Konfigurierungshandbuch 2N Access Unit

v.2.43

www.2n.com

Inhalt:

1. Produktbeschreibung

Zu den 2N Zutrittseinheiten gehören die **2N Access Unit, die 2N Access Unit 2.0, die 2N Access Unit QR** und die **2N Access Unit M**. Die 2N Zutrittseinheiten bieten zusammen mit zusätzlicher Software und 2N IP Sprechanlagen eine komplette Zutrittskontrolllösung für jede Einrichtung.

Die 2N Zutrittseinheiten können in Kombination mit einem numerischen Tastenfeld als Codeschloss verwendet werden.

Die 2N Zutrittseinheiten können mit einem zweiten RFID-Kartenleser ausgestattet werden, der nicht nur berechtigten Personen den Zutritt zum Objekt ermöglicht, sondern auch Teil des Objektschutzsystems oder des Anwesenheitssystems in Ihrem Unternehmen wird.

Die 2N Zutrittseinheiten können mit einem Relaisschalter (optional mit zusätzlichen Relais und Ausgängen) ausgestattet werden, der zur Steuerung eines Elektroschlosses oder anderer angeschlossener Geräte verwendet werden kann. Die Zutrittseinheiten lassen sich sehr flexibel einrichten, z.B. wann und wie diese Schalter aktiviert werden sollen - per Code, automatisch, per Tastendruck, etc.

Im Handbuch werden die folgenden Symbole und Piktogramme verwendet:

Unfallgefahr

- **Richten sie** sich immer nach diesen Hinweisen, um Unfallgefahr zu vermeiden.

Warnung

- **Richten sie** sich immer nach diesen Hinweisen, um Beschädigung des Geräts vorzubeugen.

Hinweis

- **Wichtiger Hinweis** Nichteinhaltung dieser Hinweise kann zu mangelhaften Funktion des Geräts führen.

Tipp

- Nützliche Infos für einfachere und schnellere Verwendung oder Einstellung.

Bemerkung

- Verfahren und Ratschläge für wirksame Ausnutzung der Geräteeingenschaften.

2. Express-Begleiter durch die grundlegende Einstellung

Einloggen in die Web-Konfigurationsschnittstelle

Das Gerät wird mithilfe der Web-Konfigurationsschnittstelle konfiguriert. Für den Zugriff müssen Sie die IP-Adresse des Geräts kennen. Das Gerät muss mit dem lokalen IP-Netzwerk verbunden sein und gespeist werden.

Anmeldung mit einem Domänennamen

An das Gerät kann man sich durch Eingabe der Domäneadresse im Format *hostname.local anschließen* (z.B.: 2NAccessUnitM-00000001.local). Der Hostname eines neuen Geräts setzt sich aus dem Gerätenamen und der Seriennummer des Geräts zusammen. Die Formate für Gerätenamen im Hostnamen sind unten aufgeführt. Die Seriennummer wird ohne Bindestriche in den Domänennamen eingegeben. Der Hostname kann später in der Sektion System > Netzwerk geändert werden.

2N-Gerät	Bezeichnung des Geräts im Hostnamen
2N Access Unit	2NAccessUnit
2N Access Unit 2.0	2NAccessUnit20
2N Access Unit M	2NAccessUnitM
2N Access Unit QR	2NAccessUnitQR

Die Anmeldung mit einem Domänennamen hat bei der Verwendung der dynamischen IP-Adresse des Geräts einen Vorteil. Während sich die dynamische IP-Adresse ändert, bleibt der Domänenname derselbe. Sie können von einer vertrauenswürdigen Zertifizierungsstelle signierte Zertifikate für einen Domänennamen erzeugen.

Anmeldung mit IP-Adresse

Falls Sie die IP-Adresse schon kennen, geben Sie sie in ihren beliebten Webbrowser ein. Wir empfehlen die aktuelle Version des Webbrowsers Chrome, Firefox oder Internet Explorer (Edge) zu verwenden. 2N-Ausrüstung ist mit älteren Versionen der Webbrowser nicht voll kompatibel.

Details zur Anmeldung

Verwenden Sie für das erste Anmelden an der Konfigurationsschnittstelle den Namen admin und das Passwort 2n (Passwort, das nach dem Zurücksetzen der Anlage in den Ausgangsstatus gültig ist). Das Ausgangspasswort empfehlen wir nach dem ersten Anmelden sofort ändern – s. Einstellung im Menü **Dienste > Web Server** – Parameter Passwort. Merken Sie sich das gewählte Passwort gut bzw. notieren Sie sich dieses. Falls Sie das Passwort vergessen, werden Sie den Zutrittsterminal in den Ausgangsstatus zurücksetzen müssen (siehe Installationshandbuch zum jeweiligen Modell) und Sie werden dadurch gleichzeitig sämtliche durchgeführte Einstellungsänderungen verlieren.

Einstellung des Anschlusses an das lokale Netz (gilt für 2N Access Unit, 2N Access Unit 2.0 a 2N Access Unit M)

Das Gerät ist werkseitig so eingestellt, dass es automatisch eine IP-Adresse von einem DHCP-Server bezieht. Wenn Sie es also an ein Netzwerk anschließen, in dem ein DHCP-Server so konfiguriert ist, dass er allen neuen Geräten IP-Adressen zuweist, erhält auch das 2N-Gerät seine eigene IP-Adresse.

Die IP-Adresse kann entweder direkt über den Status des DHCP-Servers bezogen werden (entsprechend der MAC-Adresse auf dem Etikett) oder direkt vom Gerät über die Sprachfunktion mitgeteilt werden - siehe Installationshandbuch (Link unten).

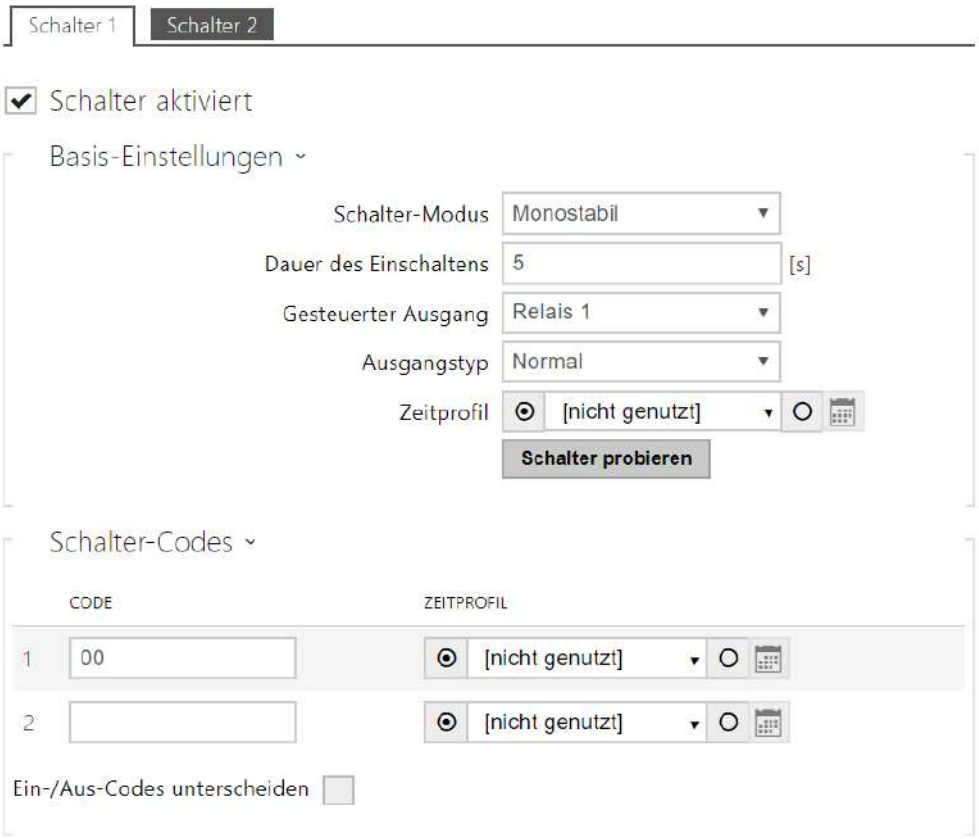
Wenn es in Ihrem Netzwerk keinen DHCP-Server gibt, müssen Sie das 2N-Gerät mit Hilfe der RESET-Taste auf eine statische Adresse einstellen, siehe Installationsanleitung des jeweiligen Modells. Ihr Interkom wird dann die Festadresse **192.168.1.100** erhalten, die Sie nur für das erste Anmelden benutzen, und Sie können sie danach ändern.

Upload Firmware

Nach erstem Anmelden zu 2N-Gerät empfehlen wir gleichzeitig, die Firmware upzugraden. Die neueste Gerätefirmware finden Sie unter 2N.com. Zum Firmware-Upgrade dient die Taste **Firmware-Upgrade** im Menü **System > Wartung**. Nach dem Upload der Firmware in die Anlage führt die Anlage einen Neustart durch und die Aktualisierung ist fertig. Die Aktualisierung dauert ungefähr eine Minute.

Einstellung der Einschaltung des elektrischen Schlosses

An das Gerät 2N kann ein elektrisches Türschloss anschließen, das mittels auf der nummerischen Tastatur eingegebenen Code bedient werden kann. Schließen Sie das elektrische Türschloss entsprechend der Anleitung im Installationshandbuch an das betreffende Modul an.



Geben Sie in der Registerkarte **Hardware > Schalter > Schalter 1** den Schalter mittels des Feldes Schalter freigegeben frei, stellen sie den Parameter Gesteuerter Schalter auf den Ausgang des Interkoms ein, an den das elektrische Türschloss angeschlossen ist. Stellen Sie danach einen oder mehrere Codes für das Einschalten des Schalters – des elektrischen Türschlosses ein.

3. Lizenzierte Funktionen

Die 2N Zutrittseinheiten können unterstützt Standardlizenzen, die bereits Teil des Geräts sind. Dies sind die Enhanced Integration, Enhanced Security und NFC-Lizenz. Die NFC-Lizenz kann man nur mit der Variante **2N Access Unit** oder **2N Access Unit 2.0** verwenden, die den 13.56 MHz Kartenleser enthält.

Eine Übersicht über die Lizenzen und deren Eigenschaften finden Sie in der folgenden Tabelle.

License	Features	2N Access Unit 1.0	2N Access Unit 2.0	2N Access Unit M
Enhanced Integration (Standard license part of the device)	Advanced switch setting options	✅	✅	✅
	HTTP API	✅	✅	✅
	Automation function	✅	✅	✅
	E-mail sending (SMTP client)	✅	✅	✅
	Automatic update (TFTP/HTTP client)	✅	✅	✅
	FTP client	✅	✅	✅
	SNMP client	✅	✅	✅
	TR-069	✅	✅	✅
	Synergis	✅	✅	✅
Enhanced Security (Standard license part of the device)	802.1x support	✅	✅	✅
	SIPS (TLS) support	✅	✅	✅
	Switch Blocking by Tamper	✅	✅	✅
	SRTP support	❌	❌	❌
	Silent alarm	✅	✅	✅
	Limit unsuccessful access attempts	✅	✅	✅
	Anti-Passback	✅	✅	✅
	Scrambled keypad	❌	❌	❌
NFC (Standard license part of the device)	NFC support	✅	✅	✅
Lift Control Support	Lift Control	✅	✅	✅

✅ – Enthält aus der Fertigung

⭐ – Lizenzierte Funktion, ist nachzukaufen

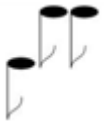
❌ – Kann man nicht verwenden

4. Signalisierung der Betriebsstatus

Die 2N Zutrittseinheiten können signalisiert mittels Tonmeldungen Änderungen und Übergänge zwischen den verschiedenen Betriebszuständen. Für jede Art der Statusänderung existiert eine andere Meldungsart. Die Liste der einzelnen Meldungen ist in der folgenden Tabelle angeführt:

Anmerkung

- *Man kann die Signalisierung mancher der vorstehenden Zustände ändern, siehe Kapitel Nutzertöne.*

Töne	Bedeutung
	**Interne Applikation gestartet** Nach dem Einschalten der Einspeisung oder nach dem Neustart das Gerät ist der Start der internen Applikation in Gang gesetzt. Der erfolgreiche Start der internen Applikation wird durch diese Tonkombination signalisiert.
	**An das lokale Netz angeschlossen, IP-Adresse erhalten** Nach dem Start der internen Applikation meldet sich das Gerät zum lokalen Netz an. Die erfolgreiche Anmeldung zum lokalen Netz wird durch diese Tonkombination signalisiert.
	**Vom lokalen Netz abgekoppelt, IP-Adresse verloren** Falls es zum Abkoppeln des UTP-Kabels vom das Gerät kommt, wird dieser Status durch diese Tonkombination signalisiert.
	**Zurücksetzen der Netzparameter in den Ausgangsstatus** Nach dem Einschalten der Einspeisung ist das Zeitlimit von 30 Sekunden für die Eingabe des Codes für das Zurücksetzen der Netzparameter in den Ausgangsstatus eingestellt. Das Zurücksetzen der Netzparameter in den Ausgangsstatus wird im konkreten Installationshandbuch beschrieben.

5. Konfigurierung über Web-Schnittstelle

Startbildschirm

Der Startbildschirm erscheint nach dem Anmelden an der Webschnittstelle das Gerät. Sie können jederzeit mittels der Taste zu diesem zurückkehren, die in der linken oberen Ecke auf den weiteren Seiten der Schnittstelle angebracht ist.

In der Kopfzeile erscheint der Name das Gerät (siehe Parameter Angezeigter Name in der Einstellung **Dienste > Web Server > Grundeinstellung**). Sie können die Sprache über das Menü in der oberen rechten Ecke der Webschnittstelle auswählen. Sie können sich über die Taste "Abmelden" in der oberen rechten Ecke der Seite abmelden, über das Fragezeichen-Symbol Hilfe aufrufen oder über die Sprechblase Feedback geben.

Die Startseite dient als das erste Niveau des Menüs und schnelle Navigation (durch das Anklicken eines beliebigen Kastens) zu ausgewählten Teilen des Zutrittsterminals. In manchen Kacheln wird gleichzeitig der Status der ausgewählten Dienste angezeigt.

Konfigurationsmenü

Die Konfiguration das Gerät ist in 5 Hauptmenüs unterteilt – **Status**, **Adressverzeichnis**, **Hardware**, **Leistungen** und **System**; jedes Menü ist in weitere Abschnitte unterteilt – siehe nachfolgende Übersicht.

Status

- **Gerät** – Grundinformationen über das Gerät
- **Services** – Information über gestartete Dienste und ihren Status
- **Lizenz** – Aktueller Status der Lizenz und der verfügbaren Funktionen das Gerät
- **Zugriffsprotokoll** – Liste der letzten zehn angelegten Zutrittskarten
- **Ereignisse** – Liste der stattgefundenen Ereignisse

Verzeichnis

- **Benutzer** – Einstellung der Telefonnummern der Nutzer, der Kurzwahltasten, der Zutrittskarten und die Nutzercodes für die Schalterbedienung
- **Zeitprofile** – Einstellung der Zeitprofile
- **Feiertage** – Einstellung der festen und beweglichen Feiertage im Kalenderjahr

Hardware

- **Schalter** – Einstellung der Einschaltung des elektrischen Schlosses, der Beleuchtung u.Ä.
- **Audio** – Lautstärke des Audios, des Signalisierungstons u.Ä.
- **Tastatur** – Einstellung der Tastatur und Eingeben der Codes
- **Hintergrundlicht** – Einstellung der Helligkeitsstufe der Hintergrundbeleuchtung
- **Kartenleser** – Einstellung des Kartenlesers, Wiegand-Interface
- **Digitale Eingänge** – Steuerung der Eingänge
- **Extender** – Einstellung der erweiternden Module das Gerät
- **Aufzugsteuerung** – Einstellungen für den Zugang zu den einzelnen Etagen mit dem Aufzug

Services

- **Zugangskontrolle** – Einstellungen der Ein- und Ausstiegsregeln
- **E-Mail** – Ermöglicht das Versenden der E-Mails einzustellen, z. B. beim ungültigen Zutrittsversuch
- **Mobile Key** – Einstellung des Bluetooth und Verwaltung der angeschlossenen Geräte
- **Automatisierung** – Flexible Einstellung das Gerät gemäß den spezifischen Anforderungen des Nutzers
- **HTTP API** – Die Applikationsschnittstelle für die Bedienung von ausgewählten Funktionen gemäß
- **Benutzertöne** – Einstellung und Upload der Nutzertöne

- **Webserver** – Einstellung des Webservers und des Zutrittcodes
- **SNMP** – Die Funktionalität, die die entfernte Aufsicht das Gerät im Netz mittels des SNMP-Protokolls ermöglichen.

System

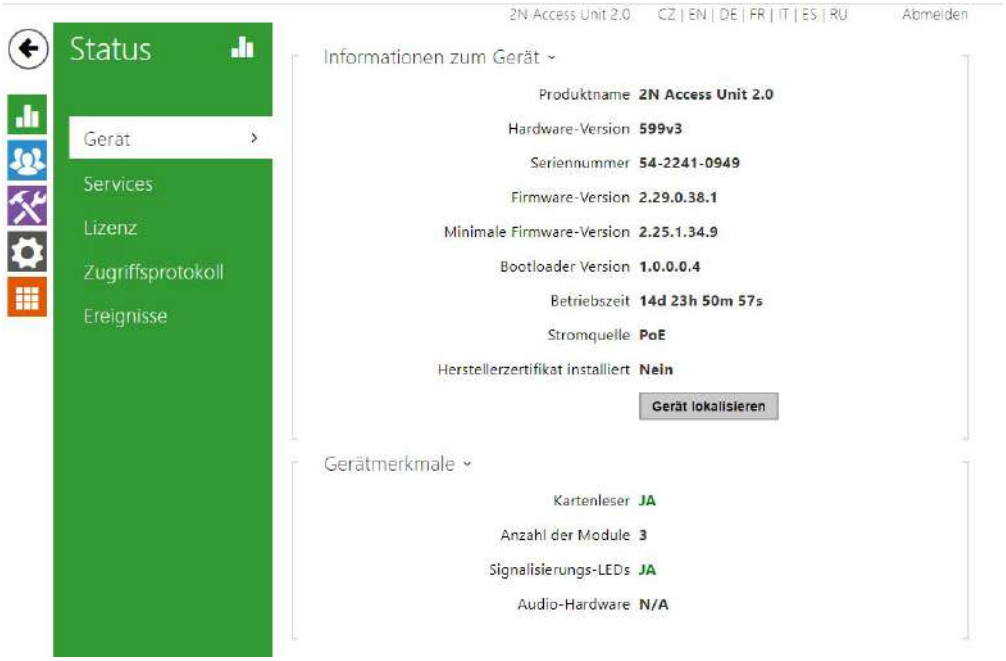
- **Netzwerk** – Einstellung des Anschlusses an das lokale Netz, 802.1x, Abfangen von Paketen
- **Datum und Uhrzeit** – Einstellung der realen Zeit und der Zeitzone
- **Funktion** – Einstellung der Testfunktionen
- **Lizenz** – Einstellung von Lizenzen, Aktivierung der Trial-Lizenz
- **Zertifikate** – Einstellung der Zertifikate und der Privatcodes
- **Auto Provisioning** – Einstellung der automatischen Aktualisierungen der Firmware und der Konfiguration
- **Syslog** – Einstellung des Absendens von Systemnachrichten an den Syslog-Server
- **Wartung** – Sicherheitskopie und Konfigurationswiederherstellung, Firmwareaktualisierung

- 5.1 Status
- 5.2 Verzeichnis
- 5.3 Hardware
- 5.4 Services
- 5.5 System

Hinweis

Warnung
Um volle Funktionsfähigkeit und garantierte Leistung zu erzielen, empfehlen wir ausdrücklich, die Aktualität der benutzter Version des Produkts oder Geräts schon bei der Installierung zu prüfen. Der Kunde nimmt hiermit zur Kenntnis, dass das Produkt oder Gerät nur in dem Fall die garantierte Leistung erzielen und voll funktionsfähig werden kann, wenn die neueste Version des Produktes oder Geräts verwendet wird, die auf volle Interoperabilität getestet wurde und vom Hersteller nicht als inkompatibel mit bestimmten Versionen anderer Produkte bezeichnet wurde, alles das nur in Übereinstimmung mit Hinweisen, Anleitungen oder Empfehlungen des Herstellers und nur in Verbindung mit geeigneten Produkten und Geräten anderer Hersteller. Die neuesten Versionen sind auf Internetseiten https://www.2n.com/cs_CZ/ zu finden, ggf. erlauben die einzelnen Geräte nach ihrer technischen Möglichkeiten eine Aktualisierung in der Konfigurationsschnittstelle. Falls der Kunde eine andere als die neueste Version des Produktes oder Geräts verwendet, oder eine Version, die der Hersteller als inkompatibel mit bestimmten Versionen anderer Produkte bezeichnet hat, oder wenn der Kunde das Produkt oder Gerät in Widerspruch mit Hinweisen, Anleitungen oder Empfehlungen des Herstellers verwendet, oder in Kombination mit ungeeigneten Produkten oder Geräten anderer Hersteller, ist er mit allen eventuellen Funktionsbeschränkungen solches Produkts oder Geräts und damit verbundenen Folgen einverstanden. Durch Verwendung einer anderen als neuesten Version des Produkts oder Geräts, ggf. einer Version, die der Hersteller als inkompatibel mit bestimmten Versionen anderer Produkte bezeichnet hat, oder durch Verwendung des Produkts oder Geräts in Widerspruch mit Hinweisen, Anleitungen oder Empfehlungen des Herstellers, oder durch Verwendung zusammen mit ungeeigneten Produkten oder Geräten anderer Hersteller, stimmt der Kunde zu, dass die Gesellschaft 2N TELEKOMUNIKACE a.s. für keine Beschränkung der Funktionsfähigkeit solches Produkts oder keinen mit der eventuell Funktionsbeschränkung verbundenen Schaden verantwortlich ist.

5.1 Status



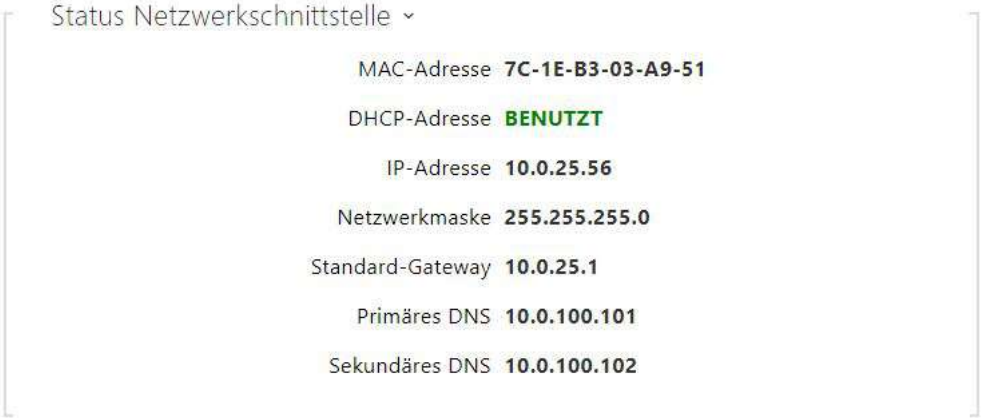
Im Menü **Zustand** ist der aktuelle Zustand des Zutrittsterminals übersichtlich angezeigt, sowie Info darüber. Das Menü ist in folgende Registerkarten unterteilt.

Registerkarte Geräte

Zeigt Informationen über das Modell und seine Eigenschaften, die Version der Firmware und des Bootloaders u.Ä. an.

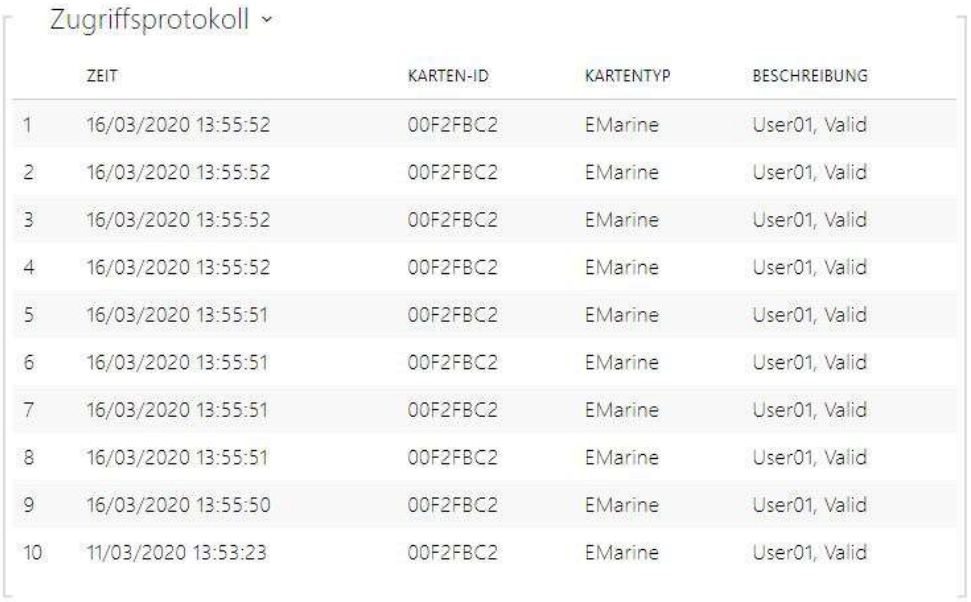
Registerkarte "Services"

Zeigt den Status der Netzschnittstelle und der ausgewählten Dienste an.



Registerkarte Zugriffsprotokoll

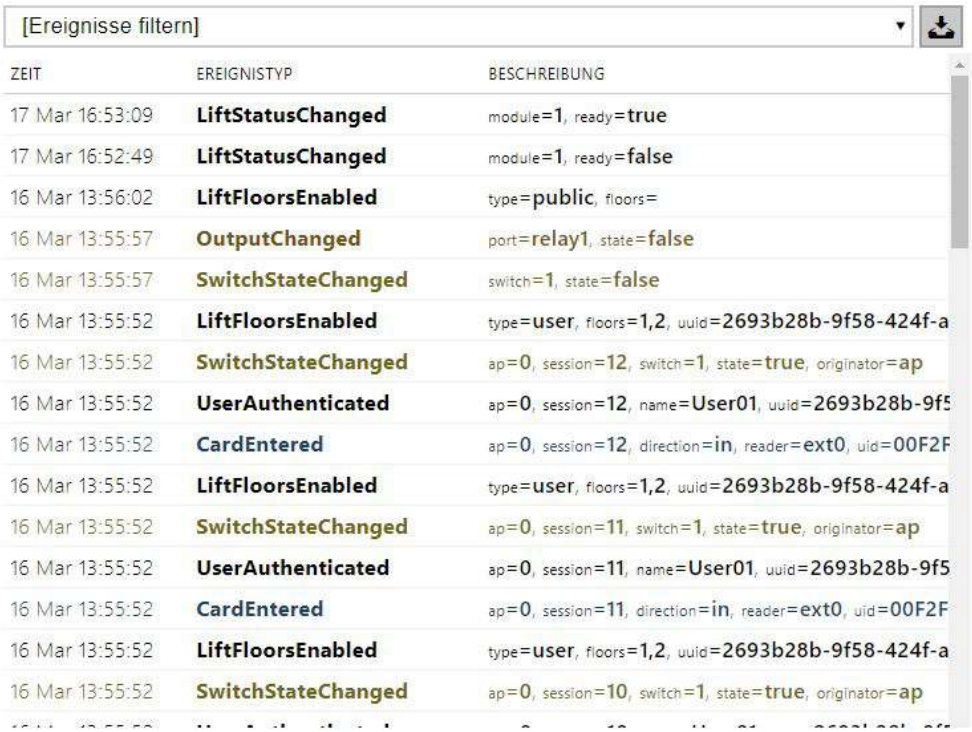
Auf der Registerkarte **Historie der Zutritte** werden die letzten 10 Eintragungen über angelegte Karten angezeigt. Jede Eintragung enthält die Uhrzeit zu der die Karte angelegt wurde, ihre ID, ihren Typ und die Beschreibung, die die Information enthält, ob die Karte gültig ist bzw. welchem Nutzer sie zugeordnet wurde.


Zugriffsprotokoll

	ZEIT	KARTEN-ID	KARTENTYP	BESCHREIBUNG
1	16/03/2020 13:55:52	00F2FBC2	EMarine	User01, Valid
2	16/03/2020 13:55:52	00F2FBC2	EMarine	User01, Valid
3	16/03/2020 13:55:52	00F2FBC2	EMarine	User01, Valid
4	16/03/2020 13:55:52	00F2FBC2	EMarine	User01, Valid
5	16/03/2020 13:55:51	00F2FBC2	EMarine	User01, Valid
6	16/03/2020 13:55:51	00F2FBC2	EMarine	User01, Valid
7	16/03/2020 13:55:51	00F2FBC2	EMarine	User01, Valid
8	16/03/2020 13:55:51	00F2FBC2	EMarine	User01, Valid
9	16/03/2020 13:55:50	00F2FBC2	EMarine	User01, Valid
10	11/03/2020 13:53:23	00F2FBC2	EMarine	User01, Valid

Registerkarte "Ereignisse"

Auf dieser Registerkarte sieht man die letzten 500 Ereignisse, die die Anlage aufgezeichnet hat. Jedes Ereignis enthält die Uhrzeit und das Datum der Erfassung, den Ereignistyp und die Beschreibung, die das Ereignis näher spezifiziert. Man kann die Ereignisse im Rollmenü über der Eintragung der Ereignisse selbst nach dem Ereignistyp filtern.



-  – die Taste dient zum Export aller aufgezeichneten Ereignisse in CSV-Datei.

Ereignis	Bedeutung
AccessLimited	Ereignis, das nach 5 erfolglosen Authentifizierungsversuchen eintritt (Karte, Code, Fingerabdruck). Das Zutrittsmodul bleibt dann für 30 Sekunden gesperrt, auch im Fall, dass die nachfolgende Authentifizierung gültig war.
ApiAccessRequested	Ereignis, bei dem die Anforderung an /api/accesspoint/grantaccess mit dem Ergebnis "success" : true geschickt wurde.
AccessTaken	Nach dem Anlegen der Karte im Anti-Passback-Bereich.
CardHeld	Beim Anlegen der Karte, das 4 s und länger dauert.
CardEntered	Nach dem Anlegen der Karte.

Ereignis	Bedeutung
CodeEntered	Nach der Eingabe des Codes auf der nummerischen Tastatur, der mit dem Zeichen * endet.
DeviceState	Indikation des Anlagenstatus, wie z.B. des Starts.
DoorOpenTooLong	Erkennung einer lang geöffneten Tür, einstellbar in der Hardware / Tür / Tür.
DoorStateChanged	Erkennt das Öffnen/Schließen der Tür. Sie können die Einstellung in der Hardware / Tür / Tür.
FingerEntered	Autorisierung mittels des Fingerabdruckes.
InputChanged	Signalisiert eine Änderung des logischen Eingangs.
KeyPressed	Beim Drücken der Taste (die Ziffern sind 0,1,2...,9 und die Kurzwahltasten sind %1,%2 usw.).

Ereignis	Bedeutung
KeyReleased	Beim Loslassen der Taste (die Ziffern sind 0,1,2...,9 und die Kurzwahltasten sind %1,%2 usw.).
LiftFloorsEnabled	Zutritt zur Etage mit Aufzug.
LiftStatusChanged	Erkennung der Anschliessung/Abtrennung des Lift Control Moduls.
LoginBlocked	Bei der Eingabe von 3 fehlerhaften Logins im Web, in die Anlage. Enthält Angaben über die IP-Adresse dieser Zutritte.
MobKeyEntered	Autorisierung mittels Bluetooth.
OutputChanged	Signalisiert eine Änderung des logischen Eingangs.
RegistrationStateChanged	Statusänderung der Registrierung zum SIP-Proxy.
RexActivated	Ereignis bei Aktivierung des Eingangs, das auf REX-Taste eingestellt ist.
SilentAlarm	Ereignis des SilentAlarms nach der Eingabe des Codes, der um eine Eins höher als der richtige Code ist. Das heißt, der Code für das Öffnen ist 123 und der Code des SilentAlarms ist 124. Oder nach dem Anlegen des Fingers an das Modul des Fingerabdruckscanners, der für die Verwendung zur Aktivierung des SilentAlarm gekennzeichnet ist.
SwitchesBlocked	Schalter mit ungültiger Eingabe des Zugangs blockiert.
SwitchOperationChanged	Änderung der Schalterfunktion (signalisiert den Status der Verriegelung oder des Haltens des Schalters, Start und Neustart des Timers oder dessen Beendigung - Übergang zum permanenten Halten).
SwitchStateChanged	Änderung des Schalterstatus, Einstellung in der Hardware / Schalter.
TamperSwitchActivated	Signalisiert Aktivierung des Schutzschalters –Öffnen des Gerätegehäuses. Die Funktion des Schutzschalters muss im Menu Digitale Eingänge / Schutzschalter konfiguriert werden.

Ereignis	Bedeutung
UnauthorizedDoorOpen	Erkennung des nicht autorisierten Türöffnens, einstellbar in der Hardware / Tür / Tür.
UserAuthenticated	Signalisiert die Authentifizierung des Benutzers und nachfolgendes Öffnen der Tür.
UserRejected	Ungültige Nutzerüberprüfung.

5.2 Verzeichnis

Hier ist eine Übersicht dessen, was Sie in dem Kapitel finden:

5.2.1 Benutzer

Die Nutzerliste ist eines der wichtigsten Teile das Gerät. Die Benutzerliste enthält wichtige Benutzerinformationen, die Gerätefunktionen wie das Öffnen von Türen mit RFID-Karten, das Aktivieren von Codeschlössern, die Benachrichtigung von Benuezern über den Zugang per E-Mail usw. ermöglichen.
Die Benutzerliste ist in einer Tabelle zusammengestellt, die bis 10,000 Posten enthält – jedem Benutzer ist üblicherweise gerade ein Posten zugeteilt. Die Benutzerliste enthält Informationen über die Benutzer, die berechtigt sind, das Objekt mittels RFID-Karte zu betreten.

Wenn Sie einen externen Kartenleser verwenden, der an das Gerät mittels der Wiegand-Schnittstelle angeschlossen ist, kommt es bei der Übertragung der ID-Karte mittels dieser Schnittstelle zur Verkürzung der ID auf 6 oder 8 Zeichen (gemäß der Einstellung des Übertragungsmodus). Wenn Sie die gleiche Karte an den internen Leser anlegen, erhalten Sie die

komplette ID, die in der Regel länger ist als – 8 und mehr Zeichen. Die letzten 6 ggf. 8 Zeichen der ID sind jedoch identisch. Dies wird beim Vergleich der ID-Karten mit der Datenbank im Gerät genutzt – wenn die verglichenen IDs eine unterschiedliche Länge haben, werden sie vom Ende aus verglichen und die Übereinstimmung muss mindestens in 6 Zeichen gefunden werden. Wenn die IDs gleich sind, werden alle Zeichen verglichen. Mittels dieses Mechanismus wird die gegenseitige Kompatibilität des internen und externen Lesers erreicht.

Alle Karten, die an den internen Leser angelegt wurden oder die mittels der Wiegand-Schnittstelle angenommen wurden, werden aufgezeichnet und sie können sich die letzten 10 angelegten Karten im Menü **Status > Historie der Zutritte** anschauen. Sie können in der Liste außer der ID-Karten auch ihren Typ, die Uhrzeit des Anlegens und ggf. weitere Informationen finden. Sie können im Falle eines kleinen Systems beim Eingeben der ID-Karten einen einfachen Trick nutzen – legen Sie die Karte an den Leser das Gerät an und suchen Sie sie in der Registerkarte **Historie der Zutritte** aus. Markieren sie die ID der Karte mittels der Maus; z.B. mittels des doppelten Klickens auf die ID der Karte, und drücken Sie die Tasten CTRL+C. Nunmehr haben Sie die ID der Karte in der Zwischenablage und Sie können Sie mittels der Tasten CTRL+V in ein beliebiges Feld in den Geräteeinstellungen eingeben.

Nach dem Anlegen der Karte an den RFID-Leser wird die Karten-ID mit der Kartendatenbank im Gerät verglichen. Wenn die ID der angelegten Karte einer der Karten in der Datenbank entspricht, wird die jeweilige Aktion – Aktivierung des Schalters (Öffnen des elektrischen Türschlosses u.Ä.) durchgeführt. Die Nummer des aktivierten Schalters können Sie in den Einstellungen **Hardware > Kartenleser** über den Parameter Assoziierter Schalter, bzw. in der Einstellung **Hardware > Module** über den Parameter **Assoziierter Schalter** beim Kartenlesermodul ändern.

Die Benutzerlisten-Suchfunktion funktioniert wie eine Volltextsuche im Namen und in der E-Mail. Sie sucht nach sämtlichen Übereinstimmungen in der ganzen Liste.Ein neuer Benutzer wird mithilfe der Taste oberhalb der Tabelle hinzugefügt. Die Schaltfläche dient der detaillierten Anzeige der Nutzereinstellung dient die Schaltfläche  . Zur Einstellung der Anzeige der Tabellenspalten dient die Ikone  , die Standardeinstellung der Tabelle zeigt Name, E-Mail des Benutzers und seine eingestellte Zutritte an. Der Entfernung eines Nutzers von der Liste, wenn alle seine eingegebenen Daten gelöscht werden, dient die Schaltfläche  . In der Spalte für Zutritte werden die Schaltflächen  angezeigt, die die aktive Authentifizierung des Nutzers beschreiben.

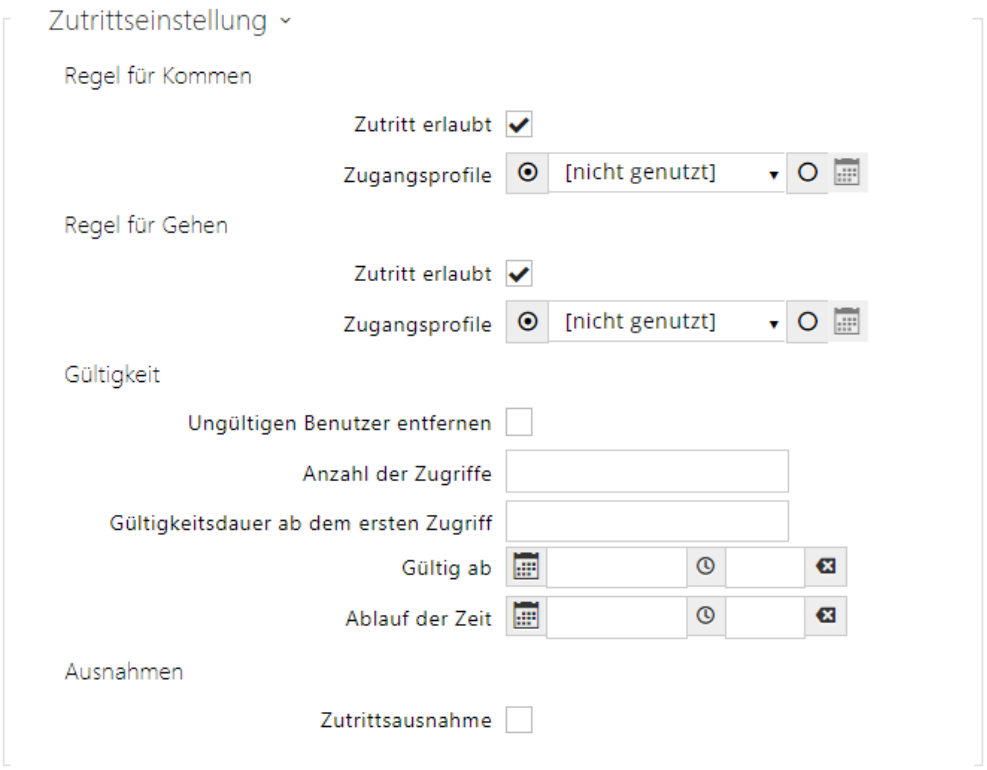
Über das Symbol / können Sie eine CSV-Datei mit einer Benutzerliste vom/auf das Gerät exportieren/importieren. Wenn das Verzeichnis leer ist, wird eine reine Kopfzeilendatei (in englischer Sprache) exportiert, die als Vorlage für den Import von Benutzern dienen kann. Wenn eine leere Kopfzeilendatei importiert und die Variante **Verzeichnis ersetzen** gewählt wird, wird die ganze Datei gelöscht. Beim Import können bis zu 10.000 Benutzer hochgeladen werden, je nach Gerätetyp.

Hinweis

- Spezielle Benutzer, wie z. B. die von **My2N** oder **2N Access Commander** angelegten, werden nicht in den Verzeichnisexport einbezogen.
- Wenn Sie eine CSV-Datei mit Microsoft Excel bearbeiten, muss die Datei im Format CSV UTF-8 (mit Trennzeichen) gespeichert werden.

Jede Eintragung in der Nutzerliste enthält folgende Angaben:

- **Name** – Keine Pflichtangabe, dient der besseren Orientierung in der Liste, z.B. der Nutzersuche.
- **E-mail** – die E-Mail-Adresse des Benutzers, die für den Versand von Informationen per E-Mail verwendet wird, z. B. über den Zugriff des Benutzers auf das Objekt oder bei Verwendung von 2N Automation. Geben Sie eine oder mehrere E-Mail-Adressen ein, die durch ein Komma oder Semikolon getrennt sind.



- **Regel für das Kommen**
  - **Zutritt erlaubt** – erlaubt die Authentifizierung in diesem Zutrittspunkt.
  - **Zutrittsprofile** – bietet die Auswahl aus vordefinierten Profilen aus dem **Verzeichnis > Zeitprofile** oder die manuelle Einstellung des Profils direkt für dieses Element an.
- **Regel für Gehen**
  - **Zutritt erlaubt** – erlaubt die Authentifizierung in diesem Zutrittspunkt.
  - **Zutrittsprofile** – bietet die Auswahl aus vordefinierten Profilen aus dem **Verzeichnis > Zeitprofile** oder die manuelle Einstellung des Profils direkt für dieses Element an.
- **Gültigkeit**
  - **Ungültigen Benutzer entfernen** – Wählen Sie, ob der Benutzer vom Gerät entfernt wird, sobald er ungültig ist (d.h. seine Gültigkeitsdauer abgelaufen ist oder die Anzahl seiner autorisierten Zugriffe 0 beträgt).
  - **Anzahl der Zugriffe** – Legen Sie die Anzahl der autorisierten Zugriffe für diesen Benutzer fest. Lassen Sie das Feld leer, um unendlich viele Zugriffe festzulegen.
  - **Gültigkeitsdauer ab dem ersten Zugriff** – Legen Sie die Zeit fest, in der der Benutzer ab seiner ersten erfolgreichen Autorisierung gültig ist. Lassen Sie es leer für keine relative Gültigkeitsdauer. Relative Gültigkeit kann die Gültigkeitsdauer verkürzen, aber niemals verlängern. Die Zeit wird im Format HH:MM eingestellt, z.B. 06:09.

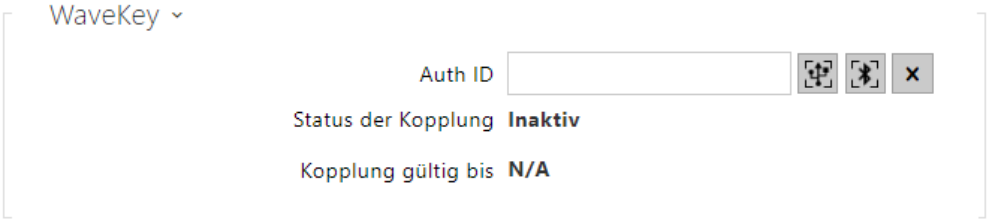
  - **Gültigkeit ab** – ermöglicht den Gültigkeitsanfang des eingestellten Zutrittes einzustellen. Lassen Sie das Feld leer, damit der Start nicht eingeschränkt ist. Das Gültig ab muss dem Gültig bis vorausgehen.
  - **Ablauf der Zeit** – ermöglicht das Gültigkeitsende des eingestellten Zutrittes einzustellen. Lassen Sie das Feld leer, damit das Ende nicht eingeschränkt ist. Gültig bis muss nach Gültig ab liegen.
- **Zutrittsausnahme** – Ermöglichen Sie diesem Benutzer, die Regeln für den Zugriffsblock und die Anti-Passback-Regeln zu umgehen.

Jedem Benutzer kann ein separater Code zum Einschalten des Schalters zugeteilt werden. Die Schalter-Benutzercodes können beliebig mit den im Menü eingegebenen Schalter-Universal-Codes kombiniert werden **Hardware > Schalter**. Wenn sich die Codes mit anderenin der Gerätekonfiguration schon eingegebenen Codes überlappen, dann erscheint bei diesen sich überlappenden Codes das Zeichen ⓘ.

- **PIN-Code** – Ermöglicht den persönlichen nummerischen Zutrittscode des Nutzers einzustellen. Der Code muss mindestens zwei Zeichen enthalten.
  -  generiert ein QR-Code-Bild. Codes mit weniger als 4 Stellen können aus Sicherheitsgründen nicht durch das Lesen des QR-Codes eingegeben werden. Die Codes dürfen nur Ziffern enthalten. Wenn eine Authentifizierung mit einem hexadezimalen QR-Code erforderlich ist, muss dieser Code vor der Eingabe in ein dezimales Format umgewandelt werden.
- **Schalter** – Ermöglicht den persönlichen Code des Nutzers für das Einschalten des Schalters einzustellen. Der Code darf bis 16 Zeichen lang sein und darf nur die Ziffern 0–9 enthalten. Der Code muss mindestens zwei Zeichen für die Türentriegelung von der Gerätetastatur und mindestens ein Zeichen für die Türentriegelung mit DTMF vom Telefon enthalten.
  -  generiert ein QR-Code-Bild. Codes mit weniger als 4 Stellen können aus Sicherheitsgründen nicht durch das Lesen des QR-Codes eingegeben werden. Die Codes dürfen nur Ziffern enthalten. Wenn eine Authentifizierung mit einem hexadezimalen QR-Code erforderlich ist, muss dieser Code vor der Eingabe in ein dezimales Format umgewandelt werden.

Jedem Benutzer des Geräts können zwei RFID-Zugangskarten zugewiesen werden.

- **Karten-ID** – Ermöglicht die ID der Zutrittskarte des Nutzers einzustellen. Jedem Benutzer können max. zwei Zugangskarten zugewiesen werden. ID der Zugangskarte ist eine Sequenz von 6–32 Zeichen, 0–9, A–F. Nach dem Anlegen der gültigen Karte an den Leser kommt es zum Einschalten des Schalters, der mit dem jeweiligen Kartenleser assoziiert ist. Falls der Modus der doppelten Authentifizierung gewählt ist, wird der Schalter durch den eingegeben nummerischen Code aktiviert.
- **Virtuelle Karten-ID** – Ermöglicht die ID der virtuellen Zutrittskarte des Nutzers einzustellen. Jeder Nutzer kann gerade eine virtuelle Karte zugeordnet haben. Die ID der virtuellen Karte ist die Sequenz von 6–32 Zeichen aus der Menge 0–9, A–F. Die Nummer der virtuellen Karte wird zur Identifizierung des Nutzers in Anlagen verwendet, die über eine Wiegand-Schnittstelle angeschlossen sind. Nach der Identifizierung des Benutzers wird die virtuelle Karten-ID auf dem Bluetooth- oder Biometrieleser an die Wiegand-Schnittstelle gesendet, wenn in der Konfiguration (Services > Zugangskontrolle) festgelegt ist, dass IDs an Wiegand gesendet werden.



Dieser Bereich wird nur angezeigt, wenn das Bluetooth-Modul angeschlossen ist.

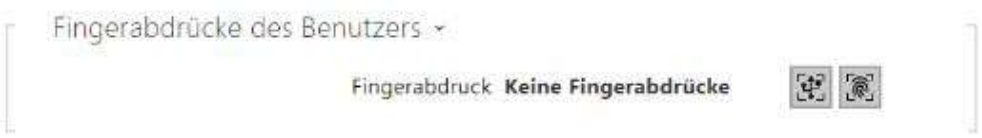
- **Auth-ID** – einzigartige WaveKey-ID für den Zugriffskontrolle. Während des Pairing-Vorgangs wird sie auf dem mobilen Gerät gespeichert. Die Authentifizierungs-ID besteht aus 32 hexadezimalen Zeichen.
- **Status der Kopplung** – Der aktuelle Kopplungsstatus (Ist nicht aktiv, Warten auf Kopplung, PIN-Gültigkeit abgelaufen oder Gekoppelt).
- **Kopplung gültig bis** – Datum und Uhrzeit des Gültigkeitsendes der generierten Autorisierung-PIN.
  - Über USB-Leser kopplen
  - über diese Anlage kopplen

- Auth-ID löschen

Kopplen mittels Bluetooth-Modul im Geräte

Das Vorgehen für die Kopplung eines Mobiltelefons mit dem Nutzer ist folgendes:

1. Die Kopplung wird beim ausgesuchten Nutzerkonto mit dem Drücken der Taste bei der Position Auth-ID gestartet.
2. Es erscheint ein Dialogfenster mit dem PIN-Code.
3. In der Applikation **2N Mobile Key** den jeweiligen Leser aussuchen und die Taste Start Pairing drücken.
4. In das Feld für den Eingang den Code aus Punkt 2 eingeben.
5. Die Kopplung ist beendet.

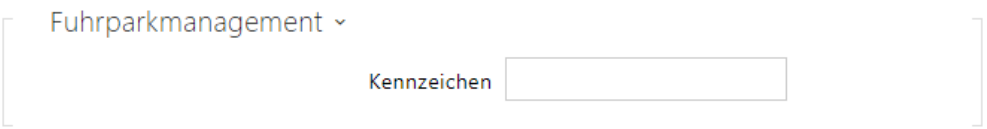


- **Fingerabdrücke** – zeigt die Zahl der eingestellten Fingerabdrücke an, man kann bis zu 2 verschiedene Fingerabdrücke einstellen. Dieser Abschnitt wird nur in der Anwesenheit des Moduls des Biometrischen Scanners angezeigt.
  - Einscannen des Fingers über USB-Leser
  - das Modul des Fingerabdruckscanners einlesen

Hinweis

- Die Kapazität der Benutzer-Fingerabdrücke ist auf max. 2000 pro Gerät begrenzt.

Ein detailliertes Verfahren zum Hochladen der Fingerabdrücke des Benutzers finden Sie in Unterkapitel 5.2.1.1.



Mit die Geräte können erkannte Fahrzeugkennzeichen, die in einer HTTP-Anfrage von Kameras von der Firma AXIS gesendet wurden und die mit einer zusätzlichen VaxALPR-Anwendung auf

api/lpr/licenseplate ausgestattet sind, genutzt werden (weitere Informationen finden Sie im HTTP-API-Handbuch für IP-Sprechanlagen).
Wenn die Funktion aktiviert ist, wird das Ereignis nach Erhalt einer gültigen HTTP-Anfrage im Verlauf unter dem Ereignis LicensePlateRecognized aufgezeichnet.

