TANlock®

# Manual for TANlock 3.1

**Version 1.00**

**Originally in German**

# Table of Contents

# 1 Configuration and IT Integration

## 1.1 Default settings

The default settings of the TANlock are:
DHCP disabled / static IP: http://192.168.0.90
Subnetmask: 255.255.255.0
VLAN disabled

**ATTENTION**

**Property damage possible due to unauthorized third-party access.**

- An activated HTTP protocol with enabled user management can allow individuals in an insufficiently secured network to create users on a lock and thereby gain unauthorized access.
- Unauthorized third-party access is always traceable because the user management logging cannot be disabled.

## 1.2 Configuration

The following configuration refers to the software tl- handle_2.2.0.

**NOTE**

**T**ANlock GmbH offers a tailored configuration service, including training if needed. The TANlock is then immediately ready for use.

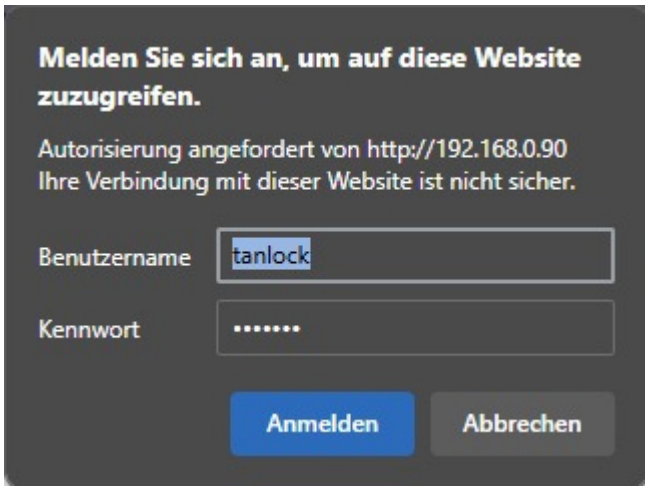
### 1.2.1 Connecting the TANlock via Web Browser

**NOTE**

For the connection via Ethernet, your PC must be in the same IP subnet as the TANlock.

- Open the web browser (e.g. Google Chrome)
- Enter the IP adress http://192.168.0.90 in the adress bar

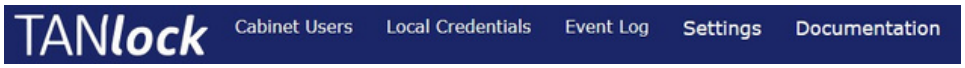
☐ Log in with the username "tanlock" and password "TANlock," then click the "Login" button.




*Graphic 11: Login*

## 1.3 Tabs

In the tab of the administration interface, you will find the current settings of the TANlock. Here you can make changes.




*Graphic 12: Overview Tabs*

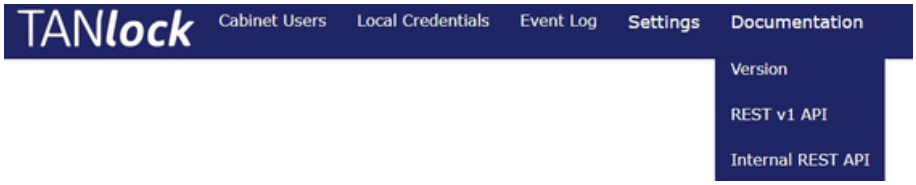
The following tabs are available in the section:

- Cabinet Users
- Local Credentials
- Event Log
- Settings
- Documentation

Save any changed settings on the TANlock by clicking "Save."

You can refresh the display of the settings by clicking "Refresh."

