ConnectedCooking Installationsanleitung

RATIONAL ConnectedCooking is a cloud-based software solution that provides flexible, easy-to-use features to centrally manage your SelfCookingCenter® and VarioCooking Center®.

In the standard case for customer who do not have special network security settings it is recommend to use DHCP in order to assign correct IP and DNS information in the ovens. If your network is configured by an IT administrator or an IT department please note the following information in order to enable the ovens to connect to the ConnectedCooking cloud.

What are the requirements?

1. The ovens at least have the software version SCC-07-00-07
2. The ovens are connected to the internet
3. The following ports are opened in the firewall:
    a. Port **8883** to **mqtt.rational.inovex.io** (optional)
    b. Port **443** to **stg.rational.inovex.io**
4. If static IP addresses are used make sure that DNS server addresses and gateway address is given. **Important:** After changing the IP address configuration it is necessary to **restart** the SelfCookingCenter or VarioCooking Center.

Drawing of the principle

1. Registration

- Set up the account on www.connectedcooking.com

2. Adding the units

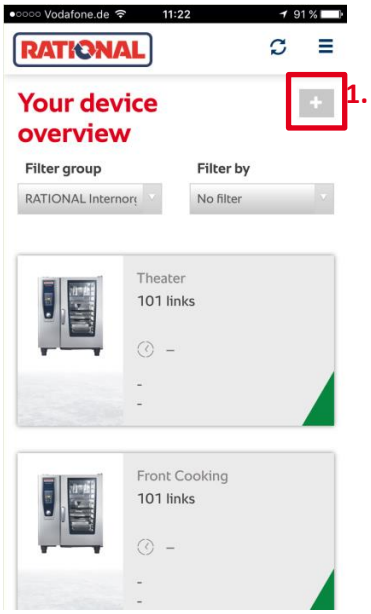
- Scan the QR-Code or enter the registration code

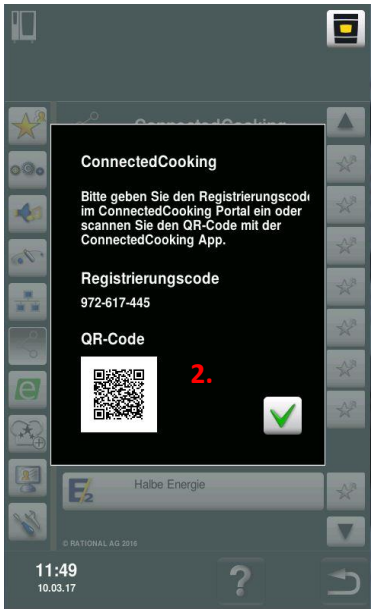
3. Ready to use

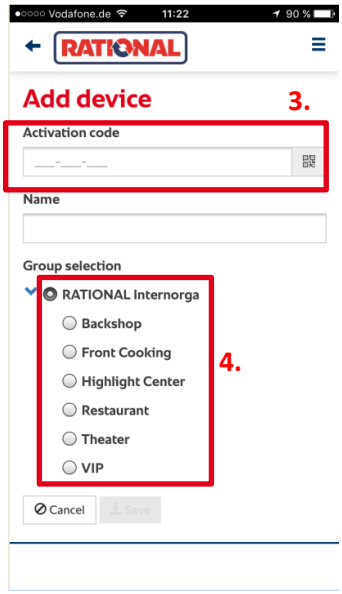
1. **Software update**
   Please update the unit with Software Version 7.

2. Activate DHCP
   Please activate DHCP in the network settings.

3. **ConnectedCooking**
   Please activate ConnectedCooking and a registration code







4. Register a unit
You can either scan the QR code with your iPhone/Android or enter the registration code into the mask manually.
Please also assign a name for every unit (e.g. SelfCookingCenter61E or VarioCookingCenter112L) and assign it to the corresponding group.

Security information

Communications:

- forced SSL encrypted communication between web/mobile clients and cloud portal (unencrypted communication not possible)
- forced SSL encrypted communication between kitchen devices and cloud web services (unencrypted communication not possible)
- insecure TLS and SSL protocol versions blocked

Unit registration:

- RSA encrypted device registration process

User access and login data

- role based REST API access control
- user passwords stored as salted & encrypted hashes

Data base

- database server not part of DMZ (behind second firewall, access only from internal services)

System architecture and data center

- system divided into three subnets (DMZ, middleware, backend), firewall between each subnet
- latest security patches installed
- access to internal services only via dedicated vpn