TVHS30000

Ⓓ Bedienungsanleitung Software

Version 06/2023

(D)	**Diese Bedienungsanleitung enthält wichtige Hinweise zur Inbetriebnahme und Handhabung.** **Achten Sie hierauf, auch wenn Sie dieses Produkt an Dritte weitergeben.** **Heben Sie deshalb diese Bedienungsanleitung zum Nachlesen auf!** Eine Auflistung der Inhalte finden Sie im Inhaltsverzeichnis mit Angabe der entsprechenden Seitenzahlen auf **Seite 8**.

TVHS30000

Bedienungsanleitung

Version 06/2023

Originalbedienungsanleitung in deutscher Sprache. Für künftige Verwendung aufbewahren!

Einführung

Sehr geehrte Kundin, sehr geehrter Kunde,

wir bedanken uns für den Kauf dieses Produkts.

Hiermit erklärt ABUS Security-Center, dass das Gerät der RED-Richtlinie 2014/53/EU entspricht. Das Gerät erfüllt zudem die Anforderungen der folgenden EU-Richtlinien: EMV Richtlinie 2014/30/EU sowie RoHS Richtlinie 2011/65/EU. Der vollständige Text der EU-Konformitätserklärung ist unter der folgenden Internetadresse verfügbar: www.abus.com/TVHS30000

Um diesen Zustand zu erhalten und einen gefahrenlosen Betrieb sicherzustellen, müssen Sie als Anwender diese Bedienungsanleitung beachten!

Lesen Sie sich vor Inbetriebnahme des Produkts die komplette Bedienungsanleitung durch, beachten Sie alle Bedienungs- und Sicherheitshinweise!

Bei Fragen wenden Sie sich an ihren Facherrichter oder Fachhandelspartner!

Haftungsausschluss

Diese Bedienungsanleitung wurde mit größter Sorgfalt erstellt. Sollten Ihnen dennoch Auslassungen oder Ungenauigkeiten auffallen, so teilen Sie uns diese bitte schriftlich unter der auf der Rückseite des Handbuchs angegebenen Adresse mit.
Die ABUS Security-Center GmbH & Co. KG übernimmt keinerlei Haftung für technische und typographische Fehler und behält sich das Recht vor, jederzeit ohne vorherige Ankündigung Änderungen am Produkt und an den Bedienungsanleitungen vorzunehmen.
ABUS Security-Center ist nicht für direkte und indirekte Folgeschäden haftbar oder verantwortlich, die in Verbindung mit der Ausstattung, der Leistung und dem Einsatz dieses Produkts entstehen. Es wird keinerlei Garantie für den Inhalt dieses Dokuments übernommen.

Symbolerklärung

	**Das Symbol mit dem Blitz im Dreieck wird verwendet, wenn Gefahr für die Gesundheit besteht, z.B. durch elektrischen Schlag.**
	**Ein im Dreieck befindliches Ausrufezeichen weist auf wichtige Hinweise in dieser Bedienungsanleitung hin, die unbedingt zu beachten sind.**
	**Dieses Symbol ist zu finden, wenn Ihnen besondere Tipps und Hinweise zur Bedienung gegeben werden sollen.**

Wichtige Sicherheitshinweise

	**Bei Schäden die durch Nichtbeachten dieser Bedienungsanleitung verursacht werden, erlischt der Garantieanspruch. Für Folgeschäden übernehmen wir keine Haftung!**
	**Bei Sach- oder Personenschäden, die durch unsachgemäße Handhabung oder Nichtbeachten der Sicherheitshinweise verursacht werden, übernehmen wir keine Haftung. In solchen Fällen erlischt jeder Garantieanspruch!**

Sehr geehrte Kundin, sehr geehrter Kunde, die folgenden Sicherheits- und Gefahrenhinweise dienen nicht nur zum Schutz Ihrer Gesundheit, sondern auch zum Schutz des Geräts. Lesen Sie sich bitte die folgenden Punkte aufmerksam durch:

- Es sind keine zu wartenden Teile im Inneren des Produktes. Außerdem erlischt durch das Zerlegen die Zulassung (CE) und die Garantie/Gewährleistung.
- Durch den Fall aus bereits geringer Höhe kann das Produkt beschädigt werden.
- Montieren Sie das Produkt so, dass direkte Sonneneinstrahlung nicht auf den Bildaufnehmer des Gerätes fallen kann. Beachten Sie die Montagehinweise in dem entsprechenden Kapitel dieser Bedienungsanleitung.
- Das Gerät ist für den Einsatz im Innen- und Außenbereich (IP66) konzipiert.

Vermeiden Sie folgende widrige Umgebungsbedingungen bei Betrieb:

- Nässe oder zu hohe Luftfeuchtigkeit
- Extreme Kälte oder Hitze
- Direkte Sonneneinstrahlung
- Staub oder brennbare Gase, Dämpfe oder Lösungsmittel
- starke Vibrationen
- starke Magnetfelder, wie in der Nähe von Maschinen oder Lautsprechern.
- Die Kamera darf nicht auf unbeständigen Flächen installiert werden.

Allgemeine Sicherheitshinweise:

- Lassen Sie das Verpackungsmaterial nicht achtlos liegen! Plastikfolien/-tüten, Styroporteile usw., könnten für Kinder zu einem gefährlichen Spielzeug werden.
- Die Videoüberwachungskamera darf aufgrund verschluckbarer Kleinteile aus Sicherheitsgründen nicht in Kinderhand gegeben werden.
- Bitte führen Sie keine Gegenstände durch die Öffnungen in das Geräteinnere
- Verwenden Sie nur die vom Hersteller angegebenen Zusatzgeräte/Zubehörteile. Schließen Sie keine nicht kompatiblen Produkte an.
- Bitte Sicherheitshinweise und Bedienungsanleitungen der übrigen angeschlossenen Geräte beachten.
- Überprüfen Sie vor Inbetriebnahme das Gerät auf Beschädigungen, sollte dies der Fall sein, bitte das Gerät nicht in Betrieb nehmen!
- Halten Sie die Grenzen der in den technischen Daten angegebenen Betriebsspannung ein. Höhere Spannungen können das Gerät zerstören und ihre Sicherheit gefährden (elektrischer Schlag).

Sicherheitshinweise

1. Stromversorgung: Achten Sie auf die auf dem Typenschild angegebenen Angaben für die Versorgungsspannung und den Stromverbrauch.

2. Überlastung
Vermeiden Sie die Überlastung von Netzsteckdosen, Verlängerungskabeln und Adaptern, da dies zu einem Brand oder einem Stromschlag führen kann.

3. Reinigung
Reinigen Sie das Gerät nur mit einem feuchten Tuch ohne scharfe Reinigungsmittel.
Das Gerät ist dabei vom Netz zu trennen.

Warnungen

Vor der ersten Inbetriebnahme sind alle Sicherheits- und Bedienhinweise zu beachten!

1. Beachten Sie die folgenden Hinweise, um Schäden an Netzkabel und Netzstecker zu vermeiden:

- Wenn Sie das Gerät vom Netz trennen, ziehen Sie nicht am Netzkabel, sondern fassen Sie den Stecker an.
- Achten Sie darauf, dass das Netzkabel so weit wie möglich von Heizgeräten entfernt ist, um zu verhindern, dass die Kunststoffummantelung schmilzt.

2. Befolgen Sie diese Anweisungen. Bei Nichtbeachtung kann es zu einem elektrischen Schlag kommen:

- Öffnen Sie niemals das Gehäuse oder das Netzteil.
- Stecken Sie keine metallenen oder feuergefährlichen Gegenstände in das Geräteinnere.
- Um Beschädigungen durch Überspannungen (Beispiel Gewitter) zu vermeiden, verwenden Sie bitte einen Überspannungsschutz.

3. Bitte trennen Sie defekte Geräte sofort vom Stromnetz und informieren Ihren Fachhändler.

	Vergewissern Sie sich bei Installation in einer vorhandenen Videoüberwachungsanlage, dass alle Geräte von Netz- und Niederspannungsstromkreis getrennt sind.
	Nehmen Sie im Zweifelsfall die Montage, Installation und Verkabelung nicht selbst vor, sondern überlassen Sie dies einem Fachmann. Unsachgemäße und laienhafte Arbeiten am Stromnetz oder an den Hausinstallationen stellen nicht nur Gefahr für Sie selbst dar, sondern auch für andere Personen. Verkabeln Sie die Installationen so, dass Netz- und Niederspannungskreise stets getrennt verlaufen und an keiner Stelle miteinander verbunden sind oder durch einen Defekt verbunden werden können.

Auspacken

Während Sie das Gerät auspacken, handhaben sie dieses mit äußerster Sorgfalt.

	Bei einer eventuellen Beschädigung der Originalverpackung, prüfen Sie zunächst das Gerät. Falls das Gerät Beschädigungen aufweist, senden Sie dieses mit Verpackung zurück und informieren Sie den Lieferdienst.

Inhaltsverzeichnis

1. Bestimmungsgemäße Verwendung

Das FaceXess Gerät dient im Innen- bzw. Außenbereich als Zutrittskontrollsystem mit Gesichtserkennung kombiniert mit einer Video-Tür-Kommunkationanlage.

Eine andere Verwendung als oben beschrieben kann zur Beschädigung des Produkts führen, außerdem bestehen weitere Gefahren. Jeder andere Einsatz ist nicht bestimmungsgemäß und führt zum Verlust der Garantie bzw. Gewährleistung; sämtliche Haftung wird ausgeschlossen. Dies gilt auch, wenn Umbauten und/oder Veränderungen am Produkt vorgenommen wurden.
Lesen Sie sich die Bedienungsanleitung vollständig und aufmerksam durch, bevor Sie das Produkt in Betrieb nehmen. Die Bedienungsanleitung enthält wichtige Informationen für Montage und Bedienung.

2. Symbolerklärung

	Das Symbol mit dem Blitz im Dreieck wird verwendet, wenn Gefahr für die Gesundheit besteht, z. B. durch elektrischen Schlag.
	Ein im Dreieck befindliches Ausrufezeichen weist auf wichtige Hinweise in dieser Bedienungsanleitung hin, die unbedingt zu beachten sind.
	Dieses Symbol ist zu finden, wenn Ihnen besondere Tipps und Hinweise zur Bedienung gegeben werden sollen.

3. Merkmale und Funktionen

Türsprechanlage mit Touchscreen, Kamera & Gesichtserkennung für interaktionslosen Zutritt.

Die Türstation identifiziert berechtigte Personen mit intelligenter Gesichtserkennung und entriegelt die Eingangstür automatisch. Damit bietet das Video-Türsprechsystem einen bequemen, interaktionslosen Zugang, berührungslos und ohne Chipkarte oder andere Identmedien. Der Erkennungsbereich ist flexibel einstellbar, der Gesichtsscan auf bis zu 3 m Entfernung dauert nur Bruchteile einer Sekunde.

Eine fast ganz normale Klingel

Eben nur fast: Denn das FaceXess Display kann individuell gestaltet werden, z. B. mit Haus-Nr., Adresse, Wunschmotiven usw.

Sicher und individuell

Die Dual-Kamera (optisch, IR) erkennt zuverlässig, ob eine Person eintreten darf oder nicht – ob bei Gegenlicht, Dunkelheit oder wenn die Person Mütze oder Maske trägt. Die Anti-Spoofing-Funktion prüft anhand diverser Merkmale, ob es sich um eine echte und berechtigte Person handelt, oder eine Manipulation, z. B. durch Davorhalten von Fotos oder Videos.In sensiblen Bereichen ist oft eine 2-Faktor-Autentifzierung gefragt. So kann die Gesichtserkennung auch mit PIN-Code oder Chipkarte kombiniert werden. Die Nutzerdaten (Gesichter) werden lokal und verschlüsselt auf dem Gerät gespeichert. Unbekannte Personen werden nicht erfasst.

Sehen, Sprechen, Öffnen

ABUS FaceXess ist einfach intuitiv zu bedienen. Das 7-Zoll-Touch-Display mit virtueller Klingeltaste ist die Bedienoberfläche der Türstation. Auf dem Smartphone (ABUS Link Station-App) oder dem optionalen Innenmonitor sieht man, wer vor der Tür steht, spricht mit der Person und schaltet den E-Türöffner. Bis zu 3 Wohnparteien können angelegt werden (je 6 Monitore). Das Außenterminal kann auch stand-alone als reiner Türöffner verwendet werden.

- IP-Video-Türsprechanlage mit Gesichtserkennung, entriegelt eingelernten Personen vollautomatisch, in Bruchteilen einer Sekunde, die Haustür. Optional: Zutritt per PIN-Code oder Chipschlüssel/Schlüsselkarte am integrierten NFC-Kartenleser.

- Zutritt für eingelernte Nutzer am 7‘‘Touchscreen per Gesichts-Scan oder PIN-Code-Eingabe. Unbekannte Personen nutzen die virtuelle Klingeltaste auf dem Display.

- Sehen, wer vor der Tür steht: Live-Bild, Gegensprechen und Türöffnen per Innenmonitor oder Link Station-App, auch von unterwegs. Top-Bildqualität und -Kontraste dank 2 MPx Dual-Kamera.

- Gute Sprachqualität dank hochwertigem Mikrofon und Lautsprecher mit Geräuschunterdrückung (Noice-Cancellation: keine Störgeräusche, keine Echos).

- Sicherer Zutritt, hoher Manipulationsschutz: Terminal ist nicht mit Foto/Video zu überlisten (Anti-Spoofing-Technologie). Optional: 2-Faktor-Authentifizierung kombiniert Gesichtserkennung mit PIN-Code/Schlüsselkarte.

- Für bis zu 3 Wohnparteien: je Klingelpartei sind bis zu 6 Monitore via LAN/PoE oder WLAN (Wi-Fi) integrierbar

- Schnell und sicher installiert: Die Türstation benötig eine externe Stromversorgung. Die Datenanbindung erfolgt über LAN/WAN und eine Datenleitung (2 Adern) zum abgesetzten Schaltmodul, das den Tür-Aktor ansteuert.

- Wetterfestes Terminal für den Außenbereich (Schutzart IP65)

- Ganz ohne Schlüssel: nie mehr wegen vergessenen Schlüsseln vor verschlossener Haustür stehen

4. Gerätebeschreibung

Weitere Informationen zu Anschlüssen und dem korrekten Verbau des Gesichtserkennungs-Terminals finden Sie in der Installationsanleitung, verfügbar unter www.abus.com .

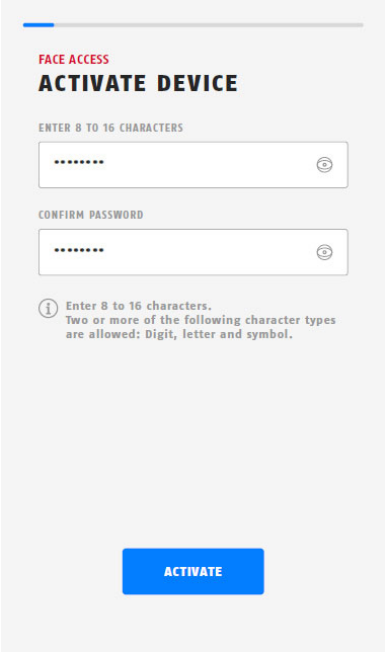
5. Beschreibung der Anschlüsse

Weitere Informationen zu Anschlüssen und dem korrekten Verbau des Gesichtserkennungs-Terminals finden Sie in der Installationsanleitung, verfügbar unter www.abus.com .

6. Erstinbetriebnahme

6.1 Aktivierung des Gerätes über den lokalen Touch Monitor

Nach Start des Gerätes erscheint die Eingabemaske zur Vergabe des Gerätepassworts.



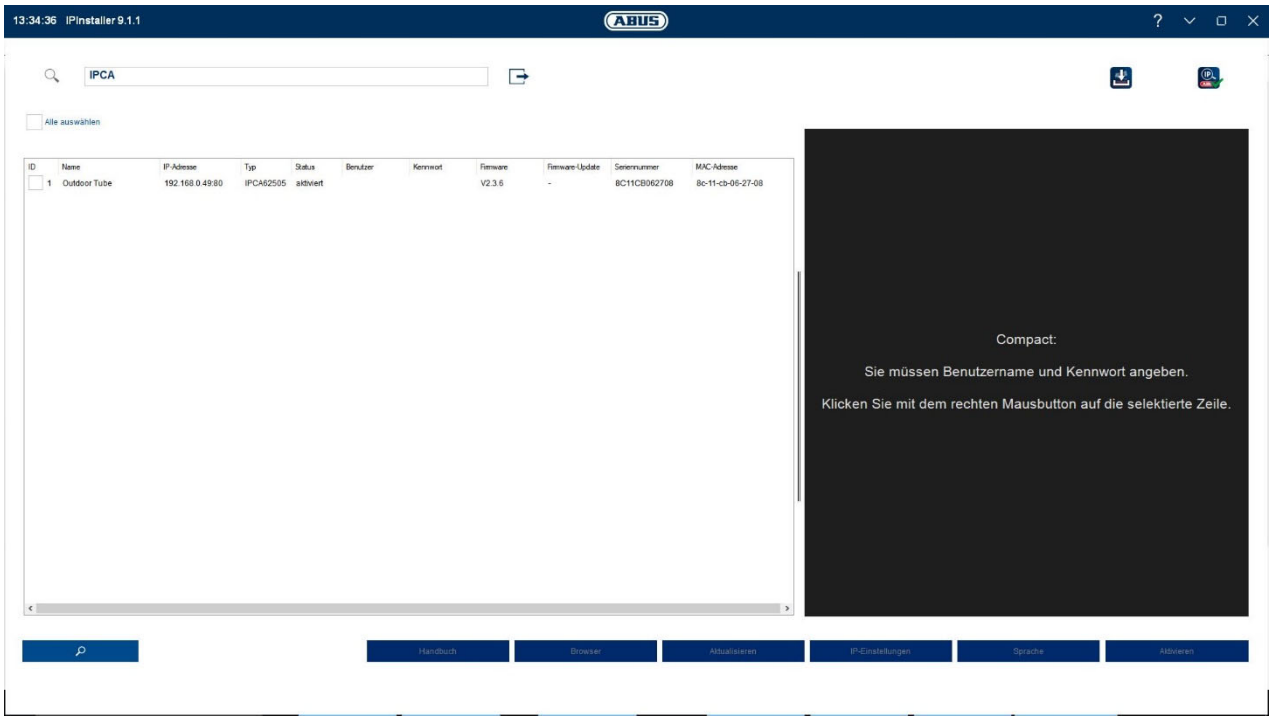
Ein sicheres Kennwort muss mindestens folgende Anforderungen erfüllen:
- 8-16 Zeichen
- Gültige Zeichen: Zahlen, Kleinbuchstaben, Großbuchstaben, Sonderzeichen (!“#$%&()*+,-./:;<=>?@[\]^_{|}~Leerzeichen)
- 2 verschiedene Arten von Zeichen müssen verwendet werden

6.2 Aktivierung des Gerätes über den ABUS IP Installer

Für diesen Weg der Aktivierung muss das Gerät zunächst in das IP Netzwerk eingebunden werden. Dies geschieht über den verdrahteten Netzwerkanschluss (LAN Anschluss). Die Vergabe der IP Adresse erfolgt autmatisch über das DHCP Protokoll.

Installieren und starten Sie den ABUS IP Installer. Dieser ist über die ABUS Web-Seite www.abus.com beim jeweiligen Produkt verfügbar.

Über die Taste „Aktivieren“ kann das Gerätepasswort vergeben werden.

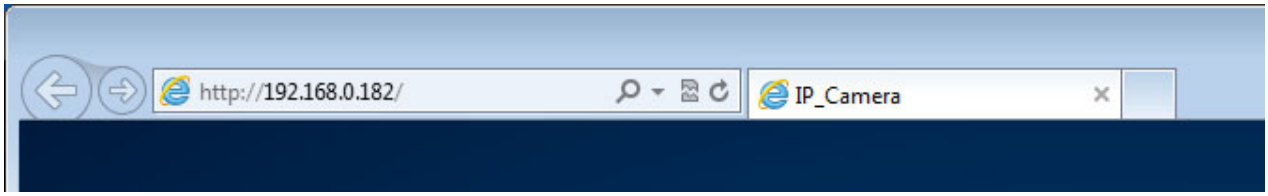


6.3 Aktivierung des Gerätes über den Web-Browser

Für diesen Weg der Aktivierung muss das Gerät zunächst in das IP Netzwerk eingebunden werden. Dies geschieht über den verdrahteten Netzwerkanschluss (LAN Anschluss). Die Vergabe der IP Adresse erfolgt autmatisch über das DHCP Protokoll.

Die IP Adresse, welche das Gerät vom DHCP Server zugewiesen bekommen hat, können sie über den ABUS IP Installer einsehen.

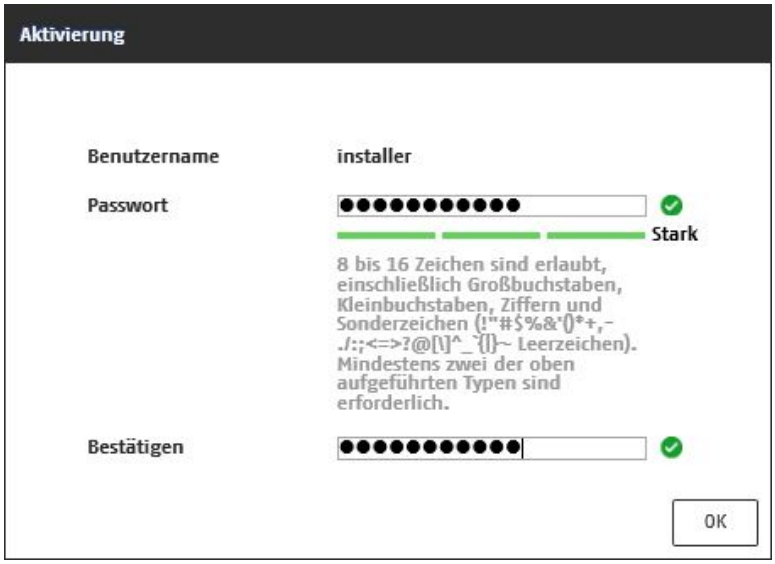
Geben Sie die IP Adresse des Gerätes in die Adressleiste des Browsers ein. Nun können Sie die Erstpasswortvergabe vornehmen.



Aus IT-Sicherheitsgründen wird gefordert ein sicheres Kennwort mit entsprechender Verwendung von Kleinbuchstaben, Großbuchtstaben, Zahlen und Sonderzeichen zu verwenden.

Ab Werk ist kein Kennwort vergeben, dies muss bei der ersten Verwendung des Gerätes vergeben werden. Dies kann über den ABUS IP-Installer (Schaltfläche „Aktivieren“) oder über die Web-Seite geschehen.

Ein sicheres Kennwort muss mindestens folgende Anforderungen erfüllen:
- 8-16 Zeichen
- Gültige Zeichen: Zahlen, Kleinbuchstaben, Großbuchstaben, Sonderzeichen (!“#$%&()*+,-./:;<=>?@[\]^_{|}~Leerzeichen)
- 2 verschiedene Arten von Zeichen müssen verwendet werden



6.4 Video-Plugin installieren

Für die Installation der Video-Plugins benötigen Sie entsprechende Rechte am PC.

Edge (Internet Explorer Modus) / Internet Explorer

Für die Videodarstellung im Internet-Explorer wird ein sogenanntes ActiveX Plugin verwendet. Dieses Plugin muss im Browser installiert werden. Eine Entsprechende Abfrage für die installation erscheint direkt nach Eingabe von Benutzername und Passwort.

