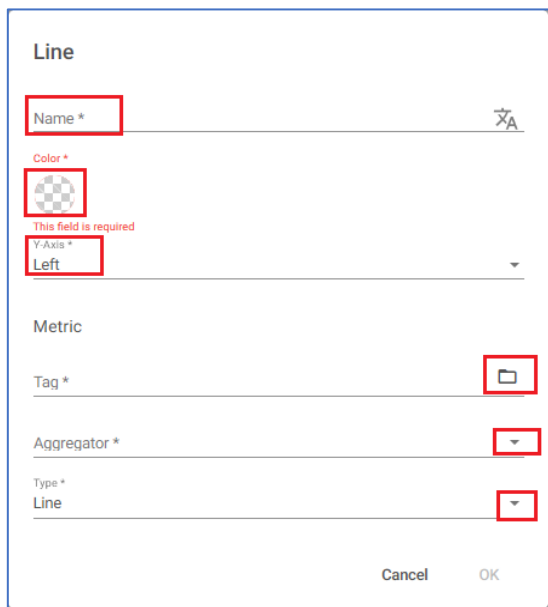


Abb. 93 Liniendetails konfigurieren und Tag hinzufügen

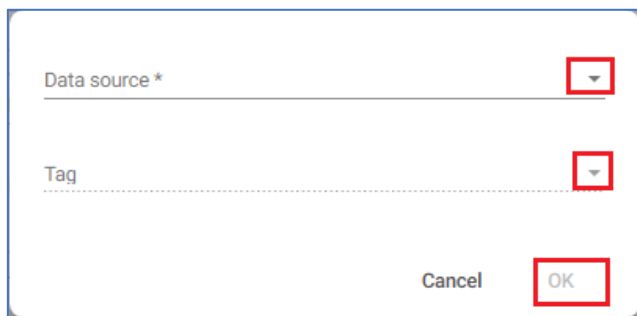


Abb. 94 Datenquelle und Tag hinzufügen

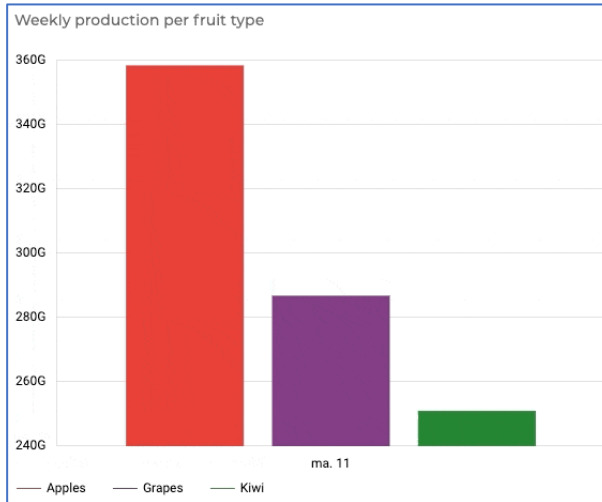


Abb. 95 Beispiel Zeitraum Balkendiagramm

Period Barchart

>

INFO

Title

✕A

Subtitle

✕A

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 96 Zeitraum Balkendiagram Details

Bar

Name *

Color *

This field is required

Metric

Tag *

Aggregator *

Cancel

OK

Abb. 97 Balkendetails konfigurieren und Tag hinzufügen

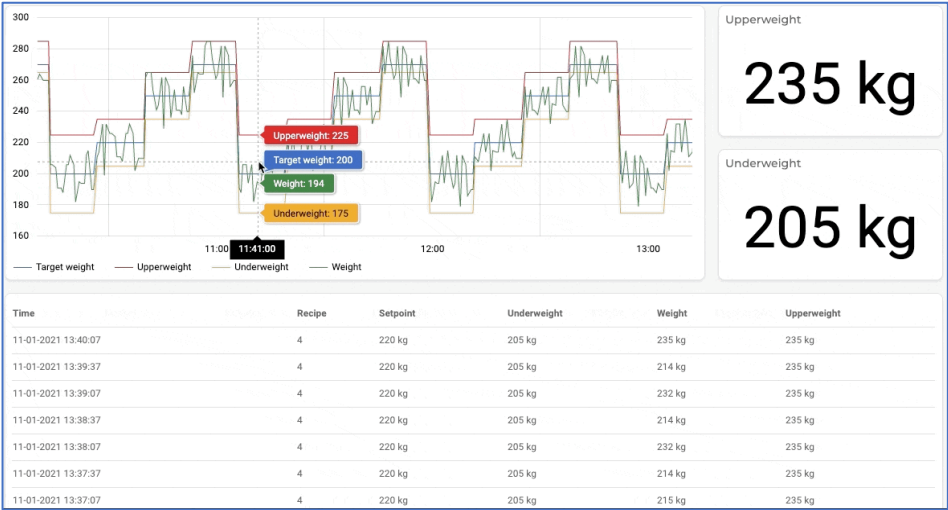


Abb. 98 Beispiel einer Überwachungsseite mit den Komponenten
Liniendiagramm, Wert und Datentabelle

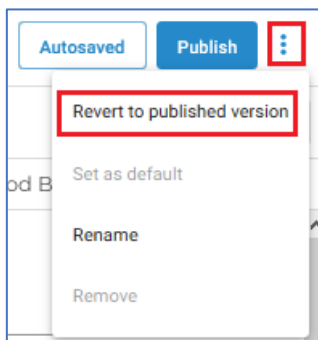


Abb. 99 Es ist möglich auf eine veröffentlichte Version zurückzugreifen.

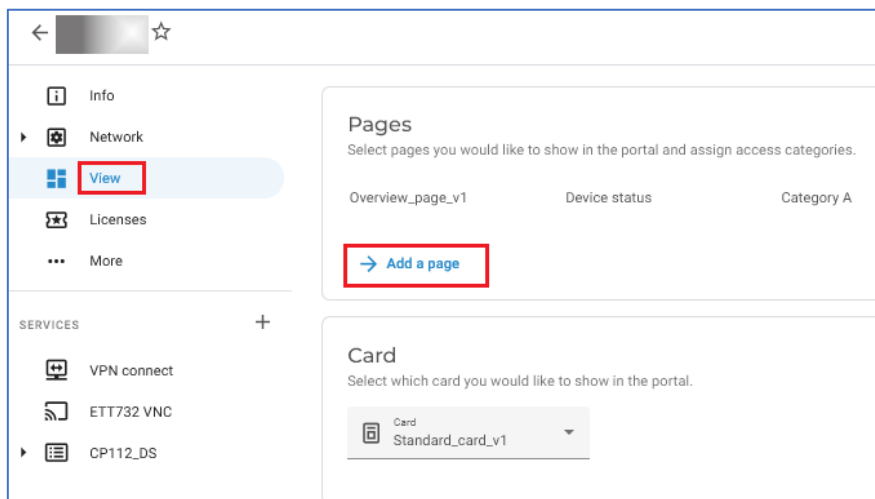


Abb. 100 Fleet Manager → Device → View → “Add page” um dem Gerät eine Seite hinzufügen.

X Add a page

Page *

Access category *
Category A

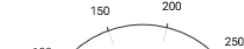
Cancel Add

Abb. 101 Geräteseite hinzufügen

Device status
First Dashboard


SIGMA TEK

Web Access
 ETT732 VNC

Torque


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

Abb. 102 Navigation zwischen Seiten von Portal->Device ist möglich.

5.7.4 Cloud-Benachrichtigungen

Die Cloud-Benachrichtigungen bieten die Möglichkeit Benachrichtigungen über wichtige Maschinen-Events aufzuzeichnen und diese auch per E-Mail zu verschicken.

Für Cloud-Benachrichtigungen ist eine Lizenz erforderlich; aktive und verfügbare Lizenzen werden im Apps Menü → Fleet Manager → Device → Licenses (Abb.103) angezeigt.

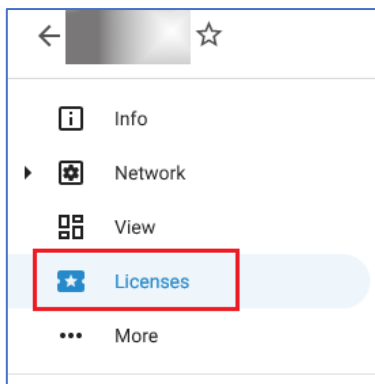


Abb.103 Licenses klicken, um auf die Gerätlizenzen Seite zu gelangen.

5.7.4.1 Cloud-Benachrichtigungen aktivieren

1. Eine Lizenz von Ihrem SIGMATEK-Vertreter erwerben.
2. Activate Cloud Notify über Licenses (Abb. 104).
3. Aktivierungscode eingeben und aktivieren (Abb. 105).
4. Benachrichtigung über Fleet Manager hinzufügen → Device → More(...) → Benachrichtigung hinzufügen (Abb. 106).
5. Wählen Sie die betreffende Verbindung aus, geben Sie die Alarmdetails ein und drücken Sie auf Add (Abb. 107).

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

Abb. 104 Cloud Notify über Licenses aktivieren.