Wenn ein Bild als Teil der HTTP-Anfrage gesendet wird (z. B. ein Abschnitt des Fotos oder das gesamte Foto der Szene bei der Kennzeichenerkennung), wird es gespeichert. Die letzten fünf Fotos werden im Gerätespeicher gespeichert, der über eine an api/lpr/image gesendete HTTP-Anfrage vom Gerät gelesen werden kann und im **2N Access Commander** System verfügbar ist.

Für eine korrekte Funktion ist es ratsam, dass jedes Kennzeichen genau einem Eintrag im Verzeichnis zugeordnet ist.Bei mehreren Eintragungen eines Kennzeichens ist es nicht möglich, einen Eintrag in dem Verzeichnis, in dem die Kennzeichen konfiguriert sind, eindeutig zuzuweisen (der erste Eintrag, für den das angegebene Kennzeichen konfiguriert ist, wird ausgewählt und seine Zugriffsregeln werden angewendet).

- **Kennzeichen** – setzt die Fahrzeugkennzeichen des angegebenen Eintrags im Verzeichnis. Einem durch Kommas getrennten Eintrag können mehrere Kennzeichen zugewiesen werden (maximal 20). Die eingegebenen Kennzeichen werden verwendet, um Kennzeichen anhand des Bildes der externen Kamera zu erkennen (weitere Informationen finden Sie im Interoperabilitätshandbuch). Ein Kennzeichen kann maximal 10 Zeichen enthalten. Die Länge der angegebenen Zeichenfolge ist auf 255 Zeichen begrenzt.

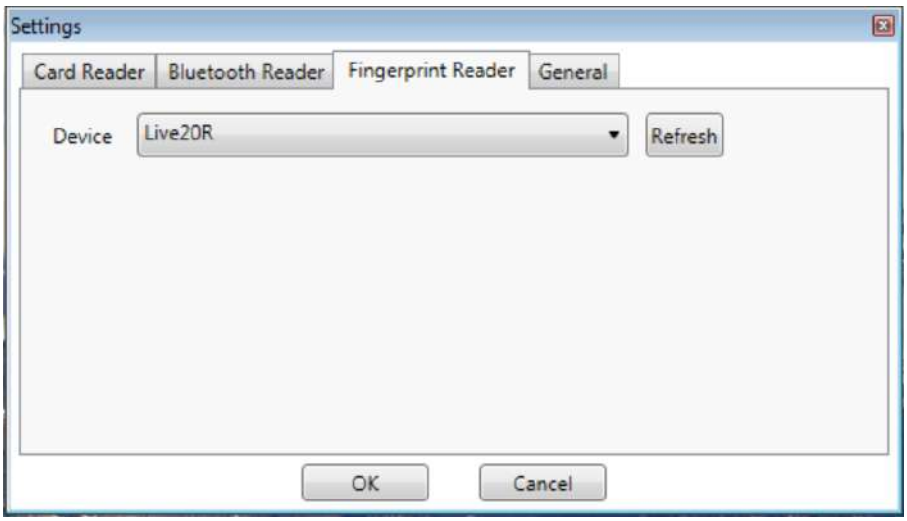
- **Etagen** – Auswahl der für den Benutzer zugänglichen Etagen.
- **Zeitprofil** – Bietet die Auswahl eines oder mehrerer Zeitprofile gleichzeitig an, die angewendet werden. Die Einstellung der Zeitprofile selbst ist im Abschnitt **Verzeichnis > Zeitprofile möglich**.
  -  Mit der Markierung wird die Auswahl aus vordefinierten Profilen oder die manuelle Einstellung des Zeitprofils für das jeweilige Element eingestellt.
  -  Mit der Markierung wird das Zeitprofil direkt für das jeweilige Element eingestellt.

5.2.1.1 Anweisungen für das Einstellen der Nutzerfingerabdrücke

Die Fingerabdrücke können über den **2N Access Unit Biometrischen Fingerabdruckleser** (Best.-Nr. 916019) oder den externen USB-Fingerabdruckleser (Best.-Nr. 9137423E) gelesen werden. Das Vorgehen ist folgendes:

1a) Das Lesen über das Modul **2N Access Unit Biometrischer Fingerabdruckleser** kann über die Web-Schnittstelle des Geräts beim konkreten Benutzer in der Rubrik Adressverzeichnis / Benutzer / Benutzer-Fingerabdrücke durch Auswahl der Funktion Lesen über das Fingerabdruckleser-Modul erfolgen  .

1b) Das Einlesen über das Modul des Fingerabdruckscanners kann mittels des **2N IP USB-Drivers** durchgeführt werden, wählen Sie in seiner Einstellung Fingerprint Reader (Fingerabdruckscanner) und bestätigen Sie mit der Taste OK. In der Schnittstelle der Anlage beim konkreten Nutzer im Abschnitt Verzeichnis / Nutzer / Nutzerfingerabdrücke Einlesen über das Modul des Fingerabdruckscanner wählen  .



2) Durch Anklicken den Finger zum Einlesen des Fingerabdruckes wählen.

Man kann für einen Nutzer bis zu zwei Fingerabdrücke einstellen.

3) Für das Einlesen des Fingerabdruckes auf die Taste FINGER EINSCANNEN klicken.

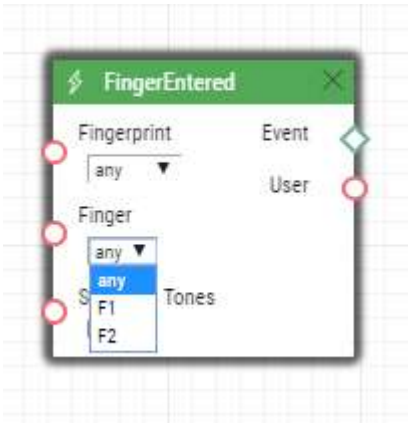
4) Legen Sie den gewählten Finger an den externen USB-Scanner an. Für eine höhere Genauigkeit wird dieser Prozess insgesamt dreimal wiederholt.

Bei Nichtübereinstimmung der gelesenen Fingerabdrücke wiederholen Sie das Prozess.

5) Sofern das Scannen der Finger in Ordnung war, bestätigen Sie die Einstellung, indem Sie die Taste FERTIG anklicken.

Zur Einstellung der Fingerfunktion klicken Sie auf das Menü-Symbol , es wird das Menü mit den verfügbaren Funktionen angezeigt:

- Tür öffnen
- SilentAlarm. Kann man nur im Fall der aktiven Funktion Öffnen der Tür einstellen.
- Die Automatisierung F1 – generiert das Ereignis FingerEntered in Automation. F1 dient der Unterscheidung des angelegten Fingers in Automation.
- Automatisierung F2 – generiert das Ereignis FingerEntered in Automation. F2 dient der Unterscheidung des angelegten Fingers in Automation.



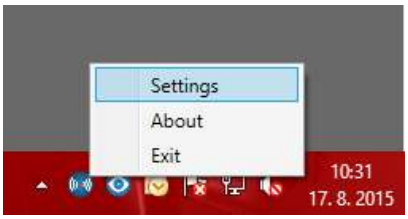
Nach dem Einstellen der Fingerabdrücke und ihrer Funktionen mit dem Klicken auf SPEICHERN UND SCHLIESSEN bestätigen.

6) In der Registerkarte Benutzer kann die aktuelle Einstellung überprüft werden.

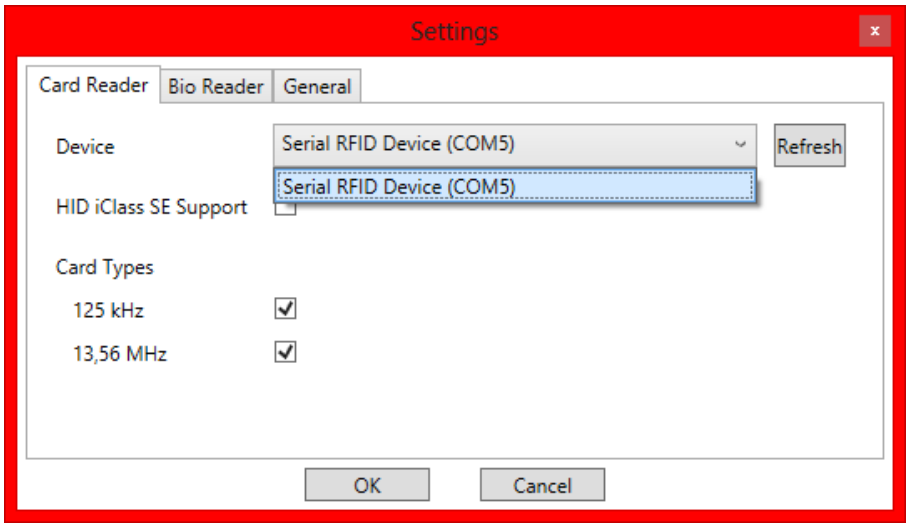
5.2.1.2 USB-RFID-Kartenleser

Man kann die Karten-ID über den USB-RFID-Leser einlesen. Das Vorgehen ist folgendes:

1. Gehen Sie in die Einstellung des **2N® IP USB-Drivers**



2. Stellen Sie den COM-Port des angeschlossenen Lesers ein



3. Auf der Webseite beim Nutzer die Taste des Karteneinlesens drücken

Legen Sie die Karte an den Leser an

4. Die Karte ist eingelesen

5. Vergessen Sie nicht, die Konfiguration zu speichern.

5.2.2 Zeitprofile

Man kann ausgewählte Funktionen das Geräte, wie z.B. Zutritt mittels der RFID-Karte oder des nummerischen Codes zeitlich einschränken. Sie können den angeführten Funktionen sog. **Zeitprofil** zuordnen, das bestimmt, wann die jeweilige Funktion verfügbar ist und wann nicht. Mit Zeitprofilen kann man folgende Anforderungen lösen:

- Anrufe an den ausgewählten Nutzer außerhalb der vorbehaltenen Zeit ganz sperren
- Anrufe von ausgewählten Telefonnummern des Nutzers außerhalb der vorbehaltenen Zeit sperren
- Zutritt mittels der RFID-Karte des Nutzers außerhalb der vorbehaltenen Zeit sperren
- Zutritt mittels des ausgewählten Zutrittscodes außerhalb der vorbehaltenen Zeit sperren
- das Einschalten des Schalters außerhalb der vorbehaltenen Zeit sperren

Jedes Zeitprofil definiert die Verfügbarkeit der Funktion, mit der es mittels des Wochenkalenders verbunden ist. Man kann einfach die Zeit von–bis und ggf. die Tage in der Woche einstellen, an denen die Funktion verfügbar sein soll. Das Geräte ermöglicht bis zu 20 verschiedene Zeitprofile zu erstellen. Sie können der jeweiligen Funktion ein beliebig erstelltes Zeitprofil zuordnen, siehe Einstellung Nutzer, Zutrittskarten, Schalter.

Sie können die Gültigkeit des Zeitprofils nicht nur mittels der Einstellung des Wochenkalenders, sondern auch mittels spezieller Aktivierungs- und Deaktivierungscodes steuern. Die Aktivierungs-und Deaktivierungscodes kann man jederzeit mittels der nummerischen Tastatur des Zutrittsterminals eingeben. Auf diese Art und Weise kann man manuell einige der Funktionen z.B. beim Betreten oder Verlassen des Objekts aktivieren bzw. deaktivieren.

Die Einstellung der Zeitprofile befindet sich im Menü **Verzeichnis > Zeitprofile**.

Parameterliste

- **Profilbezeichnung** – geben Sie einen Namen für das Zeitprofil ein, damit Sie es leicht identifizieren können, wenn Sie es in Schaltern, Zugangskontrolle, Telefonnummern usw. auswählen.

Dient der Einstellung der Zeit des aktiven Profils im Rahmen der wöchentlichen Periodizität. Das Profil ist aktiv, wenn die aktuelle Zeit in die eingestellten Intervalle fällt.

Falls der jeweilige Tag als Feiertag bezeichnet ist (siehe Einstellung **Verzeichnis > Feiertage**), dann wird ohne Hinsicht darauf, was für ein Wochentag ist, die letzte Zeile der Tabelle angewendet, die als Feiertag bezeichnet ist.

Der richtigen Anwendung dieser Funktion wegen ist es erforderlich, dass die Anlage die richtige eingestellte aktuelle Uhrzeit hat (siehe Kapitel Datum und Uhrzeit).

Anmerkung

- *Man kann im Rahmen eines Tages eine beliebige Anzahl von Intervallen einstellen, z.B. 8:00–12:00, 13:00–17:00, 18:00–20:00.*
- *Wenn Sie wollen, dass das Profil den ganzen Tag aktiv ist, geben Sie ein Intervall ein, das den ganzen Tag deckt, z.B. 00:00–24:00*

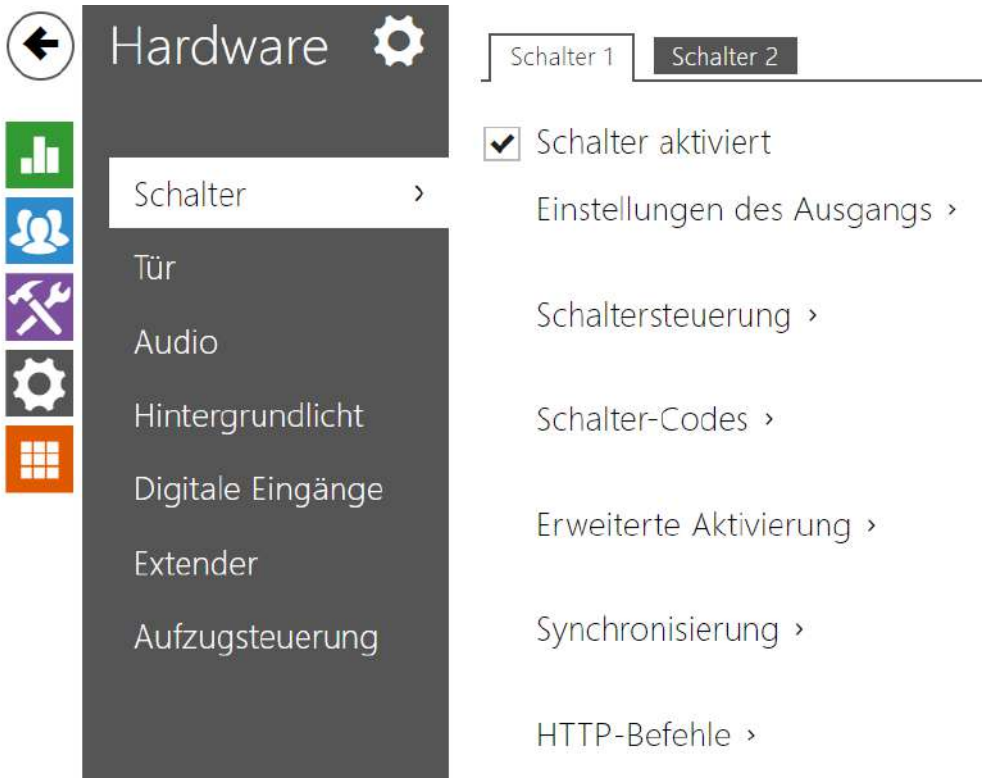
5.2.3 Feiertage

Auf dieser Seite werden Tage eingestellt, auf die ein Feiertag (ggf. ein Ruhetag) fällt. Für Tage, auf die ein Feiertag fällt, kann man im Zeitprofil abweichende Intervalle als in den anderen Tagen einstellen.
Man kann die Feiertage für die folgenden 10 Jahre im Voraus einstellen (das Jahr ist durch das Anklickens der Jahreszahl im oberen Teil der Seite zu wählen). Auf der Seite wird der Kalender für das ganze Jahr angezeigt. Durch das Anklickens des Kalendertages wird ein Feiertag markiert oder gelöscht. Regelmäßige Feiertage (Feiertage, die sich jedes Jahr am gleichen Kalendertag wiederholen) sind mit grüner Farbe markiert. Unregelmäßige Feiertage (die auf einen konkreten Kalendertag nur im jeweiligen Jahr zufallen) sind mit blauer Farbe markiert. Das erste Anklicken bezeichnet den Tag als den regelmäßigen Feiertag, das nachfolgende Anklicken bezeichnet den Tag als den unregelmäßigen Feiertag und ein weiteres Anklicken löscht den Tag aus der Liste der Feiertage.

5.3 Hardware

Hier ist eine Übersicht dessen, was Sie in dem Kapitel finden:

5.3.1 Schalter



Die Schalter ermöglichen eine sehr flexible Steuerung von verschiedenen Geräten (wie die elektrische Türschlösser, Beleuchtung, Ergänzungssignalisierung des Klingelns u.Ä. sind). Das Gerät ermöglicht 2 unabhängige Schalter zu konfigurieren, die man für beliebigen Zweck benutzen kann.

Der Schalter kann aktiviert werden:

- mittels der Eingabe des gültigen Codes auf der nummerischen Tastatur,
- mittels des Anlegens einer gültigen RFID-Karte an den Leser,
- mit definierter Verzögerung nach dem Einschalten eines anderen Schalters,
- mittels des Zeitprofils *),
- durch den Empfang eines HTTP-Befehls aus einer anderen Anlage im Netz,
- mittels der Automatisierung über Action.ActivateSwitch *).

Falls erforderlich, kann man die Schalteraktivierung mittels des gewählten Zeitprofils sperren.

Bermekung

- Für mit *) gekennzeichnete Optionen sind die entsprechenden aktiven Lizenzen erforderlich.

Sperren und halten des Schalters
Die Schaltbedingungen können mit zwei Funktionen geändert werden. Eine sperrt, die andere hält den Schalter. Wenn der Schalter gesperrt ist, befindet er sich permanent im „Aus“-Zustand und kann erst nach dem Entsperren getätigt werden (das Sperren hat eine höhere Priorität als das Halten - wenn der Schalter gleichzeitig gesperrt ist und gehalten wird, wird die Sperrung angewendet). Wenn der Schalter gehalten wird, befindet er sich permanent im „geschlossenen“ Zustand und kann erst nach dem Loslassen getätigt werden.
Das Sperren und Halten kann unter anderem über Zeitprofile gesteuert werden. Es wird nicht empfohlen, das Zeitprofil für die Sperrfunktion zu verwenden (die Zeitprofil-Sperrsteuerung ist aufgrund der Abwärtskompatibilität im Gerät vorhanden), da in diesem Fall der Schalter am Ende des Zeitprofils entsperrt wird, auch wenn der Schalter manuell gesperrt wurde.
Die aktuelle Kombination dieser beiden Funktionen wird über den Parameter **Aktuelle Funktion des Schalters** angezeigt (Normal - Sperren und Halten ist deaktiviert; Halten - Sperren ist deaktiviert und Halten aktiviert; Gesperrt - Sperren ist aktiviert, die Einstellung für Halten wird nicht berücksichtigt).
Nach dem Neustart des Geräts wird überprüft, ob die Sperre oder das Halten vom Zeitprofil beeinflusst wird. In diesem Fall wird die entsprechende Funktion bezüglich der Zeitprofileinstellung aktiviert oder deaktiviert. Wenn nicht, wird der letzte Sperrzustand vor dem Ausschalten des Geräts oder der Haltezustand in den inaktiven Zustand versetzt (der Schalter wird nicht gehalten).

Wenn der Schalter aktiv ist, kann man einstellen:

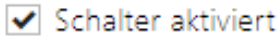
- das Schalten eines beliebigen logischen Zutrittsterminals (Relais, Leistungsausgang)
- Einschalten des Ausgangs, an welchem das Modul angeschlossen ist **2N IP Sicherheitsrelais**
- das Abschicken des HTTP-Befehls an eine andere Anlage

Der Schalter kann im monostabilen oder bistabilen Modus arbeiten. Im monostabilen Modus wird der Schalter nach der eingestellten Zeit automatisch ausgeschaltet. Im bistabilen Modus wird der Schalter durch die erste Aktivierung eingeschaltet und durch die nächste ausgeschaltet.

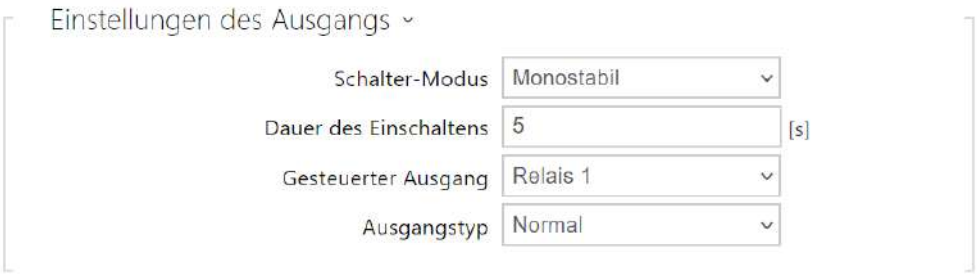
Der Schalter kann seinen Status signalisieren mittels:

- konfigurierbaren Pieptons
- Signalisierungs-LED

Registerkarte Schalter 1–2



- **Schalter aktiviert** – erlaubt oder verbietet global die Steuerung des Schalters. Ist der Schalter deaktiviert, kann dieser nicht durch die verfügbaren Codes (einschließlich der Nutzercodes der Schalter), durch einen Anruf oder über eine Kurzwahltaste aktiviert werden.



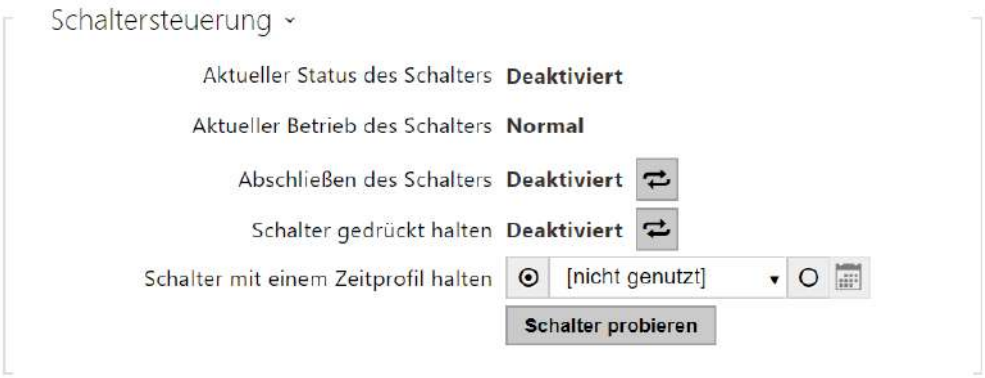
- **Schalter-Modus** – Stellt den monostabilen oder bistabilen Schaltermodus ein. Im monostabilen Modus wird der Schalter nach eingestellter Schaltzeit automatisch ausgeschaltet. Im bistabilen Modus wird der Schalter mit der ersten Aktivierung eingeschaltet und mit der folgenden ausgeschaltet.
- **Dauer des Einschaltens** – Hier wird die Einschaltzeit des Schalters im monostabilen Modus eingestellt. Die eingestellte Schaltzeit wird nicht im bistabilen Modus angewendet.
- **Gesteuerter Ausgang** – weisen Sie dem Schalter einen physischen Ausgang zu. Wählen Sie einen der verfügbaren Geräteausgänge: Relaisausgang, aktiver Ausgang, Erweiterungsausgang. Wenn Sie 'Keiner' auswählen, wird der Schalter keinen physischen Ausgang steuern, kann jedoch externe Geräte über HTTP-Befehle steuern.
- **Ausgangstyp** – wenn Sie ein Sicherheitsrelais verwenden, setzen Sie den Ausgangstyp auf **Sicherheit**. Im Sicherheitsmodus funktioniert der Ausgang im inversen Modus, d. h. bleibt geschlossen und steuert das Sicherheitsrelaismodul mithilfe einer spezifischen Impulsfolge. Wenn Sie ein reverses Türschloss verwenden (d.h. die Tür wird bei Spannungszufuhr auf das Schloss verriegelt), stellen Sie den Ausgangstyp auf den Wert **Invers** ein. Wenn mehrere Schalter auf denselben Ausgang eingestellt sind, aber unterschiedliche Arten von Ausgängen haben, werden sie gemäß der folgenden Priorität gesteuert: 1. Security, 2. Umkehrung, 3. Normal.

Bemerkung

- *Für den Ausgangstyp: **Security** kann man die Zeit für das Schalten des Schalters nur auf 1 s und höher einstellen. Für den Ausgangstyp: **Normal**, **Invers** kann man die Schaltzeit auf 0.1 s und höher einstellen.*

Sicherheit

- Der 12-V-Ausgang dient zum Anschließen des Schlosses. Befindet sich das Gerät (2N IP Intercom, 2N Zutrittseinheiten) jedoch an einem Ort (Gebäudemantel), an dem die Gefahr eines unbefugten Eindringens in das Gerät besteht, wird dringend empfohlen, das 2N Sicherheitsrelais (Bestellnummer 9159010) zu verwenden, um eine maximale Installationssicherheit zu gewährleisten.



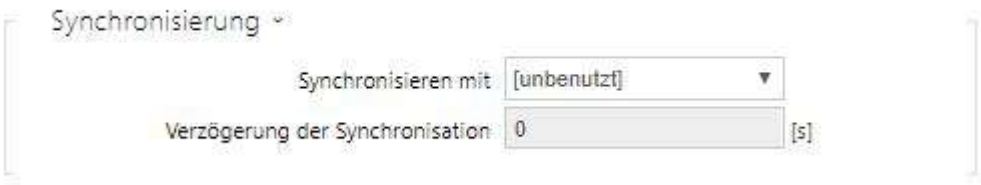
- **Aktueller Status des Schalters** – zeigt den aktuellen Status des Schalters an (Ein oder Aus).
- **Aktueller Betrieb des Schalters** – zeigt den aktuellen Betrieb des Schalters an.
  - **Normal**: Der Schalter ist nicht gesperrt oder wird nicht gehalten.
  - **Gehalten**: Der Schalter wird gehalten und ist nicht gesperrt.
  - **Gesperrt**: Der Schalter ist gesperrt (in diesem Fall spielt es keine Rolle, ob der Schalter gehalten wird, die Sperre hat Priorität).
- **Abschließen des Schalters** – umschalten zwischen den Zuständen entriegelt und verriegelt. Wenn der Schalter verriegelt ist (EIN), ist sein logischer Zustand 0 und kann erst wieder gesteuert werden, wenn er entriegelt ist.
- **Schalter gedrückt halten** – ein: Der Schalter befindet sich permanent in Position 1 und kann erst nach dem Loslassen betätigt werden (wenn sowohl das Halten als auch das Verriegeln aktiv sind, ist der Schalter gesperrt. Aus: Der Schalter wird nicht in Position 1 gehalten.
- **Schalter mit einem Zeitprofil halten** – uermöglicht es, dem Schalter ein vordefiniertes Zeitprofil zuzuweisen oder manuell ein Zeitprofil festzulegen, mit dem der Schalter geschlossen werden kann. Sofern das zugeordnete Zeitprofil nicht aktiv ist, kann der Schalter durch Anlegen einer gültigen RFID-Karte, oder die Eingabe eines Codes werden.
- **Die Taste „Schalter probieren“** – ermöglicht es manuell die Funktion des Schalters zu aktivieren, zum Beispiel des elektrischen Schlosses oder einer anderen angeschlossenen Anlage.

Hinweis

- Wenn der Schalter gesperrt ist und das Gerät aus- und wieder eingeschaltet wird, bleibt der Schalter nach dem Einschalten des Geräts weiterhin gesperrt. Der Schalter verhält sich genauso, wenn er deaktiviert und anschließend aktiviert wird.
- Wenn der Schalter gehalten und das Gerät aus- und wieder eingeschaltet wird, wird der Schalter nach dem Einschalten nicht gehalten. Der Schalter wird nach dem Einschalten des Geräts nur gehalten, wenn das Zeitprofil für das Halten des Schalters eingestellt ist und dieses Profil zum Zeitpunkt des Einschaltens des Geräts aktiv ist. Der Schalter verhält sich genauso, wenn er deaktiviert und anschließend aktiviert wird.

Liste der Universalcodes, mittels denen man aus der Tastatur das Gerät die Schalter aktivieren kann. Für jeden Schalter kann bis 10 Universalcode eingegeben werden.

- Der **Code** – Ermöglicht es den Zifferncode des Schalters einzugeben. Der Code muss mindestens zwei Zeichen für die Türentriegelung vom Gerät und mindestens ein Zeichen für die Türentriegelung mit DTMF vom Telefon enthalten. Wir empfehlen mindestens vier Zeichen zu verwenden. Codes 00 und 11 kann man nicht von der numerischen Tastatur eingeben, sie sind für Öffnen über DTMF reserviert, von der Tastatur werden sie nicht akzeptiert. Der Code wird mit dem Zeichen * bestätigt. Der Code darf bis zu 16 Zeichen lang sein.
- **Zeitprofil** – Ermöglicht dem Schaltercode ein Zeitprofil zuzuordnen und so seine Gültigkeit zu steuern.
- **Ein-/Aus-Codes unterscheiden** – Legen Sie fest, ob Codes in ungeraden Zeilen (1, 3, ...) für die Aktivierung des Schalters und Codes in geraden Zeilen (2, 4, ...) für die Deaktivierung im bistabilen Modus verwendet werden.



- **Synchronisieren** – Erlaubt die Funktion der Schaltersychronisierung, die das automatische Einschalten des Schalters nach der eingestellten Zeit nach dem Schalten eines anderen Schalters ermöglicht. Die Länge des Intervalls zwischen dem Schalten der Schalter wird durch den Parameter **Verzögerung der Synchronisation** bestimmt.
- **Verzögerung der Synchronisation** – Stellt die Länge des Intervalls zwischen dem synchronisierten Einschalten von zwei Schaltern ein. Der Parameter wird nicht angewendet, wenn die Funktion **Synchronisieren** nicht erlaubt ist.

- **Einschaltbefehl** – Legen Sie die URL für den HTTP- oder HTTPS-GET-Request fest, der bei Aktivierung des Schalters gesendet wird. Der Befehl muss in der Form http://ip_adresse/weg sein. Z.B. http://192.168.1.50/relay1=on.
- **Ausschaltbefehl** – Legen Sie die URL für den HTTP- oder HTTPS-GET-Request fest, der bei Deaktivierung des Schalters gesendet wird. Der Befehl muss in der Form http://ip_adresse/weg sein. z. B. http://192.168.1.50/relay1=off.
- **Benutzername** – Nutzername für die Authentifizierung des Anschlusses an ein externes Gerät (WEB-Relais usw.). Der Parameter ist nur dann verbindlich, wenn das externe Gerät eine Authentifizierung verlangt.
- **Passwort** – Passwort zur Authentifizierung des Anschlusses an einem externen Gerät (WEB-Relais, usw.). Der Parameter ist nur dann verbindlich, wenn das externe Gerät eine Authentifizierung verlangt.

Tipp

Im Fall der Verwendung des externen Relais **Best-Nr.: 9137410E** werden folgende HTTP-Befehle verwendet:

- **Für Dauerschalten** – http://ip_adresse/state.xml?relayState=1 (z.B.: http://192.168.1.10/state.xml?relayState=1)
- **Für Schalten auf vordefinierte Zeit (defaultmäßig 1,5 s)** – http://ip_adresse/state.xml?relayState=2 (z.B.: http://192.168.1.10/state.xml?relayState=2)
- **Für Ausschalten** – http://ip_adresse/state.xml?relayState=0 (z:B..: http://192.168.1.10/state.xml?relayState=0)

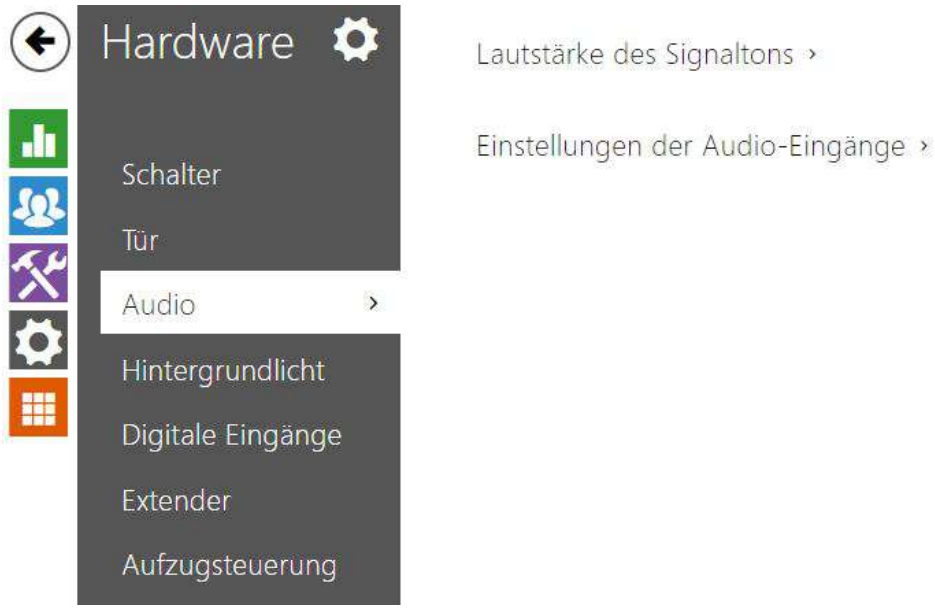
Im Fall der Verwendung des externen Relais **Best-Nr.: 9137411E** werden folgende HTTP-Befehle verwendet (das Zeichen X in den Befehlen muss durch die Relaisnummer ersetzt werden):

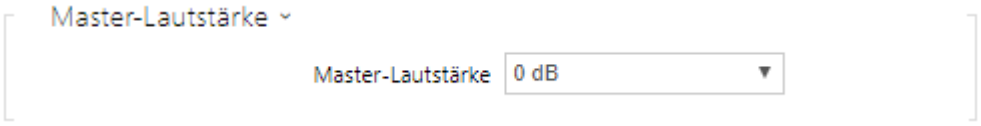
- **Für Dauerschalten** – http://ip_adresse/state.xml?relayXState=1 (z.B.: http://192.168.1.10/state.xml?relay1State=1)
- **Für Schalten auf vordefinierte Zeit (defaultmäßig 1,5 s)** – http://ip_adresse/state.xml?relayXState=2 (z.B.: http://192.168.1.10/state.xml?relay1State=2)
- **Für Ausschalten** – http://ip_adresse/state.xml?relayXState=0 (z.B.: http://192.168.1.10/state.xml?relay1State=0)

Registerkarte Erweiterte

- **Ausgang 1 maximale Leistung** – legt den maximalen Wert der Leistungsaufnahme von Ausgang 1 fest.

5.3.2 Audio



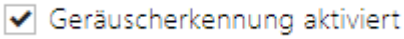


- **Master-Lautstärke** – stellen Sie die Gesamtlautstärke entsprechend der gewünschten Anruf Lautstärke ein und passen Sie dann bei Bedarf andere Lautstärken an. Diese Einstellung wirkt sich auf die Lautstärke aller Geräusche aus.

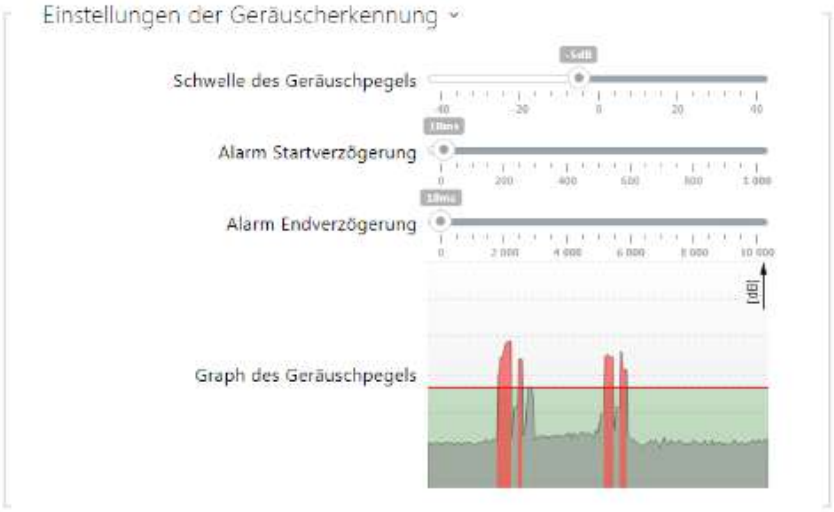
- **Adaptiver Modus aktiviert** – aktivieren Sie den adaptiven Lautstärkemodus, der die Gerätelautstärke allmählich aufgrund des Unterschieds zwischen der gemessenen aktuellen Geräuschpegel und dem ausgewählten Empfindlichkeitsschwellenwert bis zum eingestellten Maximalwert erhöht. Diese Einstellung erhöht außerdem die Gesamtlautstärke.
- **Maximale Verstärkung** – legen Sie den maximalen Gewinn fest, der auf die Gesamtlautstärke angewendet werden kann, sobald der aktuelle Geräuschpegel den Sensibilitätsschwellenwert überschreitet.

- **Sensibilitätsschwelle** – legen Sie den Umgebungsgeräuschpegel fest, der bestimmt, wann die Lautstärke zu steigen beginnt.
- **Aktueller Geräuschpegel** – zeigt das aktuell gemessene Niveau des umgebenden Lärms an.
- **Aktuelle adaptive Verstärkung** – zeigt die aktuell angewendete Verstärkung der Gesamtlautstärke an. Der Wert ist durch die Differenz des aktuellen Schallpegels und der festgelegten Sensibilitätsschwelle bestimmt und überschreitet nie die eingestellte maximale Verstärkung.

- **Lautstärke der Tastenbetätigung** – stellen Sie die Lautstärke des Tastendrucks ein. Der Wert bezieht sich auf die Gesamtlautstärke.
- **Laustärke Warnsignal** – stellen Sie die Lautstärke der Warn- und Signalisierungstöne ein, die im Abschnitt Signalisierung von Betriebszuständen beschrieben sind. Der Wert bezieht sich auf die Gesamtlautstärke.
- **Lautstärke Schalteraktivierung** – stellen Sie die Lautstärke des Schaltton aktivieren ein. Der Wert bezieht sich auf die Gesamtlautstärke.
- **Lautstärke der benutzerdefinierten Tönen** – stellen Sie die Lautstärke der vom Automation abgespielten Benutzergeräusche ein. Der Wert bezieht sich auf die Gesamtlautstärke.



- **Geräuscherkennung aktiviert** – schaltet die automatische Lärmerkennung bzw. das Überschreiten der eingestellten Schwelle des Niveaus des Mikrfonsignals ein. Sie können den Alarm, der durch die Überschreitung des Schwellenwertes ausgelöst wird, mittels des Ereignisses der Automatisierung **Event.NoiseDetected** verarbeiten und ihn an weitere Nutzerabschnitte anknüpfen.



- **Schwelle des Geräuschpegels** – stellt das Schwellenniveau des Signals aus dem Mikrophon ein, bei dessen Überschreitung der Alarm ausgelöst wird.
- **Alarm Startverzögerung** – stellt die Zeit ein, während der das Signal über dem Schwellenwert sein muss, damit der Alarm ausgelöst wird.
- **Alarm Endverzögerung** – stellt die Zeit ein, während der das Signal unter dem Schwellenwert sein muss, damit der Alarm beendet wird.
- **Graph des Geräuschpegels** – zeigt die Historie des gemessenen Signalniveaus an. Rot sind die Zeitpunkte markiert, in den der Alarm aktiviert ist.

5.3.3 Kamera

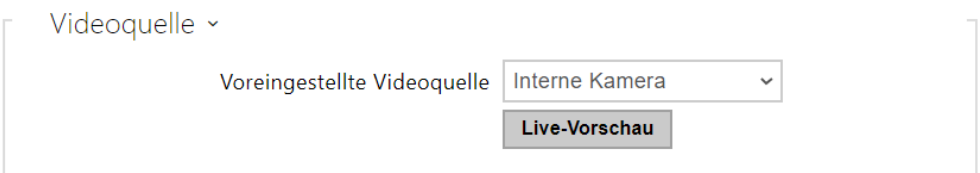
Dieses Menü ist nur bei 2N Geräten verfügbar, die mit einer internen Kamera ausgestattet sind oder den Anschluss einer externen Kamera erlauben - 2N Access Unit QR. Das Kamerasignal kann per E-Mail versendet, über das ONVIF/RTSP-Protokoll an ein anderes Gerät gestreamt (z.B. Videoüberwachung) oder einfach als JPEG-Bilder über das HTTP-Protokoll vom Gerät heruntergeladen werden.

Als Signalquelle kann angewendet werden:

- interne integrierte Kamera,
- übliche externe IP-Kamera, die RTSP-Stream mit den MJPEG-Codecs (max. Auflösung 640 x 480) oder H.264 (max. Auflösung 640 x 480 Base Line Profile) unterstützt. Die maximale empfohlene Aufnahmefrequenz beträgt in beiden Fällen 15 Aufnahmen pro Sekunde. Bei höheren Aufnahmefrequenzen kann es zu unerwünschten Effekten kommen (Herabsetzung der Abspielkontinuität).

Im Menü Kamera werden die Parameter der Kamera wie Helligkeit, Farbsättigung ggf. Anmeldeangaben für die externe IP-Kamera eingestellt. Parameter, die mit Videoanrufen und mit dem Videostreaming zusammenhängen, befinden sich im Menü **Dienste > Streaming** und **Dienste > E-Mail**.

Registerkarte Grundlegende Einstellung



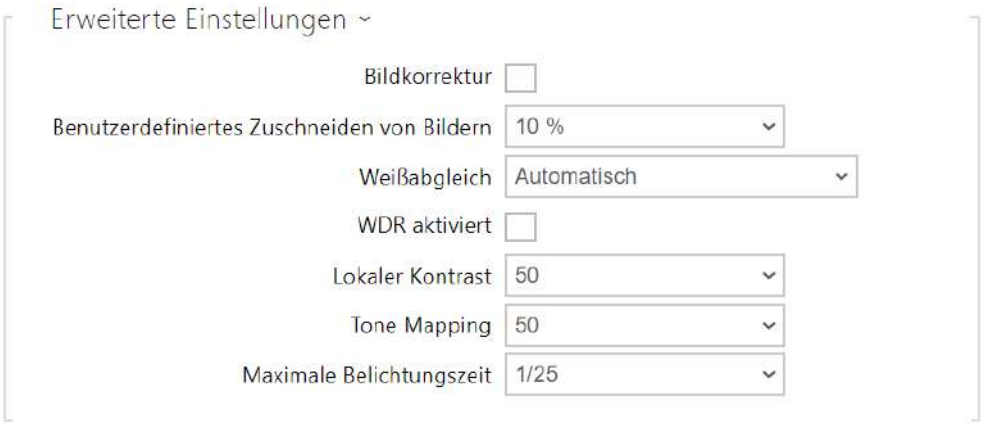
- **Voreingestellte Videoquelle** – stellt die Ausgangsquelle des Videosignals ein. Man kann zwischen der internen Kamera (bzw. zum Interkom angeschlossener Kamera) und der externen Kamera wählen. Die Änderung der Ausgangsquelle des Videosignals wird bei

RTSP-Stream und bei der Benutzung von HTTP API angewendet. Sie müssen in der Applikation **2N IP Eye** die externe Kamera manuell wählen. Falls die externe Kamera nicht richtig angeschlossen oder eingestellt ist, werden die Zeichen N/A auf blauem Hintergrund angezeigt.

- **Live-Vorschau** – zeigt ein Fenster mit einer Live-Ansicht der ausgewählten Kamera an.

Registerkarte Interne Kamera

- **Helligkeitsstufe** – stellt das Helligkeitsniveau des Kamerabildes ein.
- **Belichtungsstufe** – stellt die Belichtungsstufe des Bildes ein (höhere Werte bedeuten, dass das Gerät eine längere Belichtungszeit bevorzugt).
- **Kontrast** – legt den Kamerabildkontrast fest.
- **Farbsättigung** – stellt die Sättigkeit/Farbensaturation des Kamerabildes ein.
- **Kameramodus** – ermöglicht die Einstellung verschiedener Bildaufnahmemodi je nach der tatsächlichen Installation des Geräts (Innen- und Außeneinsatz). Bei Innenanwendung kann man verschiedene Modi der durch Kunstlichtquellen verursachten Flimmerunterdrückung wählen. Bei Außeninstallierungen kann man den Modus der Unterdrückung der Sonneneinstrahlung einstellen.
- **Live-Vorschau** – zeigt ein Fenster mit einer Live-Ansicht der Gerätekamera im ausgewählten Modus an.

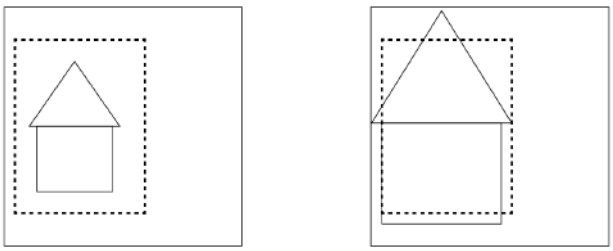


Die Funktionsgruppe Erweiterte Einstellungen gilt für die Modelle 2N IP der Sprechanlage **2N IP Style/2N IP Verso 2.0**.

- **Bildkorrektur** – Fischaugenobjektivkorrektur aktivieren.
- **Benutzerdefiniertes Zuschneiden von Bildern** – legt den standardmäßigen Mittelzuschnitt des Bildes fest (die Kanten werden gleichmäßig abgeschnitten).
- **Weißabgleich** – das Einstellen eines festen Weißabgleichs entsprechend der vorherrschenden Lichtquelle ist geeignet, wenn der automatische Weißabgleich nicht ausreicht (eine falsch ausgewählte Weißabgleichvariante führt zu einer unerwünschten Farbgebung des Bildes).
- **WDR aktiviert** – WDR (Wide Dynamic Range) sollte aktiviert sein, wenn die Szene sehr dunkle und dennoch sehr helle Stellen enthält. WDR stellt sicher, dass die gesamte Szene sichtbar ist.
- **Lokaler Kontrast** – durch Einstellen einer höheren Stufe wird der Kontrast der Schnittstelle zwischen den hellen und dunklen Teilen der Szene verbessert.
- **Tone Mapping** – durch Einstellen einer höheren Ebene wird das Bild hervorgehoben und die Sichtbarkeit verbessert (in diesem Fall kann das Bild eine verzerrte Farbe aufweisen).
- **Maximale Belichtungszeit** – legt die maximale Zeit fest, die ein einzelnes Bild belichtet und aufgenommen wird. Wenn mehr Licht verfügbar ist, ist der Verschluss möglicherweise nicht immer geöffnet und die Kamera stellt automatisch eine kürzere aktuelle Belichtungszeit ein.

Hinweis

- Nach dem Ändern der Einstellung Benutzerdefiniertes Szenentrimmen für ARTPEC-7-Geräte ist es notwendig, die Bereichsdefinition für den Bewegungserkennungsbereich und den Privatbereich zu überprüfen, die sich räumlich ändern, siehe Abbildung.

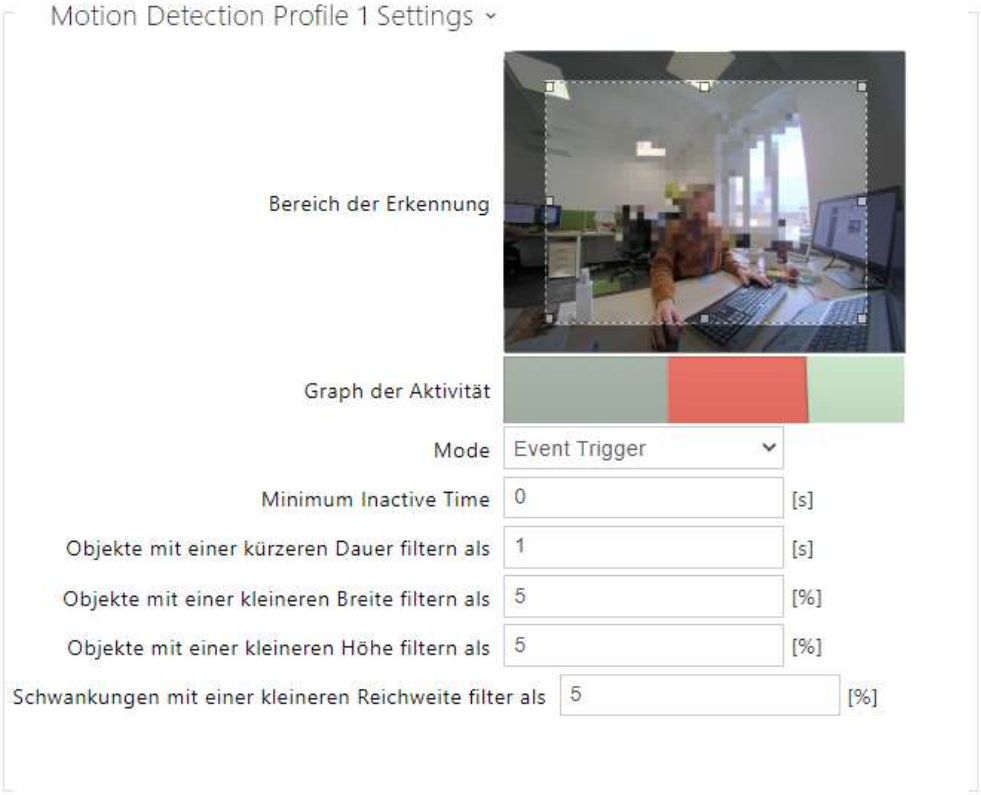


- **Bewegungserkennung aktiviert** – ermöglicht die automatische Bewegungserkennung vom Bild der internen Kamera einzuschalten. Die Bewegung wird mittels der Änderung des Helligkeitsbestandteils im ausgewählten Teil des Bildes in der Zeit erkannt. Bei der Bewegung von Objekten in der Einstellung der Kamera kommt es zur Änderung eines bestimmten Teiles des Bildes – zur Aktivität, die man in Prozenten ausdrücken kann. Wenn die Aktivität die obere Empfindlichkeitsschwelle überschreitet, wird eine Bewegung erkannt. Die Bewegung wird so lange erkannt, solange die Aktivität nicht unter die eingestellte untere Empfindlichkeitsschwelle sinkt. Man kann die Empfindlichkeitsschwellen gemäß den Anforderungen, der konkreten Installation, einstellen und genauso kann man auch den Erkennungsbereich (den Ausschnitt, in dem die betrachtete Aktivität ist) einstellen.