	Falls die Installation des ActiveX Plugins im Internet Explorer geblockt wird, so ist es nötig die Sicherheitseinstellungen für die ActiveX Installation/Initialisierung zu reduzieren.

Google Chrome / Microsoft Edge

Für die Videodarstellung in diesen Browsern wird ein weiteres Video-Plugin benötigt. Falls das Plugin im PC fehlt, so wird dieses Plugin zum Download und zur Installation auf dem PC angeboten (nach Login in die Webseite, Link in der Mitte der Live-Ansicht).

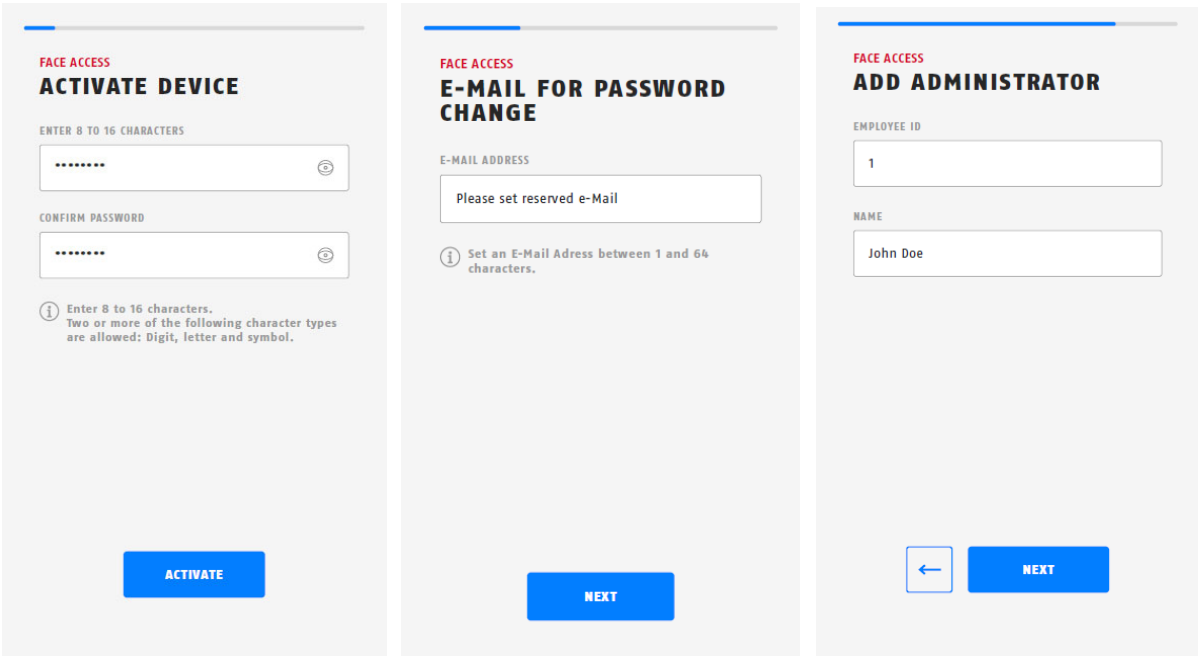
 Eine Firmwareaktualisierung über das Web-Interface ist nur mit installiertem Video-Plugin möglich.

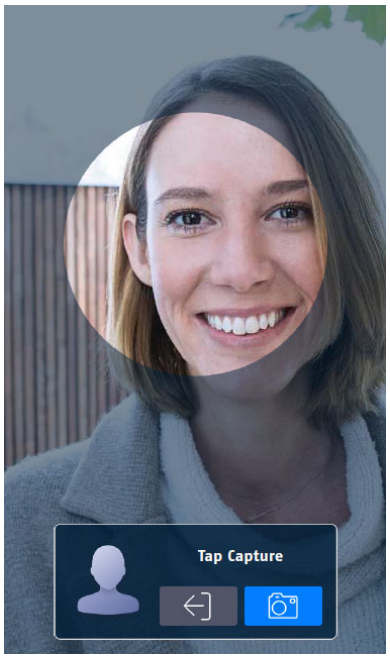
7. Konfiguration und Bedienung über den Touch Monitor

Die Bedienung und Konfiguration des Gesichtserkennungs-Terminals kann direkt über das Anzeigegerät per Berührungssteuerung erfolgen (im Folgenden „Touch-Display“).

7.1 Einrichtungs-Assistent

Der Einrichtungsassistent führt Sie Schritt für Schritt durch die wichtigsten Menüpunkte, um das Gerät für die grundlegende Funktion bereit zu machen. Lesen Sie die Anweisungen im Display, füllen Sie die entsprechenden Felder aus, und schließen Sie alle Schritte des Assistenten ab.





(Beispielbilder der Schritte des Einrichtungsassistenten)

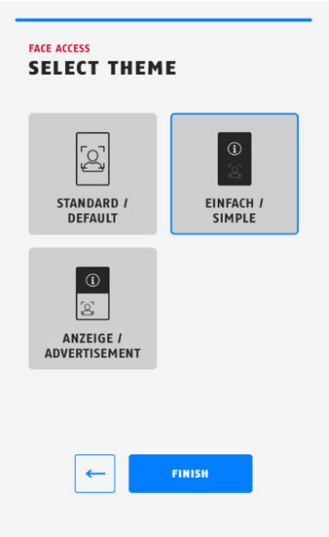
7.2 Hauptbedienseite

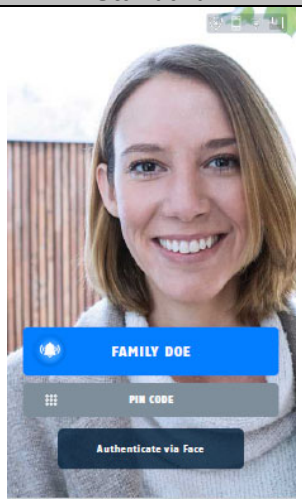
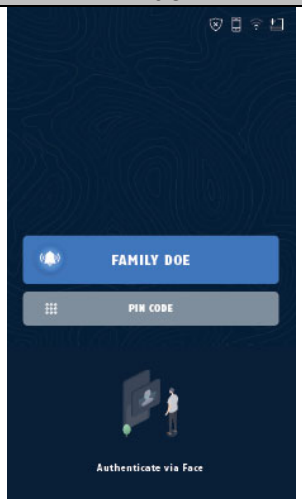
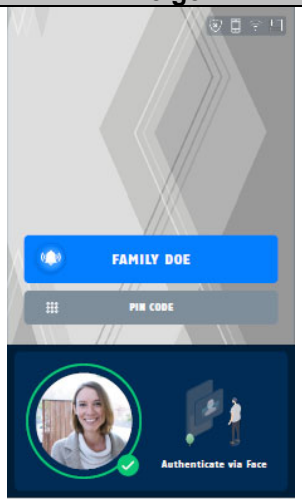
7.2.1 Ansichtoptionen (Themen)

Standard: Es werden bei Konfiguration nur Ruftaste(n), Pin-Code und QR-Code Taste angezeigt, sowie bei Wunsch das Vorschauvideo der Person.

Einfach: Es werden bei Konfiguration nur Ruftaste(n), Pin-Code und QR-Code Taste angezeigt. Das Vorschauvideo wird nicht angezeigt. Die Gesichtserkennung im Hintergrund aktiv.

Information: Der Unterschied zum Standardmodus ist, dass im oberen Bereich des Displays Platz für die Anzeige von Informationen ist.



Standard	Einfach	Anzeige
		
		

7.2.2. Symbole und Informationsanzeigen

In der rechten oberen Ecke der Hauptansicht im Display befinden sich vier Symbole mit folgenden Informationen.

Symbol	Funktion
	Anzeige der aktiven Verbingung zur ABUS Link Station Cloud bzw. aktiver Verbindung zu einem ABUS Link Station Account. Symbol: Verbindung zur Cloud erfolgreich, Verknüpfung zu Account erfolgreich Symbol mit „X“: Keine Verbindung zur Cloud Symbol mit „!“: Verbindung zur Cloud erfolgreich, keine Verknüpfung zu Account
	Anzeige der Verbindung zur einem WiFi Netzwerk. Symbol: Verbindung zu WiFi Netzwerk erfolgreich Symbol mit „X“: Keine Verbindung zu einem WiFi Netzwerk
	Anzeige der Verbindung zu einem kabelgebundenen Netzwerk (LAN). Symbol: Verbindung zu Netzwerk erfolgreich Symbol mit „X“: Keine Verbindung zu einem Netzwerk
	Dieses Icon ist aktuell nicht in Verwendung und hat keine Funktion.

7.2.3 Einstellbare Bedientasten

Am lokalen Display könnten verschiedene Bedientasten aktiviert werden.

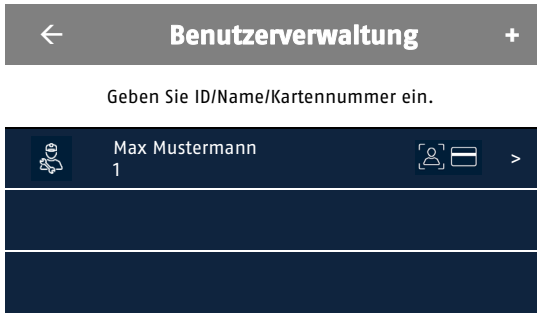
Taste	Funktion
	Klingeltaste(n) für den Anruf von bis zu 3 Wohnungen
	Öffnen der Eingabemaske für den Pincode.
	Öffnen der Maske für das Vorzeigen eines QR Codes.

7.3 Administrator-Menü

7.3.1 Benutzer

In der Einstellungsseite Benutzerverwaltung werden alle eingerichteten Benutzer angezeigt.

Jede Zeile gibt Auskunft über Nutzername, ID, Benutzertyp und welche Medien für den jeweiligen Benutzer eingerichtet sind.



 Wenn dieses Zeichen for dem Benutzernamen angezeigt wird, so hat dieser Benutzer Administratorrechte. Dieser Benutzer kann Einstellungen im Konfigurationsmenü vornehmen, und z.B. weitere Benutzer einrichten.

 Wenn diese Symbole weiß dargestellt sind, dann sind für den Benutzer ein Gesicht für die Gesichtserkennung bzw. mindestens eine Chipkarte für die Authentifizierung eingerichtet.

 Durch Drücken dieses Pfeilsymbols können die Eigenschaften, Medien und Berechtigungen eines eingerichteten Benutzers konfiguriert werden.

 Drücken Drücken des Plus-Symbols können weitere Benutzer eingerichtet werden.

Über das Eingabefeld kann nach Benutzern in der Liste gesucht werden

 Durch Drücken dieses Pfeilsymbols kann das Menü verlassen werden.

Mitarbeiter ID:
Vergabe einer individuellen Identifikationsnummer. Länge 1 – 32 Zeichen. Kombination aus Kleinbuchstaben, Großbuchstaben oder Ziffern.

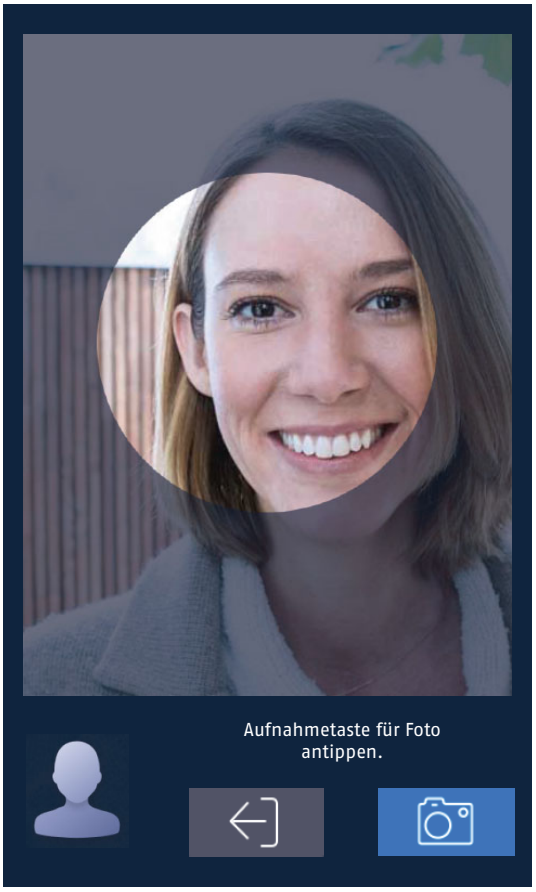
Name:
Vergabe eines Namens. Länge 1 – 128 Zeichen (Empfehlung: max. 24 Zeichen). Kombination aus Kleinbuchstaben, Großbuchstaben, Ziffern oder Sonderzeichen (.,#?!@%^$Leerzeichen*()\&/-_=[]+;:“ˆ`~|<>{})

Gesicht:
Speicherung eines Gesichtsbildes für den Benutzer. Die Person muss in Richtung des Gesichtserkennungsterminal schauen, und das Gesicht muss sich im hell markierten Kreis befinden (siehe Grafik unten rechts).

Der Administrator muss den Benutzer in Kenntnis darüber setzten, dass sein Gesichtsbild im Gerät gespeichet und verarbeitet wird. Auf die Verarbeitung des Gesichtsbildes wird ebefalls im Punkt Datenschutz hingewiesen.

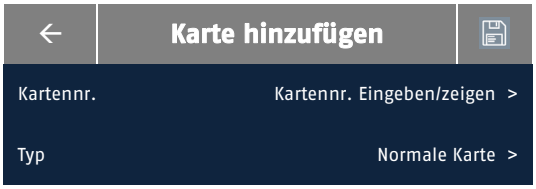
Speicherung des Bildes. Es dauert ca. 3 Sekunden, bis das Geisicht erfolgreich analysiert und erfasst wurde. Bestätigen Sie die Speicherung anschließend und verlassen Sie diesen Menüpunkt (grüner Haken).

Verlassen des Menüs, ohne ein Bild zu speichern.



Karte:
Jedem Benutzer können bis zu 5 Chipkarten hinzugefügt werden. Tippen Sie auf den Pfeil hinter der Zeile Karte.
Im Menü Kartenverwaltung sind alle eingelernten Karten pro Benutzer einsehbar.

Über die + Taste gelangen Sie in das Menü um Karten hinzuzufügen.
Halten Sie nun die gewünschte Karte vor das Terminal. Der Kartenleser ist im unteren Bereich verbaut. Sie können eine Kartennummer auch manuell eingeben.



Wählen Sie anschließend den Kartentyp:

Normale Karte:	Normale Verwendung
Zwangskarte:	Auch Nötigungkarte. Es erfolgt die Authentifizierung und es wird ein Nötigungsalarm an App und CMS Software verschickt.
Super-Karte:	Ein Super-Karte hat immer Zugang, auch wenn spezielle Zeitplänge für den Zugang über Karte programmiert sind (Programmierung über ABUS CMS möglich)
Patrouillen-Karte:	Dieser Kartentyp wird für Rundgänge von Gerät zu Gerät verwendet

Pin Code:
Jedem Benutzer kann ein individueller Pin Code zugewiesen werden. Die Pin Codes aller Benutzer dürfen nur jeweils ein Mal existieren.

Zur Verwendung lesen Sie bitte den Abschnitt Zutrittskontrolle.

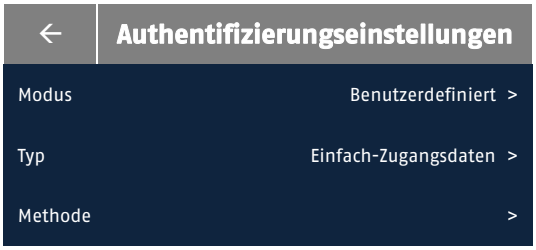
Auth. Einstellungen:
Festlegung der Art und nötigen Anzahl der Zugangsmedien für jeden Benutzer (z.B. Doppel-Verifikation über Gesicht und Pin Code).

Gerätemodus: Die Authentifizierungseinstellungen für den Benutzer folgen den allg. Einstellungen des Gerätes (Standard: Einfach-Verifikation)

Benutzerdefiniert: Individuelle Einstellung für jeden Benutzer.

Einfach-Zugangsdaten: ein Medium muss für den Zugang des Benutzers präsentiert werden (Gesicht, Pin oder Karte).

Mehrfach-Zugangsdaten: zwei Medien müssen für Zugang des Benutzers präsentiert werden (Kombination aus Gesicht, Pin oder Karte)



Benutzerrolle:
Festlegung, ob ein Benutzer Administratorrechte erhalten soll.
Ein Administrator kann lokal am Touch-Bedienteil Änderungen an der gesamten Konfiguration vornehmen (z.B. weitere Benutzer hinzufügen oder Öffnungsmedien hinzufügen).

Der Zugriff über Web-Interface oder ABUS CMS Software kann nur über das Gerätepasswort erfolgen, welches bei der Erstinbetriebnahme vergeben wurde.

7.3.2 Zutrittsoptionen

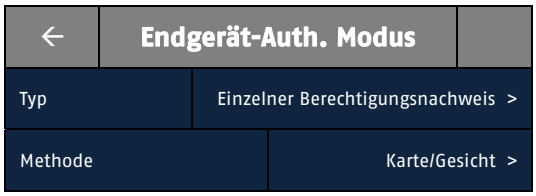
Endgerät-Authorisierungs Modus:

Festlegen der erlaubten Authentifizierungsmethoden, welche direkt im Gerät verbaut und nutzbar sind.

Typ: Einfacher Berechtigungsnachweis:
Eine einzelne Authentifizierungsmethode ist für die Identifizierung eines Benutzers notwendig.
Gesicht oder Karte oder Passwort (Pin)

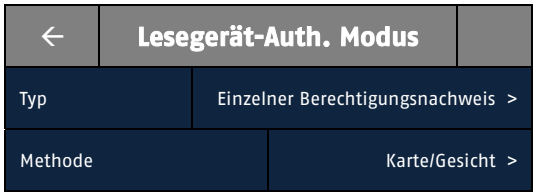
Mehrere Berechtigungsnachweise:
Zwei Authentifizierungsmethoden sind für die Identifizierung eines Benutzers notwendig.

Methode: Gesicht oder Karte
Gesicht oder Passwort (Pin)
Karte oder Passwort (Pin)



Lesegerät-Authorisierungs Modus:

Festlegen der erlaubten Authentifizierungsmethoden, welche an das Gerät angeschlossen werden können (z.B. über RS-485 oder Wiegand-Schnittstelle).



Die Konfiguration erfolgt analog zum Punkt Endgerät-Authorisierungs Modus.

NFC-Karte aktivieren:
In diesem Punkt kann die Verwendung von NFC Karten (ausser Mifare Classic) aktiviert oder deaktiviert werden.

M1-Karte aktivieren:
Bei Aktivierung können vom Typ „Mifare Classic“ (M1) verwendet werden.

Das Verfahren „Mifare Classic“ gilt als nicht sicher. Daher sollten Karten von diesem Typ nur in Kombination mit der Methode „Mehrere Berechtigungsnachweise“ (Karte+Pin oder Gesicht+Karte) verwendet werden.

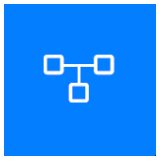
Fern-Authentifizierung:
Funktion aktuell nicht in Funktion

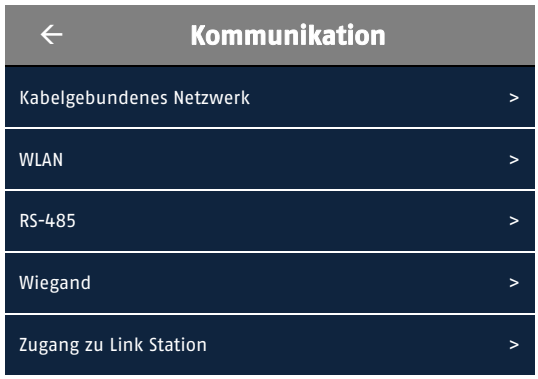
Türkontakt:
Funktion nicht verwendet

Öffnungsdauer (s):
Einstellung der Schaltdauer für das Relais (z.B. für elekt. Türöffner, Kabelbaum Bezeichnung „LOCK“)

Authentifizierungsintervall (s):
Einstellen der Zeitdauer, bevor eine neue Erkennung von Gesichtern oder Karten erfolgt.
Nach der 1. Erkennung wird diese Zeitspannung zunächst abgewartet.

7.3.3 Kommunikation





Kabelgebundenes Netzwerk

DHCP: Über die DHCP-Funktion werden alle nötigen Netzwerkeinstellungen automatisch ermittelt. Ein DHCP-Server muss sich im IP-Netzwerk befinden. DHCP ist per Standard aktiv.

IPv4-Adresse: IP Adresse im Netzwerk
IPv4-Subnetzmaske: Subnetzmaske im Netzwerk
IPv4-Gateway: IP Adresse des Routers

IPv6-Modus: Auto: Die IPv6 Verbindungsdaten werden vom DHCP Server bereitgestellt.
Manuell: manuelle Vergabe
Router Advertisement: Die IPv6 Verbindungsdaten werden vom DHCP Server (Router) in Verbindung mit dem ISP (Internet Service Provider) bereitgestellt.
IPv6-Adresse: IP Adresse im Netzwerk
Subnet-Präfix-Länge: manuelle Vergabe
IPv6-Gateway:
Router Advertisement:

DNS automat. abrufen: Die Schaltfläche ist nur vorhanden, wenn die DHCP-Funktion aktiviert ist. Die IP-Adresse eines DNS-Servers wird damit automatisch ermittelt.
Bevorzugter DNS-Server: Eingabe einer IP-Adresse eines DNS Servers.
Alternativer DNS-Server: Eingabe einer IP-Adresse eines DNS Servers.

WLAN (WiFi)

WLAN aktivieren: Aktivierung der WLAN Funktion

Bei aktivierter WLAN Schnittstelle sucht das Gerät nach sichtbaren und grundsätzlich verfügbaren WLAN Zugangspunkten (Auflistung der WLAN SSIDs).
Wählen Sie anschließend das gewünschte WLAN aus.
Sie werden nun aufgefordert das Passwort für das WLAN Netzwerk einzugeben.
Nach erfolgreicher Verbindung erfolgt die Vergabe der IP Adress automatisch per DHCP-Funktion.

RS-485
Aktivierung und Konfiguration der RS-485 Schnittstelle. Über diese Schnittstelle kann z.B. ein ABUS Sicherheitsmodul (TVAC20340) für die sichere Verbindung eines elekt. Türöffners ermöglicht werden.

Sobald die RS-485 Option „Steuergerät“ ausgewählt wurde, so muss nach Verlassen des Menüs das Terminal neu gestartet werden.
Nach dem Neustart stehen die drahtgebundenen Eingänge (Türsensor und Türtaster) sowie Ausgänge (Relais NO/NC) am Terminal selbst nicht mehr zur Verfügung.
Dannach müssen die Ein- und Ausgänge am Sicherheitsmodul verwendet werden.

Weitere RS-485 Betriebsmodi:

Zugangs-Controller:	Funktion nicht verwendet
Steuergerät:	Anschluss des Sicherheitsmoduls
Kartenleser:	Anschluss eines externen Kartenlesers per RS-485
Aufzugsmodul:	Funktion nicht verwendet

Wiegand
Das Gerät verfügt über eine Wiegand-Schnittstelle. Die Schnittstelle kann die Formate Wiegand 26 Bit oder 34 Bit verarbeiten (max. 8 bzw. 10-stellige Kartennummer, Streichung der ersten Stellen bei längeren Kartennummern).
Die Wiegand-Schnittstelle muss zunächst aktiviert werden.

