

TVHS30000



Ⓧ **Bedienungsanleitung Software**

Version 10/2023



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 10/2023



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!

Alle enthaltenen Firmennamen und Produktbezeichnungen sind Warenzeichen der jeweiligen Inhaber. Alle Rechte vorbehalten.

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, Styroporsteile 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 Niederspannungstromkreis 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	9
2. Symbolerklärung	9
3. Merkmale und Funktionen	10
4. Gerätebeschreibung	11
5. Beschreibung der Anschlüsse	11
6. Erstinbetriebnahme	11
6.1 Aktivierung des Gerätes über den lokalen Touch Monitor	11
6.2 Aktivierung des Gerätes über den ABUS IP Installer.....	11
6.3 Aktivierung des Gerätes über den Web-Browser.....	12
6.4 Video-Plugin installieren	13
7. Konfiguration und Bedienung über den Touch Monitor	14
7.1 Einrichtungs-Assistent	14
7.2 Hauptbedienseite	15
7.2.1 Ansichtoptionen (Themen).....	15
7.2.2 Symbole und Informationsanzeigen.....	16
7.2.3 Einstellbare Bedientasten	16
7.3 Administrator-Menü.....	17
7.3.1 Benutzer.....	17
7.3.2 Zutrittsoptionen	20
7.3.3 Kommunikation	21
7.3.4 Grundeinstellungen.....	23
7.3.5 Biometrische	24
7.3.6 Datenbank.....	26
7.3.7 Systemwartung	27
7.3.8 Darstellung.....	28
8. Konfiguration und Bedienung über Web-Browser	29
8.1 Konfiguration über Web-Browser.....	29
8.1.1 Lokale Konfiguration	29
8.1.2 System	31
8.1.2.1 Systemeinstellungen.....	31
8.1.2.1.1 Grundlegende Informationen	31
8.1.2.1.2 Zeiteinstellungen	32
8.1.2.1.3 DST / Sommerzeit.....	33
8.1.2.1.4 Über / Lizenzinformationen	33
8.1.2.2 Wartung	34
8.1.2.2.1 Aktualisierung und Wartung.....	34
8.1.2.2.2 Protokollabfrage / Logbuch	35
8.1.2.3 Sicherheit.....	35
8.1.2.3.1 Sicherheitsdienst.....	35
8.1.2.3.2 Zertifikatsverwaltung	35
8.1.2.4 Benutzerverwaltung	36
8.1.2.4.1 Scharfschaltung / Unscharfschaltung Info.....	36
8.1.3 Netzwerk.....	37
8.1.3.1 TCP/IP	37
8.1.3.2 Port	38
8.1.3.3 WiFi.....	39

8.1.3.4	Cloud Zugriff / ABUS Link Station	40
8.1.3.5	HTTP Socket.....	41
8.1.4	Video.....	42
8.1.4.1	Video.....	42
8.1.4.2	Audio.....	43
8.1.4.3	Audio-Ausgabe	43
8.1.5	Bild.....	44
8.1.6	Allgemein	46
8.1.6.1	Authentifizierungseinstellungen	46
8.1.6.2	Datenschutz	48
8.1.6.3	Gesichtserkennungsparameter.....	49
8.1.6.4	Kartensicherheit	50
8.1.6.5	Kartenauthentifizierungseinstellungen	51
8.1.7	Gegensprechanlage.....	52
8.1.7.1	Geräte-Nummer	52
8.1.7.2	Verknüpfte Netzwerkgeräte	53
8.1.7.3	Taste zum Anrufen.....	54
8.1.8	Zugangskontrolle	55
8.1.8.1	Türparameter	55
8.1.8.2	Aufzugssteuerung	56
8.1.8.3	RS-485.....	56
8.1.8.4	Wiegand-Einstellungen.....	57
8.1.9	Biometrie.....	58
8.1.9.1	Bereichskonfiguration	60
8.1.10	Thema.....	61
8.1.10.1	Mediendatenbank	62
9.	Einbindung und Verwendung von Monitoren der Moduvis Türsprechanlage	63
9.1	Systemübersicht Face Terminal / Monitore(e).....	63
9.2	Konfiguration von Face Terminal und Monitor(en).....	64
9.3	Verwendung von FaceXess als Nebentür.....	65
10.	Konfiguration und Bedienung über die ABUS CMS Software.....	66
10.1	Einbindung in ABUS CMS Software	66
10.2	Personen verwalten	67
10.3	Zutrittsgruppen verwalten und übertragen in FaceXess	68
10.4	Ereignisanzeige und Ereignissuche.....	70
10.5	Zeitplangesteuerte Zutritte	70
11.	Wartung und Reinigung	71
11.1	Wartung	71
11.2	Reinigung.....	71
12.	Entsorgung.....	72
13.	Technische Daten	72

1. Bestimmungsgemäße Verwendung

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




	<p>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.</p> <p>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.</p>
---	---

	<p>Bei Verlassen des Hauses oder der Wohnung für längere Zeit ist es ratsam Türen mechanisch zu verriegeln.</p>
---	---

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

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

3. Merkmale und Funktionen

Türsprechanlage mit Touchscreen, Kamera & Gesichtserkennung für interaktionslosen Zutritt.

Die Türstation identifiziert berechnete 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 berechnete Person handelt, oder eine Manipulation, z. B. durch Davorhalten von Fotos oder Videos. In sensiblen Bereichen ist oft eine 2-Faktor-Authentifizierung 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 (Noise-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 benötigt 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.

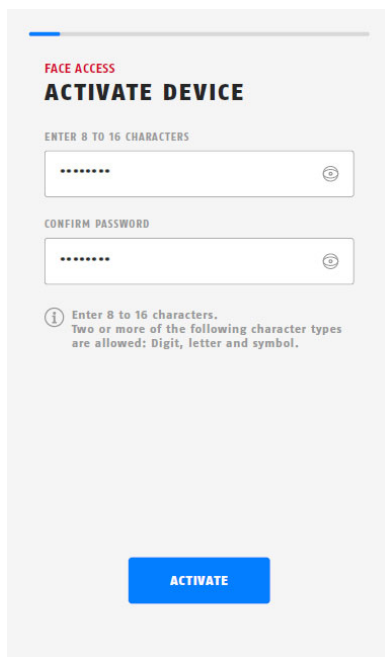
5. Beschreibung der Anschlüsse

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:

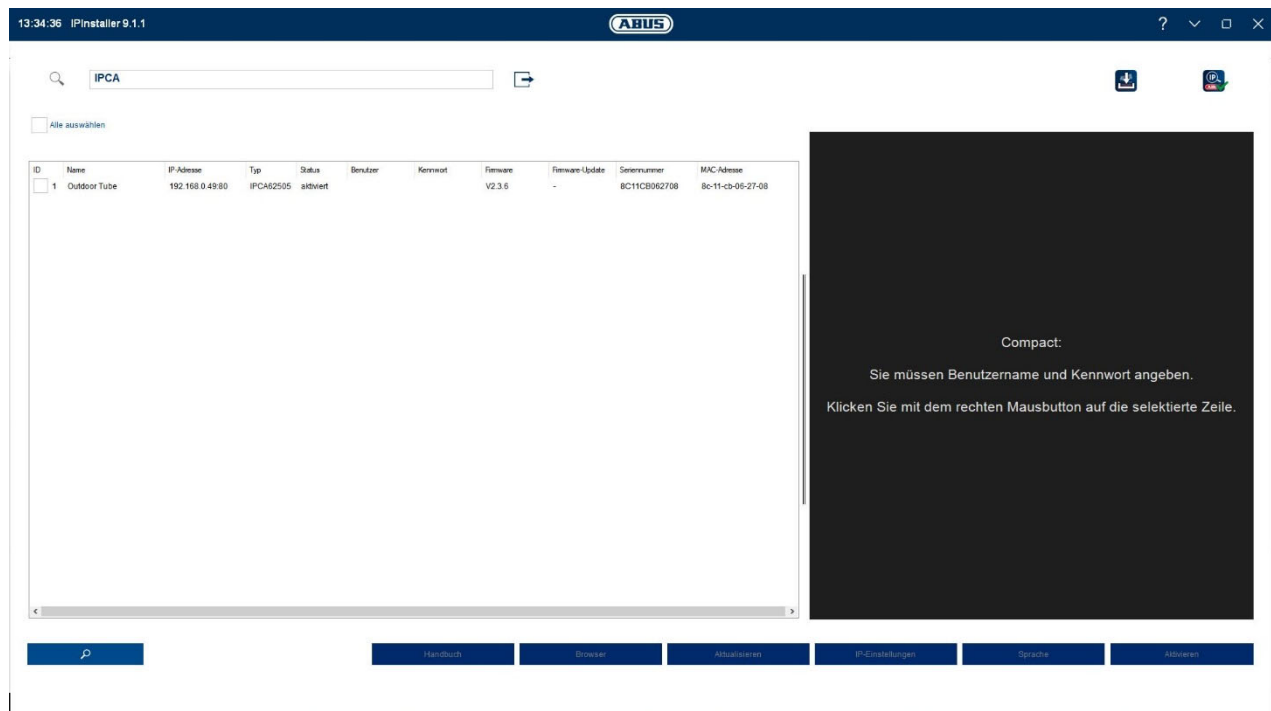
- 8-16 Zeichen
- Gültige Zeichen: Zahlen, Kleinbuchstaben, Großbuchstaben, Sonderzeichen (!"#\$\$%&()*+,-./:;<=>?@[\\]^_{}~Leerzeichen)
- 2 verschiedene Arten von Zeichen müssen verwendet werden

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 automatisch 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 automatisch 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, Großbuchstaben, 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

Aktivierung

Benutzername installer

Passwort ✔

Stark

8 bis 16 Zeichen sind erlaubt, einschließlich Großbuchstaben, Kleinbuchstaben, Ziffern und Sonderzeichen (!"#\$%&'()*+,-./:;<=>@[\\]^_`{|}~ Leerzeichen). Mindestens zwei der oben aufgeführten Typen sind erforderlich.


Bestätigen ✔

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).



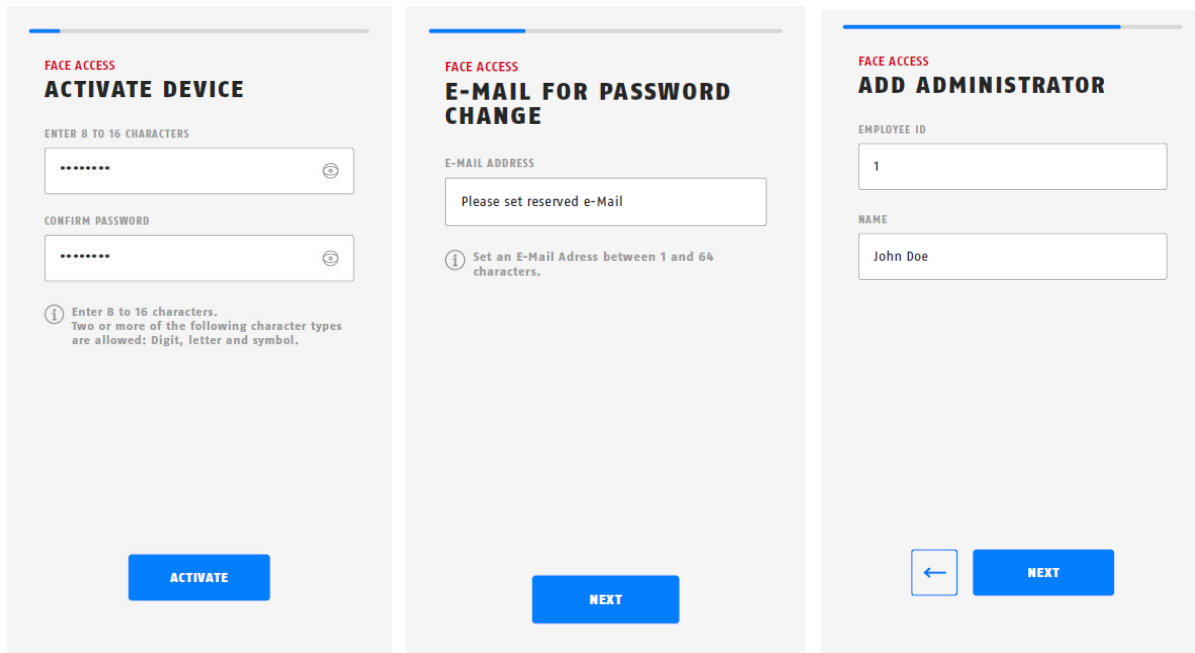
Eine Firmwareaktualisierung über das Web-Interface ist nur mit installiertem Video-Plugin möglich.

7. Konfiguration und Bedienung über den Touch Monitor

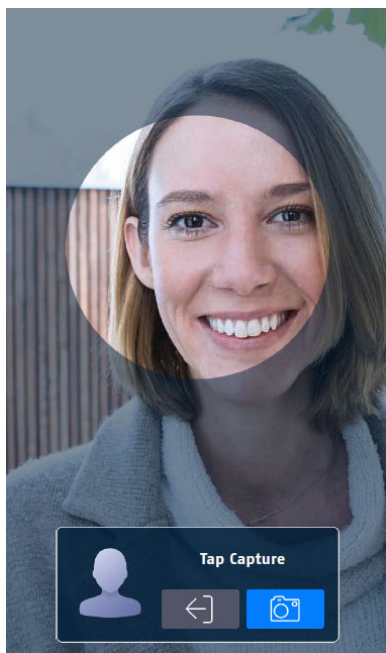
Die Bedienung und Konfiguration des Gesichtserkennungs-Terminals kann direkt über das Anzeigegerät per Berührungssteuerung erfolgen (im Folgenden „Touch-Display“).

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.



The image shows three sequential screenshots of the 'FACE ACCESS' setup assistant interface. The first screen is titled 'ACTIVATE DEVICE' and prompts the user to 'ENTER 8 TO 16 CHARACTERS' and 'CONFIRM PASSWORD'. It features two password input fields with masked characters and a blue 'ACTIVATE' button at the bottom. A help icon and text specify: 'Enter 8 to 16 characters. Two or more of the following character types are allowed: Digit, letter and symbol.' The second screen is titled 'E-MAIL FOR PASSWORD CHANGE' and prompts the user to 'E-MAIL ADDRESS' with the instruction 'Please set reserved e-Mail'. It includes a text input field and a blue 'NEXT' button. A help icon and text specify: 'Set an E-Mail Address between 1 and 64 characters.' The third screen is titled 'ADD ADMINISTRATOR' and prompts for 'EMPLOYEE ID' and 'NAME'. It features two text input fields with the values '1' and 'John Doe' respectively, and blue buttons for a back arrow and 'NEXT'.

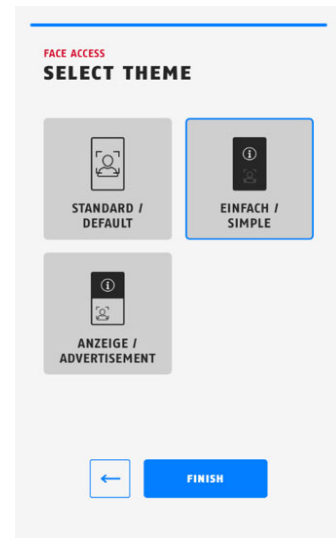


(Beispielbilder der Schritte des Einrichtungsassistenten)

7.2 Hauptbedienseite

7.2.1 Ansichtsoptionen (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 Verbindung 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 Nutzernamen, ID, Benutzertyp und welche Medien für den jeweiligen Benutzer eingerichtet sind.



Wenn dieses Zeichen für 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.

Geben Sie ID/Name/Kartennummer ein.

Über das Eingabefeld kann nach Benutzern in der Liste gesucht werden



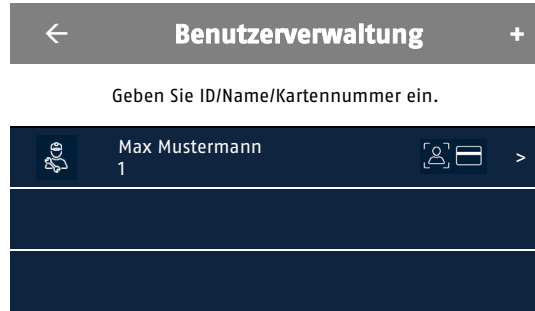
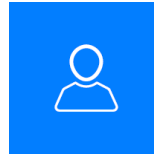
Durch Drücken dieses Pfeilsymbols kann das Menü verlassen werden.

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*()\&/- _=[]+;:“”~|<>{}`)



Benutzerdaten		
Mitarbeiter-ID	1	
Name	Max Mustermann	>
Gesicht	Konfiguriert	>
Karte	0/5	>
Pin Code	Nicht konfiguriert	>
Auth. Einstellungen	Gerätemodus	>
Benutzerrolle	Administrator	>

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).



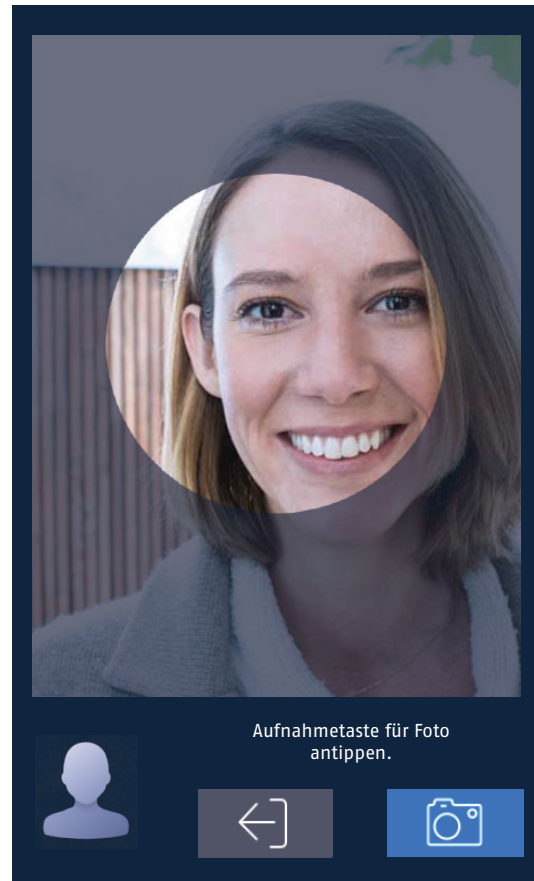
Der Administrator muss den Benutzer in Kenntnis darüber setzen, dass sein Gesichtsbild im Gerät gespeichert und verarbeitet wird. Auf die Verarbeitung des Gesichtsbildes wird ebenfalls im Punkt Datenschutz hingewiesen.



Speicherung des Bildes. Es dauert ca. 3 Sekunden, bis das Gesicht 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.

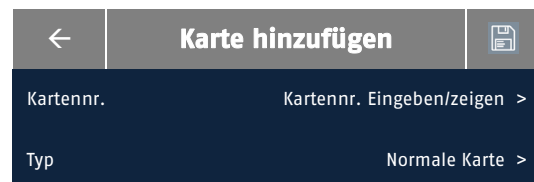
Halten Sie nun die gewünschte Karte vor das Terminal. Der Kartenleser ist im unteren Bereich verbaut. Sie können eine Kartenummer auch manuell eingeben.

Wählen Sie anschließend den Kartentyp:

Normale Karte: Normale Verwendung
Zwangskarte: Auch Nötigungskarte. 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



Normale Karte	✓
Zwangskarte	
Super-Karte	
Patrouillen-Karte	

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.

Pin Code eingeben	
Neuer Pin Code	
Pin Code bestätigen	
Geben Sie bitte 4 bis 8 Ziffern ein.	
Abbrechen	OK

Gerätemodus	✓
Benutzerdefiniert	

Authentifizierungseinstellungen	
Modus	Benutzerdefiniert >
Typ	Einfach-Zugangsdaten >
Methode	>


Normalbenutzer	✓
Administrator	

7.3.2 Zutrittsoptionen

Endgerät-Authorisierungs Modus:

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



 Eine Änderung des Endgeräte-Authentifizierungs Modus wird nicht auf bereits eingelernte Benutzer angewendet. Es ist somit erforderlich, bereits eingelernte Benutzer erneut einzulernen.

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.

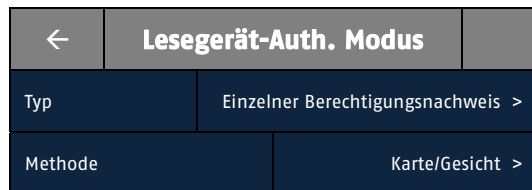
Methode: Gesicht oder Karte
Gesicht oder Passwort (Pin)
Karte oder Passwort (Pin)



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.



← Kommunikation	
Kabelgebundenes Netzwerk	>
WLAN	>
RS-485	>
Wiegand	>
Zugang zu Link Station	>

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, 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 funktionieren soll.

Ausgang: Es werden Daten im Wiegand Format an einen Empfänger übertragen. Als Daten wird die Kartennummer der als erstes eingelernten 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 anschließend 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 Netzwerkverbindung
- Live-Bildübertragung zur App
- Gegensprechen (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.

← Allgemeine Einstellungen	
Stimmeneinstellungen	>
Zeiteinstellungen	>
Ruhezustand	60 >
Sprache wählen	Deutsch >
Block-Nr.	1 >
Gebäude-Nr.	1 >
Einheit-Nr.	1 >
Bildkorrektur	Deaktivieren >

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 / Angegebene 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.

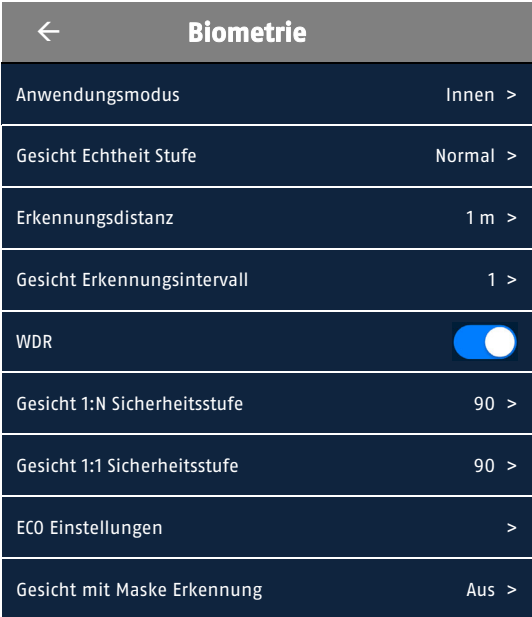
Gesicht Erkennungsintervall

Der Erkennungsintervall (1 bis 10 Sekunden) kann ungewünschte wiederholte Gesichtsidifikation 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



← Biometrie	
Anwendungsmodus	Innen >
Gesicht Echtheit Stufe	Normal >
Erkennungsdistanz	1 m >
Gesicht Erkennungsintervall	1 >
WDR	<input checked="" type="checkbox"/>
Gesicht 1:N Sicherheitsstufe	90 >
Gesicht 1:1 Sicherheitsstufe	90 >
ECO Einstellungen	>
Gesicht mit Maske Erkennung	Aus >

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.

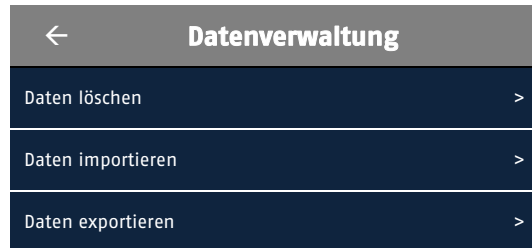
Erinnerung an Tragen: Die Person kann an das Tragen der Maske erinnert werden (Meldung im Display) und die Tür öffnet sich.

Muss tragen: Die Person wird an das Tragen 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 eingelernten 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
Zutrittskontrolleneinstellungen: 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. Ansonsten 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 wie 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
Zutrittskontrolleneinstellungen: 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 Drittsoftware 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 eingelernten Anzahl der Benutzer, Gesichter, Karten und Ereigniseinträge (Logbuch) mit der restlich verfügbaren Menge.

Geräteaktualisierung

Diese Seite zeigt die aktuell installierte Firmware-Version. Weithin kann über 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

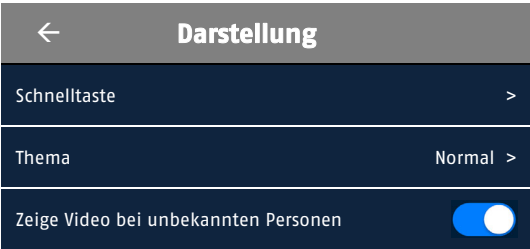
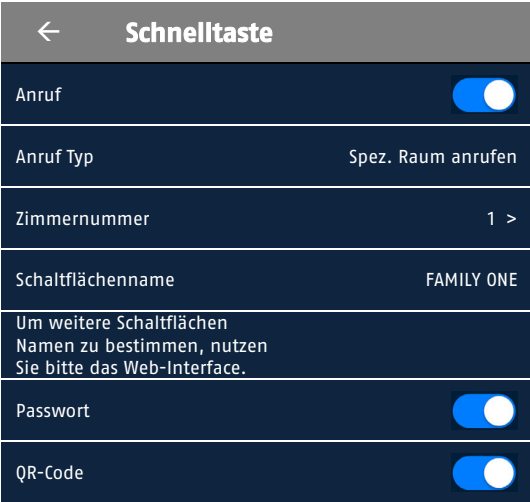
Standardeinstellungen (bedingt)

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

Neustart

Neustarten des Gerätes







7.3.8 Darstellung

<p>Schnelltaste</p> <p>Anruf: Bei Aktivierung wird im Display des Gerätes min. eine Ruftaste angezeigt</p> <p>Anruf-Typ: Zentrale Anrufen: Spez. Raum anrufen Anruf App</p> <p>Zimmernr. Schaltflächenname: FAMILY ONE</p> <p>Passwort: Schaltfläche für die PIN Eingabe.</p> <p>QR Code: Kartenummer als QR Code (CMS nötig)</p> <p>Thema</p> <p>Standard: Es werden bei Konfiguration nur Ruftaste(n), Pin-Code und QR-Code Taste angezeigt, sowie bei Wunsch das Vorschauvideo der Person.</p> <p>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.</p> <p>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.</p> <p>Zeige Video bei unbekannter Person</p> <p>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.</p>	 
--	--

8. Konfiguration und Bedienung über Web-Browser

Falls das Terminal über ein Netzkabel 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 Chrome, 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	Beschreibung
	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

The screenshot shows the ABUS configuration web interface. At the top, there is a navigation bar with the ABUS logo, 'LIVE-ANSICHT', 'BENUTZER', 'SUCHEN', and 'KONFIGURATION'. Below this is a sidebar menu with categories like 'LOKAL', 'SYSTEM', 'SYSTEMEINSTELLUNGEN', 'WARTUNG', 'SICHERHEIT', 'BENUTZERVERWALTUNG', 'NETZWERK', 'VIDEO / AUDIO', 'BILD', and 'ALLGEMEIN'. The main content area is titled 'GRUNDLEGENDE INFORMATIONEN' and contains a list of device settings:

Gerätename	Face Access Terminal
Sprache	Deutsch
Modell	DS-K1T673DWX
Seriennummer	P11732014
Geräte-QR-Code	QR-Code anzeigen
Firmwareversion	V3,3,13 build 230510
Codierungsversion	V1,0 build 191119
Web-Version	v4,41,51build230413
Plug-In-Version	V3,0,7,29

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

The screenshot shows the ABUS configuration interface. At the top, there is a navigation bar with 'LIVE-ANSICHT', 'BENUTZER', 'SUCHEN', and 'KONFIGURATION'. Below this, a sidebar on the left contains menu items: 'LOKAL', 'SYSTEM', 'SYSTEMEINSTELLUNGEN' (highlighted in red), 'WARTUNG', 'SICHERHEIT', 'BENUTZERVERWALTUNG', 'NETZWERK', and 'VIDEO / AUDIO'. The main content area is titled 'ZEITEINSTELLUNGEN' and contains the following settings:

- Zeitzone:** A dropdown menu set to '(GMT+01:00) Amsterdam, Berlin, Rom, Paris'.
- Zeit synchronisieren:** Two radio buttons: 'NTP' (unselected) and 'Manuelle Zeitsynchronisation' (selected).
- Gerätezeit:** A text input field showing '2023-05-16 11:32:35'.
- Zeit einstellen:** A text input field showing '2023-05-16 11:32:28' with a calendar icon, and a checkbox for 'Synchronisation mit Computerzeit' which is currently unchecked.

