TANlock®

Technische Dokumentation

Version 1.0

FATH Mechatronics GmbH

Gewerbepark Hügelmühle 31

91174 Spalt

Inhalt

1) TANlock – Technische Daten, Maße

a) Technische Daten

i) Umgebungsbedingungen

Umgebungstemperatur [°C]	0 … +70
Betriebstemperatur [°C]	0 … +40
Lagertemperatur [°C]	0 … +70
Zulässige Luftfeuchte [%]	< 80, nicht kondensierend

ii) Elektrische Spezifikation

Gesamtsystem TANlock

Min. Spannung am POE [V]	40
Max. Spannung am POE [V]	58
Min. Stromstärke [mA]	2
Max. Stromaufnahme [mA] (bei 58 V Spannung)	20
Leistungsklasse	0
Voraussetzungen für POE Switch	nach IEE 802.3af-2003 / potentialgetrennt
Leistungsaufnahme [W]	1,2
Max. Schaltstrom Relais [A]	2
Max. Schaltspannung Relais [V]	220 DC / 250 AC
Max. Schaltleistung [W]	60
Max. Spannung Wartungsschnittstelle [V]	5

Schloss

Stromaufnahme [mA] bei 58 V Spannung	84
Leistungsaufnahme [W]	4,9

iii) Abmessungen und Gewicht

Länge [mm]	235,55
Breite [mm]	40
Höhe [mm]	29,23
Gewicht [g]	695
Material	Zink Druckguss
Dorn	Vierkant 8 mm mit M4 Innengewinde

iv) Typenschild

Das Typenschild finden Sie auf der Rückseite des TANlock.

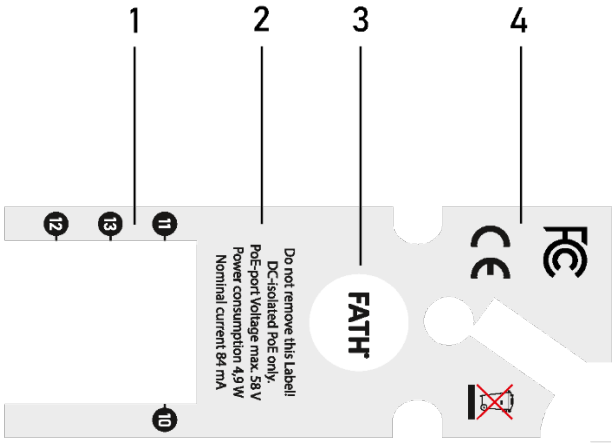


Abbildung 1: Typenschild TANlock

Pos. 1 Bauteile
Pos. 2 Elektrische Spezifikation
Pos. 3 Hersteller, Logo
Pos. 4 Kennzeichnungen und Warnhinweise

b) Anschlüsse, Bedien- und Anzeigeelemente

i) Korpus

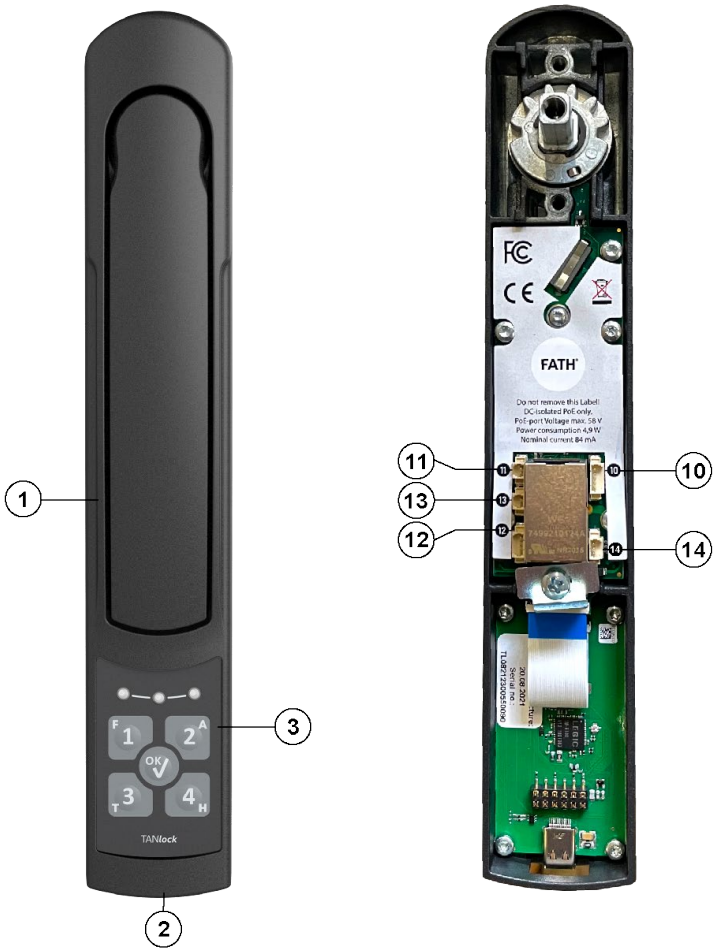


Abbildung 2: Anschlüsse, Bedien- und Anzeigeelemente des TANlock

Pos. 1	Korpus
Pos. 2	USB-C Schnittstelle
Pos. 3	TANlock Authentifikationsmodul (TAM)
Pos. 10	Extension Modules 1-5
Pos. 11	Door Sensor 0
Pos. 12	CAN-Bus
Pos. 13	Door Sensor 1
Pos. 14	Relais Interface

ii) TANlock Authentifizierungsmodule (TAMs)

Der TANlock 3 verfügt über vielfältige Möglichkeiten zur Authentifikation.