Wählen Sie aus, ob die Schnittstelle als Ausgang oder Eingang funktionierten soll.

Ausgang:	Es werden Daten im Wiegand Format an einen Empfänger übertragen. Als Daten wird die Kartennummer der als erstes eingelernen Karte eines Benutzers übertragen.
Eingang:	Ein externer Kartenleser der die Kartendaten im Wiegand-Format überträgt kann angeschlossen werden.

Zugang zu Link Station

Sie ABUS Link Station Funktion bietet Zugriff über die ABUS Link Station APP.

Die Funktion muss aktiviert werden und es muss ein sog. Verifizierungs-Code vergeben werden.

In der ABUS Link Station App kann anschießend durch Scannen des QR Codes und tippen des Verifizierungs-Codes das Terminal zur App hinzugefügt werden.

Verwendbare Funktionen sind:
- Übertragung der Sabotagemeldung (Sabotagekontakt an der Rückseite des Terminals)
- Status Netwerkverbindung
- Live-Bildübertagung zur App
- Gegenspechen (2-Wege-Audio)

- Türkontakt über App schalten (Sequenz)
- Türkontakt über App schalten (dauerhaft)
- Anruffunktion von Terminal zu App über Klingeltaste im Touch-Display

Für die Anruffunktion von Terminal zu App ist folgende Einstellung nötig:

Lokales Display-Menü:	Admin-Menü / Darstellung / Schnelltaste / Anruf-App
Web-Interface:	Admin-Login / Konfiguration / Gegensprechanlage / Taste zum Anrufen / APP

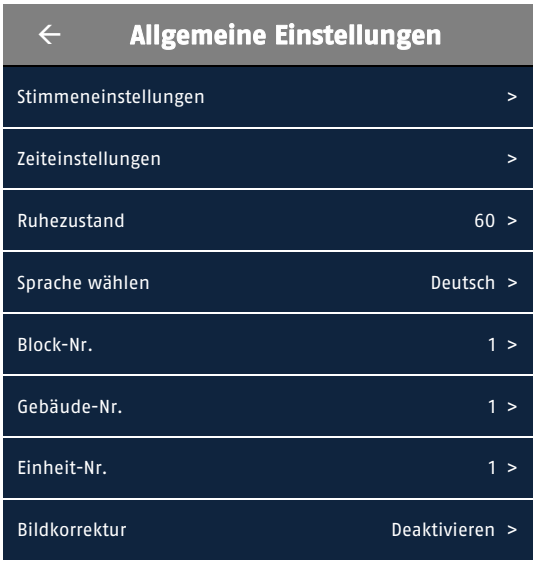
7.3.4 Grundeinstellungen

Stimmeneinstellungen / Toneinstellungen

Sprachausgabe:	Aktivieren der Sprachausgabe bei Zutritt und aktivieren des Tastentones bei Eingabe
Lautstärke:	0 -10

Zeiteinstellungen

Zeitzone:	Einstellung der Zeitzone
Aktuelle Uhrzeit:	Manuelle Zeiteinstellung. Über die Web-Oberfläche kann optional die NTP-Funktion zur automatischen Ermittlung der Uhrzeit erfolgen.
DST-Einstellung:	Einstellung der Daten zur Normal-/Sommerzeitumstellung.



Ruhezustand

Der Monitor des Terminals zeigt nach 20 Sekunden ohne eine Bildschirmaktivität das Standard-Hintergrundbild an (fester Zeitraum).

Nach weiteren 20 – 999 Sekunden tritt der Monitor in den Ruhezustand, d.h. das Display ist aus. Dieser Zeitraum kann eingestellt werden.

Sprache wählen

Es stehen DEUTSCH und ENGLISCH als Anzeigesprache im lokalen Display zur Verfügung.

Block- / Gebäude- / Einheit-Nr.

Diese Parameter ordnen das Terminal im Kontext der Verwendung als Gegensprechanlage dem gewünschten Haupt-Monitor-Bereich zu.

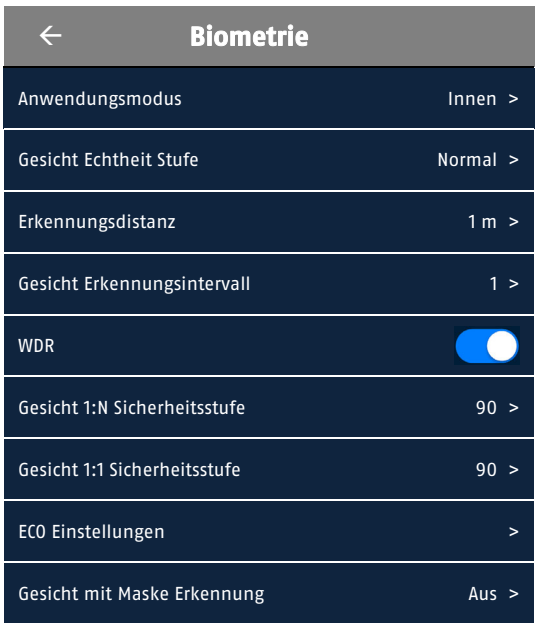
Die Konfiguration der Haupt-Monitor Nummer erfolgt im Menü „Admin-Menü / Darstellung / Schnelltaste / Spez. Raum anrufen / Zimmernummer“ für den 1. Haupt-Monitor (bzw. 1. Wohnung).

Es können bis zu 3 Tasten zum Rufen von 3 verschiedenen Haupt-Monitoren (bzw. Wohnungen) programmiert werden.
Die Konfiguration aller 3 Tasten (inkl. Benamung) erfolgt im Web-Interface des Terminals (Admin-Login / Konfiguration / Gegensprechanlage / Taste zum Anrufen / Angegebende Innenstation anrufen“)

Bildkorrektur

Die Bildkorrektur dient zum Aufhellen oder Glätten der Videodarstellung im Display.

7.3.5 Biometrische



Anwendungsmodus

Wählen Sie, in welchem Bereich das Terminal installiert wurde (innen, außen). Je nach Auswahl werden bestimmte Voreinstellungen für das Gerät und im Speziellen für das Kameramodul vorgenommen.

Gesicht Echtheit Stufe

Dieser Einstellungspunkt entscheidet, wie detailliert die Überprüfung der Echtheit des Gesichtes erfolgen soll. Je genauer die Überprüfung stattfindet, um so länger dauert die Überprüfung. Die Überprüfung kann mehrere Sekunden lang andauern, was sich negativ auf das Bedienerlebnis auswirkt.

Erkennungsdistanz

Die Einstellung der Erkennungsdistanz (0,5 bis 2 Meter, Auto) kann eine ungewünschte Erkennung bei Vorbeilaufen vermeiden. Prinzipiell ist davon abzuraten, eine größere Erkennungsdistanz einzustellen, da die Gesichtsmerkmale bei kürzerer Distanz deutlicher für die Kamera erkennbar sind.

Bei der Option Auto ist keine Distanzgrenze vorhanden, das Terminal entscheidet aufgrund der Erkennbarkeit eines Gesichtes selbst über den Beginn der Gesichtsanalyse.

Gesicht Erkennungsintervall

Der Erkennungsintervall (1 bis 10 Sekunden) kann ungewünschte wiederholte Gesichtsidentifikation vermeiden, wenn Sie sich vor dem Gerät befinden. Der Wert ist praktisch eine Pausenzeit zwischen 2 Identifikationen.

WDR

Falls es unvermeidbar ist, dass das Terminal entgegen einer Starken Lichtquelle (z.B. Sonne) installiert ist, dann kann diese Funktion helfen die Erkennung von Gesichtern zu verbessern (Wide Dynamik Range – Großer Dynamikbereich für die Kamera)
Gesicht 1:N Sicherheitsstufe

Des ist die Sicherheitsstufe für den Vergleich eines aufgenommen Gesichtsbildes (Live) mit vielen Gesichtsbildern in der Benutzerdatenbank.
Je größer der Wert, desto kleiner ist die Falschakzeptanzrate und umso größer ist die Falschrückweisungsrate.

Gesicht 1:1 Sicherheitsstufe

Dies ist die Sicherheitsstufe für den Vergleich eines aufgenommen Gesichtsbildes (Kamera) mit genau einem Gesichtsbild aus der Benutzerdatenbank. Dieser Wert kommt nur bei der Verwendung der Methode „Mehrere Berechtigungsnachweise“ zur Geltung, da vor Gesichtsvergleich der Benutzer sich bereits per Karte oder PIN teilweise authentifiziert hat.

ECO Einstellungen

Bei schwachen Lichtverhältnissen kann das Terminal durch die zusätzliche Nutzung von Infrarot-Licht die Erkennung verbessern. (Extended Camera Operation / Erweiterte Kamera Verwendung)

ECO Schwellwert:	Je höher der Wert, desto schneller wird der ECO Modus durch das Terminal verwendet.
ECO Modus (1:1):	Analog normale 1:1 Sicherheitsstufe.
ECO Modus (1:N):	Analog normale 1:N Sicherheitsstufe.

Gesicht mit Maske Erkennung

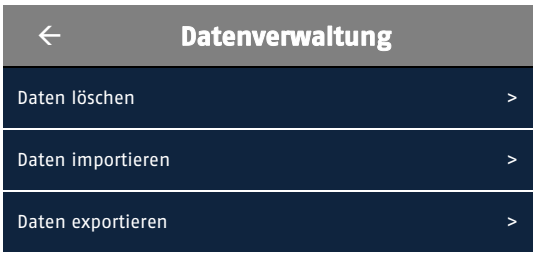
Nach Aktivierung dieser Funktion prüft das Terminal, ob eine erkannte Person einen Mund-Nasen-Schutz (umgangssprachlich „Maske“) trägt.

Erinnerung an Tragen:	Die Person kann an das Tragen der Maske erinnert werden (Meldung im Display) und die Tür öffnet sich.
Muss tragen:	Die Person wird an das Trage der Maske erinnert. Die Tür wird erst geöffnet werden, wenn die Person eine Maske trägt.

7.3.6 Datenbank

Daten löschen

Benutzerdaten löschen: Löschen aller eingelernen Benutzer. Die Benutzerverwaltung ist anschließend leer. Zugang zum Administrator-Menü ist anschließend nur noch mit dem Admin-Kennwort des Gerätes möglich.



Datenimport

Benutzerdaten: Import von Benutzer
Gesichtsdaten: Importieren von Gesichtsbildern für existierende Benutzer
Zutrittskontrolleinstellungen: Konfigurationseinstellungen des Gerätes

Der Datenimport kann durch Verwendung der USB-C Schnittstelle am Gerät erfolgen. Falls eine Datenbankdatei von zuvor exportierten Daten importiert werden soll, die ein Passwort hat, dann müssen sie dies eingeben. Ansonnsten drücken Sie nur OK.

- Falls Sie Daten von einem Gerät auf ein anderes Gerät übertragen möchten, so müssen Sie als Erstes immer die Benutzerdaten importieren. Anschließend können Gesichtsbilder importiert werden.
- Das USB Laufwerk muss FAT32 unterstützen.
- Der Ordner, in dem sich Gesichtsbilder auf dem USB Stick befinden müssen, lautet „enroll_pic“.
- Es können weitere Ordner „enroll_pic1“, „enroll_pic2“ usw. erstellt werden.
- Die Dateinamen der Bilder müssen wir folgt aufgebaut sein.
  Karten-Nr._Name_Abteilung_Mitarbeiter-ID_Geschlecht.jpg

  Geschlecht: „male“ oder „female“
  Mitarbeiter ID max. 32 Zeichen, Kleinbuchstaben, Großbuchstaben und Ziffern. Die ID muss eindeutig sein, und darf nicht mit „0“ beginnen.
- Anforderungen für Gesichtsbild: Gesamtes Gesicht, direkt in die Kamera schauen, keinen Hut oder andere Kopfbedeckung, Bildformat JPEG oder JPG, Auflösung min. 640 x 480 Pixel, Bildgröße zwischen 60 KByte bis 200 KByte

Datenexport

Gesichtsdaten: Export ausschließlich von Gesichtsbildern
Ereignisdaten: Logbuchdaten
Benutzerdaten: Benutzerdetails
Zutrittskontrolleinstellungen: Konfigurationseinstellungen des Gerätes

Bitte diese Funktion nicht verwenden, falls Klingeltasten aktiviert sind.

Der Datenexport kann durch Verwendung der USB-C Schnittstelle am Gerät erfolgen. Der Export erfordert eine Vergabe eines Passwortes (4 – 6 Zeichen).

- Die Daten werden als Datenbankformat exportiert und sind nicht durch Drittsoftwaren lesbar
- Es werden USB Sticks von 1 – 32 GByte unterstützt.
- Es sollten min. 512 Mbyte Speicherplatz vorhanden sein.

7.3.7 Systemwartung

System Informationen

Diese Seite zeigt diverse Informationen des Gerätes an (Gerätemodell, Seriennummer, Firmwareversion, MAC-Adresse, Produktionsdatum, Geräte-QR-Code, Open-Source-Informationen).

Der Geräte-QR-Code dient für die Einbindung in die Link Station App.

Kapazität

Anzeige der eingelernen Anzahl der Benutzer, Gesichter, Karten und Ereigniseinträge (Logbuch) mit der restlich verfügbaren Menge.

Geräteaktualisierung

Diese Seite zeigt die aktuall installierte Firmware-Version. Weithin kann üer den USB-C Anschluss an der Unterseite des Gerätes eine Aktualisierung der Firmware vorgenommen werden. Die Firmwaredatei muss sich dazu im Wurzelverzeichnis des USB Sticks befinden.

Link Station Verknüpfung aufheben

Nach Drücken dieser Schaltfläche und Eingabe des Administrator-Passwortes wird das Gerät vom aktuell verbundenen Link Station Account entfernt.

Werkseinstellungen laden

Rücksetzen aller Einstellungen auf Werkseinstellungen

Standardeinstellungen (bedingt)

Rücksetzen der Einstellungen ausser: Kommunikationseinstellungen, Über CMS/Web importierte Benutzerinformationen

Neustart

Neustarten des Gerätes

7.3.8 Darstellung

Schnelltaste

Anruf: Bei Aktivierung wird im Display des Gerätes min. eine Ruftaste angezeigt

Anruf-Typ: Zentrale Anrufen:
Spez. Raum anrufen
Anruf App

Zimmernr.

Schaltflächenname: FAMILY ONE

Passwort: Schaltfläche für die PIN Eingabe.

QR Code: Kartennummer als QR Code (CMS nötig)

Thema

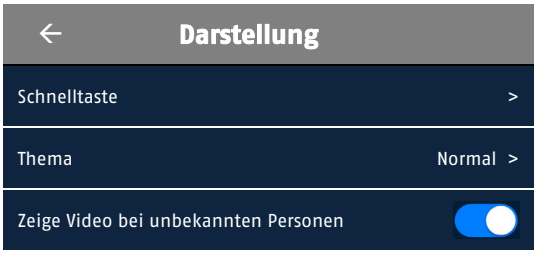
Standard: Es werden bei Konfiguration nur Ruftaste(n), Pin-Code und QR-Code Taste angezeigt, sowie bei Wunsch das Vorschauvideo der Person.

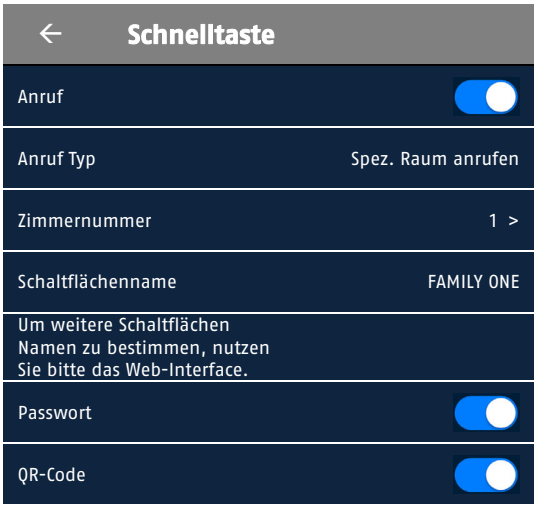
Einfach: Es werden bei Konfiguration nur Ruftaste(n), Pin-Code und QR-Code Taste angezeigt.
Das Vorschauvideo wird nicht angezeigt. Die Gesichtserkennung im Hintergrund aktiv.

Information: Der Unterschied zum Standardmodus ist, dass im oberen Bereich des Displays Platz für die Anzeige von Informationen ist.
Die Programmierung erfolgt über die Web-Oberfläche.

Zeige Video bei unbekannter Person

Bei deaktivierter Option wird für Personen, die nicht in der Benutzerdatenbank mit Bild hinterlegt sind, kein Live-Video im Display angezeigt.
Es erscheinen nur aktivierte Ruftasten, Pin Code Eingabe oder QR-Code Taste.





8. Konfiguration und Bedienung über Web-Browser

Falls das Terminal über ein Netzwerkkabel bereits erfolgreich mit einem Netzwerk verbunden ist, oder die WiFi Einstellungen erfolgreich über das Display programmiert wurden, so kann die Web-Seite des Terminals über einen Browser aufgerufen werden (bevorzugt Chome, Edge). Die IP Adresse des Geräte finden Sie über den zuvor beschriebenen ABUS IP Installer.

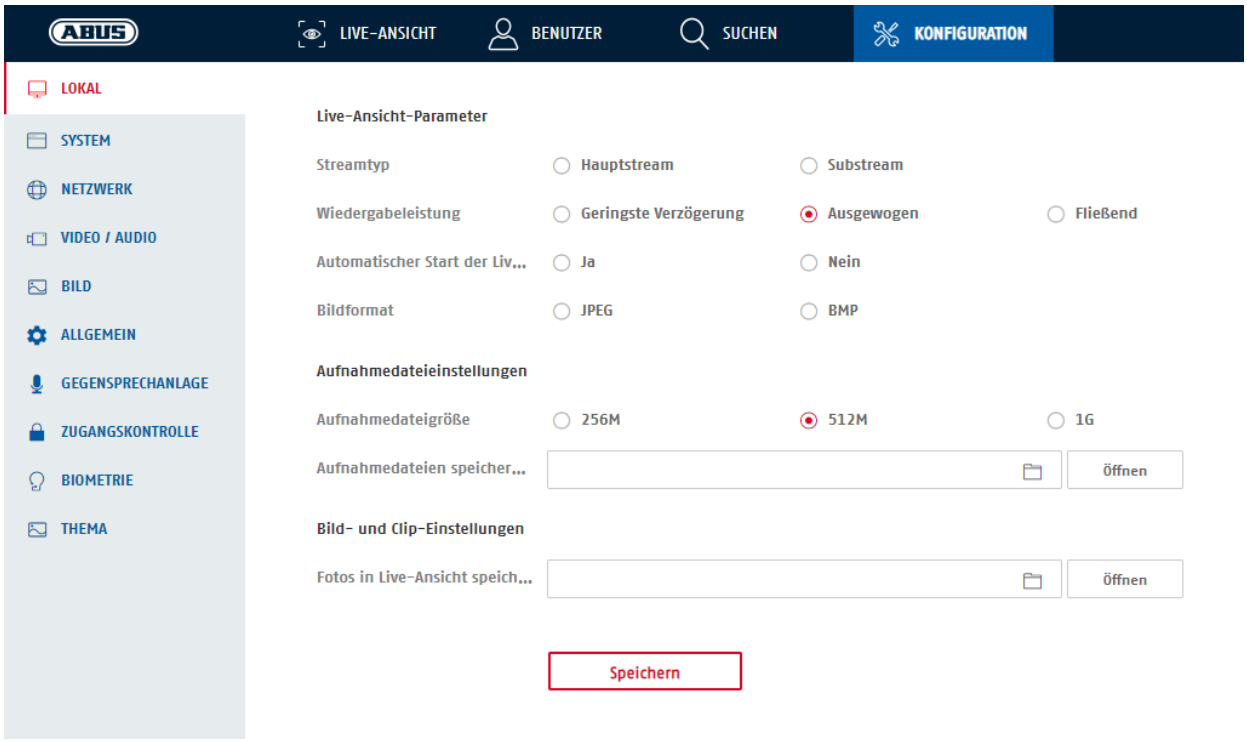
Folgende Bedienelemente werden auf den Einstellungsseiten im Web-Browser verwendet.

Funktionselement	Beschreibeung
	Vorgenommene Einstellungen auf der Seite speichern. Es ist darauf zu achten, dass Einstellungen nur nach Drücken der Schaltfläche für das Speichern übernommen werden.
	Funktion aktiviert
	Funktion deaktiviert
	Listenauswahl
	Eingabefeld
	Schieberegler

8.1 Konfiguration über Web-Browser

8.1.1 Lokale Konfiguration

Unter dem Menüpunkt „Lokale Konfiguration“ können Sie Einstellungen für die Live-Ansicht, Dateipfade der Aufzeichnung und Momentaufnahmen vornehmen.



Live-Ansicht Parameter

Streamtyp: Festlegung, welche Videoqualität als Standard in der Seite „Live-Ansicht“ dargestellt werden soll.
Hauptstream (1. Video-Strom), hohe Qualität
Substream (2. Video-Strom), niedrige Qualität

Wiedergabeleistung: Diese Einstellung beeinflusst die Pufferung des Video-Streams. Bei „Geringste Verzögerung“ wird kaum gepuffert, bei „Fließend“ wird entsprechend mehr zwischengepuffert, was aber zu zeitverzögerter Darstellung führen kann.

Automatischer Start der Live-Ansicht: Wenn Sie die Option aktivieren, dann wird sofort nach Aufrufen der Seite „Live-Ansicht“ das Live-Bild gestartet.

Bildformat: Einstellung, in welchem Format das Einzelbild aus der Liveansicht (Schaltfläche Sofortbild) gespeichert werden soll (JPEG, BMP).

Aufnahme-Dateieinstellungen

Hier können Sie die Dateigröße für Aufzeichnungen, den Aufzeichnungspfad und den Pfad für heruntergeladene Dateien definieren. Um die Änderungen zu übernehmen klicken Sie auf „Speichern“.

Aufnahme-Dateigröße: Sie haben die Auswahl zwischen 256 MB, 512 MB und 1 GB als Dateigröße für die Aufzeichnungen und heruntergeladenen Videos zu wählen.

Speichern unter: Sie können hier den Dateipfad festlegen, welcher für manuelle Aufzeichnungen verwendet werden soll.