At the bottom of the settings area, there is a red-bordered button labeled 'Speichern'.

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 Zeitzone-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

GRUNDLEGENDE INFORMATIONEN ZEITEINSTELLUNGEN **SOMMERZEIT** ÜBER

Sommerzeit aktivieren

Startzeit	März	Letzter	Sonntag	02
Endzeit	Oktober	Letzter	Sonntag	03
SZ-Verschiebung	60Minute(n)			

Speichern

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.

Exportieren der Geräteparameter / der Protokolldatei: Vergeben Sie ein Passwort für die Exportdatei.

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 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

ABUS LIVE-ANSICHT BENUTZER SUCHEN

LOKAL SYSTEM SYSTEMEINSTELLUNGEN WARTUNG SICHERHEIT BENUTZERVERWALTUNG NETZWERK

SICHERHEITSDIENST ZERTIFIKATSVERWALTUNG

Stufe Kompatibler Modus

SSH aktivieren

HTTP aktivieren

Speichern

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 erstellt werden, und zum Zweiten kann ein HTTPS-Zertifikat, welches durch eine CA Stelle zertifiziert wurde, hochgeladen werden.

ABUS LIVE-ANSICHT BENUTZER SUCHEN KONFIGURATION

LOKAL SYSTEM SYSTEMEINSTELLUNGEN WARTUNG SICHERHEIT BENUTZERVERWALTUNG NETZWERK VIDEO / AUDIO BILD ALLGEMEIN GEGENSPRECHANLAGE ZUGANGSKONTROLLE BIOMETRIE THEMA

SICHERHEITSDIENST ZERTIFIKATSVERWALTUNG

Zertifikat-Dateien

Zertifikatstyp HTTPS

Zertifikat erstellen Erstellen Keine Datei

Passwörter importieren

Zertifikatstyp SYSLOG

Zertifikat hochladen Installieren

Kommunikationszertifikat importieren

Zertifikatstyp SYSLOG


Zertifikat hochladen Installieren

CA-Zertifikat importieren

Benutzerdefinierte ID

Zertifikat hochladen Installieren

8.1.2.4 Benutzerverwaltung

Nr.	Benutzername	Benutzerrolle	Vorgang
1	admin	Administrator	


Gesamt 1 Elemente

Benutzer ändern ✕

Benutzername	<input type="text" value="admin"/>
Benutzerrolle	<input type="text" value="Administrator"/>
Altes Passwort	<input type="password"/>
Neues Passwort	<input type="password"/>
	<small>gültige Passwort-Zeichenzahl [8-16], Ihr Passwort darf eine Kombination aus Ziffern, Kleinbuchstaben, Großbuchstaben und Sonderzeichen enthalten und muss aus mindestens zwei dieser Zeichenarten bestehen.</small>
Bestätigen	<input type="text"/>

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

The screenshot shows the ABUS network configuration interface. The top navigation bar includes 'LIVE-ANSICHT', 'BENUTZER', 'SUCHEN', and 'KONFIGURATION'. The left sidebar has categories: 'LOKAL', 'SYSTEM', 'NETZWERK', 'ALLGEMEINE EINSTELLUN...', 'ERWEITERT', 'VIDEO / AUDIO', 'BILD', 'ALLGEMEIN', 'GEGENSPRECHANLAGE', 'ZUGANGSKONTROLLE', 'BIOMETRIE', and 'THEMA'. The main content area is titled 'TCP/IP' and contains the following settings:

DHCP	<input checked="" type="checkbox"/>
LAN	LAN1
IPv4-Adresse	192,168,0,100
IPv4-Subnetzmaske	255,255,255,0
IPv4-Standard-Gateway	192,168,0,1
IPv6-Modus	Route Advertisement Route Adv. anzeigen
IPv6-Adresse	::
IPv6-Subnetz-Präfix-L...	0
IPv6 Standardgateway	::
MAC-Adresse	8c:11:cb:0e:5f:44
MTU	1500
NIC-Typ	Auto
DNS-Server	
DHCP	<input type="checkbox"/>
Bevorzugter DNS-Server	0,0,0,0
Alternativer DNS-Server	0,0,0,0

DHCP: Falls ein DHCP-Server verfügbar ist, klicken Sie DHCP an, um automatisch eine IP-Adresse und weitere Netzwerkeinstellungen zu übernehmen. Die Daten werden automatisch von dem Server übernommen und können nicht 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 nicht 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

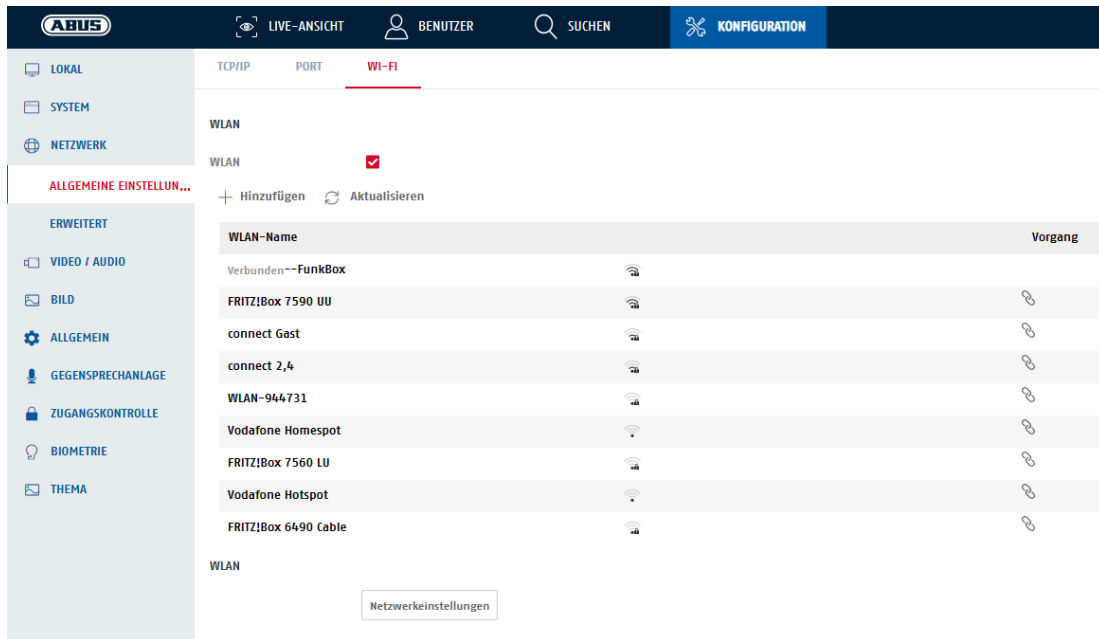
Falls die WiFi Funktion nicht bereits bei der lokalen Einrichtung am Display aktiviert wurde, so kann dies auch hier im Web-Interface erfolgen.









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 Netzwerkparameter (das ist meist so, da viele Acces Points die DHCP Funktion aktiviert haben).



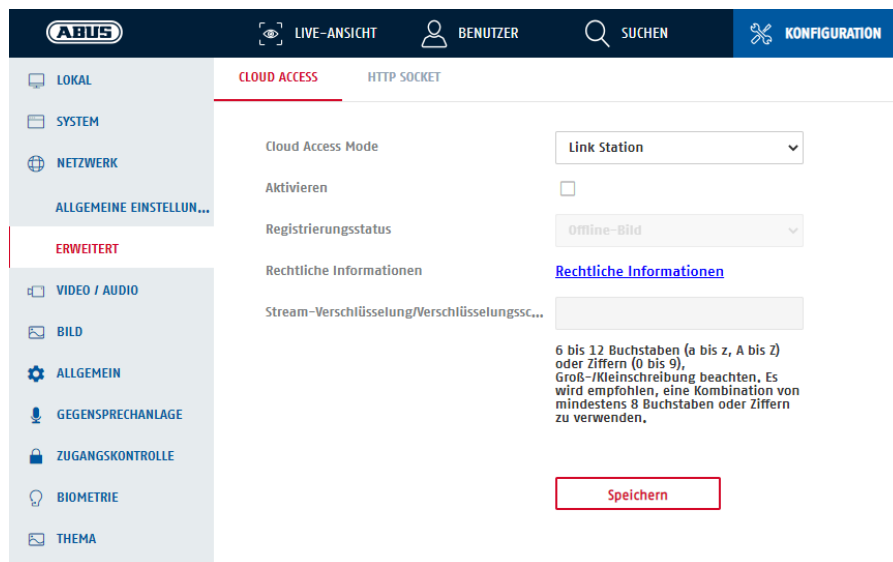
WLAN-Name	Vorgang
Verbunden--FunkBox	
FRITZ!Box 7590 UU	
connect Gast	
connect 2,4	
WLAN-944731	
Vodafone Homespot	
FRITZ!Box 7560 LU	
Vodafone Hotspot	
FRITZ!Box 6490 Cable	

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 ab fotografiert werden.



Verwendbare Funktionen sind:

- Übertragung der Sabotagemeldung (Sabotagekontakt an der Rückseite des Terminals)
- Status Netzwerkverbindung
- Live-Bildübertragung zur App
- Gegensprechen (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

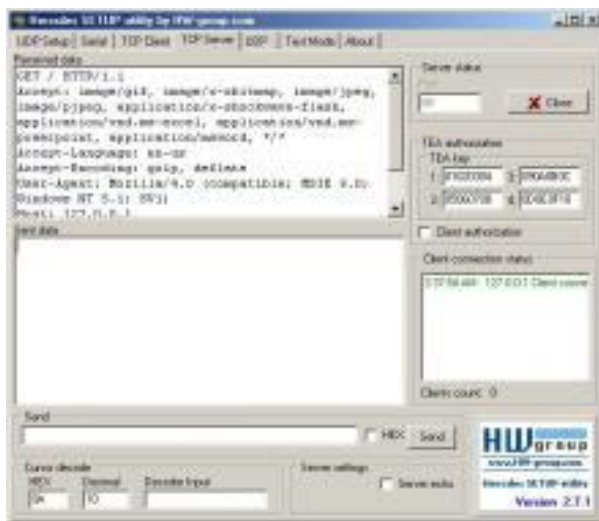
Ereignisinformationen können per JSON Telegram an einen Alarm Host gesendet werden. Auf diese Weise können Ereignisse an eine Drittanbietersoftware übermittelt und weiter verarbeitet werden. Alarminformati
Zum einfachen Testen dieser Funktion kann z.B. die TCP Server Funktion der Software „Hercules Setup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

The screenshot shows the configuration interface for the ABUS system. The top navigation bar includes 'LIVE-ANSICHT', 'BENUTZER', 'SUCHEN', and 'KONFIGURATION'. The left sidebar contains menu items: 'LOKAL', 'SYSTEM', 'NETZWERK', 'ALLGEMEINE EINSTELLUN...', 'ERWEITERT', 'VIDEO / AUDIO', 'BILD', and 'ALLGEMEIN'. The main content area is titled 'HTTP SOCKET' and contains the following settings:

- IP-Adresse/Domänenname des Ereignisalar...: 0,0,0,0
- URL: /
- Port: 0
- Protokoll: HTTP

At the bottom right, there are two buttons: 'Standard' and 'Speichern' (highlighted with a red border).

Hercules Setup Utility:



8.1.4 Video

8.1.4.1 Video

The screenshot shows the ABUS configuration interface. At the top, there is a navigation bar with 'LIVE-ANSICHT', 'BENUTZER', 'SUCHEN', and 'KONFIGURATION'. Below this is a sidebar menu with options like 'LOKAL', 'SYSTEM', 'NETZWERK', 'VIDEO / AUDIO', 'BILD', 'ALLGEMEIN', 'GEGENSPRECHANLAGE', 'ZUGANGSKONTROLLE', 'BIOMETRIE', and 'THEMA'. The main content area is titled 'VIDEO' and contains the following settings:

Videokanal	Kamera1
Kameraname	P11732014
Streamtyp	Hauptstream
Videotyp	Video und Audio
Auflösung	1280*720
Bitrate-Typ	Konstante
Videoqualität	Niedrig
Bildfrequenz	25 fps
Max. Bitrate	2048 Kbps
Videocodierung	H.264
I Frame Intervall	25

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 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.

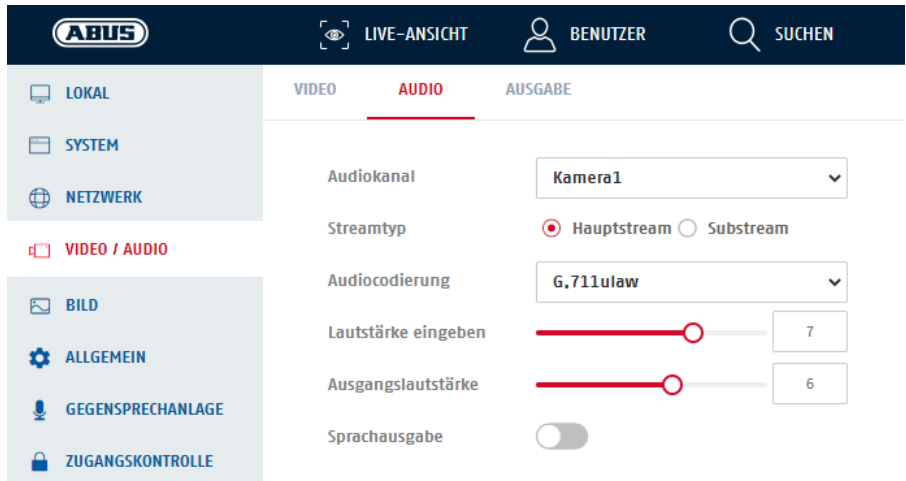
Max. Bitrate: Die Bitrate des Videostroms wird auf einen bestimmten Wert fest eingestellt, stellen Sie die max. Bitrate zwischen 32 und 16384 Kbps ein. Ein höherer Wert entspricht einer höheren Videoqualität, beansprucht aber eine größere Bandbreite.

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 jeweils 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 erfolgreicher oder nicht erfolgreicher Authentifizierung 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 erfolgreicher oder nicht erfolgreicher Authentifizierung erfolgen.

8.1.5 Bild

Videostandard	PAL(50HZ) ▼
WDR	Deaktivieren ▼

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 Kameraparameter fest (Helligkeit, Kontrast, Sättigung, Schärfe). Diese Einstellungen gelten für das lokale Display sowie den Videostream (Web, App).

Standard

Bildeinstellung

Ergänzung Lichtparameter

Bildkorrektur

Bildfusion

Ergänzungslichttyp: IR-Zusatzlicht

Zusatzlichtmodus: EIN

LED-Helligkeit: 50

Ergänzende Lichtparameter

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

Standard

Bildeinstellung

Ergänzung Lichtparameter

Bildkorrektur

Bildfusion

Bildkorrektur aktivieren:

Aufhellen: 0

Glätten: 0

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

Standard

Bildeinstellung

Ergänzung Lichtparameter

Bildkorrektur

Bildfusion

Bildfusion: Automatisch Deaktivieren

Empfindlichkeit: 2

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 diesen 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 aktivieren: Bei Deaktivierung dieser Option wird der komplette interne Kartenleser im Terminal deaktiviert 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 Türöffnung 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

LOKAL SYSTEM NETZWERK VIDEO / AUDIO BILD ALLGEMEIN GEGENSPRECHANLAGE ZUGANGSKONTROLLE BIOMETRIE THEMA

AUTHENTIFIZIERUNGSEINSTELLUNGEN **DATENSCHUTZ** GESICHTSERKENNUNGSPARAMETER

KARTENAUTHENTIFIZIERUNGSEINSTELLUNGEN

Ereignisspeichereinstellungen

Ereignisspeichertyp

Authentifizierungseinstellungen

Authentifizierungsergebnis anzeigen Gesichtsbild Name Mitarbeiter-ID

Bild hochladen und speichern

Bild hochladen nach Autorisierung

Bild speichern nach Autorisierung

Registriertes Bild speichern

Bild verknüpfter Kamera hochladen

Bild verknüpfter Kamera speichern

Ereignisspeichereinstellungen: Diese Option legt fest, wie oft und in welcher Frequenz 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 Ereignisse 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.

Alle Bilder im Gerät löschen

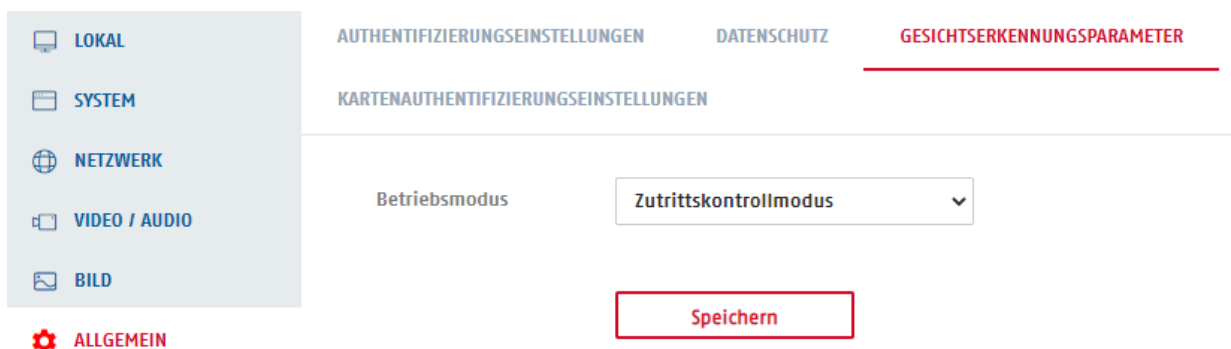
Registrierte Gesichtsbilder löschen

Aufgenommene Bilder löschen

Löschen

- Registrierte Gesichtsbilder löschen:  Löschen aller Gesichtsbilder aller eingerichtet 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

The screenshot shows the 'Kartensicherheit' (Card Security) settings page. On the left is a navigation menu with categories: LOKAL, SYSTEM, NETZWERK, VIDEO / AUDIO, BILD, ALLGEMEIN, GEGENSPRECHANLAGE, ZUGANGSKONTROLLE, BIOMETRIE, and THEMA. The main content area is titled 'KARTENAUTHENTIFIZIERUNGSEINSTELLUNGEN' and lists the following settings:

Option	Status
NFC-Karte aktivieren	<input checked="" type="checkbox"/>
M1-Karte aktivieren	<input checked="" type="checkbox"/>
M1-Kartenverschlüsselung	<input type="checkbox"/>
Sektor	13
EM-Karte aktivieren	<input checked="" type="checkbox"/>
DESFire-Karte aktivieren	<input checked="" type="checkbox"/>
Inhalt DESFire-Karte lesen	<input type="checkbox"/>
FeliCa-Karte aktivieren	<input checked="" type="checkbox"/>

M1-Karte aktivieren:

M1-Kartenverschlüsselung:

EM-Karte aktivieren:

DesFire-Karte aktivieren:

Inhalt DesFire-Karte lesen:

FeliCa-Karte aktivieren:

Mifare Classic (M1) Karten.

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-Karten mit 125 kHz

Mifare Desfire Karten (unverschlüsselt) können zwar gelesen werden, jedoch stehen die Sicherheitsmechanismen der Desfire Karte nicht zur Verfügung.

Funktion aktuell nicht unterstützt

Der Kartenleser kann Karten vom Typ Sony FeliCa erkennen und verwenden.



Es wird empfohlen, die Kartenlesefunktion nur in Verbindung 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 Verschlüsselung können zwar gelesen werden, fallen jedoch in ihrer Sicherheitsperformance auf das Niveau von Mifare Classic zurück.

8.1.6.5 Kartenauthentifizierungseinstellungen

AUTHENTIFIZIERUNGSEINSTELLUNGEN

DATENSCHUTZ

GESICHTSERKENNUNGSPARAMETER

KARTENSICHERHEIT

KARTENAUTHENTIFIZIERUNGSEINSTELLUNGEN

Kartennr.-Regel

Kartenauthentifizierungsmodus








Wiegand 34 (4 Bytes) ▼

Speichern

Diese Funktion ist gültig in Verbindung mit einem angeschlossenen Wiegand Kartenleser (über Anschlusskabel „Wiegand W0, W1 und GND“). Es wird hierbei festgelegt, in welchem 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

 LOKAL	GERÄTENR.	VERKNÜPFTE NETZWERKEINSTELLUNGEN	TASTE ZUM ANRUFEN
 SYSTEM	Gerätetyp	Zugangskontrollgerät	▼
 NETZWERK	Etage Nr.	1	▼
 VIDEO / AUDIO	Türstation Nr.	0	
 BILD	Erweiterte Einstellungen	_____ ^	
 ALLGEMEIN	Block Nr.	1	
 GEGENSPRECHANLAGE	Gebäude Nr.	1	
 ZUGANGSKONTROLLE	Einheit Nr.	1	
 BIOMETRIE			
 THEMA			
		Speichern	

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 nächstes 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

GERÄTENR.	VERKNÜPFTE NETZWERKEINSTELLUNGEN	TASTE ZUM ANRUFEN
Gerätetyp	Zugangskontrollgerät	
SIP-Server-IP	0.0.0.0	
Hauptstation IP	0.0.0.0	
Speichern		

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.

GERÄTENR.	VERKNÜPFTE NETZWERKEINSTELLUNGEN	TASTE ZUM ANRUFEN
Gerätetyp	Türstation	
Haupt-Türstation IP	0.0.0.0	
SIP-Server-IP	0.0.0.0	
Hauptstation IP	0.0.0.0	
Speichern		

8.1.7.3 Taste zum Anrufen

GERÄTENR. VERKNÜPFTE NETZWERKEINSTELLUNGEN **TASTE ZUM ANRUFEN DRÜCKEN**

Nr.	Tasteneinstellungen			
01	<input checked="" type="checkbox"/> Angegebene Innenstation anrufen	<input type="checkbox"/> Anruf-Überwachungszentrale	<input type="checkbox"/> APP	
01	<input checked="" type="checkbox"/> Aktivieren	Zimmer...	<input type="text" value="1"/>	Name <input type="text" value="FAMILY ONE"/>
02	<input checked="" type="checkbox"/> Aktivieren	Zimmer...	<input type="text" value="2"/>	Name <input type="text" value="FAMILY TWO"/>
03	<input checked="" type="checkbox"/> Aktivieren	Zimmer...	<input type="text" value="3"/>	Name <input type="text" value="FAMILY THREE"/>

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

Angebene Innenstation anrufen:

Es können bis 3 Ruftasten für 3 unterschiedliche Apparments eingblendet 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 Appartmentnummer im jeweiligen Hauptmonitor.

Die Bezeichnung der Namen erlaubt deutsche 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.

Beispiel 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

Parameter	Wert
Türnr.	Tür1
Name	
Öffnungsdauer	5 s
Zeitüberschreitungsalarm bei geöffneter Tür	30 s
Türkontakt	<input checked="" type="radio"/> Geschlossen lassen <input type="radio"/> Geöffnet lassen
Ausgangstastentyp	<input type="radio"/> Geschlossen lassen <input checked="" type="radio"/> Geöffnet lassen
Ausschalten der Türverriegelung	<input checked="" type="radio"/> Geschlossen lassen <input type="radio"/> Geöffnet lassen
Verlängerte Öffnungsdauer	15 s
Tür bleibt offen Dauer mit der ersten Person	10 m
Nötigungscode Geben Sie 0 bis 8 Stellen ein.
Super-Passwort Geben Sie 0 bis 8 Stellen ein.

Speichern

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 geöffneter 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 Öffnungsdauer.

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 Terminal eingibt, so wird die Tür geöffnet und sogleich ein Nötigungsalarm an 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

TÜRPARAMETER	AUFZUGSSTEUERUNGSPARAMETER	RS-485
Aufzugssteuerung akti...	<input checked="" type="checkbox"/>	
Aufzug Nr.	<input type="text" value="Aufzug Nr,1"/>	
Aufzugs-Controller-Typ	<input type="text" value="Default"/>	
Schnittstellentyp	<input type="text" value="RS485"/>	
Anzahl Untergeschosse	<input type="text" value="0"/>	
<input type="button" value="Speichern"/>		

Die Option Aufzugssteuerung wird aktuell nicht verwendet.

8.1.8.3 RS-485

TÜRPARAMETER	AUFZUGSSTEUERUNGSPARAMETER	RS-485
RS-485 aktivieren	<input checked="" type="checkbox"/>	
Nr.	<input type="text" value="1"/>	
Peripheriegerätetyp	<input type="text" value="Kartenleser"/>	
RS-485-Adresse	<input type="text" value="1"/>	
Baudrate	<input type="text" value="19200"/>	
Datenbit	<input type="text" value="8"/>	
Stoppbit	<input type="text" value="1"/>	
Parität	<input type="text" value="Keine"/>	
Flusssteuerung	<input type="text" value="Keine"/>	
Kommunikationsmodus	<input type="text" value="Halbduplex"/>	

Die RS-485 Schnittstelle wird in erster Linie im Zusammenhang mit dem ABUS Sicherheitsmodul TVHS20340 verwendet. Dieses Modul dient zum sicheren Anschluss aller externen 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

TÜRPARAMETER	AUFZUGSSTEUERUNGSPARAMETER	RS-485	WIEGAND-EINSTELLUNGEN
Wiegand	<input type="checkbox"/>		
Wiegand-Richtung	<input type="radio"/> Eingang	<input checked="" type="radio"/> Ausgang	
Wiegand-Modus	<input type="text" value="Wiegand 26"/>		
<input type="button" value="Speichern"/>			

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 Kartenummer über die Wiegand-Schnittstelle versendet.

