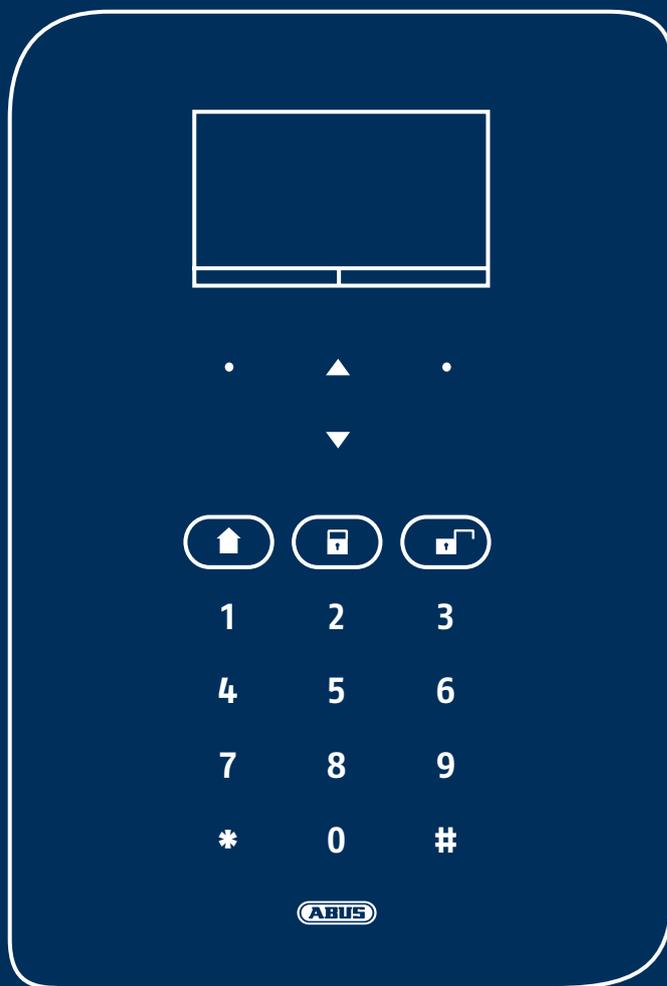
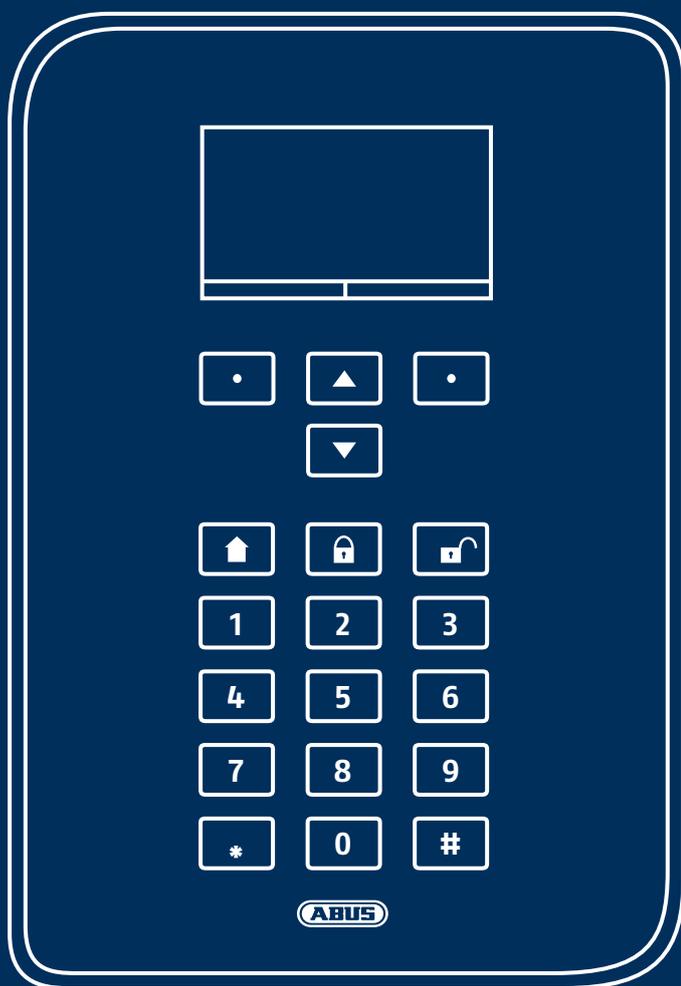


SECVEST

Instructions pour l'installation



Deutsch

Diese Bedienungsanleitung enthält wichtige Hinweise zur Inbetriebnahme und Handhabung.

Achten Sie hierauf, auch wenn Sie dieses Produkt an Dritte weitergeben.

Eine Auflistung der Inhalte finden Sie im Inhaltsverzeichnis mit Angabe der entsprechenden Seitenzahlen.

English

These user manual contains important information for installation and operation.

This should be also noted when this product is passed on to a third party.

A list of contents with the corresponding page number can be found in the index.

Français

Ce mode d'emploi appartient à de produit.

Il contient des recommandations en ce qui concerne sa mise en service et sa manutention.

Vous trouverez le récapitulatif des indications du contenu à la table des matières avec mention de la page correspondante.

Nederlands

Deze gebruiksaanwijzing hoort bij dit product.

Er staan belangrijke aanwijzingen in betreffende de ingebruikname en gebruik, ook als u dit product doorgeeft aan derden.

U vindt een opsomming van de inhoud in de inhoudsopgave met aanduiding van de paginanummers.

Dansk

Denne manual hører sammen med dette produkt.

Den indeholder vigtig information som skal bruges under opsætning og efterfølgende ved service.

Indholdet kan ses med sideanvisninger kan findes i indekset .

Italiano

Queste istruzioni contengono avvertenze importanti per la messa in funzione e l'utilizzo. La preghiamo pertanto di conservare le presenti istruzioni per eventuali consultazioni future. Le presenti istruzioni sono parte integrante del prodotto, pertanto vanno osservate anche in caso di cessione del prodotto a terzi.

Limite de la responsabilité

Nous avons apporté le plus grand soin à la rédaction du présent manuel afin d'en assurer l'exactitude. Cependant, le rédacteur et la société ABUS Security-Center GmbH & Co. KG déclinent toute responsabilité pour les éventuels sinistres et dommages résultant d'une installation et d'une utilisation non conformes, d'une utilisation non autorisée et du non-respect des consignes de sécurité et des avertissements. Nous déclinons toute responsabilité en cas de dommages consécutifs. Le produit et ses composants ne peuvent faire l'objet d'aucune modification ou transformation. Le non-respect des présentes remarques annule la garantie du produit. Tous les liens externes contenus dans le texte ne donnent lieu à aucune responsabilité de contenu de la part d'ABUS Security-Center GmbH & Co. KG, mais sont la responsabilité unique du fournisseur de services correspondant. ABUS Security-Center GmbH & Co. KG a vérifié avec soin les sites externes rattachés aux liens au moment de la publication, et d'éventuelles violations de droit n'étaient pas détectables au moment de la création des liens. Il n'existe aucune influence sur des modifications ultérieures. Toute responsabilité d'ABUS Security-Center GmbH & Co. KG est donc exclue.

Sous réserve de modifications techniques.

© ABUS Security-Center GmbH & Co. KG, 01/2020



Remarque

Version logicielle 3.01.17

Le présent manuel s'applique à la version 3.01.17 du logiciel et à toutes les versions logicielles publiées antérieurement. Toutes les nouveautés applicables uniquement à partir d'une certaine version logicielle sont marquées, par exemple $\geq 2.00.00$. Tous les éléments applicables uniquement jusqu'à une certaine version logicielle sont également marqués, par exemple $< 2.00.00$.

Déclaration de conformité

La société ABUS Security-Center déclare que l'équipement radioélectrique du type FUAA50xxx est conforme à la directive RED 2014/53/UE. Le texte complet de la déclaration de conformité UE est disponible à l'adresse Internet suivante :

www.abus.com Recherche d'articles FUAA50xxxx/Downloads

La déclaration de conformité peut également être demandée à l'adresse suivante :

ABUS Security-Center GmbH & Co. KG

Linker Kreuthweg 5

86444 Affing

ALLEMAGNE

Garantie



Remarque

- Le plus grand soin est apporté à la conception et à la fabrication des produits ABUS en conformité avec les normes en vigueur.
- La garantie couvre uniquement les vices résultant de défauts matériels ou de fabrication présents au moment de la vente. En présence d'un défaut matériel ou de fabrication avéré, la centrale est réparée ou remplacée à la discrétion du donneur de garantie.
- La garantie se termine, dans de tels cas, à expiration de la durée d'origine de la garantie de 2 ans. Toute revendication dépassant ce cadre est expressément exclue.
- ABUS décline toute responsabilité pour les vices et dommages résultant d'effets extérieurs (p. ex. avaries de transport, emploi de la force, manipulation incorrecte), d'une utilisation inappropriée, de l'usure normale ou de la non-observation des présentes instructions.
- En cas de recours à la garantie, il convient de joindre au produit concerné l'original de la preuve d'achat mentionnant la date d'achat et une brève description du défaut.
- Si vous deviez constater un défaut déjà présent à l'achat sur la centrale, nous vous prions de vous adresser directement à votre revendeur au cours des deux premières années.

Sommaire

Limite de la responsabilité	2
Déclaration de conformité	3
Garantie	3
Sommaire	4
Guide de démarrage rapide	8
À qui s'adressent ces instructions d'installation ?	8
Installation de la centrale d'alarme Secvest	8
Programmation/configuration de la Secvest	8
Test de fonctionnement de la Secvest.....	8
Consignes de sécurité	9
Signification des pictogrammes	9
Utilisation conforme	9
Généralités.....	10
Alimentation électrique.....	11
Remarques concernant la batterie	13
Raccordements.....	15
Mode sans fil.....	15
Implantation de la centrale d'alarme.....	15
Priorité d'édition	16
Emballage	16
Contenu de la livraison	16
Présentation de l'appareil	17
Vue avant.....	17
Affectation des touches internationale.....	18
Dos de l'appareil (plaque de montage).....	19
Introduction	21
Termes, définitions.....	21
Surveillance des erreurs et du sabotage de la centrale	37
Conditions de temps	37
Montage / installation	38
Aperçu des sorties, bornier.....	38
Fixation murale de la plaque de montage.....	40
Position du système d'alarme sans fil (centrale)	40
Fixation de la plaque de montage	40
Raccordement des périphériques.....	41
Montage du module de téléphonie mobile en option.....	41
Insertion de la carte micro SD	42
Mesures finales.....	42
Remplacement de la partie supérieure, surface avant tactile, surface avant à touches	42
Mise en service	43
Première mise en service/restauration de la programmation d'usine	43
Si la centrale est déjà installée	44
Connexion au système d'alarme sans fil	44
Déconnexion du système d'alarme sans fil	45
Programmation/configuration	46
Remarques	46
Éléments de commande des menus	47
Écran d'authentification.....	48

Menu principal	49
Info	51
Centrale	51
Communication.....	55
RTC.....	56
Ethernet.....	57
Mobile.....	58
Modules hybrides	60
Customisation	61
État.....	62
Composants.....	63
Programmation dans l'interface Web	63
Détecteur	67
Zones IP.....	67
Zones sans fil.....	80
Zones filaires.....	82
Zones MoHy.....	83
Clavier de commande sans fil	86
Ajouter un élément de commande sans fil.....	86
Sirènes extérieures.....	88
Sirènes sans fil.....	88
Sirènes filaires	89
Générateur de signal intérieur	90
Module d'info/sirène d'intérieur	93
WAM (module universel)	95
Verrous de porte.....	97
Répéteur RF	99
Modules hybrides	103
Sorties.....	107
Sorties sans fil	108
Configuration des sorties radio	108
Sorties filaires	117
Configuration des sorties filaires.....	117
Sorties MoHy	118
Configuration des sorties MoHy.....	119
Sorties mixtes	121
Partitions	124
Configuration de partitions.....	125
Tous act.....	125
Configuration de partitions	134
Act. interne	134
Configuration de partitions	144
Désactivée.....	144
Configuration de partitions	148
Réaction agression.....	148
Système	150
Généralités	151
Installateur détails.....	161
Accès utilisateur	163
RAZ Util.	167
Confirmation	168
Hardware	171
Réglages de sécurité.....	174
Mise à niveau de la centrale.....	191
Contrôler la mise à niveau ?.....	194
Sauvegarder/Restaurer	195

Sommaire

Rapport	198
Communication	201
Réseau.....	201
Configuration de réseau.....	202
Configuration Mobile IP.....	205
Paramétrage E-mail.....	211
Setup Transmission VoIP.....	213
TS Reporting.....	215
TS Reporting, répertoire tél.....	218
TS Reporting, ID client.....	220
TS Reporting, canaux FF (uniquement avec le protocole "Format rap.").....	221
TS Reporting, événements CID/SIA (avec tous les protocoles SAUF "Format rap.").....	222
Cryptage.....	224
TS Reporting, plus.....	230
Appel d'urgence de soin.....	234
Appel soins de santé, répertoire tél.....	236
Appel soins de santé, ID client.....	237
Transmetteur vocal.....	238
Transmetteur vocal, événement.....	242
Transmetteur vocal, destinations.....	243
Transmetteur vocal, appel de test.....	244
SMS.....	246
SMS, événement.....	248
SMS, destinations.....	250
SMS, destinations, message X.....	252
SMS, destinations, transférer.....	253
SMS, destinations, message, téléphone destinataires.....	254
SMS, messages.....	255
SMS, SMS RTC.....	256
SMS, appel de test.....	258
E-mail.....	260
E-mail, événement.....	262
E-mail, destinations.....	264
E-mail, messages.....	265
E-mail, appel de test.....	266
options de communication.....	268
Contacts.....	273
Appel d'urgence de soin.....	280
Test.....	281
Historique.....	302
Clavier virtuel.....	305
Annexe.....	306
Caractéristiques techniques.....	306
Équipement compatible.....	322
Valeurs par défaut/Réglages d'usine matériel.....	330
Valeurs par défaut/Réglages d'usine logiciel.....	331
Mode installateur.....	331
Menu utilisateur.....	349
Assistant de démarrage.....	354
Signaux sonores, acoustiques.....	355
Maintenance et entretien.....	357
Maintenance et entretien par l'installateur.....	357
Maintenance et entretien par l'utilisateur.....	357
Mise à niveau logicielle.....	358
Set de fichiers logiciels pour V3.01.17.....	360
Mise à niveau logicielle avec nouveaux fichiers depuis la carte SD.....	362

Mise à niveau logicielle avec nouveaux fichiers sur le PC	363
Mise à niveau logicielle avec nouveaux fichiers depuis le serveur FTP	371
Mise à niveau logicielle avec Secvest Update Utility	373
AES / TS Reporting	374
Formats de protocole AES/TS Reporting	374
Événements CID / SIA.....	378
Messages d'erreur par e-mail	390
Messages d'erreur par TCP/IP	391
Vue d'ensemble des messages SSL	391
Messages d'erreur par VOIP	393
Messages d'erreur GSM CME/CMS.....	394
Codes d'erreur CME.....	394
Codes d'erreur CMS.....	396
Historique.....	398
Entrées de journal de bord	398
Numéros utilisateur.....	411
Dépannage et recherche d'erreurs	413
Redémarrage manuel (extinction et rallumage)	413
Effectuer un appel test GSM/mobile manuellement, carte prépayée.....	417
LED de diagnostic sur la platine principale et le module GSM/de téléphonie mobile	418
Trace, enregistrement des processus de communication.....	420
Routeur, IAD, pare-feu	423
Fuseaux horaires	424
Centre de notification du réseau fixe	425
Centre de notification du réseau GSM	426
Notification par SMS.....	426
Notification par e-mail / setup e-mail	427
Configuration Mobile IP/Communication données mobiles.....	430
Service après-vente et support.....	431
Mise hors service de la centrale	432
Protection des données.....	432
Élimination	433
Index.....	434

Guide de démarrage rapide

À qui s'adressent ces instructions d'installation ?

Ces instructions d'installation vous aideront à parcourir les différents menus de l'interface de programmation.

Elles s'adressent au technicien formé ayant acquis, lors d'un séminaire organisé par la société ABUS Security-Center GmbH & Co. KG, les connaissances suivantes :

- Installation du système d'alarme sans fil
- Installation des périphériques de la centrale d'alarme sans fil (par ex. détecteurs, émetteurs d'alarme, module GSM/GPRS, caméras de surveillance)
- Configuration des périphériques du système d'alarme sans fil

Ces instructions d'installation énumèrent les possibilités de configuration accessibles dans les différents menus.

Installation de la centrale d'alarme Secvest

L'installation du système d'alarme sans fil Secvest est décrite dans le chapitre Montage/Installation.

Des informations supplémentaires figurent dans le document "Quick Guide FUAA50000" également fourni.

Le manuel d'installation/de l'utilisateur peut également être téléchargé au format PDF.

Lien de téléchargement du document :

www.abus.com/ger/products/FUAA50000

Programmation/configuration de la Secvest

La programmation/configuration du système d'alarme sans fil y est décrite.

Test de fonctionnement de la Secvest

Une fois l'installation et la programmation terminées, effectuez un test de fonctionnement complet de tous les systèmes et périphériques.

Informez l'utilisateur sur les commandes principales suivantes :

- Connexion/déconnexion
- Activation/désactivation
- Utilisation de la Secvest, télécommande
- Création d'un protocole de transmission



Remarque

Tenez compte des remarques générales d'utilisation.

Dans tous les cas, veuillez remettre à l'utilisateur le manuel d'utilisation et le guide de démarrage rapide, et, le cas échéant, les présentes instructions d'installation.

Consignes de sécurité

Signification des pictogrammes

Les symboles suivants sont utilisés dans la documentation ainsi que sur l'appareil :

Symbole	Mot-signal	Signification
	Danger	Avertissement relatif aux risques de blessure ou dangers pour votre santé.
	Danger	Avertissement de risques de blessures ou de risques pour votre santé du fait du courant électrique.
	Important	Avertissement de sécurité relatif au risque d'endommager l'appareil/les accessoires.
	Remarque	Informations importantes.
		La directive européenne WEEE 2012/19/UE régit le traitement et l'exploitation des appareils électroniques usagés. Ce symbole signifie que, dans un souci de protection de l'environnement, l'appareil en fin de vie ne doit pas être éliminé avec les ordures ménagères ou industrielles, mais recyclé conformément aux dispositions légales en vigueur. Le recyclage de votre appareil usagé peut être assuré par les organismes officiels de collecte présents dans votre pays. Respectez les prescriptions locales pour l'élimination des matériaux. Vous obtiendrez de plus amples détails concernant la collecte (y compris pour les pays ne faisant pas partie de l'Union européenne) auprès des administrations locales. Le tri et le recyclage permettent de préserver les ressources naturelles et d'assurer un recyclage du produit dans le respect des règles de protection de la santé et de l'environnement.

1. ... Opération obligatoire ou conseillée, à effectuer dans l'ordre indiqué dans le texte
2. ...

- ... Énumération sans ordre particulier dans le texte ou dans l'avertissement
- ...

Utilisation conforme

Utilisez l'appareil exclusivement aux fins pour lesquelles il a été construit et conçu ! Toute autre utilisation est considérée comme non conforme !

Cet appareil est conçu exclusivement pour les applications suivantes :

- système de détection de danger, centrale d'alarme.

Ce produit est conforme aux exigences des directives européennes et nationales en vigueur.

La conformité de ce produit a été prouvée. Les déclarations et documents correspondants sont consultables auprès du fabricant.

Lorsque vous utilisez ce produit, respectez les consignes du manuel afin de ne pas altérer la conformité du produit et sa sécurité de fonctionnement. Pour toute question, adressez-vous à votre revendeur spécialisé. Des remarques générales plus détaillées et des remarques concernant l'assistance produit figurent sur www.abus.com sur la page générale ou sur le portail des partenaires pour les revendeurs et les installateurs.

 **Danger**
 Avant de commencer les travaux d'installation et de maintenance, définissez la centrale d'alarme en mode Installateur. Le mode Installateur évite que les alarmes ne s'activent lorsque le couvercle de la centrale ou d'autres composants est ouvert.

Les indications suivantes sont utilisées dans le texte :

Signification

Généralités

Avant la première utilisation du matériel, lisez attentivement les indications, et plus particulièrement les avertissements, même si vous êtes autorisé à utiliser des appareils électroniques.



Danger

Le non-respect des présentes instructions entraîne l'annulation de la garantie.

Nous déclinons toute responsabilité pour les dommages consécutifs !



Danger

Nous déclinons toute responsabilité pour les éventuels préjudices corporels ou matériels résultants du non-respect des consignes de sécurité.

Dans de tels cas, la garantie devient caduque !

Conservez ces instructions en lieu sûr pour pouvoir vous y référer ultérieurement.

Si vous revendez ou donnez l'appareil, remettez également le présent manuel.

Cet appareil a été fabriqué dans le respect des normes de sécurité internationales.



Remarque

Version logicielle $\geq 1.01.02$

Lors de la première configuration de la centrale, **aucun code d'installateur par défaut** et **aucun code d'administrateur par défaut** n'est défini. Ils doivent être attribués individuellement avec l'assistant de configuration.

Après la première mise en service, modifiez le **nom d'installateur (code=nom)** et le **nom d'administrateur (code=nom)** attribués **automatiquement** en choisissant des noms d'utilisateur sûrs. Respectez l'utilisation des données d'accès lorsque vous ajoutez des utilisateurs.

Utilisation des données d'accès pour se connecter aux systèmes de sécurité

Principes :

- Les noms d'utilisateur et les codes pour se connecter aux systèmes de sécurité ne doivent être connus que des utilisateurs légitimes et ne doivent en aucun cas être transmis à des personnes non autorisées.
- Si le nom d'utilisateur et le code doivent être transmis par écrit, ne jamais les donner dans un unique mail.
- Il est nécessaire de modifier régulièrement les noms d'utilisateur et les codes.

Standards

- Un nom d'utilisateur doit comprendre au moins 8 caractères.
- Il est idéalement composé de caractères issus d'au moins trois des catégories suivantes : majuscules, minuscules, caractères spéciaux et chiffres.
- Les noms d'utilisateur ne doivent surtout pas être votre nom personnel, le nom de membres de votre famille, de votre animal de compagnie, de votre meilleur ami, de votre vedette préférée, de votre loisir ou des dates de naissance.
- Évitez les noms d'utilisateur et les codes que vous utilisez sur d'autres sites ou qui peuvent être devinés facilement par d'autres personnes.
- Le nom d'utilisateur ne doit pas figurer dans des dictionnaires, ni être une désignation de produit.
- Il ne doit pas être composé de variantes courantes, de schémas de répétitions ou de schémas de caractères, tels qu'asdfgh ou 1234abcd, etc.
- Évitez d'ajouter des chiffres uniquement à la fin du nom d'utilisateur ou l'un des caractères spéciaux usuels ! ? Ajoutez # au début ou à la fin d'un nom d'utilisateur simple pour le compléter.
- Les noms d'utilisateur et les codes doivent être modifiés après 180 jours au plus tard.
- Les nouveaux noms d'utilisateur et les codes ne doivent pas être identiques aux trois derniers utilisés.
- Les nouveaux noms d'utilisateur et les codes doivent avoir au moins deux caractères différents du nom d'utilisateur et du code précédents.
- N'utilisez pas de macros et de scripts pour la saisie des noms d'utilisateur et des codes.



Généralités concernant les centrales d'alarme

Une installation incorrecte ou bâclée peut entraîner une mauvaise interprétation des signaux et déclencher des fausses alertes.

Les coûts d'intervention des secours, par exemple, des pompiers ou de la police, sont à la charge de l'exploitant.

Lisez donc attentivement cette notice et tenez compte, lors de l'installation de la centrale, de la désignation exacte des câbles et des composants utilisés.

Alimentation électrique

- Pour éviter tout risque d'incendie ou d'électrocution, installez la centrale d'alarme et ses périphériques à l'abri de la pluie et au sec.
- Ce matériel ne doit pas être installé à proximité d'une baignoire, d'une piscine ou de projections d'eau.
- La modification du matériel est interdite.
- Le matériel et les accessoires endommagés ne doivent plus être utilisés.
- Toute utilisation différente de celle décrite précédemment peut endommager ce produit. En outre, cela peut présenter des risques comme par ex. court-circuit, incendie, électrocution, etc.



Remarque

Le raccordement au réseau électrique public est soumis à la réglementation nationale en vigueur. Renseignez-vous préalablement.

- De la condensation peut se former à l'intérieur du matériel en cas d'élévation brutale de la température, par exemple s'il est transporté de l'extérieur à l'intérieur. Dans ce cas, attendez quelques heures avant la mise en service.
- Déconnectez l'appareil du réseau électrique avant toute intervention de maintenance ou d'installation.



Danger

La modification du matériel entraîne l'annulation de la garantie.



Danger

La centrale est alimentée par un bloc d'alimentation intégré.

Celui-ci est raccordé au réseau électrique 230 VCA du bâtiment par une ligne séparée.

Le raccordement au réseau électrique du bâtiment doit être effectué dans le respect de la réglementation nationale.

L'alimentation électrique de secours est assurée par une batterie interne.

Si vous devez remplacer un fusible, utilisez exactement le même modèle. Vous ne devez en aucun cas en utiliser un de capacité supérieure.



Remarque

Filtre antiparasite

Nous recommandons l'installation d'un ferrite sur l'alimentation secteur 230 V.

Par ex. ferrite Würth 742 711 32S ou 742 715 3.

Cela évite un dysfonctionnement éventuel de la centrale, lorsque des perturbations électromagnétiques encore autorisées par la directive CEM mais très fortes surviennent.



Danger

Fixez l'appareil dans un endroit sec à l'intérieur.

La centrale d'alarme doit être suffisamment ventilée.

La température ambiante ne doit pas tomber en dessous de 0 °C ou dépasser 50 °C.

Cette centrale d'alarme a été conçue exclusivement pour une utilisation à l'intérieur.

Le taux d'humidité maximum ne doit pas dépasser 90 % (sans condensation).

Aucun corps étranger métallique ne doit être introduit dans la centrale d'alarme.

Toute intervention sur la centrale d'alarme doit être effectuée lorsque celle-ci est hors tension.

Remarques concernant la batterie

!!! Veuillez lire très attentivement les informations suivantes !!!

Respectez à la lettre ce qui suit ! ABUS Security-Center GmbH & Co. KG décline toute responsabilité pour les accidents survenus en raison d'une manipulation non conforme à ces mesures de précaution.

Avant l'utilisation de la batterie, veuillez lire attentivement le manuel d'utilisation et les consignes de sécurité relatives à la manipulation.

Une mauvaise utilisation de cellules lithium-ions rechargeables peut entraîner des fuites, de la chaleur, de la fumée, une explosion ou un incendie, et réduire la capacité.



Danger



Danger



Important

Il est strictement interdit de :

- Chauffer la batterie ou de la jeter au feu.
- Jeter la batterie dans des liquides, tels que eau, essence ou boissons et la mouiller.
- Laisser tomber la batterie.
- Utiliser la batterie à proximité d'un feu ou dans une voiture dans laquelle la température peut être supérieure à 60 °C. Ne chargez ni ne déchargez la batterie dans de telles conditions.
- Mettre les batteries dans des poches de vêtements ou des sacs avec des objets métalliques tels que des colliers, des épingles à cheveux, des pièces ou des vis.

Ne stockez ni ne transportez les batteries avec de tels objets.

- Court-circuiter les raccordements (+) et (-) avec d'autres métaux.
- Percer ou piquer les batteries avec un objet tranchant tel qu'une aiguille.
- Démonter ou modifier la batterie.
- Souder ou braser directement sur la batterie.
- Placer la batterie dans un four à micro-ondes, un séchoir ou un réservoir haute pression.
- Utiliser les batteries avec des piles sèches ou d'autres piles primaires.
- Utiliser ensemble des nouvelles et anciennes batteries, des batteries de différents lots, des batteries d'un autre type ou d'une autre marque.
- Charger avec la polarité inversée.

Conservez les batteries hors de portée des enfants, afin qu'elles ne puissent pas être avalées par inadvertance. Si de jeunes enfants utilisent la batterie, l'adulte responsable de leur sécurité doit leur expliquer l'utilisation correcte.

Chargez la batterie uniquement à l'aide d'un chargeur spécifique, et conformément aux spécifications du produit. Chargez la batterie uniquement avec la méthode CC/CV.

Arrêtez le chargement de la batterie si le procédé de chargement n'est pas terminé au sein de la durée indiquée.

Arrêtez l'utilisation de la cellule en cas de chaleur, odeur, décoloration, déformation anormales ou d'un autre état anormal lors de l'utilisation, du chargement ou du stockage.

Ne placez pas la batterie dans un appareil avec (+) et (-) inversés.

En cas de raccordement inversé de la batterie, celle-ci n'est pas chargée. En outre, cela réduit les propriétés de chargement et de déchargement ainsi que les caractéristiques de sécurité. Cela entraîne un réchauffement du produit et une fuite.

N'utilisez pas de batterie présentant des bosses ou des déformations importantes.

Maintenez directement la batterie à l'écart du feu en cas de fuite ou d'odeur désagréable.

Si du liquide s'écoule sur votre peau ou vos vêtements, lavez-les directement à l'eau claire.

Si du liquide s'écoulant de la batterie touche vos yeux, ne vous frottez pas les yeux. Nettoyez-les soigneusement avec de l'huile alimentaire propre et consultez immédiatement un médecin.

Les batteries ont des cycles de vie. Lorsque la durée pendant laquelle la batterie fait fonctionner des appareils est bien plus courte qu'habituellement, alors la durée de vie de la batterie est écoulée. Remplacez la batterie par une autre batterie du même type.

Si la batterie ne doit pas être utilisée pendant une longue période, retirez-la de l'appareil et conservez-la dans un endroit présentant une humidité de l'air faible et une température modérée.

Consignes de sécurité

Lorsque la batterie est en cours de chargement, d'utilisation ou de stockage, maintenez-la à l'écart d'objets ou de matériaux présentant une charge statique.

Lorsque les bornes de la batterie sont sales, nettoyez-les avec un chiffon sec avant d'utiliser la batterie.

Stockez les cellules conformément aux spécifications concernant la plage de température de stockage. Une fois la batterie entièrement déchargée, nous recommandons de la charger de 7,4 à 8,0 V sans l'utiliser pendant une longue période.

Ne dépassez pas les plages de température suivantes :

	de	à
Plage de température de chargement	0 °C	45 °C
Plage de température de déchargement	-20 °C	60 °C
Stockage inférieur à 1 mois	-20 °C	60 °C
Stockage inférieur à 3 mois	-20 °C	45 °C
Stockage inférieur à 1 an	-20 °C	25 °C

En cas de stockage prolongé, maintenez la batterie à un état de charge de 50 %.

Nous recommandons de recharger la batterie jusqu'à 50 % de sa capacité totale tous les 3 mois après son obtention, et de maintenir la tension entre 7,4 et 8,0 V. Conservez la batterie dans un endroit frais et sec.

Raccordements



Remarque

Cet appareil fonctionne à très basses tensions de sécurité (Safety Extra Low Voltage, SELV). Les circuits électriques des zones, les circuits électriques des sorties commutables et l'alimentation électrique 12 V des centrales d'alarme ABUS utilisent également la même plage de tension.

SELV est une tension électrique faible, qui en raison de sa faiblesse et de l'isolation, fournit une protection particulière contre un choc électrique, par rapport aux circuits électriques à tension plus élevée.

Le module RTC contient un mélange de raccordements apparentés à des systèmes d'alarme et des connexions de télécommunication. Les raccordements typiques de systèmes d'alarme sont conçus pour des basses tensions de sécurité (Safety Extra Low Voltage, SELV). Les connexions de télécommunication sont conçues pour des tensions du réseau de télécommunications (Telecommunications Network Voltage, TNV).



Important

Il est extrêmement important que les deux types de raccordements soient séparés dans leurs branchements. Utilisez un câble séparé pour chacun. Branchez les raccordements correspondants uniquement à des raccordements externes adaptés (par ex. raccordements de systèmes d'alarme) ou à des raccordements téléphoniques adaptés. Seul un électricien professionnel est habilité à raccorder les circuits électriques TNV, en conformité avec les directives locales.



Remarque

La centrale doit être installée en lieu sûr, hors de la vue des éventuels cambrioleurs, tout en étant facilement accessible pour l'opérateur.

La centrale d'alarme doit être installée sur une surface plane, afin que la protection anti-sabotage au dos soit inaccessible lorsque la centrale est montée.

La centrale doit être installée à hauteur d'homme.

Mode sans fil



Remarque

Aucune licence radio n'est exigée pour l'utilisation de la Secvest et de ses périphériques.

L'émission et la réception peuvent être perturbées par d'autres signaux (téléphones DECT, etc.).

La conformité R&TTE ou le respect de la directive RED 2014/53/UE des appareils à commande sans fil de cette centrale a été testé par un laboratoire indépendant.

Implantation de la centrale d'alarme

Contenu de la livraison



Remarque

La centrale doit être installée hors de portée des enfants en bas âge.



Remarque

Positionnez la centrale d'alarme de manière à ce que les signaux sonores restent audibles à distance.

La centrale doit être positionnée dans une zone surveillée de sorte que les personnes non autorisées soient obligées de passer par une zone sous surveillance lorsque la centrale est activée.

La centrale d'alarme doit être installée à proximité d'une prise de courant ou d'une alimentation électrique.

Si le transmetteur vocal est utilisé, la centrale d'alarme doit être raccordée à une prise téléphonique.

La centrale d'alarme doit être installée à plus de 1 mètre de tout objet métallique (miroirs, radiateurs, etc.).

- Matériel d'installation

Priorité d'édition



Remarque

Lorsque plusieurs détecteurs sont activés simultanément, la centrale traite toujours les zones de type Agression (détecteur anti-agression) et Alarme immédiate (détecteur anti-effraction) en premier, puis les zones de type Feu (détecteur autonome avertisseur de fumée) et enfin les autres types de zones (types d'alarmes).

La centrale traite toujours les alarmes avant les avertissements (signaux).

Emballage



Danger

Ne laissez pas les emballages ni les petites pièces à portée des enfants – risque d'asphyxie !

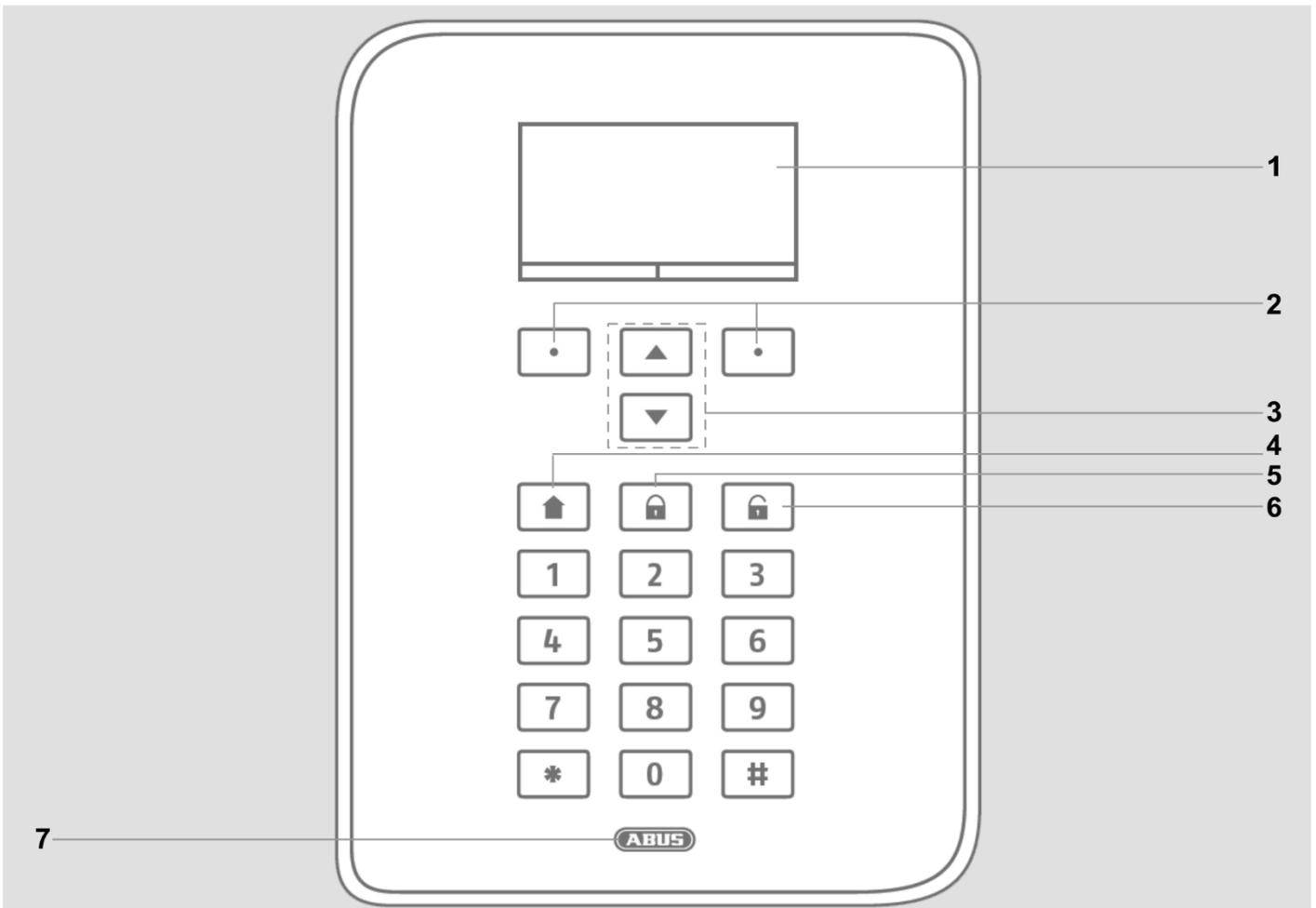
Retirez tout le matériel d'emballage avant d'utiliser l'appareil.

Contenu de la livraison

- 1x centrale d'alarme sans fil Secvest
- 1x batterie
- Guide de démarrage rapide et consignes de sécurité

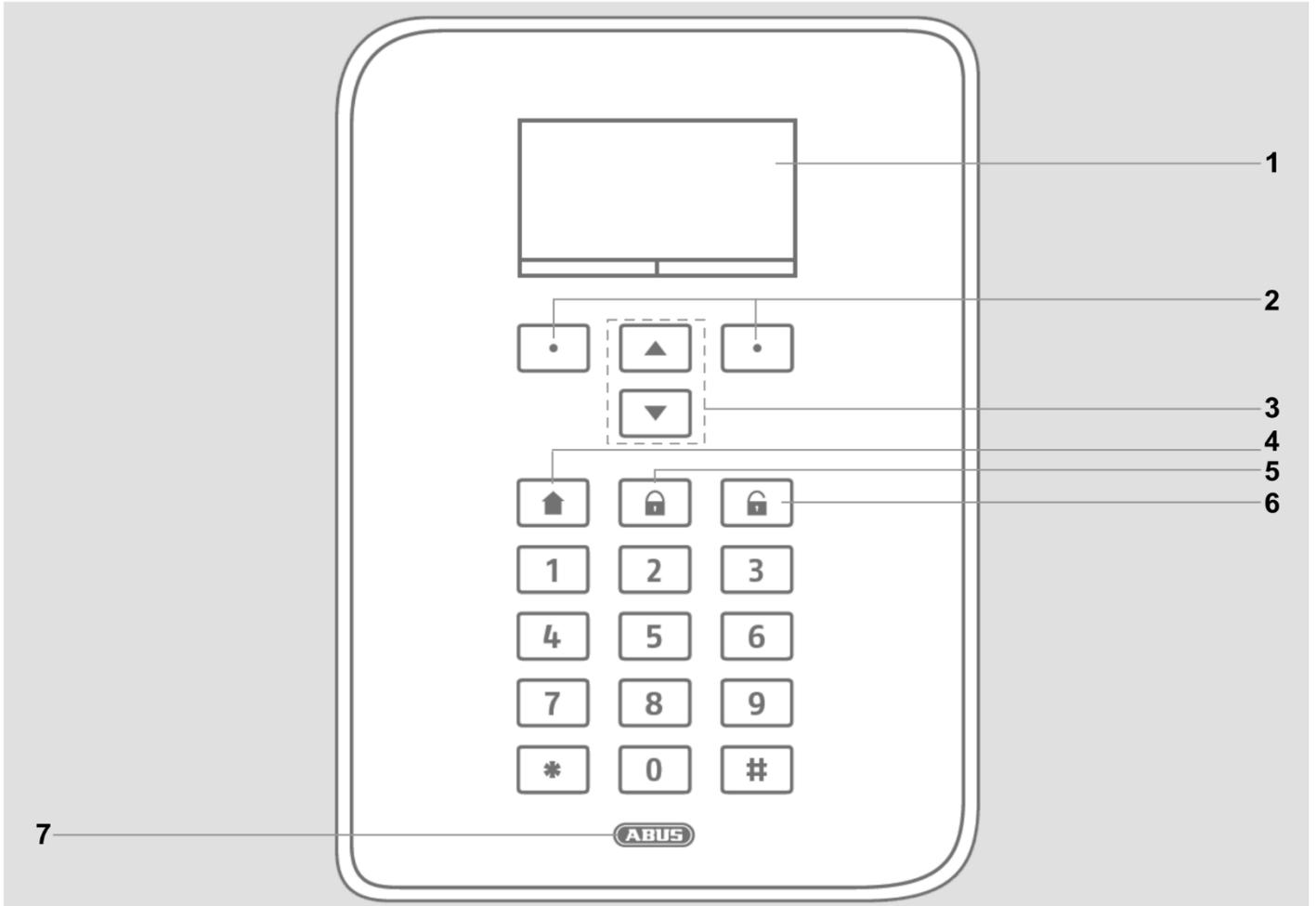
Présentation de l'appareil

Vue avant

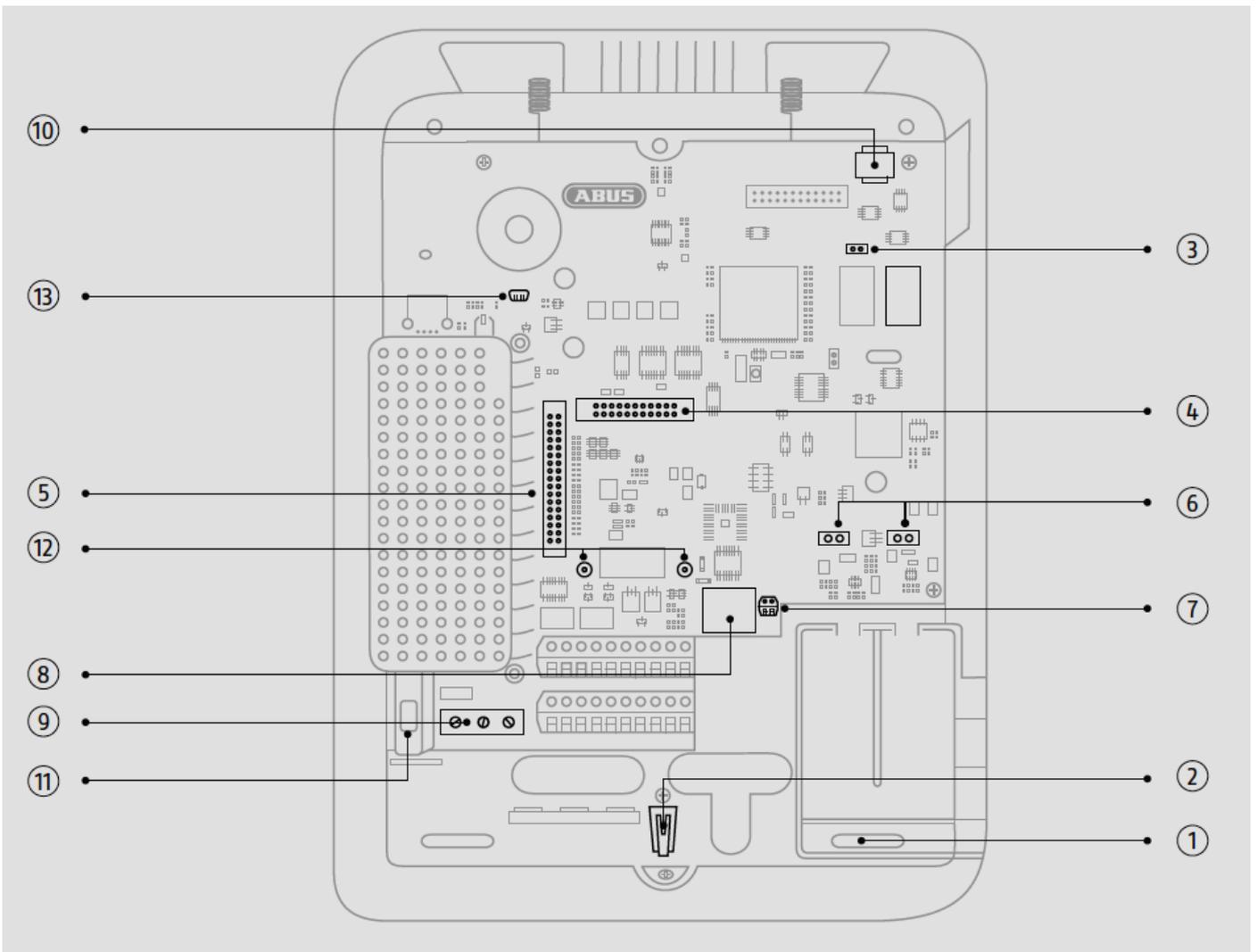


N°	Désignation/fonction	N°	Désignation/fonction
1	Affichage d'état Affichage de l'état ou des menus	5	Touche d'activation La surveillance de toutes les zones disponibles est activée.
2	Touches de confirmation Permettent de naviguer dans un niveau de menu supérieur/inférieur, de sélectionner des options ou de quitter un menu	6	Touche de désactivation La surveillance est désactivée.
3	Touches de navigation Navigation vers le haut/bas	7	Lecteur de clé Proximity Zone de lecture du badge de proximité. Maintenez le badge devant le logo ABUS.
4	Touche d'activation interne La surveillance de l'enveloppe extérieure est activée (activation interne).		