- **Empfindlichkeitsschwelle** – ermöglicht die untere und die obere Empfindlichkeitsschwelle und die Algorithmushysterese der Bewegungserkennung einzustellen.
- **Erkennungsbereich** – ermöglicht den Rechteckausschnitt des Bildes einzustellen, in dem die Bewegungserkennung durchgeführt wird.
- **Aktivitätsdiagramm** – zeigt die Historie der erkannten Aktivität (Änderungen des Helligkeitsbestandteils des Bildes) zusammen mit der eingestellten unteren und oberen Empfindlichkeitsschwelle an.
- **Dauerfilter aktiviert** – aktiviert die Bewegungsfilterung nach Mindestdauer.
- **Objekte mit einer kürzeren Dauer filtern als** – legt die Mindestzeit in Sekunden fest, für die eine Bewegung kontinuierlich aufgezeichnet werden muss, damit ein Bewegungserkennungsereignis angekündigt wird. Der Einstellbereich liegt zwischen 1 bis 5 s. Die Bewegung muss auch die anderen in diesem Abschnitt festgelegten Bedingungen erfüllen.
- **Filter in der Größe des Objektes aktiviert** – aktiviert die Bewegungsfilterung gemäß der minimalen Objektgröße (Breite und Höhe).
- **Objekte mit einer kleineren Breite filtern als** – legt die Mindestbreite von Objekten im Verhältnis zur Gesamtbreite des Kamerabilds fest, die das erkannte Objekt haben muss, damit ein Ereignis angekündigt wird. Der Einstellbereich liegt zwischen 3 und 100 %. Die Bewegung muss auch die anderen in diesem Abschnitt festgelegten Bedingungen erfüllen.
- **Objekte mit einer kleineren Höhe filtern als** – legt die Mindesthöhe von Objekten relativ zur gesamten Höhe des Kamerabilds fest, die das erkannte Objekt haben muss, damit das

Ereignis angekündigt wird. Der Einstellbereich liegt zwischen 3 und 100 %. Die Bewegung muss auch die anderen in diesem Abschnitt festgelegten Bedingungen erfüllen.
- **Filter für Schwankungen aktiviert** – ermöglicht das Filtern der Bewegung schwankender Objekte.
- **Schwankungen mit einer kleineren Reichweite filter als** – legt die minimale Schwingung schwankender Objekte auf die volle Breite oder Höhe des Kamerabilds fest, die die Schwankung überschreiten muss, um das Objekt zu erkennen (die Einstellung hat keine Auswirkung auf nicht schwankende Objekte). Der Einstellbereich liegt zwischen 3 und 20 %. Die Bewegung muss auch die anderen in diesem Abschnitt festgelegten Bedingungen erfüllen.

- **Bewegungserkennung – Profil 1/2 eingeschaltet** – ermöglicht es, die automatische Bewegungserkennung im Bild der internen Kamera einzuschalten. Die Bewegung wird mithilfe der Verfolgung der Änderung der Helligkeitskomponente im ausgewählten Teil des Bildes in der Zeit erkannt. Bei der Bewegung von Objekten im Bildwinkel der Kamera kommt es zur Änderung eines bestimmten Teils des Bildes. Wenn die Aktivität die Obergrenze der Sensibilität übersteigt, wird Bewegung signalisiert. Bewegung wird so lange signalisiert, solange die Aktivität nicht unter die Untergrenze der Sensibilität sinkt.

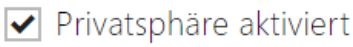


- **Bereich der Erkennung** – ermöglicht den Rechteckausschnitt des Bildes einzustellen, in dem die Bewegungserkennung durchgeführt wird.
- **Graph der Aktivität** – zeigt den Verlauf der erkannten Aktivität auf der Zeitachse an. Grün bedeutet keine Bewegung, grau bedeutet eine erkannte Bewegung, die aber nicht die Bedingungen erfüllt, rot bedeutet eine erkannte Bewegung, die die Bedingungen erfüllt.
- **Modus** – der Modus des Auslösens von Ereignissen ist so entworfen, dass er kurze Ereignisse der Bewegungserkennung für Aktionen generiert, wie z.B. das Aufnehmen von Bildern. Der Modus des Aufnehmens ist so entworfen, dass er längere Ereignisse generiert, z.B. für das Aufnehmen mithilfe von ONVIF.
- **Minimale Inaktivitätszeit** – stellt die minimale Zeit zwischen zwei Ereignissen der Bewegungserkennung ein. Das verhindert die Entstehung zahlreicher Ereignisse in schneller Folge hintereinander.
- **Objekte mit einer kürzeren Dauer filtern als** – legt die Mindestzeit in Sekunden fest, für die eine Bewegung kontinuierlich aufgezeichnet werden muss, damit ein Bewegungserkennungsereignis angekündigt wird. Der Einstellbereich liegt zwischen 1 bis 5 s. Die Bewegung muss auch die anderen in diesem Abschnitt festgelegten Bedingungen erfüllen.
- **Objekte mit einer kleineren Breite filtern als** – legt die Mindestbreite von Objekten im Verhältnis zur Gesamtbreite des Kamerabilds fest, die das erkannte Objekt haben muss, damit ein Ereignis angekündigt wird. Der Einstellbereich liegt zwischen 3 und 100 %. Die Bewegung muss auch die anderen in diesem Abschnitt festgelegten Bedingungen erfüllen.

- **Objekte mit einer kleineren Höhe filtern als** – legt die Mindesthöhe von Objekten relativ zur gesamten Höhe des Kamerabilds fest, die das erkannte Objekt haben muss, damit das Ereignis angekündigt wird. Der Einstellbereich liegt zwischen 3 und 100 %. Die Bewegung muss auch die anderen in diesem Abschnitt festgelegten Bedingungen erfüllen.
- **Schwankungen mit einer kleineren Reichweite filter als** – legt die minimale Schwingung schwankender Objekte auf die volle Breite oder Höhe des Kamerabilds fest, die die Schwankung überschreiten muss, um das Objekt zu erkennen (die Einstellung hat keine Auswirkung auf nicht schwankende Objekte). Der Einstellbereich liegt zwischen 3 und 20 %. Die Bewegung muss auch die anderen in diesem Abschnitt festgelegten Bedingungen erfüllen.

Hinweis

- Bei Geräten mit ARTPEC-7-Prozessor werden bewegte Objekte auch außerhalb des aktiven Bereichs ausgewertet, inklusive der eingestellten Filter (bei Verwendung von **Benutzerdefiniertem Zuschneiden von Bildern** werden Objekte auch in Teilen des Bildes ausgewertet, die beschnitten sind und der Benutzer nicht in der Vorschau sehen kann). Objekte, die in die aktive Zone eindringen, lösen anschließend ein Bewegungserkennungsereignis aus. Wenn der Zeitfilter beispielsweise auf 5 s eingestellt ist, löst ein Objekt, das sich 10 s lang außerhalb des aktiven Bereichs bewegt, unmittelbar nach dem Betreten des aktiven Bereichs ein Bewegungserkennungsereignis aus, da es die Filterbedingung bereits außerhalb des aktiven Bereichs erfüllt hat. Das Objekt wird auch beim Verlassen des aktiven Bereichs weiterhin erkannt und beim erneuten Betreten des aktiven Bereichs löst es sofort ein Ereignis aus (es sei denn, es verlässt den Kamerabildbereich vollständig und wird nicht „vergessen“).



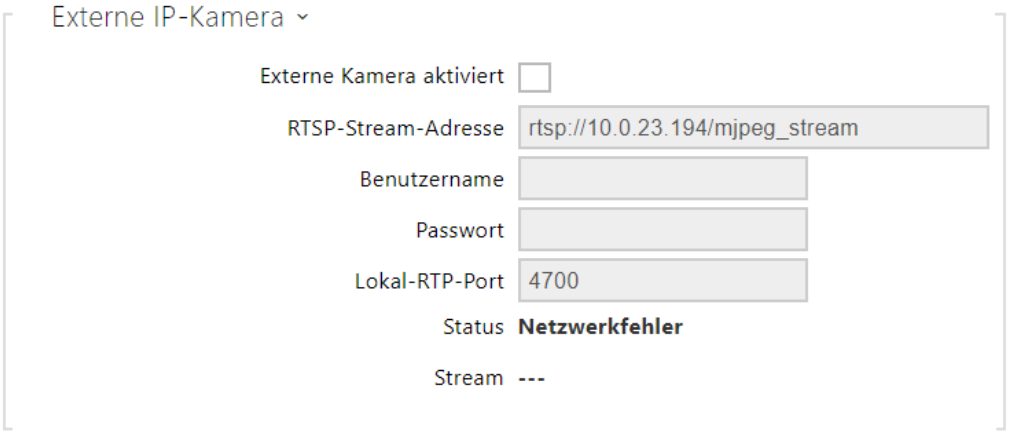
- **Privatsphäre aktiviert** – Aktiviert die Datenschutzfunktion, die einen Teil des Bildes mit der ausgewählten Farbe oder dem ausgewählten Mosaik maskiert.

- **Abdeckungsmodus** – legt die Farbe oder das Mosaik des abgedeckten Bereichs fest.
- **Die Rauheit des Mosaiks** – legt die Rauheit des Mosaiks im Bereich Schutz der Privatsphäre fest.
- **Bereich Schutz der Privatsphäre** – legt die Position und Größe des Datenschutzbereichs fest.

Hinweis

- Der Schutz der Privatsphäre kann andere Funktionen wie das Lesen von QR-Codes oder die Bewegungserkennung einschränken. Es wird nicht empfohlen, den Schutz der Privatsphäre gleichzeitig mit diesen Funktionen zu verwenden.

Registerkarte Externe Kamera



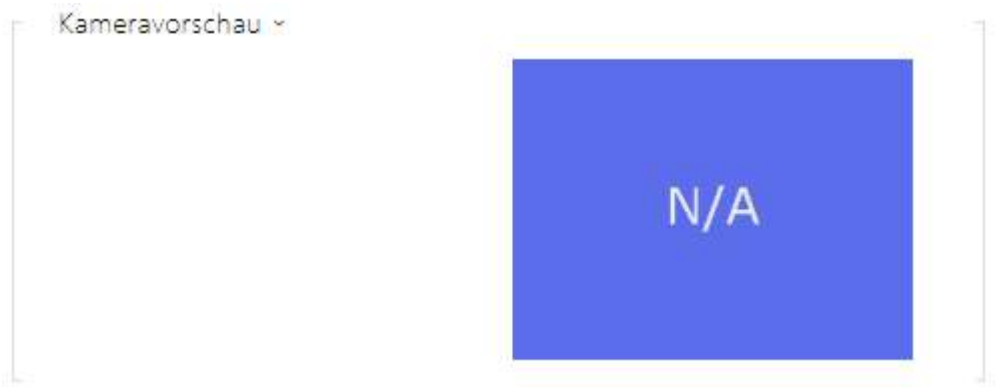
- **Externe Kamera aktiviert** – erlaubt das Herunterladen des RTSP-Streams von der externen IP-Kamera. Geben Sie die gültige RTSP-Stream-Adresse bzw. den Benutzernamen und das Passwort ein, damit die Funktion korrekt ausgewählt wird.
- **RTSP-Stream-Adresse** – die die RTSP-Stream-Adresse der IP-Kamer im Format rtsp://ip_adresse_kamera/parameter1=x&parameter2=y, siehe Tabelle der Parameter unten. Die Parameter sind speziell für das ausgewählte IP-Kameramodell vorgesehen. Wenn Sie als externe Kamera ein anderes Interkom **2N IP** benutzen, wenden Sie die Adresse in der Form http://ip_adresse/mjpeg_stream oder http://ip_adresse/h264_stream an.

Parameter	Beschreibung	Beispiel / Werte
vcodec	Video Codec	vcodec=h264 für den Codec H.264 vcodec=mjpeg für den Codec MJPEG
vres	Videoauflösung	vres=1920x1080 für FullHD
fps	Video Frame Rate	fps=15 (1 bis 30 fps, der maximal mögliche Wert für den MJPEG-Videocodec ist 15 fps)
vbr	Bitrate	vbr=768 für 768 kbps
audio	Audio	• audio=1 (aktiviert) • audio=0 (deaktiviert)
zipstream	Zipstream (nur für H.264 verfügbar)	• zipstream=off (deaktiviert) • zipstream=low • zipstream=medium • zipstream=high • zipstream=higher

- **Benutzername** – Nutzername für die Authentifizierung des Anschlusses an die externe IP-Kamera. Der Parameter ist nur dann verbindlich, wenn die externe IP-Kamera die Authentifizierung verlangt.
- **Passwort** – Passwort für die Authentifizierung des Anschlusses an die externe IP-Kamera. Der Parameter ist nur dann verbindlich, wenn die externe IP-Kamera die Authentifizierung verlangt.
- **Lokaler RTP-Port** – stellt den lokalen UDP-Port für den Empfang des RTP- Streams ein.

Tipp

- FAQ: Externe Kamera – Wie stellt man sie vom Interkom 2N IP ein?



Im Fenster Kameraeinsicht wird das aktuelle aus der externen Kamera empfangene Bild angezeigt. Falls die externe Kamera nicht richtig angeschlossen oder eingestellt ist, werden die Zeichen N/A auf blauem Hintergrund angezeigt.

Im Fenster Kommunikation der externen IP-Kamera wird der Verlauf der RTSP-Kommunikation mit der eingestellten externen IP-Kamera einschließlich der eventuellen Fehler und der Störungsstatus angezeigt.

5.3.4 Hintergrundlicht

In dieser Registerkarte kann man unabhängig das Unterbeleuchtungsniveau der Namensschilder, der Tasten und das Leuchtniveau der Signalisierungs-LED einstellen.

- **Hintergrundlicht** – Stellt die Helligkeitsstufe der Hintergrundbeleuchtung tagsüber. Der Wert wird in Prozenten der höchstmöglichen LED-Helligkeit angegeben.

- **Signalisierungs-LED** – Legt die Helligkeitsstufe der Signal-LED tagsüber fest. Der Wert wird in Prozenten der höchstmöglichen LED-Helligkeit angegeben.

Anmerkung

- Die Einstellung der Helligkeitsstufe beeinflusst die Funktionsfähigkeit, den Verbrauch und das Gesamtaussehen der Anlage. Hohe Helligkeit der Namensschilder- und Tastenunterbeleuchtung kann beim niedrigen Niveau des umgebenden Lichts die Verblendung der Person verursachen, die vor ddas Gerät steht, und erhöht gleichzeitig generell den Verbrauch der Anlage. Niedrige Helligkeit der Signalisierungs-LED führt bei der Verwendung das Gerät in der direkten Sonne zur Herabsetzung des Kontrastes zwischen der ausgeschalteten und eingeschalteten LED und zur schwierigen Erkennung des LED-Status.

5.3.4.1 Hintergrundbeleuchtung (2N Access Unit QR)

Auf dieser Registerkarte kann die Beleuchtungsstärke der Signal-LEDs unabhängig eingestellt werden.

Wenn das Gerät mit einem Umgebungslichtsensor ausgestattet ist, wählt es automatisch die geeignete Beleuchtungsstärke innerhalb des eingestellten Wertebereichs. Siehe Tabellen unten:

Funktion	2N-Zugangseinheit QR
Steuerung der Beleuchtungsstärke	**Ja**
Umgebungslichtsensor	**Ja**

Die Parametereinstellungen in der Gruppe Hintergrundbeleuchtung gelten für die Hintergrundbeleuchtung der Haupteinheit und der Erweiterungsmodule.

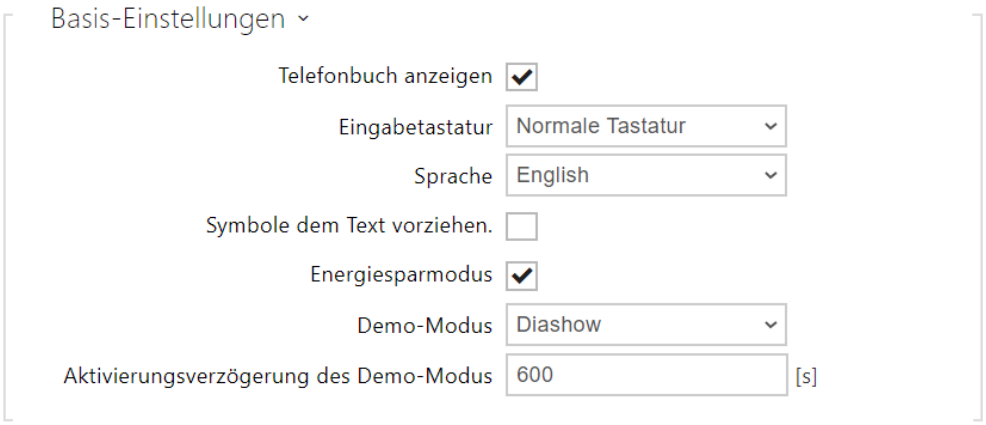
- **Intensität tagsüber** - legt den Wert für die Intensität der Hintergrundbeleuchtung bei Tag fest. Der Wert wird als Prozentsatz der maximal möglichen LED-Helligkeit angegeben.
- **Intensität bei Nacht** - legt den Wert der LED-Helligkeit bei Nacht fest. Der Wert wird als Prozentsatz der maximal möglichen LED-Helligkeit angegeben. Wenn die Intensität bei Tag und die Intensität bei Nacht auf denselben Wert eingestellt sind, wird die Umgebungshelligkeit nicht berücksichtigt.
- **Aktueller Wert** - zeigt den aktuell automatisch gewählten Wert für die LED-Intensität entsprechend der aktuell erfassten Umgebungshelligkeit an.

5.3.5 Display

Die 2N Zutrittseinheiten können (2N Access Unit 2.0 und 2N Access Unit QR) um ein Displaymodul erweitert werden. Das Farb-LCD-Display bietet eine Touch-Tastaturfunktion und zeigt den Status des Geräts an (z. B. Öffnen der Tür, Verweigerung des Zutritts usw.) oder kann

auch im Präsentationsmodus verwendet werden, in dem nach einer festgelegten Zeit der Inaktivität Präsentationen in Form einer Reihe hochgeladener Bilder auf dem Display angezeigt werden. Zwischen den einzelnen Bildern wird automatisch umgeschaltet und man kann die Dauer des Anzeigens eines Bildes einstellen.

Registerkarte Display



- **Telefonbuch anzeigen** – ermöglicht die Funktion des Telefonbuchs auf dem Display einschalten und ausschalten.
- **Eingabetastatur** – stellt die Freigabe und die Art der Tastatur ein
  - **Deaktiviert** – die Tastatur ist für den Eingang nicht verfügbar
  - **Normale Tastatur** – stellt das Anzeigen der üblichen Tastaturart ein
  - **Verschlüsselte Tastatur** – diese Funktion wird zufälligerweise die Reihenfolge der Tasten der nummerischen Tastatur vor jedem neuen Anzeigen auf dem Display durchmischen. Die Funktion erschwert das Ablesen des eingegebenen Codes bei Beobachtung durch eine weitere Person.
- **Sprache** – stellt die Sprache der Texte ein, die auf dem Display angezeigt werden. Man kann eine der vordefinierten Sprachen wählen.
- **Symbole dem Text vorziehen** – die Symbole auf dem Display werden vor dem Text positioniert.
- **Energiesparmodus** – ermöglicht die Aktivierung des Sparmodus, in dem die Displayhelligkeit gesenkt wird. Wenn es während der Dauer von zwei Verzögerungen der Präsentationsaktivierung zu keinem Ereignis kommt, war die Aktivierung des Sparmodus erfolgreich. Der Sparmodus ist im Fall des Wertes 0, der in der Spalte für die Verzögerung der Präsentationsaktivierung angeführt ist, ausgeschaltet. Bei einer Bewegung vor der Kamera des Gerätes oder bei einem beliebigen Ereignis auf dem Display (z.B. Aktivierung

des Türschlosses oder Berührung des Displays) wird das Display in volle Helligkeit übergehen.
- **Demo-Modus** – legt fest, ob das Gerät im Leerlauf in den Demo-Modus wechselt. Im Demo-Modus kann ein anderes Verhalten gewählt werden (Präsentation, Firmenlogo, Adresse).
- **Aktivierungsverzögerung des Demo-Modus** – legt die Leerlaufzeit fest, nach der das Gerät in den Demo-Modus wechselt, zwischen 1 bis 600 Sekunden.

- **Originalsprache** – ermöglicht die Schablone der Lokalisierungsdatei für die eigene Übersetzung herunterzuladen. Es handelt sich um eine XML-Datei mit allen auf dem Display angezeigten Texten.
- **Benutzersprache** – ermöglicht es eine eigene Lokalisierungsdatei hochzuladen, zu löschen und herunterzuladen.

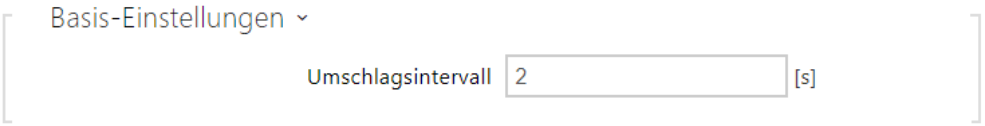
Anmerkung

Wenn Ihnen keine der vordefinierten Sprachen des Displays zusagt, gehen Sie wie folgt vor:

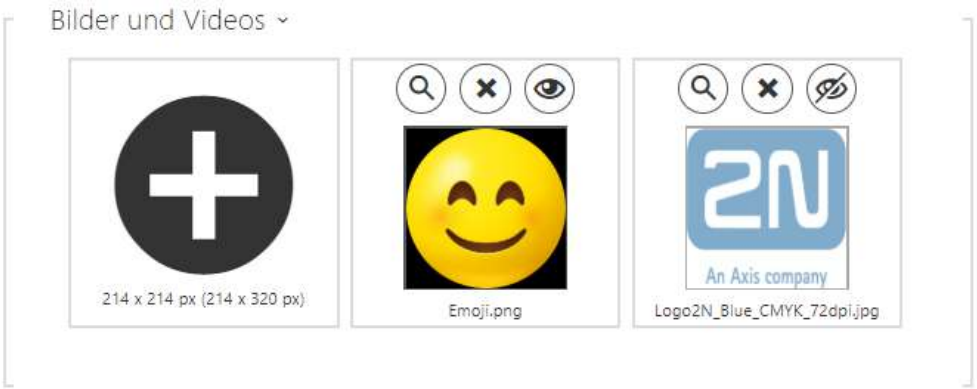
- laden sie die originale Sprachdatei herunter (sie ist in Englisch),
- passen Sie die Datei mithilfe des Texteditors an (ersetzen Sie die englischen Texte durch eigene),
- laden Sie die angepasste Lokalisierungsdatei zurück in das Gerätes hoch,
- stellen Sie den Parameter **Spracheinstellung > Sprache** auf den Wert **eigene** ein,
- texte direkt auf dem Display des Gerätes kontrollieren und ggf. ändern.

Registerkarte Diashow

In dieser Registerkarte wird die Liste der Bilder eingestellt, die im Modus Präsentation angezeigt werden. Man kann bis zu 8 Bilder hochladen, die dann nach und nach mit eingestellter Verzögerung umgeschaltet werden.



- **Umschlagsintervall** – stellt die Dauer des Anzeigens eines Bildes der Präsentation ein, bevor es zum Umschalten zum weiteren Bild kommt.



Die Maße der eingespielten Bilder sollten 214 x 214 Pixel sein. Im anderen Fall werden sie automatisch der Displayauflösung angepasst.

Um eine Vorschau des hochgeladenen Bildes anzuzeigen, verwenden Sie das Lupensymbol 
. Das Bild kann mit dem Symbol  gelöscht werden. Mit dem Symbol  können Sie die Anzeige des ausgewählten Bilds oder Videos auf dem Display ausblenden.

Wenn kein Bild hochgeladen wurde, wird der Modus Präsentation nicht aktiviert.

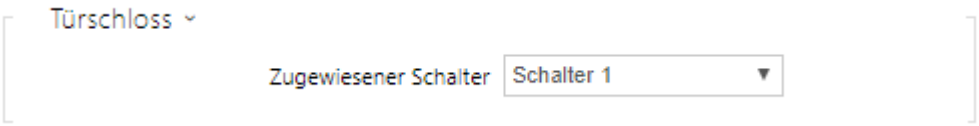
Tipp

- Um den angezeigten Teil "Mit Berührung beginnen" auf dem Display zu verbergen, ist ein Bild mit einer Auflösung von 214 x 320 px hochzuladen.

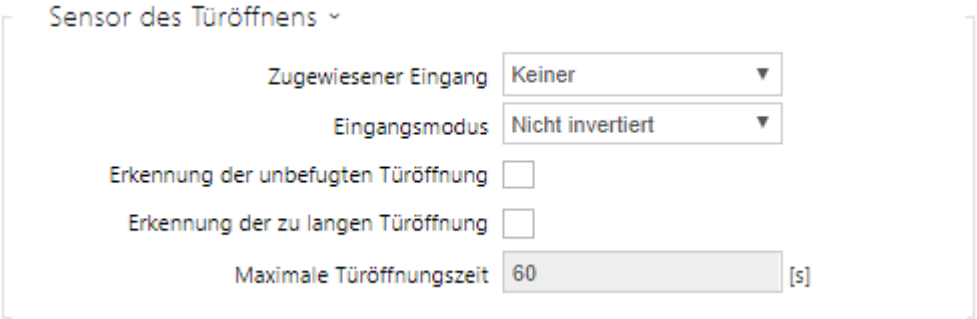
5.3.7 Digitale Eingänge

In diesem Teil der Interkomkonfiguration können Sie die Parameter, die mit digitalen Eingängen zusammenhängen, und ihre Verknüpfung mit weiteren Funktionen einstellen.

Registerkarte Türen

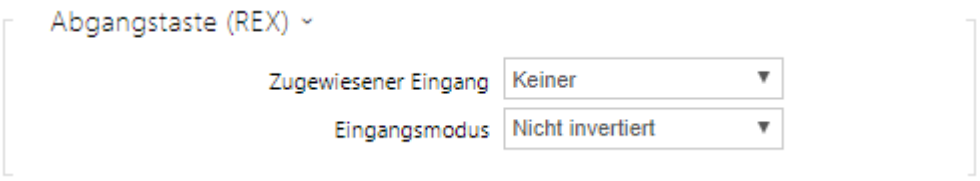


- **Zugewiesener Schalter** – ermöglicht den Schalter zu wählen, der für die Bedienung des elektromagnetischen Schlosses der Tür bestimmt ist. Nach dem Status dieses Schalters richtet sich die Signalisierung der Türentriegelung (grünes Symbol der Tür, grüne LED).



- **Zugewiesener Eingang** – ermöglicht einen der logischen Eingänge (ggf. keinen Eingang) für die Erkennung der offenen Tür zu bestimmen.

- **Eingangsmodus** – ermöglicht das aktive Niveau (Polarität) des Eingangs einzustellen. Nicht invertiert / Invertiert.
- **Erkennung der unbefugten Türöffnung** – ermöglicht das Öffnen der Tür bei geschlossenen Schloss zu erkennen
- **Erkennung der zu langen Türöffnung** – ermöglicht lang geöffnete Türen zu erkennen.
- **Maximale Türöffnungszeit** – maximale erlaubte Zeit der geöffneten Tür in Sekunden.



- **Zugewiesener Eingang** – ermöglicht einen der logischen Eingänge (ggf. keinen Eingang) für die Funktion der Abgangstaste zu bestimmen. Durch Aktivierung der Abgangstaste kommt es zum Schalten des gewählten Schalters. Die Zeit und die Art der Einschaltung sind durch die aktuelle Einstellung des gewählten Schalters gegeben.
- **Eingangsmodus** – ermöglicht das aktive Niveau (Polarität) des Eingangs einzustellen. Nicht invertiert / Invertiert.

Registerkarte Sicherheit

- **Zugewiesener Eingang** – Ermöglicht einen der logischen Eingänge (ggf. keinen Eingang) für die Signalisierung des Status "Gesichert" zu bestimmen. Der Zustand "Gesichert" wird dann mit dem roten LED an der Zugangseinheit signalisiert.
- **Eingangsmodus** – Ermöglicht das aktive Niveau (Polarität) des Eingangs einzustellen.

Die Modelle, die mit einem Schutzschalter ausgestattet sind, ermöglichen das Öffnen des Gehäuses der Anlage zu erkennen und diese Situation als das Ereignis **TamperSwitchActivated** zu signalisieren. Die Ereignisse werden in einen Log eingetragen, den man mittels der HTTP API auslesen kann (siehe Handbuch **2N HTTP API**).

Wenn die Funktion erlaubt ist, werden nach der der Aktivierung des Schutzschalters alle Schalter für 30 Minuten gesperrt. Die Sperre ist auch nach dem Neustart der Anlage aktiv. Man kann ferner einzelne Ports mittels der **Automation** bedienen. Das Entsperren aller Schalter kann man mit der Taste **Entsperren**, durch das Verbieten dieser Funktion oder durch das Zurücksetzen der Konfiguration in die Fabrikeinstellung durchführen.

- **Zugewiesener Eingang** – Ermöglicht den logischen Eingang zu wählen, an den der Schutzschalter angeschlossen ist. Bei der Aktivierung des Schutzschalters wird das Ereignis **TamperSwitchActivated** signalisiert.
- **Automatische Blockierung der Schalter aktivieren** – Sperrt die Schalter durch die Aktivierung des Schutzschalters für 30 Minuten.
- **Zustand der Schalter-Blockierung** – Zeigt und ermöglicht die Einstellung der Schaltersperre.

Anmerkung

Gilt für das Modell **2N Access Unit**:

- Ab PCB Version 599v2 sind alle Modelle mit optischem Schutzschalter ausgestattet.
- Ab PCB Version 599v2 wird neu der zugeordnete Eingang durch Hintergrundbeleuchtung des Piktogramms auf dem Modul signalisiert. Bei niedrigeren PCB Versionen wird er durch Aufleuchten der LED rechts am Modul.

Registerkarte Starter

- **Auslöser für Benutzeraktionen 1, 2**
  - **Zugewiesener eingang** – ermöglicht Ihnen die Auswahl einer logischen Eingabe, der die Funktion einer Benutzeraktion ausführt. Wenn die Funktion aktiviert ist, wird das UserActionActivated Event mit dem Parameter state=in in die Liste der Events auf dem Gerät geschrieben (Deaktivierung der Funktion wird durch state=out angezeigt). Ausgehend von diesem Ereignis können beispielsweise übergeordnete Systeme Alarm schlagen, ein ganzes Gebäude verriegeln oder andere Maßnahmen ergreifen.
  - **Eingangsmodus** – wählt aus, ob die Benutzeraktion basierend auf dem inversen Wert der zugewiesenen Eingabe oder einem normalen Wert ausgewertet wird.

5.3.8 Erweiterungsmodule

Die **2N Access Unit, 2N Access Unit 2.0** und **2N Access Unit QR** können mit Erweiterungsmodulen, die über den VBUS-Bus angeschlossen werden, erweitert werden. Die verfügbaren Module sind in der Installationsanleitung des Geräts aufgeführt. Solange kein Erweiterungsmodul angeschlossen ist, wird dieser Abschnitt in der Web-Konfigurationsoberfläche nicht angezeigt. Um den Bereich zu sehen, wird empfohlen, das Gerät nach dem Anschluss des Erweiterungsmoduls neu zu starten.
Die Module sind gegenseitig verbunden und bilden eine Kette. Jedes der Module hat seine Nummer, die durch die Reihenfolge in der Kette gegeben ist (das erste Modul hat die Nummer 0).

Man kann jeden der angeschlossenen Module einzeln konfigurieren. Die Parameter sind für den jeweiligen Modultyp spezifisch.

Hinweis

- Das angeschlossene Modul wird nicht automatisch erkannt. Starten Sie das Gerät neu, um das angeschlossene Modul in der Liste der Erweiterungsmodule anzuzeigen.
- Wenn die Firmware-Versionen des anzuschließenden Moduls und des Hauptgeräts nicht kompatibel sind, wird das Modul nicht erkannt. Daher ist es notwendig, die Gerätefirmware nach dem Anschließen der Module zu aktualisieren. Die Firmware kann mittels der Webschnittstelle des Gerätes im Teil System > Wartung aktualisiert werden.

Hinweis

- Nach Ersetzen der Module müssen die neuen Module wieder konfiguriert werden. Die Konfiguration ist mit Seriennummer verknüpft.

Anmerkung

- *Die Module kann man mittels einer Textzeile, die eine Liste der Parameter enthält, konfigurieren (Parametername=Parameterwert), getrennt mit Strichpunkten. Gegenwärtig werden nur einige Parameter veröffentlicht. Die übrigen Parameter haben eher experimentellen Charakter, sie können sich künftig ändern, deswegen werden sie nicht veröffentlicht.*

Hinweis

- Nach dem Verbinden des Moduls mit dem Kartenlesegerät an das Gerät, in dem die Leseschlüssel **2N PICard** hochgeladen sind, muss das Modul mit dem Gerät gekoppelt werden. Ohne Kopplung wird das Modul des Lesegeräts keinen Zugang zu den Leseschlüsseln haben und nicht in der Lage sein, verschlüsselte Karten einzulesen. Die Kopplung des Moduls erfolgt mithilfe der Taste **Modul paaren**.

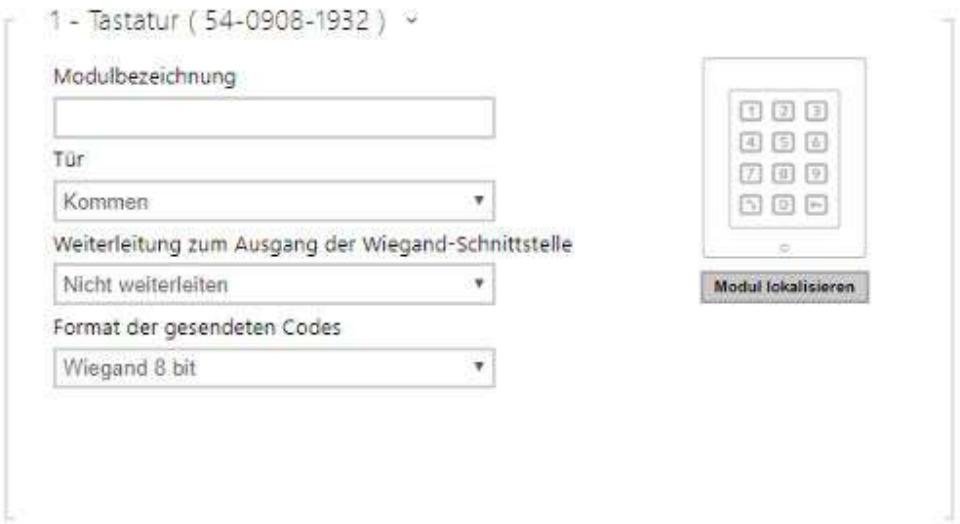
Hinweis

- Der Name des Moduls muss einzigartig sein.
- Die Module, deren Namen man nicht konfigurieren kann, können über ext <modul_position> adressiert werden.

Tipp

- Durch die Platzierung des Mauscursors auf dem Bild des Moduls werden seine grundlegenden Produktions- und Softwareinformationen angezeigt

Konfiguration des Tastaturmoduls

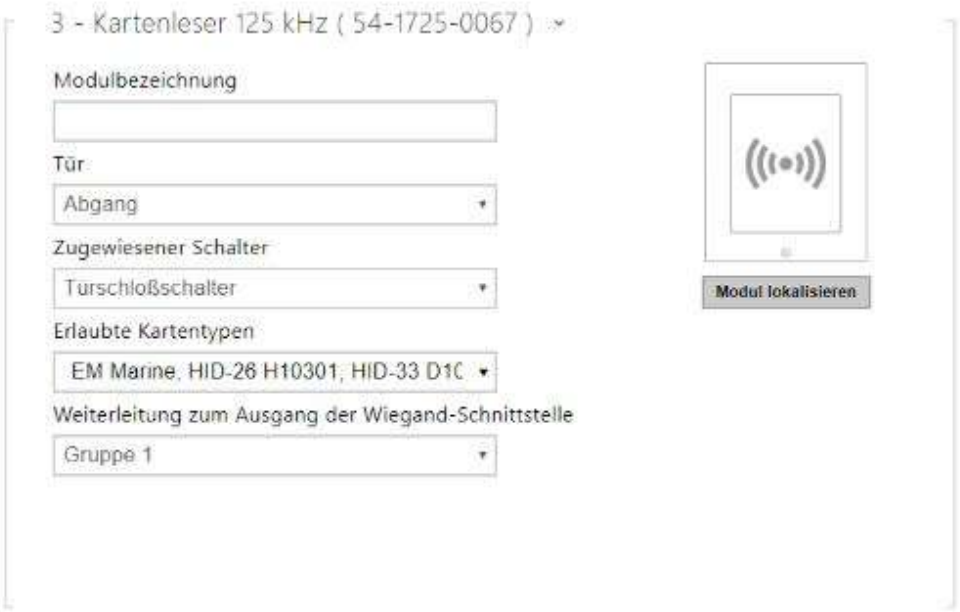


- **Modulbezeichnung** – Stellt den Modulnamen ein. Der Modulname wird beim Loggen der Ereignisse von der Tastatur verwendet.
- **Tür** – Stellt die Durchgangsrichtung bei Verwendung eines Lesegeräts ein (Kommen, Gehen). Der Richtungsparameter findet beim Anwesenheitssystem Anwendung.
- **Weiterleitung zum Ausgang der Wiegand-Schnittstelle** – Stellt die Gruppe der Wiegand-Ausgänge ein, an die alle betätigten Tasten gesendet werden.
- **Format der gesendeten Codes** – Auswahl aus 4bit und 8bit (höhere Zuverlässigkeit) des Formats.

Konfiguration des Infopanelmoduls

- Derzeit sind keine Parameter dieses Moduls veröffentlicht.

Konfiguration des 125 kHz-Kartenlesermoduls



- **Modulbezeichnung** – Stellt den Modulnamen ein. Die Bezeichnung des Moduls wird beim Loggen der Ereignisse des Kartenlesers verwendet.
- **Tür** – Stellt die Durchgangsrichtung bei Verwendung eines Lesegeräts ein (Kommen, Gehen). Der Parameter Richtung wird durch das Anwesenheitssystem genutzt.
- **Zugewiesener Schalter** – Stellt die Nummer des Schalters ein, der nach der Nutzerauthentifizierung mittels dieses Moduls aktiviert wird. Wenn die Option

Türschloßschalter eingestellt ist, werden die Authentifizierungsregeln vom Menu Hardware > Türenverwendet.

- **Erlaubte Kartentypen** – Damit kann der Typ der Karte eingestellt werden, der durch das Lesegerät akzeptiert wird. Das Lesegerät unterstützt zu einem Zeitpunkt nur einen Kartentyp.
- **Weiterleitung zum Ausgang der Wiegand-Schnittstelle** – Stellt die Gruppe mit den Wiegand-Ausgängen ein, an welche alle über die RFID-Leser erhaltenen ID weitergeleitet werden.

Tipp

- Für das schnellere Lesen der Zutrittskarten empfehlen wir, in der Einstellung des jeweiligen Moduls nur die Kartentypen auszuwählen, die der Nutzer verwendet.

Konfiguration des 13,56 MHz-Kartenlesemoduls

- **Modulbezeichnung** – Stellt den Modulnamen ein. Die Bezeichnung des Moduls wird beim Loggen der Ereignisse des Kartenlesers verwendet.
- **Tür** – Stellt die Durchgangsrichtung bei der Verwendung des Lesegerätes ein (Nicht spezifiziert, Kommen, Gehen). Der Parameter Richtung wird durch das Anwesenheitssystem genutzt.

- **Zugewiesener Schalter** – Stellt die Nummer des Schalters ein, der nach der Nutzerauthentifizierung mittels dieses Moduls aktiviert wird. Wenn die Option Türschloßschalter eingestellt ist, werden die Authentifizierungsregeln vom Menu Hardware > Türenverwendet.
- **Erlaubte Kartentypen** – Ermöglicht einen oder mehrere Typen der akzeptierten Karten zu wählen. Wenn kein Typ ausgewählt wird, dann werden alle Typen der unterstützten Karten akzeptiert.
- **Samsung NFC Kompatibilitätsmodus** – Lässt die Samsung NFC Kompatibilitätsmodus zu.
- **Weiterleitung zum Ausgang der Wiegand-Schnittstelle** – Stellt die Gruppe der Wiegand-Ausgänge ein, an die alle aufgezeichneten IDs der RFID-Karten gesendet werden.

Tipp

- Für das schnellere Lesen der Zutrittskarten empfehlen wir, in der Einstellung des jeweiligen Moduls nur die Kartentypen auszuwählen, die der Nutzer verwendet.

Konfiguration des Bluetooth-Lese-Moduls

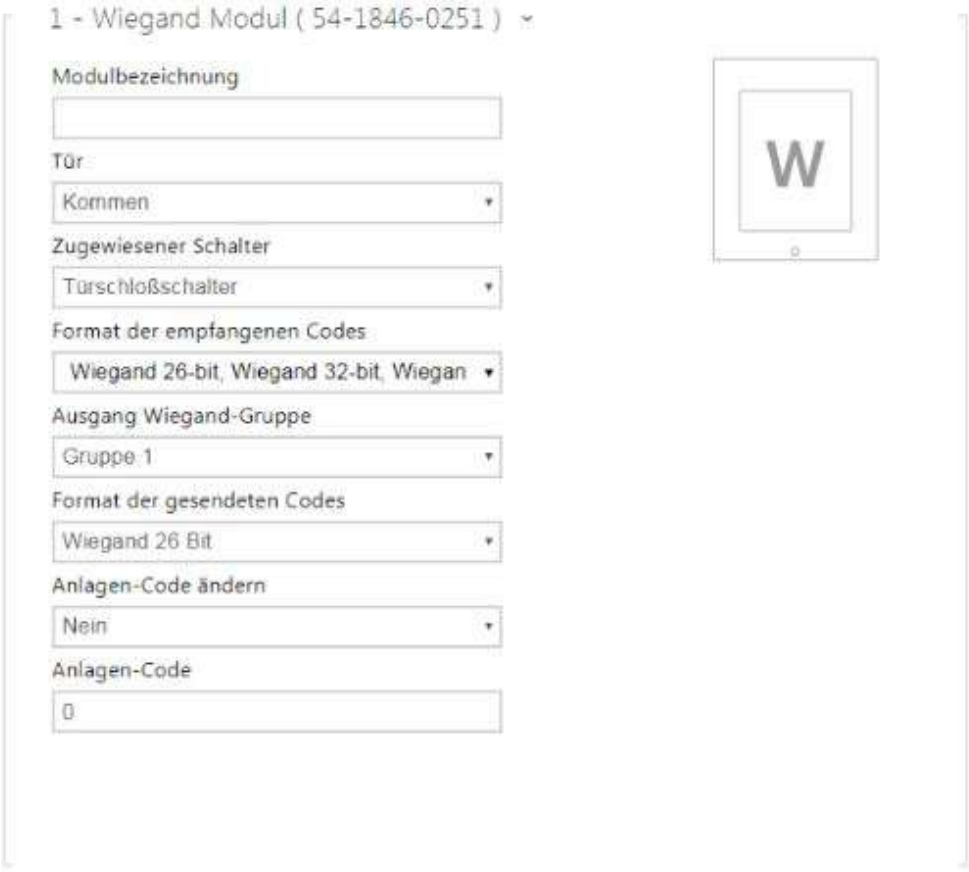
- **Modulbezeichnung** – stellt den Modulnamen ein. Die Bezeichnung des Moduls wird beim Loggen der Ereignisse aus dem Bluetoothmodul verwendet.
- **Tür** – stellt die Durchgangsrichtung bei der Verwendung des Lesegerätes ein (Nicht spezifiziert, Kommen, Gehen). Der Parameter Richtung wird durch das Anwesenheitssystem genutzt.
- **Zugewiesener Schalter** – stellt die Nummer des Schalters ein, welcher nach der Benutzer-Authentifizierung über dieses Modul aktiviert wurde. Wenn die Option Türschloßschalter eingestellt ist, werden die Authentifizierungsregeln vom Menu Hardware / Türen verwendet.
- **Signalreichweite** – stellt die maximale Reichweite des Signals, d.h. die Entfernung ein, in der das Bluetooth-Modul noch mit dem Mobiltelefon kommunizieren wird:
  - **Kurz** – die Reichweite ist bei den meisten Telefonen geringer als 2 m.
  - **Lang** – die Reichweite ist die maximal mögliche.
- **Authentifizierung starten** – stellt die Authentifizierungsart mittels des Mobiltelefons ein:
  - **Berühren der App** – man muss die Authentifizierung bestätigen, mit dem Antippen der Schaltfläche in der laufenden Applikation im Mobiltelefon
  - **Durch Drücken auf das Gerät** – die Authentifizierung muss durch Berührung auf dem Leser in Anwesenheit des Telefons mit gekoppelten **2N Mobile Key** Applikation bestätigt werden.

Konfiguration des Eingangs- und Ausgangsmoduls I/O

- **Modulbezeichnung** – Stellt den Modulnamen ein. Der Modulname wird im Rahmen der Spezifikation des Ein- oder Ausgangs in den SetOutput-, GetInput- und InputChanged-Objekten in der Einstellung **Automation** verwendet.

Konfiguration des Wiegand-Moduls

Das Wiegand-Modul ist mit einer Eingangs- und Ausgangs-Wiegand-Schnittstelle ausgestattet, die von einander unabhängig sind, unabhängige Einstellung haben und Codes gleichzeitig empfangen und senden können Man kann die Eingangs-Wiegand-Schnittstelle für den Anschluss von externen Geräten nutzen, wie RFID-Kartenleser, biometrische Scanner u.Ä. Mittels der Ausgangs-Wiegand-Schnittstelle kann man das Gerätes z.B. an das Sicherheitssystem im Gebäude anschließen (man kann die IDs der RFID-Karten, die an den angeschlossenen RFID-Leser angelegt werden, bzw. die Codes, die in einer beliebigen Eingangs-Wiegand-Schnittstelle aufgenommen wurden, absenden). Das Wiegand-Modul ist mit einem logischen Eingang und einem logischen Ausgang ausgestattet, die man mittels der Automation bedienen kann.



- **Modulbezeichnung** – Stellt den Modulnamen ein. Der Modulname wird im Rahmen der Spezifikation des Ein- oder Ausgangs in den SetOutput-, GetInput- und InputChanged-Objekten in der Einstellung **Automation** verwendet.
- **Tür** – Stellt die Durchgangsrichtung bei Verwendung eines Lesegeräts ein (Kommen, Gehen). Der Parameter Richtung wird durch das Anwesenheitssystem genutzt.
- **Zugewiesener Schalter** – Stellt die Nummer des Schalters ein, welcher nach der Benutzer-Authentifizierung über dieses Modul aktiviert wurde. Wenn die Option Türschloßschalter eingestellt ist, werden die Authentifizierungsregeln vom Menu Hardware > Türenverwendet.
- **Format der empfangenen Codes** – Stellt das Format der emfangenen Codes ein (Wiegand 26, 32, 37 und RAW).
- **Ausgang Wiegand-Gruppe** – Weist den Wiegand-Ausgang der Gruppe zu, an welche die Codes von den angeschlossenen Kartenlesern bzw. Wiegand-Ausgängen weitergeleitet werden können.
- **Format der gesendeten Codes** – Stellt das Format der gesendeten Codes ein (26 bit, 32 bit, 37 bit, RAW Format, 35 bit, Corp. 1000, 48 bit, Corp. 1000 a Auto).
- **Facility Code ändern** – Dadurch kann der erste Codeteil über die Wiegand-Schnittstelle eingestellt werden. Betrifft den Austrittsmodus der Schnittstelle für das Format des

gesendeten Codes 26 bit. Überprüfen Sie bei Ihrem Sicherheitssystemlieferanten, ob ein Facility-Code verlangt wird.
- **Anlagen-Code** – Bestimmt die Ortung des „2N IP“-Geräts im Sicherheitssystem. Geben Sie den dekadischen Lokationswert (0–255) ein.

Konfiguration des OSDP-Moduls

- **Modulbezeichnung** – legt den Modulnamen fest. Der Modulname wird verwendet, wenn Eingang oder Ausgang in den Automatisierungseinstellungen angegeben werden.
- **Gruppe für das Weiterleiten von Zugriffsdaten** – ordnet den OSDP-Ausgang einer Gruppe zu, an die Codes von angeschlossenen Kartenlesern, oder OSDP-Eingänge weitergeleitet werden können.
- **Format der gesendeten Codes** – legt das Format der ausgesendeten Codes fest.
- **OSDP Adresse** – die Adresse des OSDP-Moduls im Bereich 0–126 auf der OSDP-Leitung.
- **Baudrate** – Einstellung der Kommunikationsgeschwindigkeit entsprechend dem angeschlossenen Gerät.
- **Chiffrierschlüssel** – eigener Schlüssel für eine verschlüsselte Kommunikation.
- **Modus** – Für die Ferneinstellung des Verschlüsselungsschlüssels auf dem Peripheriegerät ist es möglich, den Installationsmodus zu verwenden, sofern dies zulässig ist. Nach Erhalt des Verschlüsselungsschlüssels wechselt es automatisch in den normalen Modus. Der Installationsmodus wird durch schnelles Blinken der Signalisierungs-LED am OSDP-Modul signalisiert.

- **Verschlüsselung erzwingen** – Legen Sie die erzwungene Verschlüsselung nur für verschlüsselte Kommunikation fest.

Hinweis

- Erfolgt die Kommunikation auf dem OSDP-Gerät nach dem Setzen der Zwangsverschlüsselung unverschlüsselt, wird diese Kommunikation abgewiesen.

Konfiguration des Moduls der Induktionsschleife

- **Modulbezeichnung** – legt den Modulnamen fest. Die Bezeichnung des Moduls wird beim Loggen der Ereignisse der Induktionsschleife verwendet.
- **Maximale Leistung** – Stellt die maximale Sendeleistung der Antenne der Induktionschleife ein. Eine größere Sendeleistung bedeutet größere Reichweite, jedoch weniger Leistung für die anderen Gerätesfunktionen. Unter normalen Umständen sollte der voreingestellte Wert von 0,25 W ausreichend sein.

Konfiguration des Displaymoduls

- **Modulbezeichnung** – Stellt den Modulnamen ein. Der Modulname wird beim Loggen der Display-Ereignisse verwendet.
- **Tür** – Stellt die Durchgangsrichtung bei Verwendung eines Lesegeräts ein (Kommen, Gehen). Der Parameter Richtung wird durch das Anwesenheitssystem genutzt.
- **Gruppe für die Weiterleitung von Zugangsdaten** - ermöglicht Ihnen das Festlegen einer Gruppe, an die alle empfangenen Benutzerzugangscodes weitergeleitet werden.
- **Format der gesendeten Codes** – Auswahl aus 4bit und 8bit (höhere Zuverlässigkeit) des Formats.

Hinweis

- Ab FW Version 2.27 ist Display nicht unterstützt am Access Unit 1.0.

Konfiguration des Fingerabdrucklesemoduls

- **Modulbezeichnung** – Stellt den Modulnamen ein. Die Bezeichnung des Moduls wird beim Loggen der Ereignisse aus dem Fingerabdruckscanner verwendet.
- **Tür** – Stellt die Durchgangsrichtung bei Verwendung eines Lesegeräts ein (Kommen, Gehen). Der Parameter Richtung wird durch das Anwesenheitssystem genutzt.
- **Zugewiesener Schalter** – Stellt die Nummer des Schalters ein, der nach der Nutzerauthentifizierung mittels dieses Moduls aktiviert wird. Wenn die Option Türschloßschalter eingestellt ist, werden die Authentifizierungsregeln vom Menu Hardware > Türenverwendet.
- **Sunlight Sensitivity Mode** – Durch die Freigabe wird verhindert, dass das Lesegerät bei direkter Sonneneinstrahlung fehlerhaft arbeitet. Um die Einstellungen zu ändern, muss das Gerät neugestartet werden. Dieser Modus kann zu einer verminderten Leseempfindlichkeit führen.