8.1.9 Biometrie

The screenshot shows the configuration page for Biometric security. The settings are as follows:

- Gesicht Anti-Spoofing:
- Sicherheitsebene bei Live-Gesichtserkennung: Normal Bekanntheit Höchste
- Erkennungsreichweite: Automatisch 0,5m 1m 1,5m 2m
- Anwendungsmodus: Innen Außen
- Gesichtserkennungsmodus: Normalmodus (dropdown)
- Kontinuierliches Gesichtserkennungsintervall: 3 s
- Neigungswinkel: 45 °
- Gierwinkel: 45 °
- Bewertungsschwelle: 50
- Übereinstimmungsschwellenwert 1:1: 90
- Gesichtsübereinstimmungsschwellenwert 1:N: 90
- Gesichtserkennungs-Zeitüberschreitenswert: 3 s
- Gesicht mit Maskenerkennung:
- ECO-Modus:
- ECO-Modus Schwellenwert: 4
- ECO-Modus (1:1): 80
- ECO-Modus (1:N): 80

Gesicht Anti-Spoofing:

Anti-Spoofing ist der Fachbegriff für die Verhinderung von Manipulationsversuchen. Es gibt diverse Parameter, 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:

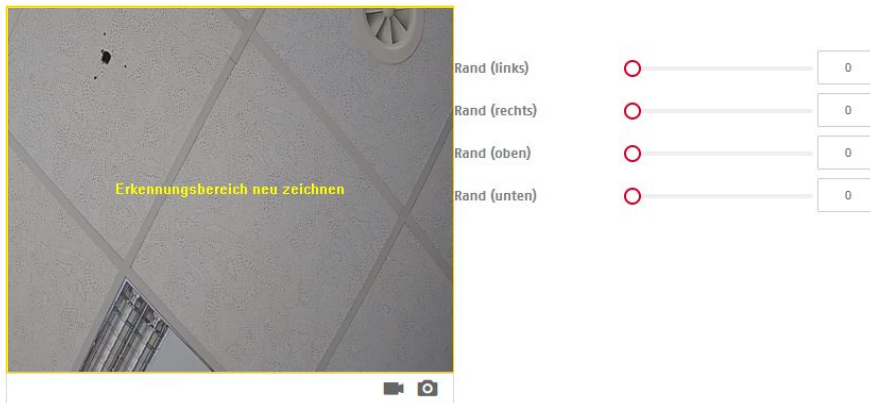
Die Auswahl „innen“ oder „außen“ beeinflusst diverse Kameraparameter (interne Parameter).

- 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 eingelernten 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-Authentifizierung).
- 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

BIOMETRIE

BEREICHSKONFIGURATION



Erkennungsbereich neu zeichnen

Rand (links) 0

Rand (rechts) 0

Rand (oben) 0

Rand (unten) 0

Speichern

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.

THEMA MEDIENDATENBANK


Anzeigemodus Standard Information Einfach

Ruhezustand

Ruhezustand nach s

Themenverwaltung + Programm hinzufügen

Begrüßungsnachricht



Vorlage

Überschrift

Schriftgröße Schriftfarbe

Untertitel

Schriftgröße Schriftfarbe


Untertitel 2

Schriftgröße Schriftfarbe

Hintergrundbild

Bei Auslieferung des Hintergrundbildes an das Gerät sti...

Bild(0/8)



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: In diesem Punkt können Text und Bilder definiert werden, sowie deren Anzeigart. 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).

Wiedergabezeitplan

Begrüßungsnachricht Bild Wählen Sie zuerst ein Thema und stellen Sie die Anzeigzeit ein.



Diashow-Intervall

s

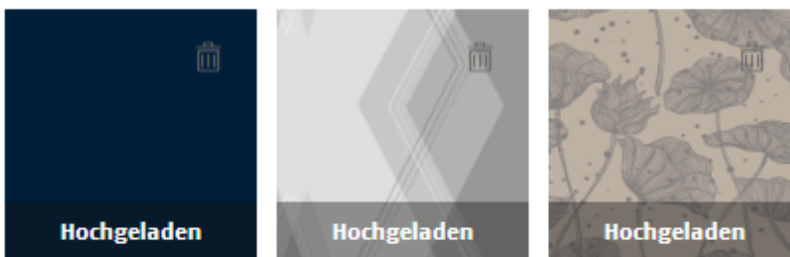
8.1.10.1 Mediendatenbank

THEMA

MEDIENDATENBANK

ⓘ Benötigtes Bildformat ist jpg. Bis zu 8 Bilder können hochgeladen werden, Max. Bildgröße; 1 MB.

+ Hinzufügen



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

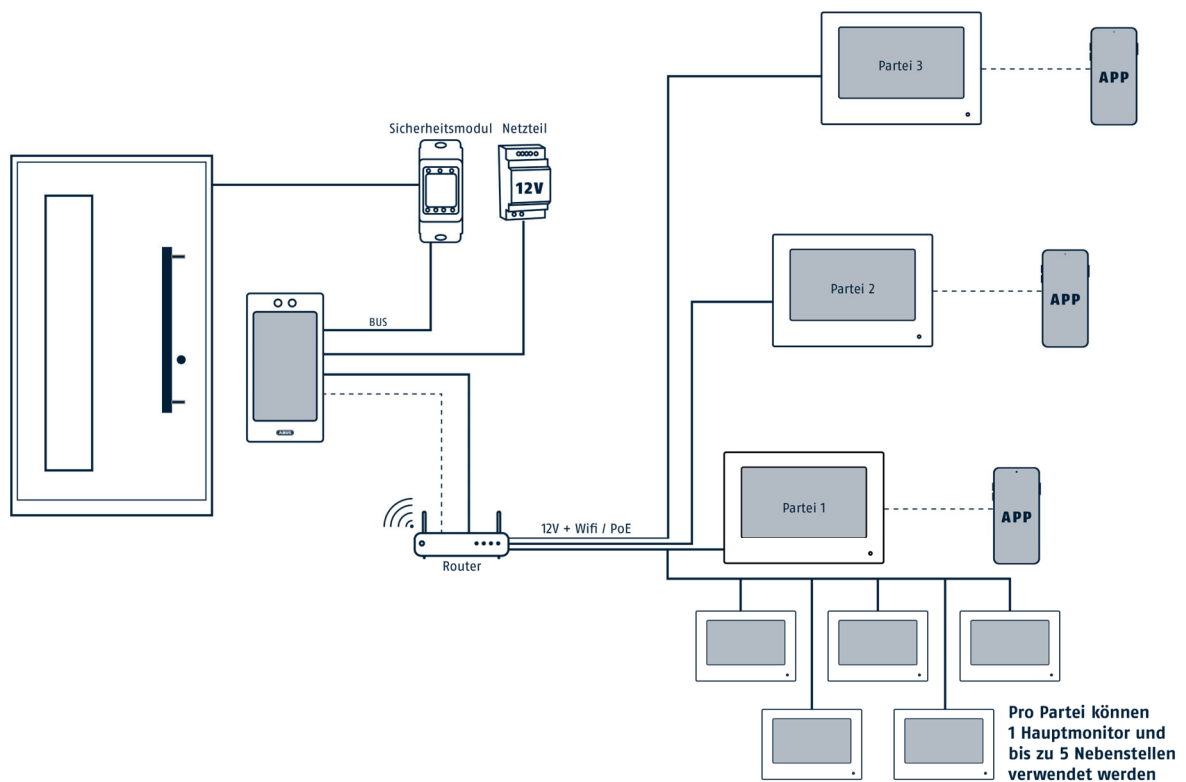
9. Einbindung und Verwendung von Monitoren der Moduvis Türsprechanlage

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).



	<p>Um sicherzustellen, dass die Information des ausgelösten Sabotagekontaktes am FaceXess Gerät in einer oder mehreren verbundenen Link Station Apps als Pop-Up Mitteilung erscheinen soll, so ist es notwendig das FaceXess Gerät auch direkt in einen Link Station Account mit einzubinden. Dies erfolgt durch Scannen des Link Station QR Codes des FaceXess Gerätes. Nur der Hauptbenutzer kann die Sabotagemitteilung erhalten.</p>
--	--

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.

	Geräteverwaltung		
Haupt-Türstation	192.168.0.26		
			
			
			

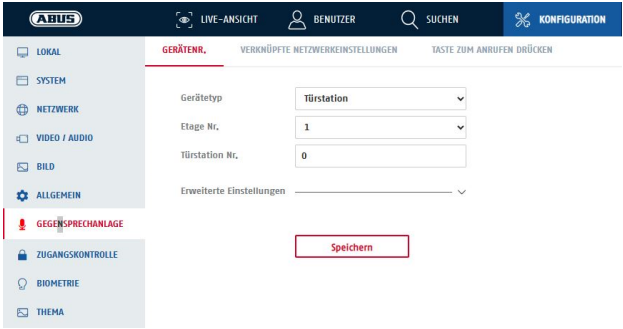
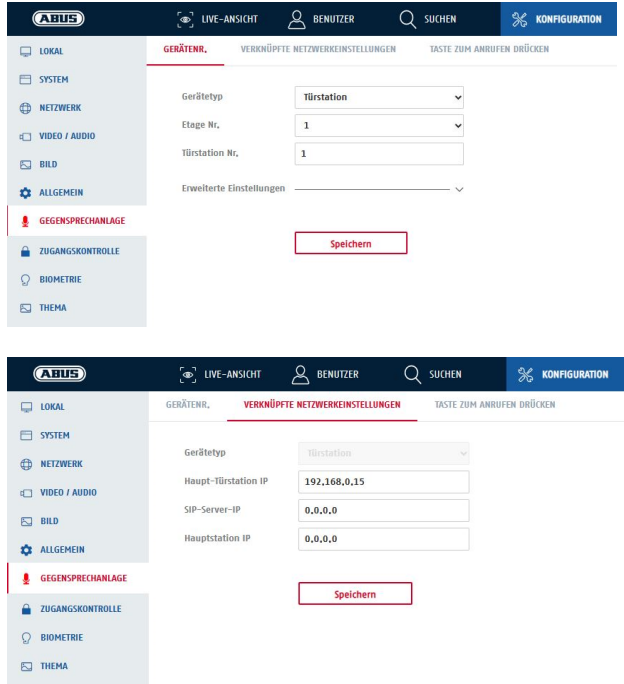
9.3 Verwendung von FaceXess als Nebentür

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.

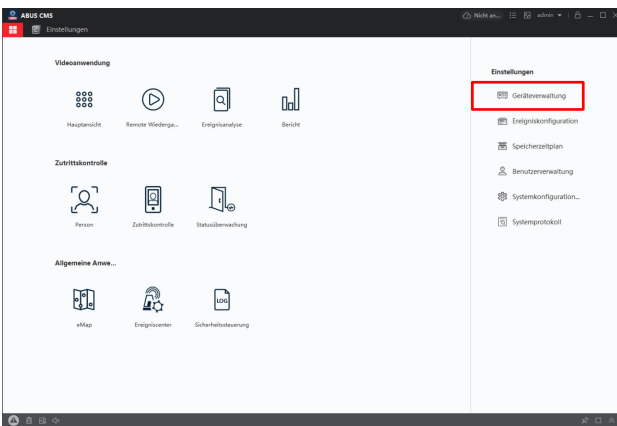
Einstellung am Gerät für den Haupteingang	Einstellung am Gerät für die 1. Nebentür
<p>Menüpunkt: Konfiguration / Gegensprechanlage / Gerätenr.</p> <p>Gerätetyp: Türstation Türstation-Nr.: 0</p> 	<p>Menüpunkt: Konfiguration / Gegensprechanlage / Gerätenr.</p> <p>Gerätetyp: Türstation Türstation-Nr.: 1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

10. Konfiguration und Bedienung über die ABUS CMS Software

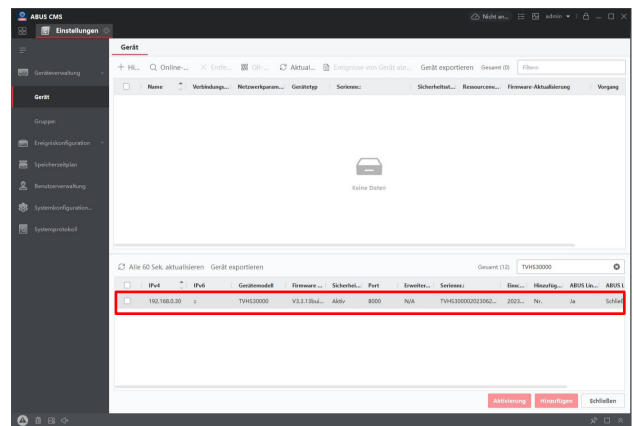
10.1 Einbindung in ABUS CMS Software

Als Erstes muss das FaceXess Geräte zur Geräteverwaltung der ABUS CMS Software hinzugefügt werden. Dazu muss das FaceXess Gerät sich entweder über eine Netzkabelverbindung oder eine WiFi-Verbindung im gleichen IP-Netzwerk wie der PC mit der installierten ABUS CMS Software befinden. Starten Sie die CMS Software und öffnen Sie den Punkt „Geräteverwaltung“.

Öffnen der Geräteverwaltung

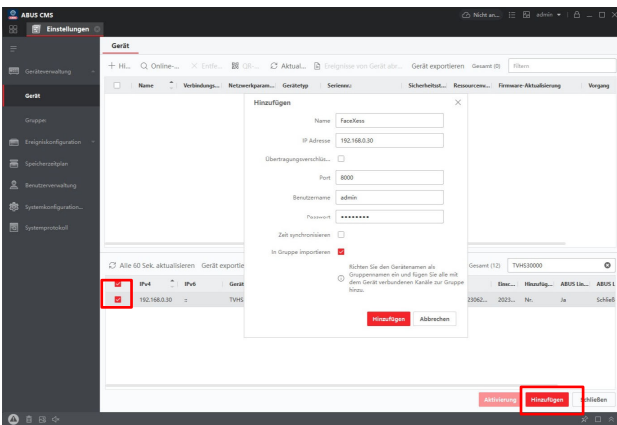


Das Gerät wird durch die CMS Software im IP Netzwerk gefunden.



Markieren und Hinzufügen

Eingabe der nötigen Verbindungsparameter: Name, IP-Adresse, Port (Standard 8000), Benutzername (Standard „admin“), Passwort (Geräte-Passwort)



Hinzufügen

Name:

IP Adresse:

Übertragungsverschlüs...

Port:

Benutzername:

Passwort:

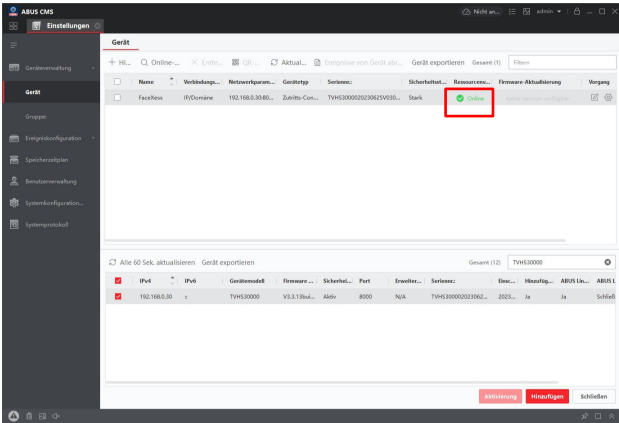
Zeit synchronisieren

In Gruppe importieren

Richten Sie den Gerätenamen als Gruppennamen ein und fügen Sie alle mit dem Gerät verbundenen Kanäle zur Gruppe hinzu.

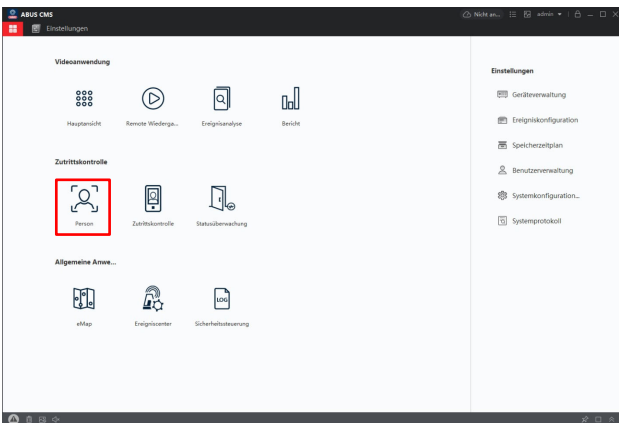
Hinzufügen **Abbrechen**

Das FaceXess Geräte wurde nun erfolgreich zur ABUS CMS hinzugefügt (Status „Online“, grün).

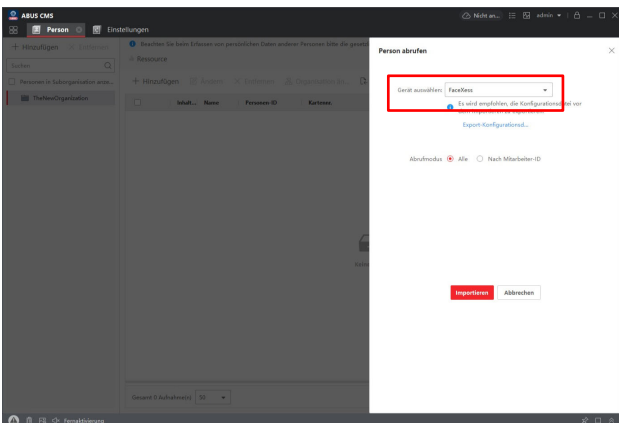


10.2 Personen verwalten

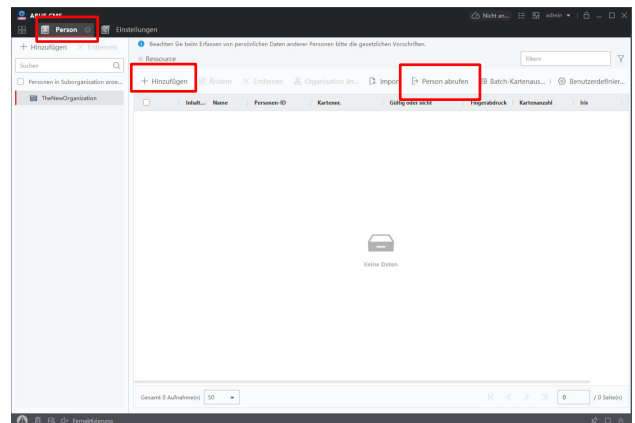
Öffnen Sie den Menüpunkt Zutrittskontrolle / Person.



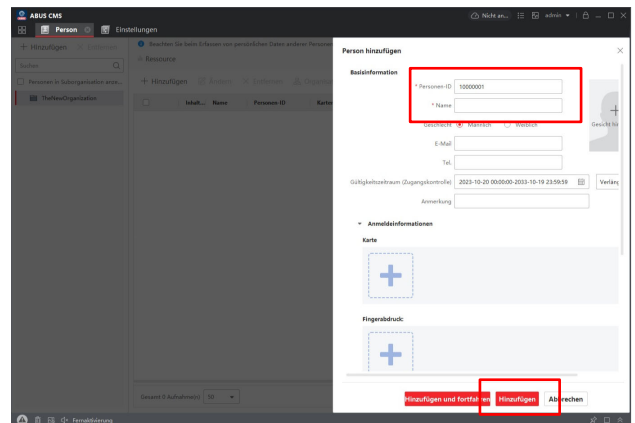
Wenn Sie Informationen von einem FaceXess Gerät abrufen, müssen Sie zunächst eines der verbundenen FaceXess Geräte auswählen. Im Anschluss werden die Informationen der Personen heruntergeladen und zur Personenliste hinzugefügt.



Sie können Personen manuell hinzufügen, oder die Personeninformationen von einem FaceXess Gerät über das Netzwerk abrufen.



Beim manuellen Hinzufügen sind min. die Personen ID sowie der Name einzugeben. Weiterhin können ein Bild der Person hochgeladen, Kartennummern zugewiesen oder ein individueller PIN Code vergeben werden. Die Markierung der Person als Administrator ist ebenfalls möglich.



Klicken Sie auf das + Zeichen im Personenvorschaubild.

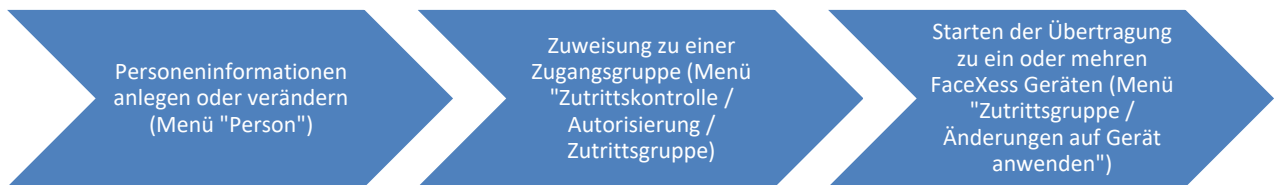
Nach erfolgreichem Hinzufügen erscheint die Person in der Personenübersicht.

ID	Name	Personen-ID	Kennzeichen	Gültigkeitszeitraum	Freigegeben	Kontrollstatus	IK
1	Max	1	347773148	Nicht abgerufen	0	1	0



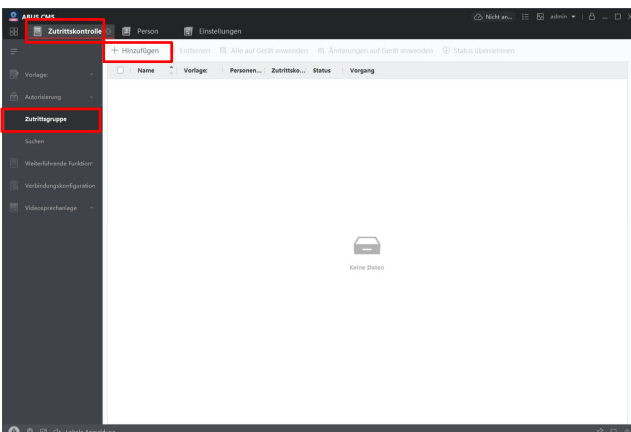
Die Personen sind nun in der ABUS CMS Software angelegt. Im nächsten Schritt müssen eine oder mehrere Zutrittsgruppen erstellt werden. Zutrittsgruppen können sich z.B. im erlaubten Zeitraum für einen Zutritt unterscheiden.

Für das erfolgreiche Übertragen von Personeninformationen in ein oder mehrere FaceXess Geräte sind folgende Schritte in der ABUS CMS Software nötig.

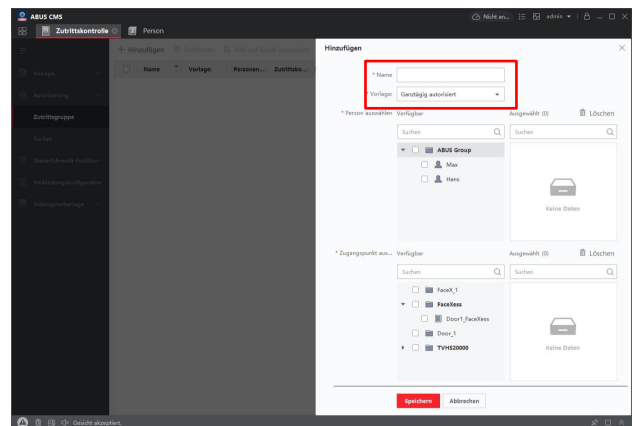


10.3 Zutrittsgruppen verwalten und übertragen in FaceXess

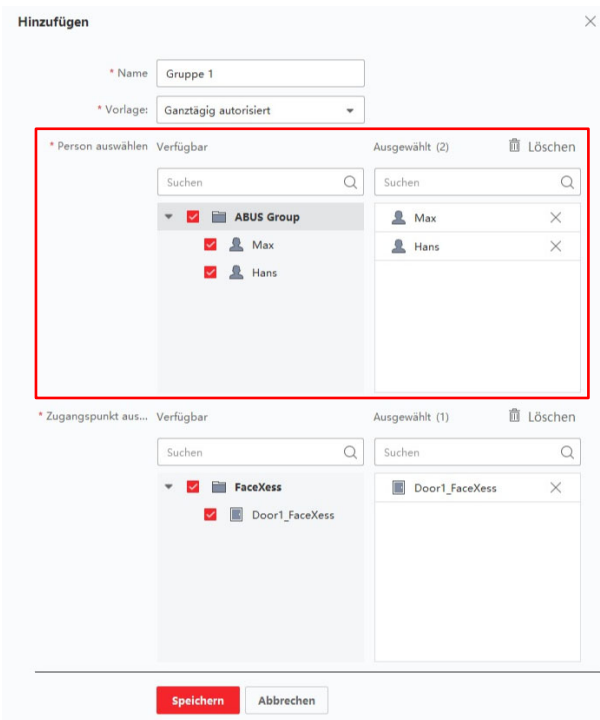
Klicken Sie im Menü Zutrittskontrolle / Zutrittsgruppe auf den Menüpunkt „Hinzufügen“.



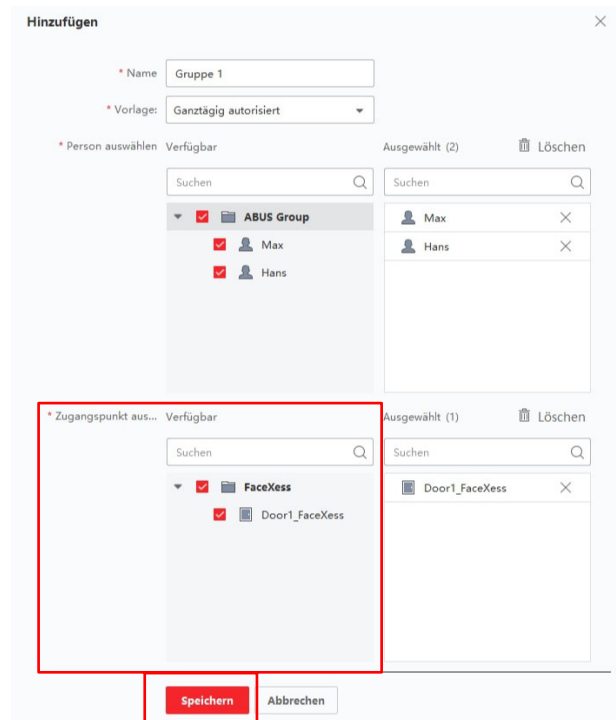
Vergeben Sie einen Gruppennamen. Im Punkt darunter wird festgelegt, in welchem Zeitraum die Zutrittsgruppe Zutritt erhalten kann (Ganztätig ist Standard, weitere Optionen siehe Punkt 10.4)



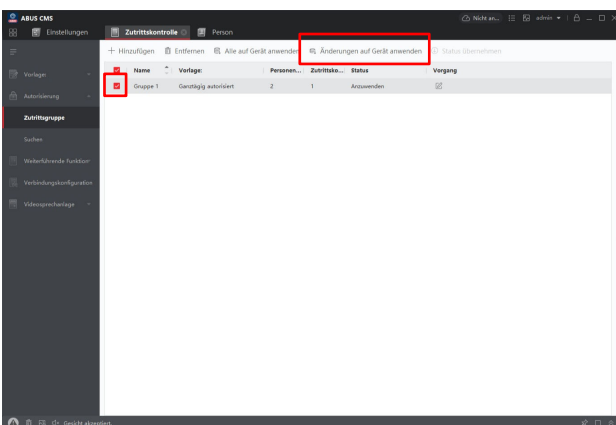
Aus der Liste der verfügbaren Personen wählen Sie die Personen aus, die der Zutrittsgruppe angehören sollen.