Affectation des touches internationale



Dos de l'appareil (plaque de montage)



N°	Désignation/fonction	N°	Désignation/fonction
1	Orifice de fixation pour vis	8	Sortie pour câble LAN
2	Interrupteur anti-sabotage du boîtier	9	Sortie secteur 110 V/230 VCA 50/60 Hz
3	Broches de réinitialisation de code (goupilles), voir remarque ci-dessous	10	Support de carte micro-SD
4	Raccordement pour module de téléphonie mobile en option	11	Porte-fusible de secteur
5	Raccordement du câble plat	12	Trous pour support en plastique pour module de téléphonie mobile en option
6	Raccordements pour accus	13	USB Mini-B
7	Raccordement téléphonique analogique		

**Remarque****Broches de réinitialisation de code**

Si les codes de l'utilisateur 1 et/ou de l'installateur ne sont plus connus, tous les réglages utilisateur peuvent être supprimés.

Présentation de l'appareil

Tous les utilisateurs, toutes les balises Proximity, toutes les télécommandes et tous les émetteurs d'appel d'urgence sont supprimés. Après la réinitialisation, vous êtes invité à attribuer un nouveau code installateur et un nouveau code administrateur.

1. Si possible, passez en mode Installateur.

Remarque :

Si vous ne pouvez pas accéder au mode Installateur, la centrale d'alarme lance une alarme anti-sabotage lors de l'ouverture du boîtier.

2. Ouvrez le boîtier. Débranchez l'ensemble de l'alimentation électrique (tension secteur et batteries).

Remarque :

Cette procédure ne fonctionne pas si l'interrupteur anti-sabotage du couvercle est fermé.

3. Identifiez les broches de réinitialisation de code (goupilles) sur la platine principale (voir figure ci-dessus).

4. Court-circuitez les deux broches de réinitialisation de code (goupilles). Utilisez pour cela un tournevis ou un cavalier. Laissez le court-circuit jusqu'à l'étape 6.

5. Rétablissez l'alimentation électrique. Le système démarre après une courte pause. La centrale d'alarme supprime désormais toutes les informations utilisateur et commence ensuite l'attribution de vos nouveaux codes installateurs et administrateur (comme avec l'assistant de démarrage).

6. Retirez le court-circuit des broches de réinitialisation de code (goupilles).

7. Rebranchez la batterie.

8. Fermez le couvercle de la centrale d'alarme ainsi que l'interrupteur anti-sabotage.

Introduction**Termes, définitions****2G**

Norme de téléphonie mobile de deuxième génération, voir GSM

3G

Norme de téléphonie mobile de troisième génération, voir UMTS

4G

Norme de téléphonie mobile de quatrième génération, voir LTE

CRA

Centre de réception des alarmes, consultez les normes EN 50518-1/2/3, EN 50136, VdS 2471 et STS pour plus de détails.

Protection anti-effraction active

Même une simple tentative d'effraction est détectée. Cette fonction est assurée par des périphériques intégrant non seulement les technologies sans fil les plus récentes et une protection anti-effraction mécanique (détecteurs mécatroniques) très efficace, mais qui surveillent en même temps l'ouverture d'une porte ou d'une fenêtre au moyen de détecteurs de champ magnétique innovants.

Activation, désactivation

Lorsqu'elle est activée, la centrale d'alarme donne l'alerte dès qu'un détecteur d'intrusion est actionné (par exemple, ouverture d'une porte). Lorsqu'elle est désactivée, la centrale d'alarme ne donne pas l'alerte quand un détecteur d'intrusion est actionné ; les détecteurs de danger sont programmés différemment : par exemple, si de la fumée est détectée, l'alerte doit être donnée même si la centrale est désactivée.

Système d'alarme

Terme courant désignant les systèmes d'alarme anti-effraction ou de détection de danger.

Type d'alarme

Le système d'alarme peut déclencher les types d'alarme suivants : alarme interne, alarme locale, alarme externe, alarme silencieuse.

Sirène

Appareil qui donne l'alerte par un signal acoustique (sirène) ou optique (stroboscope). Les transmetteurs peuvent également donner l'alerte.

Détecteur d'alarme

Appareil qui envoie un message à la centrale d'alarme lorsqu'un événement défini se produit (par ex. mouvement, bris de verre, vibration).

Centrale d'alarme, centrale

Désigne la centrale de commande de toute l'installation, qui traite toutes les informations, les transmet et réagit aux informations entrantes.

Zone d'alarme

Chaque zone est surveillée par un détecteur (installation sans fil) ou un groupe de détecteurs (installation filaire) et peut être programmée séparément.

APN

Access Point Name

ou « point d'accès » est le nom de la passerelle entre un réseau dorsal d'un réseau de téléphonie mobile (par ex. GPRS, 3G ou 4G) et un réseau de données externe à base de paquets, le plus souvent l'Internet public.

ITA

Installation de transmission d'alarme

Protection de l'enveloppe extérieure

Cette fonction surveille tous les accès, à savoir, les portes d'entrée, de terrasse et de cave, les lucarnes ainsi que toutes les fenêtres ; des détecteurs d'ouverture, de bris de glace et des protections de fenêtre/porte sans fil sont généralement utilisés. Lorsque la centrale d'alarme est activée en interne, il est possible de séjourner dans le bâtiment.

Sirène d'extérieur

Périphérique d'alarme pour l'extérieur, émettant généralement un signal sonore et visuel (sirène et stroboscope).

APL

Point de terminaison dans la technologie des lignes, extrémité du réseau d'accès téléphonique

L'extrémité du câble de dérivation de la ligne d'abonné au sein du réseau téléphonique correspond au point de terminaison dans la technologie des lignes ou au répartiteur domestique des lignes téléphoniques.

Utilisateur

Les différents utilisateurs du système d'alarme (par ex. propriétaire ou locataire) peuvent recevoir des droits d'accès et des codes d'utilisateur différents.

Aide en ligne

Système électronique d'assistance à l'utilisation du système d'alarme.

Détecteur de mouvement

Détecte les personnes par les mouvements thermiques (PIR), les ultrasons (US) ou les micro-ondes/radars (MW).

Alarme sans fil bidirectionnelle (2WAY)

Unidirectionnelle : les périphériques d'activation (par ex. simple télécommande) et les modules de commande transmettent uniquement des commandes à la centrale d'alarme. Bidirectionnelle : ces périphériques peuvent également accuser réception des messages de la centrale d'alarme et les analyser (par exemple, par des voyants à LED, etc.).

BS8243

Norme britannique qui regroupe une série de méthodes permettant de réduire les fausses alertes générées par les systèmes d'alarme anti-effraction et de protection contre les vols à main armée.

Méthode de chargement de batterie CC/CV

Le procédé de chargement IU, aussi dénommé CCCV pour constant current constant voltage, combine le procédé de chargement par courant constant avec celui par tension constante. Dans la première phase de chargement, la batterie est chargée par un courant constant limité par le chargeur. Par rapport au procédé de chargement par tension constante uniquement, cela limite le courant de charge de départ habituellement élevé. Une fois la tension de fin de charge sélectionnée atteinte sur la batterie, la régulation du courant passe à la régulation de tension et la deuxième phase de chargement avec tension constante commence, et le courant de charge réduit de manière autonome à mesure que l'état de charge de l'accumulateur augmente. Dans les batteries lithium-ion, la non-atteinte d'un courant de charge minimal sélectionné peut être utilisée comme critère d'arrêt du chargement.

Clé électronique/Proximity

« Clé » électronique permettant de pénétrer dans le bâtiment sans devoir saisir un code.

CLIP

Calling Line Identification Presentation (présentation de l'identification de la ligne appelante)

Codage des signaux radio

Ce procédé sécurise la transmission des signaux entre la centrale d'alarme et ses périphériques et empêche la manipulation des données.

Contact ID, CID

Protocole de transfert des données à un CRA ou une STS.

DD243

Norme britannique pour la confirmation d'alarme séquentielle.

DHCP

Le Dynamic Host Configuration Protocol (DHCP) est un protocole de communication en informatique. Il permet d'attribuer la configuration réseau à des clients par le biais d'un serveur.

Le DHCP permet d'intégrer automatiquement un ordinateur dans un réseau existant sans avoir à le configurer manuellement. Seule l'assignation automatique de l'adresse IP doit être configurée sur le client. Au démarrage de l'ordinateur sur le réseau, il peut obtenir l'adresse IP, le masque de réseau, la passerelle et le serveur DNS d'un serveur DHCP. Sans DHCP, certains réglages sont nécessaires sur l'ordinateur selon le réseau auquel il est connecté.

Écran

Afficheur de la centrale d'alarme permettant de la commander et de la programmer.

DNS

Le Domain Name System (DNS) est l'un des services les plus importants dans de nombreux réseaux basés sur IP. Sa tâche principale est de répondre aux demandes de résolution de nom.

Le DNS fonctionne comme un service de renseignements téléphoniques. L'utilisateur connaît le domaine (le nom d'un ordinateur du réseau IP connu des utilisateurs), par exemple domaine.org. Il l'envoie en tant que requête. L'adresse Internet est alors convertie en adresse IP (le numéro de connexion dans le réseau IP) par le DNS. Par exemple une adresse IPv4 au format 192.168.2.21 qui mène à l'ordinateur correspondant.

Fin de ligne double (FDLD)

Variante de câblage des centrales d'alarme filaires également pour les zones câblées.

Détecteur filaire, détecteur câblé

Détecteur d'alarme et de danger relié à la centrale d'alarme par des câbles.

Zone filaire, zone d'alarme filaire

Zone surveillée par un ou plusieurs détecteurs filaires (généralement branchés en série).

RGPD

Règlement général sur la protection des données

DTMF

Dual Tone Multi-Frequency

(Signalisation multifréquence bitonale)

La sélection multifréquence est une technique de numérotation couramment utilisée dans la téléphonie analogique.

Elle est utilisée dans les protocoles de stations de contrôle FF, CID, Scancom, Scanfast.

Système d'alarme anti-effraction, système anti-effraction

Centrale d'alarme capable de détecter une intrusion et de donner l'alerte (communément appelée « système d'alarme »)

Identification individuelle des détecteurs

Permet d'identifier avec précision le détecteur qui a été activé (voir aussi Zone d'alarme sans fil).

EN 50131

Série de normes européennes des systèmes d'alarme, de détection d'intrusion et d'agression

Détecteur de vibrations

Détecte les vibrations qui se produisent en cas de tentative d'intrusion.

Ethernet/LAN

Ethernet est une technique pour les réseaux de données locaux (LAN), les logiciels (protocoles, etc.) et le matériel (câbles, répartisseurs, cartes réseau, etc.) spécifiée pour les réseaux de données câblés.

Alarme externe

(Type d'alarme)

Situation où toutes les sirènes réagissent en même temps (à l'intérieur et à l'extérieur). L'événement est en outre signalé à une station de télésurveillance.

Format rapide, FR

Protocole de transfert des données à un CRA ou une STS. Basé sur DTMF

Accès à distance/Configuration à distance

Maintenance/programmation de la centrale d'alarme hors du lieu à surveiller (par ex. par Internet)

FSK

Frequency Shift Keying, utilisé pour le protocole de station de contrôle SIA.

Système d'alarme sans fil

Système d'alarme dont les détecteurs sont reliés à la centrale par liaison radio (sans fil). L'installation est rapide et facile et offre plus de flexibilité.

Zone d'alarme sans fil, zone sans fil

Zone couverte par la centrale d'alarme sans fil où les détecteurs radio sont identifiés et surveillés.

Clavier de commande sans fil

Facilite l'activation/la désactivation de la centrale d'alarme, par exemple dans un deuxième local (entrée/sortie du bâtiment) ; le clavier radio bidirectionnel permet également de consulter l'état du matériel.

Protection de fenêtre sans fil/Système de protection de porte sans fil

Association d'une protection mécanique et d'un détecteur d'alarme électronique. La surveillance supplémentaire de l'effet de levier est possible pour détecter même les tentatives d'effraction.

Télécommande sans fil

Facilite l'activation/la désactivation de la centrale d'alarme indépendamment du lieu, interrogation des états, alarme en cas d'urgence, etc.

Détecteur sans fil

Détecteur d'alarme et de danger raccordé à la centrale d'alarme par une liaison radio (sans fil).

Interrupteur à clé sans fil

Facilite l'activation/la désactivation de la centrale sans saisie du code (par une clé).

Portée sans fil

La distance maximale entre la centrale d'alarme et les détecteurs sans fil varie selon la disposition des lieux.

Détecteur de bris de glace

Ce type de détecteur réagit au bris de glace. On distingue les détecteurs de bris de glace passifs, actifs et acoustiques.

Système d'alarme, système de détection de danger

Système capable de détecter les Intrusions et autres dangers/urgences et de donner l'alerte.

Secteur extérieur abrité

Partition, à l'extérieur des bâtiments, protégée contre les intempéries (auvent d'entrée, terrasse, etc.)

GMT

Greenwich Mean Time (temps moyen de Greenwich) désigne le temps solaire moyen au méridien d'origine. L'expression Greenwich Mean Time (GMT) est encore utilisée aujourd'hui pour le fuseau horaire « temps de l'Europe de l'Ouest » (WET, UTC+0). La désignation « GMT », utilisée en partie par les protocoles Internet dans les horodatages, signifie toujours UTC. La plupart des appareils électroniques continuent en outre d'utiliser la mention GMT pour l'heure et la date. Le réglage du fuseau horaire correspondant au lieu où se trouve l'utilisateur s'effectue souvent en saisissant ou en sélectionnant les heures, situées avant (+) ou après (-) l'heure universelle (GMT/UTC).

Exemple Allemagne :

Heure d'hiver : UTC/GMT +1

Heure d'été : UTC/GMT +2

GPRS

General Packet Radio Service, **abrégié en GPRS (français : « service sans fil général orienté paquets ») est la désignation pour le service orienté paquets de transmission de données dans les réseaux GSM.**

GSM

Global System for Mobile Communications (précédemment Groupe Spécial Mobile) est une norme des réseaux de communication mobiles entièrement numériques principalement utilisée pour la téléphonie, mais également pour le transfert de données par commutation de circuits et par commutation de paquets et les SMS.

Désigne plus précisément les technologies de 2^e génération.

Est cependant également utilisé comme terme générique pour toutes les générations, 2G = GSM, 3G = UMTS, 4G = LTE.

Codes d'erreur GSM CME CMS

Codes d'erreur CME

Codes d'erreur liés au matériel GSM

Codes d'erreur CMS

Codes d'erreur liés au réseau GSM

GUI

Graphic User Interface, désigne l'écran de la centrale, la programmation et l'utilisation via des touches de menu sur la centrale.

M/H

Module hybride, MoHy, module supplémentaire sans fil pour la Secvest avec des zones filaires et des sorties filaires.

HTTPS

L'HyperText Transfer Protocol Secure (protocole de transfert hypertexte sécurisé) est un protocole de communication Internet utilisé pour transférer les données en toute sécurité.

L'HTTPS s'utilise pour assurer la confidentialité et l'intégrité de la communication entre le serveur Web et le navigateur Internet (client) sur Internet. Cette sécurité repose notamment sur le cryptage et l'authentification.

Sans cryptage, les données transférées par Internet peuvent être lues par quiconque a accès au réseau.

MoHy

Module hybride, M/H, module supplémentaire sans fil pour la Secvest avec des zones filaires et des sorties filaires.

IAD

Un **Integrated Access Device** (« dispositif d'accès intégré » ou routeur) désigne un appareil permettant le raccordement réseau de ports NGN par le participant.

ICMP

L'**Internet Control Message Protocol** sert dans des réseaux informatiques à échanger des messages d'informations et d'erreurs via le protocole Internet.

ICMP Ping.

Ping envoie un paquet « Echo-Request » (ping) à l'adresse cible de l'hôte à vérifier. Le destinataire doit, s'il prend en charge le protocole, envoyer une réponse selon la spécification du protocole : ICMP « Echo-Reply » (pong). Si l'ordinateur cible n'est pas accessible, le routeur responsable répond : « Network unreachable » (réseau non accessible) ou « Host unreachable » (hôte non accessible).

IMEI

L'**International Mobile Station Equipment Identity (IMEI)** est un numéro de série unique à 15 chiffres permettant d'identifier clairement les terminaux de téléphonie mobile.

IMSI

L'**International Mobile Subscriber Identity (IMSI, en français identité internationale d'abonné mobile)** permet d'identifier clairement des abonnés des réseaux mobiles (reconnaissance interne). En plus d'autres données, l'IMSI est enregistrée sur une carte à puce spéciale, la carte SIM (Subscriber Identity Module). Le numéro IMSI est attribué par les opérateurs mobiles une fois pour chaque client dans le monde. L'IMSI n'a rien à voir avec le numéro de téléphone qui est associé à la carte SIM.

Générateur de signal int.

Sirène optique/acoustique pour l'intérieur (en complément de la sirène extérieure)

Sirène d'intérieur

Alarme généralement acoustique pour l'intérieur (en complément de la sirène extérieure)

Protection intérieure

Permet de sécuriser l'intérieur, notamment les zones qu'un cambrioleur devra généralement traverser. On utilise pour cela des détecteurs de mouvement et des barrières infrarouges.

Installation

Montage et mise en service de la centrale d'alarme et des différents périphériques.

Alerte interne

L'alarme retentit uniquement dans le bâtiment, les sirènes d'extérieur restent muettes.

Utilisation intuitive

L'utilisation des appareils est considérablement facilitée par un menu très intuitif.

IP

L'**Internet Protocol (IP)** est un protocole réseau largement diffusé dans les réseaux informatiques.

Mobile IP

Synonyme pour la transmission basée sur IP 4G (LTE) et 2G (GPRS)

Brouillage

Un brouilleur de fréquence empêche ou rend difficile la réception normale de l'émission sans fil d'ondes électromagnétiques. Comme l'émetteur brouillé, le brouilleur envoie de l'énergie sous forme d'ondes électromagnétiques et brouille totalement ou partiellement les ondes initiales.

Avertisseur combiné

Avertisseur combinant une sirène (signal acoustique) et un stroboscope (signal optique).

Extensions de communication

Permettent de transmettre les messages d'alarme via des canaux supplémentaires, par ex. la téléphonie mobile (module de téléphonie mobile) pour les messages vocaux/texte ou des protocoles numériques.

Composants

Voir Composants du système

LAN/Ethernet

Voir Ethernet/LAN

Station de télésurveillance

Voir STS

Niveau 1-4

voir niveau d'accès 1-4

Ligne

Autre terme désignant une zone, principalement utilisé dans le domaine filaire.

Alarme locale

(Type d'alarme)

Avec ce type d'alarme, les sirènes retentissent à l'intérieur et à l'extérieur (en Allemagne, l'alarme sonore extérieure (sirène) doit s'arrêter au bout de 3 minutes, tandis que l'alarme visuelle (flash) peut clignoter indéfiniment).

LTE

Long Term Evolution (en abrégé **LTE**, également **3.9G**) est une désignation pour la norme de téléphonie mobile de troisième génération. Une extension s'appelle *LTE-Advanced* ou 4G, elle est compatible en aval avec LTE dans le projet Next Generation Mobile Networks (NGMN). Pour des raisons de marketing, LTE est déjà présenté comme 4G et LTE-Advanced comme 4G+, ce qui n'est cependant pas correct d'un point de vue technique.

Avec jusqu'à 300 mégabits par seconde, des taux de téléchargement significativement plus élevés qu'avec les anciennes normes sont possibles selon les conditions de réception.

La gamme de fréquence utilisée pour cela par les fournisseurs d'accès LTE est uniquement la bande de fréquence UHF (également appelée ultra hautes fréquences). Plusieurs fréquences y sont utilisées, variant régionalement dans la plage UHF moyenne à supérieure d'env. 700 à 2 600 mégahertz.

Le schéma de base de l'Universal Mobile Telecommunications Systems (UMTS, 3G) est maintenu pour le LTE (3.9G). Un équipement ultérieur rapide et peu coûteux des infrastructures de la technologie UMTS vers LTE-Advanced (4G) par ex. est donc possible.

MAC

L'adresse MAC (Media Access Control, Ethernet-ID) est l'adresse matérielle de chaque carte réseau permettant d'identifier clairement l'appareil sur le réseau.

Urgence médicale

Cette fonction d'alarme permet d'appeler de l'aide en cas d'urgence médicale.

Mobile

Synonyme pour les transmissions suivantes dans le réseau de téléphonie mobile :

- Appels vocaux avec un numéro de téléphone, par ex. +49 173 1234567
- Reporting CRA/STS basé de manière classique sur DTMF ou FSK, tel que FF, CID, SIA, Scancom, Scanfast, Tunstall
- Envoi de SMS

S/A

Seulement actif, un utilisateur ou un type de zone pour activer uniquement l'installation.

NC

Normally closed (normalement fermé), contact ou commutateur s'ouvrant en cas d'activation

NO

Normally open (normalement ouvert), contact ou commutateur se fermant en cas d'activation

Station de télésurveillance

Voir STS

STS

La centrale d'appel d'urgence, aussi appelée station de télésurveillance (STS), transfère, accepte, archive et traite les messages enregistrés dans la zone des abonnés, provenant par ex. de systèmes d'alarme ou de dispositifs privés ou professionnels via les lignes de courant louées de l'exploitant du réseau (lignes réservées) ou le réseau téléphonique public (Datex-P / X.25 / X.31, IP, GSM, ISDN, en Suisse via TUS (Alarmnet)), et assure le suivi des messages (intervention). Les STS des prestataires de sécurité privés gèrent également les interventions des services de secours (police/pompiers).

NTP

Network Time Protocol

Le Network Time Protocol (NTP) est un standard permettant de synchroniser les horloges des systèmes informatiques via des réseaux de communication à base de paquets. Le NTP utilise le protocole de transport sans connexion UDP. Il a été spécialement conçu pour permettre une indication fiable de l'heure via les réseaux avec une durée de vie variable des paquets.

Dans le langage courant, NTP désigne à la fois le protocole et l'implémentation de référence du logiciel. Le Simple Network Time Protocol (SNTP) est une version simplifiée du NTP.

O/C

Open Circuit, circuit électrique ouvert

Détecteur d'ouverture

Le détecteur reconnaît l'ouverture d'une fenêtre, d'une porte, d'un volet roulant, d'une porte de garage, etc.

Surveillance de périmètre

Surveillance sans faille d'espaces ouverts vastes, d'un périmètre ou d'un parc de stationnement, à l'aide de barrières infrarouges et de détecteurs de mouvement et/ou de caméras de surveillance à détection intelligente de mouvement.

Port

Un port fait partie d'une adresse réseau.

Programmation

Permet le réglage précis de la centrale d'alarme selon les besoins et les souhaits de l'utilisateur (par exemple pour des zones/partitions spécifiques).

RTC

Réseau téléphonique commuté, analogique, a/b

Détecteurs autonomes avertisseurs de fumée

Les détecteurs optiques autonomes avertisseurs de fumée permettent de sauver des vies en réagissant à la présence de particules de fumée dans l'air (en général de gaz toxiques) : les sondes thermiques/détecteurs de différentiel de chaleur réagissent en cas de dépassement d'une température maximale (par ex. 65 °C) ou de hausse brutale de la température.

Sorties relais

Sorties de commutation pour appareils externes (éclairage, volets roulants électriques, autres alarmes, etc.)

Code tournant (RC)

Le code tournant est une technologie offrant une protection optimale contre la lecture et la subtilisation de code afin de barrer l'accès des personnes non autorisées.

Routeur

Voir IAD

RSSI

Le **Received Signal Strength Indicator** constitue un indicateur pour l'intensité de la réception d'applications de communication sans câble.

S/C

Short Circuit, court-circuit

Sabotage, protection anti-sabotage, manipulation

Chaque périphérique est surveillé pour éviter toute manipulation de la centrale d'alarme et de ses périphériques. L'ouverture de boîtiers de détecteurs et le débranchement de câbles déclenchent TOUJOURS une alarme. Les périphériques sont généralement protégés par un contact dans le couvercle (déclenchant une alarme lors de l'ouverture) et un contact d'arrachage du boîtier mural.

Scancom

Un protocole d'appel soins de santé.

Scancom est similaire à Scanfast à l'exception du canal 8 utilisé pour établir une liaison phonique bidirectionnelle entre la centrale d'alarme et la station de télésurveillance.

Scanfast

Un protocole d'appel soins de santé.

Scanfast est similaire à Format rapide. Il n'utilise cependant que le canal 2 (appel soins de santé) et le canal 3 (inactivité). Les canaux 1, 4, 5, 6, 7, 8 sont toujours "5" (inutilisés).

Activation, désactivation

Activer/désactiver la centrale d'alarme.

Périphériques d'activation

Périphériques permettant d'activer/désactiver la centrale d'alarme (par ex. télécommande, interrupteur à clé, élément de commande)

Carte SD, carte micro SD

Carte micro SD pour l'enregistrement de :

- logiciel d'application dans le dossier INSTALL ;
- fichiers langue dans le dossier INSTALL ;
- images de TVIP41550 dans le dossier IMG_X ;
- Configuration de la centrale lors de la sauvegarde via le GUI dans le dossier CONFIG
- traces dans le dossier TRACE.

Pour les images et éléments similaires, une fonction de mémoire circulaire est intégrée. La centrale d'alarme contrôle pour cela à chaque minute si la mémoire est pleine ou non.

Si la carte SD est pleine, les enregistrements les plus anciens sont automatiquement supprimés. Vous obtenez quand même le message d'erreur « Carte SD pleine ». Pour pouvoir confirmer ce message d'erreur, vous devez supprimer manuellement des données de la carte SD.



Danger

Protection des données

Tenez compte des remarques relatives à la carte SD dans le chapitre « Mise hors service de la centrale ».

Bande de fréquence de sécurité (868 MHz)

Cette plage de fréquences est réservée par les pouvoirs publics à la transmission de signaux radio du domaine de la sécurité. Les interférences causées par les casques sans fil, téléphones portables, systèmes d'ouverture de porte de garage, etc. sont donc quasiment exclues.

Europe : Définition de l'utilisation des fréquences de la conférence européenne des postes et télécommunications (CEPT).

Allemagne : BNetzA-Bundesnetzagentur

Autriche : le plan d'utilisation des fréquences est publié par le Ministère fédéral du Transport, de l'Innovation et de la Technologie.

Suisse : le plan d'utilisation des fréquences est appelé Plan national d'attribution des fréquences (PNAF) et est publié par l'OFCOM.

Détecteur sismique

Voir Détecteur de choc

SELV

Basses tensions de sécurité (Safety Extra Low Voltage).

Serveur

Un serveur est un programme qui attend d'être contacté par un client pour lui rendre un service donné.

SHA

SHA-2 (de l'anglais secure hash algorithm, algorithme de hachage sécurisé) est le terme générique pour les quatre fonctions de hachage cryptographiques SHA-224, **SHA-256**, SHA-384 et SHA-512, qui ont été standardisés en 2001 comme les successeurs de SHA-1 par la norme NIST d'origine américaine.

SIA

Protocole de transfert des données à un CRA ou une STS.

SIA-IP (DC-09)

Un protocole de transfert des données basé sur IP (par ex. FF, SIA ou CID) à une station de télésurveillance.

Générateur de signal

Générateur de signal, bip sonore, sirène

Sirène

Poste d'alarme qui déclenche une alarme à la réception d'une commande par la centrale (sirène, stroboscope, etc.).

SIM

Subscriber identity module, carte à puce pour téléphones portables

SMS

Le Short Message Service ("Service de messages courts") est un service de télécommunication qui permet d'envoyer des messages sous forme de texte. Il a été initialement développé pour la téléphonie mobile GSM et est maintenant disponible sur le réseau fixe.

SMSC

Short Message Service Centre (centre de service de messages courts)

F-SMSC = SMSC pour les réseaux fixes

SMTP, serveur SMTP

Simple Mail Transfer Protocol

Le Simple Mail Transfer Protocol (SMTP, en français : protocole simple de transfert de courrier) est un protocole Internet servant à échanger des e-mails sur les réseaux informatiques.

Il est principalement utilisé pour alimenter et transférer les e-mails. D'autres protocoles spécialisés, comme POP3 ou IMAP, sont utilisés pour récupérer les messages.

Les serveurs SMTP acceptent généralement les connexions sur le port 25 ("smtp"). Les serveurs plus récents utilisent également le port 587 pour accepter les messages des utilisateurs authentifiés devant être livrés à d'autres serveurs de messagerie ("submission").

SNTP

Simple Network Time Protocol

Le Network Time Protocol (NTP) est un standard permettant de synchroniser les horloges des systèmes informatiques via des réseaux de communication à base de paquets. Le NTP utilise le protocole de transport sans connexion UDP. Il a été spécialement conçu pour permettre une indication fiable de l'heure via les réseaux avec une durée de vie variable des paquets.

Dans le langage courant, NTP désigne à la fois le protocole et l'implémentation de référence du logiciel. Le Simple Network Time Protocol (SNTP) est une version simplifiée du NTP.

Transmetteur vocal

Périphérique de la centrale permettant de transférer les messages vocaux. La transmission des informations d'alarme s'effectue en texte clair. Le texte à transférer est enregistré à l'aide d'un microphone sur la centrale d'alarme.

SSL

Secure Sockets Layer est un protocole réseau permettant le transfert sécurisé des données.

Transport Layer Security (TLS, en français : sécurité de couche transport), largement connu sous son nom précédent Secure Sockets Layer (SSL), est un protocole de cryptage hybride destiné au transfert sécurisé des données sur Internet. Depuis la version 3.0, le protocole SSL a été perfectionné et standardisé sous un nouveau nom, TLS, où la version 1.0 de TLS correspond à la version 3.1 de SSL.

Le cryptage TLS est aujourd'hui principalement utilisé avec HTTPS. La plupart des serveurs Web prennent en charge TLS 1.0, un grand nombre également SSLv2 et SSLv3 avec de nombreuses méthodes de cryptage.

État

État de la centrale d'alarme : activée, activée en interne ou désactivée.

Indication d'état

Message renvoyé par la centrale d'alarme à un module (périphériques d'activation, module d'information, etc.) concernant son état actuel.

Demande d'état

Interrogation de la centrale d'alarme concernant l'état du système (par exemple, par appel de touche de la télécommande radio)

Alerte silencieuse

(Type d'alarme)

Aucune sonnerie ne retentit (tout reste silencieux, à l'intérieur comme à l'extérieur). Une station de contrôle est cependant alertée de manière invisible (un cambrioleur ne doit pas être alerté, mais au contraire pris par surprise ; un agresseur ne doit pas être provoqué, etc.).

Supervision

La centrale d'alarme surveille si les détecteurs sont présents et actifs. Les périphériques répondent environ toutes les 4 minutes. Si les messages d'état ne sont plus envoyés pendant une durée prolongée, la centrale réagit.

JT

Le jack téléphonique est un type de connecteur utilisé en Allemagne pour les connexions téléphoniques.

Sert de connexion au réseau téléphonique public ou d'interface a/b pour les connexions téléphoniques analogiques des périphériques supplémentaires.

Manipulation

Voir Sabotage

TAP

Telocator Alphanumeric Protocol, protocole de transmission des messages courts.

Dommages techniques

Dégâts des eaux, fuite de gaz, etc. (protection uniquement par détecteurs de danger spéciaux).

Partitions

Il est possible de subdiviser un système d'alarme en plusieurs partitions, chacune fonctionnant de manière autonome.

Chaque partition (par ex., maison, atelier) peut être commandée et programmée séparément et comprendre le nombre souhaité de zones/détecteurs.

Numéroteur téléphonique

Dispositif servant à transmettre les messages d'alarme d'une centrale d'alarme par téléphone. Les transmetteurs vocaux peuvent être intégrés à une centrale d'alarme ou ajoutés en tant que périphériques complémentaires.

TNV

Tensions du réseau de télécommunications (Telecommunications Network Voltage)

Tunstall

Un protocole d'appel soins de santé.

Interférences

Voir Brouillage

DT

Dispositif de transmission selon EN 50136

UCP

Universal Computer Protocol

UMTS

L'**Universal Mobile Telecommunications System (UMTS)** est une norme de téléphonie mobile de troisième génération (3G), qui offre des taux de transmission de données considérablement supérieurs (jusqu'à 42 Mbit/s avec HSPA+, sinon max. 384 kbit/s) qu'avec la norme de téléphonie mobile de deuxième génération (2G), la norme GSM (jusqu'à 220 kbit/s pour EDGE, sinon max. 55 kbit/s pour GPRS).

UTC

Universal Time Coordinated désigne le temps universel coordonné actuellement mondialement utilisé, voir également GMT.

VdS

Verband der Schadensversicherer (Association allemande des assureurs). Elle fixe les directives pour les différents niveaux de sécurité.

VDS-A s'applique au domaine non professionnel

VDS-Home s'applique aux systèmes de gestion des dangers domestiques

VDS-B s'applique au domaine professionnel

VDS-C s'applique aux banques et aux bijouteries (établissements professionnels à haut risque)

WAN

Un Wide Area Network (réseau étendu) est un réseau informatique qui s'étend sur une zone géographique très étendue contrairement à un LAN. Synonyme scientifique populaire d'Internet.

Détecteur d'inondation

Permet de détecter les dégâts des eaux/inondations. Il comprend un appareil de base et un capteur d'eau (à installer systématiquement à l'emplacement susceptible d'être inondé en premier).

INTERFACE WEB

Interface Web, signifie l'accès au serveur Web de la centrale via un navigateur Web.

Certifications

Déclarations d'instituts indépendants attestant de la qualité et de la sécurité des centrales d'alarme (en Allemagne : UVV et VdS pour la protection contre les sinistres).

Zone

Autre terme désignant une ligne. Décrit un circuit électrique fermé auquel les contacts d'alarme ou anti-sabotage sont raccordés et qui est relié à une centrale d'alarme anti-effraction. Dans les zones sans fil, il y a en général un détecteur pour chaque zone

Niveau d'accès 1-4

Niveau d'accès 1-4, également appelé Level 1-4, conformément aux normes

EN 50131-1 §8.3.1

EN 50131-3 §8.3.1

EN 50136-2 §5.2

EN 50136-3 §6.2

Niveau d'accès 1

Accès à tous

Niveau d'accès 2

Accès utilisateur, par exemple pour un opérateur

Niveau d'accès 3

Accès utilisateur, par exemple pour le personnel d'une société de surveillance

Niveau d'accès 4

Accès utilisateur, par exemple pour la personne chargée de la configuration

Remarque :

Le niveau d'accès 4 est utilisé en cas de modification du logiciel d'exploitation sans que vous ayez besoin d'activer un dispositif de sabotage au niveau de la centrale ou un dispositif de commande supplémentaire.

Activation forcée, armement forcé

Les zones possédant cet attribut sont automatiquement exclues, lors de l'activation de la centrale d'alarme ou d'une partition, si elles sont ouvertes.

Surveillance des erreurs et du sabotage de la centrale

La centrale surveille en continu les états d'erreurs et de sabotage. La surveillance s'applique aux éléments suivants :

- **Contact anti-sabotage :**
Les contacts anti-sabotage de la centrale sont surveillés en continu.
- **Supervision**
La centrale surveille en continu les messages de supervision des composants à la centrale.
- **Brouillage/Interférence :**
La centrale surveille les tentatives d'interférences du signal sans fil et surveille les tentatives d'interférences du signal sans fil sur des composants sélectionnés. Si un brouillage y est détecté, le message « Brouillage ou interférence » est envoyé à la centrale.
- **Raccordements de zone**
- **Ports de communication**
- **Alimentation électrique :**
La centrale surveille l'alimentation électrique sous des conditions de charge et enregistre les dysfonctionnements.
- **Charge aux sorties de tension.**

Conditions de temps

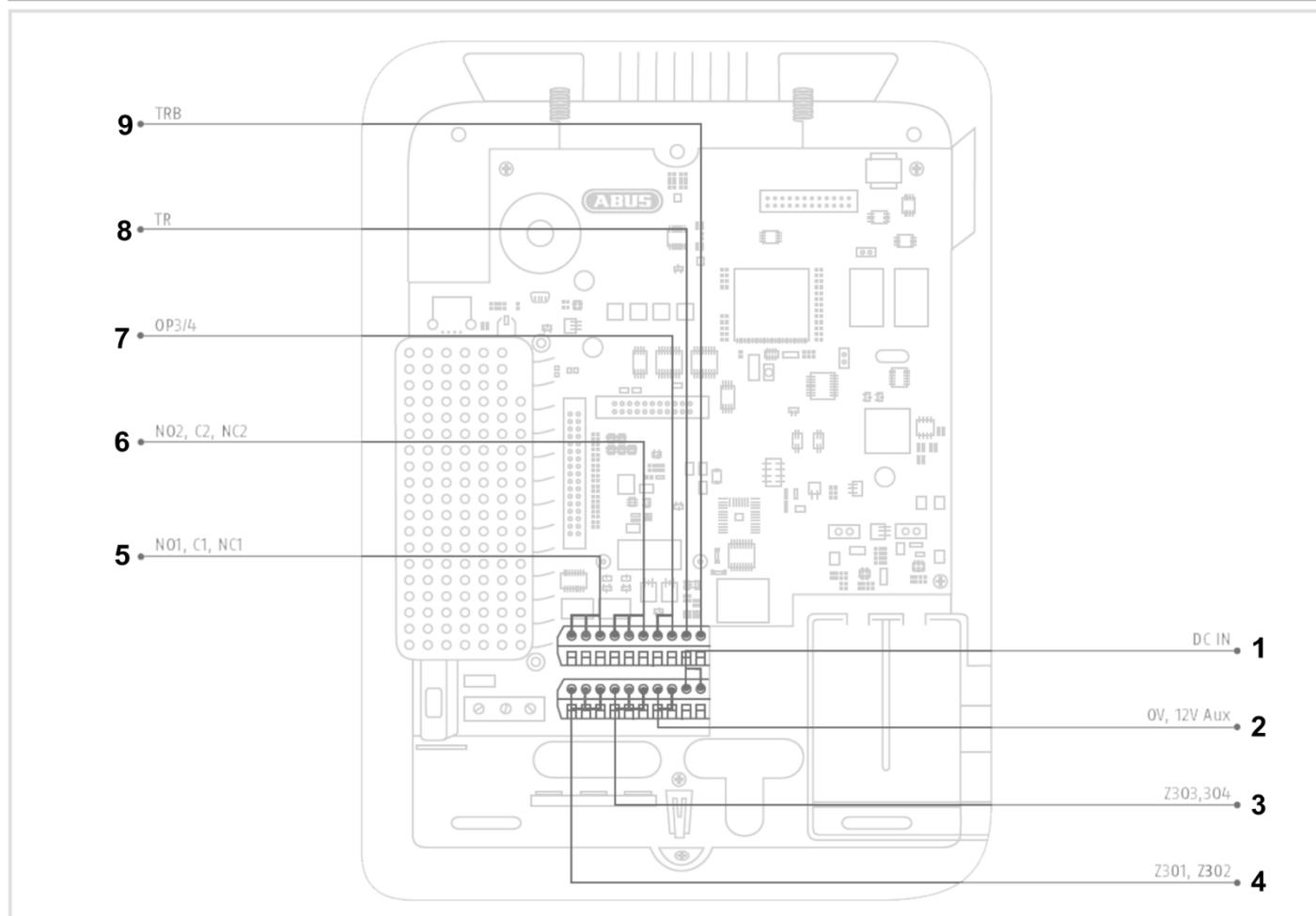
La centrale a été conçue de manière à ce que des modifications d'état des zones supérieures à 400 ms soit reconnues (EN 50131-1 chapitre 8.9.1 et EN 50131-3 chapitre 8.9 et annexe B).

Les signaux de cambriolage, d'agression ou de sabotage doivent durer au minimum 400 ms.

La centrale a été conçue de manière à ce que des modifications d'états de défaut (signaux de défaut) supérieures à 10 s soient reconnues (EN 50131-1 chapitre 8.9.1 et EN 50131-3 chapitre 8.9 et annexe B).

Montage / installation

Aperçu des sorties, bornier



N°	Désignation/fonction	N°	Désignation/fonction
1	DC IN 13,8V + : raccordement de l'alimentation électrique 13,8 V	6	NO2, C2, NC2 – Sortie relais 2 : contact de relais sans potentiel, 30 V CC, 24 V CA rms, 500 mA
2	0V, 12V Aux : sortie de tension 13,8 V  Remarque En cas de coupure de courant, cette sortie n'est pas sauvegardée par la batterie. En cas de coupure de courant, la tension de sortie est de 0 V.	7	OP3/4 – Sorties transistor : pour une sirène filaire, un stroboscope et un émetteur sonore Sortie de transistor Open Drain 500 mA 13,8 VCC  Remarque En cas de coupure de courant, ces sorties chutent à 0 V.
3	Z303, Z304 : zones filaires 303 et 304	8	TR – Tamper Return : entrée anti-sabotage pour la sortie anti-sabotage d'une sirène câblée  Remarque À la livraison, un pontage à fil est raccordé à 0 V. Ainsi, aucun message d'erreur (sabotage) n'apparaît si aucune sirène filaire n'est raccordée.

4	Z301, Z302 : zones filaires 301 et 302	9	TRB – Trouble : entrée de message de défaut pour la sortie défaut d'une sirène filaire  Remarque À la livraison, un pontage à fil est raccordé à 0 V. Ainsi, aucun message d'erreur (défaut) n'apparaît si aucune sirène filaire n'est raccordée.
5	NO1, C1, NC1 – sortie relais 1 : contact de relais sans potentiel, 24 VCA rms / 500 mA		

Fixation murale de la plaque de montage

Position du système d'alarme sans fil (centrale)



Remarque

La centrale doit être installée en lieu sûr, hors de la vue des éventuels cambrioleurs, tout en étant facilement accessible pour l'opérateur.

La centrale d'alarme doit être installée sur une surface plane, afin que la protection anti-sabotage au dos soit inaccessible lorsque la centrale est montée.

La centrale doit être installée à hauteur d'homme.



Remarque

La centrale doit être installée hors de portée des enfants en bas âge.



Remarque

Positionnez la centrale d'alarme de manière à ce que les signaux sonores restent audibles à distance.

La centrale doit être positionnée dans une zone surveillée de sorte que les personnes non autorisées soient obligées de passer par une zone sous surveillance lorsque la centrale est activée.

La centrale d'alarme doit être installée à proximité d'une prise de courant ou d'une alimentation électrique.

Si un transmetteur vocal est utilisé, la centrale doit être raccordée à une prise téléphonique.

La centrale d'alarme doit être installée à plus de 1 mètre de tout objet métallique (miroirs, radiateurs, etc.).

Fixation de la plaque de montage



Danger

La centrale est alimentée par un bloc d'alimentation intégré.

Celui-ci est raccordé au réseau électrique 230 VCA du bâtiment par une ligne séparée.

Le raccordement au circuit électrique du bâtiment doit être effectué dans le respect de la réglementation nationale.

Vérifiez que l'alimentation secteur est hors tension et sécurisée contre toute remise en service accidentelle.



Remarque

Nous recommandons l'installation d'un ferrite sur l'alimentation secteur 230 V.

Par ex. ferrite Würth 742 711 32S ou 742 715 3.

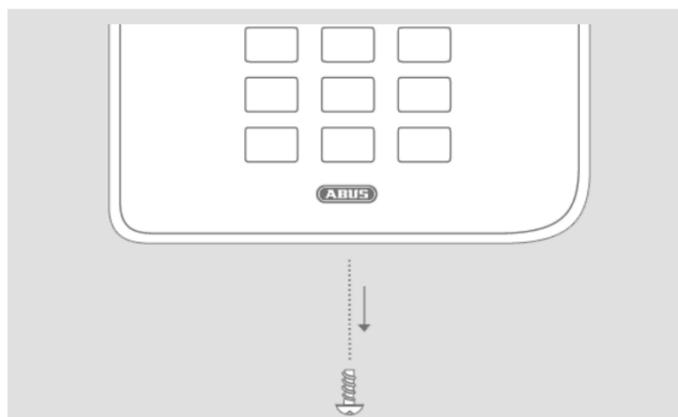
Cela évite un dysfonctionnement éventuel de la centrale, lorsque des perturbations électromagnétiques encore autorisées par la directive CEM mais très fortes surviennent.



Danger

Vérifiez qu'aucune gaine ne passe dans le mur où vous comptez procéder à l'installation.

1. Déterminez l'emplacement des trous sur le mur à l'aide du gabarit de perçage fourni dans le guide de démarrage rapide.
2. Desserrez la vis située au bas du boîtier.



3. Ouvrez prudemment le boîtier.
4. Retirez prudemment le connecteur du câble plat du bornier sur la carte.
5. Séparez la partie supérieure du boîtier de la partie inférieure.

**Remarque**

Lors du montage, assurez-vous que l'interrupteur anti-sabotage du boîtier (1) est directement en contact avec le mur !

Assurez-vous que la partie inférieure et les périphériques intégrés ne sont pas endommagés lors du serrage des vis et que toutes les vis sont serrées !

6. Fixez la partie inférieure au mur.
7. Le montage doit être effectué hors tension.
8. Fixez la bride de décharge de traction.
9. Branchez le câble réseau sur la prise de la carte.
10. Insérez la(es) batterie(s) dans le compartiment de batterie.

Raccordement des périphériques**Généralités concernant les centrales d'alarme**

Une installation incorrecte ou bâclée peut entraîner une mauvaise interprétation des signaux et déclencher de fausses alertes.

Les coûts éventuels des interventions de secours, comme celles des pompiers ou de la police, sont à la charge de l'exploitant de la centrale d'alarme. Lisez donc attentivement cette notice et tenez compte, lors de l'installation de la centrale, de la désignation exacte des câbles et des composants utilisés.

11. Raccordez tous les périphériques aux borniers.
12. Vérifiez que toutes les connexions sont correctement fixées.

**Important :**

Lors du raccordement de composants avec une tension d'alimentation externe séparée, installez une liaison équipotentielle à tous les raccordements à la masse, raccordements 0 Volt et raccordements négatifs. Vous obtenez ainsi des niveaux de signal définis sur les fils de connexion entre les composants.

Dans un système de sécurité, la surveillance anti-sabotage du câblage entre les composants est également importante, voire obligatoire.

**Important :**

Placez les câbles de manière à ce qu'ils ne soient pas écrasés.

**Important :**

À la livraison, un pontage à fil est raccordé entre le raccordement TR (Tamper Return) et 0 V ainsi qu'entre le raccordement TRB (Trouble) et 0 V. Ainsi, aucun message d'erreur (sabotage ou défaut) n'apparaît si aucune sirène filaire n'est raccordée.