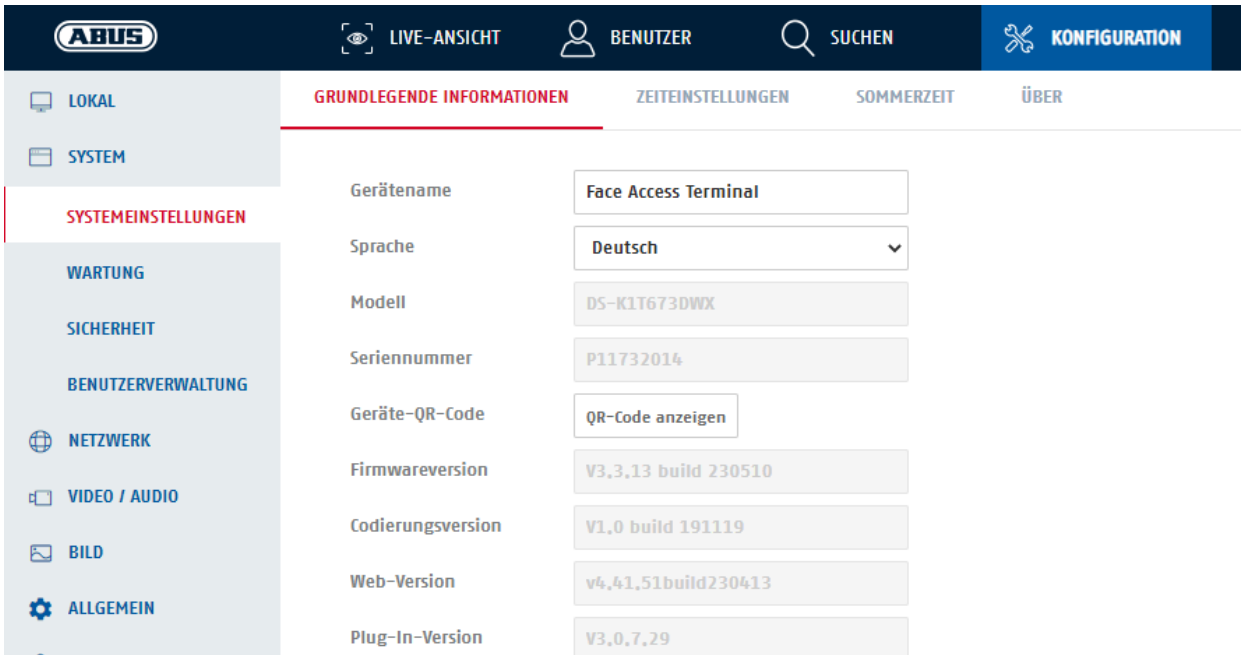
Bild- und Clip Einstellungen

Fotos in Live-Ansicht speichern: Wählen Sie den Dateipfad für Sofortbilder aus der Liveansicht aus.

8.1.2 System

8.1.2.1 Systemeinstellungen

8.1.2.1.1 Grundlegende Informationen



Gerätename: Hier können Sie einen Gerätenamen für die Kamera vergeben. Klicken Sie auf „Speichern“ um diesen zur übernehmen.

Sprache: Sie können zwischen deutscher und englischer Sprache für die Anzeige im Web-Interface wählen.

Modell: Anzeige der Modellnummer

Seriennummer: Anzeige der Seriennummer

Geräte-QR-Code: Bei Drücken dieser Schaltfläche wird die Seriennummer als QR Code dargestellt. Dies erleichtert das Hinzufügen des Terminals zur ABUS Link Station App.

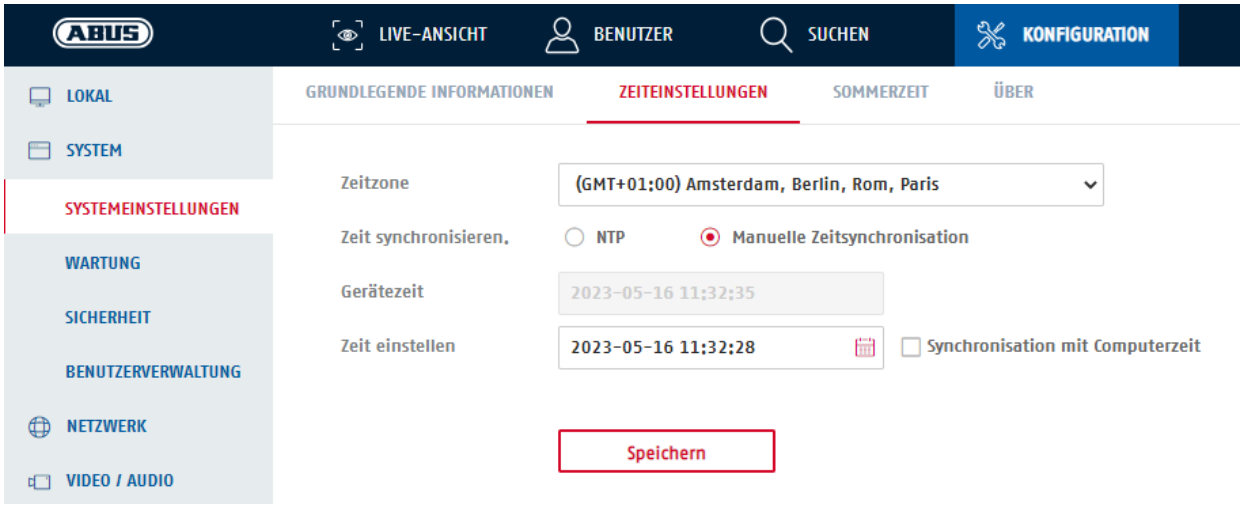
Firmware-Version: Anzeige der Firmware Version

Cod.-Version: Anzeige der Codierungsversion

Web-Version: Anzeige der Webseiten-Version

Plug-In-Version: Anzeige der Version des Video-Plugin zur Video Darstellung.

8.1.2.1.2 Zeiteinstellungen



Zeitzone
Auswahl der Zeitzone (GMT)

Zeiteinstellungsmethode

NTP: Mit Hilfe des Network Time Protokolls (NTP) ist es möglich, die Uhrzeit der Kamera mit einem Zeitserver zu synchronisieren.Aktivieren Sie NTP um die Funktion zu nutzen.

Server-Adresse: IP-Serveradresse des NTP Servers.

NTP-Port : Netzwerk-Portnummer des NTP Dienstes (Standard: Port 123)

NTP-Aktualisierungsintervall: 1-10080 Min.

Man. Zeitsynchron.

Gerätezeit: Anzeige der Gerätezeit des Computers

Zeiteinstellung: Anzeige der aktuellen Uhrzeit anhand der Zeitzonen-Einstellung.
Klicken Sie „Synchr. mit Comp-Zeit“ um die Gerätezeit des Computers zu übernehmen.

	Übernehmen Sie die getroffenen Einstellungen mit „Speichern“

8.1.2.1.3 DST / Sommerzeit

Sommerzeit

Sommerzeit aktivieren: Wählen Sie „Sommerzeit“, um die Systemzeit automatisch an die Sommerzeit anzupassen.

Startzeit: Legen Sie den Zeitpunkt für die Umstellung auf Sommerzeit fest.

Endzeit: Legen Sie den Zeitpunkt der Umstellung auf die Winterzeit fest.

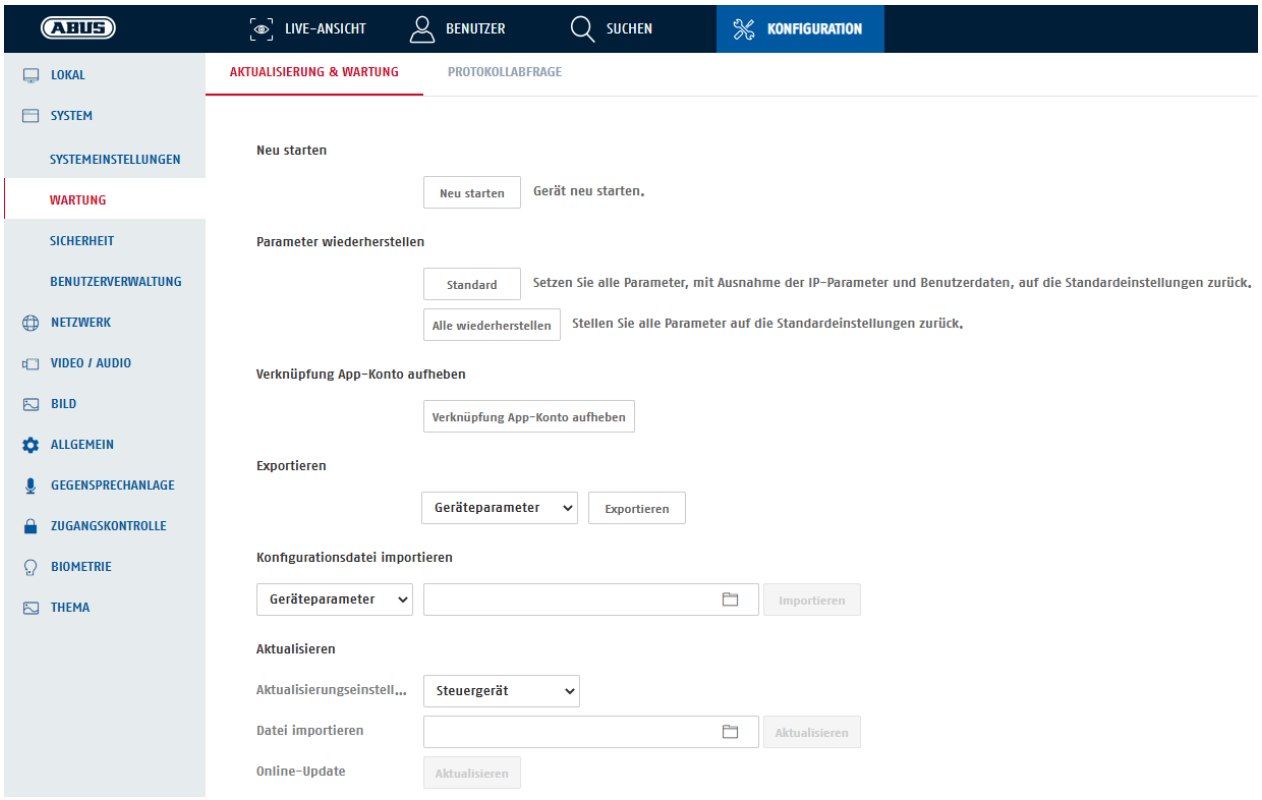
	Übernehmen Sie die getroffenen Einstellungen mit „Speichern“

8.1.2.1.4 Über / Lizenzinformationen

Anzeige von Open Source Lizenzinformationen

8.1.2.2 Wartung

8.1.2.2.1 Aktualisierung und Wartung



Neustart: Klicken Sie „Neustart“ um das Gerät neu zu starten.

Parameter wiederherstellen

Standard: Rücksetzung der Werte bis auf IP-Parameter und Benutzerdaten.
Alles Wiederherstellen: Rücksetzen aller Werte.

Verknüpfung App-Konto aufheben: Diese Schaltfläche hebt die aktuelle Verknüpfung von Terminal und Link Station Account auf.

Eportieren der Geräteparameter / der Protokolldatei: Vergeben Sie eine Passwort für die Exportdateil

Importieren d. Geräteparameter: Wählen Sie hier den Dateipfad um eine Konfigurations-Datei zu importieren.

Aktualisieren

Steuergerät (Terminal): Wählen Sie den Pfad aus, in dem die neue Firmware abgelegt ist.

Online-Update: Diese Funktion steht nicht zur Verfügung.

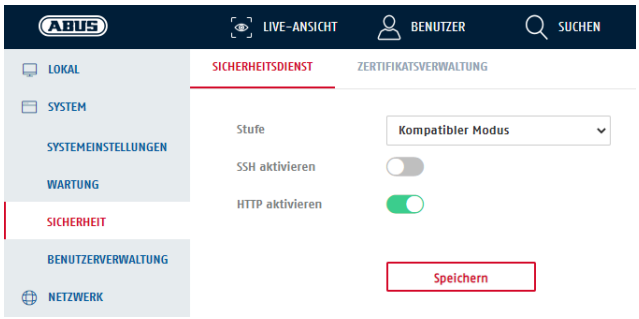
	Übernehmen Sie die getroffenen Einstellungen mit „Speichern“

8.1.2.2.2 Protokollabfrage / Logbuch

In diesem Punkt können Log-Informationen der Kamera angezeigt werden. Damit Log-Informationen gespeichert werden muss eine SD-Karte in der Kamera installiert sein.

8.1.2.3 Sicherheit

8.1.2.3.1 Sicherheitsdienst



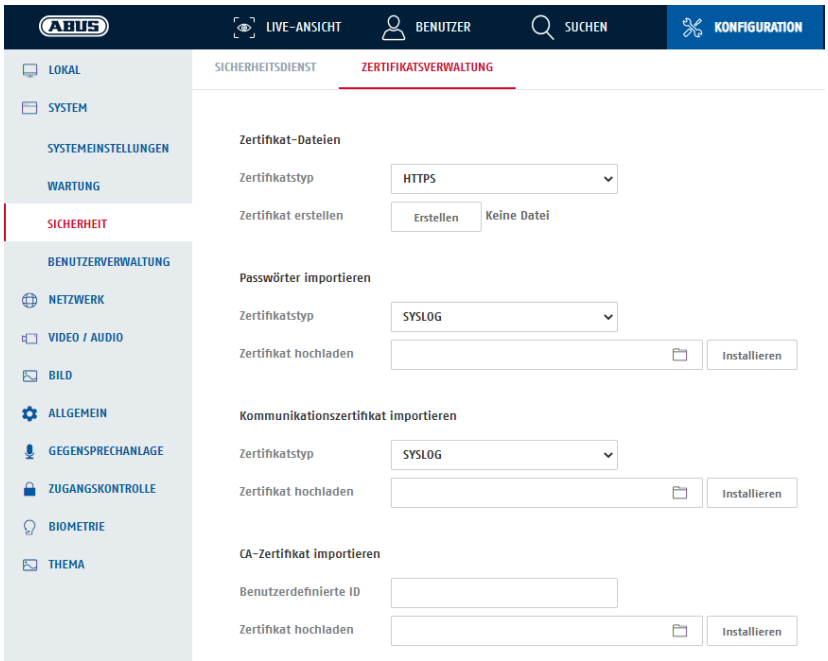
SSH aktivieren: Diese Funktion aktiviert den Telnet Port und das Telnet Protokoll.

HTTP aktivieren: Eine Deaktivierung der http Schnittstelle zur Darstellung der Web-Seite ist möglich.

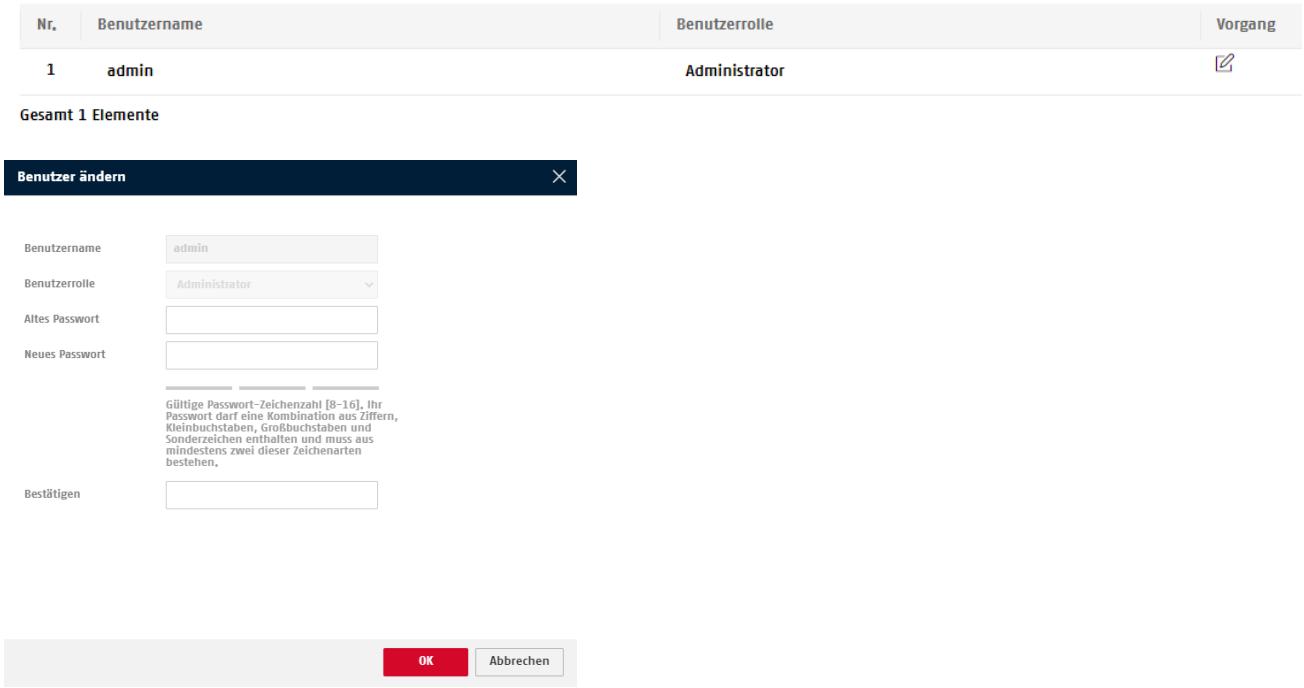
Hinweis: Nach Deaktivierung kann die Funktion nur durch Rücksetzen des Terminals wieder aktiviert werden („Alles wiederherstellen“).

8.1.2.3.2 Zertifikatsverwaltung

In diese Einstellungsseite kann zum Einen ein selbstsigniertes HTTPS-Zertifikat erstellte werden, und zum Zweiten kann ein HTTPS-Zertifikat, welches durch eine CA Stelle zertifiziert wurde, hochgeladen werden.



8.1.2.4 Benutzerverwaltung



Unter diesem Menüpunkt können Sie das Passwort des Administrator Benutzers ändern.
Klicken Sie dazu auf das Bearbeiten Symbol hinten in der Zeile 1.

Sie müssen dazu das alte Passwort eingeben, sowie das neue Passwort eingeben und bestätigen.

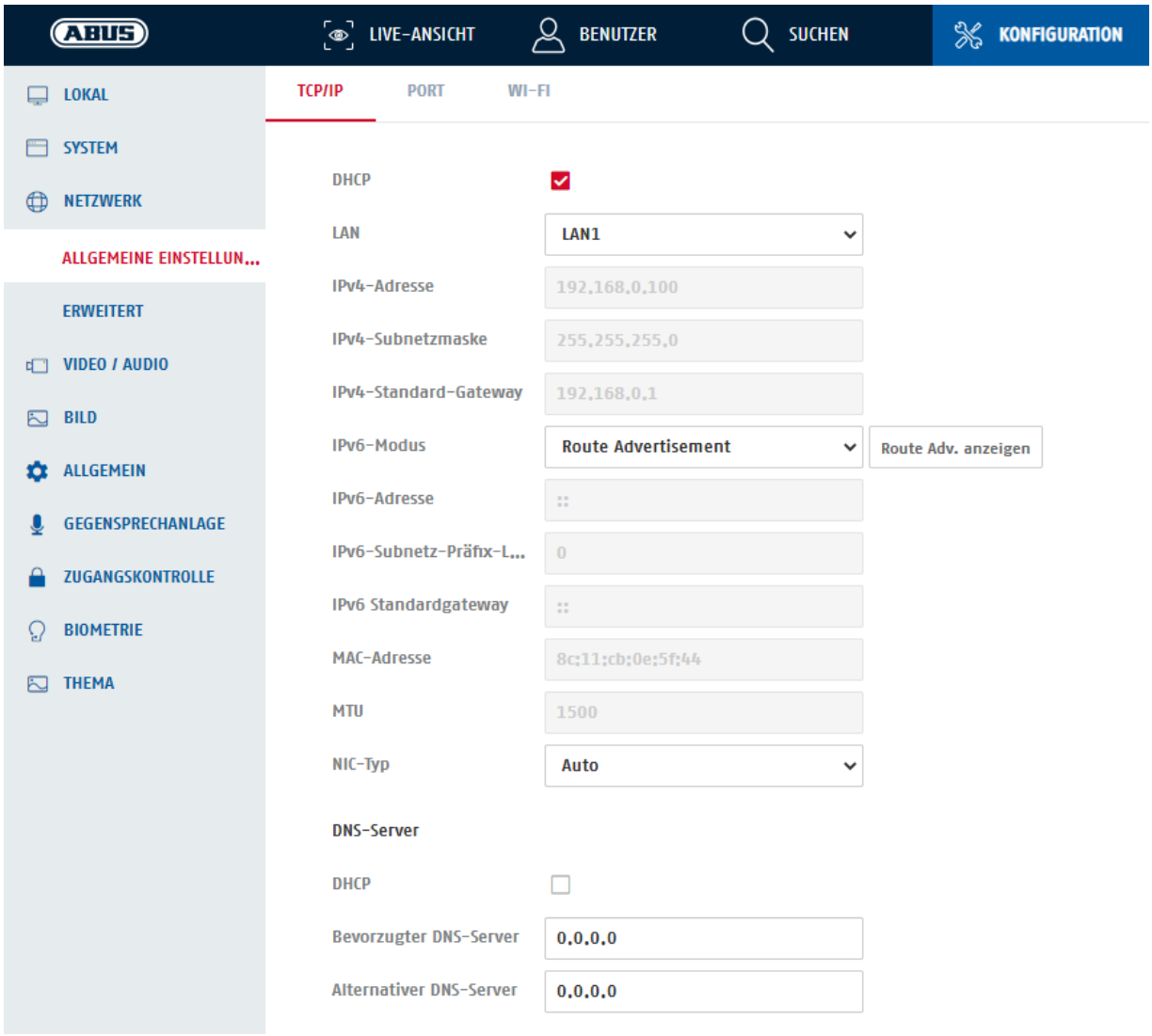
	Übernehmen Sie die getroffenen Einstellungen mit „OK“. Klicken Sie „Abbrechen“ um die Daten zu verwerfen.

8.1.2.4.1 Scharfschaltung / Unscharfschaltung Info

Diese Funktion wird nicht unterstützt.

8.1.3 Netzwerk

8.1.3.1 TCP/IP



DHCP: Falls ein DHCP-Server verfügbar ist, klicken Sie DHCP an, um automatisch eine IP-Adresse und weitere Netzwereinstellungen zu übernehmen. Die Daten werden automatisch von dem Server übernommen und können nich manuell geändert werden.
Falls kein DHCP-Server verfügbar ist, füllen Sie bitte folgende Daten manuell aus.

IPv4-Adresse: Einstellung der IP-Adresse für die Netzwerkschnittstelle

IPv4 Subnetzmaske: Manuelle Einstellung der Subnetzmaske

IPv4-Standard-Gateway: Einstellung des Standard-Routers (z.B. IP Adresse Ihrer Fritz Box)

IPv6 Modus: Manuell: Manuelle Konfiguration der IPv6 Daten
DHCP: Die IPv6 Verbindungsdaten werden vom DHCP Server bereitgestellt.
Route Advertisement: Die IPv6 Verbindungsdaten werden vom DHCP Server (Router) in Verbindung mit dem ISP (Internet Service Provider) bereitgestellt.

IPv6 Adresse: Anzeige der IPv6 Adresse. Im IPv6 Modus „Manuell“ kann die Adresse konfiguriert werden.

IPv6 Subnetzmaske: Anzeige der IPv6 Subnetzmaske.

IPv6 Standard Gateway: Anzeige des IPv6 Standard Gateways (Standard Router)

MAC-Adresse: Hier wird die IPv4 Hardware-Adresse des Terminals angezeigt, diese können Sie nich verändern.

MTU: Einstellung der Übertragungseinheit, wählen Sie einen Wert 500 – 9676. Standardmäßig ist 1500 voreingestellt.

