Konfigurationshandbuch für 2N IP Interkoms

v.2.43

www.2n.com

Inhalt:

1. Produktbeschreibung

Die Tür-**Interkoms 2N IP** sind in der Lage das klassische Klingeltastentableau mit lautem Telefon und das ganze System der Kabelverteilungen, Klingeln und Haustelefone in Objekten zu ersetzen, in denen die Kabelleitungen der strukturierten Verkabelung installiert sind. Das Interkom gewährt viel bessere und breitere Dienste als übliche Haustelefone Die Installierung des Interkoms in Ihr Netz ist sehr einfach, es reicht es mittels eines UTP-Kabels an weitere Elemente des lokalen Netzes anzuschließen und die erforderlichen Parameter einzustellen.

Das Interkom kann dank des integrierten SIP-Protokolls sämtliche Dienste der VoIP-Netze nutzen – Rufumleitung bei Abwesenheit (auf einen anderen Arbeitsplatz, auf Anrufbeantworter oder Mobiltelefon) oder Anrufumschaltung (z.B. vom Sekretariat auf die konkrete gewünschte Person).

Die Interkoms sind mit optionaler Kurzwahltastenzahl ausgestattet, die es ermöglichen, den Anruf auf die Nummer des Nutzers aufzubauen, die vorher in der Nutzerliste im Interkom gespeichert wurde. Jeder Kurzwahltaste kann man bis drei Telefonnummern zuordnen, die man gleichzeitig oder nacheinander anrufen kann. Dank des integrierten Kalenders kann man einzelne Tasten so konfigurieren, dass der angerufene Teilnehmer jeweils erreicht wird oder im Gegenteil das Anrufen der ausgewählten Nummern außerhalb der festgelegten Zeit verhindert wird.

Einige Modelle des **Interkoms 2N IP** sind mit einer nummerischen Tastatur ausgestattet, die man als ein Codeschloss oder klassisches Tastentelefon benutzen kann.

Die **Interkoms 2N IP** ermöglichen den Nutzern im Netz das Geschehen vor der Kamera mittels des Video-Streaming-Dienstes zu beobachten. Dank der vollen Unterstützung des ONVIF-Standards können sie ein Bestandteil des Video-Surveillance-Systems in Ihrem Objekt werden.

Die **Interkoms 2N IP** können mit einem RFID-Kartenleser ausgestattet werden, der das Objekt nicht nur autorisierten Personen zugänglich macht, sondern gleichzeitig ein Bestandteil des Sicherheitssystems des Objektes oder des Anwesenheitssystems in Ihrer Firma ist.

Die **Interkoms 2N IP** sind mit einem Relaisschalter (optional mit weiteren Relais und Ausgängen) ausgestattet, mit dem man das elektrische Schloss oder ein anderes an das Interkom angeschlossene Gerät bedienen kann. Man kann im Interkom flexibel einstellen, wann und wie diese Schalter aktiviert werden sollen – mit einem Code, automatisch beim Anruf, durch das Drucken einer Kurzwahltaste u.Ä. Zur Erhöhung der Sicherheit wird immer empfohlen, das 2N® Sicherheitsrelais (Bestellnummer 9159010) zu verwenden.

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

Einstellung des Anschlusses an das lokale Netz

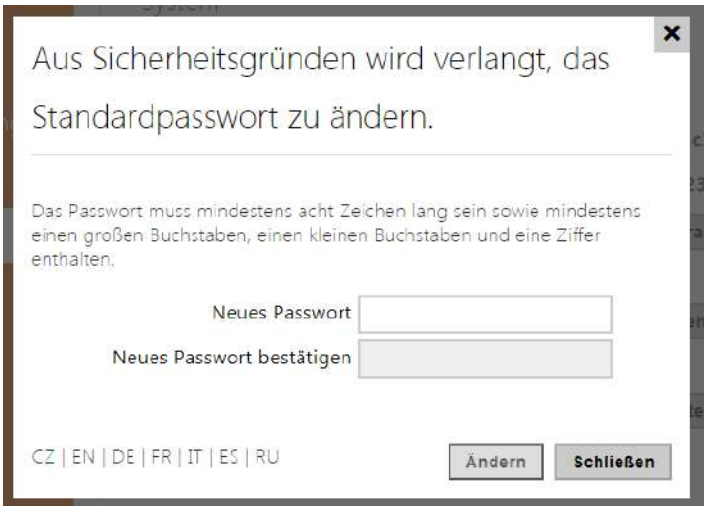
Damit Sie sich an der Konfigurationsschnittstelle des Interkoms anmelden können, müssen Sie ihre IP-Adresse kennen. Die **Interkoms 2N IP** haben als Fabrikeinstellung das automatische Erhalten der IP-Adresse vom DHCP-Server eingestellt. Wenn Sie somit das Interkom an das Netz anschließen, in dem sich der DHCP-Server befindet, der so konfiguriert ist, dass er die IP-Adressen allen neuen Anlagen zuteilt, wird auch Ihr Interkom seine eigene IP-Adresse erhalten. Sie können die IP-Adresse des Interkoms direkt anhand des DHCP-Servers-Status (gemäß der MAC-Adresse des Interkoms, die auf dem Herstellerschild angeführt ist) erfahren bzw. das Interkom kann sie Ihnen direkt mittels der Voice-Funktion mitteilen – siehe Installationshandbuch zum jeweiligen Interkom-Modell.

Wenn es in Ihrem Netz keinen DHCP-Server gibt, müssen Sie die statische Adresse mithilfe der Interkomtasten einstellen, siehe Installationshandbuch zum jeweiligen Interkom-Modell. 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.

Falls Sie die IP-Adresse Ihres Interkoms schon kennen, geben Sie sie in ihren beliebten Webbrowser ein. Wir empfehlen die aktuelle Version des Webbrowsers Chrome, Firefox oder Internet Explorer 9+ zu verwenden. Die **2N IP Interkoms** sind mit älteren Versionen der Webbrowser nicht voll kompatibel.

Verwenden Sie für das erste Anmelden an der Konfigurationsschnittstelle den Namen admin und das Passwort 2n (Passwort, das nur nach dem Zurücksetzen der Anlage in den Ausgangsstatus gültig ist).

Das Interkom verlangt nach dem ersten Anmelden eine Passwortänderung. Es werden nur starke Passwörter akzeptiert – mindestens acht Zeichen, die mindestens einen großen Buchstaben, einen kleinen Buchstaben und eine Ziffer enthalten.



Merken Sie sich das gewählte Passwort gut bzw. notieren Sie sich dieses. Falls Sie das Passwort vergessen, werden Sie das Interkom in den Ausgangsstatus zurücksetzen müssen (siehe Installationshandbuch zum jeweiligen Modell) und Sie werden dadurch gleichzeitig sämtliche durchgeführte Einstellungsänderungen verlieren.

Tipp

- FAQ: IP_Adresse – Wie stellt man die IP-Adresse des 2N IP Interkoms fest

Firmware Upload

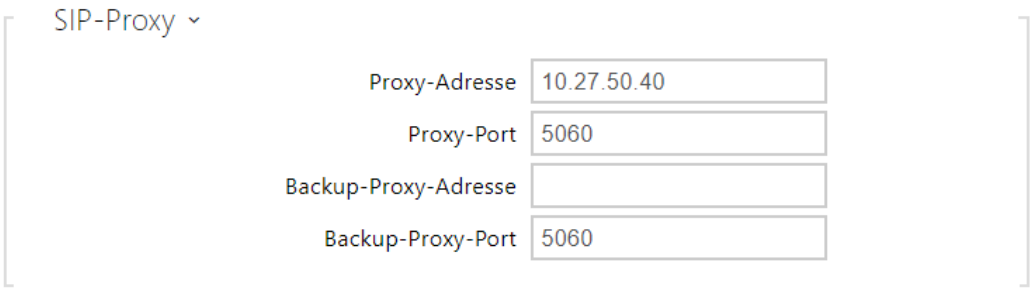
Wir empfehlen nach der ersten Anmeldung im Interkom gleichzeitig auch die Interkom-Firmware zu aktualisieren. Die neueste Firmware für Ihr Interkom finden Sie auf der Webseite www.2n.cz. Der Firmwareaktualisierung dient die Taste **Firmware aktualisieren** im Menü **System / Wartung**. Nach dem Upload der Firmware in die Anlage führt die Anlage einen Neustart durch und die Aktualisierung ist fertig. Die Aktualisierung dauert ungefähr eine halbe Minute.

Einstellung des Anschlusses an den SIP-Server

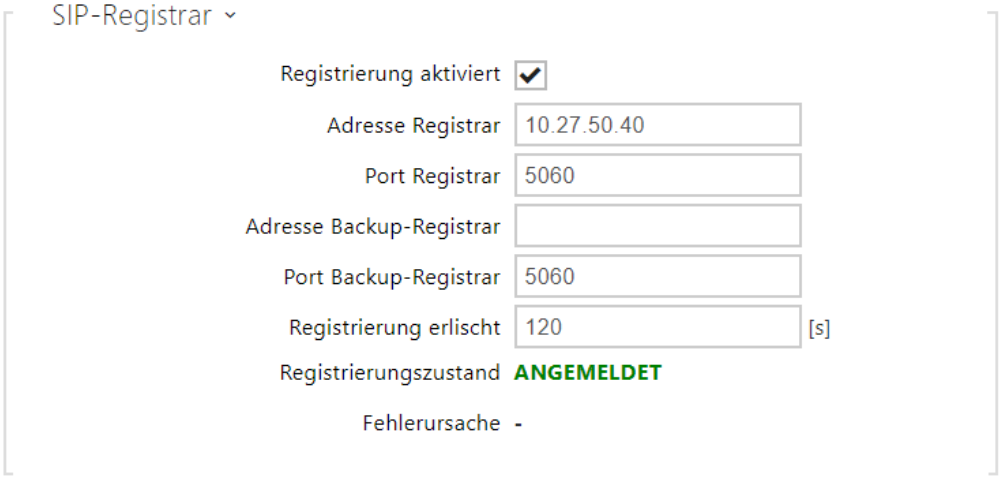
Damit das Interkom telefonieren kann und im Rahmen Ihrer VoIP-Infrastruktur erreichbar ist, müssen Sie einige wichtige Parameter einstellen. Diese Parameter werden im Menü **Dienste / Telefon / SIP** eingestellt.

- **Angezeigter Name** – stellen Sie den Namen ein, der auf dem Telefon des Angerufenen als die Identifikation des Anrufenden angezeigt wird. Dieser Name wird auch im Anmeldefenster und auf der Startseite der Webschnittstelle angezeigt.
- **Telefonnummer (ID)** – stellen Sie die eigene Telefonnummer des Interkoms (ggf. eine andere eindeutige aus Zeichen und Ziffern bestehende ID) ein. Diese Nummer zusammen mit der Domain identifiziert das Interkom eindeutig bei Anrufen und bei der Registrierung.
- **Domain** – stellen Sie den Domain-Name des Dienstes ein, bei dem das Interkom registriert ist. Stimmt gewöhnlich mit der SIP-Proxy- oder Registrar-Adresse überein. Wenn Sie in Ihrer Interkominstallation keinen SIP-Proxy benutzen, geben Sie die IP-Adresse des Interkoms ein

Wenn Sie in Ihrem Netz einen SIP-Server (Proxy, Registrar) benutzen, muss man die Adresse dieser Elemente im Netz einstellen:



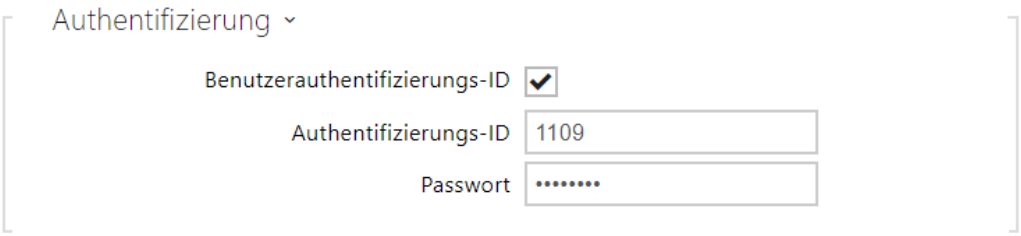
- **Proxy-Adresse** – stellen Sie die IP-Adresse oder den Domainnamen von SIP-Proxy ein.
- **Proxy-port** – legt den SIP-Proxy-Port (üblicherweise 5060) fest.
- **Backup-Proxy-Adresse** – IP-Adresse oder Domainname des Backup-SIP-Proxys. Die Adresse kommt dann zum Einsatz, wenn der Haupt-Proxy auf die Anforderungen nicht antwortet.
- **Backup-Proxy-Port** – Stellt den port des Backup-SIP-Proxys (gewöhnlich 5060) ein.



- **Registrierungsgenehmigung** – genehmigen Sie die Interkomregistrierung beim eingestellten SIP-Registrar.
- **Registrar-Adresse** – stellen Sie die IP-Adresse oder den Domainnamen von SIP-Registrar ein. Die Adresse von SIP-Proxy und SIP-Registrar ist gewöhnlich die gleiche.
- **Port Registrar** – legt den SIP-Registrar-Port (üblicherweise 5060) fest.

- **Adresse Backup-Registrar** – IP-Adresse oder Domainname des Backup-SIP-Registrars. Die Adresse kommt dann zum Einsatz, wenn der Haupt-Registrar auf die Anforderungen nicht antwortet.
- **Port Backup-Registrar** – Stellt den port des Backup-SIP-Registrars (gewöhnlich 5060) ein.
- **Registrierung erslicht** – definiert, wann die Registrierung erslicht, die die Auslastung des Netzwerks und SIP-Registrars durch regelmäßig gesendete Registrierungsanfoderungen betrifft. Der SIP-Registrar kann die Frist für das Erlöschen ändern, ohne dass ihnen daas mitgeteilt wird.
- **Registrierungszustand** – zeigt den aktuellen Registrierungsstatus an (Nicht registriert, Registrierung läuft..., Registriert, Registrierung wird beendet...).
- **Fehlerursache** – zeigt die Fehlerursache des letzten Registrierungsversuchs an – zeigt die letzte Fehlerantwort des Registrars, z.B. 404 Not Found an.

Wenn Ihr SIP-Server die Authentifizierung der Endanlagen verlangt, geben Sie folgende Parameter ein:

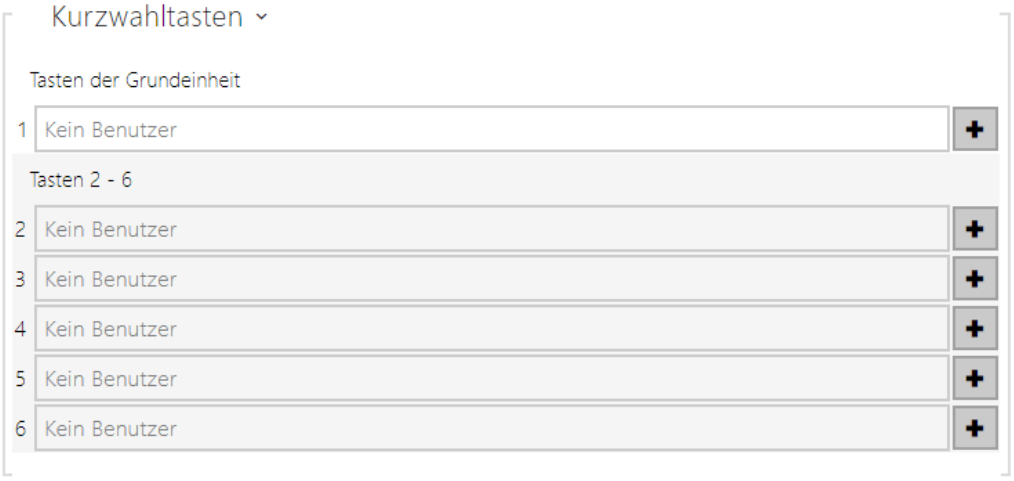


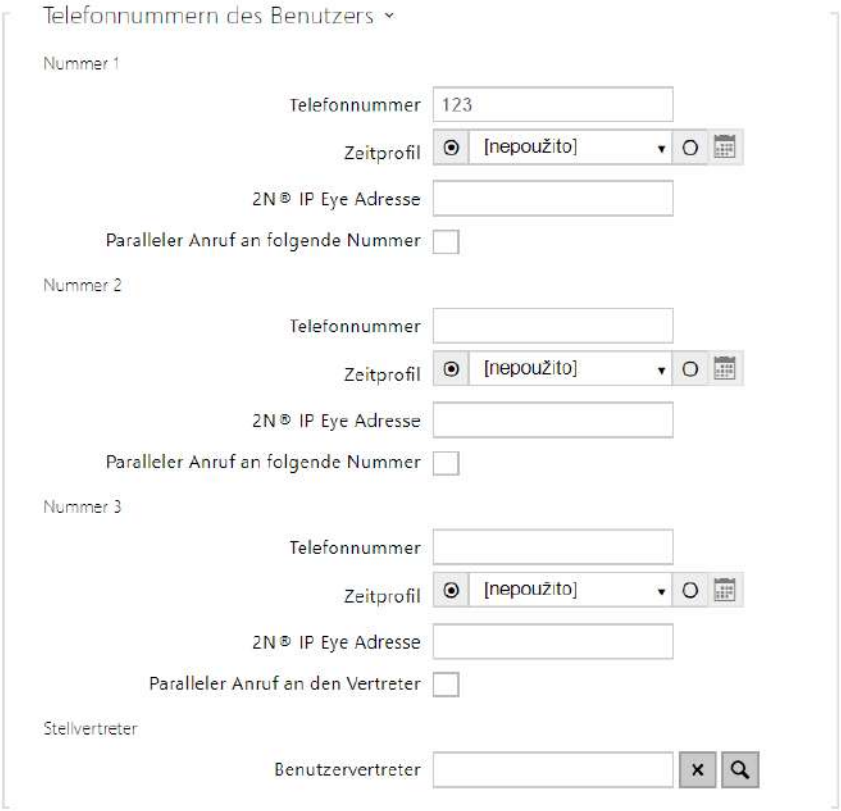
- **Passwort** – Geben Sie das Passwort ein, das bei der Authentifizierung des Interkoms verwendet wird.

Einstellung der Kurzwahltasten

Alle Modelle der **Interkoms 2N IP** sind mit Kurzwahltasten ausgestattet. Wenn der Nutzer eine der Kurzwahltasten drückt, wird die Telefonnummer angerufen, die in der jeweiligen Position in der Nutzerliste voreingestellt ist.

Wählen Sie im Menü **Adressbuch / Nutzer** aller potentiell verfügbaren Tasten auf dem Interkom an. Enthält die Liste der Tasten einschließlich jener, die im Interkom nicht physisch anwesend sind. Bei manchen Modellen (**2N® IP Vario**, **2N® IP Verso**) ist die Tastenliste in Gruppen je 8 bzw. 5 Tasten aufgeteilt, die den erweiternden Tastenmodulen entsprechen. In das Editierungsfeld kann manden Nutzer mittels der Schaltfläche  , mittels seiner Bezeichnung und durch die Bestätigung mit der Taste hinzufügen. Man kann den gefragten Nutzer auch in der Liste mittels des Fulltextfeldes über den Namen suchen. Eine Kurzwahltaste können mehrere Nutzer gleichzeitig teilen.

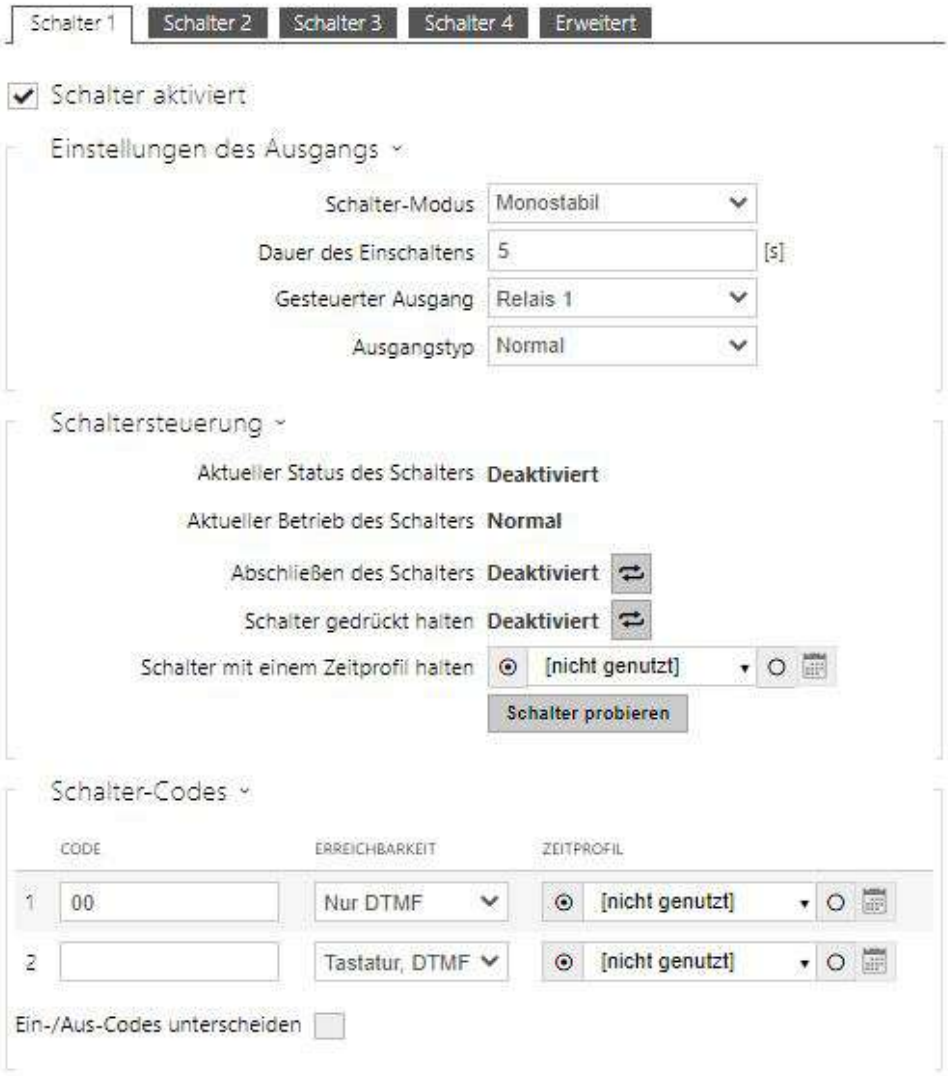




Sie können die **Interkoms 2N IP** auch mit einem oder mehreren IP-Telefonen ohne den SIP-Server verwenden. Für Anrufe aus dem Interkom wird das sog. Direct SIP Call verwendet. Füllen Sie in einem solchen Fall statt der Telefonnummer die SIP-Adresse des angerufenen Telefons in der Form sip:Telefon_Nummer@ip_adresse_des_Telefons aus.

Einstellung der Einschaltung des elektrischen Schlosses

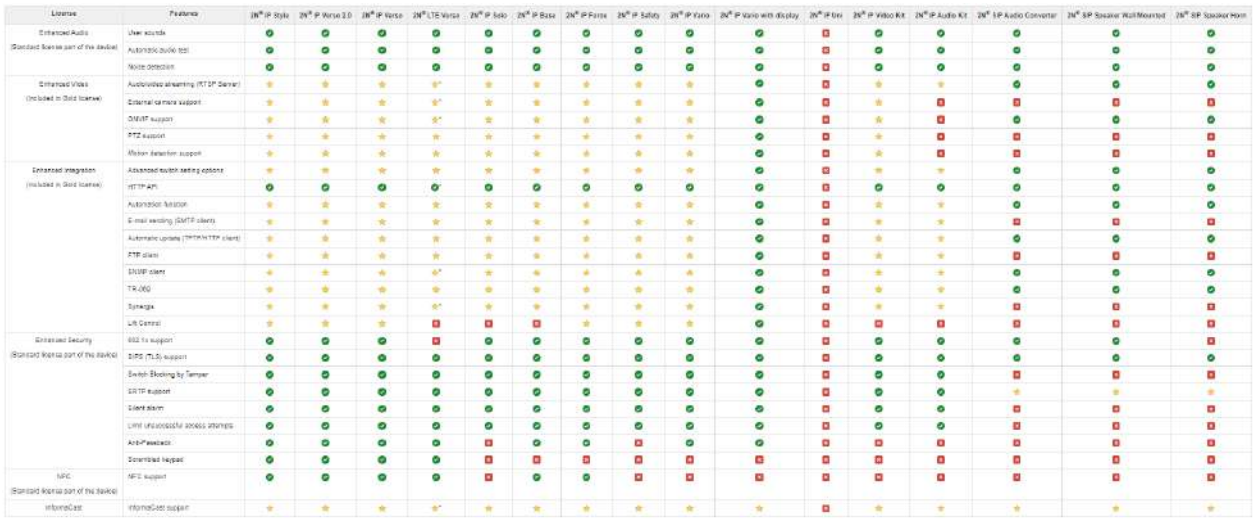
Man kann an die **Interkoms 2N IP** ein elektrisches Türschloss anschließen, das man mittels des Codes, der auf der nummerischen Tastatur des Interkoms eingegeben wird bzw. des Codes, der auf der Tastatur des IP-Telefons während des Anrufes eingegeben wird, bedienen. Schließen Sie das elektrische Türschloss gemäß der Anleitung im Installationshandbuch an das jeweilige Modell 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. Unterschiede zwischen den Modellen und Funktionslizenzierung

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



– Enthält aus der Fertigung
– Lizenzierte Funktion, ist nachzukaufen
– Kann man nicht verwenden

*) Die Verfügbarkeit von Diensten hängt von den Einstellungen Ihres Mobilfunknetzes ab.

3.1 Unterschiede zwischen Modellen

Dieses Handbuch ist für die ganze Familie der **2N IP Interkoms** gemeinsam und deshalb sind manche hier beschriebenen Funktionen nur bei konkreten Modellen bzw. erst nach der Eingabe des gültigen Lizenzschlüssels verfügbar. In diesem Kapitel ist die Übersicht der Unterschiede zwischen den einzelnen Modellen angeführt. Die Auflistung der Unterschiede ist nicht komplett, sie ist nur auf die beschränkt, die die Konfigurationsmöglichkeiten beeinflussen. Wenn die jeweilige Funktion nicht bei allen Modellen verfügbar ist, ist im jeweiligen Kapitel eine Bemerkung und ein Verweis auf dieses Kapitel angeführt.

In der nachstehenden Tabelle ist eine Übersicht der Eigenschaften und Funktionen der einzelnen Modelle der **Interkoms 2N IP** angeführt.

Eigenschaft/ Modell	**2N® IP Style**	**2N® IP Verso 2.0**	**2N® IP Verso**	**2N® IP Base**	**2N® IP Solo**	**2N® IP Vario**	**2N® IP Force**	**2N® IP Safety**	**2N® IP Uni**	**2N® IP Audio Kit**	**2N® IP Video Kit**
Bestellnummer	9157...	91552...	9155...	9156...	91553...C	9137...	9151...	9152...	9153...	9154...	9154...C
Prozessor Artpec	Ja		Nein								

Eigenschaft/ Modell	2N® IP Style	2N® IP Verso 2.0	2N® IP Verso	2N® IP Base	2N® IP Solo	2N® IP Vario	2N® IP Force	2N® IP Safety	2N® IP Uni	2N® IP Audio Kit	2N® IP Video Kit
Integrierte Kamera	Ja		Fakultativ	Ja		Fakultativ		Nein			
Kameraauflösung	1280 x 960	1920 x 1440	1280 x 960			640 x 480	640 x 480 oder 1280 x 960				
Unterstützung einer externen Analogkamera	Nein										Ja
Unterstützung einer externen IP-Kamera	Ja								Nein		Ja
Interner RFID-Kartenleser	Ja	Fakultativ			Nein	Fakultativ		Nein			
Display	Ja	Fakultativ	Nein	Nein	Fakultativ	Nein					
Zusatzschalter	Ja	Fakultativ	Nein	Fakultativ					Nein		

Eigenschaft/ Modell	2N® IP Style	2N® IP Verso 2.0	2N® IP Verso	2N® IP Base	2N® IP Solo	2N® IP Vario	2N® IP Force	2N® IP Safety	2N® IP Uni	2N® IP Audio Kit	2N® IP Video Kit
Anzahl der Tasten der Basiseinheit	0	1		1 oder 2	1	1, 3 oder 6	1, 2 oder 4	1	1 oder 2	bis 16 externe programmierbare Tasten	
Erweiterung der Anzahl der Tasten (Extender)	0	bis 145		Nein		bis 48	Nein				
Numerische Tastatur	Ja	Fakultativ		Nein		optional		Nein			
Digitaler Eingang	Ja					Fakultativ			Nein	2	
Breitband-Audiocodecs (L16, G.722)	Ja								Nein		Ja
Verstärkerleistung	4 W	2 W				150 mW	10 W			10 W	
Einstellungen des Mikrofonverstärkers	Nein									Ja	
Erweiterung der Verstärkerleistung auf 10 W	Nein						Ja		Nein	Nein	
Tamper / Schutzschalter	Ja	Fakultativ		Ja		Nein	Fakultativ		Ja	Nein	

Eigenschaft/ Modell	2N® IP Style	2N® IP Verso 2.0	2N® IP Verso	2N® IP Base	2N® IP Solo	2N® IP Vario	2N® IP Force	2N® IP Safety	2N® IP Uni	2N® IP Audio Kit	2N® IP Video Kit
Anzahl der Positionen in der Nutzerliste	10 000								2	16	
Nutzervertreter bei Unerreichbarkeit	Ja								Nein	Ja	
Anzahl der bedienten Schalter	4			2	4				1	4	
Anzahl der Universalcodes der Schalter	10			2	10				2	10	
Anzahl der Nutzerprofile	20										
JPEG-HTTP-Video	Ja							Nein			Ja
Unterstützung **2N® IP Eye**	Ja							Nein			Ja
Telefonmodus	Ja			Nein		Ja		Nein		Ja	

Einige Funktionen der **2N IP Interkoms** sind nur nach der Eingabe des gültigen Lizenzschlüssels verfügbar (siehe Kapitel Lizenzen).

3.2 Funktionslizenzierung

Funktionslizenzierung

Für die normale Nutzung der 2N IP-Sprechanlage sind die Basislizenzen, die bereits ab Werk im Gerät enthalten sind, ausreichend. 2N IP-Sprechanlagen können um weitere Funktionen erweitert werden, die einer kostenpflichtigen Lizenz unterliegen.

Lizenztypen

Einige Funktionen der **2N IP Interkoms** sind nur nach der Eingabe des gültigen Lizenzschlüssels verfügbar. Zu Verfügung stehen folgende Lizenztypen:

- NFC (Teil des Gerätes)
- Enhanced Audio (Teil des Gerätes
- Enhanced Security (Teil des Gerätes)
- Gold (Best.-Nr. 9137909)
- InformaCast (Best.-Nr. 9137910)

Bemerkung

- Die Lizenz InformaCast ermöglicht die Anwendung des SingleWire-InformaCast-Protokolls.

2N® IP Style, Verso, Base, Solo, Vario, Force, Safety und **Audio Kit** mit **Video Kit** unterstützen dieses Lizenzschema. Für das Modell **2N® IP Uni** sind keine Lizenzen verfügbar.

Tipp

- Die Übersicht der Unterschiede zwischen den Modellen und Funktionslizenzierung finden Sie im Kapitel 3. Unterschiede zwischen den Modellen und Funktionslizenzierung.

In der folgenden Tabelle werden alle Funktionen genannt, die durch die Eingabe der Lizenzschlüssels aktiviert werden, die den vorstehend angeführten Lizenzen entsprechen. Man kann die Lizenzen beliebig kombinieren.

Funktion	Enhanced Audio	Enhanced Video	Enhanced Integration	Enhanced Security	NFC	InformaCast	IP intercoms Lift module license	Lizenz
Benutzerdefinierte Töne	•							Teil des Gerätes
Automatischer Audiotest	•							Teil des Gerätes

Funktion	Enhanced Audio	Enhanced Video	Enhanced Integration	Enhanced Security	NFC	InformaCast	IP intercoms Lift module license	Lizenz
Lärmerkennung	•							Teil des Gerätes
Audio/ Video-Streaming (RTSP-Server)		•						GOLD
Unterstützung einer externen IP-Kamera		•						GOLD
ONVIF-Unterstützung		•						GOLD
Unterstützung der PTZ-Funktion		•						GOLD
Unterstützung der Bewegungserkennung		•						GOLD
Erweiterte Möglichkeiten der Schaltereinstellung			•					GOLD
HTTP API (siehe Anmerkung weiter unten)			•					Teil des Gerätes

Funktion	Enhanced Audio	Enhanced Video	Enhanced Integration	Enhanced Security	NFC	InformaCast	IP intercoms Lift module license	Lizenz
Funktion für die Automatisierung			•					GOLD
E-Mails-Absenden (SMTP-Client)			•					GOLD
Automatisches Update (TFTP/ HTTP-Client)			•					GOLD
FTP-Client			•					GOLD
SNMP-Client			•					GOLD
TR-069			•					GOLD
Unterstützung 802.1x				•				Teil des Gerätes
SIPS -(TLS)-Unterstützung				•				Teil des Gerätes
SRTP-Unterstützung				•				Teil des Gerätes
SilentAlarm				•				Teil des Gerätes

Funktion	Enhanced Audio	Enhanced Video	Enhanced Integration	Enhanced Security	NFC	InformaCast	IP intercoms Lift module license	Lizenz
Einschränkung der erfolglosen Zutrittsversuche				•				Teil des Gerätes
Schalter-Blockierung				•				Teil des Gerätes
Verschlüsselte Tastatur				•				Teil des Gerätes
NFC-Support					•			Teil des Gerätes
InformaCast-Unterstützung						•		InformaCast
Anti-Passback				•				Teil des Gerätes
Genetec Synergis			•					GOLD
Aufzugsteuerung							•	GOLD
IP Relais			•					GOLD

Welche weiteren Produkte haben das gleiche Lizenzschema?

2N® SIP Audio Converter, **2N® SIP Speaker** und **2N® SIP Speaker Horn**, die mit der schon installierten Gold-Lizenz verkauft werden, man kann sie daher nur auf InformaCast upgraden.

Wie kann ich die Lizenz erwerben?

Die Lizenz wird durch die Gesellschaft 2N gemäß der Seriennummer generiert. Sobald Sie sich entscheiden, welche Lizenz Sie haben wollen, teilen Sie Ihrem Vertreiber die Nummer Ihrer Einheit mit und er wird Ihnen den Lizenzschlüssel zu Verfügung stellen.

Die Lizenz selbst werden Sie z.B. per E-Mail in der Form eines Codes (alphanummerischer Kette) erhalten, den Sie kopieren und in das Interkom eingeben.

Die Lizenzen sind nicht zeitlich begrenzt. Sobald Sie die Lizenz einmal erwerben, haben Sie sie für immer.

Wenn Sie die Lizenz aktivieren wollen, schließen Sie sich an die Webschnittstelle des jeweiligen Interkoms an und geben Sie den kopierten Lizenzschlüssel in das Feld im Menü System / Lizenz ein. Klicken Sie auf Speichern und die lizenzierten Funktionen werden sofort aktiviert.

Man kann die Lizenzen automatisch im Menü System / Lizenzen herunterladen.

Tipp

- FAQ: Lizenz für 2N IP Interkoms – Wie kann man Sie erhalten

Kann ich eine Demo-Lizenz bekommen?

Ja, Ihnen stehen 800 Stunden der Gold-Lizenz zu Verfügung, während denen Sie die lizenzierten Eigenschaften ausprobieren können. Dieses Demo ist standardmäßig ausgeschaltet, aber Sie können sie in der Webschnittstelle des jeweiligen Interkoms im Menü System / Lizenzen aktivieren. Auf dem Countdownzähler sehen Sie die restliche Zeit und nach dem Ablauf der Probezeit werden alle lizenzierten Funktionen wieder deaktiviert.

Für die Lizenzen G.729 und InformaCast existiert keine Probiermöglichkeit.

4. Signalisierung der Betriebsstatus

Die **2N IP Interkoms** signalisieren 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
	**Bestätigungssignalisierung der Anrufverlängerung** Das **2N IP Interkom** hat aus dem Grund des Sperrschutzes die maximale Anruflänge eingestellt, siehe Kap. Sonstiges.
	**Interne Applikation gestartet** Nach dem Einschalten der Einspeisung oder nach dem Neustart des **2N IP Interkoms** ist der Start der internen Applikation des **2N IP Interkoms** 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 **2N IP Interkom** 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 **Interkom 2N IP** kommt, wird dieser Status durch diese Tonkombination signalisiert.
	**Ungültige Telefonnummer oder ungültiger Code für das Einschalten des Schalters** **2N IP Interkoms** ermöglichen, mit der Hilfe der Tastatur direkt die Telefonnummer der Nebenstelle zu wählen oder den Code für das Öffnen der Tür einzugeben. Wenn der Code ungültig ist, 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 Kap. Konfiguration der Anlage im konkreten Installationshandbuch des **2N IP Interkoms** beschrieben.
	**Signalisierung des sich nähernden Anrufendes** Die**2N IP Interkoms** ermöglichen das Zeitlimit einzustellen, nach dessen Ablauf der Anruf beendet wird. Man kann den Anruf durch das Drücken einer Taste vom VoIP-Telefon verlängern. Das Zeitlimit ist aus dem Grund des Schutzes vor der Anrufsperre eingestellt.
	**Verbundener Anruf beim Anrufen von einem VoIP-Telefon auf das 2N IP Interkom** Beim Anrufen von einem VoIP-Telefon auf die **Interkoms 2N IP** wird ein kurzer Ton zum Zweck der Signalisierung der Anrufverbindung abgespielt.

5. Interkomkonfiguration

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.

Domänename

An das Gerät kann man sich durch Eingabe der Domäneadresse im Format *hostname.local anschließen* (z.B.: 2NIPStyle-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 IP Verso	2NIPVerso

2N-Gerät	Bezeichnung des Geräts im Hostnamen
2N IP Verso 2.0	2NIPVerso20
2N LTE Verso	2NLTEVerso
2N IP Style	2NIPStyle
2N IP One	2NIPOne
2N IP Vario	2NIPVario
2N IP Base	2NIPBase
2N IP Force	2NIPForce
2N IP Safety	2NIPSafety
2N IP Solo	2NIPSolo
2N IP Uni	2NIPUni

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.

Startbildschirm

Der Startbildschirm erscheint nach dem Anmelden an der Webschnittstelle des Interkoms. 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 Interkomname (siehe Parameter Angezeigter Name in der Einstellung **Dienste/ Telefon / SIP**). 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 der Interkomkonfiguration. In manchen Kästen wird gleichzeitig der Status der ausgewählten Dienste angezeigt.

Konfigurationsmenü

Die Konfiguration der **2N IP Interkoms** ist in 5 Untermenüs aufgeteilt – **Status**, **Verzeichnis**, **Hardware**, **Dienste** und **System**; jedes der Untermenüs ist in weitere Teile aufgeteilt, siehe folgende Übersicht.

Status

- **Gerät** – Basisinformationen über das Interkom
- **Services** – Information über gestartete Dienste und ihren Status
- **Lizenz** – aktueller Status der Lizenz und der verfügbaren Funktionen des Interkoms
- **Zugriffsprotokoll** – zeigt die letzten 10 Zugriffsdatensätze an
- **Anrufaufzeichnungen** – zeigt die letzten 20 getätigten Anrufe
- **Ereignisse** – zeigt die letzten 500 Ereignisse an, die das Gerät aufgezeichnet hat

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

Wählen

- **Allgemeine Einstellungen** – Einstellung betreffend eingehende und ausgehende Anrufe
- **Wählen** – Einstellung der Kurzwahltasten
- **SIP 1** – Einstellungen des SIP-Intercom-Kontos
- **SIP 2** – Einstellungen des SIP-Intercom-Kontos
- **Lokalanrufe** – Einstellung der Lokalanrufe, der Verbindung, der Videoparamete
- **Crestron** – Verbindungseinstellungen mit Crestron-Geräten

Services

- **Zugangskontrolle** – Einstellungen der Ein- und Ausstiegsregeln
- **Streaming** – Einstellung des Audio- und Videostreamings (ONVIF, RTSP, Multicast u.Ä.)
- **E-Mail** – Einstellung der absendenden E-Mails und der Verbindung zum SMTP-Server
- **Automatisierung** – flexible Interkomeinstellung gemäß den spezifischen Anforderungen des Nutzers
- **HTTP API** – Einstellung der HTTP API-Autorisierung
- **Benutzertöne** – Einstellung und Upload der Nutzertöne
- **Webserver** – Einstellung des Webservers und des Zutrittcodes

- **Audio-Test** – Einstellung des automatischen Audiotests
- **SNMP** – Einstellung des SNMP-Dienstes

Hardware

- **Schalter** – Einstellung der Einschaltung des elektrischen Schlosses, der Beleuchtung u.Ä.
- **Audio** – Lautstärke des Audios, des Signalisierungstons u.Ä., Mikrofonparameter
- **Kamera** – Einstellung der internen Kamera und der externen IP-Kamera
- **Tastatur** – Einstellung des Verhaltens der Tasten und der Tastatur
- **Hintergrundlicht** – Einstellung der Hintergrundbeleuchtung
- **Display** – grundlegende Displayeinstellung
- **Kartenleser** – Einstellung des Kartenlesers, Wiegand-Interface
- **Digitale Eingänge** – Digitaleingangseinstellungen
- **Extender** – Einstellung der erweiternden Module **2N® IP Verso**
- **Aufzugsteuerung** – Einstellungen für den Zugang zu den einzelnen Etagen mit dem Aufzug

System

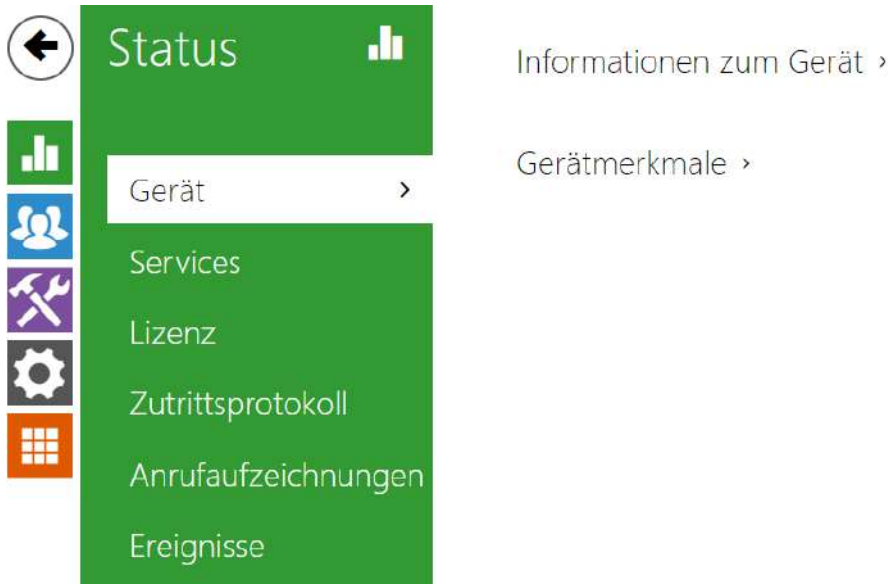
- **Netzwerk** – Einstellung des Anschlusses an das lokale Netz, 802.1x, Abfangen von Paketen
- **Datum & Uhrzeit** – Einstellung der realen Zeit und der Zeitzone
- **Funktion** – Einstellung der Testfunktionen
- **Lizenz** – Einstellung von Lizenzen, Aktivierung der Trial-Lizenz
- **Zertifikate** – 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 Anrufen
- 5.4 Services
- 5.5 Hardware
- 5.6 System
- 5.7 Verwendete Ports

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

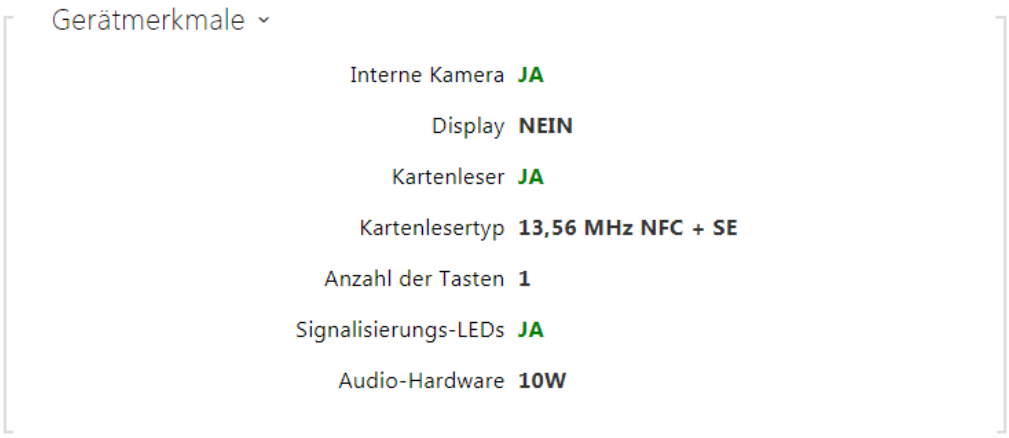


Im Menü **Status** werden übersichtlich die aktuellen Informationen und Eigenschaften der Anlage angezeigt. Das Menü ist in fünf Registerkarten aufgeteilt: **Gerät**,
Services, **Zutritteprotokoll, Anrufaufzeichnungen** und **Ereignisse**.

Registerkarte Gerät

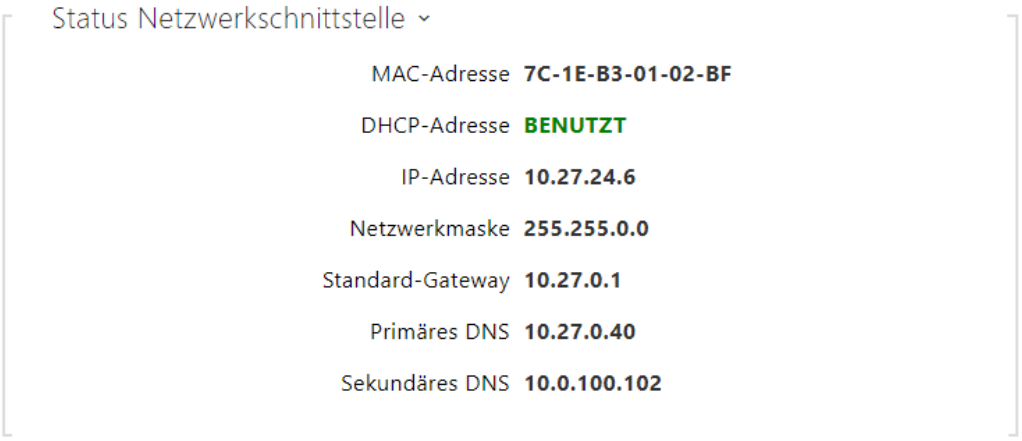
Zeigt Informationen über das Modell und seine Eigenschaften, die Version der Firmware und des Bootloaders u.Ä. an.

- **Herstellerzertifikat installiert** – gibt das Benutzerzertifikat und den privaten Schlüssel an, die verwendet werden, um die Berechtigung der Sprechanlage zur Kommunikation mit dem Server von Drittanbietergeräten zu überprüfen.
- **Gerät lokalisieren** – optische und akustische Signalisierung des Geräts. Optische Signalisierung ist nur dann möglich, wenn das Gerät mit Hinterleuchtung ausgestattet ist (**2N® IP Style, 2N® IP Verso**, **2N® IP Solo**, **2N® IP Base**, **2N® IP Vario**, **2N® IP Force**, **2N® IP Safety** und **2N® IP Uni**). Hat das Gerät keinen integrierten Lautsprecher, überprüfen Sie, ob zur Tonsignalisierung ein externer Lautsprecher angeschlossen ist (**2N® IP Audio Kit** a **2N® IP Video Kit**).



Registerkarte Dienste

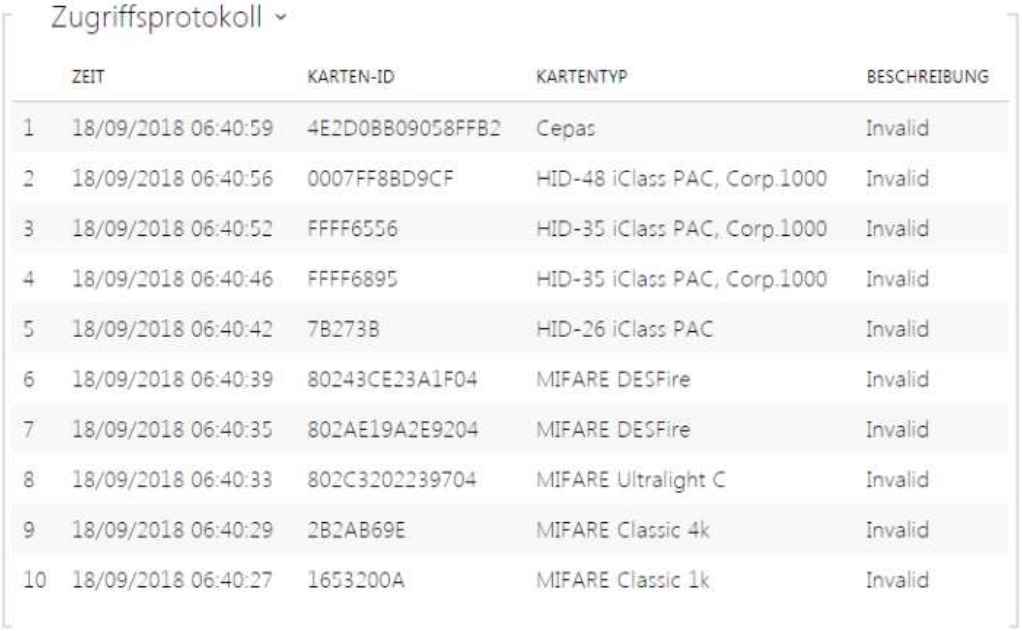
Zeigt den Status der Netzschnittstelle und der ausgewählten Dienste an




Telefonstatus (SIP2)
Telefonnummer (ID) 111
Registrierungszustand NICHT ANGEMELDET
Fehlerursache -
Registriert bei
Letzte Registrierung N/A

Registerkarte Zutritteprotokoll

Auf der Registerkarte **Zutritteprotokoll** 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.

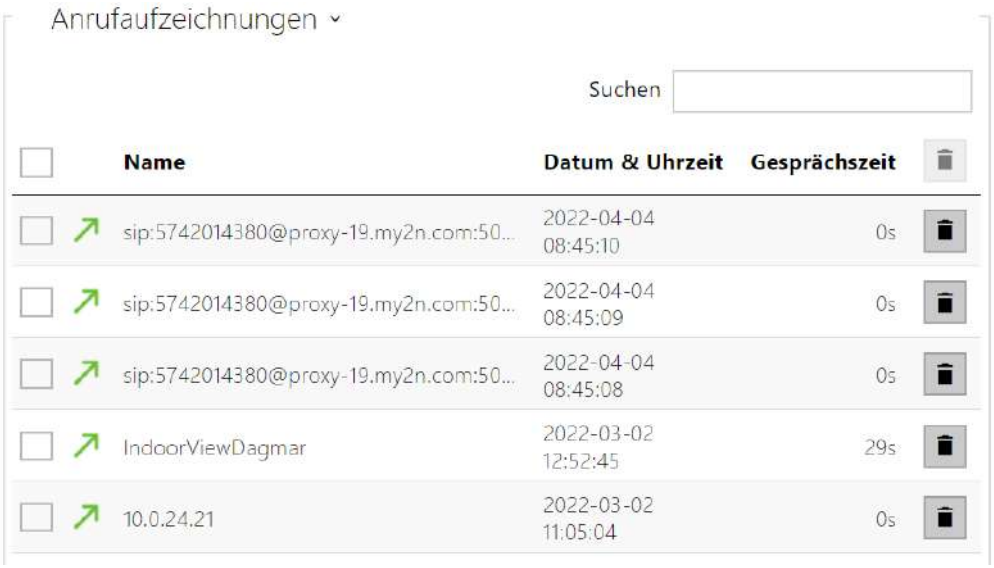


Zugriffsprotokoll

	ZEIT	KARTEN-ID	KARTENTYP	BESCHREIBUNG
1	18/09/2018 06:40:59	4E2D0BB09058FFB2	Cepas	Invalid
2	18/09/2018 06:40:56	0007FF8BD9CF	HID-48 iClass PAC, Corp.1000	Invalid
3	18/09/2018 06:40:52	FFFF6556	HID-35 iClass PAC, Corp.1000	Invalid
4	18/09/2018 06:40:46	FFFF6895	HID-35 iClass PAC, Corp.1000	Invalid
5	18/09/2018 06:40:42	7B273B	HID-26 iClass PAC	Invalid
6	18/09/2018 06:40:39	80243CE23A1F04	MIFARE DESFire	Invalid
7	18/09/2018 06:40:35	802AE19A2E9204	MIFARE DESFire	Invalid
8	18/09/2018 06:40:33	802C3202239704	MIFARE Ultralight C	Invalid
9	18/09/2018 06:40:29	2B2AB69E	MIFARE Classic 4k	Invalid
10	18/09/2018 06:40:27	1653200A	MIFARE Classic 1k	Invalid

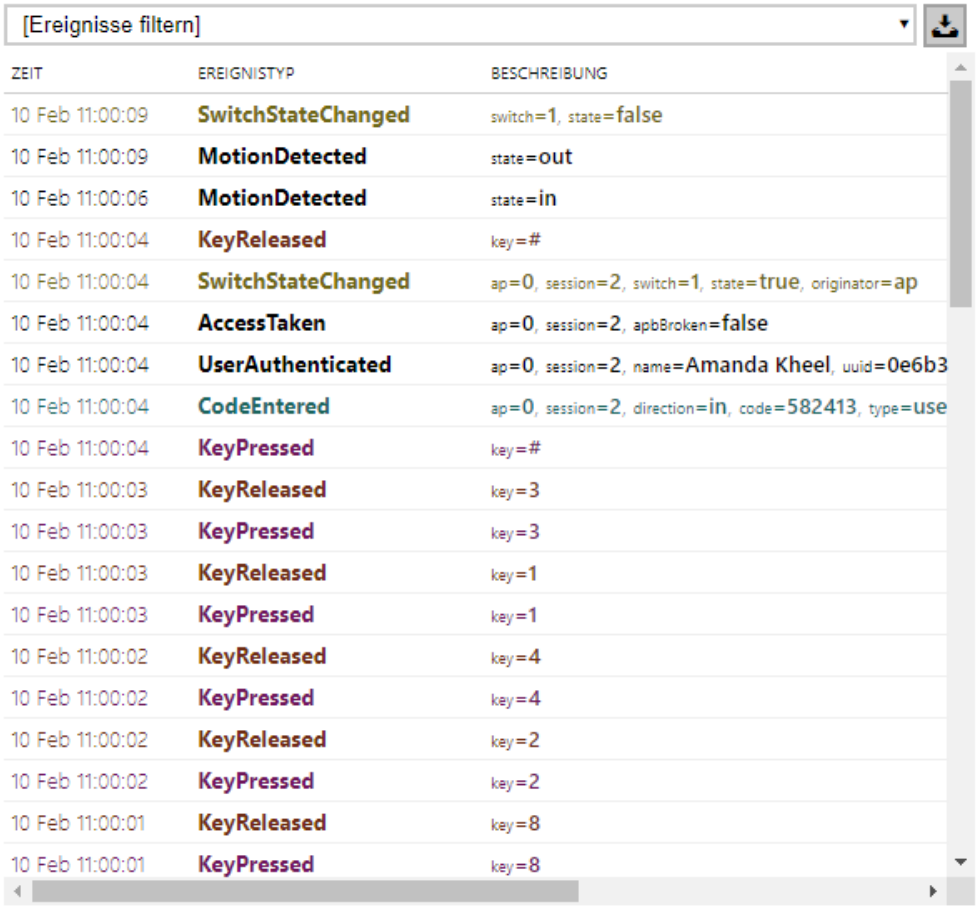
Registerkarte Anrufaufzeichnungen

Die Gesprächseinträge zeigen die Übersicht über alle erfolgten Gespräche an. Jedes Gespräch enthält Informationen über den Typ des Kontakts, über die ID des Angerufenen/des Anrufenden, über das Datum und die Zeit des Gesprächs, seine Länge und den Status (eingehend, ausgehend, versäumt, anderswo angenommen, Taste der Klingel). Das Feld für die Suche ermöglicht die Volltextsuche in den Namen der Gespräche. Das Ankreuzfeld dient zur Kennzeichnung aller Gespräche zum gesammelten Löschen. Ein ausgewählter Gesprächseintrag kann auch einzeln mithilfe der Taste  gelöscht werden. Die Übersicht zeigt die letzten 20 Einträge, die vom neuesten zum ältesten Gespräch geordnet sind.



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.
AudioLoopTest	Ergebnis des durchgeführten Audiotests.

Ereignis	Bedeutung
CallSessionStateChanged	Ereignis, das Richtung, Stand des Anrufs, Adresse, Nummer der gebildeten Sitzung und Folge des generierten Anrufs beschreibt.
CallStateChanged	Wenn sich der Anrufstatus ändert (ringing, connected, terminated), zeigt er auch die Richtung (eingehend, ausgehend) und die Identifikation der Gegenpartei oder des SIP-Kontos an.
CardHeld	Beim Anlegen der Karte, das 4 s und länger dauert.
CardEntered	Nach dem Anlegen der Karte.
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.
DtmfEntered	Empfang des DTMF Codes im Gespräch oder lokal außerhalb des Gesprächs.
DtmfPressed	Eingabe des DTMF Codes im Gespräch oder lokal außerhalb des Gesprächs.
DtmfSent	Absendung des DTMF Codes im Gespräch oder lokal außerhalb des Gesprächs.
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.).
KeyReleased	Beim Loslassen der Taste (die Ziffern sind 0,1,2...,9 und die Kurzwahltasten sind %1,%2 usw.).

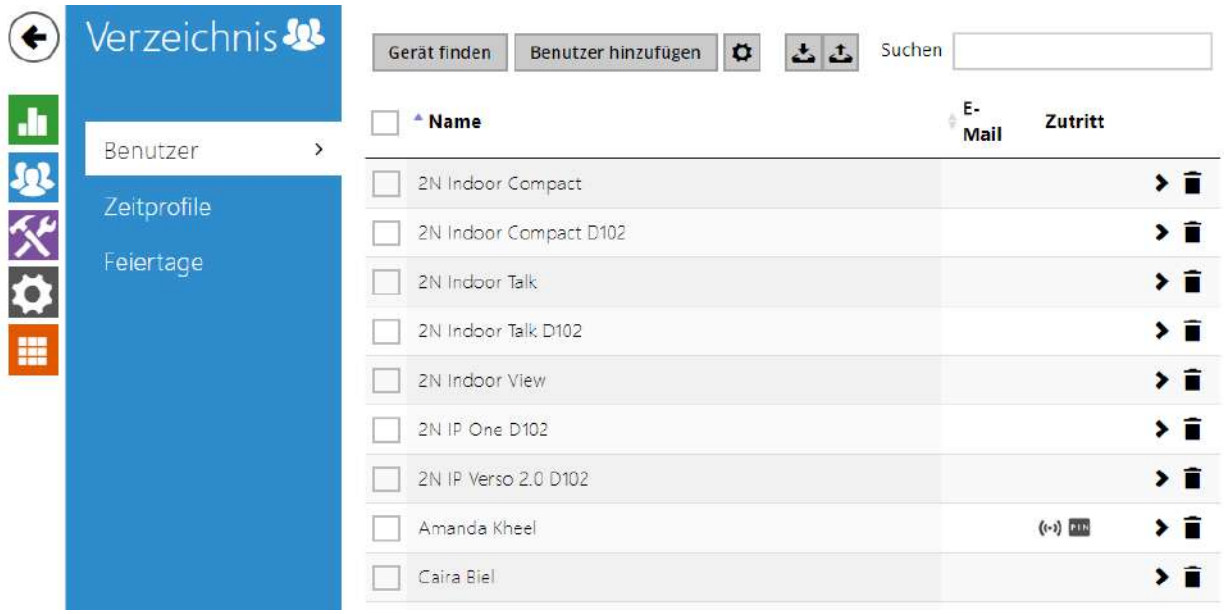
Ereignis	Bedeutung
LiftFloorsEnabled	Zutritt zur Etage mit Aufzug.
LiftStatusChanged	Erkennung der Anschliessung/Abtrennung des Lift Control Moduls.
LoginBlocked	Bei der Eingabe von 3 fehlerhaften Logins im Web, in die Anlage. Enthält Angaben über die IP-Adresse dieser Zutritte.
MobKeyEntered	Autorisierung mittels Bluetooth.
MotionDetected	Nach der Aktivierung der Bewegungserkennung, Sie können die Einstellung in der Hardware / Kamera / Internen Kamera durchführen.
NoiseDetected	Nach der Aktivierung der Lärmerkennung, Sie können die Einstellung in der Hardware / Audio durchführen.
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.

Ereignis	Bedeutung
TamperSwitchActivated	Signalisiert Aktivierung des Schutzschalters –Öffnen des Gerätegehäuses. Die Funktion des Schutzschalters muss im Menu Digitale Eingänge / Schutzschalter konfiguriert werden.
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.
VirtualInput	Änderung des virtuellen Eingangs.
VirtualOutput	Änderung des virtuellen Ausgangs.
CallSessionStateChanged	Informiert über die Phase des Anrufs, in der er sich befindet (Aufbau, Verbindung, Klingelton, Verbindung, Beendigung).

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 der Interkomkonfiguration. Sie enthält wichtige Informationen über die Nutzer, die die Interkomfunktionen verfügbar machen, wie das Türöffnen mittels der RFID-Karten oder das Einschalten des Codeschlosses, das Informieren des Nutzers über verpasste Anrufe mittels E-Mails u.Ä.sind.

Sie kann bis 10 000 Nutzer enthalten (bei einzelnen Modellen der **2N IP Interkoms** kann die Zahl der Positionen abweichen). Sie enthält die Nutzer, die mittels der Kurzwahltasten (man kann sie auch anrufen) erreichbar sein sollten, sowie gleichzeitig die Nutzer, die nur den Zutritt zum Objekt mittels der RFID-Karte, des Codes u.Ä. haben sollen.

Wenn Sie einen externen Kartenleser verwenden, der an das Interkom 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 Interkom 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

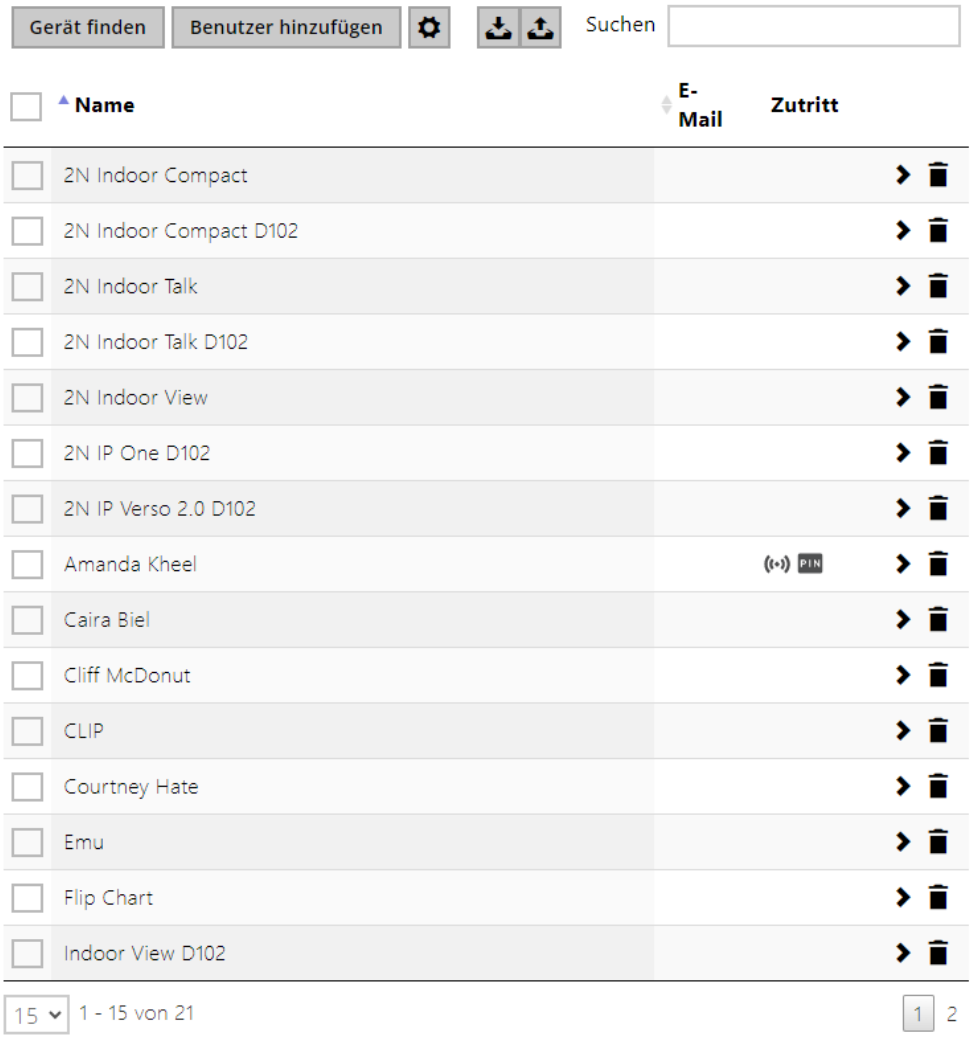
Trick nutzen – legen Sie die Karte an den Leser des Interkoms an und suchen Sie sie in der Registerkarte **Historie der Zutritte** aus. Markieren sie die ID der Karte mittels der Maus; z.B. mittels des doppelten Klickens auf die ID der Karte, und drücken Sie die Tasten CTRL+C. Nunmehr haben Sie die ID der Karte in der Zwischenablage und Sie können Sie mittels der Tasten CTRL+V in ein beliebiges Feld in der Interkomeinstellung eingeben.