Activate Cloud Notify

Activation code *

This field is required

Cancel
Activate

Abb. 105 Aktivierungscode eingeben und Activate klicken

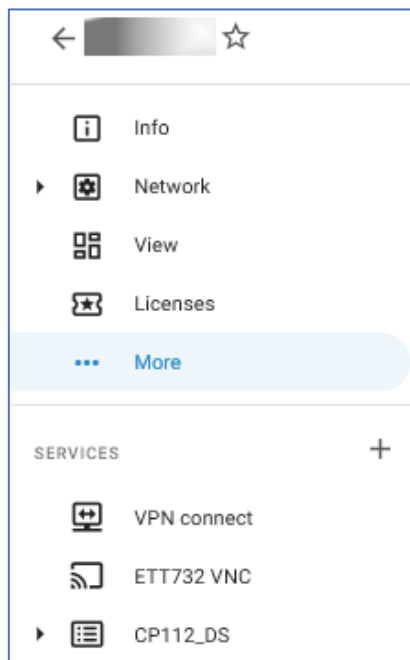


Abb. 106 Benachrichtigung über Fleet Manager hinzufügen → Device → More
(...) → Add notification

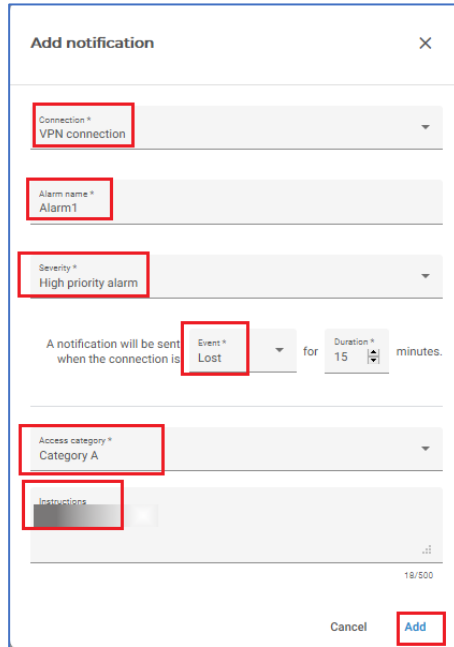


Abb. 107 Benachrichtigung Details eingeben

5.7.4.2 Cloud-Benachrichtigungen einrichten

1. Dataquelle Service einrichten: siehe Abschnitt 5.7.1.
2. Alarmer einrichten:
 - a. In Fleet Manager → Select device → Data Service → Alarm triggers → Add trigger (Abb. 108).
 - b. Die Quelle und die Parameter für den Alarm-Tigger einstellen und Add klicken (Abb. 109);
 - i. Name
 - ii. Schweregrad
 - iii. Wegbedingung
 - iv. Schwellenwert oder Variable
 - v. Periodenzeit
 - vi. Befehle
 - vii. Zugriffskategorie

- c. Der neue Alarm wird im Fleet Manager → Select device → Data Service → Alarm triggers angezeigt. “Push config to device” klicken (Abb. 110).
3. Einrichtung von Empfängern aus den Alarmen (Abb. 111):
 - a. Die Empfänger müssen als Gerätebenutzer registriert sein.
 - b. Über das Apps Menü → Admin → roles → auf add category access klicken.

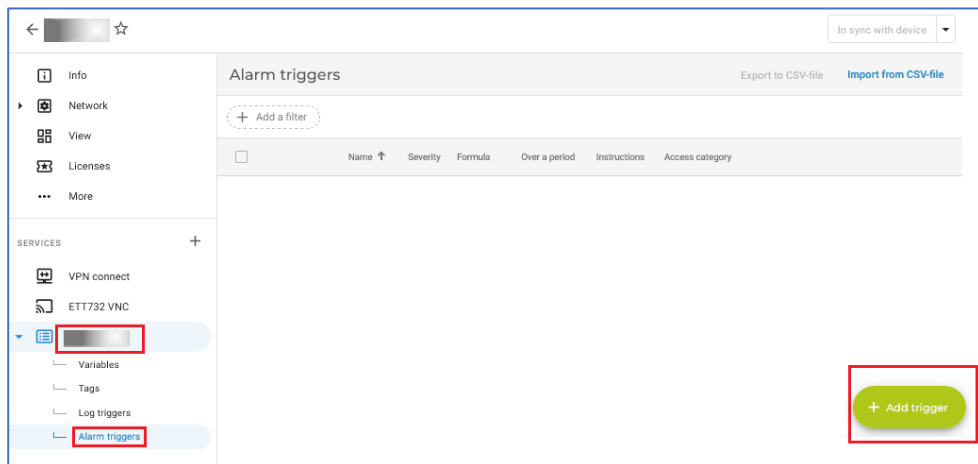


Abb. 108 Hinzufügen eines Triggers über das Datenquelle-Menü.

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

Abb. 109 Einstellung der Quelle und der Parameter für den 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

Abb. 110 "Push Config to device" zur Synchronisierung mit dem Gerät

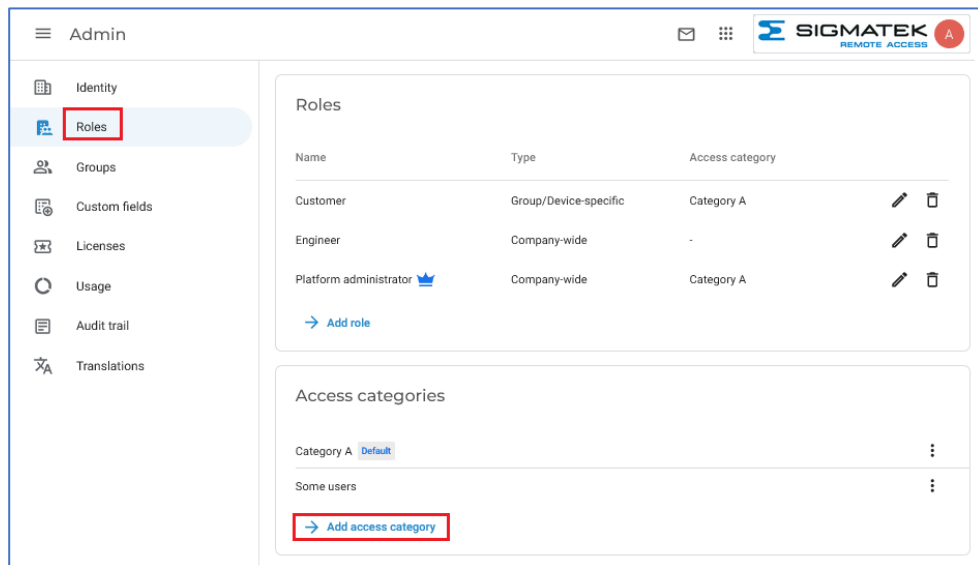


Abb. 111 Benutzer Zugriffskategorie zum Erhalt von Benachrichtigungen für bestimmte Alarme bearbeiten.

5.8 Benutzerverwaltung

Unter Admin über das APP Menü → Admin (Abb. 112) können Benutzer und ihre Geräteberechtigungen verwaltet werden. Die Kernkomponenten zur Benutzerverwaltung sind Rollen, Zugriffskategorien und Gruppen:

- Rollen – ist eine Auswahl von Verwaltungs- oder Geräteberechtigungen, die der Benutzer in der RAP-Cloud hat. Es gibt zwei Typen:
 - Die Option „Company-wide role“ ermöglicht die Auswahl einer größeren Anzahl von Verwaltungsoptionen für diesen Benutzer.
 - Die Option „Group/Device specific“ beschränkt den Benutzer auf gruppen- oder gerätespezifische Berechtigungen.
 - Das Hinzufügen einer neuen Rolle erfolgt über die Verwaltungsseite und das Klicken auf Roles → Add Roll (Abb. 113).
 - Berechtigungen bearbeiten und auf Add klicken (Abb. 114).
 - Die Standardrollen Kunde, Ingenieur und Plattformadministrator sind verfügbar und können auch bearbeitet werden.

- Zugriffskategorien – sind die Auswahl von Seiten und Diensten.
 - Das Diagramm in Abb. 115 zeigt wie Zugriffskategorien funktionieren. Eine Zugriffskategorie wird hinzugefügt, wenn ein bestimmter Dienst wie zuvor in den Abschnitten 5.6.2.1, 5.7.3 und 5.7.4.2 für einen VNC-Server, eine Geräteseite bzw. Cloud-Benachrichtigungen konfiguriert wurde.
 - Eine neue Zugriffskategorie kann über die Admin Seite → Add access category (Abb. 116) hinzugefügt werden.
 - Der neuen Zugriffskategorie einen Namen hinzufügen (Abb. 117).
- Gruppen – die Auswahl von Geräten und Benutzern.
 - Eine Gruppe wird Benutzern zugewiesen, denen keine „Company wide role“ zugewiesen haben.
 - Gruppen können in Listen von Gruppentypen organisiert werden, um einen strukturierteren Ansatz zu erhalten, wenn viele Gruppen existieren (z.B. Kunde, Maschinentyp, Region).
 - Um ein Gerät für Benutzer sichtbar zu machen, denen keine "unternehmensweite Rolle" zugewiesen ist, fügen Sie das Gerät über den Flottenmanager → Gerät auswählen zur Bearbeitung → Info → Gruppen → Bearbeiten (Abb. 118).
 - Die Erstellung einer neuen Gruppe erfolgt über die Verwaltungsseite und Gruppen → Gruppentyp auswählen → "+ Neue Gruppe hinzufügen" (Abb. 119).