**Important :**

Veillez à ce que les extrémités de fils dénudés n'entrent pas en contact avec des surfaces ou contacts conducteurs sur les cartes.

Pour cette raison, isolez le cas échéant les extrémités de fils dénudés inutilisées.

Montage du module de téléphonie mobile en option

S'il est disponible :

Connectez le module de téléphonie mobile au bornier (CON 7 GSM/GPRS) de la carte. Veillez à n'endommager et à ne toucher aucun composant électronique. (Voir également le manuel d'installation des modules de téléphonie mobile correspondants).

**Important :**

Insertion de la carte micro SD

1. Insérez la carte SD dans le support de carte SD prévu si elle n'est pas déjà préinstallée.
2. Vérifiez que la carte SD est correctement insérée dans son support.

Mesures finales

1. Vérifiez si toutes les connexions sont en bon état et correctement fixées afin d'éviter les fausses alertes.
2. Branchez le connecteur du câble plat de la partie supérieure de l'appareil au bornier (CON 2) de la carte.



Le logiciel de la centrale d'alarme détecte automatiquement le type de la partie supérieure du boîtier, surface avant tactile ou surface avant à touches.

Lors de l'activation, le logiciel contrôle quelle surface avant est installée.

Cela signifie que l'interface utilisateur et certaines fonctions changent pour prendre en charge la surface avant tactile Secvest ou la surface avant à touches Secvest.

Si le logiciel détecte une surface avant tactile, il passe en fonctionnement tactile Secvest. Sinon, le logiciel prend en charge le fonctionnement à touches Secvest.

Remarque :

Pour plus de détails, voir la section 10.5.1 « Fonctions » du manuel d'utilisation

3. Branchez le câble de raccordement de la/des batterie(s) au connecteur (BATT1 CON8, BATT2 CON9) de la carte.



Après le branchement de la batterie, l'installation démarre.

Activez également l'alimentation électrique principale.

Branchez le bloc d'alimentation externe sur la prise ou réactivez le circuit électrique avec lequel la Secvest est alimentée avec 230 V.

Conseil :

En débranchant et en rebranchant le fusible principal de 230V dans la Secvest, vous pouvez lancer une désactivation/activation de l'alimentation électrique de 230 V.

4. Fermez le boîtier avec précaution en l'accrochant d'abord en haut dans les crochets prévus à cet effet, en le rabattant vers le bas et en le pressant dans les crans d'arrêt.
5. Fermez le boîtier avec la vis située au bas du boîtier.

Remplacement de la partie supérieure, surface avant tactile, surface avant à touches



Procédez dans l'ordre suivant :

- **Mise à niveau** du logiciel de la centrale d'alarme à la version la plus récente (prise en charge Secvest tactile, version logicielle $\geq 2.01.08$).
- **Débranchez** entièrement la centrale d'alarme de son alimentation électrique, de la/des batterie(s) et de l'alimentation électrique externe.
- **Remplacez** la surface avant.
- **Rebranchez** entièrement la centrale d'alarme à son alimentation électrique, à la/aux batterie(s) et à l'alimentation électrique externe.

Sinon, cela peut entraîner des défauts de sensibilité des touches tactiles et de la fonction Proximity.

Mise en service

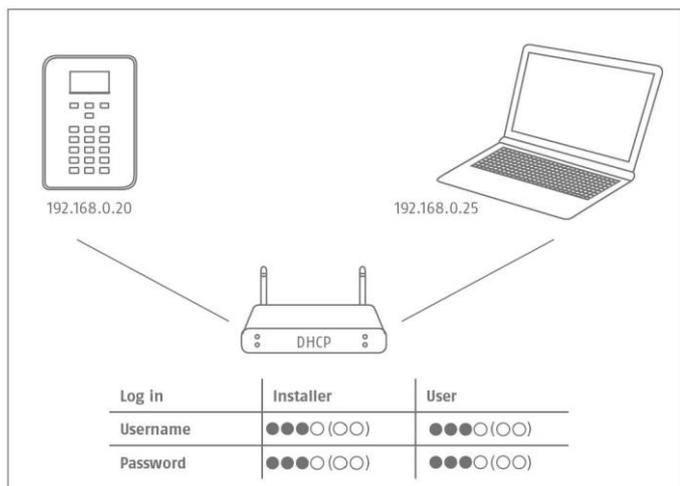
Première mise en service/restauration de la programmation d'usine



Remarque

Il est **impossible** d'accéder à la centrale d'alarme sans fil via le serveur Web sans exécuter l'assistant d'installation et de démarrage.

1. Connectez votre PC au réseau de votre client.



2. Activez l'alimentation électrique.
3. Suivez l'assistant d'installation et de démarrage sur la centrale.
4. Sélectionnez :
 - La langue de menu souhaitée.
 - La version logicielle souhaitée pour la centrale d'alarme.
 - Le pays pour les réglages nationaux.
 - La date actuelle.
 - L'heure actuelle.
 - Le basculement automatique ou manuel entre l'heure d'été et l'heure d'hiver.
 - Message d'erreur CA en présence d'une alimentation électrique 230 V. Des messages d'erreur s'affichent alors si des anomalies surviennent.
 - Message d'erreur de courant continu externe en présence d'une alimentation électrique CC 13,8 V. Des messages d'erreur s'affichent alors si des anomalies surviennent.
 - Batterie 2, si elle doit être utilisée.
 - Le type de zone filaire (par ex. 2 fils FSL 2K2/4K7).
 - Si l'accès via le serveur Web est autorisé ou non. Par défaut, il est autorisé.
 - Si la centrale d'alarme doit obtenir automatiquement l'adresse IP ou si vous souhaitez saisir manuellement l'adresse IP.

- automatique : DHCP activé
- manuel : DHCP désactivé, les menus de saisie suivants s'affichent :
 - Adresse IP
 - Masque de sous-réseau IP
 - Passerelle adresse IP
 - Première adresse IP du serveur DNS
- Port HTTP interne

L'écran affiche alors

- l'adresse IP de la centrale d'alarme sans fil
- DHCP ON/OFF
- la version actuelle du logiciel
- le numéro de série de la centrale d'alarme sans fil
- la référence de la centrale d'alarme sans fil

Notez l'adresse IP !

- AES/NSL Reporting, si des rapports relatifs à la station de contrôle doivent être générés
- la longueur du code d'accès, 4 ou 6 caractères
- le code installateur (version logicielle $\geq 1.01.00$)
- le code administrateur (version logicielle $\geq 1.01.02$)

5. L'écran affiche alors :

- les données de login provisoires pour l'installateur et l'administrateur

6. L'affichage « Veuillez vérifier si de nouvelles versions logicielles sont disponibles. » apparaît.

Le contrôle s'effectue en mode Installateur.

Dans le menu utilisateur de niveau 4, vous pouvez également effectuer ce contrôle puis une mise à niveau logicielle.

7. Sur votre PC, ouvrez le navigateur Internet et entrez l'adresse IP affichée par la centrale. Vous pouvez aussi utiliser le programme d'installation ABUS IP Installer pour afficher la centrale d'alarme et y accéder automatiquement. Il se trouve dans l'espace de téléchargement sur www.abus.com.

8. Connectez-vous au système d'alarme sans fil via le navigateur Internet.



Remarque

Lors de la première configuration de la centrale, il peut s'écouler jusqu'à trois minutes avant que le

navigateur Internet n'accède à la centrale d'alarme sans fil car le certificat SSL se crée automatiquement pendant ce délai.

Un écran s'affiche avec le message suivant : Création du certificat SSL en cours, ceci peut durer quelques minutes.

Les fonctions réseau ne sont pas disponibles pendant ce temps.



Remarque

Le message suivant s'affiche : Initialisation réseau, veuillez patienter...

- Connectez-vous au système d'alarme sans fil en tant qu'installateur.



Remarque

L'utilisation d'une adresse IP fixe au lieu d'une adresse IP attribuée dynamiquement (DHCP) peut être judicieuse dans certains cas.

Certains routeurs attribuent d'autres adresses IP à leurs clients après un certain temps. Dans ce cas, les autres appareils ne connaissent pas encore cette nouvelle adresse IP.

Si la centrale est déjà installée

- Connectez-vous au système d'alarme sans fil en tant qu'installateur.
- Accédez au sous-menu suivant : Info>Transmission>Ethernet.
- Notez l'adresse IP.
- Déconnectez-vous de la centrale.
- Ouvrez maintenant le navigateur Internet sur le PC et entrez l'adresse IP affichée par la centrale.
- Ouvrez maintenant le navigateur Internet sur le PC et entrez l'adresse IP affichée par la centrale.
- Connectez-vous au serveur Web en tant qu'installateur à l'aide du nom d'utilisateur et du mot de passe.

Connexion au système d'alarme sans fil

- Ouvrez votre navigateur Internet.
- Saisissez l'adresse IP indiquée sous la forme suivante : **xxx.xxx.xxx.xxx**.

Vous basculez alors automatiquement vers https.



Remarque

Tant qu'un utilisateur (opérateur, installateur) est directement connecté à la centrale d'alarme sans fil, vous ne pouvez pas accéder au navigateur Internet pour des raisons de sécurité !

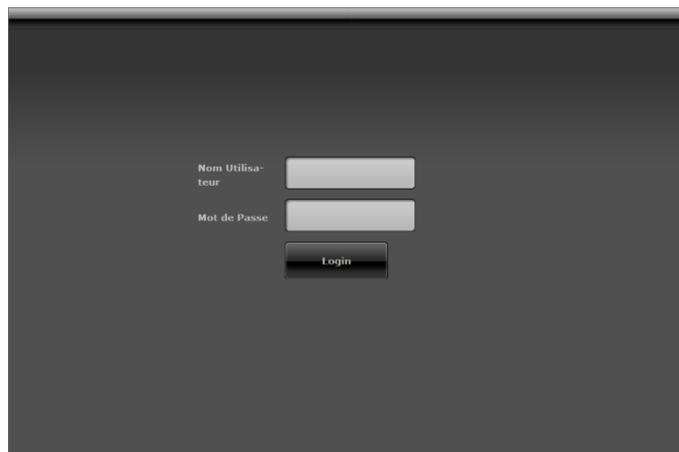


Remarque

Selon le navigateur utilisé, vous êtes informé que la connexion/le certificat n'est pas sûr(e).

Confirmez l'exception de sécurité et enregistrez-la.

- Chargez la page. L'écran d'authentification s'ouvre.



- Connectez-vous en tant qu'**installateur** avec le nom d'utilisateur et le mot de passe d'installateur.

Remarque pour les versions logicielles < 1.01.00

Le mot de passe d'installateur par défaut est 9999(99)

- Cliquez sur le bouton **Login** ou appuyez sur la **touche Entrée** du clavier.
- Le menu principal s'affiche.



Version logicielle >=3.00.03

Après connexion, le logiciel interroge automatiquement le serveur FTP ABUS : « De nouveaux logiciels sont-ils disponibles ? ».

Si le serveur FTP répond « Oui », le menu contextuel suivant s'ouvre.



Cliquez sur le bouton **Annuler**.

Vous trouverez de plus amples informations sur la mise à niveau logicielle dans le chapitre Mise à niveau logicielle en annexe.



Remarque

Une mise à niveau logicielle via le serveur Web peut uniquement être effectuée par un utilisateur de type niveau 4.

Déconnexion du système d'alarme sans fil

Cliquez sur le bouton **Logout**.

Si vous travaillez directement sur la centrale, appuyez sur la touche de menu « **Quitter** ».



Important !

Enregistrement des réglages :

Version logicielle <2.00.00

Lorsque vous effectuez des modifications en mode Installateur, l'application Secvest enregistre ces modifications dans la mémoire temporaire jusqu'à ce que vous quittiez le mode Installateur.

Lorsque vous quittez le mode Installateur, la centrale enregistre ces modifications dans une mémoire permanente.

Si vous coupez totalement l'alimentation de la centrale **AVANT** d'avoir quitté le mode Installateur, toutes les modifications de la centrale sont perdues.

Cela ne s'applique pas lorsque vous rétablissez la programmation Usine ; cette modification est immédiatement prise en compte.

Version logicielle >=2.00.00

Lorsque vous effectuez des modifications en mode Installateur, après confirmation, elles sont directement écrites dans la mémoire permanente de la Secvest.

Elles sont également conservées même en cas de panne de courant avant la fermeture du mode Installateur.



Important !

Fonction de déconnexion automatique :

Basée sur la fonction de déconnexion automatique de la Secvest, celle-ci intervient désormais aussi dans l'interface Web et l'application Secvest.

- L'installateur ou un utilisateur de niveau 4 est connecté dans l'interface Web. En cas d'inactivité, la déconnexion intervient automatiquement au bout d'**1 heure**.
- Application iOS / Android : Conformément à la norme VdS 3169, en l'absence de saisie l'application ouverte est fermée au bout de 4:15 minutes
 - (si l'option « Mémoriser le PIN » est paramétrée sur Non).
- Un utilisateur normal ou l'administrateur est connecté. En cas d'inactivité, la déconnexion intervient automatiquement au bout d'**1 minute**.



Important !

Horaires activation/désactivation, calendrier hebdomadaire

Veillez vous renseigner auprès de l'utilisateur de la centrale concernant un calendrier éventuellement programmé dans le menu utilisateur.

Si la centrale se trouve en mode Installateur, les événements planifiés sont décalés. Ils NE sont PAS annulés. Les événements en attente sont exécutés à la sortie du mode Installateur.

Cela signifie qu'après avoir quitté le mode Installateur, la centrale passe à l'état souhaité et programmé par l'utilisateur pour cet horaire.

Programmation/configuration

Remarques

Consultez le manuel d'utilisateur pour connaître les détails relatifs à l'activation et à la désactivation du système, sur le comportement de la centrale et l'affichage (interface utilisateur).

La centrale d'alarme sans fil se programme/configure en mode Installateur.

Il existe deux méthodes pour programmer/configurer la centrale d'alarme sans fil :

- Via le panneau de commande directement sur la centrale d'alarme sans fil.
- Via le navigateur Internet du serveur Web intégré.

La section suivante décrit uniquement la programmation/configuration de la centrale d'alarme sans fil via le serveur Web intégré.

Le serveur Web intégré permet d'effectuer tous les réglages de la centrale d'alarme sans fil à partir d'un simple navigateur Internet.

Version logicielle < 2.00.00

La configuration/programmation des périphériques (sans fil) s'effectue directement sur la centrale d'alarme sans fil.

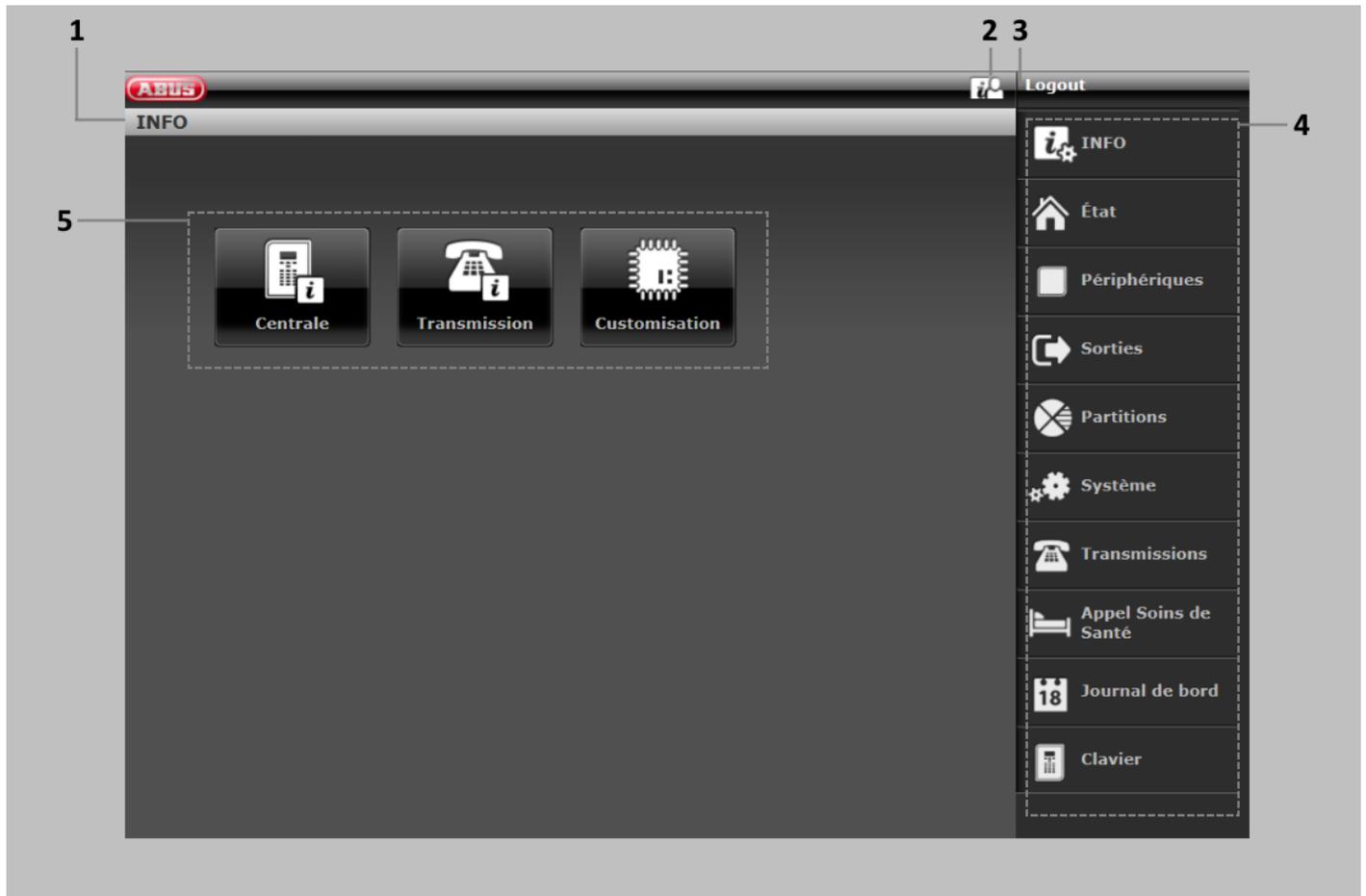
Version logicielle >= 2.00.00

La configuration/programmation des périphériques (sans fil) peut s'effectuer directement sur la centrale d'alarme sans fil ou via le serveur Web.

Consultez également la section « Valeurs par défaut / Programmation Usine » en annexe.

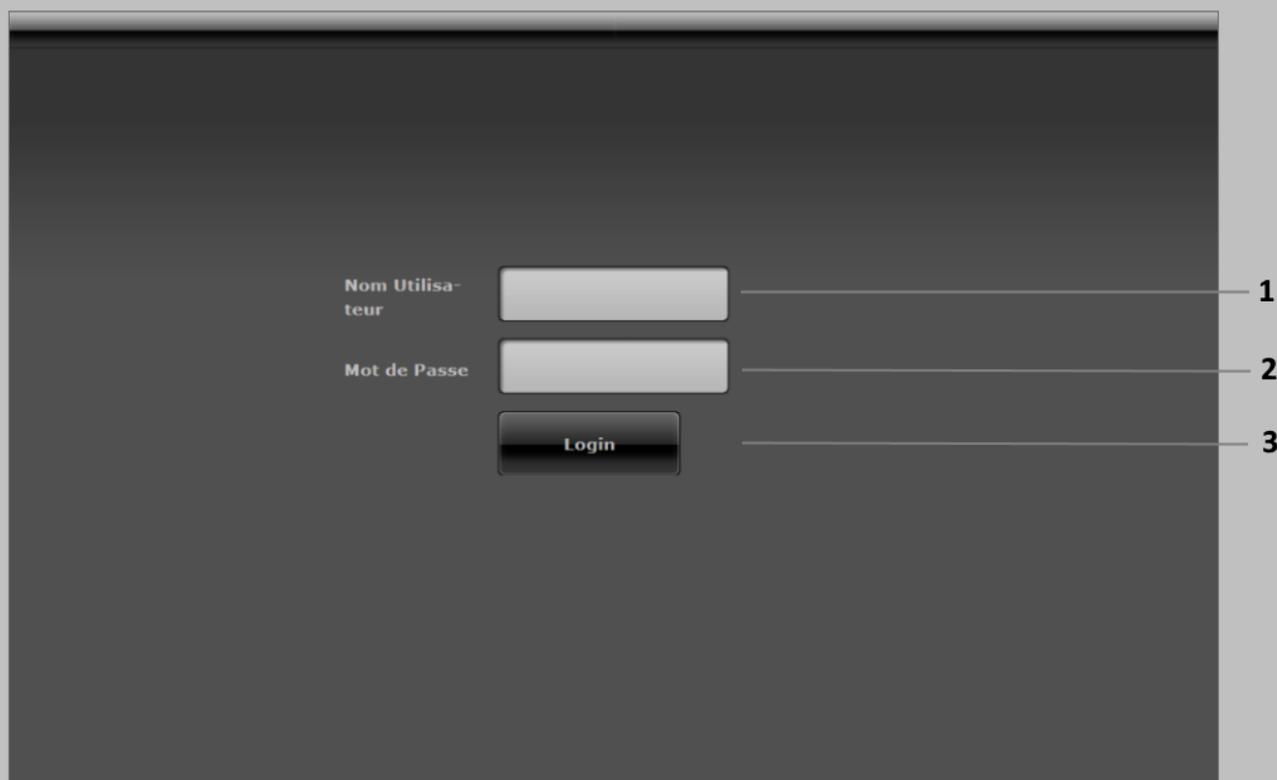
Ce paragraphe contient des informations de référence sur les options disponibles dans le mode Installateur.

Éléments de commande des menus



N°	Désignation/fonction	N°	Désignation/fonction
1	Barre d'informations <ul style="list-style-type: none"> Menu principal actif, ici : "Info" avec d'autres sous-menus 	4	Liste des menus principaux <ul style="list-style-type: none"> Les menus principaux s'affichent
2	Bouton de l'aide en ligne <ul style="list-style-type: none"> Cliquez sur ce bouton pour ouvrir la documentation actuelle au format PDF. Cette documentation peut également être enregistrée localement. 	5	Liste des sous-menus <ul style="list-style-type: none"> Les sous-menus du menu principal actif s'affichent Cliquez sur le sous-menu pour le développer et accéder aux réglages
3	Bouton de déconnexion <ul style="list-style-type: none"> Cliquez sur le bouton pour déconnecter l'utilisateur de la centrale. 		

Écran d'authentification



N°	Désignation/fonction	N°	Désignation/fonction
1	Champ de saisie du nom d'utilisateur <ul style="list-style-type: none"> Entrez le nom de l'installateur. Veillez à respecter la casse. 	3	Bouton de connexion
2	Champ de saisie du mot de passe <ul style="list-style-type: none"> Entrez le mot de passe d'installateur Remarque pour les versions logicielles < 1.01.00 Le mot de passe d'installateur par défaut est 9999(99). Veillez à respecter la casse. 		



Remarque

Vous êtes déconnecté automatiquement au bout de 15 minutes d'inactivité.
Vous devez alors ressaisir vos identifiants.

Menu principal



N°	Désignation/Fonction	P.	N°	Désignation/fonction	P.
1	INFO Informations générales sur : <ul style="list-style-type: none"> • la centrale (état du logiciel et du matériel) • la transmission • le module hybride • la personnalisation du client (customisation) 	51	4	Sorties Vue d'ensemble/configuration des sorties : <ul style="list-style-type: none"> • Sorties sans fil • Sorties filaires • Sorties MoHy • Sorties mixtes 	107
2	État Informations sur l'état des partitions du système d'alarme	62	5	Partitions Vue d'ensemble/configuration des partitions	124
3	Composants Vue d'ensemble/configuration des périphériques : <ul style="list-style-type: none"> • Zones IP • Zones sans fil • Zones filaires • Zones MoHy • Clavier de commande sans fil • Sirènes extérieures, sirènes sans fil, sirènes filaires • Module d'info/sirène d'intérieur • WAM • Verrous de porte • Répéteur RF • Module hybride • Générateur de signal intérieur 	63	6	Système Vue d'ensemble/configuration de la centrale d'alarme : <ul style="list-style-type: none"> • Généralités • Installateur détails • Accès utilisateur • RAZ utilisateur • Confirmation • Hardware • Réglages de sécurité • Sauvegarder/Restaurer • Mise à niveau logicielle de la centrale < 1.01.00 • Rapport 	150

Programmation/configuration

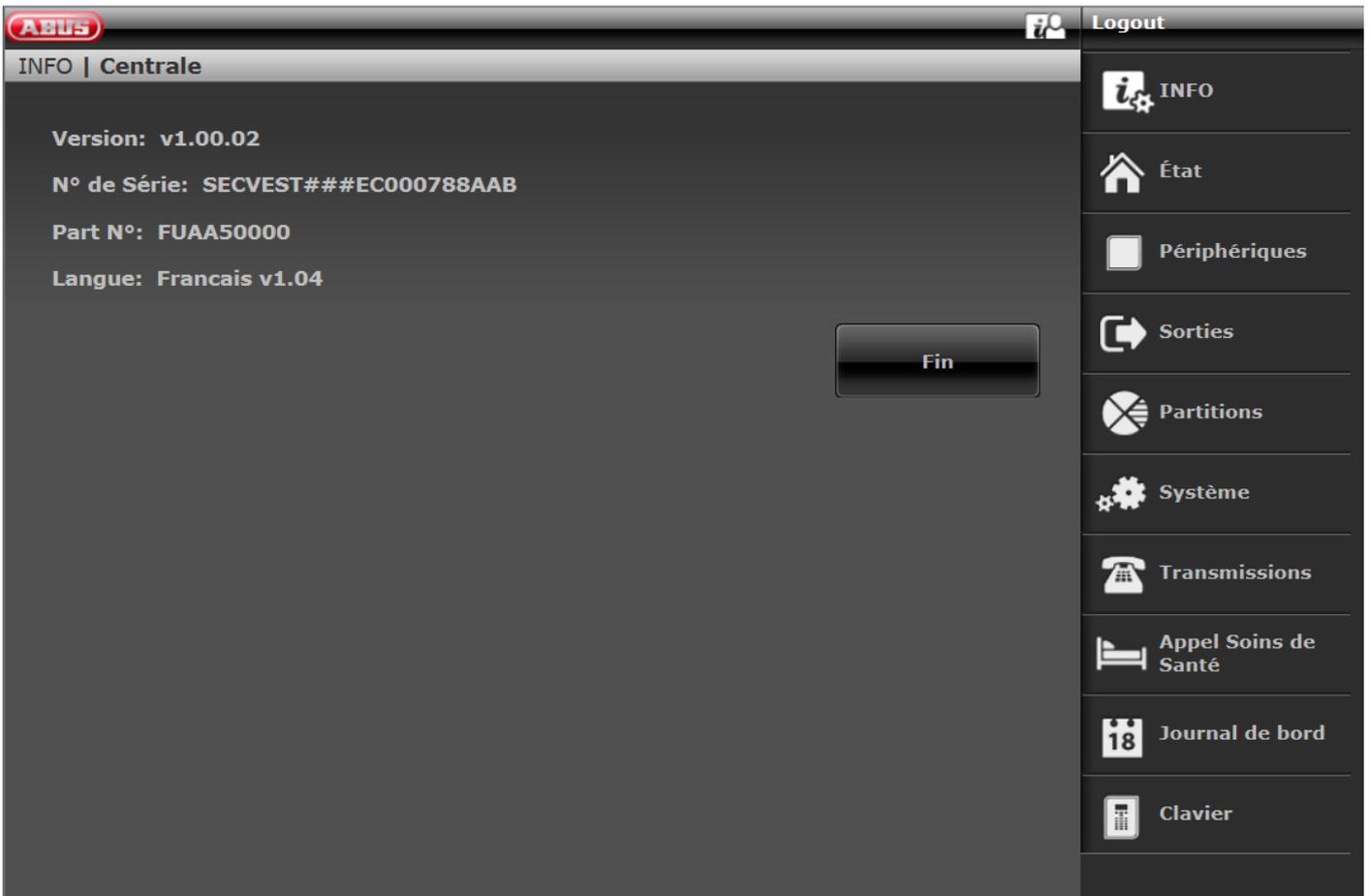
N°	Désignation/Fonction	P.	N°	Désignation/fonction	P.
7	Communication Vue d'ensemble/Configuration des interfaces de communication et des types de transmission <ul style="list-style-type: none">• Réseau• TS Reporting• Appel d'urgence de soin• Transmetteur vocal• SMS• E-mail• options de communication• Contacts	201	9	Historique Vue d'ensemble des défauts, des événements et des actions sur tous les périphériques de la centrale d'alarme	302
8	Appel d'urgence de soin Vue d'ensemble/configuration de l'appel d'urgence de soin	234	10	Clavier virtuel/clavier Clavier virtuel de la Secvest. S'utilise comme le clavier en façade de la Secvest.	
X	Test Vue d'ensemble/Exécution de toutes les fonctions de test possibles				

Info



Centrale

Version logicielle <2.00.00



Désignation/Fonction	Explication
Version	Numéro de version du logiciel actuellement installé dans le système d'alarme.
N° de série	Numéro de série du système d'alarme
Réf. art.	Référence du système d'alarme
Langue	Numéro de version de la langue réglée

ABUS Logout

INFO | Centrale

Version: v2.01.07 Langue: Français v1.11
 N° de Série: SECVEST###GC028819AAB Part N°: FUA50000
 Appareil RF Exclusivité: Non
 Heure Centrale: 09:54 Date: 12/06/2017 Date & Heure
 Zones: Disponible: 58 Utilisé: IP: 0 RADIO: 5 Filaire: 0
 Claviers Radio: 2 Sirs Radio: 1
 MAWs: 0 Serrures porte: 2
 Partitions: 1
 Sorties: Disponible: 36 Utilisé: RADIO: 0 Filaire: 0
 sabotage boîtier centrale: Non Sabotage Sirène: Non RF Brouillage: Non
 Défaut 220V centrale: **Oui** Défaut DC Externe Non
 Ext. Tension DC In: 14.2V
 État Batt.1: 8.2V État Batt.2: Bloqué
 Auxiliaire: 14.1V

Fin

- INFO
- État
- Périphériques
- Sorties
- Partitions
- Système
- Transmissions
- Appel Soins de Santé
- Test
- 18 Journal de bord
- Clavier

Désignation/Fonction	Explication
Version, langue	Numéro de version du logiciel actuellement installé dans le système d'alarme. Numéro de version de la langue réglée
N° de série	Numéro de série du système d'alarme
Part. N°	Référence du système d'alarme
RF Device Exclusivity	Oui Il est possible d'ajouter uniquement de nouveaux périphériques sans fil en vente depuis 2015, par ex. FUMK500XX. Non Il est possible d'ajouter tous les périphériques sans fil, par ex. les détecteurs d'installations existantes comme FU8320.
Heure de la centrale d'alarme, date	Heure et date actuelles de la centrale d'alarme
Date et heure	Synchronise la date et l'heure de la centrale d'alarme avec la date et l'heure du PC, par un clic
Zones	Vue d'ensemble des zones d'alarme disponibles et programmées Zones IP (IP), zones sans fil (SANS FIL), zones filaires à la centrale (FILAIRE), zones MoHy (M/H)
Sirènes sans fil	Nombre de composants utilisés
Générateur de signal int.	Nombre de composants utilisés
Répéteur RF	Nombre de composants utilisés
Clavier de commande sans fil	Nombre de composants utilisés
WAM	Nombre de composants utilisés
Verrous de porte	Nombre de composants utilisés
Modules hybrides	Nombre de composants utilisés
Partitions	Nombre de partitions utilisées

Sorties	Vue d'ensemble des sorties disponibles et programmées Sorties sans fil (SANS FIL), sorties filaires à la centrale (FILAIRE), sorties MoHy (M/H)
Sabo. boîtier	Indique si le contact anti-sabotage de l'avant du boîtier ou si le contact anti-sabotage mural s'est déclenché
Sabo. sirène	Indique si le contact anti-sabotage de la sirène filaire raccordée s'est déclenché (entrée TR de la centrale)
RF Brouillage	Indique si la centrale d'alarme a détecté un brouillage RF
Défaut CA centrale d'alarme	Indique si une alimentation 230 V est reliée à la centrale d'alarme ou si une anomalie a été détectée
Anomalie CC externe	Indique si une alimentation en courant continu 13,8 V externe est reliée à la centrale d'alarme ou si une anomalie a été détectée.
Tension d'entrée CC DC In - U	Indique la tension de l'alimentation en courant continu externe
État Batt.	État de la batterie correspondante (le cas échéant avec tension)
Auxiliaire	Tension de sortie aux bornes de la sortie de tension

Version logicielle >= 3.00.05

ABUS Abmelden

Info | Zentrale

Version: v3.00.05 Sprache: Deutsch v1.29
 Serien Nr.: SECVEST###GC028819AAB Part No.: FUAA50000
 RF Device Exclusivity: Nein
 Uhrzeit Zentrale: 10:50 Datum: 08/03/2018 Datum & Uhrzeit
 Zonen: Verfügbar: 58 Verwendet: IP: 0 FUNK: 4 VERDRAHTET: 0
 Funk Sirenen: 0 Indoor Sounders: 1 RF Repeater: 0
 Funk Bedienteil: 0 UVM: 0 Türschlösser: 0
 Teilbereiche: 2
 Ausgänge: Verfügbar: 36 Verwendet: FUNK: 0 VERDRAHTET: 1
 Gehäusefront Sabo: Nein Schallgeber Sabo: Nein RF Jamming: Nein
 AC Störung Zentrale: Ja Externe DC Störung Nein
 Ext. DC Voltage In: 14.3V
 Akku 1 Status: 8.2V Akku 2 Status: Gesperrt
 Auxiliary: 14.1V

Schließen

- Info
- Status
- Komponenten
- Ausgänge
- Teilbereiche
- System**
- Kommunikation
- Pflegenotruf
- Test
- Logbuch
- Tastatur

Version logicielle >= 3.01.14

The screenshot displays the ABUS software interface. At the top left is the ABUS logo. The main content area shows system information for a central unit (Zentrale). On the right side, there is a vertical navigation menu with various icons and labels. At the bottom right of the main area is a 'Schließen' (Close) button.

ABUS Abmelden

Info | Zentrale

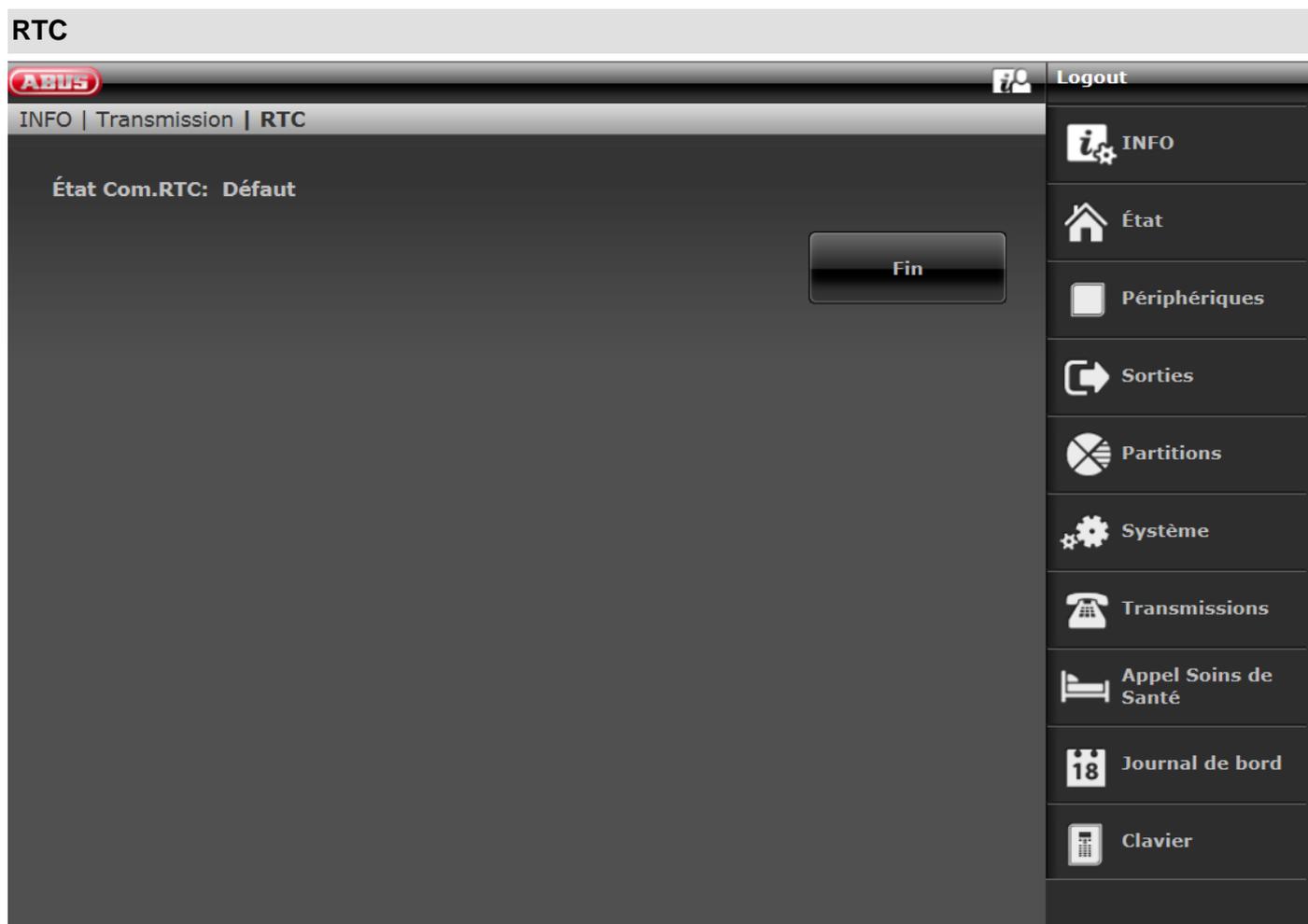
Version: v3.01.14 Sprache: Deutsch v1.40
Serien Nr.: SECVEST###GC028819AAB Part No.: FUA50000
RF Device Exclusivity: Nein
Uhrzeit Zentrale: 11:04 Datum: 23/04/2019 Datum & Uhrzeit
Zonen: Verfügbar: 73 Verwendet: IP: 2 FUNK: 10 VERDRAHTET: 1 H/M: 13
Funk Sirenen: 1 Innen-SG: 4 RF Repeater: 1
Funk Bedienteil: 1 UVM: 0 Türschlösser: 1 Hybrid Module: 2
Teilbereiche: 4
Ausgänge: Verfügbar: 44 Verwendet: FUNK: 2 VERDRAHTET: 3 H/M: 8
Gehäuse Sabo: Nein SG Sabo: Nein RF Jammung: Nein
AC Störung Zentrale: Ja Externe DC Störung Nein
Ext. DC In - U: 14.2V
Akku 1 Status: 8.1V Akku 2 Status: 8.1V
Auxiliar: 14.0V

Schließen

- Info
- Status
- Komponenten
- Ausgänge
- Teilbereiche
- System
- Kommunikation
- Pflegenotruf
- Test
- Logbuch
- Tastatur

Communication

The screenshot displays the 'Communication' configuration page in the ABUS system. At the top left, the 'ABUS' logo is visible. Below it, the page title 'Info | Kommunikation' is shown. The main content area features three large, dark buttons with white icons and labels: 'PSTN' (with a telephone icon), 'Ethernet' (with a network diagram icon), and 'Mobil' (with a mobile phone icon). On the right side, there is a vertical sidebar menu titled 'Abmelden' at the top. The menu items, from top to bottom, are: 'Info' (with an 'i' and gear icon), 'Status' (with a house icon), 'Komponenten' (with a square icon), 'Ausgänge' (with a right-pointing arrow icon), 'Teilbereiche' (with a circle and diagonal lines icon), 'System' (with a gear icon), 'Kommunikation' (with a telephone icon), 'Pflagenotruf' (with a bed icon), 'Test' (with a gear icon), 'Logbuch' (with a calendar icon showing '18'), and 'Tastatur' (with a keyboard icon).



Désignation/Fonction	Explication
État communication RTC	Consultation de l'état de la communication RTC. La Secvest vérifie la ligne téléphonique connectée. "OK" s'affiche. Si elle n'est pas connectée, activée ou est en dérangement, "Défaut" s'affiche.

Ethernet

ABUS
Logout

[INFO](#) | [Transmission](#) | [Ethernet](#)

Adresse MAC: 8C-11-CB-54-0C-1F

Adresse IP: 192.168.10.100 DHCP

Masque sous-réseau IP: 255.255.255.0 DHCP

Passerelle adresse IP: 192.168.10.10 DHCP

DNS Adresse IP primaire: 192.168.10.10 DHCP

INFO

État

Périphériques

Sorties

Partitions

Système

Transmissions

Appel Soins de Santé

Journal de bord

Clavier

Désignation/Fonction	Explication
Adresse MAC	Il s'agit de l'adresse matérielle de la carte réseau de la Secvest. Chaque adresse MAC est unique au monde.
Adresse IP	Si la Secvest fait partie d'un réseau, l'adresse IP s'affiche ici, par ex. 192.168.178.23. Si (DHCP) apparaît entre parenthèses juste après, cela signifie que la Secvest a automatiquement reçu son adresse IP, par exemple d'un serveur DHCP dans un routeur. Si elle ne fait pas partie d'un réseau, « 0.0.0.0 » apparaît ici.
Masque sous-réseau IP	Le masque de sous-réseau s'affiche ici. Dans un réseau privé, il s'agit en général de 255.255.255.0.
Passerelle adresse IP	Si la Secvest fait partie d'un réseau, l'adresse IP de la passerelle s'affiche ici. Le routeur, par ex. la Freebox, est un exemple de passerelle de réseau privé.
DNS adresse IP primaire	Il s'agit de l'adresse IP du « Domain Name System » (DNS).
État de la liaison IP (uniquement GUI)	Consultation de l'état Ethernet. La Secvest contrôle le câble LAN raccordé et son propre raccordement Ethernet. "OK" s'affiche. Si quelque chose n'est pas connecté, activé ou est perturbé, le message d'erreur « Défaut » s'affiche.

Mobile

Info | Kommunikation | SIERRA HL7692
Abmelden

Netzwerk: Reg. Home

Kunden-Nr.: +4915161721567

Signalstärke: : RSSI: 4 (G)

IMEI: 355465070121476

IMSI: 26201140656191

Version: RHL769x.2.23.172400.

Schließen

- Info
- Status
- Komponenten
- Ausgänge
- Teilbereiche
- System
- Kommunikation
- Pflegenotruf
- Test
- Logbuch
- Tastatur

Désignation/Fonction	Explication														
	<p>Remarque Ces menus s'affichent uniquement lorsqu'un module de téléphonie mobile avec une carte SIM active a été installé dans la centrale.</p>														
SIERRA HL7692	Fabricant et type du module de téléphonie mobile utilisé														
Réseau Puissance du signal	<p>Affichage si et comment une carte SIM est intégrée au réseau de téléphonie mobile.</p> <p>Exemple : Reg. Home RSSI : 4 (G)</p> <table border="1" style="width: 100%; border-collapse: collapse; margin-top: 10px;"> <tr> <td style="width: 20%;">« Not Reg. »</td> <td>Non enregistré ; le module ne recherche pas de réseau de téléphonie mobile.</td> </tr> <tr> <td>« Reg. Home »</td> <td>Enregistré ; réseau domestique (« Reg. Home » est remplacé par le nom du fournisseur d'accès dès que ce dernier est disponible).</td> </tr> <tr> <td>« Searching... »</td> <td>Non enregistré ; le module recherche un réseau de téléphonie mobile.</td> </tr> <tr> <td>« Reg. Denied »</td> <td>Enregistrement refusé</td> </tr> <tr> <td>« Reg. Unknown »</td> <td>Inconnu</td> </tr> <tr> <td>« Reg. Roam »</td> <td>Enregistré ; réseau en Roaming (« Reg. Roam » est remplacé par le nom du fournisseur d'accès en Roaming dès que ce dernier est disponible)</td> </tr> <tr> <td>RSSI</td> <td>Indique la puissance de la réception de téléphonie mobile, comme l'affichage par barres sur un smartphone. La plage de valeurs va de 0 (très mauvaise) à 9 (très bonne).</td> </tr> </table>	« Not Reg. »	Non enregistré ; le module ne recherche pas de réseau de téléphonie mobile.	« Reg. Home »	Enregistré ; réseau domestique (« Reg. Home » est remplacé par le nom du fournisseur d'accès dès que ce dernier est disponible).	« Searching... »	Non enregistré ; le module recherche un réseau de téléphonie mobile.	« Reg. Denied »	Enregistrement refusé	« Reg. Unknown »	Inconnu	« Reg. Roam »	Enregistré ; réseau en Roaming (« Reg. Roam » est remplacé par le nom du fournisseur d'accès en Roaming dès que ce dernier est disponible)	RSSI	Indique la puissance de la réception de téléphonie mobile, comme l'affichage par barres sur un smartphone. La plage de valeurs va de 0 (très mauvaise) à 9 (très bonne).
« Not Reg. »	Non enregistré ; le module ne recherche pas de réseau de téléphonie mobile.														
« Reg. Home »	Enregistré ; réseau domestique (« Reg. Home » est remplacé par le nom du fournisseur d'accès dès que ce dernier est disponible).														
« Searching... »	Non enregistré ; le module recherche un réseau de téléphonie mobile.														
« Reg. Denied »	Enregistrement refusé														
« Reg. Unknown »	Inconnu														
« Reg. Roam »	Enregistré ; réseau en Roaming (« Reg. Roam » est remplacé par le nom du fournisseur d'accès en Roaming dès que ce dernier est disponible)														
RSSI	Indique la puissance de la réception de téléphonie mobile, comme l'affichage par barres sur un smartphone. La plage de valeurs va de 0 (très mauvaise) à 9 (très bonne).														