Nach dem Anlegen der Karte an den RFID-Leser wird die Karten-ID mit der Kartendatenbank im Interkom 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. Sie können die Nummer des aktivierten Schalters in der Einstellung **Hardware / Kartenleser** mittels des Parameters Assoziierter Schalter (Modelle **2N® IP Base**, **Vario**, **Force**) beziehungsweise in der Einstellung **Hardware / Module** mittels des Parameters **Assoziierter Schalter** beim Modul des Kartenlesers (Modell **2N® IP Style**, **2N® IP Verso**) ändern.

Das Verknüpfen der Nutzer mit den Kurzwahltasten wird im Menü **Hardware / Tastendurchgeführt**. Sie können die Verbindungen zwischen den einzelnen Nutzern und den Tasten jederzeit nach Bedarf ändern. Die meisten **2N IP Interkoms** sind mit einer oder mehreren Kurzwahltasten ausgestattet. Ihre Zahl, die Möglichkeiten der Erweiterung finden Sie im Installationshandbuch des jeweiligen Interkommodells.

Warnung

- Das Geräteverzeichnis, das von **2N® Access Commander** verwaltet wird, nicht über Webschnittstelle des Gerätes zu ändern. Nach Synchronisierung mit **2N® Access Commander** kommt es zum Verlust der Änderungen im Verzeichnis, die über Webschnittstelle des Gerätes durchgeführt wurden.



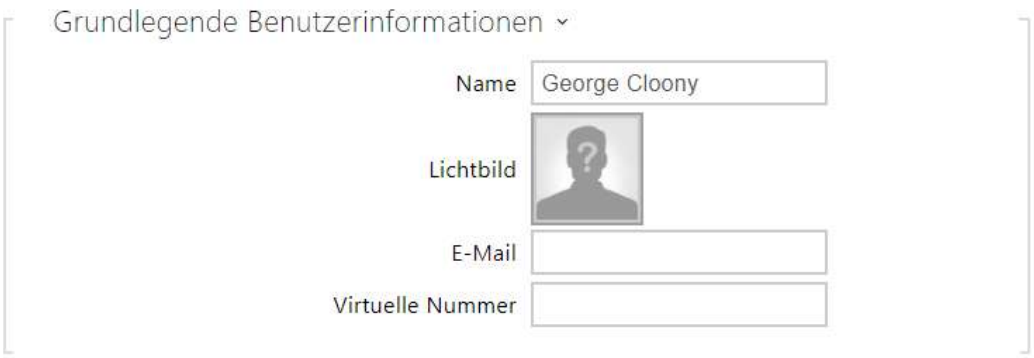
Die Funktion des Suchens im Verzeichnis funktioniert als Fulltextsuche im Namen, den Telefonnummern und in der E-Mail. Sie sucht nach sämtlichen Übereinstimmungen in der ganzen Liste. Ein neuer Benutzer wird mithilfe der Taste oberhalb der Tabelle hinzugefügt. Sie können auch nach einem Gerät in Ihrem lokalen Netzwerk suchen und es dann dem Verzeichnis als neuen Kontakt hinzufügen. Die Schaltfläche dient der detaillierten Anzeige der Nutzereinstellung dient die Schaltfläche  . Zur Einstellung der Anzeige der Tabellenspalten dient das Symbol  , 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. Die Position des Benutzers in der Liste ist alphabetisch sortiert.

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 Wenn es Benutzer im Verzeichnis gibt, werden alle exportiert, mit Ausnahme von speziellen Benutzertypen. 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.
- **Lichtbild** – ermöglicht ein Foto des Nutzers aufzunehmen. Nach dem Klicken auf den Rahmen für das Eingeben einer Fotografie erscheint der Fotografie-Editor, der ermöglicht, das ausgesuchte Foto aus einer Datei hochzuladen beziehungsweise ein Foto des Nutzers mittels der integrierten Kamera zu machen. Sie können Fotos im Format .jpg, .png und .bmp hochladen. Diese Funktion ist nur für die Modelle mit einem Display, **2N® IP Style**, **2N® IP Verso** und **2N® IP Vario** bestimmt.

Hinweis

- Wenn der Bildausschnitt nicht den gesamten Bereich des Zuschneidefensters ausfüllt, wird das resultierende Bild auf **2N® IP Style** zentriert.

- **E-Mail** – eine oder mehrere E-Mailadressen des Nutzers, an die die Information über verpasste oder alle realisierte Anrufe geschickt werden kann. Die E-Mailadressen werden mit einem Komma oder Bindestrich getrennt (z.B.: faith.pearl@gmail.com, kelly.black@gmail.com).
- **Virtuelle Nummer** – eine Nummer, die man für das Anrufen des Nutzers mittels der nummerischen Tastatur benutzen kann. Die Nummer kann zwei bis vier Ziffern haben. Die virtuellen Nummern hängen nicht mit den eigentlichen Telefonnummern der Nutzer zusammen. Sie können einen ganz anderen, von Telefonnummern unabhängigen Nummernplan bilden und so die eigentlichen Telefonnummern der Nutzer verbergen. Diese Funktion ist besonders bei Installationen mit einer ungenügender Zahl von Kurzwahltasten vorteilhaft. Der Ankömmling gibt die virtuelle Nummer auf der Tastatur ein und drückt die Taste *. Wenn Sie diese Art des Anrufens des Nutzer benutzen, ist es geeignet in der Nähe des Interkoms eine übersichtliche Liste der Nutzernamen und ihrer virtuellen Nummern einschließlich einer einfachen Bedienungsanleitung anzubringen. Sie können die Funktion der virtuellen Nummern im Menü **Services / Telefon / Anrufe / Ausgehende Anrufe** mittels des Parameters **Virtuelle Nummern anrufen** einschalten. Die Zahl kann 1–7 Ziffern enthalten.

- **Unterbringung im Rahmen des Verzeichnisses** – im Ausgangszustand wird nur das Root-Verzeichnis gebildet, in das man die Nutzer direkt aus dem Verzeichnis hinzufügen kann. Das Root-Verzeichnis kann weder gelöscht noch umbenannt werden. Jeder Nutzer kann gleichzeitig ein Bestandteil von maximal 5 Untergruppen des Roof-Verzeichnisses sein.
- **Rufgruppe** – dient der Benennung der Nutzergruppen, die im Displayverzeichnis angezeigt werden. Beim Anrufen der jeweiligen Gruppe werden alle Nutzer gleichzeitig angerufen. Nach Annahme eines der Anrufe werden die übrigen Anrufe automatisch beendet.

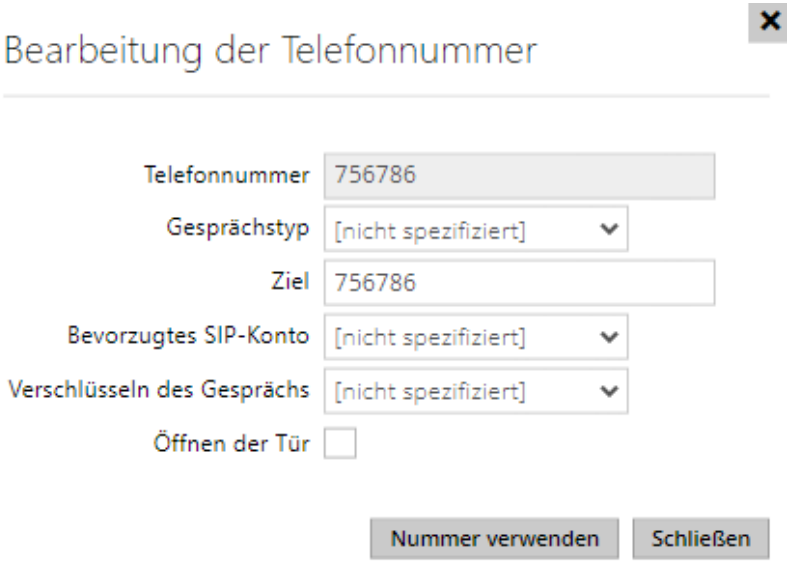
Hinweis

- Für Parameter Gerätename und Alternativname sind Zeichen <, > und / nicht erlaubt.

Bei jedem Nutzer aus der Liste kann man bis zu drei Telefonnummern eingeben. Falls der Nutzer nicht unter einer der Nummern erreichbar ist, wird nach der eingestellten Klingelzeit eine weitere Telefonnummer verwendet. Man kann auch mehrere Nummern gleichzeitig anrufen, und zwar mit der Freigabe der Funktion Anrufe in der Gruppe mit nachfolgender Nummer. Mann kann gleichzeitig die Gültigkeit jeder der Telefonnummern mittels des Zeitprofils einschränken.

- **Telefonnummer** – telefonnummer der Station, zu der der Anruf geleitet werden soll. Geben Sie die Adressen ein als sip:[user_id@]domain[:port] für direkten SIP-Anruf, z. B.:sip:200@192.168.22.15 oder sip:jName@IhreFirma. Geben Sie für Ortsgespräche mit dem 2N IP-Interkom und antwortende Einheiten die device:ID des Gerätes ein. Die Bezeichnung des Gerätes legen Sie auf den jeweiligen Geräten fest. Um ein Crestron-Gerät aufzurufen, geben Sie die Adresse in der Form RAVA:device_name ein. Falls Sie nach der Telefonnummer die Zeichen /1 resp. /2 angeben, wird für ausgehende Anrufe explizit SIP-Konto 1 resp. 2 benutzt. Falls das Telefonnummer einen Suffix /1 bzw. /2 hat, bestimmte SIP-Konto (1 oder 2) wird benutzt. Falls die Telefonnummer einen Suffix /**B** hat, wird die Türöffnung durch Rückruf aktiviert. Gleichzeitige Eingabe des Kontos, der Verschlüsselung und Öffnung durch Rückruf ist möglich, z. B. /1S /1B usw. Der Parametr kann bis 255 Zeichen enthalten.

Detaillierte Einstellungen der Rufnummer können im Bearbeitungsbildschirm vorgenommen werden, der durch Drücken der Taste  geöffnet wird.



  - **Gesprächstyp** – Stellt das Schema im URI der Zielrufnummer ein. Bei der Wahl „Ohne Schema“ wird URI um die Angaben aus der Einstellung des SIP-Kontos ergänzt. Die weiteren Einstellungen verwenden Sie für den SIP-Anruf (sip:), 2N lokales Gespräch (device:), Anrufe auf das Gerät Crestron (rava:) oder Gespräch mittels des Systems der Videonachricht, z.B. AXIS Camera Station (vms:).
  - **Ziel** – Stellt weitere Teile des URI der Zielrufnummer ein. Enthält in der Regel die Nummer, die IP-Adresse, die Domaine, den Port oder Identifikator des Geräts. Für Gespräche auf VMS wird ein Sternchen eingegeben (*).
  - **Bevorzugtes SIP-Konto** – Für Anrufe wird bevorzugt das SIP-Konto Nummer 1 oder Nummer 2 verwendet.
  - **Verschlüsseln des Gesprächs** – Es kann eine obligatorische Verschlüsselung des Gesprächs oder umgekehrt ein Gespräch ohne Verschlüsselung eingestellt werden.
  - **Öffnen der Tür** – mittels Rückruf.
- **Zeitprofil** – ermöglicht der Telefonnummer ein Zeitprofil zuzuordnen und somit ihre Gültigkeit zu steuern. Ist das Profil inaktiv, wird die Telefonnummer nicht verwendet und die nachfolgende Telefonnummer wird gewählt, wenn sie festgelegt ist.
- **2N® IP Eye Adresse** – stellt die Adresse des Computers ein, der mittels einer speziellen UDP-Nachricht über den laufenden Anruf an die Telefonnummer des Nutzers informiert wird. Diese Nachricht nutzt die Applikation **2N® IP Eye** für das Abrufen des Anzeigens des Fensters mit dem Bild aus der Kamera, dessen Nutzung für die Nutzer vorteilhaft ist, die kein Videotelefon mit Display zu Verfügung haben. Die Adresse des Computers wird in der Form eingegeben: Domain[:**port1**][:**port2**], z.B.: computer.ihrefirma.cz oder 192.168.22.111. Die Parameter **port1** und **port2** sind optional und sie werden dann verwendet, wenn auf dem Weg zwischen dem Computer und dem Interkom die

Übersetzung der Adressen (NAT) ist und man muss die Ports im Einklang mit dem Router oder mit einer anderen NAT realisierenden Anlage einstellen. Der Parameter port1 (mit dem Ausgangswert 8003) gibt den Zielport für die UDP-Nachrichten an, die der Applikation **2N® IP Eye** gesendet werden. Der Parameter port2 (mit dem Ausgangswert 80) gibt den Zielort für die HTTP-Kommunikation der Applikation **2N® IP Eye** mit dem Interkom an.

Anmerkung

- *Die Funktion "Adresse IP Eye" ist nur bei ausgewählten Modellen der **Interkoms 2N IP** verfügbar (siehe Kapitel Modell-und Lizenzenaufstellung).*
- *Wenn für die Anlage die Funktionen Enhanced Integration nicht lizenziert sind, kann man die Schlösser nur beim laufenden Anruf bedienen. Wenn ein Anruf mit einem Nutzer stattfindet, bei dem die Adresse **2N® IP Eye** ausgefüllt ist, ist für das Öffnen des Schlosses keine Lizenz erforderlich.*

Tipp

- FAQ: 2N® IP Eye – Wie man sie mit 2N IP Interkoms einstellt.

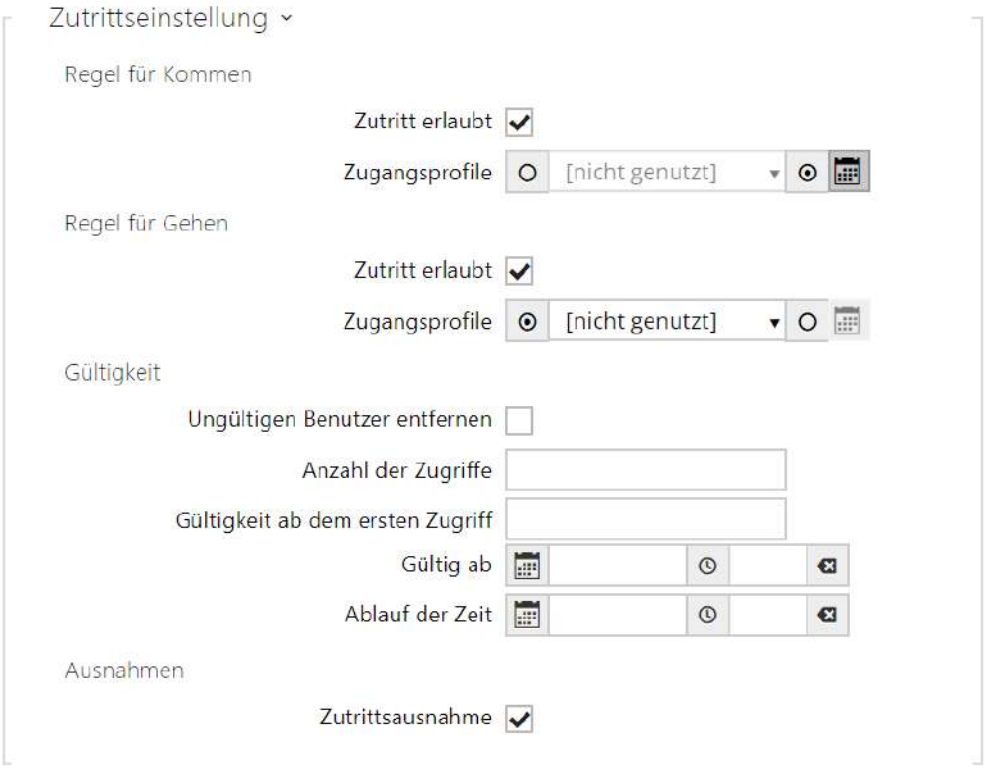
Tipp

- Video Tutorial: SW application for IP intercoms – 2N® IP Eye

- **In der Gruppe mit nachfolgender Nummer anrufen** – ermöglicht die Funktion des Gruppenanrufes, d.h. das Anrufen von mehreren Telefonnummern gleichzeitig einzustellen. Man kann die ersten zwei Nummern, die letzten zwei Nummern oder alle drei Nummern gleichzeitig anrufen. Nach der Annahme eines der Anrufe werden alle anderen Anrufe automatisch beendet.
- **In der Gruppe mit einem Vertreter anrufen** – ermöglicht die Funktion des Gruppenanrufes, d.h. das Anrufen von mehreren Telefonnummern gleichzeitig einzustellen. Man kann die ersten zwei Nummern, die letzten zwei Nummern oder alle drei Nummern gleichzeitig anrufen.. Nach Annahme eines der Anrufe werden die übrigen Anrufe automatisch beendet. Die Gesamtzahl der gleichzeitig angerufenen Nummern ist 16, wozu bei gleichzeitig benutzten Gruppenanruf und Einstellung mehreren Nummern auf einer Schnellwahltaste kommen kann.
- **Vertreter bei Unerreichbarkeit** – ermöglicht den Nutzer zu wählen, auf den im Fall der Unerreichbarkeit des jeweiligen Nutzers die Verbindung umgeleitet wird. Wählen Sie den Nutzer mittels der Taste Finden. Die Gesamtzahl der gleichzeitig angerufenen Nummern ist 16, wozu bei gleichzeitig benutzten Gruppenanruf und Einstellung mehreren Nummern auf einer Schnellwahltaste kommen kann.

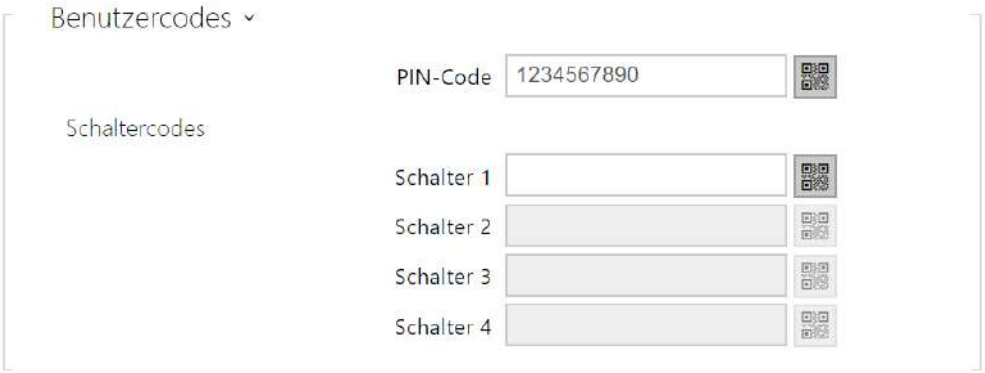
Anmerkung

- *Die Funktion "Vertreter bei Unerreichbarkeit" ist nur bei ausgewählten Modellen der **Interkoms 2N IP** verfügbar ((siehe Kapitel Modell-und Lizenzenaufstellung).*



- **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.

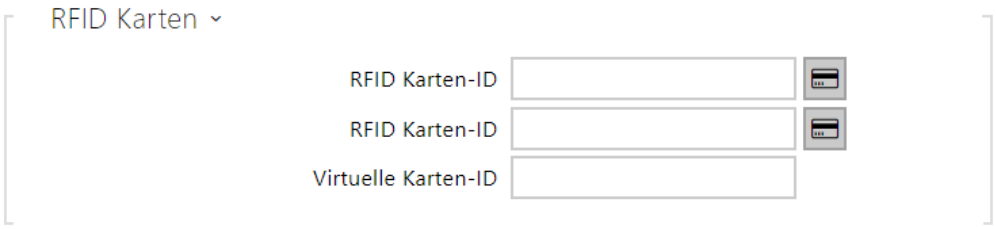
  - **Gültigkeit ab dem ersten Zugriff** – Legen Sie die Zeit fest, in der der Benutzer ab seiner ersten erfolgreichen Autorisierung gültig ist. Lassen Sie es leer für keine relative Gültigkeitsdauer. Relative Gültigkeit kann die Gültigkeitsdauer verkürzen, aber niemals verlängern. Die Zeit wird im Format 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 eigener privater QR-Code / Zahlencode zum Schließen des Schalters zugewiesen werden. Man kann die Nutzercodes der Schalter beliebig mit den Universalcodes der Schalter kombinieren, die im Menü **Hardware / Schalter** eingegeben sind. Wenn sich die Codes mit anderen in der Interkomkonfiguration schon eingegebenen Codes überlappen, dann erscheint bei diesen sich überlappenden Codes das Zeichen ⓘ.

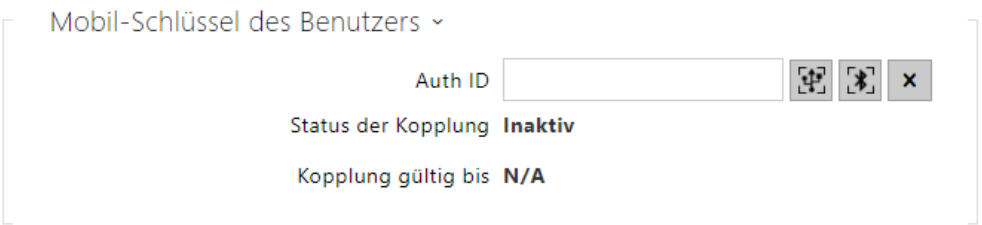
- **PIN-Code** – ermöglicht den persönlichen nummerischen Zutrittscode des Nutzers einzustellen. Der Code muss mindestens zwei Zeichen enthalten.
  - – generiert ein QR-Code-Bild. Codes mit weniger als 4 Stellen können aus Sicherheitsgründen nicht durch das Lesen des QR-Codes eingegeben werden. Die Codes 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 1–4** – 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 Interkomtastatur 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 Interkomnutzer können zwei RFID-Zutrittskarten zugeordnet werden.

- **RFID Karten-ID** – ermöglicht die ID der Zutrittskarte des Nutzers einzustellen. Jedem Benutzer können max. zwei Zugangskarten zugewiesen werden. 6–32 Zeichen, wobei 0–9, A–F möglich ist. ID der Zutrittskarte 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.
- **ID der virtuellen Karte** – 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. Für die Identifizierung des Nutzers wird die ID der virtuellen Karte auf Bluetooth oder auf biometrischem Scanner zur Wiegand-Schnittstelle gesendet, wenn in der Konfiguration (Türen / Regeln für Kommen / Fortgeschrittene Einstellung) das Absenden der Identifikatoren auf Wiegand eingestellt ist.



- **Auth-ID** – eindeutiger Identifikator des mobilen Geräts (bzw. ihres Nutzers). Der Parameterwert wird automatisch bei der Kopplung generiert. Man kann die Auth-ID auf einen anderen Nutzer verschieben ggf. es besteht die Möglichkeit sie in eine andere Anlage im Rahmen der gleichen Lokation zu kopieren.
- **Kopplungsstatus** – 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 Interkom

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.

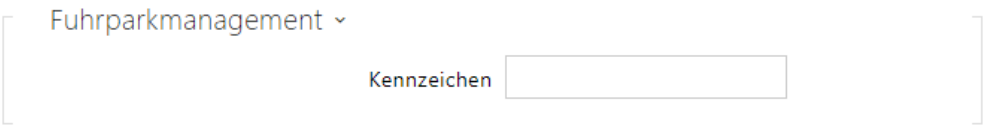
Ausführliche Informationen zu den Leistungseinstellungen **2N® Mobile Key** befinden sich im Kapitel 5.4.5 Mobile Key.

- **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 Anweisungen für das Einstellen der Nutzerfingerabdrücke.



Mit der 2N IP-Sprechanlage 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 Zutrittsregeln 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 in der Sektion Telefonbuch / Zeitprofile möglich.
    -  mit der Markierung wird die Auswahl von den vordefinierten Profile oder 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 Einstellungen der Anrufverbindung

Um mit anderen Endgeräten in IP-Netzwerken telefonieren zu können, ist es notwendig, das Gerät einem Kontakt im Adressbuch zuzuordnen.

Verbindung mit 2N-Geräten im lokalen Netzwerk

1. Stellen Sie sicher, dass die Funktion Lokale Anrufe auf beiden 2N-Geräten aktiviert ist.
2. Klicken Sie die Taste **Gerät finden**über der Tabelle an. Markieren Sie in der Liste das Gerät, mit dem Sie eine Verbindung herstellen möchten. Nach dem Hinzufügen des Geräts öffnet sich die Bearbeitung des neu hinzugefügten Benutzers.
3. In der Bearbeitung können Sie grundlegende Informationen zum Benutzer bearbeiten oder seine Zugriffsmöglichkeiten verwalten. Wenn Sie über den Ziffernblock telefonieren, stellen Sie dem Benutzer eine virtuelle Nummer ein.
4. Nach dem Speichern erscheint der Kontakt im Telefonbuch auf dem Display des Geräts. Wenn Sie Anrufe mit einer Taste am Gerät tätigen, müssen Sie dem Benutzer unter Hardware > Tasten eine Kurzwahltaste zuweisen, siehe 5.3.5 Tlačítka.
5. Für einen erfolgreichen Anruf muss der Dienst Lokale Anrufe auf dem angerufenen 2N-Gerät aktiviert sein.

Verbindung mit anderen Geräten

1. Erstellen Sie einen neuen Kontakt, indem Sie die Taste **Benutzer hinzufügen** oberhalb der Tabelle anklicken oder das Detail eines bestehenden Kontakts öffnen.
2. Klicken Sie auf das Stiftsymbol  neben dem Parameter „Telefonnummer“, um den Telefonnummerneditor zu öffnen.
3. Wählen Sie in der Bearbeitung den Anruftyp aus:

- *SIP* für einen über SIP getätigten Anruf,
- *rava* für Anrufe mit einem Creston-Gerät,
- *vms* für Anrufe mit der Axis Camera Station,
- *device* für Anrufe mit einem lokalen 2N-Gerät.

- Geben Sie im Zielfeld die Adresse des Anrufziels ein, an das der Anruf weitergeleitet werden soll. Geben Sie den SIP-URI in der Form *benutzername@host* oder die Ziel-IP-Adresse ein (z. B. *johana@255.0.255.0* oder *johana@calls.2N.com*). Geben Sie bei lokalen Anrufen die ID des angerufenen 2N-Geräts ein, siehe Lokale Anrufe in 5.4.1 Telefon.
- In der Bearbeitung können Sie grundlegende Informationen zum Benutzer bearbeiten oder seine Zugriffsmöglichkeiten verwalten. Wenn Sie über den Ziffernblock telefonieren, stellen Sie dem Benutzer eine virtuelle Nummer ein.
- Nach dem Speichern erscheint der Kontakt im Telefonbuch auf dem Display des Geräts. Wenn Sie Anrufe mit einer Taste am Gerät tätigen, müssen Sie dem Benutzer unter Hardware > Tasten eine Kurzwahltaste zuweisen, siehe 5.3.5 Tlačítka.

- Um einen Anruf erfolgreich tätigen zu können, muss der Dienst, der die Weiterleitung des Anrufs gewährleistet, auf dem angerufenen Gerät aktiviert sein.

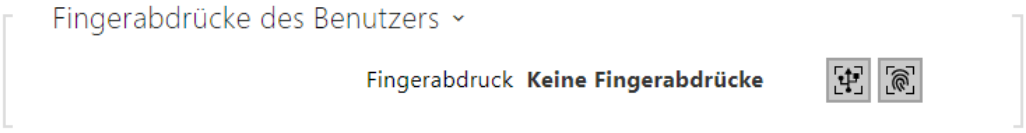
Tipp

- Jedem Benutzer können bis zu 3 Telefonnummern zugewiesen werden. Wenn der Benutzer die erste Telefonnummer nicht beantwortet, wird der Anruf an die nächste Nummer weitergeleitet. Alternativ ist es möglich, Anrufe zu mehreren Rufnummern gleichzeitig einzurichten. Das gleichzeitige Anrufen mehrerer Telefonnummern eines Benutzers wird durch Aktivieren des Kontrollkästchens *Gruppenanrufe* zwischen den angegebenen Telefonnummern eingestellt.
- Im Falle der Nichtverfügbarkeit aller Telefonnummern des Benutzers besteht die Möglichkeit, eine Anrufweiterleitung an einen Vertreter einzurichten.
- Benutzer können in Anrufgruppen gruppiert werden. Der Name der Anrufgruppe wird im Telefonbuch auf dem Display des Geräts angezeigt. Einer Kurzwahltaste kann eine Anrufgruppe zugewiesen werden. Soll der ausgehende Gruppenanruf bei der ersten Ablehnung durch einen der angerufenen Benutzer beendet werden, muss diese Funktion unter Dienste > Telefon > Anrufe eingestellt werden, siehe 5.4.1 Telefon.

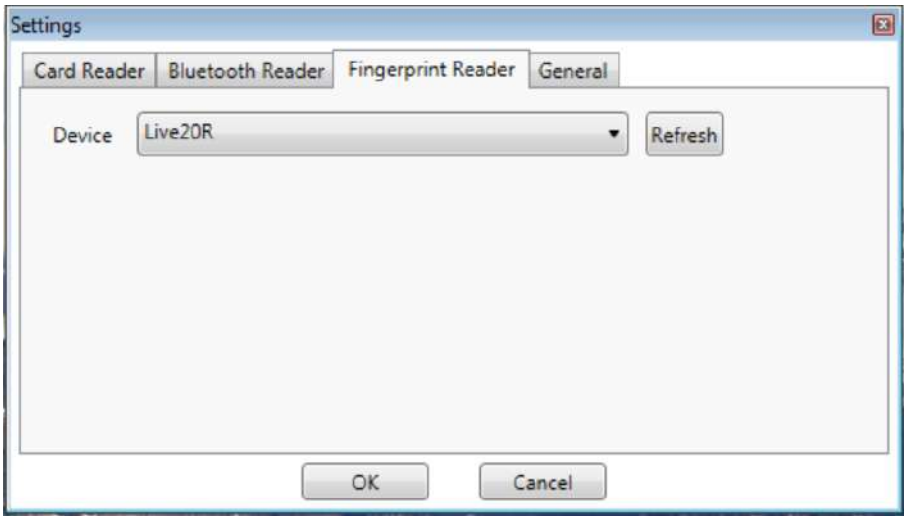
5.2.1.2 Anweisungen für das Einstellen der Nutzerfingerabdrücke

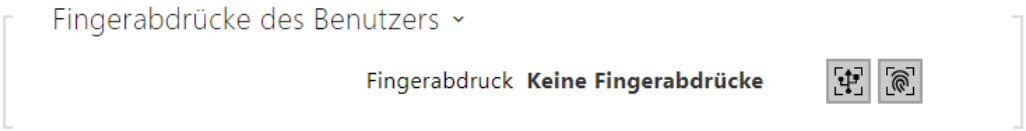
Die Fingerabdrücke kann man nur über den Fingerabdruckscanner **2N® IP Verso** (Best-Nr. 9155045) oder den externen USB-Fingerabdruckscanner (Best-Nr. 9137423E) einlesen. Das Vorgehen ist folgendes:

1a) Das Einlesen über das Modul des Fingerabdruckscanners **2N® IP Verso** kann man über die Webschnittstelle der Anlage beim konkreten Nutzer im Abschnitt Verzeichnis / Nutzer / Nutzerfingerabdrücke mittels der Wahl über den Fingerabdruckscanner einlesen  durchführen.



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  .





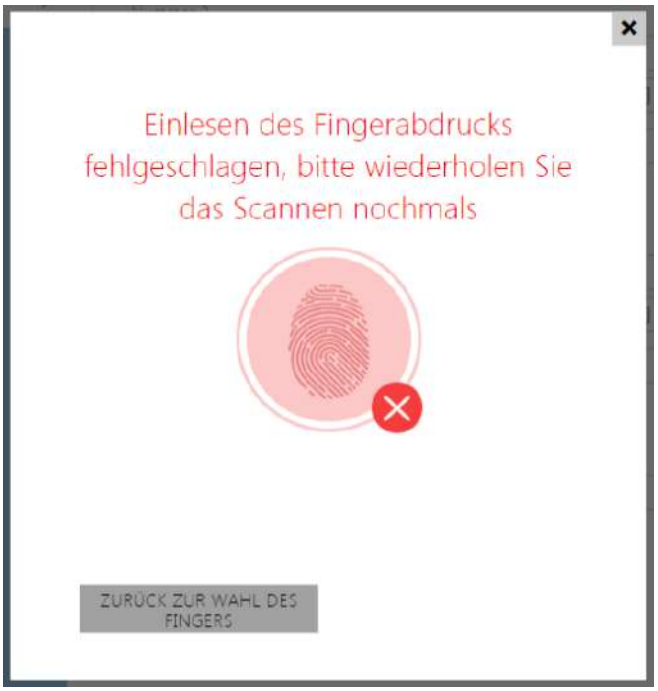
2) Durch Anklicken den Finger zum Einlesen des Fingerabdruckes wählen.

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. Wiederholen Sie der höheren Genauigkeit wegen dieses Vorgehen, insgesamt dreimal.

Bei Nichtübereinstimmung des Einlesens der Fingerabdrücke diesen Prozess wiederholen.

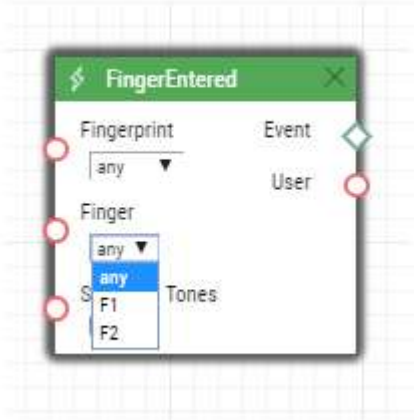


5) Wenn das Einlesen des Fingers in Ordnung verlaufen ist, mit dem Klicken auf die Taste FERTIG bestätigen.

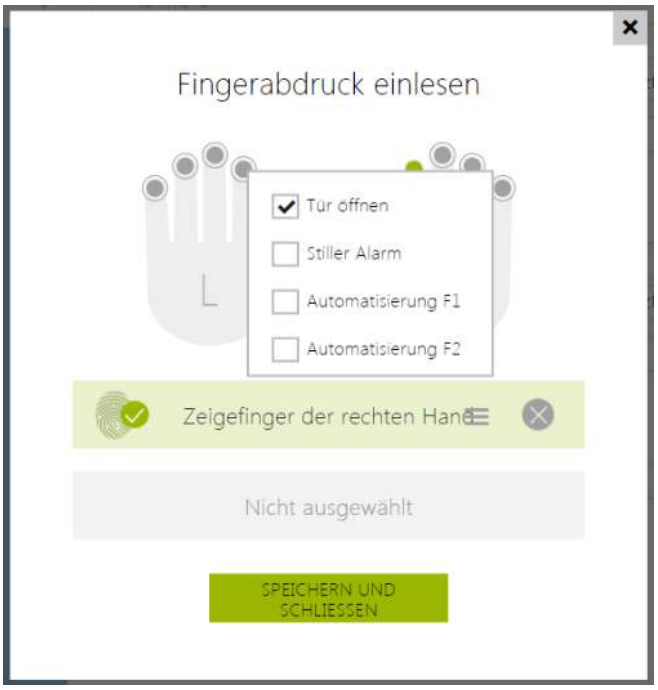
Für die Einstellung der Fingerfunktion auf die Schaltfläche des Menüs klicken

, das Angebot der verfügbaren Funktionen wird angezeigt:

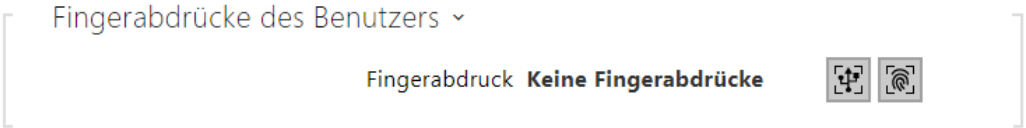
- Tür öffnen
- SilentAlarm. Kann man nur im Fall der aktiven Funktion Öffnen der Tür einstellen.
- Die Automatisierung F1 – generiert das Ereignis FingerEntered in Automation. F1 dient der Unterscheidung des angelegten Fingers in Automation.
- Automatisierung F2 – generiert das Ereignis FingerEntered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



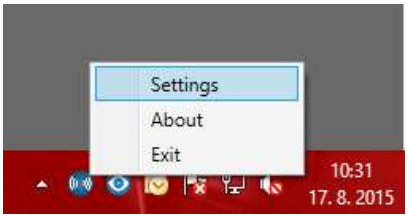
6) In der Registerkarte Nutzer kann man die aktuelle Einstellung kontrollieren.



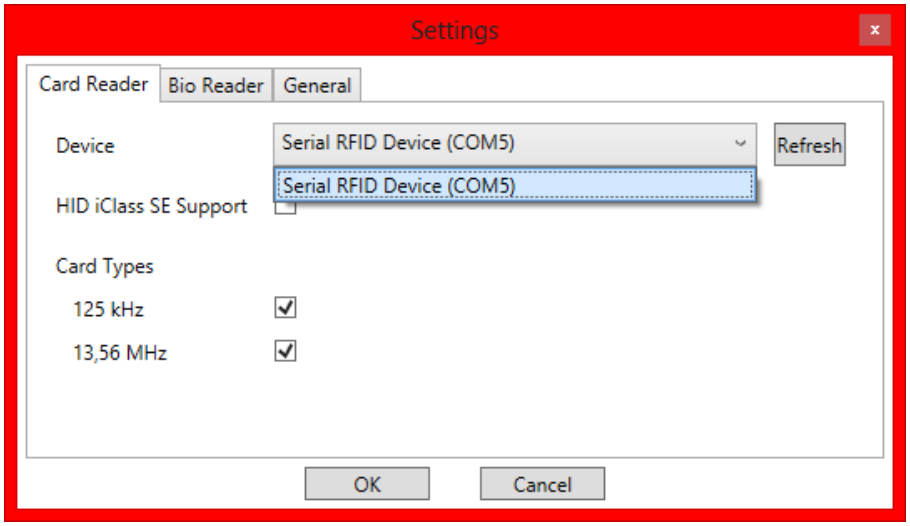
5.2.1.3 USB-RFID-Kartenleser

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

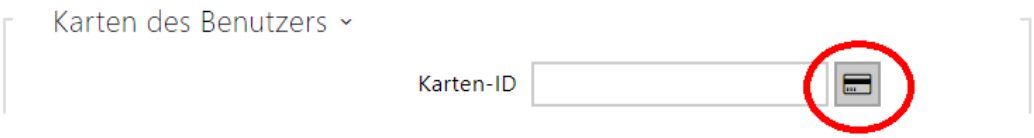
1. Gehen Sie in die Einstellung des **2N IP USB-Drivers**



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

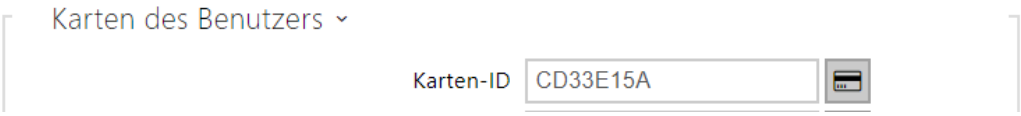


3. Auf der Webseite des 2N IP Interkoms beim Nutzer die Taste des Karteneinlesens drücken



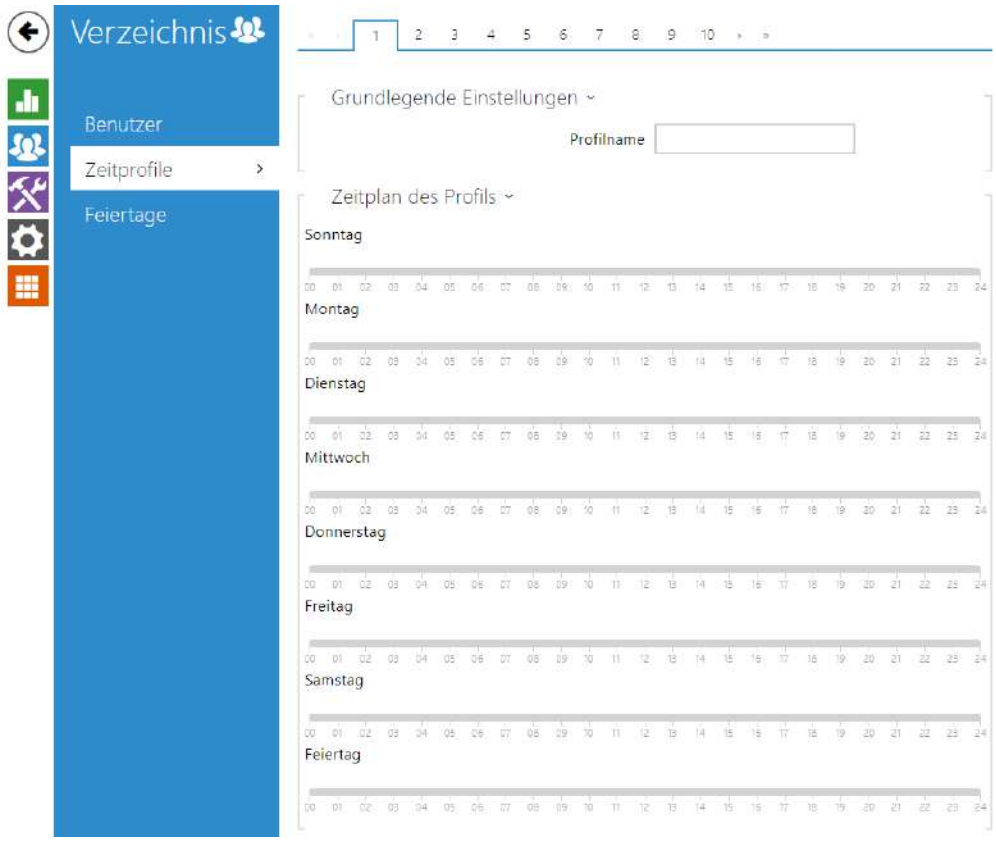
4. Legen Sie die Karte an den Leser an

5. Die Karte ist eingelesen



Vergessen Sie nicht, die Konfiguration zu speichern.

5.2.2 Zeitprofile



Man kann ausgewählte Interkomfunktionen, wie z.B. ausgehende Anrufe, 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

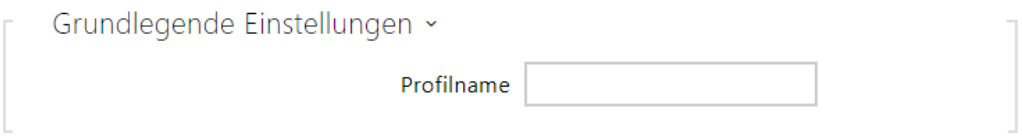
Jedes Zeitprofil definiert die Verfügbarkeit der Funktion, mit der es mittels des Wochenkalenders verbunden ist. Man kann einfach die Zeit von–bis und ggf. die Tage in der Woche einstellen, an denen die Funktion verfügbar sein soll. Die **2N IP Interkoms** ermöglichen bis zu 20 verschiedene Zeitprofile zu erstellen (bei einzelnen IP-Modellen kann sich die Zahl der

Profile unterscheiden). Sie können der jeweiligen Funktion ein beliebig erstelltes Zeitprofil zuordnen, siehe Einstellung Nutzer, Zutrittskarten, Schalter.

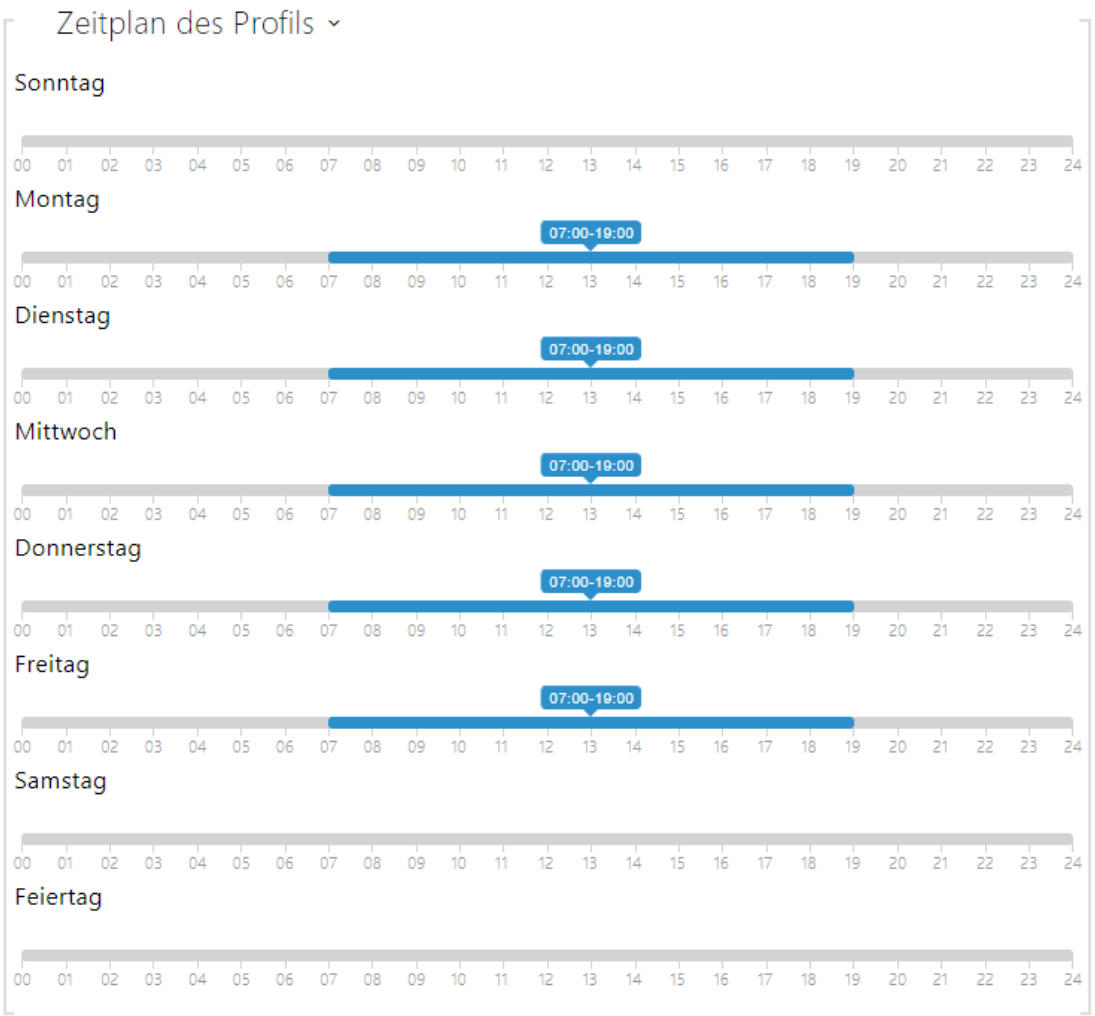
Sie können die Gültigkeit des Zeitprofils nicht nur mittels der Einstellung des Wochenkalenders, sondern auch mittels spezieller Aktivierungs- und Deaktivierungscodes steuern. Sie können die Aktivierungs-und Deaktivierungscodes jederzeit mittels der nummerischen Tastatur des Interkoms oder ihres Telefons (während des Anrufs über Interkom) 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



- **Profilname** – durch Sie gewählte Profilbezeichnung. Dieser Parameter ist optional und hilft Ihnen, Positionen in der Zeitprofilliste zu finden und Profile bei den Schalter-, Karten- und Telefonnummerneinstellungen einfacher zu finden.



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 Anrufen

Das Anrufen ist die Grundfunktion der Gegensprechanlage - sie ermöglicht Ihnen, eine Verbindung mit anderen Endgeräten in IP-Netzwerken herzustellen. Die **Interkoms 2N IP** unterstützen das erweiterte SIP-Protokoll und sind mit renommierten Herstellern der SIP-Zentralen und Endanlagen kompatibel und durch sie zertifiziert – CISCO, Avaya, Broadsoft u.a.

Das Interkom unterstützt bis zu fünf parallel laufende Anrufe – 1 ausgehenden und bis 4 eingehende. Nur einer der laufenden Anrufe kann **aktiv** sein – der Audiostream ist mit dem Mikrophon und dem Lautsprecher und der Videostream mit der Kamera verbunden. Die anderen Anrufe sind immer **nicht aktiv** – das Mikrophon und der Lautsprecher sind leise gestellt und das Interkom empfängt nur die DTMF-Zeichen, mithilfe deren die andere Seite das Interkom steuern kann – Profile, Nutzer aktivieren/deaktivieren u.Ä.

Die Interkoms werden gewöhnlich vor allem für ausgehende Anrufe verwendet und eingehende Anrufe sind immer inaktiv – das Mikrophon und der Lautsprecher sind leise gestellt. Sie können sie jedoch so konfigurieren, dass eingehende Anrufe aktiv sind und mit einem Klingelton signalisiert werden, siehe Kapitel 5.3.1 Obecné nastavení. Man kann den eingehenden Anruf mittels der Tasten * und # auf der nummerischen Tastatur annehmen und beenden.

Die **Interkoms 2N IP** verwenden für die Codierung (ggf. Kompression) die Audiostream-Protokolle **G.711**, **L16**, **G.722** und **G.729** (nach der Eingabe des Lizenzschlüssels). Die Breitbandcodecs L16 und G.722 sind nur bei ausgewählten **Interkoms 2N IP** verfügbar. Für die Kompression des Videostreams werden die Codecs **H.263** oder verwendet **H.264**. Mittels der Einstellung in der Registerkarte Audioanschl. Video können Sie Ihre Codecpräferenz wählen.

Erklärung der Begriffe der IP-Telefonie

- **SIP (Session Initiation Protocol)** – Protokoll für die Übertragung der Signalisierung der Telefonanrufe, das in der IP-Telefonie verwendet wird. Das Protokoll dient primär dem Anknüpfen, der Beendigung und der Umleitung von Verbindungen zwischen zwei SIP-Anlagen (in diesem Fall dem Interkom und einem anderen IP-Telefon). SIP-Anlagen können eine Verbindung direkt unter sich (Direct SIP Call – direktes Anrufen) anknüpfen, sie werden jedoch dafür gewöhnlich einen oder mehrere Server – SIP-Proxy und SIP-Registrar benutzen.
- **SIP-Proxy** – ein Server im IP-Netz, der für die Umleitung der Anrufe (Übergabe des Anrufs an eine weitere Entität, die näher am Ziel ist) verantwortlich ist. Auf dem Weg zwischen den Teilnehmern können ein oder auch mehrere SIP-Proxy sein.
- **SIP-Registrar** – ein Server im IP-Netz, der für die Registrierung der Teilnehmer in einem bestimmten Netzteil verantwortlich ist. Die Registrierung der SIP-Anlage ist in der Regel eine notwendige Bedingung dafür, dass der Teilnehmer für die anderen unter einer bestimmten Telefonnummer erreichbar wird. Der SIP-Registrar und der SIP-Proxy werden sehr oft gemeinsam auf einem Server installiert.
- **RTP (Real-Time Transport Protocol)** – Protokoll, dass das Standardformat der Pakete für die Audio- und Videoübertragung in IP-Netzen definiert. Die **2N IP** Interkoms nutzen dieses

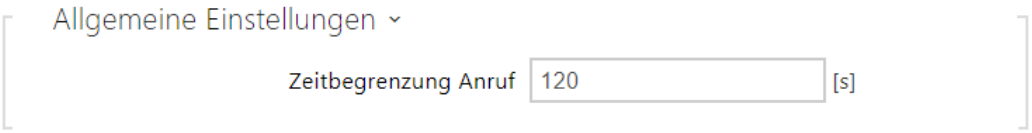
Protokoll für die Übertragung des Audio- sowie Videostreams im Verlauf des Anrufs. Die Parameter (Portnummern, Protokolle und Codecs) der Streams werden mittels des SDP-Protokolls (Session Description Protocol) definiert und ausgehandelt.

Die Interkoms **2N IP** unterstützen drei Arten der SIP-Signalisierung:

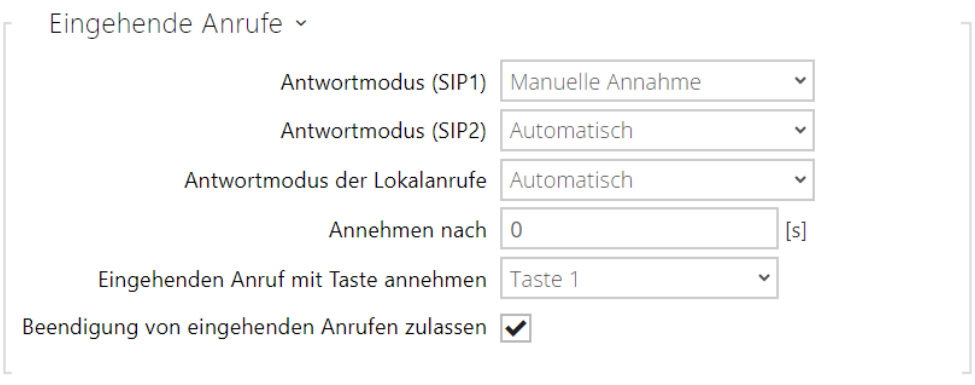
- mittels des **UDP**-Protokolls, was die übliche nicht gesicherte Signalisierungsart ist
- mittels des **TCP**-Protokolls, was eine weniger verbreitete, dennoch empfohlene Art der nicht gesicherten Signalisierungsart ist
- mittels des **TLS**-Protokolls, wo die SIP-Nachrichten gegen Abhören und Modifikation durch einen Dritten gesichert sind (gilt nicht für die Modelle **2N® IP Base**, **Uni**)

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

5.3.1 Allgemeine Einstellung



- **Zeitbegrenzung Anruf** – stellt die maximale Dauer des Anrufs ein, nach der er automatisch beendet wird. Das Interkom signalisiert das sich nähernde Ende des Anrufs mit einem Piepton in den Anruf 10 s vor seiner Beendigung. Geben Sie ein beliebiges DTMF-Zeichen in den Anruf ein (Taste # auf Ihrem IP-Telefon, z. B.), um die Dauer des Anrufes zu verlängern. Ist die maximale Gesprächsdauer auf 0 eingestellt und SRTP nicht verwendet wird, ist das Gespräch zeitlich nicht begrenzt.



- **Antwortmodus SIP1, SIP2** – stellt die Art ein, auf die das Interkom eingehende Anrufe empfangen wird. Man kann aus drei Möglichkeiten wählen:

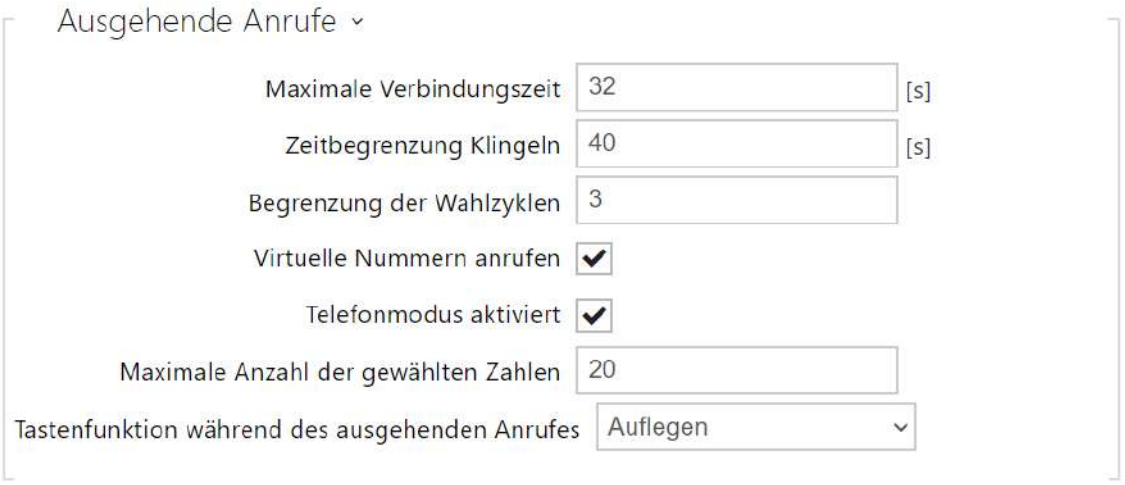
    - **Immer besetzt** – das Interkom lehnt eingehende Anrufe ab
    - **Manuelle Annahme** – das Interkom signalisiert eingehende Anrufe mittels Klingelton und der Nutzer kann sie mittels einer Taste auf der nummerischen Tastatur annehmen
    - **Automatisch** – das Interkom nimmt den eingehenden Anruf automatisch an. Den Modus der Anrufannahme für jedes SIP-Konto unabhängig einstellen.
    - **Automatisch (nur DTMF)** – Interkom nimmt den eingehenden Anruf automatisch nur für DTMF Empfang an, ohne Anschluss zum Mikrofon und Lautsprecher.
    - **Automatisch (ausgeblendet)** – die Gegensprechanlage nimmt einen eingehenden Anruf automatisch an, ohne die Identität des Anrufers oder ein entsprechendes Zeichen anzuzeigen.
- **Antwortmodus der Lokalanrufe** – stellt die Art ein, auf die das Interkom eingehende Lokalanrufe empfangen wird.
    - **Immer besetzt** – das Interkom lehnt eingehende Anrufe ab
    - **Manuelle Annahme** – das Interkom signalisiert eingehende Anrufe mittels Klingelton und der Nutzer kann sie mittels einer Taste auf der nummerischen Tastatur annehmen
    - **Automatisch** – das Interkom nimmt den eingehenden Anruf automatisch an. Den Modus der Anrufannahme für jedes SIP-Konto unabhängig einstellen.
    - **Automatisch (ausgeblendet)** – die Gegensprechanlage nimmt einen eingehenden Anruf automatisch an, ohne die Identität des Anrufers oder ein entsprechendes Zeichen anzuzeigen.
- **Annehmen nach** – die Zeit, nach der der Anruf automatisch im automatischen Beantwortermodus angenommen wird. Wenn einer der Beantwortermodi auf einem Gerät mit **Anrufbeantworterunterstützung** aktiviert ist, wird der Anruf nach dieser Zeit angenommen und die ausgewählte Nachricht sowohl im automatischen als auch im manuellen Beantwortermodus abgespielt. Wenn dieser Wert 0 ist, wird die Nachricht sofort abgespielt. Gemeinsam für alle SIP-Konten.
- **Eingehenden Anruf mit Taste annehmen** – aktiviert Annahme der eingehenden Anrufe mit ausgewählter Schnellwahltaste. Bei Einstellung auf 'Keine' ist die Funktion deaktiviert.

Hinweis

- Die Funktion Eingehende Anrufe mit Taste entgegennehmen wird bei **2N® IP Force** und **2N® IP Vario** mit Tastatur nicht angezeigt. Mit diesen Modellen ist es möglich, einen eingehenden Anruf über die mit einem grünen Hörer auf der Tastatur gekennzeichnete Taste anzunehmen, ohne dass eine vorherige Einstellung erforderlich ist.

- **Beendigung von eingehenden Anrufen zulassen** – ermöglicht es den Benutzern, das Gespräch mittels Gegensprechanlage abzulehnen oder zu beenden. Wenn die Funktion ausgeschaltet ist, funktioniert die Hörertaste für das Ablehnen oder das Beenden des Gesprächs nicht und auf dem Display wird das Symbol für das Ablehnen oder das Beenden

des Gesprächs nicht angezeigt. Das Gespräch kann weiterhin durch Beginn eines neuen ausgehenden Anrufs aus der Gegensprecheanlage unterbrochen werden.



- **Maximale Verbindungszeit** – Legt die maximale Verbindungszeit für ausgehende Anrufe fest, nach deren Ablauf sie automatisch beendet werden. Wenn die Anrufe über GSM-Gateways in das GSM-Netz geleitet werden, ist es ratsam, den Wert auf eine Zeit größer als 20 s einzustellen.
- **Zeitbegrenzung Klingeln** – stellt die maximale Dauer des Aufbaus und des Klingelns ein, nach der ausgehende Anrufe beendet werden. Wenn Anrufe in das GSM-Netz mittels der GSM-Gateway geleitet werden, sollte der Wert auf mehr als 20 s eingestellt werden. Minimaler Wert 1 s, maximaler Wert 600 s. Zum Ausschalten des Zeitparameters 0 einstellen.
- **Begrenzung der Wahlzyklen** – stellt die maximale Zahl der Wahlzyklen des Vertreters bei Unerreichbarkeit beim Anrufen des Nutzers im Telefonbuch ein. Diese Funktion hilft, die Sperre zu vermeiden, wenn der Parameter Vertreter bei Unerreichbarkeit im Telefonbuch auf den gleichen Nutzer eingestellt ist. Möglichkeiten zum Einstellen von Anrufzykluslimits sind in Unterkapitel 5.4.1.1 Limit volacích cyklů.
- **Gruppengespräche bei der ersten Ablehnung beenden** – Erlaubt dem Gerät, alle Gespräche im ausgehenden Gruppengespräch zu beenden, wenn eine der angerufenen Destinationen das Gespräch ablehnt.
- **Virtuelle Nummern anrufen** – ermöglicht das Aufrufen festgelegter virtueller Benutzernummern.
- **Modus für Anruf auf Etagen und in Wohnungen** – aktiviert den spezialen Anrufmodus auf Etage und Wohnung. In diesem Modus wird auf der nummerischen Tastatur die virtuelle Nummer des zugeordneten Teilnehmers eingegeben. TDiese Funktion ist nur am **2N® IP Vario** vorhanden. Etagen- und Wohnungscode wird ins Feld Virtuelle Nummer eingegeben. Er kann Ziffern und Buchstaben A-F enthalten.
- **Telefonmodus aktiviert** – aktiviert die Option zur direkten Herstellung der Verbindung zu den Telefonnummern, die über die numerische Tastatur der Sprechanlage gewählt

werden. Geben Sie die Reihenfolge der Telefonnummer ein, um die Verbindung herzustellen.

Tipp

- Der Aufbau des Anrufs auf eine Telefonnummer bei **2N® IP Force** und **2N® IP Vario** ist mittels der Reihenfolge der Tasten **Telefonnummer** , bei **2N® IP Verso** **Telefonnummer** und bei **2N® IP Verso** mit Display **Telefonnummer** und Drücken der Schaltfläche**Anrufen** möglich. Wenn das Schlusszeichen (die Taste im Fall der Tastatur bei **2N® IP Verso**) nicht verwendet wird, wird die Wahl nach dem Ablauf des Zeitlimits für die Codeeingabe automatisch bestätigt, als ob die Taste (die Taste im Fall der Tastatur bei **2N® IP Verso**) gedrückt würde.

- **Maximale Anzahl der gewählten Zahlen** – legt die maximale Anzahl von Zahlen für eine Telefonnummer im Telefonmodus fest. Ist diese Grenze erreicht, wird die Telefonnummer automatisch gewählt, ohne dass die Taste * betätigt werden muss.
- **Tastenfunktion während des ausgehenden Anrufes** – stellt die Schnellwahltastenfunktion während eines ausgehenden Anrufs ein. Sie können nur die Taste einstellen, der den Anruf initiiert hat.