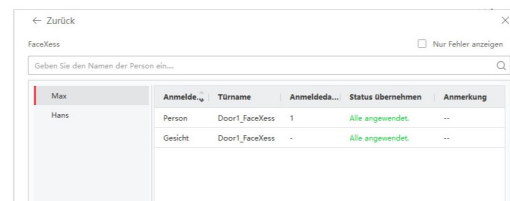
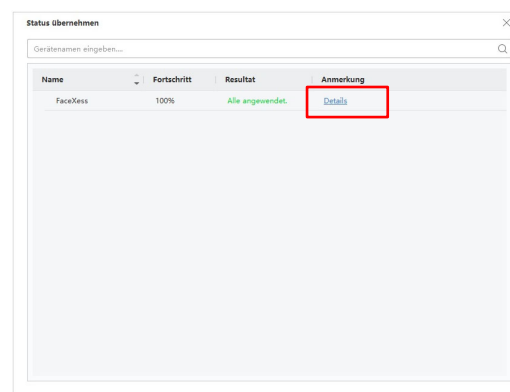
Im Weiteren definieren Sie, auf welche Geräte die Zutrittsgruppe übertragen werden soll. Eine Mehrfachauswahl von Geräten ist möglich, wenn sich die Geräte im Gleichen IP Netzwerk befinden. Drücken Sie anschließend „Speichern“.



Die Zutrittsgruppe ist nun erstellt. Wählen Sie nun die Zutrittsgruppe aus und Drücken anschließend auf „Änderungen auf Gerät anwenden“.



Es erscheint eine Statusübersicht. Falls die Resultsanzeige grün angezeigt wird, so wurden alle geänderten Parameter erfolgreich an das/die FaceXess Gerät(e) übertragen. Es können Details der Übertragung angezeigt werden.



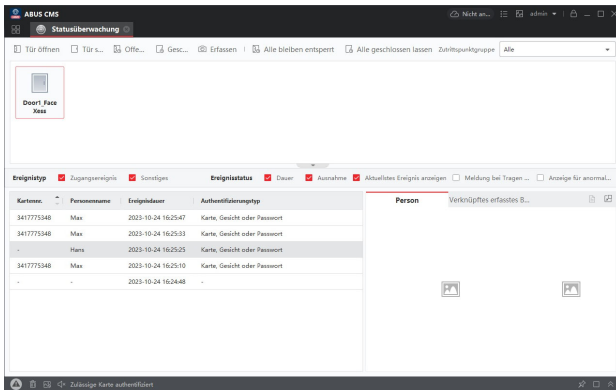
10.4 Ereignisanzeige und Ereignissuche

Ereignisse des FaceXess Gerätes können direkt live in der ABUS CMS Software oder über eine nachträgliche Suche angezeigt werden.

Live Anzeige von Ereignissen

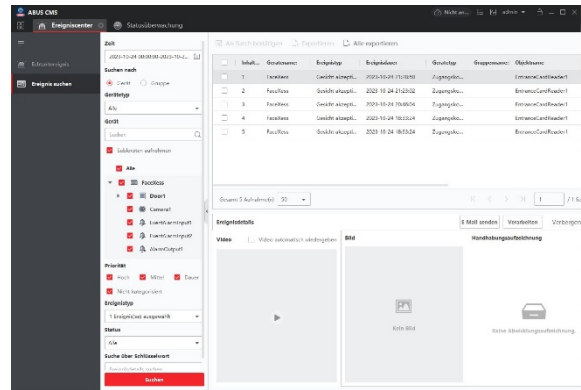
Menü: Zutrittskontrolle / Statusüberwachung

Funktionen: Live Anzeige von Authentifizierungen, Fernöffnen, Fernschließen von Türen



Suche von Ereignissen

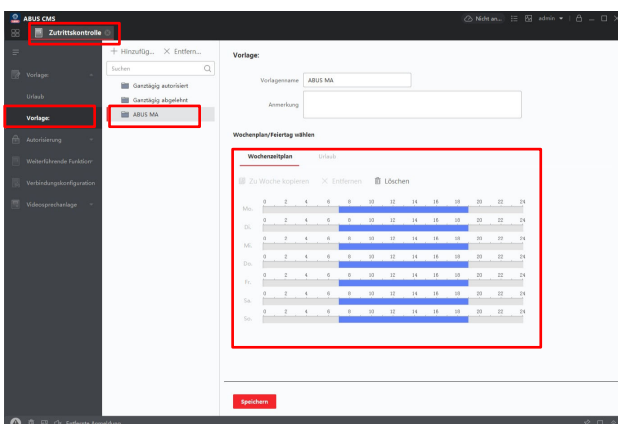
Menü: Allgemeine Anwendung / Ereigniscenter



10.5 Zeitplangesteuerte Zutritte

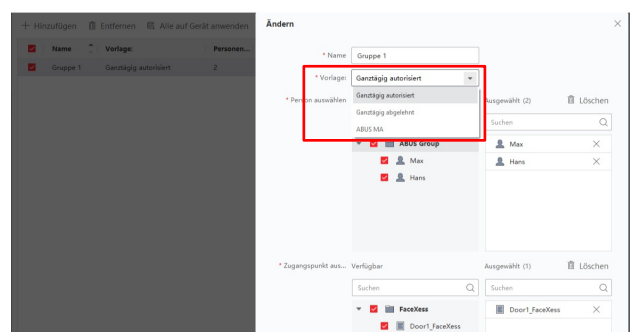
Es ist möglich unterschiedliche Zutrittsgruppen mit unterschiedlichen Zeitplänen für den Zutritt zu versehen.

Gehen Sie in das Menü „Zutrittskontrolle / Autorisierung / Vorlage“. Fügen Sie einen neuen Zeitplan hinzu. Wählen Sie die Tage und Stundenbereiche. Speichern Sie den Zeitplan



Gehen Sie in das Menü „Zutrittskontrolle / Autorisierung / Zutrittsgruppe“ und Klicken Sie doppelt auf eine Zutrittsgruppe.

Sie können nun die erstellte Zeitplanvorlage der Zutrittsgruppe zuweisen.



Zum Schluss müssen die Änderungen der Zutrittsgruppe wieder auf das Gerät oder die Geräte übertragen werden (Schaltfläche „Änderungen auf Gerät anwenden“).

11. Wartung und Reinigung


11.1 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

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

11.2 Reinigung

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

	<p>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).</p>
---	--

12. 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.

13. Technische Daten

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

14. 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.

TVHS30000



Ⓧ **Instruction manual Software**

Version 10/2023



D

These operating instructions contain important information on commissioning and handling.

Pay attention to this even if you pass this product on to third parties.

Therefore, keep these operating instructions for future reference!

A list of the contents can be found in the table of contents with the corresponding page numbers on **page 8**.

TVHS30000



Instruction manual

Version 10/2023



Original operating instructions in German language. Keep for future use!

Introduction

Dear Customer,

thank you for purchasing this product.

ABUS Security-Center hereby declares that the device complies with the RED Directive 2014/53/EU. The device also complies with the requirements of the following EU Directives: EMC Directive 2014/30/EU and RoHS Directive 2011/65/EU. The full text of the EU Declaration of Conformity is available at the following Internet address: www.abus.com/TVHS30000

To maintain this condition and to ensure safe operation, you as the user must observe these operating instructions!

Read through the complete operating instructions before commissioning the product, observe all operating and safety instructions!

All company names and product designations contained herein are trademarks of their respective owners. All rights reserved.




If you have any questions, please contact your installer or dealer!





Disclaimer

These operating instructions have been prepared with the greatest care. Should you nevertheless notice any omissions or inaccuracies, please notify us in writing at the address given on the back of the manual. ABUS Security-Center GmbH & Co. KG assumes no liability for technical and typographical errors and reserves the right to make changes to the product and operating instructions at any time without prior notice. ABUS Security-Center is not liable or responsible for any direct or indirect consequential damages arising in connection with the equipment, performance and use of this product. No warranty of any kind is given for the contents of this document.

Explanation of symbols

	The symbol with the lightning bolt in the triangle is used when there is danger to the health exists, e.g. due to electric shock.
	An exclamation point within the triangle is intended to alert the user to the presence of important instructions in this manual that should be followed.
	This symbol is to be found when special tips and notes on operation are to be given to you.

Important safety instructions

	In case of damage caused by non-observance of these operating instructions, the warranty claim expires. We accept no liability for consequential damage!
	We accept no liability for damage to property or personal injury caused by improper handling or failure to observe the safety instructions. In such cases, any warranty claim is void!

Dear customer, the following safety and hazard information is not only intended to protect your health, but also to protect the device. Please read the following points carefully:

- There are no parts inside the product that require maintenance. In addition, disassembly voids the approval (CE) and warranty/guarantee.
- Falling from even a small height can damage the product.
- Mount the product so that direct sunlight cannot fall on the image sensor of the device. Observe the mounting instructions in the corresponding chapter of these operating instructions.
- The device is designed for indoor and outdoor use (IP66).

Avoid the following adverse environmental conditions during operation:

- Wetness or excessive humidity
- Extreme cold or heat
- Direct sunlight
- Dust or flammable gases, vapors or solvents
- strong vibrations
- strong magnetic fields, such as near machines or loudspeakers.
- Do not install the camera on unstable surfaces.

General safety instructions:

- Do not leave the packaging material lying around carelessly! Plastic foils/ bags, polystyrene parts etc., could become a dangerous toy for children.
- For safety reasons, the video surveillance camera must not be placed in children's hands due to small parts that can be swallowed.
- Please do not insert any objects through the openings into the interior of the device
- Use only the attachments/accessories specified by the manufacturer. Do not connect any non-compatible products.
- Please observe the safety instructions and operating instructions of the other connected devices.
- Before commissioning, check the device for damage. If this is the case, please do not commission the device!
- Observe the limits of the operating voltage specified in the technical data. Higher voltages can destroy the device and endanger their safety (electric shock).



Safety instructions

1. Power supply: Pay attention to the specifications for the supply voltage and power consumption given on the nameplate.
2. Overload
Avoid overloading power outlets, extension cords and adapters as this may result in a fire or electric shock.
3. Cleaning
Clean the device only with a damp cloth without harsh cleaning agents.
The device must be disconnected from the mains during this process.

Warnings

Before initial start-up, all safety and operating instructions must be observed!

1. Observe the following instructions to avoid damage to the power cord and power plug:
 - When disconnecting the device from the mains, do not pull on the power cord, but grasp the plug.
 - Make sure that the power cord is as far away from heaters as possible to prevent the plastic sheathing from melting.
2. Follow these instructions. Failure to do so may result in electric shock:
 - Never open the housing or the power supply unit.
 - Do not insert any metal or flammable objects inside the device.
 - To avoid damage due to overvoltage (example thunderstorms), please use a surge protector.
3. Please disconnect defective devices from the mains immediately and inform your specialist dealer.

	When installing in an existing video surveillance system, make sure that all devices are disconnected from the mains and low-voltage circuits.
	If in doubt, do not carry out the assembly, installation and wiring yourself, but leave this to a specialist. Improper and amateurish work on the power supply system or house installations not only pose a danger to yourself, but also to other people. Wire installations so that mains and low voltage circuits always run separately and are not connected to each other at any point or can be connected by a defect.

Unpacking

While unpacking the device, handle it with extreme care.


	In case of possible damage to the original packaging, first check the device. If the device is damaged, return it with packaging and inform the delivery service.
---	---


Table of contents


1. Intended use	82
2. Explanation of symbols	82
3. Features and functions	83
4. Device description	84
5. Description of the connections	84
6. Initial commissioning	84
6.1 Activation of the device via the local touch monitor	84
6.2 Activating the device via the ABUS IP Installer.....	84
6.3 Activating the device via the web browser	85
6.4 Install video plugin	86
7. Configuration and operation via the touch monitor	87
7.1 Setup wizard	87
7.2 Main operating page	88
7.2.1 View options (themes)	88
7.2.2 Symbols and information displays	89
7.2.3 Adjustable operating keys.....	89
7.3 Administrator menu.....	90
7.3.1 User	90
7.3.2 Access options.....	93
7.3.3 Communication	94
7.3.4 Basic settings.....	96
7.3.5 Biometric.....	97
7.3.6 Database.....	99
7.3.7 System maintenance	100
7.3.8 Representation.....	101
8. Configuration and operation via web browser	102
8.1 Configuration via web browser.....	102
8.1.1 Local configuration.....	102
8.1.2 System.....	104
8.1.2.1 System settings.....	104
8.1.2.1.1 Basic information	104
8.1.2.1.2 Time settings.....	105
8.1.2.1.3 DST / Daylight saving time.....	106
8.1.2.1.4 About / License information	106
8.1.2.2 Maintenance	107
8.1.2.2.1 Updating and maintenance	107
8.1.2.2.2 Log query / logbook	108
8.1.2.3 Safety.....	108
8.1.2.3.1 Security service.....	108
8.1.2.3.2 Certificate management.....	108
8.1.2.4 User management	109
8.1.2.4.1 Arming / disarming info	109
8.1.3 Network.....	110
8.1.3.1 TCP/IP	110
8.1.3.2 Port	111
8.1.3.3 WiFi.....	112

8.1.3.4	Cloud access / ABUS Link Station	113
8.1.3.5	HTTP socket	114
8.1.4	Video.....	115
8.1.4.1	Video.....	115
8.1.4.2	Audio.....	116
8.1.4.3	Audio output.....	116
8.1.5	Image.....	117
8.1.6	General.....	119
8.1.6.1	Authentication settings.....	119
8.1.6.2	Data protection.....	121
8.1.6.3	Face detection parameters	122
8.1.6.4	Card security	123
8.1.6.5	Card authentication settings	124
8.1.7	Intercom system.....	125
8.1.7.1	Device number.....	125
8.1.7.2	Linked network devices.....	126
8.1.7.3	Call key	127
8.1.8	Access control.....	128
8.1.8.1	Door parameters	128
8.1.8.2	Elevator control	129
8.1.8.3	RS-485.....	129
8.1.8.4	Wiegand settings	129
8.1.9	Biometrics	131
8.1.9.1	Range configuration.....	132
8.1.10	Topic	134
8.1.10.1	Media database	135
9.	Integration and use of monitors of the Moduvis door intercom system.....	136
9.1	System overview Face terminal / monitor(s).....	136
9.2	Configuration of face terminal and monitor(s).....	137
9.3	Using FaceXess as a side door	138
10.	Configuration and operation via the ABUS CMS software	139
10.1	Integration in ABUS CMS software.....	139
10.2	Manage people	140
10.3	Manage and transfer access groups in FaceXess.....	141
10.4	Event display and event search.....	143
10.5	Schedule-controlled access	143
11.	Maintenance and cleaning.....	144
11.1	Maintenance	144
11.2	Cleaning.....	144
12.	Disposal.....	145
13.	Technical data.....	145

1. Intended use

The FaceXess device is used indoors or outdoors as an access control system with facial recognition combined with a video door communication system.




	<p>Any use other than that described above may result in damage to the product, and there are also other dangers. Any other use is not in accordance with the intended use and leads to the loss of the warranty or guarantee; all liability is excluded. This also applies if conversions and/or modifications have been made to the product.</p> <p>Read the operating instructions completely and carefully before commissioning the product. The operating instructions contain important information for assembly and operation.</p>
---	---

	<p>When leaving the house or apartment for a long time, it is advisable to lock doors mechanically.</p>
---	---

Any use other than that described above may result in damage to the product, and there are also other dangers. Any other use is not in accordance with the intended use and leads to the loss of the warranty or guarantee; all liability is excluded. This also applies if conversions and/or modifications have been made to the product.

Read the operating instructions completely and carefully, before you put the product into operation. The operating instructions contain important information for assembly and operation.

2. Explanation of symbols

	<p>The symbol with the lightning bolt in the triangle is used when there is danger to the health exists, e.g. due to electric shock.</p>
	<p>An exclamation point within the triangle is intended to alert the user to the presence of important instructions in this manual that should be followed.</p>
	<p>This symbol is to be found when special tips and notes on operation are to be given to you.</p>

3. Features and functions

Door phone with touch screen, camera & face recognition for interactionless access.

The door station identifies authorized persons with intelligent face recognition and automatically unlocks the entrance door. The video door intercom system thus offers convenient, interaction-free access, contactless and without a chip card or other identification media. The recognition range can be flexibly adjusted, and the face scan at a distance of up to 3 m takes only fractions of a second.

An almost normal bell

Only almost: because the FaceXess display can be customized, e.g. with house number, address, desired motifs, etc.

Safe and individual

The dual camera (optical, IR) reliably detects whether a person is allowed to enter or not - whether in backlight, darkness or if the person is wearing a cap or mask. The anti-spoofing function uses various features to check whether it is a genuine and authorized person or a manipulation, e.g. by holding photos or videos in front of them. 2-factor authorization is often required in sensitive areas. Thus, facial recognition can also be combined with PIN code or smart card. User data (faces) are stored locally and encrypted on the device. Unknown persons are not detected.

See, Speak, Open

ABUS FaceXess is easy to operate intuitively. The 7-inch touch display with virtual bell button is the user interface of the door station. On the smartphone (ABUS Link Station app) or the optional indoor monitor, you can see who is at the door, talk to the person and switch the electric strike. Up to 3 residential parties can be created (6 monitors each). The outdoor terminal can also be used stand-alone as a pure door opener.

- IP video door intercom with face recognition, unlocks the front door fully automatically, in fractions of a second. Optional: access via PIN code or chip key/key card at the integrated NFC card reader.
- Access for taught-in users on the 7" touchscreen via face scan or PIN code entry. Unknown persons use the virtual bell button on the display.
- See who is standing in front of the door: live image, intercom and door opening via indoor monitor or Link Station app, even when on the move. Top image quality and contrast thanks to 2 MPx dual camera.
- Good voice quality thanks to high-quality microphone and loudspeaker with noise cancellation: no noise, no echoes.
- Secure access, high protection against manipulation: terminal cannot be tricked with photo/video (anti-spoofing technology). Optional: 2-factor authentication combines facial recognition with PIN code/key card.
- For up to 3 residential parties: up to 6 monitors can be integrated per bell party via LAN/PoE or WLAN (Wi-Fi)
- Quickly and safely installed: The door station requires an external power supply. The data connection is made via LAN/WAN and a data line (2 wires) to the remote switching module that controls the door actuator.
- Weatherproof terminal for outdoor use (protection class IP65)
- Completely without keys: never again stand in front of a locked front door because of forgotten keys

4. Device description

For more information on connections and the correct installation of the face recognition terminal, please refer to the installation guide, available at www.abus.com.

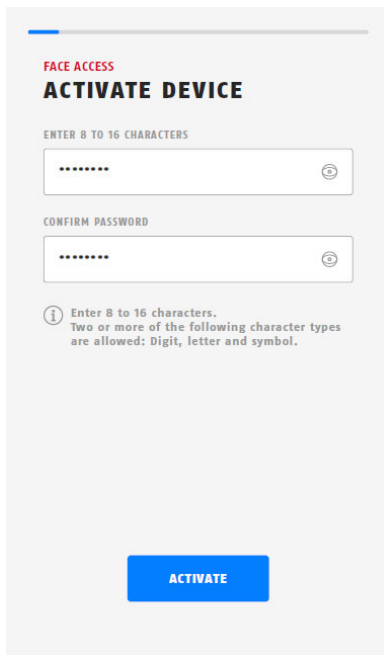
5. Description of the connections

For more information on connections and the correct installation of the face recognition terminal, please refer to the installation guide, available at www.abus.com.

6. Initial commissioning

6.1 Activation of the device via the local touch monitor

After starting the device, the input mask for assigning the device password appears.



A secure password must meet at least the following requirements:

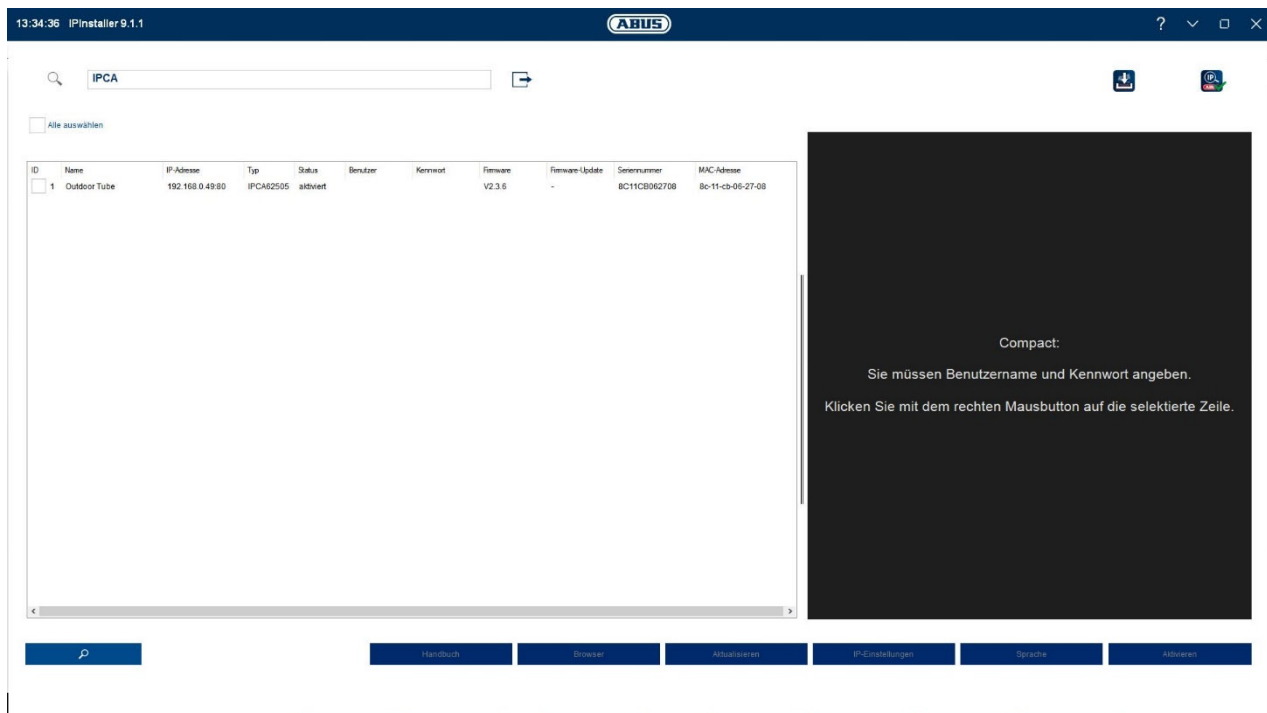
- 8-16 characters
- Valid characters: Numbers, lowercase letters, uppercase letters, special characters (!"#\$%&()*+,-./:;<=>?@[\\]^_{}~space)
- 2 different types of characters must be used

6.2 Activating the device via the ABUS IP Installer

For this method of activation, the device must first be integrated into the IP network. This is done via the wired network connection (LAN connection). The IP address is assigned automatically via the DHCP protocol.

Install and start the ABUS IP Installer. This is available via the ABUS web page www.abus.com for the respective product.

The device password can be assigned via the "Activate" key.



6.3 Activating the device via the web browser

For this method of activation, the device must first be integrated into the IP network. This is done via the wired network connection (LAN connection). The IP address is assigned automatically via the DHCP protocol.

The IP address that the device has been assigned by the DHCP server can be viewed via the ABUS IP Installer.

Enter the IP address of the device in the address bar of the browser. Now you can assign the initial password.



For IT security reasons, it is required to use a secure password with appropriate use of lowercase letters, uppercase letters, numbers and special characters.

No password is assigned ex works, this must be assigned when using the device for the first time. This can be done via the ABUS IP installer ("Activate" button) or via the web page.

A secure password must meet at least the following requirements:

- 8-16 characters
- Valid characters: Numbers, lowercase letters, uppercase letters, special characters (!"#\$\$%&()*+,-./:;<=>?@[\\]^_{}~space)
- 2 different types of characters must be used

Aktivierung

Benutzername:

Passwort:  **Stark**

8 bis 16 Zeichen sind erlaubt, einschließlich Großbuchstaben, Kleinbuchstaben, Ziffern und Sonderzeichen (!"#\$%&'()*+,-./:;<=>?@[\\]^_`{|}~ Leerzeichen). Mindestens zwei der oben aufgeführten Typen sind erforderlich.

Bestätigen: 

6.4 Install video plugin

For the installation of the video plugins you need appropriate rights on the PC.

Edge (Internet Explorer Mode) / Internet Explorer

For the video display in Internet Explorer, a so-called ActiveX plugin is used. This plugin must be installed in the browser. A corresponding query for the installation appears directly after entering user name and password.

	<p>If the installation of the ActiveX plugin is blocked in Internet Explorer, it is necessary to reduce the security settings for ActiveX installation/initialization.</p>
---	--

Google Chrome / Microsoft Edge

For video display in these browsers another video plugin is needed. If the plugin is missing in the PC, this plugin is offered for download and installation on the PC (after login to the website, link in the middle of the live view).



A firmware update via the web interface is only possible with the video plugin installed.

7. Configuration and operation via the touch monitor

The facial recognition terminal can be operated and configured directly via the display device using touch control (hereinafter referred to as "touch display").

7.1 Setup Wizard

The setup wizard guides you step by step through the most important menu items to get the device ready for basic operation. Read the instructions on the display, fill in the appropriate fields, and complete all steps of the wizard.

FACE ACCESS
ACTIVATE DEVICE

ENTER 8 TO 16 CHARACTERS

CONFIRM PASSWORD

i Enter 8 to 16 characters.
Two or more of the following character types are allowed: Digit, letter and symbol.