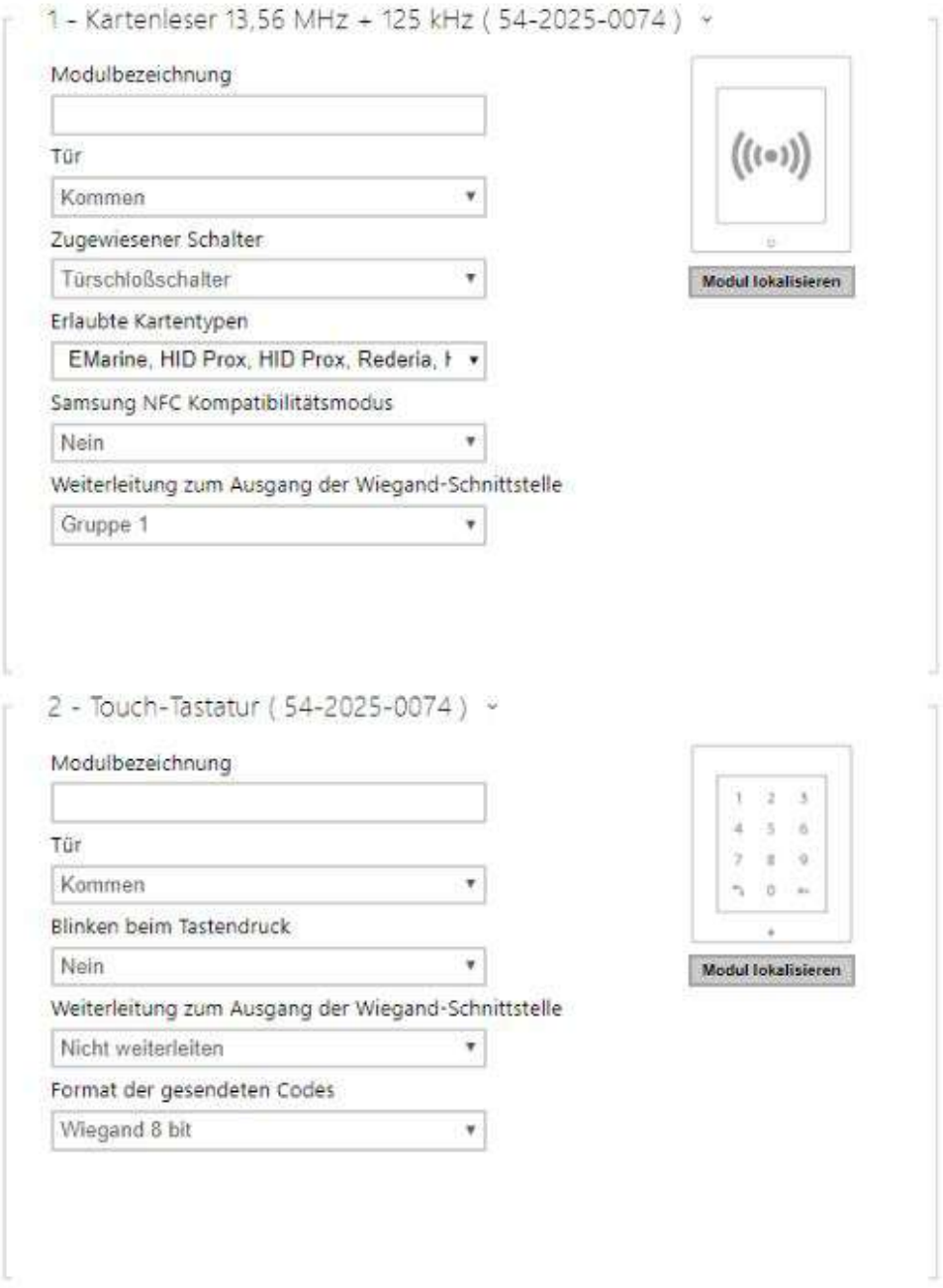
Anmerkung

- Nach Abtrennung des Fingerabdrucklesers wird nach Neustart des Geräts im Benutzerprofil bleibt im Verzeichnis der Teil Benutzerfingerabdrücke (Zahl der Abdrücke des Benutzers im Speicher) verborgen. Nach Wiedereinschalten eines beliebigen Fingerabdrucklesemoduls wird der Teil der Nutzerkonfiguration wieder angezeigt.

Konfiguration des Touchscreen-Moduls

- **Modulbezeichnung** – Stellt den Modulnamen ein. Die Modulbezeichnung wird beim Loggen der Ereignisse vom Touch-Tastatur verwendet.
- **Tür** – Stellt die Durchgangsrichtung bei Verwendung eines Lesegeräts ein (Kommen, Gehen). Der Richtungsparameter findet beim Anwesenheitssystem Anwendung.
- **Blinken beim Tastendruck** – Stellt die Lichtsignalisierung ein, Blinken bestätigt den Tastendruck. Das wird in lärmigen Räumen verwendet, wo Tonsignalisierung nicht deutlich zu hören ist.
- **Weiterleitung zum Ausgang der Wiegand-Schnittstelle** – Stellt die Gruppe der Wiegand-Ausgänge ein, an die alle empfangenen Nutzercodes gesendet werden.
- **Format der gesendeten Codes** – Auswahl aus 4bit und 8bit (höhere Zuverlässigkeit) des Formats.

Konfiguration des Touchscreen-Moduls & des RFID-Lesegeräts 125 kHz, 13.56 MHz, NFC



Kartenleser 13,56 MHz (125 kHz) (Modul-Seriennummer)

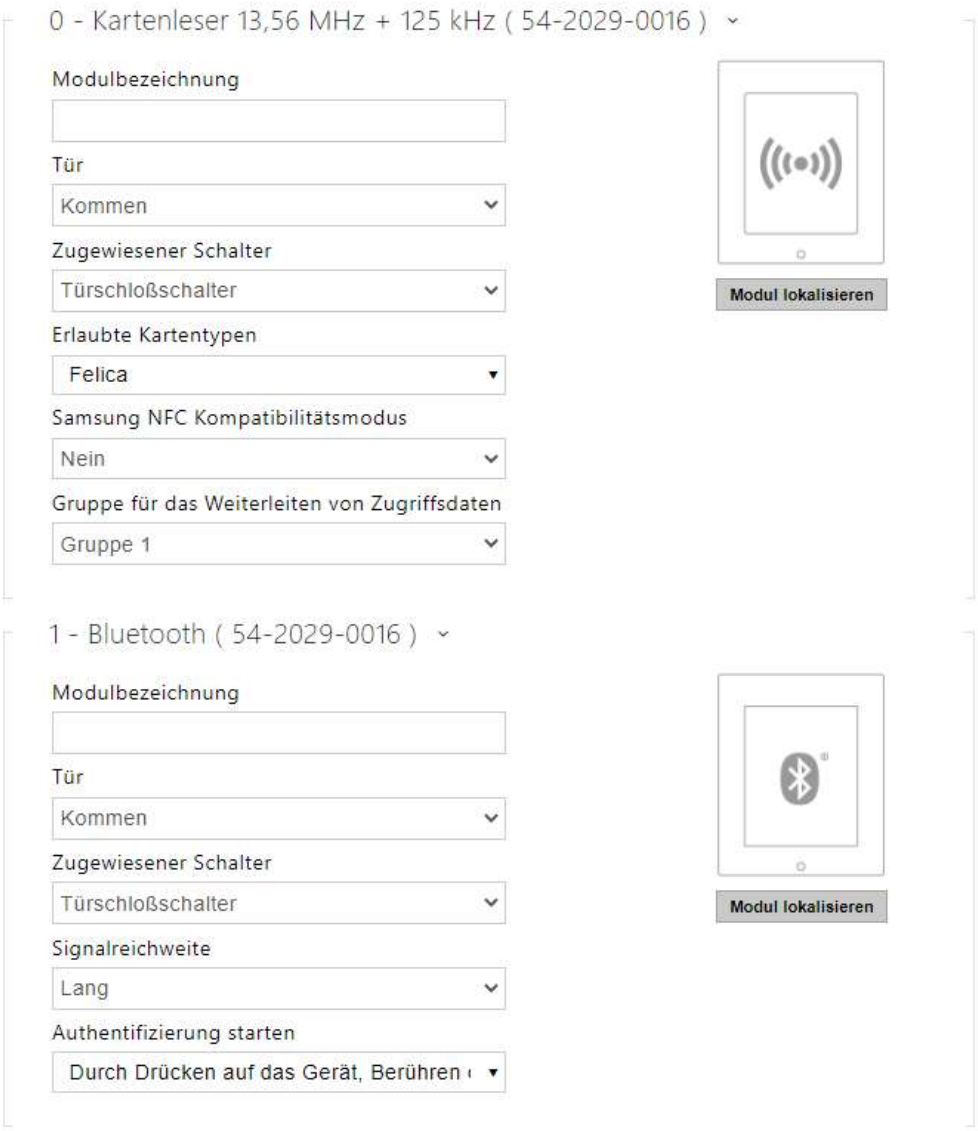
- **Modulbezeichnung** – Stellt den Modulnamen ein. Die Modulbezeichnung wird beim Loggen der Ereignisse vom Modul des Kartenlesers verwendet.

- **Tür** – Stellt die Durchgangsrichtung bei Verwendung eines Lesegeräts ein (Kommen, Gehen). Der Parameter Richtung wird durch das Anwesenheitssystem genutzt.
- **Zugewiesener Schalter** – Stellt die Nummer des Schalters ein, der nach der Nutzerauthentifizierung mittels dieses Moduls aktiviert wird. Wenn die Option Türschloßschalter eingestellt ist, werden die Authentifizierungsregeln vom Menu Hardware > Türenverwendet.
- **Erlaubte Kartentypen** – Damit kann der Typ der Karte eingestellt werden, der durch das Lesegerät akzeptiert wird. Das Lesegerät unterstützt zu einem Zeitpunkt nur einen Kartentyp.
- **Samsung NFC Kompatibilitätsmodus** – Lässt die Samsung NFC Kompatibilitätsmodus zu.
- **Weiterleitung an den Wiegand-Ausgang** – Stellt die Gruppe mit den Wiegand-Ausgängen ein, an welche alle über die RFID-Kartenleser empfangenen ID weitergeleitet werden.

Touchscreen-Display (Seriennummer)

- **Modulbezeichnung** – Stellt den Modulnamen ein. Die Modulbezeichnung wird beim Loggen der Ereignisse vom Touch-Tastatur verwendet.
- **Tür** – Stellt die Durchgangsrichtung bei Verwendung eines Lesegeräts ein (Kommen, Gehen). Der Richtungsparameter findet beim Anwesenheitssystem Anwendung.
- **Blinken beim Tastendruck** – Stellt die Lichtsignalisierung ein, Blinken bestätigt den Tastendruck. Das wird in lärmigen Räumen verwendet, wo Tonsignalisierung nicht deutlich zu hören ist.
- **Weiterleitung zum Ausgang der Wiegand-Schnittstelle** – Stellt die Gruppe der Wiegand-Ausgänge ein, an die alle empfangenen Nutzercodes gesendet werden.
- **Format der gesendeten Codes** – Auswahl aus 4bit und 8bit (höhere Zuverlässigkeit) des Formats.

Konfiguration des Bluetooth-Moduls & des RFID-Lesegeräts 125kHz, 13.56 MHz, NFC



Kartenleser 13,56 MHz (125 kHz)

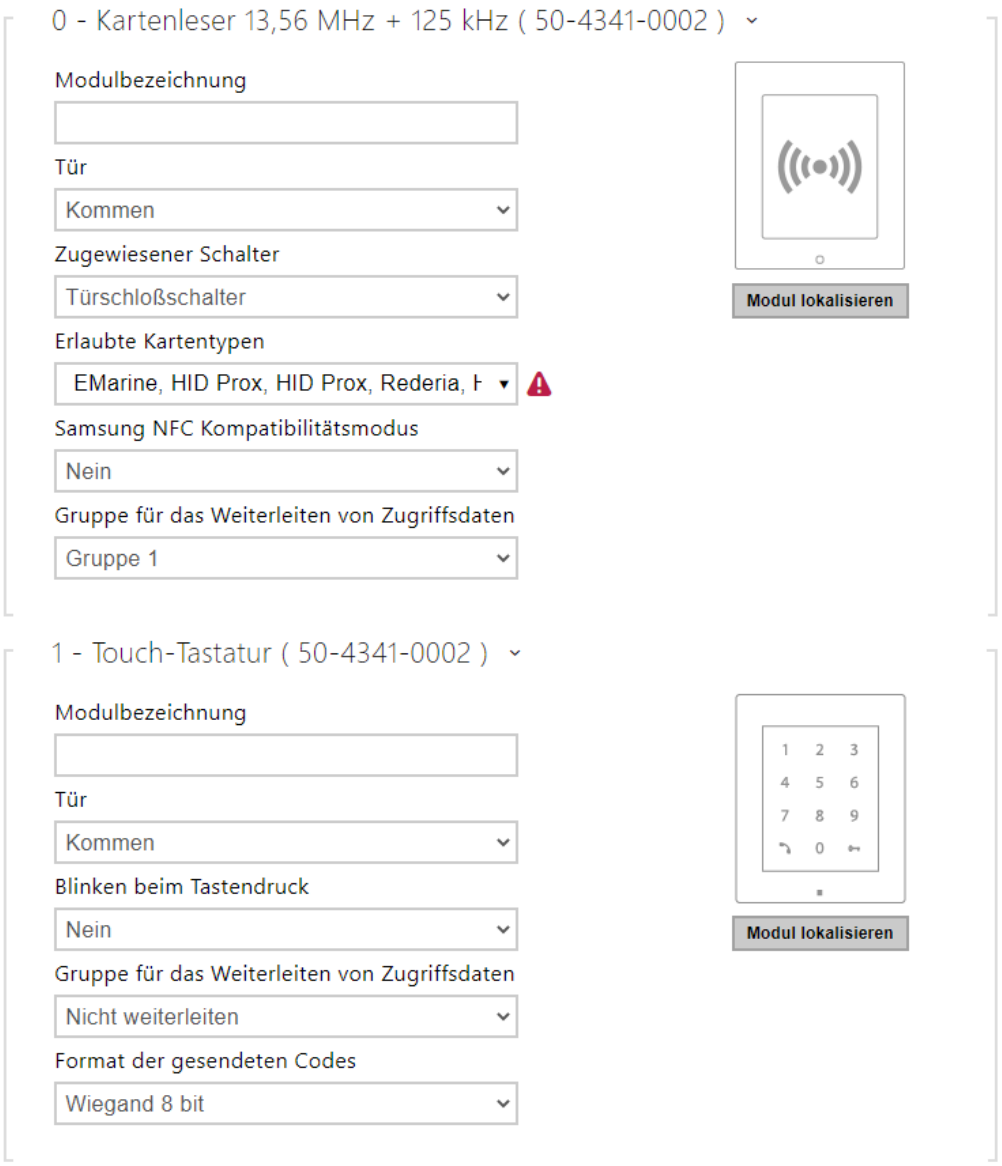
- **Modulbezeichnung** – Stellt den Modulnamen ein. Die Modulbezeichnung wird beim Loggen der Ereignisse vom Modul des Kartenlesers verwendet.
- **Tür** – Stellt die Durchgangsrichtung bei Verwendung eines Lesegeräts ein (Kommen, Gehen). Der Parameter Richtung wird durch das Anwesenheitssystem genutzt.
- **Zugewiesener Schalter** – Stellt die Nummer des Schalters ein, welcher nach der Benutzer-Authentifizierung über dieses Modul aktiviert wurde. Wenn die Option Türschloßschalter eingestellt ist, werden die Authentifizierungsregeln vom Menu Hardware > Türenverwendet.

- **Erlaubte Kartentypen** – Ermöglicht den Typ der Karte einzustellen, welcher durch das Lesegerät akzeptiert wird. Das Lesegerät unterstützt zu einem Zeitpunkt nur einen Kartentyp.
- **Samsung NFC Kompatibilitätsmodus** – Lässt die Samsung NFC Kompatibilitätsmodus zu.
- **Weiterleitung zum Ausgang der Wiegand-Schnittstelle** – Stellt die Gruppe mit den Wiegand-Ausgängen ein, an welche alle über die RFID-Leser erhaltenen ID weitergeleitet werden.

Bluetooth

- **Modulbezeichnung** – stellt den Modulnamen ein. Die Bezeichnung des Moduls wird beim Loggen der Ereignisse aus dem Bluetoothmodul verwendet.
- **Tür** – stellt die Durchgangsrichtung bei Verwendung eines Lesegeräts ein (Kommen, Gehen). Der Richtungsparameter findet beim Anwesenheitssystem Anwendung
- **Zugewiesener Schalter** – stellt die Nummer des Schalters ein, welcher nach der Benutzer-Authentifizierung über dieses Modul aktiviert wurde. Wenn die Option Türschloßschalter eingestellt ist, werden die Authentifizierungsregeln vom Menu Hardware / Türen verwendet.
- **Signalreichweite** – stellt die maximale Reichweite des Signals, d.h. die Entfernung ein, in der das Bluetooth-Modul noch mit dem Mobiltelefon kommunizieren wird:
    - **Kurz** – die Reichweite ist bei den meisten Telefonen geringer als 2 m.
    - **Lang** – die Reichweite ist die maximal mögliche.
- **Authentifizierung starten** – stellt die Authentifizierungsart mittels des Mobiltelefons ein:
    - **Berühren der App** – man muss die Authentifizierung bestätigen, mit dem Antippen der Schaltfläche in der laufenden Applikation im Mobiltelefon
    - **Durch Drücken auf das Gerät** – die Authentifizierung muss durch Berührung auf dem Leser in Anwesenheit des Telefons mit gekoppelten **2N Mobile Key** Applikation bestätigt werden.

Touch-Tastatur-&-Bluetooth-&-RFID-Lesegerät 125 kHz, 13,56 MHz, NFC



Kartenleser 13.56 MHz (125kHz) (Seriennummer)

- **Modulbezeichnung** – stellt den Modulnamen ein. Die Bezeichnung des Moduls wird beim Loggen der Ereignisse aus dem Bluetoothmodul verwendet.
- **Tür** – stellt die Durchgangsrichtung bei Verwendung eines Lesegeräts ein (Kommen, Gehen). Der Parameter Richtung wird durch das Anwesenheitssystem genutzt.
- **Zugewiesener Schalter** – stellt die Nummer des Schalters ein, welcher nach der Benutzer-Authentifizierung über dieses Modul aktiviert wurde. Wenn die Option Türschloßschalter eingestellt ist, werden die Authentifizierungsregeln vom Menu Hardware / Türen verwendet.
- **Erlaubte Kartentypen** – damit kann der Kartentyp eingestellt werden, welcher durch das Lesegerät akzeptiert wird. Das Lesegerät unterstützt zu einem Zeitpunkt nur einen Kartentyp.
- **Samsung NFC Kompatibilitätsmodus** – lässt die NFC-Kompatibilität mit Samsung-Telefonen zu.
- **Gruppe für die Weiterleitung von Zugangsdaten** - ermöglicht Ihnen das Festlegen einer Gruppe, an die alle empfangenen Benutzerzugangscodes weitergeleitet werden.

Touch-Tastatur (Seriennummer)

- **Modulbezeichnung** – stellt den Modulnamen ein. Die Bezeichnung des Moduls wird beim Loggen der Ereignisse aus dem Bluetoothmodul verwendet.
- **Tür** – stellt die Durchgangsrichtung bei Verwendung eines Lesegeräts ein (Kommen, Gehen). Der Richtungsparameter findet beim Anwesenheitssystem Anwendung
- **Blinken beim Tastendruck** – stellt die Lichtsignalisierung ein, Blinken bestätigt den Tastendruck. Das wird in lärmigen Räumen verwendet, wo Tonsignalisierung nicht deutlich zu hören ist.
- **Gruppe für die Weiterleitung von Zugangsdaten** - ermöglicht Ihnen das Festlegen einer Gruppe, an die alle empfangenen Benutzerzugangscodes weitergeleitet werden.
- **Format der gesendeten Codes** – Auswahl aus 4bit und 8bit (höhere Zuverlässigkeit) des Formats.

Bluetooth

- **Modulbezeichnung** – stellt den Modulnamen ein. Die Bezeichnung des Moduls wird beim Loggen der Ereignisse aus dem Bluetoothmodul verwendet.
- **Tür** – stellt die Durchgangsrichtung bei Verwendung eines Lesegeräts ein (Kommen, Gehen). Der Richtungsparameter findet beim Anwesenheitssystem Anwendung
- **Zugewiesener Schalter** – stellt die Nummer des Schalters ein, welcher nach der Benutzer-Authentifizierung über dieses Modul aktiviert wurde. Wenn die Option Türschloßschalter eingestellt ist, werden die Authentifizierungsregeln vom Menu Hardware / Türen verwendet.
- **Signalreichweite** – stellt die maximale Reichweite des Signals, d.h. die Entfernung ein, in der das Bluetooth-Modul noch mit dem Mobiltelefon kommunizieren wird:
  - **Kurz** – die Reichweite ist bei den meisten Telefonen geringer als 2 m.
  - **Lang** – die Reichweite ist die maximal mögliche.
- **Authentifizierung starten** – stellt die Authentifizierungsart mittels des Mobiltelefons ein. Eins, eine Kombination aus zwei oder allen dreien.
  - **Berühren der App** – man muss die Authentifizierung bestätigen, mit dem Antippen der Schaltfläche in der laufenden Applikation im Mobiltelefon
  - **Durch Drücken auf das Gerät** – die Authentifizierung muss durch Berührung auf dem Leser in Anwesenheit des Telefons mit gekoppelten **2N Mobile Key** Applikation bestätigt werden.

Hinweis

- Nach Ersetzen der Module müssen die neuen Module wieder konfiguriert werden. Die Konfiguration ist mit Seriennummer verknüpft.

5.3.9 Aufzugsteuerung

Durch den Anschluss des Relaismoduls AXIS A9188 an das Gerät kann der Zugang zu einzelnen Etagen eines Gebäudes über den Aufzug gesteuert werden. Es können maximal 5 dieser Relaismodule an ein Gerät angeschlossen werden, wobei jedes Modul 8 Etagen steuert, also insgesamt 64 Etagen.

Registerkarte Relaismodule

- **Dauer des Einschaltens** – Stellt die Schaltzeit des Relaismoduls ein (Bereich 1–600 s).

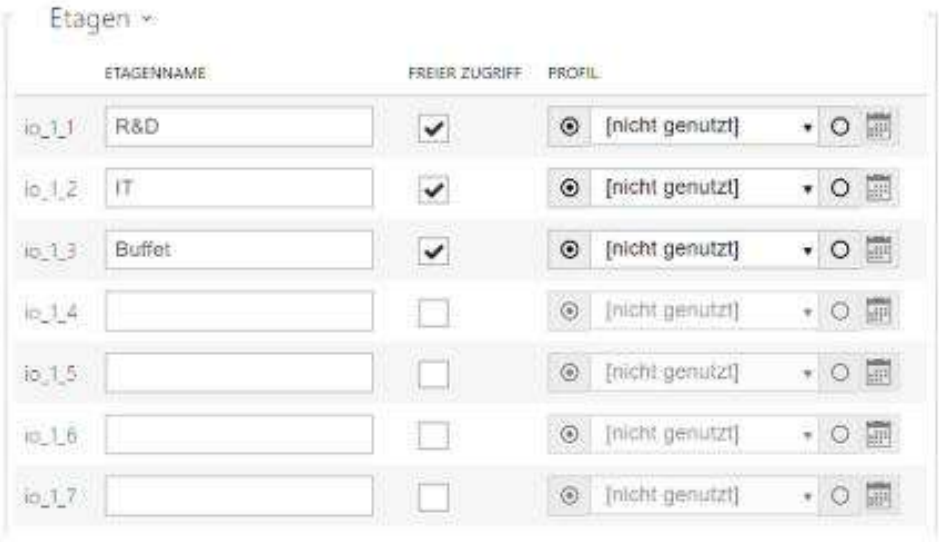
- **Aktiviert** – Dient zur Aktivierung und Deaktivierung des Moduls AXIS A9188, das zur Aufzugsteuerung bis auf 8 Etagen dient.
- **IP-Adresse** – IP-Adresse des AXIS A9188.
- **Status** – Zeigt den Zustand des angeschlossenen Moduls AXIS A9188 an (Fehler/Zutritt verweigert/Bereit/Angehalten).
- **Seriennummer** – Seriennummer des Moduls AXIS A9188.

- **Benutzername** – Nutzername für die Authentifizierung des Anschlusses an ein externes Gerät . Der Parameter ist nur dann verbindlich, wenn das externe Gerät eine Authentifizierung verlangt.
- **Passwort** – Passwort zur Authentifizierung des Anschlusses an einem externen Gerät (WEB-Relais, usw.). Der Parameter ist nur dann verbindlich, wenn das externe Gerät eine Authentifizierung verlangt.

Hinweis

- Authentifizierung erfolgt für alle Module mit gleichem Benutzernamen und Passwort.

Registerkarte Etagen



- **Etagenname** – Stellt den Namen der Etage ein.
- **Freier Zugriff** – Aktiviert freien Zutritt auf die Etage ohne jede Authentifizierung.
- **Profil** – Bietet die Auswahl eines oder mehrerer Zeitprofile gleichzeitig an, die angewendet werden. Die Einstellung der Zeitprofile selbst ist im Abschnitt Verzeichnis > Zeitprofile möglich.
  -  Mit der Markierung wird die Auswahl aus vordefinierten Profilen oder die manuelle Einstellung des Zeitprofils für das jeweilige Element eingestellt.
  -  Mit der Markierung wird das Zeitprofil direkt für das jeweilige Element eingestellt.

Tipp

Generierung des Zertifikats für das Relaismodul AXIS A9188

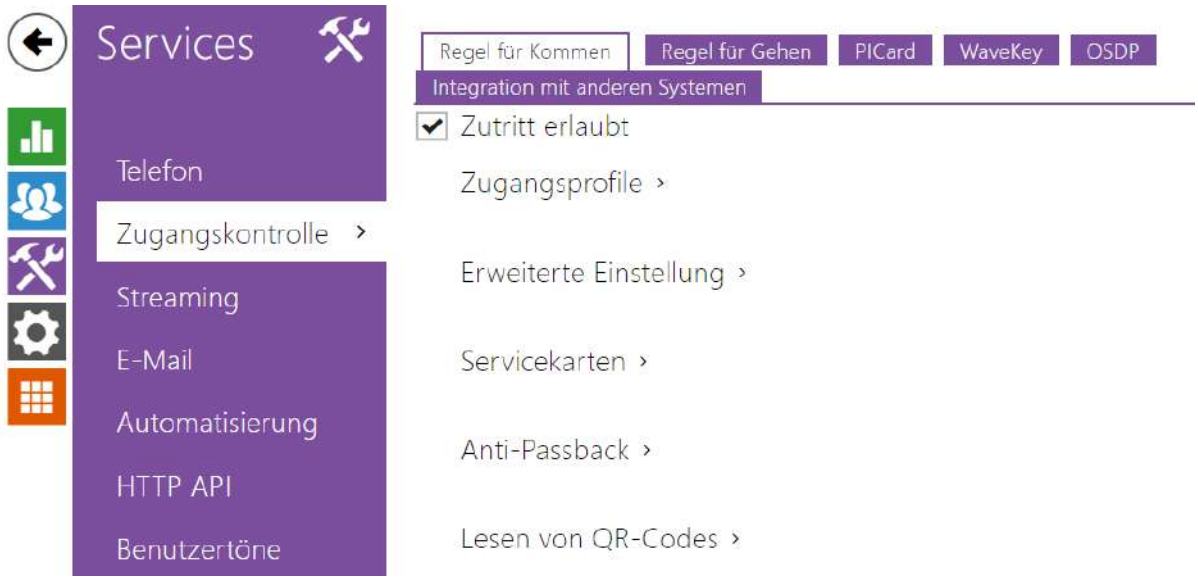
1. Suchen Sie das Relaismodul AXIS A9188 im Lokalnetz mittels AXIS IP Utility.
2. Geben Sie die root/root Anmeldedaten ein.
3. Im Menü wählen Sie Preferences > Additional device configuration.
4. Ein neues Fenster mit Gerätekonfiguration wird angezeigt.
5. Im Menü wählen Sie System Options > Security > Certificates.
6. Erstellen Sie das Zertifikat durch Anklicken Create self-signed certificate.
7. Füllen Sie alle geforderten Felder aus und bestätigen Sie mit OK-Taste.
8. Gehen Sie ins Menu System Options > Security > HTTPS über.
9. Wählen Sie das Zertifikat im Rollmenü aus and speichern Sie es durch Drücken der SAVE-Taste.
10. Gehen Sie in die Webschnittstelle das Gerätes über, Konfigurierung Hardware > Aufzugsteuerung. Geben Sie die Anmeldeangaben ein und füllen Sie die IP-Adresse des Relaismoduls aus.
11. Nach erfolgreichem Anknüpfen der Verbindung wird am Relaismodul READY angezeigt.

5.4 Services

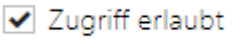
Hier ist eine Übersicht dessen, was Sie in dem Kapitel finden:

5.4.1 Zugangskontrolle

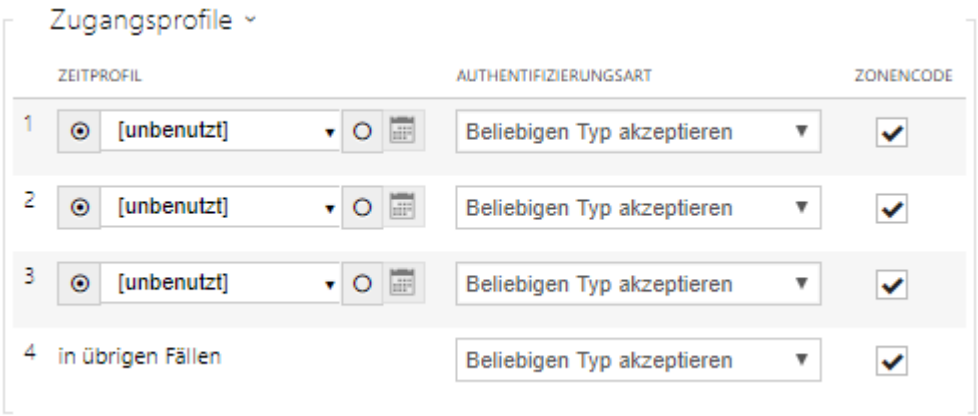
Der Zugangskontrolldienst dient der Verwaltung des Zugangs und der Überprüfung der Benutzerauthentifizierung.



Registerkarte Regeln für das Kommen



- **Zugriff erlaubt** – erlaubt den beliebigen Zutritt von der konkreten Türseite (Kommen, Gehen). Wenn der Zutritt nicht erlaubt ist, kann man die Tür von dieser Seite nicht öffnen.

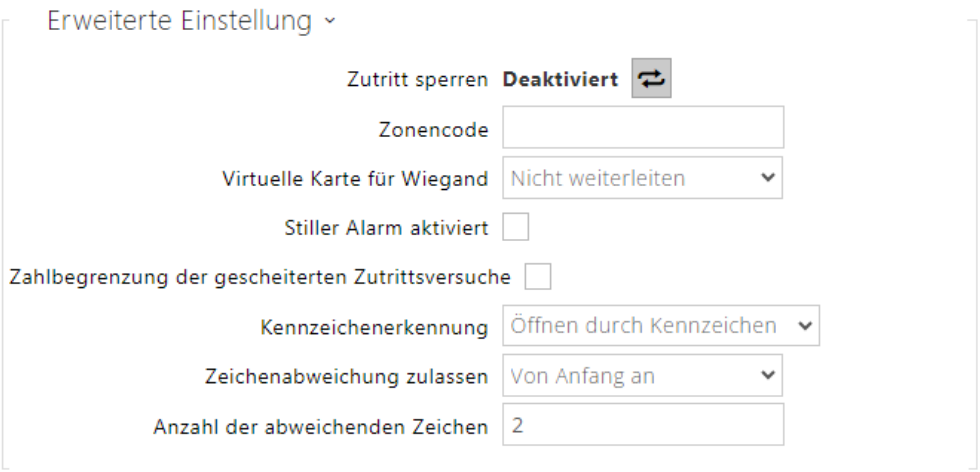


- **Zeitprofil** – bietet die Auswahl eines oder mehrerer Zeitprofile gleichzeitig an, die angewendet werden. Die Einstellung der Zeitprofile selbst ist im Abschnitt Verzeichnis > Zeitprofile möglich.
  -  wählen Sie globale Profile aus Verzeichnis > Zeitprofile.
  -  profil temporel individuel pour cet élément particulier.
- **Authentifizierungsart** – zeigt die Authentifizierungsart (Bluetooth, Fingerabdruck, Zutrittskarte, nummerischer Code oder QR-Code) in der Zeit der Gültigkeit des Zeitprofils

in dieser Zeile einschließlich der Möglichkeit der mehrfachen Authentifizierung wegen erhöhter Sicherheit an. Mittels der Möglichkeit ´Zutritt abgelehnt´ kann man den Zutritt ganz verweigern.
- **Zonencode** – erlaubt den Zonencode für die Kombination des Zeitprofils und der Authentifizierungsart in dieser Zeile. Der Benutzer kann dann den Zonencode anstelle des PIN-Codes verwenden.

Hinweis

- Falls kein Zeitprofil eingestellt ist, wird auf der jeweiligen Zeile die Authentifizierungsart ignoriert.



- **Zutritt sperren** – zeigt die aktuelle Einstellung der zutritt sperren an. Aktiviert/ Deaktiviert.
- **Zonencode** – ermöglicht den numerischen Schaltercode einzugeben. Der Code muss mindestens zwei Zeichen haben, wir empfehlen jedoch mindestens vier Zeichen zu verwenden.
- **Virtuelle Karten für Wiegand** – ermöglicht den Wiegand-Ausgang zu wählen, auf den die Nummer der virtuellen Karte des Nutzers nach seiner erfolgreichen Authentifizierung geschickt wird. Verwendbar mit beliebiger Authentifizierungsart einschließlich Codes, Fingerabdrücke u.Ä.
- **Stiller Alarm aktiviert** – jedem Zutrittscode ist ein virtueller Code zugewiesen, der um eine Eins höher ist und für die Aktivierung des SilentAlarms bestimmt ist. Zum Beispiel, wenn wird den Zutrittscode 0000 haben, dann ist der Code für die Aktivierung des SilentAlarms 0001. Die Codelänge muss gleich bleiben, d.h. also z.B. dass für Zutrittscode 9999 der SilentAlarm 0000 ist u.Ä. Die durchgeführte Aktion für den SilentAlarm kann man im Abschnitt für die Automatisierung einstellen.

Hinweis

- Wenn der Benutzer die Authentifizierung zum Auslösen des stillen Alarms verwendet und kein stiller Alarm zulässig ist, wird dessen Zugang verweigert und es wird kein Alarm ausgelöst.

- **Zahlbegrenzung der gescheiterten Zutrittsversuche** – erlaubt die Einschränkung der Zahl der erfolglosen Authentifizierungsversuche. Nach fünf erfolglosen Zutrittsversuchen (falscher numerischer Code, ungültige Karte, usw.) bleibt die 2N Zutrittseinheiten können für 30 Sekunden gesperrt, auch im Fall, dass die uthentifizierung gültig war.
- **Kennzeichenerkennung** – Wählt das Szenario nach dem Erkennen des Fahrzeugkennzeichens aus.

Hinweis

- Für eine korrekte Funktion ist es ratsam, dass jedes Kennzeichen genau einem Eintrag im Verzeichnis zugeordnet ist.Bei mehreren Eintragungen eines Kennzeichens ist es nicht möglich, einen Eintrag in dem Verzeichnis, in dem die Kennzeichen konfiguriert sind, eindeutig zuzuweisen (der erste Eintrag, für den das angegebene Kennzeichen konfiguriert ist, wird ausgewählt und seine Zutrittsregeln werden angewendet).

- **Deaktiviert**
- **Öffnen durch Kennzeichen** – Die Tür wird geöffnet, wenn der Eintrag im Verzeichnis mit dem eingetragenen Kennzeichen derzeit das Recht hat, ein- und auszutreten. Das Öffnen einer Tür (oder einer Schranke usw.) nach dem Erkennen eines gültigen Kennzeichens funktioniert **unabhängig** von den anderen Authentifizierungsmethoden, die in den Zutrittsprofilen festgelegt sind.
- **Multifaktor mit Kennzeichen** – iese Option ist nur verfügbar, wenn die Beta-Funktion aktiviert ist Multifaktor-Überprüfung von Kennzeichen. Schaltet die permanente Zugriffssperre ein und deaktiviert dauerhaft die Bluetooth-Authentifizierungsmethode (WaveKey). Sobald das Kennzeichen geladen ist, wird dem Benutzer mit dem geladenen Kennzeichen eine vorübergehende Ausnahme von 60 Sekunden gewährt, und die WaveKey-Funktion wird für diese Zeit aktiviert. Der Zugriff wird nur einem Benutzer mit geladenem Kennzeichen gewährt, der sich innerhalb von 60 Sekunden mit einer anderen Authentifizierungsmethode (WaveKey/QR-Code) authentifiziert. Nutzer mit einer dauerhaften Ausnahme sind für die gesamte Dauer der dauerhaften Zugriffssperre zugangsberechtigt, können sich aber nur innerhalb von 60 Sekunden nach Aufzeichnung des Kennzeichens auch mit dem WaveKey authentifizieren.
  Jedes weitere zugelassene Kfz-Kennzeichen hebt die vorherige vorübergehende Ausnahme auf, und wenn es einen Benutzer mit einem neu zugelassenen Kennzeichen gibt, wird diesem Benutzer eine vorübergehende Ausnahme zugewiesen.

- **Zeichenabweichung tolerieren** – wählt aus, ob eine Abweichung im erkannten Kfz-Kennzeichen toleriert wird.. Es ist möglich, zwischen Nulltoleranz, Toleranz vom Anfang, Toleranz vom Ende oder Toleranz sowohl vom Anfang als auch vom Ende an zu wählen. Bei der Auswahl der beidseitigen Zeichentoleranz wird beim Lesen des Kennzeichens zunächst die Zeichenabweichung vom Anfang toleriert, und wenn das Kennzeichen nicht erkannt wird, wird beim nächsten Lesen die Abweichung vom Ende toleriert.
- **Anzahl der Zeichenabweichungen -** wählt aus, ob eine Abweichung von einem oder zwei Zeichen toleriert wird. Die Zeichenabweichung gilt für den Anfang und/oder das Ende entsprechend der Einstellung des Parameters „Zeichenabweichung tolerieren“. Das Gerät toleriert beim ersten Lesen des Kennzeichens keine Abweichung. Nur wenn es das im Verzeichnis gespeicherte Kennzeichen nicht erkennt, toleriert es beim nächsten Laden eine einstellige Abweichung in den oben eingestellten Richtungen. Wenn das Gerät das Nummernschild dennoch nicht aus dem Verzeichnis erkennt, toleriert es beim nächsten Lesen eine Abweichung von zwei Zeichen.

Mit dem Gerät können erkannte Fahrzeugkennzeichen, die in einer HTTP-Anfrage von Kameras von der Firma AXIS gesendet wurden und die mit einer zusätzlichen VaxALPR-Applikation auf api/lpr/licenseplate ausgestattet sind, genutzt werden (weitere Informationen finden Sie im HTTP-API-Handbuch für IP-Sprechanlagen).

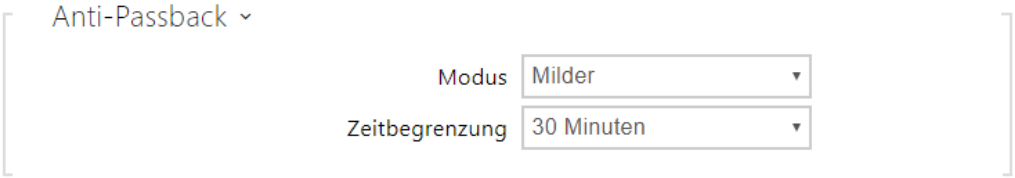
Wenn die Funktion aktiviert ist, wird das Ereignis nach Erhalt einer gültigen HTTP-Anfrage im Verlauf unter dem Ereignis LicensePlateRecognized aufgezeichnet. Wenn ein Bild als Teil der HTTP-Anfrage gesendet wird (z. B. ein Abschnitt des Fotos oder das gesamte Foto der Szene bei der Kennzeichenerkennung), wird es gespeichert. Die letzten fünf Fotos werden im Gerätespeicher gespeichert, der über eine an api/lpr/image gesendete HTTP-Anfrage vom Gerät gelesen werden kann und im **2N Access Commander** System verfügbar ist.

Warnung

- Durch das Zurücksetzen der Werkseinstellungen auf die Werkseinstellungen oder das Hochladen einer anderen Konfiguration werden die Einstellungen für die Zugriffssperre nicht geändert. Nur ein Hardware-Reset über die Reset-Taste am Gerät setzt den Parameter auf die Werkseinstellungen zurück.
  - Das Sicherheitsrelais erhöht die Sicherheit der Installation gegen Missbrauch durch einen Hardware-Reset.

Für die Verwaltung der Benutzerkarten dienen sog. Zusatz- und Lösch-Karten. Durch Anlegen der Zusatz-Karte an den Leser wird jede nachfolgend angelegte Karte als neuer Benutzer mit zugeordneter Zutrittskarte in die Liste im Verzeichnis hinzugefügt. In der Anlage wird automatisch ein neuer Benutzer der !Visitor #ID_Karte erstellt. Durch Anlegen der Lösch-Karte an den Leser wird jede nachfolgend angelegte Karte und sein Benutzer von der Liste im Verzeichnis gelöscht.

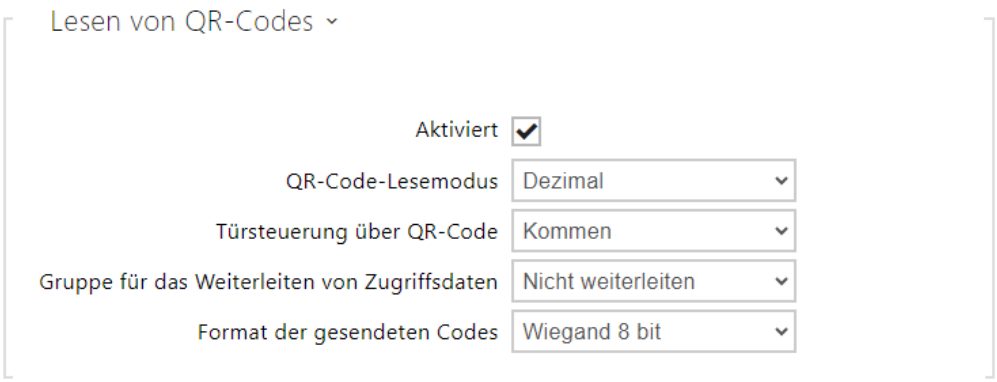
- **Plus Karten-ID** – ID der Servicekarte, die für das Hinzufügen in die Liste der installierten Karten bestimmt ist. Die Karten-ID ist die Sequenz von 6–32 Zeichen aus der Menge 0–9, A–F.
- **Minus Karten-ID** – ID der Servicekarte, die für das Entfernen von der Liste der installierten Karten bestimmt ist. Die Karten-ID ist die Sequenz von 6–32 Zeichen aus der Menge 0–9, A–F.



Anti-Passback ist eine Sicherungsfunktion, die die Benutzung der Zutrittskarte oder einer anderen Authentifizierung zum Eingang in einen Bereich zum zweiten Mal verhindert, ohne dass der Nutzer ihn vorher verlässt (somit kann die Karte keiner zweiten Personen übergeben werden, die eintreten will).

- **Modus** – wählt den Modus der Funktion Anti-Passback:

  - **Deaktiviert** – die Funktion ist defaultmäßig ausgeschaltet, der Nutzer darf die Zutrittskarte oder eine andere Authentifizierung für den Zutritt zum Eingang in einen Bereich zum zweiten Mal benutzen, ohne dass er ihn vorher verlässt.
  - **Milder** – der Nutzer darf die Zutrittskarte oder eine andere Authentifizierung für den Zutritt zum Eingang in einen Bereich zum zweiten Mal benutzen, ohne dass er ihn vorher verlässt. Im Bereich Status > Events wird ein neuer **UserAuthenticated** -Record mit dem Parameter *apbBroken*=***true*** erstellt.
  - **Strenger** – der Nutzer darf die Zutrittskarte oder eine andere Authentifizierung nicht zum zweiten Mal für den Zutritt zum Eingang in einen Bereich benutzen, ohne dass er ihn vorher verlässt. Im Bereich Status > Events wird ein neuer **UserRejected**-Record mit dem Parameter *apbBroken*=***true*** erstellt.
- **Zeitbegrenzung** – wählt die Zeit der Zutrittseinschränkung für die Funktion Anti-Passback. Man kann sie nach dem letzten Zutritt mit der jeweiligen Authentifizierung (Karte, Code usw.) während der gewählten Zeit nicht wieder in der gleichen Richtung verwenden.

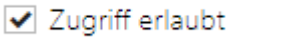


- **Aktiviert** – aktiviert/deaktiviert das Lesen von QR-Codes mit der Gerätekamera. Wenn das Lesen von QR-Codes aktiviert ist, können PIN-Codes und einzelne Schaltcodes, die mehr als zehn Ziffern haben, eingegeben werden, indem der QR-Code auf die Gerätekamera gerichtet wird.
- **QR Code Reading Mode** – Das Gerät speichert immer Dezimalcodes. Im Dezimalmodus müssen die gescannten Codes den im Gerät gespeicherten Codes mit 4 bis 15 Ziffern entsprechen. Im Hexadezimalmodus werden die Codes nach dem Scannen in Dezimal umgewandelt und mit den gespeicherten Dezimalcodes verglichen, wobei führende Nullen ignoriert werden. Akzeptierter hexadezimaler Bereich: 1000 bis FFFFFFFF.
- **Betätigung der Tür mithilfe eines QR-Codes** – Aktiviert oder deaktiviert die Türbetätigung durch Einlesen eines QR-Codes.
- **Gruppe für die Weiterleitung von Zugangsdaten** - ermöglicht Ihnen das Festlegen einer Gruppe, an die alle empfangenen Benutzerzugangscodes weitergeleitet werden.
- **Format der gesendeten Codes** – Auswahl aus 4bit und 8bit (höhere Zuverlässigkeit) des Formats.

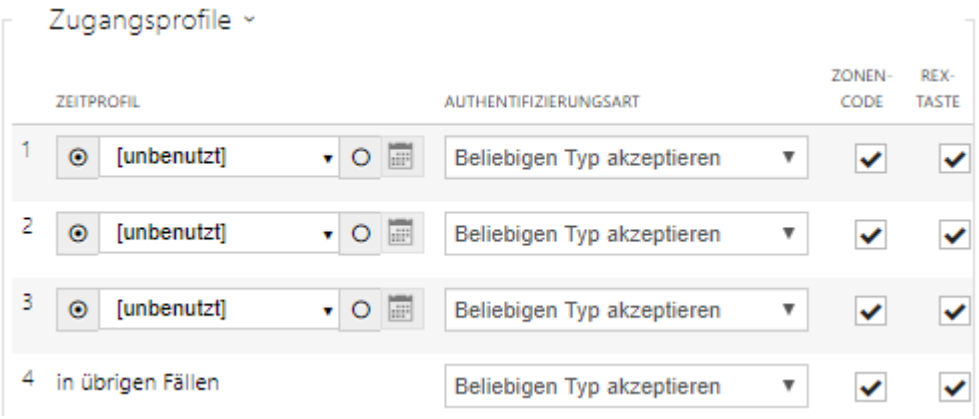
Hinweis

- Für den korrekten Betrieb des Lesens von QR-Codes verwenden Sie nicht gleichzeitig die Datenschutzfunktion.
- Für zusätzliche Sicherheit begrenzen Sie die Anzahl der fehlgeschlagenen Zugriffe im obigen Block Erweiterte Einstellungen.
- Die QR-Code-Lesefunktion ist nur bei Modellen mit Axis ARTPEC-7-Prozessor verfügbar.

Registerkarte Regeln für Gehen



- **Zugriff erlaubt** – erlaubt den beliebigen Zutritt von der konkreten Türseite (Kommen, Gehen). Wenn der Zutritt nicht erlaubt ist, kann man die Tür von dieser Seite nicht öffnen.

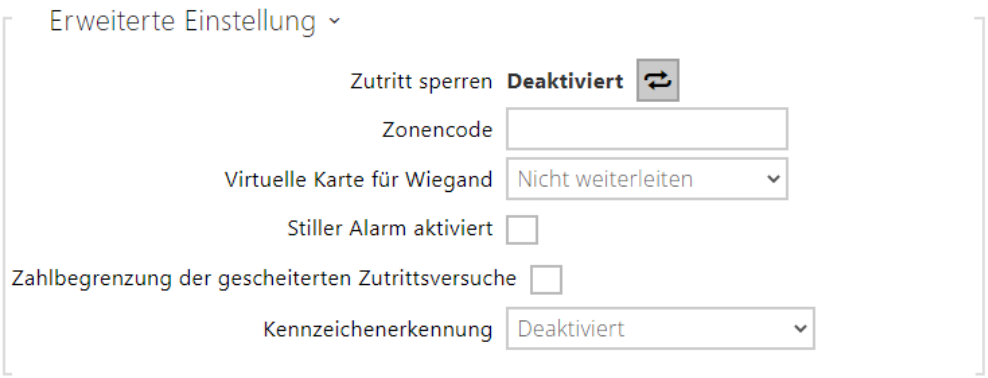


- **Zeitprofil** – bietet die Auswahl eines oder mehrerer Zeitprofile gleichzeitig an, die angewendet werden. Die Einstellung der Zeitprofile selbst ist im Abschnitt Verzeichnis > Zeitprofile möglich.
  -  Mit der Markierung wird die Auswahl aus vordefinierten Profilen oder die manuelle Einstellung des Zeitprofils für das jeweilige Element eingestellt.
- **Authentifizierungsart** – zeigt die Authentifizierungsart (Bluetooth, Fingerabdruck, Zutrittskarte, nummerischer Code) in der Zeit der Gültigkeit des Zeitprofils in dieser Zeile einschließlich der Möglichkeit der mehrfachen Authentifizierung wegen erhöhter Sicherheit an. Mittels der Möglichkeit ´Zutritt abgelehnt´ kann man den Zutritt ganz verweigern.
- **Zonencode**– erlaubt den Zonencode für die Kombination des Zeitprofils und der Authentifizierungsart in dieser Zeile. Der Benutzer kann dann den Zonencode anstelle des PIN-Codes verwenden.

- **REX-Taste** –erlaubt die Funktion der Abgangstaste für das jeweiligen Zeitprofil. Der Eingang, der der Abgangstaste zugeordnet ist, wird im Abschnitt Hardware > Türen, Registerkarte Türen eingestellt.