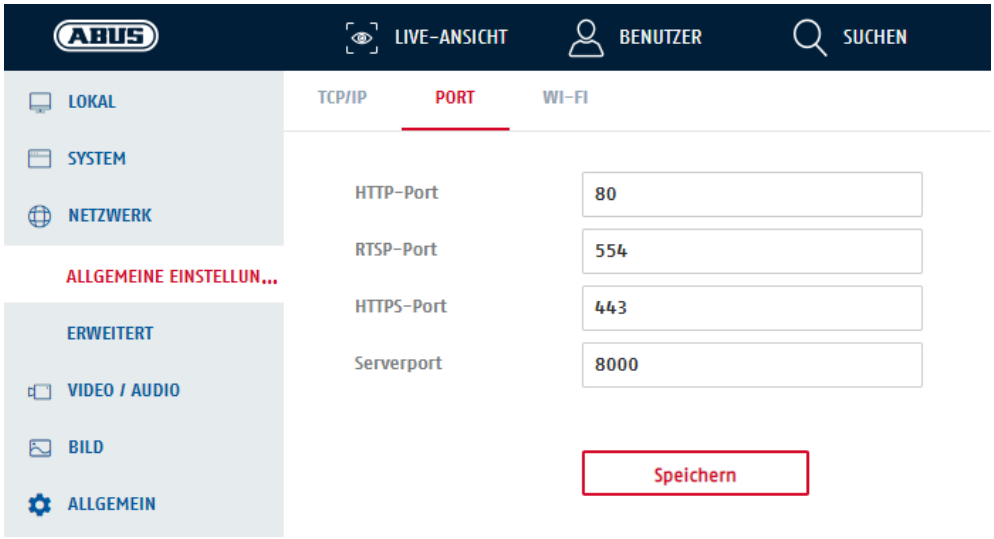
DNS-Server

Nach aktivieren der DHCP Funktion wird der DNS Server automatisch ermittelt. Alternative die manuelle Eingabe über:

Bevorzugter DNS-Server: Für einige Anwendungen sind DNS-Servereinstellungen erforderlich. (z.B. E-Mail-Versand) Geben Sie hier die Adresse des bevorzugten DNS-Servers ein.

Altern. DNS-Server: Falls der bevorzugte DNS-Server nicht erreichbar sein sollte, wird dieser alternative DNS-Server verwendet. Bitte hinterlegen Sie hier die Adresse des alternativen Servers.

8.1.3.2 Port



Falls Sie auf die Kamera von extern zugreifen möchten, müssen folgende Ports konfiguriert werden.

HTTP-Port: Der Standard-Port für die HTTP- Übertragung lautet 80. Alternativ dazu kann dieser Port einen Wert im Bereich von 1024~65535 erhalten. Befinden sich mehrere Netzwerkgeräte im gleichen Subnetz, so sollte jedes Gerät einen eigenen, einmalig auftretenden HTTP-Port erhalten.

RTSP-Port: Der Standard-Port für die RTSP- Übertragung lautet 554. Alternativ dazu kann dieser Port einen Wert im Bereich von 1024~65535 erhalten. Befinden sich mehrere Netzwerkgeräte im gleichen Subnetz, so sollte jedes Gerät einen eigenen, einmalig auftretenden RTSP-Port erhalten.

HTTPS-Port: Der Standard-Port für die HTTPS- Übertragung lautet 443.

Server Port: Der Standard-Port hierfür lautet 8000. Kommunikationsport für interne Daten. Alternativ dazu kann dieser Port einen Wert im Bereich von 1025~65535 erhalten. Befinden sich mehrere Netzwerkgeräte im gleichen Subnetz, so sollte jedes Gerät einen eigenen, einmalig auftretenden SDK-Port erhalten.

	Übernehmen Sie die getroffenen Einstellungen mit „Speichern“

8.1.3.3 WiFi

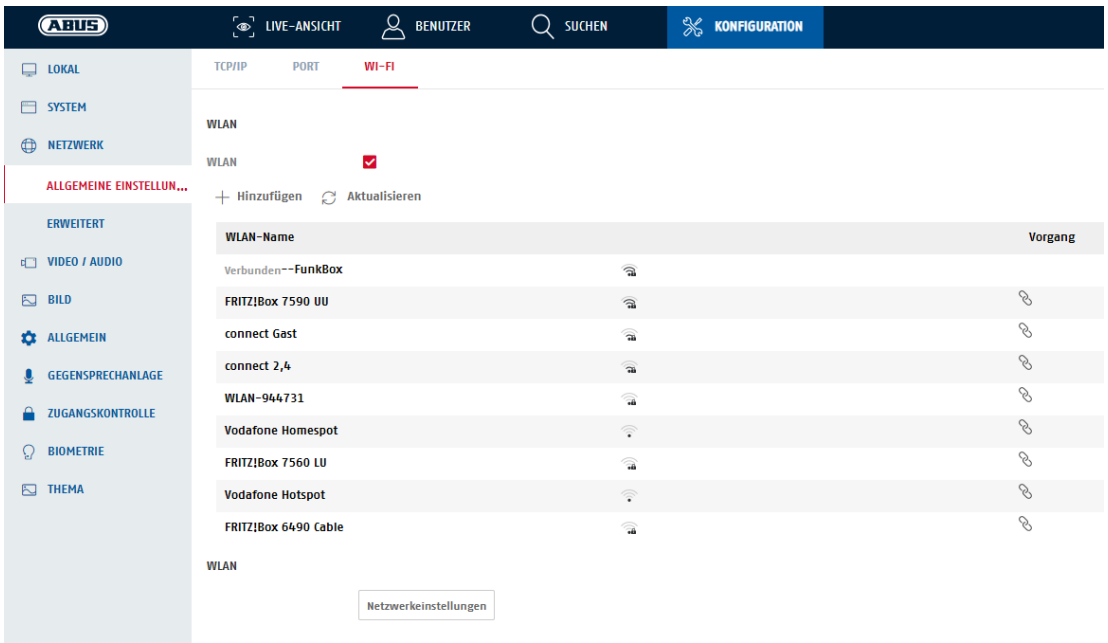
Falls die WiFi Funktion nicht bereichts bei der lokalen Einrichtung am Display aktiviert wurde, so kann dies auch hier im Web-Interface erfolgen.

Nach Aktivierung wird automatisch nach verfügbaren WiFi Access Points gesucht (nur 2.4 GHz!).

Wählen Sie einen Access Point aus, sie werden anschließend aufgefordert das Passwort des Access Points einzugeben (z.B. WiFi Passwort ihrer Fritz Box).

Alternativ kann eine Access Point Name manuell hinzugefügt werden.

Im Punkt „Netzwerkeinstellungen“ sehen Sie die ermittelten Netzwerkparatmeter (das ist meist so, da viele Acces Points die DHCP Funktion aktiviert haben).

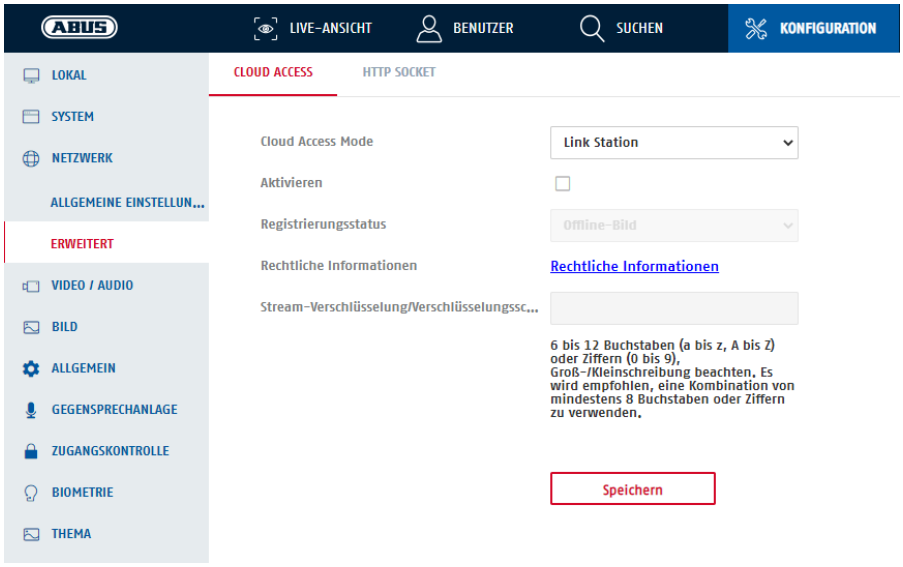


8.1.3.4 Cloud Zugriff / ABUS Link Station

Die ABUS Link Station Funktion dient zum einfachen Fernzugriff auf das ABUS Gerät per Link Station APP (iOS / Android). Produkte können einfach über QR-Code eingerichtet und freigegeben werden – ohne komplizierte Konfigurationen im Router (keine Portweiterleitungen nötig).

Aktivieren Sie die Funktion und vergeben Sie einen Verifizierungs-Code (6-12 Zeichen, A-Z, a-z, 0-9, min. 2 verschiedene Zeichentypen empfohlen).

Der QR Code (unter „System / Systemeinstellungen / Grundlegende Informationen / Geräte-QR-Code“) kann anschließend in der ABUS Link Station APP abfotografiert werden.



Verwendbare Funktionen sind:

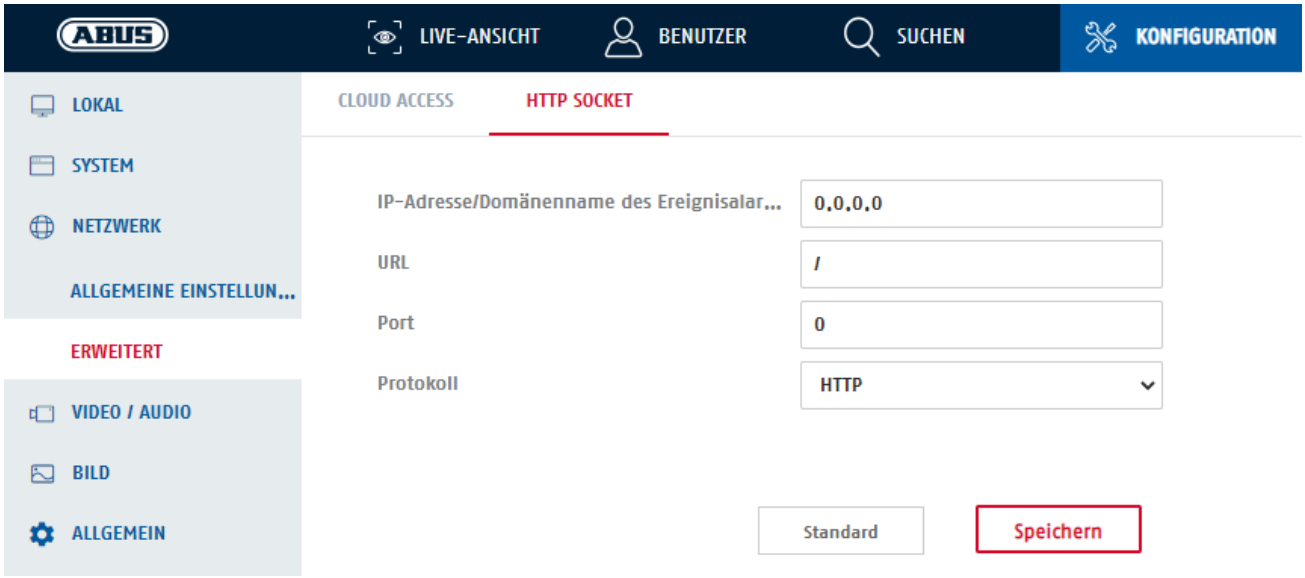
- Übertragung der Sabotagemeldung (Sabotagekontakt an der Rückseite des Terminals)
- Status Netwerkverbindung
- Live-Bildübertagung zur App
- Gegenspechen (2-Wege-Audio)
- Türkontakt über App schalten (Sequenz)
- Türkontakt über App schalten (dauerhaft)
- Anruffunktion von Terminal zu App über Klingeltaste im Touch-Display

Für die Anruffunktion von Terminal zu App ist folgende Einstellung nötig:

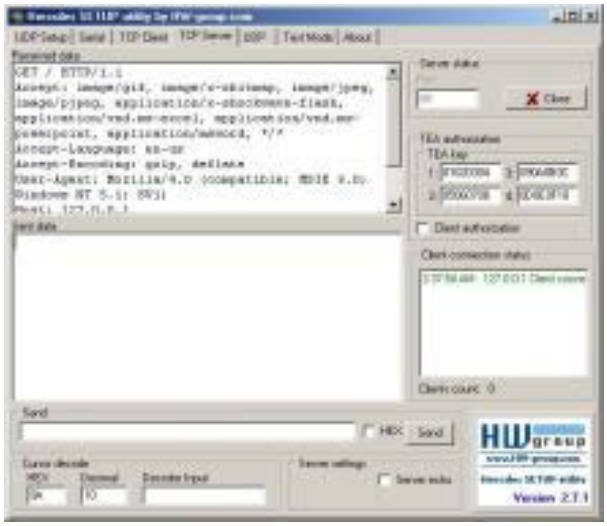
Lokales Display-Menü: Admin-Menü / Darstellung / Schnelltaste / Anruf-App
Web-Interface: Admin-Login / Konfiguration / Gegensprechanlage / Taste zum Anrufen / APP

8.1.3.5 HTTP Socket

Ereignisinformationen können per JSON Telegram an einen Alarm Host gesendet werden. Auf diese Weise können Ereignisse an eine Drittanbietersoftware übermittelt und weiter verarbeitet werden. Alarminformati
Zum einfachen Testen dieser Funktion kann z.B. die TCP Server Funktion der Software „Hercules Setup Utility“ (Hercules SETUP utility | HW-group.com) verwendet werden.

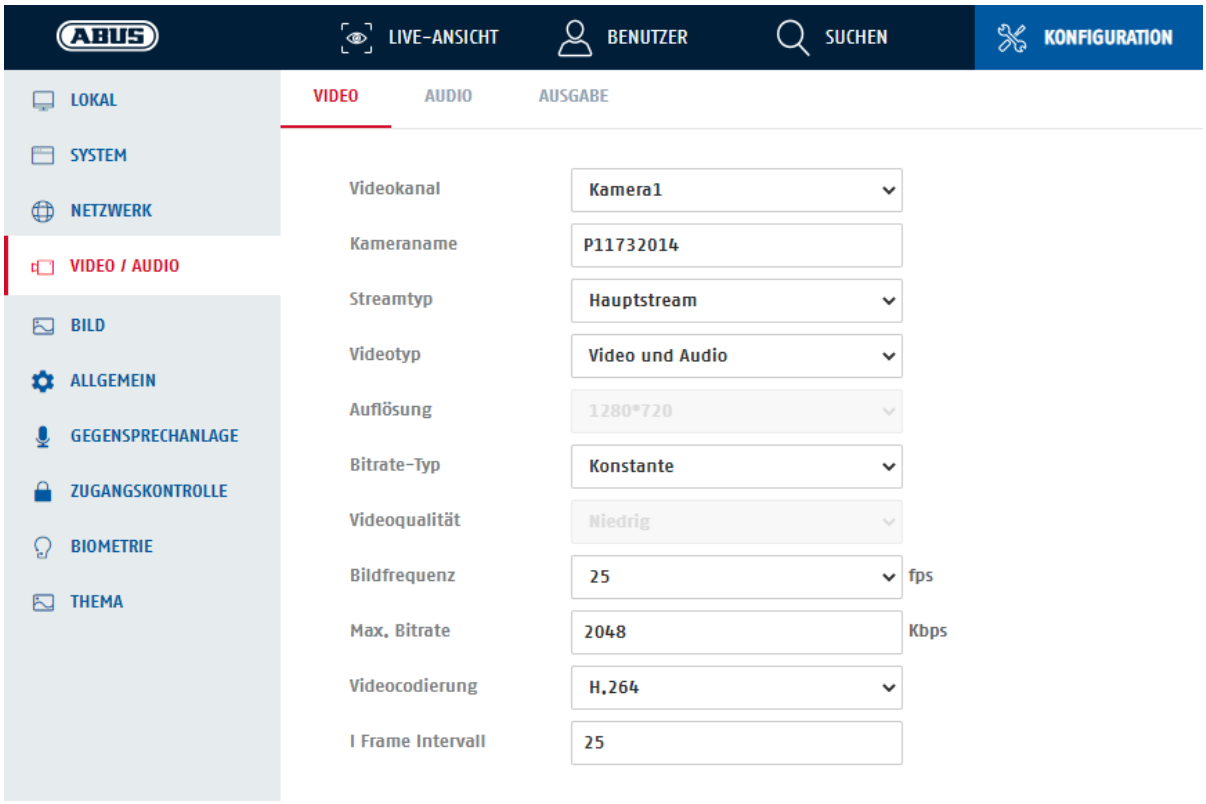


Hercules Setup Utility:



8.1.4 Video

8.1.4.1 Video



Videokanal: Nur die 1. Kamera kann in gewissen Parametern verändert werden.

Kameraname: Als Standard ist die Seriennummer als Name vergeben. Dieser Name kann geändert werden.

Stream-Typ: Wählen Sie den Stream-Typ für die Kamera. Wählen Sie „Main Stream (Normal)“ für die Aufzeichnung und Live-Ansicht mit guter Bandbreite. Wählen Sie „Sub-Stream“ für für die Live-Ansicht mit begrenzter Bandbreite.

Videotyp: Der Video Typ ist auf „Video und Audio“ per Standard festgelegt, damit Gegensprechen zum Monitor oder zur App funktionieren kann. Die Option „Video“ würde Audio blockieren.

Auflösung: Die Videoauflösung ist auf 1280x720 Pixel fixiert.

Bitratentyp: Gibt die Bitrate des Videostroms an. Die Videoqualität kann je nach Bewegungsintensität höher oder niedriger ausfallen. Sie haben die Auswahl zwischen einer konstanten und variablen Bitrate.

Videoqualität: Dieser Menüpunkt steht Ihnen nur zur Auswahl, wenn Sie eine variable Bitrate gewählt haben. Stellen Sie hier die Videoqualität der Videodaten ein. Die Videoqualität kann je nach Bewegungsintensität höher oder niedriger ausfallen.Sie haben die Auswahl zwischen sechs verschiedenen Videoqualitäten, „Minimum“, „Niedriger“, „Niedrig“, „Mittel“, „Höher“ oder „Maximum“ (dargestellt über „+“).

Bildfrequenz: Gibt die Bildrate in Bildern pro Sekunde an.

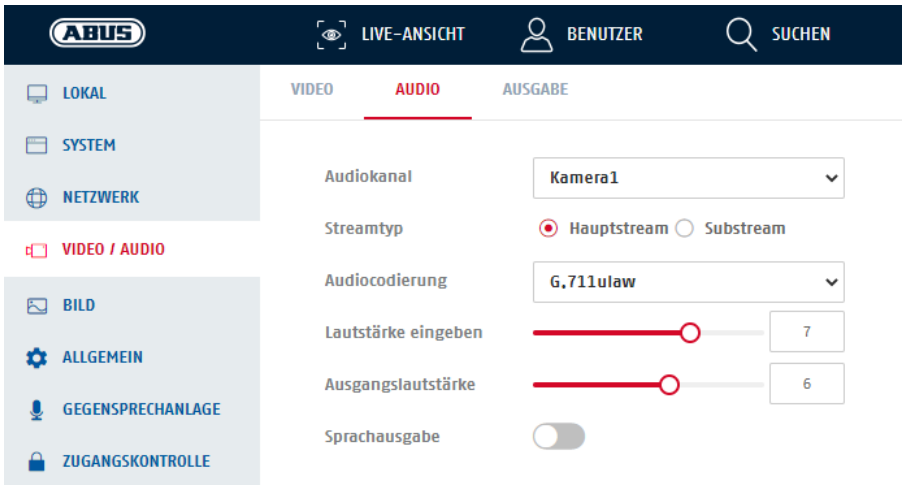
Max. Bitrate: Die Bitrate des Videostroms wird auf einen bestimmten Wert fest eingestellt, stellen Sie die max. Bitrate zwischen 32 und 16384 Kbps ein. Ein höherer Wert entspricht einer höheren Videoqualiät, beansprucht aber eine größere Bandbreite.

Videocodierung: Wählen Sie einen Standard für die Videocodierung aus, Sie haben die Auswahl zwischen H.264, H.265.

I Frame-Intervall: Stellen Sie hier das I Bildintervall ein, der Wert muss im Bereich 1 – 400 liegen.

	Übernehmen Sie die getroffenen Einstellungen mit „Speichern“

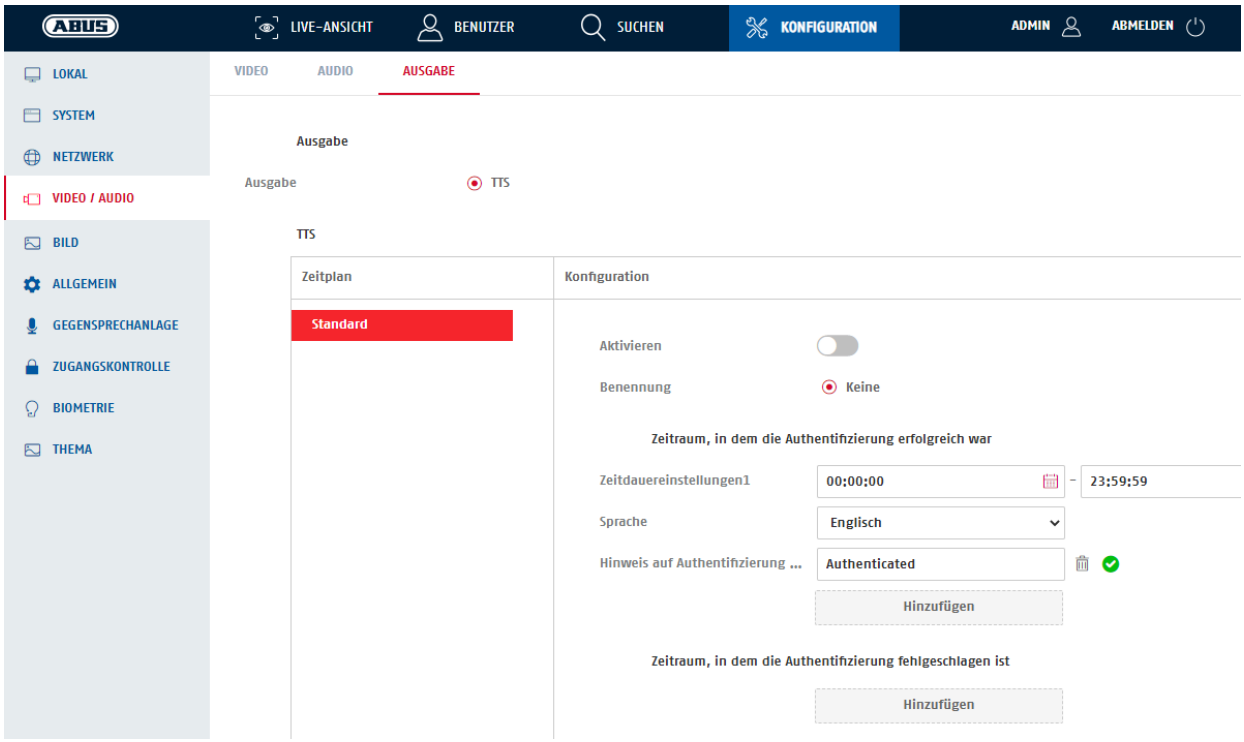
8.1.4.2 Audio



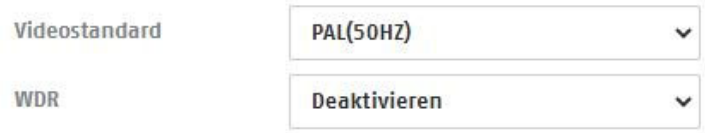
Audiokanal: Nur der Audioteil der Kamera 1 kann bearbeitet werden
Steamtyp: Die Einstellungen legen jweils die Audioeinstellungen für den Haupt- oder Substream fest.
Audiocodierung: Dies ist der verwendete Audiocodec.
Lautstärke Eingang: Lautstärke des Audio-Eingangs (Mic)
Ausgangslautstärke: Lautstärke des Audio-Ausgangs (Lautsprecher
Sprachausgabe: Die Sprachausgabe kann eine Wortmeldung bei erfolreicher oder nicht erfolgreicher Authenifizierung ausgeben (Standard ist aus).