ACTIVATE

FACE ACCESS
E-MAIL FOR PASSWORD CHANGE

E-MAIL ADDRESS

i Set an E-Mail Address between 1 and 64 characters.

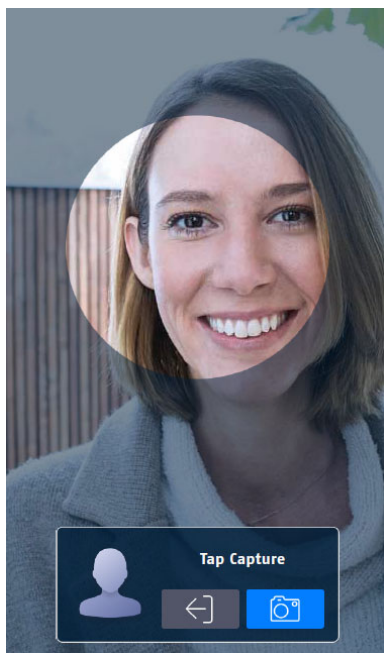
NEXT

FACE ACCESS
ADD ADMINISTRATOR

EMPLOYEE ID

NAME

← **NEXT**

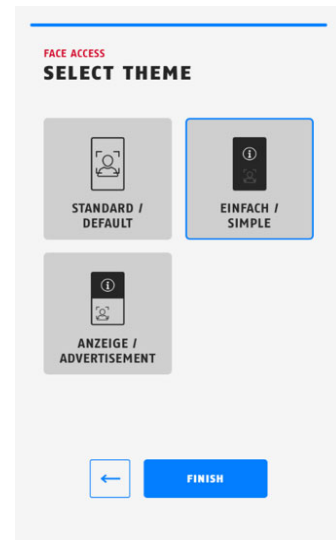


(Example images of the steps of the setup wizard)

7.2 Main operating page

7.2.1 View options (themes)





- Default:** Only call button(s), pin code and QR code button are displayed when configured, as well as the person's preview video if desired.
- Simple:** Only call button(s), pin code and QR code button are displayed during configuration. The preview video is not displayed. Face recognition active in the background.
- Information:** The difference from the standard mode is that there is space for displaying information in the upper part of the display.



Standard	Simply	Display




7.2.2. Symbols and information displays

In the upper right corner of the main view in the display there are four icons with the following information.

Symbol	Function
	<p>Display of active connection to the ABUS Link Station Cloud or active connection to an ABUS Link Station account.</p> <p>Icon: Connection to cloud successful, link to account successful Icon with "X": No connection to the cloud Icon with "!": Connection to cloud successful, no link to account</p>
	<p>Display of the connection to a WiFi network.</p> <p>Icon: Connection to WiFi network successful Symbol with "X": No connection to a WiFi network</p>
	<p>Display of the connection to a wired network (LAN).</p> <p>Icon: Connection to network successful Symbol with "X": No connection to a network</p>
	<p>This icon is currently not in use and has no function.</p>

7.2.3 Adjustable operating keys

Various operating keys could be activated on the local display.

Key	Function
	Bell button(s) for calling up to 3 apartments
	Open the input mask for the pin code.
	Open the screen for presenting a QR code.

7.3 Administrator menu

7.3.1 User

The User Management settings page displays all the users that have been set up.

Each line provides information about the user name, ID, user type and which media are set up for the respective user.



If this character is displayed after the user name, this user has administrator rights. This user can make settings in the configuration menu and, for example, set up additional users.



If these symbols are shown in white, then a face for facial recognition or at least one smart card for authentication are set up for the user.



Pressing this arrow icon allows configuring the properties, media and permissions of a set up user.



Pressing the plus icon, additional users can be set up.

Geben Sie ID/Name/Kartenummer ein.

The input field can be used to search for users in the list



By pressing this arrow symbol, the menu can be exited.

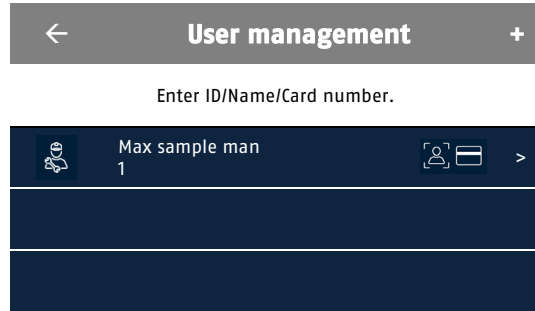
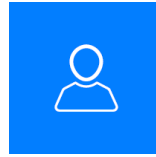
Employee ID:

Assignment of an individual identification number. Length 1 - 32 characters. Combination of lower case letters, upper case letters or digits.

Name:

Assignment of a name. Length 1 - 128 characters (recommendation: max. 24 characters). Combination of lower case letters, upper case letters, digits or special characters (`.,#?!@%^$space*()\&/- _=[]+;:'"~|<>{})`

Face:



User data	
Employee ID	1
Name	Max Mustermann >
Face	Configured >
Map	0/5 >
Pin code	Not configured >
Auth. Settings	Device mode >
User role	Administrator >

Storage of a face image for the user. The person must look in the direction of the face recognition terminal and the face must be in the brightly marked circle (see graphic below right).



The administrator must inform the user that his facial image will be stored and processed in the device. The processing of the facial image is also referred to in the Privacy section.



Saving the image. It takes approx. 3 seconds for the ghost image to be successfully analyzed and captured. Then confirm the saving and exit this menu item (green check mark).



Exit the menu without saving an image.

Map:

Up to 5 smart cards can be added to each user. Tap on the arrow behind the line Card.

In the menu Card administration all taught-in cards per user can be viewed.

Use the + button to enter the menu to add cards. Now hold the desired card in front of the terminal. The card reader is installed in the lower area. You can also enter a card number manually.

Then select the card type:

- Normal card: Normal use
- Duress card: Also coercion card. Authentication is performed and a duress alert is sent to the app and CMS software.
- Super card: A super card always has access, even if special time periods are programmed for access via card (programming via ABUS CMS possible).
- Patrol Map: This type of map is used for patrols from device to device

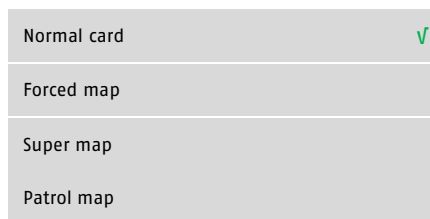
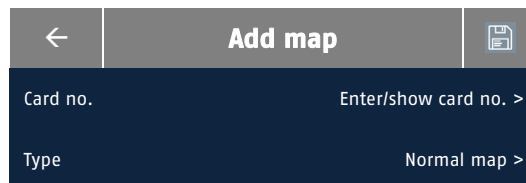
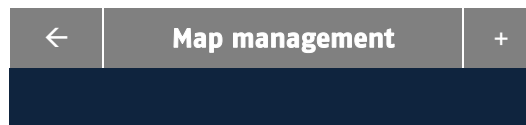
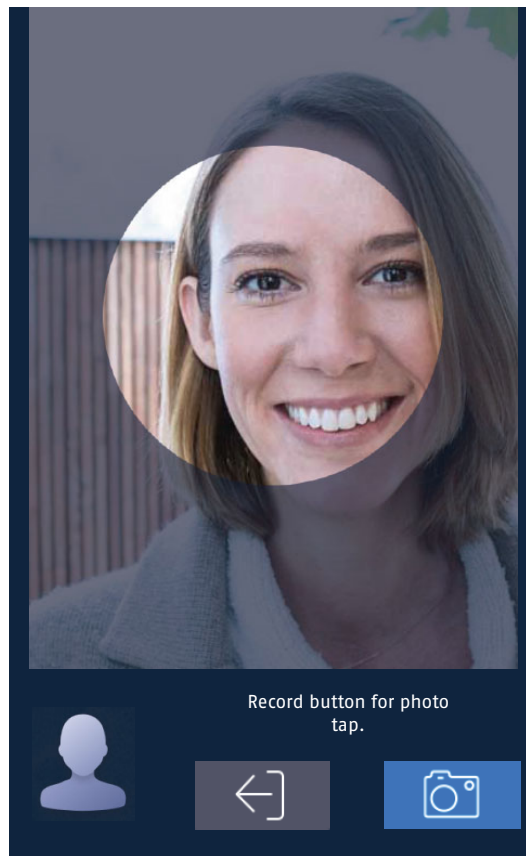
Pin Code:

Each user can be assigned an individual pin code. The pin codes of all users may only exist once each.

For use, please refer to the Access Control section.

Auth. Settings:

Determination of the type and necessary number of access media for each user (e.g. double verification via face and pin code).



Device mode: The authentication settings for the user follow the general settings of the device (default: single verification).

Custom: Individual setting for each user.

Single access data: one media must be presented for user access (face, pin or card).

Multiple access data: two media must be presented for user's access (combination of face, pin or card).

User role:

Specify whether a user should be given administrator rights.

An administrator can make changes to the entire configuration locally at the touch panel (e.g. add more users or add opening media).

	New Pin Code	
	Confirm Pin Code	
Please enter 4 to 8 digits.		
Cancel OK		

Device mode	✓
Custom	

←	Authentication settings
Mode	Custom >
Type	Single credentials >
Method	>

Normal user	✓
Administrator	




Access via web interface or ABUS CMS software can only be made via the device password that was assigned during initial commissioning.

7.3.2 Access options

End Device Authorization Mode:

Specify the allowed authentication methods, which are built directly into the device and can be used.

 A change in the terminal authentication mode is not applied to users who have already been taught in. It is therefore necessary to teach in users who have already been taught in again.

Type: Single credential:
A single authentication method is required to identify a user.
Face or card or password (pin).

Multiple credentials:
Two authentication methods are required to identify a user.

Method: Face or card
Face or password (pin)
Card or password (pin)

Reader Authorization Mode:

Defining the allowed authentication methods which can be connected to the device (e.g. via RS-485 or Wiegand interface).


The configuration is done analog to the item End Device Authorization Mode.

Activate NFC card:

In this item, the use of NFC cards (except Mifare Classic) can be enabled or disabled.

Activate M1 card:

When activated, "Mifare Classic" (M1) type can be used.

 The "Mifare Classic" method is not considered secure. Therefore, cards of this type should only be used in combination with the "multiple credentials" method (card+pin or face+card).

Remote authentication:

Function currently not in function

Door contact:



Access options	
End Device Auth. Mode	>
Reader Auth. Mode	>
Activate NFC card	<input checked="" type="checkbox"/>
Activate M1 card	<input checked="" type="checkbox"/>
Remote authentication	<input type="checkbox"/>
Door contact	Leave closed >
Opening time (s)	5 >
Authentication interval (s)	5 >

End Device Auth. Mode	
Type	Single credential >
Method	Map/Face >

Reader Auth. Mode	
Type	Single credential >
Method	Map/Face >

Function not used

Opening duration (s):

Setting of the switching duration for the relay (e.g. for elect. door opener, cable harness designation "LOCK")

Authentication interval (s):

Set the amount of time before a new recognition of faces or cards occurs.
After the 1st detection, this time voltage is initially waited for.

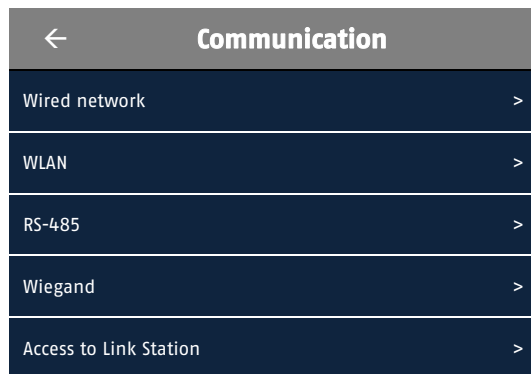
7.3.3 Communication

Wired network

DHCP: The DHCP function automatically determines all necessary network settings. A DHCP server must be located in the IP network. DHCP is active by default.

- IPv4 address: IP address in the network
- IPv4 subnet mask: Subnet mask in network
- IPv4 gateway: IP address of the router

- IPv6 mode: Auto: The IPv6 connection data is provided by the DHCP server.
 Manual: Manual assignment
 Router Advertisement: The IPv6 connection data is provided by the DHCP server (router) in conjunction with the ISP (Internet Service Provider).
- IPv6 address: IP address in the network
- Subnet prefix length: manual assignment
- IPv6 gateway:
- Router Advertisement:



- Retrieve DNS automatically: The button is only available if the DHCP function is activated. The IP address of a DNS server is thus determined automatically.
- Preferred DNS server: Enter an IP address of a DNS server.
- Alternate DNS server: Enter an IP address of a DNS server.

WLAN (WiFi)

Activate WLAN: Activation of the WLAN function

If the WLAN interface is activated, the device searches for visible and basically available WLAN access points (listing of WLAN SSIDs).

Then select the desired WLAN.

You will now be prompted to enter the password for the WLAN network.

After successful connection, the IP address is assigned automatically via DHCP function.

RS-485

Activation and configuration of the RS-485 interface. This interface can be used, for example, to enable an ABUS security module (TVAC20340) for the secure connection of an electric door opener. Door opener can be enabled.



Once the RS-485 option "Control unit" has been selected, the terminal must be restarted after exiting the menu.

After the restart, the wired inputs (door sensor and door button) and outputs (relays NO/NC) are no longer available on the terminal itself.

Then the inputs and outputs on the safety module must be used.

Other RS-485 operating modes:

Access controller: Function not used

Control unit: Connection of the safety module

Card reader: Connection of an external card reader via RS-485

Elevator module: Function not used

Wiegand

The device is equipped with a Wiegand interface. The interface can process the Wiegand 26-bit or 34-bit formats (max. 8 or 10-digit card number, deletion of the first digits for longer card numbers).

The Wiegand interface must first be activated.

Select whether the interface should function as an output or input.

Output: Data is transmitted to a receiver in Wiegand format. The card number of the user's card that was taught in first is transmitted as data.

Input: An external card reader that transmits the card data in Wiegand format can be connected.

Access to Link Station

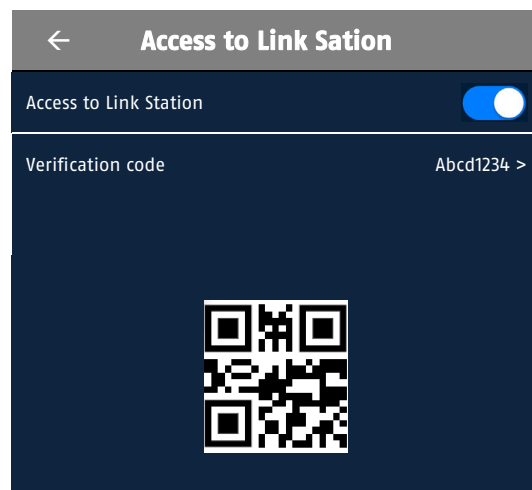
The ABUS Link Station function provides access via the ABUS Link Station APP.

The function must be activated and a so-called verification code must be assigned.

In the ABUS Link Station app, the terminal can then be added to the app by scanning the QR code and tapping the verification code.

Usable functions are:

- Transmission of the sabotage message (sabotage contact on the back of the terminal)
- Status network connection
- Live image transfer to the app
- Two-way audio
- Switch door contact via app (sequence)
- Switch door contact via app (permanent)
- Call function from terminal to app via ring button in touch display





The following setting is required for the call function from terminal to app:

Local display menu: Admin menu / Display / Quick key / Call app
 Web interface: Admin login / Configuration / Intercom / Button to call / APP

7.3.4 Basic settings

Voice settings / sound settings

Voice output: Activate voice output on access and activate key tone on entry
 Volume: 0 -10

Time settings

Time zone: Setting the time zone
 Current time: Manual time setting. The NTP function for automatic determination of the time can be optionally performed via the web interface.
 DST setting: Setting the data for the normal/summer time changeover.

← General settings	
Voice settings	>
Time settings	>
Idle state	60 >
Select language	German >
Block no.	1 >
Building no.	1 >
Unit no.	1 >
Image correction	Disable >

Idle state

The terminal's monitor will display the default background image after 20 seconds without any screen activity (fixed period).

After another 20 - 999 seconds, the monitor enters sleep mode, i.e. the display is off. This period can be set.

Select language

GERMAN and ENGLISH are available as display languages in the local display.

Block / building / unit no.

These parameters assign the terminal to the desired main monitor area in the context of intercom use.



The configuration of the main monitor number is done in the menu "Admin menu / Display / Quick key / Call special room / Room number" for the 1st main monitor (or 1st apartment).

Up to 3 keys can be programmed to call 3 different main monitors (or apartments). The configuration of all 3 buttons (incl. naming) is done in the web interface of the terminal (Admin-Login / Configuration / Intercom / Button to call / Call specified indoor station")

Image correction

Image correction is used to brighten or smooth the video representation in the display.

7.3.5 Biometric

Application mode

Select in which area the terminal was installed (inside, outside). Depending on the selection, certain presets are made for the device and in particular for the camera module.

Face authenticity level

This setting item decides how detailed the face authenticity check should be. The more detailed the verification, the longer the verification takes. The verification can last for several seconds, which has a negative impact on the user experience.

Detection distance

Setting the detection distance (0.5 to 2 meters, Auto) can avoid unwanted detection when walking past. In principle, it is not advisable to set a greater detection distance, as the facial features are more clearly recognizable to the camera at a shorter distance.

With the Auto option, there is no distance limit, the terminal decides itself on the start of the face analysis based on the recognizability of a face.

Face detection interval

The recognition interval (1 to 10 seconds) can avoid unwanted repeated face identification when you are in front of the device. The value is practically a pause time between 2 identifications.

WDR

If it is unavoidable that the terminal is installed against a strong light source (e.g. sun), then this function can help to improve the recognition of faces (Wide Dynamic Range - Wide dynamic range for the camera).

Face 1:N Safety level

Des is the security level for comparing a captured face image (live) with many face images in the user database.

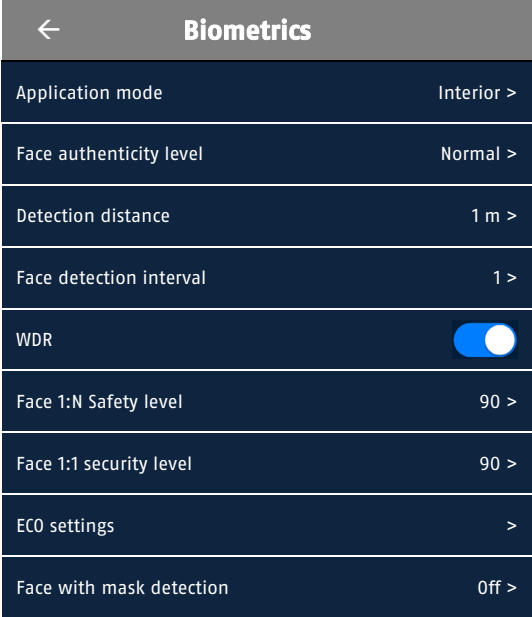
The larger the value, the smaller the false acceptance rate and the larger the false rejection rate.

Face 1:1 security level

This is the security level for comparing a captured facial image (camera) with exactly one facial image from the user database. This value only comes into effect when using the "Multiple credentials" method, since before face comparison the user has already partially authenticated himself via card or PIN.

ECO settings

In low-light conditions, the terminal can improve detection through the additional use of infrared light. (Extended Camera Operation / Extended Camera Use)



Biometrics	
Application mode	Interior >
Face authenticity level	Normal >
Detection distance	1 m >
Face detection interval	1 >
WDR	<input checked="" type="checkbox"/>
Face 1:N Safety level	90 >
Face 1:1 security level	90 >
ECO settings	>
Face with mask detection	Off >

ECO Threshold: The higher the value, the faster the ECO mode is used by the terminal.

ECO mode (1:1): Analog normal 1:1 safety level.

ECO mode (1:N): Analog normal 1:N safety level.

Face with mask detection

After activating this function, the terminal checks whether a detected person is wearing a mouth-nose protection (colloquially "mask").

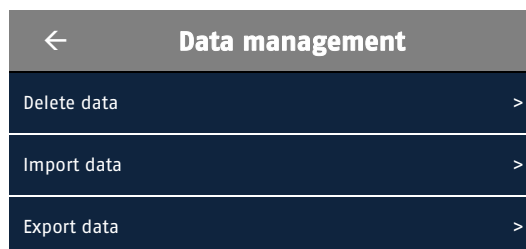
Reminder to wear: The person can be reminded to wear the mask (message in the display) and the door opens.

Must wear: The person is reminded to wear the mask. The door will not be opened until the person wears a mask.

7.3.6 Database

Delete data

Delete user data: Delete all taught-in users. The user administration is then empty. Access to the administrator menu is then only possible with the admin password of the device.



Data import

User data: Import user
Face data: Importing facial images for existing users
Access control settings: Configuration settings of the device

The data import can be done by using the USB-C interface on the device. If you want to import a database file from previously exported data that has a password, you must enter it. Otherwise, just press OK.

- If you want to transfer data from one device to another, you must always import the user data first. Afterwards, face images can be imported.
- The USB drive must support FAT32.
- The folder where face pictures must be located on the USB stick is "enroll_pic".
- More folders "enroll_pic1", "enroll_pic2" etc. can be created.
- The file names of the images must be structured as follows.
Card no._name_department_employee_ID_gender.jpg

Gender: "male" or "female"

Employee ID max. 32 characters, lower case letters, upper case letters and numbers. The ID must be unique, and must not start with "0".

- Requirements for face picture: whole face, looking directly into the camera, no hat or other headgear, picture format JPEG or JPG, resolution min. 640 x 480 pixels, picture size between 60 KByte to 200 KByte

Data export

Face data: Export of face images only
Event data: Logbook data
User details: User details
Access control settings: Configuration settings of the device.

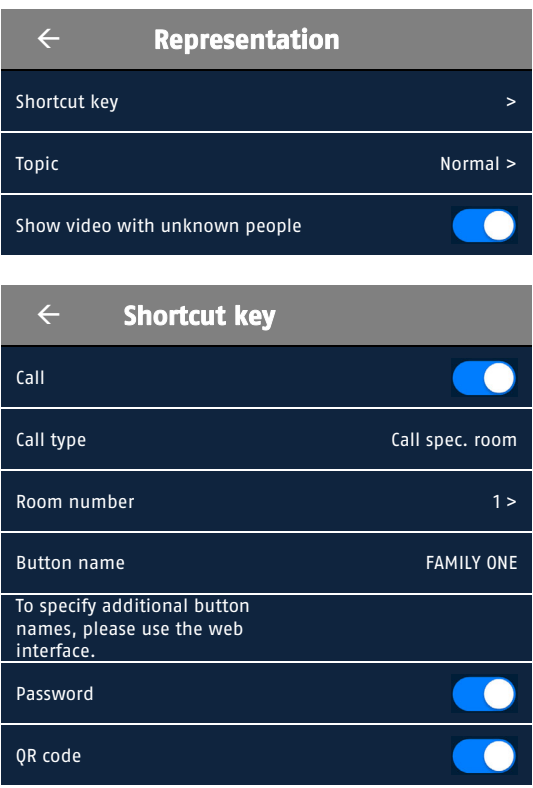


Please do not use this function if bell buttons are activated.

Data export can be performed by using the USB-C interface on the device. The export requires the assignment of a password (4 - 6 characters).

- The data is exported as a database format and is not readable by third party software
- USB sticks from 1 - 32 GByte are supported.
- There should be at least 512 Mbyte of memory available.







7.3.8 Representation

<p>Shortcut key</p> <p>Call: When activated, the display of the device shows min. one call button</p> <p>Call Type: Central Call: Call Spec. Room Call App</p> <p>Room no. Button name: FAMILY ONE</p> <p>Password: Button for PIN entry. QR Code: Card number as QR code (CMS required)</p> <p>Topic</p> <p>Default: Only call button(s), pin code and QR code button are displayed when configured, as well as the person's preview video if desired.</p> <p>Simple: Only call button(s), pin code and QR code button are displayed during configuration. The preview video is not displayed. Face recognition active in the background.</p> <p>Information: The difference from the standard mode is that there is space for displaying information in the upper part of the display. Programming is done via the web interface.</p> <p>Show video on unknown person</p> <p>If this option is deactivated, no live video is shown in the display for persons who are not stored in the user database with a picture. Only activated call buttons, pin code input or QR code button appear.</p>	 <p>The image shows two screenshots of a mobile application interface. The top screenshot is titled 'Representation' and shows settings for 'Shortcut key', 'Topic' (Normal), and 'Show video with unknown people' (toggled on). The bottom screenshot is titled 'Shortcut key' and shows settings for 'Call' (toggled on), 'Call type' (Call spec. room), 'Room number' (1), 'Button name' (FAMILY ONE), 'Password' (toggled on), and 'QR code' (toggled on). A note in the bottom screenshot states: 'To specify additional button names, please use the web interface.'</p>
--	---

8. Configuration and operation via web browser

If the terminal is already successfully connected to a network via a network cable or the WiFi settings have been successfully programmed via the display, the web page of the terminal can be called up via a browser (preferably Chrome, Edge). The IP address of the device can be found via the ABUS IP Installer described above.

The following controls are used on the settings pages in the web browser.

Functional element	Description
	Save settings made on the page. It is important to note that settings are only applied after pressing the save button.
	Function activated
	Function disabled
	List selection
	Input field
	Slider

8.1 Configuration via web browser

8.1.1 Local configuration

Under the menu item "Local configuration" you can make settings for the live view, file paths of the recording and snapshots.

The screenshot shows the 'KONFIGURATION' (Configuration) page for 'LIVE-ANSICHT' (Live View). The left sidebar contains navigation options: LOKAL, SYSTEM, NETZWERK, VIDEO / AUDIO, BILD, ALLGEMEIN, GEGENSPRECHANLAGE, ZUGANGSKONTROLLE, BIOMETRIE, and THEMA. The main content area is titled 'Live-Ansicht-Parameter' and includes the following settings:

- Streamtyp:** Radio buttons for 'Hauptstream', 'Substream', and 'Fließend'. 'Hauptstream' is selected.
- Wiedergabeleistung:** Radio buttons for 'Geringste Verzögerung', 'Ausgewogen', and 'Fließend'. 'Ausgewogen' is selected.
- Automatischer Start der Liv...:** Radio buttons for 'Ja' and 'Nein'. 'Nein' is selected.
- Bildformat:** Radio buttons for 'JPEG' and 'BMP'. 'JPEG' is selected.
- Aufnahmedateieinstellungen:**
 - Aufnahmedateigröße:** Radio buttons for '256M', '512M', and '1G'. '512M' is selected.
 - Aufnahmedateien speicher...:** A text input field with a folder icon and an 'Öffnen' button.
- Bild- und Clip-Einstellungen:**
 - Fotos in Live-Ansicht speich...:** A text input field with a folder icon and an 'Öffnen' button.

A red box highlights the 'Speichern' (Save) button at the bottom center of the configuration area.