	<p>La valeur entre parenthèses indique la disponibilité de la liaison de données.</p> <p>Disponibilité de la liaison de données :</p> <table border="1"> <tr> <td>« Sans »</td> <td>Uniquement réseau 2G disponible, langue, pas de données possible</td> </tr> <tr> <td>(G)</td> <td>Réseau GPRS disponible.</td> </tr> <tr> <td>(4G)</td> <td>Réseau LTE/4G disponible.</td> </tr> </table>	« Sans »	Uniquement réseau 2G disponible, langue, pas de données possible	(G)	Réseau GPRS disponible.	(4G)	Réseau LTE/4G disponible.
« Sans »	Uniquement réseau 2G disponible, langue, pas de données possible						
(G)	Réseau GPRS disponible.						
(4G)	Réseau LTE/4G disponible.						
IMEI	<p>L'International Mobile Station Equipment Identity (IMEI) est un numéro de série unique à 15 chiffres permettant d'identifier clairement les terminaux de téléphonie mobile.</p> <p>Ce numéro se trouve également directement sur le module.</p>						
N° de client	<p>Numéro de téléphone qui est affecté à la carte SIM.</p> <p></p> <p>Remarque</p> <p>L'affichage du numéro d'appel de la carte SIM ne se fait que si votre fournisseur d'accès a enregistré le numéro d'appel sur la carte SIM.</p>						
IMSI	<p>L'International Mobile Subscriber Identity (identité internationale d'abonné mobile) permet d'identifier clairement des abonnés des réseaux mobiles.</p>						
Adresse IP (uniquement GUI)	<p>Adresse IP du module de téléphonie mobile. Cette adresse IP est affectée de manière dynamique par le réseau de téléphonie mobile (2G/GPRS, 4G/LTE).</p>						
Version	<p>La version matérielle et logicielle du module de téléphonie mobile.</p>						
Réinitialisation (uniquement GUI)	<p>Le module de téléphonie mobile peut être réinitialisé ici sans couper l'alimentation de la centrale. Le module de téléphonie mobile se réenregistre à nouveau dans le réseau de téléphonie mobile.</p>						

Modules hybrides

Nummer	Name	Version
HyMo 1	"HyMo 1"	v1.03
HyMo 2	"HyMo 2"	v1.03

Désignation/Fonction	Explication
Numéro	Les numéros internes des modules hybrides
Nom	Les noms univoques programmés des modules hybrides
Version	La version logicielle de chaque module hybride

Customisation
Logout

ABUS
INFO | Customisation

SVP code pour customisation Centrale:

E002589AB9C75F43

SVP entrer code:

Envoyer

- INFO
- État
- Périphériques
- Sorties
- Partitions
- Système
- Transmissions
- Appel Soins de Santé
- Journal de bord
- Clavier

Désignation/Fonction	Explication
Please offer... ->	Identification de la centrale d'alarme sans fil (nécessaire pour la clé de la licence)
Please enter code	Champ de saisie de la clé de la licence pour personnaliser la centrale d'alarme (par exemple variantes de langue)

Remarque
 La personnalisation via ce menu est actuellement possible uniquement pour des applications spéciales en accord avec le département Vente ou l'assistance.

État

N°	Désignation/Fonction	N°	Désignation/fonction
1	Sélection de partition Champs de sélection/onglets pour chaque partition. <ul style="list-style-type: none"> • Une alarme confirmée par l'utilisateur, mais qui n'est pas réinitialisée, apparaît sous forme de symbole de mise en garde dans la partition correspondante. • Cliquez sur le symbole de mise en garde pour réinitialiser l'alarme. 	2	Affichage d'état L'affichage d'état fournit des informations notamment sur : <ul style="list-style-type: none"> • les défauts présents dans une partition • défauts inter-partition (par ex. « Défaut CC ext. ») • les zones ouvertes (inter-partition)

Uniquement pour l'écran de la centrale

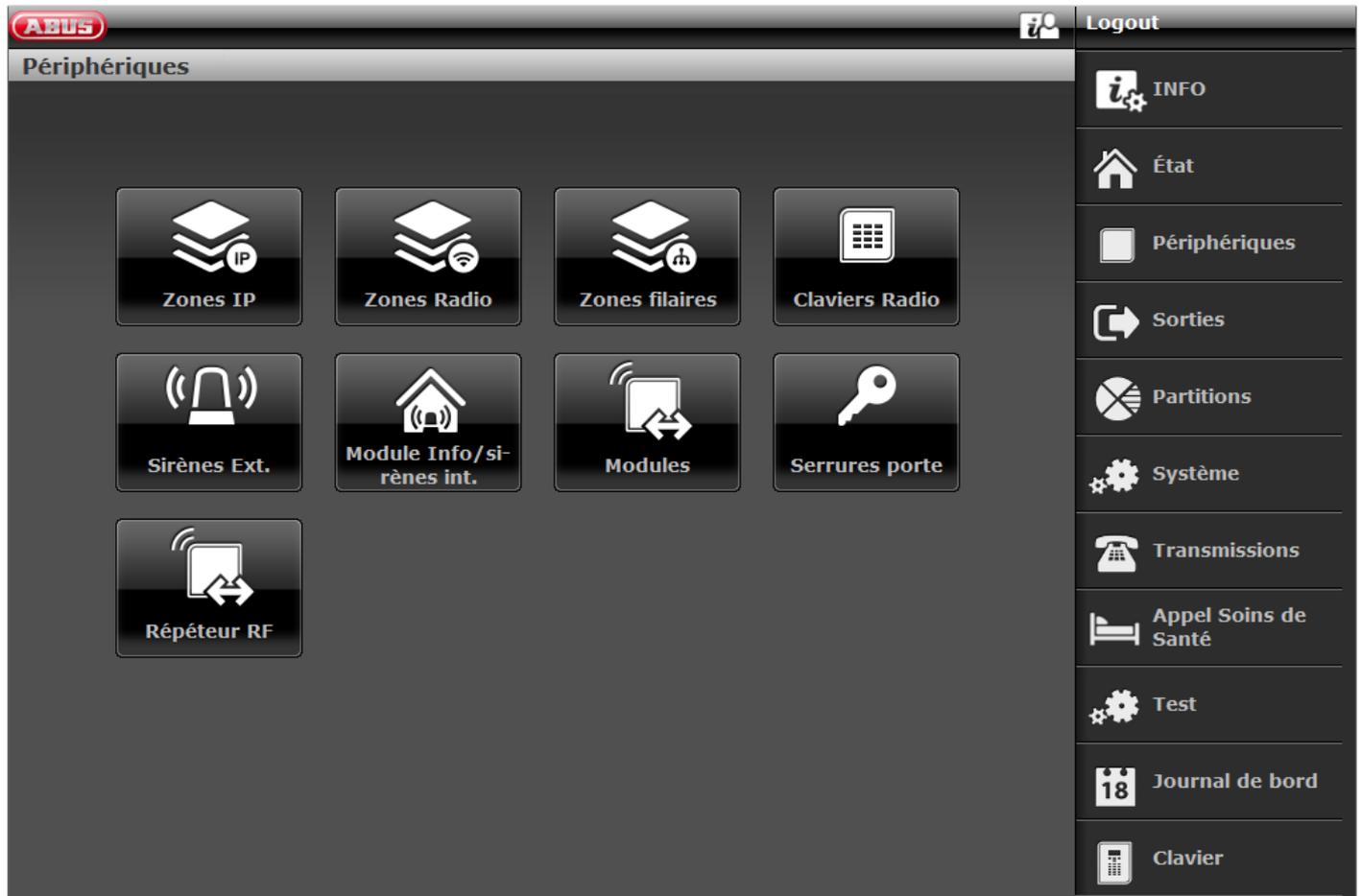


Remarque :

Un triangle d'avertissement apparaît dans le coin inférieur droit de l'écran lorsque la centrale d'alarme a constaté un problème. L'explication (la description du problème) ne s'affiche pas, à moins qu'un code d'accès de niveau 2 (utilisateur) ou d'accès de niveau 3 (installateur) ne soit saisi. Après saisie d'un code valable, le message apparaît (problème, erreur, avertissement, alarme, etc.) en texte clair. Ce message est ensuite masqué après confirmation par un utilisateur. Le message disparaît automatiquement au bout d'une minute.

Composants

Programmation dans l'interface Web



Version logicielle >= 3.00.05

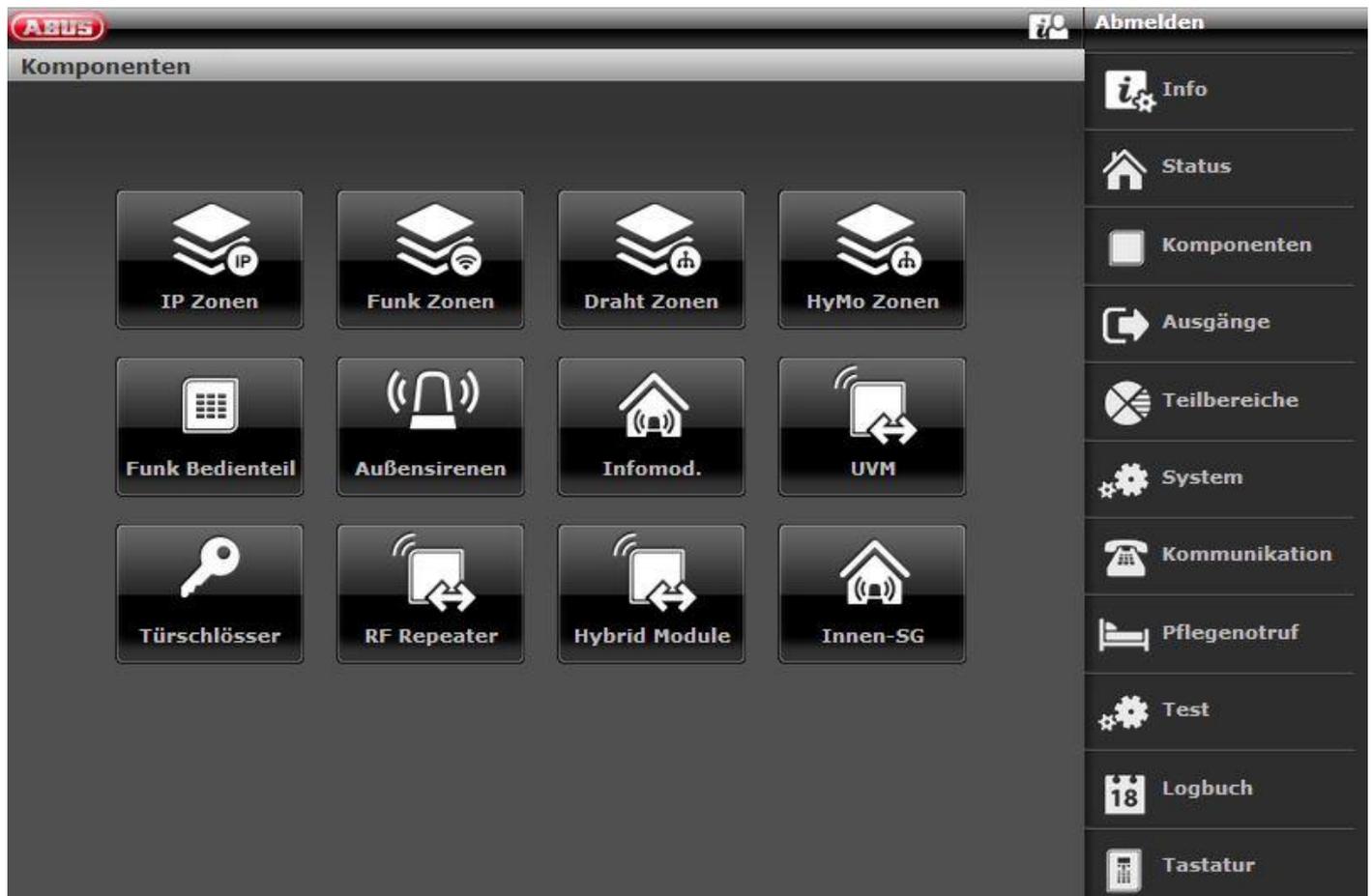
The screenshot displays the ABUS software interface for programming and configuration. The main area is titled "Komponenten" and features a grid of icons for various components:

- IP Zonen
- Funk Zonen
- Draht Zonen
- Funk Bedienteil
- Außensirenen
- Infomod.
- UVM
- Türschlösser
- RF Repeater
- Indoor Sounders

The sidebar on the right contains a menu with the following options:

- Abmelden
- Info
- Status
- Komponenten
- Ausgänge
- Teilbereiche
- System
- Kommunikation
- Pflegenotruf
- Test
- Logbuch
- Tastatur

Version logicielle >= 3.01.14



Remarque

À partir de la version logicielle 2.00.00, il est également possible de programmer les composants via l'interface Web. Pour cela, cliquez simplement sur une zone d'alarme ou une sirène non attribuée. Le système vous guide tout au long du processus de programmation. Après la programmation dans l'interface Web, il est impératif de définir le type de zone d'alarme !

La création d'une zone sans fil est présentée ici à titre d'exemple :

ABUS
Logout

Périphériques | Zones Radio | **Z204 RADIO**

Détecteur Ra-
dio appris: Non Ajouter

Type *Non Utilisé ▼ Nom Zone 204

Partitions 1 2 3 4

Annuler
Envoyer

INFO

État

Périphériques

Sorties

Partitions

Système

Transmissions

Appel Soins de Santé

Test

18 Journal de bord

Clavier

Désignation/Fonction	Explication
Nom	Nom de zone unique.
Partition	Partition de chaque zone
Type	Type de la zone sans fil
Propriétés	Vue d'ensemble des attributs de la zone sans fil correspondante

66

- Les zones IP « Attributs » sont masquées lorsque le « mode Trigger » de la caméra est réglé sur « Externe ».

Le document « ABUS_FUAA500xx_IPCx_Kameraintegration_Secvest_DE_1.01.00.pdf » contient des détails sur l'intégration des caméras de la série IPCx.

Compatibilité avec la gamme de caméras IPCx

- Intégration de jusqu'à 6 caméras
- Déclenchement externe de l'enregistrement d'images d'alarme et/ou de flux vidéo
- Les enregistrements de la caméra IPCxyyyyy sont stockés sur la carte SD intégrée de la caméra.
- Les enregistrements (vidéos/images) des caméras IPCxyyyyy peuvent être ouverts uniquement via le serveur Web de la caméra ou via l'application ABUS iDVR (et non via le journal de bord de la centrale).
- URL / lien vers la caméra dans le journal de bord pour tous les événements pour lesquels des enregistrements sont disponibles

Ajouter/Supprimer

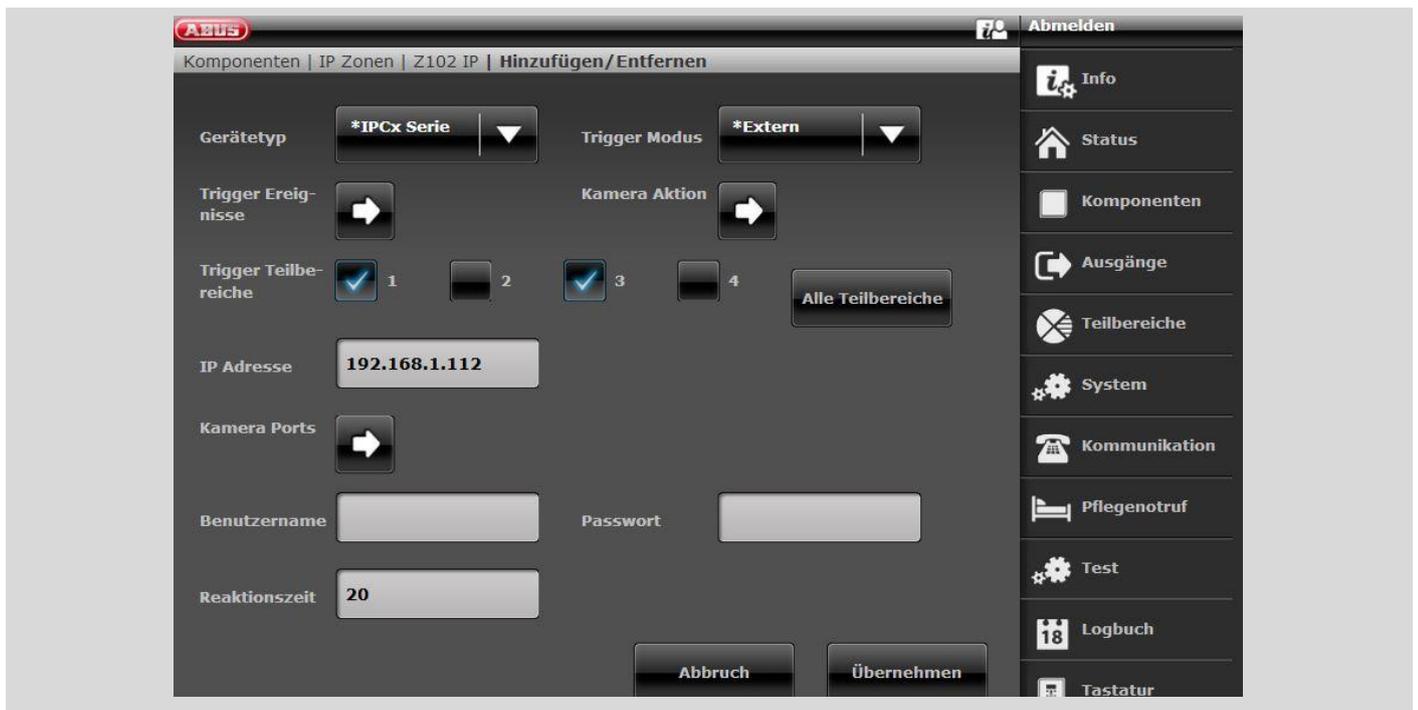
Sélectionnez la zone IP souhaitée dans le menu « Périphériques » → « Zones IP ». Le bouton « Ajouter/Supprimer... » permet d'accéder à l'écran suivant dans lequel s'effectue l'intégration :



The screenshot shows the 'Ajouter/Effacer' (Add/Delete) configuration screen for an IP camera in the ABUS system. The interface is dark-themed and includes a sidebar menu on the right with options like 'INFO', 'État', 'Périphériques', 'Sorties', 'Partitions', 'Système', 'Transmissions', 'Appel Soins de Santé', 'Test', 'Journal de bord', and 'Clavier'. The main configuration area contains the following fields and controls:

- Type Périph.**: *Plage IPCx (dropdown menu)
- Mode Trigger**: *Externe (dropdown menu)
- Trigger Événements**: Arrow button pointing right
- Action de la caméra**: Arrow button pointing right
- Trigger Partitions**: Four checkboxes labeled 1, 2, 3, and 4. Checkbox 1 is checked. A 'Toutes Partitions' button is also present.
- Adresse IP**: 192.168.0.20
- HTTP Port Interne**: 80
- RTSP Port Interne**: 554
- HTTP Port Externe**: 10311
- RTSP Port Externe**: 10311
- Nom Utilisateur**: root
- Mot de Passe**: (empty field)

At the bottom of the configuration area are two buttons: 'Annuler' (Cancel) and 'Envoyer' (Send).



Désignation/Fonction	Explication
Type de périphérique	Caméra TVIP41550 Série IPCx
Mode Trigger	<p>Interne TVIP41550 uniquement La caméra enregistre les images dès que le capteur PIR intégré se déclenche.</p> <p>Externe La caméra enregistre les images ou vidéos (série IPCx) dès que l'un des événements déclencheurs définis survient au niveau de la centrale.</p> <p>Int. + Ext. TVIP41550 uniquement La caméra enregistre les images dès que le capteur PIR intégré se déclenche ou l'un des événements déclencheurs définis survient au niveau de la centrale d'alarme.</p>
Trigger événements	(uniquement en mode Trigger "Externe" ou "Int. + Ext.") Événements pour lesquels la caméra doit enregistrer des images ou vidéos (série IPCx).

Einbruchalarm	<input checked="" type="checkbox"/>	Perimeter Warnung	<input checked="" type="checkbox"/>
Überfallalarm	<input checked="" type="checkbox"/>	Bedrohungscode	<input type="checkbox"/>
Feuer	<input checked="" type="checkbox"/>	Technik	<input checked="" type="checkbox"/>
24 h Alarm	<input type="checkbox"/>	Medizin. Alarm	<input checked="" type="checkbox"/>
Pflege-Notfall	<input checked="" type="checkbox"/>	Inaktivität Pflege	<input checked="" type="checkbox"/>
Sabotagen	<input checked="" type="checkbox"/>	Alle Aktiv	<input type="checkbox"/>
Intern Aktiv	<input type="checkbox"/>	Deaktiv	<input type="checkbox"/>
Zone folgend	<input type="checkbox"/>		
Zonen	<input type="button" value="→"/>		
<input type="button" value="Abbruch"/>		<input type="button" value="Übernehmen"/>	

Action de la caméra

uniquement dans la série IPCx
Des images et/ou vidéos doivent être enregistrées.

Videos	<input checked="" type="checkbox"/>	Bilder	<input checked="" type="checkbox"/>
<input type="button" value="Abbruch"/>		<input type="button" value="Übernehmen"/>	

Trigger partitions

(uniquement en mode Trigger "Externe" ou "Int. + Ext.")
Partitions à surveiller si des événements déclencheurs surviennent.

Adresse IP

Adresse IP de la caméra dans le réseau interne

<p>Ports caméra</p>	
<p>HTTP Port Interne</p>	<p>Port HTTP de la caméra dans le réseau interne (réglage par défaut : « 80 »)</p>
<p>HTTP Port Externe</p>	<p>Port HTTP externe pour lequel la redirection de port est configurée dans le routeur.</p>
<p>RTSP Port Interne</p>	<p>Port RTSP de la caméra dans le réseau interne (réglage par défaut : « 554 »)</p>
<p>RTSP Port Externe</p>	<p>Port RTSP externe pour lequel la redirection de port est configurée dans le routeur.</p>
<p>Nom d'utilisateur</p>	<p>TVIP Réglage par défaut « Root » Version logicielle >= 1.01.00 : aucun nom d'utilisateur n'est attribué</p>  <p>Danger Caméras IP, par ex. IPCB42500A Utilisez des noms d'utilisateur du « niveau Installateur » de la caméra. Ainsi, le système obtient l'accès à la carte SD en cas d'alarme. Les noms d'utilisateur du « niveau Master » de la caméra n'ont pas d'accès à la carte SD.</p>
<p>Mot de passe</p>	<p>Réglage par défaut : aucun mot de passe attribué</p>
<p>Temps de réponse</p>	<p>Indique la durée maximale pendant laquelle la centrale attend les réponses d'ordre de la caméra. Si le temps de réponse dépasse cette durée réglée, un message d'erreur est généré. Configuration par défaut – 20 s, plage de 1 s à 99 s</p>

Appliquez les réglages avec le bouton "Envoyer".

Attribution d'un nom de zone

 **Remarque**
Il peut être utile d'attribuer un nom de zone unique afin de pouvoir identifier plus rapidement le détecteur concerné en cas de défaut.
Par ex. DM pour détecteur de mouvement et le lieu :
Bureau01, nom du détecteur : **DM-Bureau01**

1. Cliquez dans la zone de texte **Nom**.
2. Supprimez le nom prédéfini (Zone 01).
3. Attribuez à la zone un nom unique comprenant 12 caractères maximum.
4. Confirmez le nouveau nom après avoir terminé la configuration en cliquant sur **Envoyer**.

Sélection du type de zone



Remarque

Vous pouvez modifier ici le type de zone prédéfini. Tenez compte de la description des types de zone de cette section.
Une **zone** désigne un **détecteur** programmé dans la **centrale d'alarme sans fil**.

Les zones peuvent posséder des attributs très variés.

Le détecteur ne sait pas si la centrale d'alarme sans fil est activée ou non.

C'est pourquoi un détecteur envoie toujours une alarme à la centrale d'alarme s'il enregistre un changement.

La centrale d'alarme sans fil décide ensuite si ce message entraîne une réponse alarme ou non.

1. Sélectionnez l'option de menu **Type**



Remarque

Veillez à maintenir l'état d'une zone (ouverte ou fermée) pendant au moins > 400 ms, afin que la centrale puisse détecter avec garantie la modification d'état.

EN 50131-1 chapitre 8.9.1 Détection de cambriolage, sabotage, déclenchement et détection de défauts – exigences de temps : « Les signaux de cambriolage, d'agression et de sabotage d'une durée active d'au moins 400 ms doivent être traités. »

Type	Explication
Non utilisé	Une zone pour laquelle aucun détecteur sans fil n'est programmé ou une zone dont l'entrée n'est reliée à aucun détecteur et n'est donc pas utilisée doit être programmée comme "Non utilisée". La centrale d'alarme ne répond pas lorsqu'un événement active ce détecteur.
Alarme immédiate tempo sortie	Lorsque la centrale d'alarme sans fil est activée, cette zone déclenche directement une alarme lorsqu'un détecteur sans fil envoie une modification à la centrale d'alarme sans fil ou si l'état de la zone d'alarme change. (par ex. ouverture du contact d'alarme).
	 Remarque Type de zone "Alarme immédiate tempo sortie" avec fonction supplémentaire de surveillance de l'effet levier pour les produits mécatroniques ABUS, comme le verrou de crémone de fenêtre FOS 550 E, la serrure de porte supplémentaire ou protection de fenêtre FOS 400 E. Si vous utilisez un produit mécatronique conçu pour la Secvest, programmez le type de zone "Alarme immédiate tempo sortie" dans la centrale d'alarme. Lorsque la centrale d'alarme est désactivée, on surveille les tentatives d'effraction et d'ouverture de ces détecteurs. Pour ce faire, la fenêtre doit être fermée et la sécurité verrouillée. La surveillance démarre 30 secondes après le verrouillage, délai nécessaire à l'opération d'auto-calibrage. Lorsque la protection supplémentaire mécatronique est déverrouillée, la surveillance cesse. En cas de tentative d'ouverture de la fenêtre sans déverrouillage préalable de la protection supplémentaire, le mouvement du battant de fenêtre peut déclencher une alarme. La surveillance de l'effet levier peut être désactivée dans les attributs (voir ci-dessous Attributs de zone). Il est possible de raccorder également un détecteur de bris de glace passif à certains produits mécatroniques. Si ce détecteur identifie un bris de glace, la centrale d'alarme émet toujours une réponse alarme. La centrale d'alarme exécute les actions prévues à l'état activé ou désactivé.
Blocage zone	La zone doit être fermée pour activer ou activer en interne la centrale d'alarme sans fil. Lorsque la centrale d'alarme sans fil est activée ou activée en interne, l'ouverture de cette zone ne déclenche pas d'alarme. Cette zone s'utilise avec des contacts de verrouillage.
	 Remarque A été utilisé en tant qu'attribut de zone dans la Secvest 2WAY et non pas en tant que type de zone.

Type	Explication
Alarme immédiate entrée/sortie	Une zone programmée en tant qu'alarme immédiate entrée/sortie se comporte comme une zone "Alarme immédiate tempo sortie". Une zone de ce type donne cependant l'alerte dès que le détecteur se déclenche pendant le temps de sortie.
Alarme agression	Cette zone déclenche toujours une alarme. Que la centrale d'alarme anti-effraction soit active ou non. Une alarme agression peut également être transmise silencieusement (communication). Le menu de programmation ne peut être quitté que lorsque cette zone est fermée. Programmez le bouton radio ou mural agression sur cette zone.
Incendie	<p>Cette zone déclenche toujours une alarme. Que la centrale d'alarme anti-effraction soit active ou non. L'alerte est donnée via le générateur de signal dans la centrale d'alarme sans fil, à la sirène extérieure et à d'autres générateurs de signal sous forme de tonalités d'alarme incendie impulsées. Programmez uniquement les détecteurs autonomes avertisseurs de fumée ou boutons d'alarme incendie sur cette zone.</p> <p>Cette zone déclenche toujours une communication lorsque celle-ci est autorisée.</p>  <p>Remarque concernant Partition -> Réponse alarme Le type de zone Feu, les doubles touches Feu sur la centrale et les doubles touches Feu sur le clavier de commande déclenchent toujours un reporting CRA/STS lorsque le mode d'appel pour reporting CRA/STS a été autorisé et lorsque le groupe « Feu » est autorisé pour des événements CID/SIA. Exemple : Partition X -> Réponse alarme -> Sirène Transmission de l'alarme incendie à CRA/STS</p>
Alarme 24 h	Cette zone déclenche toujours une alarme immédiate. Lorsque la centrale d'alarme sans fil est désactivée, l'alerte est d'abord donnée par le buzzer intégré dans la centrale d'alarme. À l'état activé, la sortie sirènes est également activée. Si une zone 24 h est bloquée, ceci ne s'applique qu'à l'état désactivé.
Périmètre d'avertissement	<p>Lorsque la centrale d'alarme est activée totalement ou en interne, cette zone déclenche une préalerte. La centrale d'alarme émet 2 bips toutes les 5 secondes. Toutes les 5 secondes, l'écran affiche "Périmètre d'avertiss.". Programmez par ex. les détecteurs de mouvement extérieurs sur cette zone.</p> <p>Les sirènes extérieures radio clignotent et bipent pendant environ 1 s toutes les 5 s. Le module d'information bipe toutes les secondes et la LED d'alarme rouge s'allume. La sirène d'intérieur sonne toutes les secondes. Elle doit toutefois être raccordée à un bloc d'alimentation et le fil jarretière "Uniquement alarme" ne doit pas être branché. (Il s'agit d'une tonalité d'information et non d'une alarme). La durée des signaux est de 30 s. Une sortie de type « Périmètre d'avertiss. » est activée pendant 30 secondes. S'il est programmé, seul le carillon de la porte retentit lorsque l'installation est désactivée.</p>
Entrée/sortie	Cette zone déclenche une alarme à l'issue d'un délai défini (temporisation d'entrée) lorsque la centrale d'alarme est activée. Utilisez ce type de zone, par ex. pour le détecteur d'ouverture de votre porte d'entrée. Lorsque vous quittez les lieux, la fermeture de cette zone peut également servir à mettre fin à la temporisation de sortie. Ce détecteur peut être utilisé en tant qu'alarme immédiate tempo sortie en cas d'activation interne.
Route d'entrée	Cette zone ne déclenche pas d'alarme si une zone d'entrée/sortie a activé au préalable la temporisation d'entrée. Une alarme immédiate se déclenche si aucune temporisation d'entrée n'a été activée au préalable. Utilisez ce type de zone par ex. pour un détecteur de mouvement situé dans le couloir d'entrée et orienté vers la porte d'entrée (équipée d'un détecteur d'ouverture). Ce détecteur peut être utilisé en tant que détecteur "Entrée/sortie" en cas d'activation interne. Cette zone peut être ouverte en quittant le menu de programmation.

Type	Explication
Technique	<p>Une zone technique déclenche une alarme et une transmission à l'état désactivé. À l'état activé, seule la transmission s'effectue mais aucune alarme n'est déclenchée. Si une alarme se déclenche à l'état activé dans cette zone, elle s'afficherait lors de la désactivation de la centrale d'alarme. Utilisez ce type de zone, par ex. pour des détecteurs d'inondation. Le module d'information sans fil et la sirène d'intérieur sans fil signalent les alarmes techniques, comme la centrale d'alarme, à l'aide de bips.</p>
Interrupteur à clé impulsion	<p>Programmez un interrupteur à clé (impulsion) sur la centrale d'alarme sans fil. Toute modification de cette zone a pour effet de faire passer la centrale d'alarme de l'état actif à l'état inactif ou vice-versa (selon le mode de sortie programmé).</p> <p> Remarque Des interrupteurs à clé peuvent également faire office de sorties d'application dans le contrôle d'accès et dans la domotique.</p> <p> Remarque Avec la caractéristique de zone « Surveillance interne » = On, toute modification de cette zone a pour effet de faire passer la centrale d'alarme de l'état actif en interne à l'état inactif ou vice-versa (selon le mode de sortie programmé).</p> <p> Remarque La caractéristique « Inversé » (uniquement pour les zones filaires) inverse le comportement de cette zone.</p> <p> Remarque Pour les zones filaires de ce type, effectuez également une surveillance anti-sabotage de câble, en particulier pour les applications dans le contrôle d'accès et dans la domotique. L'utilisateur ne peut pas réinitialiser le système depuis une zone d'interrupteur à clé.</p>
Interrupteur à clé maintenu	<p>Il est possible de raccorder un interrupteur à clé (maintenu) à la centrale d'alarme. Toute modification de cette zone a pour effet de faire passer la centrale d'alarme de l'état actif à l'état inactif ou vice-versa (selon le mode de sortie programmé).</p> <p> Remarque N'attribuez pas plus d'une zone de « durée d'interrupteur à clé » par partition. La centrale ne se commande alors que par l'interrupteur à clé. Si l'état n'est pas clair, par ex. lorsque le boîtier clé est fermé et simultanément désactivé sur l'élément de commande, il se peut que la centrale d'alarme revienne à l'état activé.</p> <p> Remarque Des interrupteurs à clé peuvent également faire office de sorties d'application dans le contrôle d'accès et dans la domotique.</p> <p></p>

Type	Explication
	<p>Remarque Avec la caractéristique de zone « Surveillance interne » = On, toute modification de cette zone a pour effet de faire passer la centrale d'alarme de l'état actif en interne à l'état inactif ou vice-versa (selon le mode de sortie programmé).</p> <p> Remarque La caractéristique « Inversé » (uniquement pour les zones filaires) inverse le comportement de cette zone.</p> <p> Remarque Pour les zones filaires de ce type, effectuez également une surveillance anti-sabotage de câble, en particulier pour les applications dans le contrôle d'accès et dans la domotique. L'utilisateur ne peut pas réinitialiser le système depuis une zone d'interrupteur à clé.</p>
Boîtier clé	<p>Cette zone s'utilise principalement en Scandinavie. Lorsque cette zone est ouverte, cet événement est enregistré dans la mémoire de la centrale d'alarme. Il peut également être transmis via le numéroteur téléphonique. Aucune alarme ne se déclenche.</p> <p>Lorsqu'une zone de ce type est nécessaire, l'installateur branche les fils d'alarme de cette zone (habituellement les contacts auxiliaires d'un contact de porte) à un boîtier clé externe et les fils anti-sabotage à l'interrupteur anti-sabotage du boîtier.</p> <p>Lorsque quelqu'un ouvre le boîtier, la centrale d'alarme sans fil enregistre l'événement et le signale au centre de réception des alarmes.</p>
Sabotage	<p>Cette zone s'utilise pour la surveillance anti-sabotage des périphériques externes. La surveillance de cette zone est permanente. Si la centrale d'alarme est désactivée, seule la sirène interne se déclenche. Si la centrale est active, la sirène externe et le stroboscope se déclenchent ainsi que la transmission selon la configuration.</p>
Historique seul	<p>Si une zone de type "Historique Seul" se déclenche (alarme ou sabotage), une entrée est créée dans l'historique et la sortie qui suit cette zone se déclenche. La zone peut être déclenchée lorsque la centrale d'alarme sans fil est activée ou désactivée.</p> <p>Les zones "Historique seul" peuvent être associées à plusieurs partitions et avoir pour attribut "Carillon de porte".</p>
Annulation temporisation de sortie	<p>Cette zone s'utilise pour annuler la temporisation de sortie d'une partition ayant l'attribut « Annulation temporisation sortie ». Le type de zone est habituellement utilisé pour le boîtier clé (NO). Remarque : cette zone est active pendant le temps de sortie, mais inactive, que la centrale d'alarme sans fil soit activée ou désactivée. Si l'attribut "Carillon de porte" est associé à cette zone, il retentit, que la centrale d'alarme sans fil soit activée ou désactivée.</p>
Verrouillage activé	<p>Cette zone s'utilise pour mettre fin à la temporisation de sortie d'une partition ayant l'attribut « Verrouillage activé ». Le type de zone est habituellement utilisé pour un interrupteur (NO). Remarque : Cette zone est active pendant le temps de sortie et lorsque la centrale d'alarme sans fil est activée. L'attribut "Inversé" peut être associé à cette zone.</p>
Défaut ext. WD	<p>Cette zone s'utilise pour surveiller la sortie défaut des émetteurs externes. Si une sortie défaut se déclenche avec ce type de zone, message "Défaut Ext WD" s'affiche. Ce type de zone n'est pas disponible pour les zones sans fil.</p>
Défaut Périph. AGR	<p>Cette zone s'utilise pour surveiller la sortie défaut des émetteurs d'alerte d'agression filaires. Si un émetteur d'alerte d'agression se déclenche avec ce type de zone, le message "Défaut Périph. AGR" s'affiche. Si l'utilisateur souhaite activer la centrale d'alarme sans fil avec une alarme de ce type, ce message s'affiche également. L'utilisateur peut ignorer le défaut et activer. Si ce défaut survient lorsque la centrale est active, une entrée est créée dans l'historique et la transmission programmée démarre, mais aucune alarme ne se déclenche jusqu'à la désactivation de la centrale d'alarme sans fil. Ce type de zone n'est pas disponible pour les zones sans fil.</p>

Type	Explication
Sabotage retour	Cette zone est utilisée pour surveiller la sortie antisabotage des sirènes externes. La surveillance de cette zone est permanente. Si une zone de ce type se déclenche lorsque la centrale d'alarme sans fil est désactivée, seule la sirène interne s'active. Si cette alarme se déclenche lorsque la centrale est activée, la transmission et les émetteurs externes avec stroboscope peuvent démarrer si la configuration le permet. Ce type de zone peut contenir les attributs "Test 14 jours", "Surveillance partielle", "Isoler est possible" et "Armement forcé". Ce type de zone n'est pas disponible pour les zones sans fil.
PSU Ext Défaut A/C	Cette zone s'utilise pour surveiller la sortie défaut AC d'une alimentation électrique externe. Si une zone de ce type se déclenche, la centrale d'alarme sans fil se comporte comme en cas de défaut A/C de la centrale. La réaction dépend de la programmation. Ce type de zone n'est pas disponible pour les zones sans fil.
PSU Ext Défaut Batt	Cette zone s'utilise pour surveiller la sortie défaut batterie/pile d'une alimentation électrique externe. Si ce défaut survient, les sorties programmées sur "Défaut batterie" sont activées et le message "PSU Ext Défaut Batt" s'affiche. Si ce défaut survient lorsque la centrale est active, une entrée est créée dans l'historique et la transmission programmée démarre, mais aucune alarme ne se déclenche jusqu'à la désactivation de la centrale d'alarme sans fil. Ce type de zone n'est pas disponible pour les zones sans fil.
PSU Ext tension faible	Cette zone s'utilise pour surveiller la sortie défaut « batterie/pile faible » d'une alimentation électrique externe. Si ce défaut survient, les sorties programmées sur "Tension faible" sont activées et le message "PSU Ext tension faible" s'affiche. Si ce défaut survient lorsque la centrale est active, une entrée est créée dans l'historique et la transmission programmée démarre, mais aucune alarme ne se déclenche jusqu'à la désactivation de la centrale d'alarme sans fil. Ce type de zone n'est pas disponible pour les zones sans fil.
Défaut PSU Ext	Cette zone s'utilise pour surveiller la sortie défaut d'une alimentation électrique externe. Si ce défaut survient, les sorties programmées sur "Défaut PSU Ext" sont activées et le message "Défaut PSU Ext" s'affiche. Si ce défaut survient lorsque la centrale est active, une entrée est créée dans l'historique et la transmission programmée démarre, mais aucune alarme ne se déclenche jusqu'à la désactivation de la centrale d'alarme sans fil. Ce type de zone n'est pas disponible pour les zones sans fil.
Seulement Actif	<p>Cette zone est utilisée pour ACTIVER UNIQUEMENT la centrale lors d'applications dans le contrôle d'accès et dans la domotique. Avec cette zone, la centrale NE peut PAS être DÉSACTIVÉE, en raison des exigences de la norme EN 50131 et de VdS.</p> <p>Dans la domotique, une authentification ou identification d'utilisateur univoque n'est pas toujours disponible.</p> <p>Une sortie d'une application de contrôle d'accès ou de domotique peut être raccordée à la centrale d'alarme anti-effraction.</p> <p>Toute modification dans cette zone a pour effet de faire passer la centrale d'alarme de l'état inactif à l'état actif (selon le mode de sortie programmé).</p> <p> Remarque Veuillez noter que l'application du contrôle d'accès ou de la domotique doit refermer cette zone après une durée précise (mais > 400 ms). Si l'état n'est pas clair, par ex. lorsque cette zone est ouverte et simultanément désactivée sur le clavier de commande, il se peut que la centrale revienne à l'état activé.</p> <p> Remarque Avec la caractéristique de zone « Surveillance interne » = On,</p>

Type	Explication
	<p>Toute modification dans cette zone a pour effet de faire passer la centrale d'alarme de l'état inactif à l'état actif en interne (selon le mode de sortie programmé).</p> <p> Remarque La caractéristique « Inversé » (uniquement pour les zones filaires) inverse le comportement de cette zone.</p> <p> Remarque Pour les zones filaires de ce type, effectuez également une surveillance anti-sabotage de câble, en particulier pour les applications dans le contrôle d'accès et dans la domotique. L'utilisateur ne peut pas réinitialiser le système depuis une zone uniquement active.</p>

Sélection de partition



Remarque

Les détecteurs programmés sont assignés **par défaut** à la **partition 01**.

Pour assigner le détecteur à une autre partition :

1. Sélectionnez la/les **partition(s)** où doit être surveillée la zone en cochant les cases correspondantes.



Remarque

Au moins une partition doit être sélectionnée.

Les possibilités de réglage des partitions figurent dans la section « Programmation/configuration via Serveur Web -> Partitions » de cette notice.

Vous pouvez assigner les zones du type suivant à une ou plusieurs partitions : Alarme immédiate tempo sortie, Blocage zone, Entrée/Sortie, Route d'entrée, Interrupteur à clé, Boîtier clé, Historique seul, Annulation temporisation sortie, Verrouillage activé et Alarme immédiate entrée/sortie.



Remarque

Si vous prévoyez d'utiliser des partitions activées en interne, vous devez vous assurer que les options activées en interne sont identiques pour toutes les zones utilisées de plusieurs partitions.

La centrale sans fil ne permet pas d'assigner les types de zone suivants à plus d'une partition : Alarme 24H, Feu, Alarme agression, Périmètre, Sabotage et Technique.

Sélection d'attribut de zone

1. Sélectionnez l'/les **attribut(s)** souhaité(s) en cochant les cases correspondantes.

Attribut	Explication
Supervision	<p>pour les zones IP</p> <p>Si une caméra n'a pas de contact avec la centrale pendant plus longtemps que le temps de réponse, la centrale crée une entrée dans l'historique et signale un avertissement (par ex. IP Zone Missing, IP-Zone Timeout).</p> <p>pour les zones sans fil</p> <p>Cet attribut est disponible pour les zones sans fil et permet le blocage de la surveillance pour des zones individuelles.</p> <p>En cas de réglage ON (réglage par défaut), la surveillance pour cette zone correspond à l'option globale sélectionnée dans Système -> Sécurité -> Supervision RF.</p> <p>En cas de réglage OFF, la surveillance est désactivée pour cette zone.</p>

	<p>pour les zones filaires non disponible</p> <p>pour les zones MoHy non disponible</p>
Carillon de porte	Chaque fois que cette zone se déclenche lorsque la centrale d'alarme est désactivée, la centrale d'alarme émet un signal acoustique.
Armement forcé isolé	Si une zone possède cet attribut, elle est automatiquement isolée si elle était ouverte lors de l'activation.
	<p>Remarque</p> <p>La fonction Armement forcé isolé doit également être activée dans le menu Système -> Réglages de sécurité -> Armement forcé.</p>

Attribut	Explication
Isoler est possible	<p>Si une zone possède cet attribut, un utilisateur peut l'isoler avant de l'activer.</p> <p>Si un utilisateur tente d'activer alors qu'une zone est ouverte avec cet attribut, il reçoit un avertissement et le processus d'activation est interrompu.</p> <p>L'utilisateur peut acquiescer cet avertissement et poursuivre l'activation.</p>
Sabotage ignoré	<p>Il s'agit d'un attribut supplémentaire pour les protections de portes/fenêtres mécatroniques d'ABUS. Pour cela, le type de zone "Alarme immédiate tempo sortie" doit être sélectionné.</p> <p>Si l'attribut « Sabotage ignoré » est sélectionné, la surveillance de l'effet levier des produits mécatroniques pris en charge est arrêtée lorsque la centrale d'alarme/la partition est désactivée. Cette opération n'est pas recommandée et n'est nécessaire que dans des cas spécifiques.</p> <p>Un "W" s'affiche dans la ligne Attribut de l'écran de la centrale.</p> <p>Remarque</p> <p>C'est-à-dire qu'à contrario, lorsque la centrale/la partition est activée ou activée en</p>

	interne (même si le détecteur n'est pas dans la surveillance), toute tentative d'effraction par levier est détectée et signalée.
Test 14 jours	<p>Si un détecteur déclenche souvent une fausse alerte, activez le Test 14 jours. Ce réglage est automatiquement réinitialisé au bout de 14 jours. Le détecteur ne déclenche pas d'alarme sur la centrale pendant ce délai. Tous les déclenchements sont cependant enregistrés dans la mémoire (historique).</p> <p> Remarque</p> <p>Si la zone d'alarme est déclenchée au cours de ces 14 jours pendant que le système est activé, la centrale d'alarme journalise l'événement comme « Test 14 jours défaut Znnn alarme » (nnn représente le numéro de zone). Aucune sirène n'est commandée et aucune communication n'est démarrée. Si la centrale d'alarme est désactivée, l'écran affiche le triangle pour informer l'utilisateur. Un installateur doit entrer son code d'accès pour réinitialiser l'alarme. Lors de l'activation, l'écran affiche un message bref pour informer l'utilisateur qu'une ou plusieurs zones d'alarme sont en test 14 jours. Vous pouvez utiliser cet attribut pour les types de zones suivants : alarme normale ; route d'entrée et sabotage.</p>

	<p> Remarque</p> <p>La fonction Test 14 jours doit être utilisée uniquement si un détecteur a tendance à déclencher de fausses alertes. Cette fonction est automatique. Pour tester la portée du détecteur, utilisez la fonction Test de détection mais n'activez pas le test 14 jours car cette fonction veille à ce que le détecteur ne déclenche pas d'alarme lorsque la centrale d'alarme sans fil est activée, mais enregistre uniquement un message dans la mémoire. Après 14 jours, la centrale d'alarme sans fil restaure le mode normal dans la zone.</p>
Surveillance interne	Cette zone est surveillée quand la partition de cette zone ou toutes les partitions sont activées en interne.
Surveillance d'activité	<p>La fonction du détecteur est inversée. Ne l'utiliser qu'avec l'appel soins de santé.</p> <p>Une alarme se déclenche sur la centrale lorsque le détecteur n'émet pas d'alarme pendant un délai défini.</p>
Inversion	<p>Pour les zones filaires uniquement Inverse le comportement du détecteur.</p> <p>Fermé = alarme Ouvert = aucune alarme</p>

Zones sans fil

ABUS
Logout

Périphériques | Zones Radio

Numéro	Nom	Partitions	Type	Attributs	Pile faible	Isoler	Défaut	Supervision	Sabotage	Début	RSSI
Z201 RADIO	"MK"	1	Alarme immédiate tempo sortie								9 (9)
Z202 RADIO	"FTS 96"	2	Alarme immédiate tempo sortie								9 (9)
Z203 RADIO	"Smoke"	1	Alarme Feu								9 (9)
Z204 RADIO	"Zone 204"	Aucun(e)	Non Utilisé								
Z205 RADIO	"Zone 205"	Aucun(e)	Non Utilisé								
Z206 RADIO	"Zone 206"	Aucun(e)	Non Utilisé								
Z207 RADIO	"Zone 207"	Aucun(e)	Non Utilisé								
Z208 RADIO	"Zone 208"	Aucun(e)	Non Utilisé								

←
...
1
2
3
4
5
...
→

Supprimer tous

INFO

État

Périphériques

Sorties

Partitions

Système

Transmissions

Appel Soins de Santé

Test

Journal de bord

Clavier

Désignation/Fonction	Explication
Numéro	Le numéro comprend le nom de zone et le type de périphérique (sans fil).
Nom	Nom de zone unique.
Partition	Partition de chaque zone
Type	Type de la zone sans fil
Propriétés	Vue d'ensemble des attributs de la zone sans fil

Remarque
 La description de la configuration du nom de zone, de la partition, du type de zone et des attributs de zone figure après la vue d'ensemble des « Zones IP ».