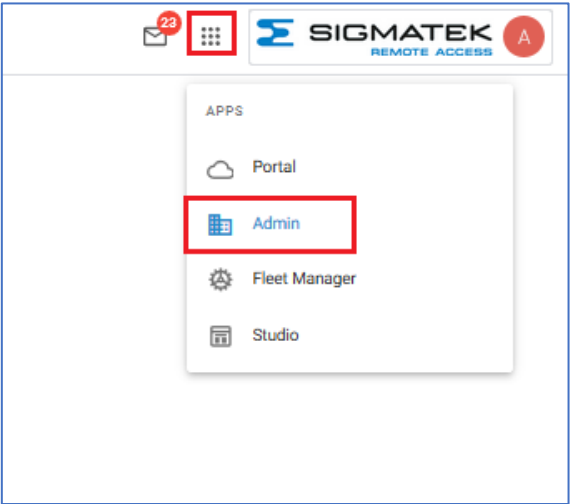


Abb. 112 APP Menü → Admin zur Verwaltung von Berechtigungen

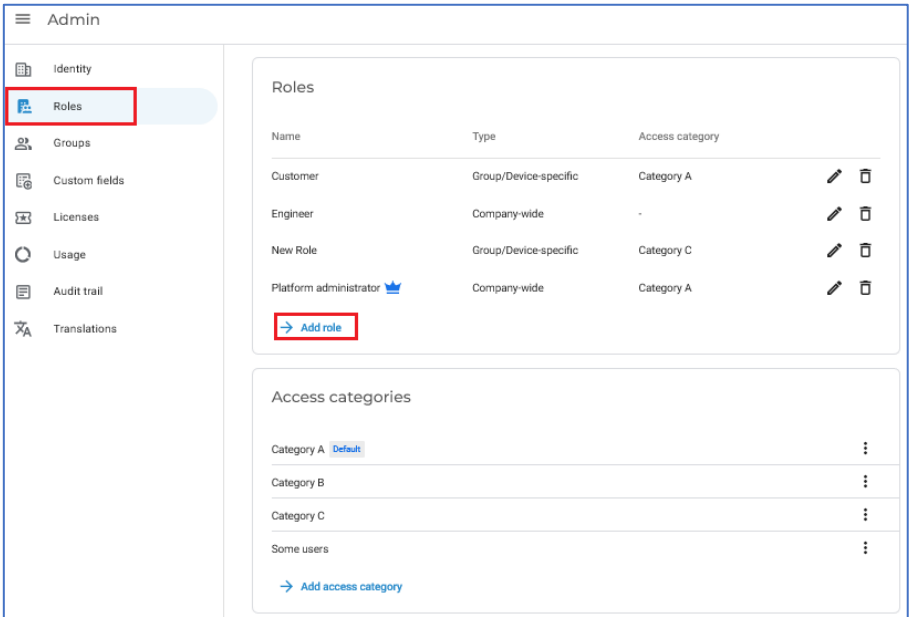


Abb. 113 Eine neue Rolle zur Admin Seite hinzufügen

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

Abb. 114 Berechtigungen bearbeiten

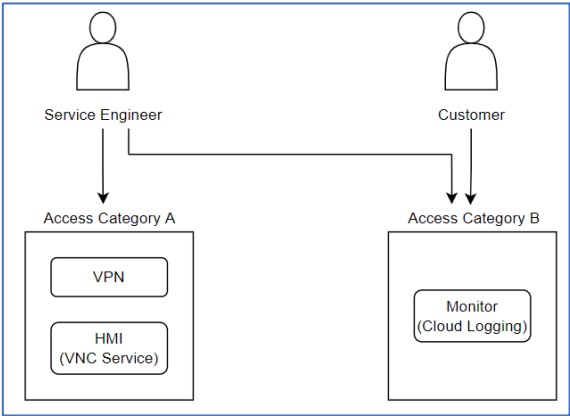


Abb. 115 Zugriffskategorie Diagramm

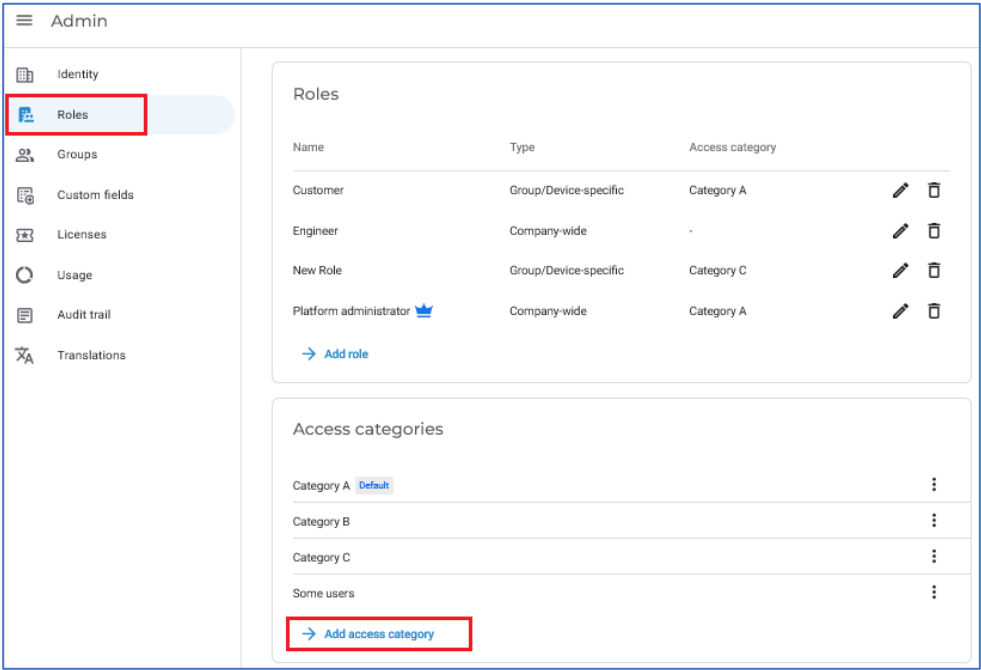
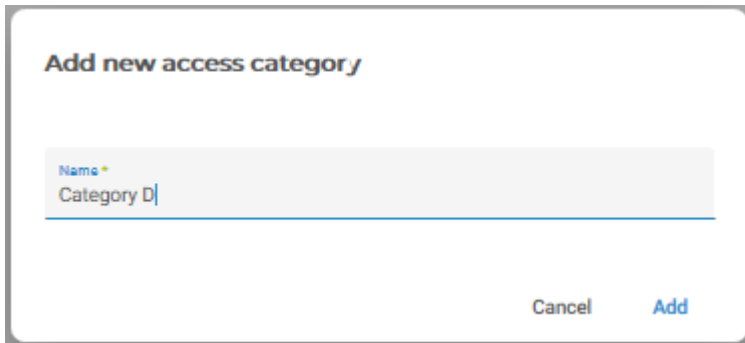


Abb. 116 Neue Zugriffskategorie hinzufügen

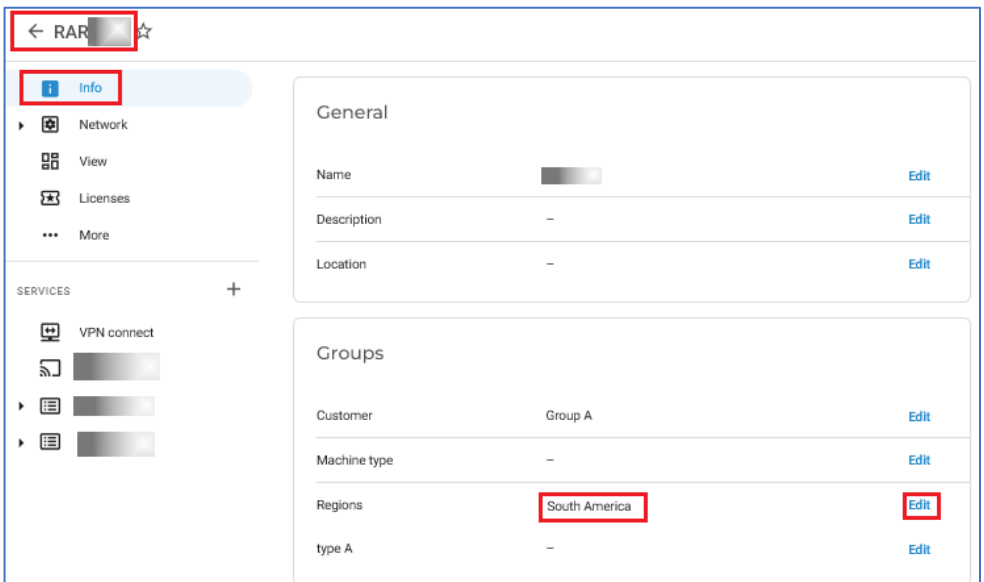


Add new access category

Name

Cancel Add

Abb. 117 Der neuen Zugriffskategorie einen Namen geben



← RAR  ☆

Info

Network

View

Licenses

More

SERVICES +

VPN connect









General

Name		Edit
Description	-	Edit
Location	-	Edit

Groups

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

Abb. 118 Ein RAR-Gerät zur Gruppe "South America" aus Gruppentyp "Regions" hinzufügen

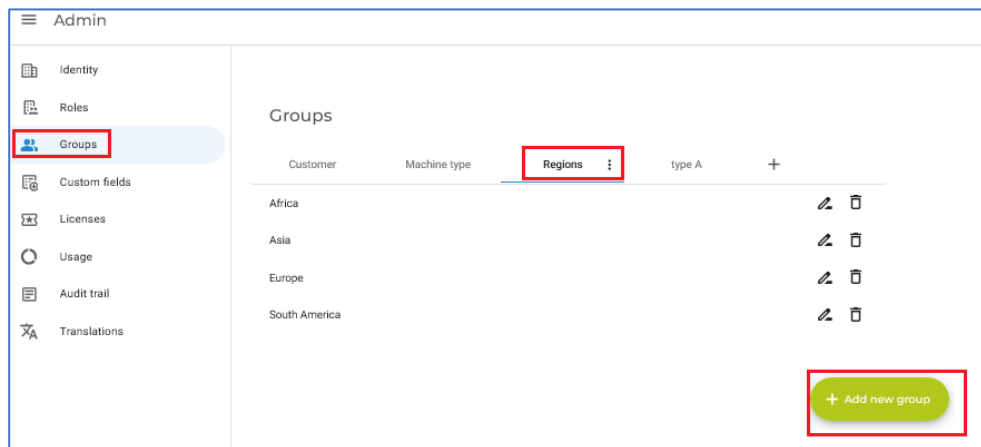


Abb. 119 Eine neue Gruppe im Gruppentyp "Regions" hinzufügen

5.8.1 Erstellen eines neuen Benutzers

Ein neuer Benutzer kann verschiedene Rollen innerhalb von RAP zugewiesen bekommen. Eine vollständige Liste aller Benutzer für ein Unternehmen kann über die Portalseite im Menü APPS → Portal → Users (Abb. 120) aufgerufen werden.

- Einen neuen Benutzer hinzufügen
 - Klicken Sie auf "+ invite users" im APPS Menü → Portal → Users (Abb. 120)
 - Füllen Sie die Details aus, einschließlich der E-Mail und der Zugriffsstufe des neuen Benutzers (Abb. 122).
 - Access Level – Sie müssen wählen, ob die Rolle für alle Geräte und Benutzer in Ihrem Unternehmen, für eine Gruppe von Geräten und Benutzern oder nur für ein Gerät gelten soll.
 - Role – Jede Rolle ist eine Kombination von Berechtigungen und bestimmt somit, was ein Benutzer tun kann und was nicht. Rollen können über Apps Menü → Admin → roles verwaltet werden.
 - Der Benutzer hat Zugriff auf alle Geräte in dieser Gruppe und die ausgewählten Rollen sind auf diese Gruppe beschränkt. Beim gerätespezifischen Zugriff können Sie ein Gerät auswählen, auf

das Sie Zugriff erhalten. Rollen können über Apps Menü → Admin → Roles verwaltet werden.

- Ausstehende Einladungen werden mit einem blauen Symbol angezeigt (Abb. 123).
- Der eingeladene Benutzer erhält eine E-Mail mit einem Anmeldelink.