Hinweis

- Falls kein Zeitprofil eingestellt ist, wird auf der jeweiligen Zeile die Authentifizierungsart ignoriert.



- **Zutritt sperren** – zeigt die aktuelle Einstellung der zutritt sperren an. Aktiviert/ Deaktiviert.
- **Zonencode** – ermöglicht den numerischen Schaltercode einzugeben. Der Code muss mindestens zwei Zeichen haben, wir empfehlen jedoch mindestens vier Zeichen zu verwenden.
- **Virtuelle Karten für Wiegand** – ermöglicht den Wiegand-Ausgang zu wählen, auf den die Nummer der virtuellen Karte des Nutzers nach seiner erfolgreichen Authentifizierung geschickt wird. Verwendbar mit beliebiger Authentifizierungsart einschließlich Codes, Fingerabdrücke u.Ä.
- **Stiller Alarm aktiviert** – jedem Zutrittscode ist ein virtueller Code zugewiesen, der um eine Eins höher ist und für die Aktivierung des SilentAlarms bestimmt ist. Zum Beispiel, wenn wird den Zutrittscode 0000 haben, dann ist der Code für die Aktivierung des SilentAlarms 0001. Die Codelänge muss gleich bleiben, d.h. also z.B. dass für Zutrittscode 9999 der SilentAlarm 0000 ist u.Ä. Die durchgeführte Aktion für den SilentAlarm kann man im Abschnitt für die Automatisierung einstellen.

Hinweis

- Wenn der Benutzer die Authentifizierung zum Auslösen des stillen Alarms verwendet und kein stiller Alarm zulässig ist, wird dessen Zugang verweigert und es wird kein Alarm ausgelöst.

- **Zahlbegrenzung der gescheiterten Zutrittsversuche** – erlaubt die Einschränkung der Zahl der erfolglosen Authentifizierungsversuche. Nach fünf erfolglosen Zutrittsversuchen (falscher numerischer Code, ungültige Karte, usw.) bleibt die 2N Zutrittseinheiten können

für 30 Sekunden gesperrt, auch im Fall, dass die Authentifizierung gültig war.

- **Kennzeichenerkennung** – Wählt das Szenario nach dem Erkennen des Fahrzeugkennzeichens aus.

> ⚠ **Hinweis**
>
> - Für eine korrekte Funktion ist es ratsam, dass jedes Kennzeichen genau einem Eintrag im Verzeichnis zugeordnet ist.Bei mehreren Eintragungen eines Kennzeichens ist es nicht möglich, einen Eintrag in dem Verzeichnis, in dem die Kennzeichen konfiguriert sind, eindeutig zuzuweisen (der erste Eintrag, für den das angegebene Kennzeichen konfiguriert ist, wird ausgewählt und seine Zutrittsregeln werden angewendet).

  - **Deaktiviert**
  - **Öffnen durch Kennzeichen** – Die Tür wird geöffnet, wenn der Eintrag im Verzeichnis mit dem eingetragenen Kennzeichen derzeit das Recht hat, ein- und auszutreten. Das Öffnen einer Tür (oder einer Schranke usw.) nach dem Erkennen eines gültigen Kennzeichens funktioniert **unabhängig** von den anderen Authentifizierungsmethoden, die in den Zutrittsprofilen festgelegt sind.
  - **Multifaktor mit Kennzeichen** – iese Option ist nur verfügbar, wenn die Beta-Funktion aktiviert ist Multifaktor-Überprüfung von Kennzeichen. Schaltet die permanente Zugriffssperre ein und deaktiviert dauerhaft die Bluetooth-Authentifizierungsmethode (WaveKey). Sobald das Kennzeichen geladen ist, wird dem Benutzer mit dem geladenen Kennzeichen eine vorübergehende Ausnahme von 60 Sekunden gewährt, und die WaveKey-Funktion wird für diese Zeit aktiviert. Der Zugriff wird nur einem Benutzer mit geladenem Kennzeichen gewährt, der sich innerhalb von 60 Sekunden mit einer anderen Authentifizierungsmethode (WaveKey/QR-Code) authentifiziert. Nutzer mit einer dauerhaften Ausnahme sind für die gesamte Dauer der dauerhaften Zugriffssperre zugangsberechtigt, können sich aber nur innerhalb von 60 Sekunden nach Aufzeichnung des Kennzeichens auch mit dem WaveKey authentifizieren.
    Jedes weitere zugelassene Kfz-Kennzeichen hebt die vorherige vorübergehende Ausnahme auf, und wenn es einen Benutzer mit einem neu zugelassenen Kennzeichen gibt, wird diesem Benutzer eine vorübergehende Ausnahme zugewiesen.

Mit dem Gerät können erkannte Fahrzeugkennzeichen, die in einer HTTP-Anfrage von Kameras von der Firma AXIS gesendet wurden und die mit einer zusätzlichen VaxALPR-Applikation auf api/lpr/licenseplate ausgestattet sind, genutzt werden (weitere Informationen finden Sie im HTTP-API-Handbuch für IP-Sprechanlagen).

Wenn die Funktion aktiviert ist, wird das Ereignis nach Erhalt einer gültigen HTTP-Anfrage im Verlauf unter dem Ereignis LicensePlateRecognized aufgezeichnet. Wenn ein Bild als Teil der HTTP-Anfrage gesendet wird (z. B. ein Abschnitt des Fotos oder das gesamte Foto der Szene bei der Kennzeichenerkennung), wird es gespeichert. Die letzten fünf Fotos werden im

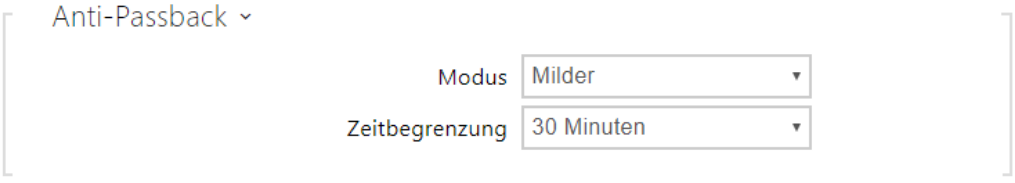
Gerätespeicher gespeichert, der über eine an api/lpr/image gesendete HTTP-Anfrage vom Gerät gelesen werden kann und im **2N Access Commander** System verfügbar ist.

Warnung

- Durch das Zurücksetzen der Werkseinstellungen auf die Werkseinstellungen oder das Hochladen einer anderen Konfiguration werden die Einstellungen für die Zugriffssperre nicht geändert. Nur ein Hardware-Reset über die Reset-Taste am Gerät setzt den Parameter auf die Werkseinstellungen zurück.
  - Das Sicherheitsrelais erhöht die Sicherheit der Installation gegen Missbrauch durch einen Hardware-Reset.

Für die Verwaltung der Benutzerkarten dienen sog. Zusatz- und Lösch-Karten. Durch Anlegen der Zusatz-Karte an den Leser wird jede nachfolgend angelegte Karte als neuer Benutzer mit zugeordneter Zutrittskarte in die Liste im Verzeichnis hinzugefügt. In der Anlage wird automatisch ein neuer Benutzer der !Visitor #ID_Karte erstellt. Durch Anlegen der Lösch-Karte an den Leser wird jede nachfolgend angelegte Karte und sein Benutzer von der Liste im Verzeichnis gelöscht.

- **Plus Karten-ID** – ID der Servicekarte, die für das Hinzufügen in die Liste der installierten Karten bestimmt ist. Die Karten-ID ist die Sequenz von 6–32 Zeichen aus der Menge 0–9, A–F.
- **Minus Karten-ID** – ID der Servicekarte, die für das Entfernen von der Liste der installierten Karten bestimmt ist. Die Karten-ID ist die Sequenz von 6–32 Zeichen aus der Menge 0–9, A–F.



Anti-Passback ist eine Sicherungsfunktion, die die Benutzung der Zutrittskarte oder einer anderen Authentifizierung zum Eingang in einen Bereich zum zweiten Mal verhindert, ohne dass der Nutzer ihn vorher verlässt (somit kann die Karte keiner zweiten Personen übergeben werden, die eintreten will).

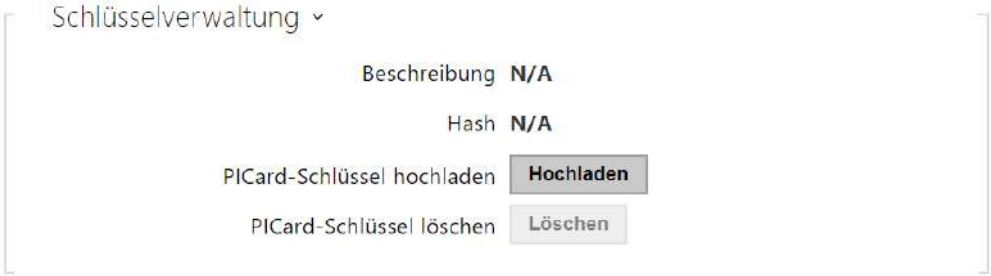
- **Modus** – wählt den Modus der Funktion Anti-Passback:

  - **Deaktiviert** – die Funktion ist defaultmäßig ausgeschaltet, der Nutzer darf die Zutrittskarte oder eine andere Authentifizierung für den Zutritt zum Eingang in einen Bereich zum zweiten Mal benutzen, ohne dass er ihn vorher verlässt.
  - **Milder** – der Nutzer darf die Zutrittskarte oder eine andere Authentifizierung für den Zutritt zum Eingang in einen Bereich zum zweiten Mal benutzen, ohne dass er ihn vorher verlässt.Im Bereich Status > Events wird ein neuer **UserAuthenticated** -Record mit dem Parameter *apbBroken*=***true*** erstellt.
  - **Strenger** – der Nutzer darf die Zutrittskarte oder eine andere Authentifizierung nicht zum zweiten Mal für den Zutritt zum Eingang in einen Bereich benutzen, ohne dass er ihn vorher verlässt. Im Bereich Status > Events wird ein neuer **UserRejected**-Record mit dem Parameter *apbBroken*=***true*** erstellt.
- **Zeitbegrenzung** – wählt die Zeit der Zutrittseinschränkung für die Funktion Anti-Passback. Man kann sie nach dem letzten Zutritt mit der jeweiligen Authentifizierung (Karte, Code usw.) während der gewählten Zeit nicht wieder in der gleichen Richtung verwenden.

Registerkarte PICard

Die 2N PICard-Technologie wird verwendet, um die Zugangsdaten auf den Zugangskarten zu verschlüsseln. Um Zugangsdaten zu lesen, benötigen 2N-Geräte Zugriff auf die entsprechenden Schlüssel, die von der Applikation 2N PICard Commander generiert werden. Diese können dann in 2N Access Commander importiert werden, was die Verteilung an alle unterstützten 2N-Geräte gewährleistet.

> **Hinweis**
>
> - Geräte, die Karten mit PICard-Technologie lesen können, sind im 2N PICard Commander Configuration Manual angeführt.



- **Beschreibung** – Bezeichnung für den erstellten Verschlüsselungsschlüssel.
- **Hash** – numerischer Identifikator des Projekts.
- **PICard-Schlüssel hochladen** – durch Auswahl der Schlüsseldatei und Eingabe eines gültigen Passworts wird der PICard-Schlüssel hochgeladen.
- **PICard-Schlüssel löschen** – löscht die hochgeladenen PICard-Schlüssel.

Registerkarte WaveKey

Das Gerät 2N, die mit dem Bluetooth-Modul ausgestattet sind, ermöglichen den Nutzer mittels der mobilen Applikation **2N Mobile Key** zu authentifizieren, die für Anlagen mit Operationssystemen iOS 12 und höher (Telefone iPhone 4s und höher) bzw. Android 6.0 Marshmallow und höher (Telefone mit der Unterstützung Bluetooth 4.0 Smart) verfügbar sind.

Nutzeridentifizierung (Auth-ID)

Die Applikation **2N Mobile Key** identifiziert sich auf das Gerät mittels eines eindeutigen Identifikators – sog. **Auth-ID.** Die Auth-ID (128bit-Nummer) wird für jeden Nutzer zufällig generiert und mittels des Prozesses der sog. **Kopplung** mit dem Nutzer, der im Interkom eingegeben ist, und seinem mobilen Gerät verknüpft.

Anmerkung

- Die generierte Auth-ID kann nicht in mehreren mobilen Geräten gleichzeitig gespeichert sein. D.h., dass die Auth-ID eindeutig das konkrete Mobilgerät (bzw. ihren Nutzer) identifiziert.

Der Wert der Auth ID kann für jeden Benutzer im Abschnitt Mobile Key der Gerätebenutzerliste festgelegt und geändert werden. Die Auth-ID kann auf einen anderen Benutzer übertragen oder auf ein anderes Gerät kopiert werden. Wenn der Feldwert gelöscht wird, wird der Zugriff des Benutzers mit dem Mobile Key gesperrt.

Kodierungsschlüssel und Lokation

Die Kommunikation zwischen der Applikation **2N Mobile Key** und das Gerät ist immer verschlüsselt. Die Applikation **2N Mobile Key** kann den Nutzer ohne die Kenntnis des Kodierungsschlüssels nicht authentifizieren. Der primäre Kodierungsschlüssel wird automatisch beim ersten Gerät generiert und man kann ihn später jederzeit manuell ändern. Der primäre Kodierungsschlüssel wird bei der Kopplung zusammen mit der Auth-ID in das mobile Gerät übertragen.

Man kann die Kodierungsschlüssel und den Lokationsidentifikator aus das Gerät exportieren und nachfolgend in weitere Interkoms importieren. Interkoms mit der gleichen Lokationsbezeichnung und gleichen Kodierungsschlüsseln bilden sog. **Lokationen**. Das mobile Gerät wird im Rahmen einer Lokation nur einmal gekoppelt und es identifiziert sich mit nur einer einzigartigen Auth-ID (man kann daher im Rahmen der Lokation die Auth-ID des Nutzers aus einem Interkom in ein anderes kopieren).

Kopplung

Unter dem Prozess der sog. Kopplung wird die Übertragung der Zutrittsdaten eines Nutzers in sein persönliches mobiles Gerät verstanden. Die Zutrittsdaten des Nutzers können in nur einem mobilen Gerät gespeichert sein – d.h. der Nutzer kann nicht z.B. zwei mobile Geräte haben, über die er sich authentifiziert. In einem mobilen Gerät können jedoch gleichzeitig die Zutrittsdaten eines Nutzers zu mehreren Lokationen gleichzeitig sein (d.h. das mobile Gerät dient als Schlüssel für mehrere Anlagen gleichzeitig).

Das Pairing eines Benutzers mit einem mobilen Gerät kann über die Benutzerliste des Geräts auf der Benutzerseite aufgerufen werden. Das Pairing kann lokal über ein an den PC angeschlossenes USB-Bluetooth-Modul oder aus der Ferne über das in das Gerät integrierte Bluetooth-Modul erfolgen. Beide Kopplungsarten führen zum gleichen Ergebnis.

Bei der Kopplung werden folgende Daten in das mobile Gerät übertragen:

- Lokationsidentifikator
- Kodierungsschlüssel der Lokation
- Auth-ID des Nutzers

Kodierungsschlüssel für die Kopplung

Im Kopplungsmodus wird aus Sicherheitsgründen für die Kommunikationsabsicherung ein anderer Code als für die Kommunikation nach der Kopplung verwendet. Dieser Code wird automatisch beim ersten Gerätstart generiert und man kann ihn später jederzeit manuell ändern.

Verwaltung der Kodierungsschlüssel

Das Gerät kann bis zu 4 Kodierungsschlüssel gültig halten – d.h. 1 primären und bis 3 sekundäre Schlüssel. Das mobile Gerät kann für die Verschlüsselung der Kommunikation einen beliebigen dieser 4 Schlüssel nutzen. Die Kodierungsschlüssel sind voll unter der Kontrolle des Systemverwalters. Die Kodierungsschlüssel sollten aus Sicherheitsgründen regelmäßig, z.B. beim Verlust des mobilen Geräts oder beim Entweichen der Gerätkonfiguration aktualisiert werden.

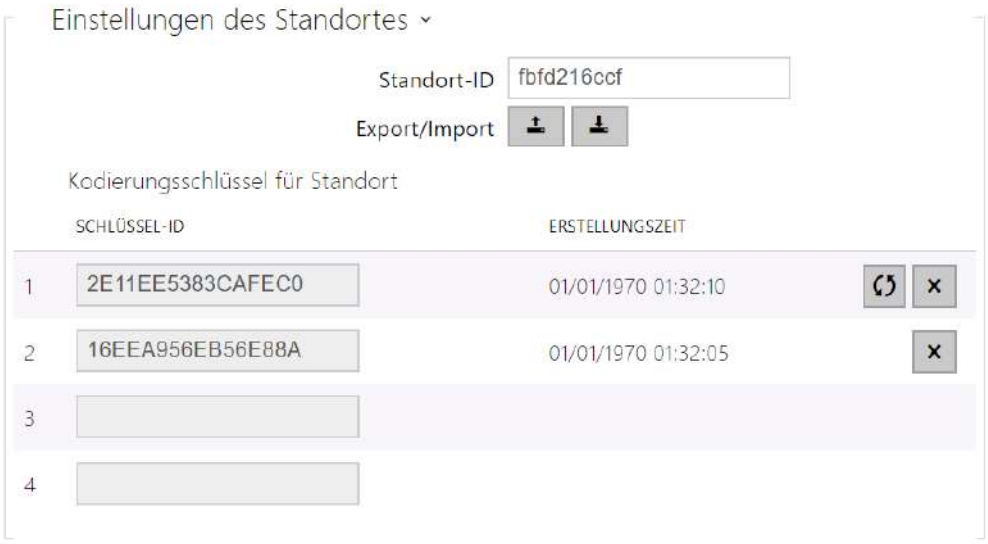
Anmerkung

- Die Kodierungsschlüssel werden automatisch beim ersten Gerätstart generiert und in der Konfigurationsdatei das Gerät gespeichert. Wir empfehlen der größeren Sicherheit wegen diese Kodierungsschlüssel vor der ersten Verwendung erneut manuell zu generieren.

Man kann den primären Schlüssel jederzeit neu generieren. Aus dem ursprünglichen primären Schlüssel wird nachfolgend der sekundäre Schlüssel, aus dem ersten sekundären wird der zweite sekundäre usw. Man kann die sekundären Schlüssel jederzeit löschen.

Nach der Entfernung des Schlüssels werden sich die Nutzer der Applikation **2N Mobile Key**, die diesen Schlüssel weiterhin nutzen, nicht authentifizieren können, wenn sie vor dem Löschen des Schlüssels die Kodierungsschlüssel in ihrem mobilen Gerät nicht aktualisieren. Die Schlüssel im mobilen Gerät werden bei jeder Anwendung der Applikation **2N Mobile Key** aktualisiert.

Parameterliste



- **Standort-ID** – eindeutiger Identifikator der Lokation, in der der Satz der eingestellten Kodierungsschlüssel gilt.
- **Taste Export** – exportiert den Lokationsidentifikator und die aktuellen Kodierungsschlüssel in eine Datei. Es ist möglich, die exportierte Datei nachfolgend in eine andere Datei zu importieren. Geräte mit der gleichen Lokationsbezeichnung und mit gleichen Kodierungsschlüsseln sog. Lokation.
- **Taste Import** – importiert die ID der Lokation und die aktuellen Kodierungsschlüssel aus der Datei, die aus einem anderen Gerät exportiert wurde. Geräte mit der gleichen Lokationsbezeichnung und mit gleichen Kodierungsschlüsseln sog. Lokation.
- **Taste primären Schlüssel erneuern** – durch das Generieren eines neuen primären Kodierungsschlüssels wird der älteste sekundäre Schlüssel gelöscht. Die Nutzer der **2N Mobile Key** Applikation, die weiterhin diesen Schlüssel benutzen, werden sich nicht authentifizieren können, wenn sie vor dieser Operation nicht die Kodierungsschlüssel in ihrem mobilen Gerät aktualisieren. Die Schlüssel im mobilen Gerät aktualisieren sich bei jeder Anwendung der Applikation **2N Mobile Key**.
- **Taste Primären Schlüssel löschen** – durch die Löschung des primären Schlüssels werden sich die Nutzer, die diesen Schlüssel verwenden, nicht mehr authentifizieren können.
- **Taste Sekundären Schlüssel löschen** – die Nutzer der Applikation **2N Mobile Key**, die weiterhin diesen Schlüssel benutzen, werden sich nach der Löschung des Schlüssels nicht

authentifizieren können, wenn sie vor dieser Operation nicht die Kodierungsschlüssel in ihrem mobilen Gerät aktualisieren. Die Schlüssel im mobilen Gerät werden bei jeder Anwendung der Applikation **2N Mobile Key** aktualisiert.

- **Gültigkeit der Pairings-PIN** – Gültigkeitsdauer der Autorisierungs-PIN für die Kopplung des mobilen Geräts des Nutzers mit das Gerät.

Tipp

- Wir empfehlen im Fall des Verlustes des Telefons mit gespeicherten Zutrittsdaten folgendes Vorgehen:

1. Löschen Sie den Wert Mobile Key Auth-ID des jeweiligen Nutzers – wodurch das verlorene Telefon gesperrt wird und ein Missbrauch unmöglich ist.
2. Generieren Sie den primären Kodierungsschlüssel (fakultativer Schritt) neu – wodurch sie den eventuellen Missbrauch des Kodierungsschlüssels unmöglich machen, der in ihrem mobilen Gerät gespeichert ist.

Warnung

- Mit dem Upgrade auf Version 2.30 wird es auch ein Upgrade für die Bluetooth-Module geben. Beim Downgrade auf Version 2.29 und niedriger können Fehlfunktionen auftreten.

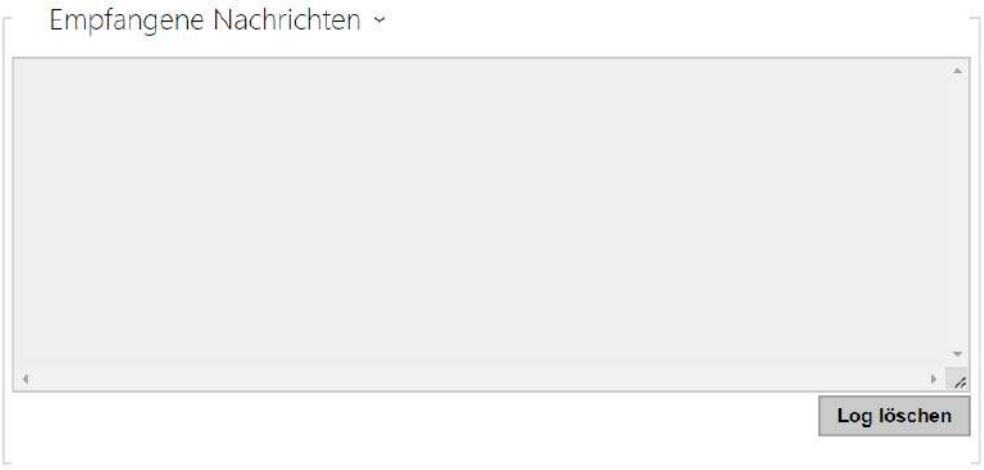
Registerkarte OSDP

Das OSDP-Protokoll gewährleistet eine sichere Kommunikation für die Übermittlung von Zugangsdaten wie z.B. der ID der Zugangskarte oder des PIN-Codes zwischen dem angeschlossenen OSDP-Gerät (Bedienteil, Türsteuergerät) und dem 2N-Gerät. Ziel ist es, die Aktivierung der Signalisierung auf dem Gerät auf der Grundlage der Antwort der Gegenstelle auf die gesendete Definition der Kartensignalisierung zu ermöglichen.

- **OSDP-Signalisierung Aktivierung** – Definitionsstring für Signalisierungszugriffserlaubnis.
- **OSDP-Signalisierung Deaktivierung** – Definitionsstring für die Signalisierung der Zugangsverweigerung.

Hinweis

- Wird in beide Parameter dieselbe Definition eingefügt, erfolgt die Auswertung mit audiovisuellen Ausdrücken, die dem Fall entsprechen, als ob autorisierter und unautorisierter Zugang kurz hintereinander verwendet würden.



Das Fenster Empfangene Nachrichten wird zum Abrufen des Definitionsstrings verwendet. Durch Anlegen der Zugangskarte an das Lesegerät der 2N Gerät wird die OSDP-Signalisierungsdefinition der Gegenstelle für den autorisierten oder nicht autorisierten Zugang angezeigt.

Die empfangene Nachricht wird mit der Zeitangabe im folgenden Format angezeigt:

13:46:39] led(0,0,0,0,0,0,0,0,1,1,1,2,2)
13:46:39] buz(0,2,1,1,1)
13:46:42] led(0,0,0,0,0,0,0,0,1,1,1,1,1)
13:46:42] buz(0,1,0,0,0)

Der Teil (ohne Zeit) wird als Definitionsstring verwendet und darf maximal 255 Zeichen lang sein, z. B.: led(0,0,0,0,0,0,0,0,1,1,1,1,1) oder buz(0,2,1,1,1). Wird auf der Gegenseite eine Übereinstimmung festgestellt, antwortet das Gerät mit einem entsprechenden Signal. Jeder Teil der Definition kann durch "*" ersetzt werden, dieser Teil wird als beliebiger Inhalt der Meldung

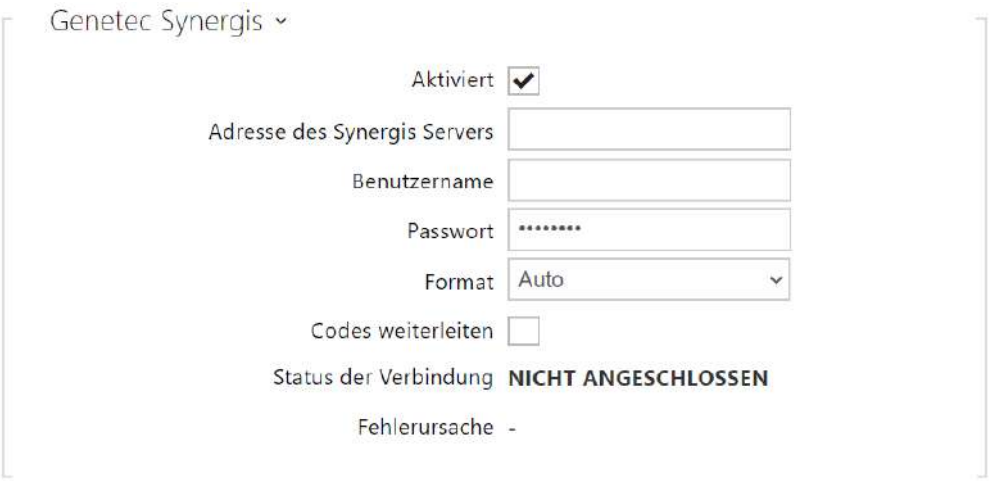
interpretiert (z. B. kann erreicht werden, dass die Signalisierung bei jedem Aufleuchten der LED 0 am Gerät aktiviert wird, unabhängig von anderen Parametern der Meldung).

- **Log löschen** – Löscht das Protokoll der empfangenen Nachricht.

Hinweis

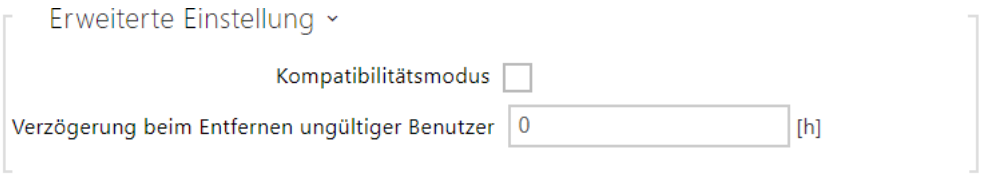
- Für eine ordnungsgemäße Funktionsweise muss in der Sektion Hardware > Erweiterungsmodule für den Kartenleser und die Tastatur der Parameter Tür / Nicht benutzt eingestellt sein. Die 2N Gerät bestätigt das Laden der Karte mit einem Signalton, nach der Auswertung antwortet das Gerät mit der entsprechenden Signalisierung.

Registerkarte Integration mit anderen Systemen



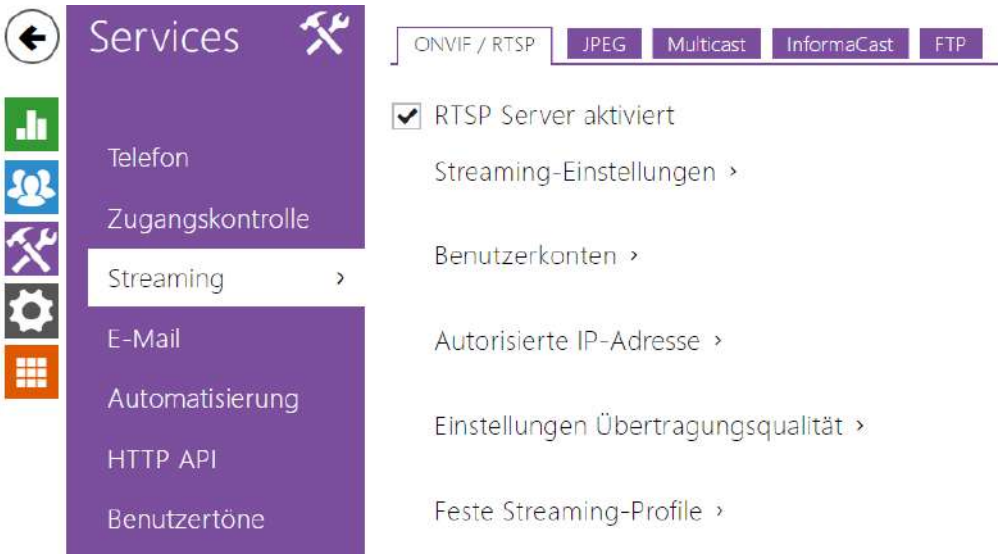
- **Aktiviert** – erlaubt die Verbindung mit dem externen Sicherheitssystem Genetec Synergis.
- **Adresse des Synergis Servers** – IP-Adresse oder der Domainname des Synergis-Servers.
- **Benutzername** – der Nutzername, der bei der Authentifizierung verwendet wird.
- **Passwort** – das Passwort, das bei der Authentifizierung verwendet wird.
- **Format** – legt das Kartenleseformat für das Senden von ID-Karten an Genetec Synergis fest.
- **Codes weiterleiten** – legt fest, ob die eingegebenen Codes weitergeleitet werden. Die Codes können maximal 6-stellig sein und am Ende muss die Bestätigungstaste gedrückt werden.
- **Verbindungszustand** – zeigt den aktuellen Status des Anschlusses an den Synergis-Server ggf. die Beschreibung des Fehlerstatus an.
- **Fehlerursache** – zeigt die Fehlerursache des letzten Versuches des Anschlusses an den Synergis-Server an – zeigt die letzte Fehlerantwort an, z.B. der Anschluss an den Server hat versagt.

Registerkarte Erweiterte



- **Kompatibilitätsmodus** – Unterstützung für ältere Kartenlesemodi. Nicht empfehlenswert für die Verwendung in Verbindung mit PICard-Karten. Wenn dieser Modus deaktiviert ist, müssen die Kartennummern für eine erfolgreiche Autorisierung genau übereinstimmen.
- **Verzögerung beim Entfernen ungültiger Benutzer** – Legt die Verzögerung fest, nach der Benutzer mit ungültigem Zugriff und aktivierter automatischer Löschung aus der Gerätebenutzerliste entfernt werden.

5.4.2 Streaming



2N Access Unit QR bieten mehrere Möglichkeiten des Audio-und Videostreamings an, siehe nachfolgende Tabelle:

Übertragungsmethode	Beschreibung
JPEG/HTTP	Herunterladen von statischen JPEG-Aufnahmen. Siehe Registerkarte JPEG nachstehend.
MJPEG/HTTP	Serie von nacheinander gehenden JPEG-Aufnahmen, Methode Server Push – Multipart/X-Mixed-Replace. Siehe Registerkarte JPEG nachstehend.
RTSP + RTP/UDP	RTSP mit einzelnen Audio-und Videostreams RTP/UDP. Unterstützt für Audio (G.711) sowie Video (H.264, H.263, MPEG-2 und MJPEG). Siehe Registerkarte RTSP nachstehend.
RTP/RTSP	RTP-Tunnelierung mittels des RTSP-Protokolls. Unterstützt für Audio (G.711) sowie Video (H.264, H.263, MPEG-2 und MJPEG). Siehe Registerkarte RTSP nachstehend.

Übertragungsmethode	Beschreibung
RTP/RTSP/HTTP	Tunnelierung des RTSP-Protokolls mittels HTTP. Unterstützt für Audio (G.711) sowie Video (H.264, H.263, MPEG-2 und MJPEG). Siehe Registerkarte RTSP nachstehend.

Übertragungsmethode	Beschreibung
RTP/UDP-Multicast	Nicht gesteuertes Multicast der RTP-Pakete. Unterstützt nur für Audio (G.711). Siehe Registerkarte Multicast nachstehend.

Begriffserklärung

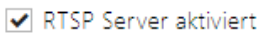
- **RTP (Real-Time Transport Protocol)** – Protokoll, das das Standardformat der Pakete für die Audio- und Videoübertragung in IP-Netzen definiert. Die Geräte 2N nutzen dieses Protokolls für die Übertragung des Audio- und Videostreams. Das Transportprotokoll für RTP ist in der Regel entweder direkt das UDP-Protokoll, es kann jedoch auch das RTSP- bzw. HTTP-Protokoll sein.
- **RTSP (Real-Time Streaming Protocol)** – Netzprotokoll für die Steuerung der Streamingserver (steuert den Aufbau, den Start und das Einstellen des Audio- und Videostreams).
- **HTTP (Hypertext Transfer Protocol)** – Protokoll, das die Übertragung eines beliebigen Inhaltes ermöglicht, das vor allem durch Webbrowser für die Kommunikation mit Webservern benutzt wird. Die Geräte 2N ermöglichen, mittels des HTTP-Protokolls statische JPEG-Bilder ggf. MJPEG-Stream auf die Art zu übertragen, die HTTP Server Push genannt wird.
- **IP Multicast** – Art der Absendung von Paketen in IP-Netzen aus einer Quelle an mehrere Stationen. Die Geräte 2N nutzen das IP-Multicast für das Senden und den Empfang des Audiostreams.
- **ONVIF (Open Network Video Interface Forum)** – ein Satz von Spezifikationen für das Suchen, die Konfiguration und die Verwaltung der Videokameras im IP-Netz. Die Geräte 2N sind ONVIF-kompatible Anlagen und implementieren voll das sog. ONVIF Profile T und Profile S.
- **JPEG** – Standardmethode der Verlustkompression des Bildes.
- **MJPEG** – Format der Videostreamkodierung, wo jedes Bild separat mittels der JPEG-Methode komprimiert wird. Die MJPEG-Kodierung produziert ein Video hoher Qualität zu Lasten der beträchtlich höheren Übertragungsgeschwindigkeit gegenüber den nachstehend angeführten Methoden.
- **H.263** – Standard für die Videostreamkompression, der in Telekommunikationen genutzt wird. Er nutzt im Gegensatz zu MJPEG die Unterschiedsinformation zwischen nacheinander gehenden Aufnahmen und gewährt eine beträchtlich höhere Kompression zu Lasten der Videostreamqualität.
- **H.263+** – wie H.263, nur eine andere Art der Bistreampaketisierung.
- **MPEG-4 part 2** – Standard für die Videostreamkompression, der eher außerhalb des Telekommunikationsbereiches angewendet wird, der jedoch sehr oft durch IP-Kameras und Video-Surveillance-Systeme unterstützt wird. Im Fall das Geräte 2N sind der Kompressionsgrad und die Bildqualität mit dem Standard H.263 vergleichbar.

- **H.264** – Standard für die Videostreamkompression. Im Gegensatz zu den H.263-Methoden produziert MPEG-4 einen Videostream gleicher Qualität bei halber Übertragungsgeschwindigkeit. Diese Kompressionsart wird manchmal auch MPEG-4 part 10 genannt.
- **G.711** – einer der üblichsten Standards für die Audioübertragung in Telekommunikationsnetzen. Verwendet die Musterfrequenz 8 kHz und die Daten werden mittels logarithmischer Kompression komprimiert.

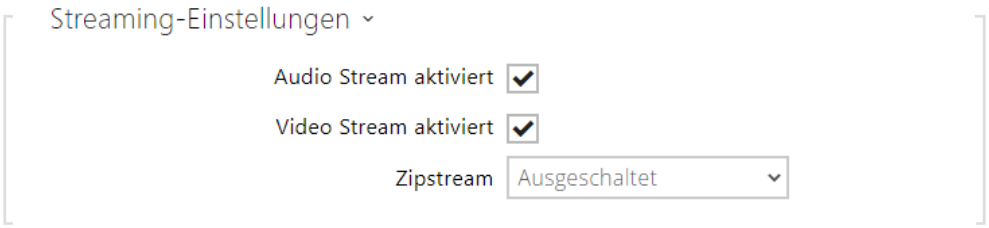
Parameterliste

Registerkarte ONVIF/RTSP

Die Geräte 2N integrieren den RTSP-Server, der in dieser Registerkarte konfiguriert wird. Der RTSP-Server ermöglicht Audio als auch Video zu streamen. Man kann die Art der Datenübertragung, die Methode und die Parameter der Videokompression und weitere Parameter wählen, die mit der Absicherung und der Qualität der Übertragung zusammenhängen.

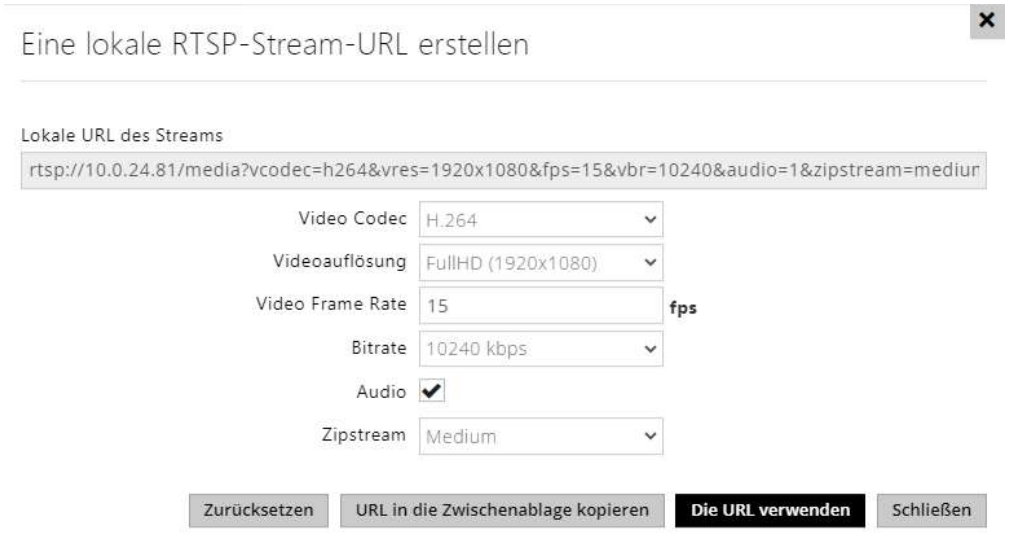


- **RTSP Server aktiviert** – erlaubt die Funktion des RTSP-Servers im Geräte.



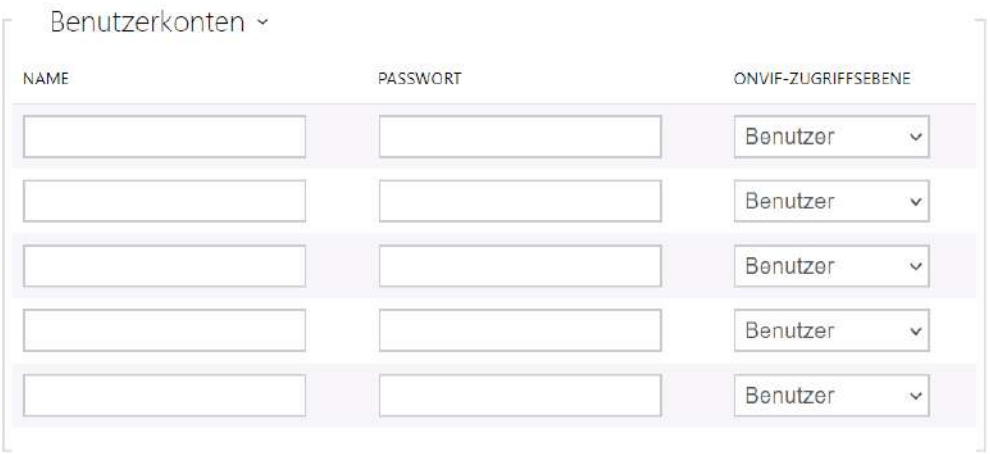
- **Audio Stream aktiviert** – erlaubt das Anbieten des Audiostreamings beim Anknüpfen der Verbindung mit dem RTSP-Server. Wenn Audio-Streaming nicht aktiviert ist, wird Audio nicht über feste Streaming-Profile oder einen lokalen URL-Stream übertragen.
- **Video Stream aktiviert** – erlaubt das Anbieten des Videostreamings beim Anknüpfen der Verbindung mit dem RTSP-Server. Wenn Video-Streaming nicht aktiviert ist, wird Video nicht über feste Streaming-Profile oder einen lokalen URL-Stream übertragen.
- **Zipstream** – Wählt das voreingestellte Kompressionsniveau des Zipstream (für H.264) aus. AXIS Zipstream bewahrt alle wichtigen forensischen Details, die Sie brauchen, und verringert die Anforderungen an die Datenübertragung und den Speicherplatz gleichzeitig durchschnittlich um 50 %. Zipstream-Kompression ist nur für Geräte mit Artpec-7-Prozessor und H.264-Codec verfügbar.

- **Lokale URL des Streams** – führt die zuletzt erzeugte und gespeicherte Stream-URL für den RTSP-Client auf. Die Bearbeitung und Erstellung der lokalen Stream-URL kann in dem Dialogfeld erfolgen, das sich durch Klicken auf das Bleistiftsymbol  öffnet.



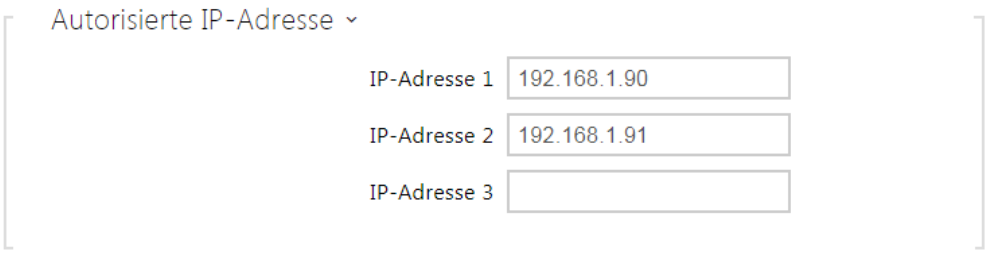
  - **Video Codec** – Auswahl der verfügbaren Video Codecs.
  - **Videoauflösung** – Auswahl der möglichen Bildauflösungen.
  - **Video Frame Rate** – Einstellung der Bildfrequenz (1 bis 30 fps, der maximal mögliche Wert für den MJPEG-Videocodec ist 15 fps).
  - **Qualität** – Auswahl der verfügbaren Übertragungsgeschwindigkeit.
  - **Audio** – Genehmigung der Tonübertragung.
  - **Zipstream** (nur für H.264 verfügbar) – die Zipstream-Einstellung der lokalen Stream-URL, die Vorrang vor dem in den **Streaming-Einstellungen** angegebenen Wert hat.

Die Zahl der RTSP-Streams ist auf 4 gleichzeitig laufende Streams beschränkt. In diese Menge fallen auch Audiostreams ohne Videos und der Audio-Rückkanal, der auf das Gerät gerichtet ist.



Für die richtige ONVIF-Funktion muss man mindestens ein Nutzerkonto errichten und das richtige Zutrittsniveau (gemäß der ONVIF-Spezifikation und der verwendeten VMS) einstellen. Ohne die Einstellung der Nutzerkonten sind nur Basisfunktionen verfügbar.

- **Name** – stellt den Nutzernamen für den Zutritt zum ONVIF-Dienst ein.
- **Passwort** – stellt das Passwort für den Zutritt zum ONVIF-Dienst ein.
- **Onvif-Zugriffsebene** – stellt das Zutrittsniveau des Nutzers zur ONVIF-Dienstleistung (Anonymous, User, Operator, Administrator) ein.

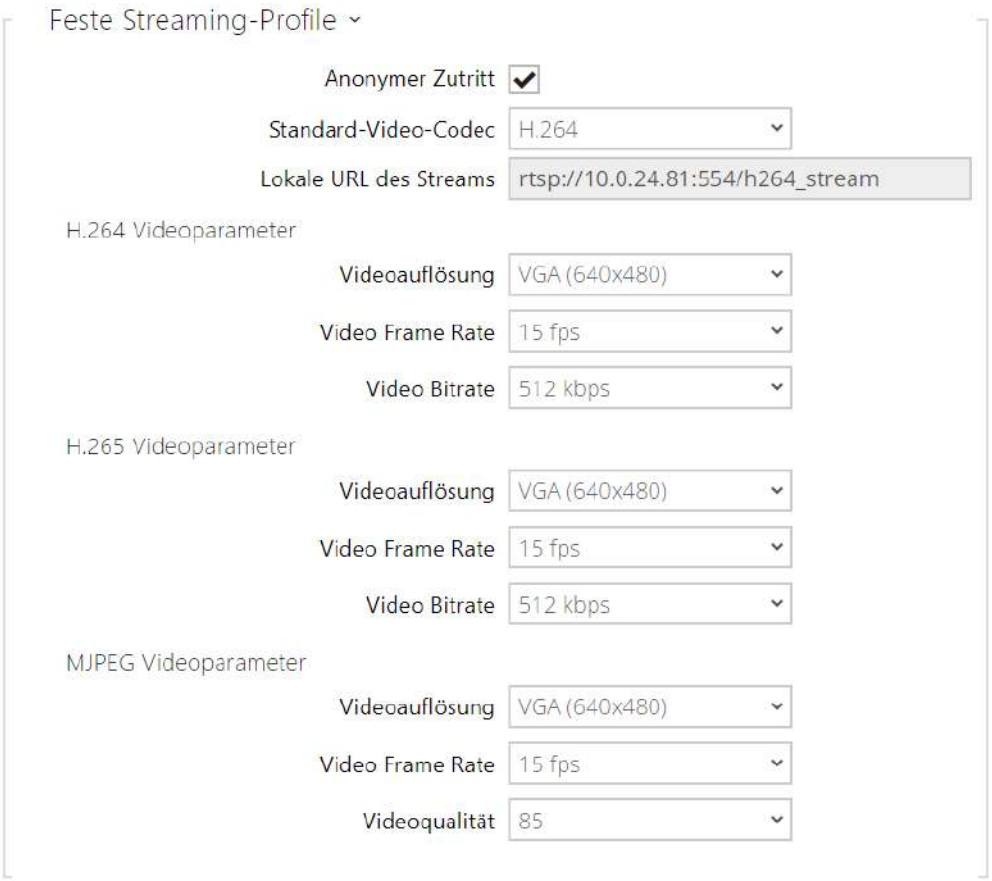


- **IP-Adresse 1** – ermöglicht es Ihnen, eine autorisierte IP-Adresse festzulegen, von der aus Sie sich beim RTSP-Server anmelden können. Wenn Sie diese Option nicht ausfüllen, können Sie sich von jeder IP-Adresse aus anmelden.

- **QoS DSCP Wert** – stellt die Priorität der RTP-Video-Pakete im Netz ein. Der eingestellte Wert wird im Feld TOS (Type of Service) im Kopf des IP-Pakets abgesendet.
- **UDP Unicast aktiviert** – erlaubt den Modus des Datenabsendens des Audio-und Videostreams mittels des RTP/UDP-Protokolls. Ist dieser Modus ausgeschalten, werden die Audio/Video-Stream-Daten nur über RTP/RTSP gesendet.
- **Maximale Videopaketgröße** – ermöglicht die maximale Größe der Videopakete einzustellen, die mittels des RTP/UDP-Protokolls versendet werden.
- **Ausgangs-RTP-Port** – stellt den lokalen RTP-Anfangs-Port im Umfang der Länge von 60 Ports ein, die bei der Audio-und Videoübertragung verwendet werden. Der voreingestellte Wert ist 4800 (d.h. der verwendet Umfang ist 4800–4859).
- **Jitter Kompensation** – stellt die Länge des Ausgleichsspeichers für die Kompensation der Ungleichmäßigkeit der Intervalle zwischen den angekommenen Audiopaketen ein. Die Einstellung eines längeren Ausgleichsspeichers erhöht die Beständigkeit des Empfangs zu Lasten einer größeren Tonverzögerung.

Tipp

- FAQ: VLC-Player – Wie kann man ein Video aus dem Interkom 2N IP anschauen
- FAQ: VLC-Player – Wie kann man Video aus dem Interkom 2N IP hochladen



Bemerkung

- ONVIF Media 1 Service unterstützt das Profil H.265 nicht.

- **Anonymer Zutritt** – Ermöglicht den Zugriff auf die ursprünglichen RTSP-Server-Streams ohne Benutzerautorisierung. Wenn dieses Feld nicht angekreuzt ist, muss sich der RTSP-Kunde für Zutritt auf Server als einer der Benutzer des ONVIF anmelden.
- **Standard-Video-Codec** – Standard-Einstellungen des angebotenen Video-Codecs beim Streamen über RTSP.
- **Local Stream URL** – eigt die Stream-URL in Abhängigkeit von der Codecwahl an.

- **Videoauflösung** – Einstellung der Bildauflösung beim Streaming mittels RTSP.
- **Video Frame Rate** – Einstellung der Aufnahmefrequenz beim Streaming mittels RTSP.
- **Video Bitrate** – stellt die Übertragungsgeschwindigkeit des Streamings mittels RTSP ein.
- **Videoqualität** – Einstellung des Bildkompressionsniveaus (nur MJPEG) im Umfang 10 (niedrige Qualität, die niedrigste Übertragungsgeschwindigkeit) – 99 (höchste Qualität, die höchste Übertragungsgeschwindigkeit).

Registerkarte JPEG

In dieser Registerkarte wird die einfachste Art des Videostreamings mittels der Methoden JPEG/HTTP und MJPEG/HTTP konfiguriert. Man kann die Bilder vom Gerät mittels der GET-Anfrage an die Adresse im Format:

- http://ip_adresse_des_interkoms/api/camera/snapshot?width=**W**&height=**H**

oder (für MJPEG, HTTP Server Push):

- http://ip_adresse_des_interkoms/api/camera/snapshot?width=**W**&height=**H**&fps=**N** herunterladen.