### 1.3.1 Tab "Documentation"

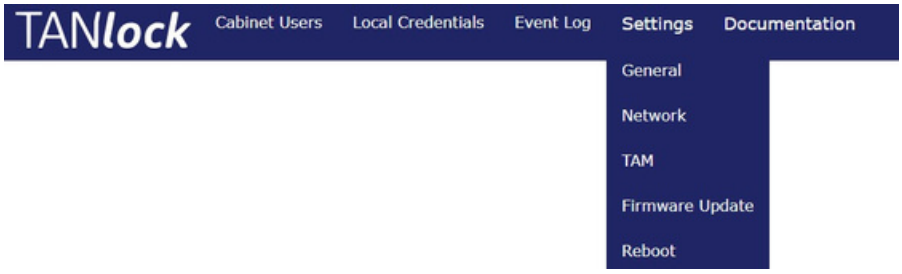



*Graphic 13: Tab"Documentation"*

The following fields are available oin the "Documentation" tab:

- **Version**:
  Here you will find the current version information of the TANlock.
- **REST v1 API:**
  Here you will find the REST v1 API documentation.
- **Internal REST API:**
  Here you will find the internal REST API documentation.

### 1.3.2 Tab "Settings“




*Graphic 14: Tab"Settings"*

The following fields are available in the "Settings" tab:

- **General:** General settings:
  - **„Time Settings“**: Either manual entry of date and time or synchronization with the browser.
- **Network**: Network settings:
  - **„Network Settings“**: Configuration of manual IP settings or activation of DHCP is possible.
- **TAM**:
  - **„TANlock Authentication Module“:** Selecting the corresponding TAM (TANlock Authentication module)
- **Firmware Update:**
  If interested, please contact your TANlock representative.

„**Reboot**:

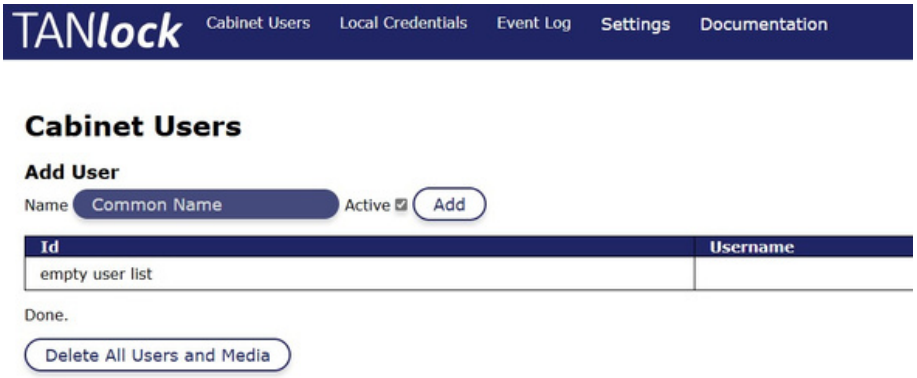
Restart of the TANlock.

### 1.3.3 Tab "Event Log"

In the "Event Log" tab, all events on the TANlock are tracked.

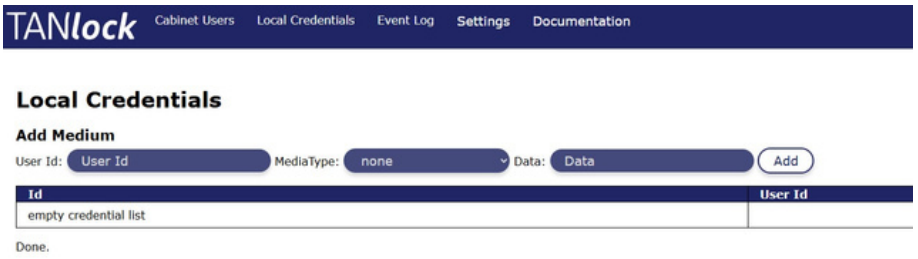
### 1.3.4 Tab "Cabinet Users"

Authorized users who are allowed to operate the TANlock are created here via the “Add” button. The respective start medium is also assigned in this section. These entries can also be deactivated or deleted here.