Abb. 120 Zugriff auf Benutzerliste erfolgt über das Menü Portal

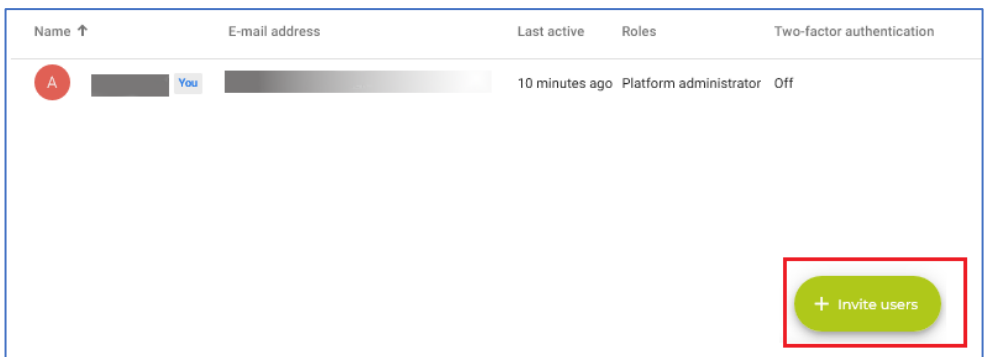


Abb.121 Neuen Benutzer laden über das Portal Menü → Users.

Invite users

Add more e-mail addresses...

Invitation message

Access level

Company-wide

Group-specific

Device-specific

Device

Role *

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

Abb. 122 Geben Sie die Details für die E-Mail und die Zugriffsstufe des neuen Benutzers ein.

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

Abb. 123 Ausstehende Einladungen werden in Blau angezeigt.

6 Beispiellösungen

In diesem Abschnitt werden mehrere universelle Fernzugriffskonfigurationen vorgestellt.

- Für die erste Lösung wird anhand eines Beispiels eine Schritt-für-Schritt-Anleitung vorgestellt.
- Für alle Lösungen wird eine Reihe von Konfigurationsvorschlägen in Form eines Diagramms bereitgestellt, das die erforderlichen Verbindungen und Schnittstelleneinstellungen veranschaulicht.

6.1 Lösungen auf Basis von Fernzugriffsrouter (RAR)

Setup-Verfahrensbeispiel basierend auf Beispiel 1:

1. Öffnen Sie LASAL CLASS 2 und stellen Sie eine Online-Verbindung zum HMI her.
2. Um über das RAR auf das HMI zuzugreifen, muss das Standard-Gateway auf die IP-Adresse des RAR geändert werden (Abb. 124).
 - a. Öffnen Sie den Autoexec.Isl Editor über Debug > File Transfer > Edit Autoexec.Isl (Abb. 124).
 - b. Setzen Sie das Gateway auf die Router IP-Adresse. (Abb. 125). Diese finden Sie über das Menü RAP Fleet Manager → Devices → Network → LAN → Router LAN IP.
 - c. Starten Sie die Steuerung neu, um die neue IP-Konfiguration zu übernehmen.
3. Verbinden Sie das HMI über ein Ethernet-Kabel mit dem RAR (Abb. 126).

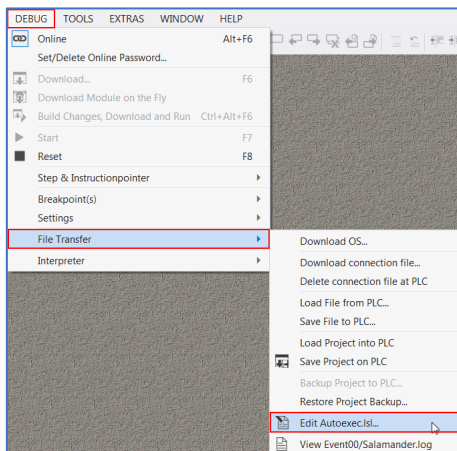


Abb. 124 Öffnen des Autoexec.IsI Editors aus LASAL CLASS 2.

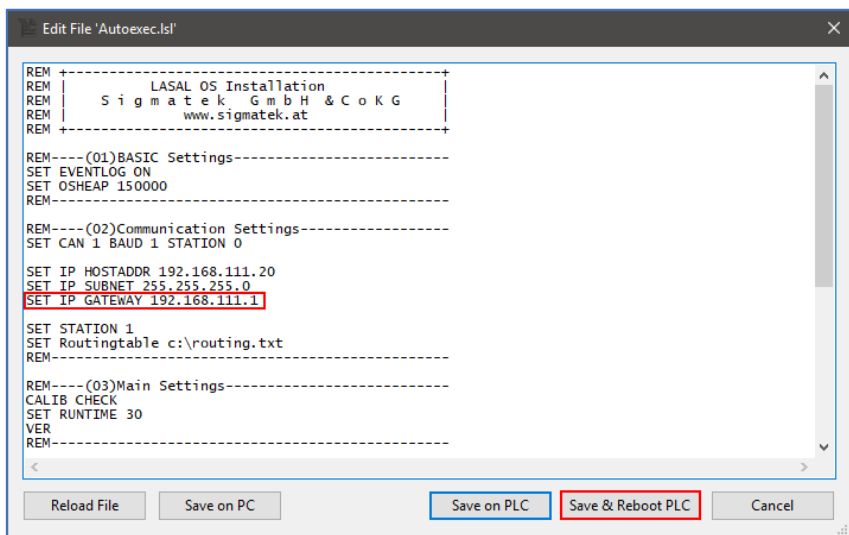


Abb. 125 Eingabe des IP-Gateways in die Autoexec.IsI.

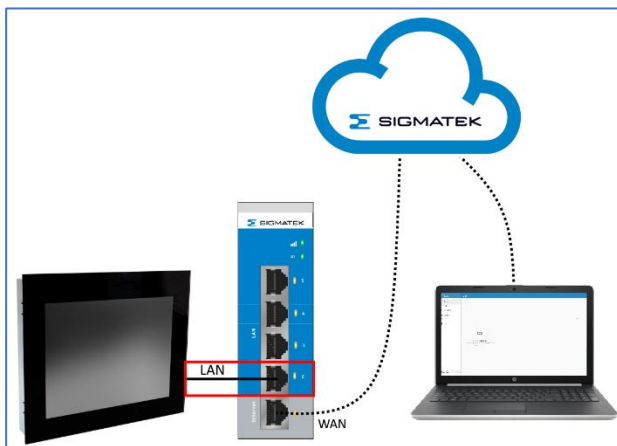
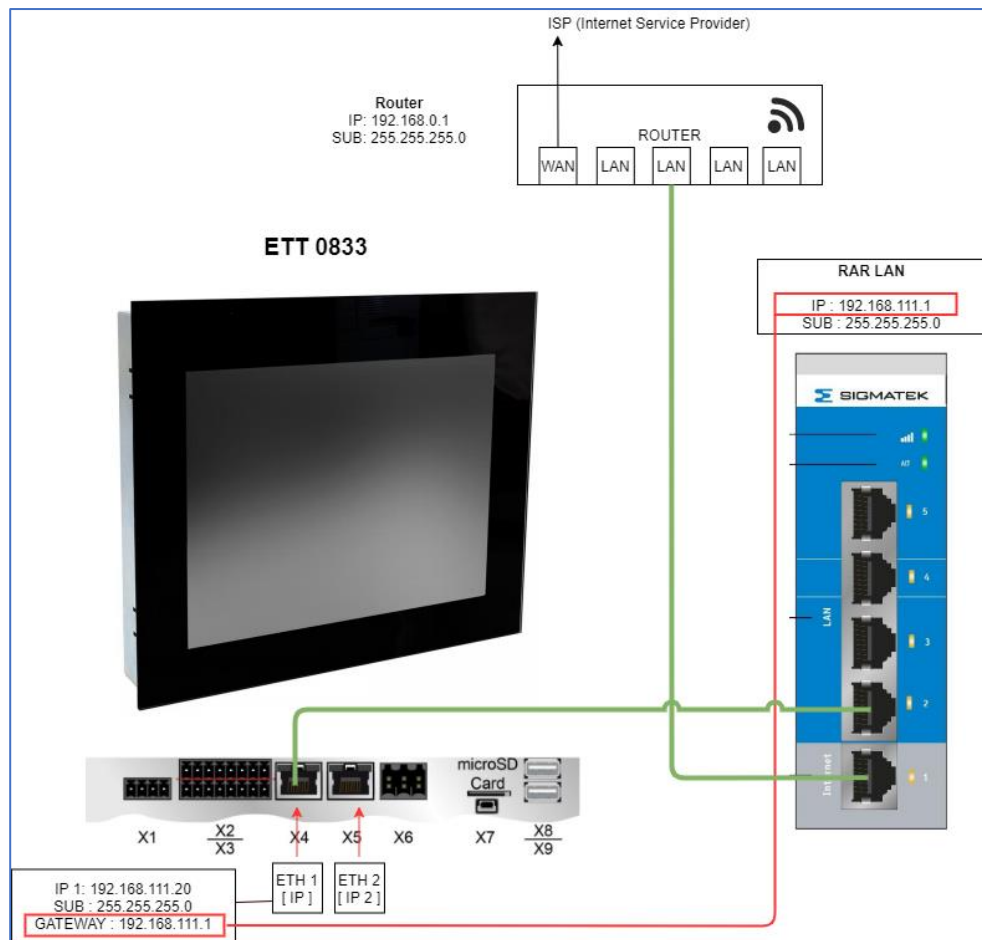
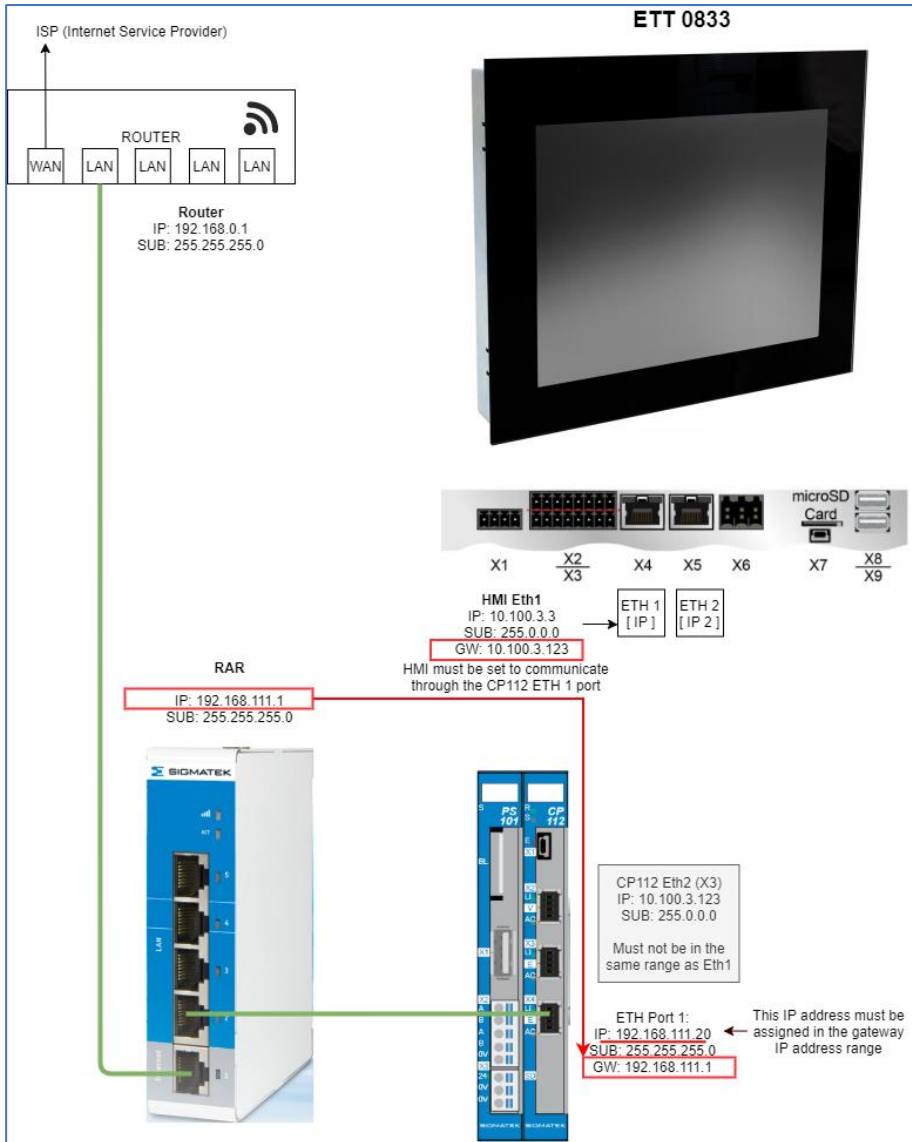