1) PIN + RFID

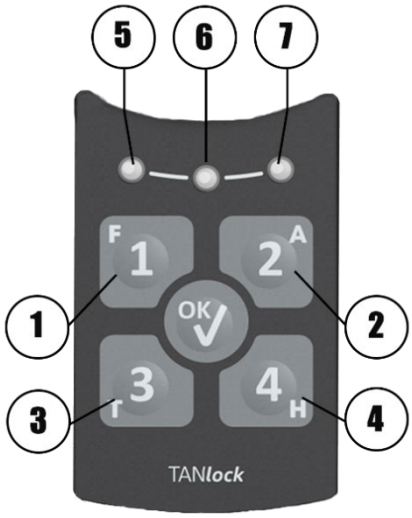


Abbildung 3: Anzeige- und Bedienelemente des PIN Modul

Pos. 1-4: Tasten zu PIN-Eingabe

Pos. 5-7: Status LEDs

2) Handvenenscan

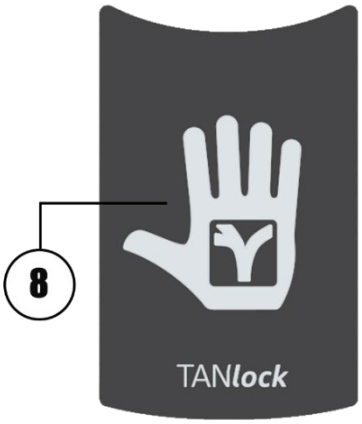


Abbildung 4: Palm Secure Venenscanner Modul

Pos. 8: Fujitsu PalmSecure Handvenenscanner

3) RFID

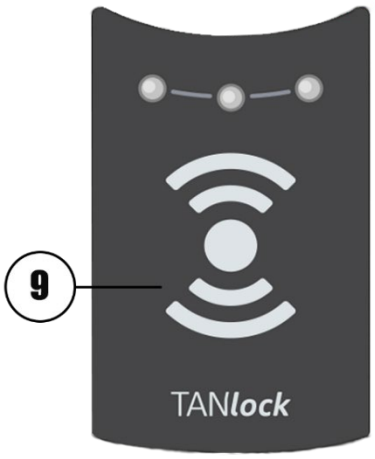


Abbildung 6: RFID-Modul

Pos. 9: RFID-Modul

4) Fingerprint

Abbildung 7: Fingerprint-Modul

Pos. 10: Fingerprint-Modul

5) Touch Display

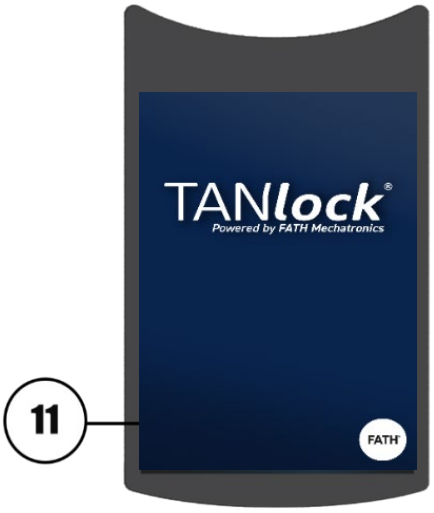


Abbildung 8: Touch Display Modul

Pos. 11: Resistives TFT-Display

iii) Schnittstellen
- Netzwerkanschluss RJ45 für PoE-Anschluss.
- 2 Kontaktsteckplätze für Micro JST-Buchse für Türkontakte, Rastermaß 1,25 mm (keine galvanische Trennung).
- 1 Micro JST-Buchse für Relais-Anschluss, Rastermaß 1,25 mm.
- USB-C Schnittstelle.

c) Montage und Schrankausschnitte

Zur Montage des TANlock sind folgende Ausstanzungen an der Schranktür notwendig.

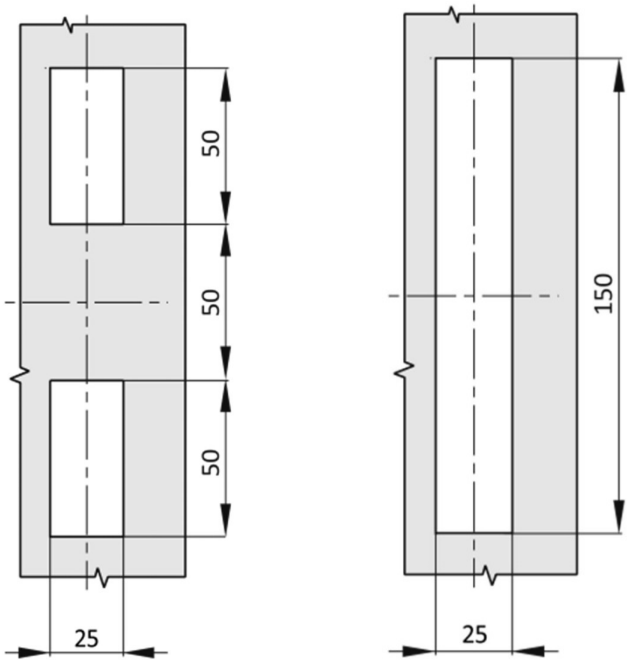


Abbildung 9: Schrankausschnitte für den TANlock

HINWEIS

Verwenden Sie die kurze Abdeckkappe, wenn die Schranktür über 2 Ausstanzungen (je 50 mm x 25 mm) verfügt.

Verwenden Sie die lange Abdeckkappe, wenn die Schranktür über 1 Ausstanzung (150 mm x 25 mm) verfügt.

d) Relais Anschluss

Der Anschluss erfolgt über einen 3 Pin JST 1.25 mm Anschluss.

Relais Interface:

Max voltage	DC 28V
Max load current	100mA
Max resistant (on)	5 Ohm

Eine Diode ist erforderlich, um das Relais vor induktiven Rückkopplungen auf der Lastseite zu schützen.

http://<IP Address>/web/v1/relais/set?id=0

http://<IP Address>/web/v1/relais

Beispiel:

Close relay 0 -https://< IP Address>/ /lab/ext/relais/write/0/1

Close relay 1 -https://< IP Address>//lab/ext/relais/write/1/1

http://<IP Address>/web/v1/relais/set?id=0

SNMP-Walk zur Anzeige des Status von Türsensoren und Relaisattributen des Gerät 1 und 2 können als Halbleiterrelais mit höherer Lastkapazität entweder AC oder DC betrieben werden.

e) Anschluss der Türkontakte

Der Anschluss erfolgt über 2-Draht-Leitung mit 1,25 mm Raster-Buchse an Anschluss 11 oder 13, (siehe Abbildung 3).

Um einen Türkontakt anzuschließen, gehen Sie wie folgt vor:

1. Führen Sie das Kabel vor der Montage des TANlock durch die Abdeckung.
2. Schließen Sie das Sensorkabel an.
   Als Sensor kann jeder stromschließende Kontakt (z. B. Reed Kontakt) dienen.
   - Der Sensor ist verbunden.

Der Sensor für den Türkontakt ist angeschlossen.

2) Verbindung mit dem TANlock

Die Standardeinstellungen des TANlock sind:

DHCP deaktiviert / feste IP: http://192.168.0.90, Subnetmask: 255.255.255.0

VLAN deaktiviert.

Für die Verbindung über Ethernet muss sich Ihr PC im gleichen IP-Subnetz befinden wie der TANlock.

a) Verbindung mit dem TANlock über einen Webbrowser

Zum Verbinden des TANlocks über einen Webbrowser kann wie folgt vorgegangen werden:

- Öffnen des Webbrowsers (Z.B. Google Chrome)
- Eingabe der IP-Adresse http://192.168.0.90 in der Adresszeile
- Im Anmeldefeld den Namen „api“ und das Passwort „lab“ eingeben und anschließend den Button „Login“ klicken
- Nun sind Sie mit dem TANlock verbunden und können weitere Einstellungen vornehmen

b) Manuelle Vergabe einer festen IP-Adresse

Um eine feste IP-Adresse manuell festzulegen, gehen Sie wie folgt vor:

1. Gehen Sie im Reiter auf „Settings“→ „General“ →“ Set Network“

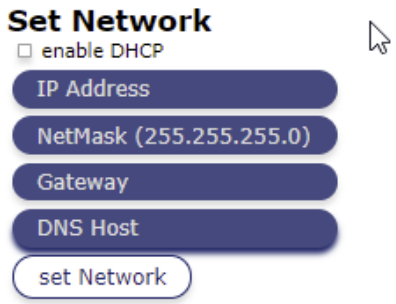


Abbildung 19: Karteikarte "Set Network"

2. Geben Sie in das erste Feld die IP-Adresse ein.
3. Geben Sie in das zweite Feld die NetMask ein.
4. Geben Sie in das dritte Feld das Gateway ein.
5. Geben Sie in das letzte Feld die DNS-Host ein.
6. Klicken Sie auf „Set Network“ um die Eingaben zu speichern.