*Graphic 15: Tab "Cabinet Users"*

### 1.3.5 Tab "Local Credentials"




*Graphic 16:Tab "LocalCredentials"*

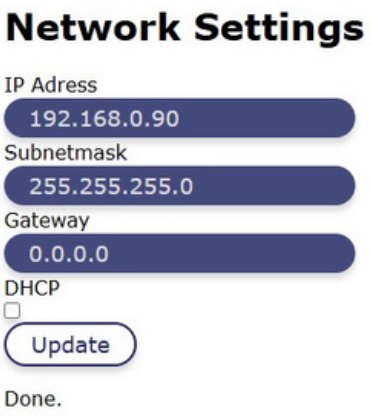
Here, media can be created, assigned to, or deleted from the user.

## 1.4 IT-Anbindung

### 1.4.1 Manual Assignment of a static IP address

To manually assign a static IP address, proceed as follows:

1. Go to the tab and click on „Settings“→ „Network“ →“ Update“




*Graphic 17: Tab "Network"*

2. Enter the IP address in the first field
3. Enter the subnet mask in the second field.
4. Enter the gateway in the third field.
5. Click “Update” to save the entries.
6. Perform a reboot via “Settings” → “Reboot.”
7. The TANlock will restart after saving the configuration.

✓ The static IP address has been set.

### 1.4.2 Using DHCP

To use a dynamic IP address, proceed as follows:

1. Check the box labeled “DHCP.”
2. Enter a reboot through„Settings“→ „Reboot“
3. The TANlock will restart after saving the configuration.

✓ The dynamic IP address has been set.

# 1.5 User Management

## 1.5.1 Permissions

*General Functionality*

As an electronic lock, TANlock allows you to electronically manage authorized users and their keys without any physical modifications to the lock. TANlock offers various options to define the individuals who are authorized to open the lock.

## 1.5.2 Local

You can store up to 5,000 users locally on the device. When using fingerprint authentication, a maximum of 32 fingerprints can be stored.
Access is still granted if the connection to the LDAP service fails in an LDAP-based solution.
This is also suitable when there is no centralized management of user permissions and a standalone lock solution is desired.
To create a user and assign a medium on the TANlock 3, proceed as follows:

Each TAM is based on RFID. Additional options, such as PIN, are layered on top of the RFID.

**1. Activate TANlock Authentication Module (TAM):**

i) „Settings“ → „TANlock Auth Module“ → „Hardware Module”

ii) Das gewünschte TAM auswählen

iii) Confirm with “update”

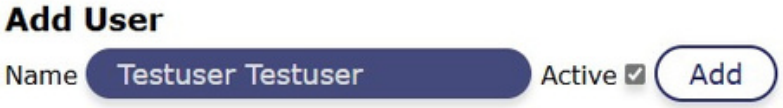
iv) Reboot under “Settings”→ “Reboot”

**2. Creating a user:**

*1.* Please go to the tab and select „ Cabinet Users“


*Graphic 18:„Add User“*

2. Enter the first and last name of the new user; optionally, you can also assign a personnel number for the user here.




*Graphic 19: „Add User“*

3. Now please click the “Add” button. The user is now created on the TANlock.


*Graphics 20 and21: „Add User“ and overview of added users*

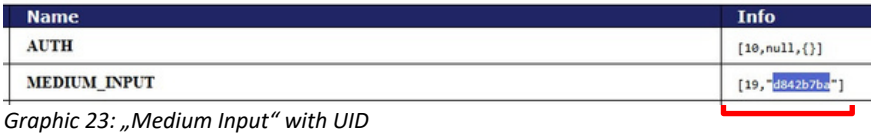
3. **Assign RFID card to user:**

**Assign RFID card:** To assign an RFID card, hold the respective RFID card in front of the TANlock.

**a. Please go to the „Event Log“ tab:**


*Graphic 22: Tab „Event Log“*

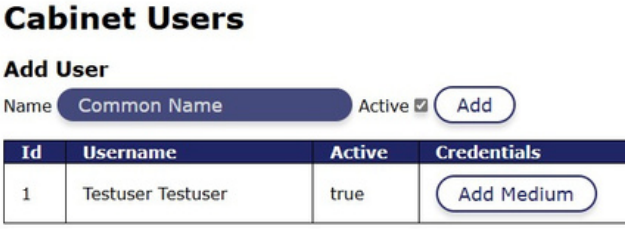
You will now see the card UID in quotation marks under the event "Medium Input."