Fonction	Explication
Éditer zones	Cette fonction permet de modifier les paramètres de la zone.
Supprimer tous	Ici, vous pouvez supprimer tous les détecteurs en une seule action. Le type de zone redevient alors "Non utilisé".

Ajout/suppression de détecteurs

- Sélectionnez le menu « Périphériques » → « Zones sans fil ».
- La fonction suivante est disponible :

Fonction	Explication
Ajouter/supprimer détecteurs	Si vous avez sélectionné cette option, vous obtenez la liste de toutes les zones possibles. Sélectionnez une zone pour laquelle vous souhaitez programmer ou supprimer un détecteur.

Ajouter détecteurs

- Sélectionnez une zone.
- Vous êtes invité à activer le contact anti-sabotage du détecteur.

Remarque
 Assurez-vous qu'aucun autre détecteur actif ne soit à l'état anti-sabotage.

Remarque

Après la programmation via l'interface Web, vous devez encore programmer la zone.

3. Cet écran indique :
 - sur quelle zone a été programmé le détecteur
 - quel type de zone a été programmé pour ce détecteur
 - quelle partition il surveille et
 - quels attributs de zone supplémentaires sont présents.
4. Vous pouvez également voir l'affichage RSSI : la puissance du signal reçu. Pour une transmission de bonne qualité, cette valeur doit être supérieure à 3.



Remarque

Lorsqu'un détecteur a été correctement programmé, la centrale d'alarme affiche le symbole  à côté du numéro de zone.

Pour une zone programmée d'un WAM (WAM fonction 3 émetteurs/récepteurs), "w2" s'affiche par exemple.

Détecteur déjà utilisé



Remarque

Il peut arriver que le message **Détecteur déjà utilisé** s'affiche lors de la programmation du détecteur après réception de la confirmation de programmation car le détecteur envoie son signal plusieurs fois.

Dans ce cas, le message n'a pas d'importance.

Il se peut que ce détecteur soit déjà programmé sur une autre zone.

Suppression de détecteur ou de détecteur et informations de zone

1. Sélectionnez la zone où le détecteur est connecté.
2. Sélectionnez :
 - **Annuler ID détecteur** si seul le détecteur doit être supprimé
 - **RAZ Zone** si le détecteur et les informations de zone doivent être supprimés
3. Confirmez votre choix en cliquant sur **Continuer**.
4. Confirmez la suppression du détecteur/de la zone en choisissant **Oui** ou **Retour** en cas de doute.

Supprimer tous

1. Sélectionnez l'option de menu **Supprimer tous**.
2. Confirmez votre choix en cliquant sur **Continuer**.
3. Confirmez la suppression des détecteurs et de la zone en choisissant **Oui** ou **Retour** en cas de doute.

Zones filaires

ABUS
Logout

Périphériques | Zones filaires

Numéro	Nom	Partitions	Type	Attributs
Z301 Filaire	"Zone 301"	Aucun(e)	Non Utilisé	
Z302 Filaire	"Zone 302"	Aucun(e)	Non Utilisé	
Z303 Filaire	"Zone 303"	Aucun(e)	Non Utilisé	
Z304 Filaire	"Zone 304"	Aucun(e)	Non Utilisé	

Supprimer tous

Pile faible
Isoler
Défaut Supervision
Sabotage
Début
RSSI:

INFO
État
Périphériques
Sorties
Partitions
Système
Transmissions
Appel Soins de Santé
Test
Journal de bord
Clavier

Désignation/Fonction	Explication
Numéro	Le numéro comprend le nom de zone et le type de périphérique (filaire).
Nom	Nom de zone unique
Partition	Partition de chaque zone
Type	Type de la zone filaire
Propriétés	Vue d'ensemble des attributs de la zone filaire

Supprimer tous (uniquement sur la centrale)

1. Sélectionnez l'option de menu **Supprimer tous**.
2. Confirmez votre choix en cliquant sur **Continuer**.
3. Confirmez la suppression des détecteurs et de la zone en choisissant **Oui** ou **Retour** en cas de doute.

Remarque

La description de la configuration du nom de zone, de la partition, du type de zone et des attributs de zone figure après la vue d'ensemble des « Zones IP ».

Zones MoHy

ABUS
Abmelden

Komponenten | HyMo Zonen

Nummer	Name	Teilbereiche	Typ	Eigenschaften	
Z401 HyMo	"Zone 401"	1	Normal Alarm	Türgong, Intern überwacht	<small>Batterieschwach Auslösen</small> <small>Supervisionsödnung</small> <small>Selbstzug</small> <small>Öffnen</small> <small>RSS:</small>
Z402 HyMo	"Zone 402"	2	Normal Alarm	Türgong, Intern überwacht	
Z403 HyMo	"Zone 403"	3	Normal Alarm	Türgong, Intern überwacht	
Z404 HyMo	"Zone 404"	4	Normal Alarm	Türgong, Intern überwacht	
Z405 HyMo	"Zone 405"	1-4	Normal Alarm	Türgong, Intern überwacht	
Z406 HyMo	"Zone 406"	1	Nur Aktiv		
Z407 HyMo	"Zone 407"	2	Nur Aktiv		
Z408 HyMo	"Zone 408"	3	Nur Aktiv		

◀ ... 1 2 ... ▶

Entfernen Alle

- Info
- Status
- Komponenten
- Ausgänge
- Teilbereiche
- System
- Kommunikation
- Pflegetruf
- Test
- Logbuch
- Tastatur

Désignation/Fonction	Explication
Numéro	Le numéro comprend le nom de zone et le type de périphérique (MoHy).
Nom	Nom de zone unique
Partition	Partition de chaque zone
Type	Type de chaque zone filaire MoHy
Propriétés	Vue d'ensemble des attributs de chaque zone filaire MoHy

Supprimer tous

1. Sélectionnez l'option de menu **Supprimer tous**.
2. Confirmez votre choix en cliquant sur **Continuer**.
3. Confirmez la question de sécurité pour supprimer la zone en choisissant **Oui** ou **Retour** en cas de doute.



Remarque

La description de la configuration du nom de zone, de la partition, du type de zone et des attributs de zone figure après la vue d'ensemble des « Zones IP ».

ABUS

Komponenten | HyMo Zonen | Z401 HyMo

Typ: *Normal Alarm

Name: Zone 401

Teilbereiche: 1, 2, 3, 4, Alle Teilbereiche

Eigenschaften:

- Türgong
- Belastungstest
- Ausblendbar Zwangsaktiv
- Intern überwacht
- invertiert
- Ausblendbar
- Aktivitätsüberwachung
- Ignoriere Hebel

Abbruch Übernehmen

Abmelden

- Info
- Status
- Komponenten
- Ausgänge
- Teilbereiche
- System
- Kommunikation
- Pflegenotruf
- Test
- Logbuch
- Tastatur



Remarque

Version logicielle \geq 3.01.16

Les zones du module hybride peuvent uniquement être attribuées aux partitions auxquelles le module hybride est également attribué.

Exemple : Si vous avez sélectionné les partitions 1 et 2 pour le MoHy, les zones de ce MoHy peuvent également uniquement être attribuées aux partitions 1 et 2.

Veuillez tenir compte de l'attribution des partitions du module hybride. Les messages du module hybride, par ex. Tamper ou Défaut CC, sont alors attribués à ces partitions.

Version logicielle $<$ 3.01.16

Les zones du module hybride peuvent être attribuées à d'autres partitions, mais il doit s'agir des partitions du module hybride.

Veuillez tenir compte de l'attribution des partitions du module hybride. Les messages du module hybride, par ex. Tamper ou Défaut CC, sont alors attribués à ces partitions.



Remarque

Le type de câblage (**type de zone filaire**) des entrées de zone de ce module hybride peut être réglé via **Périphériques -> Modules hybrides**.



Remarque

Zones

Module hybride 1

401 à 410 lorsque 2 fils est sélectionné comme type de zone

401 à 405 lorsque 4 fils est sélectionné comme type de zone

Module hybride 2

411 à 420 lorsque 2 fils est sélectionné comme type de zone

411 à 415 lorsque 4 fils est sélectionné comme type de zone

Clavier de commande sans fil

ABUS
Logout

Périphériques | **Claviers Radio**

Numéro	Nom	Partitions
CLAV.R1	"Ctrl Dev 01"	1-4
CLAV.R2	Non Ajouté	
CLAV.R3	Non Ajouté	
CLAV.R4	Non Ajouté	
CLAV.R5	Non Ajouté	
CLAV.R6	Non Ajouté	
CLAV.R7	Non Ajouté	
CLAV.R8	Non Ajouté	

- INFO
- État
- Périphériques
- Sorties
- Partitions
- Système
- Transmissions
- Appel Soins de Santé
- Test
- Journal de bord
- Clavier

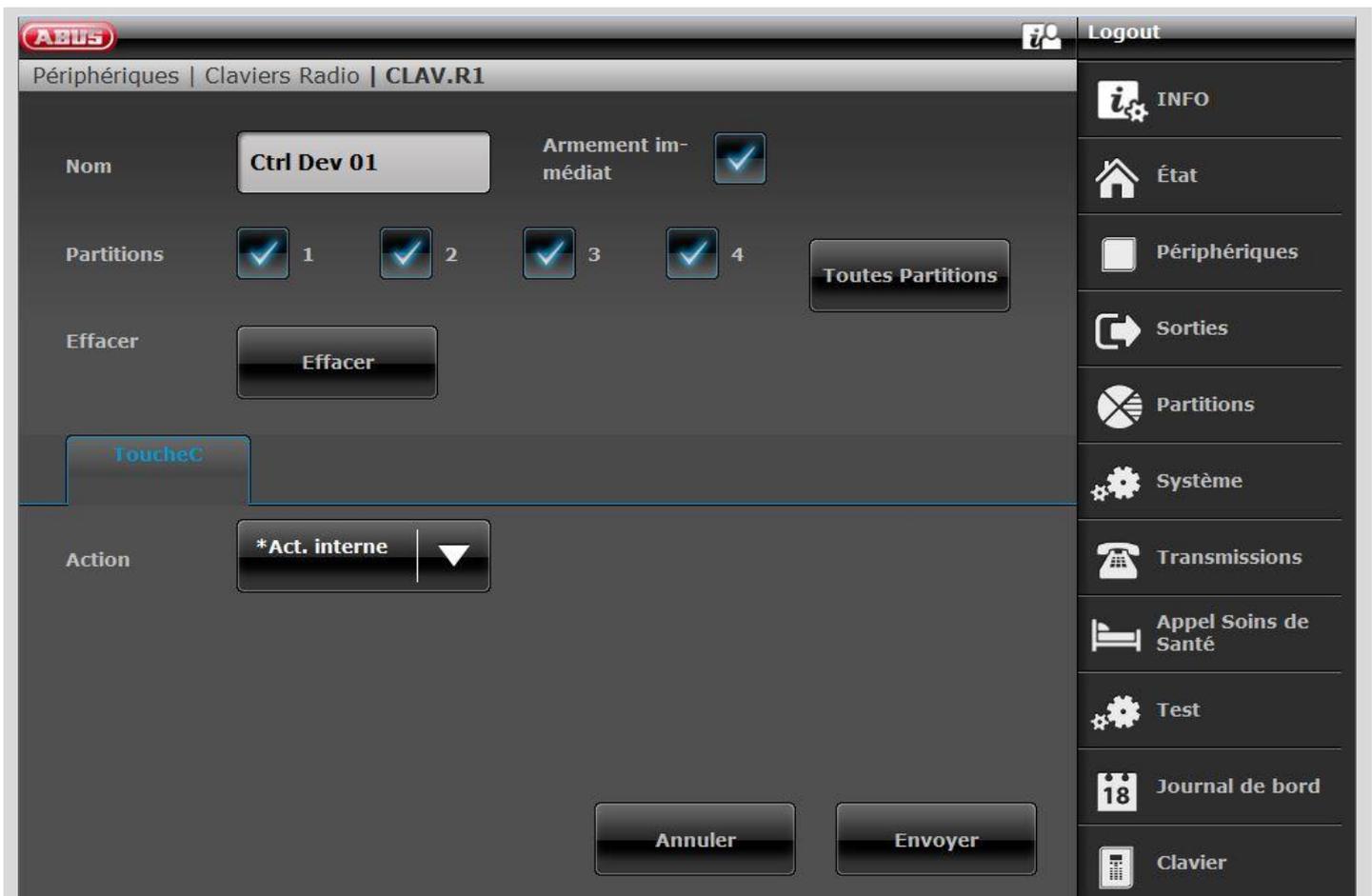
Désignation/Fonction	Explication
Numéro	Le numéro comprend le type de périphérique (CLAV.R) et le numéro séquentiel.
Nom	Nom unique de l'élément de commande radio.
Partitions	Partitions de l'élément de commande correspondant

Ajouter un élément de commande sans fil

Remarque
Jusqu'à huit éléments de commande radio peuvent être programmés.

1. Sélectionnez **Ajouter/supprimer CLAV. RAD.**
2. **Sélectionnez** le clavier de commande sans fil correspondant.
3. Déclenchez le contact anti-sabotage du clavier de commande sans fil (voir la notice séparée du clavier de commande sans fil).

Remarque
Si l'élément de commande radio est programmé, la centrale d'alarme sans fil bipera deux fois pour confirmer. Le symbole s'affiche en haut à côté du numéro du clavier de commande sans fil.



Désignation/Fonction	Explication
Nom	Nom unique de l'élément de commande radio.
Armement immédiat	Armement immédiat des partitions assignées Oui/Non .
Partitions	Partitions assignées de l'élément de commande
Bouton C Action	Sélection de l'action qui est exécutée lorsque la touche "*" est enfoncée :
	Non utilisé Bouton C sans fonction
	Activer Activation des partitions assignées
	Activer en interne Activation interne des partitions assignées
	Désactiver Désactivation des partitions assignées
	Sortie ON Activation de la sortie assignée
	Sortie OFF Désactivation de la sortie assignée
	Commuter la sortie Commutation de la sortie assignée
Sortie	(Uniquement disponible pour "Sortie ON", "Sortie OFF" et "Commutation de la sortie") Sélection de la sortie souhaitée à activer, désactiver ou commuter.

Sirènes extérieures

Sirènes sans fil

Numéro	Nom	Partitions
Sir Radio 1	Non Ajouté	
Sir Radio 2	Non Ajouté	
Sir Radio 3	Non Ajouté	
Sir Radio 4	Non Ajouté	

Supprimer tous

Désignation/Fonction	Explication
Numéro	Le numéro comprend le type de périphérique (sirène radio) et le numéro séquentiel.
Nom	Nom unique de la sirène radio

Ajouter des sirènes

1. Sélectionnez **Sirène sans fil**.
2. Sélectionnez **Ajouter/Supprimer sirène**.
3. Sélectionnez la sirène correspondante.
4. Déclenchez le contact anti-sabotage de la sirène.



Remarque

Si la sirène a été programmée, la centrale d'alarme sans fil bipe deux fois pour confirmer. Un message vous indique que la sirène a été ajoutée et la valeur de la puissance du signal reçu s'affiche.

5. Terminez la saisie avec **Retour**.



Remarque

Lorsqu'une sirène a été programmée, la centrale d'alarme affiche le symbole  à côté du numéro de sirène.

6. Quittez cet affichage avec **Retour**.
7. Sélectionnez Modifier sirène externe.
8. **Sélectionnez** maintenant la **sirène ext.** programmée.



Remarque

Si la sirène ext. doit être activée, lorsque la partition déclenche une alarme locale ou externe, réglez la partition sur **Oui**.

Supprimer tous

1. Sélectionnez l'option de menu **Supprimer tous**.
2. Confirmez votre choix en cliquant sur **Continuer**.
3. Confirmez la suppression de la sirène en choisissant **Oui** ou **Retour** en cas de doute.

Sirènes filaires

Désignation/Fonction	Explication
Numéro	Le numéro comprend le type de périphérique (sirène filaire) et le numéro séquentiel.
Nom	Nom unique de la sirène filaire

Générateur de signal intérieur

Nummer	Name	Teilbereiche
Innen-SG 1	"Innen-SG 01"	1
Innen-SG 2	Nicht hinzugefügt	
Innen-SG 3	Nicht hinzugefügt	
Innen-SG 4	Nicht hinzugefügt	

Entfernen Alle

- Info
- Status
- Komponenten
- Ausgänge
- Teilbereiche
- System
- Kommunikation
- Pflegenotruf
- Test
- Logbuch
- Tastatur

Désignation/Fonction	Explication
Numéro	Le numéro comprend le type de composant (générateur de signal int.) et le numéro séquentiel.
Nom	Nom unique du générateur de signal intérieur (12 caractères maximum).
Pas ajouté	Pour accéder au mode « Ajouter », cliquez sur le générateur de signal intérieur correspondant. La suite de la procédure est décrite comme ci-dessus sous Programmation sur l'interface Web.
Générateur de signal int. 1	Pour accéder au mode « Éditer », cliquez sur le générateur de signal intérieur correspondant.



La suite de la procédure est décrite comme ci-dessous pour le guidage menu de la centrale d'alarme.

Supprimer tous	Cliquez sur ce champ et confirmez à l'étape suivante la question de sécurité pour supprimer tous les générateurs de signal intérieurs.
Supprimer	Cliquez sur ce champ et confirmez à l'étape suivante la question de sécurité pour supprimer ce générateur de signal intérieur.
Partitions	Numéros des partitions auxquelles est assigné le générateur de signal intérieur.

Ajouter un générateur de signal int. (centrale)

1. Sélectionnez **Générateur de signal int.**
2. Sélectionnez **Ajouter/Supprimer.**
3. Sélectionnez le générateur de signal int. correspondant.
4. Déclenchez le contact anti-sabotage du générateur de signal int.



Remarque

Si un générateur de signal int. a été programmé, la centrale sans fil émet deux bips pour confirmer. Un message vous indique que le générateur de signal int. a été ajouté et la valeur de la puissance du signal reçu s'affiche.

5. Terminez la saisie avec **Retour.**



Remarque

Lorsqu'un générateur de signal int. a été programmé, la centrale affiche le symbole  à côté du numéro du générateur de signal int.

Vous pouvez ajouter **4** générateurs de signal int. au maximum.

6. Quittez cet affichage avec **Retour.**

Modifier

Sélectionnez le générateur de signal int. correspondant. Les points de sous-menu suivants s'affichent.

Nom :

Attribuez un nom unique à ce générateur de signal int.

Supprimer tous

1. Sélectionnez l'option de menu **Supprimer tous.**
2. Confirmez votre choix en cliquant sur **Continuer.**
3. Confirmez la question de sécurité de suppression de tous les générateurs de signal int. avec **Oui.** Sélectionnez **Retour** en cas de doute.



Danger

Les réglages du menu utilisateur :

Menu utilisateur -> Configuration -> Réglages Volume

Tonalités opérateur

Tonalités info

Tonalités alarme

ont également une influence sur le volume des tonalités du générateur de signal intérieur.



Remarque

En cas de fonctionnement sur piles uniquement du générateur de signal intérieur, seules des tonalités d'alarme sont émises. Aucune tonalité d'utilisation et d'information n'est émise.

Module d'info/sirène d'intérieur

ABUS Logout

Périphériques | Module Info/sirènes int.

Actualisation LED prêt Ajouter composant

Annuler Envoyer

- INFO
- État
- Périphériques
- Sorties
- Partitions
- Système
- Transmissions
- Appel Soins de Santé
- Test
- Journal de bord
- Clavier

Désignation/Fonction	Explication
Actualisation	<p>Activé Actualisation de l'état sur le module d'information activée. En cas de modification de l'état sur la centrale d'alarme ou les zones, le message "juste à temps" s'affiche.</p> <p>Désactivé Pas d'actualisation sur le module d'information et la sirène d'intérieur. La sirène d'intérieur ne déclenche donc pas d'alarme.</p>
LED prêt	<p>Activé LED prêt activée sur le module d'information.</p> <p>Désactivé LED prêt désactivée sur le module d'information.</p>

Ajouter centrale (uniquement sur la centrale)

1. Après avoir sélectionné ce point du menu, le message suivant s'affiche à l'écran :
 - Sélectionnez Ajouter/Supprimer sirène.
2. Sélectionnez la sirène correspondante.
3. Après avoir sélectionné ce point du menu, le message suivant s'affiche à l'écran :
 - Le destinataire est-il en mode programmation ?
4. Réglez la sirène d'intérieur ou le module d'information en mode programmation. Respectez pour cela les instructions du produit.
5. Activez l'envoi d'informations sans fil par la centrale d'alarme en appuyant sur **Oui**.
6. Le message suivant s'affiche :
Le récepteur a-t-il émis 2 bips ?
7. Confirmez avec **Oui**.
8. Le message de programmation avec l'ID de la centrale d'alarme a été correctement reçu et enregistré dans la sirène d'intérieur ou le module d'information.
9. Pour répéter ou annuler, appuyez sur **Non**.

WAM (module universel)

ABUS
Logout

Périphériques | Modules

Numéro	Nom
Wam 1	Non Ajouté
Wam 2	Non Ajouté
Wam 3	Non Ajouté
Wam 4	Non Ajouté
Wam 5	Non Ajouté
Wam 6	Non Ajouté
Wam 7	Non Ajouté
Wam 8	Non Ajouté

Supprimer tous

- INFO
- État
- Périphériques
- Sorties
- Partitions
- Système
- Transmissions
- Appel Soins de Santé
- Test
- Journal de bord
- Clavier

Désignation/Fonction	Explication
Numéro	Le numéro comprend le type de périphérique (WAM) et le numéro séquentiel.
Nom	Nom unique du module universel

Ajout de module universel

Remarque
 Veillez à ce que des sorties et des zones réservées soient attribuées à chaque WAM.
 Voir le tableau des sorties / zones WAM réservées.

Module universel	Sorties réservées	Zones réservées
WAM 1	229 – 232	248
WAM 2	225 – 228	247
WAM 3	221 – 224	246
WAM 4	217 – 220	245
WAM 5	213 – 216	244
WAM 6	209 – 212	243
WAM 7	205 – 208	242
WAM 8	201 – 204	241

Remarque
 Programmez le module universel en suivant les instructions de la notice d'installation WAM, par ex. en tant qu'émetteur / récepteur sans fil (fonction 3).
 Après avoir programmé le module universel selon les instructions, vous pouvez l'ajouter à l'installation.

1. Sélectionnez **Ajouter/Supprimer WAM**.
2. **Sélectionnez** le module universel correspondant (WAM). Jusqu'à **huit** modules universels peuvent être programmés.
3. Sélectionnez par exemple **WAM 1**.
4. Déclenchez le contact anti-sabotage du WAM.

Remarque
 Les modules WAM programmés sont accompagnés du **symbole** situé à côté du numéro WAM.

Vérifiez les informations du module universel.

5. Sélectionnez **Infos WAM**.

6. Sélectionnez **WAM 1**.



Remarque

Lors de l'assignation du module universel, celui-ci transfère également sa programmation afin que vous puissiez voir dans l'option Information WAM à quelle fonction le module universel a été assigné.

Fonction	Explication
Non utilisé	Le module universel n'est pas programmé.
1 Répéteur sans fil	Les signaux radio reçus par les détecteurs sans fil programmés (assignés dans le WAM) sont transmis à la centrale après la réception. Aucun réglage supplémentaire n'est nécessaire
2 Module sortie	Jusqu'à quatre relais du WAM peuvent être activés par la centrale sans fil en fonction de la programmation.
3 T/R module	Zone et module de sortie pour le raccordement de détecteurs filaires (détecteurs d'inondation) ou d'un boîtier clé maintenue/interrupteur à clé.
4 Module sirènes	Pour le raccordement d'une sirène d'extérieur filaire ou d'une alarme compacte.

WAM en tant que répéteur sans fil (WAM fonction 1)

Si le module universel est programmé avec la fonction répéteur sans fil, vous devez également assigner au WAM les détecteurs sans fil dont le signal doit être transmis via ce module.

Respectez pour cela les instructions relatives au module universel (WAM).

WAM en tant que module de sortie (WAM fonction 2)



Remarque

Si le module universel est assigné à une fonction de sortie, la centrale réserve automatiquement les sorties correspondantes à ce module dans la centrale.



Remarque

Vous n'avez plus besoin d'ajouter manuellement ces sorties.

Effectuez uniquement les réglages de la fonction des sorties en suivant les instructions de la section **Modifier les sorties**.

Ces sorties doivent seulement être configurées et non plus ajoutées.

Respectez pour cela les instructions relatives au module universel (WAM).

WAM en tant que zone et module de sortie (WAM fonction 3)



Remarque

Si le module universel est assigné à la fonction 3, la centrale réserve automatiquement la zone et les sorties correspondantes dans la centrale pour ce module.

- L'entrée 1 et l'entrée 2 forment la zone filaire du WAM.
- L'entrée 1 fait office de connexion pour le circuit d'alarme. L'entrée 2 fait office de connexion pour la ligne anti-sabotage.
- Ces deux connexions correspondent à la zone sans fil.
- Lors du câblage, respectez les instructions du module universel (WAM).

WAM en tant que module sirènes (WAM fonction 4)

Si vous avez configuré le WAM en tant que module sirènes, un écran s'affiche dans lequel vous devez configurer la partition pour laquelle la sirène doit être activée. Ce réglage s'effectue de la même manière que le réglage de la sirène ext.

La connexion de l'alarme compacte dans le WAM est décrite dans la notice du module universel (WAM).



Remarque

Notez que les sorties hors tension du WAM peuvent être soumises à **500 mA max. à 24 V**.

Il s'agit ici d'un optocoupleur ayant une résistance de passage de 2 Ω .

Supprimer tous

1. Sélectionnez l'option de menu **Supprimer tous**.
2. Confirmez votre choix en cliquant sur **Continuer**.
3. Confirmez la suppression du WAM en choisissant **Oui** ou **Retour** en cas de doute.

Verrous de porte

Numéro	Nom	Partitions
Serrure porte 1	Non Ajouté	
Serrure porte 2	Non Ajouté	
Serrure porte 3	Non Ajouté	
Serrure porte 4	Non Ajouté	
Serrure porte 5	Non Ajouté	
Serrure porte 6	Non Ajouté	
Serrure porte 7	Non Ajouté	
Serrure porte 8	Non Ajouté	

Supprimer tous

Désignation/Fonction	Explication
Numéro	Le numéro comprend le type de périphérique (verrou de porte) et le numéro séquentiel.
Nom	Nom unique des verrous de porte (par ex. Secvest Key ou verrou de porte supplémentaire).
Partitions	Numéro de partition à laquelle est assigné le verrou de porte.

Ajout de verrous de porte (centrale)

1. Sélectionnez **Verrous de porte**.
2. Sélectionnez **Ajouter/Supprimer verrous de porte**.
3. Sélectionnez le verrou de porte souhaité.
4. Déclenchez le contact anti-sabotage du verrou de porte ou insérez une pile.



Remarque

Si le verrou de porte a été programmé, la centrale d'alarme sans fil émet deux bips pour confirmer. Un message vous indique que le verrou de porte a été ajouté et la valeur de la puissance du signal reçu s'affiche.



Remarque

Lorsqu'un verrou de porte a été programmé, la centrale d'alarme affiche le symbole  à côté du numéro de verrou de porte.

6. Quittez cet affichage avec Retour.

Modifier

Sélectionnez le verrou de porte souhaité.

Les points de sous-menu suivants s'affichent :

Nom

Attribuez un nom unique à ce verrou de porte.

Partitions

5. Terminez la saisie avec **Retour**.

Sélectionnez les partitions auxquelles le verrou de porte doit être affecté.

Désactivé après effraction (version logicielle >= 3.01.16)

OUI

Secvest Key et le verrou de porte supplémentaire peuvent activer et désactiver les partitions attribuées.

NON

Partitions attribuées **sans** alarme intrusion :

Secvest Key et le verrou de porte supplémentaire peuvent activer et désactiver les partitions attribuées.

Partitions attribuées **avec** alarme intrusion :

Quelle que soit la partition attribuée à l'alarme intrusion, Secvest Key et le verrou de porte supplémentaire **ne** peuvent **pas** désactiver les partitions attribuées.

Pour la désactivation, il est nécessaire de saisir un code sur la centrale ou d'utiliser d'autres composants.

Partitions **non** attribuées **avec** alarme intrusion :

Secvest Key et le verrou de porte supplémentaire peuvent désactiver les partitions attribuées.

Supprimer verrou de porte

Confirmez la question de sécurité de suppression du verrou de porte en choisissant **Oui** ou **Retour** en cas de doute.

Supprimer tous

1. Sélectionnez l'option de menu **Supprimer tous**.
2. Confirmez votre choix en cliquant sur **Continuer**.
3. Confirmez la question de sécurité de suppression des verrous de porte en choisissant **Oui** ou **Retour** en cas de doute.

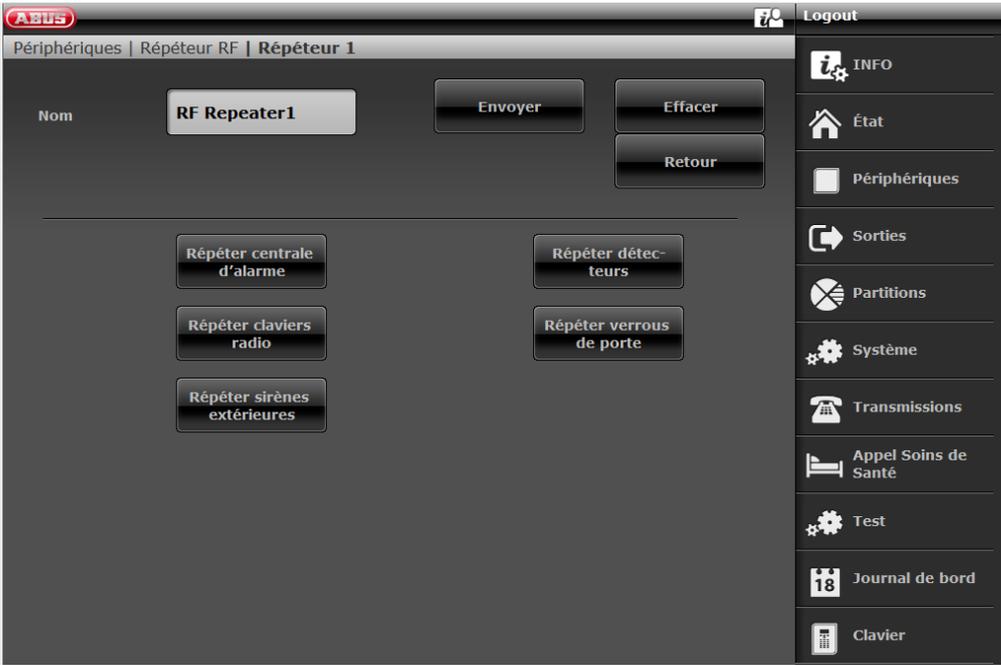
Répéteur RF

Numéro	Nom
Répéteur 1	"RF Repeater1"
Répéteur 2	Non Ajouté
Répéteur 3	Non Ajouté
Répéteur 4	Non Ajouté

[Supprimer tous](#)

- Logout
- INFO
- État
- Périphériques
- Sorties
- Partitions
- Système
- Transmissions
- Appel Soins de Santé
- Test
- Journal de bord
- Clavier

Désignation/Fonction	Explication
Numéro	Le numéro comprend le type de périphérique (répéteur RF) et le numéro séquentiel.
Nom	Nom unique du répéteur (12 caractères maximum).
Pas ajouté	Pour accéder au mode « Ajouter », cliquez sur le répéteur correspondant. La suite de la procédure est décrite comme ci-dessous pour le guidage menu de la centrale d'alarme.
Répéteur RF 1	Pour accéder au mode « Modifier », cliquez sur le répéteur correspondant.

	
<p>Supprimer tous</p>	<p>La suite de la procédure est décrite comme ci-dessous pour le guidage menu de la centrale d'alarme.</p> <p>Cliquez sur ce champ et confirmez à l'étape suivante la suppression de tous les répéteurs.</p>

Ajout de répéteur RF (centrale d'alarme)

1. Sélectionnez **Répéteur RF**.
2. Sélectionnez **Ajouter/Supprimer**.
3. Sélectionnez le répéteur correspondant.
4. Déclenchez le contact anti-sabotage du répéteur.



Remarque

Si un répéteur a été programmé, la centrale d'alarme sans fil émet deux bips pour confirmer. Un message vous indique que le répéteur a été ajouté et la valeur de la puissance du signal reçu s'affiche.

Le répéteur affiche la puissance du signal reçu de la centrale d'alarme avec les LED d'état. Vous trouverez des détails à ce sujet dans le manuel du répéteur.

5. Terminez la saisie avec **Retour**.



Remarque

Lorsqu'un répéteur a été programmé, la centrale d'alarme affiche le symbole  à côté du numéro du répéteur.

Vous pouvez ajouter **4** répéteurs au maximum.

6. Quittez cet affichage avec **Retour**.

Modifier

Sélectionnez le répéteur correspondant. Les points de sous-menu suivants s'affichent.

Nom :

Attribuez un nom unique à ce répéteur.

Répéter centrale d'alarme

Choisissez si les messages sans fil de la centrale d'alarme doivent être répétés par ce répéteur.



Remarque

Les messages de la centrale d'alarme peuvent être :

- Émission état centrale, nécessaire pour l'affichage permanent des états des partitions sur les claviers de commande FUBE5000x.
- Activation de sirènes d'extérieur (par ex. FUSG50100/1 ou FUSG50000)
- Activation de sirènes d'intérieur (par ex. FUSG50010) et de modules d'information (par ex. FUMO50030)
- Activation de générateurs de signal intérieurs (par ex. FUSG50110).
- Activation de modules hybrides (par ex. FUMO50110), est nécessaire pour la configuration ou la consultation de valeurs de courant et de tension, de la version logicielle, de valeurs de résistance, des sorties, du haut-parleur et de la puissance de signal.

Activation de sorties sans fil (par ex. prise sans fil
FUHA50010)

Répéter détecteurs

Choisissez quel(le)s détecteurs/zones sans fil doivent être répété(e)s par ce répéteur. Tous les détecteurs programmés s'affichent.

Répéter claviers de commande sans fil

Choisissez quels claviers de commande sans fil doivent être répétés. Tous les claviers de commande sans fil programmés s'affichent.

Répéter verrous de porte

Choisissez quels verrous de porte sans fil doivent être répétés. Tous les verrous de porte sans fil programmés s'affichent.

Répéter sirènes d'extérieur

Choisissez quelles sirènes d'extérieur sans fil doivent être répétées. Toutes les sirènes d'extérieur sans fil programmées s'affichent.

Répéter générateur de signal int.

Choisissez quels générateurs de signal intérieurs doivent être répétés. Tous les générateurs de signal intérieurs programmés s'affichent.

Répéter MoHy

Choisissez quels modules hybrides doivent être répétés.
Tous les modules hybrides programmés s'affichent.



Remarque

Un répéteur peut répéter au maximum 10 périphériques.

Les télécommandes et les émetteurs d'appel d'urgence (agression, médical, soin) sont toujours répétés s'ils se trouvent dans la zone de réception du répéteur.

Supprimer tous

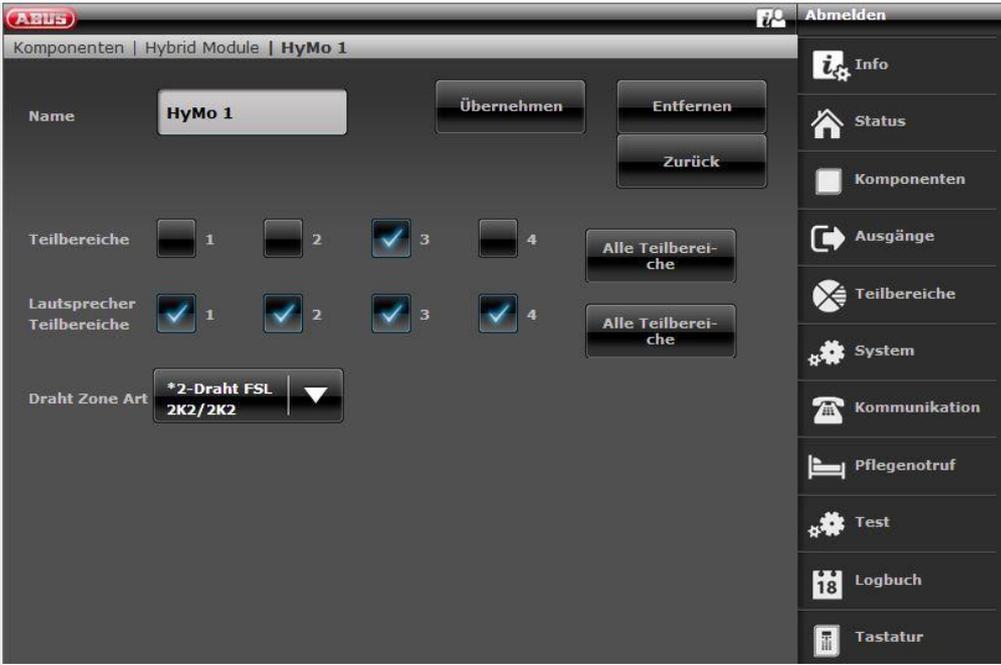
1. Sélectionnez l'option de menu **Supprimer tous**.
2. Confirmez votre choix en cliquant sur **Continuer**.
3. Confirmez la suppression de tous les répéteurs avec **Oui**. Sélectionnez **Retour** en cas de doute.

Modules hybrides

Version logicielle >= 3.01.14

Nummer	Name	Teilbereiche	Lautsprecher Teilbereiche
HyMo 1	"HyMo 1"	3	1-4
HyMo 2	"HyMo 2"	1	1-4

Désignation/Fonction	Explication
Numéro	Le numéro comprend le type de périphérique (module hybride) et le numéro séquentiel.  Remarque Vous pouvez ajouter 2 modules hybrides maximum.
Nom	Nom unique du module hybride (12 caractères maximum).
Pas ajouté	Pour accéder au mode « Ajouter », cliquez sur le module hybride correspondant. La suite de la procédure est décrite comme ci-dessous pour le guidage menu de la centrale d'alarme.
MoHy 1	Pour accéder au mode « Éditer », cliquez sur le module hybride correspondant.

	 <p>La suite de la procédure est décrite comme ci-dessous pour le guidage menu de la centrale d'alarme.</p>
<p>Supprimer tous</p>	<p>Cliquez sur ce champ et confirmez à l'étape suivante la question de sécurité pour supprimer tous les modules hybrides avec Oui. Sélectionnez Retour en cas de doute.</p>

Ajouter un module hybride (centrale)

1. Sélectionnez **Module hybride**.
2. Sélectionnez **Ajouter/Supprimer**.
3. Sélectionnez le module hybride correspondant.
4. Déclenchez le contact anti-sabotage du module hybride.



Remarque

Si un module hybride a été programmé, la centrale sans fil émet deux bips pour confirmer. Un message vous indique que le module hybride a été ajouté et la valeur de la puissance du signal reçu s'affiche.

5. Terminez la saisie avec **Retour**.



Remarque

Lorsqu'un module hybride a été programmé, la centrale affiche le symbole  à côté du numéro du module hybride. Vous pouvez ajouter 2 modules hybrides maximum.

6. Quittez cet affichage avec **Retour**.

Modifier

Sélectionnez le module hybride correspondant. Les points de sous-menu suivants s'affichent.

Nom :

Attribuez un nom unique à ce module hybride.

Partitions

Numéros des partitions auxquelles est assigné le module hybride.



Remarque

Veuillez tenir compte de l'attribution des partitions du module hybride. Les messages du module hybride, par ex. Tamper ou Défaut CC, sont alors attribués à ces partitions.

Version logicielle >= 3.01.16

Cette attribution de partition détermine également l'attribution de zones et de sorties à des partitions.

Exemple : Si vous avez sélectionné ici les partitions 1 et 2, les zones et sorties de ce MoHy peuvent également uniquement être attribuées aux partitions 1 et 2.

Version logicielle < 3.01.16

Les zones et sorties du module hybride peuvent être attribuées à d'autres partitions, mais il doit s'agir des partitions du module hybride.

Type de zone filaire

Choisissez quel type de câblage doit être pris en charge aux entrées de zone de ce module hybride.



Remarque

Un type de câblage différent est possible pour la centrale et pour chacun des 2 modules hybrides.

Types de câblage possibles :

- 2 fils FSL 2k2/4k7
- 2 fils FSL 1k/1k
- 2 fils FSL 2k/2k
- 2 fils FSL 4k7/4k7
- 4 fils NC
- 2 fils CC

Les variantes sont les mêmes que sur la centrale, voir à ce sujet :

Système -> Matériel -> Type de zone filaire

Partitions haut-parleur

Sélectionnez les partitions pour lesquelles le haut-parleur raccordé en option doit émettre des signaux.



Remarque

Le haut-parleur émet des signaux sonores :

Vous pouvez régler le volume des différents signaux sonores du haut-parleur dans le menu utilisateur.

Menu utilisateur -> Configuration -> Réglages Volume ->

Tonalités opérateur

Tonalités info

Tonalités alarme



Remarque

Les partitions haut-parleur du module hybride peuvent être attribuées à d'autres partitions, mais il doit s'agir des partitions du module hybride.



Remarque

Zones

Type de zone et attributs

Sont sélectionnés dans la section Zones MoHy.

Tous les types et attributs disponibles sont possibles pour les zones filaires. Pour plus de détails, voir Zones IP.

Module hybride 1

401 à 410 lorsque 2 fils est sélectionné comme type de zone

401 à 405 lorsque 4 fils est sélectionné comme type de zone

Module hybride 2

411 à 420 lorsque 2 fils est sélectionné comme type de zone

411 à 415 lorsque 4 fils est sélectionné comme type de zone



Remarque

Sorties

Type de sortie et attributs

Sont sélectionnés dans la section Sorties MoHy.

Tous les types et attributs disponibles sont possibles pour les sorties filaires. Pour plus de détails, voir Sorties sans fil.