Abb. 126 Auf mit dem RAR verbundenes HMI kann über den RAP sicher zugegriffen werden.

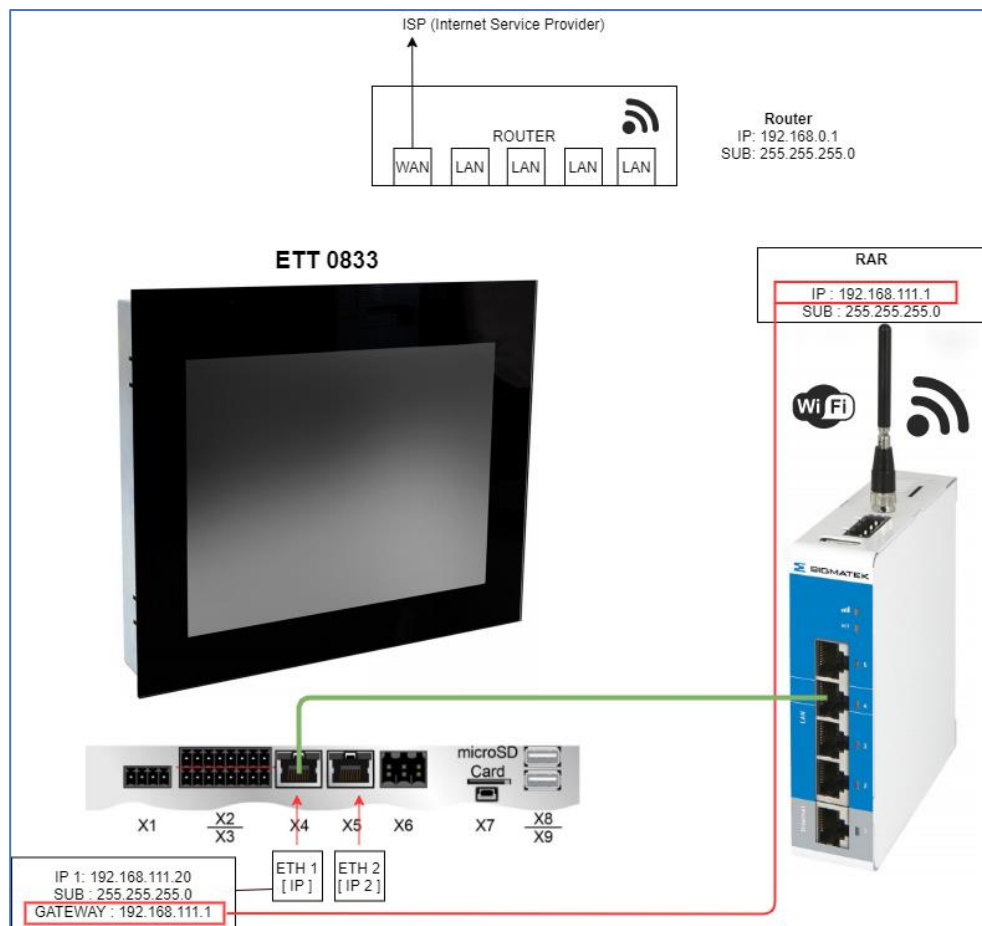
6.1.1 Beispiel 1: RAR verkabelt, Einzel-CPU-Lösung



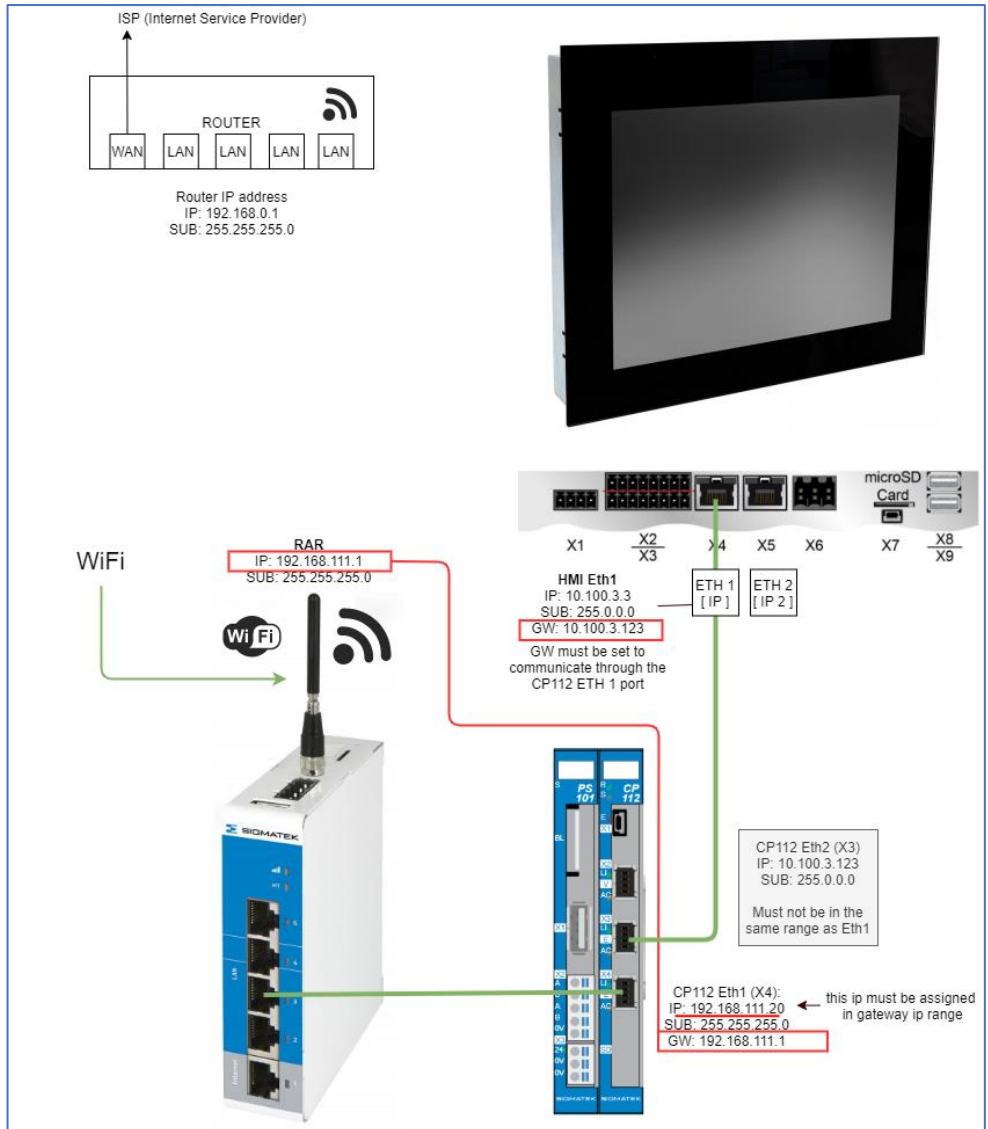
6.1.2 Beispiel 2: RAR verkabelt, Zwei-CPU-Lösung