7. Führen Sie einen Reboot durch „Settings“→ „Reboot“→“Reboot“
8. Der TANlock wird mit der Speicherung neu gestartet.

✓ Die feste IP-Adresse ist festgelegt.

c) Manuelle Benutzung von DHCP

Um eine dynamische IP-Adresse zu verwenden, gehen Sie wie folgt vor:

1. Gehen Sie im Reiter auf „Settings“→ „General“ →“ Set Network“
2. Aktivieren Sie das Kästchen „enable DHCP“
3. Führen Sie einen Reboot durch „Settings“→ „Reboot“→“Reboot“
4. Der TANlock wird mit der Speicherung neu gestartet.

✓ Die dynamische IP-Adresse ist festgelegt

3) Navigation in der Web UI

Die Web UI des TANlocks ist in folgende Reiter verteilt:

- Home
- User
- Medium
- Log
- RBAC
- API
- AuthSinks
- Settings

a) Home

Unter der Startseite „Home“ sind folgende Informationen zu finden:

- **Time:**
  Time gibt die aktuelle Uhrzeit und Datum an.
- **Device:**
  Unter Device steht der Produktname und die zugehörige Seriennummer des TANlock.
- **Network:**
  Unter Network stehen folgende Informationen: IP-Adresse, Netmask und Macadresse.
- **Sensor:**
  Die interne Sensorik gibt nachfolgende Zustände an: TANlock offen oder geschlossen, Hebel gedreht oder nicht gedreht, Motor in Bewegung oder still.
- **Version:**
  Firmware Informationen.
- **Relais:**
  Externe Anschaltung von bis zu zwei Signalgebern möglich: false= inaktiv und true= aktiv.
- **External:**
  Anschaltung von zwei Türkontakten möglich.
- **Session Information:**
  Angemeldeter User und Ablauf der Session nach 900 Sekunden (Danach Neuanmdelung nötig).

b) Settings

In der Karteikarte „Settings“ stehen folgende Felder zur Verfügung:

- **General:** Allgemeine Einstellungen:

1. **„Set Time“**: Entweder manuelle Eingabe von Zeit und Datum oder Synchronisation mit dem Browser.
2. **„Alive indication“**: In dem ausgewählten Intervall (Standard 300 Sekunden) wird ein Funktionstest der LEDs anhand eines Lauflichts signalisiert.
3. **„Set VLAN“**: Aktivierung eines VLAN möglich.
4. **„Set Network**“: Konfiguration der manuellen IP-Umgebung oder Aktivierung von DHCP möglich.
5. **„Set NTP“**: Manuelle Eintragung eines Zeitservers möglich.
6. **„Service-Mode“**: TANlock wird in die Auslieferungsstellung versetzt (Einstellungen werden nicht zurückgesetzt!).

- **Alarming:**
  - „Set Used Door Contacts“: Aktivieren und Deaktivieren der Türkontakte
  - „Set DOTL Time“: Einstellen des Voralarms (Pre Dotl Time) und des Hauptalarms (Dotl Time)

- **SSL**: einfügen von Zertifikaten

- **TANlock Auth Module:**
  - „Set TANlock Authentication Module“: Auswählen des entsprechenden TAMs (TANlock Authentifizierungsmodul)
  - „Set TANlock Device Type“: Auswahl zwischen:
    - TANlock
    - Security Drawer (Sicherheits Schublade)

- **Medium Implementations:**
  Aktivierung und Deaktivierung der zur Auswahl stehenden Medien.

- **Updater:**
  - Updater Config: Hier können Sie automatische Updates für den TANlock konfigurieren. Die Konfiguration finden Sie im Kapitel 9.c)
  - Update: Hier kann manuell ein Update für den TANlock gesucht und heruntergeladen werden.

- **Discovery:**
  „Set Discovery“: Konfigurierbarer Anmeldevorgang des TANlocks an ein Fremdsystem.

- **„Monitoring-Events“:**
  Logging sämtlicher Events am TANlock.
  HTTP: Ein HTTP-Event wird an eine URL gesendet.
  Syslog: Ein Syslog-Event wird an Zieladresse gesendet.
  SNMP-Trap: Ein Event-Trap wird an Zieladresse gesendet.

- **Sensors**:
  Aktivierung, Deaktivierung und Einstellung von optionalen Sensoren (Derzeit vorhandene Sensoren: Temperatur, Luftfeuchte und Vibrationssensor).

- **Reboot**:
  Neustart des TANlocks.

c) AuthSinks

Unter AuthSinks kann eine LDAP-Konfiguration vorgenommen werden. Mehr dazu im Kapitel 5. c).

Mit dem Protokoll LDAP lassen sich eine große Menge an Benutzerdaten schnell abfragen. Als Protokoll wird LDAP vorrangig für folgende Zwecke eingesetzt:

d) API

In der Karteikarte „API“ sind folgende Einstellungen zu finden:

1. **„SNMP“**: Aktivierung und Einstellung der SNMP-Befehle.
7. **„MIB**“: Beschreibung der SNMP-Befehle zum Download für Integrierung in Monitoring Software.
8. **„SNMP-Version“**: Version v1, v2c oder v3 möglich.
9. **„Community-Settings“**: Benennung der Benutzergruppe.
10. **„HTTP Based APIs“**: hier lässt sich die Dokumentation über die APIs öffnen.
11. **„Rest“**=Restful, standardmäßig aktiviert.
12. **„Web“**: standardmäßig aktiviert.

Für die API-Konfigurationen rufen Sie bitte Kapitel 5 „Sicher konfigurieren über die Web-API auf.

e) RBAC

Unter „RBAC“ können die Rollen der User und die Berechtigungen zugeteilt werden. Dies ist über die folgenden Einstellungen möglich:

Roles:

Hier befinden sich die vordefinierten Rollen mit ihren Berechtigungen. Über den Button „Add Roles“ können neue Rollen mit ihren ausgewählten Berechtigungen erstellt werden.

Managementusers:

Hier können Managementuser mit den unterschiedlichen Rollen angelegt und verwaltet werden.

f) Log

Unter der Karteikarte „Log“ werden alle Events am TANlock getrackt.