- **Ausgangs-RTP-Port** – stellt den lokalen RTP-Anfangs-Port im Umfang von der Länge von 64 Ports ein, die bei der Audio-und Videoübertragung verwendet werden. Der voreingestellte Wert ist 4900 (d.h. der angewendete Umfang ist 4900–4963). Der Parameter ist für beide SIP-Konten gemeinsam und wird nur beim Konto 1 eingestellt.
- **RTP-Zeitüberschreitung** – stellt das Zeitlimit für den Empfang der RTP-Pakete des Audiostreams im Rahmen des Anrufs ein. Wird dieses Limit überschritten (RTP-Pakete werden nicht geliefert), wird der Anruf durch das Interkom beendet. Stellen Sie den Parameter auf 0 ein, um diese Funktion zu deaktivieren. Der Parameter ist für beide SIP-Konten gemeinsam und wird nur beim Konto 1 eingestellt.
- **Erweiterte SIP-Protokollierung** – ermöglicht das Schreiben detaillierterer Informationen zur SIP-Telefonie in Syslog (nur für die Fehlerbehebung vorgesehen).

5.3.1.1 Limit der Anrufzyklen

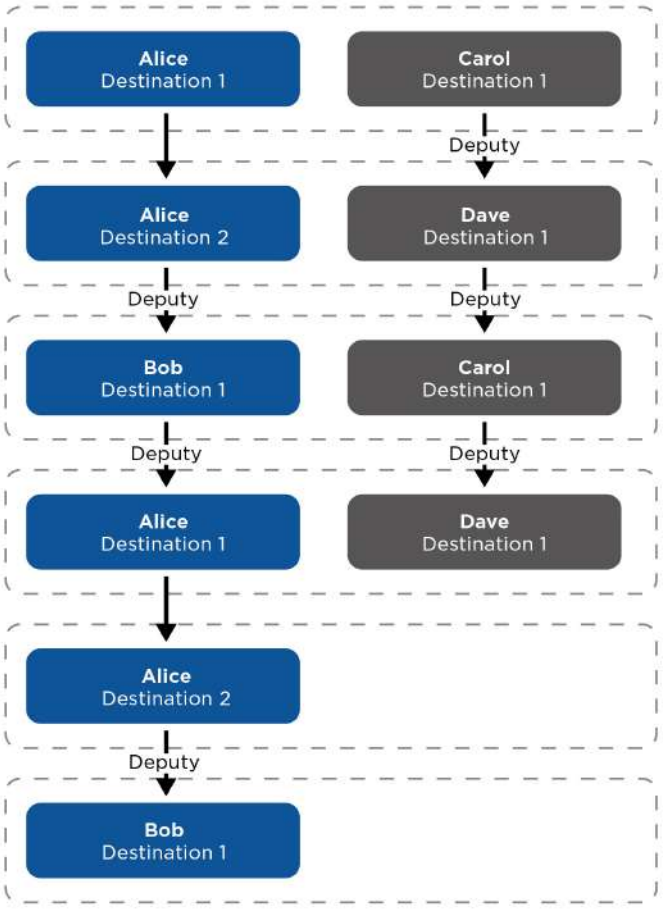
Dieser Parameter bestimmt die maximale Anzahl aufeinanderfolgender Anrufe, die an der anrufenden Station (Destination) generiert werden, falls ein Anrufzyklus von Vertretern im Falle der Nichtverfügbarkeit festgelegt wird (das einfachste Beispiel für einen Anrufzyklus ist, wenn sich ein Benutzer selber als Vertreter konfiguriert, ein weiteres Beispiel ist, wenn zwei Benutzer als gegenseitige Vertreter konfiguriert werden).

Beispiel 1

Der Algorithmus löst zunächst die Zweige des Schemas unabhängig voneinander. Im folgenden Beispiel werden die Benutzer Alice und Carol unter einer Taste konfiguriert (durch Drücken der Taste werden zwei parallele Anrufe gleichzeitig getätigt). Das Limit der Anrufzyklen ist auf 2 eingestellt. Alice hat zwei Telefonnummern (Anrufstation), andere Benutzer haben nur eine Anrufstation. Die Vertreter sind wie folgt konfiguriert:

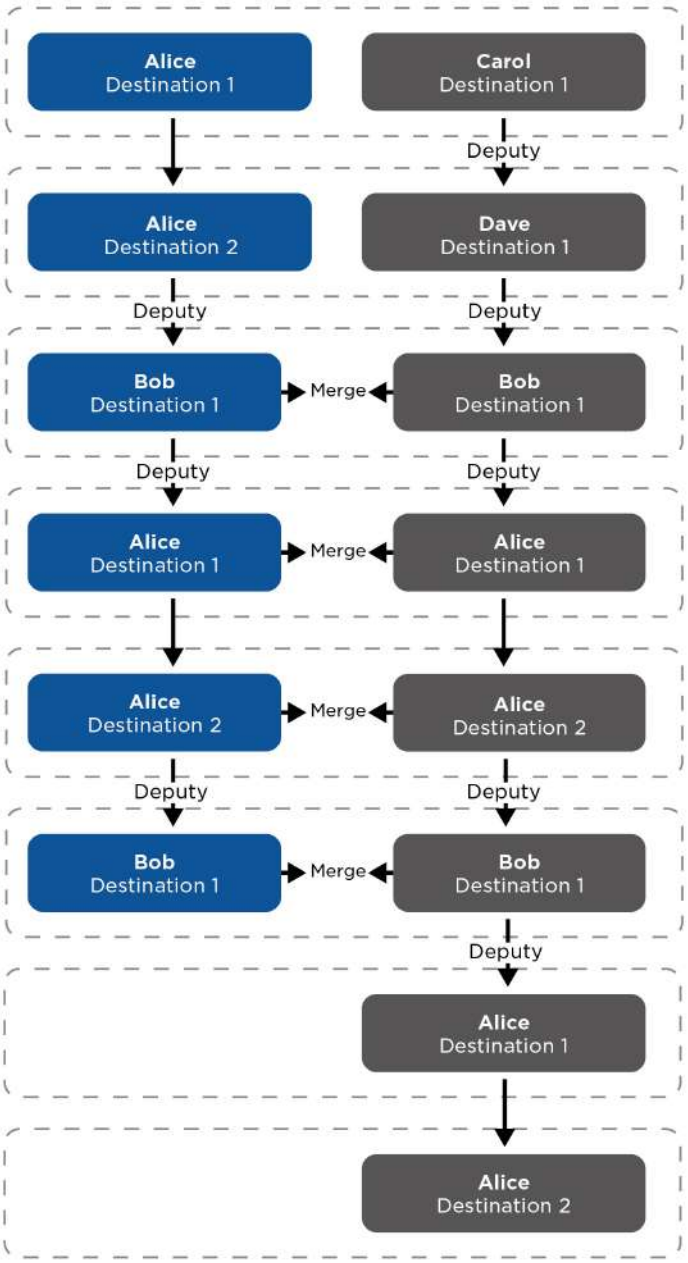
- Alice ist Bobs Vertretung
- Bob ist Alices Vertretung
- Carol ist Daves Vertretung
- Dave ist Carols Vertretung

Das resultierende Anrufschema lautet wie folgt (falls niemand den Anruf beantwortet oder ablehnt):



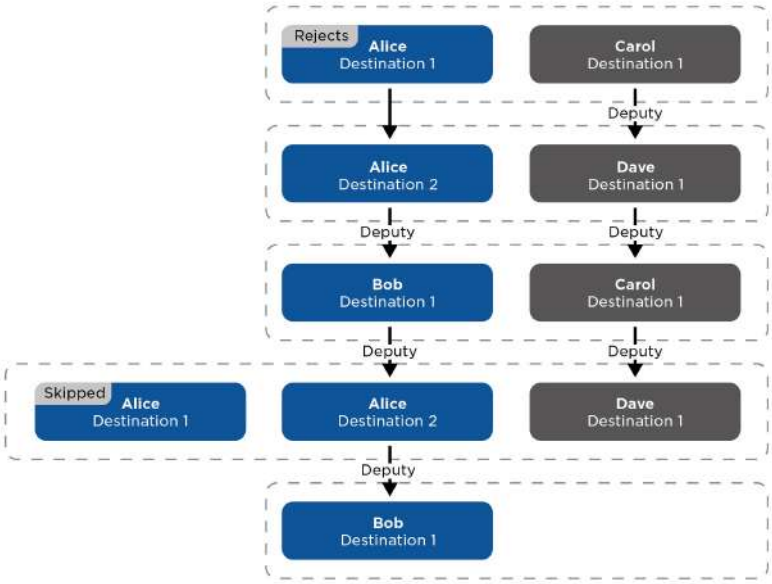
Beispiel 2

Nehmen wir das vorherige Beispiel und ändern Daves Vertretung auf Bobs Vertretung. Dies verbindet die beiden Zweige (ab Schritt 3 findet nur noch ein Anruf statt). Aus der Grafik ist auch ersichtlich, dass Alice schließlich dreimal aufgerufen wird. Dies liegt daran, dass das Limit der Anrufzyklen für jeden Zweig separat gilt und Alice tatsächlich nur zweimal auf dem blauen Zweig und auch nur zweimal auf dem lila Zweig angerufen wird.



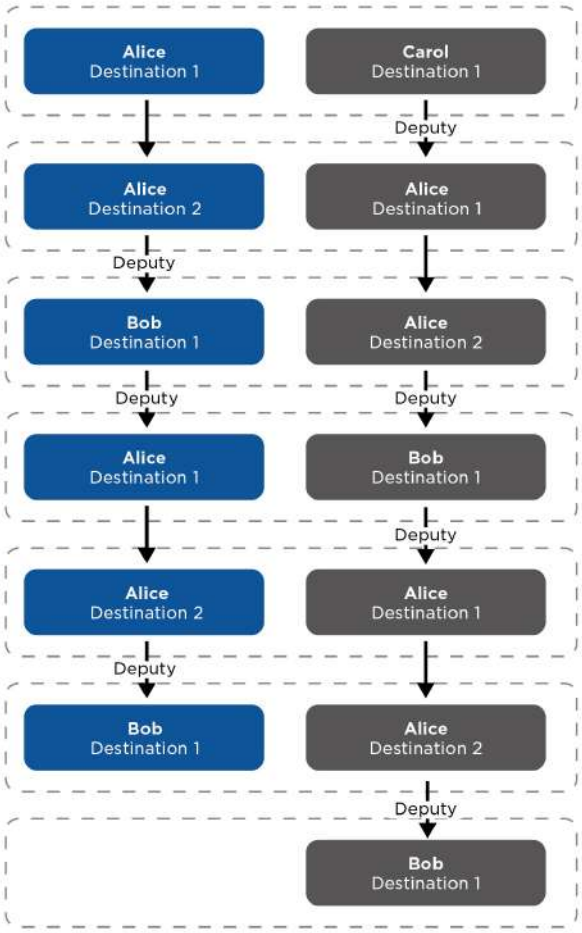
Beispiel 3

Nehmen wir die Konfiguration aus Beispiel 1 und betrachten eine Situation, in der Alice einen Anruf von ihrer ersten Station ablehnt. Der Algorithmus überspringt dieses Ziel (da der Benutzer den Anruf aktiv abgelehnt hat und es keinen Sinn macht, ihn erneut anzurufen). Durch das Ablehnen von Anrufen von verschiedenen Anrufstationen ändern sich die Anrufgruppen in den einzelnen Schritten dynamisch. Das Überspringen einer Anrufstation, die einen Anruf abgelehnt hat, gilt für alle Zweige, unabhängig davon, an welchem Zweig der Anruf abgelehnt wurde.



Beispiel 4

Es kann vorkommen, dass zwei Anrufstationen eines einzelnen Benutzers gleichzeitig angerufen werden. Dies kann erreicht werden, indem das Schema ähnlich dem folgenden Bild eingestellt wird, aber auch Destinationen übersprungen werden, die den Anruf zuvor abgelehnt haben.

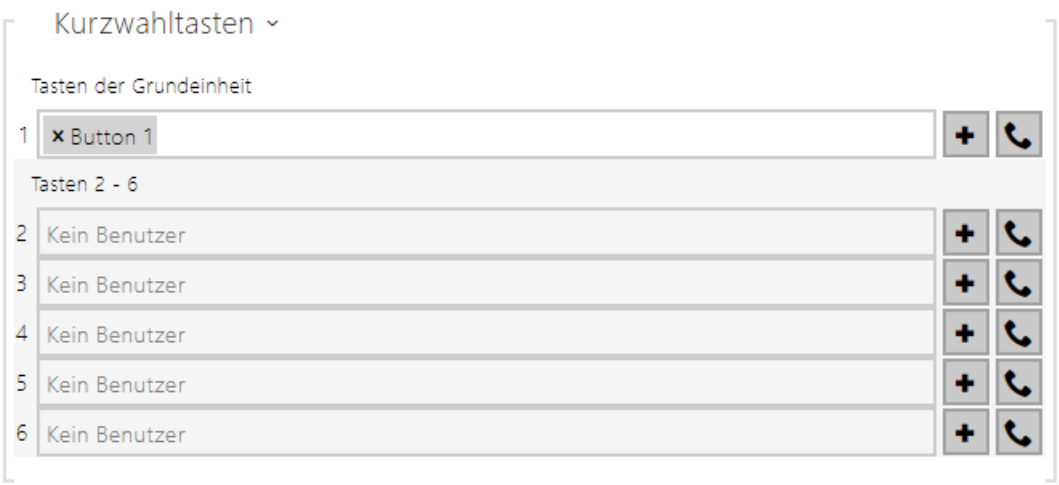


5.3.2 Wählen

Kurzwahltasten

Auf dieser Seite kann man den Kurzwahltasten die Nutzer zuordnen, die in der Nutzerliste auf der Seite **Verzeichnis > Nutzer** angeführt sind. Im Ausgangszustand sind alle verfügbaren Interkomtasten mit den Nutzern in der Liste verknüpft. Wenn eine Taste keinem Nutzer zugeordnet ist, dann kann man sie immerhin z.B. in der Automatisierung oder für das Schalten eines Schalters nutzen. Beim Modell **2N® IP Base** muss man zuerst die Zahl der Tasten im Menü Hardware > Erweiternde Module wählen.

- **Tastenzuordnung löschen** – alle Tastenzuordnungen zu Benutzern werden gelöscht.



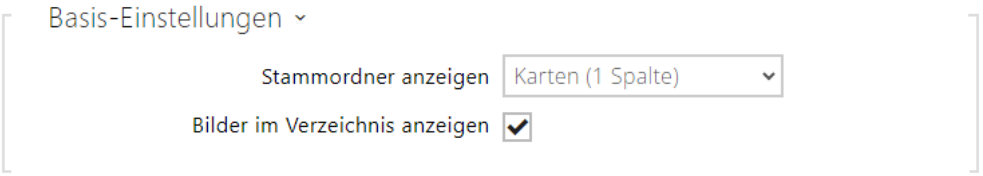
Zeigt die Liste aller potentiell verfügbaren Tasten auf dem Interkom an. Enthält die Liste der Tasten einschließlich jener, die im Interkom nicht physisch anwesend sind. Bei manchen Modellen (**2N® IP Vario**, **2N® IP Verso**) ist die Tastenliste in Gruppen je 8 bzw. 5 Tasten aufgeteilt, die den erweiternden Tastenmodulen entsprechen. In das Editierungsfeld kann manden Nutzer mittels der Schaltfläche  , mittels seiner Bezeichnung und durch die Bestätigung mit der Taste hinzufügen. Man kann den gefragten Nutzer auch in der Liste mittels des Fulltextfeldes über den Namen suchen. Eine Kurzwahltaste können mehrere Nutzer gleichzeitig teilen. Testen die eingestellte Schnellwahltaste kann man mit dem Symbol  . Nach dem Drücken der Taste wird ein Dialogfenster mit Detailangaben des laufenden Anrufs angezeigt (Teilnehmer, Richtung des Anrufs, Zustand, Ursache und Zeit des letzten Ereignisses).

Anmerkung

- Der Schnellwahltaste können bis zu 16 Benutzer hinzugefügt werden.
- Die Gesamtzahl der gleichzeitig angerufenen Nummern ist 16, wozu bei gleichzeitig benutzten Gruppenanruf und Einstellung mehreren Nummern auf einer Schnellwahltaste kommen kann.

Telefonbuch anzeigen

Auf dieser Registerkarte wird die strukturierte auf dem Display angezeigte Nutzerliste konfiguriert. Man kann die Liste in praktisch eine beliebige Gruppenzahl aufteilen und in jede der Gruppen eine beliebige Nutzerzahl aus dem Verzeichnis eingeben. Man kann einen Nutzer nicht mehrmals in eine Gruppe eintragen, aber jeder der Nutzer des Verzeichnisses kann sich in mehreren Gruppen gleichzeitig befinden.



- **Stammordner anzeigen** – Hier können Sie auswählen, ob der Stammordner des Adressbuchs auf dem Startbildschirm des Geräts angezeigt werden soll. Es ist möglich, die Anzeige in Karten (mit einem größeren Bild) oder die Anzeige der klassischen Artikelliste auszuwählen (die Anzeige von Bildern in der Artikelliste wird dann über die Einstellung Bilder anzeigen gesteuert). Die Einstellungen werden erst wirksam, wenn der Benutzer zu einem anderen Teil der grafischen Oberfläche wechselt (z. B. Suche).
- **Bilder im Verzeichnis anzeigen** – Hier können Sie auswählen, ob Bilder in der Verzeichnisanzeige auf dem Bildschirm angezeigt werden sollen, wenn sie in einer Artikelliste angezeigt werden.

Im linken Seitenabschnitt werden die erstellten Ordner sowie die eigentlichen Benutzer angezeigt. Einen neuen Ordner kann man mittels der Taste hinzugefügt werden. Das Verzeichnis einschließlich der eingegebenen Nutzer und Gruppen kann man mit der Taste

löschen. Eine bereits erstellte Gruppe kann durch Betätigen der Taste umbenannt werden. Ein Benutzer vom Hauptbaum des Verzeichnisses in den Ordner wird mit dem Symbol verschoben.

Im rechten Teil der Seite werden die Nutzer angezeigt, die aktuell in der ausgewählten Gruppe eingetragen sind. Mit der Taste kann ein Benutzer der Gruppe hinzugefügt werden, er bleibt aber auch im Hauptbaum des Verzeichnisses. Benutzer können durch Betätigen der Taste entfernt werden.

Gruppen und Benutzer werden alphabetisch auf dem Display aufgelistet. Die Reihenfolge der Gruppen und Benutzer kann man durch Zuordnung einer Priorität mit Symbol ändern. Die Verzeichnispositionen haben 8 mögliche Prioritäten. Bei Priorität 1 steht die Position am Anfang der Liste, bei keiner Priorität am Ende der Liste. Wenn es mehrere Positionen mit der gleichen Priorität gibt, werden sie gruppiert und alphabetisch sortiert.

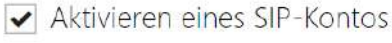
Hinweis

- Jede neue Einstellung des Verzeichnisses muss man immer speichern.
- Änderungen an den Einstellungen (Anzeige von Fotos, Stammordner, Inhalt usw.) werden erst wirksam, wenn das Display in das Such- oder Wählmenü wechselt.

5.3.3 SIP 1 / SIP 2

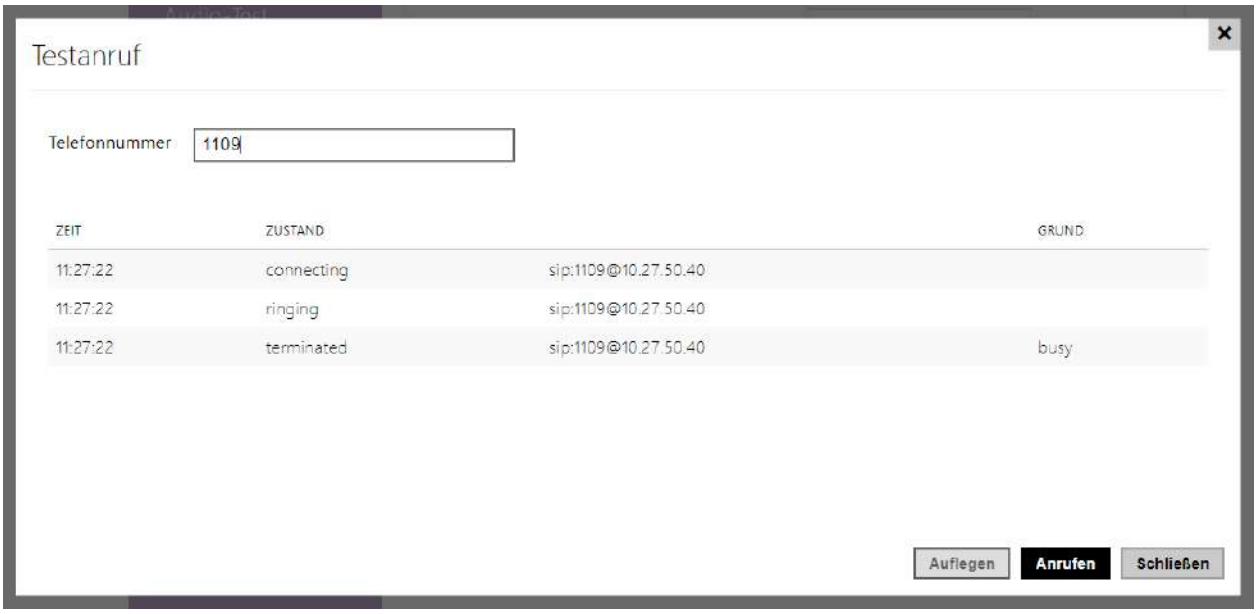
Die Interkoms **2N IP** ermöglichen zwei unabhängige SIP-Konten. Das Interkom kann so parallel unter zwei Telefonnummern, bei zwei verschiedenen SIP-Zentralen u.Ä. registriert sein. Aus der Sicht der eingehenden Anrufe sind beide SIP-Konten gleichwertig. Die ausgehenden Anrufe werden primär mittels des 1. Kontos realisiert. Falls das Konto SIP 1 nicht registriert ist (z.B. aus dem Grund einer Störung der SIP-Zentrale), wird für die ausgehenden Anrufe automatisch das Konto SIP 2. verwendet. Bei Telefonnummern im Telefonbuch kann man explizit die Nummer anführen, die für den ausgehenden Anruf verwendet werden soll (z.B. **2568/1** – Anrufen der Nummer 2568 mittels des Kontos SIP 1, **sip:1234@192.168.1.1/2** Anrufen der sip uri mittels des Kontos SIP 2).

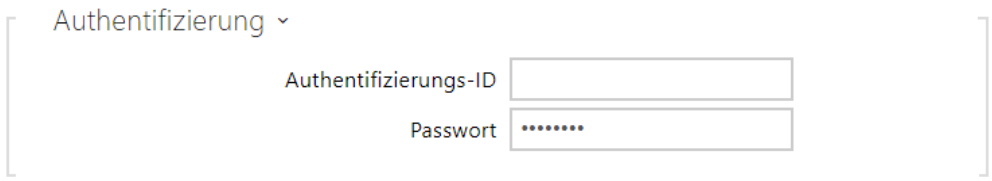
Registerkarte Konfiguration



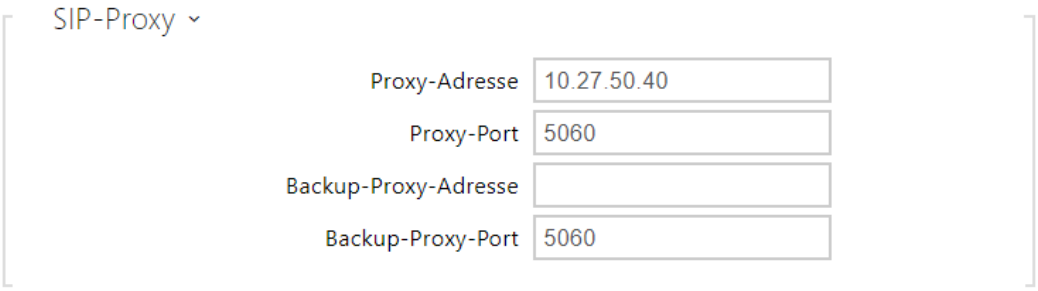
- **Aktivieren eines SIP-Kontos** – ermöglicht die Verwendung eines SIP-Kontos zum Telefonieren. Wenn das Konto nicht aktiviert ist, kann es nicht verwendet werden, um ausgehende Anrufe zu tätigen oder eingehende Anrufe zu empfangen.

- **Name anzeigen** – stellt den Namen ein, der auf dem Telefon des Angerufenen als die Identifizierung des Anrufers angezeigt wird.
- **Telefonnummer (ID)** – stellt die eigene Telefonnummer des Interkoms (ggf. eine andere eindeutige ID, die sich aus Zeichen und Ziffern zusammensetzt) ein. Diese Nummer zusammen mit der Domain identifiziert das Interkom eindeutig bei Anrufen und bei der Registrierung.
- **Domain** – stellt den Domainnamen des Dienstes ein, bei der das Interkom registriert ist. Stimmt gewöhnlich mit der SIP-Proxy- oder Registrar-Adresse überein.
- **Testanruf** – ruft das Dialogfenster mit der Möglichkeit einen Testanruf auf die gewählte Telefonnummer durchzuführen ab, siehe nachstehend.

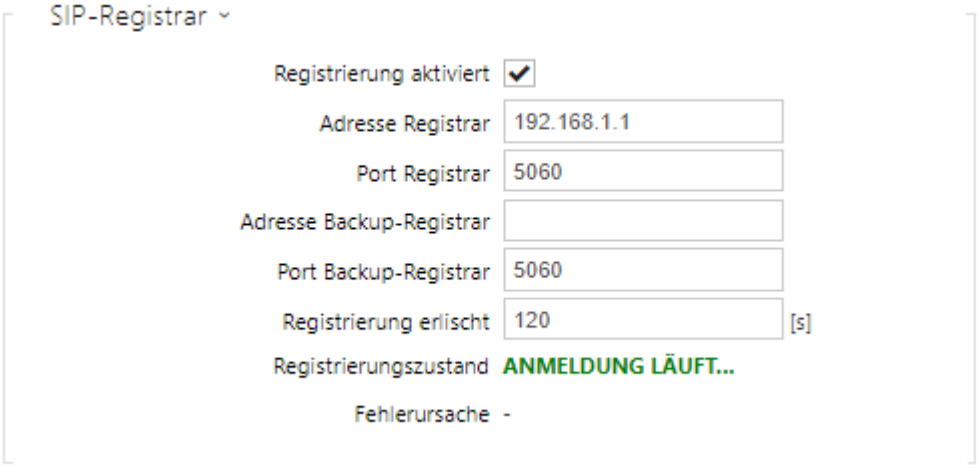




- **Authentifizierungs-ID** – alternative Benutzer-ID, die für die Geräteauthentifizierung verwendet wird. Wenn dieser Parameter leer ist, wird die Telefonnummer (ID) verwendet.
- **Passwort** – Passwort, das bei der Interkomauthentifizierung verwendet wird. Der Parameter wird nur angewendet, wenn Ihre PBX eine Authentifizierung verlangt.



- **Proxy-Adresse** – IP-Adresse oder der Domainname von SIP-Proxy.
- **Proxy-Port*** – stellt den Port SIP-Proxy ein. Das Gerät verwendet den Standardport gemäß Transportschicht (5060 oder 5061) oder den von DNS erhaltenen Port, wenn der Parameter leer oder auf 0 gesetzt ist.
- **Proxy-Backup-Adresse** – IP-Adresse oder Domainname von SIP-Proxy. Die Adresse wird in dem Fall angewendet, wenn der Hauptproxy nicht auf Anforderungen antwortet.
- **Backup-Proxy-Port*** – stellt den Port der Backup-SIP-Proxy ein. Das Gerät verwendet den Standardport gemäß Transportschicht (5060 oder 5061) oder den von DNS erhaltenen Port, wenn der Parameter leer oder auf 0 gesetzt ist.



- **Registrierung aktiviert** – erlaubt die Interkomregistrierung beim eingestellten SIP-Registrar.
- **Adresse Registrar** – IP-Adresse oder der Domainnamen von SIP-Registrar.

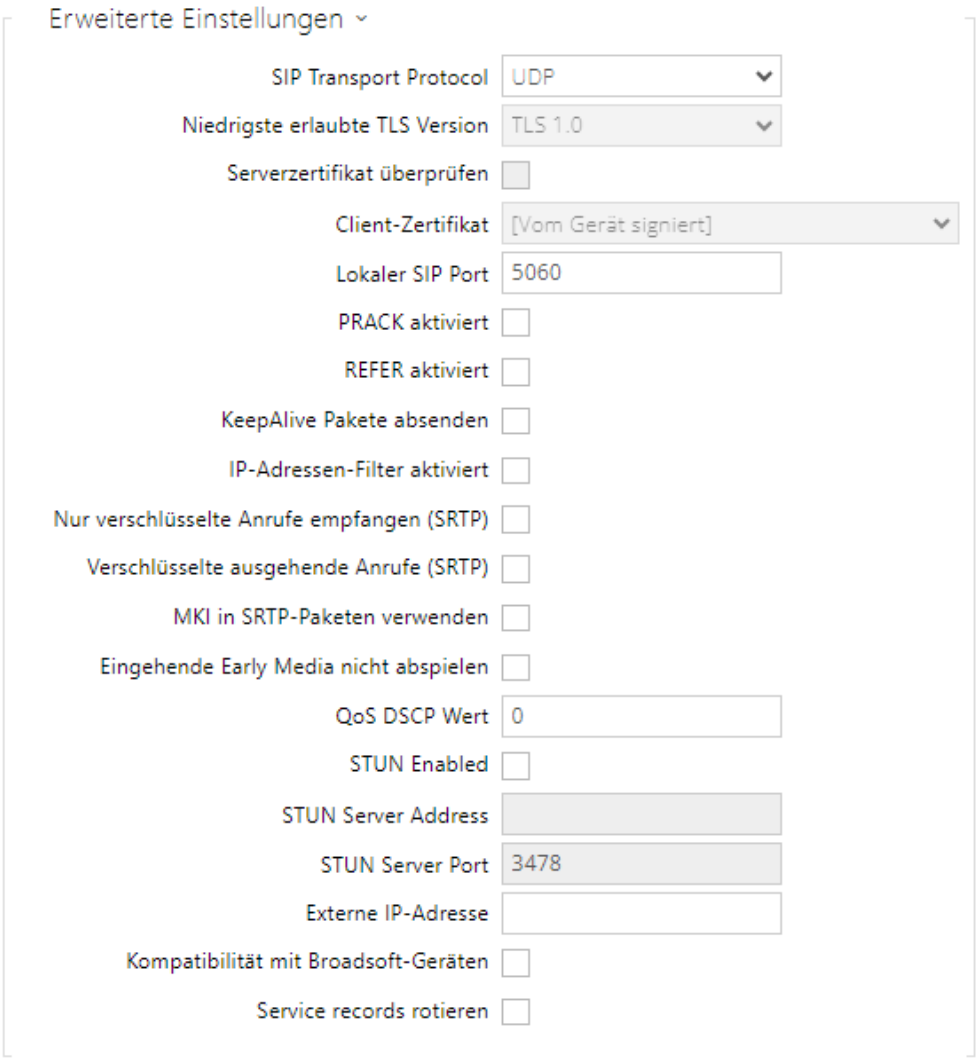
- **Port Registrar*** – stellt den Port des SIP-Registrars ein. Das Gerät verwendet den Standardport gemäß Transportschicht (5060 oder 5061) oder den von DNS erhaltenen Port, wenn der Parameter leer oder auf 0 gesetzt ist.
- **Adresse Backup-Registrar** – IP-Adresse oder Domainanme des Backup-SIP-Registrars. Die Adresse wird in dem Fall verwendet, wenn der Hauptregistrar nicht auf Anforderungen antwortet.
- **Port Backup-Registrar*** – stellt den Port des Backup-Registrars ein. Das Gerät verwendet den Standardport gemäß Transportschicht (5060 oder 5061) oder den von DNS erhaltenen Port, wenn der Parameter leer oder auf 0 gesetzt ist.
- **Registrierung erlischt** – ermöglicht die Zeit des Registrierungsablaufes einzustellen, was die Belastung des Netzes und den SIP-Registrars mit periodisch eingesandten Registrierungsanforderungen beeinflusst. SIP-Registrar kann die Gültigkeitsdauer ohne Ihre Kenntnis anpassen.
- **Registrierungszustand** – zeigt den aktuellen Registrierungsstatus an (Nicht registriert, Registrierung läuft..., Registriert, Registrierung wird beendet...).
- **Fehlerursache** – zeigt die Fehlerursache des letzten Registrierungsversuchs an – zeigt die letzte Fehlerantwort des Registrars, z.B. 404 Not Found an.

Tipp

- Den Outbound-Proxy kann man so einstellen, dass die Outbound-Proxy-Adresse sich in die Parameter Proxy-Adresse und Registrar-Adresse ausfüllt. Domain = Registraradresse.

Hinweis

- Wenn der **Parameter*** leer gelassen wird oder der Wert des Parameters 0 ist, wird der Standardport gemäß dem ausgewählten Transportprotokoll verwendet (5060 für TCP oder UDP, 5061 für TLS).



- **SIP Transport Protocol** – stellt das Protokoll ein, dass für die SIP-Kommunikation verwendet wird. Man kann zwischen UDP (Voreinstellung), TCP oder TLS wählen.

- **Niedrigste erlaubte TLS Version** – Legt die niedrigste erlaubte TLS Version fest, mit der man sich auf dem Server anmelden und Verbindungen herstellen kann.
- **Serverzertifikat überprüfen** – überprüft das öffentliche Zertifikat des SIP-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 SIP-Server überprüft wird.
- **Lokaler SIP Port** – stellt den lokalen Port ein, den das Interkom für die SIP-Signalisierung nutzt. Die Änderung dieses Parameters macht sich erst nach dem Neustart des Interkoms bemerkbar. Der voreingestellte Wert des Parameters ist 5060.
- **PRACK aktiviert** – erlaubt die PRACK-Methode (zuverlässiges Bestätigen der SIP-Nachrichten mit den Codes 101–199).
- **REFER aktiviert** – erlaubt die Umleitung der Anrufe mittels der REFER-Methode.
- **Keep Alive Pakete schicken** – stellt ein, ob das Interkom im Verlauf des Anrufs in regelmäßigen Zeitabständen den Status der angerufenen Station mittels SIP-OPTIONS-Anforderungen abfragen wird (dient der Erkennung eines Ausfalls der Station im Verlauf des Anrufs).
- **IP-Adressen-Filters aktiviert** – ermöglicht die Sperrfunktion des SIP-Pakete-Empfangs von anderen Adressen, als die SIP-Proxy- und die SIP-Registrar-Adresse sind. Der primäre Zweck der Funktion ist die Erweiterung der Kommunikationssicherheit und die Beseitigung von nicht autorisierten Anrufen.
- **Nur verschlüsselte Anrufe empfangen (SRTP)** – stellt die Einschränkung der eingehenden Anrufe auf diesem Konto auf ein, die mittels des SRTP-Protokolls verschlüsselte werden. Nicht verschlüsselte Anrufe werden abgelehnt. Gleichzeitig wird der größeren Sicherheit wegen empfohlen, TLS als Transportprotokoll für SIP zu verwenden.
- **Verschlüsselte ausgehende Anrufe (SRTP)** – stellt ausgehende Anrufe auf diesem Konto ein, die mittels des SRTP-Protokolls verschlüsselt werden. Gleichzeitig wird der größeren Sicherheit wegen empfohlen, TLS als Transportprotokoll für SIP zu verwenden.
- **MKI in SRTP-Paketen verwenden** – erlaubt die Verwendung der MKI (Master Key Indentifier - Schlüsselkennung), die von der Gegenseite zur Identifikation des Hauptschlüssels bei der Rotation mehrerer Schlüssel in den SRTP Paketen verlangt wird.
- **Eingehende Early Media nicht abspielen** – verhindert die Übertragung eines eingehenden Ton-Streams vor der Annahme des Gesprächs (Early-Medien), der von manchen Zentralen oder anderen Geräten versandt wird. Stattdessen soll der übliche lokale Klingelton ertönen.
- **QoS DSCP Wert** – stellt die Priorität der SIP-Pakete im Netz ein. Der eingestellte Wert wird im Feld TOS (Type of Service) im Kopf des IP-Pakets abgesendet. Der Wert wird als Dezimalstelle eingegeben.

Tip

Empfohlene QoS DSCP Werte			
	QoS dezimal	**QoS hexadezimal**	**Qos DSCP dezimal (ToS)**
Signalisierung	24 / 26	18 / 1A	96 / 104
Audio	46	2E	184
Video	40	28	160

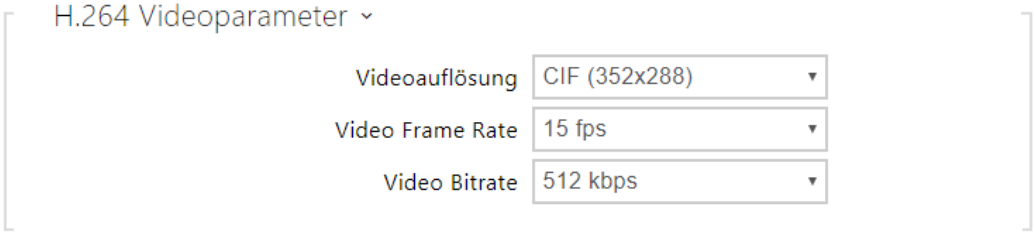
- **STUN aktiviert –** Aktivieren Sie die STUN-Funktionalität für das SIP-Konto. Die Adresse und Ports, die vom konfigurierten STUN-Server erhalten wurden, werden in SIP-Headern und SDP-Medienverhandlungen verwendet.
- **STUN-Serveradresse** – Legen Sie die IP-Adresse des STUN-Servers fest, der für dieses SIP-Konto verwendet wird.
- **STUN-Serverport –** Legen Sie den Port des STUN-Servers fest, der für dieses SIP-Konto verwendet wird.
- **Externe IP-Adresse** – stellen Sie die öffentliche IP-Adresse oder die Bezeichnung des Routers ein, an den das Interkom angeschlossen ist. Lassen Sie dieses Feld leer, wenn die IP-Adresse der Sprechanlage öffentlich ist.
- **Kompatibilität mit Broadsoft-Geräten** – Stellt den Kompatibilitätsmodus mit Broadsoft-Zentralen ein. Wenn in diesem Modus die Sprechanlage ein Re-invite von der Zentrale empfängt, antwortet sie statt komplettes Menü mit einer Wiederholung des zuletzt gesandten SDP mit aktuell genutzten Codecs.
- **Service records rotieren** – Aktiviert das Rotieren der SRV für SIP-proxy und Registrar. Das ist eine alternative Methode für Übergang zu Reserve-Server beim Ausfall oder bei Nichterreichbarkeit der Hauptserver.

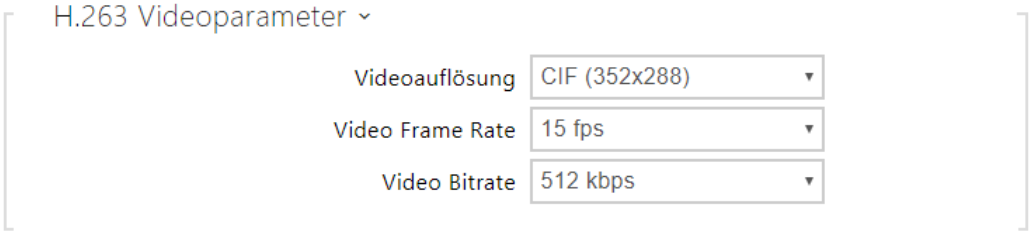
Hinweis

- Um die NAPTR/SRV-DNS-Abfrage zu verwenden, ist es erforderlich, die Porteinstellung für Proxy/Registrar aufzuheben.

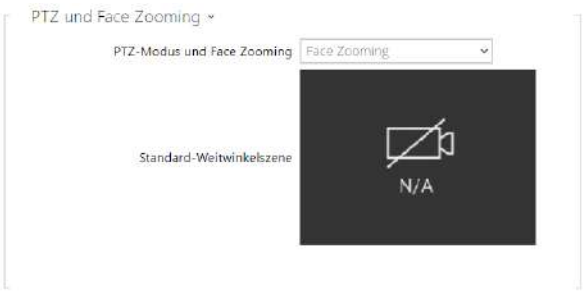
Registerkarte Video

- Ermöglicht die Verwendung einzelner Videocodecs zu erlauben/zu verbieten, die beim Aufbau der Verbindung angeboten werden, und ihre Priorität einzustellen.





- **Videoflösung** – stellt die Bildauflösung bei Telefonanrufen ein.
- **Video Frame Rate** – stellt die Aufnahmefrequenz des Videos bei Telefonanrufen ein.
- **Video Bitrate** – stellt die Übertragungsgeschwindigkeit des Videostreams bei Telefonanrufen ein.



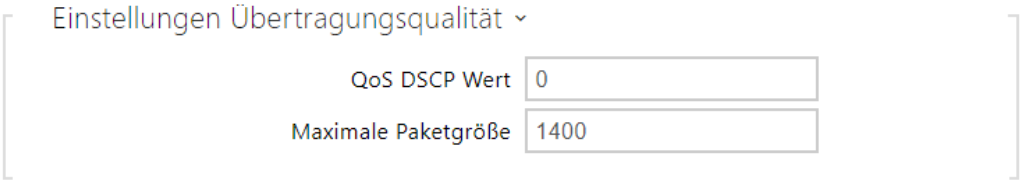
- **PTZ-Modus** – erlaubt die Funktion PTZ (Pan-Tilt-Zoom), die ermöglicht den angezeigten Ausschnitt des Kamerabildes im Verlauf des Anrufs mittels DTMF zu wählen (die Lizenz **GOLD** ist erforderlich).

Wenn die Funktion erlaubt ist, kann man die Kamera mittels der nummerischen Tastatur des IP-Telefons bedienen. Der PTZ-Modus wird mit der Taste ***** eingeschaltet und ausgeschaltet. Die Bedeutung der Tasten des IP-Telefons im PTZ-Modus ist folgende:

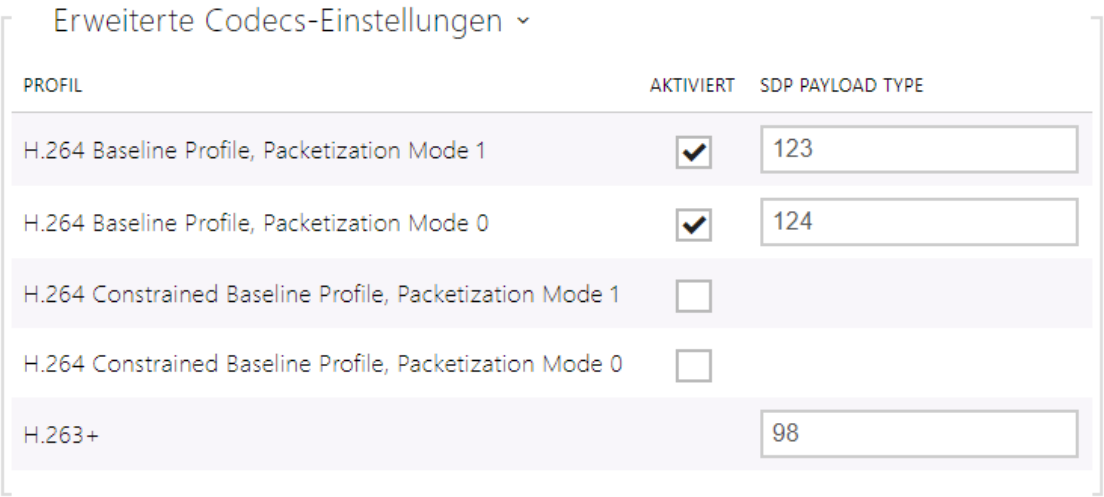
Taste des IP-Telefons	Funktionen im PTZ-Modus
*****	Einschalten und Ausschalten der PTZ-Funktion
1	Annäherung
3	Entfernung
2	Verschiebung eines Bildausschnittes nach oben
4	Verschiebung eines Bildausschnittes nach links
6	Verschiebung eines Bildausschnittes nach rechts
8	Verschiebung eines Bildausschnittes nach unten
5	Rückkehr zum Ausgangsstatus

- **PTZ und Face Zooming** – Ermöglicht PTZ (Pan-Tilt-Zoom) oder Face-Zooming, mit dem Sie den angezeigten Ausschnitt des Kamerabildes während eines Anrufs anpassen können. Bei der Wahl *Face Zooming* nähert sich das Bild der Kamera dem Gesicht des Benutzers an, der am Gerät steht. Bei der Wahl *Face Zooming – nur Neigung* verschiebt sich der Kameraausschnitt nur so, dass er das Gesicht einfängt.

> **Hinweis**
>
> - Die Funktion Face Zooming ist nur bei Modellen mit dem ARTPEC-7-Prozessor von Axis verfügbar.



- **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. Der Wert wird als Dezimalstelle eingegeben. Die empfohlenen QoS-Werte für Signalisierung, Audio und Video sind in der obigen Tabelle aufgeführt.
- **Maximale Paketgröße** – ermöglicht die maximale Größe der versendeten RTP-Video-Pakete einzustellen.



Das Verzeichnis der erweiterten Einstellungen der Codecs kann sich entsprechend dem Typ des Geräts unterscheiden.

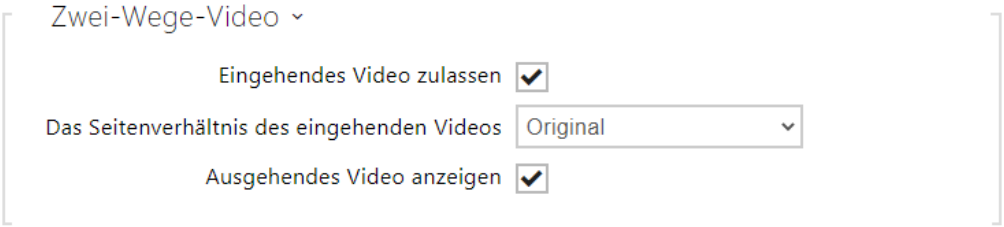
- **H.264 Baseline Profile, Packetization Mode 1**
- **H.264 Baseline Profile, Packetization Mode 0**
- **H.264 Main Profile, Packetization Mode 1**
- **H.264 Main Profile, Packetization Mode 0**
- **H.264 High Profile, Packetization Mode 1**
- **H.264 High Profile, Packetization Mode 0**
- **H.264 Constrained Baseline Profile, Packetization Mode 1**
- **H.264 Constrained Baseline Profile, Packetization Mode 0**
  - **Aktiviert** – erlaubt den Paketierungs-Modus und stellt den Payload-Typ für einzelne Codecs ein Der Payload-Typ wird automatisch im Falle ausgewählt, dass er nicht automatisch eingestellt werden kann.
  - **SDP Payload Type** – legt den Payload Type für den Video Codec H.264 (Paketierungsmodus 1) fest. Sie können einen Wert im Bereich von 96 bis 127 einstellen. 0, um diesen Codec-Typ zu deaktivieren.

- **H.263+**
  - **SDP Payload Type** – **l**egt den Payload Type für den Video Codec H.263+ fest. Geben Sie einen Wert im Bereich von 96 bis 127 ein.

- **Verwenden Sie das sendrecv-Attribut für Videos** – zuvor war die Einstellung als Kompatibilität mit Polycom-Telefonen markiert. Diese Einstellung dient für die Sicherstellung der Kompatibilität mit einigen Geräten von Drittanbietern (Polycom/Cisco und andere). Wenn dieser Modus aktiviert ist, sendet die Gegensprechanlage das sendrecv-Flag anstatt von sendonly in der SDP-Nachricht im Video-Codec-Menü.

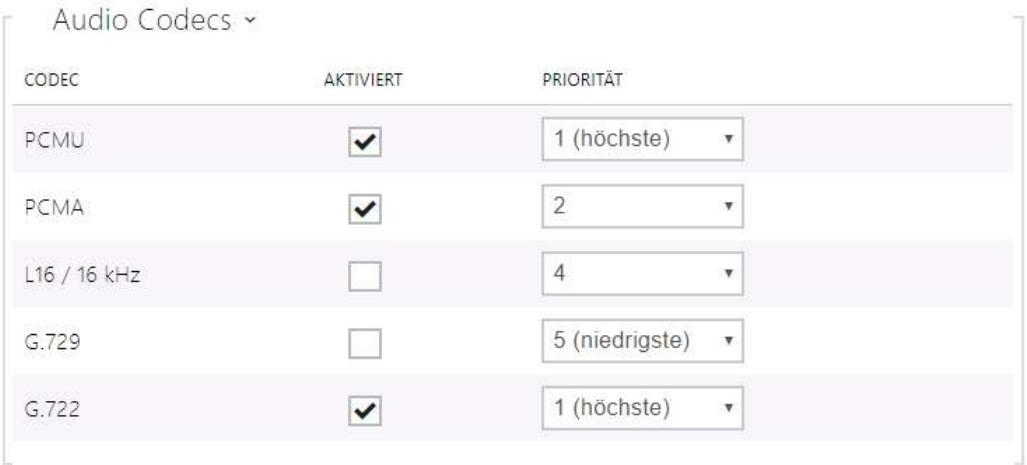
Tipp

Für die Funktion Video Preview auf dem Telefon **Grandstream GXV 3275** (Video wird mittels Early Media übertragen) muss man nichts konfigurieren. Überprüfen Sie für den Anschluss über PBX beim Hersteller, ob die jeweilige Zentrale diese Funktion unterstützt. Für die Funktion Video Preview auf dem Telefon **Gigaset Maxwell 10** (Video wird mittels .jpg Bilder übertragen) muss man in der Registerkarte **HTTP API** bei der Position **Camera API** den **Anschlusstyp** = **Nicht gesicherter (TCP)** und die **Authentifizierung** = **Keine** einstellen.



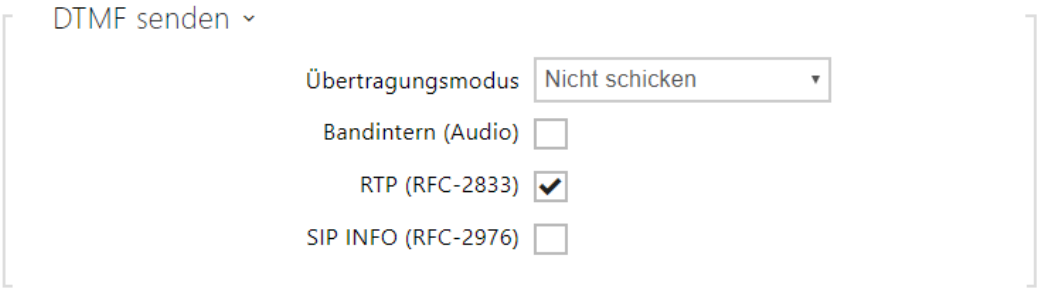
- **Eingehendes Video zulassen** – wenn dieser Modus aktiviert ist, zeigt die Sprechanlage das Video des Gesprächspartners an, wenn der andere Teilnehmer dies zulässt.
- **Das Seitenverhältnis des eingehenden Videos** – stellt das bevorzugte Seitenverhältnis des auf dem Bildschirm angezeigten eingehenden Videos ein. Wenn ein nicht originales Seitenverhältnis ausgewählt wird, wird das Video so zugeschnitten, dass es die Bildschirmbreite im neuen Seitenverhältnis ausfüllt.
- **Ausgehendes Video anzeigen** – legt fest, ob die Sprechanlage eine Vorschau des im Anruf gesendeten Videos anzeigt.

Registerkarte Audio



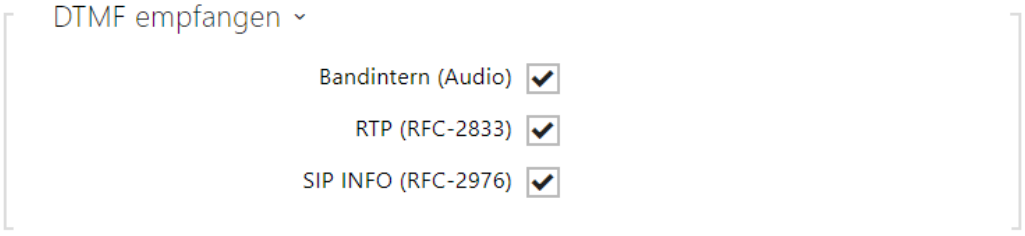
- Ermöglicht die Verwendung einzelner Audiocodecs zu erlauben/zu verbieten, die beim Aufbau der Verbindung angeboten werden, und ihre Priorität einzustellen. Die Breitband-Codecs L16 und G.722 sind nur bei ausgewählten Interkommodellen verfügbar. Der Codec G.729 ist nur bei ausgewählten Interkommodellen verfügbar, und zwar mit der gültigen G.729-Lizenz. Der Codec G.729 ist bei allen „2N IP“-Interkoms vorhanden.

Diese Registerkarte dient der Einstellung der Absendeart der DTMF-Zeichen vom Interkom. Überprüfen Sie der richtigen Funktion wegen die Möglichkeiten und die Einstellung des DTMF-Empfangs durch die andere Seite.

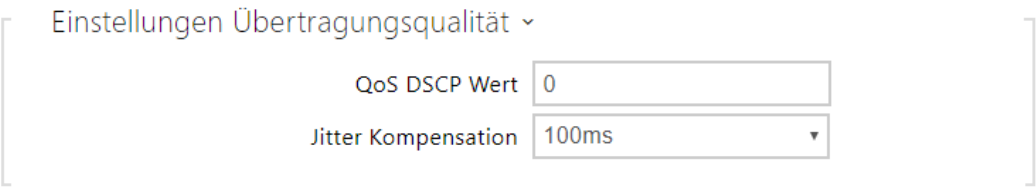


- **Übertragungmodus** – stellt ein, ob es im Anrufverlauf möglich sein wird, die DTMF-Zeichen beim Drücken der Tasten 0 bis 9, * und # auf der nummerischen Interkomtastatur abzusenden. Das Absenden können Sie bei nur eingehenden oder ausgehenden Anrufen bzw. bei allen Anrufen einstellen.
- **Banditern (Audio)** – erlaubt die klassische Art des DTMF-Absendens im Audioband mittels standardisierter Doppeltöne.
- **RTP (RFC-2833)** – erlaubt das Absenden der DTMF-Zeichen mittels des RTP-Protokolls gemäß RFC-2833.
- **SIP INFO (RFC-2976)** – erlaubt das Absenden der DTMF-Zeichen mittels der SIP-INFO-Nachrichten gemäß RFC-2976.

Diese Registerkarte dient der Einstellung des Empfangs der DTMF-Zeichen vom Interkom. Überprüfen Sie der richtigen Funktion wegen die Möglichkeiten und die Einstellung des DTMF-Empfangs durch die andere Seite.



- **Banditern (Audio)** – erlaubt den Empfang der klassischen Doppeltöne im Audioband.
- **RTP (RFC-2833)** – erlaubt den Empfang der DTMF-Zeichen mittels des RTP-Protokolls gemäß RFC-2833.
- **SIP INFO (RFC-2976)** – erlaubt den Empfang der DTMF-Zeichen mittels der SIP-INFO-Nachrichten gemäß RFC-2976.

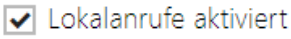


- **QoS DSCP Wert** – stellt die Priorität der RTP-Audio-Pakete im Netz ein. Der eingestellte Wert wird im Feld TOS (Type of Service) im Kopf des IP-Pakets abgesendet. Der Wert wird als Dezimalstelle eingegeben. Die empfohlenen QoS-Werte für Signalisierung, Audio und Video sind in der obigen Tabelle aufgeführt.
- **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.

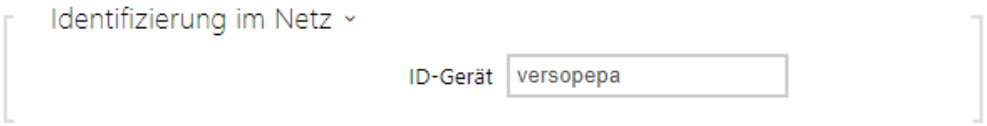
5.3.4 Lokalanrufe

In dieser Registerkarte wird der Anschluss der Einheiten 2N an das Interkom konfiguriert. Der Basisparameter ist der Zutrittscode, der einerseits ermöglicht, die Kommunikation zwischen dem Interkom und der Einheit 2N sicherzustellen, ggf. im Rahmen des lokalen Netzes mehrere unabhängige Interkomgruppen und Einheiten 2N zu bilden Man kann ebenfalls die Auflösung und die Qualität des Videos einstellen, das auf den Einheiten 2N angezeigt wird.

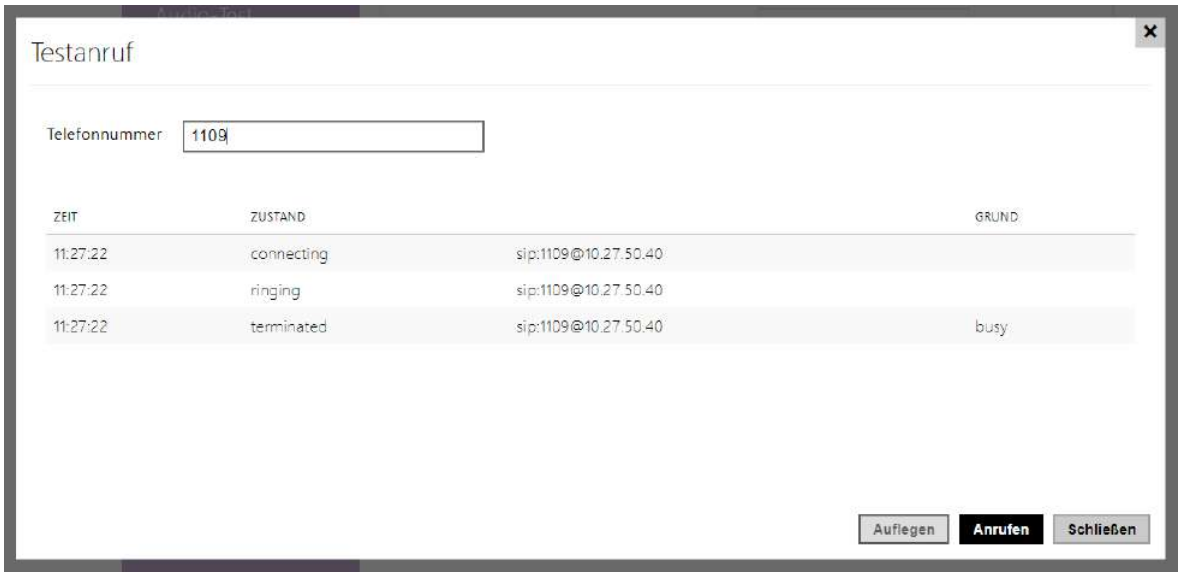
Konfiguration

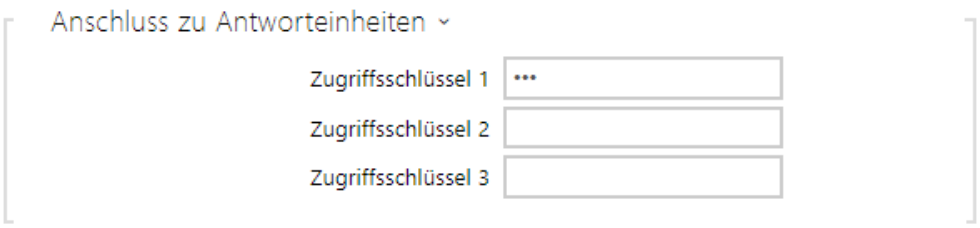


- **Lokalanrufe aktiviert** – aktiviert Anrufe zwischen 2N Geräten im Lokalnetz. Ist diese Funktion ausgeschalten, können andere Geräte im Netz dieses Gerät nicht finden, d. h. sie können dieses Gerät im Format device:device_ID nicht anrufen.



- **ID-Gerät** – legt die Geräteidentifizierung fest, die in der Liste der Lokalgeräte in allen 2N-Geräten des gleichen Lokalnetzes angezeigt wird. Durch Einstellung der Benutzertelefonnummer in diesen Geräten auf device:Geräte-ID kann man den Anruf auf dieses Gerät leiten.
- **Testanruf** – ruft das Dialogfenster mit der Möglichkeit einen Testanruf auf die gewählte Telefonnummer durchzuführen ab, siehe nachstehend.

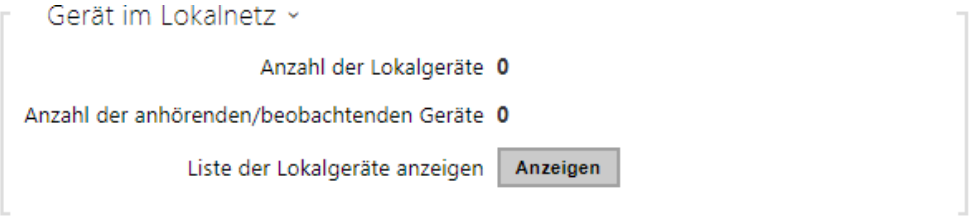




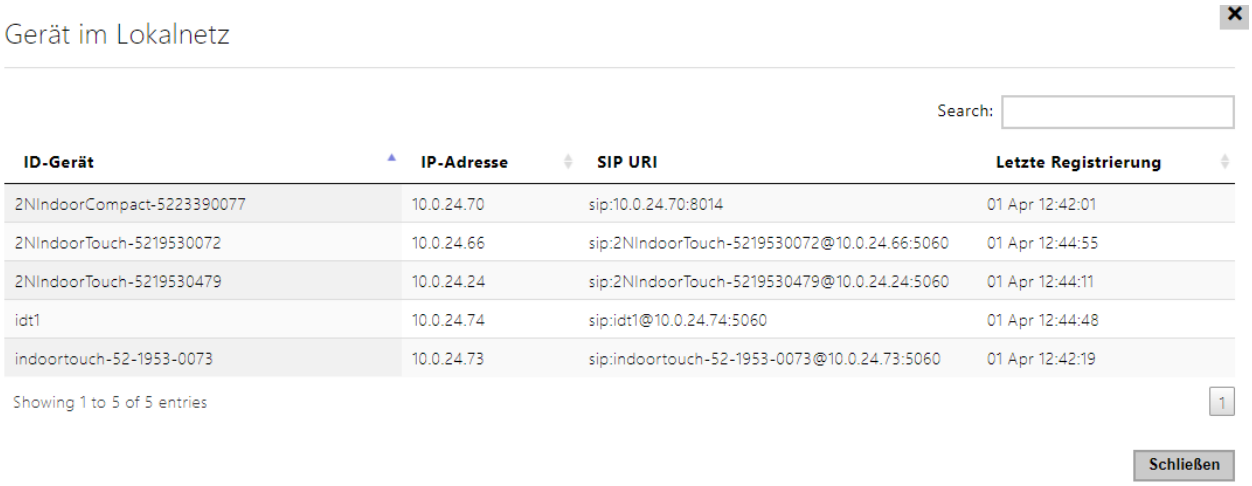
- **Zugriffsschlüssel 1–3** – legt den gemeinsamen Zugriffsschlüssel für Sprechanlage und Antworteinheite fest. Sollten die eingegebenen Schlüssel in den Antworteinheiten und in den Sprechanlagen nicht miteinander übereinstimmen, sie können miteinander nicht kommunizieren, d.h. die Sprechanlage kann nicht die Antworteinheit anrufen und umgekehrt.

Anmerkung

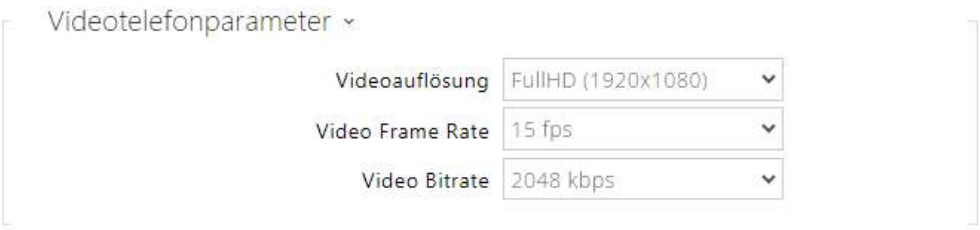
Falls Sie im Netz **2N® Indoor Touch** benutzen, dass mit der Firmware der Version 2 oder 3 ausgestattet ist, kann man den Zutrittscode nicht verwenden und er muss als leer eingestellt werden. Der Zutrittscode kann nur mit **2N® Indoor Touch** der Version 4 und höher benutzt werden.