8.1.4.3 Audio-Ausgabe

Das Audio Ausgabe-Modul ist ein Text-To-Speech Modul mit der Ausgabesprache Englisch. In 4 verschiedenen Zeiträumen können Meldungen bei erfolreicher oder nicht erfolgreicher Authenifizierung erfolgen.



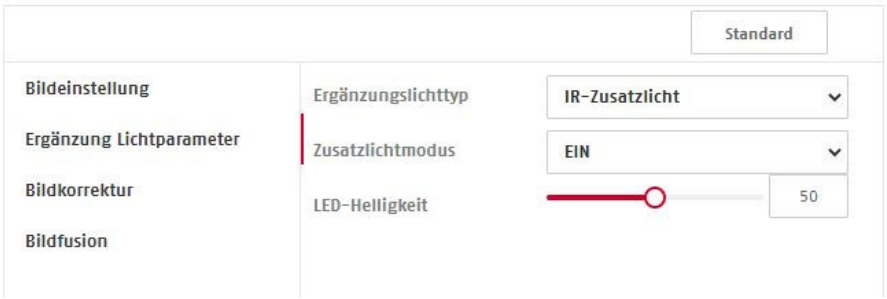
8.1.5 Bild



Videostandard: Legen Sie hier den Videostandard bzw. die Netzfrequenz für die Einsatzregion des Terminals fest (PAL, 50 Hz, 25 Bilder/s oder NTSC, 60 Hz, 30 Bilder/s)

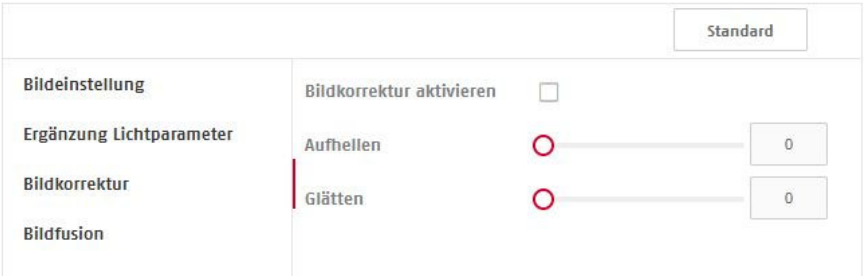
WDR: Falls der Kontrast zwischen Hintergrund und Vordergrund (Gesicht) zu groß ist, dann kann die WDR (Wide Dynamic Range) Funktion bei der Darstellung und Erkennung helfen.

Bildeinstellungen: Legen Sie hier diverse Kamaraparameter fest (Helligikeit, Kontrast, Sättigung, Schärfe). Diese Einstellungen gelten für das lokale Display sowie den Videostream (Web, App).

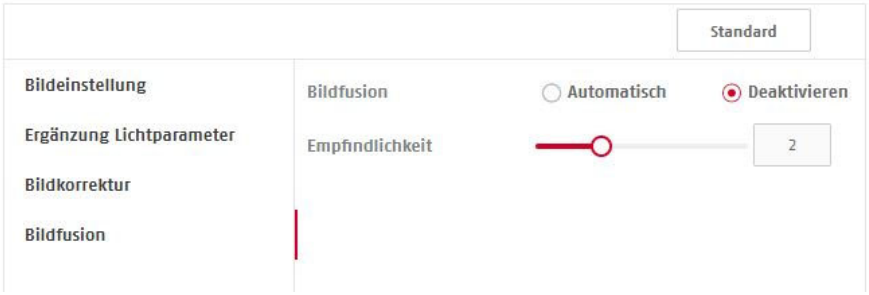


Ergänzende Lichtparameter

Ergänzungslichttyp: Als zusätzliche Lichtquelle steht Infrarot-Licht (IR) zur Verfügung.
Zusatzlichtmodus: Die zusätzliche Lichtquelle kann aktivert (Standard) oder deaktiviert werden.
LED-Helligkeit: Stufenlose Einstellung der IR-Licht Intensität.



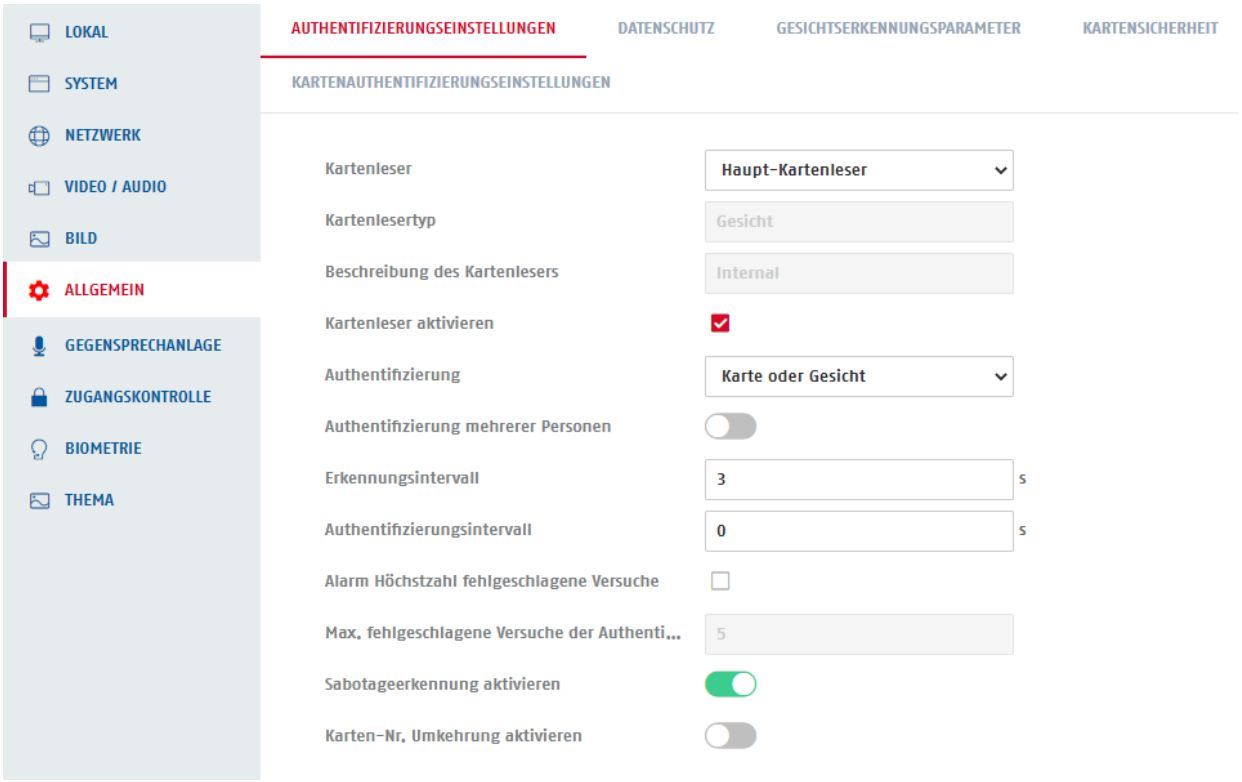
Bildkorrektur aktivieren: Aktivieren Sie diese Option, um das Aufhellen und Glätten des Videobildes zu verwenden.
Die Optionen werden nur am lokalen Bildschirm angewendet.



Bildfusion: Bei schlechten Lichtverhältnissen ist es möglich das Infrarotbild der 2. Kamera über das Bild der 1. Kamera zu legen. Somit entsteht ein helles Bild auch bei disen schlechten Lichtverhältnissen. Dies hilft bei der Erkennung von Gesichtern.
Empfindlichkeit: Je höher der Wert, desto früher wird das Infrarotbild dem normalen Bild überlagert.

8.1.6 Allgemein

8.1.6.1 Authentifizierungseinstellungen



Kartenleser: Festlegung, welcher Kartenleser konfiguriert werden soll, bzw. welche Kombination mit der Gesichtserkennung erfolgen soll.

Haupt-Kartenleser: Der eingebaute Kartenleser im Terminal.
Sub-Kartenleser: Ein z.B. über RS-485 angeschlossener Kartenleser.

Kartenlesertyp: *Nicht verwendet*
Beschreibung d. Kartenlesers: *Nicht verwendet*

Kartenleser aktvieren: Bei Deaktivierung dieser Option wird der komplette interne Kartenleser im Terminal deaktviert und kann nicht verwendet werden.

Authentifizierung: An dieser Stelle legen Sie die Anzahl und Art der Authentifizierungsmedien für alle Benutzer fest. Beispiel: Option „Karte und Gesicht“ bedeutet, dass alle eingelernten Benutzer beide Medien präsentieren müssen, um authentifiziert zu werden. Dies gilt nur, wenn die Benutzereinstellung den Geräteeinstellungen folgt.
Jeder Benutzer kann auch individuelle Authentifizierungsregeln besitzen.

Karte oder Gesicht
Karte oder Gesicht oder Passwort(Pin)
Karte und Gesicht
Karte
Gesicht und Passwort(Pin)
Gesicht und Karte
Gesicht

Hinweis: die Option „Fingerabdruck“ ist nicht verfügbar.

Authentifizierung mehrerer Personen: Mit dem Gesichtserkennungs Terminal ist es möglich, dass eine definierte Gruppe von Personen nötig ist, um erfolgreich Zutritt zu erlangen. Alle Personen der Gruppe müssen sich dazu innerhalb eines definierten Zeitraumes erfolgreich über Gesicht am Gerät authentifizieren.

Die weitere Programmierung der Personengruppen erfolgt über die ABUS CMS Software (siehe Kapitel 9).

Erkennungsintervall: Festlegen eines Zeitraums, bevor die Erkennung ein und derselben Person A wieder erfolgen soll. Wird in diesem Zeitraum eine Person B erkannt, so kann Person A wieder erkannt werden.

Authentifizierungsintervall: Diese Option limitiert die Erkennung einer Person A für den eingegebenen Zeitraum. Die Person A kann sich nur 1 Mal innerhalb dieses Zeitraumes authentifizieren.

Hinweis: Bei Verwendung der Mehrfachauthentifizierung Gesicht + Pin ist es ratsam, den Intervall auf min. 3 Sekunden einzustellen. Ansonsten erscheint nach Eingabe des Pins und erfolgreicher Türöffung sofort wieder die Pin-Eingabeseite.

Alarm Höchstzahl fehlgeschl. Versuche: Funktion für die Alarmierung bei mehrfacher falschen Anmeldung.

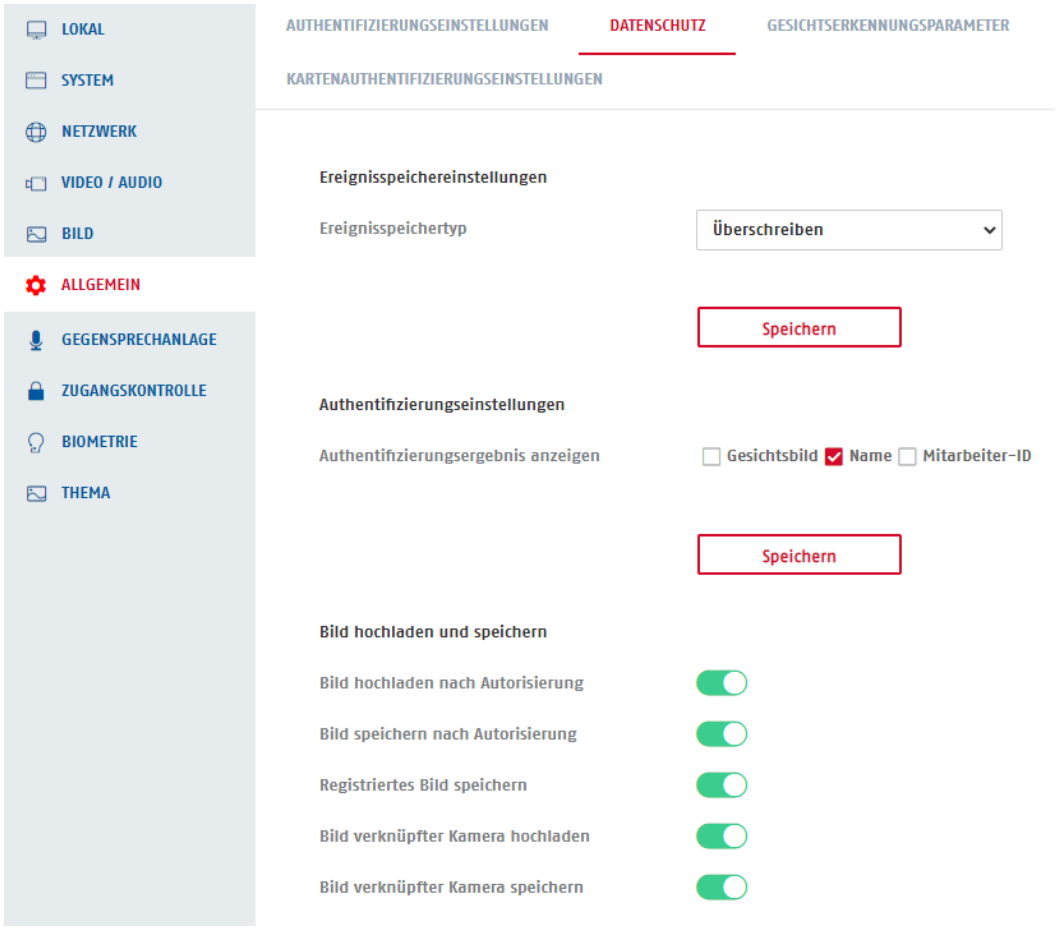
Max. fehlgeschl. Versuche: Anzahl (1 – 10) Versuche, bis Alarm ausgelöst wird

Sabotageerkennung aktivieren: Der Sabotageschalter befindet sich auf der Rückseite des Terminals. Falls dieser durch Abnehmen des Terminals von der Wand ausgelöst wird, so kann bei aktiver Netzwerk- und Internetverbindung eine PUSH Benachrichtigung zum verknüpften Konto der ABUS Link Station APP gesendet werden.

Karten-Nr. Umkehrung aktivieren: Die ausgelesene Kartennummer kann bei Bedarf in ihrer Verarbeitung umgekehrt werden.

Hinweis: Nach Aktivierung dieser Funktion müssen bereits eingelernte Karten erneut den Benutzern zugeordnet werden (erneutes Einlernen nötig).

8.1.6.2 Datenschutz



Ereignisspeichereinstellungen: Diese Option legt fest, wie oft und in welcher Frquenz der Ereignisspeicher gelöscht werden soll.

Überschreiben: Wenn das System 95% Ereignisspeicherstand feststellt, dann löscht es die ältesten 5%.

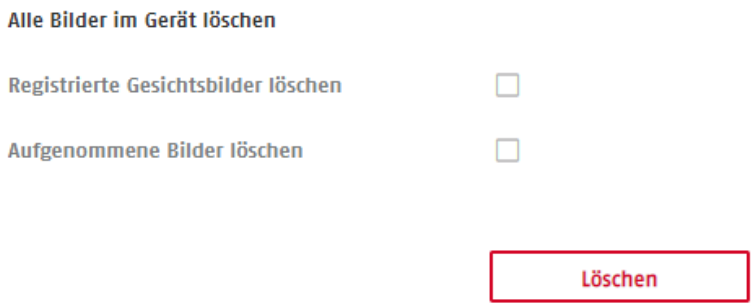
Alte Ereignisse periodisch löschen: wählen Sie einen Zeitraum von 10 Min. bis 86400 Min. Diese ist der Zeitraum, in dem Ereinisse noch gespeichert werden.

Alte Ereignisse nach angegebener Zeit löschen: Legen Sie einen Zeitpunkt fest an welchem täglich der Ereignisspeicher gelöscht werden soll.

Authentifizierungsergebnis anzeigen: Die Option legt die Art und Weise der Darstellung einer erkannten Person im Display fest. Die ausgewählten Optionen (Gesichtsbild, Name, Benutzer-ID) werden im Bereich der grünen Info-Meldung mit angezeigt.

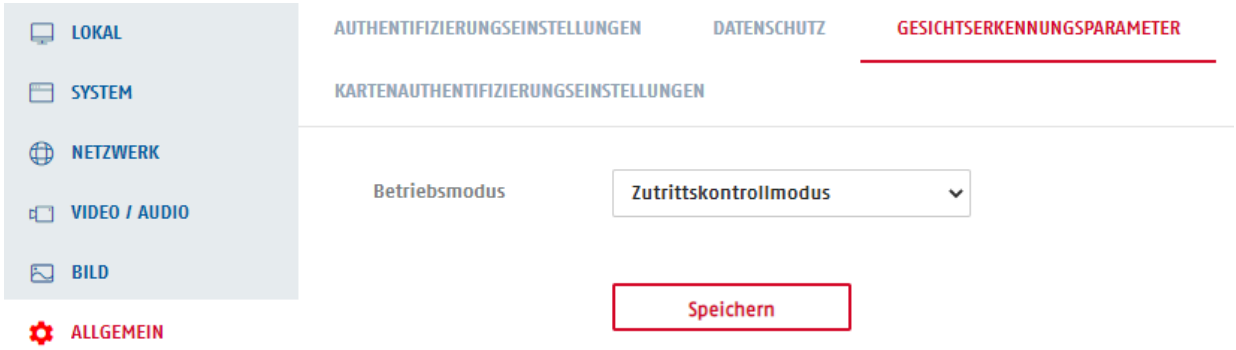
Bild hochladen und speichern:

Bild hochladen nach Autorisierung:	Nach Autorisierung einer Person wird das Bild vom Benutzer aus der Datenbank zu einer aktuell verbundenen ABUS CMS Software hochgeladen. Dies kann im Menüpunkt „ABUS CMS / Access Control / Monitoring“ in der Ereignisliste angezeigt werden.
Bild speichern nach Autorisierung:	Nach Autorisierung einer Person wird ein Bild dieser Szene im Terminal gespeichert. Der Aufruf erfolgt über Ereignisliste („Suchen“) im Web-Interface des FaceXess Gerätes.
Registriertes Bild speichern:	Nach Autorisierung einer Person wird das registrierte Bild in der Ereignisliste gespeichert.
Bild verknüpfter Kamera hochladen:	Übertragung des aktuellen Bildes zur ABUS CMS Software, falls eine verknüpfte Aktion über die ABUS CMS Software programmiert wurde.
Bild verknüpfter Kamera speichern:	Speicherung des aktuellen Bildes im Gerät, falls eine verknüpfte Aktion über die ABUS CMS Software programmiert wurde.



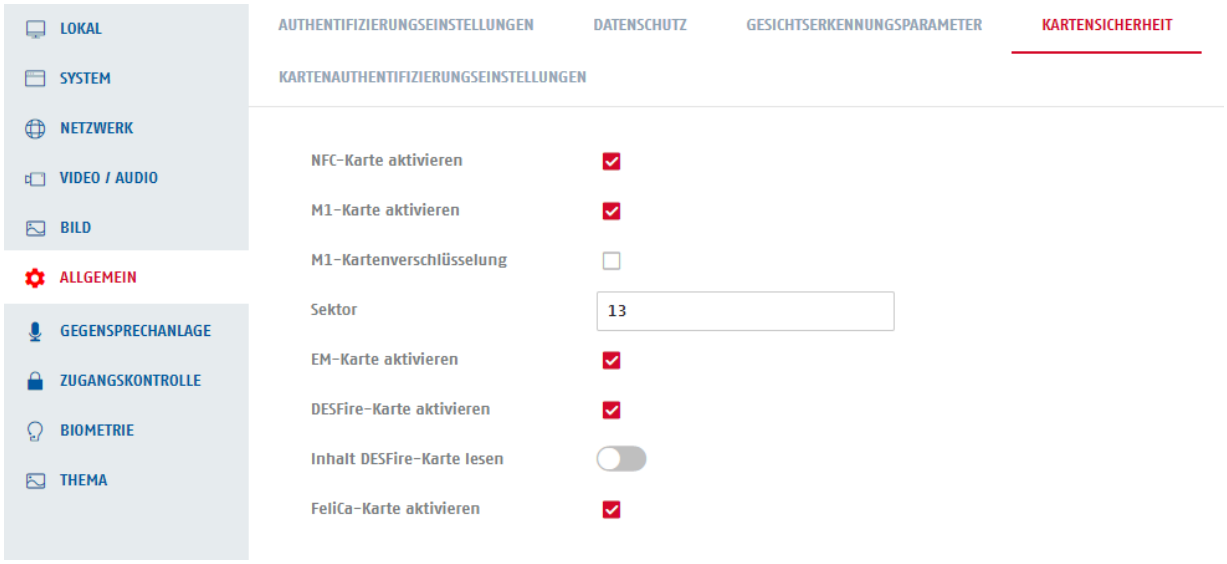
Registrierte Gesichtsbilder löschen:	Löschen aller Gesichtsbilder aller eingerichtetet Benutzer. Die Gesichtsbilder sind anschließend unwiederholbar gelöscht.
Aufgenommene Bilder löschen:	Alle Bilder, die in der Ereignisliste gespeichert wurden, werden gelöscht.

8.1.6.3 Gesichtserkennungsparameter



Diese gesamte Einstellungsseite ist auf die Option Zutrittskontrollmodus fixiert. Es gibt keine andere Auswahl.

8.1.6.4 Kartensicherheit



M1-Karte aktivieren:	Mifare Classic (M1) Karten.
M1-Kartenverschlüsselung:	Eine Sondervariante (selten) der Mifare Classic Karte (M1) mit Verschlüsselung. Nach Aktivierung können ausschließlich solche Mifare Classic Karten verwendet werden (keine Standard M1 Karten mehr).
EM-Karte aktvieren:	EM-Karten mit 125 kHz
DesFire-Karte aktivieren:	Mifare Desfire Karten (unverschlüsselt) können zwar gelesen werden, jedoch stehen die Sicherungsmechanismen der Desfire Karte nicht zur Verfügung.
Inhalt DesFire-Karte lesen:	Funktion aktuell nicht unterstützt
FeliCa-Karte aktivieren:	Der Kartenleser kann Karten vom Typ Sony FeliCa erkennen und verwenden.

Es wird empfohlen, die Kartenlesefunktion nur in Verbindungs einer mehrfachen Auswertung von Authentifizierungsmerkmalen zu verwenden (z.B. Karte + Gesicht oder Gesicht + PIN).