Live view parameters

Stream Type: Specify which video quality should be displayed as default in the Live View page.
 Main stream (1st video stream), high quality.
 Substream (2nd video stream), low quality

Playback performance: This setting influences the buffering of the video stream. With "Lowest delay", hardly any buffering takes place, with "Smooth", correspondingly more buffering takes place, but this can lead to delayed display.

Automatic start of live view: If you activate the option, then the live image is started immediately after calling up the "Live View" page.

Image format: Setting in which format the single image from the live view (Instant Image button) should be saved (JPEG, BMP).

Recording file settings

Here you can define the file size for recordings, the recording path and the path for downloaded files. To apply the changes click on "Save".

Recording file size: You can choose between 256 MB, 512 MB and 1 GB as the file size for the recordings and downloaded videos.

Save as: Here you can specify the file path to be used for manual recordings.

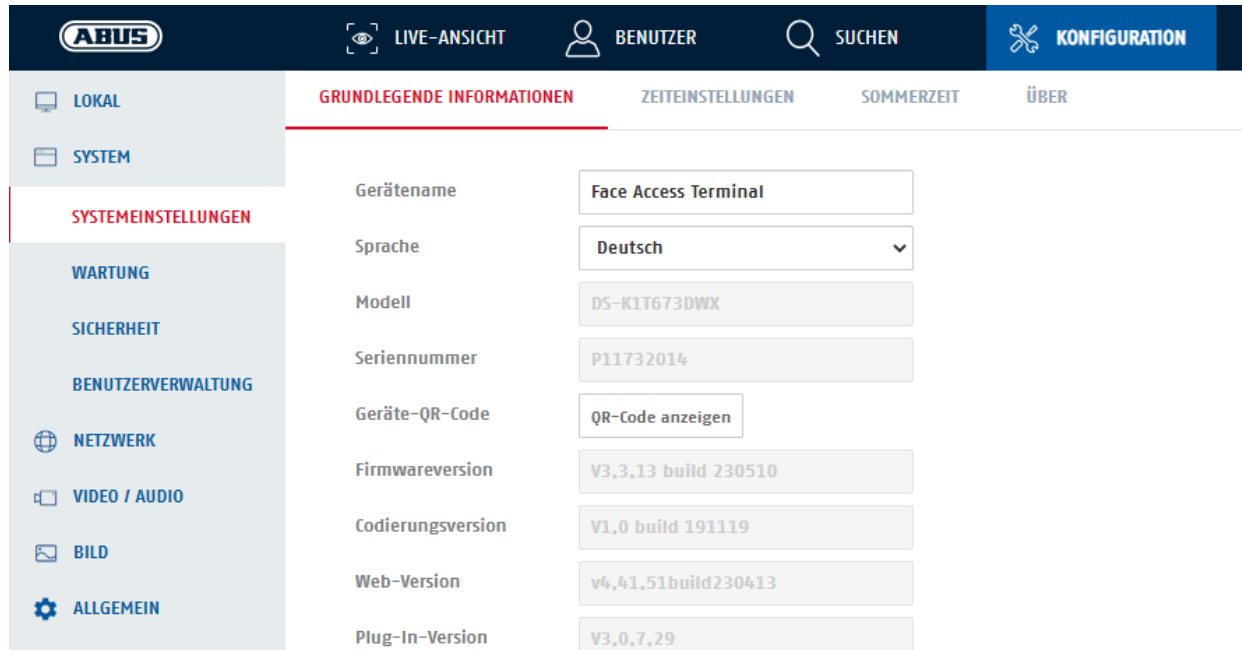
Image and clip settings

Save photos in live view: Select the file path for instant images from live view.

8.1.2 System

8.1.2.1 System settings

8.1.2.1.1 Basic information



The screenshot shows the ABUS configuration interface. At the top, there is a navigation bar with the ABUS logo, a 'LIVE-ANSICHT' button, a user profile icon labeled 'BENUTZER', a search icon labeled 'SUCHEN', and a 'KONFIGURATION' button. Below this is a sidebar menu with options: LOKAL, SYSTEM, SYSTEMEINSTELLUNGEN (highlighted in red), WARTUNG, SICHERHEIT, BENUTZERVERWALTUNG, NETZWERK, VIDEO / AUDIO, BILD, and ALLGEMEIN. The main content area is titled 'GRUNDLEGENDE INFORMATIONEN' and contains a list of device settings:

Gerätename	Face Access Terminal
Sprache	Deutsch
Modell	DS-K1T673DWX
Seriennummer	P11732014
Geräte-QR-Code	QR-Code anzeigen
Firmwareversion	V3,3,13 build 230510
Codierungsversion	V1,0 build 191119
Web-Version	v4,41,51build230413
Plug-In-Version	V3,0,7,29

Device name: Here you can assign a device name for the camera. Click on "Save" to apply this name.

Language: You can choose between German and English language for the display in the web interface.

Model: Model number display

Serial number: Display of the serial number

Device QR code: When this button is pressed, the serial number is displayed as a QR code. This makes it easier to add the terminal to the ABUS Link Station app.

Firmware version: Display of the firmware version

Cod. version: Display of the coding version

Web version: Display the web page version

Plug-in version: Display the version of the video plug-in for video display.

8.1.2.1.2 Time settings

The screenshot shows the ABUS configuration interface. At the top, there is a navigation bar with 'LIVE-ANSICHT', 'BENUTZER', 'SUCHEN', and 'KONFIGURATION'. Below this, a sidebar on the left contains menu items: 'LOKAL', 'SYSTEM', 'SYSTEMEINSTELLUNGEN' (highlighted in red), 'WARTUNG', 'SICHERHEIT', 'BENUTZERVERWALTUNG', 'NETZWERK', and 'VIDEO / AUDIO'. The main content area is titled 'ZEITEINSTELLUNGEN' and includes the following settings:

- Zeitzone:** A dropdown menu set to '(GMT+01:00) Amsterdam, Berlin, Rom, Paris'.
- Zeit synchronisieren:** Two radio buttons: 'NTP' (unselected) and 'Manuelle Zeitsynchronisation' (selected).
- Gerätezeit:** A text input field showing '2023-05-16 11:32:35'.
- Zeit einstellen:** A text input field showing '2023-05-16 11:32:28' with a calendar icon, and a checkbox for 'Synchronisation mit Computerzeit' which is unchecked.

A red-bordered 'Speichern' button is located at the bottom of the settings area.

Time zone

Time zone selection (GMT)

Time setting method

NTP: Using the Network Time Protocol (NTP), it is possible to synchronize the camera's time with a time server. Enable NTP to use the function.

Server address: IP server address of the NTP server.


NTP port : Network port number of the NTP service (default: port 123).

NTP update interval: 1-10080 min.

Man. Time synchronous.

Device time: Display of the device time of the computer

Time setting: Display the current time based on the time zone setting.
Click "Sync with Comp Time" to accept the device time of the computer. to take over.

	Apply the settings made with "Save".
---	--------------------------------------

8.1.2.1.3 DST / Daylight saving time

GRUNDLEGENDE INFORMATIONEN ZEITEINSTELLUNGEN **SOMMERZEIT** ÜBER

Sommerzeit aktivieren

Startzeit	März	Letzter	Sonntag	02
Endzeit	Oktober	Letzter	Sonntag	03
SZ-Verschiebung	60Minute(n)			


Speichern

Summertime

Activate daylight saving time: Select "Daylight Saving Time" to automatically adjust the system time to daylight saving time.

Start time: Set the time for the changeover to daylight saving time.

End time: Set the time for the changeover to winter time.

	Apply the settings made with "Save".
--	--------------------------------------

8.1.2.1.4 About / License information

Display of open source license information

8.1.2.2 Maintenance

8.1.2.2.1 Updating and maintenance

Restart: Click "Restart" to restart the device.

Restore parameters

Default: Reset values except for IP parameters and user data.

Restore all: Reset all values.

Unlink App Account: This button unlinks the current terminal and Link Station account.

Export the device parameters / log file: Assign a password for the export file part

Import d. device parameters: Select here the file path to import a configuration file.

Refresh

Control device (terminal): Select the path where the new firmware is stored.

Online update: This function is not available.



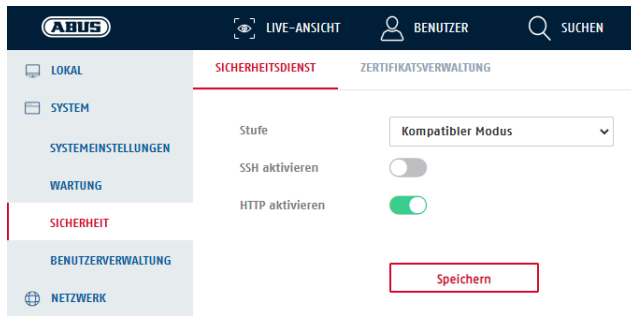
Accept the settings made with "Save".

8.1.2.2 Log query / logbook

In this item, log information of the camera can be displayed. An SD card must be installed in the camera for log information to be saved.

8.1.2.3 Safety

8.1.2.3.1 Security service



Enable SSH: This function enables the Telnet port and protocol.

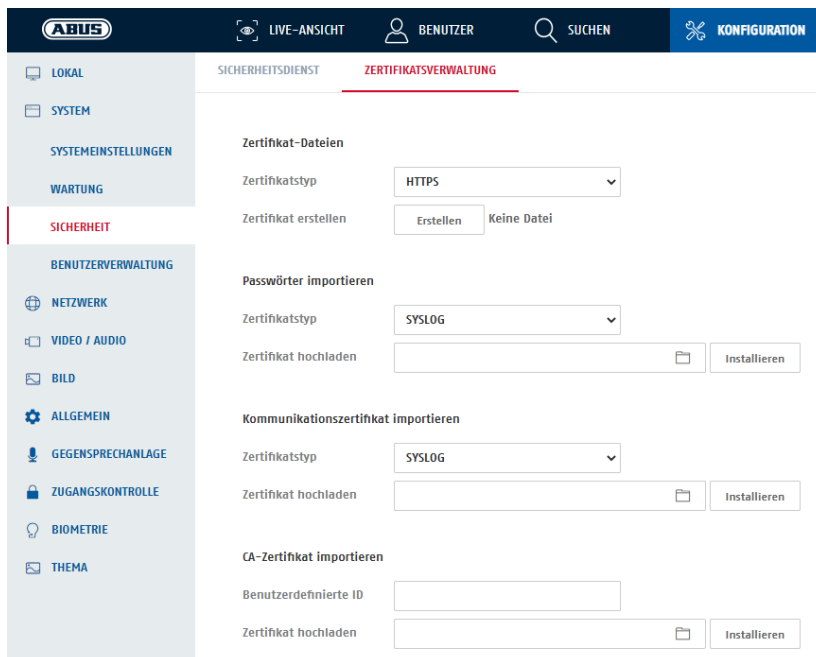
Enable HTTP: Deactivation of the http interface for displaying the web page is possible.




Note: After deactivation, the function can only be reactivated by resetting the terminal ("Restore all").

8.1.2.3.2 Certificate management

On the one hand, a self-signed HTTPS certificate can be created in this settings page, and on the other hand, an HTTPS certificate certified by a CA can be uploaded.



8.1.2.4 User management

Nr.	Benutzername	Benutzerrolle	Vorgang
1	admin	Administrator	

Gesamt 1 Elemente

Benutzer ändern ✕

Benutzername

Benutzerrolle

Altes Passwort


Neues Passwort

gültige Passwort-Zeichenzahl [8-16], Ihr Passwort darf eine Kombination aus Ziffern, Kleinbuchstaben, Großbuchstaben und Sonderzeichen enthalten und muss aus mindestens zwei dieser Zeichenarten bestehen.

Bestätigen

Under this menu item you can change the password of the administrator user. To do this, click on the Edit icon at the back of row 1.

To do this, you must enter the old password, as well as enter and confirm the new password.

	Accept the settings you have made by clicking "OK". Click "Cancel" to discard the data.
---	--

8.1.2.4.1 Arming / disarming info

This function is not supported.

8.1.3 Network

8.1.3.1 TCP/IP

The screenshot shows the ABUS network configuration interface. The top navigation bar includes 'LIVE-ANSICHT', 'BENUTZER', 'SUCHEN', and 'KONFIGURATION'. The left sidebar has categories: 'LOKAL', 'SYSTEM', 'NETZWERK', 'ALLGEMEINE EINSTELLUN...', 'ERWEITERT', 'VIDEO / AUDIO', 'BILD', 'ALLGEMEIN', 'GEGENSPRECHANLAGE', 'ZUGANGSKONTROLLE', 'BIOMETRIE', and 'THEMA'. The main content area is titled 'TCP/IP' and contains the following settings:

DHCP	<input checked="" type="checkbox"/>
LAN	LAN1
IPv4-Adresse	192,168,0,100
IPv4-Subnetzmaske	255,255,255,0
IPv4-Standard-Gateway	192,168,0,1
IPv6-Modus	Route Advertisement Route Adv. anzeigen
IPv6-Adresse	::
IPv6-Subnetz-Präfix-L...	0
IPv6 Standardgateway	::
MAC-Adresse	8c:11:cb:0e:5f:44
MTU	1500
NIC-Typ	Auto
DNS-Server	
DHCP	<input type="checkbox"/>
Bevorzugter DNS-Server	0,0,0,0
Alternativer DNS-Server	0,0,0,0

- DHCP:** If a DHCP server is available, click DHCP to automatically apply an IP address and other network settings. The data is automatically taken from the server and cannot be changed manually. If no DHCP server is available, please fill in the following data manually.
- IPv4 address:** Setting the IP address for the network interface
- IPv4 subnet mask:** Manual setting of the subnet mask
- IPv4 default gateway:** Setting of the default router (e.g. IP address of your Fritz Box).
- IPv6 Mode:**
Manual: Manual configuration of the IPv6 data.
DHCP: The IPv6 connection data is provided by the DHCP server.
Route Advertisement: The IPv6 connection data is provided by the DHCP server (router) in conjunction with the ISP (Internet Service Provider).
- IPv6 address:** Display of the IPv6 address. In IPv6 mode "Manual" the address can be configured.

- IPv6 subnet mask: Display the IPv6 subnet mask.
- IPv6 Standard Gateway: Display of the IPv6 default gateway (default router).
- MAC address: The IPv4 hardware address of the terminal is displayed here, you cannot change it.
- MTU: Setting of the transmission unit, select a value 500 - 9676. 1500 is preset by default.

DNS server

After activating the DHCP function, the DNS server is determined automatically. Alternative the manual input via:

- Preferred DNS server: DNS server settings are required for some applications. (e.g. sending e-mail) Enter the address of the preferred DNS server here.
- Alternate. DNS server: If the preferred DNS server is not available, this alternative DNS server will be used. Please enter the address of the alternative server here.

8.1.3.2 Port

TCP/IP	PORT	WI-FI
HTTP-Port	<input type="text" value="80"/>	
RTSP-Port	<input type="text" value="554"/>	
HTTPS-Port	<input type="text" value="443"/>	
Serverport	<input type="text" value="8000"/>	

Speichern

If you want to access the camera externally, the following ports must be configured.

- HTTP port: The default port for HTTP transmission is 80, alternatively this port can be given a value in the range 1024~65535. If there are multiple network devices on the same subnet, each device should be assigned its own unique HTTP port.
- RTSP port: The default port for RTSP transmission is 554, alternatively this port can be given a value in the range 1024~65535. If there are multiple network devices on the same subnet, each device should be assigned its own unique RTSP port.
- HTTPS port: The default port for HTTPS transmission is 443.
- Server port: The default port for this is 8000. communication port for internal data. Alternatively, this port can be given a value in the range 1025~65535. If there are multiple network devices on the same subnet, each device should be given its own unique SDK port.



Apply the settings made with "Save".

8.1.3.3 WiFi

If the WiFi function was not already activated on the display during local setup, this can also be done here in the web interface.

After activation, the system automatically searches for available WiFi access points (2.4 GHz only!).

Select an access point, you will then be prompted to enter the password of the access point (e.g. WiFi password of your Fritz Box).

Alternatively, an access point name can be added manually.

In the item "Network settings" you can see the determined network parameters (this is usually the case, since many access points have the DHCP function enabled).

The screenshot shows the ABUS web interface with the 'WI-FI' configuration page. The left sidebar contains navigation options like 'LOKAL', 'SYSTEM', 'NETZWERK', and 'ERWEITERT'. The main content area shows the 'WLAN' section with a red checkmark indicating it is active. Below this, there are buttons for '+ Hinzufügen' and 'Aktualisieren'. A table lists detected WLAN access points with columns for 'WLAN-Name' and 'Vorgang'. The table contains the following entries:

WLAN-Name	Vorgang
Verbunden--FunkBox	
FRITZ!Box 7590 UU	
connect Gast	
connect 2,4	
WLAN-944731	
Vodafone Homespot	
FRITZ!Box 7560 LU	
Vodafone Hotspot	
FRITZ!Box 6490 Cable	

At the bottom of the page, there is a button labeled 'Netzwerkeinstellungen'.

8.1.3.4 Cloud access / ABUS Link Station

The ABUS Link Station function is used for easy remote access to the ABUS device via Link Station APP (iOS / Android). Products can be easily set up and released via QR code - without complicated configurations in the router (no port forwarding necessary).

Activate the function and assign a verification code (6-12 characters, A-Z, a-z, 0-9, min. 2 different character types recommended).

The QR code (under "System / System settings / Basic information / Device QR code") can then be photographed in the ABUS Link Station APP.

The screenshot shows the configuration page for 'CLOUD ACCESS'. The 'Cloud Access Mode' is set to 'Link Station'. The 'Aktivieren' checkbox is unchecked. The 'Registrierungsstatus' is set to 'Offline-Bild'. There is a link for 'Rechtliche Informationen'. A text input field for 'Stream-Verschlüsselung/Verschlüsselungss...' is present, with a note below it: '6 bis 12 Buchstaben (a bis z, A bis Z) oder Ziffern (0 bis 9), Groß-/Kleinschreibung beachten. Es wird empfohlen, eine Kombination von mindestens 8 Buchstaben oder Ziffern zu verwenden.' A red 'Speichern' button is at the bottom.

Usable functions are:

- Transmission of the sabotage message (sabotage contact on the back of the terminal)
- Status network connection
- Live image transfer to the app
- Two-way audio
- Switch door contact via app (sequence)
- Switch door contact via app (permanent)
- Call function from terminal to app via ring button in touch display



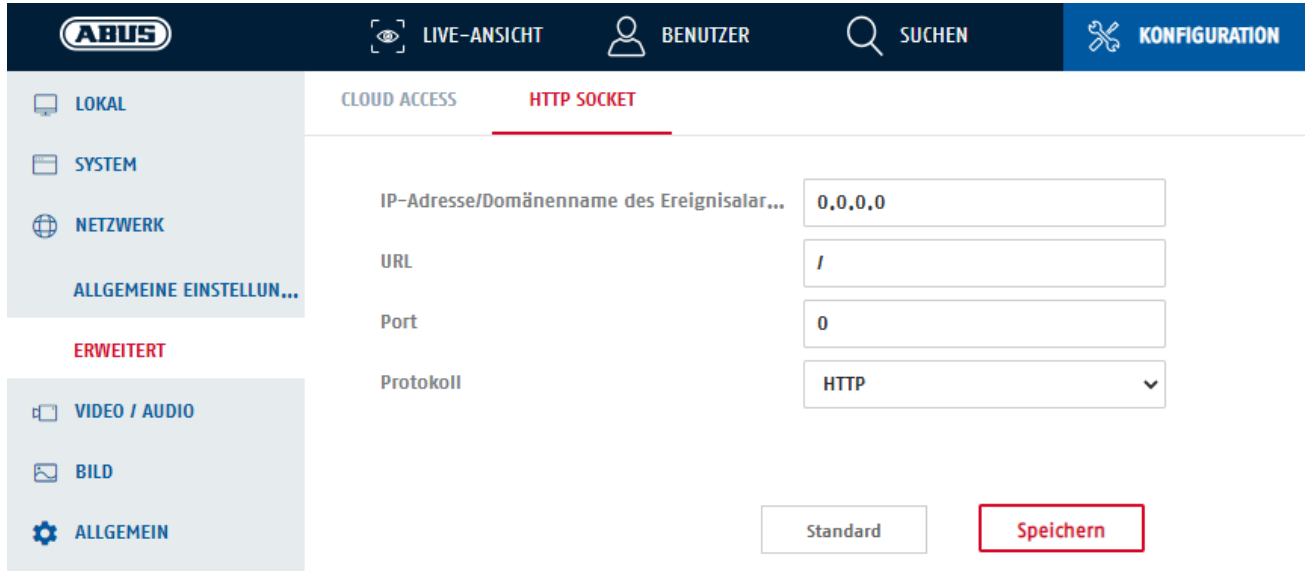
The following setting is required for the call function from terminal to app:

Local display menu: Admin menu / Display / Quick key / Call app

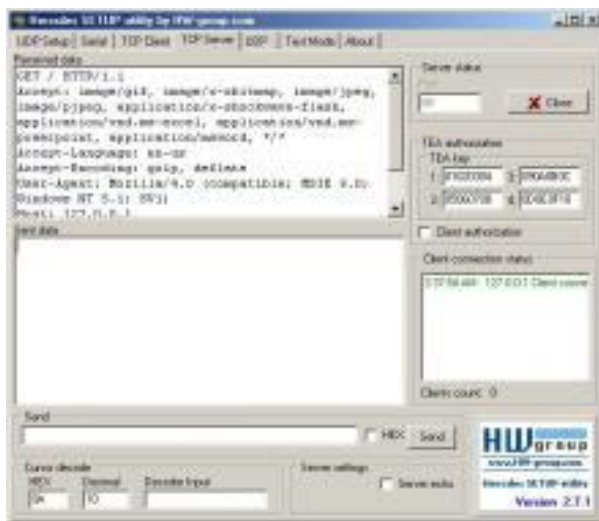
Web interface: Admin login / Configuration / Intercom / Button to call / APP

8.1.3.5 HTTP socket

Event information can be sent to an alarm host via JSON Telegram. In this way, events can be transmitted to third-party software for further processing. Alarm informati For easy testing of this function, the TCP Server function of the "Hercules Setup Utility" software (Hercules SETUP utility | HW-group.com) can be used, for example.



Hercules Setup Utility:



8.1.4 Video

8.1.4.1 Video

The screenshot shows the ABUS configuration interface. At the top, there is a navigation bar with 'LIVE-ANSICHT', 'BENUTZER', 'SUCHEN', and 'KONFIGURATION'. Below this is a sidebar menu with options like 'LOKAL', 'SYSTEM', 'NETZWERK', 'VIDEO / AUDIO', 'BILD', 'ALLGEMEIN', 'GEGENSPRECHANLAGE', 'ZUGANGSKONTROLLE', 'BIOMETRIE', and 'THEMA'. The main content area is titled 'VIDEO' and contains the following settings:

Videokanal	Kamera1
Kameraname	P11732014
Streamtyp	Hauptstream
Videotyp	Video und Audio
Auflösung	1280*720
Bitrate-Typ	Konstante
Videoqualität	Niedrig
Bildfrequenz	25 fps
Max. Bitrate	2048 Kbps
Videocodierung	H.264
I Frame Intervall	25

Video channel: Only the 1st camera can be changed in certain parameters.

Camera name:The serial number is assigned as the name by default. This name can be changed.

Stream type: Select the stream type for the camera. Select "Main Stream (Normal)" for recording and live view with good bandwidth. Select "Sub Stream" for live view with limited bandwidth.

Video Type: The video type is set to "Video and Audio" by default so that intercom to the monitor or app can work. The "Video" option would block audio.

Resolution: The video resolution is fixed at 1280x720 pixels.

Bitrate type: Specifies the bit rate of the video stream. The video quality can be higher or lower depending on the motion intensity. You can choose between a constant and variable bit rate.

Video quality: This menu item is only available if you have selected a variable bitrate. Set the video quality of the video data here. The video quality can be higher or lower depending on the motion intensity. You have the choice between six different video qualities, "Minimum", "Lower", "Low", "Medium", "Higher" or "Maximum" (represented via "+").

Frame rate: Specifies the frame rate in frames per second.

Max. Bitrate: The bitrate of the video stream is fixed to a certain value, set the max. bitrate between 32 and 16384 Kbps. A higher value corresponds to a higher video quality, but requires a larger bandwidth.

Video encoding: Select a standard for video encoding, you can choose between H.264, H.265.

I Frame Interval: Set the I frame interval here, the value must be in the range 1 - 400.



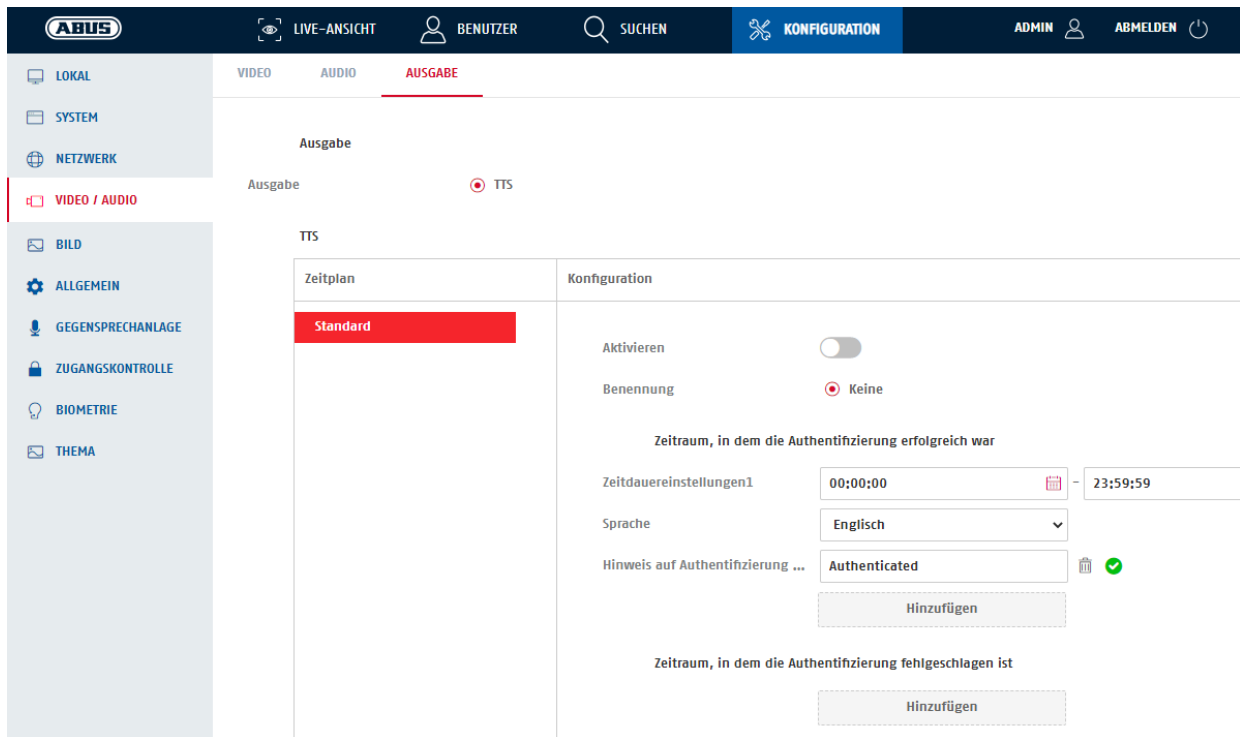
Accept the settings made with "Save".