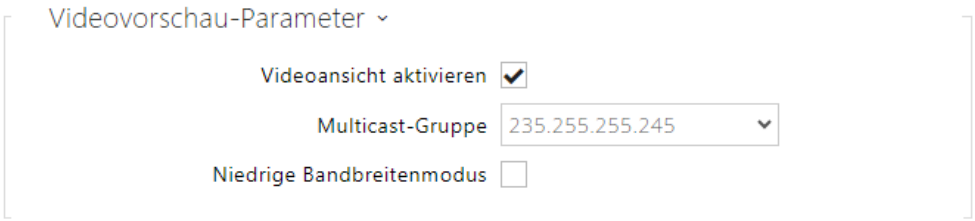
- **Anzahl der Lokalgeräte** – zeigt die aktuelle Zahl der lokal Einheiten 2N an.
- **Anzahl der anhörenden/beobachten Geräte** – zeigt die aktuelle Zahl der Einheiten 2N an, die das Video aus dem Interkom verfolgen.
- **Liste der Lokalgeräte anzeigen** – öffnet das Fenster mit der Liste der lokal Anlagen 2N.



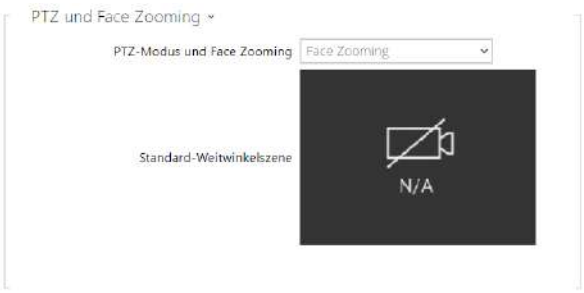
Video



- **Videoauflösung** – legt die Videoauflösung für Telefonanrufe.
- **Video Frame Rate** – legt die Video Frame Rate für Telefonanrufe (für Video Codec) fest
- **Videoqualität** – legt die Video Stream Bitrate für Telefonanrufe (für Video Codec) fest.



- **Videoansicht aktivieren** – aktiviert Versenden der Videoansicht im Muticast.
- **Multicast-Gruppe** – stellt die Multicastadresse ein, an die der Videostream vom Interkom gesendet wird. Man kann 1 von 8 voreingestellten Adressen wählen bzw. den Modus einstellen, in dem das Interkom die Adresse automatisch wählt.
- **Niedrige Bandbreitenmodus** – reduziert die Qualität des Videovorschau-Streams, um die Bandbreite zu schonen.



- **PTZ-Modus** – erlaubt die Funktion PTZ (Pan-Tilt-Zoom), die ermöglicht den angezeigten Ausschnitt des Kamerabildes im Verlauf des Anrufs mittels DTMF zu wählen (die Lizenz **GOLD** ist erforderlich).

Wenn die Funktion erlaubt ist, kann man die Kamera mittels der nummerischen Tastatur des IP-Telefons bedienen. Der PTZ-Modus wird mit der Taste ***** eingeschaltet und ausgeschaltet. Die Bedeutung der Tasten des IP-Telefons im PTZ-Modus ist folgende:

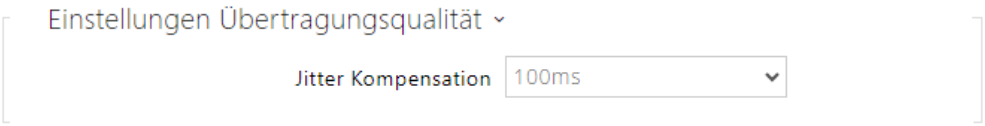
Taste des IP-Telefons	Funktionen im PTZ-Modus
*****	Einschalten und Ausschalten der PTZ-Funktion
1	Annäherung
3	Entfernung
2	Verschiebung eines Bildausschnittes nach oben
4	Verschiebung eines Bildausschnittes nach links
6	Verschiebung eines Bildausschnittes nach rechts
8	Verschiebung eines Bildausschnittes nach unten
5	Rückkehr zum Ausgangsstatus

- **PTZ und Face Zooming** – Ermöglicht PTZ (Pan-Tilt-Zoom) oder Face-Zooming, mit dem Sie den angezeigten Ausschnitt des Kamerabildes während eines Anrufs anpassen können. Bei der Wahl *Face Zooming* nähert sich das Bild der Kamera dem Gesicht des Benutzers an, der am Gerät steht. Bei der Wahl *Face Zooming – nur Neigung* verschiebt sich der Kameraausschnitt nur so, dass er das Gesicht einfängt.

> **Hinweis**
>
> - Die Funktion Face Zooming ist nur bei Modellen mit dem ARTPEC-7-Prozessor von Axis verfügbar.

- **Eingehendes Video zulassen** – wenn dieser Modus aktiviert ist, zeigt die Sprechanlage das Video des Gesprächspartners an, wenn der andere Teilnehmer dies zulässt.
- **Das Seitenverhältnis des eingehenden Videos** – stellt das bevorzugte Seitenverhältnis des auf dem Bildschirm angezeigten eingehenden Videos ein. Wenn ein nicht originales Seitenverhältnis ausgewählt wird, wird das Video so zugeschnitten, dass es die Bildschirmbreite im neuen Seitenverhältnis ausfüllt.
- **Ausgehendes Video anzeigen** – stellt das bevorzugte Seitenverhältnis des auf dem Bildschirm angezeigten eingehenden Videos ein. Wenn ein nicht originales Seitenverhältnis ausgewählt wird, wird das Video so zugeschnitten, dass es die Bildschirmbreite im neuen Seitenverhältnis ausfüllt.

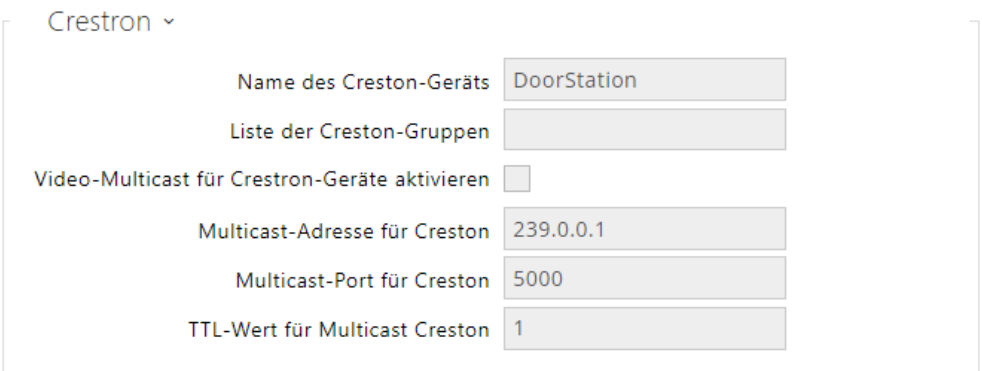
Audio



- **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.

5.3.5 Crestron

- **Crestron Network Discovery aktivieren** – erlaubt die Identifizierung der 2N IP Interkoms im Rahmen des Crestron-Netzes.



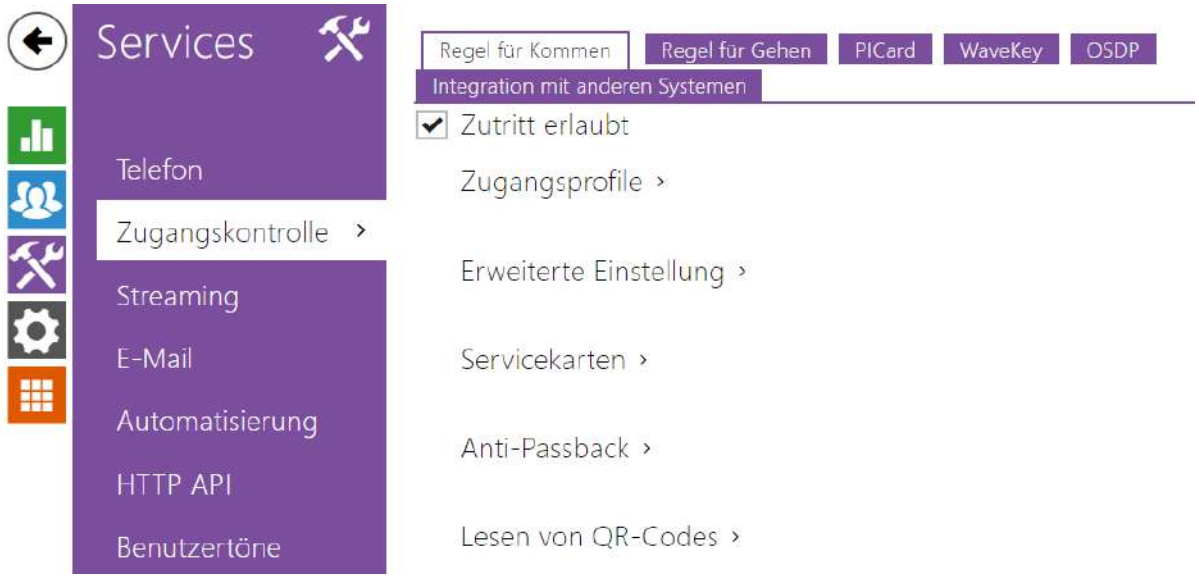
- **Name des Creston-Geräts** – Bezeichnung der Anlage.
- **List der Crestron-Gruppen** – Bezeichnung der Gruppe.
- **Video-Multicast für Crestron-Geräte aktivieren** – lässt Video-Multicast für Crestron-Panels zu. Dadurch können mehrere Crestron-Geräte das gleiche Video empfangen, wodurch die Übertragungskapazität des örtlichen Netzes geschont wird.
- **Multicast-Adrresse für Crestron** – Multicast-Adresse, welche für Multicast-Video mit Crestron-Gerät verwendet wird.
- **Multicast-Port für Crestron** – Multicast-Port, welcher für Multicast-Video mit Crestron-Gerät verwendet wird.
- **TTL-Wert für Multicast Crestron** – TTL-Wert (Time To Live), welcher zum Senden des Videos als Early-Medien für Crestron-Geräte verwendet wird.

5.4 Services

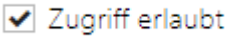
Hier ist eine Übersicht dessen, was Sie im Kapitel finden:

5.4.1 Zugangskontrolle

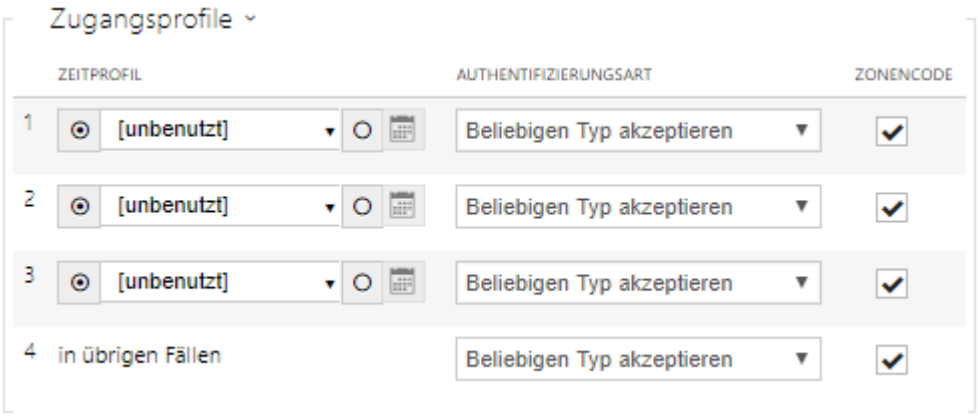
Der Zugangskontrolldienst dient der Verwaltung des Zugangs und der Überprüfung der Benutzerauthentifizierung.



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.



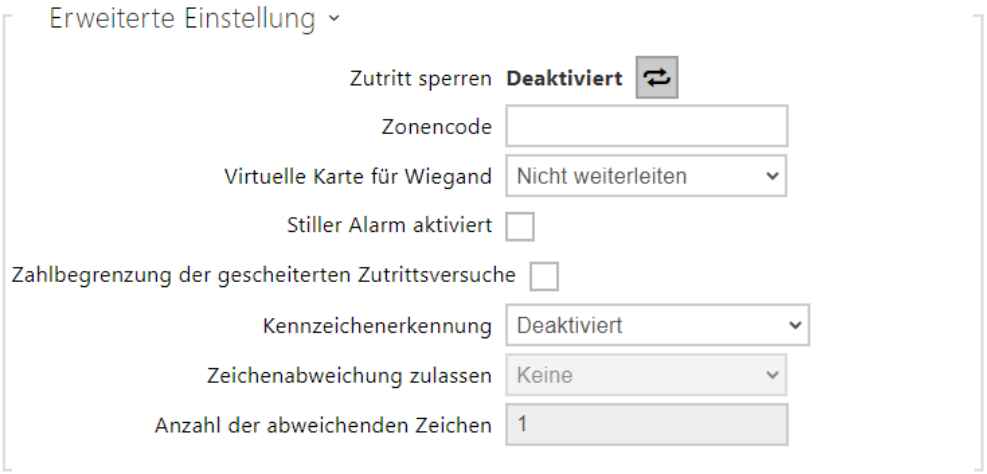
- **Zeitprofil** – bietet die Auswahl eines oder mehrerer Zeitprofile gleichzeitig an, die angewendet werden. Die Einstellung der Zeitprofile selbst ist im Abschnitt Verzeichnis / Zeitprofile möglich.

-  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.

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 das Zutrittsmodul 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.

- **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).

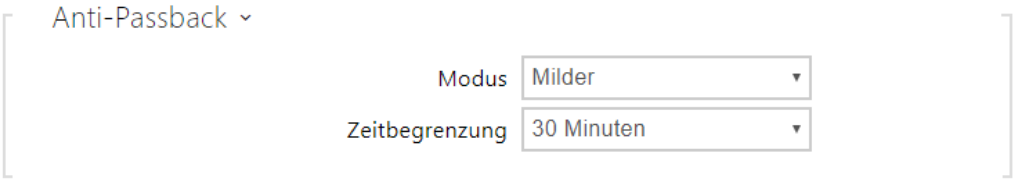
Wenn die Funktion aktiviert ist, wird das Ereignis nach Erhalt einer gültigen HTTP-Anfrage im Verlauf unter dem Ereignis LicensePlateRecognized aufgezeichnet. Wenn ein Bild als Teil der HTTP-Anfrage gesendet wird (z. B. ein Abschnitt des Fotos oder das gesamte Foto der Szene bei der Kennzeichenerkennung),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

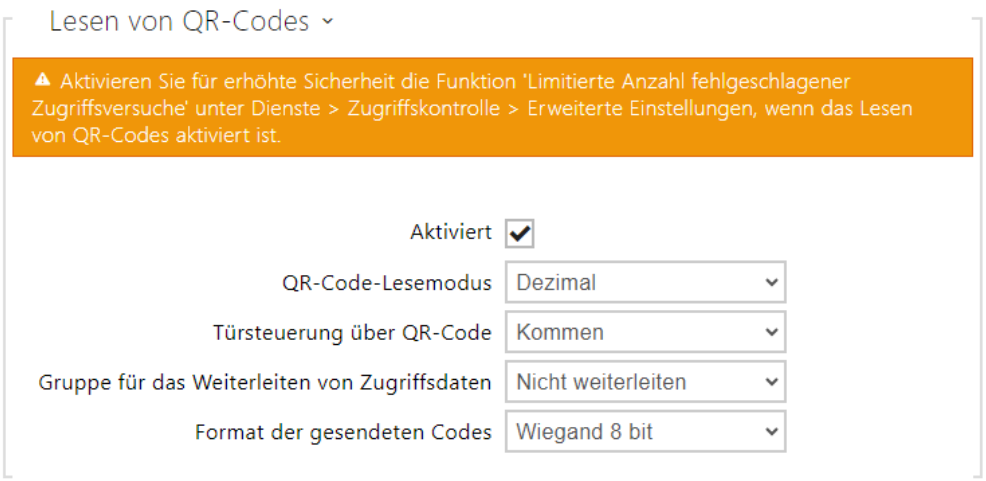
- **Plus Karten-ID** – ID der Servicekarte, die für das Hinzufügen in die Liste der installierten Karten bestimmt ist. Die Karten-ID ist die Sequenz von 6–32 Zeichen aus der Menge 0–9, A–F.
- **Minus Karten-ID** – ID der Servicekarte, die für das Entfernen von der Liste der installierten Karten bestimmt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

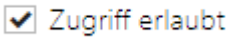


- **Aktiviert** – aktiviert/deaktiviert das Lesen von QR-Codes mit der Gerätekamera. Wenn das Lesen von QR-Codes aktiviert ist, können PIN-Codes und einzelne Schaltcodes, die mehr als zehn Ziffern haben, eingegeben werden, indem der QR-Code auf die Gerätekamera gerichtet wird.
- **QR Code Reading Mode** – 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.

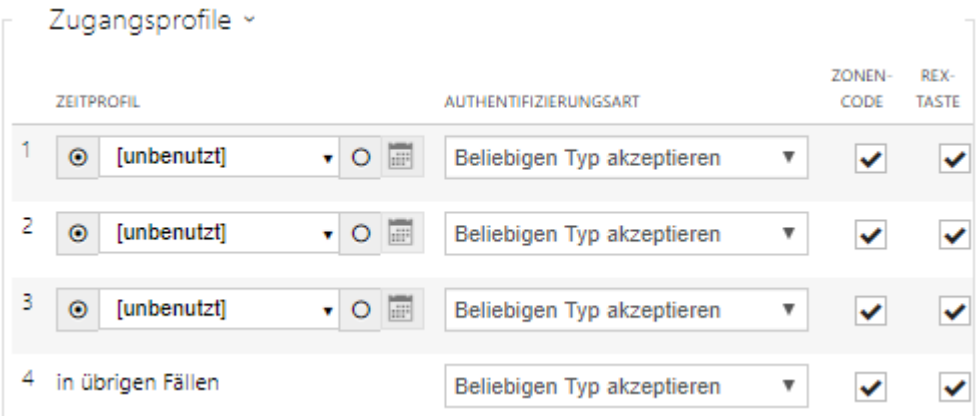
Hinweis

- 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



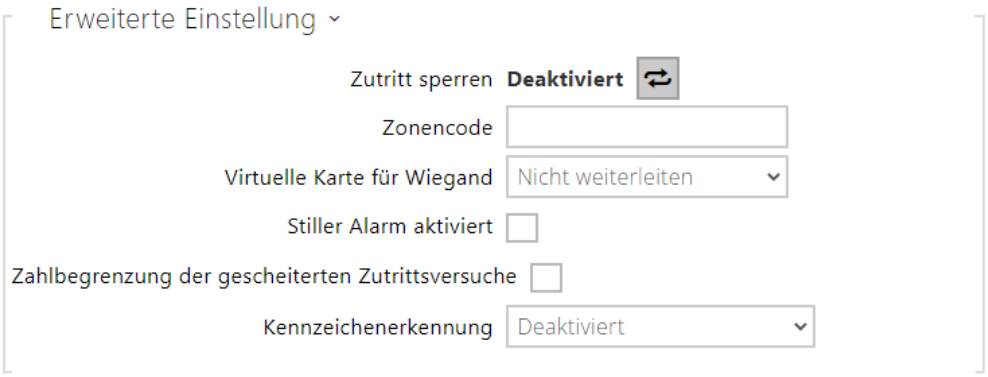
- **Zugriff erlaubt** – erlaubt den beliebigen Zutritt von der konkreten Türseite (Kommen, Gehen). Wenn der Zutritt nicht erlaubt ist, kann man die Tür von dieser Seite nicht öffnen.



- **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 das Zutrittsmodul 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.

- **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).

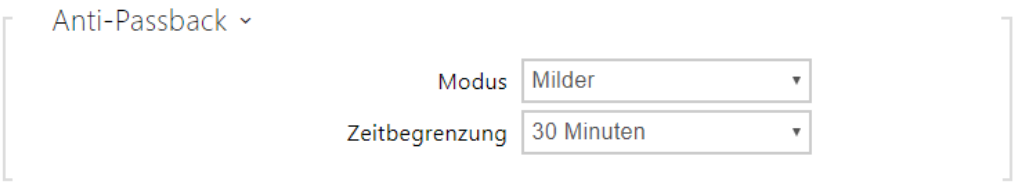
Wenn die Funktion aktiviert ist, wird das Ereignis nach Erhalt einer gültigen HTTP-Anfrage im Verlauf unter dem Ereignis LicensePlateRecognized aufgezeichnet. Wenn ein Bild als Teil der HTTP-Anfrage gesendet wird (z. B. ein Abschnitt des Fotos oder das gesamte Foto der Szene bei der Kennzeichenerkennung),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

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

Die **Interkoms 2N IP**, 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 der Interkomseite 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.

Man kann den Wert Auth-ID im Abschnitt Mobile Key des Telefonbuchs einstellen und ändern. Die Auth-ID kann man einem anderen Nutzer zuordnen bzw. in ein anderes Interkom 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 Interkom 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 Interkomstart 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 Interkom 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).

Die Kopplung des Nutzers mit dem mobilen Gerät kann man im Telefonbuch des Interkoms auf der Seite des jeweiligen Nutzers initiieren. Die Kopplung kann man physisch lokal mittels des USB-Bluetooth-Moduls, das an einen PC angeschlossen ist ggf.über ein Bluetooth-Modul, das im Interkom 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 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 Interkomstart generiert und man kann ihn später jederzeit manuell ändern.

Verwaltung der Kodierungsschlüssel

Das Interkom 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.

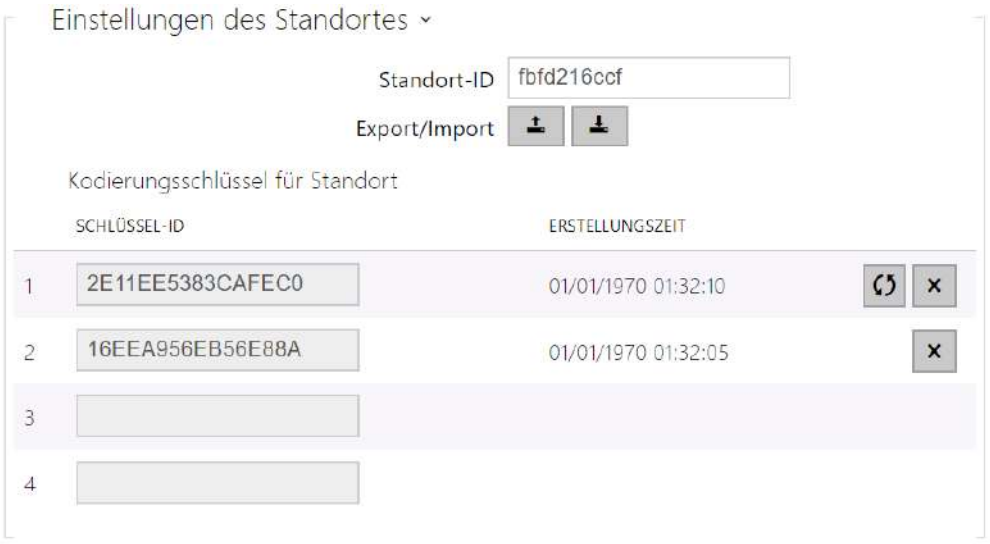
beim Verlust des mobilen Geräts oder beim Entweichen der Interkomkonfiguration aktualisiert werden.

> **Anmerkung**
>
> - Die Kodierungsschlüssel werden automatisch beim ersten Interkomstart generiert und in der Konfigurationsdatei des Interkoms 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 Interkom 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 dem Interkom.

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 bietet eine sichere Kommunikation für das Senden von Zugangsdaten, wie z. B. die ID der Zugangskarte oder den PIN-Code, zwischen dem angeschlossenen OSDP-Gerät (Bedienfeld, Tür-Controller) und der **2N IP-Sprechanlage**. Das Ziel ist, die Aktivierung der Signalisierung auf **2N IP-Sprechanlage** auf der Grundlage der Antwort der Gegenstelle auf die gesendete Kartensignalisierungsdefinition 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 IP-Sprechanlage 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)

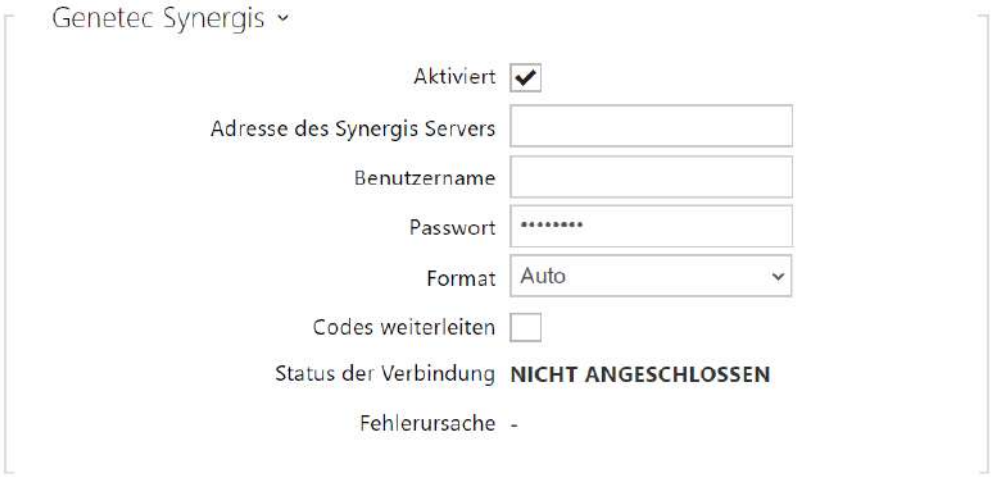
Der Teil (ohne Zeit) wird als Definitionsstring verwendet und darf maximal 255 Zeichen lang sein, z. B.: led(0,0,0,0,0,0,0,0,1,1,1,1,1) oder buz(0,2,1,1,1). Wird auf der Gegenseite eine Übereinstimmung festgestellt, antwortet das Gerät mit einem entsprechenden Signal. Jeder Teil der Definition kann durch "*" 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 IP-Sprechstelle bestätigt das Laden der Karte mit einem Signalton, nach der Auswertung antwortet das Gerät mit der entsprechenden Signalisierung.

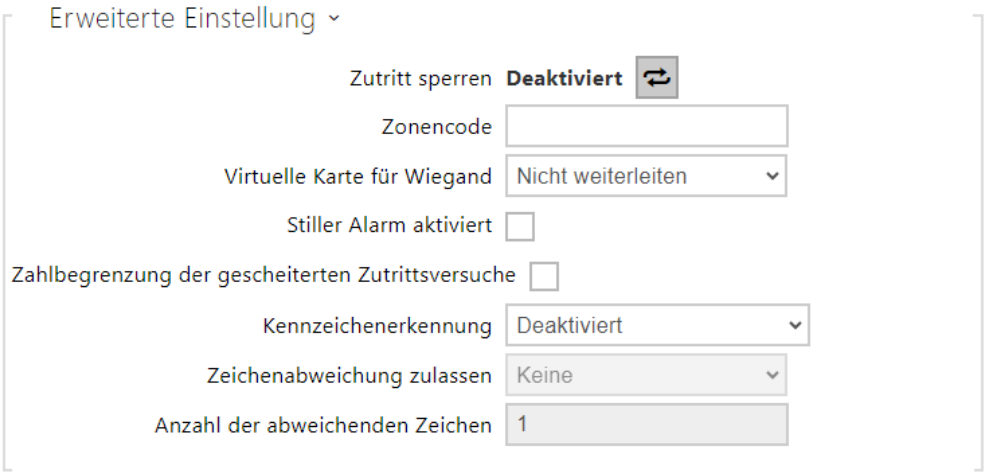
Registerkarte Integration mit anderen Systemen



- **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.

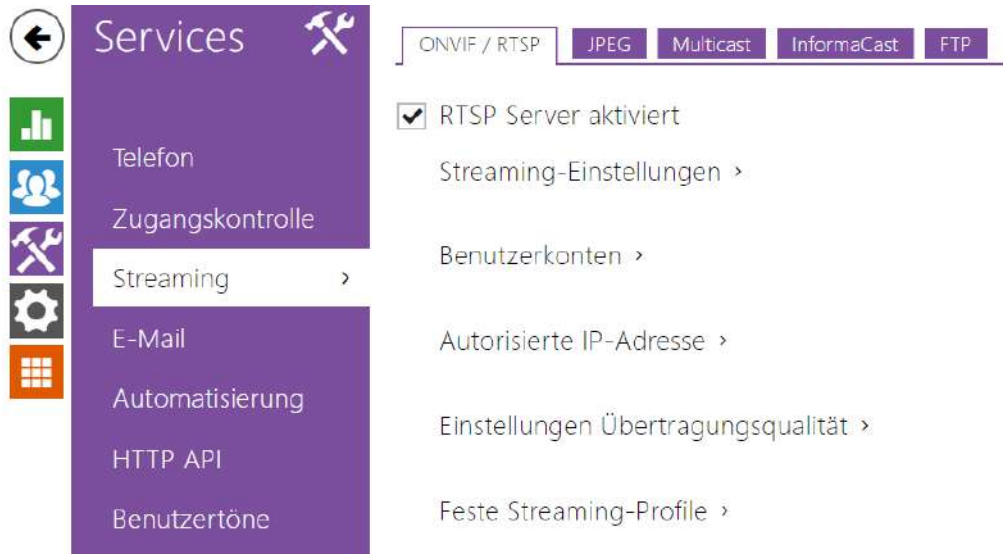
- **Codes weiterleiten** – legt fest, ob die eingegebenen Codes weitergeleitet werden. Die Codes können maximal 6-stellig sein und am Ende muss die Bestätigungstaste gedrückt werden.
- **Verbindungszustand** – zeigt den aktuellen Status des Anschlusses an den Synergis-Server ggf. die Beschreibung des 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.

5.4.2 Streaming



Die **Interkoms 2N IP** 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

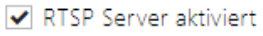
- **RTP (Real-Time Transport Protocol)** – Protokoll, das das Standardformat der Pakete für die Audio- und Videoübertragung in IP-Netzen definiert. Die **2N IP Interkoms** nutzen dieses Protokolls für die Übertragung des Audio- und Videostreams. Das Transportprotokoll für RTP ist in der Regel entweder 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 Interkoms **2N IP** 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 **Interkoms 2N IP** 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 **Interkoms 2N IP** 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 der Interkoms **2N IP** 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.

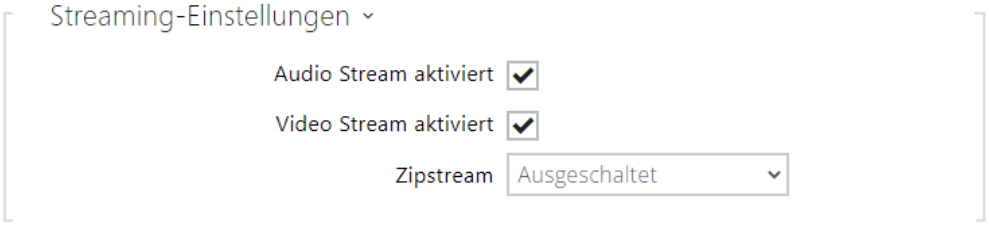
Parameterliste

Registerkarte ONVIF/RTSP

Die Interkoms **2N IP** 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.

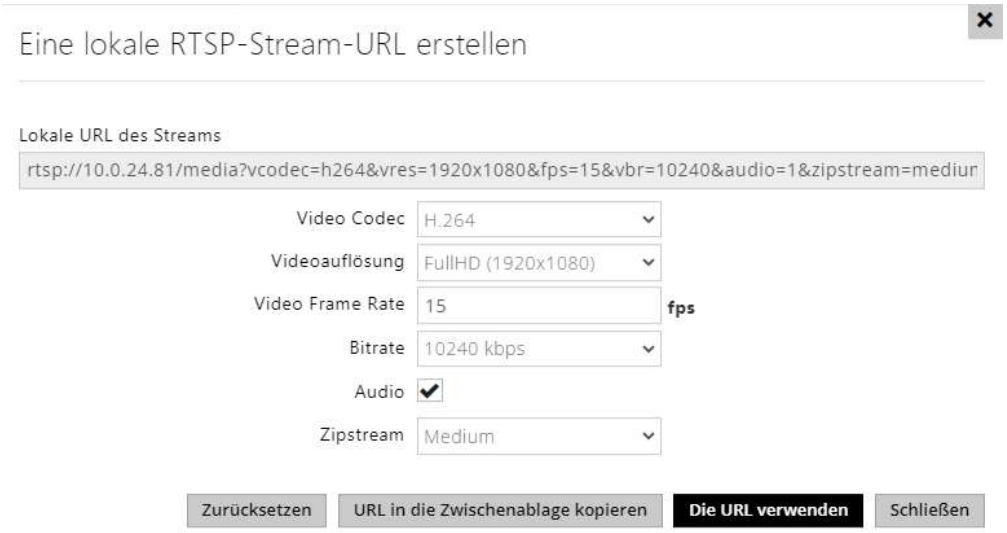


- **RTSP Server aktiviert** – erlaubt die Funktion des RTSP-Servers im Interkom.



- **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.

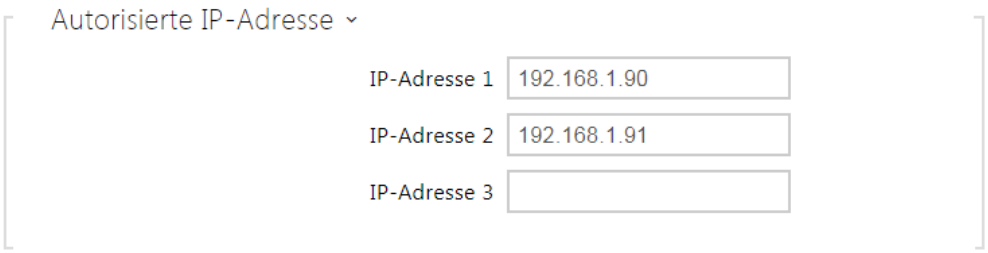


  - **Video Codec** – Auswahl der verfügbaren Video Codecs.
  - **Videoauflösung** – Auswahl der möglichen Bildauflösungen.
  - **Video Frame Rate** – Einstellung der Bildfrequenz (1 bis 30 fps, der maximal mögliche Wert für den MJPEG-Videocodec ist 15 fps).
  - **Qualität** – Auswahl der verfügbaren Übertragungsgeschwindigkeit.
  - **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 Interkom 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.

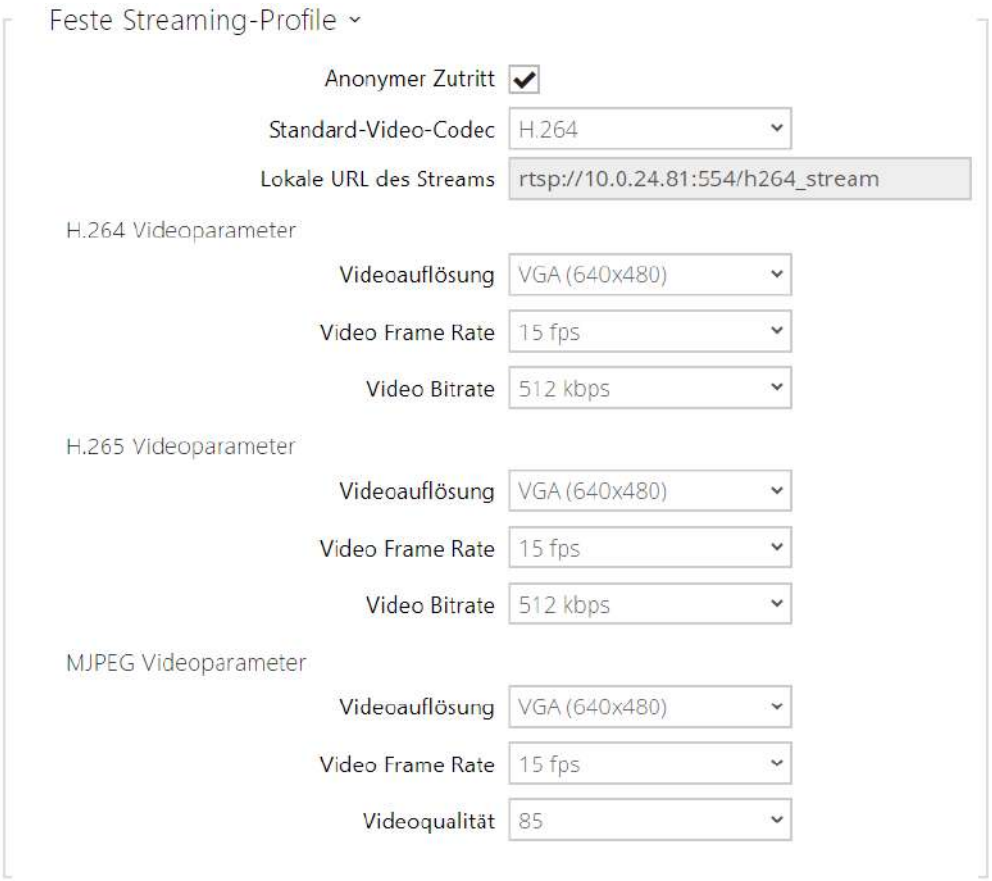


- **IP-Adresse 1–4** – ermöglicht bis zu 4 autorisierte IP-Adressen einzustellen, zu denen man sich vom RTSP-Server anmelden kann. Ist keines der vier Felder ausgefüllt, kann eine beliebige IP-Adresse für den Log-in verwendet werden.

- **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 Interkom 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).

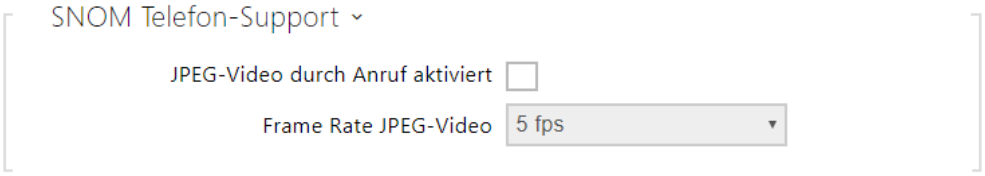
In der nachfolgenden Tabelle sind die maximalen Zahlen der gleichzeitig laufenden MJPEG/HTTP-Streams angeführt, bei denen es noch nicht zur Senkung der Frequenz der versendeten Aufnahmen unter der Verwendung des Basisniveaus der JPEG-Kompression kommt.

Interkomtyp	Auflösung	Streamzahl
Force/Vario	640 x 480	15
Force HD	640 x 480	15
Force HD	1280 x 960	3
Verso	640 x 480	8
Verso	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.

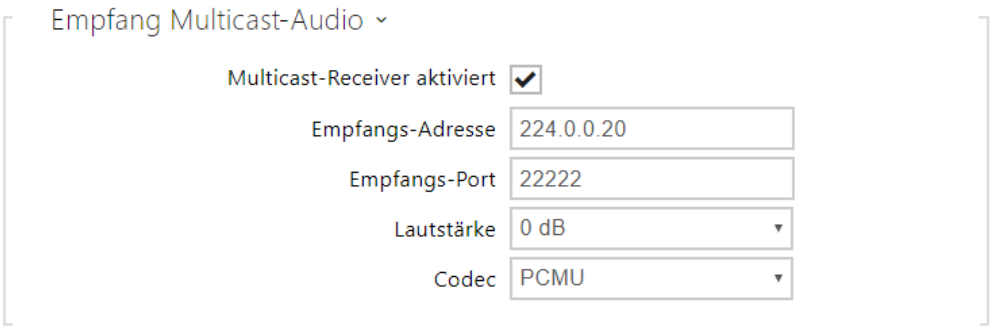


Manche IP-Telefone (SNOM 820/870) unterstützen keine Videoanrufe, aber können im Verlauf eines Anrufs periodisch JPEG-Aufnahmen herunterladen und anzeigen, die aus der definierten IP-Adresse heruntergeladen wurden. Die Interkoms **2N IP** unterstützen diese Funktion und man kann sie in dieser Registerkarte einstellen.

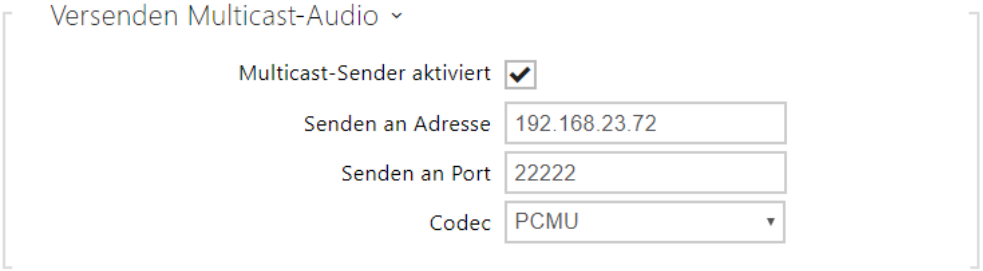
- **JPEG-Video durch Anruf aktivieren** – erlaubt die Funktion des Herunterladens der Kameraaufnahmen durch die Telefone Snom 820/870 im Anrufverlauf.
- **Frame Rate JPEG-Video** – stellt die Aufnahmefrequenz bzw. die Periodizität des Herunterladens der Kameraaufnahmen durch die Telefone Snom 820/870 ein.

Registerkarte Multicast

Die Interkoms **2N IP** ermöglichen das Audio (Signal aus dem Mikrofon oder einem anderen Audioeingang des Interkoms) mittels der RTP-Pakete zu streamen, die an die Multicastadresse gesendet werden, und gleichzeitig den Audiostream im gleichen Format zu empfangen und ihn mittels des eingebauten Lautsprechers (ggf. eines anderen konfigurierten Audioausgangs) abzuspielen. Der Audiostream wird mittels des Codecs G.711 u-law kodiert.



- **Multicast-Receiver aktiviert** – erlaubt den Empfang der RTP-Pakete an der gewählten Multicastadresse und dem Port. Der empfangene Audiostream wird auch im Verlauf eines aktiven Anrufs abgespielt, wo es zum Vermischen des Tons aus beiden Quellen kommt.
- **Empfangs-Adresse** – stellt die Multicast-IP-Adresse ein, an der die Multicast-RTP-Pakete erwartet werden.
- **Empfangs-Port** – stellt den lokalen Port für den Empfang der Multicast-RTP-Pakete ein.
- **Lautstärke** – ermöglicht die Lautstärke des Abspielens des empfangenen Audiostreams einzustellen.
- **Codec** – ermöglicht das Audiocodec für das Dekodieren der eingehenden RTP-Pakete einzustellen. Man kann zwischen PCMU, PCMA, G.722, L.16 wählen. Die Breitbandcodecs G.722 und L16 sind nur bei ausgewählten Interkommodellen verfügbar.



- **Multicast-Receiver aktiviert** – erlaubt das Absenden der RTP-Pakete an gewählte Multicastadressen und Ports.
- **Senden an Adresse** – stellt die Ziel-Multicast-IP-Adresse ein, an die der Audiostream gesendet wird.
- **Senden an Port** – stellt den Zielport ein, zu dem der Audiostream gesendet wird.
- **Codec** – ermöglicht den Audiocodec für das Dekodieren der ausgehenden RTP-Pakete einzustellen. Man kann zwischen PCMU, PCMA, G.722, L.16 wählen. Die Breitbandcodecs G.722 und L16 sind nur bei ausgewählten Interkommodellen verfügbar.

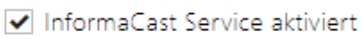
Registerkarte InformaCast

Die Interkoms **2N IP** unterstützen das Protokoll Informacast für das Audiostreaming. Das Protokoll Informacast ermöglicht einen Audiostream (Unicast/Multicast RTP/UDP kodiert mit dem Codec G.711 U-law) zwischen dem Interkom und dem Informacast-Server ggf. einem anderen Informacast-Client aufzubauen.

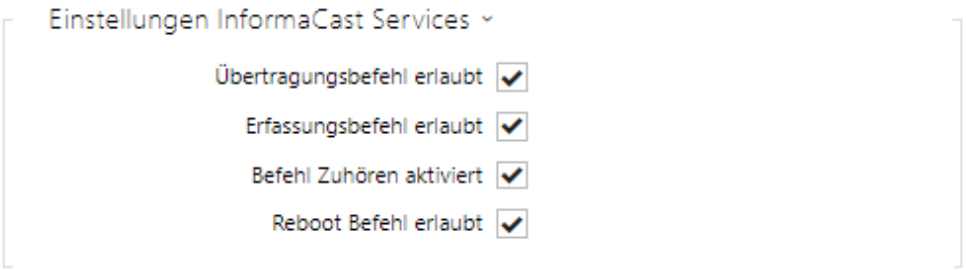
Nach der Freigabe des Dienstes werden im lokalen Netz automatisch mittels des SLP-Protokolls Informacast-Server gesucht und das Interkom registriert sich automatisch bei diesen. Der Informacast-Server, bei dem das Interkom registriert ist, kann dem Interkom Befehle für den Aufbau des Audiostreams senden:

- **Broadcast** – das Interkom empfängt den Audiostream vom Informacast-Server und spielt ihn mittels des eingebauten Lautsprechers ab.
- **Capture** – das Interkom zeichnet das Audio mittels des internen Mikrophons auf und sendet den Audiostream an den Informacast-Server.
- **Listen** – das Interkom empfängt den Audiostream, der durch einen anderen Informacast-Client gesendet wird.

Das Interkom unterstützt die Registrierung bei bis zu 4 Informacast-Servern gleichzeitig und ermöglicht den Aufbau von bis zu 6 parallelen Audiostreams.



- **InformaCast Service erlaubt** – erlaubt die Dienstleistung Informacast auf der Interkomseite.



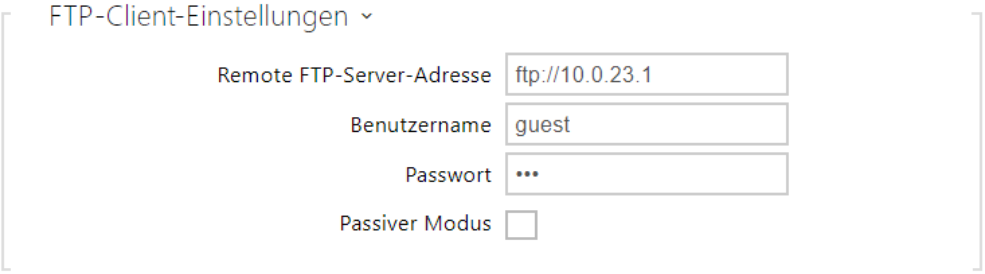
- **Übertragungsbefehl erlaubt** – erlaubt den Broadcast-Befehl, der ermöglicht den Audiostream aufzubauen, der vom Informacast-Server an das Interkom gesendet wird.
- **Erfassungbefehl erlaubt** – erlaubt den Capture-Befehl, der ermöglicht den Audiostream aufzubauen, der vom Interkom an den Informacast-Server gesendet wird.
- **Befehl Zuhören aktiviert** – erlaubt den Listen-Befehl, der ermöglicht den Audiostream aufzubauen, der vom anderen Informacast-Client an das Interkom gesendet wird.
- **Reboot Befehl erlaubt** – erlaubt den Reboot-Befehl, der dem Informacast-Server ermöglicht, das Interkom neu zu starten.

Registerkarte FTP

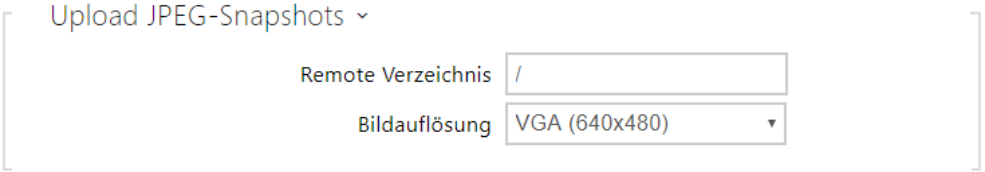
In dieser Registerkarte kann man die Zutrittsdaten zum FTP(S)-Server einstellen, auf dem Aufnahmen aus der internen oder externen an das Interkom angeschlossenen Kamera gespeichert werden können. Die Aufnahmen werden auf dem FTP-Server im JPEG-Format, in der gewählten Auflösung gespeichert, die Bezeichnung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

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

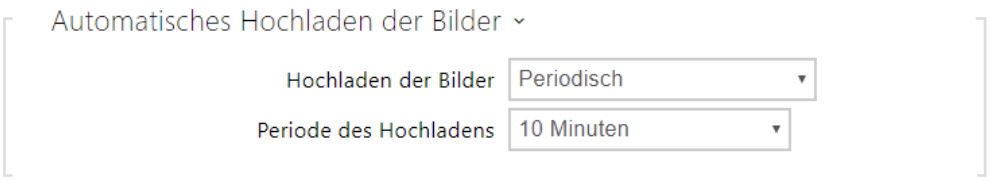
- **FTP Client aktiviert** – erlaubt die Dienstleistung für die Speicherung einer Aufnahme aus der Kamera auf dem FTP-Server.



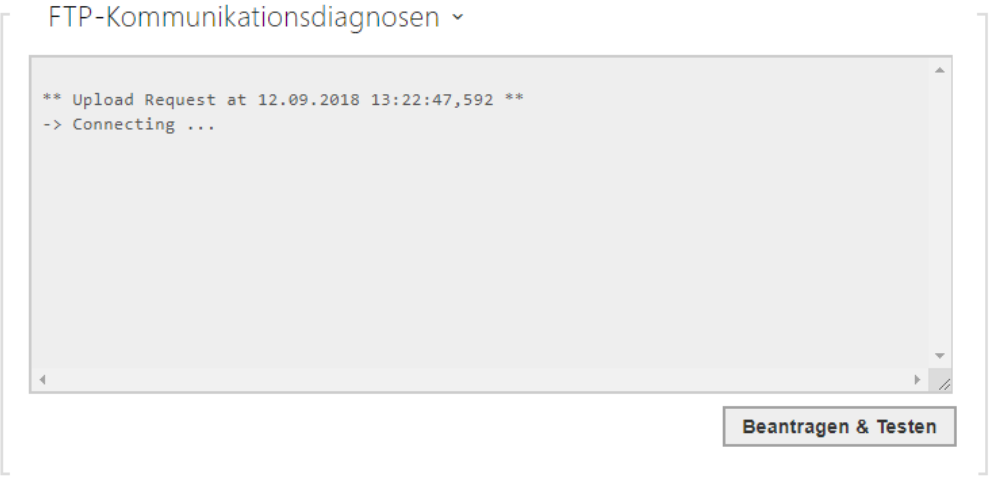
- **Remote FTP-Servers-Adresse** – stellt die Adresse des FTP-Servers ein. Die Adresse muss in der Form ftp://ip_adresse oderftps://ip_adresse sein.
- **Benutzername** – stellt den Namen des FTP-Server-Nutzers ein. Der Parameter ist verbindlich, wenn der FTP-Server die Authentifizierung des Nutzers verlangt.
- **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.

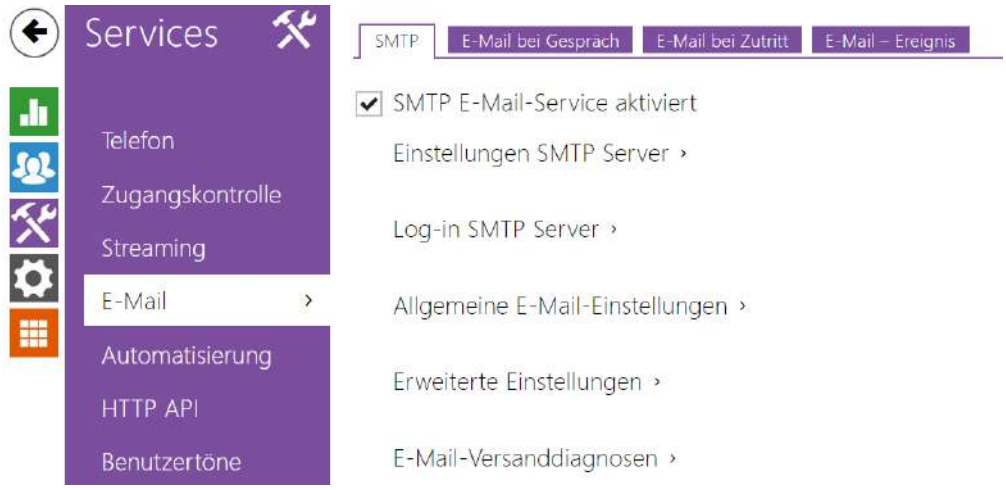


- **Hochladen der Bilder** – ermöglicht das automatische Absenden von Bildern an den FTP-Server beim Anrufanfang bzw. periodisch nach dem Ablauf der festgelegten Zeit einzustellen. Man kann das automatische Senden ausschalten (Wahl Automatisierung), danach kann man weiterhin die Bilder über die Automatisierungsaktion 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

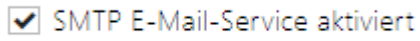


Wenn Sie die Nutzer über verpasste bzw. alle realisierten Anrufe aus dem Interkom informieren wollen, können Sie das **Interkom 2N IP** so konfigurieren, das es nach jedem solchen Anruf dem angerufenen Nutzer eine E-Mail schickt. Sie können einen eigenen Betreff und den Text der E-Mail einstellen. Wenn Ihr Interkom mit einer Kamera ausgestattet ist, können Sie der E-Mail automatisch eine oder mehrere Aufnahmen aus der Kamera hinzufügen, die während des Gesprächs oder Klingelns aufgezeichnet wurden.
Das Interkom 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.

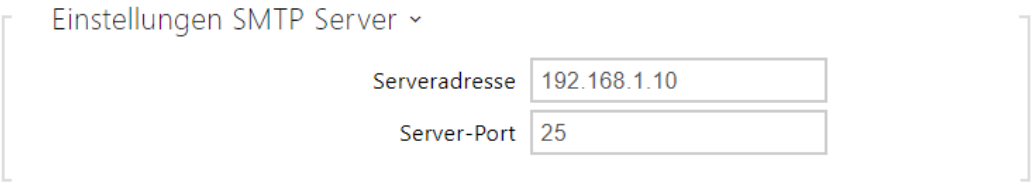
Man kann die E-Mails auch mithilfe der Automatisierung mittels der Aktion **Action.SendEmail** absenden.

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

Registerkarte SMTP

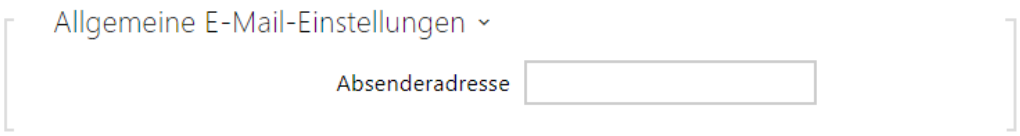


- **SMTP E-Mail-Service aktiviert** – ermöglicht den Dienst des Absendens der E-Mails aus dem Interkom zu erlauben oder zu sperren.

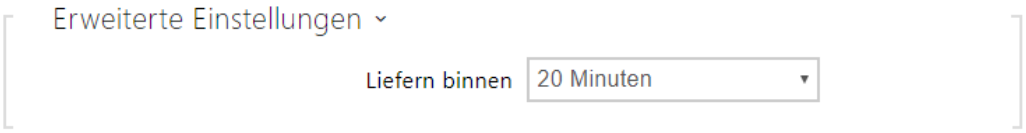


- **Serveradresse** – Adresse des SMTP Servers, an den die E-Mails gesendet werden.
- **Server-Port** – Port des SMTP-Servers. Ändern Sie den Wert nur dann, wenn die Einstellung des SMTP-Servers nicht-standardmäßig ist. Der typische Wert des SMTP-Ports liegt bei 25.

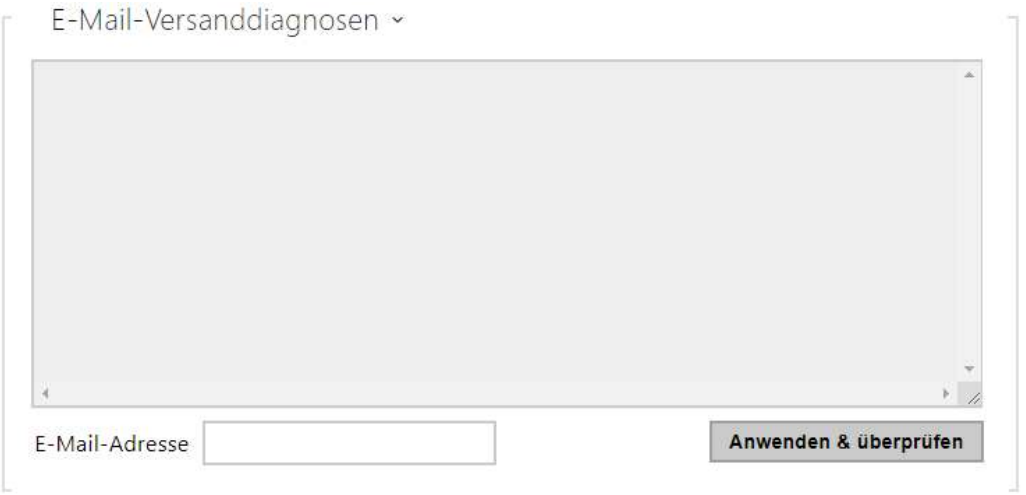
- **Benutzername** – wenn der SMTP-Server die Autorisierung verlangt, muss in diesem Feld der gültige Name für das Anmelden zum Server angeführt sein. Im anderen Fall können Sie das Feld leer lassen.
- **Passwort** – Passwort für das Anmelden des Interkoms zum SMTP-Server.
- **Client-Zertifikat** – spezifiziert das Kundenzertifikate und den privaten Schlüssel, mit Hilfe deren die Verschlüsselung der Kommunikation zwischen dem Interkom 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 Interkomstart 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 Interkom versucht, eine E-Mail an einen unerreichbaren SMTP-Server zuzustellen.



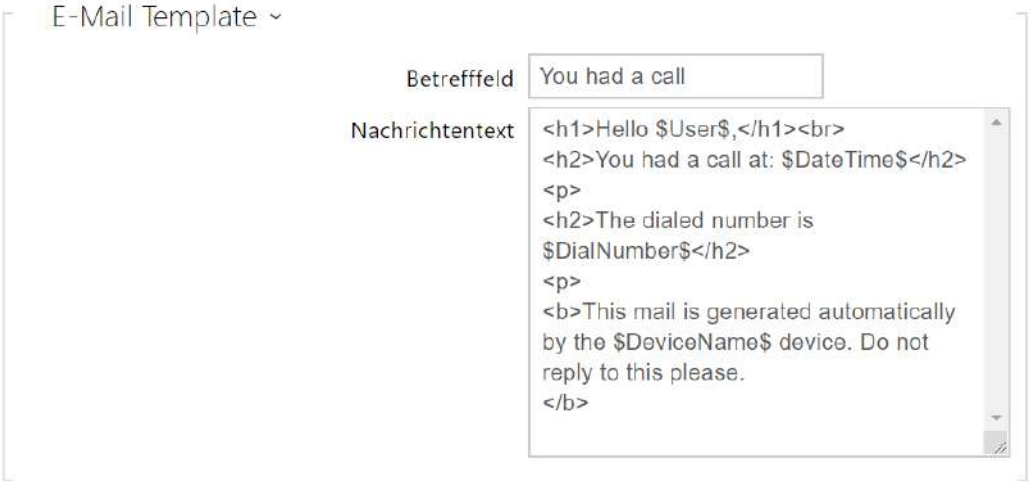
Mittels der Taste **Anwenden & überprüfen** kann man eine Test-E-Mail an die eingegebene Adresse senden und so die Funktionsfähigkeit der aktuellen Einstellung der Absendung von E-Mails testen. Geben Sie in das Feld Adresse der Test-E-Mail die Ziel-E-Mailadresse ein und drücken Sie die Taste. Im Verlauf 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. Der E-Mail wird eine Aufnahme aus der Kamera hinzugefügt. Gilt auch für Modelle ohne Kamera, wo ein Bild mit N/A geschickt wird.

Registerkarte E-Mail bei Gespräch

In dieser Karte kann man das Absenden von E-Mails im Verlauf der ausgehenden Anrufe einstellen.

- **Dem Benutzer eine E-Mail senden, im Fall** – ermöglicht das Senden einer E-Mail an den Benutzer bei ausgehenden oder verpassten Anrufen. Die E-Mail wird nach dem Auflegen geschickt. Man kann zwischen folgende Möglichkeiten wählen:
  - **E-Mail nicht senden** – bei ausgehenden Anrufen werden keine E-Mails gesendet.
  - **Alle ausgehenden Anrufe** – die E-Mail wird nach jedem ausgehenden Anruf geschickt.
  - **Verpasste ausgehende Anrufe** – die E-Mail wird nach jedem nicht angenommenen ausgehenden Anruf gesendet

> **Anmerkung**
>
> - Man kann die E-Mails jeweils mittels der Automatisierung absenden.



- **Betrefffeld** – stellt den Betreff der abgesendeten E-Mail ein.
- **Nachrichtentext** – bearbeiten Sie den Text, der verschickt werden soll. Verwenden Sie im Text die HTML-Formatierungszeichen. Man kann Sonderzeichen für Datum, Zeit, Identifizierung der Sprechanlage und angerufene Station verwenden. Man kann

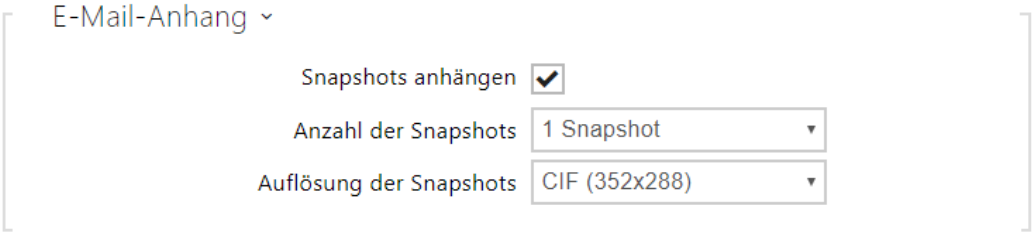
Sonderzeichen für Datum, Zeit, und Identifizierung der Sprechanlage verwenden. Diese Sonderzeichen werden vor dem Absenden der Nachricht durch den aktuellen Wert ersetzt. Die Liste der in der Vorlage gefundenen Platzhalter ist in der Übersichtstabelle am Ende dieses Kapitels dargestellt.

Nachrichtentext

```
<p>Hello <b>$User$</b>
</p>
<p>You had a call on: <b>$DateTime$</b>
  <br>The number dialed was: <b>$DialNumber$</b>
</p>
<p>This e-mail message is generated automatically by device: <b>$DeviceName$</b>. Do
not reply to this message.
</p>
```

Hinweis

- Erfolgt der Aufruf an mehrere Benutzer, ist der Platzhalter für den Namen des angerufenen Benutzers $User$ leer.

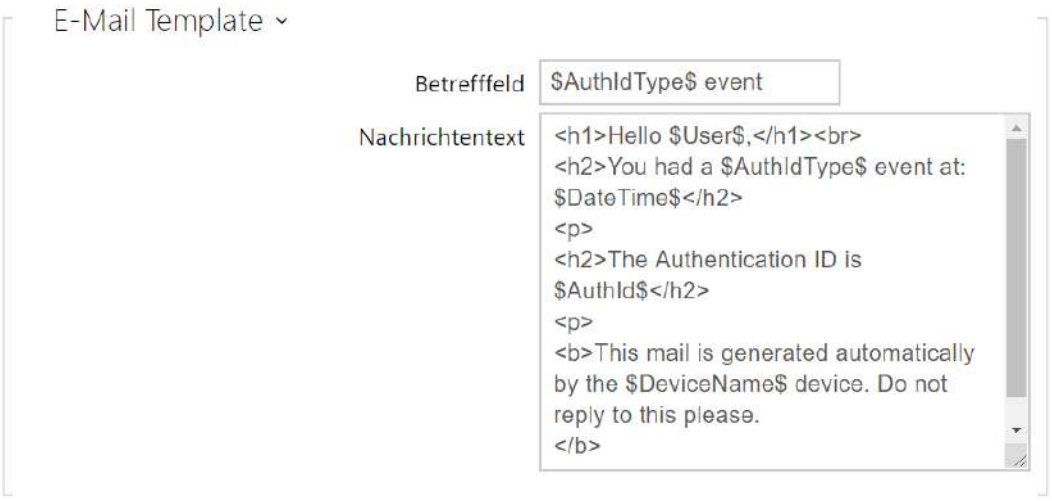


- **Snapshots anhängen** – erlaubt das Absenden des Anhangs mit einer oder mehreren Aufnahmen aus der Kamera, die während des Anrufs oder der Klingelns aufgezeichnet wurden.
- **Anzahl der Snapshots** – stellt die Zahl der Aufnahmen ein, die der E-Mail hinzugefügt werden.
- **Auflösung der Snapshots** – stellt die Auflösung der versendeten Aufnahmen ein.