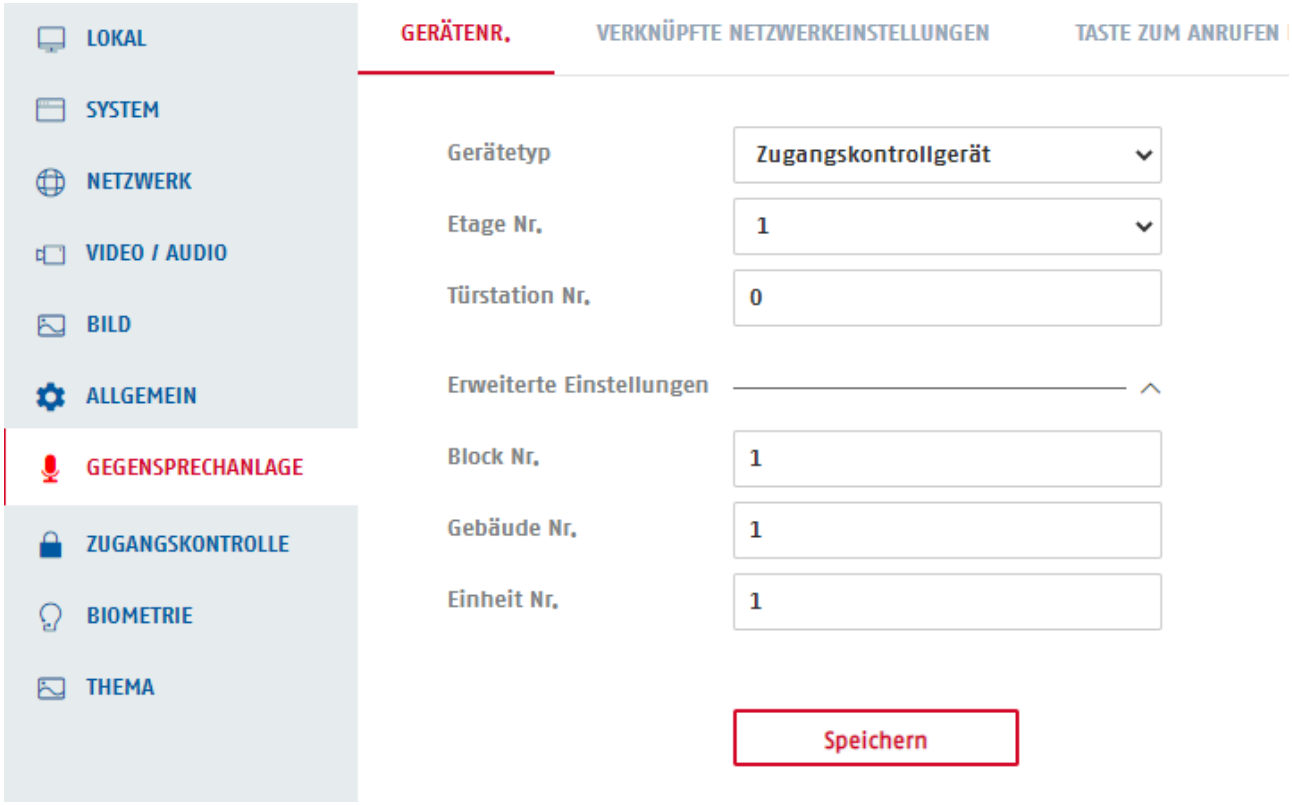
Der Kartenleser kann aktuell nur Karten vom Typ Mifare Classic (M1) lesen. Karten von ABUS Security Center mit Verschlüsselung können nicht gelesen werden.
Karten vom Typ Mifare Desfire ohne Verschlüsslung können zwar gelesen werden, fallen jedoch in ihrer Sicherheitsperformance auf das Niveau von Mifare Classic zurück.

8.1.6.5 Kartenauthentifizierungseinstellungen

Diese Funktion ist gültig in Verbindung mit einem angeschlossenem Wiegand Kartenleser (über Anschlusskabel „Wiegand W0, W1 und GND). Es wird hierbei festgelegt, in welchen Format die Kartendaten ausgelesen werden (komplette Kartennummer ohne zusätzliche Kodierung, Wiegand 26 Bit oder 34 Bit).

8.1.7 Gegensprechanlage

8.1.7.1 Geräte-Nummer



Für ein Verwendung des Terminals in Verbindung mit Monitor-Innenstationen wählen Sie zunächst die Option „Zugangskontrollgerät“ oder „Türstation“ aus.

Gerätetyp: Zugangskontrollgerät oder Türstation – Das Terminal arbeitet als Haupt-Gesichtserkennungsterminal, mit Option als Gegensprechanlage für max. 3 Wohneinheiten

Außentürstation – nicht verwendet

Verwendung des Gerätes am Haupteingang (oder einziger Eingang)
Als nächtest muss die „Türstation Nr.“ den Wert 0 haben. Die weiteren 3 Hauptmonitor der Wohnungen verwenden die Nummern 1, 2 und 3.

Verwendung des Gerätes am Nebeneingang
Das Gerät arbeitet als Gesichtserkennungsterminal am Nebeneingang (max. 99), mit Option als Gegensprechanlage für max. 3 Wohneinheiten. Ein Haupt-Gesichtserkennungsterminal muss im System vorhanden sein.
Der Wert für den Punkt „Türstation Nr.“ muss 1 – 99 betragen.

Nach Umstellung der „Türstation Nr.“ von 0 auf 1 (oder höher) startet das Gerät neu.

Die weiteren Einstellungen für Block, Gebäude und Einheit Nr. können in dieser Anwendung jeweils auf dem Wert „1“ verbleiben.

8.1.7.2 Verknüpfte Netzwerkgeräte

Die Funktion SIP Server wird aktuell nicht unterstützt.

Falls der Wert für „Türstation Nr.“ im Menü „Geräte Nummer“ 1 oder höher ist, so erscheint ein weiteres Eingabefeld „Haupt Türstation IP“

Bei Verwendung des Terminals als Gerät am Nebeneingang muss im Punkt „Hauptstation Türstation IP“ die IP-Adresse des ersten Gesichtserkennungs-Terminals (Haupteingang) eingetragen werden.

8.1.7.3 Taste zum Anrufen

Diese Konfigurationsseite beschreibt die Konfiguration der Ruftaste(n) auf dem Touch Display des Terminals.

Angegebene Innenstation anrufen:	Es können bis 3 Ruftasten für 3 unterschiedliche Apparments eingeblendet und aktiviert werden. Die Reihenfolge der Tasten bei der Anzeige im Display ist von unten nach oben umgesetzt. Die Reihenfolge kann aber über die „Apartmentnr.“ des Monitors manipuliert werden. Die Angabe der „Zimmernummer“ ist gleichzeitig die Einstellung der Apparmentnummer im jeweiligen Hauptmonitor. Die Bezeichnung der Namen erlaubt deusche Umlaute sowie Groß- und Kleinschreibung. Die Länge der Tastenbezeichnung sollte 22 Zeichen nicht überschreiten.
Anruf-Überwachungszentrale (CMS):	Bei Auswahl erscheint nur eine Ruftaste „Management Center“ im Display. Bei Drücken der Ruftaste wird ein Ruf zu einer verbundenen ABUS CMS Software getätigt. In der CMS Software erscheint ein Pop-Up Fenster, worüber eine 2-Wege-Audio Kommunkation aufgebaut werden kann, oder das Relais am Terminal entfernt geschalten werden kann (Tür öffnen).
APP:	Anruf der verbundenen Link Station App.

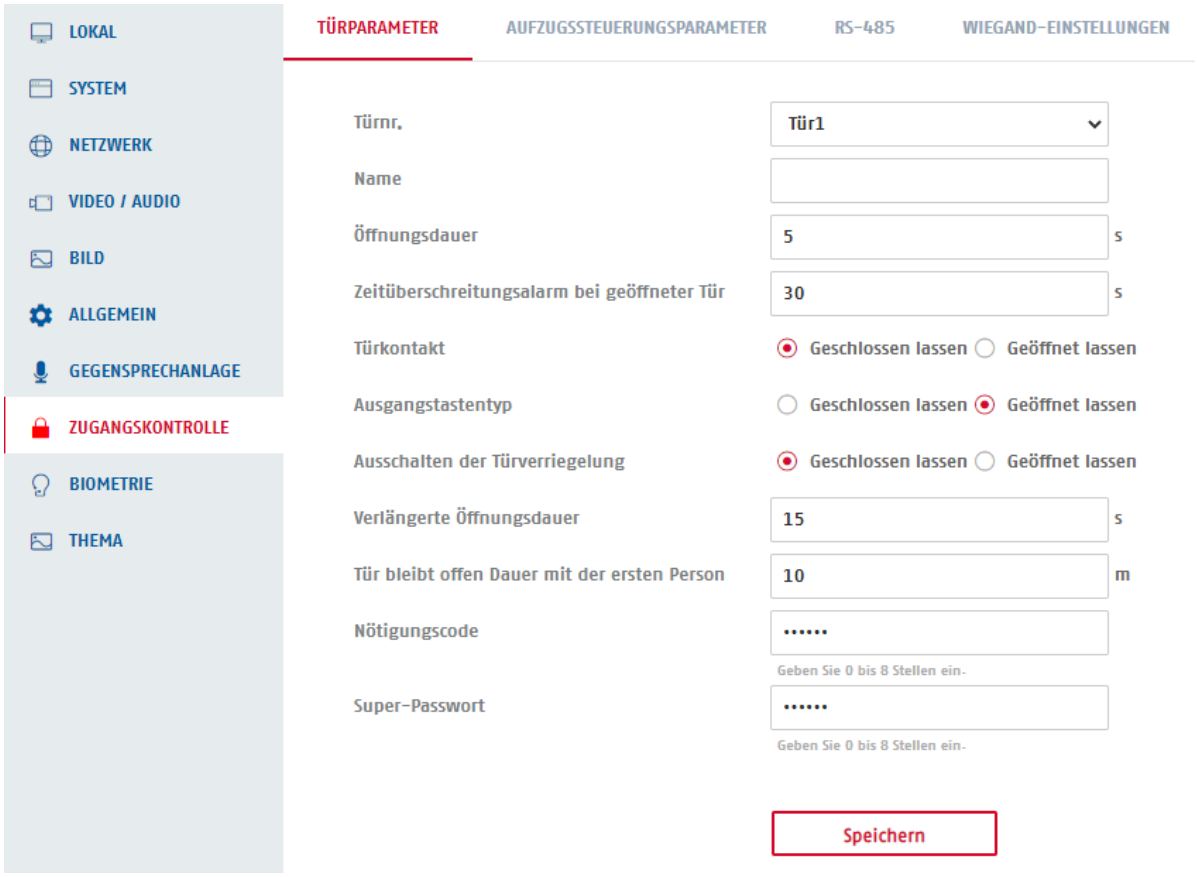
Falls das System 2 oder 3 Monitore enthält, so dann dies auch als Gegensprechanlage innerhalb des Gebäudes zwischen den Wohnungen verwendet werden. Die Eingabe des Rufkommandos am jeweiligen Monitor lautet dann wie folgt.

Beipiel INTERCOM ruf zwischen Innenstationen 1, 2 oder 3:

Ruf von Monitor 1 zu Monitor 2:	1-1-1-2
Ruf von Monitor 3 zu Monitor 1:	1-1-1-1

8.1.8 Zugangskontrolle

8.1.8.1 Türparameter



Türnummer: Das Terminal stellt den Zugang über eine Tür dar. Der Wert ist auf „Tür 1“ fixiert.
Name: Bezeichnung für die Tür

Öffnungsdauer (1 – 255 Sek.): Dauer für die Schaltzeit des Relais nach erfolgreicher Authentifizierung.

Zeitüberschreitungsalarm bei geöffnetet Tür: Falls die Tür länger als die eingestellte Zeit in diesem Punkt geöffnet bleibt wird dieser Status in der ABUS CMS Software in der Ereignisliste angezeigt.

Türkontakt: Es kann ein Türkontakt an der Tür installiert werden, der den Öffnungsstatus der Tür widerspiegelt. Dafür stehen 2 Kontakte am Anschlusskabel zur Verfügung. Der Status wird in der ABUS CMS Software in der Ereignisliste angezeigt.

Ausgangstastentyp: Die Ausgangstaste (BTN) hat keine Funktion.

Verlängerte Öffnungsdauer: Personen mit erweitertem Zutritt erhalten eine längere Öffnungdauer.

Tür bleibt offen mit der ersten Person: Dieser Punkt steht in Verbindung mit der Funktion „Tür offen lassen nach erster Person für Zeitraum“. Nach Erkennen einer Person aus einer definierten Personengruppe kann die Tür für diesen Zeitraum offen bleiben.

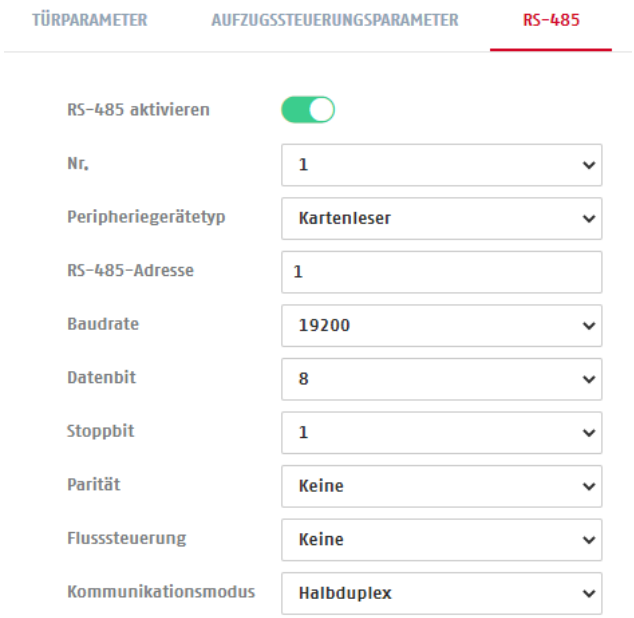
Nötigungscode: Falls eine Person diesen Code am Terninal eingibt, so wird die Tür geöffnet und sogleich ein Nötigungsalarm and die verbundene ABUS CMS Software gesendet.

Super-Passwort:	Ein globaler Pin-Code für die Türöffnung. Super-Passwort und Nötigungscode müssen unterschiedlich sein.

8.1.8.2 Aufzugssteuerung

Die Option Aufzugssteuerung wird aktuell nicht verwendet.

8.1.8.3 RS-485



Der RS-485 Schnittstelle wir in erster Linie im Zusammenhang mit dem ABUS Sicherheitsmodul TVHS20340 verwendet. Dieses Modul dient zum sicheren Anschluss aller exernen Komponenten wie z.B. einem Türöffner.

Für die Verwendung des Sicherheitsmoduls muss als Peripheriegerätetyp die Option „Zugangs-Controller“ eingestellt werden.

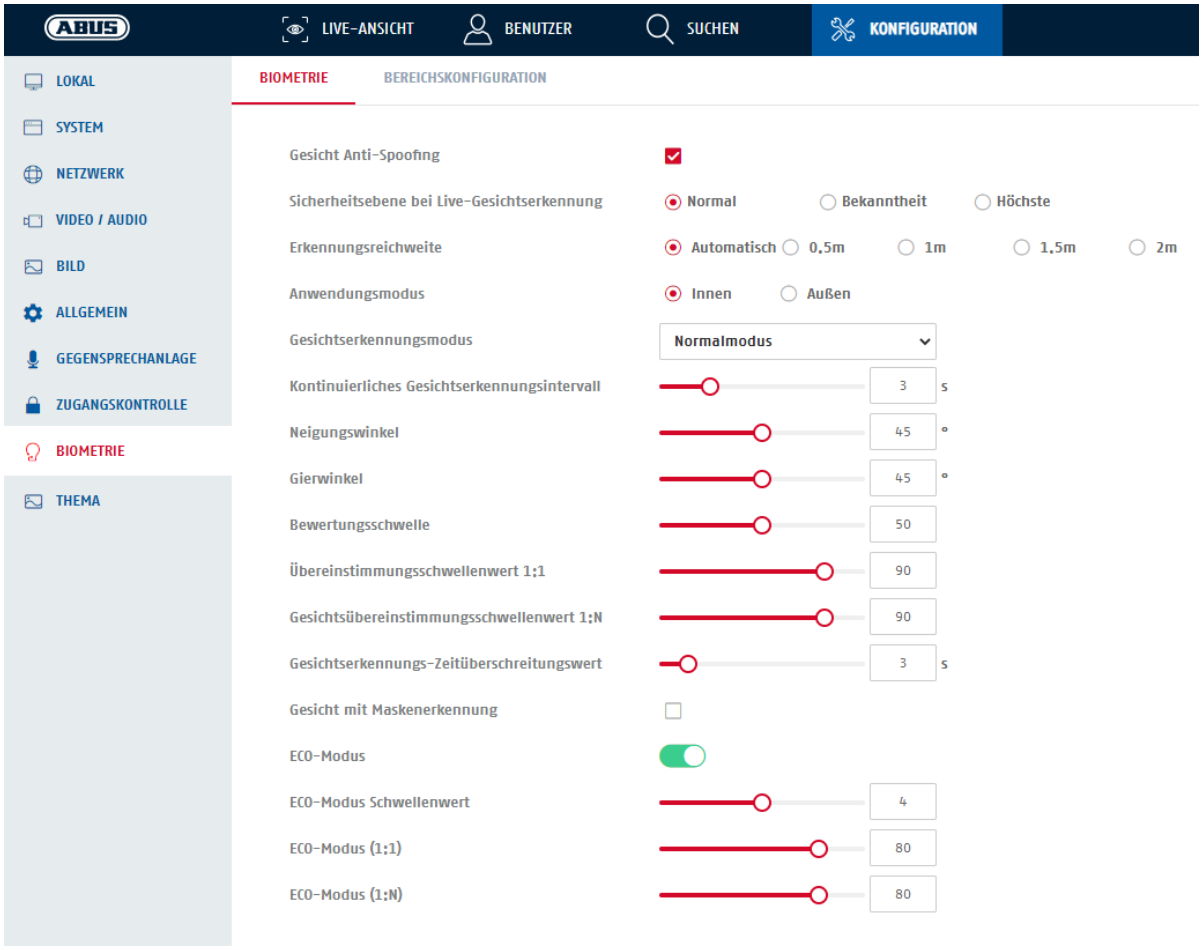
8.1.8.4 Wiegand-Einstellungen

Das Terminal verfügt über ein sog. Wiegand-Schnittstelle. Die Schnittstelle kann als Eingang oder Ausgang konfiguriert werden.

Als Eingang kann ein Wiegand Kartenleser an die Wiegand-Schnittstelle angeschlossen werden.

Als Ausgang können Kartendaten nach Erfassung an eine Zutrittskontroleinheit versendet werden, welche das Wiegand Protokoll entgegennehmen kann.
Info: Bei Erkennen eines Gesichtes und erfolgreicher Authentifizierung wird die als erstes programmierte Kartennummer über die Wiegand-Scnittstelle versendet.

8.1.9 Biometrie



Gesicht Anti-Spoofing: Anti-Spoofing ist der Fachbegriff für die Verhinderung von Manipulationsversuchen. Es gibt diverse Paramter, um die Echtheit einer vor dem Terminal stehenden Person zu überprüfen.

Sicherheitsebene bei Live-Gesichtserkennung: Die Sicherheitsstufe kann in 3 Stufen (Normal, Mittel, Hoch) eingestellt werden. Je höher die Stufe eingestellt ist, desto länger dauert die Erkennung von Personen, um so besser ist die Erkennung aber auch gegen Manipulation geschützt (z.B. Angriff durch Vorhalten eines gedruckten Bildes).

Eine noch höhere Sicherheit kann durch eine Verwendung einer Mehrfaktor-Authentifizierung erreicht werden (z.B. Gesicht + Pin).

Erkennungsreichweite: Die Einstellung der Erkennungsdistanz (0,5 bis 2 Meter, Auto) kann eine ungewünschte Erkennung bei Vorbeilaufen vermeiden. Prinzipiell ist davon abzuraten, eine größere Erkennungsdistanz einzustellen, da die Gesichtsmerkmale bei kürzerer Distanz deutlicher für die Kamera erkennbar sind.

Bei der Option Auto ist keine Distanzgrenze vorhanden, das Terminal entscheidet aufgrund der Erkennbarkeit eines Gesichtes selbst über den Beginn der Gesichtsanalyse.

Anwendungsmodus: Die Auswahl „innen“ oder „außen“ beeinflusst diverse Kameraparameter (interne Parameter).

Gesichtserkennungsmodus: Normalmodus – In diesem Modus ist es möglich, Gesichtsbilder von Personen auch über die ABUS CMS Software über die Netzwerkschnittstelle hochzuladen.

Erweiterter Modus – In diesem Modus ist das Hochladen von Gesichtsbildern von Personen über die ABUS CMS Software nicht möglich. Die Gesichtsbilder müssen immer lokal am Gerät eingelernt werden.

 Nach Umstellung und Speicherung des Erweiterten Modus startet das Gerät neu und es werden alle bisher gespeicherten Gesichtsbilder aller eingelernen Benutzer gelöscht. Die Benutzereinträge selbst bleiben erhalten.
Alle Benutzer müssen anschließend neu direkt am FaceXess Gerät eingelernt werden.

 Bitte ändern Sie den Modus nicht, nachdem Sie begonnen haben, Personen einzulernen.

Kontinuierliches Gesichtserkennungsintervall: Einstellung, alle wieviel Sekunden die Gesichtserkennung durchgeführt werden soll (1-10 Sek.)

Neigungswinkel: Dies ist der Winkel, wenn Personen von zu weit oben oder unten auf das FaceXess Gerät schauen.

Gierwinkel: Dies ist der Winkel der max. Gesichtsrotation vor der Kamera (Kopf wird schief gehalten).

Bewertungsschwelle:

Übereinstimmungsschwellwert 1:1: Dieser Wert gibt an, wie genau die im Live-Bild erkannten Gesichtsmerkmale mit dem gespeicherten Bild in der Datenbank übereinstimmen muss. Ein hoher Wert bedeutet, es muss eine hohe Übereinstimmung vorliegen.
Dieser Wert gilt nur bei Verwendung von eine Mehrfach-Authentifizierung (z.B. Gesicht + Karte).

Übereinstimmungsschwellwert 1:N: Dieser Wert gibt an, wie genau die im Live-Bild erkannten Gesichtsmerkmale mit dem gespeicherten Bild in der Datenbank übereinstimmen muss. Ein hoher Wert bedeutet, es muss eine hohe Übereinstimmung vorliegen.
Dieser Wert gilt für den Abgleich des Live-Bildes mit allen Gesichtsbildern in der Datenbank (bei Einfach-Authenifizierung).

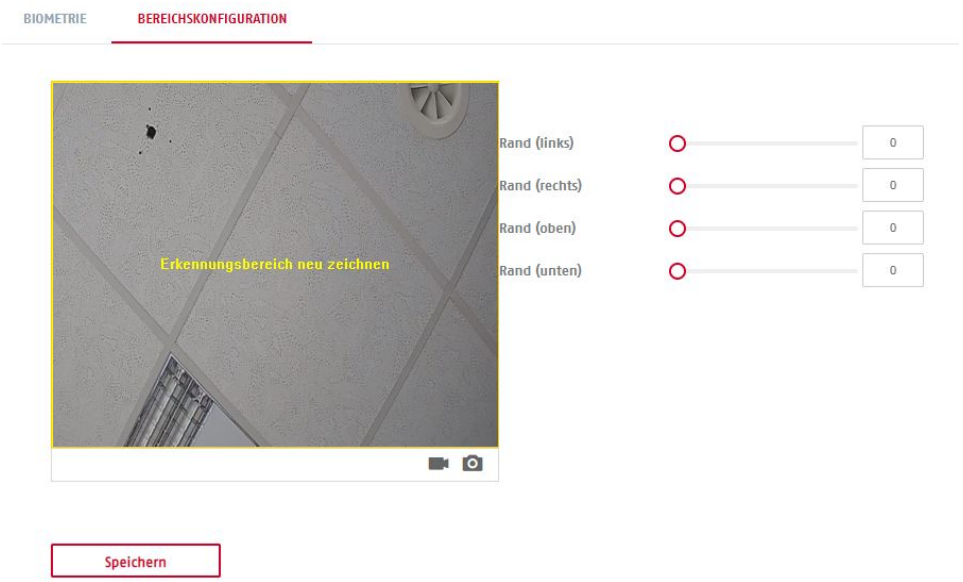
Gesichtserkennung Zeitüberschreitung: Für dieser maximale Dauer wird die Gesichtserkennung nach Erkennen einer Person durchgeführt. Falls bis zum Ablauf dieser Zeit das Gesicht nicht erkannt wurde, so erscheint eine Fehlermeldung.