Module hybride 1

401 à 404

Module hybride 2

405 à 408



Remarque

Terminal TR sur module hybride

Si cette entrée du module hybride est commandée, la centrale signale

« Module hybride X générateur de signal sabotage »



Remarque

Terminal MAINS FAIL sur module hybride

Si cette entrée du module hybride est commandée, la centrale signale
« **Module hybride X défaut réseau PSU** »



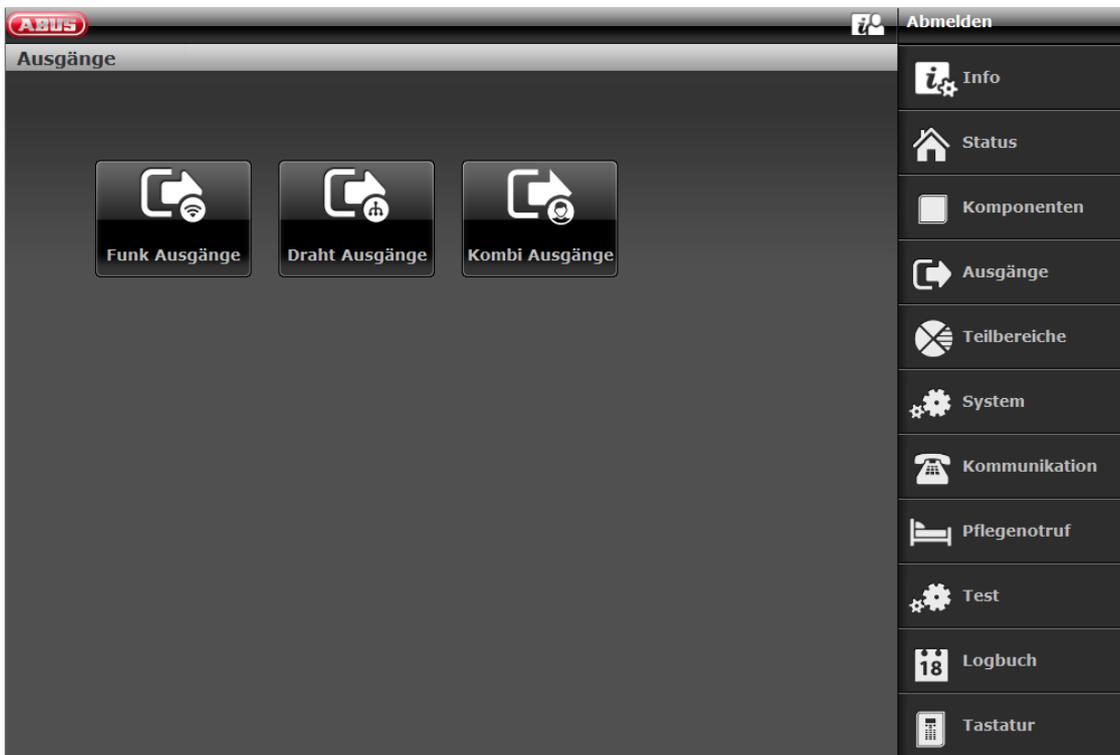
Remarque

Terminal LOW BATT sur module hybride

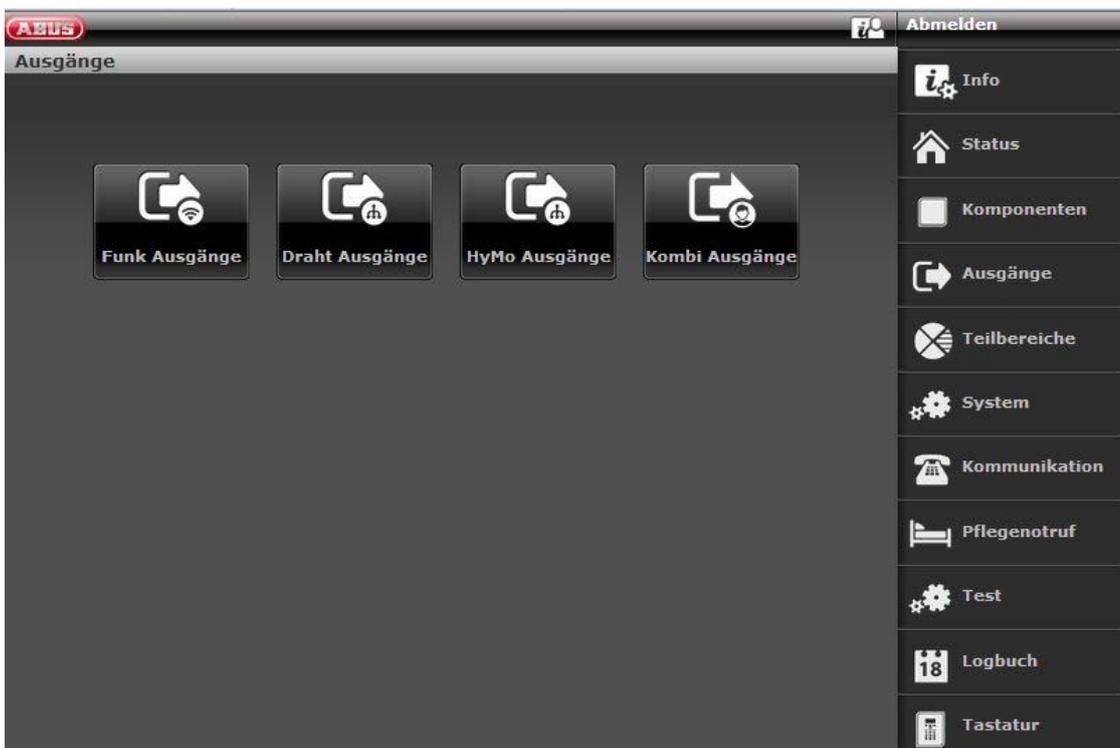
Si cette entrée du module hybride est commandée, la centrale signale
« **Module hybride X défaut batterie PSU** »

Sorties

Version logicielle < 3.01.14



Version logicielle >= 3.01.14



Sorties sans fil

ABUS
 Logout

Sorties

Numéro	Nom	Type	État	Attributs
Sortie Radio 201	"Ausgang 201"	Défini par U		
Sortie Radio 202	"Ausgang 202"	Non Utilisé		
Sortie Radio 203	"Ausgang 203"	Non Utilisé		
Sortie Radio 204	"Ausgang 204"	Non Utilisé		
Sortie Radio 205	"Ausgang 205"	Non Utilisé		
Sortie Radio 206	"Ausgang 206"	Non Utilisé		
Sortie Radio 207	"Ausgang 207"	Non Utilisé		
Sortie Radio 208	"Ausgang 208"	Non Utilisé		
Sortie Radio 209	"Ausgang 209"	Non Utilisé		
Sortie Radio 210	"Ausgang 210"	Non Utilisé		

◀
...
1
2
3
4
...
▶

INFO

État

Périphériques

Sorties

Partitions

Système

Transmissions

Appel Soins de Santé

Journal de bord

Clavier

Désignation/Fonction	Explication
Numéro	Le numéro comprend le type de périphérique (sortie radio) et le numéro séquentiel.
Nom	Nom unique de la sortie.
Type	Type de sortie radio.
État	État actuel de la sortie radio.
Propriétés	Attributs de la sortie radio.

Configuration des sorties radio

Remarque
La Secvest intègre jusqu'à 32 sorties radio.

Modification des sorties

1. Cliquez sur la ligne de la sortie souhaitée.

Remarque
Il est utile d'attribuer un nom de sortie unique afin de pouvoir identifier plus rapidement la sortie en cas de défaut.

2. **Supprimez** le nom prédéfini.
3. Attribuez un nom unique à la sortie comprenant 12 caractères maximum.

Inversion des sorties (polarité)

Remarque
Vous pouvez inverser ou non la sortie correspondante. Sélectionnez pour cela **Normal** ou **Inversé**.

Sélection du type de sortie

Remarque
Le tableau ci-après présente une vue d'ensemble des différents types de sortie.

4. Confirmez la sélection avec **Envoyer** après avoir terminé la configuration.

Type	Explication	Assignment possible de partitions
Non utilisé	Cette sortie n'est pas en fonction et n'est jamais activée.	Oui
Alarme intrusion	Cette sortie est activée lorsque l'un des types de zone ou événements suivants se déclenche lorsque la centrale est active : <ul style="list-style-type: none"> • Alarme immédiate tempo sortie • Sabotage (uniquement dans la centrale activée) • Route d'entrée • Zone sabotage (uniquement dans la centrale activée) • Temporisation d'entrée écoulée • Alarme 24H (uniquement dans la centrale activée) 	Oui
Conf. Alarme intrusion	Ce type fonctionne uniquement si le mode de confirmation BS8243 est sélectionné dans « Système -> Confirmation ». <p>Une alarme Intrusion confirmée s'est produite (alarme normale).</p> <p>La centrale active la sortie lorsque :</p> <ul style="list-style-type: none"> • Deux "alarmes normales" se sont déclenchées dans la même partition pendant le délai de confirmation. • Une "alarme normale" et un message de sabotage se sont déclenchés dans la même partition pendant le délai de confirmation. <p>On peut utiliser ce type de sortie pour une ou plusieurs partitions.</p> <p>Notez que les alarmes normales et les alarmes sabotage doivent se produire dans la même partition que la sortie.</p> <p>La sortie est désactivée lorsqu'un utilisateur réinitialise le système.</p>	Oui
Tps confirm. intrusion	La sortie est activée pendant la temporisation de la confirmation d'une alarme Intrusion et est désactivée une fois la temporisation écoulée.	Non
Périmètre d'avertissement	La sortie est activée en cas de déclenchement d'une alerte périmétrique.	Oui
Alarme agression	Cette sortie est activée en cas de déclenchement d'une alarme agression.	Oui
Confirmer Al. AGR	Une alarme agression confirmée s'est produite. <p>La centrale active la sortie dans les conditions suivantes :</p> <ul style="list-style-type: none"> • Les utilisateurs ont déclenché une alarme sur au moins deux médaillons d'alerte pendant le délai de confirmation de l'agression. • Un médaillon d'alerte est activé et l'alarme anti-sabotage d'un médaillon d'alerte s'est déclenchée pendant le délai de confirmation. <p>On peut affecter ce type de sortie à une ou plusieurs partitions. Notez que les médaillons d'alerte (et les avertissements anti-sabotage) doivent être affectés à la même partition.</p> <p>La sortie est désactivée dès qu'un utilisateur réinitialise le système.</p>	Non

Programmation/configuration

Type	Explication	Assignment possible de partitions
Tps confirme alarme AGR	La sortie est activée pendant la temporisation de la confirmation d'une alarme agression et est désactivée après écoulement de la temporisation.	Non
Code contrainte	Un code "contrainte" a été utilisé. La centrale active la sortie dès qu'un utilisateur entre un code contrainte et désactive la sortie uniquement lorsque l'utilisateur a réinitialisé le système.	Oui
Alarme confirmée	Cette sortie est activée lorsqu'une alarme est interrompue par l'utilisateur pendant le délai possible dans la partition sélectionnée. La sortie est réactivée lorsque l'alarme est confirmée.	Oui
Incendie	Cette sortie est activée en cas d'activation d'une alarme feu.	Oui
Technique	Cette sortie est activée lorsqu'une zone possédant l'attribut Technique a déclenché une alarme. Elle est désactivée dès que la zone à l'origine de l'alarme est réinitialisée (résolution de la cause de l'alarme technique) ET dès que l'utilisateur confirme l'alarme technique sur la centrale à l'aide d'un code valide.	Oui
24 heures	Cette sortie est activée lorsqu'une zone possédant l'attribut "Alarme 24H" a déclenché une alarme.	Oui
Alarme de zone	La sortie est activée quand la zone sélectionnée signale une alarme et est à nouveau désactivée lorsque l'alarme est réinitialisée.	Non
Sirène externe	Cette sortie est activée en cas d'alarme locale dans la partition sélectionnée pendant la durée de sirène externe définie. La sortie ne commute pas en cas d'alarme technique ou d'alarme agression.	Oui
Sirène interne	Cette sortie est activée en cas d'alarme locale dans la partition sélectionnée pendant la durée de sirène interne définie. La sortie ne commute pas en cas d'alarme technique ou d'alarme agression.	Oui
Flash extern.	Cette sortie est activée en cas d'alarme locale dans la partition sélectionnée et reste active jusqu'à la désactivation de la centrale sans fil. Parallèlement, la sortie est activée pendant 10 secondes après l'activation réussie de la partition, si le signal flash EXTERNE a été activé pour la confirmation.	Oui
Flash intern.	Cette sortie est activée en cas d'alarme locale dans la partition sélectionnée et reste active jusqu'à la désactivation de la centrale sans fil. Parallèlement, la sortie est activée pendant 10 secondes après l'activation réussie de la partition, si le signal flash INTERNE a été activé pour la confirmation.	Oui
Alarme annulation	Cette sortie est activée lorsqu'une alarme est interrompue par l'utilisateur pendant le délai possible dans la partition sélectionnée. La désactivation s'effectue dès que l'alarme est confirmée.	Oui

Type	Explication	Assignment possible de partitions
Alarme annulation	Cette sortie est activée lorsqu'une alarme est interrompue par l'utilisateur pendant le délai possible dans la partition sélectionnée. La désactivation s'effectue dès que l'alarme est confirmée.	Oui
Alarme Alarme	Cette sortie est activée en cas d'appel médical d'urgence.	Oui
Appel d'urgence de soin	Cette sortie est activée en cas d'appel soins de santé.	Oui
Sabotage	La sortie est activée lorsque la centrale reçoit un message sabotage de l'un des appareils suivants : <ul style="list-style-type: none"> • Centrale d'alarme (couvercle ou arrachement) • Élément de commande (couvercle ou arrachement) • Zone de type "Sabotage" • Tous les détecteurs sans fil ou WAM • Sirènes La centrale d'alarme désactive la sortie dès que le sabotage a été éliminé.	Oui
Défaut radio	Cette sortie est activée dès que survient l'un des trois défauts radio ci-dessous. Il peut s'agir de : RF Batterie basse, RF Supervision, RF Brouillage. La désactivation de la sortie s'effectue uniquement en cas de réinitialisation sur la centrale.	Oui
RF Supervision	Cette sortie est activée dès qu'une zone sans fil signale un défaut supervision. La sortie reste activée tant que tous les défauts supervision ne sont pas fermés.	Oui
RF Brouillage	La sortie correspondante commute en cas de détection de brouillage. La sortie reste activée jusqu'à l'élimination du brouillage radio.	Non
RF Batterie basse	La sortie est activée dès qu'un détecteur sans fil envoie un message de batterie faible. La sortie reste activée jusqu'à ce que tous les détecteurs n'envoient plus de messages de ce type.	Oui
Défaut batterie	La sortie est activée lorsque la centrale constate un défaut sur la batterie de secours OU si une zone de type « PSU Ext Défaut Batt » a été déclenchée. Si l'alarme a été déclenchée par une zone avec « PSU Ext Défaut Batt », la centrale désactive la sortie uniquement quand la zone même a été réinitialisée et l'utilisateur a confirmé le défaut sur la centrale avec un code valide. Si l'alarme a été déclenchée par un défaut de la batterie de secours, la sortie est à nouveau désactivée dès que la centrale détecte une batterie adaptée et opérationnelle. Remarque : Vérifiez le fonctionnement de la batterie à l'aide de la fonction de test via le menu sur la centrale.	Non

Type	Explication	Assignment possible de partitions
Défaut A/C	<p>La sortie est activée si la centrale n'est pas sous tension OU si une zone de type « PSU Ext Défaut A/C » a été déclenchée.</p> <p>La temporisation d'activation de cette sortie dépend de la valeur définie dans « Système -> Tempo Défaut A/C [min] (minutes) ».</p> <p></p> <p>Remarque L'installation est conforme à la norme VdS , lorsqu'elle utilise ce type de sortie pour signaler un défaut CA.</p>	Non
Défaut PSU Ext	<p>La sortie est activée lorsqu'une alimentation externe détecte un défaut et que celui-ci est signalé par le type de zone « Défaut PSU Ext ».</p> <p>La sortie est désactivée uniquement lorsque le défaut a été résolu et l'utilisateur a confirmé l'alarme avec un code valide sur la centrale.</p>	Non
PSU Ext tension faible	<p>La sortie est activée lorsqu'une alimentation externe détecte une tension basse par le type de zone « PSU Ext tension faible ».</p> <p>La centrale désactive la sortie dès que la zone a été réinitialisée et que l'utilisateur a confirmé le défaut avec un code valide.</p>	Non
Défaut général	<p>La sortie est activée dès que survient un événement entraînant un défaut.</p> <p>Il peut s'agir de :</p> <ul style="list-style-type: none"> • RF Batterie basse • RF Supervision • RF Brouillage • Défaut A/C • Défaut batterie • Défaut PSU Ext • Sabotage <p>Notez que la sortie s'active quelques secondes après la détection du défaut A/C et N'EST PAS influencée par la temporisation définie.</p> <p></p> <p>Danger Version logicielle < 3.01.11 L'installation n'est plus conforme à la norme VdS lorsque vous utilisez ce type de sortie pour signaler un défaut CA, car il se déclenche directement. Pour la signalisation, utilisez le type défaut CA pour rester conforme à la norme VdS.</p> <p></p> <p>Remarque</p>	Oui

	Version logicielle >= v3.01.11 L'installation est conforme à la norme VdS , lorsqu'elle utilise ce type de sortie pour signaler un défait CA . Ce type de sortie est désormais déclenché lors d'un défaut CA après une temporisation conforme à VdS.	
Défaut ligne	La sortie est activée dès que la centrale constate un défaut de la ligne de transmission et est désactivée en l'absence (en cas de disparition) du défaut.	Non
Prêt pour arm. total	Cette sortie s'active lorsque la partition est prête à être activée. Lorsqu'un détecteur est assigné à plusieurs partitions, la partition correspondante est prête même si ce détecteur est encore ouvert.	Oui
Arm total complet	La sortie s'active dès que le système a correctement effectué l'activation. La sortie s'active pendant env. 10 secondes.	Oui

Programmation/configuration

Type	Explication	Assignment possible de partitions
Tous act.	Cette sortie s'active uniquement lorsque toutes les partitions configurées dans le système ont été activées.	Oui
Armement réalisé	Cette sortie s'active lorsque le système ou la partition a été activé(e) ou activé(e) en interne (pendant env. 10 secondes).	Oui
Activé	Cette sortie s'active lorsque la partition est activée.	Oui
Réarmé	La sortie s'active dans un système activé en interne si le système a été réactivé au moins une fois. Si le mode confirmation a été réglé sur DD243 ou BS8243, la centrale active la sortie dès que le système est réactivé (après le délai de confirmation). Si le mode confirmation a été réglé sur "Basique", la centrale active la sortie dès que le système est réactivé (après écoulement de la durée de la sirène). Dans une système comprenant des partitions, on peut assigner plusieurs partitions à la sortie. La sortie est à nouveau désactivée lorsqu'un utilisateur ou l'installateur réinitialise le système ou la partition.	Oui
Prêt pour arm. partiel	Cette sortie s'active lorsque la partition est prête à être activée en interne. Lorsqu'un détecteur est assigné à plusieurs partitions, la partition correspondante est prête même si ce détecteur est encore ouvert.	Oui
Arm partiel complet	Cette sortie s'active lorsque le système ou la partition a été activé(e) en INTERNE (pendant env. 10 secondes).	Oui
Act. interne	Cette sortie s'active lorsqu'une partition est activée en interne.	Oui
Défaut arm.	Cette sortie s'active en cas d'échec de l'activation. Elle reste active jusqu'à ce que l'utilisateur confirme le défaut.	Oui
Act. autom. Avertissement	Cette sortie est activée lorsque le temps d'avertissement pour l'activation automatique s'écoule. (voir le menu utilisateur Calendrier arm./désarm.). Cette sortie se désactive lorsque l'activation s'est produite ou un utilisateur retarde ou annule l'activation automatique.	Oui
Désarm. compl.	La sortie s'active dès que la centrale a été désactivée ou se désactive à l'issue d'une alarme. La sortie commute pendant env. 10 secondes.	Oui
Zones isolées (lors arm.)	Cette sortie s'active lorsque l'utilisateur isole une zone pendant qu'il active la centrale. La sortie est désactivée dès que la centrale d'alarme réinitialise la zone.	Oui

Type	Explication	Assignment possible de partitions
Zones isolées (système)	(La sortie fonctionne uniquement si le mode confirmation DD243 ou BS8243 est sélectionné). En cas d'alarme non confirmée, la centrale se réactive lorsque le délai de confirmation est écoulé. Si la zone ayant causé l'alarme non confirmée est encore ouverte au moment de la réactivation, la centrale isolera cette zone et activera cette sortie. La centrale réinitialisera la zone et réactivera la sortie lorsqu'un utilisateur ou l'installateur réinitialise le système.	
Entrée/Sortie suiveuse	Cette sortie s'active pendant le délai de temporisation (temporisation d'entrée ou de sortie). La sortie ne commute pas si la partition a été configurée en mode "Armement immédiat" ou "Armement silencieux".	Oui
Verrouillage activé ouvert	Une zone de blocage est présente. La centrale active la sortie dès qu'une zone de type "Blocage" est déclenchée et désactive la sortie quand la zone est fermée.	Non
Début/Fin	La sortie s'active quand le système (ou la partition) est désactivé(e). Elle se désactive quand le système (ou la partition) est activé(e). Si vous affectez plusieurs partitions à cette sortie, la sortie est désactivée dès que l'une de ces partitions est active ou active en interne. Remarque : Comparée à d'autres sorties, celle-ci est déjà inversée par le réglage par défaut. La tension électrique est de 0 V si le système est désactivé.	Oui
Suivant zone	Cette sortie suit l'état d'une zone. Si vous avez sélectionné ce type, vous obtenez une vue d'ensemble des zones. Sélectionnez une zone correspondante.	Non
Éclairage de courtoisie	Cette sortie s'active pendant l'écoulement du délai de temporisation d'entrée/de sortie et se désactive 10 secondes après l'écoulement du délai de temporisation d'entrée/de sortie.	Oui
Install. sur site	La sortie s'active dès que le système se trouve en mode Installateur et se désactive dès que l'installateur l'a quitté avec succès.	Non
Test de détection	La sortie est activée lorsqu'un utilisateur démarre un test de détection aussi bien en tant qu'installateur qu'en tant qu'utilisateur normal. Pendant le délai entre la mise en silencieux d'une alarme et la confirmation d'alarme, la sortie est également activée.	Non

Type	Explication	Assignment possible de partitions
Défini par U	<p>Une sortie de ce type peut être commandée à distance de manière personnalisée via différents périphériques, notamment une télécommande, un élément de commande ou une centrale d'alarme.</p> <p>Les options « Utilisateur commutable » et « Utilisateur configurable » confèrent à l'utilisateur des droits d'accès à la configuration de la sortie dans l'écran Menu utilisateur. Le bouton « Polarité » permet d'inverser les états de commutation.</p> <p>Si la sortie ne doit être activée que pendant un certain temps (réponse impulsionnelle), désélectionnez la case correspondant au bouton « En continu » et réglez la durée souhaitée.</p> <p>Par ailleurs, la sortie peut être associée à une programmation qui détermine quand elle doit être activée ou désactivée. Il faut pour cela cocher la case correspondant au bouton « En continu ». Réglez ensuite les heures d'activation et de désactivation, puis sélectionnez les jours de semaine souhaités.</p> <p>La sortie peut aussi être activée par des événements qui surviennent. Vous pouvez définir jusqu'à 3 événements dans l'onglet « Événement ». La liste contient tous les types de sortie possibles.</p>	Non
RAZ détecteur autonome avertisseur de fumée	<p>Cette sortie est toujours activée (0V) sauf si un utilisateur confirme une alarme feu.</p> <p>Après une telle confirmation, le système désactive la sortie pendant 3 secondes.</p> <p>Le type de sortie est conçu pour interagir avec les connexions de réinitialisation basse tension sur les détecteurs de fumée filaires.</p> <p>Notez qu'il existe également des détecteurs de fumée exigeant une double confirmation de réinitialisation (détecteurs ayant besoin de temps pour réinitialiser les contacts d'alarme après une impulsion de réinitialisation).</p>	Oui
Arm PIR filaire	<p>La condition préalable est l'activation de la centrale ou de la partition.</p> <p>Cette sortie se désactive quand la centrale ou la partition est désactivée ou si un événement alarme se produit.</p> <p>En revanche, la sortie s'active pendant une seconde en cas de réinitialisation ou si le mode installateur est fermé sur la centrale.</p> <p>Remarque : Si la polarité "normale" est sélectionnée, la sortie est commandée avec + 12 V si elle a été activée et 0 V si elle a été désactivée. Définissez la polarité "inversée" pour inverser ce comportement.</p>	Oui
Sortie mixte 1	<p>Une sortie de ce type combine différents événements. Vous trouverez des détails à ce sujet dans le chapitre « Sorties mixtes ».</p>	
...		
Sortie mixte 10		

Sorties filaires

Logout

Sorties				
Numéro	Nom	Type	État	Attributs
Sortie Filaire 301	"Ausgang 301"	Non Utilisé		
Sortie Filaire 302	"Ausgang 302"	Non Utilisé		
Sortie Filaire 303	"Ausgang 303"	Non Utilisé		
Sortie Filaire 304	"Ausgang 304"	Non Utilisé		

INFO
 État
 Périphériques
 Sorties
 Partitions
 Système
 Transmissions
 Appel Soins de Santé
 Journal de bord
 Clavier

Désignation/Fonction	Explication
Numéro	Le numéro comprend le type de périphérique (sortie filaire) et le numéro séquentiel.
Nom	Nom unique de la sortie filaire.
Type	Type de sortie filaire.
État	État actuel de la sortie filaire.
Propriétés	Attributs de la sortie filaire.

Configuration des sorties filaires

Remarque
La Secvest intègre jusqu'à quatre sorties filaires.

Modification des sorties

1. Cliquez sur la ligne de la sortie souhaitée.

Remarque
Il est utile d'attribuer un nom de sortie unique afin de pouvoir identifier plus rapidement la sortie en cas de défaut.

2. **Supprimez** le nom prédéfini.
3. Attribuez un nom unique à la sortie comprenant 12 caractères maximum.
4. Confirmez la sélection avec **Envoyer** après avoir terminé la configuration.

Inversion des sorties (polarité)

Remarque
Vous pouvez inverser ou non la sortie correspondante. Sélectionnez pour cela **Normal** ou **Inversé**.

Sélection du type de sortie

Remarque
La section Sorties sans fil présente une vue d'ensemble des différents types de sortie.

1. Sélectionnez l'option de menu **Type**.

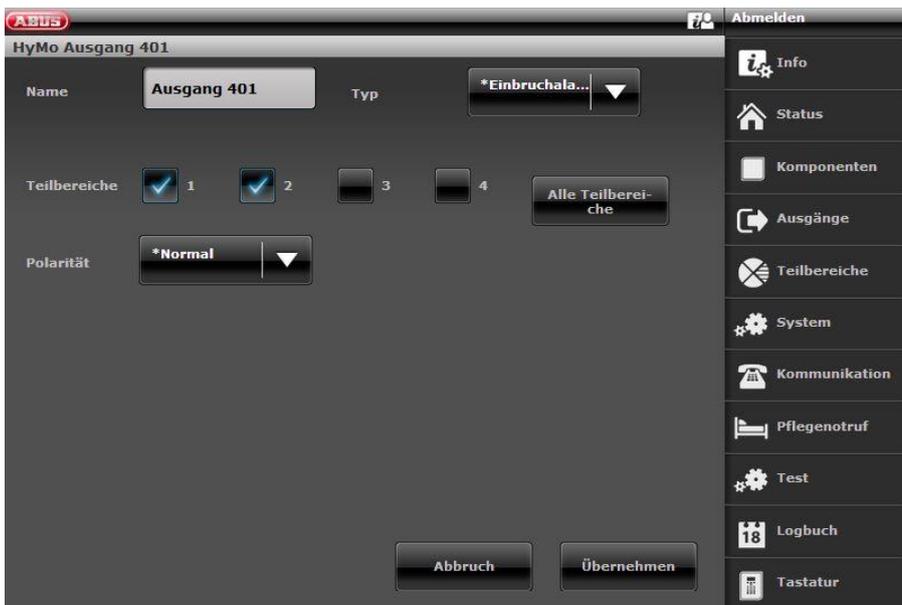
Sorties MoHy

ABUS
Abmelden

Ausgänge			
Nummer	Name	Typ	Status
HyMo Ausgang 401	"Ausgang 401"	Einbruchalarm	Aus
HyMo Ausgang 402	"Ausgang 402"	Aktivierung fertig	Aus
HyMo Ausgang 403	"Ausgang 403"	RF Batt. schwach	Aus
HyMo Ausgang 404	"Ausgang 404"	Ben. definiert	Aus
HyMo Ausgang 405	"Ausgang 405"	Überfallalarm	Aus
HyMo Ausgang 406	"Ausgang 406"	Einbruchalarm	Aus
HyMo Ausgang 407	"Ausgang 407"	Externe Sirene	Aus
HyMo Ausgang 408	"Ausgang 408"	Externer Blitz	Aus

Info
Status
Komponenten
Ausgänge
Teilbereiche
System
Kommunikation
Pflegetruf
Test
18 Logbuch
Tastatur

Désignation/Fonction	Explication
Numéro	Le numéro comprend le type de périphérique (sortie MoHy) et le numéro séquentiel.
Nom	Nom unique de la sortie filaire MoHy.
Type	Type de sortie filaire MoHy.
État	État actuel de la sortie filaire MoHy.



Configuration des sorties MoHy



Remarque

Chaque module hybride dispose de quatre sorties de relais ou sorties filaires.

Modification des sorties

1. Cliquez sur la ligne de la sortie souhaitée.



Remarque

Il est utile d'attribuer un nom de sortie unique afin de pouvoir identifier plus rapidement la sortie en cas de défaut.

2. **Supprimez** le nom prédéfini.
3. Attribuez un nom unique à la sortie comprenant 12 caractères maximum.
4. Confirmez la sélection avec **Envoyer** après avoir terminé la configuration.

Inversion des sorties (polarité)

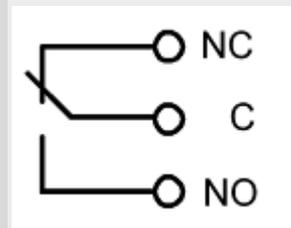


Remarque

Vous pouvez inverser ou non la sortie correspondante. Sélectionnez pour cela **Normal** ou **Inversé**.

La sortie du MoHy est une sortie relais.

Si **Normal** est sélectionné :



Vous pouvez ouvrir (NC-C) ou fermer (NO-C) un circuit électrique raccordé.

Si **Inversé** est sélectionné, le comportement est inversé !

Vous pouvez ouvrir (NO-C) ou fermer (NC-C) un circuit électrique raccordé.

Sélection du type de sortie



Remarque

La section Sorties sans fil présente une vue d'ensemble des différents types de sortie.

1. Sélectionnez l'option de menu **Type**.



Remarque

Version logicielle \geq 3.01.16

Les sorties du module hybride peuvent uniquement être attribuées aux partitions auxquelles le module hybride est également attribué. Exemple : Si vous avez sélectionné les partitions 1 et 2 pour le MoHy, les sorties de ce MoHy peuvent également uniquement être attribuées aux partitions 1 et 2.

Veillez tenir compte de l'attribution des partitions du module hybride. Les messages du module hybride, par ex. Tamper ou Défaut CC, sont alors attribués à ces partitions.

Version logicielle $<$ 3.01.16

Les sorties du module hybride peuvent être attribuées à d'autres partitions, mais il doit s'agir des partitions du module hybride.

Veillez tenir compte de l'attribution des partitions du module hybride. Les messages du module hybride, par ex. Tamper ou Défaut CC, sont alors attribués à ces partitions.



Remarque

Sorties

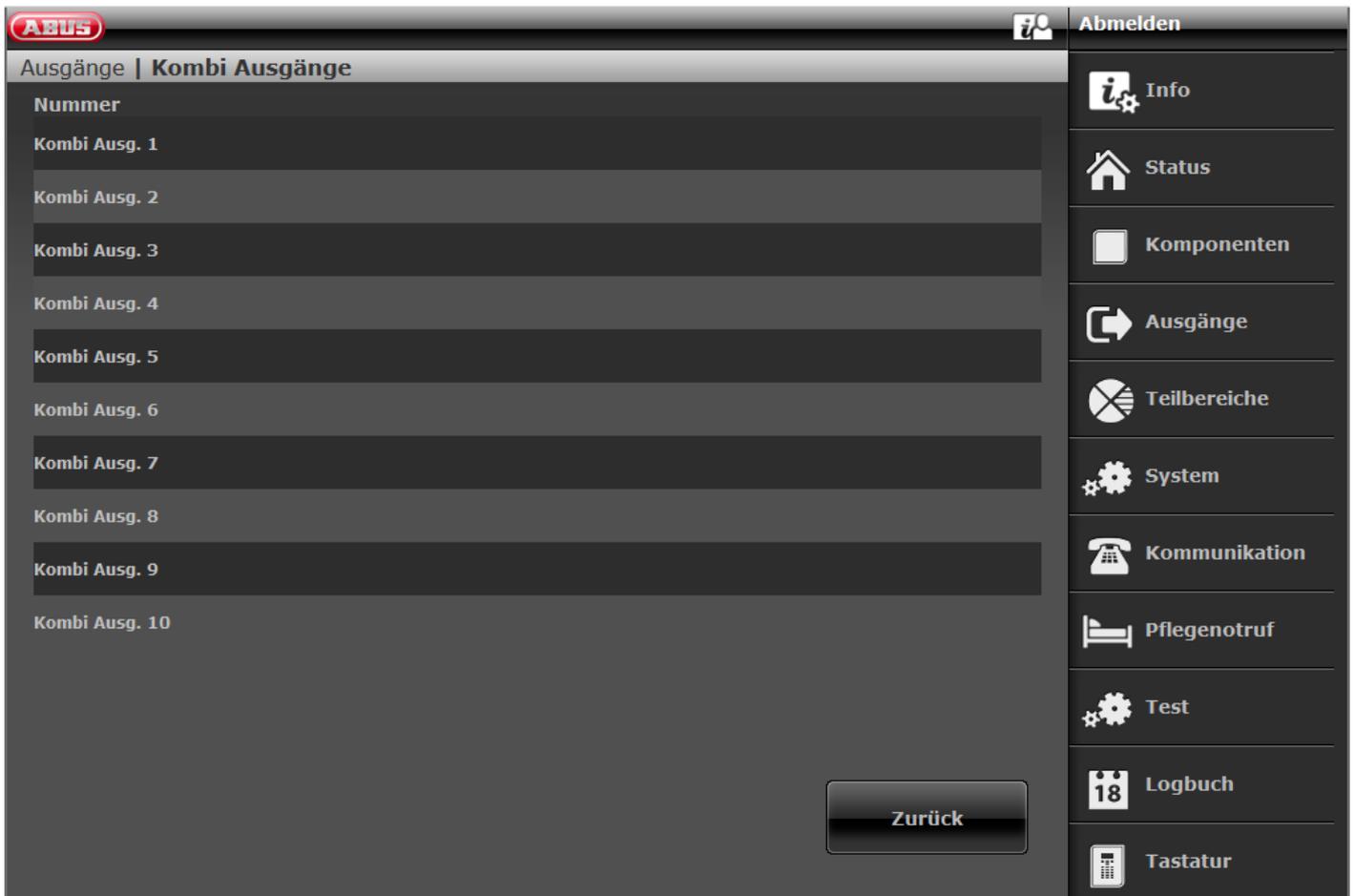
Module hybride 1

401 à 404

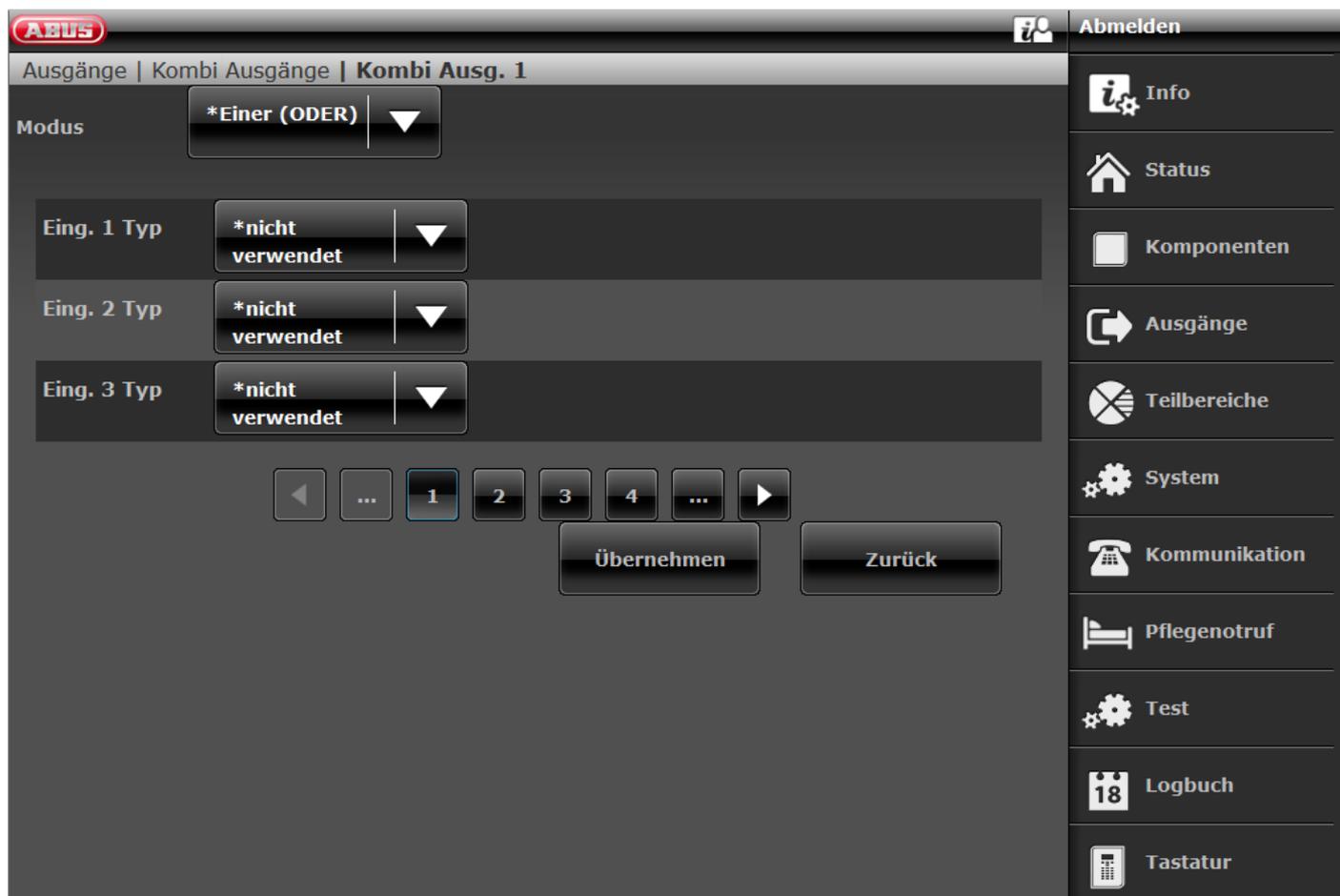
Module hybride 2

405 à 408

Sorties mixtes



Une « sortie mixte » est un élément logique virtuel au sein de la centrale d'alarme. Elle s'apparente à une porte ET ou à une porte OU dans l'électronique numérique, mais n'existe qu'au sein de la configuration de la centrale d'alarme. Une « sortie mixte » peut posséder jusqu'à 10 entrées virtuelles. Une entrée virtuelle est un événement tel qu'une « Alarme intrusion » ou une « Alarme agression ».



Vous pouvez utiliser une « Sortie mixte » pour activer une sortie sans fil ou filaire.
 Pour ce faire, sélectionnez pour une sortie sans fil ou filaire le type « Sortie mixte ».

Vous avez sélectionné « Sortie mixte 1 ». Vous souhaitez l'utiliser pour activer la « Sortie sans fil 203 » de la centrale d'alarme. Attribuez le type « Sortie mixte 1 » à la « Sortie sans fil 203 ».

Vous devez sélectionner un mode pour chaque « Sortie mixte ». Ce mode peut soit être TOUT (ET), soit CERTAINS (OU).

Pour le mode ET, **toutes** les entrées de la « Sortie mixte » doivent être actives afin que la « Sortie mixte » soit active.
 Pour le mode OU, **certaines** entrées de la « Sortie mixte » doivent être actives afin que la « sSortie mixte » soit active.

Exemple :

Demande :

Une sortie sans fil doit commuter si une porte (zone 203) est ouverte ET qu'un installateur s'est connecté en mode installateur.

Solution :

Configurez la sortie sans fil avec le type « Sortie mixte 1 » et configurez la « Sortie mixte 1 » comme suit :

Sortie mixte	Mode	Entrée
1	TOUT (ET)	Type entrée 1 = installateur sur site Type entrée 2 = suivant zone (zone 203)



Remarque

Une entrée peut être la sortie d'une autre « Sortie mixte ». Vous pouvez cependant uniquement sélectionner « Sorties mixtes » avec un nombre plus élevé d'entrées.

Si par ex. la centrale d'alarme prend en charge 10 « Sorties mixtes » et que vous définissez « Sortie mixte 8 », vous pouvez uniquement utiliser les sorties de la « Sortie mixte 9 » et de la « Sortie mixte 10 » en tant qu'entrées.

Partitions

ABUS
 Logout

Index	Name
Partition 1	"Partition 1"
Partition 2	"Partition 2"
Partition 3	"Partition 3"
Partition 4	"Partition 4"
Lien Arm. compl.	Partitions: Aucun(e)

INFO

État

Périphériques

Sorties

Partitions

Système

Transmissions

Appel Soins de Santé

Journal de bord

Clavier

Désignation/Fonction	Explication
Index	Liste des partitions Partition 1 à 4 et lien arm. compl.
Nom	Nom de la partition attribuée lors de la programmation. Dans la ligne « Lien arm. compl. » s'affichent les partitions sélectionnées
Lien arm. compl.	Cette option permet de définir une partition commune. La partition 1 est toujours la partition commune. Vous pouvez relier la partition 1 à d'autres partitions. Cela signifie que, quand toutes les partitions reliées sont activées, la partition 1 s'active automatiquement. Le système réagit en cas d'alarme en fonction des réponses alarme programmées de la partition 1.

Configuration de partitions

Consultez le manuel d'utilisateur pour connaître les détails relatifs à l'activation et à la désactivation du système, sur le comportement de la centrale et l'affichage (interface utilisateur). Choisissez pour chaque partition un nom unique, par ex. Appartement, Atelier, Bureau, etc. (max. 12 caractères) !

Tous act.

Désignation/Fonction	Explication
Nom	Nom unique de la partition. Vous pouvez nommer ici la partition, par ex. maison, atelier, bureau. Le nom peut comprendre 12 caractères maximum. La centrale affiche ce nom pour l'utilisateur même lors de l'activation.
Tous act.	Réglages d'activation complète de la partition.
Mode sortie	Sélectionnez ici le mode d'activation lorsque vous quittez les lieux. Remarque : voir également le manuel d'utilisateur, chapitre « 8. Activation et désactivation de l'installation
	<p>Armement temporisé</p> <ul style="list-style-type: none"> Utilisez cette option pour activer la partition uniquement après un certain délai. Sélectionnez la temporisation de sortie dans "Tps sortie". La centrale enregistre le début de cette activation temporisée. Cette option n'est pas conforme à BS8243:2010.

Désignation/Fonction	Explication
Mode sortie, suite	<p>Sortie finale armement</p> <ul style="list-style-type: none"> Utilisez cette option pour exclure l'activation d'une partition en fermant une dernière porte de sortie. Cette porte possède un détecteur avec le type de zone "Entrée/Sortie". Si la porte a été fermée, la partition s'active après écoulement du temps supplémentaire. Notez que la temporisation de sortie de cette option est infinie, c'est-à-dire que lorsque la zone est fermée (porte fermée), la centrale attend, lors de l'activation, que cette zone soit ouverte puis refermée. La centrale enregistre l'heure de démarrage de l'activation (et non pas l'activation même) dans l'historique. N'essayez pas d'utiliser une zone PIR en tant qu'entrée/sortie pour une partition. Les détecteurs sans fil PIR disposent d'un délai de "blocage" après chaque activation pour préserver la batterie. Si vous activez une partition (ou l'activez en interne), un détecteur PIR peut encore être bloqué. Pendant ce délai, il ne peut pas envoyer de signal d'achèvement du processus d'activation. <p>Armement immédiat</p> <ul style="list-style-type: none"> La partition est immédiatement activée sans signal d'avertissement acoustique. Lorsque la partition a été activée, la confirmation est acoustique. Remarque : Cette option n'est pas conforme à BS8243:2010. <p>Armement silencieux</p> <ul style="list-style-type: none"> La partition est activée après écoulement de la temporisation de sortie. Sélectionnez la temporisation de sortie dans "Tps sortie". Aucun signal sonore n'est cependant émis pendant ce délai. Lorsque la partition a été activée, la confirmation est acoustique. La centrale enregistre l'heure de démarrage dans l'historique. Les signaux sonores sont audibles pendant le temps d'entrée. Remarque : Cette option n'est pas conforme à BS8243:2010. <p>Verrouillage activé</p> <ul style="list-style-type: none"> Le mode "Verrou activ." influence aussi bien l'activation que la désactivation de la partition. <p>Pour ce mode, vous devez prévoir un détecteur avec le type de zone "Verrou activ." et un détecteur avec le type de zone "Entrée/Sortie" sur la dernière porte de sortie. Le détecteur avec le type de zone "Verrou activ." est utilisé sur une serrure adaptée avec un contact de verrouillage.</p> <p>Activation de la partition</p> <ul style="list-style-type: none"> L'utilisateur doit d'abord démarrer la séquence d'activation à l'aide de son code utilisateur, de son badge de proximité ou de sa télécommande. La centrale émet la tonalité de sortie et enregistre l'heure de démarrage dans l'historique. Si la zone de type "Entrée/sortie" est ouverte, la centrale émet une tonalité de sortie interrompue. La tonalité de sortie retentit jusqu'à ce que l'utilisateur : <ol style="list-style-type: none"> ferme la dernière porte de sortie et ; verrouille la porte en actionnant le contact de verrouillage. Après activation du contact de verrouillage, la partition s'active à l'issue du temps supplémentaire. Par ailleurs, la zone de type "Entrée/Sortie" est transformée en zone de type "Alarme immédiate tempo sortie". La centrale enregistre l'activation de la zone de type "Verrou activ." dans l'historique.