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** – bearbeiten Sie den Text, der verschickt werden soll. Verwenden Sie im Text die HTML-Formatierungszeichen. Man kann Sonderzeichen für Datum, Zeit, Identifizierung der Sprechanlage und angerufene Station verwenden. Man kann Sonderzeichen für Datum, Zeit, und Identifizierung der Sprechanlage verwenden. Diese Sonderzeichen werden vor dem Absenden der Nachricht durch den aktuellen Wert ersetzt. 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>
```

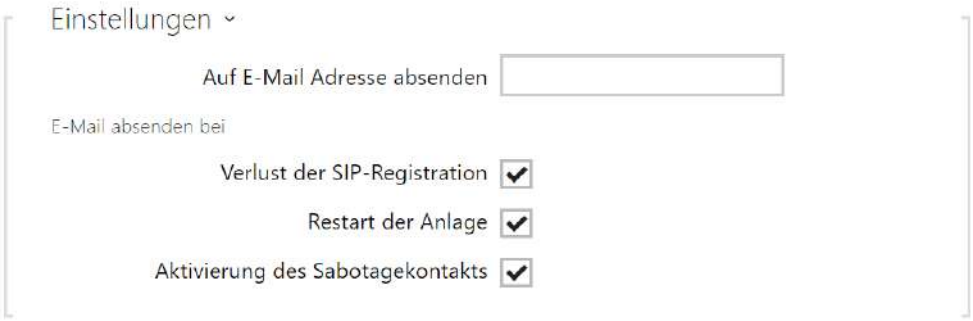
Hinweis

- 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.

- **Snapshot anhängen** – erlaubt das Absenden des Anhangs mit einer Aufnahme aus der Kamera, die zum Zeitpunkt des Kartenanlegens aufgezeichnet wurde.
- **Auflösung der Snapshots** – stellt die Auflösung der versendeten Aufnahme ein.

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:

- **Verlust der SIP-Registration**
- **Restart der Anlage**
- **Aktivierung des Sabotagekontakts**

Meldung beim Verlust der SIP-Registration – einstellung der Nachricht, die beim Verlust der SIP-Registration auf die angegebene E-Mail-Adresse gesendet wird.

- **Betrefffeld** – stellt den Betreff der abgesendeten E-Mail ein.
- **Nachrichtentext** – bearbeiten Sie den Text, der verschickt werden soll. Verwenden Sie im Text die HTML-Formatierungszeichen. Man kann Sonderzeichen für Datum, Zeit, Identifizierung der Sprechanlage und angerufene Station verwenden. Man kann

Sonderzeichen für Datum, Zeit, und Identifizierung der Sprechanlage verwenden. Diese Sonderzeichen werden vor dem Absenden der Nachricht durch den aktuellen Wert ersetzt. Die Liste der in der Vorlage gefundenen Platzhalter ist in der Übersichtstabelle am Ende dieses Kapitels dargestellt.

Nachrichtentext

```
<p>Hello,
</p>
<p>SIP account <b>$SipAccountNumber$</b> of device <b>$DeviceName$</b> (IP:
<b>$Ip4Address$</b>) got unregistered 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.

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** – bearbeiten Sie den Text, der verschickt werden soll. Verwenden Sie im Text die HTML-Formatierungszeichen. Man kann Sonderzeichen für Datum, Zeit, Identifizierung der Sprechanlage und angerufene Station verwenden. Man kann Sonderzeichen für Datum, Zeit, und Identifizierung der Sprechanlage verwenden. Diese Sonderzeichen werden vor dem Absenden der Nachricht durch den aktuellen Wert ersetzt.

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** – bearbeiten Sie den Text, der verschickt werden soll. Verwenden Sie im Text die HTML-Formatierungszeichen. Man kann Sonderzeichen für Datum, Zeit, Identifizierung der Sprechanlage und angerufene Station verwenden. Man kann Sonderzeichen für Datum, Zeit, und Identifizierung der Sprechanlage verwenden. Diese Sonderzeichen werden vor dem Absenden der Nachricht durch den aktuellen Wert ersetzt. Die Liste der in der Vorlage gefundenen Platzhalter ist in der Übersichtstabelle am Ende dieses Kapitels dargestellt.

- **Kamera-Snapshots anhängen** – aktiviert das Versenden von Anhängen einschließlich eines oder mehrerer Kamera-Snapshots, die bei ausgehenden Telefonanrufen erstellt wurden.
- **Zahl der angehängten Snapshots** – legt die Anzahl der Snapshots fest, die an die E-Mail-Nachricht angehängt werden sollen.
- **Auflösung der Snapshots** – Legt die Auflösung der Snapshots für die Bilder, die verschickt werden sollen, fest.

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 Abschnitt Services / Webserver / Basis-Einstellungen . Wir empfehlen, einen Namen zu verwenden, der eindeutig definiert, um welches Gerät es sich handelt.

Liste der Platzhalter

Auftreten	Platzhalter	Beschreibung
Immer	$DateTime$	aktuelles Datum und Uhrzeit
	$DeviceName$	Gerätebezeichnung
	$Ip4Address$	IP-Adresse des Geräts
	$SoftwareVersion$	FW-Version
	$BuildTime$	Erstellungsdatum und -zeit
	$UpTime$	Betriebszeit des Gerätes

Auftreten	Platzhalter	Beschreibung
Abhängig vom konkreten Fall	$User$	Benutzername
	$RebootReason$	Grund für den Neustart
	$DialNumber$	Angerufene Nummer, eingehend oder ausgehend
	$SipAccountNumber$	SIP-Kontonummer
	$AuthId$	Authentifizierungs-ID
	$AuthIdDirection$	Richtung (Eingang/Ausgang)
	$AuthIdType$	Authentifizierungsart
	$AuthIdValid$	gültig, ungültig
	$AuthIdReason$	Grund für die Ablehnung

Übersicht über Platzhalter in Ereignissen

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

Platzhalter / Funktion	E-Mail bei Zutritt	E-Mail bei Gespräch	E-mail bei Verlust der SIP-Registration	E-mail bei Restart der Anlage	E-mail bei Aktivierung des Sabotagekontakts	E-Mail bei Diagnose senden	Automatisierung
$RebootReason$				*			
$DialNumber$		*				• (sendet “E-Mail-Test”)	CallStateChanged
$SipAccountNumber$			*				
$AuthId$	*						CardEntered, CardHeld
$AuthIdDirection$	*						CardEntered, CardHeld
$AuthIdType$	*						CardEntered, CardHeld
$AuthIdValid$	*						CardEntered, CardHeld
$AuthIdReason$	*						

5.4.4 Automatisierung

Die **Interkoms 2N IP** bieten 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 bieten die **Interkoms 2N IP** die spezielle programmierbare Schnittstelle **Automation** an. Die typische Anwendung der **Automation** ist für Applikationen, die eine kompliziertere Verknüpfung mit Systemen Dritter erfordern.

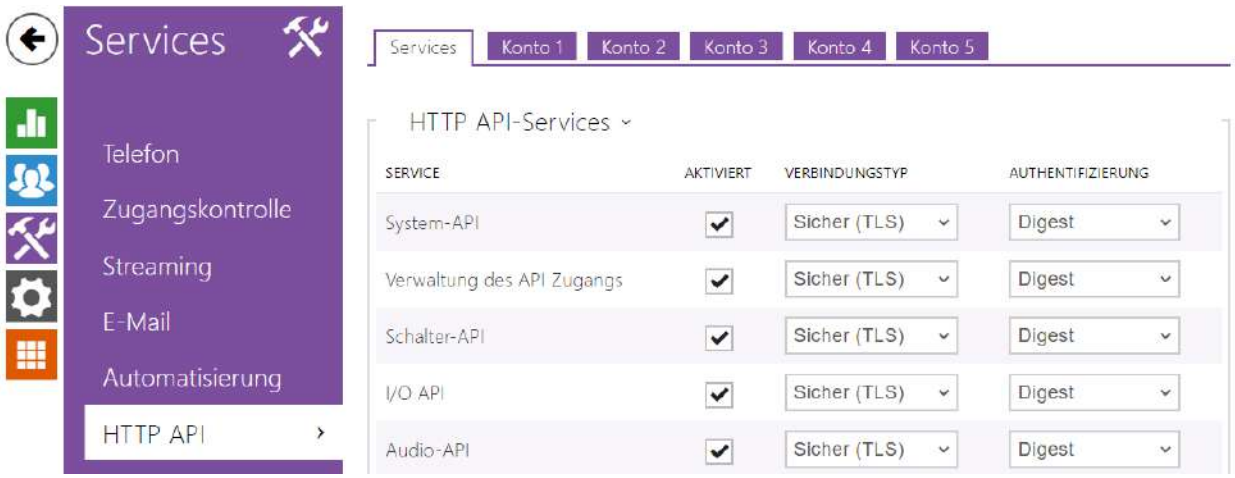
Eine detaillierte Beschreibung der Funktion und Konfiguration von **Automation** befindet sich im Konfigurationshandbuch Automation.

Anmerkung

- *Die Automatisierungsfunktion ist nur mit der Lizenz Gold.*

5.4.5 HTTP API

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



Services

HTTP API ist gemäß der Funktion in folgende Leistungen aufgeteilt:

- **System-API** – ermöglicht Konfigurationsänderungen, Erwerben des Status und Upgrade vom Interkom.
- **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 Interkoms.
- **Audio-API** – ermöglicht die Steuerung des Tonabspielens und der Überwachung des Anlagenmikrophons.
- **Kamera-API** – ermöglicht die Steuerung und Verfolgung des Bildes aus der Kamera.
- **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.

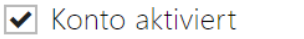
Die detaillierte Beschreibung und Einstellung von HTTP API ist im Handbuch HTTP API angeführt.

Tipp

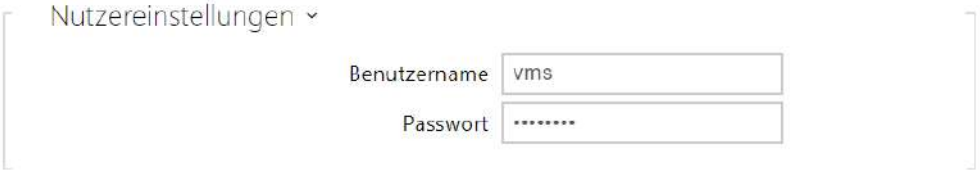
- Für die Funktion Video Preview auf dem Telefon Gigaset Maxwell 10 muss man in der Registerkarte **HTTP API** bei der Position **Camera API** den**Typ des Anschlusses = Nicht gesichert (TCP)** und der **Authentifizierung = Keine** einstellen.

Konto 1–5

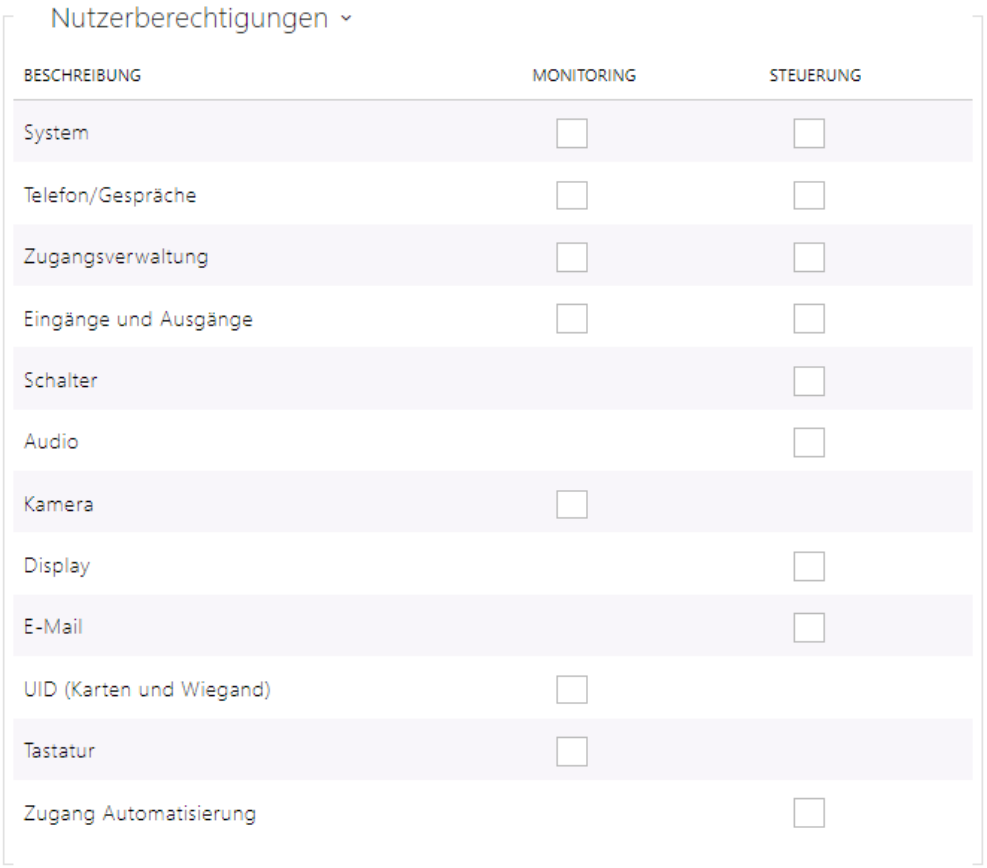
2N IP interkom ermöglicht bis zu fünf Benutzerkonten zu verwalten, die für den Zugriff auf die Dienstleistungen bestimmt sind **HTTP API**. Das Benutzerkonto enthält den Benutzernamen und das Benutzerpasswort sowie eine Tabelle mit den Zugriffsberechtigungen des Benutzers für jede Dienstleistung **HTTP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



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



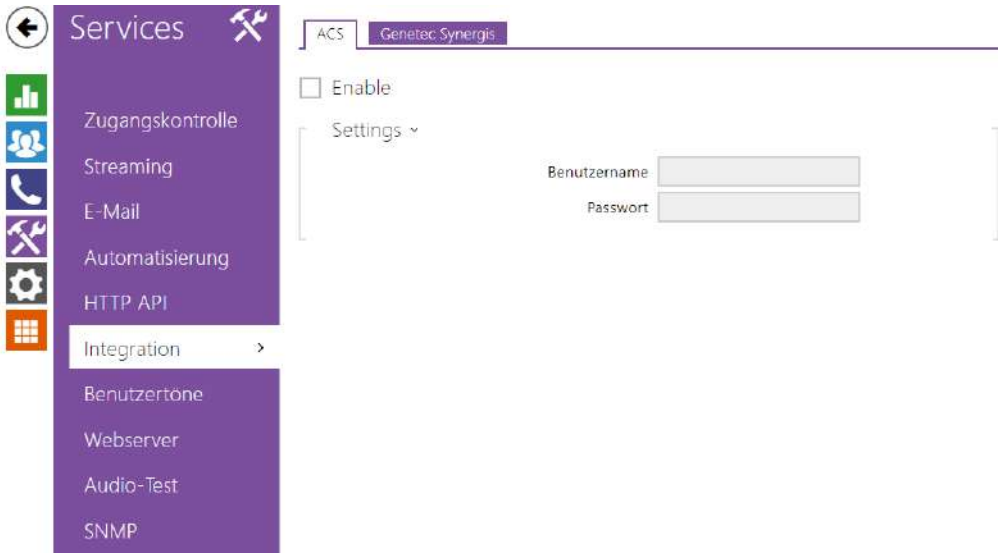
- **Benutzername** – geben Sie den Benutzernamen für die Authentifizierung des HTTP API ein.
- **Passwort** – geben Sie das Authentifizierungspasswort für HTTP API ein.



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

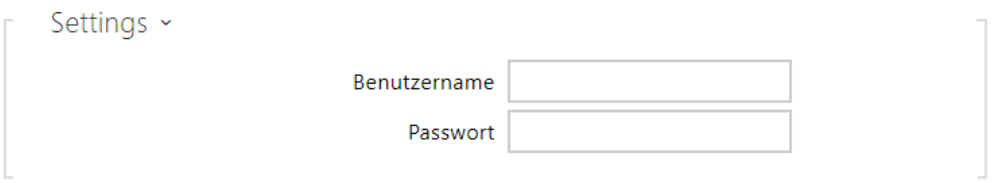
5.4.6 Integration

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



Registerkarte ACS

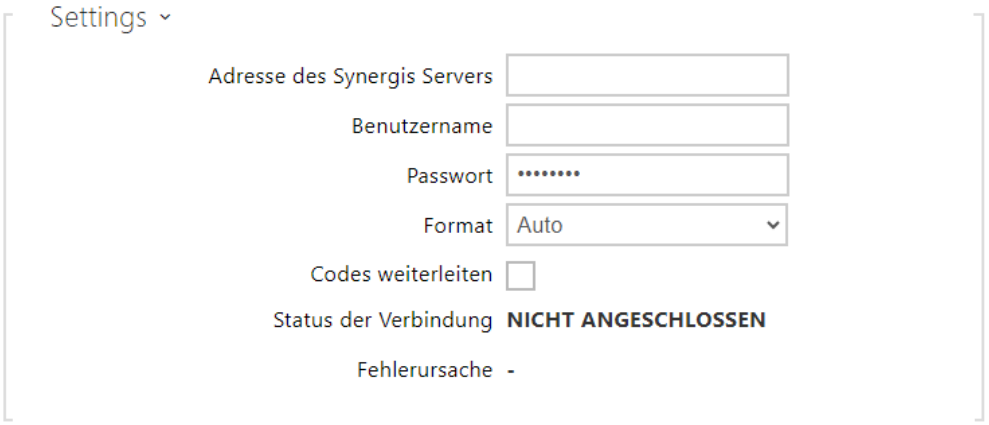
- **Freigegeben** - erlaubt die Anruffunktion an Axis Camera Station (ACS). Für Anrufe an ACS wird ein spezieller URI in der Form vms:* verwendet.



- **Benutzername** - Name für Benutzer für die ACS-Anrufauthentifizierung.
- **Passwort -** Passwort für die ACS-Anrufauthentifizierung.

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.

5.4.7 Benutzertöne

Die Interkoms **2N IP** signalisieren standardmäßig manche Betriebsstatus mittels einer Tonsequenz, siehe Kapitel Signalisierung der Betriebsstatus. Wenn Ihnen die standardmäßigen Signaltöne nicht genügen, können Sie sie anpassen.
Das Interkom ermöglicht die Tonsignalisierung für diesen Status zu ändern:

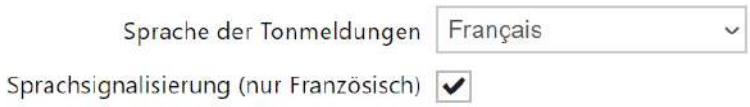
a. **Klingeln vor dem Entgegennehmen des Anrufes**
b. **Begrüssungston**
c. **Besetztzeichen**
d. **Signal Auflegen**
e. **Signal ungültiger Eingang**
f. **Signal ungültige Position**
g. **Signal Aktivierung des Schalters**

Sie können die Signalisierung des vorstehend angeführten Status entweder ganz leise Stellen, durch einen der zehn vordefinierten Töne oder eine eigene Tondatei ersetzen, die Sie einfach in das Interkom hochladen. Die Tondateien müssen im Format WAV sein und die PCM-Kodierung mit der Probefrequenz 8 oder 16 kHz und der Auflösung der Probe 8 oder 16 bits verwenden. Die Dateigröße darf bei **2N IP Interkoms** 256 kB, bei **2N® SIP Horn** 2048 kB nicht überschreiten.

Frequenz	Bits auf Probe	Tonlänge	Tonqualität
16 kHz	16 bit	up to 8 s	1 best
16 kHz	8 bit	up to 16 s	2
8 kHz	16 bit	up to 16 s	3 (not recommended combination)
8 kHz	8 bit	up to 32 s	4 low

Sie können die eingespielten Tondateien mithilfe der Automatisierung mittels der Aktion **Action.PlayUserSound** abspielen. Sie können die Töne mittels des Lautsprechers des Interkoms und/oder direkt in den Telefonanruf abspielen.

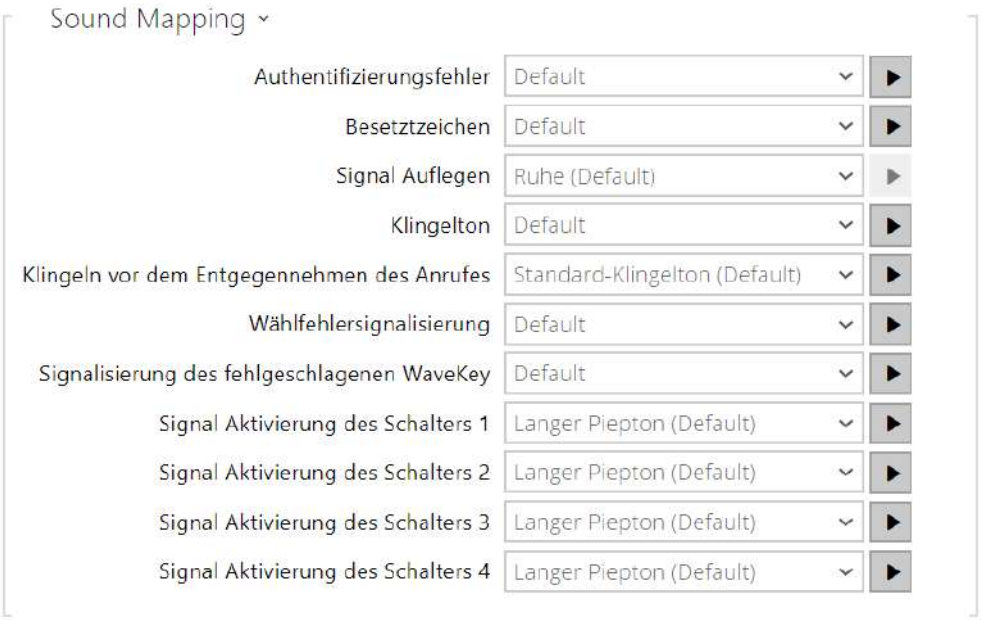
Parameterliste



- **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.

- **Sprachsignalisierung (nur Französisch)** – um die gesetzlichen Bestimmungen in französischsprachigen Regionen einzuhalten, kann die Sprachsignalisierung für behinderte Menschen auf Französisch für die folgenden Aktionen aktiviert werden: Anrufaufbau, Anrufverbindung und Türentriegelung.

Sound Mapping



- **Authentifizierungsfehler** – legt den Ton fest, der abgespielt wird, wenn der Zugriff verweigert wird.
- **Besetztzeichen** – legt den Besetztton fest (der ertönen soll, wenn der Angerufene besetzt ist).
- **Signal Auflegen** – legt den Ton fest, der ertönen soll, wenn der Anruf endet.
- **Klingelton** – legt den Ton fest, der ertönen soll, wenn beim Angerufenen geklingelt wird. Der Klingelton der Zentrale hat Vorrang vor dem eingestellten Klingelton im Interkom.
- **Klingeln vor dem Entgegennehmen des Anrufes** – legt den Ton fest, der ertönen soll, bevor ein eingehender Anruf beantwortet wird (Klingelton der Sprechanlage).
- **Wählfehlersignalisierung** – legt den Ton fest, der ertönen soll, wenn eine Kurzwahltaste gedrückt wird, die entsprechende Position im Telefonbuch jedoch nicht programmiert ist.
- **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.

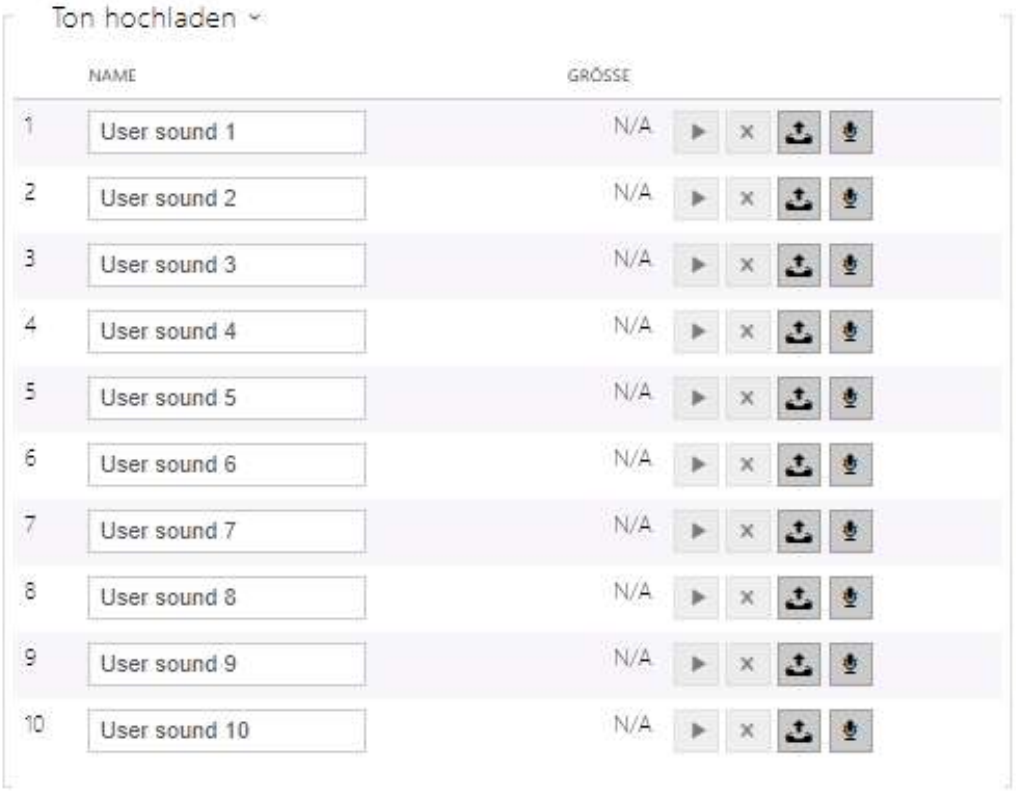
Hinweis

- Wenn der Wortlaut des zugewiesenen Audios nicht abgespielt werden kann, liegt dies daran, dass das Audio auf "Lautlos" gestellt ist.

Töne hochladen

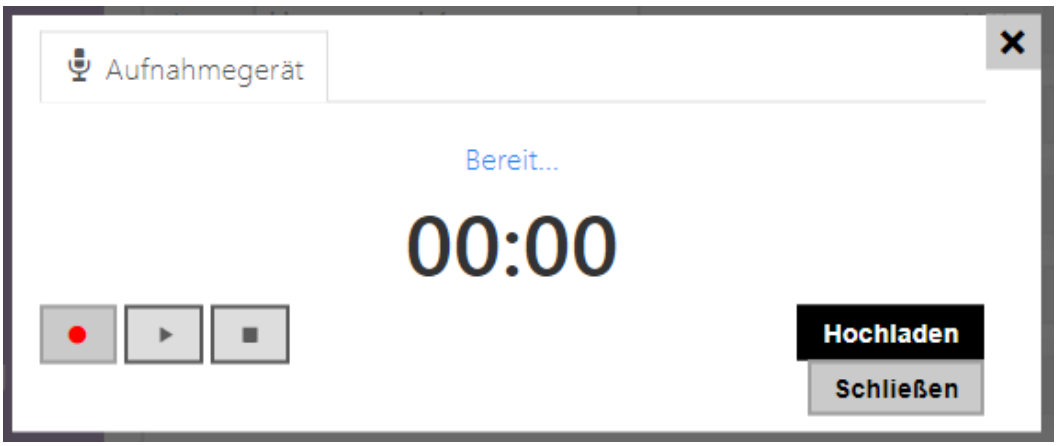
Sie können in das Interkom bis zu 10 eigene Tondateien hochladen. Sie können der größeren Übersichtlichkeit wegen jedem hochgeladenen Ton eine eigene Bezeichnung zuordnen.

Die Tondatei wird in das Interkom durch das Drücken der Taste hochgeladen. Wählen Sie im Dialogfenster eine in Ihrem PC gespeicherte Datei aus und drücken Sie die Taste **Hochladen**. Sie können die Datei mittels der Taste löschen. Man kann die hochgeladene Tondatei (lokal auf seinem PC) mittels der Taste abspielen. Sie können mittels der Taste die Tondatei direkt mittels des Mikrophons in Ihrem PC hochladen.



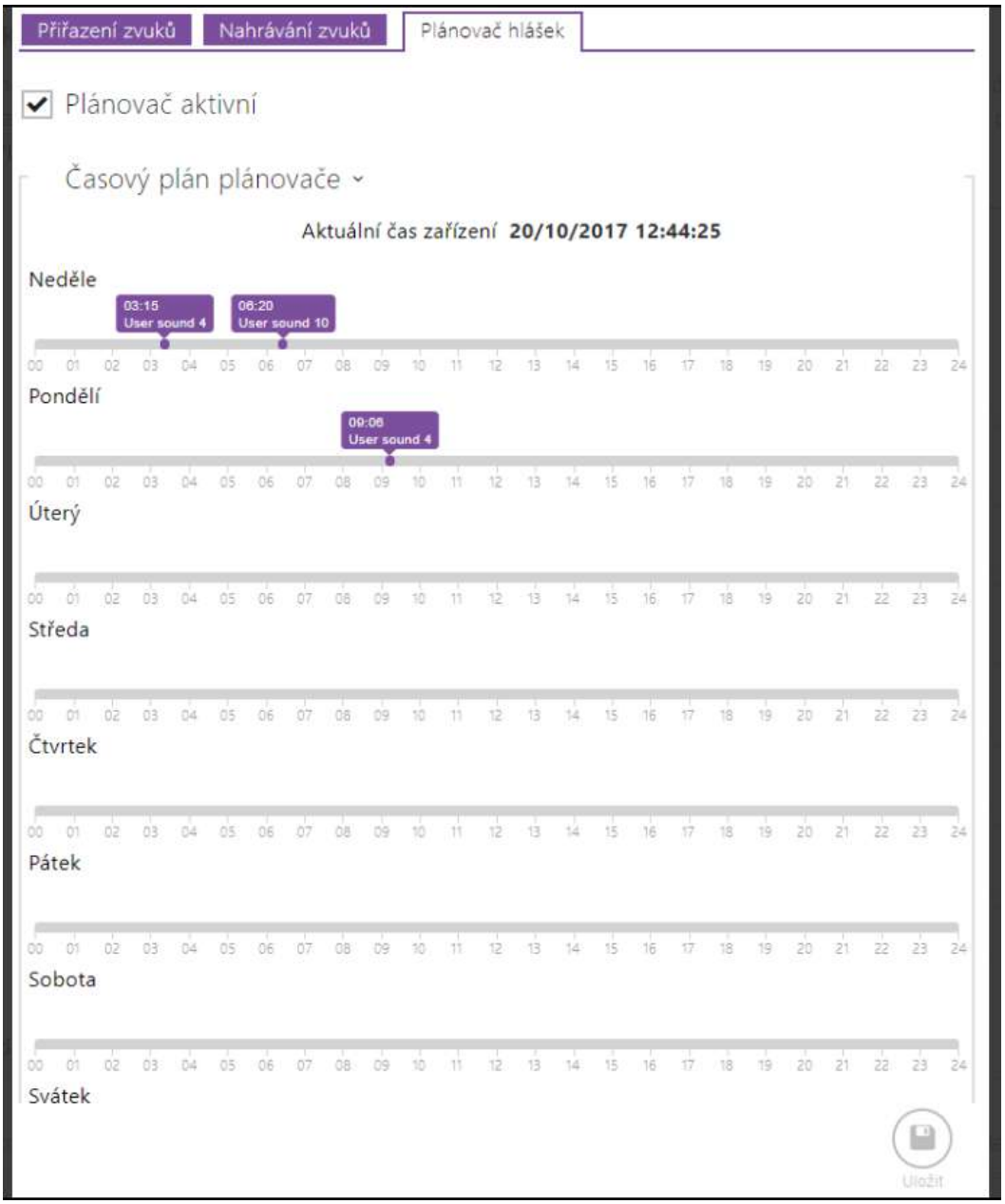
Sie können die Tondatei mittels des Mikrophons in Ihrem PC aufzeichnen. Mittels der Taste wird die Aufzeichnung abgespielt. Beendet wird sie durch Drücken der Taste . Man kann den

aufgezeichneten Ton mittels der Taste ▶ abspielen. Der Ton wird nach dem Drücken der Taste **Hochladen** im Interkom gespeichert.



Planer von Meldungen

Ermöglich das regelmäßige Abspielen der Nutzertöne in der eingestellten Uhrzeit. Man kann im Zeitplan genaue Uhrzeiten für einzelne Wochentagen einstellen, an denen der jeweilige Ton abgespielt wird. Das Abspielen des Tons wird durch das Klicken auf die geforderte Stelle auf der Zeitachse des gewählten Tages durchgeführt. Beim Hinzufügen kann man die genaue Uhrzeit einstellen, den Nutzerton wählen und seine Lautstärke einstellen. Die Registerkarte **Planer der Meldungen** ist nur für **2N SIP Audio** Produkte verfügbar.



- **Planer aktiv** – aktiviert das Abspielen der voreingestellten Nutzertöne gemäß dem Zeitplaner.

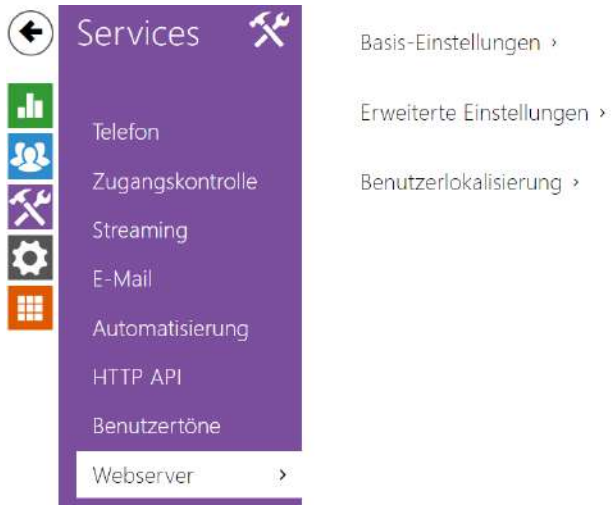
Tipp

- Für die Hilfe, wie man Nutzertöne erstellt, gehen Sie gemäß den Informationen in diesem Link vor https://wiki.2n.cz/hip/inte/latest/en/10-media-applications/audacity.

Anmerkung

- Die Funktion für die Tonaufzeichnung ist bei Webbrowsern nicht verfügbar, die nicht den Standard WebRTC (z.B. Internet Explorer) unterstützen.

5.4.8 Webserver



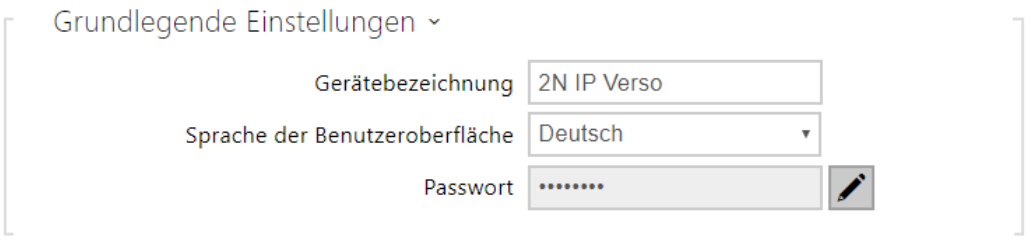
Man kann die **Interkoms 2N IP** mittels eines üblichen Webbrowsers konfigurieren, der auf den Webserver zugreift, der im Interkom integriert ist. Für die Kommunikation zwischen dem Webbrowser und dem Interkom wird das gesicherte HTTPS-Protokoll verwendet. Nach der Anmeldung im Interkom muss man den 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 Interkomfunktionen genutzt:

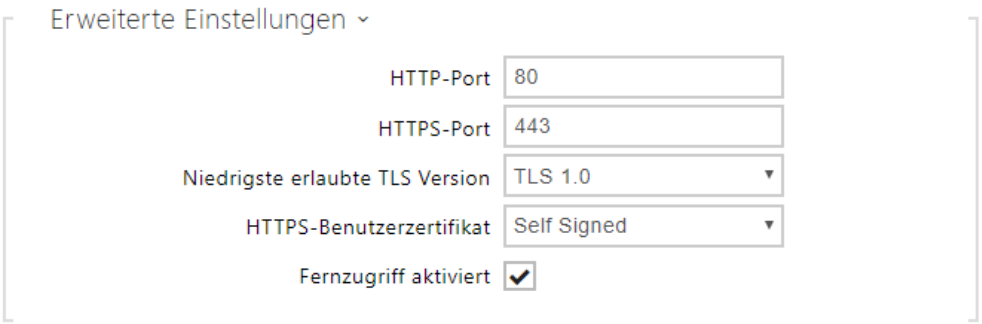
a. Herunterladen von JPEG-Aufnahmen ggf. MJPEG-Videos, siehe Kapitel Streaming.
b. ONVIF-Protokoll für Videostreaming, siehe Kapitel Streaming
c. HTTP-Befehle für die Bedienung der Schalter, siehe Kapitel Schalter
d. Ereignisse Event.HttpTrigger in **Automation**, siehe jeweiliges Handbuch.

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 (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.
- **Passwort** – stellt das Passwort für die Anmeldung zum Interkom ein. Für die Passwortänderung die Taste benutzen. 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 erfolgt erst nach dem Neustart des Interkoms.
- **Der HTTPS-Port** – stellt den Kommunikationsport des Webservers für die Kommunikation mittels des gesicherten HTTPS-Protokolls ein. Die Änderung des Ports erfolgt erst nach dem Neustart des Interkoms.
- **Niedrigste erlaubte TLS Version** – Legt die niedrigste erlaubte TLS Version fest, mit der man sich auf dem Server anmelden und Verbindungen herstellen kann.
- **HTTPS-Benutzerzertifikat** – stellt das Nutzerzertifikat und den privaten Schlüssel ein, mit Hilfe deren die Verschlüsselung der Kommunikation zwischen dem HTTP-Server des

Interkoms und dem Webbrowser auf der Seite des Nutzers durchgeführt wird. 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 des Interkoms von IP-Adressen außerhalb des lokalen Netzes zu erlauben.

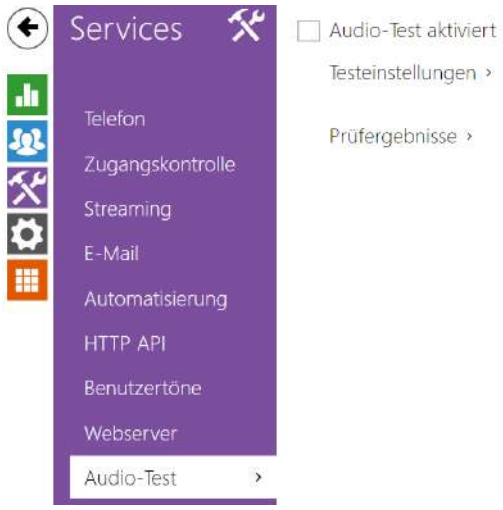
- **Originalsprache** – ermöglicht aus der Anlage die Originaldatei herunterzuladen, die alle Texte der Nutzerschnittstelle in englischer Sprache enthält. Die Datei ist im Format XML siehe nachstehend.
- **Benutzersprache** – ermöglicht die Nutzerdatei mit eigenen Übersetzungen der Texte der Nutzerschnittstelle hochzuladen, herunterzuladen und gegebenenfalls zu löschen.

language = xml

```
 xml<?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>
```

Modifizieren Sie bei der Übersetzung nur die Werte der Elemente **<s>** und ändern sie nicht die Attributwerte **id**. Die Bezeichnung der Sprache, die durch das Attribut **language** des Elements **<strings>** gegeben ist, wird in den Möglichkeiten des Parameters Sprache der Webschnittstelle 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.

5.4.9 Audio-Test

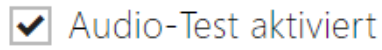


Die **Interkoms 2N IP** ermöglichen eine regelmäßige Kontrolle des eingebauten Lautsprechers und Mikrophons durchzuführen. Der Lautsprecher generiert im Verlauf des Tests einen oder mehrere kurze Töne. Der generierte Ton wird mittels des eingebauten Mikrophons aufgenommen und, wenn er richtig erkannt 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 des Interkoms anzeigen oder mittels **Automation** *verarbeiten.*

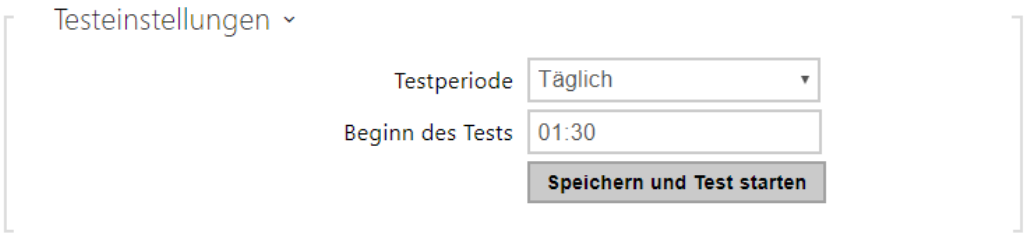
Anmerkung

- *Wenn während des Audiotests ein Anruf läuft, wird der Audiotest aufgeschoben, bis der Anruf beendet ist. Der Audiotest wird gleich nach dem Ende des Anrufes durchgeführt.*

Parameterliste



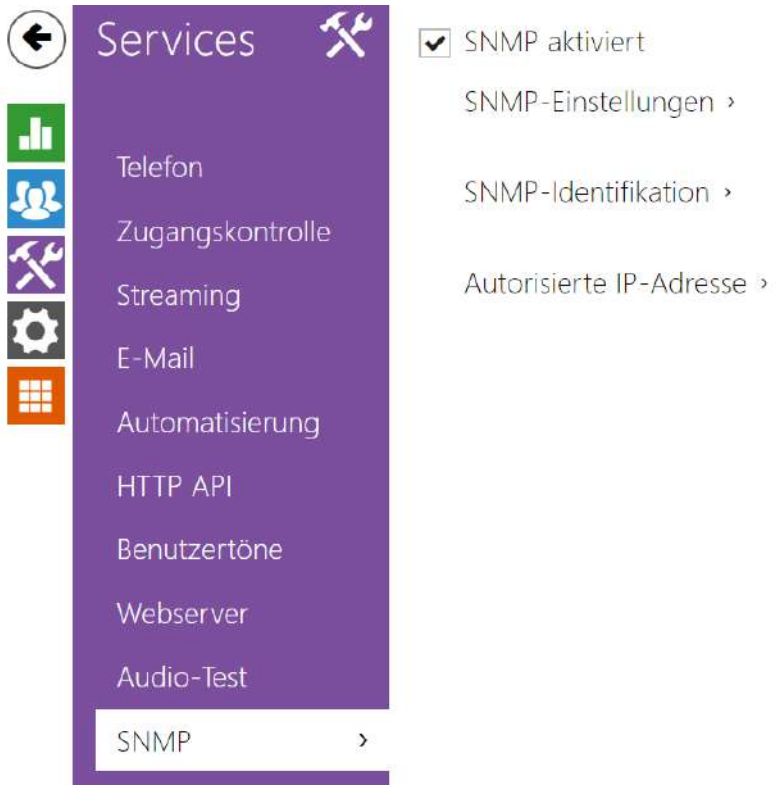
- **Freigabe des Audiotests** – erlaubt das automatische Durchführen des Audiotests.



- **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 des Interkoms erwarten kann.
- **Speichern und Test starten** – mittels der Taste können Sie den Test sofort starten, ohne Hinsicht auf die aktuelle Einstellung.

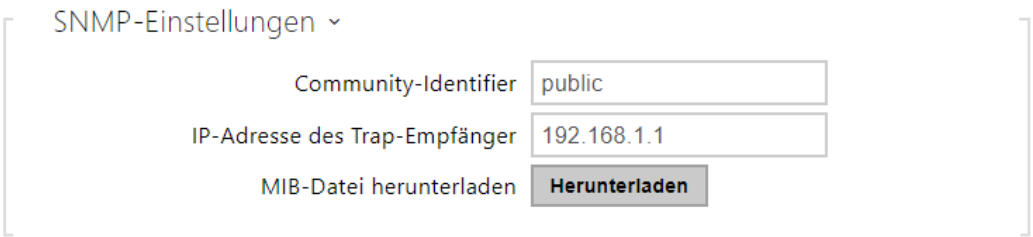
- **Teststatus** – zeigt durchgehend den Status des Testverlaufs an.
- **Letzter Testzeitpunkt** – zeigt die Uhrzeit des zuletzt durchgeführten Tests an.
- **Letztes Testergebnis** – zeigt das Ergebnis des zuletzt durchgeführten Tests an.

5.4.10 SNMP



Die **Interkoms 2N IP** integrieren die Funktionalität, die die entfernte Aufsicht der Interkoms im Netz mittels des SNMP-Protokolls ermöglichen. Der SNMP-Agent, der in der Anlage integriert ist, ist nach der Eingabe des Lizenzschlüssels mit der Lizenz **Enhanced Integration** verfügbar. Die Interkoms unterstützen das SNMP-Protokoll der Version 2c.

Parameterliste

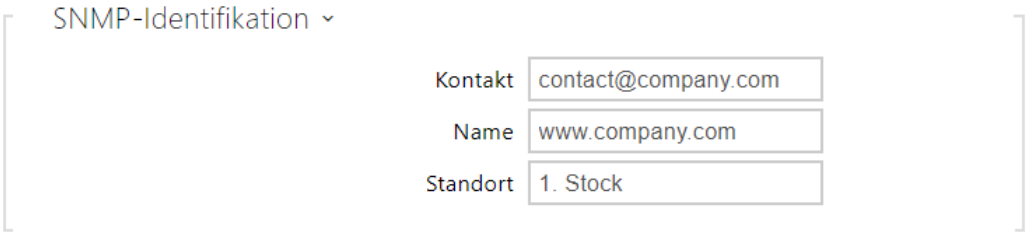


- **Community-Identifier** – Textkette, die den Zutrittscode für den Zutritt zu Objekten in der MIB-Tabelle repräsentiert.
- **IP-Adresse des Trap-Empfänger** – IP-Adresse, an die die SNMP-Traps gesendet werden.

Anmerkung

- In der derzeitigen Version werden keine Traps unterstützt. Das **2N IP Interkom** arbeitet nur im Modus Anforderung - Antwort.

- **MIB-Datei herunterladen** – ermöglicht die aktuelle Definition der MIB-Tabelle von der Anlage herunterzuladen.



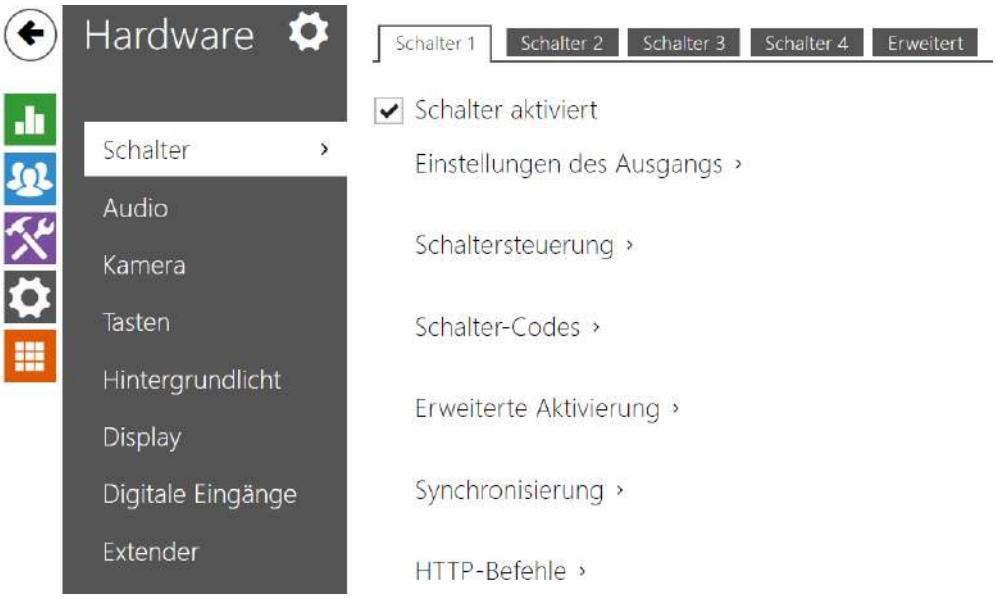
- **Kontakt** – ermöglicht den Kontakt des Anlagenverwalters (z.B. Name, E-Mail u.Ä.) einzugeben.
- **Name** – ermöglicht die Bezeichnung der Anlage einzugeben.
- **Standort** – ermöglicht die Beschreibung der Anlagenunterbringung (z.B. 1. Etage) einzugeben.

- **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 Hardware

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

5.5.1 Schalter



Die Schalter ermöglichen eine sehr flexible Steuerung von verschiedenen zum Interkom angeschlossenen Peripherien (wie die elektrische Türschlösser, Beleuchtung, Ergänzungssignalisierung des Klingelns u.Ä. sind).

Die **2N IP Interkoms** ermöglichen bis zu 4 (kann sich bei verschiedenen Modellen unterscheiden) 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 des Interkoms oder durch den Empfang der DTMF-Sequenz der Zeichen beim Anruf,
- mittels des Anlegens einer gültigen RFID-Karte an den Leser,
- mit definierter Verzögerung nach dem Einschalten eines anderen Schalters,
- mittels eines eingehenden oder ausgehenden Anrufes,
- durch das Drücken einer der Kurzwahltasten *),
- 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:

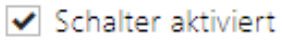
- das Schalten eines beliebigen logischen Interkomausgangs (Relais, Leistungsausgang)
- das Schalten des Ausgangs, an den das Modul **2N® IP Interkom – Sicherheitsrelais** angeschlossen ist
- das Abschicken des HTTP-Befehls an eine andere Anlage

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.

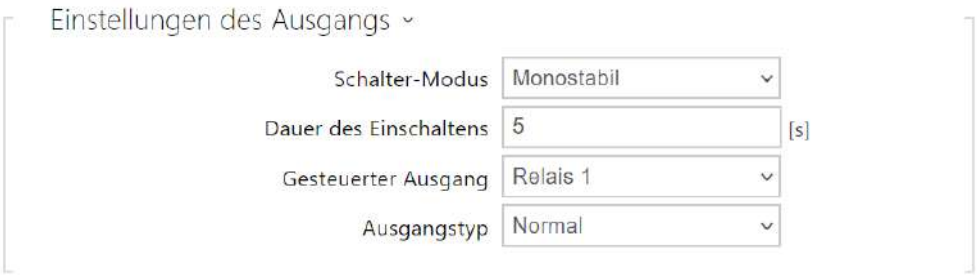
Der Schalter kann seinen Status signalisieren mittels:

- konfigurierbaren Pieptons ggf. gewählten Nutzertons
- Signalisierungs-LED-Diode, wenn das Interkom damit ausgestattet ist
- auf dem Display (wenn das jeweilige Interkommodell damit ausgestattet ist) mittels der Schaltfläche der offenen Tür

Registerkarte Schalter 1–4



- **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.



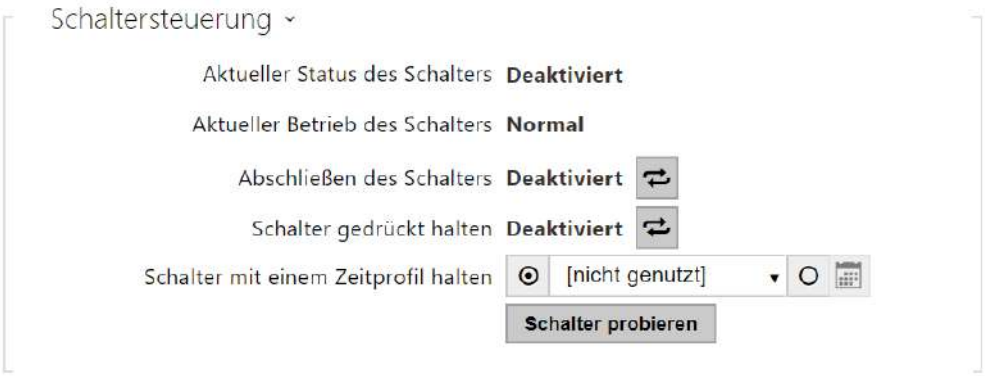
- **Schalter-Modus** – stellt den monostabilen oder bistabilen Schaltermodus ein. Im monostabilen Modus wird der Schalter nach eingestellter Schaltzeit automatisch ausgeschaltet. Im bistabilen Modus wird der Schalter mit der ersten Aktivierung eingeschaltet und mit der folgenden ausgeschaltet.
- **Dauer des Einschaltens** – stellt die Schaltzeit des Schalters im monostabilen Modus ein. Die eingestellte Schaltzeit wird nicht im bistabilen Modus angewendet.
- **Gesteuerter Ausgang** – weimst dem Schalter einen elektrischen Ausgang zu. Wählen Sie einen aus den verfügbaren aus: Relais, Leistungsausgang, Ausgänge auf Erweiterungsmodulen u. ä. Relais, Stromausgang, Extenderausgang. Wenn Sie keinen auswählen, steuertder Schalter keinen elektrischen Ausgang an, kann jedoch externe Ausrüstung über HTTP-Befehle steuern.
- **Ausgangstyp** – stellen Sie den Ausgangstyp auf Sicherheit, wenn Sie das 2N® IP Sicherheitsrelaismodul verwenden. Im Sicherheitsmodus arbeitet der Ausgang im Inverse-Modus, d.h. dieser bleibt geschlossen und steuert das 2N® IP Sicherheitsrelaismodul über eine spezifische Pulssequenze an. 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.

Anmerkung

- ***2N® IP Vario*** *– auf dem Konfigurationsstecker ist die interne Einspeisung und das Schaltrelais einzustellen.* ***2N® IP Force*** *– Sicherheitsrelais wird an die Klemmen DOOR + und – angeschlossen.*
- *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-Gegensprechanlage, 2N Access Unit) 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.



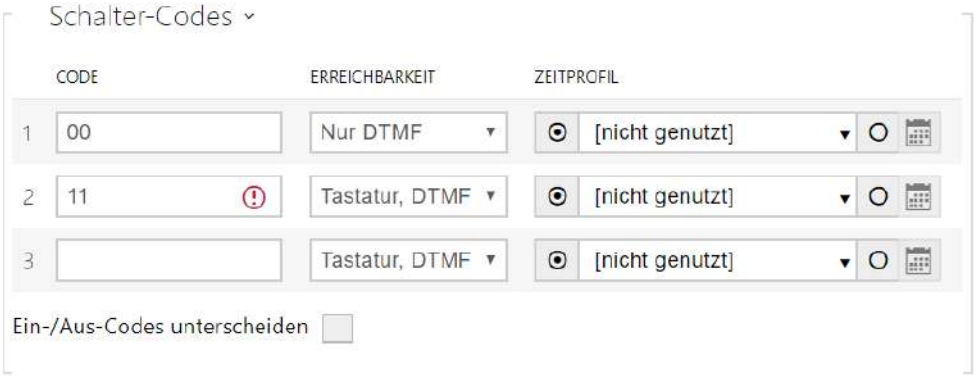
- **Aktueller Status des Schalters** – zeigt den aktuellen Status des Schalters an (Ein oder Aus).
- **Aktueller Betrieb des Schalters** – zeigt den aktuellen Betrieb des Schalters an.
  - **Normal**: Der Schalter ist nicht gesperrt oder wird nicht gehalten.
  - **Gehalten**: Der Schalter wird gehalten 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** – ein: Der Schalter befindet sich permanent in Position 0 und kann erst betätigt werden, wenn er entsperrt ist. Aus: Der Schalter ist nicht gesperrt.
- **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, durch einen Anruf, die Eingabe eines Codes oder einer Kurzwahltaste aktiviert 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 dem Telefongerät oder der Interkomtastatur die Schalter aktivieren kann. Für jeden Schalter kann man bis 10 Universalcodes eingeben (die Zahl der Codes kann sich bei einzelnen Interkommodellen unterscheiden).

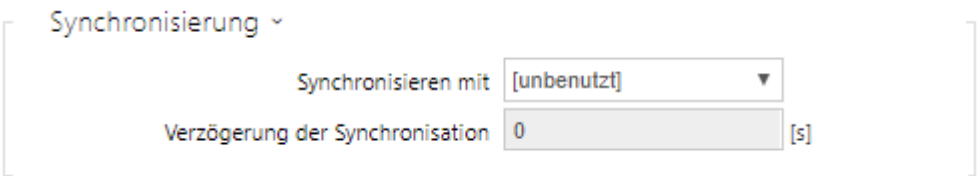
- **Code** – ermöglicht es den Zifferncode des Schalters einzugeben. Der Code muss mindestens zwei Zeichen für die Türentriegelung von der Interkomtastatur und mindestens ein Zeichen für die Türentriegelung mit DTMF vom Telefon enthalten. Wir empfehlen mindestens vier Zeichen zu verwenden. Codes 00 und 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.
- **Erreichbarkeit** – sie ermöglicht die Eingabe des Codes nach dem Einschalten des Schalters von der nummerischen Interkomtastatur oder vom Telefongerät des Nutzers zu sperren.
- **Zeitprofil** – ermöglicht dem Schaltercode ein Zeitprofil zuzuordnen und so seine Gültigkeit zu steuern.
- **Ein-/Aus-Codes unterscheiden** – ermöglicht den Modus der Schaltercodes einzustellen, wobei ungerade Codes (1., 3. usw.) für das Einschalten und gerade (2., 4. usw.) für das Ausschalten verwendet werden. Dieser Modus kann nur verwendet werden, wenn der Schalter in den bistabilen Modus eingestellt ist.

- **Aktivierung durch Anruf** – ermöglicht es die Aktivierung des Schalters durch einen eingehenden bzw. ausgehenden Anruf einzustellen. Beim ausgehenden Anruf wird der Schalter nach dem Erhalt der SIP-Nachricht 180 Ringing aktiviert, mit der die Gegenseite bestätigt, dass es klingelt. Im bistabilen Modus bleibt der Schalter während der ganzen Anrufzeit aktiv. Im monostabilen Modus wird der Schalter am Anfang des Anrufs aktiviert und dann nach der eingestellten Schaltzeit ausgeschaltet.
- **Aktivierung durch Kurzwahltaste** – ermöglicht dem Schalter eine der Kurzwahltasten zuzuordnen. Der Schalter wird jedes Mal aktiviert, wenn die Taste gedrückt wird.

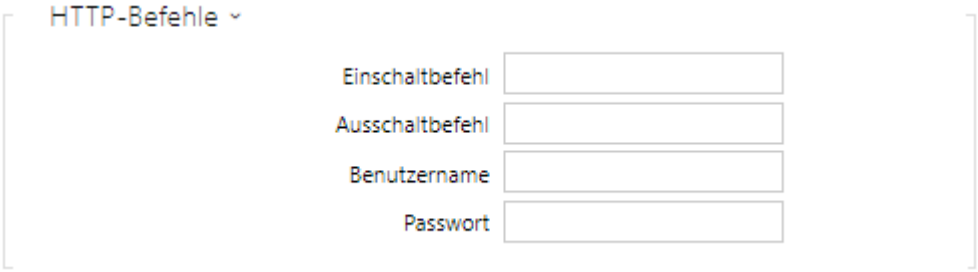
Anmerkung

- *Die Aktivierung mittels einer Kurzwahltaste ist nur mit der Lizenz Gold.*



- **Synchronisieren mit** – 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 mit** nicht erlaubt ist.



- **Einschaltbefehl** – ermöglicht den Befehl einzustellen, der an die externe Anlage (z.B. WEB-Relais) beim Schalten des Schalters geschickt wird. Der Befehl wird mittels des HTTP-Protokolls geschickt (GET Request). Der Befehl muss in der Form http://ip_adresse/weg sein. Z.B. http://192.168.1.50/relay1=on.
- **Ausschaltbefehl** – ermöglicht den Befehl einzustellen, der an die externe Anlage (z.B. WEB-Relais) beim Ausschalten des Schalters geschickt wird. Der Befehl wird mittels des HTTP-Protokolls geschickt (GET Request). 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.). B.). Der Parameter ist nur dann verbindlich, wenn das externe Gerät eine Authentifizierung verlangt.
- **Passwort** – Passwort für die Authentifizierung des Anschlusses an ein externes Gerät (WEB-Relais usw.). B.). Der Parameter ist nur dann verbindlich, wenn das externe Gerät eine Authentifizierung verlangt.

Tipp

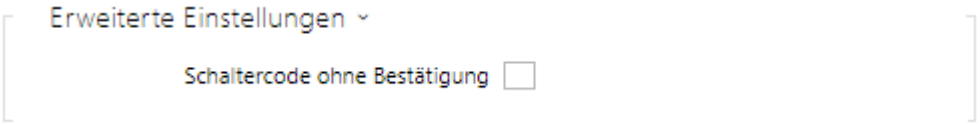
Die HTTP-Befehle geben keine URL-Codierung hinzu. Wenn der Befehl, z.B. http://10.27.24.6/message.cgi?action=9%3A%2F eingegeben wird, dann wird Folgendes abgesendet: http://10.27.24.6/message.cgi?action=9%3A%2F
Wenn der Befehl mit der URL-Codierung abgeschickt werden soll, muss man ihn in dieser Form eingeben, z.B. http://10.27.24.6/message.cgi?action=9%253A%252F, dann wird Folgendes abgesendet: http://10.27.24.6/message.cgi?action=9%253A%252F.

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

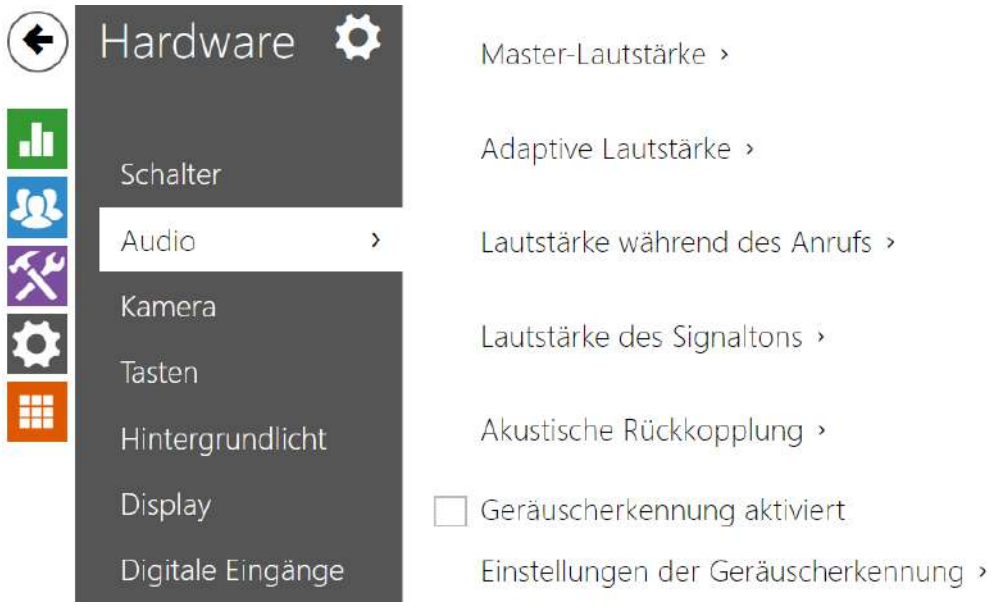


- **Schaltercode ohne Bestätigung** – erlaubt die Aktivierungsmöglichkeit **des ersten Schaltercodes,** der in der Codeliste seitens des Telefons ohne die Bestätigung mit dem Zeichen * angeführt ist. Beim Abhaken wird der erste Code nicht bestätigt. Diese Einstellung betrifft nicht die anderen Codes des Schalters, die in der Liste angeführt sind und die Eingabe des Codes mittels der Tastatur, diese müssen immer mit * bestätigt

werden. Dient der Einstellung der rückwirkenden Kompatibilität mit älteren Interkommodellen der Gesellschaft 2N.