Gesicht mit Maskenerkennung: Das Gerät kann erkennen, ob eine Person einen Mund-Nasen-Schutz (umgangssprachlich Maske) trägt.
Die erkannte Person kann an das Tragen der Maske erinnert werden, oder die Person muss eine Maske tragen, um Zutritt zu erlangen.

ECO-Modus: Bei schwachen Lichtverhältnissen kann das Terminal durch die zusätzliche Nutzung von Infrarot-Licht die Erkennung verbessern. (Extended Camera Operation / Erweiterte Kamera Verwendung)

ECO Schwellwert: Je höher der Wert, desto schneller wird der ECO Modus durch das Terminal verwendet.
ECO Modus (1:1): Analog normale 1:1 Sicherheitsstufe.
ECO Modus (1:N): Analog normale 1:N Sicherheitsstufe.

8.1.9.1 Bereichskonfiguration

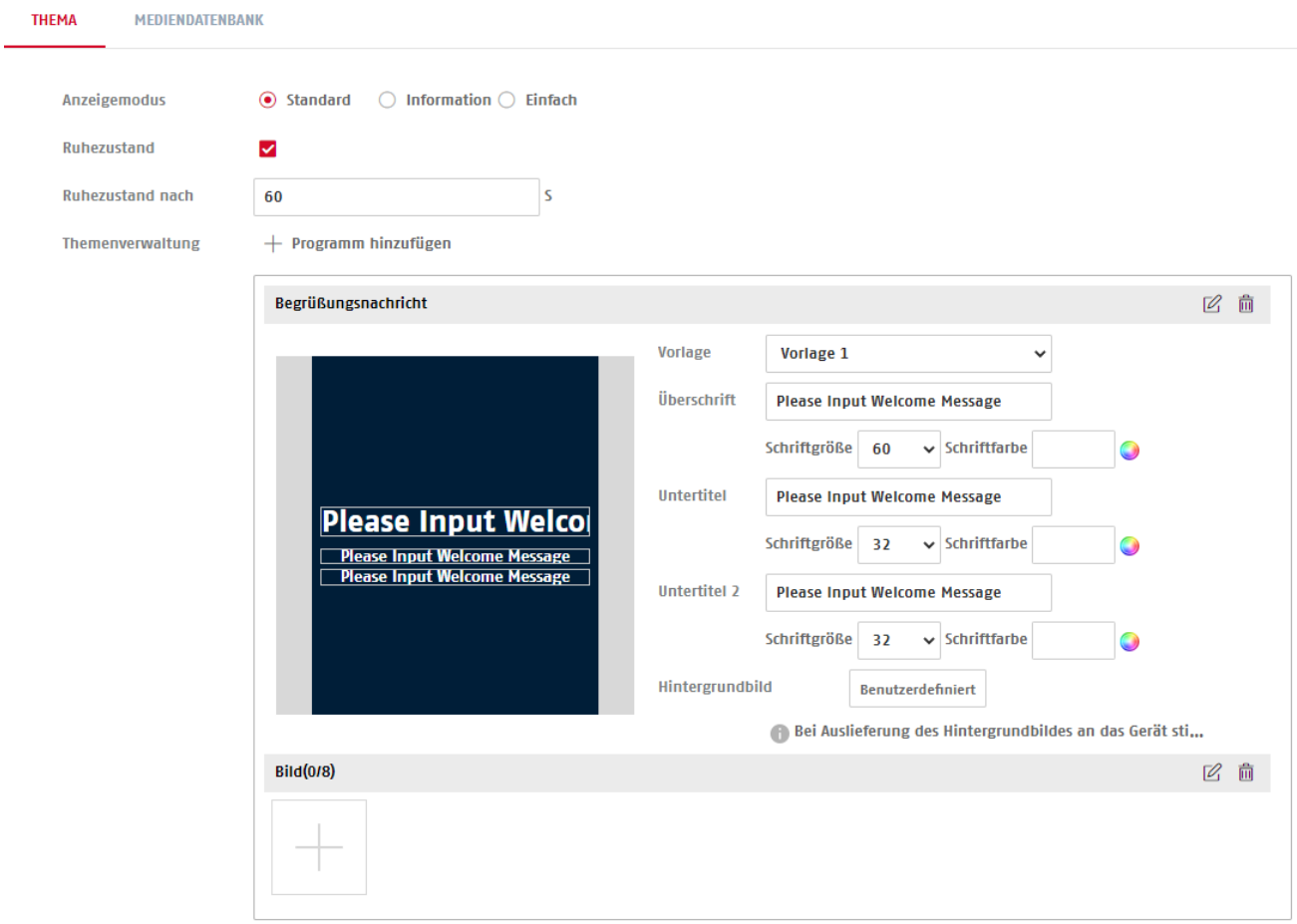


Die Funktion limitiert den Erkennungsbereich für die Gesichtserkennung, und kann somit störende Bereiche ausblenden. Die Markierung erfolgt über die Maus im Vorschaubild.

8.1.10 Thema

Es können 3 verschiedene Darstellungen der Hauptseite am Display eingestellt werden.

Standard: Es werden bei Konfiguration nur Ruftaste(n), Pin-Code und QR-Code Taste angezeigt, sowie bei Wunsch das Vorschauvideo der Person.
Einfach: Es werden bei Konfiguration nur Ruftaste(n), Pin-Code und QR-Code Taste angezeigt. Das Vorschauvideo wird nicht angezeigt. Die Gesichtserkennung im Hintergrund aktiv.
Information: Der Unterschied zum Standardmodus ist, dass im oberen Bereich des Displays Platz für die Anzeige von Informationen ist.



Ruhezustand: Der Monitor des Terminals zeigt nach 20 Sekunden ohne eine Bildschirmaktivität das Standard-Hintergrundbild an (fester Zeitraum).

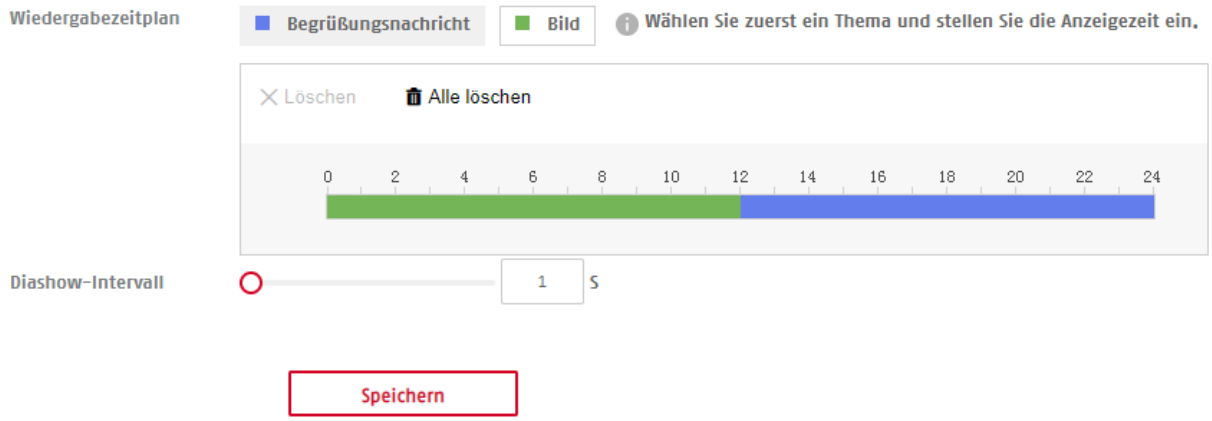
Nach weiteren 20 – 999 Sekunden tritt der Monitor in den Ruhezustand, d.h. das Display ist aus. Dieser Zeitraum kann eingestellt werden.

Themenverwaltung:
Programm hinzufügen: In diesem Punkt können Text und Bilder definiert werden, sowie deren Anzeigeart. Ein Programm ist bereits als Standard voreingestellt. Dies kann auch gelöscht werden. Sie können ein neues Programm erstellen.

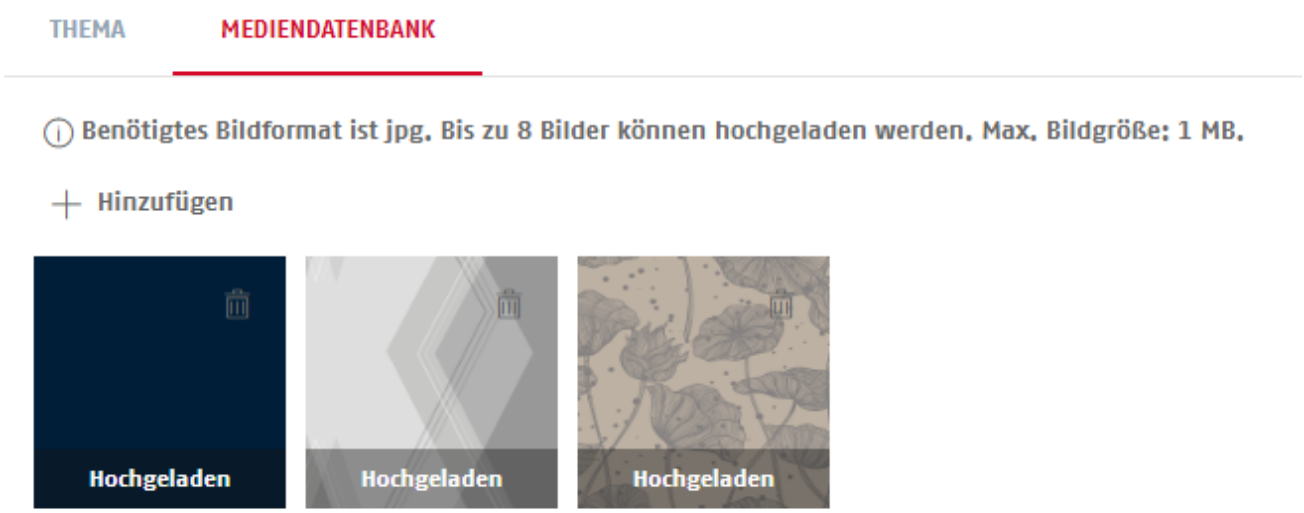
Begrüßungsnachricht: Text, Schriftgröße, Schriftfarbe und Hintergrundbild können definiert werden.

Bild: Es können max. 8 Bilder definiert werden, welche rollierend dargestellt werden können.

Die Darstellung der Texte und Bild kann über einen Zeitplan definiert werden (z.B. Texte am Tag und Bilder in der Nacht).



8.1.10.1 Mediendatenbank



Hinzufügen: Es können max. 8 Bilder in der Mediendatenbank vorhanden sein. 3 Bilder sind bereits hinterlegt, weitere Bilder können hochgeladen werden.

Das Bildformat muss wie folgt sein:
- jpg Format, max. 1 MB groß, 600 x 704 Pixel, 24 Bit Farbtiefe

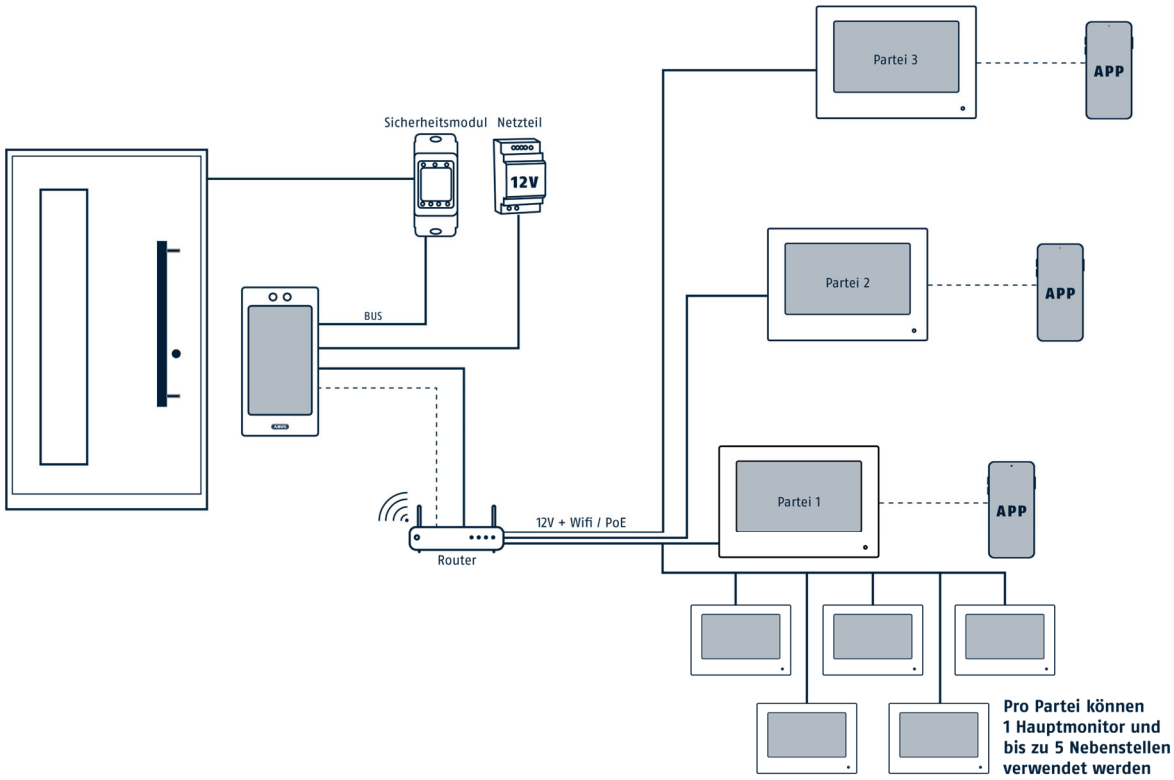
9. Einbindung und Verwendung von Monitoren der Moduvis Türsprechanlage

9.1 Systemübersicht Face Terminal / Monitore(e)

Die jeweiligen Hauptmonitore in den Wohnungen kommunizieren über das IP-Netzwerk mit dem FaceXess Gerät. Die Verbindung der Geräte wird im nächsten Abschnitt beschrieben.

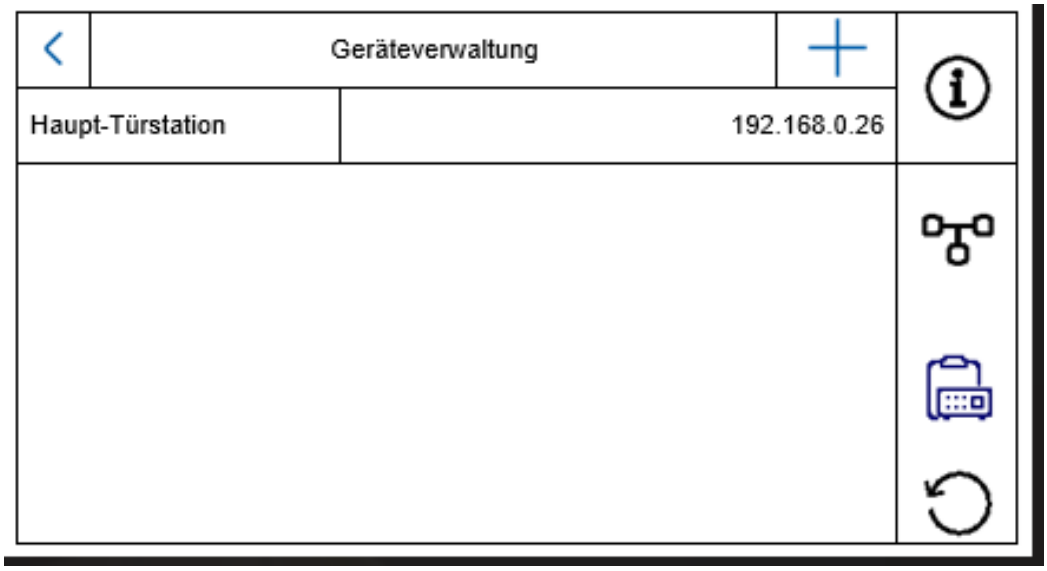
Jeder Hauptmonitor kann weitere 5 Erweiterungsmonitor erhalten. Von allen Monitoren ist die 2-Wege Audio Kommunikation nach Klingelaktion sowie die Öffnung der Tür möglich.

Die ABUS Link Station App kann sich über einen ABUS Link Station Account mit dem Hauptmonitor verbinden. Somit sind die Hauptbenutzer der Wohnungen getrennt (bei Klingeln an Wohnung 1 wird nur der verbundene Link Station Account der Wohnung 1 benachrichtigt).



9.2 Konfiguration von Face Terminal und Monitor(en)

Für die Verbindung vom FaceXess Gerät mit dem jeweiligen Hauptmonitor der Wohnung muss die IP-Adresse (LAN oder WLAN) des FaceXess Gerätes in den Hauptmonitor unter Geräteverwaltung / Haupt-Türstation eingetragen werden.



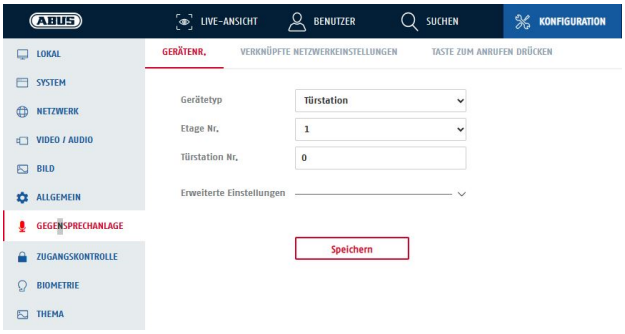
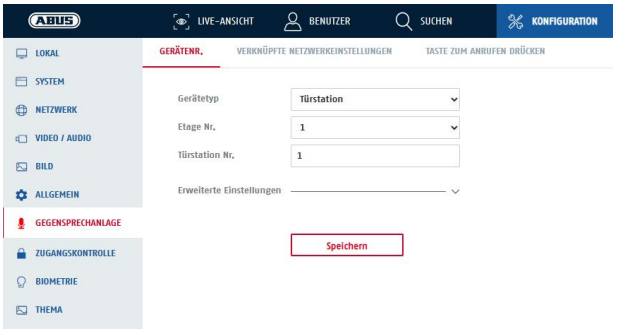
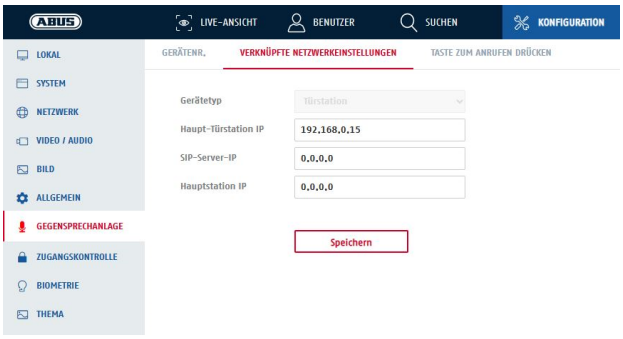
9.3 Verwendung von FaceXess als Nebentür

Ein FaceXess Gerät kann in Kombination mit Moduvis Monitoren und weiteren FaceXess Geräten für Haupt- und Nebentüren verwendet werden.

Praktische Beispiele für Konfigurationen mit Nebentüren sind z.B.:

Haupeingang: FaceXess Gerät (TVHS30000)
Nebeneingang: FaceXess Gerät (TVHS30000)

Es können bis zu 99 Geräte für Nebeneingänge programmiert werden.
Die Programmierung erfolgt über das Web-Interface des FaceXess Gerätes oder über die ABUS CMS Software.

Einstellung am Gerät für den Haupteingang	Einstellung am Gerät für die 1. Nebentür
Menüpunkt: Konfiguration / Gegensprechanlage / Gerätenr. Gerätetyp: Türstation Türstation-Nr.: 0 	Menüpunkt: Konfiguration / Gegensprechanlage / Gerätenr. Gerätetyp: Türstation Türstation-Nr.: 1 Menüpunkt: Konfiguration / Gegensprechanlage / Verknüpfte Netzwerkeinstellungen Haupt-Türstation IP: IP Adresse des FaxeXess Gerätes am Haupteingang (hier z.B: 192.168.0.15)  

10. Wartung und Reinigung

10.1 Wartung

Überprüfen Sie regelmäßig die technische Sicherheit des Produkts, z.B. Beschädigung des Gehäuses.

Wenn anzunehmen ist, dass ein gefahrloser Betrieb nicht mehr möglich ist, so ist das Produkt außer Betrieb zu setzen und gegen unbeabsichtigten Betrieb zu sichern.

Es ist anzunehmen, dass ein gefahrloser Betrieb nicht mehr möglich ist, wenn

- das Gerät sichtbare Beschädigungen aufweist,
- das Gerät nicht mehr funktioniert

	**Bitte beachten Sie:** Das Produkt ist für Sie wartungsfrei. Es sind keinerlei für Sie überprüfende oder zu wartende Bestandteile im Inneren des Produkts, öffnen Sie es niemals.

10.2 Reinigung

Reinigen Sie das Produkt mit einem sauberen trockenen Tuch. Bei stärkeren Verschmutzungen kann das Tuch leicht mit lauwarmem Wasser angefeuchtet werden.

	Achten Sie darauf, dass keine Flüssigkeiten in das Gerät gelangen. Verwenden Sie keine chemischen Reiniger, dadurch könnte die Oberfläche des Gehäuses und des Bildschirms angegriffen werden (Verfärbungen).

11. Entsorgung

	Achtung: Die EU-Richtlinie 2002/96/EG regelt die ordnungsgemäße Rücknahme, Behandlung und Verwertung von gebrauchten Elektronikgeräten. Dieses Symbol bedeutet, dass im Interesse des Umweltschutzes das Gerät am Ende seiner Lebensdauer entsprechend den geltenden gesetzlichen Vorschriften und getrennt vom Hausmüll bzw. Gewerbemüll entsorgt werden muss. Die Entsorgung des Altgeräts kann über entsprechende offizielle Rücknahmestellen in Ihrem Land erfolgen. Befolgen Sie die örtlichen Vorschriften bei der Entsorgung der Materialien. Weitere Einzelheiten über die Rücknahme (auch für Nicht-EU Länder) erhalten Sie von Ihrer örtlichen Verwaltung. Durch das separate Sammeln und Recycling werden die natürlichen Ressourcen geschont und es ist sichergestellt, dass beim Recycling des Produkts alle Bestimmungen zum Schutz von Gesundheit und Umwelt beachtet werden.

12. Technische Daten

Die technischen Daten der einzelnen Kameras sind unter www.abus.com über die Produktsuche verfügbar.

13. Open Source Lizenzhinweise

Wir weisen auch an dieser Stelle darauf hin, dass die Netzwerküberwachungskamera u.a. Open Source Software enthalten. Lesen Sie hierzu die dem Produkt beigefügten Open Source Lizenzinformationen.