Die Werte W und H spezifizieren die Bildauflösung (es werden die Auflösungen 160 x 120, 320 x 240, 640 x 480, 176 x 144, 322 x 272, 352 x 288, 1280 x 960 unterstützt – nur Modelle, die mit einer 1 MPix-Kamera ausgestattet sind). Der Wert N spezifiziert die Zahl der Aufnahmen pro Sekunde (man kann zwischen den Werten 1 bis 10 wählen).

In der nachfolgenden Tabelle sind die maximalen Zahlen der gleichzeitig laufenden MJPEG/HTTP-Streams angeführt, bei denen es noch nicht zur Senkung der Frequenz der versendeten Aufnahmen unter der Verwendung des Basisniveaus der JPEG-Kompression kommt.

Gerättyp	Auflösung	Streamzahl
2N Access Unit QR	1280 x 960	2

Anmerkung

- *Die Methode HTTP Server Push mit dem Inhalt Multipart/X-Mixed-Replace wird nicht durch alle Webbrowser unterstützt: Sie können die Funktion z.B. im Webbrowser Firefox ausprobieren:*

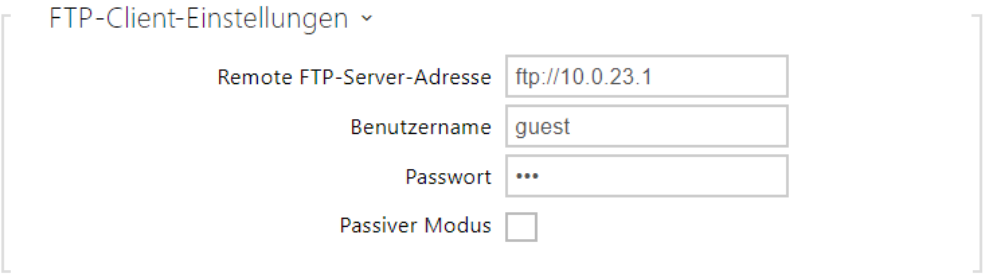
- **Niveau der JPEG-Kompression** – stellt das Niveau der JPEG-Kompression im Umfang (1–99) ein. Der empfohlene Wert liegt bei 85. Der Parameter wirkt sich auf die Bildgröße und Bildqualität aus.

Registerkarte FTP

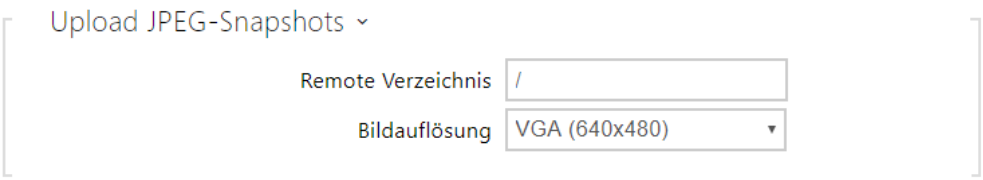
In dieser Registerkarte kann man die Zutrittsdaten zum FTP(S)-Server einstellen, auf dem Aufnahmen aus der internen oder externen an das Gerät angeschlossenen Kamera gespeichert werden können. Die Aufnahmen werden auf dem FTP-Server im JPEG-Format, in der gewählten Auflösung gespeichert, die Bezeichnung der Aufnahmedatei enthält das Datum und die Uhrzeit der Aufnahmeerstellung.

Die Aufnahmen werden auf dem FTP-Server entweder automatisch (periodisch) ggf. mithilfe der Automatisierung mittels der Aktion **Action.UploadSnapshotToFTP** gespeichert.

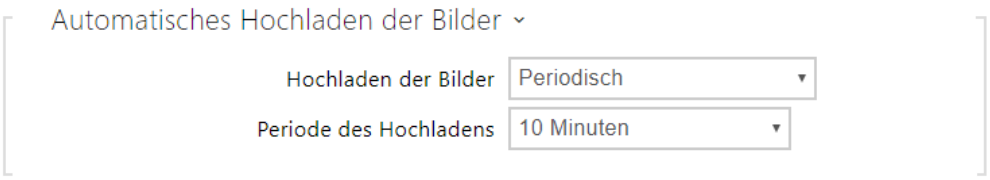
- **FTP Client aktiviert** – erlaubt die Dienstleistung für die Speicherung einer Aufnahme aus der Kamera auf dem FTP-Server.



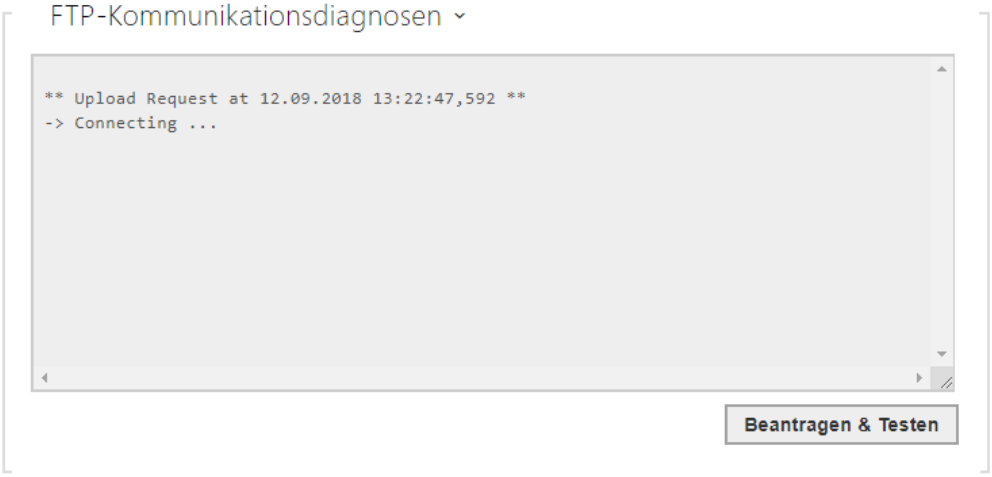
- **Remote FTP-Servers-Adresse** – stellt die Adresse des FTP-Servers ein. Die Adresse muss in der Form ftp://ip_adresse oderftps://ip_adresse sein.
- **Benutzername** – stellt den Namen des FTP-Server-Nutzers ein. Der Parameter ist verbindlich, wenn der FTP-Server die Authentifizierung des Nutzers verlangt.
- **Passwort** – stellt das Passwort des vorstehend angeführten Nutzers des FTP-Servers ein.
- **Passiver Modus** – stellt den passiven Übertragungsmodus (als/wie Webbrowser) ein.



- **Remote Verzeichnis** – stellt das Verzeichnis des FTP-Servers ein, in dem die Aufnahmen aus der Kamera gespeichert werden.
- **Bilderauflösung** – stellt die Auflösung der gespeicherten Bilder ein.

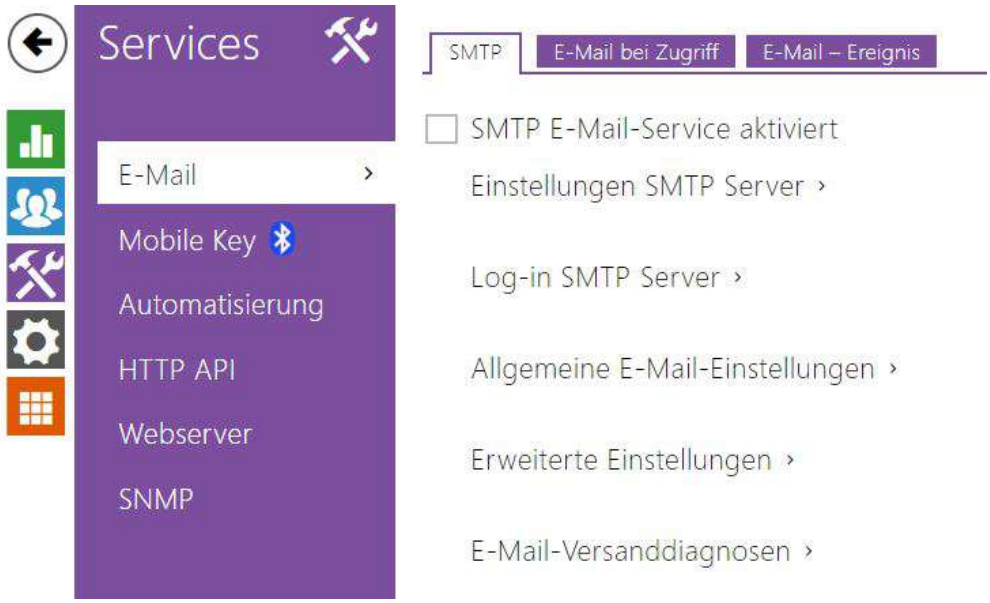


- **Hochladen der Bilder** – ermöglicht das automatische Absenden von Bildern an den FTP-Server beim Anrufanfang bzw. periodisch nach dem Ablauf der festgelegten Zeit einzustellen. Man kann das automatische Senden ausschalten (Wahl Automatisierung), danach kann man weiterhin die Bilder über die Automatisierungsaktion Action.UploadSnapshotToFtp senden.
- **Periode des Hochladens** – stellt die Periode der automatischen Absendung der Bilder am FTP bei der Einstellung des Parameters **Hochladen der Bilder** auf den Wert **Periodisch** ein. Die Periode kann schrittweise auf Werte von 10 Sekunden bis 30 Minuten eingestellt werden.



Nach dem Drücken der Taste **Speichern und Testen** kommt es zur Speicherung der aktuell eingestellten Konfiguration des FTP-Servers, Erfassung des Bildes aus der Kamera und seiner Speicherung auf dem FTP-Server. Im Verlauf der Bildspeicherung wird im oben abgebildeten Fenster der detaillierte Verlauf der Kommunikation mit dem FTP-Server angezeigt.

5.4.3 E-Mail

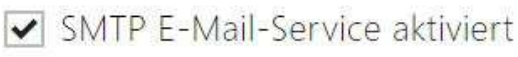


Die E-Mail-Adresse des Benutzers, die für den Versand von Informationen per E-Mail verwendet wird, z. B. über den Zugriff des Benutzers auf das Objekt oder bei Verwendung von 2N Automation. Sie können einen eigenen Betreff und den Text der E-Mail einstellen. Wenn Ihr Gerät mit einer Kamera ausgestattet ist, können Sie der E-Mail automatisch eine oder mehrere Aufnahmen aus der Kamera hinzufügen.
Das Gerät sendet E-Mails an alle Nutzer, die in der Nutzerliste eine gültige E-Mailadresse eingestellt haben. Falls Sie den Parameter **E-Mail** in der Nutzerliste unausgefüllt lassen, werden die E-Mails an die eingestellte Basis-E-Mailadresse versendet.

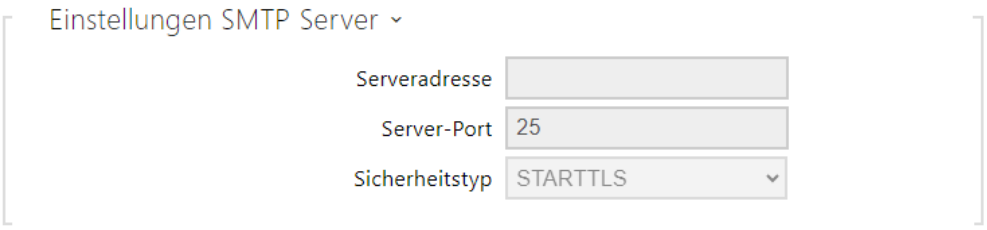
Man kann die E-Mails auch mithilfe der Automatisierung mittels der Aktion **Action.SendEmail** absenden.

> **Anmerkung**
>
> - *Die E-Mail-Funktion ist nur mit der Gold-Lizenz verfügbar.*

Registerkarte SMTP

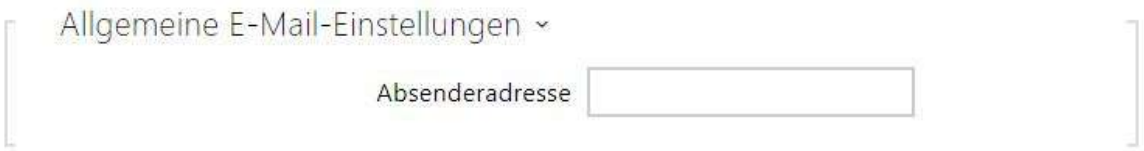


- **SMTP E-Mail-Service aktiviert** – Ermöglicht den Dienst des Absendens der E-Mails aus das Gerät zu erlauben oder zu sperren.



- **Serveradresse** – Adresse des SMTP Servers, an den die E-Mails gesendet werden.
- **Server-Port** – Port des SMTP-Servers. Ändern Sie den Wert nur dann, wenn die Einstellung des SMTP-Servers nicht-standardmäßig ist. Der typische Wert des SMTP-Ports liegt bei 25.
- **Sicherheitstyp** – Wählt die Art der Sicherheit für die Kommunikation mit dem SMTP-Server aus. Welche Art von Sicherheit der Server erfordert, ist in der Regel in seiner Dokumentation zu finden.

- **Benutzername** – Wenn der SMTP-Server die Autorisierung verlangt, muss in diesem Feld der gültige Name für das Anmelden zum Server angeführt sein. Im anderen Fall können Sie das Feld leer lassen.
- **Passwort** – Passwort für das Anmelden das Gerät zum SMTP-Server.
- **Client-Zertifikat** – Spezifiziert das Kundenzertifikat und den privaten Schlüssel, mit Hilfe deren die Verschlüsselung der Kommunikation zwischen dem Gerät und dem SMTP-Server durchgeführt wird. Man kann einen der drei Sätze der Nutzerzertifikate und privaten Schlüssel wählen, siehe Kapitel Zertifikate, oder die Einstellung **SelfSigned** belassen, wo das automatisch generierte Zertifikat verwendet wird, das beim ersten Gerätstart erstellt wurde.



- **Absenderadresse** – Stellt die Absenderadresse für alle von der Anlage ausgehenden E-Mails ein.

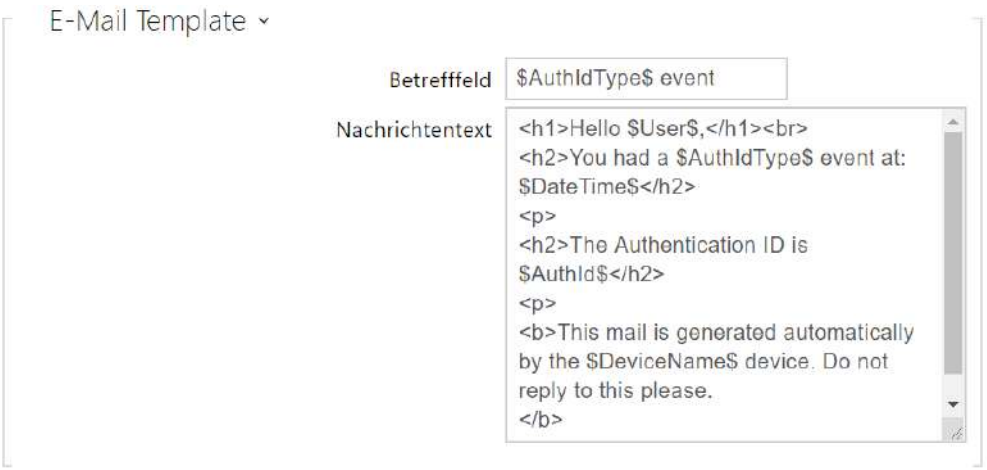
- **Liefern binnen** – Stellt die maximale Zeit ein, während der das Gerät versucht, eine E-Mail an einen unerreichbaren SMTP-Server zuzustellen.

Mittels der Taste **Anwenden & überprüfen** kann man eine Test-E-Mail an die eingegebene Adresse senden und so die Funktionsfähigkeit der aktuellen Einstellung der Absendung von E-Mails testen. Geben Sie in das Feld Adresse der Test-E-Mail die Ziel-E-Mailadresse ein und drücken Sie die Taste. Im Verlauf des Absendens der E-Mail wird im Fenster der aktuelle Status des Absendens ausgeschrieben, aus dem man ein eventuelles Problem mit der E-Maileinstellung auf dem Interkom ggf. mit einem anderen Netzelement erkennen kann.

Registerkarte E-Mail – bei Zugriff

In dieser Registerkarte kann man das Absenden der E-Mails zum Zeitpunkt des Anlegens der RFID-Karte an den Kartenleser, der Identifizierung durch das Bluetooth-Modul oder den Fingerabdruckscanner einstellen.

- **Auf E-Mail Adresse absenden** – Einstellung der E-Mail-Adresse des Administrators.
- **E-Mail senden bei** – Ermöglicht das Absenden der E-Mail nach dem Anlegen der RFID-Karte, der Identifizierung durch das Bluetooth-Modul oder den Fingerabdruckscanner. Man kann zwischen folgenden Möglichkeiten wählen:
  - **E-Mail nich senden** – es wird keine E-Mail verschickt.
  - **Alle Zugriffe** – E-mail wird nach jedem aufgezeichneten Zugriff gesendet.
  - **Verweigerte Zugriffe** – E-mail wird nur nach verweigertem Zugriff gesendet.



- **Betrefffeld** – Stellt den Betreff der abgesendeten E-Mail ein.
- **Nachrichtentext** – Ermöglicht den Inhalt der abgesendeten Nachricht zu ändern. Verwenden Sie im Text die HTML-Formatierungszeichen. Sie können in den Text Sonderzeichen einfügen, um den Nutzernamen, das Datum und die Uhrzeit, die Identifizierung der Sprechanlage bzw. den Identifikator der angelegten Karte, den gelesenen Bluetoothidentifikator oder den Fingerabdruckidentifikator, die Art des verwendeten Identifikators und die Information über die Gültigkeit des Identifikators zu ersetzen. Die Liste der in der Vorlage gefundenen Platzhalter ist in der Übersichtstabelle am Ende dieses Kapitels dargestellt.

Nachrichtentext

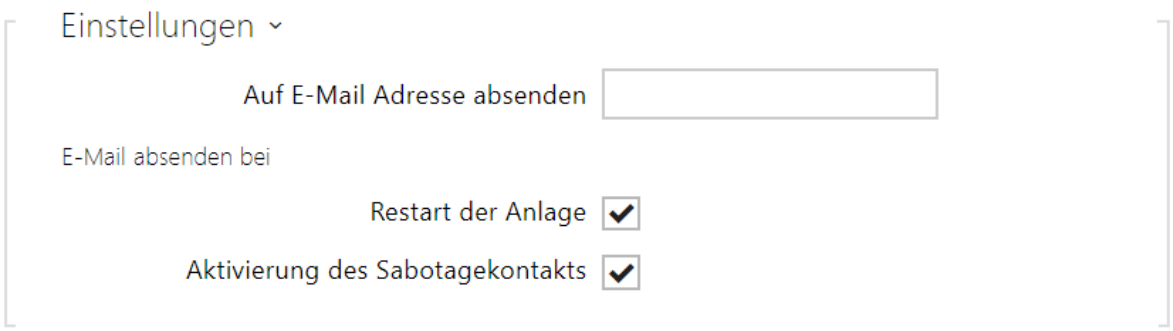
```
<p>Hello,
</p>
<p>User <b>$User$</b> generated a new access event on device <b>$DeviceName$</b> (IP:
<b>$Ip4Address$</b>)
</p>
<ul>
  <li>Authentication Type: <b>$AuthIdType$</b>
  </li>
  <li>Authentication ID: <b>$AuthId$</b>
  </li>
  <li>Validity: <b>$AuthIdValid$</b>
  </li>
  <li>Reason: <b>$AuthIdReason$</b>
  </li>
  <li>Direction: <b>$AuthIdDirection$</b>
  </li>
  <li>Date/Time: <b>$DateTime$</b>
  </li>
</ul>
<p>This e-mail message is generated automatically by device: <b>$DeviceName$</b>. Do
not reply to this message.
</p>
```

Hinweis

- Für die Sonderzeichen $AuthIdType$ a $AuthIdValid$ kann man die erweiterte Syntax verwenden, die dem Ersatz von eingebauten Werten dient, zum Beispiel für einen Text in Deutsch: $AuthIdValid|Valid=gültig|Invalid=ungültig$.
- Bei einem ungültigen $AuthId$-Wert wird die erste Hälfte der ID maskiert, z. B.: ******11188, **********792d9044158891fa usw.
- Bei einem gültigen $AuthId$-Wert wird die gesamte ID **** maskiert.
- Im Fall, dass man den Wert des Sonderzeichens in der Ersatzkette nicht findet,wird er direkt verwendet.

Registerkarte E-Mail – Ereignis

Auf dieser Registerkarte kann man Senden der Warnungen über E-Mail einstellen, im Falle SIP Ausfall, Neustart des Geräts oder Aktivierung des Schutzschalters.



Auf E-Mail Adresse absenden – ermöglicht Senden der E-Mails einzustellen. Man kann zwischen folgenden Möglichkeiten wählen:

- **Restart der Anlage**
- **Aktivierung des Sabotagekontakts**

Meldung beim Neustart des Geräts – einstellung der Nachricht, die beim Neustart des Geräts auf die angegebene E-Mail-Adresse gesendet wird.

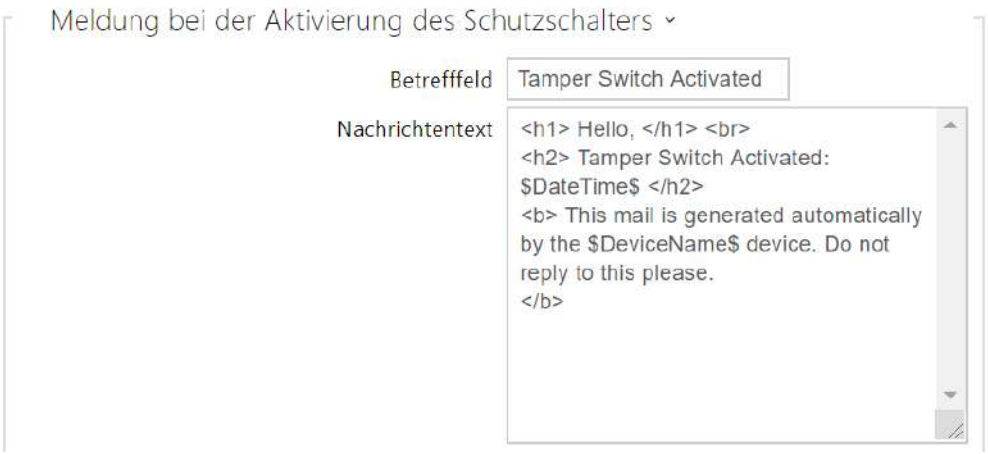
- **Betrefffeld** – Stellt den Betreff der abgesendeten E-Mail ein.
- **Nachrichtentext** – Ermöglicht den Inhalt der abgesendeten Nachricht zu ändern. Verwenden Sie im Text die HTML-Formatierungszeichen. Sie können in den Text Sonderzeichen einfügen, um den Nutzernamen, das Datum und die Uhrzeit, und die Identifizierung des Geräts zu ersetzen. Die Liste der in der Vorlage gefundenen Platzhalter ist in der Übersichtstabelle am Ende dieses Kapitels dargestellt.

Nachrichtentext

```
<p>Hello,
</p>
<p>Device <b>$DeviceName$</b> (IP: <b>$Ip4Address$</b>) rebooted on <b>$DateTime$</b>
</p>
<ul>
  <li>Reason: <b>$RebootReason$</b>
  </li>
  <li>Uptime: <b>$UpTime$</b>
  </li>
  <li>Firmware version: <b>$SoftwareVersion$</b>
  </li>
  <li>Build date: <b>$BuildTime$</b>
  </li>
</ul>
<p>This e-mail message is generated automatically by device: <b>$DeviceName$</b>. Do
not reply to this message.
</p>
```

Hinweis

- Im Fall, dass man den Wert des Sonderzeichens in der Ersatzkette nicht findet,wird er direkt verwendet.



Meldung bei der Aktivierung des Schutzschalters – einstellung der Nachricht, die bei der Aktivierung des Schutzschalters auf die angegebene E-Mail-Adresse gesendet wird.

- **Betrefffeld** – Stellt den Betreff der abgesendeten E-Mail ein.
- **Nachrichtentext** – Ermöglicht den Inhalt der abgesendeten Nachricht zu ändern. Verwenden Sie im Text die HTML-Formatierungszeichen. Sie können in den Text

Sonderzeichen einfügen, um den Nutzernamen, das Datum und die Uhrzeit, und die Identifizierung des Geräts zu ersetzen. Die Liste der in der Vorlage gefundenen Platzhalter ist in der Übersichtstabelle am Ende dieses Kapitels dargestellt.

Nachrichtentext

```
<p>Hello,
</p>
<p>Tamper switch of device <b>$DeviceName$</b> (IP: <b>$Ip4Address$</b>) was
activated on <b>$DateTime$</b>
</p>
<p>This e-mail message is generated automatically by device: <b>$DeviceName$</b>. Do
not reply to this message.
</p>
```

Hinweis

- Im Fall, dass man den Wert des Sonderzeichens in der Ersatzkette nicht findet,wird er direkt verwendet.

Hinweis

- Der Name für den Platzhalter $DeviceName$ ist direkt mit dem Wert des Parameters *Device Name* im Services / Web-Server / Basis-Einstellungen . Wir empfehlen, einen Namen zu verwenden, der eindeutig definiert, um welches Gerät es sich handelt.

Liste der Platzhalter

Auftreten	Platzhaltersymbol	Beschreibung
Stets	$DateTime$	aktuelles Datum und Uhrzeit
	$DeviceName$	Name der Einrichtung
	$Ip4Address$	IP-Adresse des Geräts
	$SoftwareVersion$	FW-Version
	$BuildTime$	Erstellungsdatum und -zeit
	$UpTime$	Betriebszeit der Geräte

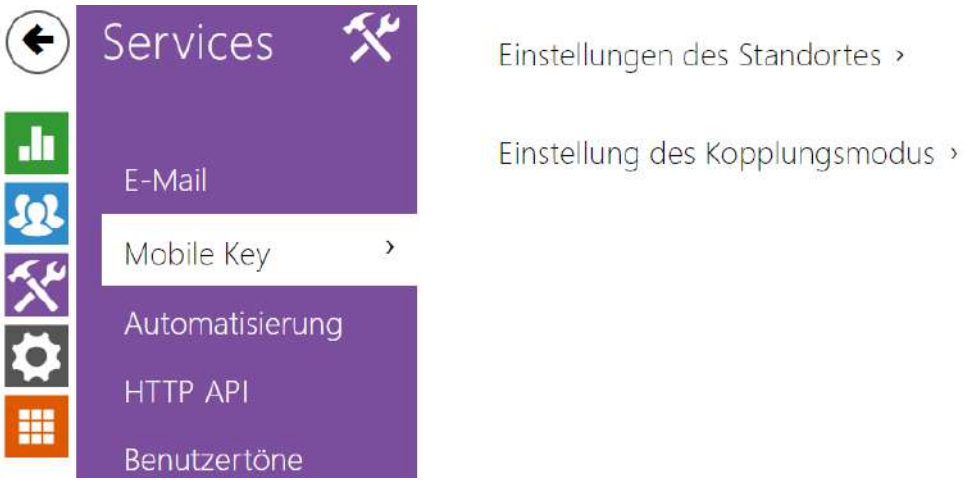
Auftreten	Platzhaltersymbol	Beschreibung
Abhängig vom konkreten Fall	$User$	Nutzername
	$RebootReason$	der Grund für den Neustart
	$AuthId$	Authentifizierungs-ID
	$AuthIdDirection$	Richtung (aus/ein)
	$AuthIdType$	Authentifizierungsart
	$AuthIdValid$	gültig, ungültig
	$AuthIdReason$	Grund für die Ablehnung

Übersicht über Platzhalter in Ereignissen

Platzhalter / Funktion	E-Mail bei Zutritt	E-mail – Verlust der SIP-Registration	E-mail – Restart der Anlage	E-mail – Aktivierung des Sabotagekontakts	E-Mail - Diagnose senden	Automatisierung
$DateTime$	*	*	*	*	*	*
$DeviceName$	*	*	*	*	*	*
$Ip4Address$	*	*	*	*	*	*
$SoftwareVersion$	*	*	*	*	*	*
$BuildTime$	*	*	*	*	*	*
$UpTime$	*	*	*	*	*	*
$User$	*				*	*
$RebootReason$			*			

Platzhalter / Funktion	E-Mail bei Zutritt	E-mail – Verlust der SIP-Registration	E-mail – Restart der Anlage	E-mail – Aktivierung des Sabotagekontakts	E-Mail - Diagnose senden	Automatisierung
$DialNumber$					• (wird senden "E-Mail test")	CallState Changed
$SipAccountNumber$		*				
$AuthId$	*					CardEntered, CardHeld
$AuthIdDirection$	*					CardEntered, CardHeld
$AuthIdType$	*					CardEntered, CardHeld
$AuthIdValid$	*					CardEntered, CardHeld
$AuthIdReason$	*					

5.4.4 Mobile Key



Die Zutrittseinheiten können mit einem Bluetooth-Modul ausgestattet werden, das die Benutzerauthentifizierung über die mobile App **2N Mobile Key** ermöglicht, die für Geräte mit iOS 12 und höher (iPhone 4S und höher) oder Android 6.0 Marshmallow und höher (Bluetooth 4.0 Smartphones) verfügbar ist.

Nutzeridentifizierung (Auth-ID)

Die Applikation **2N Mobile Key** identifiziert sich auf der Seite des 2N Zutrittseinheiten eines eindeutigen Identifikators – sog. **Auth-ID**. Die Auth-ID (128bit-Nummer) wird für jeden Nutzer zufällig generiert und mittels des Prozesses der sog. **Kopplung** mit dem Nutzer, der im 2N Zutrittseinheiten eingegeben ist, und seinem mobilen Gerät verknüpft.

> ⓘ **Anmerkung**
>
> - Die generierte Auth-ID kann nicht in mehreren mobilen Geräten gleichzeitig gespeichert sein. D.h., dass die Auth-ID eindeutig das konkrete Mobilgerät (bzw. ihren Nutzer) identifiziert.

Man kann den Wert Auth-ID im Abschnitt Mobile Key des Telefonbuchs des 2N Zutrittseinheiten einstellen und ändern. Die Auth-ID kann man einem anderen Nutzer zuordnen bzw. in einen anderen 2N Zutrittseinheiten kopieren. Nach dem Löschen des Feldwertes kommt es zur Sperre des Nutzerzutrittes.

Kodierungsschlüssel und Lokation

Die Kommunikation zwischen der Applikation **2N Mobile Key** und dem 2N Zutrittseinheiten ist immer verschlüsselt. Die Applikation **2N Mobile Key** kann den Nutzer ohne die Kenntnis des Kodierungsschlüssels nicht authentifizieren. Der primäre Kodierungsschlüssel wird automatisch beim ersten Start des 2N Zutrittseinheiten generiert und man kann ihn später jederzeit manuell ändern. Der primäre Kodierungsschlüssel wird bei der Kopplung zusammen mit der Auth-ID in das mobile Gerät übertragen.

Man kann die Kodierungsschlüssel und den Lokationsidentifikator aus dem 2N Zutrittseinheiten exportieren und nachfolgend in weitere Geräte 2N importieren. Die Geräte 2N mit der gleichen Lokationsbezeichnung und gleichen Kodierungsschlüsseln bilden sog. **Lokationen.** Das mobile Gerät wird im Rahmen einer Lokation nur einmal gekopplt und es identifiziert sich mit nur einer einzigartigen Auth-ID (man kann daher im Rahmen der Lokation die Auth-ID des Nutzers aus einem Geräte 2N in ein anderes kopieren).

Kopplung

Unter dem Prozess der sog. Kopplung wird die Übertragung der Zutrittsdaten eines Nutzers in sein persönliches mobiles Gerät verstanden. Die Zutrittsdaten des Nutzers können in nur einem mobilen Gerät gespeichert sein – d.h. der Nutzer kann nicht z.B. zwei mobile Geräte haben, über die er sich authentifiziert. In einem mobilen Gerät können jedoch gleichzeitig die Zutrittsdaten eines Nutzers zu mehreren Lokationen gleichzeitig sein (d.h. das mobile Gerät dient als Schlüssel für mehrere Anlagen gleichzeitig).

Das Pairing eines Benutzers mit einem mobilen Gerät kann im Geräteverzeichnis auf der Seite des Benutzers aufgerufen werden. Die Kopplung kann man physisch lokal mittels des USB-Bluetooth-Moduls, das an einen PC angeschlossen ist ggf. über ein Bluetooth-Modul, das im Gerät integriert ist durchführen. Beide Kopplungsarten führen zum gleichen Ergebnis.

Bei der Kopplung werden folgende Daten in das mobile Gerät übertragen:

- Lokationsidentifikator
- Kodierungsschlüssel der Lokation
- Auth-ID des Nutzers

Kodierungsschlüssel für Kopplung

Im Kopplungsmodus wird aus Sicherheitsgründen für die Kommunikationsabsicherung ein anderer Code als für die Kommunikation nach der Kopplung verwendet. Dieser Code wird automatisch beim ersten 2N Zutrittseinheiten generiert und man kann ihn später jederzeit manuell ändern.

Verwaltung der Kodierungsschlüssel

Die Geräte kann bis zu 4 Kodierungsschlüssel gültig halten – d.h. 1 primären und bis 3 sekundäre Schlüssel. Das mobile Gerät kann für die Verschlüsselung der Kommunikation einen beliebigen dieser 4 Schlüssel nutzen. Die Kodierungsschlüssel sind voll unter der Kontrolle des Systemverwalters. Die Kodierungsschlüssel sollten aus Sicherheitsgründen regelmäßig, z.B. beim Verlust des mobilen Geräts oder beim Entweichen der Konfiguration die 2N Zutrittseinheiten aktualisiert werden.

> **Anmerkung**
>
> - Die Kodierungsschlüssel werden automatisch beim ersten Start des 2N Geräte generiert und in der Konfigurationsdatei des 2N Geräte gespeichert. Wir empfehlen der größeren Sicherheit wegen diese Kodierungsschlüssel vor der ersten Verwendung erneut manuell zu generieren.

Man kann den primären Schlüssel jederzeit neu generieren. Aus dem ursprünglichen primären Schlüssel wird nachfolgend der sekundäre Schlüssel, aus dem ersten sekundären wird der zweite sekundäre usw. Man kann die sekundären Schlüssel jederzeit löschen.

Nach der Entfernung des Schlüssels werden sich die Nutzer der Applikation **2N Mobile Key**, die diesen Schlüssel weiterhin nutzen, nicht authentifizieren können, wenn sie vor dem Löschen des Schlüssels die Kodierungsschlüssel in ihrem mobilen Gerät nicht aktualisieren. Die Schlüssel im mobilen Gerät werden bei jeder Anwendung der Applikation **2N Mobile Key** aktualisiert.

Parameterliste

- **Standort-ID** – Eindeutiger Identifikator der Lokation, in der der Satz der eingestellten Kodierungsschlüssel gilt.
- **Taste Export** – Exportiert den Lokationsidentifikator und die aktuellen Kodierungsschlüssel in eine Datei. Es ist möglich, die exportierte Datei nachfolgend in eine andere Datei zu importieren. Geräte mit der gleichen Lokationsbezeichnung und mit gleichen Kodierungsschlüsseln sog. Lokation.
- **Taste Import** – Importiert die ID der Lokation und die aktuellen Kodierungsschlüssel aus der Datei, die aus einem anderen 2N Geräte exportiert wurde. Geräte mit der gleichen Lokationsbezeichnung und mit gleichen Kodierungsschlüsseln sog. Lokation.

- **Taste primären Schlüssel erneuern** – Durch das Generieren eines neuen primären Kodierungsschlüssels wird der älteste sekundäre Schlüssel gelöscht. Die Nutzer der 2N Mobile Key Applikation, die weiterhin diesen Schlüssel benutzen, werden sich nicht authentifizieren können, wenn sie vor dieser Operation nicht die Kodierungsschlüssel in ihrem mobilen Gerät aktualisieren. Die Schlüssel im mobilen Gerät aktualisieren sich bei jeder Anwendung der Applikation **2N Mobile Key**.
- **Taste Primären Schlüssel löschen** – Durch die Löschung des primären Schlüssels werden sich die Nutzer, die diesen Schlüssel verwenden, nicht mehr authentifizieren können.
- **Taste Sekundären Schlüssel löschen** – Die Nutzer der Applikation **2N Mobile Key**, die weiterhin diesen Schlüssel benutzen, werden sich nach der Löschung des Schlüssels nicht authentifizieren können, wenn sie vor dieser Operation nicht die Kodierungsschlüssel in ihrem mobilen Gerät aktualisieren. Die Schlüssel im mobilen Gerät werden bei jeder Anwendung der Applikation **2N Mobile Key** aktualisiert.

- **Die Gültigkeit der Kopplung-PIN** – Gültigkeitsdauer der Autorisierungs-PIN für die Kopplung des mobilen Geräts des Nutzers mit dem 2N Geräte.

Tipp

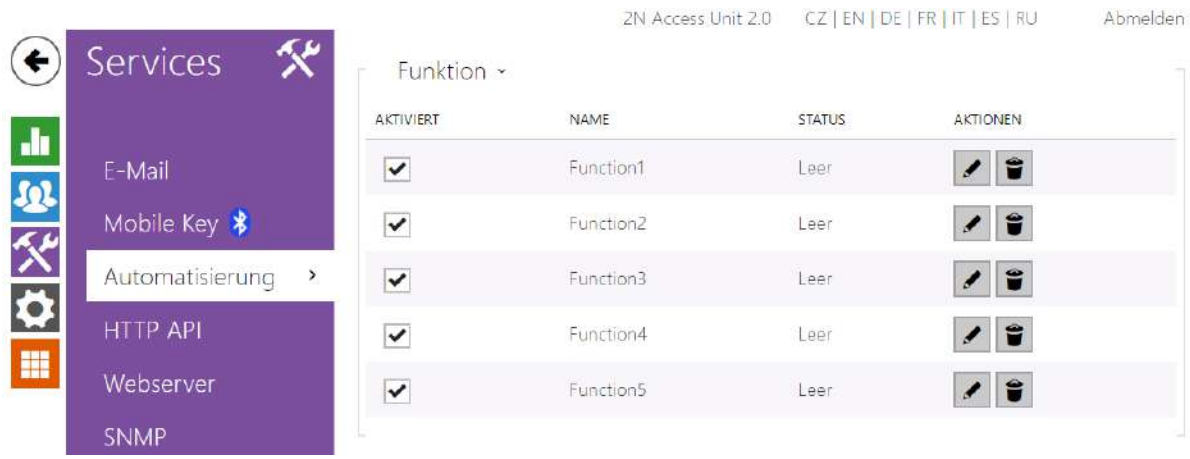
- Wir empfehlen im Fall des Verlustes des Telefons mit gespeicherten Zutrittsdaten folgendes Vorgehen:

1. Löschen Sie den Wert Mobile Key Auth-ID des jeweiligen Nutzers – wodurch das verlorene Telefon gesperrt wird und ein Missbrauch unmöglich ist.
2. Generieren Sie den primären Kodierungsschlüssel (fakultativer Schritt) neu – wodurch sie den eventuellen Missbrauch des Kodierungsschlüssels unmöglich machen, der in ihrem mobilen Gerät gespeichert ist.

Warnung

- Mit dem Upgrade auf Version 2.30 wird es auch ein Upgrade für die Bluetooth-Module geben. Beim Downgrade auf Version 2.29 und niedriger können Fehlfunktionen auftreten.

5.4.5 Automatisierung



Die 2N Zutrittseinheiten können bietet sehr flexible Möglichkeiten der Einstellung gemäß unterschiedlicher Anforderungen an. Es kommen Situationen vor, in denen der übliche Umfang der Einstellung (z.B. das Verhalten der Schalter oder Anrufe) nicht ausreichend ist und für diese Fälle bietet der 2N Geräte die spezielle programmierbare Schnittstelle **Automation** an. Die typische Anwendung der **Automation** ist für Applikationen, die eine kompliziertere Verknüpfung mit Systemen Dritter erfordern.

Eine detaillierte Beschreibung der Funktion und Konfiguration von **Automation** befindet sich im Konfigurationshandbuch Automation.

> **Anmerkung**
>
> - *Die Automatisierungsfunktion ist nur mit der Lizenz Gold oder Enhanced verfügbar Integration.*

5.4.6 HTTP API

2N HTTP API ist die Applikationsschnittstelle für die Bedienung von ausgewählten Interkomfunktionen mittels des **HTTP**-Protokolls. Diese Schnittstelle ermöglicht, die 2N Geräte mit Produkten Dritter, z.B. Systemen der Hausautomatisierung, Gebäudesicherungs- und Überwachungssystemem der Gebäude u.Ä. einfach zu integrieren.

Services

2N HTTP API ist gemäß der Funktion in folgende Leistungen aufgeteilt:

- **System-API** – ermöglicht Konfigurationsänderungen, Erwerben des Status und Upgrade vom Gerät.
- **Verwaltung des API Zugangs** – ermöglicht Steuerung der Zugriffe und Verifikationsart der Benutzerauthentisierung.
- **Schalter-API** – ermöglicht die Steuerung und Kontrolle des Schalterstatus, z.B. des Öffnens der Türschlösser u.Ä.
- **I/O API** – ermöglicht die Steuerung und Beaufsichtigung der logischen Eingänge und Ausgänge des Geräte.
- **Display API** – ermöglicht die Displaysteuerung und das Anzeigen der Nutzerinformationen auf dem Display.
- **E-Mail API** – ermöglicht aus der Anlage Nutzer-E-Mails abzusenden.
- **Telefon/Anruf-API** – ermöglicht die Steuerung und Verfolgung der eingehenden und ausgehenden Anrufe.
- **Logging-API** – ermöglicht aufgezeichnete Ereignisse der Anlage abzulesen.
- **Automatisierungs-API** – ermöglicht die Einstellung von sicheren/unsicheren Kommunikations- und Autorisierungsanforderungen.

Man kann für jeden Dienst das Transportprotokoll (**HTTP** oder **HTTPS**) und die Authentifizierungsart (**Keine**, **Basic** oder **Digest**) einstellen. Man kann in der Konfiguration **HTTP API** bis zu fünf Nutzerkonten (mit eigenem Namen und Passwort) mit der Möglichkeit des detaillierten Zutrittes zu einzelnen Diensten und Funktionen errichten.

Für jeden Dienst können Sie die erforderliche Authentifizierungsmethode für an das Gerät gesendete Anfragen festlegen. Wird die Authentifizierung nicht durchgeführt, wird die Anfrage zurückgewiesen. Die Authentifizierung von Anfragen erfolgt über das in RFC-2617 beschriebene

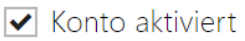
Standard-Authentifizierungsprotokoll. Die folgenden drei Authentifizierungsmethoden können ausgewählt werden:

- **Keine** – Der Dienst erfordert keine Authentifizierung. In diesem Fall ist der Dienst im lokalen Netz völlig ungeschützt.
- **Basic** – Der Dienst erfordert eine Basic-Authentifizierung gemäß **RFC-2617**. In diesem Fall benötigt der Dienst ein Kennwort, das jedoch in einem offenen Format gesendet wird. Wir empfehlen, diese Option nach Möglichkeit mit dem **HTTPS**-Protokoll zu kombinieren.
- **Digest** – Der Dienst erfordert eine Digest-Authentifizierung gemäß **RFC-2617**. Diese Option ist die Standardeinstellung und die sicherste der oben genannten Methoden.

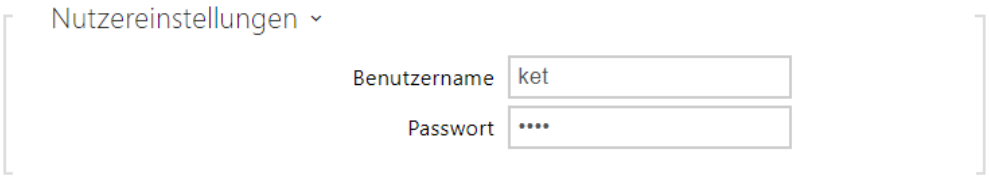
Die detaillierte Beschreibung und Einstellung von HTTP API ist im Handbuch 2N HTTP API.

Konto 1–5

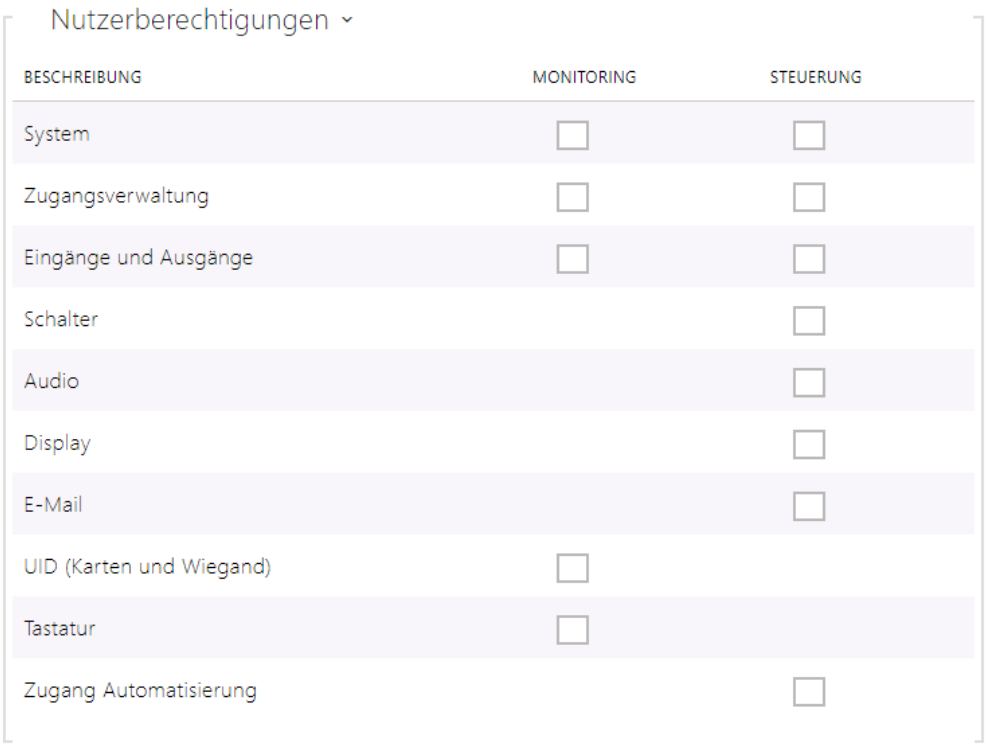
Die 2N Geräte ermöglicht bis zu fünf Benutzerkonten zu verwalten, die für den Zugriff auf die Dienstleistungen bestimmt sind **HTTP API**. Das Benutzerkonto enthält den Benutzernamen und das Benutzerpasswort sowie eine Tabelle mit den Zugriffsberechtigungen des Benutzers für jede Dienstleistung **HTTP API**.



- **Konto aktiviert** – aktiviert dieses Benutzerkonto.



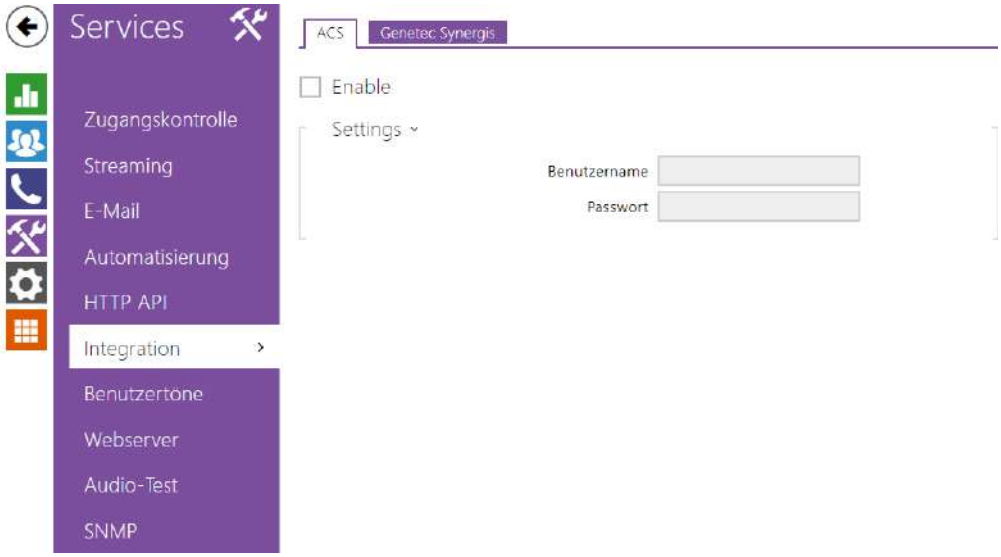
- **Benutzername** – geben Sie den Benutzernamen für die Authentifizierung des HTTP API ein.
- **Passwort** – geben Sie das Authentifizierungspasswort für HTTP API ein.



Mithilfe der Tabelle der Zugriffsberechtigungen können Sie die Privilegien des Benutzerkontos für einzelne Dienstleistungen steuern.

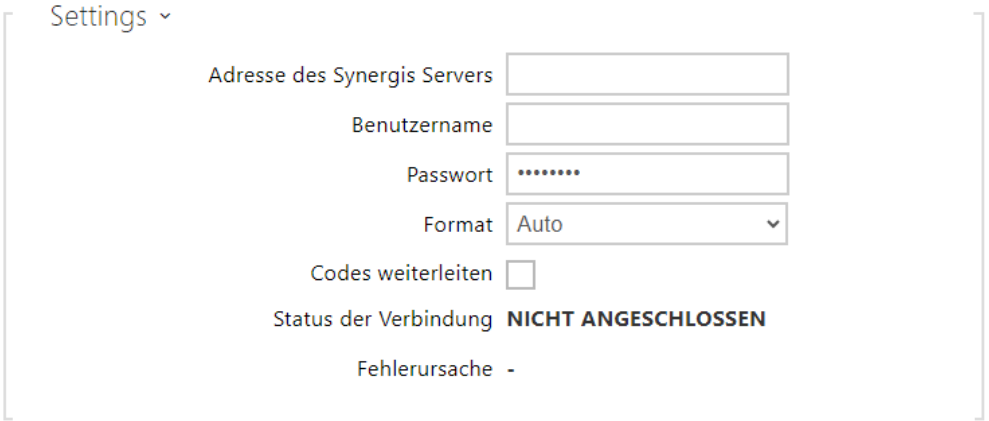
5.4.7 Integration

Der Dienst Integration ermöglicht es dem Gerät, sich mit Systemen von Drittanbietern zu verbinden.