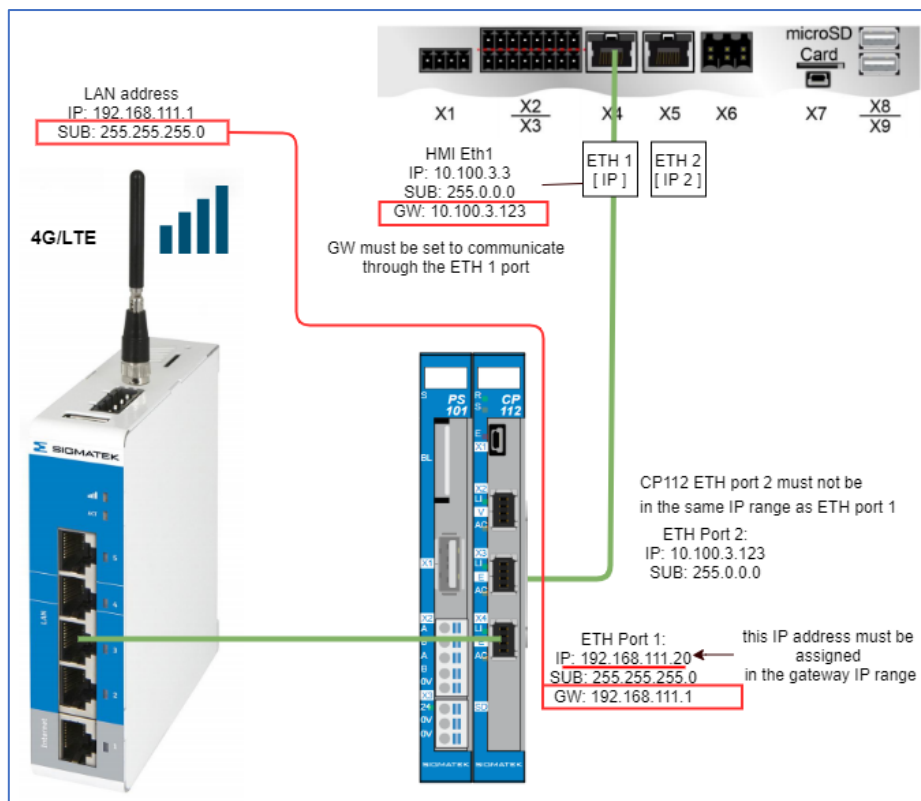
6.1.3 Beispiel 3: RAR + WIFI, Einzel-CPU-Lösung



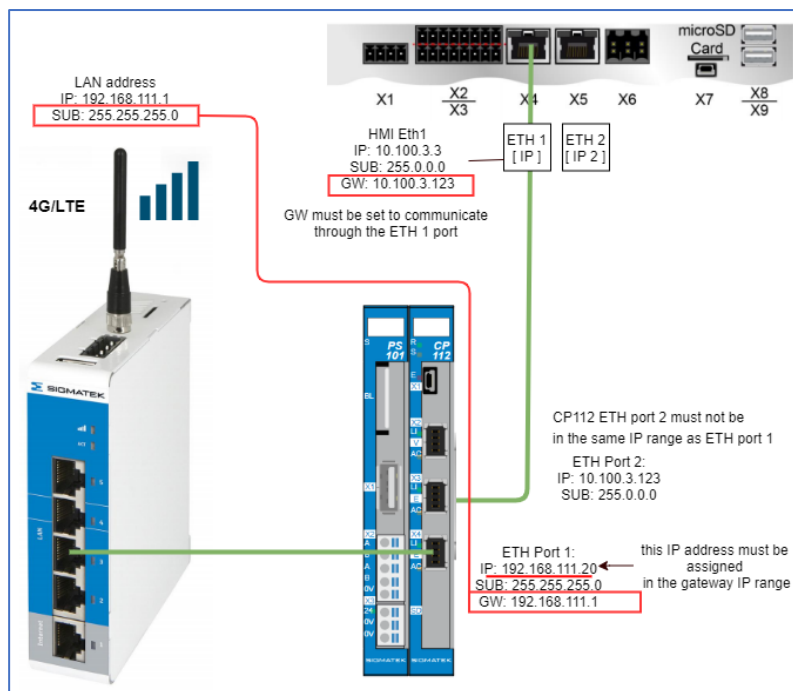
6.1.4 Beispiel 4 RAR + WIFI, Zwei-CPU-Lösung



6.1.5 Beispiel 5: RAR + Mobilfunk, Einzel-CPU-Lösung

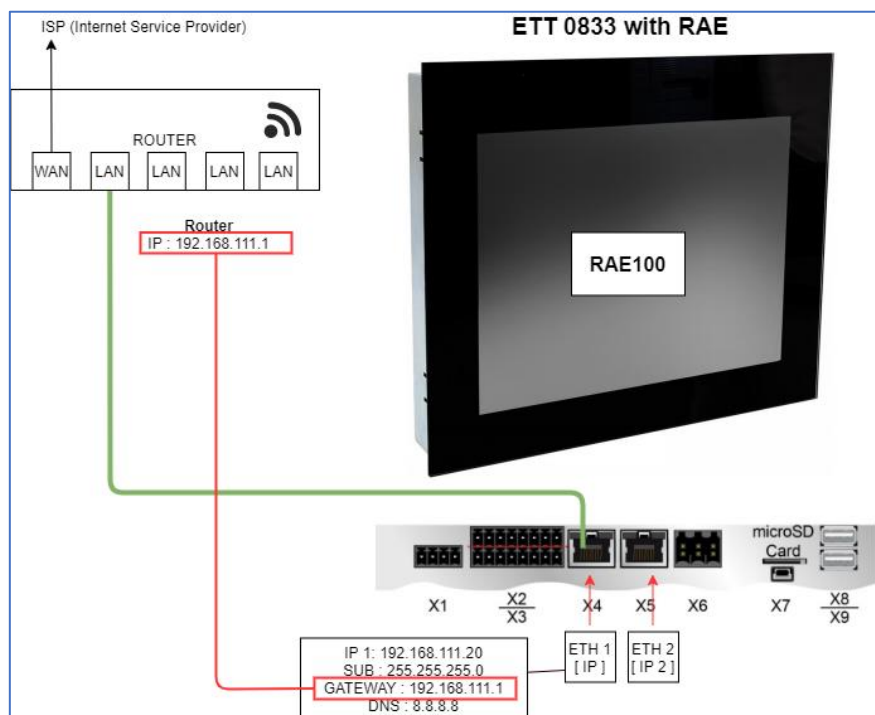


6.1.6 Beispiel 6: RAR + Mobilfunk, Zwei-CPU-Lösung



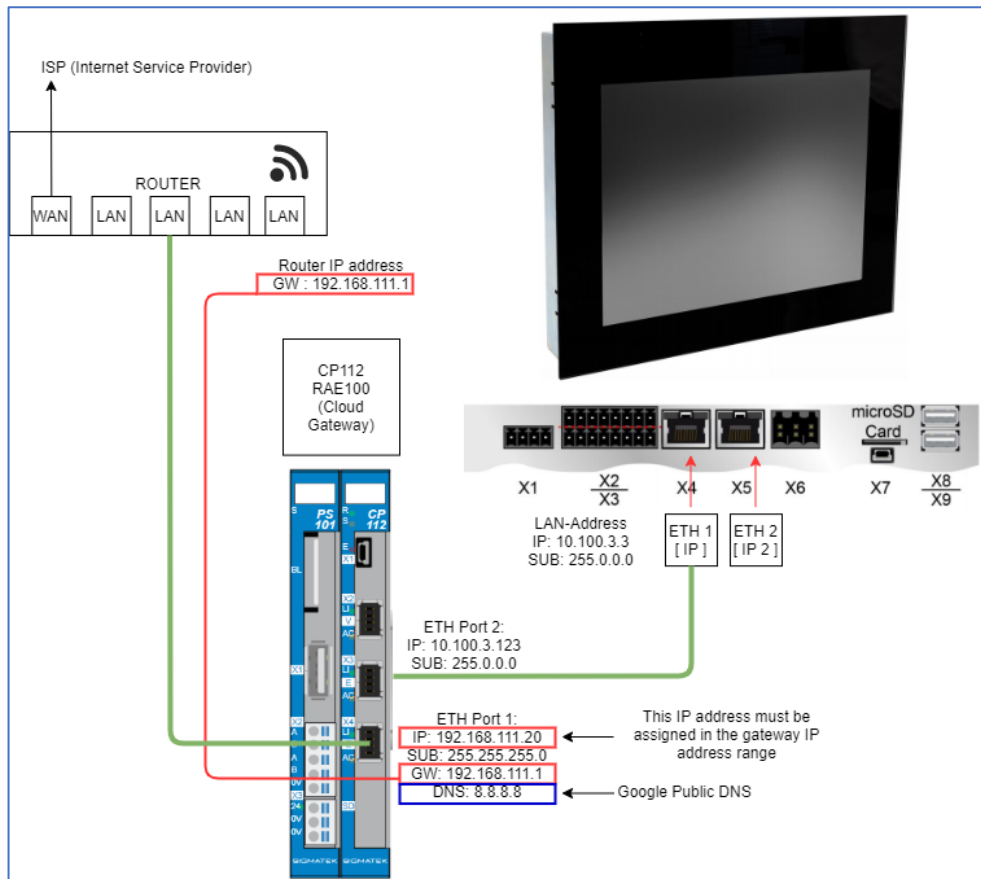
6.2 Eingebettete Fernzugriffslösungen (RAE)