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

5.5.2 Audio

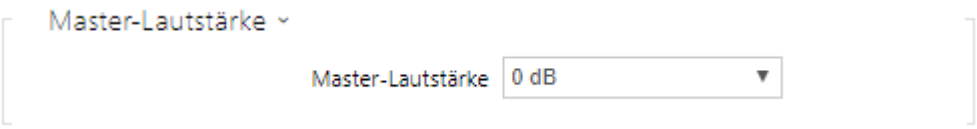


Alle Modelle der 2N IP Interkoms sind mit einem Lautsprecher bzw. mit dem Ausgang eines Leistungsverstärkers ausgestattet, an den man einen externen Lautsprecher anschließen kann. In diesem Teil der Konfiguration werden die Lautstärke der Telefonanrufe und die Lautstärke der Signalisierung verschiedener Betriebszustände der Anlage eingestellt. Der Parameter **Gesamtlautstärke** steuert die Gesamtlautstärke der Anlage und beeinflusst nicht nur die Lautstärke des Anrufs, sondern auch die Lautstärke der Signalisierungstöne u.Ä. Stellen sie diesen Parameter gemäß der Lärmintensität der Umgebung ein, in der das Interkom benutzt wird. Falls die Lärmintensität der Umgebung nicht konstant ist, kann man den adaptiven Modus nutzen, der es ermöglicht die Gesamtlautstärke zeitweilig gemäß dem aktuellen Niveau des umgebenden Lärms zu erhöhen.

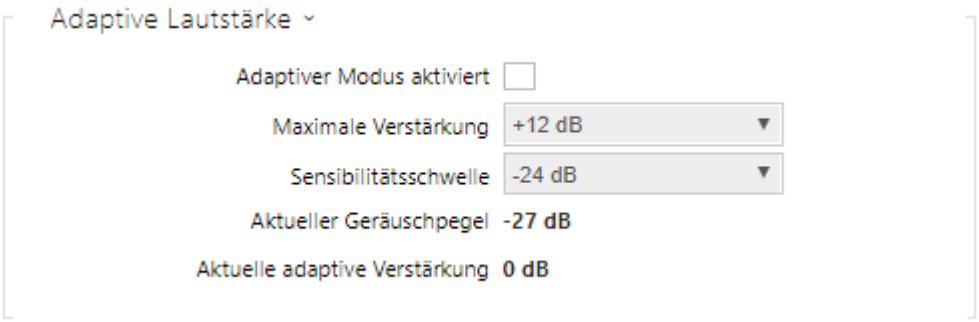
Modell	Gesamtlautstärke
IP Style	−12 dB .. +8 dB (2 x 4 W)
IP Vario	−10 db .. +0 dB (150 mW)
Force/Safety 1W	−12 dB .. +6 dB (1 W)
Force/Safety 10W	−12 dB .. +20 dB (10 W)
IP Uni	−12 dB .. +6 dB (1 W)

Modell	Gesamtlautstärke
IP Verso	−8 dB .. +8 dB (2 W)
IP Solo	−8 dB .. +4 dB (2 W)
IP Base	−8 dB .. +8 dB (2 W)
Audio/Video Kit	−10 dB .. +10 dB
SIP Speaker	−10 dB .. +10 dB
SIP Speaker Horn	−16 dB .. +16 dB

Parameterliste

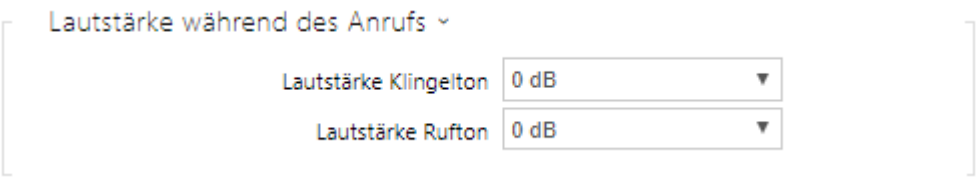


- **Master-Lautstärke** – stellt die Gesamtlautstärke der Anlage ein. Diese Einstellung betrifft die Lautstärke der Telefonanrufe sowie aller Signaltöne.



- **Adaptiver Modus aktiviert** – schaltet den Adaptiv-Modus der Lautstärkesteuerung ein, in dem die Lautstärke des Lautsprechers automatisch gemäß der Lärmintensität der Umgebung eingestellt wird, in der das Interkom installiert ist.
- **Maximale Verstärkung** – die maximale Verstärkung, die man im Adaptiv-Modus auf die Gesamtlautstärke anwenden kann.

- **Sensibilitätsschwelle** – die Schwelle des umgebenden Lärms, bei der es zur Anwendung der Adaptivverstärkung kommt.
- **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 Klingelton** – stellt die Lautstärke der Signalisierung des eingehenden Anrufs ein.
- **Lautstärke Ruftöne** – stellt die Lautstärke des Wähltons, des Klingeltons und des Besetztzeichen ein. Wenn die Ruftöne automatisch von der Telefonzentrale generiert werden, wird diese Einstellung nicht genutzt.

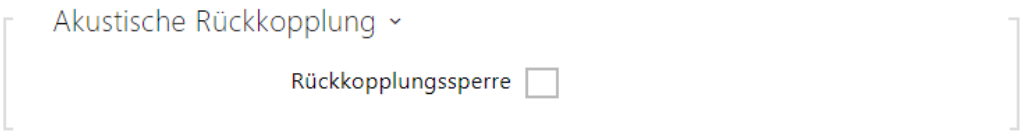
- **Lautstärke Tastenton** – stellt die Lautstärke des Pieptons ein, der beim Drücken der Taste generiert wird. Die Werte der Lautstärke sind gegenüber der eingestellten Gesamtlautstärke relativ.
- **Laustärke Warnsignal** – stellt die Lautstärke der Warn- und Signalisierungstöne ein, die im Kapitel Signalisierung des Betriebsstatus beschrieben sind. Die Werte der Lautstärke sind gegenüber der eingestellten Gesamtlautstärke relativ.
- **Lautstärke Schalteraktivierung** – stellt die Lautstärke des Tons ein, der bei der Schalteraktivierung generiert wird. Die Werte der Lautstärke sind gegenüber der eingestellten Gesamtlautstärke relativ.

- **Lautstärke der benutzerdefinierten Tönen** – stellt die Lautstärke der abgespielten Nutzertöne ein. Die Werte der Lautstärke sind gegenüber der eingestellten Gesamtlautstärke relativ.

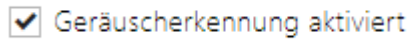
- **Ausgangsaudioeingang** – ermöglicht den Audioeingang (Mikrophon. Linieneingang oder Eingang des Audiomoduls) einzustellen, der für Telefonanrufe und das Audiostreaming verwendet wird.
- **Verstärkung des Mikrofoneingangs** – ermöglicht die Verstärkung des Mikrofoneingangs einzustellen.
- **Verstärkung des Linieneingangs** – ermöglicht die Verstärkung des Linieneingangs unabhängig von der Einstellung der Mikrofonverstärkung einzustellen.

Tipp

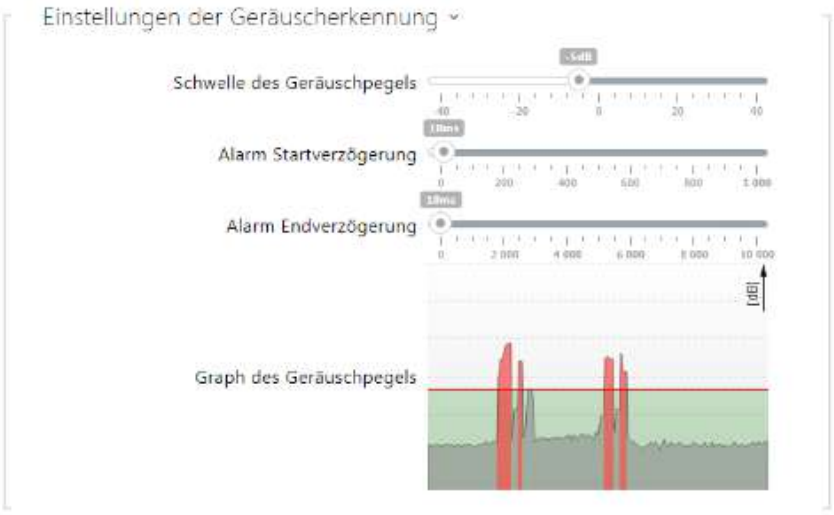
Die Mikrofonverstärkung kann man nur bei den Modellen **2N® SIP Speaker Horn**, **2N® IP Audio Kit** und **2N® IP Video Kit** einstellen.
Die Einstellung des Mikrofoneingangs (ggf. des Linieneingangs) hängt mit dem Niveau des Eingangssignals und der Art der externen Mikrofoninstallation zusammen. Der breite Umfang der Verstärkungseinstellung (0 bis 39 dB beim Mikrofoneingang und −6 dB bis 24 dB beim Linieneingang) sollte für die meisten Installationen ausreichend sein. Die Verstärkung sollte so eingestellt sein, das ausreichende Hörbarkeit gewährleistet wird, und gleichzeitig so, dass es bei höherer Lautstärke zu keiner übermäßigen akustischen Rückkopplung und der nachfolgenden Sättigung (bzw. Linieneingang) kommt, die die Verschlechterung der Echounterdrückungsfunktion (AEC) verursachen kann.



- **Rückkopplungssperre** – stellt den Modus der automatischen Unterdrückung der akustischen Rückkopplung (gewöhnlich Pfeifen) zwischen dem Interkomlautsprecher und dem Hörer des Telefongerät ein, wenn es in der unmittelbaren Nähe des Interkoms angebracht ist. Dieser Modus ist implizit ausgeschaltet.



- **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.

5.5.3 Kamera

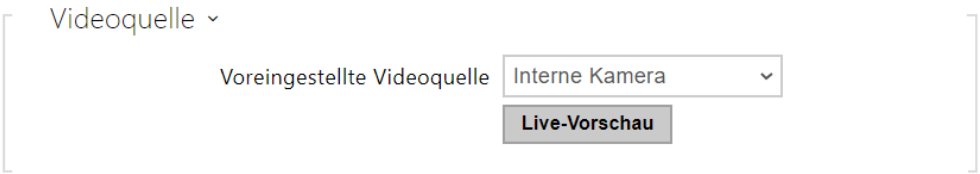
Dieses Menü ist nur bei den **Interkoms 2N IP**, verfügbar, die mit einer internen Kamera ausgestattet sind oder den Anschluss einer externen Kamera ermöglichen. Das Signal aus der Kamera kann man direkt in den Anruf auf Videotelefon streamen, mittels E-Mails abschicken, mittels des ONVIF/RTSP-Protokolls auf ein anderes Gerät (z.B. Video Surveilance) streamen oder einfach vom Interkom als JPEG-Aufnahmen mittels des HTTP-Protokolls herunterladen.

Als Signalquelle kann angewendet werden:

- interne integrierte Kamera oder externe Analogkamera (nur **2N® IP Video Kit**)
- 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).

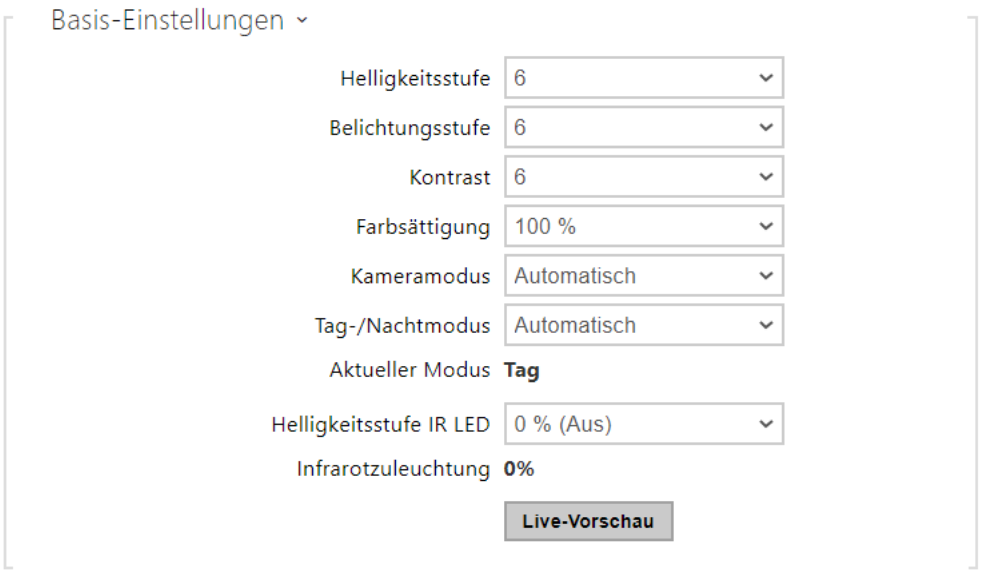
Im Menü Kamera werden die Parameter der Kamera wie Helligkeit, Farbsättigung ggf. Anmeldeangaben für die externe IP-Kamera eingestellt. Parameter, die mit Videoanrufen und mit dem Videostreaming zusammenhängen, befinden sich im Menü **Dienste / Telefon**, **Dienste / Streaming** und **Dienste / E-Mail**.

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, und zwar auch dann, wenn die Anlage keine interne Kamera hat und nur eine externe angeschlossen ist. Wenn an das Interkom keine interne Kamera angeschlossen ist, kann man als die Ausgangsvideoquelle nur die externe IP-Kamera 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 Live-Vorschau von 2N IP-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. Der Parameter ist nur beim Modell **2N® IP Style** verfügbar.
- **Farbsättigung** – stellt die Sättigkeit/Farbensaturation des Kamerabildes ein.
- **Kameramodus** – ermöglicht verschiedene Modi der Bildabtastung gemäß der aktuellen Interkominstallation (Innen-und Außenanwendung). Bei Innenanwendung kann man verschiedene Modi der durch Kunstlichtquellen verursachten Flimmerunterdrückung wählen. Bei Außeninstallierungen kann man den Modus der Unterdrückung der Sonneneinstrahlung einstellen.
- **Automatische Herabsetzung der Aufnahmefrequenz** – erlaubt das automatische Herabsetzen der Aufnahmefrequenz bei verschlechterten Lichtbedingungen, wodurch es zur Verbesserung der Bildqualität zu Lasten der Aufnahmefrequenz kommt.

- **Bildzuschneiden** – Der Beobachtungswinkel der Kamera des Interkoms **2N® IP Force** ist so eingestellt, dass die Kamera einen möglichst großen Bereich erfasst. Dieser Paramater ermöglicht das automatische Bildzuschneiden der Kamera so einzustellen, dass in der Einstellung der Rahmen der Anlage nicht erscheint, was in manchen Fällen störend wirken kann. Deaktivieren Sie diese Funktion, um den bestmöglichen Blickwinkel zu erreichen. Der Parameter ist nur beim Modell **2N® IP Force** verfügbar.
- **Tag-/Nachtmodus** – stellt die Art des Tages- und Nachtmodus der Kamera ein. Die Optionen sind automatisch (gesteuert durch die Helligkeit im Raum) oder permanent auf den Tages-/Nachtmodus eingestellt.
- **Aktueller Modus** – zeigt den aktuell gewählten Kameramodus (Tag/Nacht) an. Die Kamera benutzt im Tagesmodus ein Filter für die Deaktivierung der Infrarotstrahung und die IR-Zuleuchtung ist ausgeschaltet. Im Nachtmodus. Im Nachtmodus sind der Filter für die Deaktivierung der Infrarotstrahlung ausgeschaltet und die IR-Zuleuchtung eingeschaltet.
- **Helligkeitsstufe IR LED** – ermöglicht das Niveau der Infrarotzuleuchtung im Umfang 0–100 % in mehreren Schritten einzustellen. Die Infrarotzuleuchtung ist im Nachtmodus automatisch eingeschaltet. Die Einstellung des Zuleuchtungsniveau ist nur bei dem Modell **2N® IP Style,2N® IP Verso** und **2N® IP Force** mit HD-Kamera verfügbar.
- **Aktuelles Helligkeitsstufe IR LED** – zeigt das aktuelle Niveau der Infrarotzuleuchtung in % des Maximums an. Das Niveau kann automatisch unter den eingestellten Wert so gesenkt werden, dass es nicht zur Überschreitung der maximalen möglichen Leistungsabnahme aus der Einspeisungsquelle kommt (gewöhnlich beim Anschluss einer größeren Zahl der erweiternden Module und der Einspeisung mittels PoE).
- **Live-Vorschau** – zeigt ein Fenster mit Live-Vorschau von 2N IP-Kamera an.

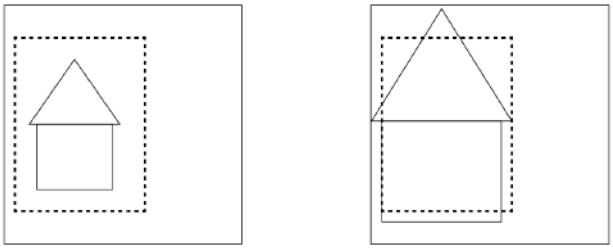
Die Funktionsgruppe Erweiterte Einstellungen gilt für die Modelle 2N IP der Sprechanlage **2N® IP Style**.

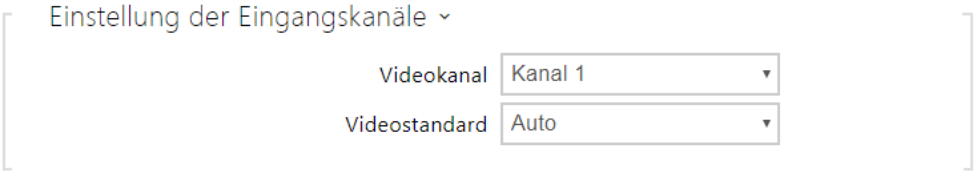
- **Bildkorrektur** – legt die digitale Korrektur (Ausrichtung) des internen Kamerabilds des Geräts fest.
- **Benutzerdefiniertes Zuschneiden von Bildern** – legt den standardmäßigen Mittelzuschnitt des Bildes fest (die Kanten werden gleichmäßig abgeschnitten).
- **Weißabgleich** – das Einstellen eines 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.





Anmerkung

- *Diese Einstellung ist nur bei Modellen verfügbar, die mit Eingängen für die externe Analogkamera ausgestattet sind.*

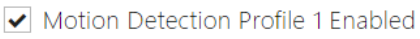
- **Video-Eingang** – ermöglicht einen der zwei Eingänge für den Anschluss einer Analogkamera zu wählen. Sie können den Eingang während des Betriebs auch mittels der Automatisierung über Action.SetCameraInput ändern.
- **Videostandard** – ermöglicht den Videostandard der angeschlossenen Kamera einzustellen. Ändern Sie den Parameterwert nur dann, wenn die automatische Erkennung des Videostandards (der Wert Auto) nicht richtig funktioniert.

- **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.

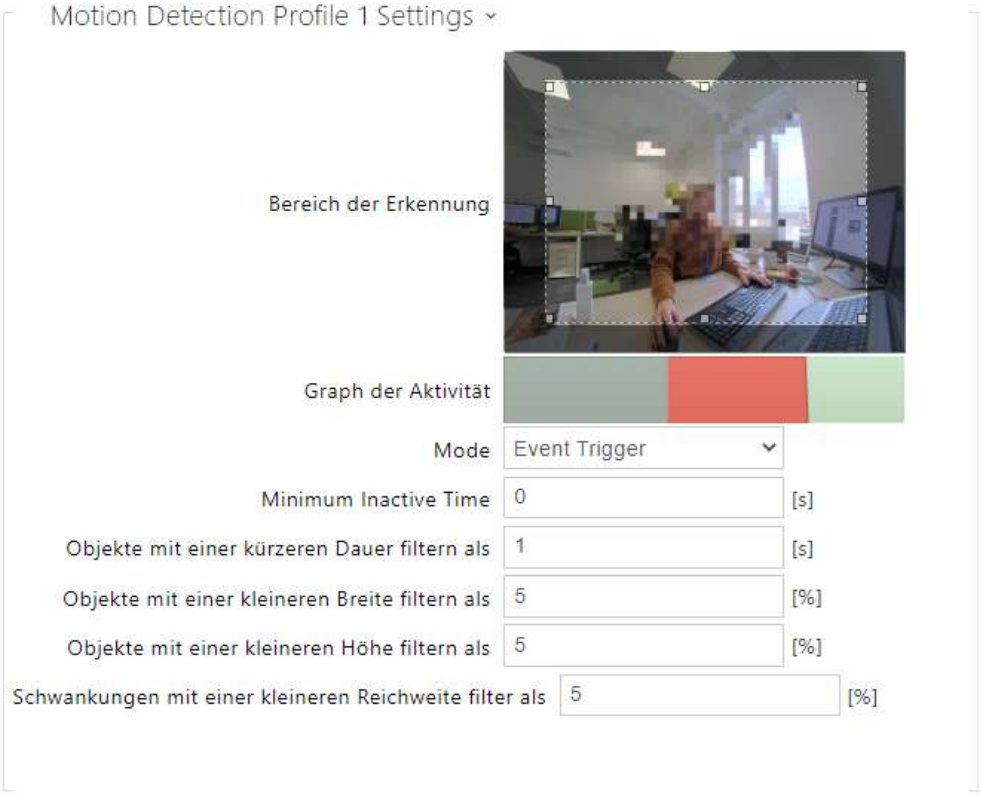
- **Empfindlichkeitsschwelle** – ermöglicht die untere und die obere Empfindlichkeitsschwelle und die Algorithmushysterese der Bewegungserkennung einzustellen.
- **Erkennungsbereich** – ermöglicht den Rechteckausschnitt des Bildes einzustellen, in dem die Bewegungserkennung durchgeführt wird.
- **Aktivitätsdiagramm** – 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 und Schutz der Privatsphäre für Geräte mit ARTPEC-7 Prozessor



- **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.

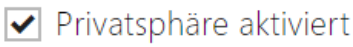


- **Bereich der Erkennung** – ermöglicht den Rechteckausschnitt des Bildes einzustellen, in dem die Bewegungserkennung durchgeführt wird.
- **Graph der Aktivität** – zeigt den Verlauf der erkannten Aktivität auf der Zeitachse an. Grün bedeutet keine Bewegung, grau bedeutet eine erkannte Bewegung, die 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“).



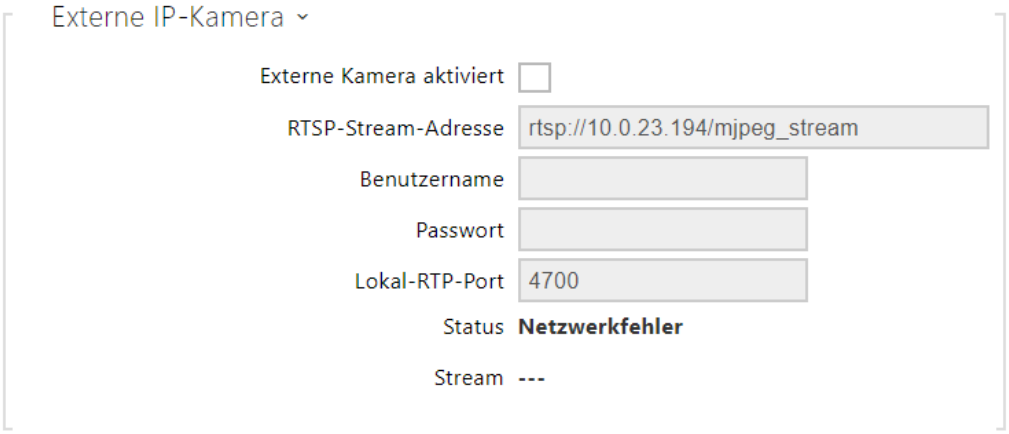
- **Privatsphäre aktiviert** – Aktiviert die Datenschutzfunktion, die einen Teil des Bildes mit der ausgewählten Farbe oder dem ausgewählten Mosaik maskiert.

- **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



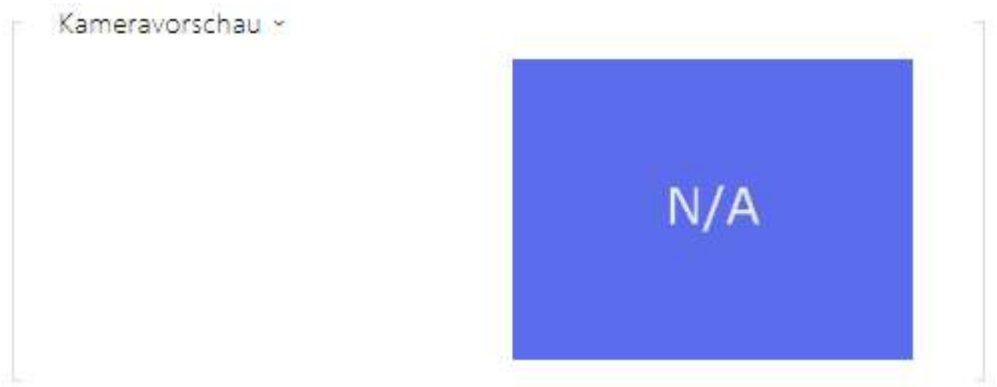
- **Externe Kamera aktiviert** – erlaubt das Herunterladen des RTSP-Streams von der externen IP-Kamera. Geben Sie die gültige RTSP-Stream-Adresse bzw. den Benutzernamen und das Passwort ein, damit die Funktion korrekt ausgewählt wird.
- **RTSP-Stream-Adresse** – die die RTSP-Stream-Adresse der IP-Kamer 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.
- **Lokal-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.

5.5.4 Tastatur

Dieser Teil der Konfiguration dient der Funktionseinstellung der nummerischen Tastatur und der Kurzwahltasten. Die **Interkoms 2N IP** ermöglichen:

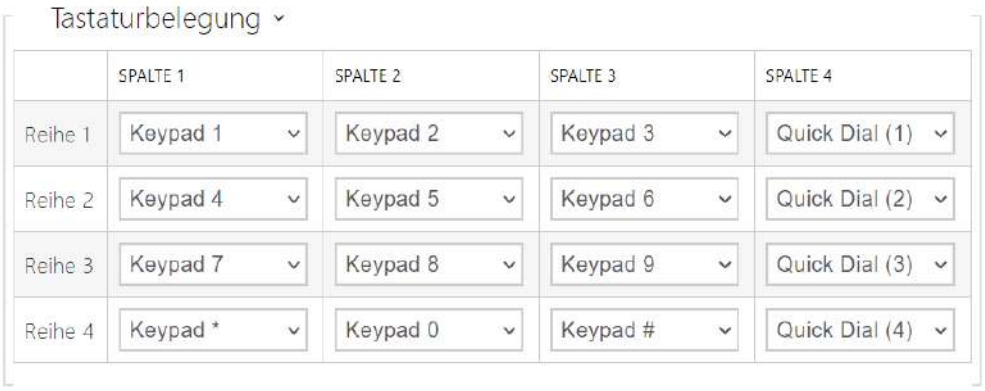
- verwenden des numerischen Tastenfelds, um anzurufen, indem die virtuelle Nummer des Benutzers eingegeben wird,
- die nummerische Tastatur für die Eingabe des Zutrittscodes, z.B. für die Entriegelung des Türschlosses zu verwenden,
- die Funktion der Taste # einzustellen,
- das Zeitlimit bei der Eingabe der Codes und der Telefonnummern einzustellen
- die Funktion der Knöpfe und der Tasten zu wählen, die an das **2N® IP Audio/Video Kit** angeschlossen sind.

Tastaturbelegung

Die Interkommodelle **2N® IP Audio Kit** und **2N® IP Video Kit** sind mit acht Klemmen für den Anschluss von externen Tasten oder einer externen Tastatur ausgestattet und ermöglichen den Anschluss von bis zu 16 Tasten. Man kann die Funktion jeder Taste unabhängig einstellen.

Die Tasten sind in eine Matritze mit 4 Spalten x 4 Zeilen organisiert und dem entspricht auch ihre Einstellung.

Die Voreinstellung der Tasten ist auf folgendem Bild angeführt.



Sie können jeder Position der Matrize eine der Funktionen – Taste der nummerischen Tastatur 0 bis 9, *, # oder eine der Kurzwahltasten 1–16 zuordnen.

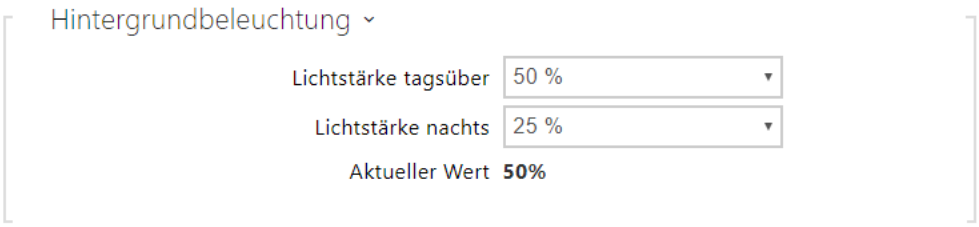
5.5.5 Hintergrundlicht

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

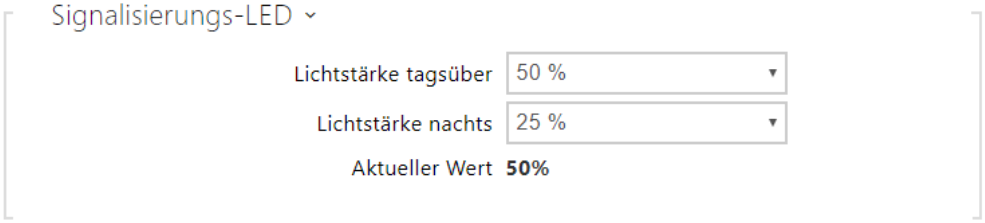
Falls das Interkom mit einem Sensor des Niveaus des umgebenden Lichts ausgestattet ist, wird es automatisch das geeignete Niveau der Unterbeleuchtung im Umfang der eingestellten Werte wählen. Ausgewählte Interkoms ermöglichen es das Niveau der Unterbeleuchtung der Namenschilder (Tasten) und der Signalisierungs-LED (z.B. unterbeleuchtete Piktogramme) unabhängig zu steuern. Siehe nachstehende Tabellen:

Eigenschaft/ Modell	2N® IP Style	2N® IP Verso / LTE Verso	2N® IP Solo	2N® IP Base	2N® IP Vario	2N® IP Force	2N® IP Safety	2N® IP Uni	2N® IP Audio Kit	2N® IP Video Kit
Steuerung des Unterbeleuchtungsniveaus	**Ja**			**Ja**	**Ja**				Nein	
Sensor des Niveaus des umgebenden Lichts	**Ja**			Nein	Nein				Nein	

Eigenschaft/ Modell	2N® IP Style	2N® IP Verso / LTE Verso	2N® IP Solo	2N® IP Base	2N® IP Vario	2N® IP Force	2N® IP Safety	2N® IP Uni	2N® IP Audio Kit	2N® IP Video Kit
Unabhängige Steuerung des Unterbeleuchtungsniveaus der Namensschilder und der Signalisierungs-LED	**Ja**			**Ja**	Nein				Nein	



Die Parametereinstellungen in der Gruppe Hintergrundbeleuchtung gelten für die Hintergrundbeleuchtung der Haupteinheit, der Tasten und der Zusatzmodule.



- **Lichtstärke tagsübe** – stellt den Wert der Unterbeleuchtungsintensität am Tag ein. Der Wert wird in Prozenten der höchstmöglichen LED-Helligkeit angegeben.
- **Lichtstärke nachts** – stellt den Helligkeitswert der LED in der Nacht ein. Der Wert wird in Prozenten der höchstmöglichen LED-Helligkeit angegeben. Falls die Parameter Intensität am Tag und Intensität in der Nacht auf den gleichen Wert eingestellt sind, wird das Niveau des umgebenden Lichts nicht berücksichtigt.
- **Aktueller Wert** – zeigt den aktuell automatisch gewählten Wert der LED-Intensität gemäß dem aktuell erkannten Niveau des umgebenden Lichts an.

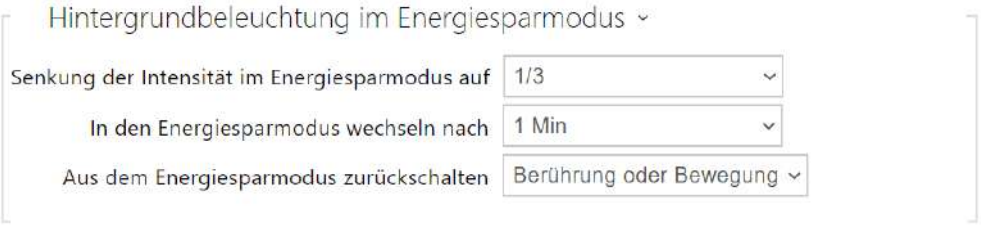
Anmerkung

- Die Einstellung der Helligkeitsintensität 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 dem Interkom steht, und erhöht gleichzeitig generell den Verbrauch der Anlage. Niedrige Helligkeit der Signalisierungs-LED führt bei der Verwendung des Interkoms in der direkten Sonne zur Herabsetzung des Kontrastes zwischen der ausgeschalteten und eingeschalteten LED und zur schwierigen Erkennung des LED-Status.

Einstellung der Display-Hintergrundbeleuchtung der Sprechanlage 2N® IP Style

Die Parametereinstellungen in den Gruppen Hintergrundbeleuchtung und Hintergrundbeleuchtung im Energiesparmodus gelten für die Display-Hintergrundbeleuchtung und die Umgebungs-LED.

- **Intensität im aktiven Modus während des Tages** – legt den Maximalwert der Helligkeit der Hintergrundbeleuchtung während des Tages fest (der Wert wird vom Umgebungslichtsensor gesteuert). Der Wert wird als Prozentsatz der maximal möglichen Helligkeit angegeben.
- **Intensität im aktiven Modus bei Nacht** – legt den Maximalwert der Helligkeit der Hintergrundbeleuchtung bei Nacht fest (der Wert wird vom Umgebungslichtsensor gesteuert). Der Wert wird als Prozentsatz der maximal möglichen Helligkeit angegeben.
- **Aktueller Wert** – zeigt den aktuell automatisch ausgewählten Wert der Hintergrundbeleuchtungsintensität entsprechend der aktuell erfassten Umgebungslichtstärke an.



- **Senkung der Intensität im Energiesparmodus auf** – schwächungsgrad der Hinterleuchtung, wenn das Gerät in Inaktivmodus übergeht.
- **In den Energiesparmodus wechseln nach** – legt fest, wie lange das Gerät inaktiv ist (d.h. wie lange das Gerät nicht interagiert). Danach wechselt es automatisch in den Energiesparmodus. Der Wert wird in Sekunden zwischen 1 und 600 angegeben.
- **Aus dem Energiesparmodus zurückschalten** – **l**egt die Interaktionsmodi fest, mit denen der Energiesparmodus unterbrochen werden kann. Sie können zwischen Berühren des Bildschirms und Berühren oder Bewegungserkennung wählen. Darüber hinaus wechselt das Gerät während der Benutzerauthentifizierung, des eingehenden Anrufs und anderer Betriebszustände immer aus dem Energiesparmodus.

Die Parametereinstellungen in der Gruppe Signalisierungs-LEDs gelten für Signalisierungs-LEDs (Hintergrundbeleuchtung des Lesers **2N® IP Style**).

- **Lichtstärke tagsüber** – legt die Helligkeitsstufe der Signal-LED tagsüber fest. Der Wert wird in Prozent der höchstmöglichen LED-Helligkeit angegeben.
- **Lichtstärke nachts** – legt die Helligkeitsstufe der Signal-LED nachts fest. Der Wert wird in Prozent der höchstmöglichen LED-Helligkeit angegeben. Falls die Parameter Intensität am Tag und Intensität in der Nacht auf den gleichen Wert eingestellt sind, wird das Niveau des umgebenden Lichts nicht berücksichtigt.
- **Aktueller Wert** – zeigt den aktuell automatisch ausgewählten Wert der Hintergrundbeleuchtungsintensität entsprechend der aktuell erfassten Umgebungslichtstärke an.

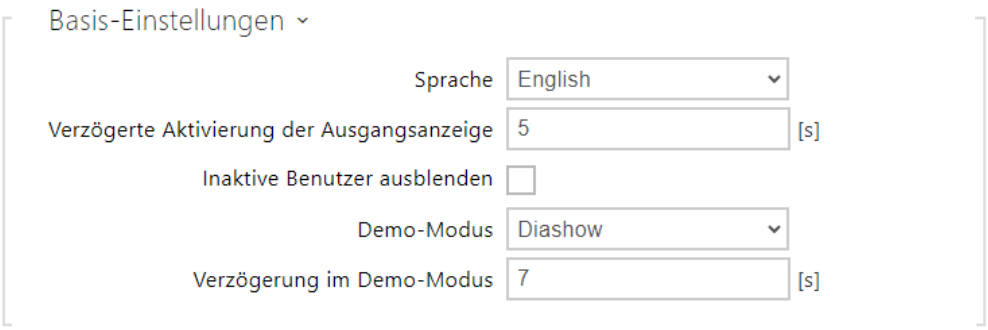
5.5.6 Display

Manche Modelle des Interkoms **2N® IP Vario** bzw. **2N® IP Verso** können mit einem LCD-Farbdisplay ausgestattet sein. Auf dem Display wird der Status der Anlage (z.B. Anrufverlauf, Türöffnen) angezeigt und das Display kann gleichzeitig in mehreren Modi arbeiten:

Display – erlaubt im Fall von **2N® IP Vario** die Funktion des Displays und der Spracheinstellung. Bei **2N® IP Verso** ermöglich die Grund- und die Spracheinstellung.

Präsentation – nach eingestellter Untätigkeitsdauer kann eine Präsentation in der Form von aufgenommenen Bildern angezeigt werden. Zwischen den einzelnen Bildern wird automatisch umgeschaltet und man kann die Dauer des Anzeigens eines Bildes einstellen.

Registerkarte Display (nur Modelle 2N® IP Vario)



- **Sprache** – Stellt die Sprache der auf dem Display angezeigten Texte ein. Es kann eine der vordefinierten Sprachen ausgewählt werden – Englisch, Tschechisch, Deutsch, Italienisch, Französisch, Spanisch, Russisch, Finnisch, Dänisch, Polnisch, Niederländisch, Portugiesisch, Türkisch, Norwegisch, Schwedisch oder eine benutzerdefinierte Sprache (custom).
- **Verzögerung der Präsentationsaktivierung** – stellt die maximale Untätigkeitsdauer des Nutzers ein (d.h. die Zeit, während der der Nutzer die Anlage nicht mittels der Tasten oder der nummerischen Tastatur bedient), nach der es zum automatischen Umschalten in den Präsentationsmodus kommt. Andernfalls wird das Default-Fenster mit dem Logo 2N angezeigt.
- **Inaktive Benutzer ausblenden** – wenn diese Option aktiviert ist, wird der Benutzer, der ein aktives Zeitprofil hat und nicht kontaktiert werden kann, automatisch ausgeblendet.
- **Demo-Modus** – legt fest, ob das Gerät im Leerlauf in den Demo-Modus wechselt. Im Demo-Modus kann ein anderes Verhalten gewählt werden (Deaktiviert, Diashow).
- **Aktivierungsverzögerung des Demo-Modus** – stellt das Zeitintervall von 1 bis 600 Sekunden ein, nach dem das Gerät in den Demomodus übergeht. Es gibt immer eine feste Zeitspanne von 15 Sekunden, vor deren Ablauf das Gerät zur Startseite zurückkehrt.

- **Originalsprache** – ermöglicht die Schablone der Lokalisierungsdatei für eine 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.
- **Nutzerfonts** – ermöglicht eigene Fonts für die auf dem Display angezeigten Texte hochzuladen, zu löschen und herunterzuladen. Die Datei muss im Format TTF sein und sie darf nicht größer als 4 MB sein.

Anmerkung

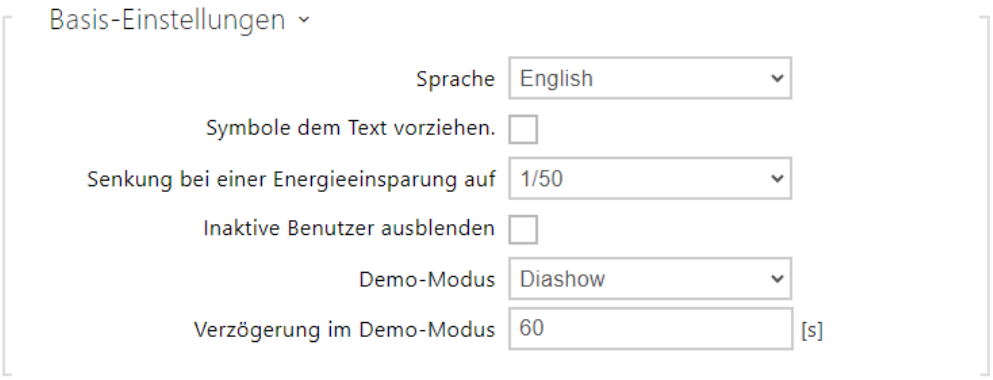
Wenn Ihnen keine der vordefinierten Sprachen des Displays zusagt, gehen Sie wie folgt vor:

- 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 Interkom hoch,
- stellen Sie den Parameter **Spracheinstellung | Sprache** auf den Wert **eigene** ein,
- kontrollieren Sie die Texte direkt auf dem Interkomdisplay und ändern Sie sie gegebenenfalls.

Falls Ihnen das graphische Aussehen der Namenschilder nicht gefällt, können Sie in das Interkom einen eigenen Hintergrund der Namensschilder hochladen. Das Bild muss die Auflösung 320 x 240 Pixel haben. Wenn Sie in das Interkom ein eigenes Bild des Namensschildes hochladen, wird das ursprüngliche Aussehen der Namensschilder ersetzt, die Zuordnung der Nutzer zu den einzelnen Tasten bleibt jedoch aufrecht.

Registerkarte Display (nur Modelle 2N® IP Verso)

- **Tastaturtaste für die Eingabe des Codes** – schaltet die Bildschirmtastatur zur Eingabe von Zahlencodes ein.
- **Tastaturmodus zur Eingabe des Codes** – legt den Bildschirmtastaturmodus für die Eingabe von Zahlencodes fest. Modi sind normale Tastaturen oder Tastaturen mit gemischten Tasten für zusätzliche Sicherheit. Die Einstellungen gelten auch für die Tastatur während der Mehrfachauthentifizierung.



- **Sprache** – stellt die Sprache der Texte ein, die auf dem Display angezeigt werden. Es kann eine der vordefinierten Sprachen ausgewählt werden – Englisch, Tschechisch, Deutsch, Italienisch, Französisch, Spanisch, Russisch, Finnisch, Dänisch, Polnisch, Niederländisch, Portugiesisch, Türkisch, Norwegisch, Schwedisch oder eine benutzerdefinierte Sprache (custom).
- **Symbole dem Text vorziehen** – die Symbole auf dem Display werden vor dem Text positioniert.
- **Senkung bei einer Energieeinsparung auf** – 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 Interkomkamera oder bei einem beliebigen Ereignis auf dem Display (z.B. Aktivierung des Türschlosses oder Berührung des Displays) wird das Display in volle Helligkeit übergehen.
- **Inaktive Benutzer ausblenden** – wenn diese Option aktiviert ist, wird der Benutzer, der ein aktives Zeitprofil hat und nicht kontaktiert werden kann, automatisch ausgeblendet.

- **Demo-Modus** – legt fest, ob das Gerät im Leerlauf in den Demo-Modus wechselt. Im Demo-Modus kann ein anderes Verhalten gewählt werden (Deaktiviert, Diashow).
- **Verzögerung im Demo-Modus** – stellt das Zeitintervall von 1 bis 600 Sekunden ein, nach dem das Gerät in den Demomodus übergeht. Es gibt immer eine feste Zeitspanne von 15 Sekunden, vor deren Ablauf das Gerät zur Startseite zurückkehrt.

- **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.

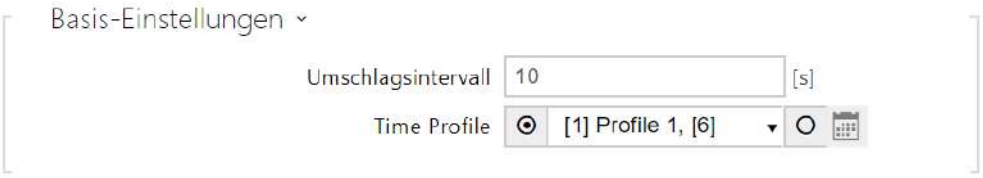
Anmerkung

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

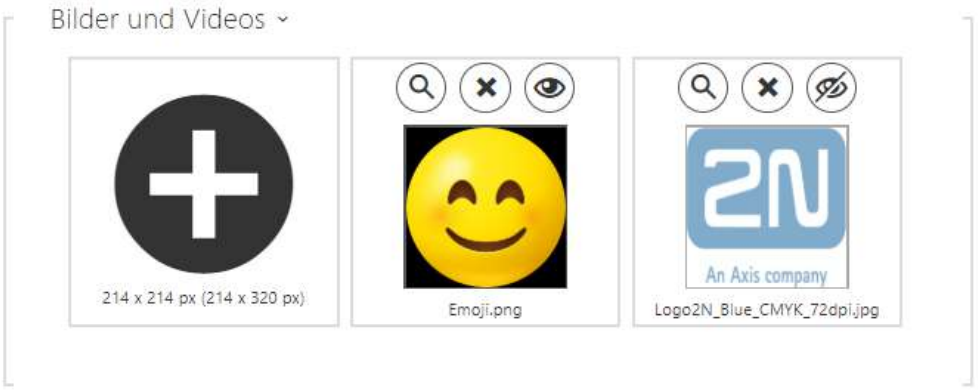
- laden sie die originale Sprachdatei herunter (sie ist in Englisch),
- passen Sie die Datei mithilfe des Texteditors an (ersetzen Sie die englischen Texte durch eigene),
- laden Sie die angepasste Lokalisierungsdatei zurück in das Interkom hoch,
- stellen Sie den Parameter **Spracheinstellung / Sprache**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

Registerkarte Diashow Modelle 2N® IP Verso

Auf dieser Registerkarte wird die Liste der im Präsentationsmodus angezeigten Bilder und Videos eingestellt. Es können bis zu 8 Bilder/Videos hochgeladen werden, die schrittweise mit einer eingestellten Verzögerung umgeschaltet werden.



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



Die Auflösung hochgeladener Bilder/Videos sollte 214 x 214 oder 214 x 320 Pixel bis zu einer maximalen Größe von 2 MB betragen.
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. Die Anzeige kann durch Klicken auf das variable Symbol des Bildes oder Videos vom Zeitprofil abhängig gemacht werden. Wenn das Zeitprofil nicht aktiv ist, wird die Präsentation den Inhalt, der vom Zeitprofil abhängig ist, nicht enthalten. Die Präsentation wird im gleichen Fall immer

den Inhalt enthalten, der nicht vom Zeitprofil abhängig ist. Wenn kein Bild hochgeladen wurde, wird der Modus Präsentation nicht aktiviert.

Tipp

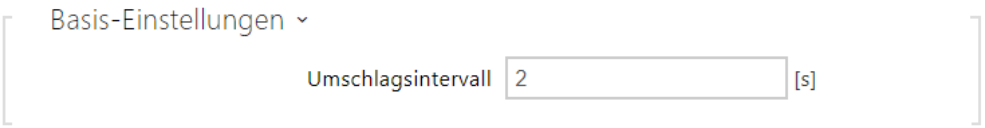
- Um den angezeigten Teil "Mit Berührung beginnen" auf dem Display des Modells **2N® IP Verso** zu verbergen, ist ein Bild mit einer Auflösung von 214 x 320 px hochzuladen.

Hinweis

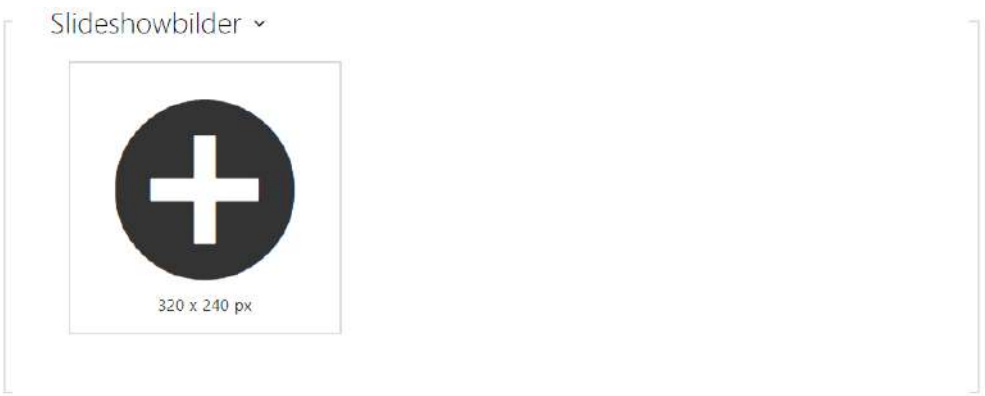
- FW-Versionen unter 2.35 können keine Videos mit einer Auflösung von 214 x 320 hochladen.

Registerkarte Diashow Modelle 2N® IP Vario)

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 Auflösung hochgeladener Bilder sollte 320 x 240 Pixel betragen. 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.

Hinweis

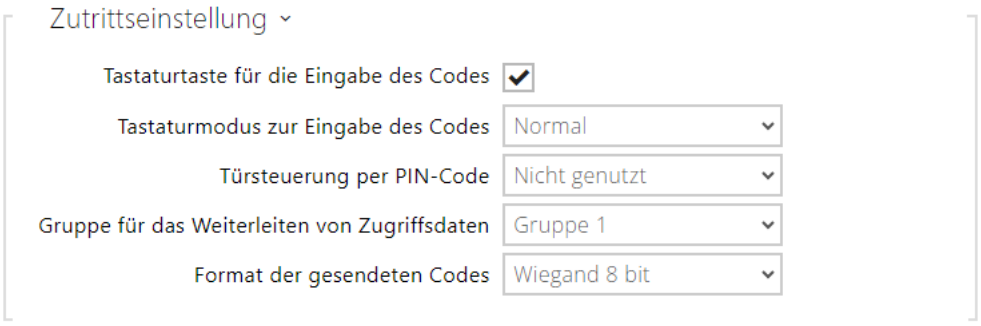
- **2N® IP Vario** unterstützt nur die Bildanzeige.

5.5.6.1 Display 2N® IP Style

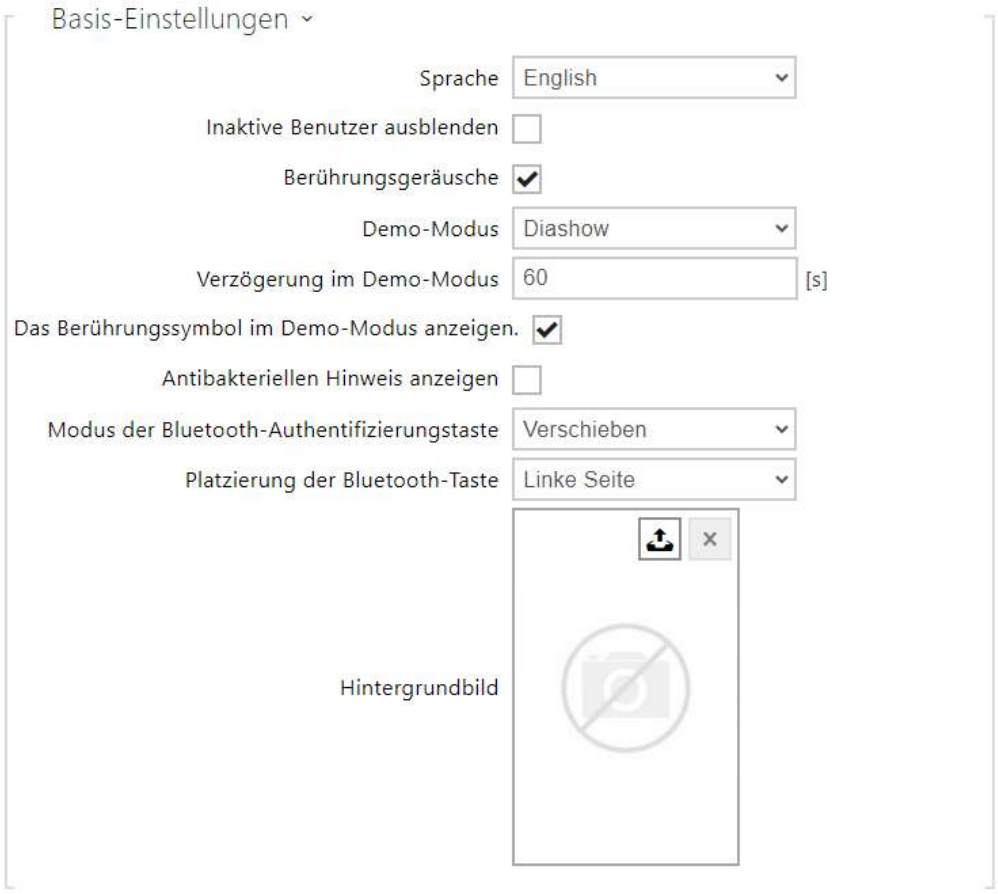
2N IP-Sprechanlage **2N® IP Style** ist mit einem 10″ Farb-LCD-Display mit einer Auflösung von 800 x 1280 ausgestattet. Auf dem Display wird der Status der Anlage (z.B. Anrufverlauf, Türöffnen) angezeigt und das Display kann gleichzeitig in mehreren Modi arbeiten:

- **Display** – zeigt ein Adressbuch mit anrufbaren Benutzern und eine Zifferntastatur für den Codezugriff.
- **Diashow** – nach einer bestimmten Zeit der Inaktivität kann eine Slideshow 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.
- **Logo** – nach einer bestimmten Zeit der Inaktivität kann das in die Gerätekonfiguration hochgeladene Logo auf dem Display erscheinen.
- **Adresse** – nach einer bestimmten Zeit der Inaktivität kann das Display die Adresse und Hausnummer oder eine andere Ortskennung anzeigen.
- **Datum & Uhrzeit** – ermöglicht die Einstellung von Datum, Uhrzeit und Wetterparametern.
- **Begrüßungsnachricht** – Ermöglicht, die Meldung einzustellen, die nach erfolgreicher Authentifizierung auf dem Display erscheint.

Registerkarte **Display**



- **Tastaturtaste für die Eingabe des Codes** – schaltet die Bildschirmtastatur zur Eingabe von Zahlencodes ein.
- **Tastaturmodus zur Eingabe des Codes** – legt den Bildschirmtastaturmodus für die Eingabe von Zahlencodes fest. Modi sind normale Tastaturen oder Tastaturen mit gemischten Tasten für zusätzliche Sicherheit. Die Einstellungen gelten auch für die Tastatur während der Mehrfachauthentifizierung.
- **Türsteuerung per PIN-Code** – Aktiviert oder deaktiviert die Türsteuerung durch Eingabe eines PIN-Codes über den Bildschirm.
- **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.



- **Sprache** – stellt die Sprache der Texte ein, die auf dem Display angezeigt werden. Es kann eine der vordefinierten Sprachen ausgewählt werden – Englisch, Tschechisch, Deutsch, Italienisch, Französisch, Spanisch, Russisch, Finnisch, Dänisch, Polnisch, Niederländisch, Portugiesisch, Türkisch, Norwegisch, Schwedisch oder eine benutzerdefinierte Sprache (custom).
- **Inaktive Benutzer ausblenden** – wenn diese Option aktiviert ist, wird der Benutzer, der ein aktives Zeitprofil hat und nicht kontaktiert werden kann, automatisch ausgeblendet.
- **Berührungstöne** – aktiviert die akustische Signalisierung von Berührungen auf dem Display.
- **Demo-Modus** – legt fest, ob das Gerät im Leerlauf in den Demo-Modus wechselt. Im Demo-Modus kann ein anderes Verhalten gewählt werden (Deaktiviert, Diashow, Logo, Adresse, Datum & Uhrzeit).
- **Verzögerung im Demo-Modus** – legt die Leerlaufzeit fest, nach der das Gerät in den Demo-Modus wechselt, zwischen 1 bis 600 Sekunden.

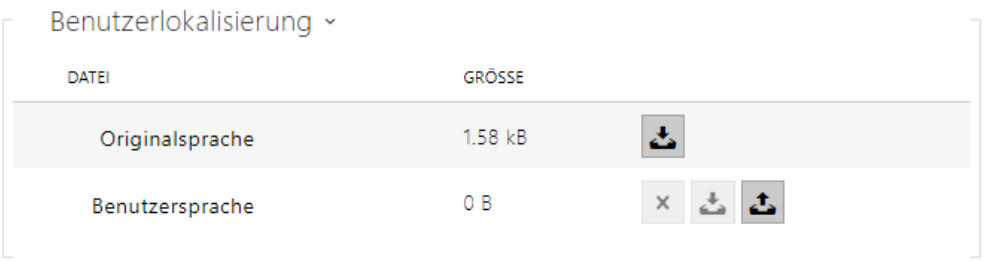
Hinweis

- Das Gerät hat nach 60 Sekunden der Inaktivität eine feste Rückkehr zum anfänglichen Anzeigebildschirm. Nach Ablauf dieser Zeit beginnt die in diesem Parameter eingestellte Zeit herunterzuzählen und das Gerät wechselt dann in den Demonstrationsmodus.
- Nach 2 Minuten Inaktivität wird der Displayschoner des **2N® IP Style** Geräts ausgelöst, bei dem die Helligkeit des Displays in 20-Sekunden-Intervallen abwechselnd verringert und erhöht wird. Der Schoner wird durch eine Berührung des Displays, einen Zugriffsversuch, einen eingehenden Anruf, eine Benachrichtigung auf dem Display oder eine Bewegungserkennung beendet, auch wenn die Bewegungserkennung nicht aktiviert ist. Wenn der Bildschirmschoner im Hintergrund im Vorschaumodus läuft, schaltet das Gerät beim Beenden des Bildschirmschoners durch Berühren auch auf die Startseite um.

- **Das Berührungssymbol im Demo-Modus erlauben** – erlaubt die Anzeige des Berührungssymbols (pulsierende Hand) im Demo-Modus.
- **Antibakteriellen Hinweis anzeigen** – erlaubt das Anzeigen der Information über die antibakterielle Schicht auf dem Display (optionales Zubehör für 2N® IP Style) im Laufe der Zeit, in der das Gerät im Anzeige-Modus ist.
- **Modus der Bluetooth-Authentifizierungstaste** – legt fest, ob die Taste zum Aktivieren der Bluetooth-Authentifizierung durch Verschieben oder Berühren aktiviert wird
- **Platzierung der Bluetooth-Taste** – legt fest, ob die Taste zum Aktivieren der Bluetooth-Authentifizierung durch Ziehen oder Berühren aktiviert wird. Die Einstellungen werden erst wirksam, wenn sich keine Telefone mit der Anwendung Mobile Key in der Nähe des **2N® IP Style** befinden.
  - **Verschieben** – um das Schloss zu schließen, ziehen Sie die Taste von links nach rechts auf dem Display.
  - **Berührung** – drücken Sie die Taste um das Schloss zu schließen.
- **Hintergrundbild** – ermöglicht das Hochladen eines Hintergrundbilds (das in verschiedenen Bildschirmen auf dem Display verwendet wird). Die Datei muss ein Bild mit einer Auflösung von mindestens 800 x 1280 Pixel sein. Bilder mit höherer Auflösung werden reduziert.

Hinweis

- Änderungen in der Anzeige des Stammordners werden erst im Display angezeigt, wenn Sie das Such- oder Wählmenü aufrufen.
- Um die Position und den Authentifizierungsmodus der Bluetooth-Taste auf dem Display zu ändern, trennen Sie alle verfügbaren Geräte mit Bluetooth-Authentifizierung oder bewegen Sie sie außerhalb der Reichweite des **2N® IP Style**.



- **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

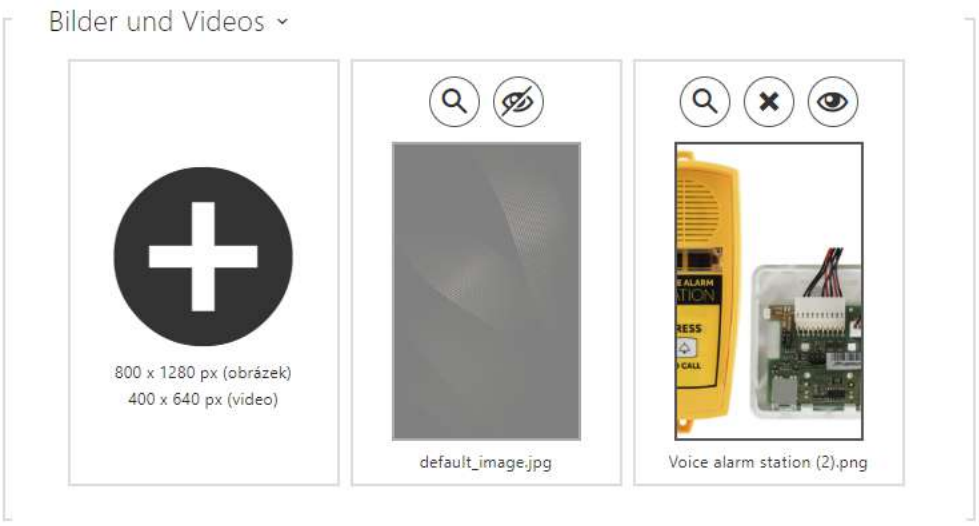
Wenn Ihnen keine der vordefinierten Sprachen des Displays zusagt, gehen Sie wie folgt vor:

- 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 Interkom hoch,
- stellen Sie den Parameter **Spracheinstellung / Sprache** auf den Wert **eigene** ein,
- kontrollieren Sie die Texte direkt auf dem Interkomdisplay und ändern Sie sie gegebenenfalls.

Registerkarte Diashow

In dieser Registerkarte wird die Liste der Bilder eingestellt, die im Modus Präsentation angezeigt werden. Es können bis zu 14 Bilder/Videos hochgeladen werden, die schrittweise mit einer eingestellten Verzögerung umgeschaltet werden.

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



Die Maße der eingespielten Bilder sollten 800 x 1280 Pixel für die Modelle **2N® IP Style** sein. Im anderen Fall werden sie automatisch der Displayauflösung angepasst.

Videodateien müssen eine Auflösung von 400 x 640 px, eine maximale Größe von 7 MB und eine maximale Framerate von 24 fps haben.

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. Die Anzeige kann durch Klicken auf das variable Symbol des Bildes oder Videos vom Zeitprofil abhängig gemacht werden. Wenn das Zeitprofil nicht aktiv ist, wird die Präsentation den Inhalt, der vom Zeitprofil abhängig ist, nicht enthalten. Die Präsentation wird im gleichen Fall immer

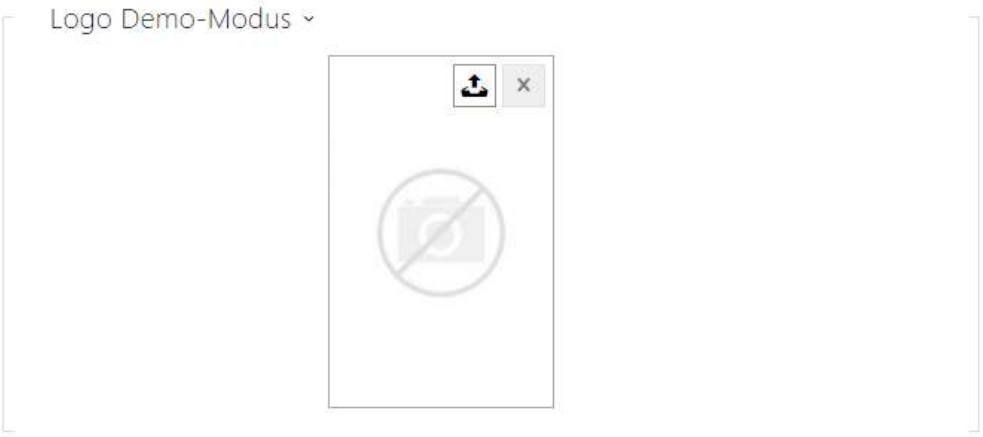
den Inhalt enthalten, der nicht vom Zeitprofil abhängig ist. Wenn kein Bild hochgeladen wurde, wird der Modus Präsentation nicht aktiviert.

Hinweis

- Die „Slideshow“-Vorschau erscheint nur auf dem Display, wenn der angegebene Modus im Menü Hardware / Display / Display aktiviert wird.

Registerkarte Logo

Ermöglicht das Hochladen eines Logos für den Demo-Modus. Ein Bild mit einer Auflösung von mehr als 800 x 1280 Pixel wird verkleinert. Die kleinere Datei bleibt klein und füllt nicht den gesamten Bereich aus. PNG-Bilder mit transparentem Hintergrund werden ebenfalls unterstützt.