Registerkarte Genetec Synergis

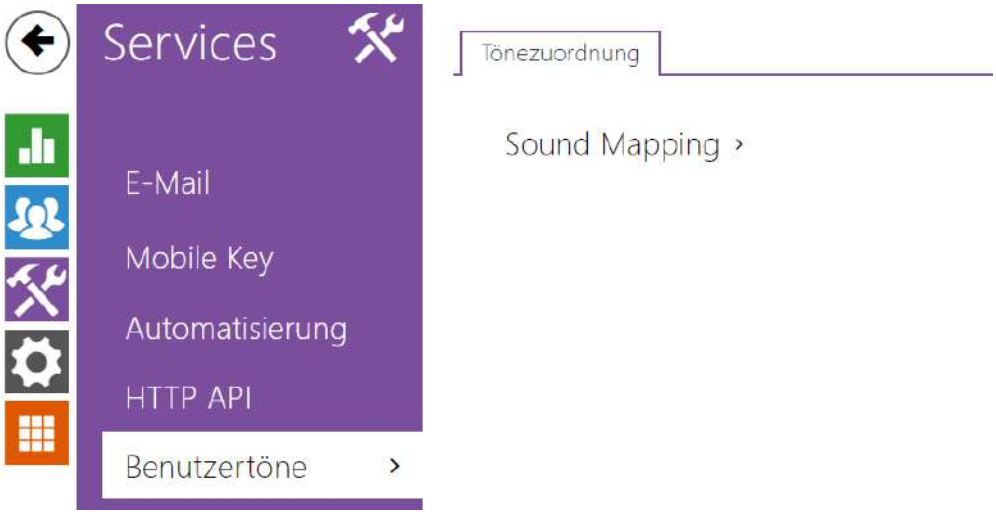
- **Freigegeben**– erlaubt die Verbindung mit dem externen Sicherheitssystem Genetec Synergis.



- **Adresse des Synergis Servers**– IP-Adresse oder der Domainname des Synergis-Servers.
- **Benutzername**– der Benutzername, der bei der Authentifizierung verwendet wird.

- **Passwort**– das Passwort, das bei der Authentifizierung verwendet wird.
- **Format -** Format der gesendeten Codes
- **Codes weiterleiten -** stellt ein, ob die eingegebenen Codes weitergeleitet werden, Die Codes können maximal 6-stellig sein und am Ende muss die Bestätigungstaste gedrückt werden.

5.4.8 Benutzertöne



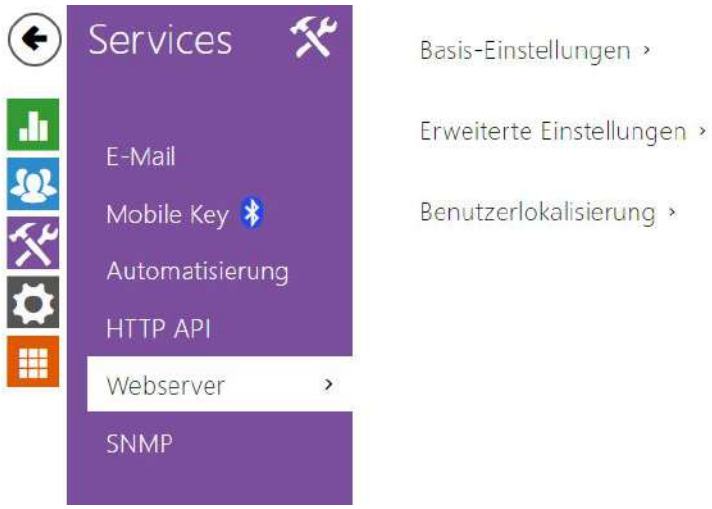
Mit Benutzer-Sounds kann die Art der Tonsignalisierung des geschlossenen Schalters eingestellt oder vollständig stummgeschaltet werden. Das Aktivieren der Tonsignalisierung zur Authentifizierung ist in Abschnitt 5.4.1 Zugangskontrolle möglich.

- **Sprache der Tonmeldungen** – wählt die Sprache der Tonmeldungen der Sprechanlage aus. Ist für das Ereignis eine Datei gemappt, für die ihre Übersetzung vorhanden ist, wird die Meldung in der gewählten Sprache abgespielt. Ist die Übersetzung nicht vorhanden, wird die Meldung Englisch oder als sprachneutraler Ton gesendet.

- **Authentifizierungsfehler** – legt den Ton fest, der abgespielt wird, wenn der Zugriff verweigert wird.
- **Signalisierung des fehlgeschlagenen WaveKey** – stellt den Ton ein, der abgespielt wird, wenn kein Telefon die Tür während der Suchdauer öffnete.

- **Signal Aktivierung des Schalters 1–4** – legt den Ton fest, der ertönen soll, wenn ein Schalter 1–4 aktiviert wird. In der Einstellung der einzelnen Schalter muss man die Signalisierung des Schaltens konkretisieren, siehe Kapitel Schalter.

5.4.9 Webserver



Man kann die 2N Zutrittseinheiten können mittels eines üblichen Webbrowsers konfigurieren, der auf den Webserver zugreift, der im Gerät integriert ist. Für die Kommunikation zwischen dem Webbrowser und dem Gerät wird das gesicherte HTTPS-Protokoll verwendet. Nach der Anmeldung im Zutrittsterminal muss man den Anmeldenamen und das Passwort eingeben. Der Originalname und das Ausgangs-Passwort für die Anmeldung sind **admin** und **2n**. Wir empfehlen das Ausgangs-Passwort so früh wie möglich zu ändern.

Der Dienst Webserver wird auch durch weitere Gerätfunktionen genutzt:

a. HTTP-Befehle für die Bedienung der Schalter, siehe Kapitel Schalter.
b. Ereignisse Event.HttpTrigger in **2N Automation**, siehe jeweiliges Handbuch.

Für diese speziellen Fälle kann man für die Kommunikation das nicht gesicherte HTTP-Protokoll nutzen.

Parameterliste

- **Gerätebezeichnung** – Stellt die Bezeichnung der Anlage ein, die in der rechten oberen Ecke der Webschnittstelle, im Anmeldefenster und eventuell in weiteren Applikationen (**2N® IP Manager**, **2N® IP Network Scanner** u.Ä.) angezeigt wird.
- **Sprache der Benutzeroberfläche** – Stellt die Ausgangssprache nach der Anmeldung zum Administrations-Webserver ein. Sie können die Sprache der Webschnittstelle jederzeit mittels der Tasten in der oberen Leiste der Seite ändern.
- **Zutrittspasswort** – Stellt das Passwort für Anmelden zum Zutrittsterminal ein. Verwenden Sie , um das Passwort zu ändern. Das Passwort muss mindestens 8 Zeichen enthalten, davon einen kleinen Buchstaben des Alphabets, einen großen Buchstaben des Alphabets und mindestens eine Ziffer.

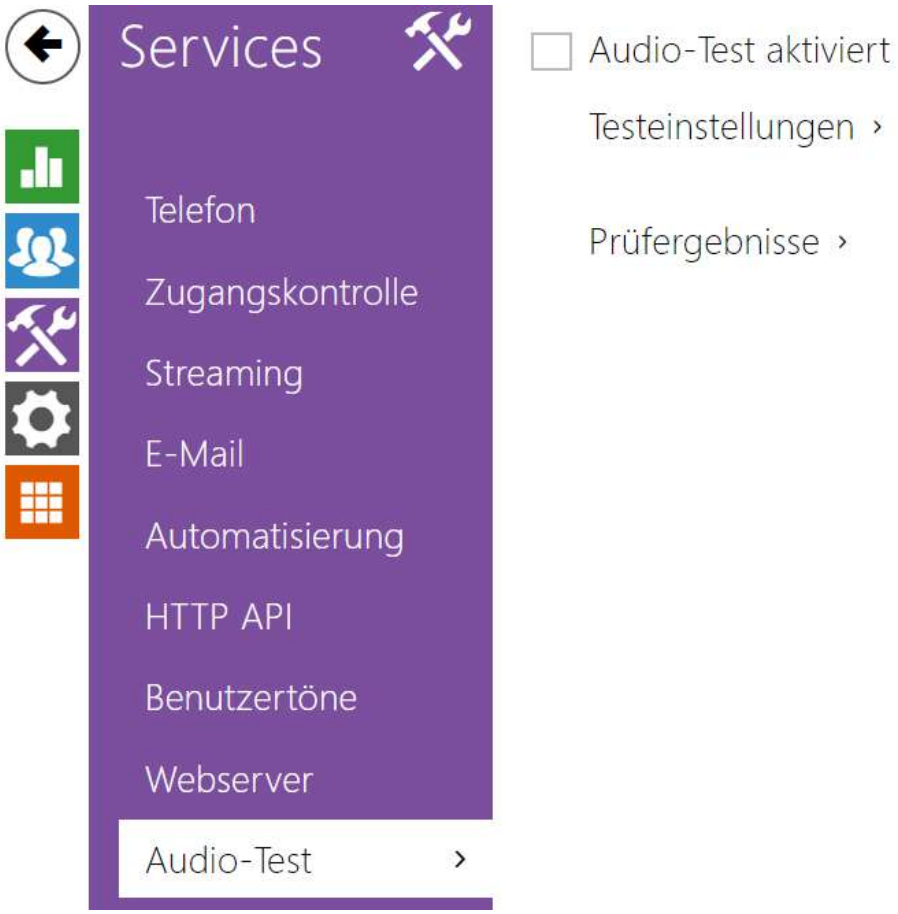
- Der **HTTP-Port** – Stellt den Kommunikationsport des Webservers für die Kommunikation mittels des nicht gesicherten HTTP-Protokolls ein. Die Änderung des Ports wird erst nach einem Neustart das Gerät wirksam.
- Der **HTTPS-Port** – Stellt den Kommunikationsport des Webservers für die Kommunikation mittels des gesicherten HTTPS-Protokolls ein. Die Änderung des Ports wird erst nach einem Neustart das Gerät wirksam.
- **Niedrigste erlaubte TLS Version** – Gibt die niedrigste TLS-Version an, die eine Verbindung zu Geräten herstellen darf.
- **HTTPS-Benutzerzertifika**t – Stellt das Benutzerzertifikat und den persönlichen Code ein, mit welchem das Chiffrieren der Kommunikation zwischen dem HTTP-Server vom Zutrittsterminal und dem Webbrowser auf der Benutzerseite erfolgt. Man kann einen der drei Sätze der Nutzerzertifikate und privaten Schlüssel wählen, siehe Kapitel Zertifikate, oder die Einstellung **Self Signed** belassen, wo das automatisch generierte Zertifikat verwendet wird, das beim ersten Interkomstart erstellt wurde.
- **Fernzugriff aktiviert** – Ermöglicht den entfernten Zutritt zum Webserver das Gerät von IP-Adressen außerhalb des lokalen Netzes zu erlauben.

- **Originalsprache** – Ermöglicht aus der Anlage die Originaldatei herunterzuladen, die alle Texte der Nutzerschnittstelle in englischer Sprache enthält. Die Datei ist im Format XML siehe nachstehend.
- **Benutzersprache** – Ermöglicht das Hochladen, Herunterladen und optionale Löschen einer Benutzerdatei mit eigenen Übersetzungen der Texte der Benutzeroberfläche.

```
<?xml version="1.0" encoding="UTF-8"?>
<strings language="English" languageshort="EN">
  <!-- Global enums-->
  <s id="enum/error/1">Invalid value!</s>
  <s id="enum/bool_yesno/0">NO</s>
  <s id="enum/bool_yesno/1">YES</s>
  <s id="enum/bool_user_state/0">ACTIVE</s>
  <s id="enum/bool_user_state/1">INACTIVE</s>
  <s id="enum/bool_profile_state/0">ACTIVE</s>
  <s id="enum/bool_profile_state/1">INACTIVE</s>
  ..
  ..
  ..
</strings>
```

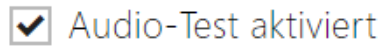
Bei der Übersetzung modifizieren Sie nur die Werte der Elemente **<s>** und ändern Sie nicht die Attributwerte **id**. Die Abkürzung der Sprache, die durch das Attribut **language** des Elements **<strings>** wird in der Parameterwahl Sprache der Web-Schnittstelle angeführt. Die Abkürzung der Sprache, die durch das Attribut **languageshort** des Elements **<strings>** gegeben ist, wird in der Liste der Sprachen in der rechten oberen Ecke des Fensters angeführt und dient zum schnelleren Umschalten zwischen den Sprachen.

5.4.10 Audio-Test

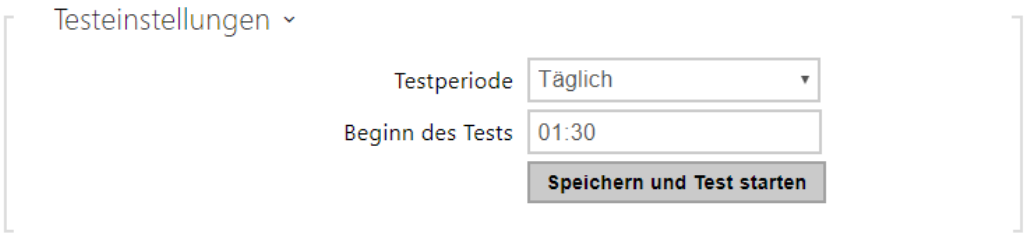


Modell **2N Access Unit QR** ermöglicht eine regelmäßige Kontrolle des eingebauten Lautsprechers und Mikrophons durchzuführen. Der Lautsprecher generiert im Verlauf des Tests einen oder mehrere kurze Töne. Der generierte Ton wird mittels des eingebauten Mikrophons aufgenommen und, wenn er richtig erkannt wird, wird der Test für erfolgreich erklärt. Die Testdauer beträgt ungefähr 4 s. Falls der Test nicht erfolgreich ist (was z.B. durch extremen umgebenden Lärm verursacht werden kann), wird er in 10 Minuten noch einmal wiederholt. Man kann das Ergebnis des letzten Tests in der Konfirmationsschnittstelle das Geräte anzeigen oder mittels **Automation** *verarbeiten.*

Parameterliste



- **Freigabe des Audiotests** – erlaubt das automatische Durchführen des Audiotests.



- **Testperiode** – ermöglicht die Periode der Durchführung des Tests einzustellen. Der Test kann automatisch einmal täglich oder einmal wöchentlich gestartet werden.
- **Uhrzeit des Teststarts** – ermöglicht die Uhrzeit einzustellen, zu der der Test regelmäßig durchgeführt werden soll. Die Uhrzeit kann man im Format HH:MM einstellen. Wir empfehlen Ihnen, eine solche Uhrzeit festzulegen, in der man nur die minimale Nutzung das Gerät erwarten kann.
- **Speichern und Test starten** – mittels der Taste können Sie den Test sofort starten, ohne Hinsicht auf die aktuelle Einstellung.

- **Teststatus** – zeigt durchgehend den Status des Testverlaufs an.
- **Letzter Testzeitpunkt** – zeigt die Uhrzeit des zuletzt durchgeführten Tests an.
- **Letztes Testergebnis** – zeigt das Ergebnis des zuletzt durchgeführten Tests an.

5.4.11 SNMP

Die 2N Zutrittseinheiten können integrieren die Funktionalität, die die entfernte Aufsicht der Zutrittseinheiten können im Netz mittels des SNMP-Protokolls ermöglicht. Das Gerät unterstützen das SNMP-Protokoll der Version 2c.

Parameterliste

- **SNMP aktiviert** – Ermöglicht Aktivierung dieser Funktion.

- **Community-Identifier** – Textkette, die den Zutrittscode für den Zutritt zu Objekten in der MIB-Tabelle repräsentiert.
- **IP-Adresse des Trap-Empfänger** – IP-Adresse, an die die SNMP-Traps gesendet werden.
- **MIB-Datei herunterladen** – Ermöglicht die aktuelle Definition der MIB-Tabelle von der Anlage herunterzuladen.

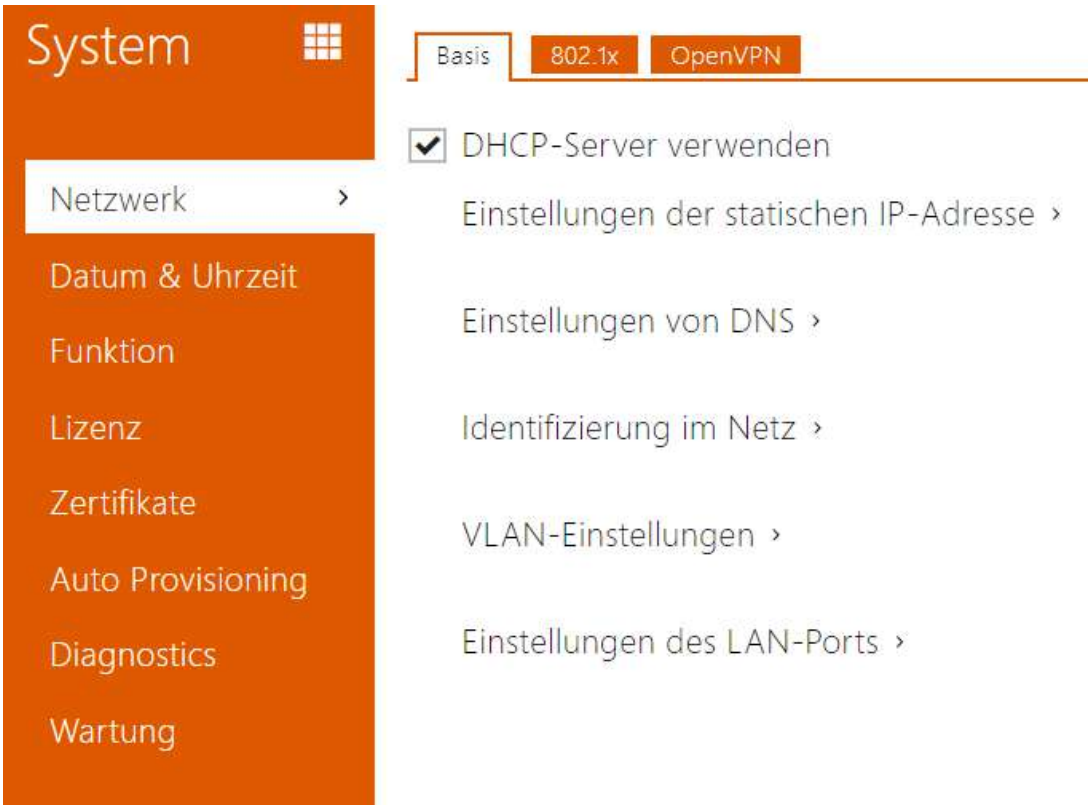
- **Kontakt** – Ermöglicht den Kontakt des Anlagenverwalters (z.B. Name, E-Mail u.Ä.) einzugeben.
- **Name** – Ermöglicht die Bezeichnung der Anlage einzugeben.
- **Standort** – Ermöglicht die Beschreibung der Anlagenunterbringung (z.B. 1. Etage) einzugeben.

- **IP-Adresse** – Ermöglicht es bis zu 4 gültige IP-Adressen für den Zutritt zum SNMP-Agent einzugeben. Der Zutritt von anderen Adressen wird gesperrt. Wenn das Feld unausgefüllt bleibt, kann man von einer beliebigen IP-Adresse auf die Anlage zugreifen.

5.5 System

Hier ist eine Übersicht dessen, was Sie im Kapitel finden:

5.5.1 Netzwerk



Die 2N Zutrittseinheiten schließt sich an das lokale Netz an und der richtigen Funktion wegen muss es die gültige IP-Adresse eingestellt haben bzw. es kann die IP-Adresse vom DHCP-Server in diesem Netz bekommen. Die IP-Adresse und die DCHP-Einstellung werden in der Registerkarte Netz konfiguriert.

Tipp

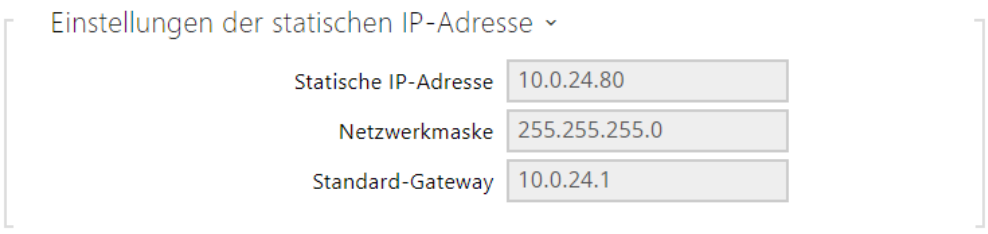
- *Wenn Sie die aktuelle IP-Adresse Ihres Interkoms erfahren wollen, können Sie die Applikation **2N IP Network Scanner** nutzen, die frei zum Herunterladen auf der Webseite 2N.com zu Verfügung steht, oder Sie können den Mechanismus anwenden, der im Installationshandbuch des jeweiligen Zutrittseinheiten angeführt ist.*

Wenn Sie in Ihrem Netz den RADIUS-Server und den Mechanismus der Überprüfung der angeschlossenen Geräte, der von den Protokollen 802.1x ausgeht, nutzen, können Sie das Gerät so konfigurieren, dass es die Authentifizierung EAP-MD5 oder EAP-TLS anwendet. Der Einstellung dieser Funktion dient die Registerkarte 802.1x.

In der Registerkarte Trace können Sie das Abfangen der eingehenden und ausgehenden Pakete auf der Netzschnittstelle das Geräte starten. Die Datei mit den abgefangenen Paketen kann man herunterladen und nachfolgend z.B. mithilfe der Applikation Wireshark (www.wireshark.org) verarbeiten.

Parameterliste

- **DHCP-Server verwenden** – Erlaubt das automatische Erwerben der IP-Adresse vom DHCP-Server im lokalen Netzt. Wenn es in Ihrem Netz keinen DHCP-Server gibt oder man ihn aus einem anderen Grund nicht benutzen kann, verwenden Sie die manuelle Netzeinstellung.



- **Statische IP-Adresse** – Statische IP-Adresse das Gerät. Die Adresse wird gemeinsam mit den nachstehenden Parametern angewendet, wenn der Parameter DHCP-Server anwenden nicht eingestellt ist.
- **Netzwerkmaske** – Stellt die Netzmaske ein.
- **Standard-Gateway** – Adresse der Default-Gateway, die die Kommunikation mit Anlagen außerhalb des lokalen Netzes ermöglicht.

- **Primäres DNS** – Adresse des primären DNS-Servers für die Übersetzung der Domainnamen in IP-Adressen. Im Fall der Wiederherstellung des Default-Zustandes des Geräts wird der primäre DNS-Servers auf die Adresse 8.8.8.8 eingestellt.
- **Sekundäres DNS** – Adresse des sekundären DNS-Servers, der in dem Fall angewendet wird, wenn der primäre DNS-Server nicht erreichbar ist. Im Fall der Wiederherstellung des Default-Zustandes des Geräts wird der sekundäre DNS-Servers auf die Adresse 8.8.4.4 eingestellt.

- **Hostname** – Einstellung der Identifikation das Gerät im Netz.
- **Identifikator des Herstellers** – Legt die Hersteller-ID als Zeichenfolge für DHCP Option 60 fest.

- **VLAN aktiviert** – Schaltet die Unterstützung des virtuellen Netzes (VLAN gemäß Empfehlung 802.1q) ein. Der einwandfreien Funktion wegen ist es ebenfalls erforderlich, die ID des virtuellen Netzwerks einzustellen.
- **VLAN ID** – Gewählte ID des virtuellen Netzes im Umfang 1-4094. Die Anlage wird nur mit dieser ID markierte Pakete empfangen. Im Fall einer ungeeigneten Einstellung kann es zum Anschlussverlust kommen und nachfolgend muss man die Anlage mittels der Fabrikeinstellung in die Voreinstellung zurücksetzen.

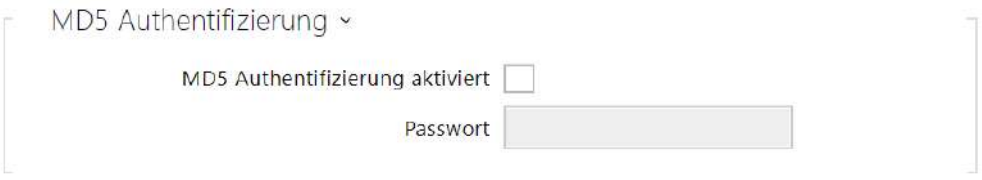
- **Gewünschte Port-Modus** – Bevorzugter Modus des Netzschnittstellenports (Automatisch oder Half Duplex – 10 mbps). Ermöglicht die Übertragungsgeschwindigkeit dann auf 10 Mbps zu senken, wenn die verwendete Netzinfrastruktur (Verkabelung) für den Betrieb mit 100 Mbps nicht zuverlässig ist.
- **Aktueller Portzustand** – Aktueller Status des Netzschnittstellenports Half oder Full Duplex – 10 mbps oder 100 mbps).

Registerkarte 802.1x

Hinweis

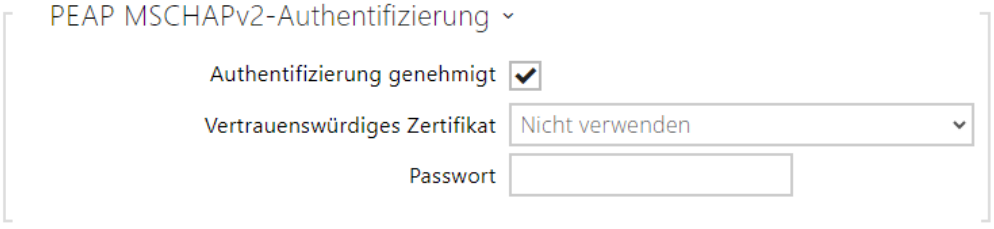
- Änderungen an den Authentifizierungseinstellungen werden nach einem Neustart des Geräts wirksam.

- **Identität des Gerätes** – Nutzername (Identität) für die Authentifizierung mittels der Methoden EAP-MD5 und EAP-TLS.



- **MD5 Authentifizierung aktiviert** – Erlaubt die Anwendung der Anlagenauthentifizierung im Netz mittels des Protokolls 802.1x EAP-MD5. Aktivieren Sie diese Funktion nicht, wenn Ihr Netz nicht 802.1x unterstützt. Im anderen Fall wird Ihr Interkom unerreichbar.
- **Passwort** – Zutrittspasswort, das für die Authentifizierung mittels der Methode EAP-MD5 angewendet wird.

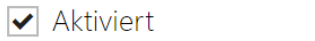
- **TLS Authentifizierung aktiviert** – Erlaubt die Anwendung der Anlagenauthentifizierung im Netz mittels des Protokolls 802.1x EAP-TLS. Aktivieren Sie diese Funktion nicht, wenn Ihr Netz nicht 802.1x unterstützt. Sonnst können Sie nicht mehr auf Ihres Gerät zugreifen.
- **Vertrauenswürdiges Zertifikat** – Spezifiziert den Satz der Zertifikate der Zertifizierungsautoritäten für die Überprüfung der Gültigkeit des öffentlichen Zertifikats des RADIUS-Servers. Man kann eine der drei Gruppen der Zertifikate auswählen; siehe Kapitel Zertifikate. Wenn das Zertifikat der Zertifizierungsautorität nicht angeführt ist, wird das öffentliche Zertifikat des RADIUS-Servers nicht verifiziert.
- **Benutzerzertifikat** – Spezifiziert das Nutzerzertifikat und den privaten Schlüssel, mit Hilfe deren die Berechtigung des Zutrittsterminals verifiziert wird, im lokalen Netz auf dem Port des Netzelementes zu kommunizieren, das mittels 802.1x gesichert ist. Man kann einen der drei Sätze der Nutzerzertifikate und privaten Schlüssel wählen, siehe Kapitel Zertifikate.



- **Authentifizierung genehmigt** – Genehmigt die die Verwendung der Geräteauthentifizierung im Netzwerk mit Hilfe des Protokolls 802.1x EAP-TLS. Aktivieren Sie diese Funktion nicht, wenn Ihr LAN 802.1x nicht unterstützt. Aktivieren Sie diese dennoch, können Sie nicht mehr auf Ihres Gerät zugreifen.
- **Vertrauenswürdiges Zertifikat** – gibt das CA-Zertifikat zum Überprüfen der Gültigkeit des öffentlichen Zertifikats des RADIUS-Servers an. Wenn nicht angegeben, wird das öffentliche Zertifikat des RADIUS-Servers nicht überprüft.
- **Passwort** – Das Passwort, das für die Authentifizierung durch die PEAP MSCHAPv2-Methode verwendet wird.

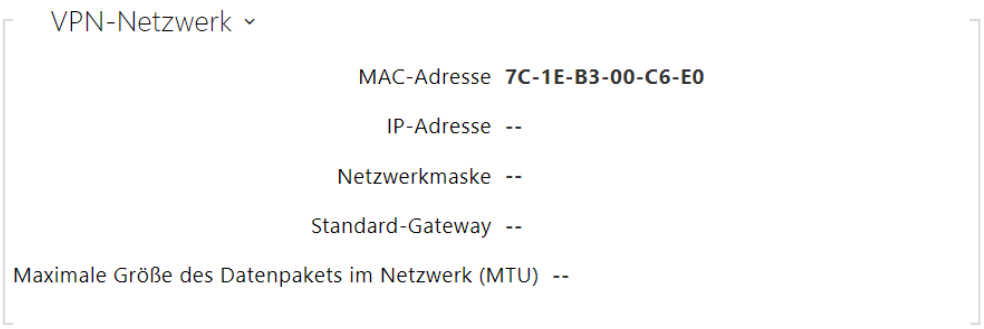
Registerkarte OpenVPN

Über OpenVPN kann das Gerät an ein anderes Netzwerk angeschlossen werden.



- **Aktiviert** – Schaltet das virtuelle Privatnetz (VPN) ein.

- **Default Schnittstelle** – falls aktiviert, wird aller ausgehende Netzbetrieb außerhalb der Lokalnetzmaske zur VPN-Schnittstelle geleitet.
- **Server-Adresse** – adresse des OpenVPN-Servers.
- **Server-Port** – port des OpenVPN-Servers.
- **Vertrauenswürdiges Zertifikat** – legt die Gruppe von Zertifikaten fest, die von den Zertifizierungsbehörden herausgegeben werden, um die öffentliche Zertifikatsgültigkeit des OpenVPN-Servers zu überprüfen. Man kann eine der drei Gruppen der Zertifikate auswählen; siehe hierzu den Unterabschnitt Zertifikate. Wird kein Zertifikat der Zertifizierungsautorität angeführt, wird das öffentliche Zertifikat des OpenVPN-Servers nicht verifiziert.
- **Client-Zertifikat** – spezifiziert die Gruppe der Client-Zertifikate für Überprüfung der Identität des Clients durch OpenVPN-Server. Man kann eine der drei Gruppen der Zertifikate auswählen; siehe hierzu den Unterabschnitt Zertifikate. Wird kein Client-Zertifikat angeführt, wird die Identität des OpenVPN-Clients nicht verifiziert.
- **Status** – zeigt den Zustand der Anschließung an OpenVPN an. Angeschlossen/Abgetrennt.
- **Fehler** – zeigt den Fehlertyp der Anschließung an OpenVPN an, falls aufgetreten.
- **Start** – schließt das Gerät an OpenVPN an.
- **Stop** – trennt das Gerät vom OpenVPN ab.



- **VPN-Netzwerk** – zeigt Basisinformationen über VPN an.

Tipp

- Detaillierte Informationen über Einstellung des OpenVPN-Servers und -Clients finden Sie im Abteil FAQ.

5.5.2 Datum und Uhrzeit

Wenn Sie die Einstellung der Zeitprofile für die Codes für das Einschalten der Schalter u.Ä. verwenden, müssen das interne Datum und die Uhrzeit im Zutrittseinheiten richtig eingestellt sein.

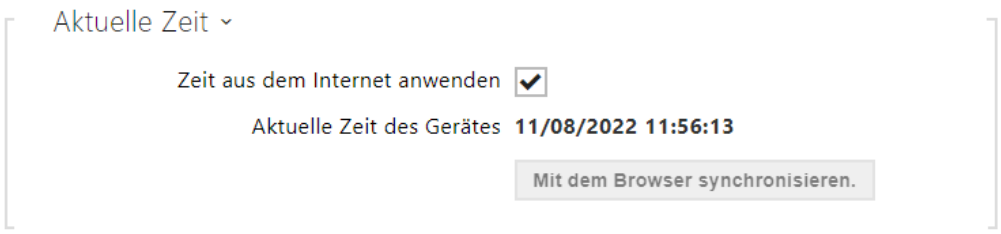
Die 2N Zutrittseinheiten sind mit einer Echtzeit-Backup-Uhr ausgestattet, mit der Sie einen Stromausfall für mehrere Tage überbrücken können. Die Zeit kann jederzeit mit der Internetzeit synchronisiert werden, indem die Funktion **Aktuelle Zeit aus dem Internet verwendet** oder mit

der aktuellen Zeit auf dem PC über die Schaltfläche **Synchronisieren im Browser** synchronisiert wird.

> **Anmerkung**
>
> - *Die richtige Datum- und Uhrzeiteinstellung ist für die Grundfunktion das Gerät nicht unerlässlich. Das aktuelle Datum und die aktuelle Uhrzeit sind für die richtige Funktion der Zeitprofile und für das richtige Anzeigen der Uhrzeit der Ereignisse in verschiedenen Listen (Syslog, Eintragungen über angelegte Karten, Log der Anlage, der mittels **2N HTTP API** heruntergeladen wird u.Ä.) erforderlich.*

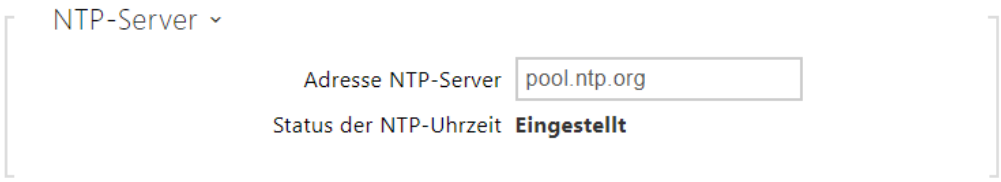
Bei normalen Betriebsbedingungen ist die Genauigkeit des Kreises der realen Zeit im Gerät ungefähr ±0,005 %, was einen Fehler bis ±2 Minuten/Monat bedeuten kann. Für maximale Genauigkeit und Zuverlässigkeit empfehlen wir immer die Verwendung der Funktion **Aktuelle Uhrzeit aus dem Internet verwenden**.

Parameterliste



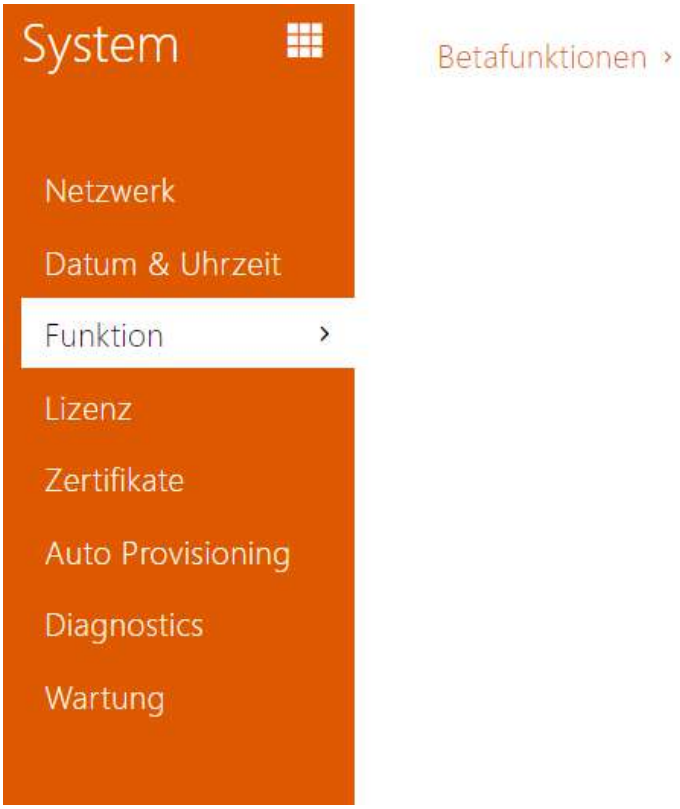
- **Zeit aus dem Internet anwenden** – Aktiviert die Nutzung des NTP-Servers für die Zeitsynchronisierung des Gerätes.
- **mit dem Browser synchronisieren** – Sie können die Uhrzeit im Gerät jederzeit mit der aktuellen Uhrzeit in Ihrem PC mittels der Taste synchronisieren.

- **Automatische Erkennung** – legt fest, ob die Zeitzone vom My2N-Dienst automatisch erkannt wird. Wenn die automatische Erkennung deaktiviert ist, wird die Einstellung im Parameter Manuelle Auswahl (manuell ausgewählte Zeitzone oder benutzerdefinierte Regel) verwendet.
- **Erkannte Zeitzone** – zeigt die automatisch erkannte Zeitzone an. Zeigt N/A an, wenn der Dienst nicht verfügbar oder deaktiviert ist.
- **Manuelle Auswahl** – legt die Zeitzone für den Installationsstandort des Geräts fest. Die Einstellung bestimmt die Zeitverschiebung und die Wechsel zwischen Sommerzeit und Winterzeit.
- **Eigene Regel** – wird das Gerät an einem Standort installiert, der nicht im Zeitzonenparameter enthalten ist, muss die Zeitzone manuell eingestellt werden. Die Regel wird nur angewendet, wenn der Zeitzonenparameter manuell eingestellt wird.



- **NTP-Server nutzen** – Erlaubt die Verwendung des NTP-Servers für die Synchronisierung der internen Zeit das Gerät. Weder die Server-IP-Adresse noch der Domänenname können eingestellt werden, wenn die Funktion „**Internetzeit verwenden**“ deaktiviert ist.
- **Adresse NTP-Server** – Stellt die IP-Adresse oder den Domainnamen des NTP-Servers ein, gemäß dem das Gerät die interne Uhrzeit synchronisiert.

5.5.3 Funktion



Zeigt eine Liste der veröffentlichten Beta-Funktionen für Benutzertests an.
In der Liste ist angeführt:

- Bezeichnung der Funktion,
- den Funktionsstatus, der angibt, ob die Funktion läuft oder angehalten wurde,
- eine Aktion zum Starten oder Stoppen der Funktion.

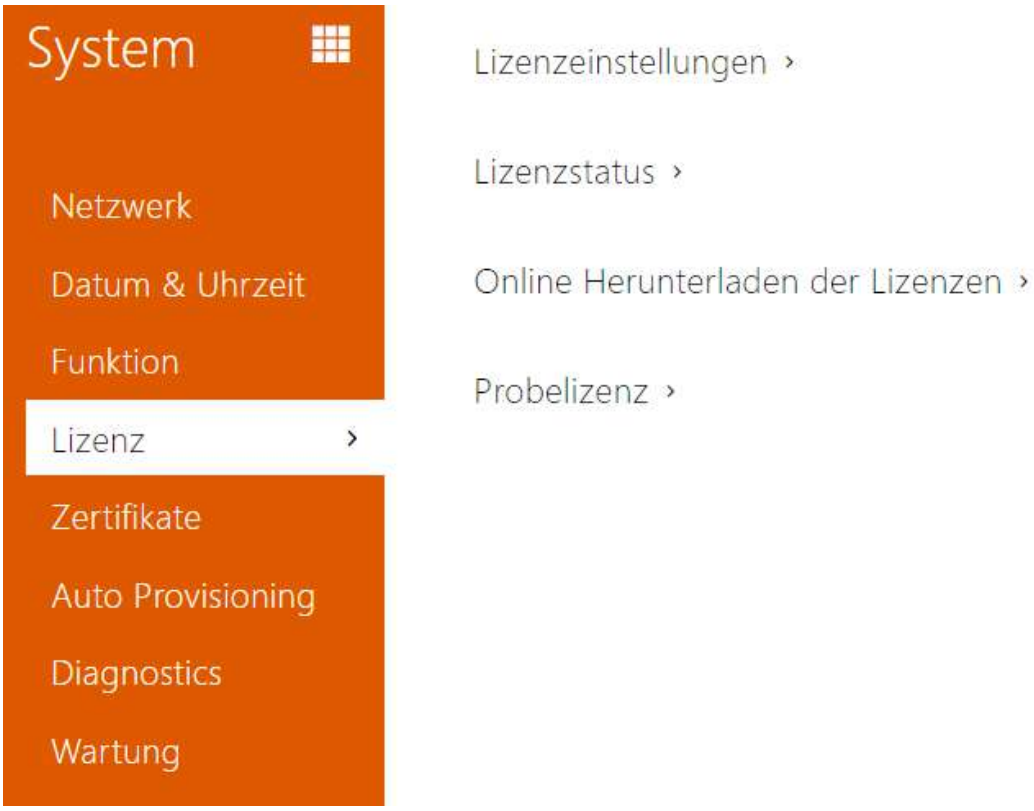
Aktivierung oder Deaktivierung der Funktion erfolgt erst nach einem Neustart des Geräts. Bis zum Neustart des Geräts kann die Anforderung der Zustandsänderung mit der Aktion **Abbrechen** rückgängig gemacht werden.

Bemerkung

- Testeigenschaften sind nicht garantiert und die Gesellschaft 2N TELEKOMUNIKACE a.s.haftet nicht für Funktionseinschränkungen und etwaige, infolge der Einschränkung der Beta-Funktionen entstandenen Schäden. Die Beta-Funktionen werden nur zu Testzwecken bereitgestellt.

Bezeichnung der Betafunktion	Beschreibung
Passwortgeschützte Konfigurationsdatei	Mit dieser Funktion kann die Konfigurationsdatei während des Backups mit einem Passwort verschlüsselt werden (siehe 5.5.8 Wartung). Beim Hochladen einer Konfigurationsdatei auf das Gerät ist ein Passwort erforderlich, mit dem die Konfigurationsdatei gesichert wird. Wenn das Passwort nicht übereinstimmt, wird die Konfigurationsdatei nicht auf das Gerät hochgeladen.
Multifaktor-Prüfung der Kennzeichen	Wenn diese Funktion aktiviert ist, erscheint die Option Multifaktor unter Dienste > Zutrittskontrolle > Zugangsregeln > Erweiterte Einstellungen > Erkennung von Kennzeichen. Der Zugriff wird erst gestattet, wenn mindestens zwei Authentifizierungsmethoden kombiniert wurden, je nach den Einstellungen der Zugriffsregel. Nach dem Erkennen des Kennzeichens ist es erforderlich, innerhalb von 60 Sekunden die nächste Authentifizierungsmethode einzugeben.

5.5.4 Lizenz

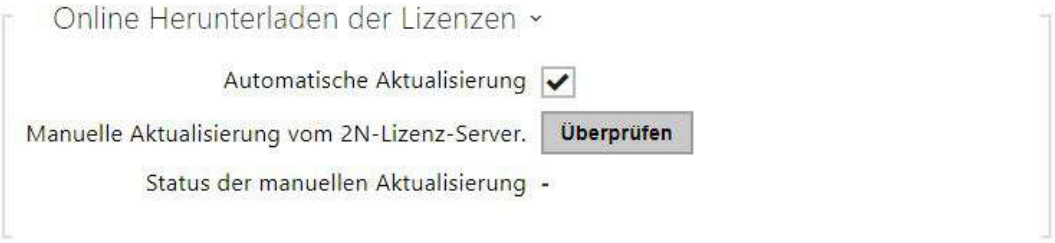


Einige Funktionen die 2N Zutrittseinheiten können. Sind nur nach der Eingabe des gültigen Lizenzschlüssels verfügbar. Die Liste der möglichen Lizenzierung der Zutrittseinheiten können finden Sie im Kapitel **Lizenzierte Funktionen**.

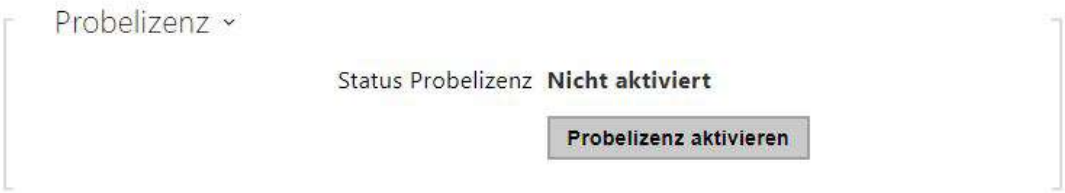
Parameterliste

- **Seriennummer** – Zeigt die Seriennummer der Anlage an, für die die Lizenz gültig ist.
- **Lizenzschlüssel** – Ermöglicht den gültigen Lizenzcode einzugeben.
- **Lizenzschlüssel ist gültig** – Zeigt an, ob der eingegebene Lizenzschlüssel gültig ist.

- **Standardlizenz** – zeigt eine Liste der Lizenzen an, die dem Gerät ab Werk beiliegen.
  - **Erweiterte Sicherheit** – Zeigt an, ob Funktionen verfügbar sind, die durch die Lizenz Enhanced Security aktiviert wurden.
  - **NFC-Support** – Zeigt an, ob die NFC-Funktion verfügbar ist
  - **Erweiterte Integration** – Zeigt an, ob Funktionen verfügbar sind, die durch die Lizenz Enhanced Security aktiviert wurden.
  - **Unterstützung der Aufzugsteuerung** – Zeigt an, ob die Funktion der aktivierten Lift Module Lizenz verfügbar ist.



- **Automatische Aktualisierung** – Die Anlage aktualisiert den Lizenzschlüssel über den Lizenzserver 2N.
- **Manuelle Aktualisierung** – Manuelle Anfrage betreffend die Überprüfung der Lizenzverfügbarkeit.
- **Status der manuellen Aktualisierung** – Läuft, aktualisiert, nicht spezifiziert., Fehler: Lizenz nicht vorhanden.



- **Status Probelizenz** – Zeigt den Status der Trial-Lizenz (nicht aktiviert, aktiviert, Gültigkeit abgelaufen) an.
- **Lizenzablauf** – Zeigt die restliche Laufzeit der Trial-Lizenz an.

5.5.5 Zertifikate

Manche 2N Netzleistungen des Zutrittseinheiten nutzen für die Kommunikation mit anderen Geräten im Netz das gesicherte TLS-Protokoll. Dieses Protokoll verhindert, dass der Inhalt der Kommunikation von Dritten abgehört ggf. zu modifiziert wird. Beim Anknüpfen der Verbindung mittels des TLS-Protokolls läuft eine einseitige bzw. beidseitige Authentifizierung, die Zertifikate und private Codes erfordert.

Leistungen des Zutrittseinheiten, die das TLS-Protokoll nutzen:

1. Webserver (HTTPS-Protokoll)
2. E-Mail (SMTP-Protokoll)
3. 802.1x (EAP-TLS-Protokoll)
4. SIPs

Mit 2N Zutrittseinheiten u können Sie Zertifikatsätze von Zertifizierungsstellen hochladen, mit denen die Identität des Geräts überprüft wird, mit dem die Sprechanlage kommuniziert, und gleichzeitig persönliche Zertifikate und private Schlüssel hochladen, um die Kommunikation zu verschlüsseln.

Jeder Leistung des Zutrittsterminals, die Zertifikate verlangt, können Sie einen der Zertifikatsätze zuordnen, siehe die Kapitel **Webserver**, **E-mail** und **Streaming**. Die Zertifikate können durch mehrere Dienste geteilt werden.

2N Zutrittseinheiten:

- akzeptiert Zertifikate in den Formaten DER (ASN1) und PEM.
- unterstützt die AES-, DES- und 3DES-Verschlüsselung.
- unterstützt Algorithmen:
  - RSA-Schlüsselgröße bis zu 2048 Bit für vom Benutzer hochgeladene Zertifikate; intern bis zu 4096-Bit-Schlüssel (beim Verbinden - Zwischenzertifikate und gleichwertige Zertifikate)
  - Elliptic Curves

Hinweis

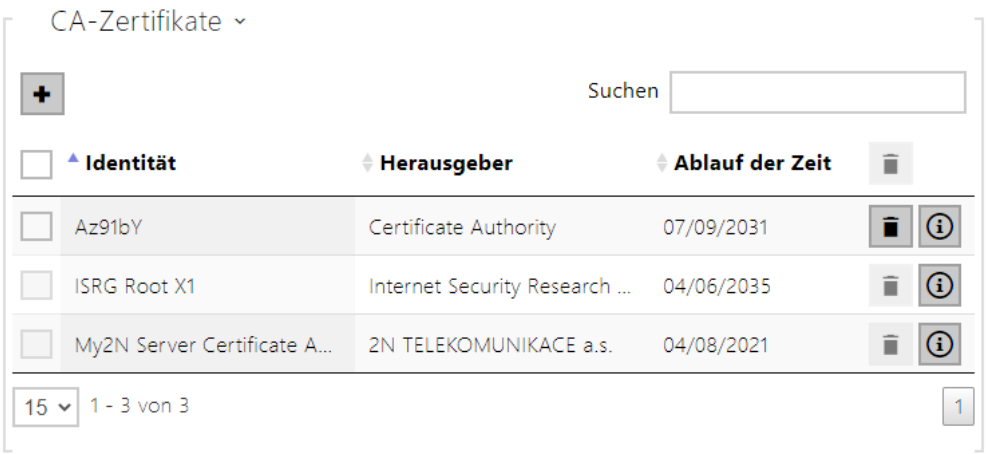
- CA-Zertifikate müssen das X.509 v3-Format verwenden.

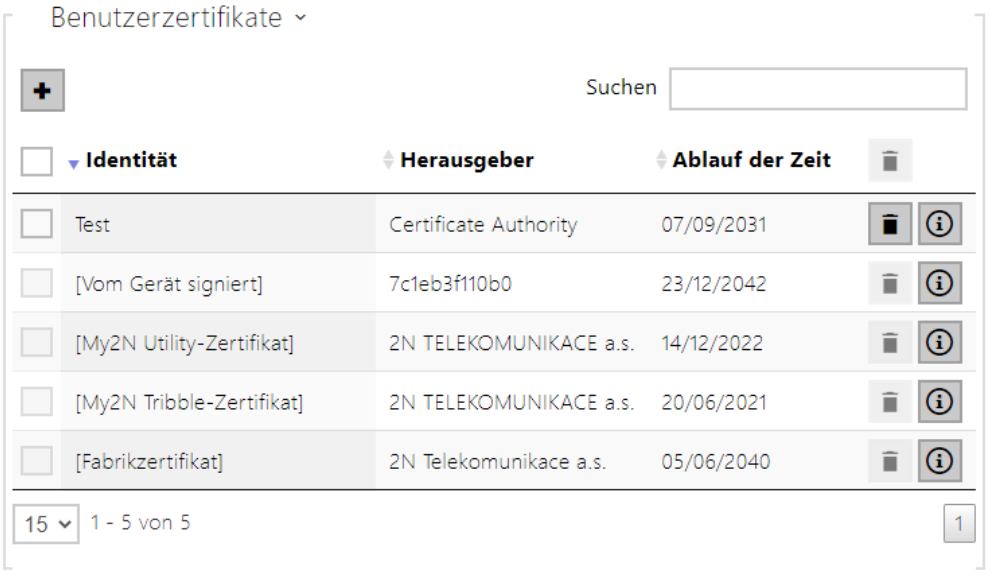
Beim ersten Anschluss der Einspeisung an den Zutrittseinheiten werden automatisch das sog. **Self Signed Zertifikat** und der **private Schlüssel** generiert, den man für den Dienst **Webserver** und **E-Mail** verwenden kann, ohne die Notwendigkeit ein eigenes Zertifikat und den privaten Schlüssel hochladen zu müssen.