Unabhängig von der Verwaltung und Gestaltung der Benutzerverwaltung bietet der TANlock eine Überwachung. Folgende Ereignisse werden dabei vom TANlock unter dem Reiter „Log“ erfasst und protokolliert:

- TANlock ist gestartet: „STARTUP“.
- Eingabe wurde gestartet: „MEDIUM_INPUT“.
- Eingabe wurde berechtigt: Event „AUTH“.
  uid= angelegter User (siehe Reiter „Users“), identifier = zugeordneter PIN, type = Benutztes Medium für Authentifizierung (siehe „Settings“ → „Medium Implementation“).
- Falsche PIN-Eingabe: Rote LED leuchtet am TANlock auf, Event „AUTH“ gibt die Eingabe wieder.
- Schloss wurde entriegelt: Event „HAL_LOCKED“: „false“
- Schloss wurde verriegelt: „HAL_LOCKED“: „true“
- Hebel wurde gedreht: „HAL_HANDLE“: „true“
- Hebel wurde zurück in Ausgangsstellung gedreht: „HAL_HANDLE“: „false“
- Türkontakt wurde geöffnet: „EXT_CHANGED“: „false“= geöffnet.
- Türkontakt wurde geschlossen: „EXT_CHANGED“: „true“= geschlossen.

g) Users

In der Karteikarte „Users“ können berechtigte Benutzer über den Button „Add User“ angelegt werden. Diese können hier ebenfalls verwaltet werden. Mehr dazu finden Sie im Kapitel 4. b) Rollenmanagement.

h) Medium

In der Karteikarte „Medium“ stehen folgende Felder zur Verfügung:

Fingerprint: Hier werden Fingerprints den Usern angelegt, zugeordnet oder gelöscht werden. Es können maximal 32 Fingerprints hinterlegt werden.

All Mediums: Hier werden die unter „Settings“ → „Medium Implementations“ aktivierten Medien den Usern zugeordnet.

4) Rechtemanagement

a) Rollen verwalten

Unter der Karteikarte „RBAC“→ „Roles“ können verschiedene Rollen mit verschiedenen Permissions (API, lesen, schreiben und andere) erstellt und gewartet werden.

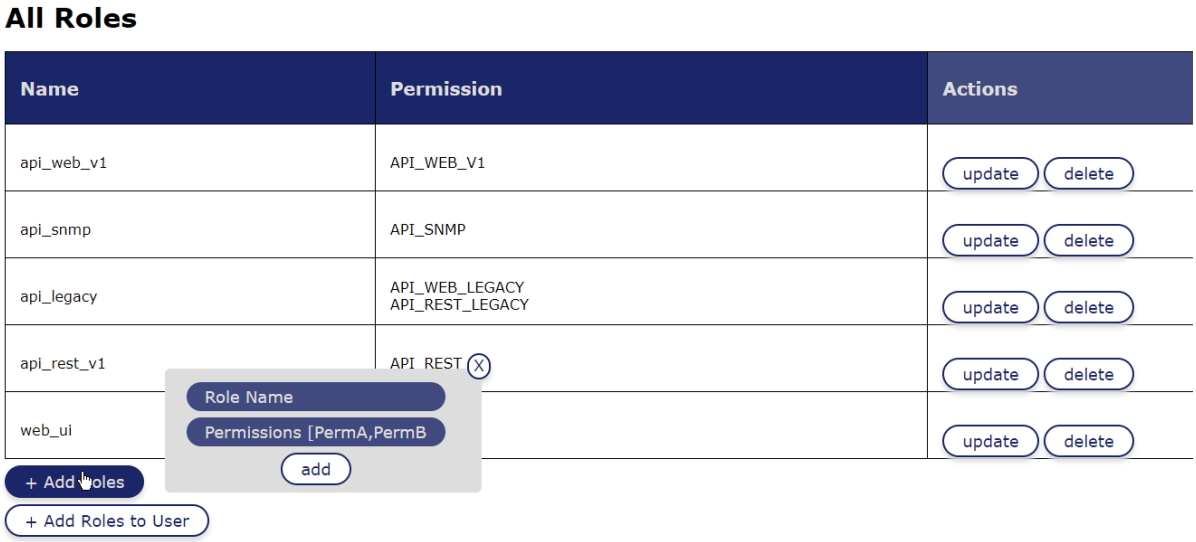


Abbildung 20: Rollenmanagement.

Über den Button „+Add Roles“ können neue Rollen mit den entsprechend gewünschten Permissions erstellt werden. Dies muss mit „add“ bestätigt werden.

b) Rollen Zuweisung (Autorisieren von Benutzern)

Hier befinden sich die vordefinierten Rollen mit ihren Berechtigungen. Um Benutzern Rollen zu zuweisen und ihnen damit bestimme Erlaubnisse zu erteilen, muss Karteikarte „RBAC“→ „Roles“ geöffnet werden. Dort kann über den Button „+ Add Roles to User“ einem bestehenden User Rechte zugeschrieben werden.

In das aufgehende Feld müssen dann der User Name, sein Passwort und die gewünschten rollen eingetragen werden. Mit dem Button „update“ wird dies gespeichert.

Die Voreingestellten Rollen sind:

- api_web_v1 (Mit der API-Permission „API_WEB_V1“)
- api_SNMP (Mit der API-Permission „API_SNMP“)
- api_legacy (Mit der API-Permission „API_WEB_LEGACY“ und „API_REST_LEGACY“)
- api_rest_v1 (Mit der API-Permission „API_REST_V1“)
- web_ui (Mit der API-Permission „WEB_UI“)

Einen Überblick über die Permissions finden Sie im hier.

api Permissions	write Permissions	read Permissions	other Permissions
WEB_UI API_SNMP API_WEB_LEGACY API_REST_LEGACY API_WEB_V1 API_REST_V1	WRITE_INFO WRITE_RELAIS WRITE_USER WRITE_MEDIUM WRITE_RBAC_USERS WRITE_RBAC_ROLES WRITE_DISCO WRITE_NETWORK WRITE_FLOCK WRITE_LOG WRITE_LOG_SINK WRITE_UPDATER WRITE_RESTAPI_CONFIG WRITE_WEBAPI_CONFIG WRITE_SENSORS WRITE_SENSOR_ALARMINGS WRITE_HWMOD WRITE_SSL WRITE_AUTHSINKS	READ_INFO READ_STATE READ_EXTERNALS READ_RELAIS READ_USER READ_MEDIUM READ_CURRENT_USER READ_AUTH_CHAIN READ_RBAC_USERS READ_RBAC_ROLES READ_RBAC_PERMISSIONS READ_DISCO READ_NETWORK READ_FLOCK READ_LOG READ_LOG_SINK READ_UPDATER READ_RESTAPI_CONFIG READ_WEBAPI_CONFIG READ_SENSORS READ_SENSOR_ALARMINGS READ_HWMOD READ_AUTHSINKS	REBOOT TRIGGER_UPDATER DOWNLOAD_UPDATER DO_OPEN DO_INPUT SET_TIME RELOAD_RBAC READ_SENSORS WRITE_SENSORS READ_SNMP_CONFIG WRITE_SNMP_CONFIG PREPARE_OPEN

c) Managementuser

Unter „RBAC“→ „Managementuser“ finden Sie die Einstellungen zur Verwaltung der Managementuser. Durch diese können den Benutzern die Rollen und Berechtigungen zugeteilt werden.

d) Konfiguration der Authentifizierungsmethode

Als elektronisches Schloss können Sie bei TANlock die zugangsberechtigten Personen und deren Schlüssel elektronisch ohne Veränderungen des Schlosses anpassen.