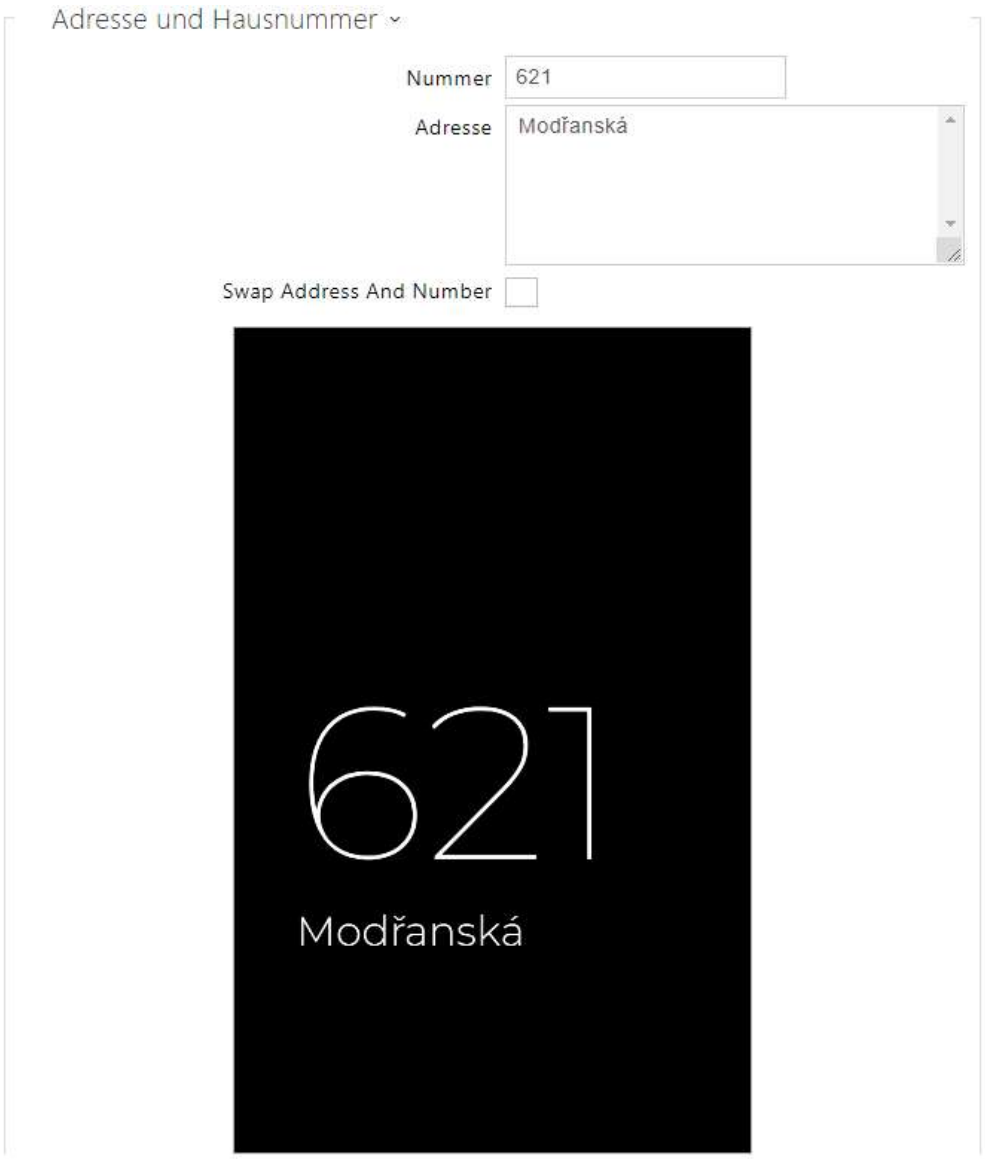


Hinweis

- Die „Logo“-Vorschau erscheint nur auf dem Display, wenn der angegebene Modus im Menü Hardware / Display / Display aktiviert wird.

Registerkarte Adresse

Ermöglicht Ihnen, eine Hausadresse oder eine andere Identifizierung für den Demomodus festzulegen, die auf dem Bildschirm angezeigt wird, wenn das Gerät inaktiv ist.



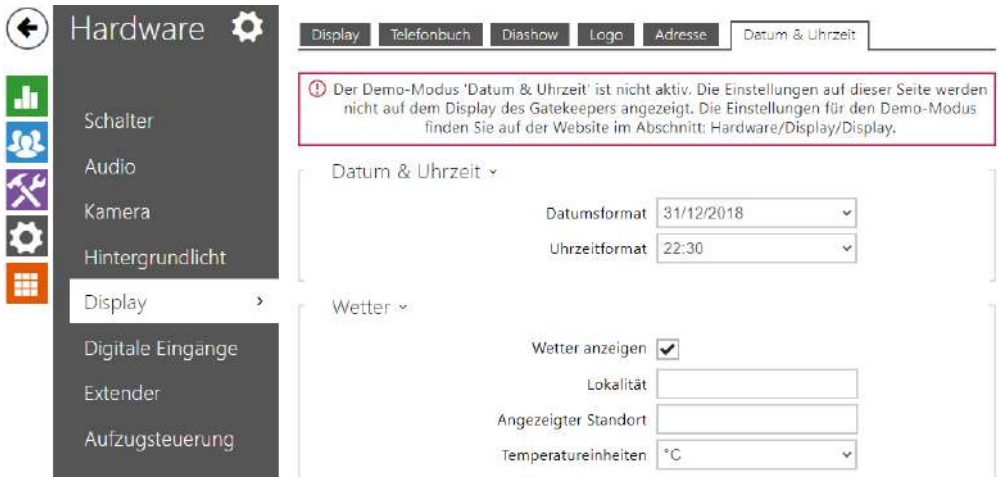
- **Nummer** – ermöglicht die Eingabe der Hausnummer oder einer anderen Identifizierung gemäß den örtlichen Gepflogenheiten. Erscheint im Demo-Modus, wenn Adresse ausgewählt ist.
- **Adresse** – ermöglicht die Eingabe der Adresse, des Gebäudenamens usw., die im Demo-Modus angezeigt werden, wenn die Option Adresse ausgewählt ist.
- **Adresse und Nummer tauschen** – vertauscht die Reihenfolge, in der Nummer und Adresse angezeigt werden.

Hinweis

- Die „Adresse“-Vorschau erscheint nur auf dem Display, wenn der angegebene Modus im Menü Hardware / Display / Display aktiviert wird.

Datum & Uhrzeit

Ermöglicht die Einstellung von Datum, Uhrzeit und Wetterparametern.



- **Datumsformat** – einstellung des am Gerätebildschirm angezeigten Datumformats.
- **Uhrzeitformat** – einstellung des am Gerätebildschirm angezeigten Uhrzeitformats.

Wetter

- **Wetter anzeigen** – das Gerätedisplay zeigt Informationen zum aktuellen Wetter an.
- **Lokalität** – standort für die Wettervorhersage, in dem sich dieses Gerät befindet. Wenn es nicht ausgefüllt ist, wird der automatisch ermittelte Standort verwendet.
- **Angezeigter Standort** – Auf dem Display angezeigter Standort. Wenn es nicht ausgefüllt ist, wird der Standort aus der Wettervorhersage angezeigt.
- **Temperatureinheiten** – Auswahl der auf dem Display angezeigten Temperatureinheiten. Zur Auswahl stehen °C und °F.

Begrüßungsnachricht

	
Benutzerdefiniertes Bild	Textnachricht

Ermöglicht, die Meldung einzustellen, die nach erfolgreicher Authentifizierung auf dem Display erscheint.Registerkarte Display

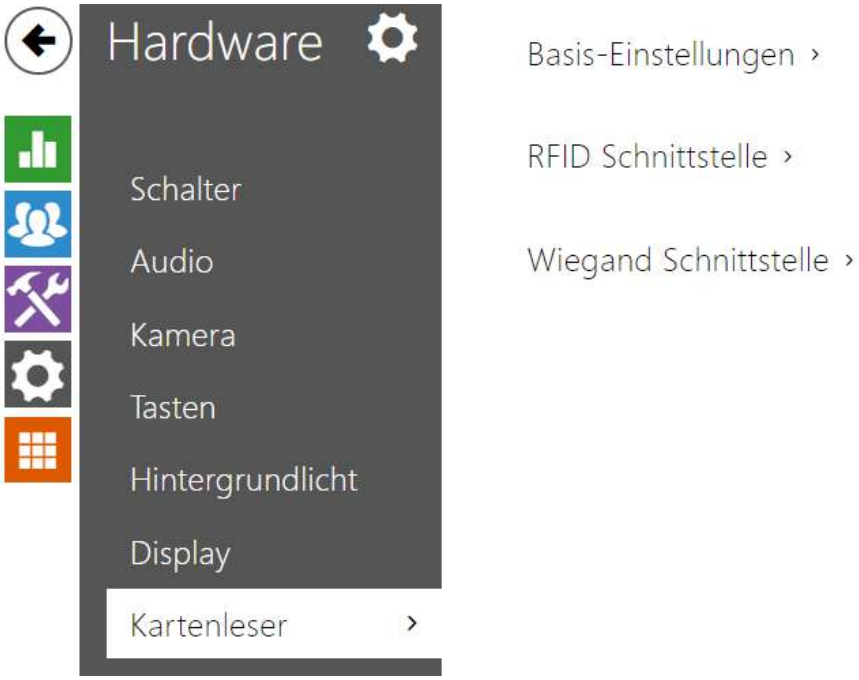
- **Modus des Begrüßungsbildschirms** – Wählen Sie den Inhaltstyp der Begrüßungsnachricht.
- **Zeit der Anzeige** – Stellt die Zeit ein, in der das Gerät die Begrüßungsnachricht anzeigen wird.
- **Symbol** – Wählen Sie das Symbol für die textliche Begrüßungsnachricht:

		
Info	Hinweis	Betreten verboten

 Pfeil nach links	 Pfeil nach oben	 Pfeil nach rechts
 Pfeil links abbiegen	 Pfeil nach unten	 Pfeil rechts abbiegen

- **Überschrift der Nachricht** – Stellt die Überschrift der textlichen Begrüßungsnachricht ein.
- **Text der Nachricht** – Stellt den Text der textlichen Begrüßungsnachricht ein.
- **Bestätigung** – Stellt ein, ob die textliche Begrüßungsnachricht das Bestätigungsfeld 'OK' hat.
- **Eigenes Bild hochladen** – Lädt das Bild hoch, das als Begrüßungsnachricht angezeigt wird. Das Bild muss eine Auflösung von 800 x 1280 px und das Format JPEG oder PNG haben.

5.5.7 Kartenleser

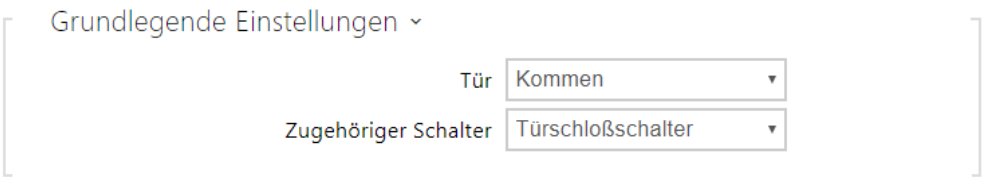


Dieses Menü ist nur bei den Interkommodellen **2N® IP Base**, **2N® IP Vario** und **2N® IP Force** verfügbar. Beim Modell **2N® IP Verso** wird hier nur die Möglichkeit der Einschränkung der erfolglosen Zutrittsversuche konfiguriert. Die anderen Funktionen werden im Abschnitt Erweiternde Module konfiguriert.

Der Kartenleser ermöglicht die effektive Steuerung des Zutritts zum Gebäude mittels kontaktloser RFID-Karten. Der Typ der unterstützten Karten hängt vom konkreten Modell des verwendeten Lesers ab.

Die Kartenleser für die Modelle **2N® IP Vario** und **2N® IP Force** sind mit einer Wiegand-Schnittstelle ausgestattet. Die Schnittstelle kann entweder als die Eingangsschnittstelle oder als die Ausgangsschnittstelle funktionieren. Die Schnittstellenrichtung ist konfigurierbar. Man kann die Schnittstelle im Eingangsmodus zum Anschluss der externen Kartenleser, Fingerabdruckscanner, Biometriescanner u.Ä. nutzen. Im Ausgangsmodus kann man mittels dieser Schnittstelle das Interkom z.B. an die Sicherheitszentrale anschließen und die IDs aus den angelegten Karten zu dieser Zentrale senden.

Grundlegende Einstellungen

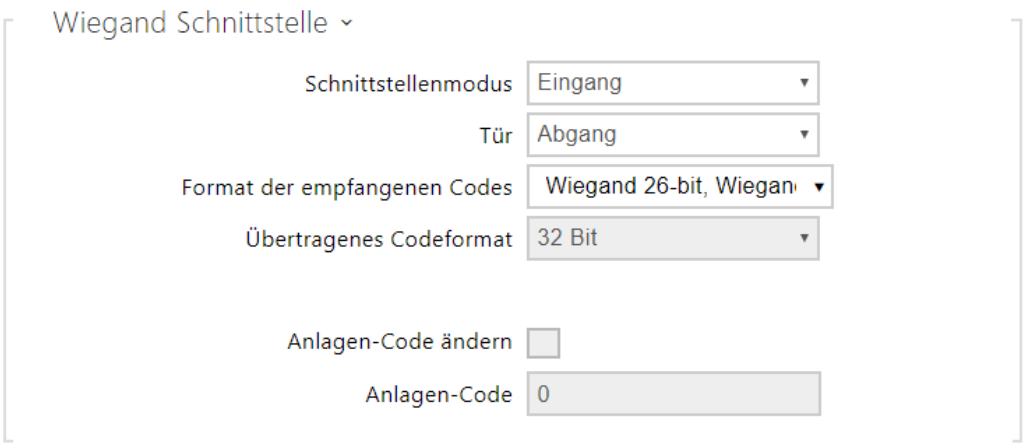


- **Tür** – passt die Durchlaufrichtung an, wenn ein Lesegerät verwendet wird (Coming, Exiting). Die Richtung des Parameters wird vom Anwesenheitssystem verwendet.
- **Zugenhöriger Schalter** – stellt die Nummer des Schalters ein, der nach dem Anlegen einer gültigen RFID-Karte aktiviert wird. Der eingestellte Wert wird im Fall der gültigen Karte des Nutzers bei gleichzeitig eingestellter Funktion der doppelten Authentifizierung dieses Nutzers nicht angewendet. In diesem Fall wird nach dem Anlegen der gültigen Karte die Eingabe des nummerischen Codes für das Einschalten des Schalters abgewartet und dieser nummerische Code identifiziert nachfolgend den eingeschalteten Schalter.

RFID-Schnittstelle

- **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.

Wiegand-Schnittstelle

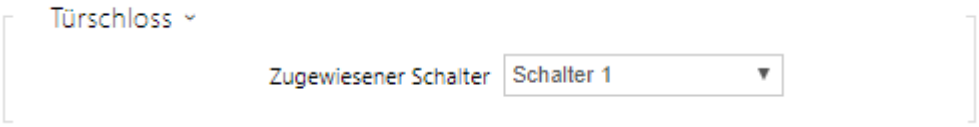


- **Schnittstellenmodus** – ermöglicht die Funktion der Wiegand-Schnittstelle einzuschalten und die Schnittstelle als eine Eingangs- oder Ausgangsschnittstelle einzustellen. Immer, wenn die Wiegand-Schnittstelle als die Eingangsschnittstelle eingestellt ist, werden zu dieser die IDs der an den internen Leser angelegten Karten gesendet.
- **Tür** – passt die Durchlaufrichtung an, wenn ein Lesegerät verwendet wird (Coming, Exiting). Die Richtung des Parameters wird vom Anwesenheitssystem verwendet.
- **Format der empfangenen Codes** – stellt das Format der empfangenen Codes (Wiegand 26, 32, 37 a RAW) ein.
- **Übertragenes Codeformat** – stellt das Format der gesendeten Codes (Wiegand 26, 32, 37 a RAW) ein.
- **Anlagen-Code ändern** – ermöglicht den ersten Teil des Codes über die Wiegand-Schnittstelle zu ändern. Betrifft den Austrittsmodus der Schnittstelle für das Format des gesendeten Codes 26 bit. Überprüfen Sie beim Lieferanten der Sicherheitszentrale, ob der Facility-Code erforderlich ist.
- **Anlagen-Code** – bestimmt die Lokation des **2N IP** Interkoms im System der Sicherheitszentrale. Geben Sie den dekadischen Lokationswert (0–255) ein.
- **Richtung** – stellt die Durchgangsrichtung bei der Verwendung des Lesegerätes ein (Nicht spezifiziert, Kommen, Gehen). Der Parameter Richtung wird durch das Anwesenheitssystem genutzt.

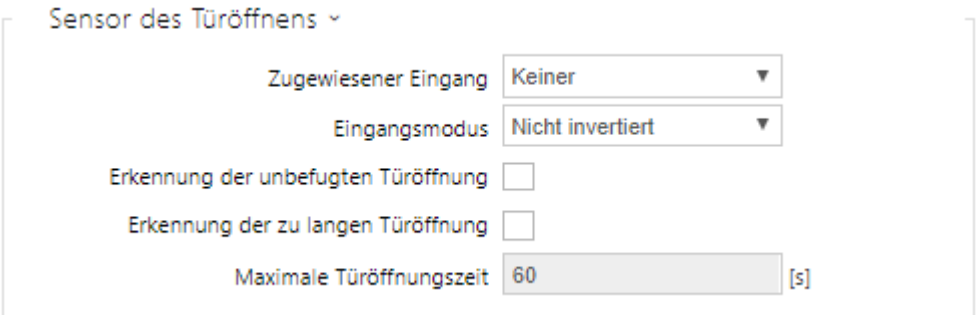
5.5.8 Digitale Eingänge

In diesem Teil der Interkomkonfiguration können Sie die Parameter, die mit digitalen Eingängen zusammenhängen, und ihre Verknüpfung mit weiteren Interkomfunktionen einstellen. Die digitalen Eingänge sind nur bei ausgewählten Interkommodellen ggf. nach der Installation des geeigneten Zubehörs verfügbar (z.B. Kartenleser).

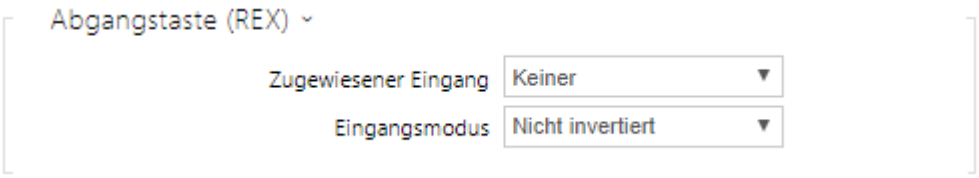
Registerkarte Türen



- **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).

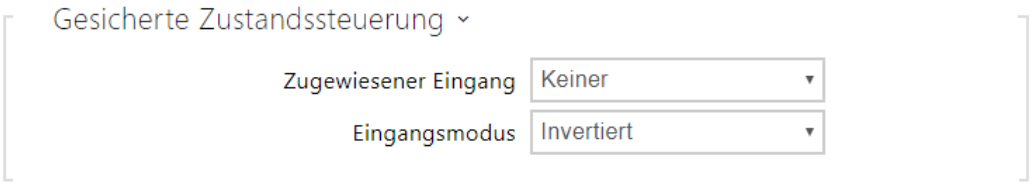


- **Zugewiesener Eingang** – ermöglicht einen der logischen Eingänge (ggf. keinen Eingang) für die Erkennung der offenen Tür zu bestimmen.
- **Eingangsmodus** – ermöglicht das aktive Niveau (Polarität) des Eingangs einzustellen. Nicht invertiert / Invertiert.
- **Erkennung der unbefugten Türöffnung** – 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 Status "Gesichert" wird dann durch die rote LED des Interkoms signalisiert (deren Platzierung sich bei einzelnen Interkomtypen unterscheidet).
- **Eingangsmodus** – ermöglicht das aktive Niveau (Polarität) des Eingangs einzustellen.

Anmerkung

- *Die Signalisierung des Status Gesichert wird gewöhnlich in Verbindung mit der Sicherheitszentrale verwendet, die an einen der digitalen Eingänge des Interkoms angeschlossen ist. Die Leitung, aus der Zentrale, wird direkt oder mittels eines erweiternden Moduls an das Interkom angeschlossen. Die Platzierung der Signalisierungs-LED des Status Gesichert unterscheidet sich bei einzelnen Interkommodellen:*

  *Die Interkoms **2N® IP Vario** (91371…U) sind mit einer roten Signalisierungs-LED ausgestattet, die in der Mitte der unterbeleuchteten Namensschilder platziert ist.*
  *Die Interkoms **2N® IP Force** sind mit einer roten Signalisierungs-LED ausgestattet, die im Fenster des installierten Kartenlesers platziert ist*
  *Die Interkoms **2N® IP Verso** sind mit einem roten Piktogramm eines Hängeschlosses in der linken oberen Ecke des Basismoduls ausgestattet*

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 **HTTP API**).

Wenn die Funktion erlaubt ist, werden nach der Tamperaktivierung 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 Tamperaktivierung für 30 Minuten.
- **Zustand der Schalter-Blockierung** – zeigt und ermöglicht die Einstellung der Schaltersperre.

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.

5.5.9 Extender

Die Sprechanlagen **2N® IP Verso** und **2N® IP Style** können mit sogenannten Erweiterungsmodulen erweitert werden, die über den VBUS-Bus an die Basiseinheit der Sprechanlage angeschlossen werden. Zu Verfügung stehen die nachstehend angeführten Module:

- Tastaturmodul
- Modul des Infopanels

- Modul des Kartenlesers
- Bluetooth-Modul
- Modul der Eingänge und Ausgänge
- Modul der Wiegand-Schnittstelle
- Modul der OSDP-Schnittstelle
- Modul der Induktionsschleife
- Displaymodul
- Modul des Fingerabdruckscanners (Biometrischer Scanner)
- Touch-Tastatur
- Touch-Tastatur & RFID-Lesegerät 125 kHz, 13,56 MHz
- Bluetooth-&-RFID-Lesegerät 125 kHz, 13,56 MHz
- Touch-Tastatur-&-Bluetooth-&-RFID-Lesegerät 125 kHz, 13,56 MHz

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 1). Die Grundeinheit ist ein spezieller Modulfall und hat die Nummer 0.

Man kann die meisten 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 angeschlossenen erweiternden Module werden in der Reihenfolge angezeigt, die ihrer Verbindung entspricht. Die Module, die in größerer Entfernung von der Grundeinheit angeschlossen sind, werden in der Liste weiter unten angezeigt. Wenn an das Interkom mehrere Module gleichen Typs angeschlossen sind, kann es schwierig sein, die Einstellung dem konkreten Modul zuzuordnen. In diesem Fall kann man die angeschlossenen Module mittels der Taste **Modul lokalisieren** identifizieren. Das Modul leuchtet nach dem Drücken der Taste mehrmals kurz auf.

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

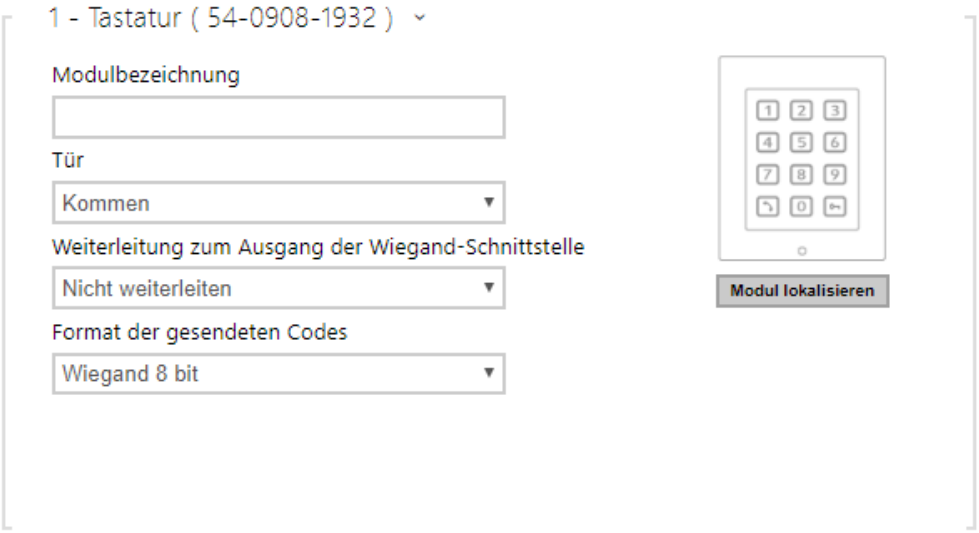
Konfiguration des Moduls der Grundeinheit

- **Gerät lokalisieren** – Licht- und Tonsignalisierung der konkreten Anlage. Anm.: Die optische Signalisierung wird nur bei Anlagen mit der Unterbeleuchtung der Bedienungselemente stattfinden (Verso, Base, Vario, Force, Safety und Uni). Falls die Anlage keinen integrierten Lautsprecher hat, muss für das Abspielen des Tonzeichens ein externer Lautsprecher angeschlossen werden (Audio Kit und Video Kit).

Konfiguration des Tastenmoduls

- **Tastenfunktion** – ermöglicht den Tasten Positionen in der Nutzerliste zuzuordnen.

Konfiguration des Tastaturmoduls

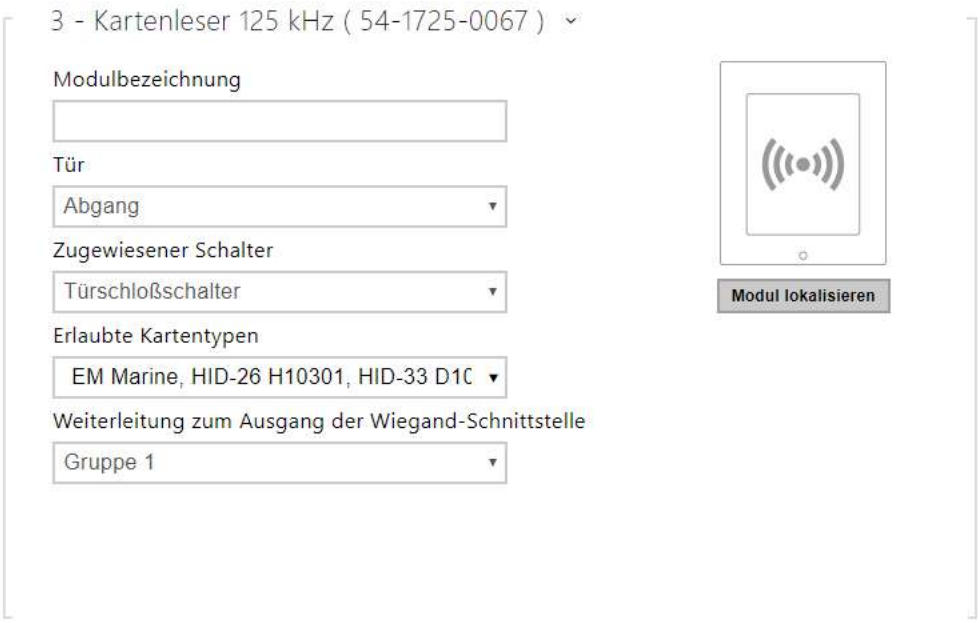


- **Modulbezeichnung** – legt den Modulnamen fest. Der Modulname wird beim Loggen der Ereignisse von der Tastatur verwendet.
- **Tür** – stellt die Durchgangsrichtung bei Verwendung eines Lesegeräts ein (Kommen, Abgang). Der Richtungsparameter findet beim Anwesenheitssystem Anwendung.
- **Weiterleitung 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 Modul veröffentlicht.

Konfiguration des Kartenlesemoduls 125 kHz



- **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, 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** – ermöglicht den Typ der Karte einzustellen, der durch das Lesegerät akzeptiert wird. Das Lesegerät unterstützt zu einem Zeitpunkt nur einen Kartentyp.
- **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 Kartenlesemoduls 13,56 MHz

- **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, 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** – ermöglicht den Typ der Karte einzustellen, der 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.
- **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-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 Reichweite des Signals ein (der Wert 5 ist die größte Reichweite, der Wert 1 die kleinste), d.h. die Entfernung, auf die das Bluetooth-Modul noch mit dem Mobiltelefon kommunizieren wird. Bei der Einstellung wird empfohlen, die reale Reichweite des Signals auszuprobieren, die durch mehrere Faktoren beeinflusst wird (insbesondere die räumliche Anordnung der Installation, das verwendete Mobiltelefon und seine Position).
- **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 Gerä**t – die Authentifizierung muss durch Berührung auf dem Leser in Anwesenheit des Telefons mit gekoppelten **2N® Mobile Key** Applikation bestätigt werden.
  - **Bewegungserkennung** – die Authentisierung wird durch die Bewegungserkennung in Anwesenheit eines Telefons mit gekoppelter **2N® Mobile Key** Applikation gestartet.
- **Profil detekce pohybu** – nastavuje profil detekce pohybu, kterým se bude modul pro autentizaci pomocí mobilního telefonu řídit.
- **Bewegungserkennungsprofil** – stellt das Profil der Bewegungserkennung ein, nach dem sich das Modul für die Authentisierung mithilfe des Mobiltelefons richten wird.

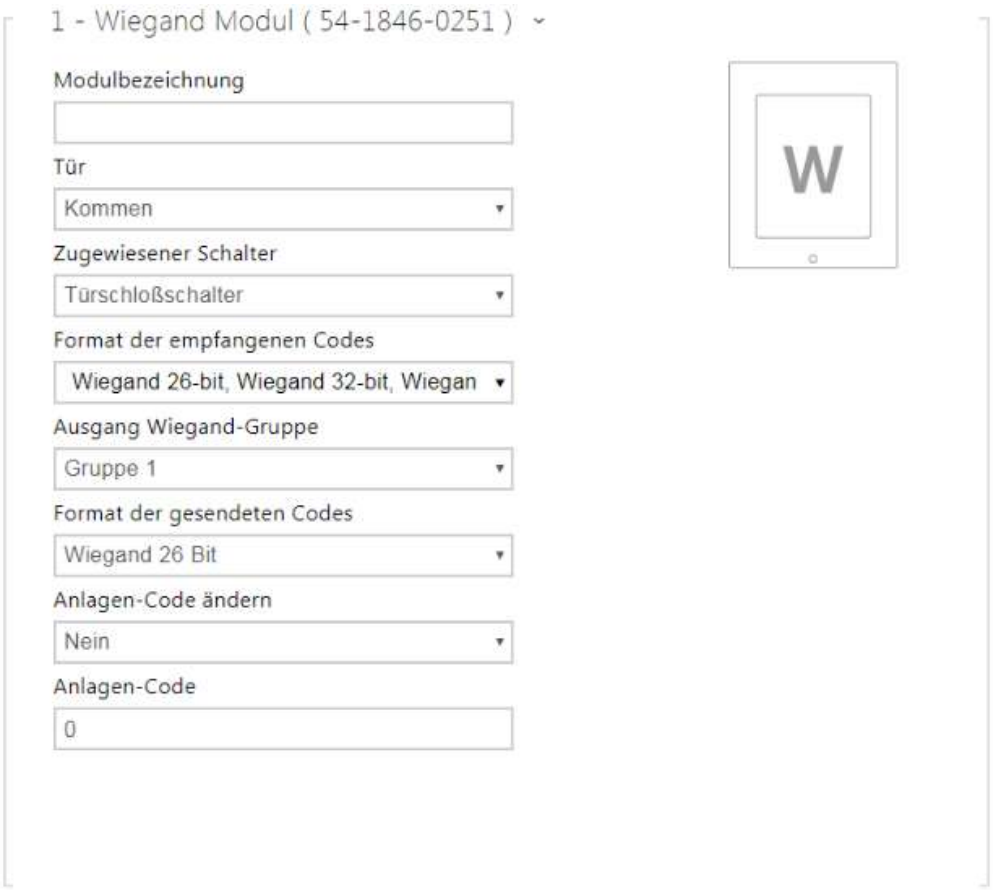
Konfiguration des Moduls der Eingänge und Ausgänge

- **Modulbezeichnung** – stellt den Modulnamen ein. Die Bezeichnung des Moduls wird bei der Spezifizierung des Eingangs oder Ausgangs in den Objekten SetOutput, GetInput und InputChanged 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 Interkom 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.



- **Modulname** – stellt den Modulnamen ein. Die Bezeichnung des Moduls wird bei der Spezifizierung des Eingangs oder Ausgangs in den Objekten SetOutput, GetInput und InputChanged in der Einstellung Automation verwendet.
- **Richtung** – stellt die Durchgangsrichtung bei der Verwendung des Lesegerätes ein (Nicht spezifiziert, Kommen, Gehen). Der Parameter Richtung wird durch das Anwesenheitssystem genutzt.
- **Mehrfache Authentifizierung** – erlaubt die mehrfache Authentifizierung des Nutzers mittels des Lesegerätes, das an das Wiegand-Modul angeschlossen ist (bzw. die Authentifizierung wird durch die Einstellung auf der Karte des Nutzers gesteuert, siehe Verzeichnis / Nutzer). Bei einzelnen an das Interkom angeschlossenen Lesegeräten kann man die mehrfache Authentifizierung ausschalten, d.h. es ist nicht notwendig, dass der Nutzer nach dem Kartenanlegen den Nutzercode auf der nummerischen Tastatur eingibt.
- **Assoziierter Schalte**r – stellt die Nummer des Schalters ein, der nach dem Empfang des gültigen Codes aktiviert wird.
- **Format der empfangenen Codes** – stellt das Format der empfangenen Codes (26 Bit, 32 Bit, 37 Bit, RAW Format, 35 Bit, Corp. 1000, 48 Bit, Corp. 1000 und Auto) ein.

- **Signalisierung des Kartenlesens** – stellt die Art der Signalisierung des empfangenen Codes ein.
  - **Vollständige** – die Tonsignalisierung unterscheidet zwischen einem gültigen und einem ungültigen Code.
  - **Ein Piepton** – der gültige sowie ungültige Code werden mit einem Piepton signalisiert
  - **Keine** – der empfangene Code wird mit keinem Ton signalisiert.
- **Auf den Wiegand-Ausgang weiterleiten** – stellt die Gruppe der Wiegand-Ausgänge ein, an die alle empfangenen Codes gesendet werden.
- **Format der empfangenen Codes** – stellt das Format der gesendeten Codes (Wiegand 26, 32, 37 und RAW) ein.
- **Gruppe des Wiegand-Ausgangs** – ordnet den Wiegand-Ausgang der Gruppe zu, an die die Codes aus den angeschlossenen Kartenlesern bzw. Wiegand-Eingängen gesendet werden können.

Konfiguration des OSDP-Moduls

Das OSDP-Modul ist mit einer (Input-Output) OSDP (RS-485)-Schnittstelle ausgestattet. Über die OSDP-Schnittstelle kann die 2N IP-Sprechanlage beispielsweise mit dem Sicherheitssystem im Gebäude, dem Control Panel verbunden werden (es ist möglich, die ID der an das angeschlossene RFID-Lesegerät angeschlossenen RFID-Karten abzuschicken, gegebenenfalls PIN-Codes).

- **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

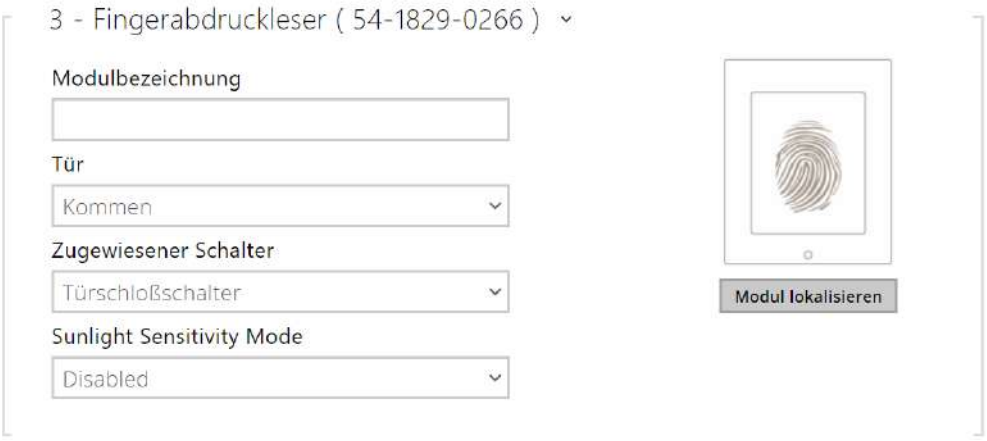
- **Modulbezeichnung** – legt den Modulnamen fest. Die Bezeichnung des Moduls wird beim Loggen der Ereignisse der Induktionsschleife verwendet.
- **Maximaler Stromverbrauch** – stellt die maximale Sendeleistung der Antenne der Induktionschleife ein. Eine größere Sendeleistung bedeutet größere Reichweite, jedoch

weniger Leistung für die anderen Interkomfunktionen. 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.

Konfiguration des Moduls des Fingerabdruckscanners (Biometrischer Scanner)



- **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, Abgang). 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.
- **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.

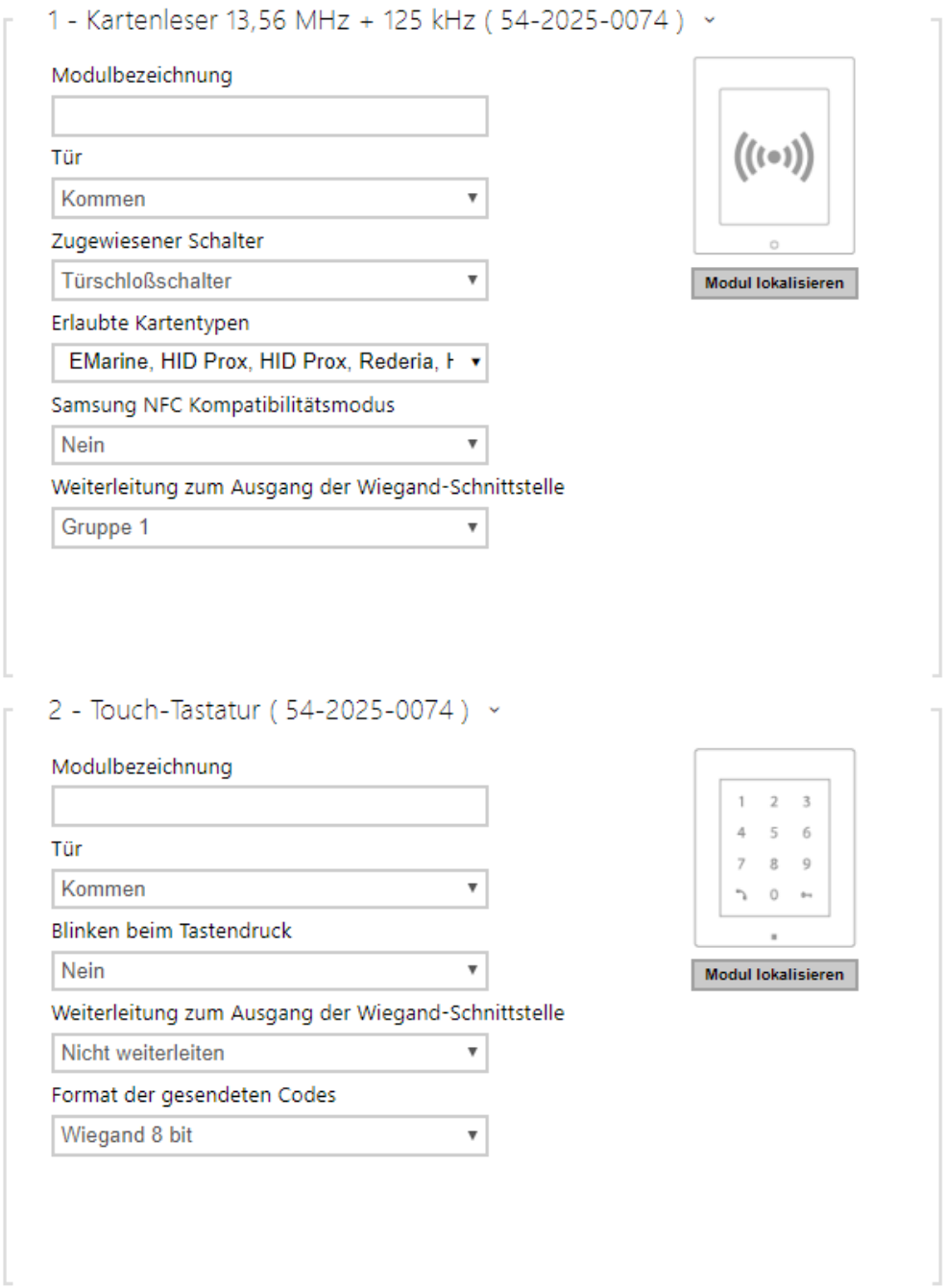
Hinweis

- Beim Abschalten des Fingerabdrucklesemoduls wird nach Neustart des Geräts im Nutzerprofil im Verzeichnis die Rubrik Nutzerfingerabdrücke verborgen. Sie zeigt an, wieviel Abdrücke der Nutzer im Speicher der Sprechanlage geladen hat. Nach Wiedereinschalten eines beliebigen Fingerabdrucklesemoduls wird der Teil der Nutzerkonfiguration wieder angezeigt.

Touch-Tastatur

- **Modulbezeichnung** – legt den Modulnamen fest. Die Modulbezeichnung wird beim Loggen der Ereignisse vom Touch-Tastatur verwendet.
- **Tür** – stellt die Durchgangsrichtung bei Verwendung eines Lesegeräts ein (Kommen, Abgang). 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 betätigten Tasten gesendet werden.
- **Format der gesendeten Codes** – Auswahl aus 4bit und 8bit (höhere Zuverlässigkeit) des Formats.

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



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

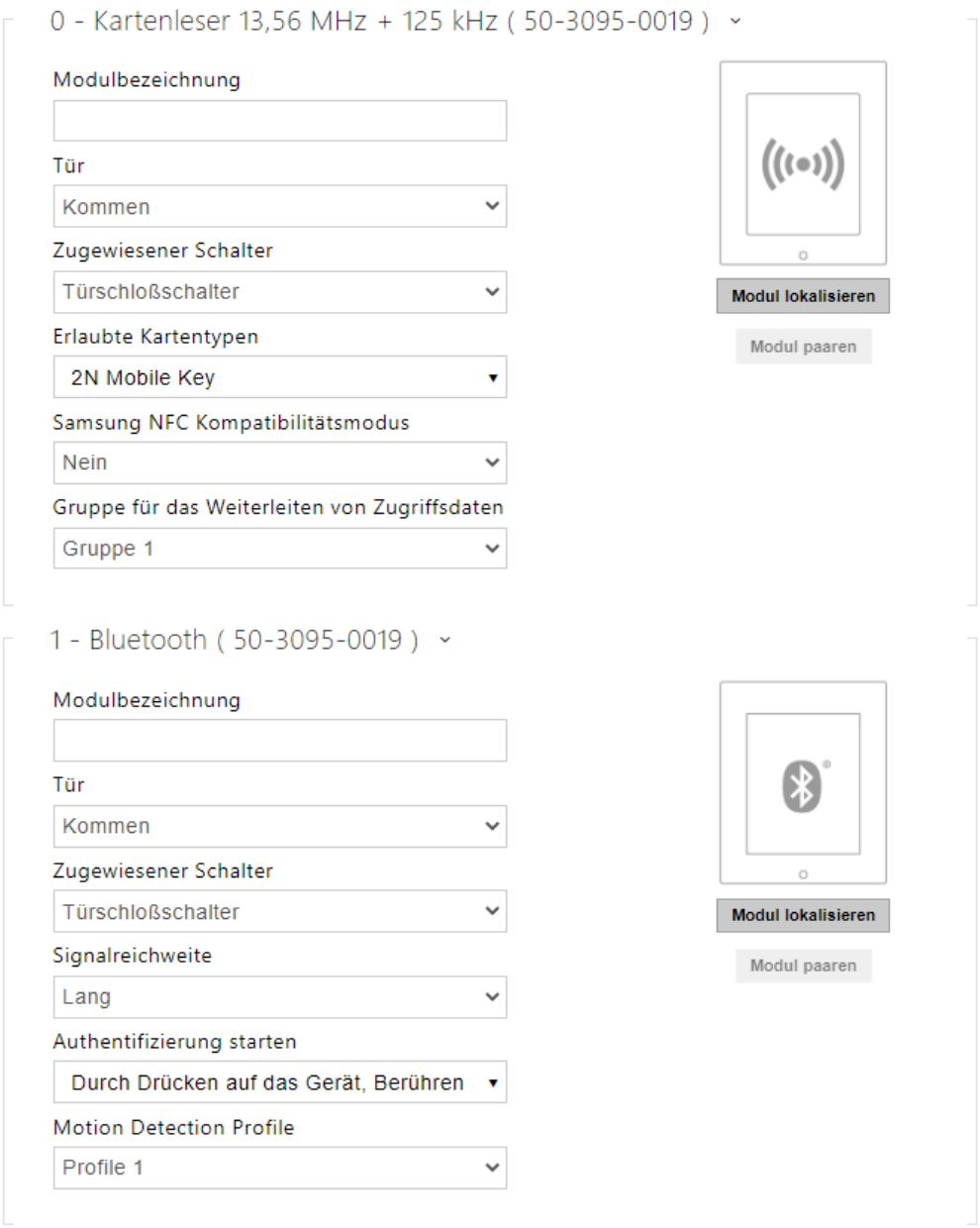
- **Modulbezeichnung** – legt den Modulnamen fest. Die Modulbezeichnung wird beim Loggen der Ereignisse vom Modul des Kartenlesers verwendet.
- **Tür** – stellt die Durchgangsrichtung bei Verwendung eines Lesegeräts ein (Kommen, Gehen). Der Parameter Richtung wird durch das Anwesenheitssystem genutzt.

- **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 / Türen verwendet.
- **Erlaubte Kartentypen** – udamit 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 NFC-Kompatibilität mit Samsung-Telefonen zu.
- **Weiterleitung zum Ausgang der Wiegand-Schnittstelle** – stellt die Gruppe mit den Wiegand-Ausgängen ein, an welche alle über die RFID-Kartenleser empfangenen ID weitergeleitet werden.

Touch-Tastatur (Seriennummer)

- **Modulbezeichnung** – legt den Modulnamen fest. Die Modulbezeichnung wird beim Loggen der Ereignisse vom Modul des Kartenlesers verwendet.
- **Tür** – stellt die Durchgangsrichtung bei Verwendung eines Lesegeräts ein (Kommen, Abgang). 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 betätigten Tasten gesendet werden.
- **Format der gesendeten Codes** – Auswahl aus 4bit und 8bit (höhere Zuverlässigkeit) des Formats.

Bluetooth-&-RFID-Lesegerät 125 kHz, 13,56 MHz / 2N IP Style



Kartenleser 13.56 MHz (125kHz) (Seriennummer)

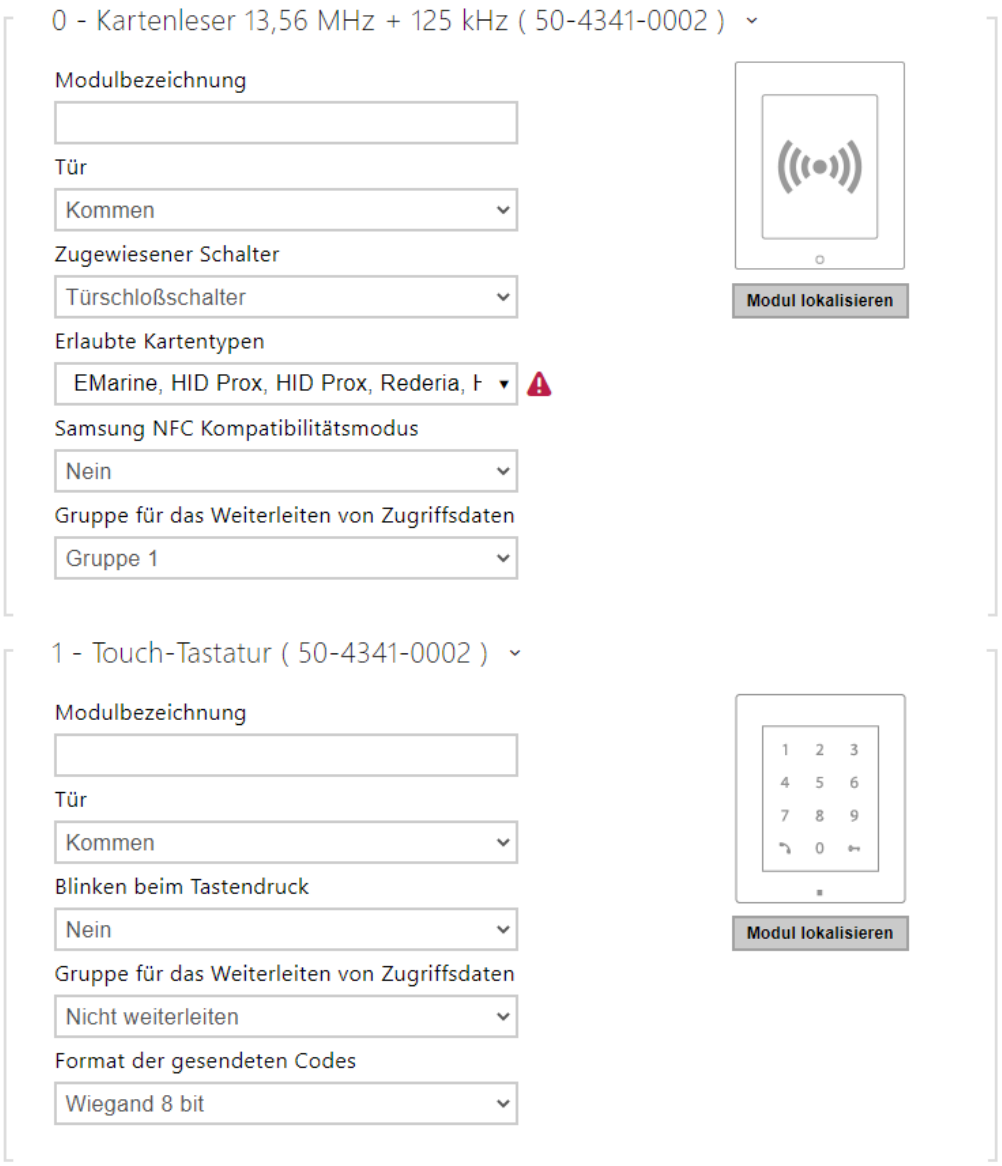
- **Tür** – stellt die Durchgangsrichtung bei Verwendung eines Lesegeräts ein (Kommen, Gehen). Der Parameter Richtung wird durch das Anwesenheitssystem genutzt.
- **Zugewiesener Schalter** – stellt die Nummer des Schalters ein, welcher nach der Benutzer-Authentifizierung über dieses Modul aktiviert wurde. 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.
- **RFID-Symbol Hintergrundbeleuchtun** (nur für IP Style) – schaltet die Hintergrundbeleuchtung des RFID-Symbols an der Anlage ein oder aus.
- **Samsung NFC Kompatibilitätsmodus** – lässt die NFC-Kompatibilität mit Samsung-Telefonen zu.
- **Weiterleitung zum Ausgang der Wiegand-Schnittstelle** – stellt die Gruppe mit den Wiegand-Ausgängen an, an welche alle über die RFID-Lesegeräte empfangenen ID weitergeleitet wurden.

Bluetooth (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
- **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 Reichweite des Signals ein (der Wert 5 ist die größte Reichweite, der Wert 1 die kleinste), d.h. die Entfernung, auf die das Bluetooth-Modul noch mit dem Mobiltelefon kommunizieren wird. Bei der Einstellung wird empfohlen, die reale Reichweite des Signals auszuprobieren, die durch mehrere Faktoren beeinflusst wird (insbesondere die räumliche Anordnung der Installation, das verwendete Mobiltelefon und seine Position).
- **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 Gerä**t – die Authentifizierung muss durch Berührung auf dem Leser in Anwesenheit des Telefons mit gekoppelten **2N® Mobile Key** Applikation bestätigt werden.
  - **Bewegungserkennung** – die Authentisierung wird durch die Bewegungserkennung in Anwesenheit eines Telefons mit gekoppelter **2N® Mobile Key** Applikation gestartet.
- **Bewegungserkennungsprofil** – stellt das Profil der Bewegungserkennung ein, nach dem sich das Modul für die Authentisierung mithilfe des Mobiltelefons richten wird.

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.

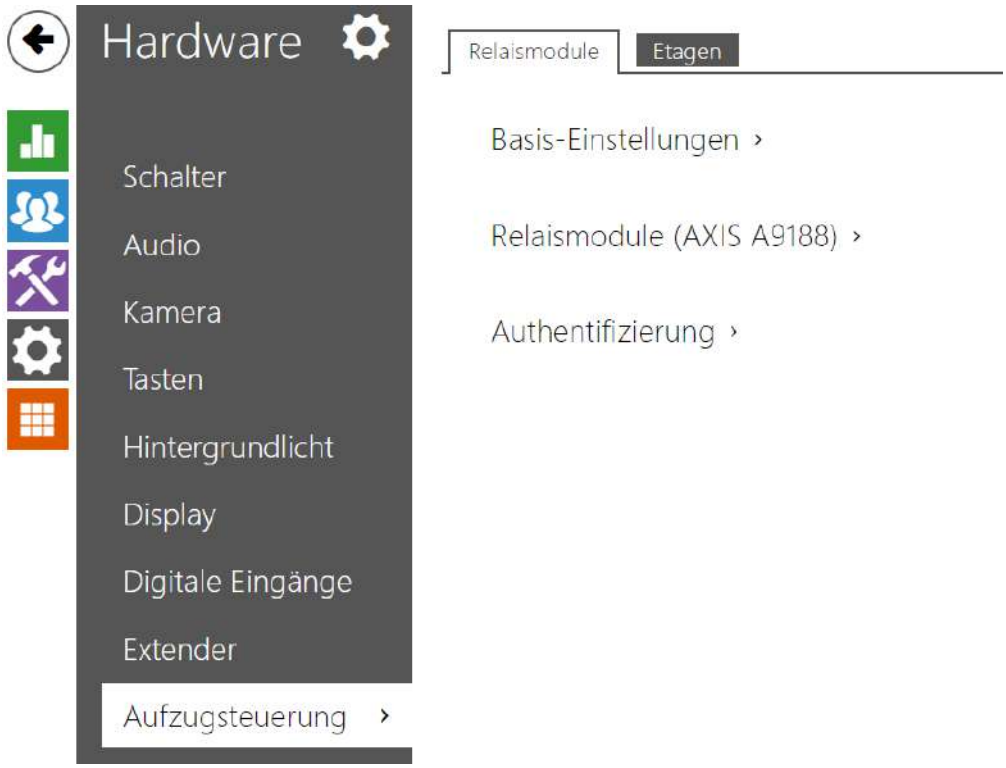
Touch-Tastatur (Seriennummer)

- **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 Reichweite des Signals ein (der Wert 5 ist die größte Reichweite, der Wert 1 die kleinste), d.h. die Entfernung, auf die das Bluetooth-Modul noch mit dem Mobiltelefon kommunizieren wird. Bei der Einstellung wird empfohlen, die reale Reichweite des Signals auszuprobieren, die durch mehrere Faktoren beeinflusst wird (insbesondere die räumliche Anordnung der Installation, das verwendete Mobiltelefon und seine Position).
- **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 Gerä**t – die Authentifizierung muss durch Berührung auf dem Leser in Anwesenheit des Telefons mit gekoppelten **2N® Mobile Key** Applikation bestätigt werden.
    - **Bewegungserkennung** – die Authentisierung wird durch die Bewegungserkennung in Anwesenheit eines Telefons mit gekoppelter **2N® Mobile Key** Applikation gestartet.

5.5.10 Aufzugsteuerung

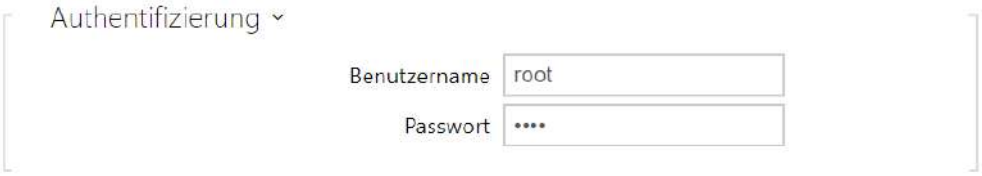


Durch Anschließen des Relaismoduls AXIS A9188 zur 2N IP Sprechanlage (**2N® IP Style, 2N® IP Verso**, **2N® IP Force**, **2N®**, **IP Safety**, **2N® IP Vario**) kann man den Zutritt auf einzelne Etagen mit Aufzug steuern. Zu einer 2N IP-Sprechanlage kann man max. 8 solche Relaismodule anschließen, dabei jeder der Module 8 Etagen bedienen kann, insgesamt also 64 Etagen.

Registerkarte Relaismodule

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

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

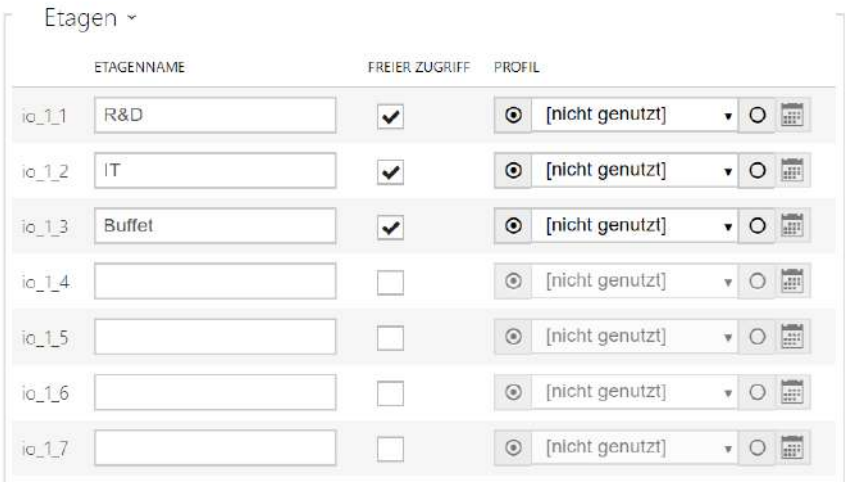


- **Nutzername** – Nutzername für die Authentifizierung des Anschlusses an ein externes Gerät. Der Parameter ist nur dann verbindlich, wenn das externe Gerät eine Authentifizierung verlangt.
- **Passwort** – Passwort zur Authentifizierung des Anschlusses an einem externen Gerät (WEB-Relais, usw.).Der 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 Zutritt** – 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 in der Sektion Telefonbuch / Zeitprofile möglich.
  -  mit der Markierung wird die Auswahl von den vordefinierten Profile oder manuelle Einstellung des Zeitprofils für das jeweilige Element eingestellt.
  -  mit der Markierung wird das Zeitprofil direkt für das jeweilige Element eingestellt. {page break

Tip

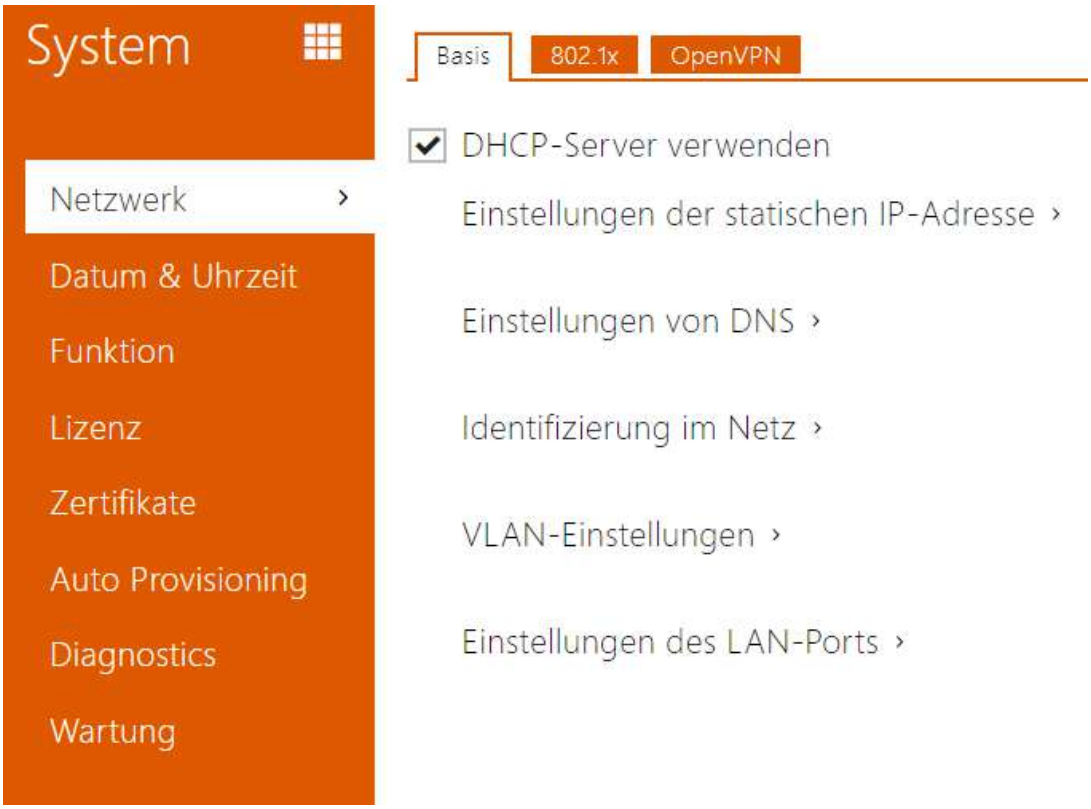
Generierung des Zertifikats für das Relaismodul AXIS A9188

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.
9. Wählen Sie das Zertifikat im Rollmenü aus and speichern Sie es durch Drücken der SAVE-Taste.
10. Gehen Sie in die Webschnittstelle der 2N IP-Sprechanlage 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.

5.6 System

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

5.6.1 Netzwerk



2N IP Interkom 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® Network Scanner** nutzen, die frei zum Herunterladen auf der Webseite www.2n.com zu Verfügung steht, oder Sie können den Mechanismus anwenden, der im Installationshandbuch des jeweiligen Interkoms angeführt ist – das Interkom wird Ihnen seine IP-Adresse mittels der Voice-Funktion selbst mitteilen.*

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 Interkom so konfigurieren, dass es die Authentifizierung EAP-MD5 oder EAP-TLS anwendet. Der Einstellung dieser Funktion dient die Registerkarte 802.1x.

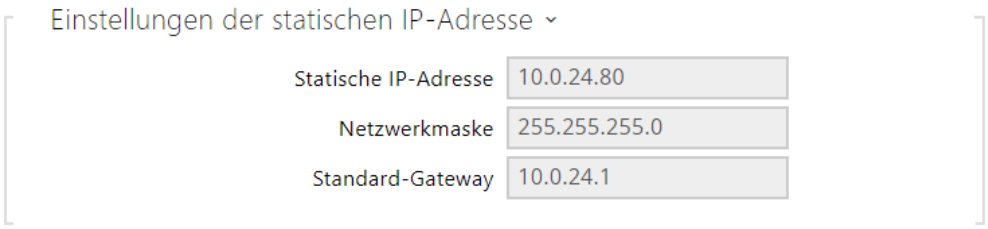
In der Registerkarte Trace können Sie das Abfangen der eingehenden und ausgehenden Pakete auf der Netzschnittstelle des Interkoms starten. Die Datei mit den abgefangenen Paketen kann man herunterladen und nachfolgend z.B. mithilfe der Applikation Wireshark (www.wireshark.org) verarbeiten.

Parameterliste

Netzwerk

Registerkarte Grundlegendes

- **DHCP-Server anwenden** – 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.