Anmerkung

Falls Sie das Self Signed Zertifikat für die Verschlüsselung der Kommunikation zwischen dem Webserver des Zutrittseinheiten und dem Webbrowser verwenden, ist die Kommunikation abgesichert, aber der Webbrowser wird sie darauf hinweisen, dass er die Glaubwürdigkeit des Zertifikats des Zutrittseinheiten nicht überprüfen kann.

Die aktuelle Übersicht der hochgeladenen Zertifikate von Zertifizierungsstellen und persönlichen Zertifikaten wird auf zwei Registerkarten angezeigt:





Durch das Drücken der Taste  können Sie das Zertifikat in die Anlage hochladen, das in Ihrem PC gespeichert ist. Im Dialogfenster kann die ID des Zertifikats zur Identifizierung bei seiner Auswahl, Korrektur oder Löschung ausgefüllt werden. Die ID darf max. 40 Zeichen lang sein, sie kann kleine und große Alphabet-Zeichen, Ziffern und die Zeichen '_' a '-' enthalten. Die ID ist nicht obligatorisch. Wählen Sie im Dialogfenster die Datei mit dem Zertifikat (ggf. dem privaten Schlüssel) und drücken Sie die Taste **Hochladen**. Durch Drücken der Taste  entfernen Sie das Zertifikat aus dem Gerät. Durch das Drücken der Taste  werden die Informationen zum Zertifikat angezeigt.

Hinweis

- Nach dem Aktualisieren der Firmware oder dem Neustart ändert das Gerät das **selbstsignierte** Zertifikat in ein neues. Das auf dem Gerät angezeigte Zertifikat muss mit dem Zertifikat auf der Website überprüfen und vergleichen werden, ob sie identisch sind.

Hinweis

Im Fall der Zertifikate, die von elliptischen Kurven ausgehen, kann man nur die Kurven secp256r1 (aka prime256v1 aka NIST P-256) und secp384r1 (aka NIST P-384) verwenden.

5.5.6 Aktualisierung

Mit 2N Zutrittseinheiten können Sie die Firmware und Konfiguration gemäß den angegebenen Regeln aus dem Repository auf dem von Ihnen definierten TFTP- oder HTTP-Server automatisch herunterladen und aktualisieren.

Die Adresse des TFTP und HTTP-Servers kann manuell konfiguriert werden. Das Gerät unterstützt die automatische Adressenerkennung mithilfe eines lokalen DHCP-Servers (Option 66).

My2N

- **My2N aktiviert** – erlaubt den Anschluss an den Dienst My2N ggf. an einen anderen ACS-Server.

- **Seriennummer** – zeigt die Seriennummer des Geräts an, für das der My2N-Code gültig ist.
- **My2N Security Code** – zeigt den vollen Code an, der zur Aktivierung der Applikation dient.

Zeigt Informationen zum Verbindungsstatus des Geräts zu My2N an.

- **My2N ID** – einzigartiger Identifikator der Gesellschaft, der mittels des My2N-Portals erstellt wurde.

Registerkarte Firmware

In dieser Registerkarte wird das automatische Herunterladen der Firmware vom durch Sie definierten Server eingestellt. Der Zutrittsterminal vergleicht in eingestellten Intervallen die Datei auf dem Server mit der aktuellen Firmware und im Fall, dass die Firmware auf dem Server neuer ist, führt es die automatische Aktualisierung einschließlich des Neustarts des Zutrittsterminals (ca.30 s) durch. Wir empfehlen deshalb die Aktualisierung zeitlich so einzustellen, dass sie in der Zeit der minimalen Interkomnutzung (z.B. in der Nacht) stattfindet. Die

2N Zutrittseinheiten erwartet auf Servern Dateien mit den Bezeichnungen:

1. **MODEL**-firmware.bin – Firmware des Zutrittseinheiten
2. **MODELL**-common.xml – gemeinsame Konfiguration aller Zutrittseinheiten des jeweiligen Modells
3. **MODELL**-**MACADDR**.xml – spezifische Konfiguration für einen Zutrittseinheiten

MODELL in der Bezeichnung der Datei spezifiziert das Gerätmodell:

1. **au – 2N Access Unit**
2. **aug2 – 2N Access Unit 2.0**
3. **aum – 2N Access Unit M**
4. **auqr - 2N Access Unit QR**

MACADDR ist die MAC-Adresse das Gerät im Format 00-00-00-00-00-00. Die MAC-Adresse des Zutrittseinheiten ist auf dem Herstellerschild oder direkt in der Schnittstelle in der Registerkarte **Status** zu finden.

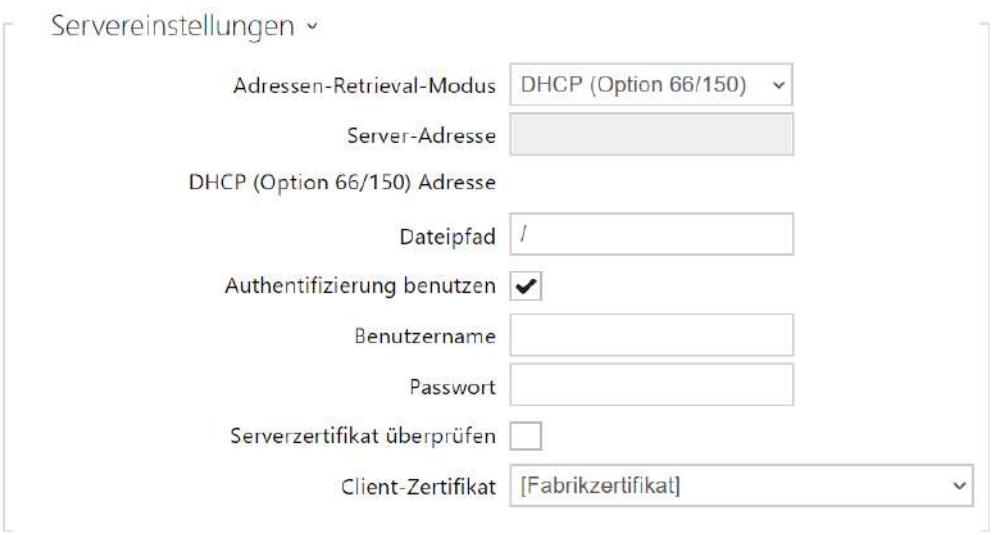
Beispiel:

2N Access Unit 2.0 mit der MAC-Adresse 00-87-12-AA-00-11 wird vom TFTP-Server Dateien mit diesen Bezeichnungen herunterladen:

- aug2-firmware.bin
- aug2-common.xml
- aug2-00-87-12-aa-00-11.xml

Parameterliste

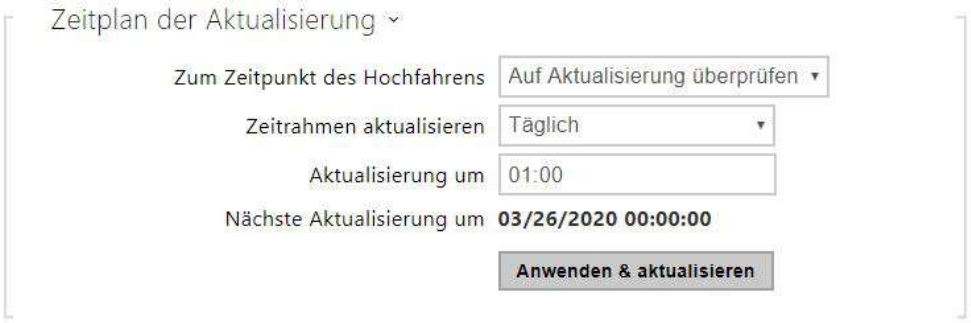
- **Aktualisierung der Firmware aktiviert** – Erlaubt das automatische Herunterladen der Firmware/Konfiguration vom TFTP/HTTP-Server.



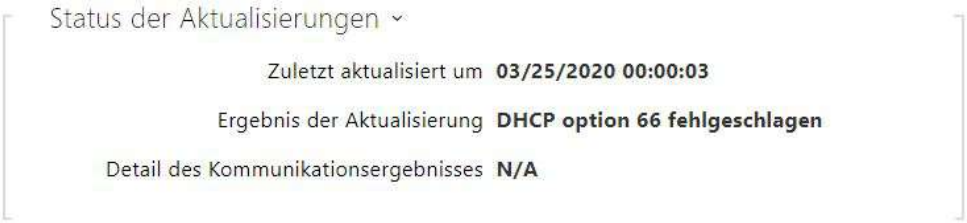
- **Adresse Datenabrufmodus** – Ermöglicht zu wählen, ob die Adresse des TFTP/HTTP-Servers manuell eingegeben wird oder ob man die Adresse verwendet, die automatisch vom DHCP-Servers mittels des Parameters Option 66 übermittelt wurde.
- **Server-Adresse** – Ermöglicht manuell die Adresse des TFTP-Servers einzugebentftp://ip_adresa), HTTP (http://ip_adresa) oder HTTPS (https://ip_adresa).
- **DHCP (Option 66/150) Adresse** – Zeigt die Adresse an, die mittels DHCP Option 66 oder 150 übermittelt wurde.
- **Dateipfad** – legen Sie den Pfad zum Firmware-Ordner fest. Geben Sie / ein, um nach model-firmware.bin (spezifisches Modell) im Stammverzeichnis des Servers zu suchen. Details zu Modellen usw. finden Sie in der Seitenleiste (?).
- **Authentifizierung benutzen** – Ermöglicht die Anwendung der Authentifizierung für den Zutritt zum HTTP-Server einzustellen.
- **Benutzername** – Der Nutzername, der für die Authentifizierung auf dem Server benutzt wurde.
- **Passwort** – Das Passwort, dass für die Authentifizierung auf dem Server benutzt wurde.
- **Serverzertifikat überprüfen** – überprüft das öffentliche Zertifikat des ACS-Servers anhand der auf das Gerät hochgeladenen CA-Zertifikate.
- **Client-Zertifikat** – gibt das Kundenzertifikat und den privaten Schlüssel an, mit denen die Berechtigung der Sprechanlage zur Kommunikation mit dem ACS-Server überprüft wird.

Bemerkung

- Das Gerät enthält Factory Cert Zertifikat, ein unterzeichnetes Zertifikat, das z. B. zur Integrierung mit British Telecom verwendet werden kann.



- **Zum Zeitpunkt des Hochfahrens** – Erlaubt die Kontrolle oder die Durchführung der Aktualisierung nach jedem Start des Zutrittseinheiten.
- **Zeitrahmen aktualisieren** – Stellt die Periode der Aktualisierung ein. Automatische Aktualisierung kann man einmal stündlich, täglich, wöchentlich oder monatlich einstellen, oder die Periode manuell einstellen.
- **Aktualisierung um** – Ermöglicht die Uhrzeit im Format HH:MM einzustellen, in der regelmäßig die Aktualisierung durchgeführt werden soll. So kann man die Durchführung der Aktualisierung zu der Uhrzeit einstellen, in der der Zutrittseinheiten am wenigsten genutzt wird. Der Parameter wird nicht angewendet, wenn die Aktualisierungsperiode so eingestellt ist, dass sie kürzer als ein Tag ist.
- **Nächste Aktualisierung um** – Zeigt die Uhrzeit der weiteren geplanten Aktualisierung an.



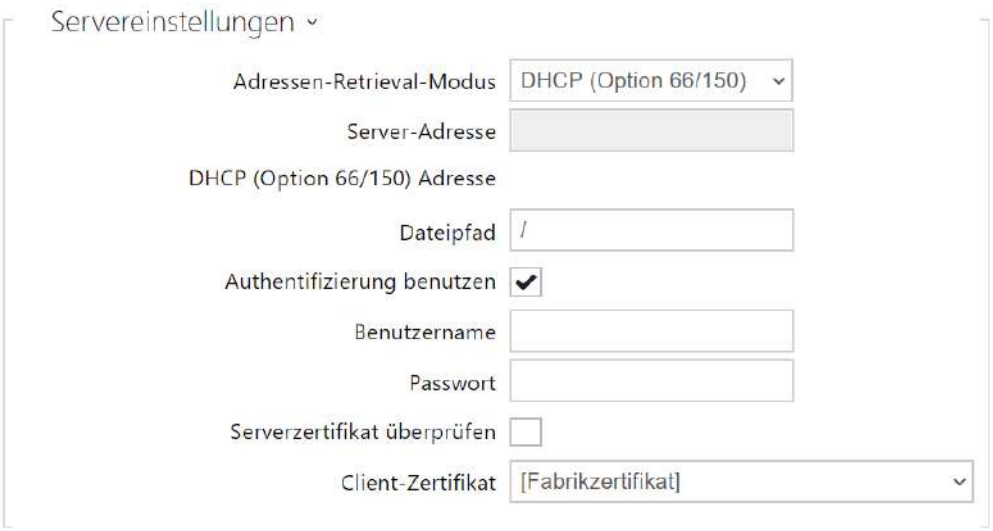
- **Zuletzt aktualisiert um** – Zeigt die Uhrzeit der zuletzt durchgeführten Aktualisierung an.
- **Ergebnis der Aktualisierung** – Zeigt das Ergebnis der zuletzt durchgeführten Aktualisierung an. Nachfolgend sind die möglichen Werte aufgeführt: DHCP option 66 failed, Firmware is up to date, Server connection failed, Running..., File not found.
- **Detail des Kommunikationsergebnisses** – Fehlercode bezüglich der Kommunikation mit dem Server oder Status des Protokollcodes TFTP/HTTP.

Ergebnis	Beschreibung
Läuft...	Synchronisierung gerade läuft
Aktualisiert	Konfiguration/Firmware wurde fehlerfrei aktualisiert Nach Herunterladen der Firmware kommt es in wenigen Sekunden zum Neustart des Geräts.
Firmware ist aktuell	Der Versuch neue Firmware herunterzuladen hat gezeigt, dass die Gerätefirmware aktuell ist.
Server nicht erreichbar	Es ist nicht gelungen, die Serveradresse mittels DHCP Option 66 oder 150 einzulesen.
Ungültiger Domainname	Domainname des Servers ist nicht gültig, bzw. der DNS-Server ist fehlerhaft konfiguriert oder nicht erreichbar.
Server nicht erreichbar	Der angefragte HTTP/TFTP-Server antwortet nicht.
Herunterladen fehlgeschlagen	Beim Herunterladen der Datei ist ein weiter nicht spezifizierter Fehler aufgetreten
Datei nicht gefunden	Die Datei wurde auf dem Server nicht gefunden
Datei ist ungültig	Die Datei, die herunterladen werden soll, ist beschädigt oder falschen Typs.

Registerkarte Konfiguration

In dieser Registerkarte wird das automatische Herunterladen der Konfiguration vom durch Sie definierten Server eingestellt. Das Gerät wird in eingestellten Abständen die Datei vom Server herunterladen und sich rekonfigurieren. Bei dieser Aktualisierung wird der Zutrittseinheiten nicht neugestartet.

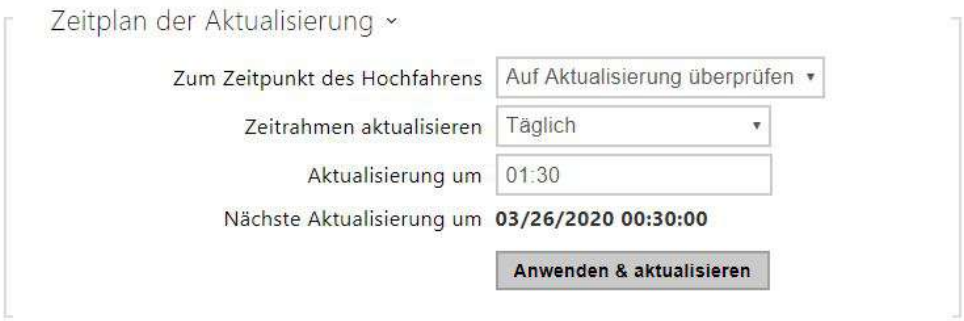
- **Aktualisierung der Konfiguration aktiviert** – Erlaubt das automatische Herunterladen der Firmware/Konfiguration vom TFTP/HTTP-Server.



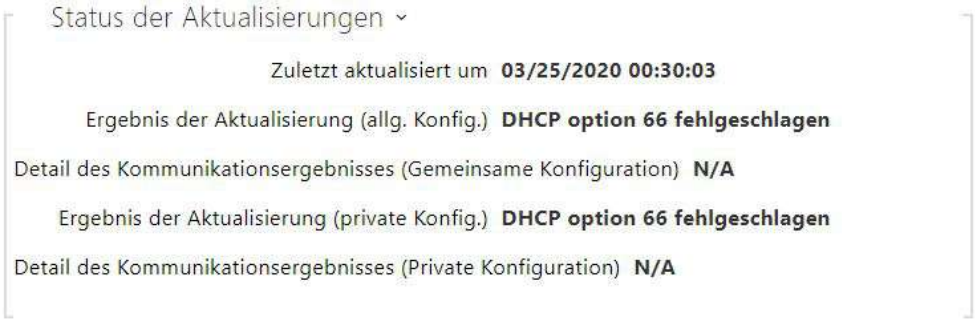
- **Adressen-Retrieval-Modus** – Ermöglicht zu wählen, ob die Adresse des TFTP/HTTP-Servers manuell eingegeben wird oder ob man die Adresse verwendet, die automatisch vom DHCP-Servers mittels des Parameters Option 66 übermittelt wurde.
- **Server-Adresse** – Ermöglicht manuell die Adresse des TFTP-Servers einzugebentftp://ip_adresa), HTTP (http://ip_adresa) oder HTTPS (https://ip_adresa).
- **DHCP (Option 66) Adresse** – Zeigt die Adresse an, die mittels DHCP Option 66 oder 150 übermittelt wurde.
- **Dateipfad** – Stellt das Verzeichnis bzw. die Vorsilbe der Dateibezeichnung mit der Firmware oder Konfiguration auf dem Server ein. Das Interkom erwartet Dateien mit den Bezeichnungen XhipY_firmware.bin, XhipY-common.xml a XhipY-MACADDR.xml, wo X das Präfix ist, das durch diesen Parameter gegeben ist, und Y das Gerätmodell spezifiziert.
- **Authentifizierung benutzen** – Ermöglicht die Anwendung der Authentifizierung für den Zutritt zum HTTP-Server einzustellen.
- **Benutzername** – Der Nutzername, der für die Authentifizierung auf dem Server benutzt wurde.
- **Passwort** – Das Passwort, dass für die Authentifizierung auf dem Server benutzt wurde.
- **Serverzertifikat überprüfen** – überprüft das öffentliche Zertifikat des ACS-Servers anhand der auf das Gerät hochgeladenen CA-Zertifikate.
- **Client-Zertifikat** – gibt das Kundenzertifikat und den privaten Schlüssel an, mit denen die Berechtigung der Sprechanlage zur Kommunikation mit dem ACS-Server überprüft wird.

Bemerkung

- Das Gerät enthält Factory Cert Zertifikat, ein unterzeichnetes Zertifikat, das z. B. zur Integrierung mit British Telecom verwendet werden kann.



- **Zum Zeitpunkt des Hochfahrens** – Erlaubt die Kontrolle oder die Durchführung der Aktualisierung nach jedem Gerätstart.
- **Zeitrahmen aktualisieren** – stellt die Periode der Aktualisierung ein. Automatische Aktualisierung kann man einmal stündlich, täglich, wöchentlich oder monatlich einstellen, oder die Periode manuell einstellen.
- **Aktualisierung um** – Ermöglicht die Uhrzeit im Format HH:MM einzustellen, in der regelmäßig die Aktualisierung durchgeführt werden soll. So kann man die Durchführung der Aktualisierung zu der Uhrzeit einstellen, in der das Gerät am wenigsten genutzt wird. Der Parameter wird nicht angewendet, wenn die Aktualisierungsperiode so eingestellt ist, dass sie kürzer als ein Tag ist.
- **Nächste Aktualisierung um** – Zeigt die Uhrzeit der weiteren geplanten Aktualisierung an.



- **Zuletzt aktualisiert um** – Zeigt die Uhrzeit der zuletzt durchgeführten Aktualisierung an.
- **Ergebnis der Aktualisierung (allg. Konfig.)** – zeigt das Ergebnis der zuletzt durchgeführten gemeinsamen Aktualisierung an. Nachfolgend sind die möglichen Werte

aufgeführt: DHCP option 66 failed, Firmware is up to date, Server connection failed, Running..., File not found.

- **Detail des Kommunikationsergebnisses(Gemeinsame Konfiguration)** – Fehlercode bezüglich der Kommunikation mit dem Server oder Status des Protokollcodes TFTP/HTTP.
- **Ergebnis der Aktualisierung (Private Konfiguration)** – Die private Konfigurierung erfolgt erst nach Aktualisierung der gemeinsamen Konfiguration. En Gerät mit privaten Konfiguration wird nach MAC-Adresse identifiziert. Zeigt das Ergebnis der zuletzt durchgeführten Aktualisierung an. Nachfolgend sind die möglichen Werte aufgeführt: DHCP option 66 selhal, Firmware is up to date, Server connection failed, Running..., File not found.
- **Detail des Kommunikationsergebnisses(Private Konfiguration)** – Fehlercode bezüglich der Kommunikation mit dem Server oder Status des Protokollcodes TFTP/HTTP.

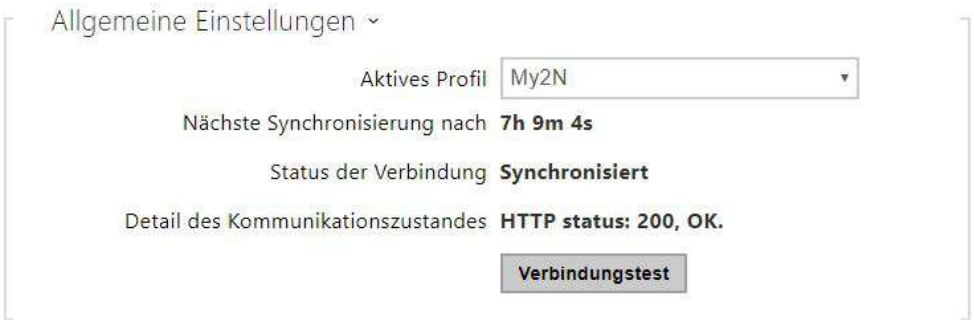
Registerkarte My2N / TR069

Auf dieser Registerkarte wird die Fernverwaltung von Geräten über das TR-069-Protokoll aktiviert und konfiguriert. Das Protokoll TR-069 ermöglicht zuverlässig die Gerätparameter zu konfigurieren, die Konfiguration wiederherzustellen und eine Sicherheitskopie zu erstellen ggf. ein Update der Firmware der Anlage durchzuführen.

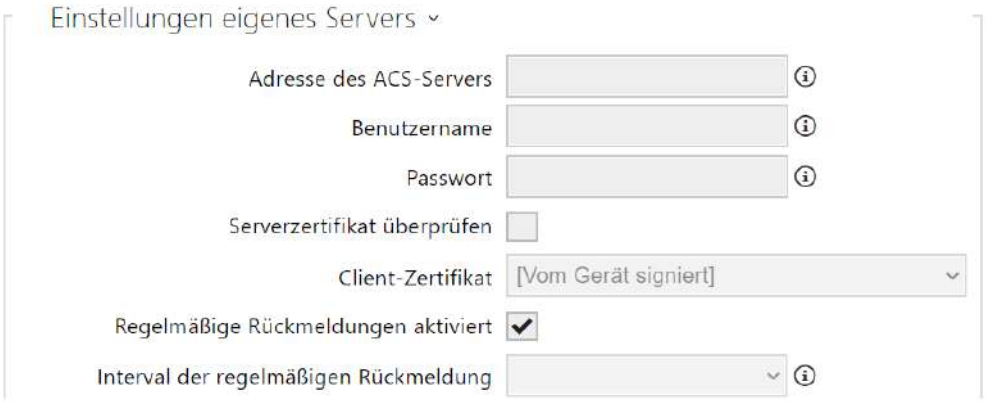
Das Protokoll TR-069 wird durch den Cloud-Dienst My2N genutzt. Für die richtige Funktion das Gerät mit My2N muss man immer die Leistung TR-069 freigeben und den Parameter aktives Profil auf den Wert My2N einstellen. Danach wird sich das Gerät periodisch zum Dienst My2N anmelden, der es konfigurieren kann.

Diese Funktion ermöglicht das Interkom an ihren eigenen ACS (Auto Configuration Server) anzuschließen. In diesem Fall ist die Verbindung zu My2N auf dem Gerät deaktiviert.

- **My2N/TR069 aktiviert** – Aktiviert die Verbindung zum My2N-Dienst bzw. zu einem anderen ACS-Server.



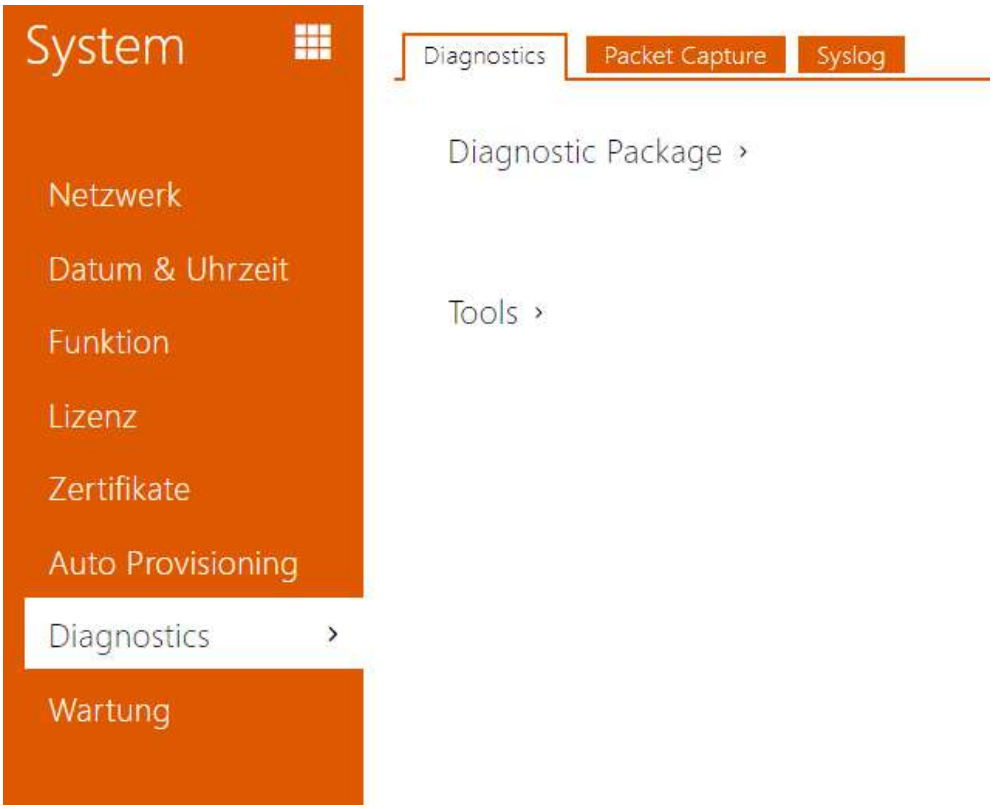
- **Aktives Profil** – Ermöglich eines der voreingestellten Profile (des ACS-Servers) zu wählen ggf. die eigene Einstellung und den Anschluss an den ACS-Server manuell zu konfigurieren.
- **Nächste Synchronisierung nach** – Zeigt an, wie lange es dauern wird, bis das Gerät Kontakt mit dem entfernten ACS-Server aufnehmen wird.
- **Status der Verbindung** – Zeigt den aktuellen Staus des Anschlusses an den ACS-Server ggf. die Beschreibung des Fehlerstatus an.
- **Detail des Kommunikationszustandes** – Fehlercode bezüglich der Kommunikation mit dem Server oder Status des Protokollcodes TFTP/HTTP.
- **Verbindungstest** – Testet die Verbindung zum TR069-Dienst gemäß dem festgelegten Profil (siehe Aktives Profil). Das Testergebnis wird im Feld Anschlussstatus angezeigt.



- **Adresse des ACS-Servers** – Stellt die Adresse des ACS-Servers im Format ipadresse[: port] ein, z.B.. 192.168.1.1:7547.
- **Benutzername** – Stellt den Nutzernamen für die Authentifizierung das Gerät auf dem ACS-Server ein.
- **Passwort** – Stellt das Nutzerpasswort für die Authentifizierung das Gerät auf dem ACS-Server ein.
- **Serverzertifikat überprüfen** – spezifiziert den Satz der Zertifikate der Zertifizierungsautoritäten für die Überprüfung der Gültigkeit des öffentlichen Zertifikats des ACS-Servers. Man kann eine der drei Gruppen der Zertifikate auswählen; siehe Kapitel Zertifikate. Ist kein Zertifikat der Zertifizierungsautorität angeführt, wird das öffentliche Zertifikat des ACS-Servers nicht verifiziert.
- **Client-Zertifikat** – spezifiziert das Nutzerzertifikat und den privaten Schlüssel, mit Hilfe deren die Berechtigung das Gerät verifiziert wird, mit dem ACS-Server zu kommunizieren. Man kann einen der drei Sätze der Nutzerzertifikate und privaten Schlüssel wählen, siehe Kapitel Zertifikate.
- **Regelmäßige Rückmeldungen aktiviert** – Erlaubt die periodische Anmeldung das Gerät zum ACS-Server.

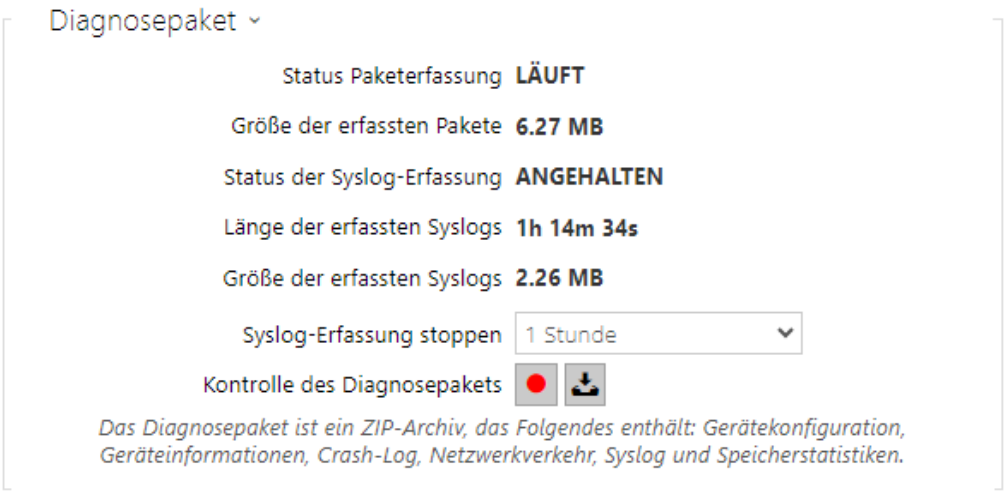
- **Interval der regelmäßigen Rückmeldung** – Stellt das Intervall der periodischen Anmeldung zum ACS-Server ein, wenn es mittels des Parameters **Regelmäßige Rückmeldungen aktiviert** erlaubt ist.

5.5.7 Diagnostik



Registerkarte Diagnostik

Die Schnittstelle ermöglicht die Erfassung von Diagnoseprotokollen, die dann heruntergeladen und an den technischen Support gesendet werden können. Die erfassten Diagnoseprotokolle helfen bei der Identifizierung und Behebung der gemeldeten Probleme. Die Protokolle enthalten Informationen über das Gerät, seine Konfiguration, den Netzwerkverkehr, das Crash-Protokoll und die Speicherstatistik.

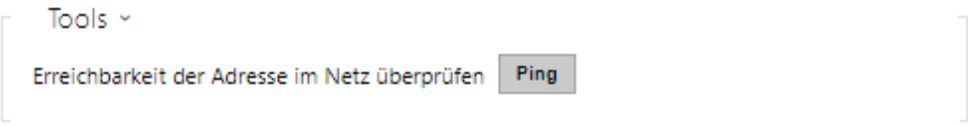


- **Status Paketerfassung** – zeigt an, ob die Paketerfassung im Bookmark Paketaufzeichnung läuft.
- **Größe der erfassten Pakete** – zeigt an, wie viele Pakete erfasst wurden.
- **Status der Syslog-Erfassung** – zeigt an, ob die Erfassung von Syslog-Nachrichten im Bookmark Syslog läuft.
- **Länge der erfassten Syslogs** – zeigt an, wie lange Syslog-Nachrichten im Bookmark Syslog erfasst werden.
- **Größe der erfassten Syslogs** – zeigt an, wie viele Syslog-Meldungen erfasst sind.
- **Syslog-Erfassung stoppen** – legt den Zeitraum fest, für den die Daten erfasst werden sollen.

Die Erfassung wird mit der Aufnahmetaste gestartet  . Beim erneuten Drücken der Aufnahmetaste wird die Erfassung neu gestartet und läuft erneut. Die Datei mit den erfassten Paketen kann über die Taste  heruntergeladen werden.

Hinweis

- Beim Starten der Diagnosedatenerfassung wird die Paketerfassung neu gestartet, wenn sie bereits läuft.



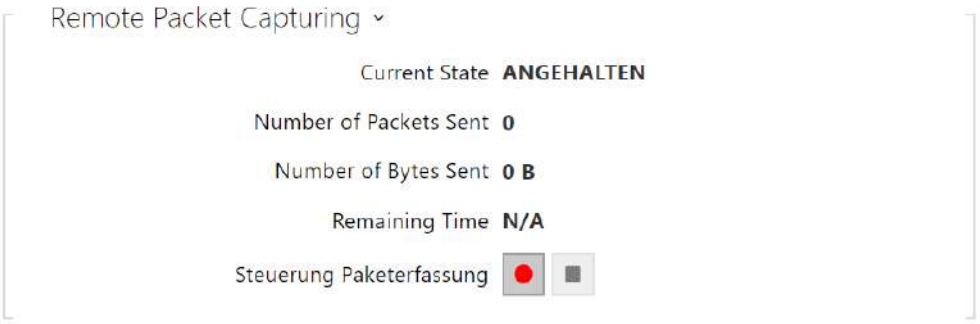
- **Erreichbarkeit der Adresse im Netz überprüfen** – dient der Überprüfung der Verfügbarkeit der jeweiligen Adresse im Netz als Befehl „Ping“ in üblichen Operationssystemen. Nach dem Drücken der Taste „Ping“ erscheint ein Dialog, in dem man diese IP-Adresse oder den Domainnamen eingeben und durch das Drücken der Taste

„Ping“ Prüfdaten an diese Adresse absenden kann. Wenn die eingegebene IP-Adresse oder der Domainname ungültig sind, wird ein Hinweis angezeigt und die Taste „Ping“ ist solange inaktiv, solange die eingegebene Adresse nicht gültig wird.
Im Dialog werden ferner der Status der Funktion und das Ergebnis angezeigt. Der Status „Fehlgeschlagen“ („Failed“) kann entweder die Nichterreichbarkeit der eingegebenen Adresse innerhalb von 10 Sekunden oder die Unmöglichkeit den Domainnamen in die Adresse zu übersetzen bedeuten. Wenn eine gültige Antwort empfangen wird, werden die IP-Adresse, von der diese Antwort kam, und die Länge des Wartens auf die Antwort in Millisekunden angezeigt.
Durch erneutes Drücken der Taste „Ping“ wird eine weitere Anfrage an die gleiche Adresse geschickt

Registerkarte Paketerfassung

In der Registerkarte Paketerfassung können Sie das Abfangen der eingehenden und ausgehenden Pakete auf der Netzschnittstelle das Gerät starten. Erfasste Pakete können lokal im Puffer der4-MB-IP-Sprechanlage, oder remote auf dem PC des Benutzers gespeichert werden. Die Datei mit den aufgezeichneten Paketen kann heruntergeladen und z. B. mit der Anwendung Wireshark (www.wireshark.org) weiterverarbeitet werden.

Wenn der Puffer während der lokalen Erfassung voll ist, werden die ältesten gespeicherten Pakete automatisch überschrieben. Beim lokalen Erfassen von Paketen empfehlen wir, die Bitrate der Videoübertragung auf unter 512 kbps zu reduzieren. Sie können das Abfangen mittels der Taste  starten, mittels der Taste  stoppen und die Datei mit den abgefangenen Paketen mittels der Taste  herunterladen.



Mit der Taste  können Sie die Fernaufnahme starten. Es ist notwendig, die Zeit (s) anzugeben, während der ein- und ausgehende Pakete erfasst werden sollen. Nach Ablauf des eingestellten Zeitwerts wird die Datei mit den erfassten Paketen automatisch auf den PC des Benutzers heruntergeladen. Sie können die Aufnahme mit der Taste  stoppen.

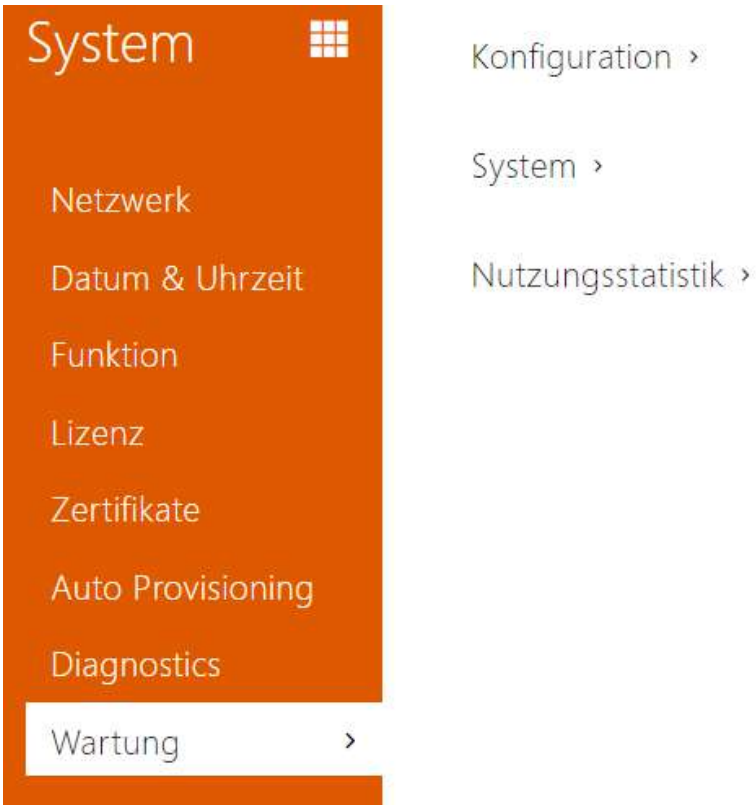
Registerkarte Syslog

Des 2N Zutrittseinheiten ermöglicht Systemnachrichten, die wichtige Informationen über den Status und die Prozesse der Anlage enthalten, an den Syslog-Server abzusenden, wo diese Nachrichten aufgezeichnet und für weitere Analysen und das Audit der betrachteten Anlage benutzt werden können. Im normalen Betrieb des Zutrittseinheiten muss man diese Leistung nicht konfigurieren.

- **Syslog-Meldung schicken** – Erlaubt das Absenden von Systemnachrichten an den Syslog-Server. Für die richtige Funktion muss die gültige Serveradresse eingestellt sein.
- **Server-Adresse** – legen Sie die IP[:Port] oder MAC-Adresse des Servers fest, auf dem die Anwendung läuft, um Syslog-Nachrichten zu erfassen.
- **Prioritätsstufe** – Legen Sie die Detailstufe für ausgehende Nachrichten fest (Error, Warning, Notice, Info, Debug 1–3). Das Niveau der Nachrichten Debug 1–3 ist nur dann empfehlenswert einzustellen, wenn es die Lokalisierung des Problems laut technischer Unterstützung erfordert.

Allgemeine Übersicht der lokalen Syslog-Nachrichten.

5.5.8 Wartung



Dieses Menü dient der Wartung der Konfiguration und der Firmware des Zutrittsterminals. Ermöglicht die Sicherheitskopie der Einstellung aller Parameter zu erstellen und diese wiederherzustellen, die Firmware des Zutrittsterminals zu aktualisieren ggf. alle Parameter des Zutrittsterminals in die Voreinstellung zurückzusetzen.

- **Konfiguration wiederherstellen** – Dient der Wiederherstellung der Konfiguration aus der vorherigen Sicherheitskopie. Nach dem Drücken der Taste wird ein Dialogfenster angezeigt, in dem Sie die Datei mit der Konfiguration wählen und in die Anlage hochladen können. Vor dem Hochladen der Datei auf das Gerät können Sie wählen, ob Sie die allgemeinen Einstellungen aus der Konfigurationsdatei übernehmen, das Verzeichnis importieren, Netzwerkeinstellungen und Zertifikate importieren oder die Verbindung zur SIP-Vermittlungsstelle aufbauen möchten.

- **Konfiguration Back-up** – Sichert die aktuelle vollständige Konfiguration des Zutrittsterminals. Nach dem Drücken der Taste kommt es zum Herunterladen der kompletten Konfiguration, die Sie in Ihrem PC speichern können.

Hinweis

- *Die Konfiguration des Zutrittsterminals kann empfindliche Daten, wie die Telefonnummern der Nutzer und die Zutrittspasswörter enthalten, gehen Sie deshalb mit der Datei umsichtig um.*

- **Konfiguration Reset** – Dient der Zurücksetzung aller Parameter des Zutrittsterminals in die Voreinstellung, mit Ausnahme der Parameter der Netzeinstellung. Wenn Sie den Zutrittsterminal in die volle Voreinstellung zurücksetzen wollen, benutzen Sie die jeweilige Verbindung oder die Taste Reset, siehe Installationshandbuch zum jeweiligen Zutrittsterminal.

Hinweis

- *Die Wiederherstellung der Voreinstellung löscht den eventuell hochgeladenen Lizenzschlüssel. Es wird somit empfohlen, ihn durch das Kopieren an einem anderen Speicherplatz für den späteren Bedarf aufzubewahren.*
- *Der Lizenzschlüssel wird bei einem HW-Reset (d.h. einem Reset über eine Taste am Gerät) nicht gelöscht, wenn die automatische Update-Funktion (System / Lizenz) aktiviert ist, die den Lizenzschlüssel vom 2N-Lizenzserver aktualisiert. Ein Software-Reset setzt alle Parameter auf die Betriebseinstellungen zurück, außer Zertifikate und Netzwerkeinstellungen.*

Bemerkung

- Die Funktionalität, Zuverlässigkeit und Sicherheit des Geräts hängen von der installierten Firmware ab. Das regelmäßige Aktualisieren der Firmware auf die aktuelle Version ist Teil der Nutzungsbedingungen des Produkts. Fehler, die durch die Verwendung einer veralteten Firmware-Version verursacht werden, können nicht reklamiert werden. Die aktuelle Firmware setzt Kundenerfahrungen und Anforderungen im Bereich der Sicherheit von personenbezogenen Daten um.

- **Firmware-Upgrade** – Dient dem Hochladen einer neuen Firmware in den Zutrittsterminal. Nach dem Drücken der Taste erscheint ein Dialogfenster, in dem Sie die Datei mit der Firmware wählen können, die für Ihren Zutrittsterminal bestimmt ist. Nach erfolgreichem Firmware-Upload wird der Zutrittsterminal automatisch neu gestartet. Nach dem Neustart ist es voll mit der neuen Firmware verfügbar. Der ganze Aktualisierungsprozess dauert weniger als eine Minute. Sie können die aktuelle Firmwareversion für Ihren Zutrittsterminal an der Adresse www.2n.com erwerben. Die Firmwareaktualisierung beeinflusst nicht die Konfiguration. Das Interkom kontrolliert die Datei der Firmware und verhindert, dass eine falsche oder beschädigte Datei hochgeladen wird.
- **Neustarten** – Führt Neustart des Zutrittsterminals durch. Der ganze Neustartprozess dauert ungefähr 30 s. Nach dem Ende des Neustarts, wenn der Zutrittsterminal seine IP Adresse erwirbt, wird das Anmeldefenster automatisch angezeigt.

Hinweis

Die Eintragung der Konfigurationsänderung des Interkoms wird in der Zeitspanne 3–15 s in Abhängigkeit von der Größe der jeweiligen Interkomkonfiguration durchgeführt. In dieser Zeit keinen Neustart des Interkoms durchführen.

- **Lizenz** – Nach dem Klicken auf die Taste Anzeigen wird ein Dialogfenster mit der Liste der angewendeten Lizenzen und der Software Dritter geöffnet. Es enthält auch den Link zum EULA-Dokument.

- **Daten für anonyme Nutzungsstatistiken senden** – Erlaubt das Absenden von anonymen statistischen Daten über die Nutzung der Anlage an den Hersteller. Diese Daten enthalten keine empfindlichen Informationen, wie z.B. Passwörter, Zutrittscodes und auch keine Telefonnummern. Die 2N TELEKOMUNIKACE a.s. verwendet diese Informationen zur

Verbesserung der Qualität, Zuverlässigkeit und Leistungsfähigkeit der Software. Die Teilnahme ist freiwillig und sie können das Absenden der statistischen Daten jederzeit widerrufen.

6. Zusatzinformationen

Hier ist eine Übersicht dessen, was Sie im Kapitel finden:

6.1 Problemlösung

Die häufigst gelöste Probleme finden Sie auf den Seiten faq.2n.cz.

6.2 Richtlinien, Gesetze und Verordnungen

2N Access Unit steht in Übereinstimmung mit folgenden Richtlinien und Bestimmungen:

- 2014/53/EU über Funkanlagen
- 2011/65/EU zur Beschränkung der Verwendung bestimmter gefährlicher Stoffe in Elektro- und Elektronikgeräten
- 2012/19/EU über Elektro- und Elektronik-Altgeräte

Industry Canada

Dieses Gerät der Klasse A entspricht den Anforderungen des kanadischen Standards ICES/ NMB-003.

FCC

Dieses Gerät wurde gemäß den Anforderungen für ein digitales Gerät der Klasse A, gemäß Abschnitt 15 der FCC-Bestimmungen zertifiziert.

ANM.: Der Zweck dieser Anforderungen besteht darin, einen angemessenen Schutz gegen schädliche Störungen in einer Wohnanlage zu schaffen. Dieses Gerät erzeugt, verwendet und strahlt möglicherweise Hochfrequenzenergie aus. Wenn es nicht gemäß den Anweisungen installiert und verwendet wird, kann es zu schädlichen Funkstörungen kommen.

Es kann jedoch nicht garantiert werden, dass es bei der gegebenen Installation zu keinen Störungen kommt. Wenn dieses Gerät eine schädliche Störung des Radio- oder Fernsehempfangs verursacht, was durch Aus- und Einschalten des Geräts festgestellt werden kann, kann der Benutzer versuchen, die Störung durch eine der folgenden Maßnahmen zu korrigieren:

- Die Empfangsantenne oder -leitung umleiten oder verlegen
- Den Abstand zwischen dem Gerät und dem Empfänger vergrößern
- Das Gerät an eine Steckdose aschließen, die sich in einem anderen Stromkreis befindet als der, an den der Empfänger angeschlossen ist

- Wenden Sie sich an den Händler oder einen erfahrenen Radio- / Fernsehtechniker

Änderungen oder Modifikationen an diesem Gerät, die nicht ausdrücklich von der für die Einhaltung verantwortlichen Partei genehmigt wurden, können zum Erlöschen der Betriebsberechtigung für dieses Gerät des Benutzers führen.

6.3 Allgemeine Anweisungen und Hinweise

Vor dem Gebrauch dieses Erzeugnisses lesen Sie, bitte, diese Gebrauchsanweisung aufmerksam durch und richten Sie sich nach den darin enthaltenen Hinweisen und Empfehlungen.

Verwendung des Produktes in Widerspruch zu dieser Gebrauchsanweisung kann zur ihrer mangelhafter Funktion oder Beschädigung oder Zerstörung führen.

Der Hersteller trägt keine Verantwortung für mögliche Schäden, verursacht durch eine andere Verwendung als in dieser Anleitung aufgeführt ist, also besonders durch falsche Verwendung, Nichteinhaltung der Hinweise und Warnungen.

Jede andere Verwendung oder Schaltanordnung als die in dieser Anleitung eingegebene Verfahren und Schaltungen ist als falsche betrachtet und der Hersteller trägt keine Verantwortung für die dadurch entstandene Folgen.

Der Hersteller haftet weiter nicht für eine Beschädigung, bzw. Zerstörung des Produktes, verursachte durch ungeeigneten Standort, Installierung, Bedienung oder Verwendung des Produktes in Widerspruch zu dieser Anleitung.

Der Hersteller trägt keine Verantwortung für mangelhafte Funktion, Beschädigung oder Zerstörung des Produktes infolge unsachgemäßen Austausches der Teilen oder Verwendung nicht originaler Ersatzteile.

Der Hersteller trägt keine Verantwortung für einen Verlust oder Beschädigung des Produktes durch eine Naturkatastrophe oder andere Natureinflüsse.

Der Hersteller trägt keine Verantwortung für eine Beschädigung des Produktes während des Transportes.

Der Hersteller gewährt keine Garantie für einen Datenverlust oder Datenbeschädigung.

Der Hersteller trägt keine Verantwortung für direkte oder indirekte Schäden, die durch Verwendung des Produktes in Widerspruch mit dieser Anleitung oder für sein Versagen infolge Verwendung in Widerspruch mit dieser Anleitung entstanden sind.

Bei der Installation und Verwendung des Produktes müssen gesetzliche Forderungen oder Bestimmungen der technischen Normen für Elektroinstallationen eingehalten werden. Der Hersteller trägt keine Verantwortung für eine Beschädigung oder Zerstörung des Produktes oder mögliche dem Kunden entstandene Schäden, falls mit dem Produkt in Widerspruch zu erwähnten Normen umgegangen wurde.

Der Kunde ist verpflichtet, auf eigene Kosten eine Softwaresicherung des Produktes sicher zu stellen. Der Hersteller trägt keine Verantwortung für Schäden, verursacht wegen mangelnder Sicherung.

Der Kunde ist verpflichtet, unmittelbar nach der Installation das Zugangswort zum Produkt zu ändern. Der Hersteller haftet für keine Schäden, die mit der Verwendung des ursprünglichen Passwortes entstehen.

Der Hersteller haftet auch für keine Mehrkosten, die dem Kunden durch Telefongespräche auf Linien mit erhöhtem Tarif entstehen.

Umgang mit Altelektrogeräten und gebrauchten Akkumulatoren

Gebrauchte Elektrogeräte und Akkumulatoren gehören nicht in den Hausmüll. Ihre ungerechte Entsorgung könnte zu Umweltschäden führen!

Die aus dem Haushalt stammende Elektrogeräte nach ihrer Brauchbarkeit, sowie gebrauchte aus Geräten herausgenommene Akkumulatoren sind in spezielle Sammelstellen abzugeben oder dem Verkäufer oder Hersteller zurückzugeben, der umweltgerechte Verarbeitung gewährleistet. Die Rückgabe ist kostenlos und an keinen Neukauf gebunden. Zurückgegebene Geräte müssen komplett sein.

Akkumulatoren niemals in Feuer werfen, weder abbauen noch kurzschließen.