6.2.1 Beispiel 7: RAE100 Einzel-CPU-Lösung

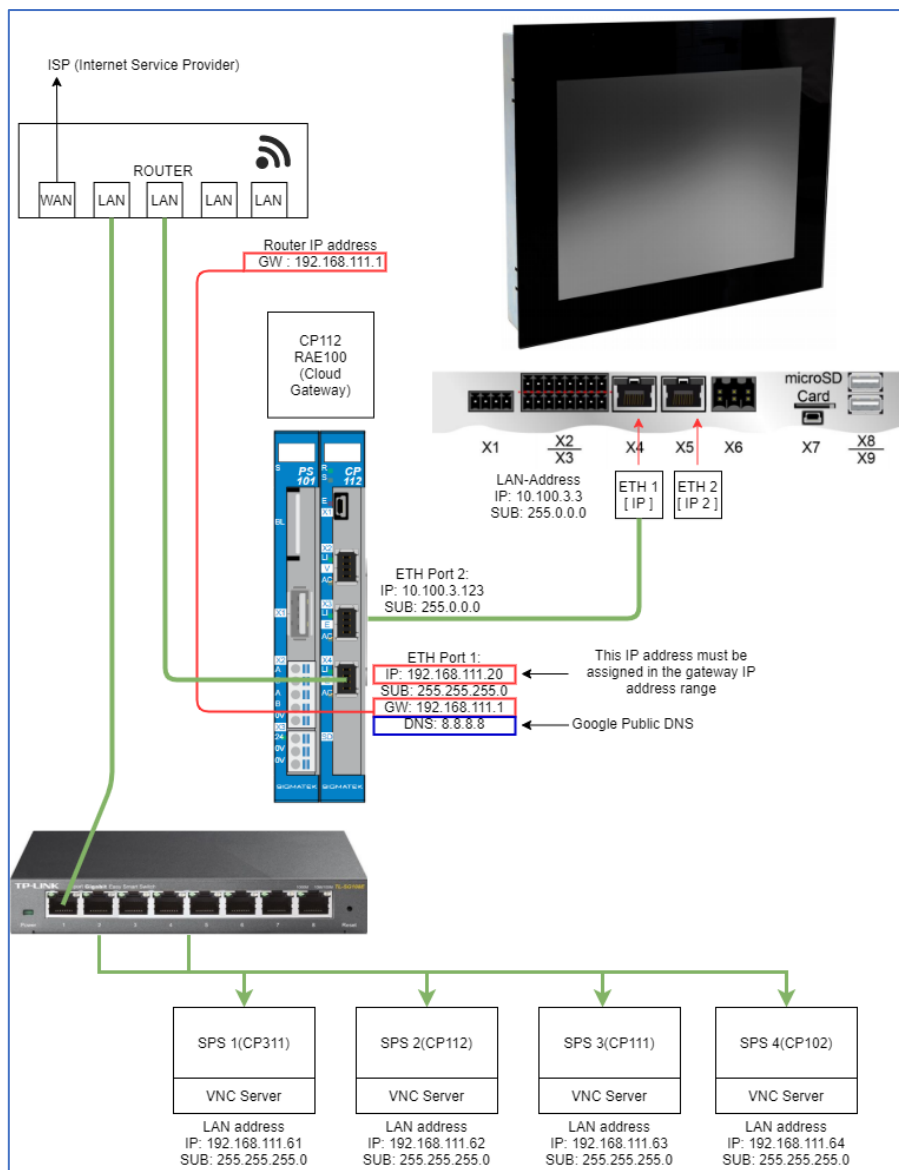


6.2.2 Beispiel 8: RAE100 Zwei-CPU Lösung

Um diese Lösung zu aktivieren, ist eine zusätzliche Einrichtung in Form eines Port-Forwarding auf der Steuerung, auf der RAE läuft, erforderlich. Siehe Abschnitt 5.5.