Generelle Funktionsweise:

TANlock bietet Ihnen verschiedene Möglichkeiten die Personen, die zum Öffnen des Schlosses berechtigt sind festzulegen. *Systembedingt können über die Tastatur des TANlock nur die vier* Ziffern 1, 2, 3, 4 als mögliche Werte für die Eingabe dienen. Sie können bis zu 5000 Benutzer lokal auf dem Gerät speichern. Bei der Authentifizierung mit dem Fingerprint Modul können maximal 32 Fingerprints gespeichert werden.

Der Zugang wird weiterhin ermöglicht, falls bei einer auf LDAP basierenden Lösung die Verbindung zum LDAP-Dienst ausfällt.
Dies bietet sich ebenfalls an, wenn keine zentrale Verwaltung von Benutzerberechtigungen erfolgt und eine autarke Schlosslösung angestrebt wird.

Um bei dem TANlock 3 einen User und ein Medium anzulegen, muss wie folgt vorgegangen werden:

Jedes TAM hat als Basis RFID. Weitere Optionen wie z.B. PIN werden über das RFID gelegt.

1. Device-Type auswählen:

i) “Settings” → “TANlock Auth Module“ → „Set TANlock Device Type”

ii) TANlock oder Sicherheitsschublade auswählen

2. TAM aktivieren:

i) „Settings“ → „TANlock Auth Module“ → „Set TANlock Authentication Module”

ii) Das gewünschte TAM auswählen

iii) Mit “set” bestätigen

iv) Reboot unter “Settings”→ “reboot”

3. Aktivieren des gewünschten Mediums:
Dazu gehen Sie bitte auf dem TAB „Settings“ in den Menüpunkt „Medium Implementation“:

Abbildung 20: Karteikarte "Medium Implementation"

Aktivieren Sie bei:
TANlock 3 **RFID**: 19_card_uid

TANlock 3 **RFID + „ok“ PIN / Zahlen PIN:** zusätzlich zu 19_card_uid auch 02_unique_pin

TANlock **3 Fingerprint**: nur 20_finger aktivieren. Bei dem Fingerprint Modul müssen Sie nach der Aktivierung ein Reboot unter „Settings→ Reboot→ Reboot“ durchführen.

All Medium Implementations

Mediumimp	Actions
01_pin_input	activate
17_card_iclass_uid	activate
50_oss_so_legic	activate
19_card_uid	activate
52_oss_so_mifare	activate
21_card_fingerprint	activate
20_finger	deactivate
15_legic_sandbox	activate
14_card_legic_advant	activate
02_unique_pin	activate
51_oss_so_desfire	activate
11_card_desfire	activate
12_card_mifare	activate
18_card_legic_uid	activate
30_hid_module_card_uid	activate
31_inflx	activate

Abbildung 21: „All Medium Implementations“

4. Anlegen eines Users:

1. Gehen Sie bitte auf dem Reiter auf die Karteikarte „Users“ und klicken auf den Button „+ Add User“

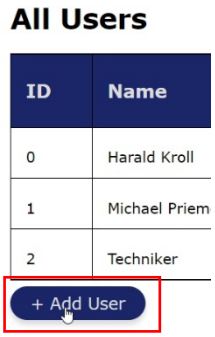


Abbildung 22: „Add User“

2. Füllen Sie folgende Information ein:
   Zeile 1: Vor- und Nachnamen des neuen Users
   Zeile 2: Vor-; Nachnamen oder Spitznamen etc.
   Zeile 3: Optional können Sie hier eine Personalnummer des Users hinterlegen

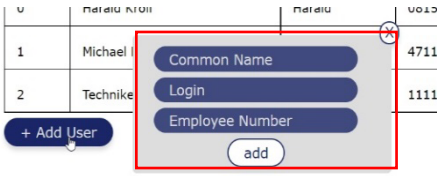
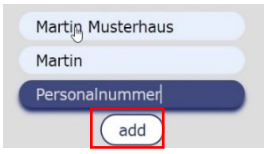


Abbildung 23: „Add User“

3. Kicken Sie nun Bitte auf den Button „Add“
   Der User ist jetzt auf dem TANlock angelegt.



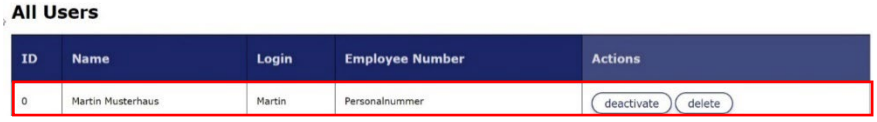


Abbildung 24 und 25: „Add User“ und Übersicht über die erstellten User

5. Dem User sein Medium zuweisen:

RFID-Karte zuweisen:

Für das zuweisen einer RFID – Karte, halten Sie die entsprechende RFID Karte vor einen TANlock.

a. Gehen Sie bitte nun auf die Karteikarte „Log“:

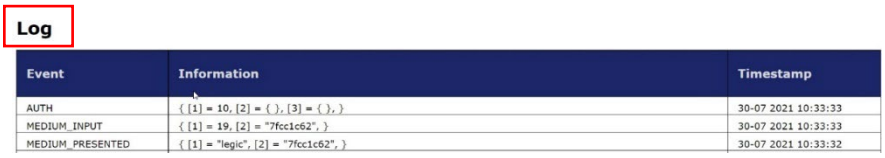


Abbildung 26: Karteikarte „Log“

Sie sehen nun unter dem Event „Medium Input“ in den Anführungszeichen eine Karten UID.

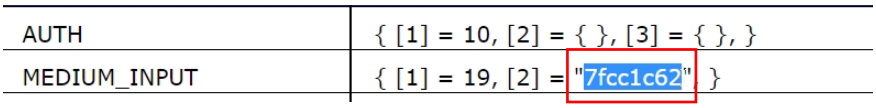


Abbildung 27: „Medium Input“ mit der UID

Kopieren Sie bitte nun die UID.

b. Gehen Sie bitte jetzt auf die Karteikarte „Medium“ → „All Mediums“

Abbildung 28: „Add New Identificationpath“

c. Drücken Sie bitte hinter dem dazugehörigen User den Button „Add New Identificationpath“

Zuordnen einer RFID-Karte:

Wählen Sie nun das Medium aus:

19: RFID Karten

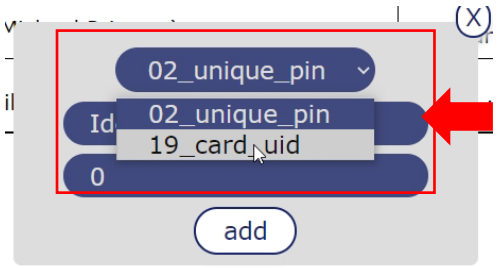


Abbildung 29: Auswählen des Identifikationspfades

Fügen Sie jetzt die Karten UID aus 3. a in

Zeile 2 „Identifier“ ein.