Désignation/Fonction	Explication
Mode sortie, suite	<p>Désactivation de la partition</p> <ul style="list-style-type: none"> • L'utilisateur déverrouille la porte et actionne ainsi le contact de verrouillage. La zone de type "Verrou activ." s'ouvre. La centrale enregistre l'activation de la zone de type "Verrou activ." dans l'historique. La zone initialement de type "Entrée/Sortie" transformée en zone de type "Alarme immédiate tempo sortie" redevient une zone de type "Entrée/Sortie". Le délai d'entrée commence à s'écouler à l'ouverture de la porte. La tonalité d'entrée qui retentit maintenant est différente de la tonalité d'entrée normale. • Si l'utilisateur verrouille à nouveau la porte sans que le délai d'entrée n'ait démarré, la centrale reste active ; la zone de type "Entrée/Sortie" redevient une zone de type "Alarme immédiate tempo sortie". La centrale interrompt la tonalité d'avertissement. • Pour être conforme à BS8243, "Après Entrée" doit être réglé sur "Jamais" pour verrouiller la confirmation. <p>Annulation de la temporisation de sortie</p> <ul style="list-style-type: none"> • Activation de la partition • L'utilisateur doit d'abord démarrer la séquence d'activation. Puis, il doit terminer l'activation après avoir quitté la partition surveillée. • L'utilisateur peut démarrer la séquence d'activation à l'aide de son code utilisateur, de son badge de proximité ou de sa télécommande. (Remarque : l'activation avec la télécommande ne doit pas être réglée sur "Immédiat", Mode installateur->Système->Accès utilisateur->Téléco arm. immédiat). • L'utilisateur termine l'activation en actionnant une zone de type "Annuler temporisation de sortie" (voir l'explication des types de zone). • Notez que le temps de sortie de cette option est infini, c'est-à-dire que la centrale d'alarme attend d'avoir reçu le signal d'arrêt du processus d'activation. Pendant ce temps, la centrale d'alarme émet la tonalité de sortie. Elle enregistre l'heure de démarrage de l'activation (et non pas l'activation même) dans l'historique. La partition est activée après écoulement du temps supplémentaire. • Désactivation de la partition • L'utilisateur peut utiliser sa télécommande. Mais l'utilisateur peut également ouvrir la porte. La zone de type "Entrée/sortie" sur cette porte démarre le temps d'entrée. Pendant le temps d'entrée, l'utilisateur doit désactiver la partition à l'aide de son code utilisateur ou de son badge de proximité sur la centrale d'alarme ou l'élément de commande. (La dernière méthode n'est pas conforme à BS8243 clause 6.4.) <p>Comme part. (partition) 1</p> <p>Cette option est disponible pour les partitions 2, 3 et 4. Si vous choisissez cette option, la centrale d'alarme utilise le même type que pour la partition 1.</p>
Temps supplémentaire [s]	<p>Cette option s'affiche uniquement pour les modes "Entrée/sortie activée", "Verrou activ." et "Annuler temporisation de sortie".</p> <p>Cette option vous permet de définir une temporisation afin que les détecteurs puissent se stabiliser avant l'activation de la partition. Ceci peut être nécessaire si des détecteurs se sont déclenchés, envoient un signal d'alarme et n'ont pas encore été réinitialisés. Pendant ce temps, la centrale d'alarme ignore les signaux d'alarme des détecteurs et les sirènes ne se déclenchent pas. Entrez 2 chiffres pour la durée en secondes de 01 à 30. La programmation d'usine du temps supplémentaire est de 15 secondes. Ainsi, les PIR radio, qui se trouvent sur la voie de sortie et qui se sont déclenchés, peuvent se stabiliser et se réinitialiser.</p>

Désignation/Fonction	Explication
Temps de sortie [s]	<p>Cette option s'affiche uniquement pour les modes "Armement temporisé" et "Armement silencieux".</p> <p>Durée de la temporisation de sortie en secondes.</p> <p>Le temps de sortie peut être compris entre 10 et 120 secondes.</p>
Temps d'entrée [s]	<p>Durée de la temporisation d'entrée en secondes.</p> <p>Le temps d'entrée peut être compris entre 10 et 120 secondes.</p>
Réponse alarme	<p>Sélectionnez ici la réponse en cas d'alarme dans cette partition.</p> <p>Interne</p> <ul style="list-style-type: none">• Centrale, sirène d'intérieur, module d'information et élément de commande. <p>Sirène</p> <ul style="list-style-type: none">• Centrale, sirène d'intérieur, module d'information et élément de commande.• Sirènes d'extérieur <p>Sirène + TS Reporting</p> <ul style="list-style-type: none">• Centrale, sirène d'intérieur, module d'information et élément de commande.• Sirènes d'extérieur• Communication avec AES/NSL <p>Une temporisation de sirène est effective en cas de réponse alarme « Sirène + Reporting STS ».</p> <p>Flash</p> <ul style="list-style-type: none">• Centrale, sirène d'intérieur, module d'information et élément de commande.• Sirènes extérieures (uniquement avec FLASH) <p>Flash + TS Reporting</p> <ul style="list-style-type: none">• Centrale, sirène d'intérieur, module d'information et élément de commande.• Sirènes extérieures (uniquement avec FLASH)• Communication avec AES/NSL <p>Une temporisation de sirène est effective en cas de réponse alarme « Flash + Reporting STS ».</p> <p> Remarque</p> <p>Lorsque « Temporisation de sirène (spécifique à l'utilisateur) » est activé (> 0), le comportement de la temporisation de sirène est le suivant :</p> <p>Temporisation de sirène (utilisateur) a uniquement des effets sur les sirènes d'extérieur pour les configurations suivantes :</p> <p>Partition -> Réponse alarme</p> <p style="padding-left: 40px;">Sirène + Reporting STS ou</p> <p style="padding-left: 40px;">Flash + TS Reporting</p> <p>Dans les autres variantes</p> <p style="padding-left: 40px;">Interne, Sirène et Flash,</p> <p>cette temporisation de sirène agit pour tous les composants (centrale, sirène intérieure, module d'information, clavier de commande et sirène extérieure). Il faut donc signaler tous ces périphériques une fois la durée de temporisation écoulée.</p> <p></p>

	<p>Remarque</p> <p>Les types de communication Numéroteur vocal, SMS, E-mail et Push n'en sont pas affectés.</p> <p></p> <p>Remarque</p> <p>concernant Partition -> Réponse alarme</p> <p>Le type de zone Feu, les doubles touches Feu sur la centrale et les doubles touches Feu sur le clavier de commande déclenchent toujours un reporting CRA/STS lorsque le mode d'appel pour reporting CRA/STS a été autorisé et lorsque le groupe « Feu » est autorisé pour des événements CID/SIA.</p> <p>Exemple :</p> <p>Partition X -> Réponse alarme -> Sirène</p> <p style="padding-left: 40px;">Transmission de l'alarme incendie à CRA/STS</p>
<p>Retard sirène [min] (CRA/STS)</p>	<p>Durée de la temporisation de(s) la sirène(s).</p> <p>La temporisation de sirène peut être comprise entre 0 et 10 minutes.</p> <p>Si une alarme s'est déclenchée, la centrale d'alarme attend l'écoulement de ce délai avant d'activer les sirènes.</p> <p>Remarque</p> <p>Une temporisation de sirène ne sera effective que si la réponse alarme comprend une transmission. Une temporisation de sirène n'est pas effective en cas de défaut de la voie de transmission.</p> <p>La temporisation de sirène n'est pas effective si « Mode installateur->Système->Confirmation->Mode confirmation-> DD243 ou BS8243 » <u>et</u> « Mode installateur->Système->Confirmation->Sirène on->ne pas confirmer » est défini.</p> <p>Si des avertisseurs sont affectés à plusieurs partitions, la centrale d'alarme utilise la temporisation de sirène la plus courte des partitions correspondantes.</p> <p></p> <p>Remarque</p> <p>Si « Temporisation de sirène (spécifique à l'utilisateur) » est activé sous Système -> Sécurité (> 0), alors ce point de menu n'apparaît pas ici.</p> <p>En outre, le comportement global de cette temporisation de sirène (CRA/STS) est bloqué !</p> <p></p> <p>Remarque</p> <p>Le but principal de la temporisation de sirène est de donner du temps à la communication avec le CRA/STS et de réagir avant que la sirène n'alarme le malfaiteur que l'alarme a été déclenchée.</p> <p>La temporisation de sirène a lieu quand :</p> <p>Partition -> Réponse alarme -> Sirène + Reporting STS/Flash+ Reporting STS</p> <p>Communication CRA/STS : oui</p> <p>Confirmation -> Mode confirmation -> Basique</p> <p style="padding-left: 40px;">Émetteur d'alarme ON -> Confirmer</p> <p style="padding-left: 80px;">Exceptions : Ne pas confirmer, voir ci-dessous</p> <p style="padding-left: 40px;">Sirène ON -> Confirmer</p>

Réglages		Effet
Sirène ON	Sirène ON	
Ne pas confirmer	Ne pas confirmer	Alarme non confirmée : les émetteurs d'alarme internes et sirènes retentissent directement et pendant toute la <i>durée de sirène</i>
		Alarme confirmée : la centrale démarre à nouveau les sirènes et les émetteurs d'alarme internes, qui retentissent alors pendant toute la <i>durée de sirène</i> , même si celle-ci est déjà écoulée.
Ne pas confirmer	Confirmer	Alarme non confirmée : les émetteurs d'alarme internes retentissent directement et pendant toute la <i>durée de sirène</i> . <i>Aucune</i> sirène externe
		Alarme confirmée : la centrale attend une temporisation de sirène possible et démarre alors aussi bien les émetteurs d'alarme internes que les sirènes externes. Ceux-ci retentissent pendant toute la durée de sirène.
Confirmer	Confirmer	Alarme non confirmée : aucun(e) émetteur d'alarme ou sirène.
		Alarme confirmée : la centrale attend une temporisation de sirène possible et démarre alors aussi bien les émetteurs d'alarme internes que les sirènes externes. Ceux-ci retentissent pendant toute la <i>durée de sirène</i> .

Pas de temporisation de sirène quand :

Pas de temporisation de sirène si Ne pas confirmer pour les deux (réglage par défaut). Voir tableau ci-dessus.

1. La temporisation de sirène n'a pas d'effet si le mode de réponse alarme ne nécessite aucune communication ou si une erreur de ligne est détectée.
2. La temporisation de sirène n'a pas non plus d'effet si Options de système - Mode de confirmation est réglé sur DD243 ou BS8243 OU si Options de système - Confirmation - Sirène ON est réglé sur « Ne pas confirmer ».
3. Les émetteurs d'alarme qui sont attribués à deux partitions ou plus utilisent la plus courte temporisation de sirène de la partition à laquelle l'émetteur d'alarme est attribué.

La temporisation de sirène est également empêchée si Options de système - Mode de confirmation est réglé sur Basique et si Sirène ON est réglé sur « Ne pas confirmer » (réglages par défaut). Il s'agit des réglages par défaut de la centrale.

La temporisation de sirène est également empêchée si la communication CRA/STS est désactivée.

Pas de temporisation de sirène en cas d'alarme incendie, d'alarme agression et d'alarme 24 h.

The screenshot shows the ABUS configuration interface for 'Partition 1' named 'Haus'. The 'Tous act.' button is highlighted. Settings include:

- Temps sirène extérieure: 3
- Flash Arm: Off
- Flash Désarm.: Off
- Bip Arm: Off
- Bip Désarm: Off
- Temps fonct. Sir. Int.: 0
- Indéfini: Checked

 The sidebar on the right contains icons for: INFO, État, Périphériques, Sorties, Partitions, Système, Transmissions, Appel Soins de Santé, Test, Journal de bord (18), and Clavier. Buttons 'Annuler' and 'Envoyer' are at the bottom.

Désignation/Fonction	Explication
Durée sirène extérieure [min]	<p>Durée de(s) la sirène(s) externe(s) en minutes.</p> <p>La durée de(s) la sirène(s) peut être comprise entre 0 et 15 minutes.</p> <p>Si des avertisseurs sont affectés à plusieurs partitions, la centrale d'alarme utilise la durée de sirène la plus longue des partitions correspondantes.</p> <p>La durée d'activité des sirènes peut aussi être prolongée selon la temporisation de sirène la plus longue des partitions affectées.</p>
Flash arm.	<p>Allumée</p> <p>Après l'activation réussie de la partition, une confirmation visuelle apparaît sur la sirène extérieure radio.</p> <p>Les sorties de type "Flash" sont commutées pendant 10 secondes après l'activation réussie de la partition.</p> <p>Éteinte</p> <p>Après l'activation réussie de la partition, aucune confirmation visuelle n'apparaît sur la sirène extérieure radio.</p>
Flash désarm.	<p>Allumée</p> <p>Après la désactivation réussie de la partition, une confirmation visuelle apparaît sur la sirène extérieure radio.</p> <p>Les sorties de type "Flash" sont commutées pendant 10 secondes après l'activation réussie de la partition.</p> <p>Éteinte</p> <p>Après la désactivation réussie de la partition, aucune confirmation visuelle n'apparaît sur la sirène extérieure radio.</p>

Désignation/Fonction	Explication
Bip arm	<p>Allumée</p> <p>Après l'activation réussie de la partition, une confirmation acoustique retentit sur la sirène extérieure radio.</p> <p>Les sorties de type "Sirène" sont commutées pendant 10 secondes après l'activation réussie de la partition.</p> <p>Éteinte</p> <p>Après l'activation réussie de la partition, aucune confirmation acoustique ne retentit sur la sirène extérieure radio.</p>
Bip désarm	<p>Allumée</p> <p>Après la désactivation réussie de la partition, une confirmation acoustique retentit sur la sirène extérieure radio.</p> <p>Les sorties de type "Sirène" sont commutées pendant 10 secondes après l'activation réussie de la partition.</p> <p>Éteinte</p> <p>Après la désactivation réussie de la partition, aucune confirmation acoustique ne retentit sur la sirène extérieure radio.</p>
Durée sirène int. [min]	<p>Durée de(s) la sirène(s) interne(s) en minutes après une alarme intrusion.</p> <p>La durée de(s) la sirène(s) peut être comprise entre 0 et 20 minutes.</p> <p>Si des avertisseurs sont affectés à plusieurs partitions, la centrale d'alarme utilise la durée de sirène la plus longue des partitions correspondantes.</p> <p>La durée d'activité des sirènes peut aussi être prolongée selon la temporisation de sirène la plus longue des partitions affectées.</p> <p>Remarque</p> <p>Pour des raisons de sécurité, les sirènes internes continuent de fonctionner en cas d'incendie ou d'alarme agression jusqu'à la confirmation de l'alarme par un utilisateur.</p> <p>Pour des raisons de sécurité, il n'y a pas de limite de temps en cas d'alarme feu ou agression.</p> <p>Comportement spécial en cas de temporisation d'entrée :</p> <p>Condition requise</p> <ul style="list-style-type: none">• Les sirènes internes (centrale d'alarme, sirène d'intérieur radio, module d'information radio) redeviennent silencieuses après l'écoulement de la durée de sirène interne.• La centrale s'est automatiquement réactivée.• (Voir également « Mode installateur → Système → Sécurité → Auto réarmement système ») <p>Comportement</p> <ul style="list-style-type: none">• Si vous accédez maintenant à la zone d'entrée (les détecteurs de type "Entrée/Sortie" et "Entrée suiveuse" s'ouvrent), les avertisseurs internes (centrale d'alarme, sirène d'intérieur radio, module d'information radio) émettent une tonalité d'alarme.• La tonalité d'entrée normale n'est pas signalée dans ce cas.

Désignation/Fonction	Explication
Durée sirène int. [min], suite	<p>Remarque</p> <p>Si vous utilisez la temporisation d'entrée, vous attendez en principe la tonalité d'entrée normale.</p> <p>Cette tonalité d'entrée retentit pendant toute la durée de la temporisation d'entrée.</p> <p>Si vous entendez une tonalité d'alarme après l'ouverture de la porte d'entrée, vous savez immédiatement que la centrale d'alarme a détecté une intrusion en votre absence.</p> <p>La temporisation continue de s'écouler. Il est donc recommandé de désactiver la centrale d'alarme pendant le délai de temporisation.</p> <p>Faites-le uniquement si vous vous en sentez capable. Il se peut que l'intrus soit encore présent !</p> <p>Si vous ne le faites pas, une alarme intrusion supplémentaire se produit après écoulement de la temporisation.</p> <p>Informez également les autres personnes ayant accès à votre propriété sur ce comportement spécifique de la centrale d'alarme.</p>
Indéfini	<p>Allumée</p> <p>Les sirènes internes émettent la tonalité d'alarme jusqu'à la confirmation de l'alarme par un utilisateur.</p> <p>Désactivé</p> <p>L'indication de durée est utilisée pour la durée de fonctionnement de(s) la sirène(s) interne(s).</p>

Configuration de partitions

Act. interne

ABUS
 Logout

Partitions | Partition 1

Nom

Tous act.
Act. interne
Désarmement
Réaction AGRESSION

Mode Sortie Arm. silencieux ▼

Temps Entrée

Réponse alarme *Sirène ▼

Temps sirène extérieure

Temps Sortie

Retard sirène

Sortie Finale Arm. Part. *Entrée/Sortie ▼

Annuler Envoyer

Logout

INFO

État

Périphériques

Sorties

Partitions

Système

Transmissions

Appel Soins de Santé

Test

18 Journal de bord

Clavier

Désignation/Fonction	Explication
Nom	Nom unique de la partition. Vous pouvez nommer ici la partition, par ex. maison, atelier, bureau. Le nom peut comprendre 12 caractères maximum. La centrale affiche ce nom pour l'utilisateur même lors de l'activation.
Act. interne	Réglages d'activation interne de la partition.
Mode sortie	Sélectionnez ici le mode d'activation interne du lieu. Remarque : voir également le manuel d'utilisateur, chapitre « 8. Activation et désactivation de l'installation
	<p>Armement temporisé</p> <ul style="list-style-type: none"> Utilisez cette option pour activer en interne la partition uniquement après écoulement de la temporisation définie. Sélectionnez la temporisation de sortie dans "Tps sortie". La centrale enregistre le début de cette activation interne temporisée. Cette option n'est pas conforme à BS8243:2010.

Désignation/Fonction	Explication
Mode sortie, suite	<p>Sortie finale armement</p> <ul style="list-style-type: none"> • Utilisez cette option pour exclure l'activation interne d'une partition en fermant une dernière porte de sortie. Cette porte possède un détecteur avec le type de zone "Entrée/Sortie". Si la porte a été fermée, la partition est activée en interne après écoulement du temps supplémentaire. • Notez que le temps de sortie de cette option est infini, c'est-à-dire que lorsque la zone est fermée (porte fermée), la centrale d'alarme attend, lors de l'activation interne, que cette zone soit ouverte et refermée. • La centrale d'alarme enregistre l'heure de démarrage de l'activation interne (et non pas l'activation interne) dans l'historique. • N'essayez pas d'utiliser une zone PIR en tant qu'entrée/sortie pour une partition. Les détecteurs sans fil PIR disposent d'un délai de "blocage" après chaque activation pour préserver la batterie. Si vous activez une partition (ou l'activez en interne), un détecteur PIR peut encore être bloqué. Pendant ce délai, il ne peut pas envoyer de signal d'achèvement du processus d'activation. <p>Armement immédiat</p> <ul style="list-style-type: none"> • La partition est immédiatement activée en interne sans signal d'avertissement acoustique. Lorsque la partition a été activée en interne, la confirmation est acoustique. • Remarque : Cette option n'est pas conforme à BS8243:2010. <p>Armement silencieux</p> <ul style="list-style-type: none"> • La partition est activée en interne après écoulement de la temporisation de sortie. Sélectionnez la temporisation de sortie dans "Tps sortie". Aucun signal sonore n'est cependant émis pendant ce délai. Lorsque la partition a été activée en interne, la confirmation est acoustique. La centrale enregistre l'heure de démarrage dans l'historique. • Les signaux sonores sont audibles pendant le temps d'entrée. • Remarque : Cette option n'est pas conforme à BS8243:2010. <p>Verrouillage activé</p> <ul style="list-style-type: none"> • Le mode "Verrou activ." influence aussi bien l'activation interne que la désactivation de la partition. • Pour ce mode, vous devez prévoir un détecteur avec le type de zone "Verrou activ." et un détecteur avec le type de zone "Entrée/Sortie" sur la dernière porte de sortie. Le détecteur avec le type de zone "Verrou activ." est utilisé sur une serrure adaptée avec un contact de verrouillage. <p>Activation interne de la partition</p> <ul style="list-style-type: none"> • L'utilisateur doit d'abord démarrer la séquence d'activation à l'aide de son code utilisateur, de son badge de proximité ou de sa télécommande. La centrale émet la tonalité de sortie et enregistre l'heure de démarrage dans l'historique. Si la zone de type "Entrée/sortie" est ouverte, la centrale émet une tonalité de sortie interrompue. La tonalité de sortie retentit jusqu'à ce que l'utilisateur a) ferme la dernière porte de sortie et ; b) verrouille la porte en actionnant le contact de verrouillage. Après l'activation du contact de verrouillage, la partition s'active en interne à l'issue du temps supplémentaire. Par ailleurs, la zone de type "Entrée/Sortie" est transformée en zone de type "Alarme immédiate tempo sortie". La centrale enregistre l'activation de la zone de type "Verrou activ." dans l'historique.

Désignation/Fonction	Explication
Mode sortie, suite	<p>Désactivation de la partition</p> <ul style="list-style-type: none">• L'utilisateur déverrouille la porte et actionne ainsi le contact de verrouillage. La zone de type "Verrou activ." s'ouvre. La centrale enregistre l'activation de la zone de type "Verrou activ." dans l'historique. La zone initialement de type "Entrée/Sortie" transformée en zone de type "Alarme immédiate tempo sortie" redevient une zone de type "Entrée/Sortie". Le délai d'entrée commence à s'écouler à l'ouverture de la porte. La tonalité d'entrée qui retentit maintenant est différente de la tonalité d'entrée normale.• Si l'utilisateur verrouille à nouveau la porte sans que le délai d'entrée n'ait démarré, la centrale reste active, la zone de type "Entrée/Sortie" redevient une zone de type "Alarme immédiate tempo sortie". La centrale interrompt la tonalité d'avertissement.• Pour être conforme à BS8243, "Après Entrée" doit être réglé sur "Jamais" pour verrouiller la confirmation. <p>Annulation de la temporisation de sortie</p> <p>Activation interne de la partition</p> <ul style="list-style-type: none">• L'utilisateur doit d'abord démarrer la séquence d'activation. Puis, il doit terminer l'activation après avoir quitté la partition surveillée.• L'utilisateur peut démarrer la séquence d'activation à l'aide de son code utilisateur, de son badge de proximité ou de sa télécommande. (Remarque : l'activation avec la télécommande ne doit pas être réglée sur "Immédiat", Mode installateur->Système->Accès utilisateur->Téléco arm. immédiat).• L'utilisateur termine l'activation en actionnant une zone de type "Annuler temporisation de sortie" (voir l'explication des types de zone).• Notez que le temps de sortie de cette option est infini, c'est-à-dire que la centrale d'alarme attend d'avoir reçu le signal d'arrêt du processus d'activation. Pendant ce temps, la centrale d'alarme émet la tonalité de sortie. Elle enregistre l'heure de démarrage de l'activation (et non pas l'activation même) dans l'historique. La partition est activée après écoulement du temps supplémentaire. <p>Désactivation de la partition</p> <ul style="list-style-type: none">• L'utilisateur peut utiliser sa télécommande. Mais l'utilisateur peut également ouvrir la porte. La zone de type "Entrée/sortie" sur cette porte démarre le temps d'entrée. Pendant le temps d'entrée, l'utilisateur doit désactiver la partition à l'aide de son code utilisateur ou de son badge de proximité sur la centrale d'alarme ou l'élément de commande. (La dernière méthode n'est pas conforme à BS8243 clause 6.4.) <p>Comme part. (partition) 1</p> <p>Cette option est disponible pour les partitions 2, 3 et 4. Si vous choisissez cette option, la centrale d'alarme utilise le même type que pour la partition 1.</p>

Désignation/Fonction	Explication
Temps supplémentaire [s]	<p>Cette option s'affiche uniquement pour les modes "Entrée/sortie activée", "Verrou activ." et "Annuler temporisation de sortie".</p> <p>Cette option vous permet de définir une temporisation afin que les détecteurs puissent se stabiliser avant l'activation interne de la partition.</p> <p>Ceci peut être nécessaire si des détecteurs se sont déclenchés, envoient un signal d'alarme et n'ont pas encore été réinitialisés.</p> <p>Pendant ce temps, la centrale d'alarme ignore les signaux d'alarme des détecteurs et les sirènes ne se déclenchent pas.</p> <p>Entrez 2 chiffres pour la durée en secondes de 01 à 30. La programmation d'usine du temps supplémentaire est de 15 secondes.</p> <p>Ainsi, les PIR radio, qui se trouvent sur la voie de sortie et qui se sont déclenchés, peuvent se stabiliser et se réinitialiser.</p>
Temps de sortie [s]	<p>Cette option s'affiche uniquement pour les modes "Armement temporisé" et "Armement silencieux".</p> <p>Durée de la temporisation de sortie en secondes.</p> <p>Le temps de sortie peut être compris entre 10 et 120 secondes.</p>
Temps d'entrée [s]	<p>Durée de la temporisation d'entrée en secondes.</p> <p>Le temps d'entrée peut être compris entre 10 et 120 secondes.</p>
Réponse alarme	<p>Sélectionnez ici la réponse en cas d'alarme dans cette partition.</p> <p>Interne</p> <ul style="list-style-type: none"> • Centrale, sirène d'intérieur, module d'information et élément de commande. <p>Sirène</p> <ul style="list-style-type: none"> • Centrale, sirène d'intérieur, module d'information et élément de commande. • Sirènes d'extérieur <p>Sirène + TS Reporting</p> <ul style="list-style-type: none"> • Centrale, sirène d'intérieur, module d'information et élément de commande. • Sirènes d'extérieur • Communication avec AES/NSL <p>Une temporisation de sirène est effective en cas de réponse alarme « Sirène + Reporting STS ».</p> <p>Flash</p> <ul style="list-style-type: none"> • Centrale, sirène d'intérieur, module d'information et élément de commande. • Sirènes extérieures (uniquement avec FLASH) <p>Flash + TS Reporting</p> <ul style="list-style-type: none"> • Centrale, sirène d'intérieur, module d'information et élément de commande. • Sirènes extérieures (uniquement avec FLASH) • Communication avec AES/NSL <p>Une temporisation de sirène est effective en cas de réponse alarme « Flash + Reporting STS ».</p> <p></p> <p>Remarque</p> <p>Lorsque « Temporisation de sirène (spécifique à l'utilisateur) » est activé (> 0), le comportement de la temporisation de sirène est le suivant :</p> <p>Temporisation de sirène (utilisateur) a uniquement des effets sur les sirènes d'extérieur pour les configurations suivantes :</p>

Partition -> Réponse alarme

Sirène + Reporting STS ou

Flash + TS Reporting

Dans les autres variantes

Interne, Sirène et Flash,

cette temporisation de sirène agit pour tous les composants (centrale, sirène intérieure, module d'information, clavier de commande et sirène extérieure). Il faut donc signaler tous ces périphériques une fois la durée de temporisation écoulée.



Remarque

Les types de communication Numéroteur vocal, SMS, E-mail et Push n'en sont pas affectés.



Remarque

concernant Partition -> Réponse alarme

Le type de zone Feu, les doubles touches Feu sur la centrale et les doubles touches Feu sur le clavier de commande déclenchent **toujours** un reporting CRA/STS lorsque le mode d'appel pour reporting CRA/STS a été autorisé et lorsque le groupe « Feu » est autorisé pour des événements CID/SIA.

Exemple :

Partition X -> Réponse alarme -> Sirène

Transmission de l'alarme incendie à CRA/STS

Désignation/Fonction	Explication
Retard sirène [min] (CRA/STS)	<p>Durée de la temporisation de(s) la sirène(s). La temporisation de sirène peut être comprise entre 0 et 10 minutes. Si une alarme s'est déclenchée, la centrale d'alarme attend l'écoulement de ce délai avant d'activer les sirènes.</p> <p>Remarque Une temporisation de sirène ne sera effective que si la réponse alarme comprend une transmission. Une temporisation de sirène n'est pas effective en cas de défaut de la voie de transmission. La temporisation de sirène n'est pas effective si « Mode installateur->Système->Confirmation->Mode confirmation-> DD243 ou BS8243 » et « Mode installateur->Système->Confirmation->Sirène on->ne pas confirmer » est défini. Si des émetteurs (ou uniquement des éléments de commande) sont affectés à plusieurs partitions, la centrale d'alarme utilise la temporisation de sirène la plus courte des partitions correspondantes.</p> <p> Remarque Vous trouverez des détails sur la temporisation de sirène dans Temporisation de sirène Partitions Toutes actives.</p> <p> Remarque Si « Temporisation de sirène (spécifique à l'utilisateur) » est activé sous Système -> Sécurité (> 0), alors ce point de menu n'apparaît pas ici. En outre, le comportement global de cette temporisation de sirène (CRA/STS) est bloqué !</p>
Durée sirène extérieure [min]	<p>Durée de(s) la sirène(s) externe(s) en minutes. La durée de(s) la sirène(s) peut être comprise entre 0 et 15 minutes. Si des émetteurs (ou uniquement des éléments de commande) sont affectées à plusieurs partitions, la centrale d'alarme utilise la durée de sirène la plus longue des partitions correspondantes.</p> <p>La durée d'activité des sirènes peut aussi être prolongée selon la temporisation de sirène la plus longue des partitions affectées.</p>
Sortie finale arm. part.	<p>Cette option commande la gestion d'une zone de type "Entrée/Sortie" en cas d'activation interne.</p> <p>Entrée/sortie</p> <ul style="list-style-type: none"> • Dans cette partition, chaque zone de type « Entrée/Sortie » ayant l'attribut « Surveillance interne » continue de fonctionner comme une zone de type « Entrée/sortie ». <p>Alarme immédiate tempo sortie</p> <ul style="list-style-type: none"> • Dans cette partition, chaque zone de type « Entrée/Sortie » ayant l'attribut « Surveillance interne » fonctionne désormais comme une zone de type « Alarme normale ».

The screenshot displays the configuration screen for 'Partition 1' in the ABUS system. At the top, the name 'Haus' is entered. Below this, there are several control buttons: 'Tous act.', 'Act. interne' (highlighted in blue), 'Désarmement', and 'Réaction AGRSSION'. The 'Route Entrée Arm. Part' is set to '*Route d'entrée'. There are also sliders for 'Flash Arm.', 'Flash Désarm.', 'Bip Arm.', and 'Bip Désarm.', along with a 'Temps fonct.Sir.Int.' set to 0 and an 'Indéfini' checkbox checked. At the bottom, there are 'Annuler' and 'Envoyer' buttons. On the right side, a vertical menu contains icons and labels for 'Logout', 'INFO', 'État', 'Périphériques', 'Sorties', 'Partitions', 'Système', 'Transmissions', 'Appel Soins de Santé', 'Test', 'Journal de bord', and 'Clavier'.

Désignation/Fonction	Explication
Route entrée arm. part	<p>Cette option commande la gestion d'une zone de type "Route d'entrée" en cas d'activation interne.</p> <p>Route d'entrée</p> <ul style="list-style-type: none"> Dans cette partition, chaque zone de type « Route d'entrée » ayant l'attribut « Surveillance interne » continue de fonctionner comme une zone de type « Route d'entrée ». <p>Entrée/sortie</p> <ul style="list-style-type: none"> Dans cette partition, chaque zone de type « Route d'entrée » ayant l'attribut « Surveillance interne » fonctionne désormais comme une zone de type « Entrée/Sortie ».
Flash arm.	<p>Allumée</p> <p>Après l'activation interne réussie de la partition, une confirmation visuelle apparaît sur la sirène extérieure radio.</p> <p>Les sorties de type "Flash" sont commutées pendant 10 secondes après l'activation réussie de la partition.</p> <p>Éteinte</p> <p>Après l'activation interne réussie de la partition, aucune confirmation visuelle n'apparaît sur la sirène extérieure radio.</p>
Flash désarm.	<p>Allumée</p> <p>Après la désactivation réussie de la partition, une confirmation visuelle apparaît sur la sirène extérieure radio.</p> <p>Les sorties de type "Flash" sont commutées pendant 10 secondes après l'activation réussie de la partition.</p> <p>Éteinte</p>

Après la désactivation réussie de la partition, **aucune** confirmation visuelle n'apparaît sur la sirène extérieure radio.

Désignation/Fonction	Explication
Bip arm	<p>Allumée</p> <p>Après l'activation interne réussie de la partition, une confirmation acoustique retentit sur la sirène extérieure radio.</p> <p>Les sorties de type "Sirène" sont commutées pendant 10 secondes après l'activation réussie de la partition.</p> <p>Éteinte</p> <p>Après l'activation interne réussie de la partition, aucune confirmation acoustique ne retentit sur la sirène extérieure radio.</p>
Bip désarm	<p>Allumée</p> <p>Après la désactivation réussie de la partition, une confirmation acoustique retentit sur la sirène extérieure radio.</p> <p>Les sorties de type "Sirène" sont commutées pendant 10 secondes après l'activation réussie de la partition.</p> <p>Éteinte</p> <p>Après la désactivation réussie de la partition, aucune confirmation acoustique ne retentit sur la sirène extérieure radio.</p>
Durée sirène int. [min]	<p>Durée de(s) la sirène(s) interne(s) en minutes après une alarme intrusion.</p> <p>La durée de(s) la sirène(s) peut être comprise entre 0 et 20 minutes.</p> <p>Si des avertisseurs sont affectés à plusieurs partitions, la centrale d'alarme utilise la durée de sirène la plus longue des partitions correspondantes.</p> <p>La durée d'activité des sirènes peut aussi être prolongée selon la temporisation de sirène la plus longue des partitions affectées.</p> <p>Remarque</p> <p>Pour des raisons de sécurité, les sirènes internes continuent de fonctionner en cas d'incendie ou d'alarme agression jusqu'à la confirmation de l'alarme par un utilisateur. Pour des raisons de sécurité, il n'y a pas de limite de temps en cas d'alarme feu ou agression.</p> <p>Comportement spécial en cas de temporisation d'entrée</p> <p>Condition requise</p> <ul style="list-style-type: none">• Les sirènes internes (centrale d'alarme, sirène d'intérieur radio, module d'information radio) redeviennent silencieuses après l'écoulement de la durée de sirène interne.• La centrale d'alarme s'est automatiquement réactivée (voir également « Mode Installateur → Système -> Sécurité → Auto réarmement système »). <p>Comportement</p> <ul style="list-style-type: none">• Si vous accédez maintenant à la zone d'entrée (les détecteurs de type "Entrée/Sortie" et "Entrée suiveuse" s'ouvrent), les avertisseurs internes (centrale d'alarme, sirène d'intérieur radio, module d'information radio) émettent une tonalité d'alarme.• La tonalité d'entrée normale n'est pas signalée dans ce cas.

Désignation/Fonction	Explication
Durée sirène int. [min], suite	<p>Remarque</p> <p>Si vous utilisez la temporisation d'entrée, vous attendez en principe la tonalité d'entrée normale. Cette tonalité d'entrée retentit pendant toute la durée de la temporisation d'entrée. Si vous entendez une tonalité d'alarme après l'ouverture de la porte d'entrée, vous savez immédiatement que la centrale d'alarme a détecté une intrusion en votre absence.</p> <p>La temporisation continue de s'écouler. Il est donc recommandé de désactiver la centrale d'alarme pendant le délai de temporisation. Faites-le uniquement si vous vous en sentez capable. Il se peut que l'intrus soit encore présent ! Si vous ne le faites pas, une alarme intrusion supplémentaire se produit après écoulement de la temporisation.</p> <p>Informez également les autres personnes ayant accès à votre propriété sur ce comportement spécifique de la centrale d'alarme.</p>
Indéfini	<p>Allumée</p> <p>Les sirènes internes émettent la tonalité d'alarme jusqu'à la confirmation de l'alarme par un utilisateur.</p> <p>Désactivé</p> <p>L'indication de durée est utilisée pour la durée de fonctionnement de(s) la sirène(s) interne(s).</p>

Configuration de partitions

Désactivée

ABUS
Logout

Partitions | Partition 1

Nom:

Réponse alarme: *Sirène + TS Reporting Retard sirène:

Temps sirène extérieure:

Temps fonct. Sir. Int.: Indéfini:

INFO

État

Périphériques

Sorties

Partitions

Système

Transmissions

Appel Soins de Santé

Test

18 Journal de bord

Clavier

Désignation/Fonction	Explication
Réponse alarme	<p>Sélectionnez ici la réponse en cas d'alarme dans cette partition.</p> <p>Interne</p> <ul style="list-style-type: none"> Centrale, sirène d'intérieur, module d'information et élément de commande. <p>Sirène</p> <ul style="list-style-type: none"> Centrale, sirène d'intérieur, module d'information et élément de commande. Sirènes d'extérieur <p>Sirène + TS Reporting</p> <ul style="list-style-type: none"> Centrale, sirène d'intérieur, module d'information et élément de commande. Sirènes d'extérieur Communication avec AES/NSL <p>Une temporisation de sirène est effective en cas de réponse alarme « Sirène + Reporting STS ».</p> <p>Flash</p> <ul style="list-style-type: none"> Centrale, sirène d'intérieur, module d'information et élément de commande. Sirènes extérieures (uniquement avec FLASH) <p>Flash + TS Reporting</p> <ul style="list-style-type: none"> Centrale, sirène d'intérieur, module d'information et élément de commande. Sirènes extérieures (uniquement avec FLASH)

• Communication avec AES/NSL

Une temporisation de sirène est effective en cas de réponse alarme « Flash + Reporting STS ».



Remarque

Lorsque « Temporisation de sirène (spécifique à l'utilisateur) » est activé (> 0), le comportement de la temporisation de sirène est le suivant :

Temporisation de sirène (utilisateur) a **uniquement** des effets sur les sirènes d'extérieur pour les configurations suivantes :

Partition -> Réponse alarme

Sirène + Reporting STS ou

Flash + TS Reporting

Dans les autres variantes

Interne, Sirène et Flash,

cette temporisation de sirène agit pour tous les composants (centrale, sirène intérieure, module d'information, clavier de commande et sirène extérieure). Il faut donc signaler tous ces périphériques une fois la durée de temporisation écoulée.



Remarque

Les types de communication Numéroteur vocal, SMS, E-mail et Push n'en sont pas affectés.



Remarque

concernant Partition -> Réponse alarme

Le type de zone Feu, les doubles touches Feu sur la centrale et les doubles touches Feu sur le clavier de commande déclenchent **toujours** un reporting CRA/STS lorsque le mode d'appel pour reporting CRA/STS a été autorisé et lorsque le groupe « Feu » est autorisé pour des événements CID/SIA.

Exemple :

Partition X -> Réponse alarme -> Sirène

Transmission de l'alarme incendie à CRA/STS

Retard sirène [min] (CRA/STS)

Durée de la temporisation de(s) la sirène(s).

La temporisation de sirène peut être comprise entre 0 et 10 minutes.

Si une alarme s'est déclenchée, la centrale d'alarme attend l'écoulement de ce délai avant d'activer les sirènes.

Remarque

Une temporisation de sirène ne sera effective que si la réponse alarme comprend une transmission.

Une temporisation de sirène n'est pas effective en cas de défaut de la voie de transmission.

La temporisation de sirène n'est pas effective si « Mode installateur->Système->Confirmation->Mode confirmation-> DD243 ou BS8243 » et « Mode installateur->Système->Confirmation->Sirène on->ne pas confirmer » est défini.
Si des avertisseurs sont affectés à plusieurs partitions, la centrale d'alarme utilise la temporisation de sirène la plus courte des partitions correspondantes.



Remarque

Vous trouverez des détails sur la temporisation de sirène dans Temporisation de sirène Partitions Toutes actives.



Remarque

Si « Temporisation de sirène (spécifique à l'utilisateur) » est activé sous Système -> Sécurité (> 0), alors ce point de menu n'apparaît **pas** ici.

En outre, le comportement global de cette temporisation de sirène (CRA/STS) est bloqué !

Durée sirène Tension d'entrée CC [min]

Durée de(s) la sirène(s) externe(s) en minutes.

La durée de(s) la sirène(s) peut être comprise entre 0 et 15 minutes.

Si des émetteurs (ou uniquement des éléments de commande) sont affectées à plusieurs partitions, la centrale d'alarme utilise la durée de sirène la plus longue des partitions correspondantes.

La durée d'activité des sirènes peut aussi être prolongée selon la temporisation de sirène la plus longue des partitions affectées.

Désignation/Fonction	Explication
Durée sirène int. [min]	<p>Durée de(s) la sirène(s) interne(s) en minutes après une alarme intrusion. La durée de(s) la sirène(s) peut être comprise entre 0 et 20 minutes. Si des avertisseurs sont affectés à plusieurs partitions, la centrale d'alarme utilise la durée de sirène la plus longue des partitions correspondantes.</p> <p>La durée d'activité des sirènes peut aussi être prolongée selon la temporisation de sirène la plus longue des partitions affectées.</p> <p>Remarque Pour des raisons de sécurité, les sirènes internes continuent de fonctionner en cas d'incendie ou d'alarme agression jusqu'à la confirmation de l'alarme par un utilisateur. Pour des raisons de sécurité, il n'y a pas de limite de temps en cas d'alarme feu ou agression.</p> <p>Comportement spécial en cas de temporisation d'entrée</p> <p>Condition requise</p> <ul style="list-style-type: none"> • Les sirènes internes (centrale d'alarme, sirène d'intérieur radio, module d'information radio) redeviennent silencieuses après l'écoulement de la durée de sirène interne. • La centrale d'alarme s'est automatiquement réactivée (voir également « Mode Installateur → Système -> Sécurité → Auto réarmement système »). <p>Comportement</p> <ul style="list-style-type: none"> • Si vous accédez maintenant à la zone d'entrée (les détecteurs de type "Entrée/Sortie" et "Entrée suiveuse" s'ouvrent), les avertisseurs internes (centrale d'alarme, sirène d'intérieur radio, module d'information radio) émettent une tonalité d'alarme. • La tonalité d'entrée normale n'est pas signalée dans ce cas. <p>Remarque Si vous utilisez la temporisation d'entrée, vous attendez en principe la tonalité d'entrée normale. Cette tonalité d'entrée retentit pendant toute la durée de la temporisation d'entrée. Si vous entendez une tonalité d'alarme après l'ouverture de la porte d'entrée, vous savez immédiatement que la centrale d'alarme a détecté une intrusion en votre absence. La temporisation continue de s'écouler. Il est donc recommandé de désactiver la centrale d'alarme pendant le délai de temporisation. Faites-le uniquement si vous vous en sentez capable. Il se peut que l'intrus soit encore présent ! Si vous ne le faites pas, une alarme intrusion supplémentaire se produit après écoulement de la temporisation. Informez également les autres personnes ayant accès à votre propriété sur ce comportement spécifique de la centrale d'alarme.</p>
Indéfini	<p>Allumée Les sirènes internes émettent la tonalité d'alarme jusqu'à la confirmation de l'alarme par un utilisateur.</p> <p>Désactivé La durée de sirène est utilisée pour la durée de fonctionnement de la ou des sirènes internes.</p>

Configuration de partitions

Réaction agression

Désignation/Fonction	Explication
Nom	Nom unique de la partition
Réaction agression	<p>Sélectionnez ici le type de signalisation d'une alarme agression dans la partition sélectionnée.</p> <p>Audible</p> <ul style="list-style-type: none"> • En cas d'alarme agression, la transmission et la signalisation d'alarme acoustique se produisent via les sirènes et émetteurs d'alarme raccordés (en fonction de la durée des sirènes). • L'écran de la centrale d'alarme affiche un triangle en cas d'alarme agression. • Les détails s'affichent après avoir saisi un code utilisateur. • L'alarme acoustique est coupée après la saisie d'un code utilisateur. <p>Silencieuse</p> <ul style="list-style-type: none"> • L'alarme agression est uniquement transmise via les voies de communication. • Il n'y a pas de signalisation d'alarme acoustique. • Les sorties de type "Sirène" ou "Agression" ne sont pas commutées. • L'écran de la centrale d'alarme n'affiche pas l'alarme agression. • L'affichage est visible uniquement quand un utilisateur veut utiliser la centrale d'alarme.