8.1.4.2 Audio

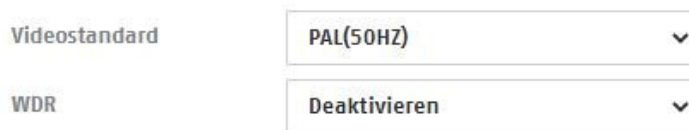
Audio channel:	Only the audio part of camera 1 can be edited
Streamtype:	The settings define the audio settings for the main or sub-stream respectively.
Audio encoding:	This is the audio codec used.
Volume input:	Volume of the audio input (Mic)
Output volume:	Volume of the audio output (loudspeaker)
Voice output:	The voice output can output a word message on successful or unsuccessful authentication (default is off).

8.1.4.3 Audio output

The audio output module is a text-to-speech module with the output language English. Messages can be issued in 4 different time periods in case of successful or unsuccessful authentication.



8.1.5 Image



Video standard: Set the video standard or network frequency for the terminal's region of use [here](#) (PAL, 50 Hz, 25 frames/s or NTSC, 60 Hz, 30 frames/s)

WDR: If the contrast between background and foreground (face) is too high, then the WDR (Wide Dynamic Range) function can help with display and detection.



Image settings: Set various camera parameters [here](#) (brightness, contrast, saturation, sharpness). These settings apply to the local display as well as the video stream (web, app).

		Standard
Bildeinstellung	Ergänzungslichttyp	IR-Zusatzlicht
Ergänzung Lichtparameter	Zusatzlichtmodus	EIN
Bildkorrektur	LED-Helligkeit	<input type="range" value="50"/>
Bildfusion		

Supplementary light parameters

Supplementary light type: Infrared light (IR) is available as an additional light source.
 Additional light mode: The additional light source can be activated (default) or deactivated.
 LED brightness: Stepless adjustment of IR light intensity.

		Standard
Bildeinstellung	Bildkorrektur aktivieren	<input type="checkbox"/>
Ergänzung Lichtparameter	Aufhellen	<input type="range" value="0"/>
Bildkorrektur	Glätten	<input type="range" value="0"/>
Bildfusion		

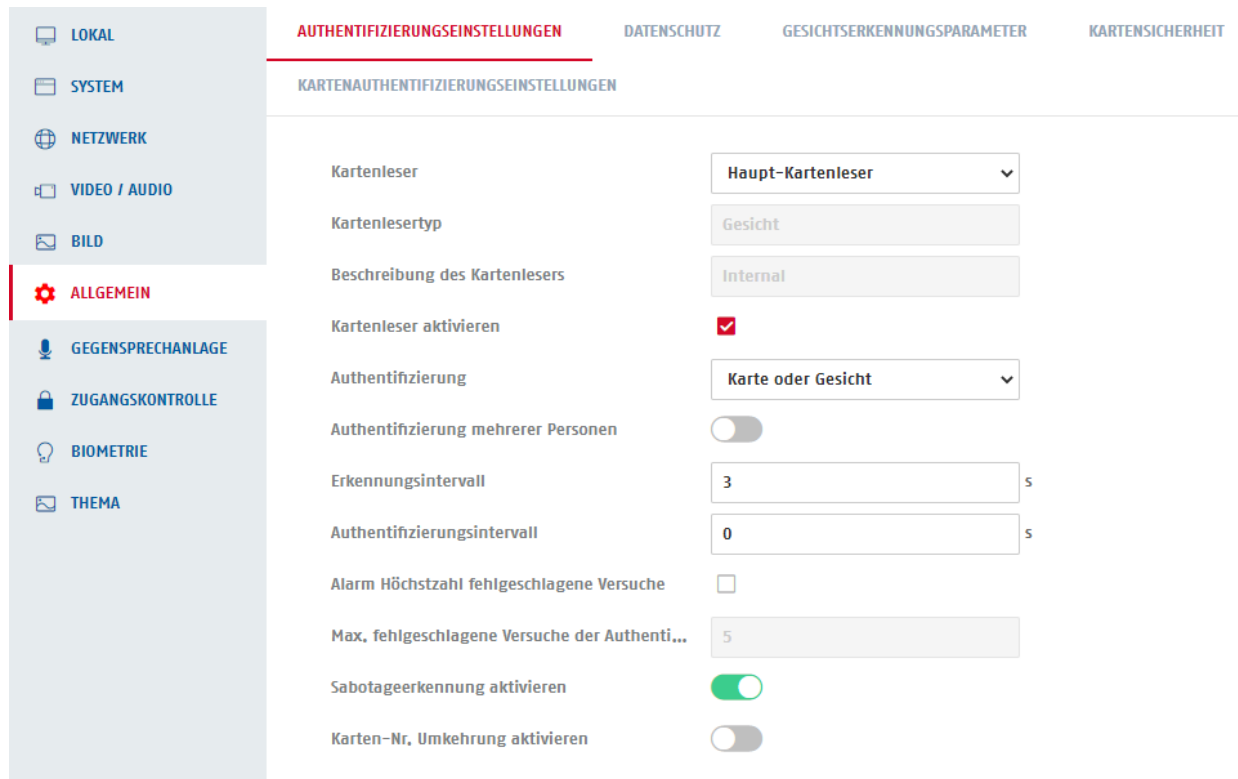
Enable image correction: Enable this option to use brightening and smoothing of the video image. The options are applied only on the local screen.

		Standard
Bildeinstellung	Bildfusion	<input type="radio"/> Automatisch <input checked="" type="radio"/> Deaktivieren
Ergänzung Lichtparameter	Empfindlichkeit	<input type="range" value="2"/>
Bildkorrektur		
Bildfusion		

Image fusion: In low light conditions it is possible to superimpose the infrared image of the 2nd camera over the image of the 1st camera. This creates a bright image even in low light conditions. This helps with the recognition of faces.
 Sensitivity: The higher the value, the earlier the infrared image is superimposed on the normal image.

8.1.6 General

8.1.6.1 Authentication settings



Card reader: Definition of which card reader is to be configured, or which combination is to be made with face recognition.


Main card reader: The built-in card reader in the terminal.

Sub-card reader: A card reader connected via RS-485, for example.

Card reader type: *Not used*

Description of the card reader: *Not used*

Activate card reader: If this option is deactivated, the complete internal card reader in the terminal is deactivated and cannot be used.

Authentication:  This is where you specify the number and type of authentication media for all users. Example: "Card and face" option means that all enrolled users must present both media to be authenticated. This only applies if the user setting follows the device settings. Each user can also have individual authentication rules.

**Card or Face Card
or Face or Password(Pin) Card
and Face
Card Face
and Password(Pin)
Face and Card
Face**



Note: the fingerprint option is not available.

Authentication of multiple persons: With the face recognition terminal, it is possible that a defined group of people is required to successfully gain access. All persons in the group must successfully authenticate themselves via their faces on the device within a defined period of time.



Further programming of the groups of persons is done via the ABUS CMS software (see chapter 9).

Recognition interval: Specify a period of time before the detection of the same person A should occur again. If a person B is detected during this period, person A can be detected again.

Authentication interval: This option limits the recognition of a person A for the entered time period. The person A can authenticate only 1 time within this period.

Note: When using multiple authentication Face + Pin, it is advisable to set the interval to min. 3 seconds. Otherwise, after entering the pin and successfully opening the door, the pin entry page appears again immediately.

Alarm maximum number of failed attempts: Function for alerting in case of multiple incorrect logins.
Max. failed attempts: Number (1 - 10) of attempts until alarm is triggered.

Enable tamper detection: The tamper switch is located on the back of the terminal. If this is triggered by removing the terminal from the wall, a PUSH notification can be sent to the linked account of the ABUS Link Station APP when the network and Internet connection is active.

Activate card no. reversal: The read card number can be reversed in its processing if required.



Note: After activating this function, cards that have already been taught-in must be reassigned to users (new teach-in required).

8.1.6.2 Data protection

Event Memory Settings:

This option determines how often and at what frequency the event memory should be cleared.

Overwrite: When the system detects 95% event memory level, it will delete the oldest 5%.

Delete old events periodically: select a period from 10 min. to 86400 min. This is the period during which events are still stored.

Delete old events after specified time: Set a time at which daily the event memory should be deleted.

Show authentication result:

The option defines the way a recognized person is shown in the display. The selected options (face image, name, user ID) are also displayed in the green info message area.

Upload and save image:

- Upload image after authorization: After authorization of a person, the image is uploaded from the database by the user to a currently connected ABUS CMS software. This can be displayed in the menu item "ABUS CMS / Access Control / Monitoring" in the event list.
- Save image after authorization: After authorization of a person, an image of this scene is saved in the terminal. The call is made via event list ("Search") in the web interface of the FaceXess device.
- Save registered image: After authorizing a person, the registered image is saved in the event list.
- Upload image of linked camera: Transfer of the current image to the ABUS CMS software if a linked action has been programmed via the ABUS CMS software.
- Save image of linked camera: Saves the current image in the device if a linked action has been programmed via the ABUS CMS software.

Alle Bilder im Gerät löschen

Registrierte Gesichtsbilder löschen

Aufgenommene Bilder löschen

Löschen

Delete registered face images:



Delete all face images of all configured users. The face images are then unrepeatably deleted.

Delete captured images:

All images saved in the event list will be deleted.

8.1.6.3 Face recognition parameters

LOKAL

SYSTEM

NETZWERK

VIDEO / AUDIO

BILD

ALLGEMEIN

AUTHENTIFIZIERUNGSEINSTELLUNGEN

DATENSCHUTZ

GESICHTSERKENNUNGSPARAMETER

KARTENAUTHENTIFIZIERUNGSEINSTELLUNGEN

Betriebsmodus

Zutrittskontrollmodus

Speichern

This entire settings page is fixed to the Access Control Mode option. There is no other selection.

8.1.6.4 Card security

Activate M1 card:
M1 card encryption:

Mifare Classic (M1) cards.
A special variant (rare) of the Mifare Classic card (M1) with encryption. After activation, only such Mifare Classic cards can be used (no more standard M1 cards).

Activate EM card:
Activate DesFire card:

EM cards with 125 kHz
Mifare Desfire cards (unencrypted) can be read, but the security mechanisms of the Desfire card are not available.

Read content of DesFire card:
Enable FeliCa card:

Function currently not supported
The card reader can recognize and use Sony FeliCa type cards.



It is recommended to use the card reading function only in connection with multiple evaluation of authentication features (e.g. card + face or face + PIN).



The card reader can currently only read cards of type Mifare Classic (M1). ABUS Security Center cards with encryption cannot be read.
Cards of type Mifare Desfire without encryption can be read, but their security performance falls back to the level of Mifare Classic.

8.1.6.5 Card authentication settings

AUTHENTIFIZIERUNGSEINSTELLUNGEN

DATENSCHUTZ

GESICHTSERKENNUNGSPARAMETER

KARTENSICHERHEIT

KARTENAUTHENTIFIZIERUNGSEINSTELLUNGEN

Kartennr.-Regel

Kartenauthentifizierungsmodus

Wiegand 34 (4 Bytes) ▼

Speichern

This function is valid in connection with a connected Wiegand card reader (via connection cable "Wiegand W0, W1 and GND). The format in which the card data is read out is defined here (complete card number without additional coding, Wiegand 26 bit or 34 bit).

8.1.7 Intercom system

8.1.7.1 Device number

	GERÄTENR.	VERKNÜPFTE NETZWERKEINSTELLUNGEN	TASTE ZUM ANRUFEN
LOKAL			
SYSTEM			
NETZWERK			
VIDEO / AUDIO			
BILD			
ALLGEMEIN			
GEGENSPRECHANLAGE			
ZUGANGSKONTROLLE			
BIOMETRIE			
THEMA			
	Gerätetyp	Zugangskontrollgerät	
	Etage Nr.	1	
	Türstation Nr.	0	
	Erweiterte Einstellungen		
	Block Nr.	1	
	Gebäude Nr.	1	
	Einheit Nr.	1	
		Speichern	

To use the terminal in conjunction with monitor indoor stations, first select the "Access control device" or "Door station" option.

Device type: Access control device or door station - the terminal works as a main face recognition terminal, with option as an intercom for max. 3 residential units.

Outdoor door station - not used

Using the device at the main input (or single input)

Next, the "Door station no." must have the value 0. The other 3 main monitors of the apartments use the numbers 1, 2 and 3.

Use of the device at the side entrance

The device works as a face recognition terminal at the side entrance (max. 99), with an option as an intercom for max. 3 residential units. A main face detection terminal must be present in the system.

The value for the item "Door station no." must be 1 - 99.



After changing the "Door station no." from 0 to 1 (or higher), the device restarts.

The other settings for Block, Building and Unit No. can each remain at the value "1" in this application.

8.1.7.2 Linked network devices

GERÄTENR.	VERKNÜPFTE NETZWERKEINSTELLUNGEN	TASTE ZUM ANRUFEN
Gerätetyp	Zugangskontrollgerät	
SIP-Server-IP	0.0.0.0	
Hauptstation IP	0.0.0.0	
Speichern		

The SIP Server function is currently not supported.



If the value for "Door station no." in the "Device number" menu is 1 or higher, an additional input field "Main door station IP" appears.

When using the terminal as a device at the secondary entrance, the IP address of the first facial recognition terminal (main entrance) must be entered in the "Main station door station IP" item.

GERÄTENR.	VERKNÜPFTE NETZWERKEINSTELLUNGEN	TASTE ZUM ANRUFEN
Gerätetyp	Türstation	
Haupt-Türstation IP	0.0.0.0	
SIP-Server-IP	0.0.0.0	
Hauptstation IP	0.0.0.0	
Speichern		

8.1.7.3 Call key

GERÄTENR. VERKNÜPfte NETZWERKEINSTELLUNGEN TASTE ZUM ANRUFEN DRÜCKEN

Nr.	Tasteneinstellungen			
01	<input checked="" type="checkbox"/> Angegebene Innenstation anrufen	<input type="checkbox"/> Anruf-Überwachungszentrale	<input type="checkbox"/> APP	
01	<input checked="" type="checkbox"/> Aktivieren	Zimmer...	<input type="text" value="1"/>	Name <input type="text" value="FAMILY ONE"/>
02	<input checked="" type="checkbox"/> Aktivieren	Zimmer...	<input type="text" value="2"/>	Name <input type="text" value="FAMILY TWO"/>
03	<input checked="" type="checkbox"/> Aktivieren	Zimmer...	<input type="text" value="3"/>	Name <input type="text" value="FAMILY THREE"/>

This configuration page describes the configuration of the call button(s) on the touch display of the terminal.

Call specified indoor station: Up to 3 call buttons for 3 different appliances can be shown and activated. The sequence of the keys in the display is implemented from bottom to top. However, the sequence can be manipulated via the "Apartment no." of the monitor.

The indication of the "room no." is at the same time the setting of the apartment number in the respective main monitor.

The designation of the names allows deutsche umlauts as well as upper and lower case. The length of the key designation should not exceed 22 characters.

Call monitoring center (CMS): When selected, only one "Management Center" call button appears in the display. When the call button is pressed, a call is made to a connected ABUS CMS software. A pop-up window appears in the CMS software, through which a 2-way audio communication can be established, or the relay on the terminal can be switched remotely (open door).

APP: Call the connected Link Station app.



If the system contains 2 or 3 monitors, then this can also be used as an intercom system within the building between the apartments. The input of the call command on the respective monitor is then as follows.

Example INTERCOM call between indoor stations 1, 2 or 3:

Call from monitor 1 to monitor 2: 1-1-1-2
 Call from monitor 3 to monitor 1: 1-1-1-1

8.1.8 Access control

8.1.8.1 Door parameters

Door number: The terminal represents access via a door. The value is fixed to "Door 1".

Name: Name for the door

Opening duration (1 - 255 sec.): Duration for the switching time of the relay after successful authentication.

Timeout alarm when the door is open: If the door remains open for longer than the set time in this item, this status will be displayed in the ABUS CMS software in the event list.

Door contact: A door contact can be installed on the door to reflect the opening status of the door. For this purpose, 2 contacts are available on the connection cable. The status is displayed in the ABUS CMS software in the event list.

Output key type: The output key (BTN) has no function.

Extended opening time: People with extended access get a longer opening time.

Door remains open with the first person: This item is related to the function "Leave door open after first person for period". After detecting a person from a defined group of people, the door can remain open for this period.

Duress code: If a person enters this code on the terminal, the door will be opened and a duress alarm will be sent to the connected ABUS CMS software.

Super password: A global pin code for door opening. Super password and duress code must be different.

8.1.8.2 Elevator control

TÜRPARAMETER	AUFZUGSSTEUERUNGSPARAMETER	RS-485
Aufzugssteuerung akti...	<input checked="" type="checkbox"/>	
Aufzug Nr.	Aufzug Nr,1	▼
Aufzugs-Controller-Typ	Default	▼
Schnittstellentyp	RS485	▼
Anzahl Untergeschosse	0	
<div style="border: 1px solid red; padding: 5px; display: inline-block;">Speichern</div>		

The Elevator control option is not currently used.

8.1.8.3 RS-485

TÜRPARAMETER	AUFZUGSSTEUERUNGSPARAMETER	RS-485
RS-485 aktivieren	<input checked="" type="checkbox"/>	
Nr.	1	▼
Peripheriegerätetyp	Kartenleser	▼
RS-485-Adresse	1	
Baudrate	19200	▼
Datenbit	8	▼
Stoppbit	1	▼
Parität	Keine	▼
Flusssteuerung	Keine	▼
Kommunikationsmodus	Halbduplex	▼

The RS-485 interface is primarily used in connection with the ABUS TVHS20340 security module. This module is used for secure connection of all external components such as a door opener.

For the use of the safety module the option "Access controller" must be set as peripheral device type.

8.1.8.4 Wiegand settings

Wiegand	<input type="checkbox"/>
Wiegand-Richtung	<input type="radio"/> Eingang <input checked="" type="radio"/> Ausgang
Wiegand-Modus	<input type="text" value="Wiegand 26"/>

Speichern

The terminal has a so-called Wiegand interface. The interface can be configured as input or output.

A Wiegand card reader can be connected to the Wiegand interface as input.

As an output, card data can be sent after capture to an access control unit that can accept the Wiegand protocol.

Info: When a face is recognized and authentication is successful, the card number programmed first is sent via the Wiegand scan interface.

8.1.9 Biometrics

The screenshot shows the ABUS configuration interface for Biometrics. The left sidebar contains navigation options: LOKAL, SYSTEM, NETZWERK, VIDEO / AUDIO, BILD, ALLGEMEIN, GEGENSPRECHANLAGE, ZUGANGSKONTROLLE, BIOMETRIE, and THEMA. The main content area is titled 'BIOMETRIE BEREICHSKONFIGURATION' and lists the following settings:

- Gesicht Anti-Spoofing:
- Sicherheitsebene bei Live-Gesichtserkennung: Normal Bekanntheit Höchste
- Erkennungsreichweite: Automatisch 0,5m 1m 1,5m 2m
- Anwendungsmodus: Innen Außen
- Gesichtserkennungsmodus: Normalmodus (dropdown)
- Kontinuierliches Gesichtserkennungsintervall: 3 s (slider)
- Neigungswinkel: 45 ° (slider)
- Gierwinkel: 45 ° (slider)
- Bewertungsschwelle: 50 (slider)
- Übereinstimmungsschwellenwert 1:1: 90 (slider)
- Gesichtsübereinstimmungsschwellenwert 1:N: 90 (slider)
- Gesichtserkennungs-Zeitüberschreitungswert: 3 s (slider)
- Gesicht mit Maskenerkennung:
- ECO-Modus:
- ECO-Modus Schwellenwert: 4 (slider)
- ECO-Modus (1:1): 80 (slider)
- ECO-Modus (1:N): 80 (slider)

Face anti-spoofing:

Anti-spoofing is the technical term for preventing attempts at manipulation. There are various parameters for checking the authenticity of a person standing in front of the terminal.

Security level for live face recognition: The

security level can be set in 3 levels (Normal, Medium, High). The higher the level is set, the longer it takes to recognize people, but the better the recognition is protected against manipulation (e.g. attack by holding a printed image).



Even higher security can be achieved by using multi-factor authentication (e.g. face + pin).

Detection distance:

Setting the detection distance (0.5 to 2 meters, Auto) can avoid unwanted detection when passing by. In principle, it is not advisable to set a longer detection distance, as the facial features are more clearly recognizable to the camera at shorter distances.

With the Auto option, there is no distance limit; the terminal itself decides on the start of the face analysis based on the recognizability of a face.

Application mode: The

selection "inside" or "outside" influences various camera parameters (internal parameters).

Face detection mode:

Normal mode - In this mode, it is possible to upload facial images of people via the ABUS CMS software through the network interface as well.

Advanced mode - In this mode, uploading facial images of persons via the ABUS CMS software is not possible. The face images must always be

taught-in locally on the device.



After changing and saving the extended mode, the device restarts and all previously saved face images of all taught-in users are deleted. The user entries themselves are retained.

All users must then be taught in again directly on the FaceXess device.



Please do not change the mode after you have started enrolling people.

Continuous face detection interval:	setting how many seconds face detection should be performed every (1-10 sec).
Tilt angle:	This is the angle when people look at the FaceXess device from too far above or below.
Yaw angle:	This is the angle of max. face rotation in front of the camera (head is held crooked).
Evaluation Threshold:	
Match threshold 1:1:	This value specifies how exactly the facial features detected in the live image must match the stored image in the database. A high value means there must be a high match. This value only applies when using multiple authentication (e.g. face + card).
Match threshold 1:N:	This value specifies how closely the facial features detected in the live image must match the stored image in the database. A high value means there must be a high match. This value applies to matching the live image with all face images in the database (for single authentication).
Face recognition Timeout:	For this maximum duration, face recognition is performed after a person has been detected. If the face has not been recognized by the end of this time, an error message appears.
Face with mask detection:	The device can detect whether a person is wearing a mouth-nose protection (colloquially mask). The detected person can be reminded to wear the mask, or the person must wear a mask to gain entry.
ECO mode:	In low light conditions, the terminal can improve detection by using infrared light additionally. (Extended Camera Operation)
ECO Threshold:	The higher the value, the faster the ECO mode is used by the terminal.
ECO mode (1:1):	Analog normal 1:1 safety level.
ECO mode (1:N):	Analog normal 1:N safety level.

8.1.9.1 Area configuration



Erkennungsbereich neu zeichnen

Rand (links) 0

Rand (rechts) 0

Rand (oben) 0

Rand (unten) 0

Speichern

The function limits the recognition area for face recognition, and can thus hide disturbing areas. The marking is done via the mouse in the preview image.

8.1.10 Topic

It is possible to set 3 different representations of the main page on the display.

Default: Only call button(s), pin code and QR code button are displayed when configured, as well as the person's preview video if desired.

Simple: Only call button(s), pin code and QR code button are displayed during configuration. The preview video is not displayed. Face recognition active in the background.

Information: The difference from the standard mode is that there is space for displaying information in the upper part of the display.

THEMA MEDIENDATENBANK


Anzeigemodus Standard Information Einfach

Ruhezustand

Ruhezustand nach s

Themenverwaltung + Programm hinzufügen

Begrüßungsnachricht ✎ 🗑



Vorlage

Überschrift

Schriftgröße Schriftfarbe

Untertitel

Schriftgröße Schriftfarbe

Untertitel 2

Schriftgröße Schriftfarbe

Hintergrundbild

Bei Auslieferung des Hintergrundbildes an das Gerät sti...

Bild(0/8) ✎ 🗑

+

Sleep mode: The terminal's monitor displays the default background image after 20 seconds without any screen activity (fixed period).

After another 20 - 999 seconds, the monitor enters the idle state, i.e. the display is off. This period can be set.

Theme management: In this item, text and images can be defined, as well as their display type.
Add program: A program is already preset as default. This can also be deleted. You can create a new program.

Greeting message: Text, font size, font color and background image can be defined.

Image: A maximum of 8 images can be defined, which can be displayed in a rolling manner.

The display of texts and image can be defined by a schedule (e.g. texts during the day and images during the night).

Wiedergabezeitplan ■ Begrüßungsnachricht ■ Bild ⓘ Wählen Sie zuerst ein Thema und stellen Sie die Anzeigzeit ein.

✕ Löschen 🗑 Alle löschen

Diashow-Intervall ○ 1 s

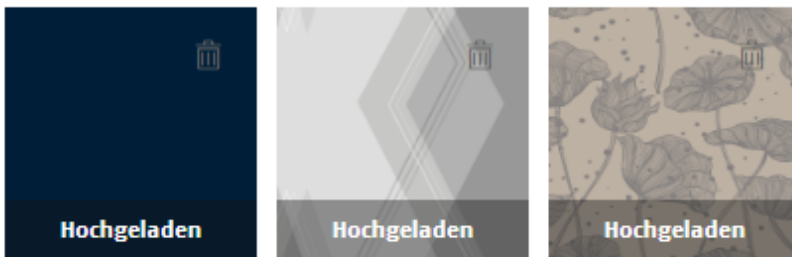
Speichern

8.1.10.1 Media database

THEMA **MEDIENDATENBANK**

ⓘ Benötigtes Bildformat ist jpg. Bis zu 8 Bilder können hochgeladen werden, Max. Bildgröße; 1 MB.

+ Hinzufügen



Add: There can be max. 8 images in the media database. 3 images are already stored, more images can be uploaded.