Zeile 3 lassen Sie bitte unverändert.

d. Drücken Sie jetzt den Button „Add“

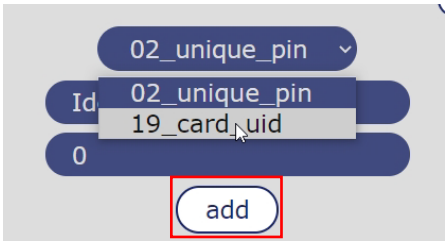


Abbildung 30: Bestätigen des Identifikationspfades

✓ Dem User wurde nun die entsprechende RFID – Karte zugeordnet.

PIN zuweisen:

1. Möchten Sie dem User auch einen Zahlen – PIN zuweisen, dann gehen Sie erneut zu Punkt **3. a** und wählen in Zeile 1 **„02_unique_PIN“** aus .

2. Tragen in Zeile 2 **„Identifier“** eine Zahlenkombination aus den Zahlen 1-4 ein.

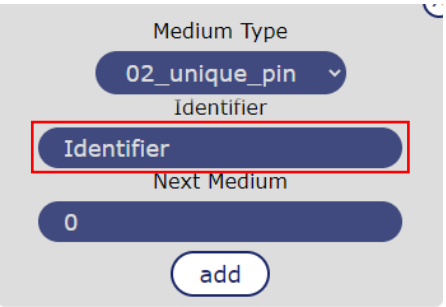


Abbildung 31: Anlegen des Codes über das Feld „Identifyer“

3. Drücken Sie jetzt den Button **„Add“**

   ✓ Dem User wurde nun der entsprechende Zahlen PIN zugeordnet.

Zum Abschluss gehen Sie bitte unter „Settings“ auf den TAB „Reboot“ und klicken dort auf den Button „Reboot“. Der TANlock wird nun neu gestartet und sämtliche Eingaben sind gespeichert.

Fingerprint zuweisen:

1. Um einem User einen Fingerprint zuzuweisen, klicken Sie im Reiter auf „Medium→ Fingerprint“.

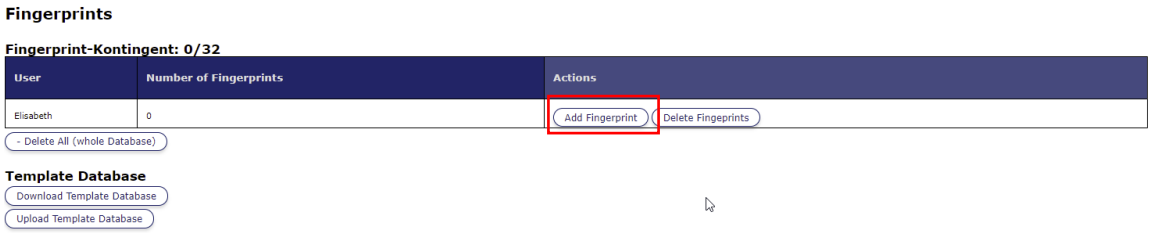


Abbildung 31: Fingerprint als Identifikationspfad

2. Klicken Sie bei dem ausgewählten User auf „Add Fingerprint“. Legen Sie Ihren Finger erst auf den Scanner, wenn die LED blinkt!

   a) Rote LED blinkt: Finger auf den Scanner legen bis die blaue LED blinkt und Finger wieder entfernen.
   b) Blaue LED blinkt: Finger auf den Scanner legen bis die gelbe LED blinkt und Finger wieder entfernen.
   c) Gelbe LED Blinkt: Finger auf den Scanner legen bis rote LED dauerleuchtet und Finger wieder entfernen.

   ✓ Nun ist der erste Finger abgespeichert und zugewiesen.

Pro User können nur maximal zwei Fingerprints zugewiesen werden!

5) Sicher konfigurieren über die Web API

Über die Web API-Schnittstelle können zwei Anwendungen, die voneinander unabhängig sind, problemlos interagieren und Daten austauschen. Die folgenden Konfigurationen stehen zur Verfügung:

a) http Konfiguration

1. Öffnen Sie den Tab „Settings“→ „Event Monitoring“
2. Aktivieren Sie das Kästchen „Enable“
3. Bestätigen Sie die Eingabe mit „set Config“
4. Führen Sie einen Reboot unter „Settings“→ „reboot“ durch
5. Nun können Sie unter „Settings“ → „Event Monitoring“ das zugehörige Feld ausfüllen.
6. Die Eingaben bestätigen Sie mit dem Button „set Config“

Abbildung 32: http-Konfiguration

b) SNMP Konfiguration

Mit der SNMP (Simple Network Monitoring Protocol) API können Sie Verwaltungsinformationen in Netzwerken übertragen, sowie Netzwerkgeräte steuern und überwachen.

Die Zustände des TANlocks können dadurch an die Monitoring Software weitergegeben werden. Unter der Karteikarte „API“ → „MIB“ finden Sie das MIB-File zum Download für die Integrierung in die Monitoring Software.

Das SNMP Monitoring wird über die Web API konfiguriert. Dazu gehen Sie wie folgt vor:

1. Öffnen Sie die Karteikarte „API“
2. Das Feld „enable SNMP“ aktivieren

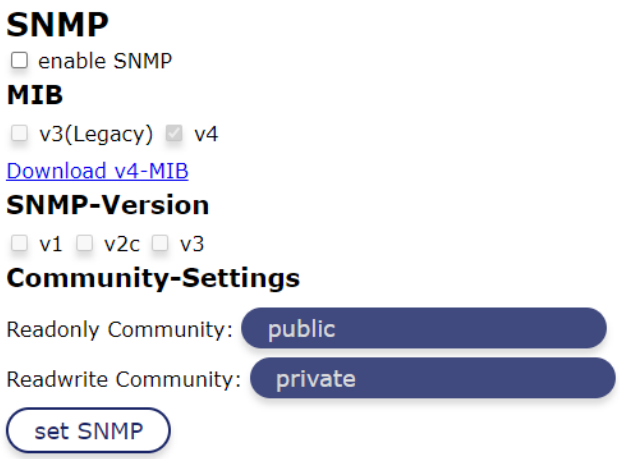


Abbildung 33: SNMP-Konfiguration

3. Auswählen, welche Version der Management Information Base (MIB) verwendet werden soll (diese kann nach der Auswahl heruntergeladen werden)
4. Danach kann die entsprechende SNMP-Version ausgewählt werden.
   a. SNMP-Version v1: Unter den „Community-Settings“ kann die entsprechende Benutzergruppe benannt werden
   b. SNMP-Version v2c: Unter den „Community-Settings“ kann die entsprechende benutzergruppe benannt werden
   c. SNMP-Version v3: Hier kann die Engine-ID bestimmt werden (Default Engine ID= 1234) und im Anschluss kann die Authorisierung über den Button User-Management angepasst werden (siehe Abbildung)