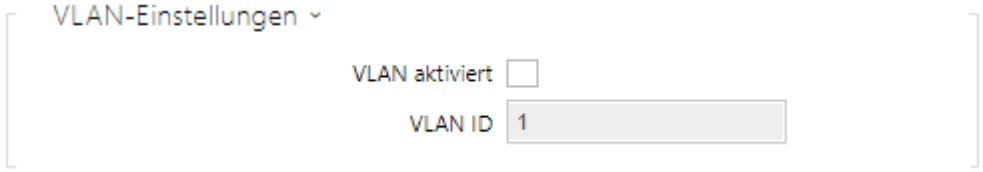


- **Statische IP-Adresse** – statische IP-Adresse des Interkoms. Die Adresse wird gemeinsam mit den nachstehenden Parametern angewendet, wenn der Parameter DHCP-Server anwenden nicht eingestellt ist.
- **Netzwerkmaske** – stellt die Netzmaske ein.
- **Standard-Gateway** – Adresse der Default-Gateway,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

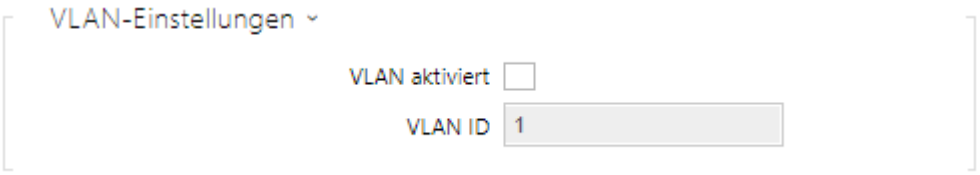
- **Primäres DNS** – Adresse des primären DNS-Servers für die Übersetzung der Domainnamen in IP-Adressen. Im Fall der Wiederherstellung des Default-Zustandes des Geräts wird der primäre DNS-Servers auf die Adresse 8.8.8.8 eingestellt.
- **Sekundäres DNS** – Adresse des sekundären DNS-Servers, der in 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 des 2N IP Interkoms im Netz.
- **Identifikator des Herstellers** – Legt die Hersteller-ID als Zeichenfolge für DHCP Option 60 fest.

- **WS-Discovery aktiviert** – aktiviert die WS-Discovery-Funktion, mithilfe deren andere ONVIF-Kliente kompatible Geräte im LAN suchen können. Aktivieren Sie die Funktion, damit Sie Ihre Sprechanlage als ein ONVIF-kompatibles Gerät nutzen können.



- **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.



- **Geforderter 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 Portstatus** – aktueller Status des Netzschnittstellenports Half oder Full Duplex – 10 mbps oder 100 mbps).

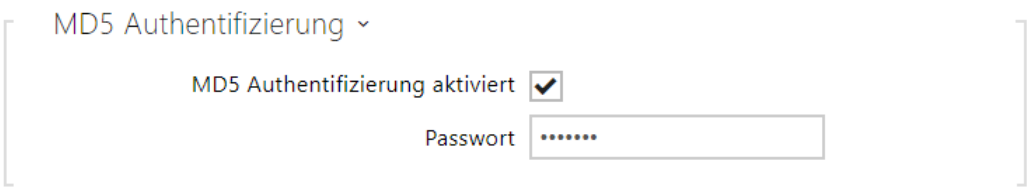
- **Verkürzte MTU** – aktiviert die Unterstützung der verkürzten MTUs (Maximum Transmission Unit) für den ordnungsgemäßen Gerätebetrieb in Netzwerken, die nur kürzere MTUs unterstützen.

Registerkarte 802.1x

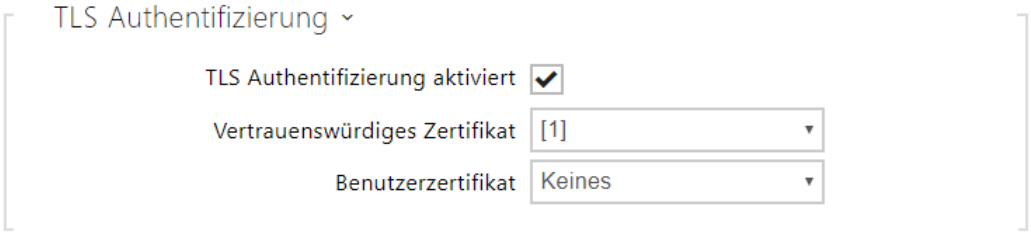
Hinweis

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

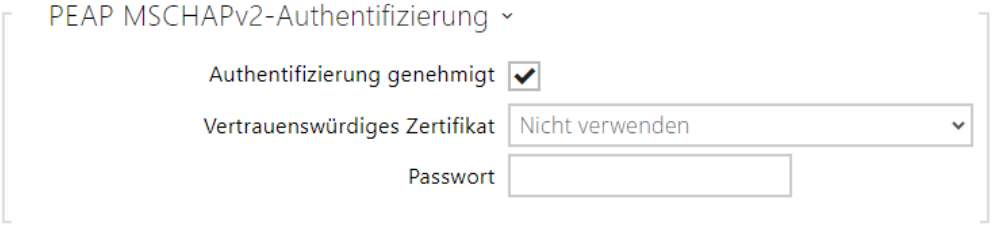
- **Identität des Gerätes** – Benutzername (Identität) für die Authentifizierung mittels der Methoden EAP-MD5 und EAP-TLS.



- **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. Im anderen Fall wird Ihr Interkom unerreichbar.
- **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 Interkoms 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.

OpenVPN

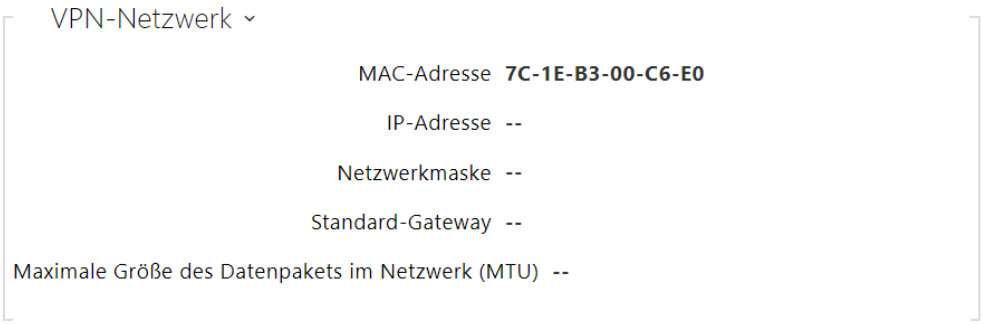
Über OpenVPN kann das Gerät an ein anderes Netzwerk angeschlossen werden.

- **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.

5.6.2 Datum und Uhrzeit

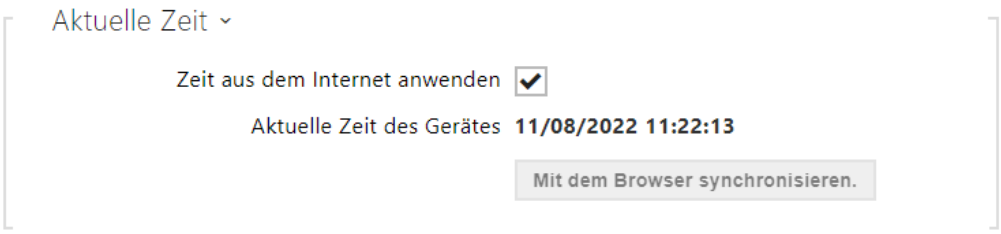
Wenn Sie die Einstellung der Zeitprofile für die Gültigkeitssteuerung der Telefonnummern, der Codes für das Einschalten der Schalter u.Ä. verwenden, müssen das interne Datum und die Uhrzeit im Interkom richtig eingestellt sein.

Die meisten Modelle des **2N IP Interkoms** sind mit einer Backup-Uhr der realen Uhrzeit ausgestattet, die ermöglicht, einen mehrtägigen Stromausfall zu überwinden. Falls das Interkom nicht mit dieser Funktion ausgestattet ist, geht die aktuelle Uhrzeit nach dem Stromausfall (ggf. Neustart) verloren. Die Folge ist, dass nach dem Anschluss des Interkoms an die Einspeisung nach einer längeren Zeit (z.B. nach der Installation eines neuen Interkoms) die Uhrzeit im Interkom auf den voreingestellten Wert eingestellt wird und erneut eingestellt werden muss. Die Gegensprechzeit 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 des Interkoms 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 **HTTP API** heruntergeladen wird u.Ä.) erforderlich.*

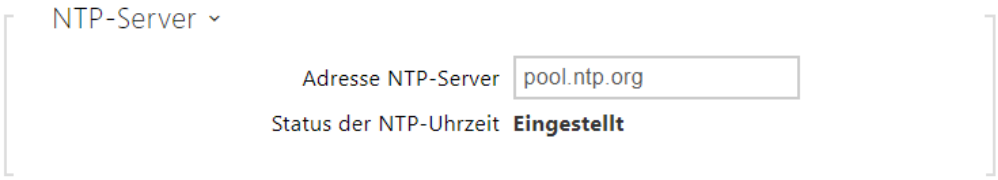
Für maximale Genauigkeit und Zuverlässigkeit empfehlen wir immer die Verwendung der Funktion **Aktuelle Uhrzeit aus dem Internet verwenden**. Unter normalen Betriebsbedingungen kann der Zeitfehler des Geräts bis zu ±2 Minuten/Monat betragen.

Parameterliste



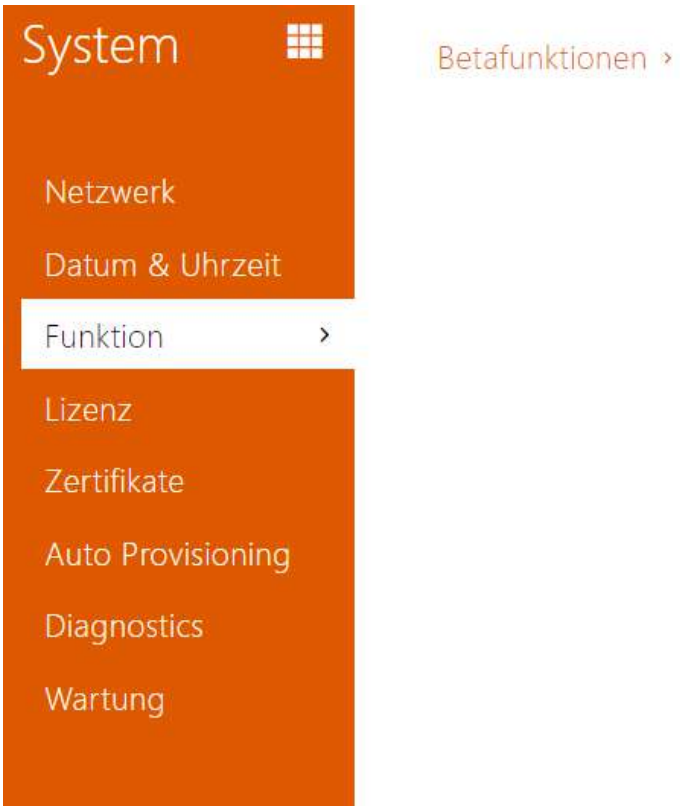
- **Zeit aus dem Internet anwenden** – Aktiviert die Nutzung des NTP-Servers für die Zeitsynchronisierung des Gerätes.
- **mit dem Browser synchronisieren** – mittels der Taste können Sie jederzeit die Uhrzeit im Interkom mit der aktuellen Uhrzeit in Ihrem PC synchronisieren.

- **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.



- **Adresse NTP-Servers** – stellt die IP-Adresse oder den Domainnamen des NTP-Servers ein, gemäß dem das Interkom die interne Uhrzeit synchronisiert. Weder die Server-IP-Adresse noch der Domänenname können eingestellt werden, wenn die Funktion „**Internetzeit verwenden**“ deaktiviert ist.
- **Status der NTP-Uhrzeit** – zeigt den Status des letzten Einstellungsversuchs der lokalen Uhrzeit mittels des NTP-Servers (Nicht eingestellt, Eingestellt, Fehler) an.

5.6.3 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.

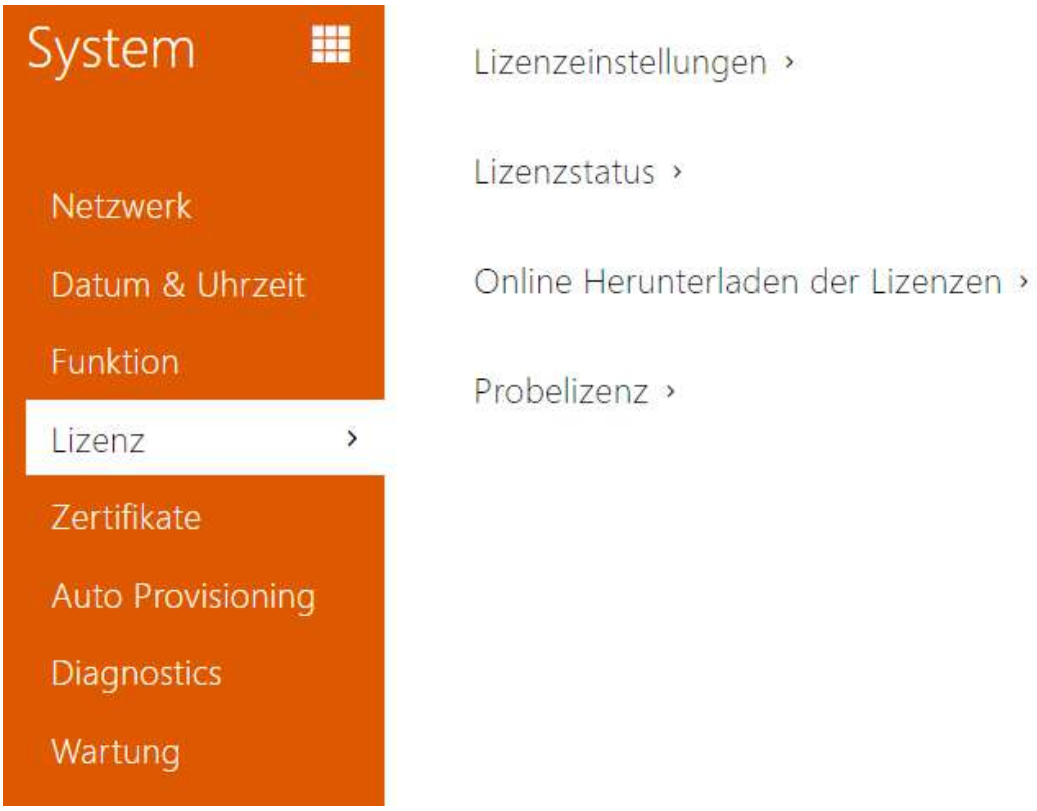
Aktivierung oder Deaktivierung der Funktion erfolgt erst nach einem Neustart des Geräts. Bis zum Neustart des Geräts kann die Anforderung der Zustandsänderung mit der Aktion **Abbrechen** rückgängig gemacht werden.

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.

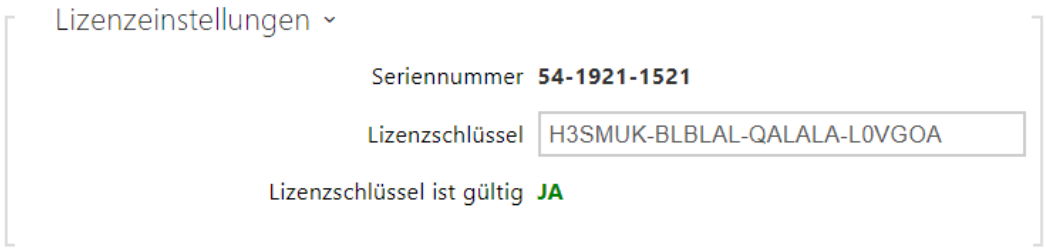
Bezeichnung der Betafunktion	Beschreibung
Passwortgeschützte Konfigurationsdatei	Mit dieser Funktion kann die Konfigurationsdatei während des Backups mit einem Passwort verschlüsselt werden (siehe 5.5.8 Wartung). Beim Hochladen einer Konfigurationsdatei auf das Gerät ist ein Passwort erforderlich, mit 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.
Noise Cancelling	Die Funktion unterdrückt die Umgebungsgeräusche des Mikrofons, wenn eine Stimme erkannt wird.

5.6.4 Lizenz



Manche Funktionen der **2N IP Interkoms** sind nur nach der Eingabe des gültigen Lizenzschlüssel verfügbar. Die Liste der Möglichkeiten der Interkomlizenzierung finden Sie im Kapitel **Unterschiede zwischen Modellen und Lizenzierung der Funktionen**.

Parameterliste

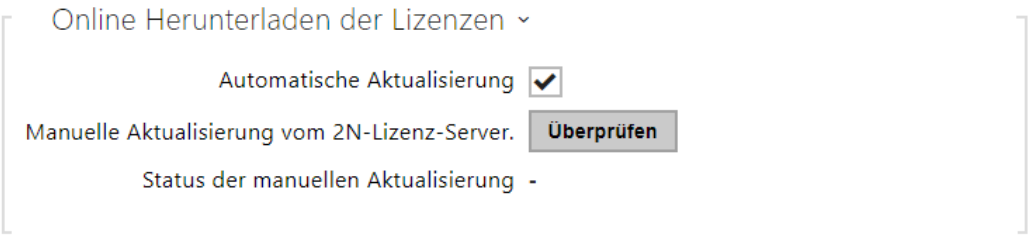


- **Seriennummer** – zeigt die Seriennummer der Anlage an, für die die Lizenz gültig ist.
- **Lizenzschlüssel** – ermöglicht den gültigen Lizenzcode einzugeben.
- **Lizenzschlüssel ist gültig** – zeigt an, ob der eingegebene Lizenzschlüssel gültig ist.

- **Standardlizenz** – zeigt eine Liste der Lizenzen an, die dem Gerät ab Werk beiliegen.
  - **Erweiterte Audiofunktion** – zeigt an, ob Funktionen verfügbar sind, die durch die Lizenz Enhanced Audio aktiviert wurden.
  - **Erweiterte Sicherheit** – zeigt an, ob Funktionen verfügbar sind, die durch die Lizenz Enhanced Security aktiviert wurden.
  - **NFC-Support** – zeigt an, ob die Unterstützung der Nutzeridentifikation mittels der Telefone mit der NFC-Technologie verfügbar ist.
- **Bezahlte Lizenzen** – zeigt eine Liste der Lizenzen an, die nach Eingabe eines gültigen Lizenzschlüssels verfügbar sind.
  - **Erweiterte Videofunktion** – zeigt an, ob Funktionen verfügbar sind, die durch die Lizenz Enhanced Video aktiviert wurden.
  - **Erweiterte Integration** – zeigt an, ob Funktionen verfügbar sind, die durch die Lizenz Enhanced Security aktiviert wurden.
  - **Informacast-Support** – zeigt an, ob die Unterstützung des Protokolls Informacast verfügbar ist.
  - **Unterstützung der Aufzugsteuerung** – zeigt an, ob die Funktion der aktivierten Lift Module Lizenz verfügbar ist.

Tipp

- Übersicht über Lizenzen und ihre Funktionen



- **Automatische Aktualisierung** – die Anlage aktualisiert den Lizenzschlüssel über den Lizenzserver 2N.
- **Manuelle Aktualisierung vom 2N-Lizenz-Server** – manuelle Anfrage betreffend die Überprüfung der Lizenzverfügbarkeit.
- **Status der manuellen Aktualisierung** – läuft, aktualisiert, nicht spezifiziert.

- **Status Probelizenz** – zeigt den Status der Trial-Lizenz (nicht aktiviert, aktiviert, Gültigkeit abgelaufen) an.
- **Lizenzablauf** – zeigt die restliche Laufzeit der Trial-Lizenz an. Bei jedem Neustart sowie beim Zurücksetzen in die Voreinstellung wird von der restlichen Laufzeit der Lizenz automatisch 1 Stunde abgezogen, ansonsten wird diese Zeit auf keine Art und Weise beeinflusst.

Hinweis

- Durch ein Software-Reset wird der Lizenzcode nicht gelöscht und es erfolgt kein Restart des eigentlichen Geräts. Bei ausgeschalteter automatischer Aktualisierung der Lizenz vor einem SW-Reset schaltet sich diese automatisch ein und schickt anschließend eine Anfrage an den Lizenz-Server. Bei eingeschalteter automatischer Aktualisierung der Lizenz wird die Anfrage innerhalb der geplanten Zeit an den Lizenz-Server geschickt.
- Bei einem Hardware-Reset wird der Lizenz-Code gelöscht. Der anschließende Restart des Geräts nach einer kurzen Zufallszeit hat eine Anfrage an den Lizenz-Server zur Folge.
    - Anfrage-Intervalle – zufällig ausgewählt im Bereich von 1 bis 100 Minuten nach dem Start und dann nach 8 Stunden bei Geräten mit Trial-Lizenz oder nach 8 Stunden über einen Zeitraum von 7 Tagen bei Geräten mit zeitlich unbegrenzter Lizenz.

5.6.5 Zertifikate

Manche Netzleistungen des **2N IP Interkoms** nutzen für die Kommunikation mit anderen Anlagen 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.

Interkomdienste, die das TLS-Protokoll nutzen:

a. Webserver (HTTPS-Protokoll)
b. E-Mail (SMTP-Protokoll)
c. 802.1x (EAP-TLS-Protokoll)
d. SIPs

Mit **2N IP Interkoms** 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.

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

- Das **2N IP Interkom** akzeptiert Zertifikate in den Formaten DER (ASN1) und PEM.
- Das **2N IP Interkom** unterstützt die AES-, DES- und 3DES-Verschlüsselung.
- Das **2N IP Interkom** 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

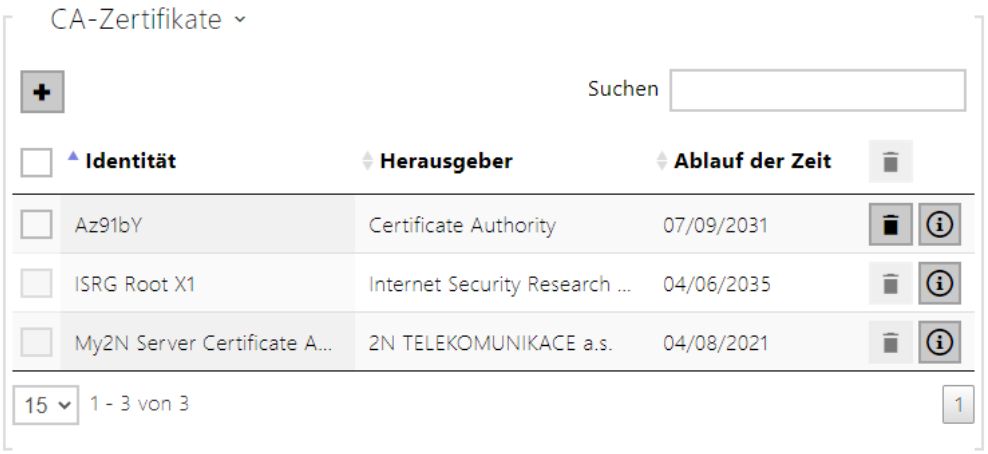
- CA-Zertifikate müssen das X.509 v3-Format verwenden.

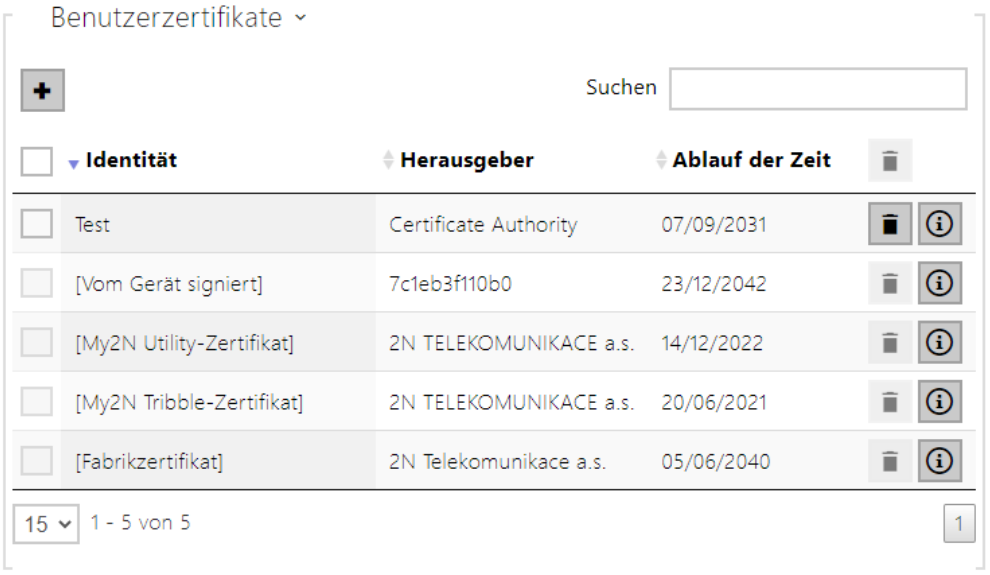
Beim ersten Anschluss der Einspeisung an das Interkom werden automatisch das sog. **Self Signed Zertifikat** und der **private Schlüssel** generiert, den man für den Dienst **Webserver** und **E-Mail** ohne die Notwendigkeit ein eigenes Zertifikat und den privaten Schlüssel hochladen zu müssen.

Anmerkung

Falls Sie das Self Signed Zertifikat für die Verschlüsselung der Kommunikation zwischen dem Webserver des Interkoms und dem Webbrowser verwenden, ist die Kommunikation abgesichert, aber der Webbrowser wird sie darauf hinweisen, dass er die Glaubwürdigkeit des Interkomzertifikats 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

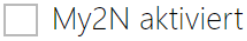
Es ist möglich, dass ein Zertifikat mit einem längeren privaten RSA-Schlüssel von mehr als 2048 bits abgelehnt wird. In diesem Fall erscheint die Meldung:
Die Datei des privaten Schlüssels bzw. das Passwort wurden nicht von der Anlage akzeptiert!
Im Fall der Zertifikate, die von elliptischen Kurven ausgehen, kann man nur die Kurven secp256r1 (aka prime256v1 aka NIST P-256) und secp384r1 (aka NIST P-384) verwenden.

5.6.6 Aktualisierung

Die **2N IP Interkoms** ermöglichen außer der manuellen Aktualisierung der Firmware und der Konfiguration auch die Firmware und Konfiguration gemäß den festgelegten Regeln vom Speicherplatz in dem durch Sie definierten TFTP- oder HTTP-Server automatisch herunterzuladen und zu aktualisieren.

Die Adresse des TFTP und HTTP-Server kann manuell konfiguriert werden. Die **2N IP Interkoms** unterstützen die automatische Feststellung der Adresse mittels des lokalen DHCP-Servers (sog. 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. Das Interkom 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 Interkomneustarts (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. Das

2N IP Interkom erwartet auf Servern Dateien mit den Bezeichnungen:

a. **MODELL**-firmware.bin – Interkomfirmware
b. **MODELL**-common.xml – gemeinsame Konfiguration aller Interkoms des jeweiligen Modells
c. **MODELL**-**MACADDR**.xml – spezifische Konfiguration für ein Interkom

MODEL im Dateinamen gibt die technische Bezeichnung der 2N IP-Sprechanlage oder des 2N IP-Audiogeräts an:

1. **hipv – 2N® IP Vario**
2. **hipf – 2N® IP Force**
3. **hipsf – 2N® IP Safety**
4. **hipak – 2N® IP Audio Kit**
5. **hipvk – 2N® IP Video Kit**
6. **hipve – 2N® IP Verso**
7. **verso2 – 2N® IP Verso 2.0**
8. **au – 2N Access Unit**
9. **aug2 – 2N Access Unit 2.0**
10. **aum – 2N Access Unit M**
11. **hipso – 2N® IP Solo**
12. **hipba – 2N® IP Base**
13. **sac – 2N® SIP Audio Converter**
14. **sassh – 2N® SIP Speaker Horn**
15. **ss – 2N® SIP Speaker**
    a. **style – 2N® IP Style**

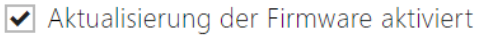
MACADDR ist die MAC-Adresse des Interkoms im Format 00-00-00-00-00-00. Die MAC-Adresse des Interkoms ist auf dem Herstellerschild oder direkt in der Schnittstelle in der Registerkarte **Interkomstatus** zu finden.

Beispiel:

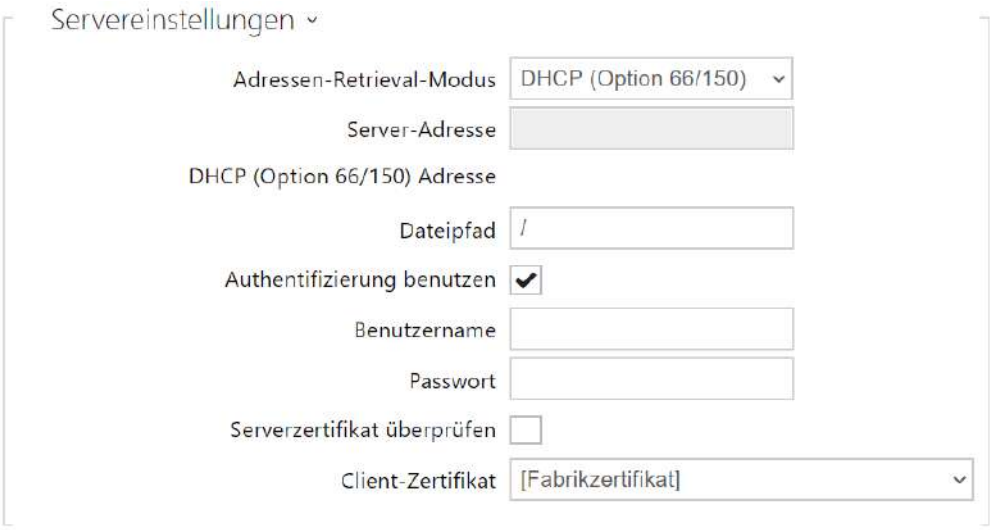
2N® IP Vario mit der MAC-Adresse 00-87-12-AA-00-11 wird vom TFTP-Server Dateien mit diesen Bezeichnungen herunterladen:

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

Parameterliste



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

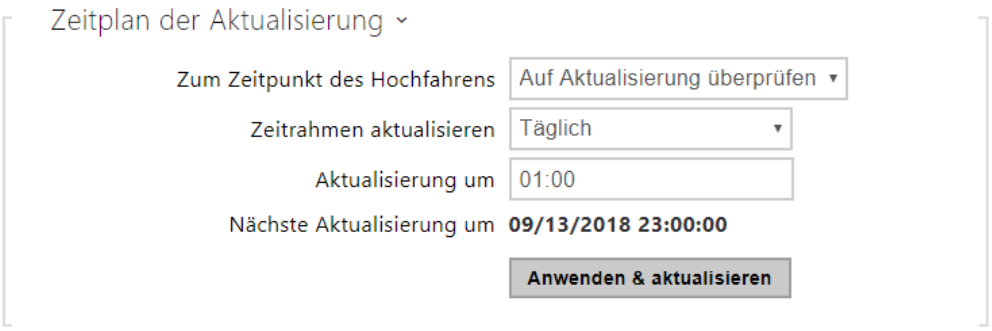


- **Adresse Datenabrufmodus** – ermöglicht zu wählen, ob die Adresse des TFTP/HTTP-Servers manuell eingegeben wird oder ob man die Adresse verwendet, die automatisch vom DHCP-Servers mittels des Parameters Option 66 übermittelt wurde.
- **Server-Adresse** – ermöglicht manuell die Adresse des TFTP-Servers einzugeben tftp://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 oder 150 übermittelt wurde.

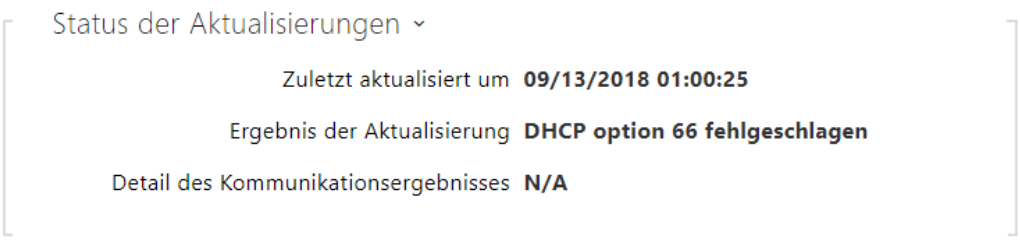
- **Dateipfad** – legen Sie den Pfad zum Firmware-Ordner fest. Geben Sie / ein, um nach model-firmware.bin (spezifisches Modell) im Stammverzeichnis des Servers zu suchen. Details zu Modellen usw. finden Sie in der Seitenleiste (?)
- **Authentifizierung benutzen** – ermöglicht die Anwendung der Authentifizierung 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.

Info

- Interkom 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 Interkomstart.
- **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 Interkom 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. Mögliche Werte sind folgende: DHCP option 66 failed, Firmware is up to date, Server connection failed, Running..., File not found.
- **Detail des Kommunikationsergebnisses** – falscher Code der Kommunikation mit Server oder Statuscode des TFTP/HTTP Protokolls.

Ergebnis	Beschreibung
Die Serveradresse ist ungültig	Die Serveradresse ist ungültig.
Das Protokoll wird nicht unterstützt	Das Protokoll wird nicht unterstützt. Unterstützt werden nur die Protokolle HTTP(s) und TFTP.
Die Position der Datei ist ungültig	Die Position der jeweiligen Datei ist ungültig
Die Funktion DHCP Option 66 ist fehlgeschlagen	Das Hochladen der Serveradresse über das DHCP-Protokoll Option 66 oder 150 ist fehlgeschlagen.
Der Domainname ist ungültig	Der Domainname des Servers ist wegen der unrichtigen Konfiguration oder unmöglichen Erreichbarkeit des DNS-Servers ungültig.
Server nicht gefunden	Der geforderte HTTP/TFTP-Server antwortet nicht.
Die Authentifizierung ist fehlgeschlagen	Die Authentifizierungsdaten HTTP sind nicht richtig.

Ergebnis	Beschreibung
Datei nicht gefunden	Die Datei wurde nicht auf dem Server gefunden.
Die Forderung befindet sich in der Warteschleife...	Die Aktualisierungsanforderung befindet sich in der Warteschleife.
Läuft...	Die Aktualisierung läuft
Die Datei ist ungültig	Die Datei zum Herunterladen ist beschädigt oder falschen Typs.
Die Firmware ist aktuell	Der Versuch der Firmwareaktualisierung hat gezeigt, dass die neueste Firmwareversion hochgeladen wurde.
Die Aktualisierung war erfolgreich	Die Aktualisierung der Konfiguration/Firmware war erfolgreich Im Fall der Firmwareaktualisierung wird die Anlage in ein Paar Sekunden neustarten.
Interner Fehler	Beim Herunterladen der Datei ist ein nicht identifizierter Fehler aufgetreten.

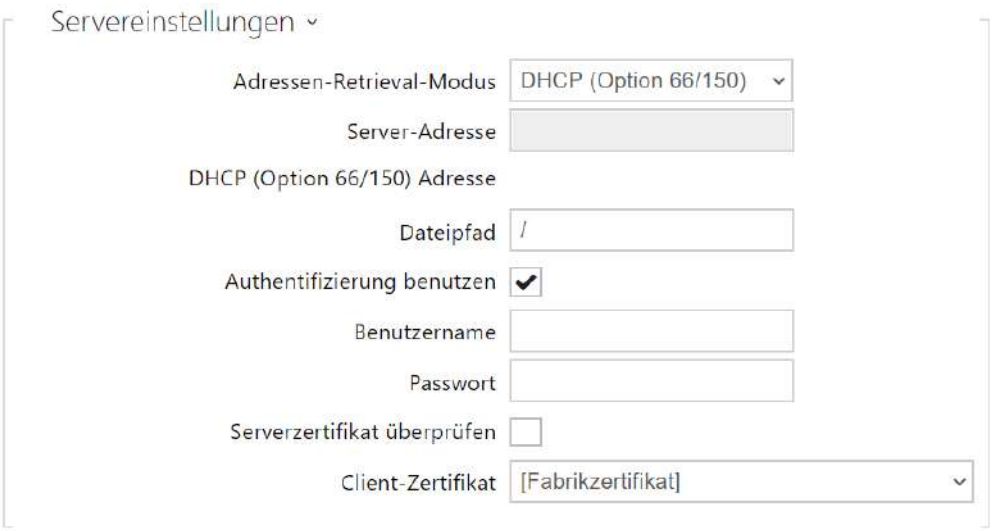
Registerkarte Konfiguration

In dieser Registerkarte wird das automatische Herunterladen der Konfiguration vom durch Sie definierten Server eingestellt. Das Interkom wird in den eingestellten Intervallen die Datei vom Server herunterladen und sich rekonfigurieren. Bei dieser Aktualisierung kommt es zu keinem Interkomneustart.

Anmerkung

- *Beim Interkom **2N® IP Vario** mit Display wird es bei jeder Aktualisierung zu einer Unterbrechung der Displayfunktion von bis mehreren Sekunden zu dem Zeitpunkt kommen, in dem seine Rekonfiguration läuft. Wir empfehlen deshalb die Aktualisierung zeitlich so einzustellen, dass sie in der Zeit der minimalen Interkomnutzung (z.B. in der Nacht) stattfindet.*

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

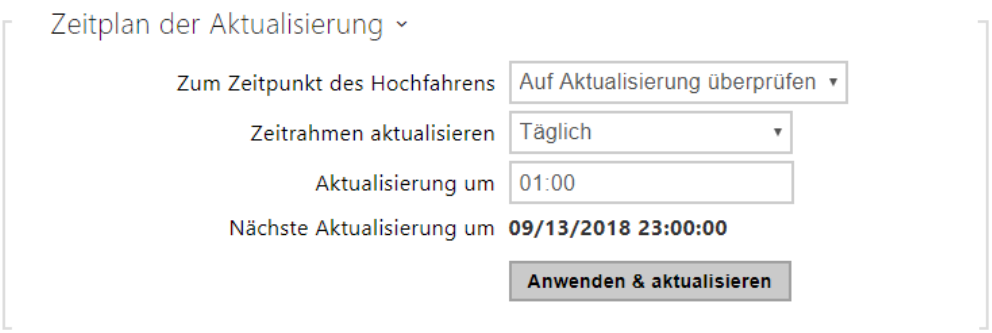


- **Adresse Datenabrufmodus** – ermöglicht zu wählen, ob die Adresse des TFTP/HTTP-Servers manuell eingegeben wird oder ob man die Adresse verwendet, die automatisch vom DHCP-Servers mittels des Parameters Option 66 übermittelt wurde.
- **Server-Adresse** – ermöglicht manuell die Adresse des TFTP-Servers 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 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 Interkommodell spezifiziert.

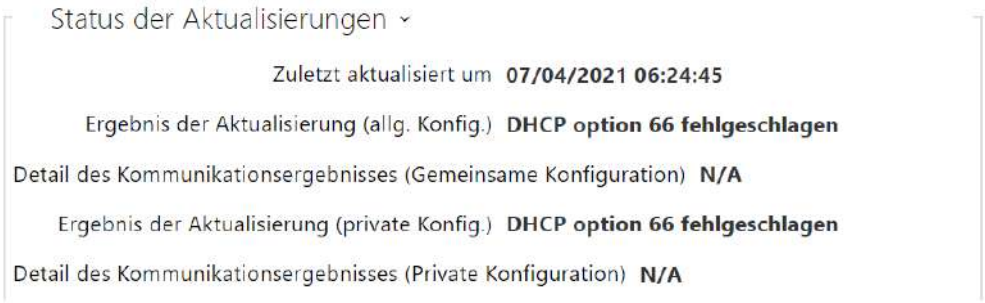
- **Authentifizierung benutzen** – ermöglicht die Anwendung der Authentifizierung für den Zutritt zum HTTP-Server einzustellen.
- **Benutzername** – der Nutzername, der für die Authentifizierung auf dem Server benutzt wurde.
- **Passwort** – das Passwort, dass für die Authentifizierung auf dem Server 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.

Info

- Interkom 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 Interkomstart.
- **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 Interkom 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 Aktualisierung an. Mögliche Werte sind folgende: DHCP option 66 failed, Firmware is up to date, Server connection failed, Running..., File not found.
- **Detail des Kommunikationsergebnisses (Gemeinsame Konfiguration)** – falscher Code der Kommunikation mit Server oder Statuscode des TFTP/HTTP Protokolls.
- **Ergebnis der Aktualisierung (private Konfig.)** – 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. Mögliche Werte sind folgende: DHCP option 66 failed, Firmware is up to date, Server connection failed, Running..., File not found.
- **Detail des Kommunikationsergebnisses (Private Konfiguration)** – falscher Code der Kommunikation mit Server oder Statuscode des TFTP/HTTP Protokolls.

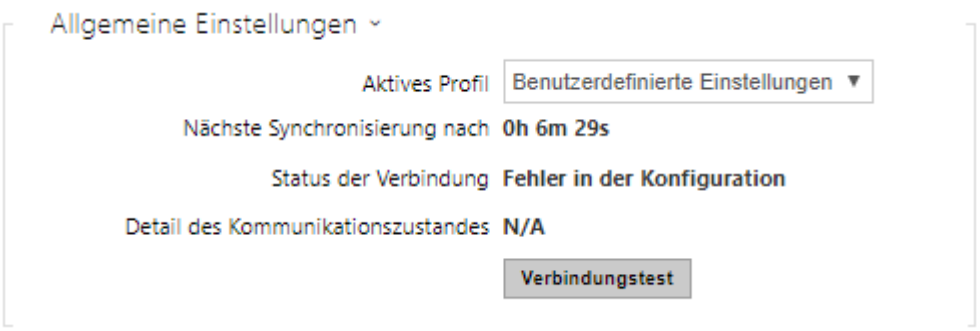
Registerkarte My2N / TR069

In dieser Registerkarte wird die Fernverwaltung des Interkoms mittels des Protokolls TR-069 erlaubt und konfiguriert. Das Protokoll TR-069 ermöglicht zuverlässig die Interkomparameter 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 des Interkoms mit My2N muss man immer die Leistung TR-069 freigeben und den Parameter aktives Profil auf den Wert My2N einstellen. Danach wird sich das Interkom 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 wird der Anschluss zum Dienst My2N auf dem Interkom ausgeschaltet.

- **My2N / TR069 erlaubt** – erlaubt den Anschluss an den Dienst My2N ggf. an einen anderen ACS-Server.

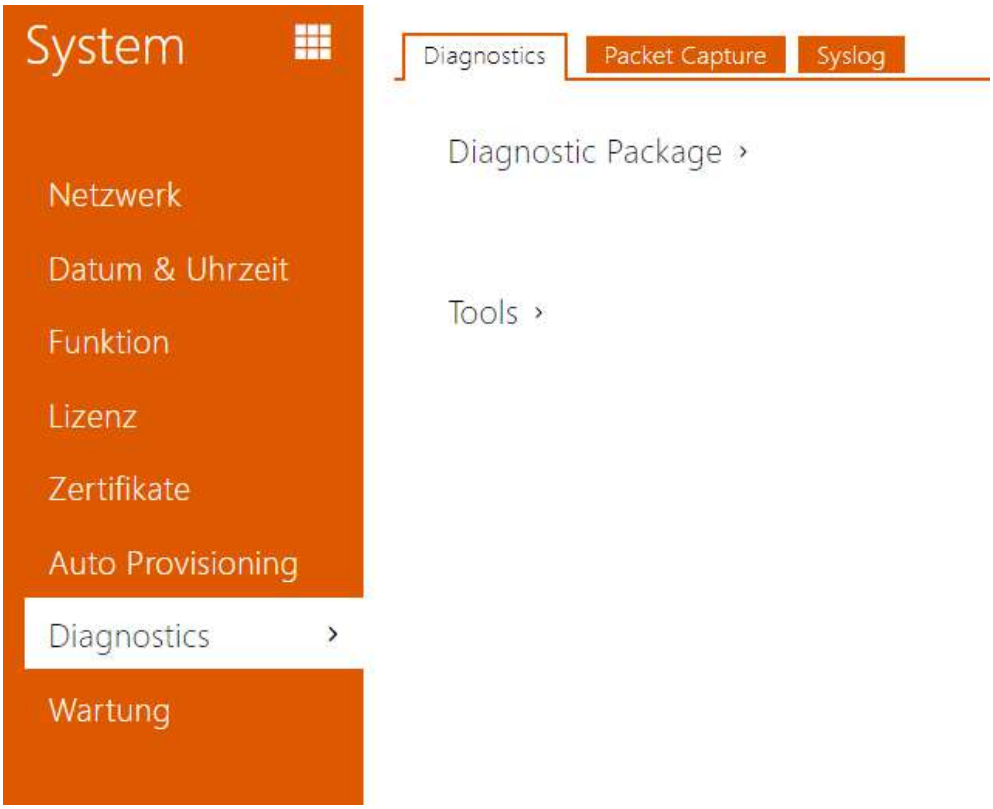


- **Aktives Profil** – ermöglich eines der voreingestellten Profile (des ACS-Servers) zu wählen ggf. die eigene Einstellung und den Anschluss an den ACS-Server manuell zu konfigurieren.
- **Nächste Synchronisierung nach** – zeigt an, wie lange es dauern wird, bis das Interkom Kontakt mit dem entfernten ACS-Server aufnehmen wird.
- **Status der Verbindung** – zeigt den aktuellen Staus des Anschlusses an den ACS-Server ggf. die Beschreibung des Fehlerstatus an.
- **Verbindungstest** – testet den Anschluss an den TR069-Dienst gemäß dem eingestellten 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 des Interkoms auf dem ACS-Server ein
- **Passwort** – stellt das Nutzerpasswort für die Authentifizierung des Interkoms auf dem ACS-Server ein
- **Serverzertifikat überprüfen** – spezifiziert den Satz der Zertifikate der Zertifizierungsautoritäten für die Überprüfung der Gültigkeit des öffentlichen Zertifikats

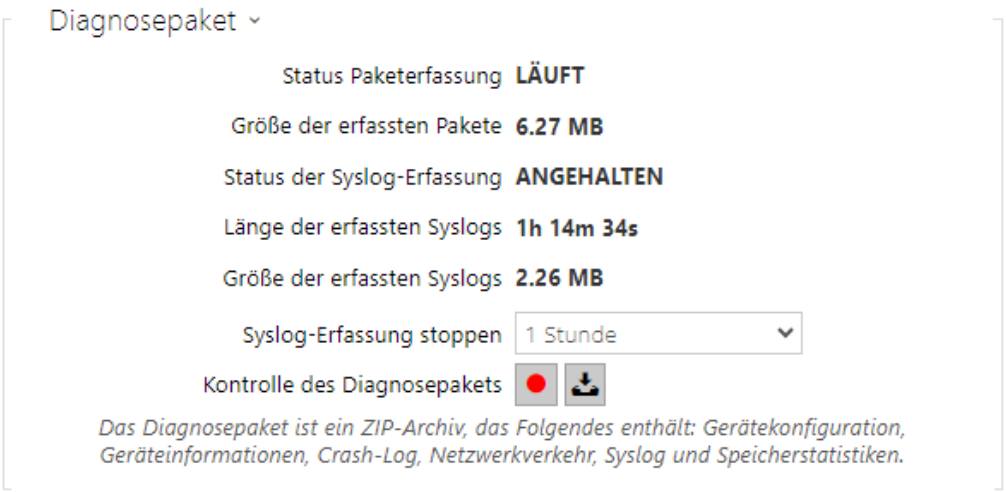
des ACS-Servers. Man kann eine der drei Gruppen der Zertifikate auswählen; siehe Kapitel Zertifikate. Ist kein Zertifikat der Zertifizierungsautorität angeführt, wird das öffentliche Zertifikat des ACS-Servers nicht verifiziert.
- **Client-Zertifikat** – spezifiziert das Nutzerzertifikat und den privaten Schlüssel, mit Hilfe deren die Berechtigung des Interkoms 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 des Interkoms zum ACS-Server.
- **Interval der regelmäßigen Rückmeldung** – stellt das Intervall der periodischen Anmeldung zum ACS-Server ein, wenn es mittels des Parameters **Freigabe der periodischen Anmeldung** erlaubt ist.

5.6.7 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.

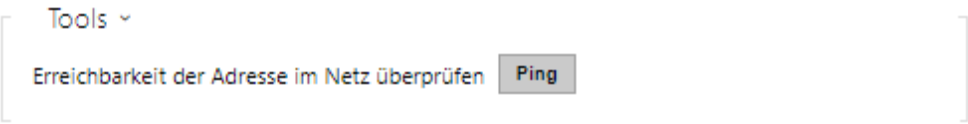


- **Status Paketerfassung** – zeigt an, ob die Paketerfassung im Bookmark Paketaufzeichnung läuft.
- **Größe der erfassten Pakete** – zeigt an, wie viele Pakete erfasst wurden.
- **Status der Syslog-Erfassung** – zeigt an, ob die Erfassung von Syslog-Nachrichten im Bookmark Syslog läuft.
- **Länge der 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



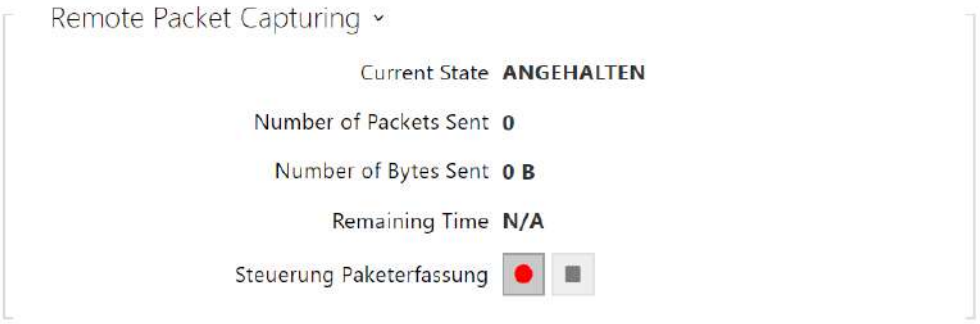
- **Erreichbarkeit der Adresse im Netz überprüfen** – dient der Überprüfung der Verfügbarkeit der jeweiligen Adresse im Netz als Befehl „Ping“ in üblichen Operationssystemen. Nach dem Drücken der Taste „Ping“ erscheint ein Dialog, in dem man diese IP-Adresse oder den Domainnamen eingeben und durch das 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 des Interkoms starten. Die erfassten Pakete können entweder lokal im Gerätepuffer gespeichert werden, dessen vom Gerät abhängt, oder entfernt auf dem Computer des Benutzers, begrenzt nur durch die angegebene Speicherzeit und den verfügbaren Speicherplatz. Die Datei mit den erfassten Paketen kann man herunterladen und nachfolgend z.B. mithilfe der Applikation Wireshark (www.wireshark.org) verarbeiten.

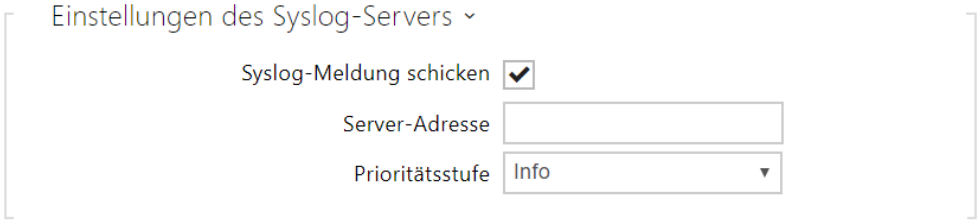
Wenn der Puffer während der lokalen Erfassung voll ist, werden die ältesten gespeicherten Pakete automatisch überschrieben. Beim lokalen Erfassen von Paketen empfehlen wir, die Bitrate der Videoübertragung auf unter 512 kbps zu reduzieren. Sie können das Abfangen mittels der Taste  starten, mittels der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



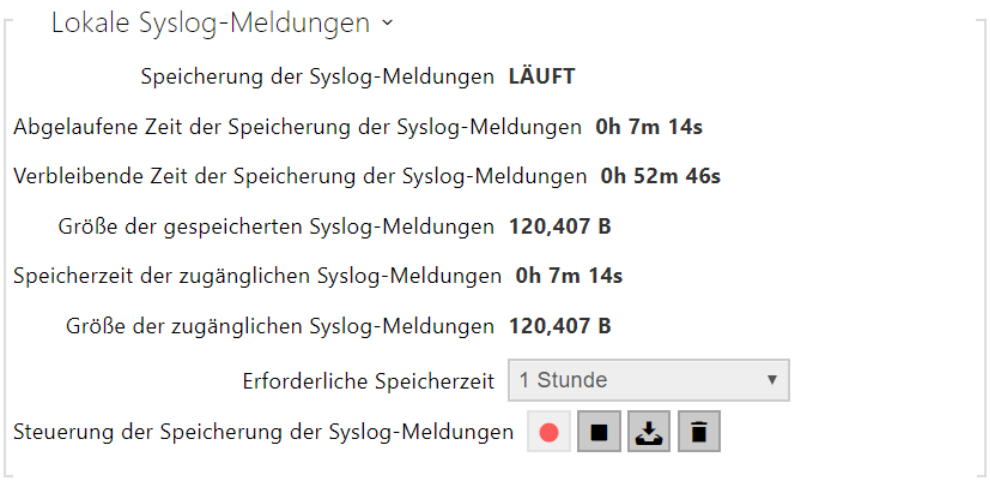
Mit der Taste  können Sie die Fernaufnahme starten. Es ist notwendig, die Zeit (s) anzugeben, während der ein- und ausgehende Pakete erfasst werden sollen. Nach Ablauf des eingestellten Zeitwerts wird die Datei mit den erfassten Paketen automatisch auf den PC des Benutzers heruntergeladen. Sie können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

Registerkarte Syslog

2N IP Interkom 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 Interkombetrieb muss man diese Leistung nicht konfigurieren.

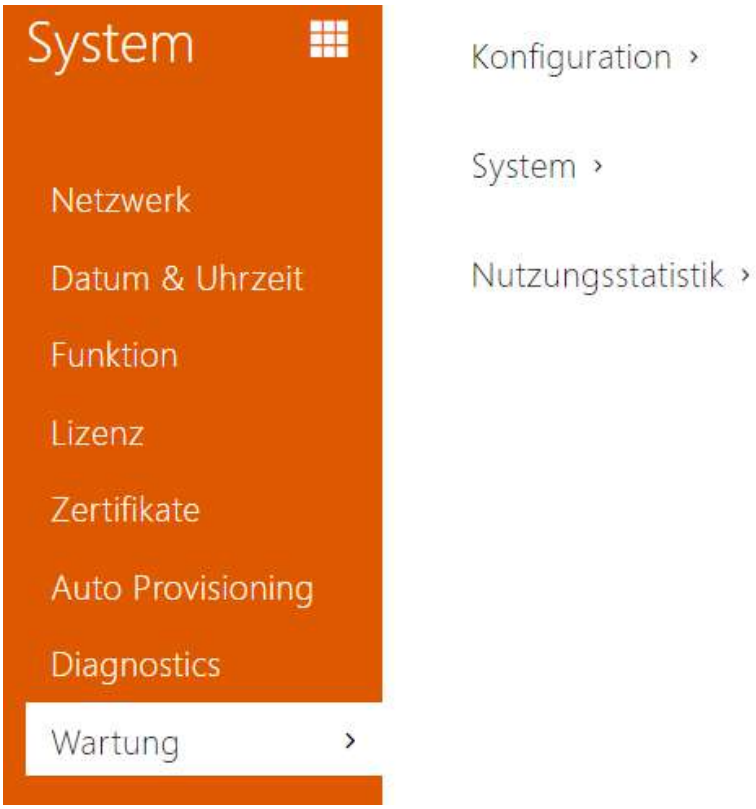


- **Syslog-Meldung schicken** – erlaubt das Absenden von Systemnachrichten an den Syslog-Server. Für die richtige Funktion muss die gültige Serveradresse eingestellt sein.
- **Server-Adresse** – legen Sie die IP[:Port] oder MAC-Adresse des Servers fest, auf dem die Anwendung läuft, um Syslog-Nachrichten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

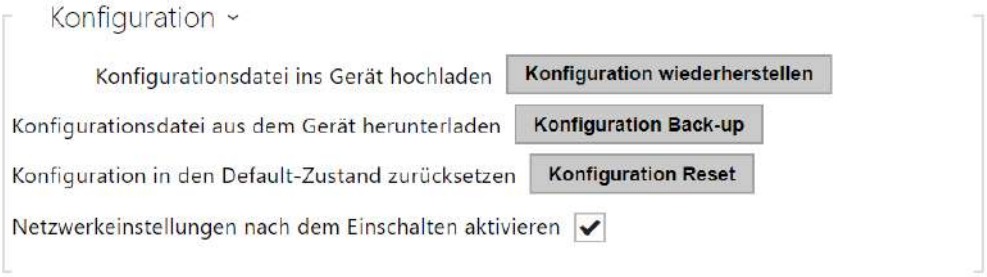


Allgemeine Übersicht der lokalen Syslog-Nachrichten.

5.6.8 Wartung



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



- **Konfiguration wiederherstellen** – dient der Wiederherstellung der Konfiguration aus der vorherigen Sicherheitskopie. Nach dem Drücken der Taste zeigt sich ein Dialogfenster in dem Sie die Datei mit der Konfiguration wählen und sie 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** – dient der Erstellung einer Sicherheitskopie der aktuellen kompletten Konfiguration des Interkoms. Nach dem Drücken der Taste kommt es zum Herunterladen der kompletten Konfiguration, die Sie in Ihrem PC speichern können.

Hinweis

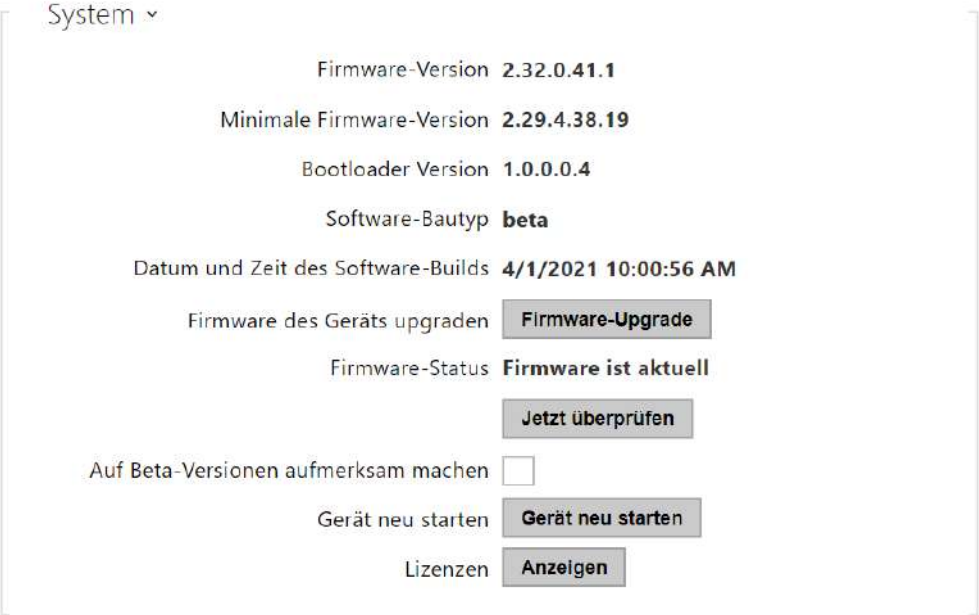
- *Die Interkomkonfiguration kann empfindliche Daten, wie die Telefonnummern der Nutzer und die Zutrittspasswörter enthalten, gehen Sie deshalb mit der Datei umsichtig um.*

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

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.*

- **Konfiguration in den Default-Zustand zurücksetzen** – erlaubt die Möglichkeit des Zurücksetzens der Netzparameter in die Voreinstellung mittels des Drückens der Reihenfolge der Kurzwahltasten nach dem Interkomneustart so, wie es im Kapitel Konfiguration im Installationshandbuch des jeweiligen Modells angeführt ist.



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 das Interkom. Nach dem Drücken der Taste erscheint ein Dialogfenster, in dem Sie die Datei mit der Firmware wählen können, die für Ihr Interkom bestimmt ist. Nach dem erfolgreichen Upload der Firmware startet das Interkom automatisch neu. 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 Ihr Interkom 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.

Warnung

- Firmware-Downgrades auf Geräten mit Artpec-Prozessor führen zu einem Werksreset, bei dem die gesamte Konfiguration, einschließlich der Lizenzschlüssel, verloren geht. Wir empfehlen Ihnen, Ihre Konfiguration zu sichern und den gültigen Lizenzschlüssel zu speichern, bevor Sie ein Downgrade durchführen.

- **Jetzt überprüfen** – dient der online Überprüfung, ob eine neuere Firmware verfügbar ist. Falls eine neue Firmware verfügbar ist, wird die Möglichkeit ihres Herunterladens mit nachfolgendem automatischem Upgrade der Anlage angeboten.
- **Gerät neu starten** – führt den Interkomneustart durch. Der ganze Neustartprozess dauert ungefähr 30 s. Nach dem Ende des Neustarts und dem Eingang der IP Adresse für das Interkom, 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.

- **Anzeigen** – 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.

5.7 Verwendete Ports

Leistung	Port	Protokoll	Richtung	Standardmäßig eingeschaltet	Einstellbar	Einstellung
802.1x	–	–	In/Out	Nein	Nein	–
DHCP	68	UDP	In/Out	Ja	Nein	–
DNS	53	TCP/ UDP	In/Out	Ja	Nein	–
Echo (device discovery)*	8002	UDP	In/Out	Ja	Nein	–
FTP	21	TCP	Out	Nein	Nein	–
2N IP Eye	8003	UDP	Out	Nein	Nein	–
HTTP	80	TCP	In/Out	Ja	Ja	5.4.8 Web server
HTTPS	443	TCP	In/Out	Ja	Ja	5.4.8 Web server
Multicast audio	22222	UDP	Out	Nein	Ja	5.4.2 Streamování
Multicast audio for ICU protocol	8006	UDP	Out	Ja	Nein	–
Multicast video for ICU protocol	8008	UDP	Out	Ja	Nein	–
Multicast video (wide) for ICU protocol	8016	UDP	In/Out	Ja	Nein	–
NTP client	123	UDP	In/Out	Ja	Nein	–
ONVIF	80, 443, 3702	TCP/ UDP	In/Out	Nein	Nein	–

Leistung	Port	Protokoll	Richtung	Standardmäßig eingeschaltet	Einstellbar	Einstellung
RTP+RTCP ports (SIP)	4900+ (range of 64 ports)	UDP	In/Out	Nein	Ja	5.4.1 Telefon
RTP+RTCP ports (External camera)	4800+ (range of 64 ports)	UDP	In/Out	Nein	Ja	5.4.2 Streamování
RTSP client	554	UDP	In/Out	Nein	Ja	5.4.1 Telefon
RTSP server	554	UDP	In/Out	Nein	Nein	–
SingleWire Commands	80	TCP	In/Out	Ja	Nein	–
SingleWire Communication	8081	TCP	Out	Ja	Nein	–
SLP	427	UDP	In/Out	Ja	Nein	–
SingleWire Media	20000+	UDP	In	Ja	Nein	–
SIP	5060, 5062	TCP/ UDP	In/Out	Nein	Ja	5.4.1 Telefon
SIPS	5061	TCP	In/Out	Nein	Ja	5.4.1 Telefon
SMTP	25	TCP	Out	Nein	Ja	5.4.3 E-Mail
Syslog	514	UDP	Out	Nein	Nein	–
TFTP	69	UDP	Out	Ja	Nein	–
My2N Knocker	443	TCP	Out	Ja	Nein	–
My2N Tribble Tunnel	443	TCP	Out	Ja	Nein	–

Leistung	Port	Protokoll	Richtung	Standardmäßig eingeschaltet	Einstellbar	Einstellung
SNMP Agent	161	UDP	In/Out	Ja	Nein	–
SNMP Trap	162	UDP	Out	Ja	Nein	–
SSDP	1900	UDP	In/Out	Ja	Nein	–
SDDP	1902	UDP	In/Out	Ja	Nein	–
Multicast receiver (Automation)	4433	UDP	In	Nein	Nein	–
WS-Discovery	3702	UDP	In/Out	Ja	Nein	–
CIP Client (Crestron)	41794	UDP	In/Out	Nein	Nein	–
Sitechannel (ICU protocol)	8004	UDP	In/Out	Ja	Nein	–

Echo – proprietäres Protokoll für das Suchen der Interkoms im Netz. Bestandteil der Produkte **2N® IP Network Scanner**, **2N® IP Eye**, **2N® Access Commander**.

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® IP Interkom steht in Übereinstimmung mit folgenden Richtlinien und Bestimmungen:

- 2014/35/EU über die Bereitstellung elektrischer Betriebsmittel zur Verwendung innerhalb bestimmter Spannungsgrenzen
- 2014/30/EU über die elektromagnetische Verträglichkeit
- 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 B entspricht den Anforderungen des kanadischen Standards ICES/ NMB-003.

FCC

Dieses Gerät wurde gemäß den Anforderungen für ein digitales Gerät der Klasse B, 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.