*Graphic 23: „Medium Input“ with UID*

Please copy the UID now.

**b. Now, please go to the „Cabinet Users“ tab.**

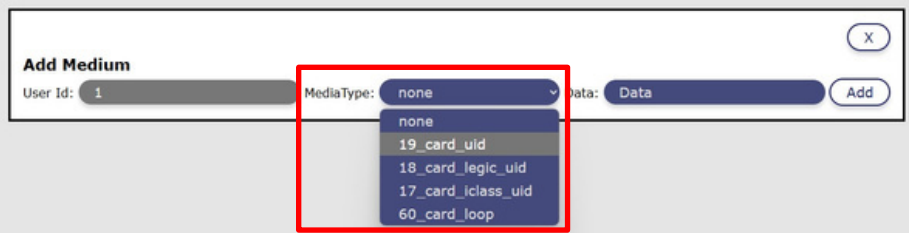



*Graphic 24: „Add Medium“*

**c. Please click the “Add Medium” button next to the corresponding user.**

**Assigning an RFID card:** Now select the medium:

**19:** RFID cards




*Graphic 25: Assigning Media Types*

Now insert the card UID from step 3.a into the “Data” field.


*Graphic 26: Inserting card UID*

**d. Now click the „Add“ button**


*Graphic 27: Confirming the new medium*

✓ The corresponding RFID card has now been assigned to the user.

Finally, please go to “Settings” and select “Reboot.”

The TANlock will now restart, and all entries will be saved.

**Assigning a fingerprint:**

1. To assign a fingerprint to a user, click on the “Cabinet Users” tab.
2. For the selected user, click on “Add Fingerprint” while no finger is on the scanner (the LEDs are not yet lit).


*Graphic 28: Fingerprint as identification trail*

a) The yellow LED will blink: Place your finger on the scanner until the yellow LED stays solid, then remove your finger.

b) The blue LED will blink: Place your finger on the scanner until the blue LED stays solid, then remove your finger.

c) The red LED will blink: Place your finger on the scanner until the red LED stays solid, then remove your finger.

✓ The first fingerprint is now saved and assigned.

### 1.5.3 External / Web Interface

Authorized users and permission concepts can be managed independently of the lock via the web API.
The advantage is that the TANlock continues to log all events, allowing every access to the TANlock to be fully traced.

More information can be found under “Documentation.”

## 1.6 Monitoring

### 1.6.1 General

Independent of the management and design of user administration, the TANlock provides monitoring. The following events are recorded and logged by the TANlock under the "Event Log" tab:

- TANlock has started: „STARTUP“.
- Input has begun : „MEDIUM_INPUT“.
- Input was authorized: „AUTH“ .
  - login= created user (see the „Users“ tab), identifier = assigned PIN/ RFID card,
    type = medium used for authentication
    (see„Settings“ → „Medium Implementation“).
  - Incorrect PIN entry: The red LED lights up on the TANlock, and the event "AUTH" records the attempt.
- Lock was unlocked: „HAL_LOCKED“: „false“
- Lock was locked: „HAL_LOCKED“: „true“
- Handle was turned: „HAL_HANDLE“: „true“
- Handle was returned to the original position „HAL_HANDLE“: „false“
- Door contact was opened: „EXT_CHANGED“: „false“= open
- Door contact was closed: „EXT_CHANGED“: „true“= closed