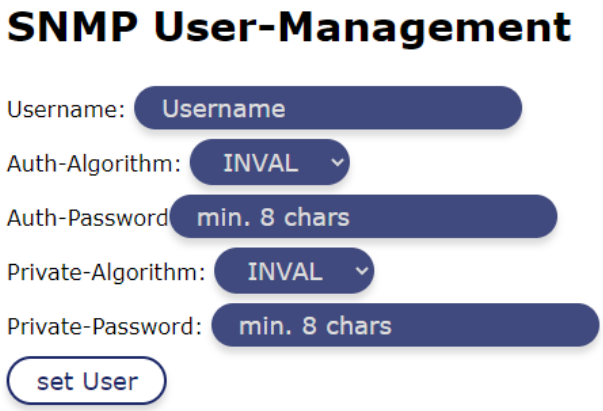


Abbildung 34: SNMP User-Management Konfiguration

5. Unter den „Community-Settings“ kann dann die entsprechende Benutzergruppe benannt werden
6. Bestätigen Sie die Eingabe mit dem Button „Set“
7. Führen Sie einen Reboot durch

✓ Sie haben das SNMP Monitoring erfolgreich konfiguriert

c) snmptrap Konfiguration

1. Konfigurieren der snmptrap:
   a. Öffnen Sie den Tab „Settings“ → „Event-Monitoring“
   b. Aktivieren Sie das Kästchen „Enable“
   c. Bestätigen Sie die Eingabe mit dem Button „set Config“
   d. Führen Sie unter „Settings“→ „Reboot“ einen Reboot durch
   e. Öffnen Sie erneut den Tab „Settings“→ „Event Monitoring“
   f. Tragen Sie das Target in das Feld „Target“ ein
   g. Bestätigen Sie die Eingaben mit dem Button „set Config“

Abbildung 35: snmptrap-Konfiguration

d) SysLog Konfiguration

Syslog ist ein Standard-Protokoll, das verwendet wird, um Systemprotokoll- oder Ereignismeldungen an einen spezifischen Server zu senden, der als Syslog-Server bezeichnet wird.

Das SysLog Monitoring wird über die Web API konfiguriert. Dazu gehen Sie wie folgt vor:

1. Öffnen Sie die Karteikarte „Settings“→ „Monitoring-Events“ → „SysLog“

2. In dem Feld SysLog muss das Kästchen „set Enable“ aktiviert sein

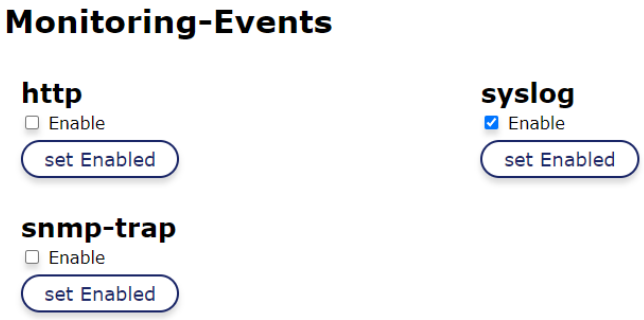


Abbildung 36: Monitoring-Events in der Web-UI

3. Führen Sie einen Reboot durch
4. In dem Feld kann das gewünschte Target hinterlegt werden

Abbildung 37: syslog Konfiguration

5. Mit dem Button „set Config“ werden die Eingaben gespeichert

✓ Sie haben das SysLog Monitoring erfolgreich konfiguriert

Die Protokolle der Events am TANlock können Sie unter der Karteikarte „Log“ aufrufen.

e) LDAP Konfiguration

Das LDAP Monitoring wird über die Web UI konfiguriert.

Dazu muss die Karteikarte „AuthSinks“ ausgewählt werden. Dort kann dann LDAP konfiguriert werden.

Voraussetzungen für die Konfiguration des TANlocks an LDAP:

- Der TANlock besitzt eine Netzwerkverbindung
- Das TAM (TANlock Authentication Module) ist konfiguriert und besitzt einen zugewiesenen Benutzer

- Die Host-URL des Host PCs liegt vor
- Die LDAP Port-Nummer liegt vor

Für die LDAP-Konfiguration gehen Sie wie folgt vor:

1. Öffnen Sie die Karteikarte „AuthSinks“
2. In den Feldern „LDAP Config“ müssen folgende Daten hinterlegt werden:
    a. Das Kästchen Enabled muss ausgewählt und der Button „Enable“ bestätigt werden
    b. Führen Sie einen Reboot unter dem Tab „Settings“→ „Reboot“ durch
    c. Fügen Sie in das Feld „Host-URL” die URL des Host-PCs sowie die LDAP Port-Nummer ein, wie beispielsweise “192.168.0.200:10389”
    d. In dem Feld „User“ tragen Sie den Namen des LDAP Users ein, beispielsweise “uid=admin, ou=system”
    e. Ein Passwort müssen ausgewählt und in der darauffolgenden Zeile bestätigt werden:
        i. Legen Sie ein Passwort fest und tragen Sie dieses in das Feld „Password“ und „(repeat)“ ein
        ii. Lassen Sie das Feld "Use TLS" leer
        iii. Lassen Sie das Feld "Base DN" leer
        iv. Bestätigen Sie die Eingaben mit dem Button "Save"

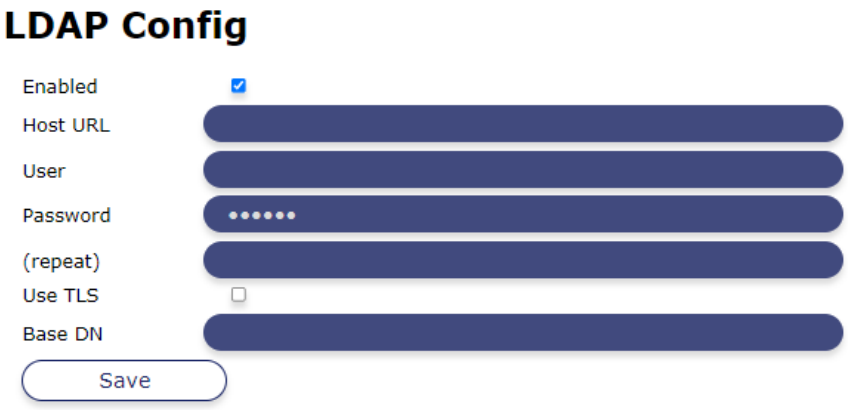


Abbildung 38: LDAP-Konfiguration

    f. Konfigurieren Sie "Medium Queries" unter "AuthSinks" -> "LDAP":
        i. Lassen Sie das Feld "Attributes" leer
        ii. Schreiben Sie „ou=system“ in das Feld "Base"

iii. Schreiben Sie „(ou=*)“ in das Feld "Filter"
iv. Schreiben Sie „base“ in das Feld "Scope"
v. Bestätigen Sie die Eingaben mit dem Button "Save"