6.2.3 Beispiel 9: RAE100 als Gateway



Beispiel Autoexec.lsl

```
REM Ethernet Schnittstellen
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 für den Zugriff auf CPxxx VNC vom RAP aus
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 Verwaltung von Benutzern

6.3.1 Beispiel 10: Remote-Access-Service

Die Kunden werden einer Kategorie zugeteilt, um die Wartung durch Service Techniker zu erleichtern. Außerdem wird so gewährleistet, dass Kunden nur auf den Cloud Logging – Dienst zugreifen können. Die Service Techniker können zusätzlich noch auf VPN und HMI zugreifen.

Admin

Identity

Roles

Groups

Custom fields

Licenses

Usage

Audit trail

Translations

Roles

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

Abb. 126 Rollenverwaltungsmenü

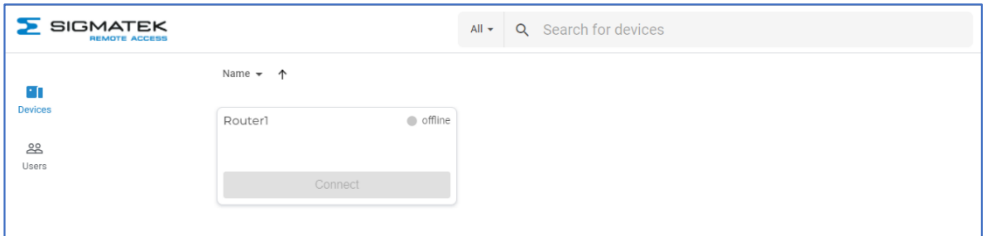


Abb. 127 Der Kunde sieht nur sein Gerät

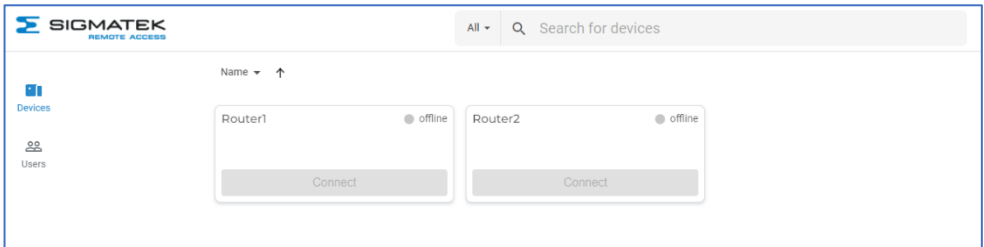


Abb. 128 Der Service Techniker kann auf alle Geräte der Kategorie A zugreifen.

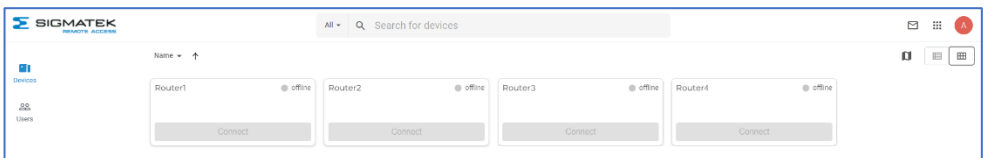


Abb. 129 Admin und Ingenieur sehen in diesem Beispiel alle Geräte

7 Installation iOS App

7.1 Startmenü und App Store

Als erstes loggen Sie sich in Ihr Gerät ein und navigieren Sie zum Startbildschirm. Suchen Sie nun die App Store App auf Ihrem Gerät. Der App Store ist in Abbildung 1 rot markiert. Öffnen Sie den App Store. Fahren Sie mit Schritt 2 fort.

Hinweis: Falls der App Store nicht auf ihrem Startbildschirm zu finden ist, wischen Sie auf der rechten Seite Ihres Startbildschirms von oben nach unten. Dadurch öffnet sich ein weiterer Bildschirm (siehe Abbildung 2) mit einer Suchleiste (Rot markiert). Dort geben Sie App Store ein.

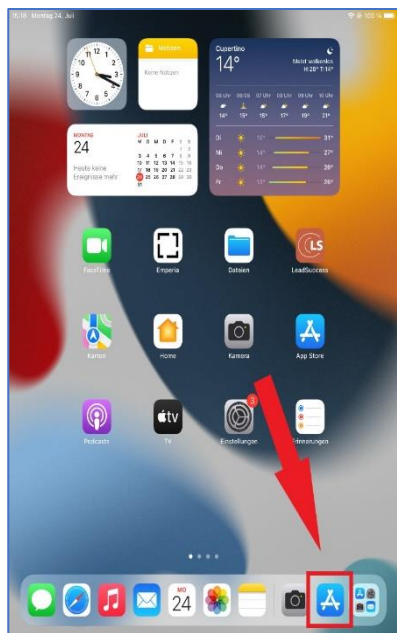


Abbildung 1 Startbildschirm



Abbildung 2 Weiterer Bildschirm mit Suchleiste

7.2 App Store – Sigmatek App

Sobald der App Store geöffnet ist, erscheint ein Fenster mit einer Vielzahl von Apps, die Sie herunterladen können. Um aber „SIGMATEK Connect“ als App zu finden, klicken Sie unten rechts auf das Lupen Symbol (siehe Abbildung 3). Auf dem Bildschirm erscheint eine Suchleiste, dort geben Sie „Sigmatek Connect“ ein. Die Suchleiste ist in Abbildung 3 Rot markiert.

Sie sollten nun ein ähnliches Bildschirmfenster sehen, wie in Abbildung 4 dargestellt. Ihnen werden nun mehrere Apps als Auswahlmöglichkeit bereitgestellt. Bitte suchen Sie die „SIGMATEK Connect“ App und klicken Sie darauf. Falls erforderlich, scrollen Sie ein wenig nach unten, um die App zu finden. In Abbildung 4 ist die App grün markiert. Fahren Sie mit Schritt 3 fort.

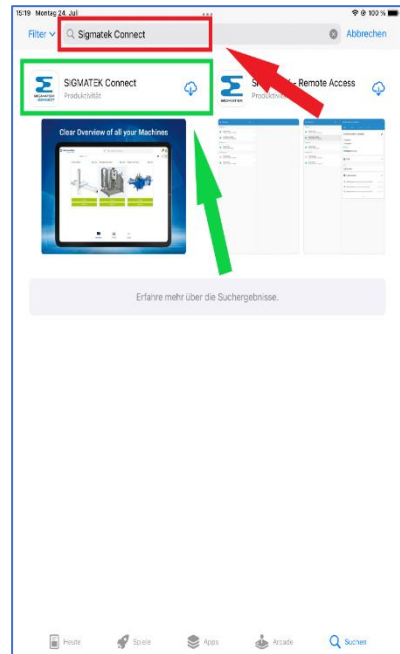
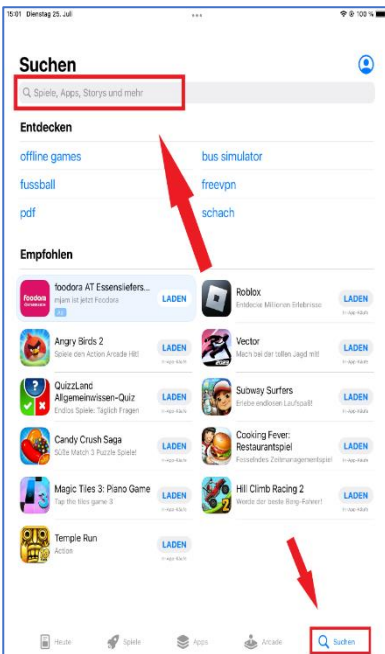


Abbildung 3 Suchleiste im App Store

Abbildung 4 Sigmatek – Connect

7.3 App installieren

Zu guter Letzt können Sie die SIGMATEK Connect App installieren.

Drücken Sie dazu auf das Wolken Symbol. Das Symbol ist in Abbildung 5 mit Rot gekennzeichnet. Warten Sie kurz, bis die Installation abgeschlossen ist.

Drücken Sie auf Öffnen/Open, um die App zu starten. (Abbildung 6, Rot markiert). Gehen Sie zu Schritt 4.

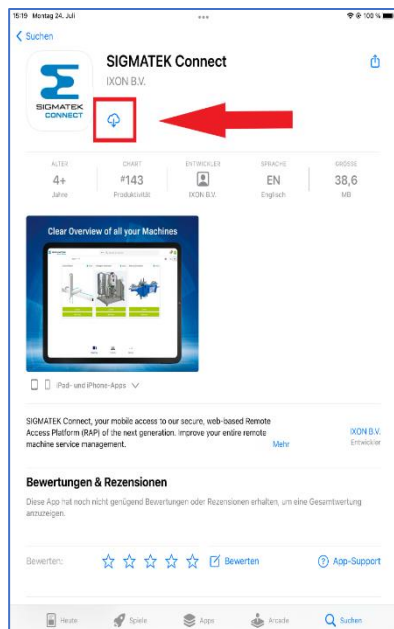


Abbildung 5 Installieren

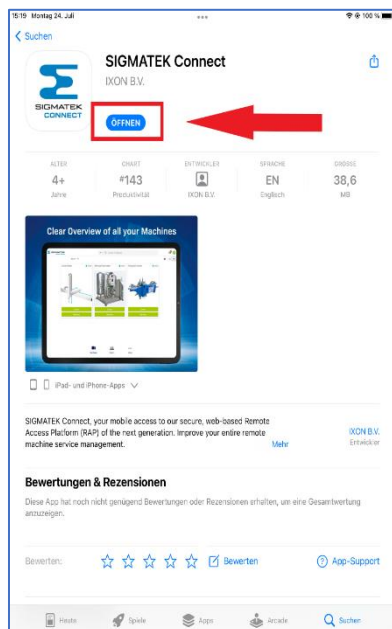


Abbildung 6 App öffnen

8 Installation Android App

8.1 Startmenü und Play Store

Als erstes loggen Sie sich in Ihr Android Gerät ein und gehen zum Startbildschirm. Suchen Sie nun die Play Store App von Android auf Ihrem Gerät. Der Play Store ist in Abbildung 1 mit Rot gekennzeichnet. Öffnen Sie den Play Store. Gehen Sie zu Schritt 2.

Hinweis: Sollte der Play Store nicht auf ihrem Startbildschirm zu finden sein, wischen Sie auf Ihrem Startbildschirm von unten nach oben. Dadurch öffnet sich ein weiterer Bildschirm (siehe Abbildung 2) mit einer Suchleiste (Rot markiert). Dort geben Sie Play Store ein.



Abbildung 1 Startbildschirm

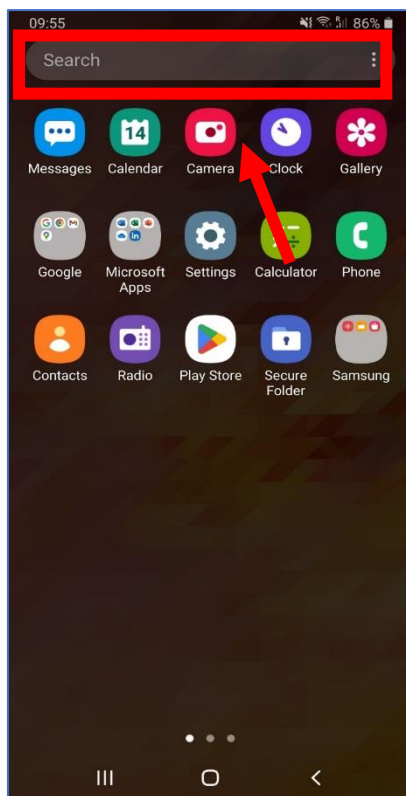


Abbildung 2 Weiterer
Bildschirm mit Suchleiste

8.2 Play Store – Sigmatek App

Sobald der Play Store geöffnet ist, erscheint ein Fenster mit ganz vielen Apps, die man sich herunterladen kann. Um aber „SIGMATEK Connect“ als App zu finden, klicken Sie oben in die Suchleiste und geben „**Sigmathek Connect**“ ein. Die Suchleiste ist in Abbildung 3 Rot markiert.

Sie sollten nun ein ähnliches Bildschirmfenster sehen wie in Abbildung 4 dargestellt. Es werden Ihnen nun mehrere Apps als Auswahlmöglichkeit bereitgestellt. Bitte suchen Sie die „**SIGMATEK Connect**“ App und klicken Sie drauf. Notfalls müssen Sie ein bisschen nach unten scrollen, um die App zu finden. In Abbildung 4, ist die App mit Grün markiert. Gehen Sie nun zu Schritt 3.

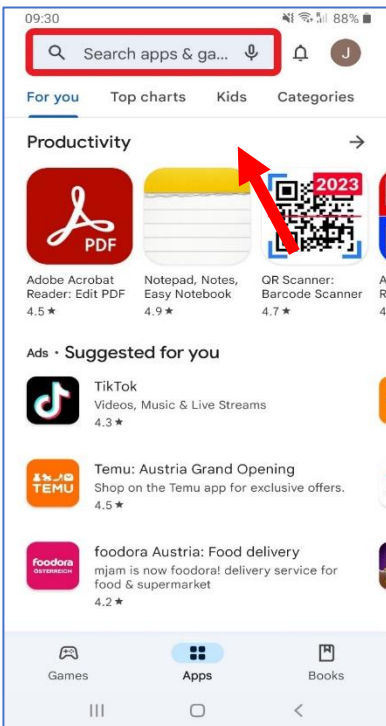


Abbildung 3 Suchleiste im Play Store

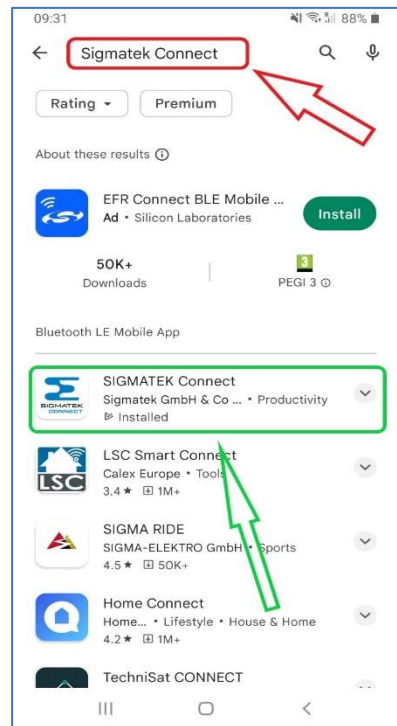


Abbildung 4 SIGMATEK Connect

8.3 App installieren

Zu guter Letzt können Sie die SIGMATEK Connect App installieren.

Drücken Sie dazu auf Installieren/Install. Der Install-Button ist in Abbildung 5 mit Rot gekennzeichnet. Warten Sie kurz, bis die Installation abgeschlossen ist.

Drücken Sie auf Öffnen/Open, um die App zu starten. (Abbildung 6, Rot markiert). Gehen Sie zu Schritt 4.

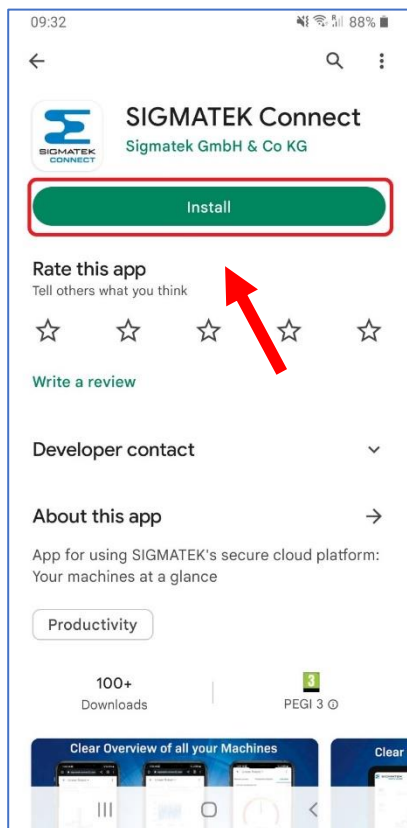


Abbildung 5 Installier - Button

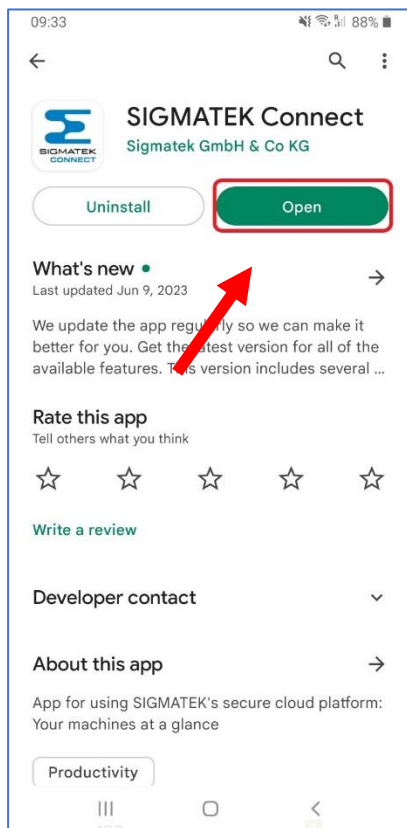


Abbildung 6 App öffnen

8.4 Sigmatek Login und Startbildschirm

Wenn Sie die App nun geöffnet haben, erscheint ein Anmeldefenster, wie in Abbildung 7 zu sehen. Gleichzeitig wird im Hintergrund die App auf ihrem Startbildschirm hinzugefügt, wie in Abbildung 8, Rot markiert, zu sehen. Sollten Sie die App nicht im Startbildschirm sehen, schauen Sie sich bitte den Hinweis bei Schritt Nummer 1 nochmal an und suchen Sie die App. Meist versteckt sie sich auf einer der anderen Bildschirmseiten. Sobald Sie die App gefunden haben, können Sie die App entspannt öffnen, wann und wo sie wollen.



Abbildung 7 Login - Plattform

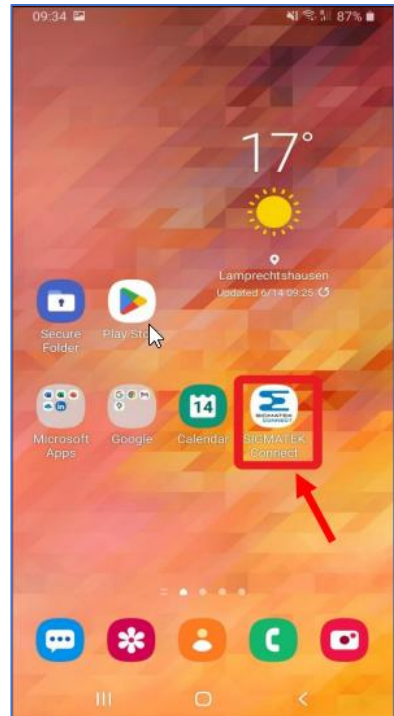


Abbildung 8 App-Verknüpfung auf
Startbildschirm