The image format must be as follows:
 - jpg format, max. 1 MB in size, 600 x 704 pixels, 24 bit color depth

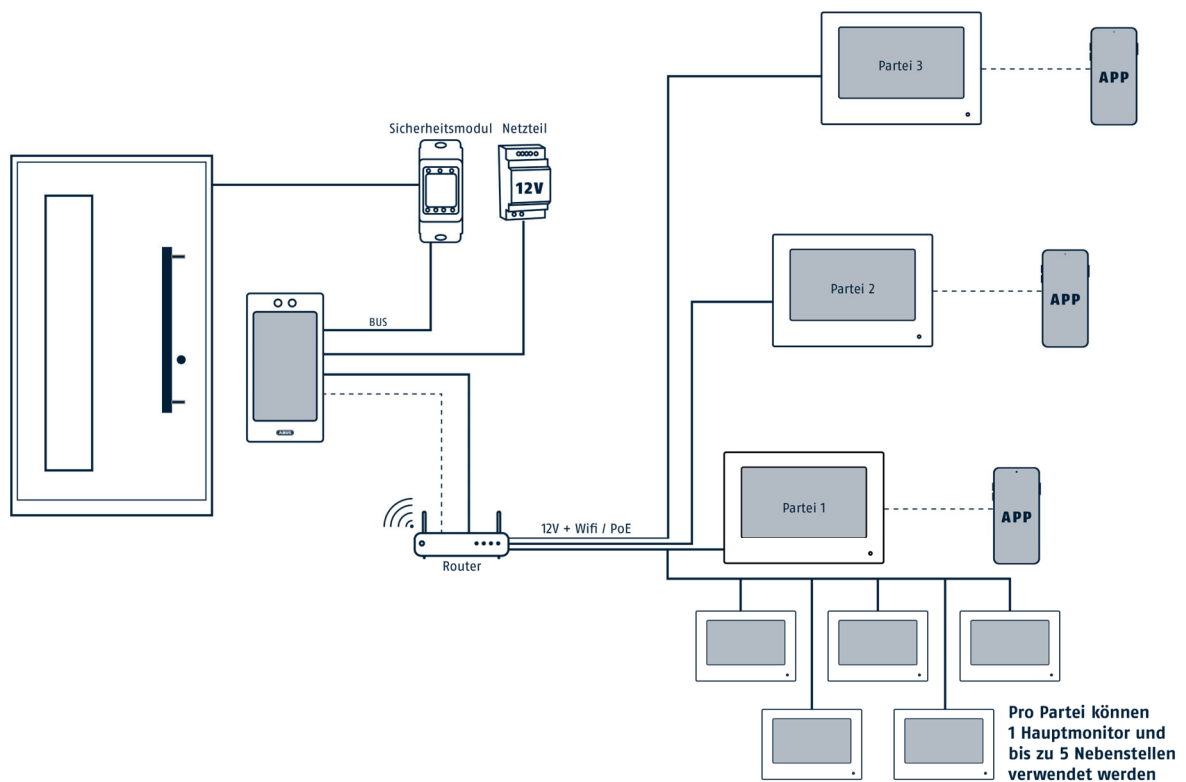
9. Integration and use of monitors of the Moduvis door intercom system

9.1 System overview Face Terminal / Monitor(s)

The respective main monitors in the apartments communicate with the FaceXess device via the IP network. The connection of the devices is described in the next section.

Each main monitor can receive another 5 extension monitors. From all monitors 2-way audio communication is possible after ringing action as well as opening the door.

The ABUS Link Station app can connect to the main monitor via an ABUS Link Station account. Thus, the main users of the apartments are separated (when the bell rings at apartment 1, only the connected Link Station account of apartment 1 is notified).



To ensure that the information about the triggered tamper contact on the FaceXess device appears as a pop-up message in one or more connected Link Station apps, it is also necessary to integrate the FaceXess device directly into a Link Station account. This is done by scanning the Link Station QR code of the FaceXess device. Only the primary user can receive the sabotage message.

9.2 Face Terminal and Monitor(s) Configuration

For the connection from the FaceXess device to the respective main monitor of the apartment, the IP address (LAN or WLAN) of the FaceXess device must be entered in the main monitor under Device management / Main door station.

<	Geräteverwaltung	+	i
Haupt-Türstation	192.168.0.26		i 🌐 📄 🔄

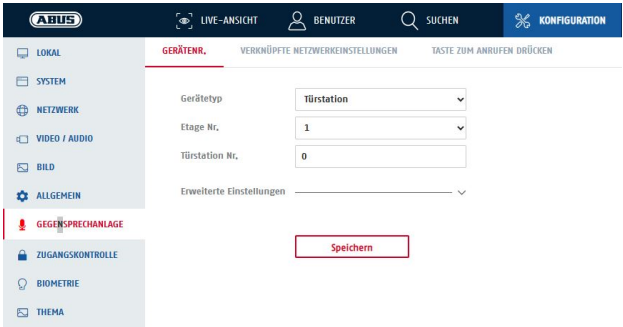
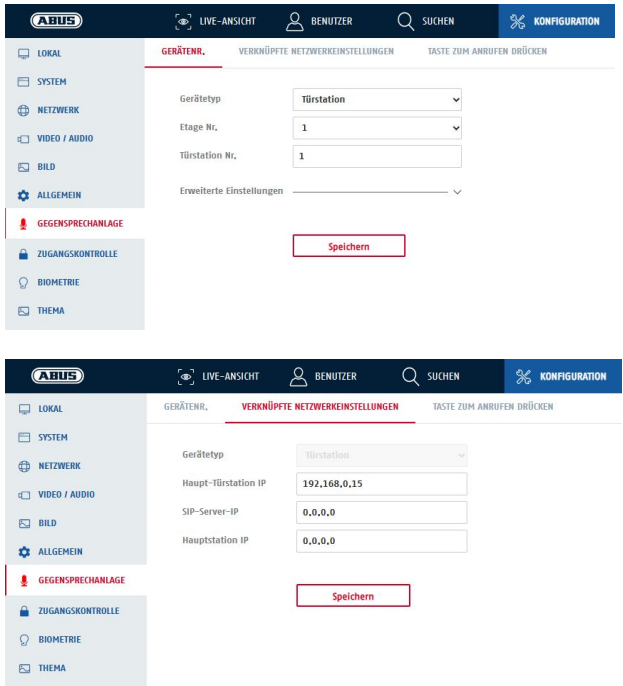
9.3 Using FaceXess as a side door

A FaceXess device can be used in combination with Moduvis monitors and other FaceXess devices for main and side doors.

Practical examples of configurations with side doors are, for example:

Main input: FaceXess device (TVHS30000)
 Side entrance: FaceXess device (TVHS30000)

Up to 99 devices can be programmed for secondary inputs.
 Programming is done via the web interface of the FaceXess device or via the ABUS CMS software.

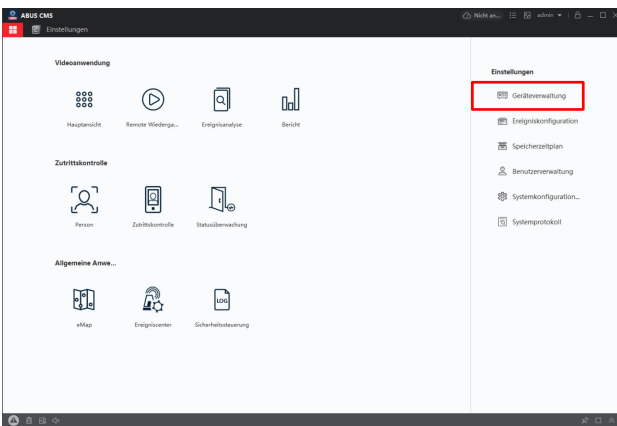
Setting on the device for the main input	Setting on the device for the 1st side door
<p>Menu item: Configuration / Intercom / Device no.</p> <p>Device type: Door station Door station no.: 0</p> 	<p>Menu item: Configuration / Intercom / Device no.</p> <p>Device type: Door station Door station no.: 1</p> <p>Menu item: Configuration / Intercom / Linked network settings</p> <p>Main door station IP: IP address of the FaceXess device at the main entrance (here e.g.: 192.168.0.15)</p> 

10. Configuration and operation via the ABUS CMS software

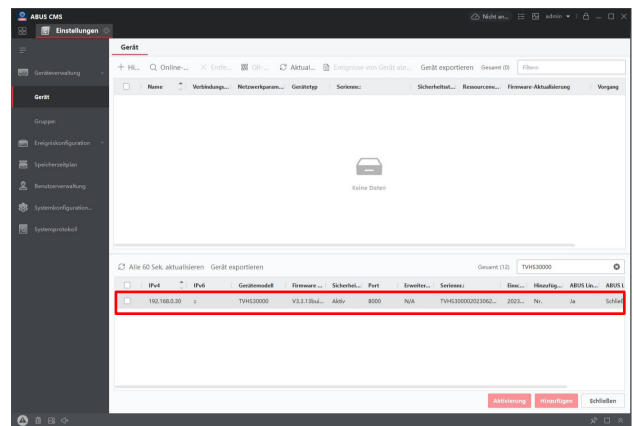
10.1 Integration in ABUS CMS software

First, the FaceXess device must be added to the device management of the ABUS CMS software. To do this, the FaceXess device must be on the same IP network as the PC with the ABUS CMS software installed, either via a network cable connection or a WiFi connection. Start the CMS software and open the "Device management" item.

Opening the device management

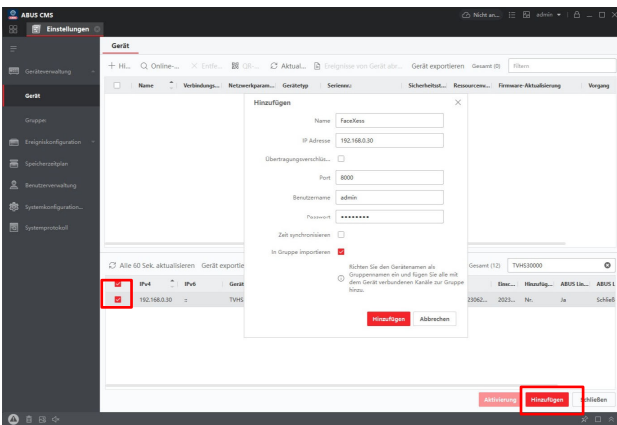


The device is found by the CMS software in the IP network.



Mark and add

Enter the necessary connection parameters: Name, IP address, port (default 8000), user name (default "admin"), password (device password).



Hinzufügen ✕

Name

IP Adresse

Übertragungsverschlüs...

Port

Benutzername

Passwort

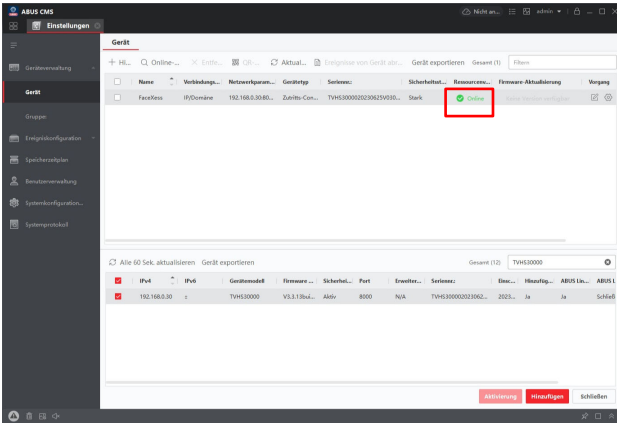
Zeit synchronisieren

In Gruppe importieren

Richten Sie den Gerätenamen als Gruppennamen ein und fügen Sie alle mit dem Gerät verbundenen Kanäle zur Gruppe hinzu.

Hinzufügen **Abbrechen**

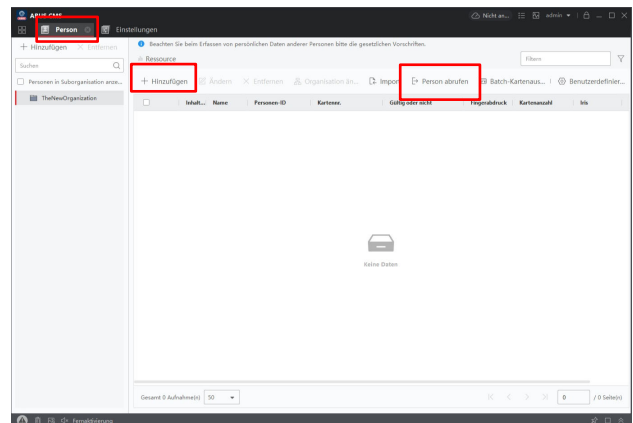
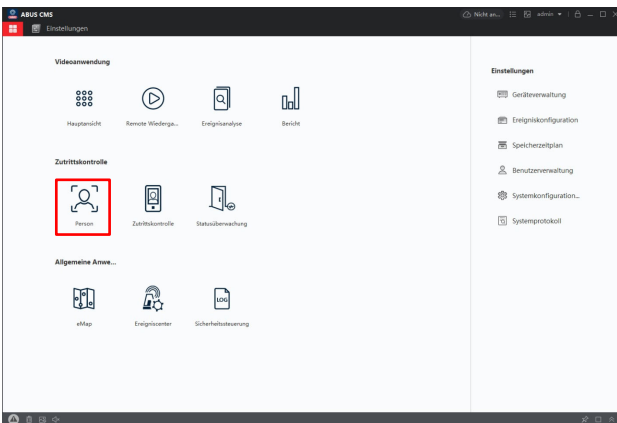
The FaceXess device has now been successfully added to the ABUS CMS (status "Online", green).



10.2 Manage people

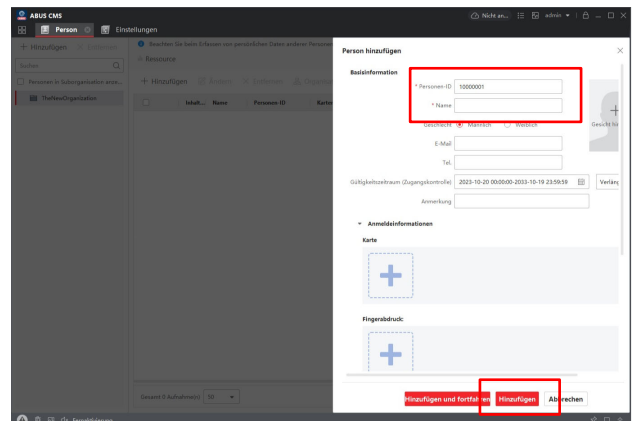
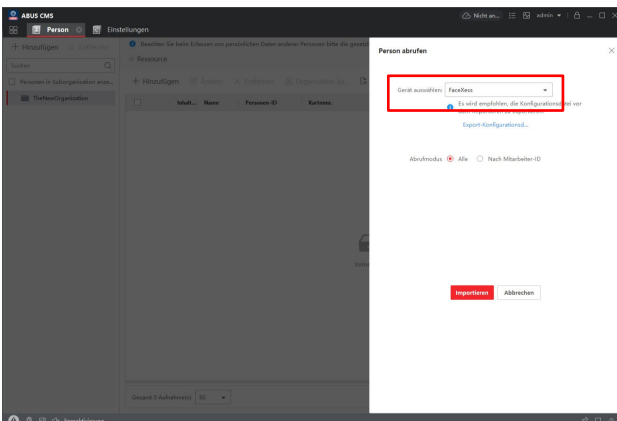
Open the menu item Access control / Person.

You can add people manually, or get the people information from a FaceXess device over the network.



When you retrieve information from a FaceXess device, you must first select one of the connected FaceXess devices. After that, the people's information will be downloaded and added to the people list.

When adding a person manually, at least the person's ID and name must be entered. Furthermore, a picture of the person can be uploaded, card numbers assigned or an individual PIN code assigned. It is also possible to mark the person as an administrator.



Click the + sign in the person preview screen.

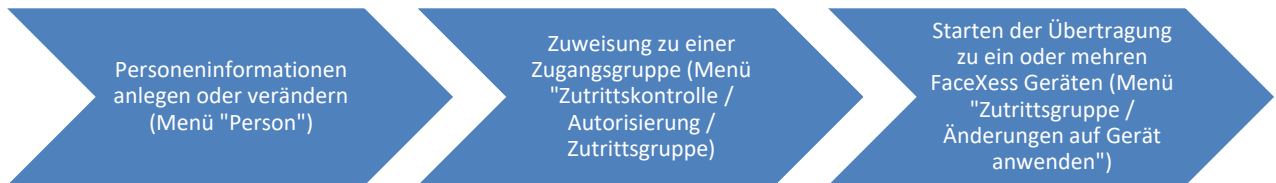
After successful addition, the person appears in the person overview.

id	Name	Personen-ID	Kategorie	Gültigkeitszeitraum	Freigegeben	Kontrolliert	IK
1	Max	1	3417773148	Nicht abgelaufen	0	1	0



The persons are now created in the ABUS CMS software. In the next step, one or more access groups must be created. Access groups can differ e.g. in the allowed period for an access.

To successfully transfer personal information to one or more FaceXess devices, the following steps are required in the ABUS CMS software.

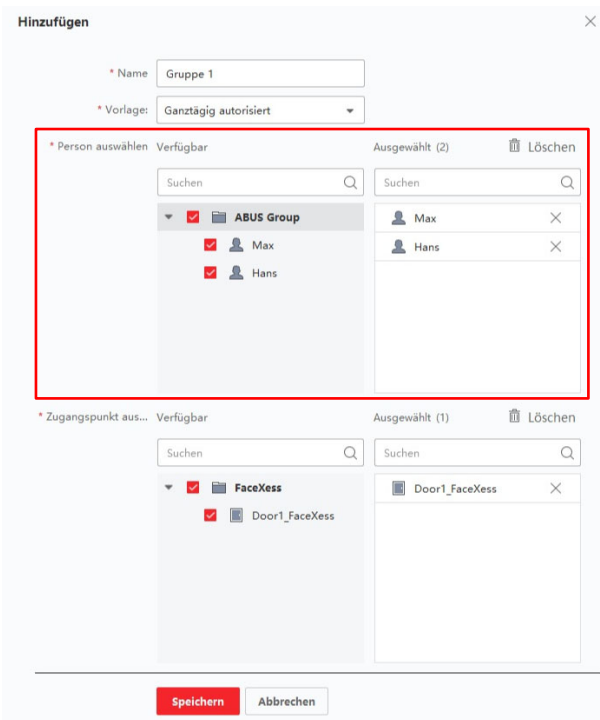


10.3 Manage and transfer access groups in FaceXess

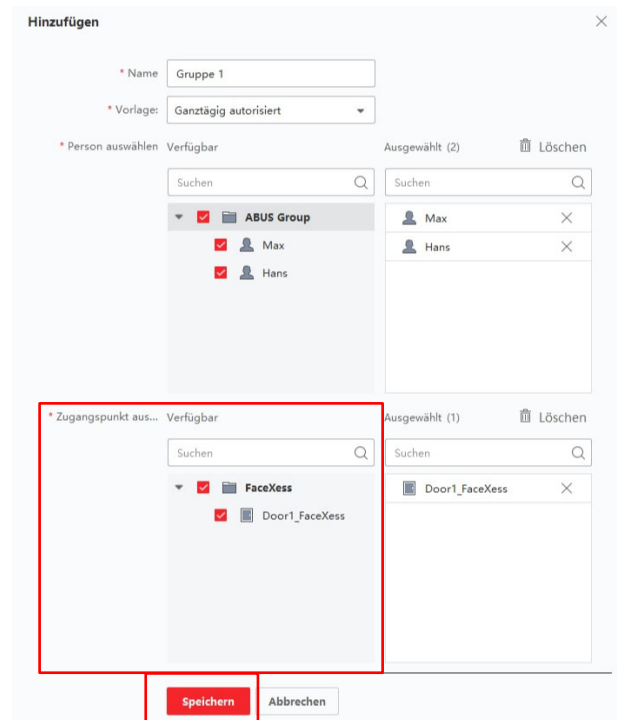
Click on the "Add" menu item in the Access control / Access group menu.

Assign a group name. In the item below, define the period during which the access group can be granted access (All day is the default, for further options see item 10.4).

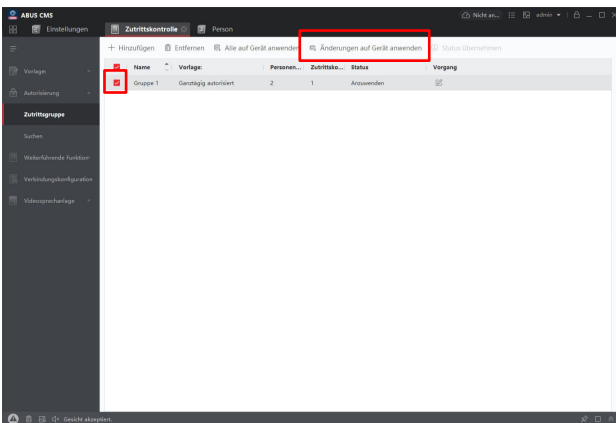
From the list of available persons, select the persons who should belong to the access group.



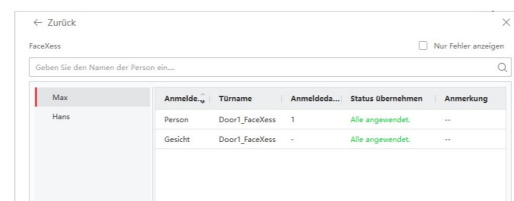
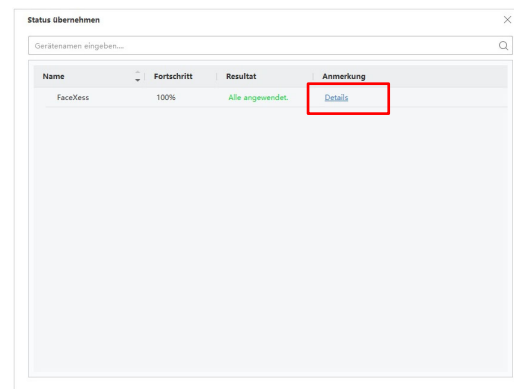
You also define the devices to which the access group is to be transferred. Multiple selection of devices is possible if the devices are located in the same IP network. Then press "Save".



The access group is now created. Now select the access group and press "Apply changes to device".



A status overview appears. If the result indicator is green, all changed parameters have been successfully transferred to the FaceXess device(s). Details of the transfer can be displayed.



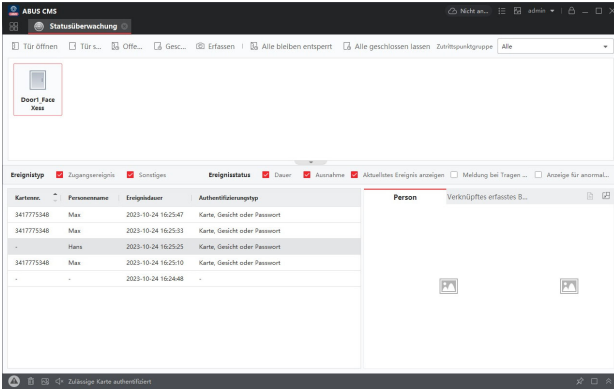
10.4 Event display and event search

Events of the FaceXess device can be displayed directly live in the ABUS CMS software or via a subsequent search.

Live display of events

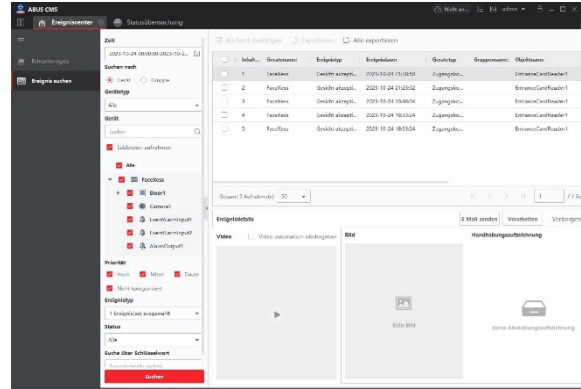
Menu: Access control / status monitoring

Functions: Live display of authentications, remote opening, remote closing of doors.



Event search

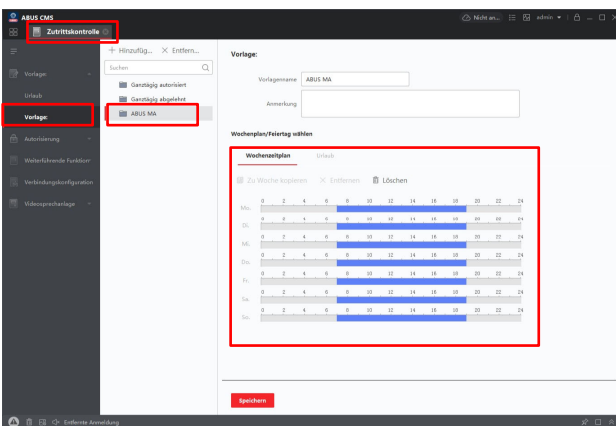
Menu: General application / Event center



10.5 Schedule controlled access

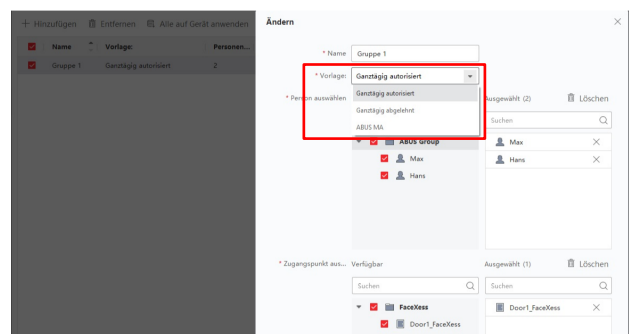
It is possible to assign different access groups with different access schedules.

Go to the "Access control / Authorization / Template" menu. Add a new schedule. Select the days and hour ranges. Save the schedule



Go to the "Access control / Authorization / Access group" menu and double-click on an access group.

You can now assign the created schedule template to the access group.



Finally, the changes to the access group must be applied to the device or devices again ("Apply changes to device" button).

11. Maintenance and cleaning


11.1 Maintenance

Regularly check the technical safety of the product, e.g. damage to the housing.

If it can be assumed that safe operation is no longer possible, the product must be taken out of service and secured against inadvertent operation.


It can be assumed that safe operation is no longer possible if

- the device has visible damage,
- the device no longer works

	<p>Please note:</p> <p>The product is maintenance-free for you. There are no components inside the product for you to check or maintain, never open it.</p>
---	--

11.2 Cleaning

Clean the product with a clean dry cloth. For heavier soiling, the cloth can be lightly moistened with lukewarm water.

	<p>Make sure that no liquids get into the device. Do not use chemical cleaners, this could attack the surface of the case and the screen (discoloration).</p>
---	---

12. Disposal



Attention: The EU Directive 2002/96/EC regulates the proper return, treatment and recycling of used electronic equipment. This symbol means that in the interest of environmental protection, the device must be disposed of at the end of its service life in accordance with the applicable legal regulations and separately from household or commercial waste. The disposal of the old device can be carried out via corresponding official collection points in your country. Follow the local regulations when disposing of the materials. For further details on take-back (also for non-EU countries), please contact your local administration. Separate collection and recycling conserves natural resources and ensures that all regulations for the protection of health and the environment are observed when recycling the product.

13. Technical data

The technical data of the individual cameras is available at www.abus.com via the product search.

14. Open Source License Notes

We would also like to point out here that the network surveillance camera contains open source software, among other things. Please read the open source license information enclosed with the product.