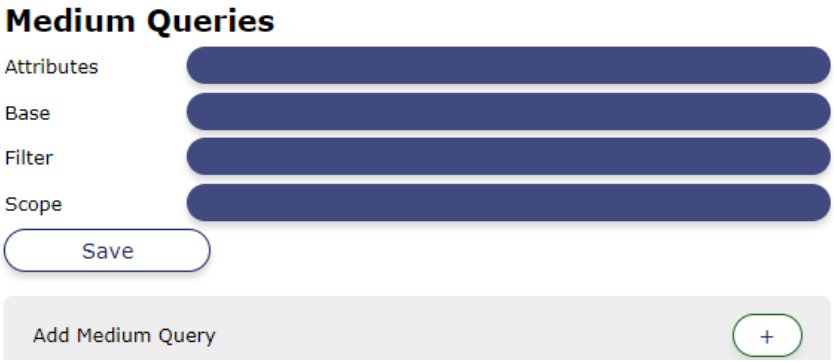


Abbildung 39: Konfiguration der Medium Queries

g. Konfigurieren Sie "Medium Mapper" unter "AuthSinks" → "LDAP":
   i. Schreiben Sie den folgenden Inhalt in das Textfeld:

```json
{"uid":0,"start": true,"next": 0}
```

   ii. Bestätigen Sie die Eingaben mit dem Button "Save"

Abbildung 40: Konfiguration des Medium Mapper

h. Konfigurieren Sie "User Queries" unter "AuthSinks" → "LDAP" (Derselbe Inhalt wie in dem Feld "Medium Queries"):
   i. Lassen Sie das Feld "Attributes" leer
   ii. Schreiben Sie „ou=system“ in das Feld "Base"
   iii. Schreiben Sie „(ou=*)“ in das Feld "Filter"

iv. Schreiben Sie „base“ in das Feld "Scope"
v. Bestätigen Sie die Eingaben mit dem Button "Save"

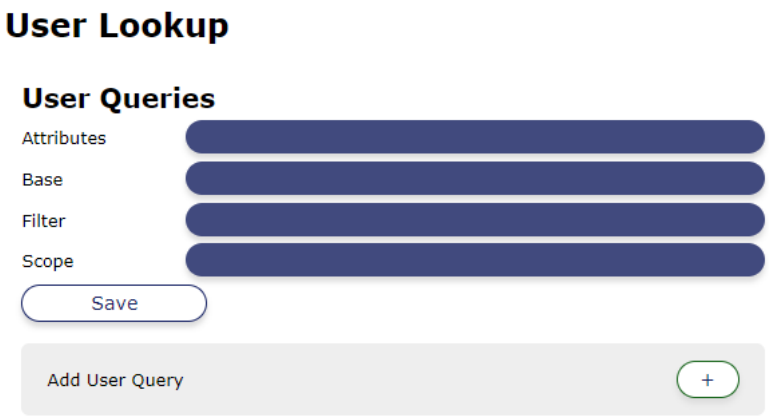


Abbildung 41: Konfiguration der User Queries

i. Konfigurieren Sie "User Mapper" unter "AuthSinks" → "LDAP":
   i. Schreiben Sie die folgenden Eingaben in das Textfeld:

```json
{"uid":0,"active": true}
```

   ii. Bestätigen Sie die Eingaben mit "Save"

Abbildung 42: Konfiguration des User Mapper

✓ Sie haben das LDAP Monitoring erfolgreich konfiguriert

6) Benutzen von Client Zertifikaten

Server- oder SSL-Zertifikate haben ähnliche Aufgaben wie Clientzertifikate. Der Unterschied besteht darin, dass Clientzertifikate den Client oder die Einzelperson identifizieren und mit Server- oder SSL-Zertifikaten der Betreiber der Website authentifiziert wird.

Der Webbrowser und der TANlock tauschen über die Clientzertifikate einen Schlüssel aus. Dabei müssen der TANlock und der Browser beide dieselben Zertifikate haben.

Der Webbrowser bzw. TANlock stellt eine Verbindung mit dem Server her und validiert die Authentizität eines SSL-Serverzertifikats. Dies zeigt dem Benutzer, dass seine Interaktion mit der Website nicht von Dritten abgehört wird und die Website genau die ist, für die sie sich ausgibt. Damit wird eine Sichere Kommunikation ermöglicht.

Mit Client-Zertifikaten können Sie Benutzer authentifizieren, ohne einen von einem Anmeldebild gelieferten Benutzernamen oder ein Kennwort zu benötigen. Daher können Sie die Client-Zertifikate auch in Single-Sign-On-Umgebungen zu integrieren.

Für das Benutzen von Client Zertifikaten muss unter „Settings“ → „SSL“ das gewünschte Zertifikat hochgeladen werden.

Abbildung 43: Upload der SSL-Zertifikate

7) Einbinden des TANlock in eigene Monitoring-Software

a) Einbindung nur für das Monitoring

Eine Einbindung des TANlocks in eine Monitoring Software von Dritten kann über die Konfiguration von snmptrap und syslog erfolgen. Genaueres finden Sie im Kapitel 5. c) (snmptrap) und 5. d) (syslog).

b) Komplette Einbindung des TANlocks

Eine komplette Einbindung des TANlocks in eine Software von Dritten kann über die Integrierung des MIB-Files (Unter dem Tab „API“ → „SNMP“ → „MIB“ zu finden) in das Monitoring System realisiert werden.

Eine weitere Option für die Einbindung ist eine Konfiguration von SNMP oder syslog in Verbindung mit LDAP, OSS, Websockets oder der restful API .

8) Konfiguration der automatischen Updates

Um den TANlock automatisch Updaten zu lassen und somit immer die aktuelle Software zu verwenden, gehen sie wie folgt vor:

- Öffnen Sie den Tab „Settings“ → „Updater“
- Unter „Updater-Config“ muss im ersten Feld

„https://firmware.tanlock.com/data/tanlock-interface-STANDARD/STANDARD“

Stehen

- Im Feld darunter können Sie den authentication header einfügen
- Mit dem Button „set updater config“ bestätigen Sie die Eingaben

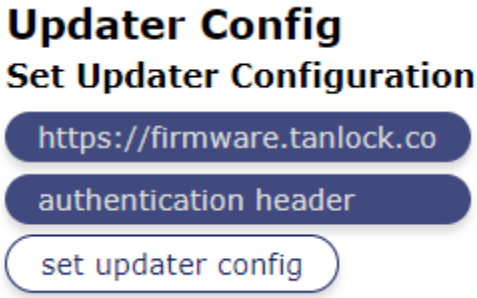


Abbildung 47: Updater Config Konfiguration