Désignation/Fonction	Explication
<p>Réaction agression, suite</p>	<p>Affiché</p> <ul style="list-style-type: none"> • En cas d'alarme agression, la communication et la signalisation d'alarme acoustique se produisent via les sirènes et émetteurs d'alarme raccordés (en fonction de la durée de sirène réglée). • L'écran de la centrale d'alarme affiche les détails de l'alarme agression. (Aucun code utilisateur ne doit être saisi pour afficher les détails.) Parallèlement, l'avertissement acoustique retentit sur la centrale d'alarme. Les sorties de type "Sirène" ou "Agression" sont commutées. <p>Remarque</p> <p>Aucune alarme agression ne peut être déclenchée et transmise si la centrale est en mode installateur.</p>

Systeme



Généralités
Logout

ABUS
Systeme | Généralités

Texte écran

Défaut A/C rapport

Ext DC Défaut Rapport

Tempo Défaut 220V (minutes)

Ext DC Défaut Retard (minutes)

INFO

État

Périphériques

Sorties

Partitions

Systeme

Transmissions

Appel Soins de Santé

Journal de bord

Clavier

Désignation/Fonction	Explication (case à cocher)
Langue	<p>Uniquement disponible sur la centrale d'alarme. Sélectionnez la langue avec la version souhaitée.</p> <p> Remarque Il est obligatoire d'effectuer la mise à jour du fichier de langue AVANT la mise à jour du fichier d'application !</p> <p>Voir chapitre « Mise à niveau logicielle avec nouveaux fichiers depuis la carte SD » en annexe</p>
Texte écran	<p>Nom affiché sur l'écran de la Secvest. 20 caractères maximum à partir de la version logicielle 1.01.00, 16 caractères maximum (raison : compatibilité avec le serveur ABUS)</p>
Réinitialiser	<p>Uniquement disponible sur la centrale d'alarme.</p> <p>Réglages d'usine à niveaux Programmation Usine</p> <p> Remarque</p>

	<p>Effectuez une copie de sauvegarde de la configuration avant de réinitialiser les réglages d'usine de la centrale. Vous pouvez l'effectuer vous-même sur la centrale ou via l'interface Internet. Vous trouverez des détails à ce sujet dans le chapitre « Sauvegarder/Restaurer ».</p>								
<p>Réglages d'usine à niveaux</p>	<p>Uniquement disponible sur la centrale d'alarme.</p> <p>Cette option de menu vous permet de réinitialiser en partie les réglages d'usine de la centrale, sans influencer le système en entier.</p> <p></p> <p>Remarque Une réinitialisation</p> <ul style="list-style-type: none"> • ne supprime pas l'historique <p>Vous pouvez sélectionner une ou plusieurs des options suivantes :</p> <p></p> <p>Remarque Vous trouverez les valeurs standard des réglages d'usine en annexe.</p>								
	<table border="1"> <thead> <tr> <th data-bbox="472 992 695 1032">Option</th> <th data-bbox="695 992 1471 1032">Effet</th> </tr> </thead> <tbody> <tr> <td data-bbox="472 1061 695 1397">Utilisateur</td> <td data-bbox="695 1061 1471 1397"> <p>Supprime tous les utilisateurs ainsi que leurs codes, badges Proximity, télécommandes, alarmes agression, médaillons médicaux et médaillons de soins. Après la réinitialisation, vous êtes invité à attribuer un nouveau code installateur et un nouveau code administrateur. Cette option a le même effet que l'utilisation des « broches de réinitialisation de code ». Vous trouverez des détails à ce sujet dans le chapitre Présentation de l'appareil -> Dos de l'appareil.</p> </td> </tr> <tr> <td data-bbox="472 1397 695 1503">Zones</td> <td data-bbox="695 1397 1471 1503"> <p>Réinitialise l'ensemble des zones, types, partitions, attributs. Pour les zones sans fil, la centrale conserve les ID de tous les détecteurs qui sont déjà programmés dans la centrale.</p> </td> </tr> <tr> <td data-bbox="472 1503 695 2069">Composants sans fil</td> <td data-bbox="695 1503 1471 2069"> <p>Supprime les ID pour les composants sans fil programmés. Faites dérouler la liste des composants et sélectionnez Oui pour chaque type que vous souhaitez supprimer. Appuyez ensuite sur OK pour confirmer votre sélection.</p> <p>Tous les composants Supprime tous les composants sans fil programmés.</p> <p>Détecteurs Supprime uniquement ces composants. Les zones sont également réinitialisées.</p> <p>Sirènes ext. Supprime uniquement ces composants.</p> <p>Sirènes int. Supprime uniquement ces composants.</p> <p>Clavier de commande sans fil Supprime uniquement ces composants.</p> <p>WAM</p> </td> </tr> </tbody> </table>	Option	Effet	Utilisateur	<p>Supprime tous les utilisateurs ainsi que leurs codes, badges Proximity, télécommandes, alarmes agression, médaillons médicaux et médaillons de soins. Après la réinitialisation, vous êtes invité à attribuer un nouveau code installateur et un nouveau code administrateur. Cette option a le même effet que l'utilisation des « broches de réinitialisation de code ». Vous trouverez des détails à ce sujet dans le chapitre Présentation de l'appareil -> Dos de l'appareil.</p>	Zones	<p>Réinitialise l'ensemble des zones, types, partitions, attributs. Pour les zones sans fil, la centrale conserve les ID de tous les détecteurs qui sont déjà programmés dans la centrale.</p>	Composants sans fil	<p>Supprime les ID pour les composants sans fil programmés. Faites dérouler la liste des composants et sélectionnez Oui pour chaque type que vous souhaitez supprimer. Appuyez ensuite sur OK pour confirmer votre sélection.</p> <p>Tous les composants Supprime tous les composants sans fil programmés.</p> <p>Détecteurs Supprime uniquement ces composants. Les zones sont également réinitialisées.</p> <p>Sirènes ext. Supprime uniquement ces composants.</p> <p>Sirènes int. Supprime uniquement ces composants.</p> <p>Clavier de commande sans fil Supprime uniquement ces composants.</p> <p>WAM</p>
Option	Effet								
Utilisateur	<p>Supprime tous les utilisateurs ainsi que leurs codes, badges Proximity, télécommandes, alarmes agression, médaillons médicaux et médaillons de soins. Après la réinitialisation, vous êtes invité à attribuer un nouveau code installateur et un nouveau code administrateur. Cette option a le même effet que l'utilisation des « broches de réinitialisation de code ». Vous trouverez des détails à ce sujet dans le chapitre Présentation de l'appareil -> Dos de l'appareil.</p>								
Zones	<p>Réinitialise l'ensemble des zones, types, partitions, attributs. Pour les zones sans fil, la centrale conserve les ID de tous les détecteurs qui sont déjà programmés dans la centrale.</p>								
Composants sans fil	<p>Supprime les ID pour les composants sans fil programmés. Faites dérouler la liste des composants et sélectionnez Oui pour chaque type que vous souhaitez supprimer. Appuyez ensuite sur OK pour confirmer votre sélection.</p> <p>Tous les composants Supprime tous les composants sans fil programmés.</p> <p>Détecteurs Supprime uniquement ces composants. Les zones sont également réinitialisées.</p> <p>Sirènes ext. Supprime uniquement ces composants.</p> <p>Sirènes int. Supprime uniquement ces composants.</p> <p>Clavier de commande sans fil Supprime uniquement ces composants.</p> <p>WAM</p>								

	<p>Supprime uniquement ces composants. Verrous de porte Supprime uniquement ces composants. Répéteur RF Supprime uniquement ces composants.</p>
Sorties	Réinitialise l'ensemble des sorties, types, partitions, attributs.
Activations	Réinitialise toutes les options d'activation, par ex. mode Sortie. Cela concerne le menu « Partitions » et le menu utilisateur « Horaires activation/désactivation ».
Systeme	<p>Réinitialise toutes les options dans le menu « Système ». Réinitialise toutes les options dans le menu utilisateur Configuration.</p> <p> Remarque Ne sont pas réinitialisés dans le menu utilisateur « Configuration » :</p> <ul style="list-style-type: none"> • Moniteur d'activité • Télécommandes • Accès Web • Mises à jour de niveau 4 • Horaires activation/désactivation
• Communication	<p>Réinitialise toutes les options dans le menu « Communication ». En particulier également le menu « Réseau -> Configuration de réseau -> Réseau Web bloqué/autorisé »</p> <p>Cela concerne également le menu « Système -> Sécurité -> Mises à jour de niveau 4 ».</p>
Programmation Usine	<p>Uniquement disponible sur la centrale d'alarme.</p> <p>Ce menu restaure la programmation d'usine de l'appareil.</p> <p> Remarque Vous trouverez les valeurs standard des réglages d'usine en annexe.</p> <p>Les menus suivants s'affichent après la confirmation :</p> <p>Langue</p> <ul style="list-style-type: none"> • Deutsch x.yz - installé • English x.yz • Nederlands x.yz • Francais x.yz • Dansk x.yz • Svenska x.yz • Italiano x.yz • Espanol x.yz

- Polski x.yz
- ...

Remarque

Seules les langues disponibles pour les références correspondantes s'affichent.

Application mise à niveau de la centrale d'alarme

- v2.00.00 – installée
- v2.00.00 07/10/2016 (2621440)
- v1.01.02 25/07/2016 (2293760)
- v1.01.00 16/02/2016 (2293760)
- v1.00.04 01/10/2015 (2293760)
- v1.00.02 26/05/2015 (2293760)
- ...

Programmation pays

- | | |
|-------------------|--------------|
| • Grande-Bretagne | • Suisse |
| • Italie | • Autriche |
| • Espagne | • Irlande |
| • Portugal | • Norvège |
| • Pays-Bas | • Danemark |
| • France | • Suède |
| • Belgique | • Grèce |
| • Allemagne | • Luxembourg |

Remarque

Chaque pays a des réglages différents pour la transmission RTC, la signalisation d'alarme et le début et la fin de l'heure d'été/hiver.

Le changement de pays ne modifie pas la langue.

La programmation pays est utilisée aux fins suivantes :

Tous les pays

Basculement automatique en heure d'été/d'hiver (début et fin de l'heure d'été propres à chaque pays)

France

Manipulation FTA (verrouillage de la zone de la première alarme (First to Alarm))

Cette option verrouille la zone qui a déclenché l'alarme en premier dans une partition afin qu'elle ne puisse entraîner aucune autre alarme/aucun autre défaut jusqu'à la restauration de la zone ou la désactivation de la centrale.

Danemark

Détection de la sonnerie du modem RTC

L'algorithme de détection de la sonnerie du modem RTC doit accepter un temps supplémentaire entre plusieurs sonneries afin de constater que la sonnerie s'est arrêtée. Le réglage normal est de 6 s, mais au Danemark, il est de 8 s.

Pays-Bas

Les fréquences de la tonalité Handshake pour le format rapide et les protocoles d'appel de soins de santé Scancom/Scanfast sont différentes aux Pays-Bas.

En général, les fréquences de la tonalité Handshake pour le format rapide sont de 1 400 Hz/2 300 Hz, mais aux Pays-Bas, elles sont de 1 600 Hz/2 000 Hz.

Programmation Usine

La programmation Usine suivante dépend actuellement de la programmation pays, voir ci-dessous et dans l'annexe « Programmation Usine ».

UK

« Mode Installateur -> Système -> Sécurité -> Brouillage » Programmation Usine « SABOTAGE »

et

« Mode Installateur -> Système -> Sécurité -> Supervision » Programmation Usine « SABOTAGE »

pour satisfaire PD6662:2010

pour tous les autres pays, programmation Usine DÉFAUT

« Mode Installateur -> Système -> Confirmation -> Mode Confirmation », programmation Usine BS8243

pour tous les autres pays, programmation Usine BASIQUE.

Allemagne (version logicielle >= 1.01.00)

« Mode Installateur -> Partitions -> Partition 1-4 -> Tous act. -> Durée sirène extérieure -> 3 minutes »

« Mode Installateur -> Partitions -> Partition 1-4 -> Act. interne -> Durée sirène extérieure -> 3 minutes »

pour tous les autres pays et l'Allemagne (version logicielle < 1.01.00), programmation Usine 15 minutes

Longueur du code d'accès

- Code utilisateur à 4 chiffres
- Code utilisateur à 6 chiffres

Remarque

Ce menu vous permet également de supprimer tous les utilisateurs.

Veillez respecter pour cela les instructions sous Système -> Sécurité -> Code utilisateur à 6 chiffres.

Type de zone filaire

- 2 fils FSL 2k2/4k7
- 2 fils FSL 1k/1k
- 2 fils FSL 2k/2k
- 2 fils FSL 4k7/4k7
- 4 fils NC
- 2 fils CC

Vue d'ensemble

- Adresse IP : 192.168.178.002
- DHCP : Allumée
- Version : v1.01.00
- S/N : SECVEST###E9000139AAE
- Part. N° : FUAA50000

Remarque

Vous obtenez ici une vue d'ensemble des données essentielles de la centrale d'alarme.

Identification

- Nom de l'installateur (serveur Web) : <Nom de l'installateur> (code=nom)
- Code : <Code installateur> tel qu'attribué dans l'assistant de démarrage

- Nom de l'administrateur (serveur Web) : <Nom de l'administrateur> (code=nom)
- Code : <Code administrateur> tel qu'attribué dans l'assistant de démarrage

Remarque

Vous obtenez ici une vue d'ensemble des données actuelles de cet utilisateur. Les détails sont décrits dans les chapitres correspondants.

Désignation/Fonction	Explication (case à cocher)
	<p> Remarque La restauration de la Programmation Usine :</p> <ul style="list-style-type: none"> • supprime tous les périphériques assignés et programmés, et tous les noms, textes et numéros enregistrés • ne supprime pas l'historique • ne supprime pas les utilisateurs avec leurs codes et périphériques • ne supprime pas le nom de l'installateur et le code installateur • ne supprime aucun message vocal enregistré individuellement. <ul style="list-style-type: none"> ○ Pour supprimer l'utilisateur des messages vocaux enregistrés, utilisez le « Test de confiance ». Lorsque le « Test de confiance » a démarré, appuyez sur la touche « 0 » « Charger défauts ». <p> Remarque Pour supprimer également tous les utilisateurs (installateurs, administrateurs et utilisateurs normaux) lors de la réinitialisation des réglages d'usine, procédez comme suit.</p> <p>Après avoir effectué toutes les étapes de la fonction Réglages d'usine, débranchez l'alimentation électrique complète de la centrale (230 V ou bloc d'alimentation 13,8 V et les batteries). Pour cela, vous ne devez pas quitter le mode Installateur.</p> <p>Une fois l'alimentation électrique rétablie, la centrale redémarre avec l'assistant de démarrage complet.</p> <p> Remarque Vous pouvez supprimer des utilisateurs dans le menu utilisateur.</p> <p>Vous pouvez utiliser les « broches de réinitialisation de code » pour supprimer l'intégralité des utilisateurs. Vous trouverez des détails à ce sujet dans le chapitre Présentation de l'appareil -> Dos de l'appareil.</p> <p>Tous les utilisateurs, toutes les balises Proximity, toutes les télécommandes et tous les émetteurs d'appel d'urgence sont alors supprimés. Après la réinitialisation, vous êtes invité à attribuer un nouveau code installateur et un nouveau code administrateur.</p>
Message défaut CA	<p>Activé Signale la présence d'un défaut de l'alimentation électrique 230 V.</p> <p>Désactivé Fonction impossible.</p>
Tempo défaut CA (minutes)	<p>Temporisation en minutes (0 à 60 minutes) avant l'apparition du message.</p> <p>En cas de défaut A/C, la centrale affiche un message d'erreur après quelques secondes, commute les sorties de type "Défaut Général" et crée une entrée dans l'historique (événements prioritaires).</p> <p>Les coupures de courant de moins de 9 secondes ne sont pas signalées.</p> <p>Si le courant est rétabli dans un délai de 9 secondes, les sorties de type "Défaut Général" sont réactivées et une entrée "Alimentation électrique restaurée" est créée dans l'historique.</p> <p>Si la coupure de courant dure plus de 9 secondes :</p> <ul style="list-style-type: none"> • Si la valeur est égale à 0 min., 10 secondes après la coupure, une tonalité d'avertissement retentit et la centrale signale la panne.

- Les sorties de type "A/C défaut" sont commutées.
- Si la valeur est supérieure à 0 min, la temporisation démarre 10 secondes après la coupure de ce minuteur.

Si le courant est rétabli avant la fin de la temporisation, les sorties de type "Défaut Général" sont réinitialisées et la restauration est consignée dans l'historique.

Aucun défaut n'est signalé.

Si le défaut persiste à la fin du délai programmé, une tonalité d'avertissement retentit et le défaut est signalé.

Les sorties de type "A/C défaut" sont activées.

Un utilisateur peut arrêter la tonalité d'avertissement en entrant son code.

L'écran de la centrale d'alarme affiche les détails de l'avertissement. Les sorties de type "Défaut général" et "Défaut A/C" restent actives.

Si le défaut est résolu, la centrale désactive les sorties de type "A/C défaut" et consigne la réinitialisation dans l'historique.

Un utilisateur peut réinitialiser l'alarme et réinitialiser les sorties de type "Défaut général" après avoir entré son code utilisateur.



Remarque

La temporisation de défaut pour le reporting CRA/STS vaut uniquement pour

- la centrale et
- MoHy avec CID 301 ou SIA AT/AR

La communication du défaut via

- le transmetteur vocal
- SMS
- e-mail
- Push

est DIRECTEMENT démarrée.

En cas de défaut PSU de composants externes

- clavier de commande
- générateur de signal int.
- WAM
- répéteur
- MoHy

la communication

- AES/TS Reporting
- transmetteur vocal
- SMS
- e-mail
- Push (uniquement « Mains Fail » (défaut CA) MoHy)

est DIRECTEMENT démarrée.

Désignation/Fonction	Explication (case à cocher)
Message défaut CC ext.	<p>Activé Signale la présence d'un défaut de l'alimentation en tension continue externe.</p> <p>Désactivé Fonction impossible.</p>
Tempo défaut CC ext. (minutes)	<p>Temporisation en minutes (0 à 60 minutes) avant l'apparition du message.</p> <p>En cas de défaut DC, la centrale d'alarme affiche un message d'erreur après quelques secondes, commute les sorties de type "Défaut général" et crée une entrée dans l'historique (évén. prioritaires).</p> <p>Les coupures de courant de moins de 9 secondes ne sont pas signalées.</p> <p>Si le courant est rétabli dans un délai de 9 secondes, les sorties de type "Défaut Général" sont réactivées et une entrée "Alimentation électrique restaurée" est créée dans l'historique.</p> <p>Si la coupure de courant dure plus de 9 secondes :</p> <ul style="list-style-type: none"> • Si la valeur est égale à 0 min., 10 secondes après la coupure, une tonalité d'avertissement retentit et la centrale signale la panne. Les sorties de type "Défaut DC" sont commutées. • Si la valeur est supérieure à 0 min, la temporisation démarre 10 secondes après la coupure de ce minuteur. <p>Si le courant est rétabli avant la fin de la temporisation, les sorties de type "Défaut Général" sont réinitialisées et la restauration est consignée dans l'historique.</p> <p>Aucun défaut n'est signalé.</p> <p>Si le défaut persiste à la fin du délai programmé, une tonalité d'avertissement retentit et le défaut est signalé. Les sorties de type "Défaut DC" sont activées.</p> <p>Un utilisateur peut arrêter la tonalité d'avertissement en entrant son code. L'écran de la centrale d'alarme affiche les détails de l'avertissement. Les sorties de type "Défaut général" et "Défaut DC" restent actives.</p> <p>Si le défaut est résolu, la centrale d'alarme désactive les sorties de type "Défaut DC" et consigne la réinitialisation dans l'historique. Un utilisateur peut réinitialiser l'alarme et réinitialiser les sorties de type "Défaut général" après avoir entré son code utilisateur.</p> <p></p> <p>Remarque</p> <p>La temporisation de défaut pour le reporting CRA/STS vaut uniquement pour</p> <ul style="list-style-type: none"> • la centrale et • MoHy avec CID 301 ou SIA AT/AR <p>La communication du défaut via</p> <ul style="list-style-type: none"> • le transmetteur vocal • SMS • e-mail <p>est DIRECTEMENT démarrée.</p> <p>En cas de défaut PSU de composants externes</p> <ul style="list-style-type: none"> • clavier de commande • générateur de signal int. • WAM • répéteur • MoHy <p>la communication</p>

- AES/TS Reporting
 - transmetteur vocal
 - SMS
 - e-mail
- est DIRECTEMENT démarrée.

Installateur détails

Désignation/Fonction	Explication
Nom de l'installateur	<p>Nom d'utilisateur, série de chiffres ou de caractères qui permettent à l'installateur de se connecter à la centrale d'alarme sur Internet. Il convient de respecter la casse.</p> <p>12 caractères maximum</p> <p>Utilisez un nom sûr ! (voir les consignes de sécurité)</p> <p>Après la première mise en service, modifiez le nom d'installateur (code=nom) attribué automatiquement en choisissant un nom d'utilisateur sûr.</p>
Code installateur	<p>Mot de passe de l'installateur sur le serveur Web, code d'accès à la centrale d'alarme.</p> <ul style="list-style-type: none"> • Il n'y a aucun code installateur pré-réglé en usine. • Le code installateur est attribué dans l'assistant de démarrage lors de la première mise en service. <p>Utilisez un code sûr ! (voir les consignes de sécurité)</p> <p>Remarque pour les versions logicielles < 1.01.00</p> <p>Programmation Usine</p> <ul style="list-style-type: none"> • 9999 (code utilisateur à 4 chiffres) • 999999 (code utilisateur à 6 chiffres) <p>Il est recommandé de modifier ce code.</p> <p>Le code installateur permet d'accéder au mode installateur ou d'effectuer une réinitialisation installateur.</p> <p>Le code installateur ne permet pas d'activer ou de désactiver la centrale d'alarme.</p>

Programmation/configuration

Confirmer nouveau code	Confirmation de mot de passe pour l'installateur en cas de nouvelle attribution de code.
Installateur No tél.	Le numéro de téléphone de l'installateur peut être enregistré ici pour l'utilisateur en cas de panne.

Accès utilisateur

ABUS
Logout

Système | Accès Utilisateur

Enregistrement mémo <input checked="" type="checkbox"/>	Fonction touches doubles <input type="checkbox"/>
Touches Soins de Santé <input type="checkbox"/>	Masquer tous/tes <input checked="" type="checkbox"/>
Armement Rapide <input type="checkbox"/>	Isoler rapidement <input type="checkbox"/>
Code Utilisateur requis <input checked="" type="checkbox"/>	Réponse 2WAY <input checked="" type="checkbox"/>
Téléco Arm Immédiat <input checked="" type="checkbox"/>	Contrainte ON <input type="checkbox"/>

Annuler
Envoyer

INFO

État

Périphériques

Sorties

Partitions

Système

Transmissions

Appel Soins de Santé

Journal de bord

Clavier

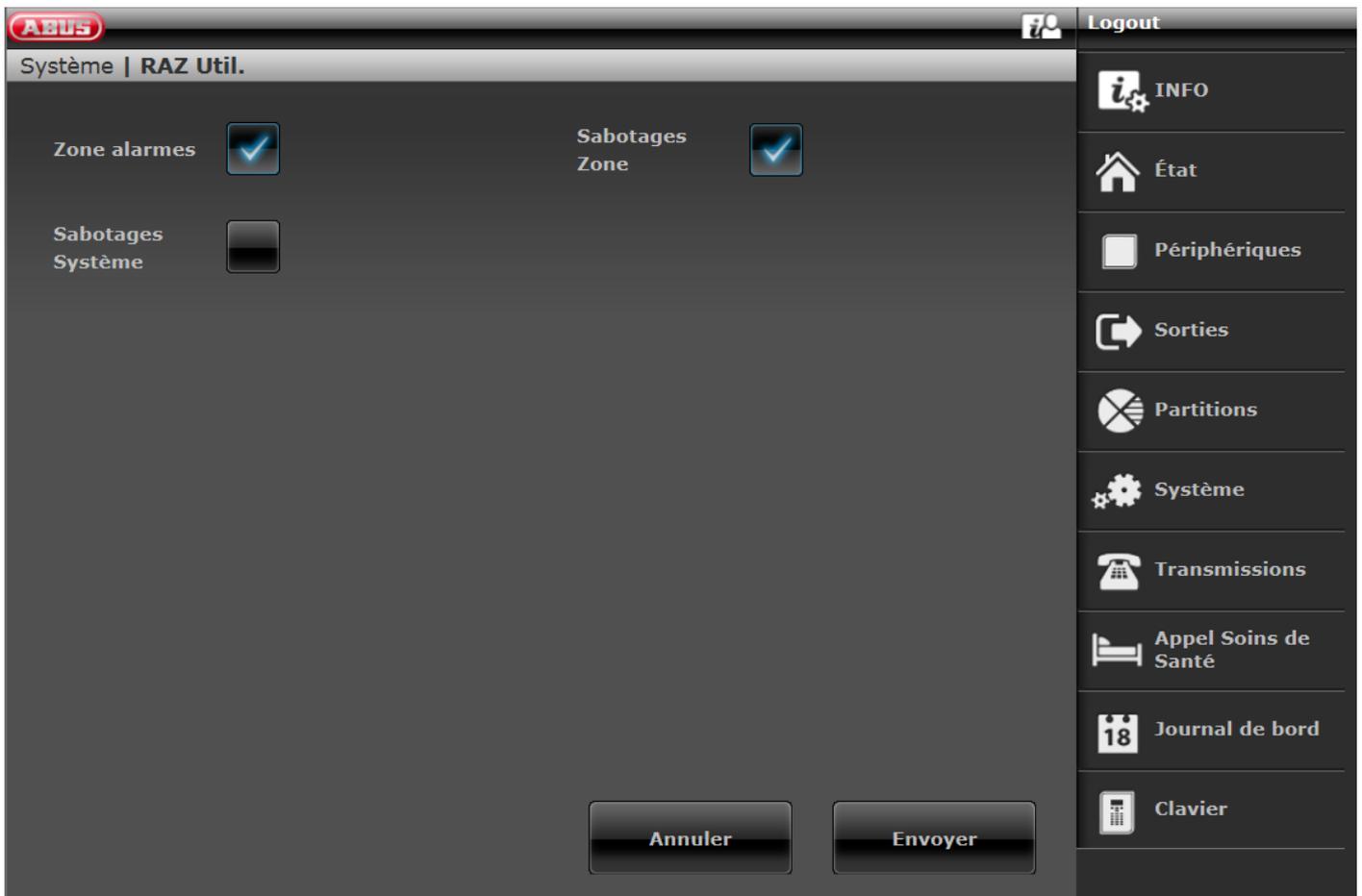
Désignation/Fonction	Explication (case à cocher)
Enregistrement mémo	<p>Activé Permet à l'utilisateur d'enregistrer un mémo. Menu utilisateur -> Mémo vocal</p> <p>Désactivé Fonction impossible.</p>
Fonction touches doubles	<p>Activé</p> <p>Déclenchement manuel possible des alarmes par l'activation simultanée des touches doubles correspondantes (feu, agression, médical) sur le la centrale d'alarme ou l'élément de commande.</p> <div style="text-align: center; margin: 10px 0;"> </div> <p>Danger</p> <p>Version logicielle >=2.01.08</p> <p>Vous utilisez la surface avant tactile du système d'alarme. Le rétroéclairage est paramétré sur « Selon le délai » et est sombre.</p> <p>En touchant une touche, l'éclairage est tout d'abord activé (premier contact). Aucune autre action n'est déclenchée par le « premier contact ». Le clavier fonctionne dès le deuxième contact pour une utilisation normale.</p> <p>Pour plus de détails, voir la section 10.5.1 Fonctions – Rétroéclairage du manuel d'utilisation.</p>

	 <p>Remarque concernant Partition -> Réponse alarme Le type de zone Feu, les doubles touches Feu sur la centrale et les doubles touches Feu sur le clavier de commande déclenchent toujours un reporting CRA/STS lorsque le mode d'appel pour reporting CRA/STS a été autorisé et lorsque le groupe « Feu » est autorisé pour des événements CID/SIA. Exemple : Partition X -> Réponse alarme -> Sirène Transmission de l'alarme incendie à CRA/STS</p> <p>Désactivé Fonction impossible.</p>
Touches Soins de Santé	<p>Activé Déclenchement manuel possible d'un appel soins de santé par l'activation simultanée des touches doubles correspondantes sur la centrale d'alarme ou l'élément de commande.</p>  <p>Danger Version logicielle >=2.01.08 Vous utilisez la surface avant tactile du système d'alarme. Le rétroéclairage est paramétré sur « Selon le délai » et est sombre. En touchant une touche, l'éclairage est tout d'abord activé (premier contact). Aucune autre action n'est déclenchée par le « premier contact ». Le clavier fonctionne dès le deuxième contact pour une utilisation normale. Pour plus de détails, voir la section 10.5.1 Fonctions – Rétroéclairage du manuel d'utilisation.</p> <p>Désactivé Fonction impossible.</p>
Masquer tous/tes	<p>Activé En cas d'activation de la centrale d'alarme, toutes les zones ouvertes peuvent être isolées manuellement en même temps.</p> <p>Désactivé En cas d'activation de la centrale, les zones ouvertes doivent être isolées manuellement et individuellement.</p>

Désignation/Fonction	Explication (case à cocher)
Armement rapide	<p>Activé Activation de la centrale d'alarme via les touches de symbole sans saisie préalable du code utilisateur.</p> <p>Désactivé Activation de la centrale d'alarme uniquement après la saisie préalable du code utilisateur.</p>
Isoler rapidement	<p>Activé Les zones ouvertes sont automatiquement isolées lors de l'activation de la centrale d'alarme (si les attributs de zone le permettent).</p> <p>Désactivé Les zones ouvertes doivent être isolées manuellement lors de l'activation de la centrale d'alarme.</p>
Code utilisateur requis	<p>Utilisez cette option pour vous assurer qu'un installateur peut accéder au système uniquement lorsqu'un utilisateur est présent.</p> <p>Activé / J (programmation Usine) Une fois que l'installateur a saisi son code, la centrale demande un code utilisateur. Ce n'est qu'après la saisie du code utilisateur que l'installateur peut accéder au système.</p> <p style="text-align: center;">Centrale d'alarme Mode Installateur -> Système -> Accès utilisateur -> Code utilisateur requis J (réglage d'usine)</p> <p>Désactivé L'installateur accède au mode installateur dès qu'il a saisi son code.</p> <p>Remarque Le réglage Désactivé/Non n'est pas conforme à la norme EN 50131.</p> <p style="text-align: center;">L'état conforme est atteint conformément au réglage d'usine, c'est-à-dire que l'utilisateur de niveau 2 doit accorder l'accès à l'utilisateur de niveau 3 (installateur). Norme EN 50131-1, chapitre 8.3.1 Niveaux d'accès (lien avec la norme EN 50131-3, chapitre 8.3.1 Niveaux d'accès (NA)) « L'accès au niveau d'accès 3 doit être évité, à moins que a) -> l'accès ait été accordé par un utilisateur du niveau d'accès 2 ou b) -> »</p> <p>Le réglage Désactivé/Non est uniquement conforme à BS8243 lorsque l'utilisateur a donné son accord écrit.</p>
Réponse 2WAY	<p>Activé La centrale d'alarme sans fil envoie un message d'état actif à la télécommande sans fil, l'élément de commande sans fil, la "Secvest Key" et le verrou de porte supplémentaire.</p> <p>Désactivé Réponse 2WAY désactivée.</p>

Désignation/Fonction	Explication (case à cocher)
Téléco arm immédiat	<p>Utilisez cette option pour choisir comment doit s'activer la centrale d'alarme après l'actionnement de la télécommande.</p> <p>Activé Les partitions possibles sont immédiatement activées ou activées en interne. Si une temporisation de sortie est configurée, celle-ci est ignorée et la centrale d'alarme est activée dès que la touche d'activation de la télécommande est actionnée.</p> <p>Désactivé Les partitions possibles sont activées ou activées en interne en fonction du mode de sortie défini.</p>
Contrainte ON	<p>Activé L'utilisateur administrateur peut créer un "Code contrainte U". Le code contrainte permet d'activer et de désactiver la centrale.</p> <p>Attention Si un intrus oblige l'utilisateur à désactiver la centrale d'alarme, l'utilisateur doit entrer le code contrainte. La centrale réagit alors comme suit :</p> <ul style="list-style-type: none">• La communication programmée en cas de menace est mise en route.• Aucun avertisseur n'est activé.• La sirène de la centrale d'alarme n'est pas activée, aucun triangle ne s'affiche en bas à droite de l'écran. <p>Le code agression permet également de réactiver en interne la centrale le groupe d'utilisateurs. Ceci est utile lorsque l'intrus vous demande de réactiver la centrale d'alarme. L'intrus vérifie dans ce cas si le code n'est soumis à aucune restriction, c'est-à-dire s'il s'agit d'un code "normal". Les sorties de type "Contrainte" commutent. Des entrées correspondantes sont créées dans l'historique.</p> <p>Désactivé Il est impossible de créer un "Code Contrainte U".</p>

RAZ Util.



Désignation/Fonction	Explication (case à cocher)
	Ces menus déterminent dans quelles circonstances un utilisateur ou un installateur peut réinitialiser la centrale après une alarme ou un sabotage.
Zone alarmes	<p>Activé Permet à l'utilisateur de réinitialiser ces alarmes déclenchées dans des zones ou sur des détecteurs.</p> <p>Désactivé Réinitialisation impossible par l'utilisateur. L'installateur doit réinitialiser la centrale après une alarme.</p>
Sabotages zone	<p>Activé Permet à l'utilisateur de réinitialiser les alarmes sabotage déclenchées dans des zones ou sur des détecteurs.</p> <p>Désactivé Réinitialisation impossible par l'utilisateur. L'installateur doit réinitialiser la centrale. Ce réglage est nécessaire pour une reconnaissance INCERT.</p>
Sabotages système	<p>Activé Permet à l'utilisateur de réinitialiser les alarmes sabotage qui concernent la centrale.</p> <p>Désactivé Réinitialisation impossible par l'utilisateur. L'installateur doit réinitialiser la centrale. Ce réglage est nécessaire pour une reconnaissance INCERT. Les sabotages systèmes peuvent être causés par :</p> <ul style="list-style-type: none"> • Contact anti-sabotage du boîtier et de la cloison de la centrale d'alarme

- Contact anti-sabotage du boîtier et de la cloison des éléments de commande
- Sabotage des sirènes filaires raccordées si la tension sur le terminal TR est supérieure à env. 3 V
- Brouillage ou supervision si sabotage est réglé

Confirmation

The screenshot shows the 'Bestätigung' (Confirmation) screen in the ABUS system configuration. The main area contains three dropdown menus: 'Best. Modus' set to '*Basis', 'Alarmgeber Ein' set to '*nicht bestätigen', and 'Sirene Ein' set to '*nicht bestätigen'. At the bottom, there are two buttons: 'Abbruch' (Cancel) and 'Übernehmen' (Accept). On the right side, there is a sidebar menu with the following items: 'Abmelden', 'Info', 'Status', 'Komponenten', 'Ausgänge', 'Teilbereiche', 'System', 'Kommunikation', 'Pflegenotruf', 'Test', 'Logbuch', and 'Tastatur'.

Désignation/Fonction	Explication (case à cocher)
Conf. Mode	<p> Remarque Respectez également les informations détaillées relatives à la temporisation de sirène. Elles sont disponibles sous Temporisation de sirène Partitions Toutes actives.</p> <p> Remarque Le mode de confirmation fonctionne uniquement lorsque la réponse alarme est réglée sur « Sirène + TS Reporting » (voir Configuration de partitions).</p> <p>Liste déroulante de sélection :</p> <ul style="list-style-type: none"> • Base <ul style="list-style-type: none"> ○ Si vous choisissez cette option, la centrale d'alarme active une sortie programmée comme « Alarme confirmée » si une deuxième zone d'alarme est activée tandis que le système se trouve en état d'alarme. La deuxième zone d'alarme doit appartenir à la partition qui se trouve en état d'alarme. L'installateur peut aussi indiquer si

	<p>les utilisateurs peuvent réinitialiser le système après une alarme de zone.</p> <ul style="list-style-type: none"> ○ Si le mode de confirmation = « Basique », l'administrateur peut en outre activer ou désactiver les fonctions de panique pour toutes les télécommandes via l'option « Menu utilisateur - Configuration - Télécommandes - Fonction de panique ». ○ Remarque : L'alarme de panique confirmée n'est pas disponible en mode de confirmation Basique. <ul style="list-style-type: none"> • DD243 • BS8243 <p> Remarque Les réglages DD243 et BS8243 sont pertinents uniquement pour le Royaume-Uni (Grande-Bretagne). La sélection de ces options exige des connaissances détaillées de ces directives.</p>
<p>Sirène ON</p>	<p>Liste déroulante de sélection :</p> <ul style="list-style-type: none"> • Ne pas confirmer <ul style="list-style-type: none"> ○ Le système est activé. La centrale d'alarme activera toutes les sirènes internes en cas de survenue d'une alarme non confirmée. • Confirmer <ul style="list-style-type: none"> ○ Le système est activé. La centrale d'alarme n'activera aucune sirène interne jusqu'à la survenue d'une alarme confirmée. <p>Remarque La centrale d'alarme ne permet pas le réglage suivant : Sirène ON – confirmer et Sirène ON – ne pas confirmer</p>
<p>Sirène ON</p>	<p>Liste déroulante de sélection :</p> <ul style="list-style-type: none"> • Ne pas confirmer <ul style="list-style-type: none"> ○ La centrale d'alarme déclenche les sirènes externes pour toutes les alarmes et ignore toute temporisation de sirène. • Confirmer <ul style="list-style-type: none"> ○ Le système est activé. La centrale d'alarme n'activera aucune sirène jusqu'à la survenue d'une alarme confirmée. <p>Remarque  La centrale d'alarme ne permet pas le réglage suivant : Sirène ON – ne pas confirmer et Sirène ON – confirmer</p>
<p>Temps confirmation (uniquement en mode confirmation DD243 et BS8243)</p>	<p>Champ de saisie de la durée de confirmation en cas d'alarme intrusion en minutes. La durée de confirmation peut être comprise entre 1 et 60 minutes.</p> <p>Remarque  Les durées de confirmation < 30 minutes ne sont pas conformes aux exigences de DD243 et BS8243.</p>

Clav bloqué tempo entrée (uniquement en mode confirmation DD243 et BS8243)	Activé L'utilisateur doit désactiver la centrale via un dispositif alternatif (pas sur l'élément de commande ni la centrale d'alarme), par ex. une télécommande ou un interrupteur à clé (important pour DD243 et BS8243). Désactivé L'utilisateur peut désactiver la centrale en entrant son code d'accès sur le clavier (élément de commande ou système d'alarme) après l'ouverture de la porte d'entrée (important pour DD234).
RAZ non confirmée (uniquement en mode confirmation DD243 et BS8243)	Liste déroulante de sélection : <ul style="list-style-type: none">• Installateur• Utilisateur
Après entrée (uniquement en mode confirmation DD243 et BS8243)	Liste déroulante de sélection : <ul style="list-style-type: none">• Jamais• 2 zones (uniquement pour DD243)• 1 zone
RAZ confirmée (uniquement en mode confirmation DD243 et BS8243)	Liste déroulante de sélection : <ul style="list-style-type: none">• Installateur• Utilisateur
Temps confirmation Alarme anti-agression (uniquement en mode confirmation BS8243)	Champ de saisie du délai de confirmation d'une alarme agression en heures. Remarques  Conformément à BS8243, le délai de confirmation doit être compris entre 8 et 20 heures.
Sabotage= seulement sabotage (uniquement en mode confirmation BS8243)	Activé Désactivé

Hardware

ABUS  Logout

Système | Hardware

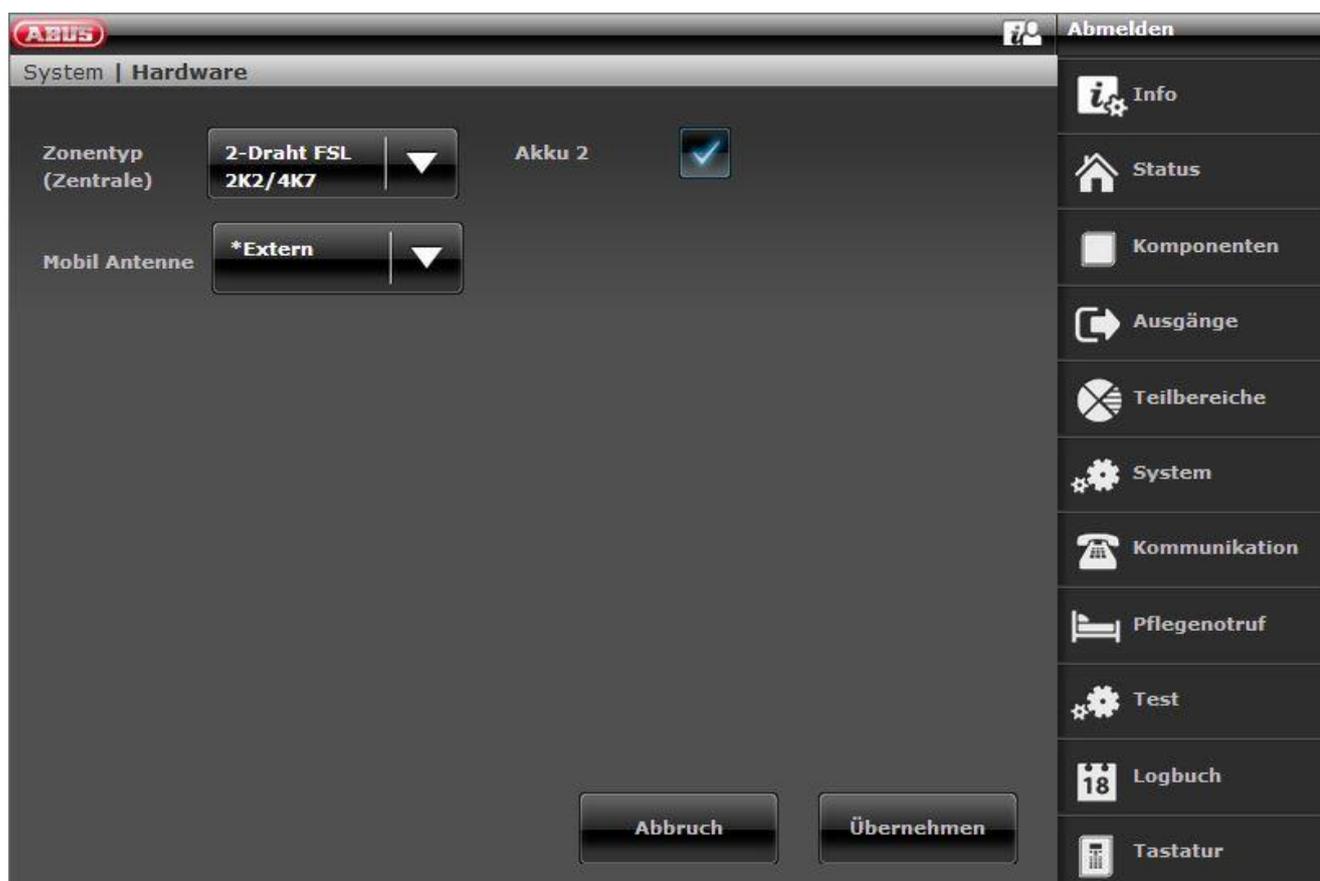
Type Zone (Centrale) **Ne pas modifier** ▼ Options Sirène radio ***Sirène + Flash** ▼

Batt. 2

Annuler **Envoyer**

-  INFO
-  État
-  Périphériques
-  Sorties
-  Partitions
-  Système
-  Transmissions
-  Appel Soins de Santé
-  **18** Journal de bord
-  Clavier

Version logicielle >= 2.00.00



Désignation/Fonction	Explication (case à cocher)
<p>Type de zone (centrale d'alarme)</p> <p>Type de zone filaire</p>	<p>Liste déroulante de sélection :</p> <p>Utilisation des entrées pour les zones filaires</p> <ul style="list-style-type: none"> • Ne pas modifier • 2 fils FSL 2k2/4k7 • 2 fils FSL 1k/1k • 2 fils FSL 2k/2k • 2 fils FSL 4k7/4k7 • 4 fils NC • 2 fils CC
<p>Options sirènes radio</p>	<p>Version logicielle < 2.00.00</p> <p>Liste déroulante de sélection :</p> <p>Configuration de sirène. Sélectionnez ici comment la sirène radio doit réagir en cas d'alarme feu, intrusion ou agression.</p> <ul style="list-style-type: none"> • Sirène + flash La sirène radio actionne la sirène et le flash en cas d'alarme • Flash La sirène radio actionne uniquement le flash en cas d'alarme <p>Version logicielle >= 2.00.00</p> <p>Voir à ce sujet Partitions -> Réponse alarme</p>
<p>Batt. 2</p>	<p>Vous avez branché une deuxième batterie. Cette option vous permet d'autoriser ou de bloquer l'émission de messages d'avertissement.</p> <p>Activé / Autorisé</p> <p>La centrale d'alarme émet des messages d'alarme si la batterie 2 manque ou a une tension faible.</p> <p>Désactivé / Bloqué</p> <p>La centrale d'alarme ignore la présence ou l'absence de la seconde batterie.</p>

Désignation/Fonction	Explication (case à cocher)
<p>Carte SD</p>	<p>Uniquement disponible sur la centrale d'alarme.</p> <p>Enlever Hardware sûrement</p> <ul style="list-style-type: none"> • Les procédures d'écriture ou de lecture éventuellement en cours sont terminées de manière conforme. • La carte SD peut être retirée en toute sécurité. <p>Hardware autorisé</p> <ul style="list-style-type: none"> • Après insertion, la carte SD peut être à nouveau mise en service. • Il est à nouveau possible d'écrire et de lire. <p> Danger Protection des données Tenez compte des remarques relatives à la carte SD dans le chapitre « Mise hors service de la centrale ».</p>
<p>Antenne GSM Antenne mobile</p>	<p>Le menu s'affiche uniquement si un module GSM/de téléphonie mobile est installé.</p> <p>Interne</p> <ul style="list-style-type: none"> • L'antenne qui se trouve directement sur le module de téléphonie mobile est utilisée. <p>Externe</p> <ul style="list-style-type: none"> • L'antenne qui a été raccordée à la connexion d'antenne du module de téléphonie mobile est utilisée. <p> Danger Pour l'installation supplémentaire du module Wi-Fi, utilisez impérativement Externe. L'antenne de téléphonie mobile interne sur la platine peut influencer voire empêcher la connexion du signal Wi-Fi.</p>

Réglages de sécurité

Version logicielle < 3.01.11

The screenshot displays the 'Einstellungen Sicherheit' (Security Settings) screen for an ABUS system. The interface is dark-themed with white text and icons. At the top left, the 'ABUS' logo is visible. The main area is divided into two columns of settings. The left column includes: 'Supervision' set to '*Störung', 'Sabotage ausblenden' (disabled), 'FB Deaktiv Aktiv' set to '*Immer', 'FBT Deaktiv Aktiv' set to '*Immer', 'System Auto Wiederaktiv' set to '*Niemals', 'Abbruchzeit [s] (Sekunden)' set to '120', 'Eingang Alarmverzögerung' (checked), and 'Fern-Updates' (checked). The right column includes: 'RF Jamming' set to '*Störung', 'Zwangsaktiv' set to '*Bestätigen', 'FB Deaktiv intern Aktiv' set to '*Immer', 'FBT Deaktiv intern Aktiv' set to '*Immer', 'Warntöne Stumm' set to '*Benutzer Code', and 'Siren Delay (User)' set to '0'. At the bottom of the settings area are 'Abbruch' and 'Übernehmen' buttons. On the right side, there is a vertical sidebar with navigation options: 'Abmelden', 'Info', 'Status', 'Komponenten', 'Ausgänge', 'Teilbereiche', 'System', 'Kommunikation', 'Pflegetruf', 'Test', 'Logbuch', and 'Tastatur'. The 'System' option is currently selected.

Version logicielle >= 3.01.11

ABUS Abmelden

System | Einstellungen Sicherheit

Zentrale | **Komponenten**

RF Supervision	*Störung ▼	RF Jamming	*Störung ▼
Sabotage ausblenden	<input type="checkbox"/>	Zwangsaktiv	*Bestätigen ▼
System Auto Wiederaktiv	*Niemals ▼	Warntöne Stumm	*Benutzer Code ▼
Abbruchzeit [s] (Sekunden)	120	Eingang Alarmverzögerung	<input checked="" type="checkbox"/>
Broadcast Status Zentrale	<input checked="" type="checkbox"/>	Level4 Updates	<input checked="" type="checkbox"/>

Abbruch Übernehmen

Info

Status

Komponenten

Ausgänge

Teilbereiche

System

Kommunikation

Pflegenotruf

Test

18 Logbuch

Tastatur

ABUS Abmelden

System | Einstellungen Sicherheit

Zentrale | **Komponenten**

Kamera Supervision	*Störung ▼	Sirenenverz. (Ben)	0
FB Deaktiv Aktiv	*Immer ▼	FB Deaktiv intern Aktiv	*Immer ▼
FBT Deaktiv Aktiv	*Immer ▼	FBT Deaktiv intern Aktiv	*Immer ▼

Abbruch Übernehmen

Info

Status

Komponenten

Ausgänge

Teilbereiche

System

Kommunikation

Pflegenotruf

Test

18 Logbuch

Tastatur

Désignation/Fonction	Explication (case à cocher)									
Code utilisateur à 6 chiffres	<p>Remarque :</p> <p>Ce menu n'existe plus à partir de la version logicielle 1.01.00. Le choix d'un code utilisateur à 4 ou 6 chiffres s'effectue exclusivement dans l'assistant de démarrage. Il n'est plus possible de modifier la longueur du code une fois que vous avez quitté l'assistant.</p> <p>Activé Code numérique à 6 chiffres pour l'installateur et l'utilisateur</p> <p>Désactivé Code numérique à 4 chiffres pour l'installateur et l'utilisateur</p> <p> Remarque</p> <ul style="list-style-type: none"> • Passage de 4 à 6 chiffres En cas de passage de 4 à 6 chiffres, les codes à 4 chiffres sont automatiquement complétés par "00". Exemple : "1234" devient "123400". • Passage de 6 à 4 chiffres En cas de passage de 6 à 4 chiffres, les codes par défaut sont rétablis. Lors de la réinitialisation des codes numériques (de 6 à 4 chiffres), la programmation d'usine de tous les utilisateurs et installateurs est restaurée (également suppression des télécommandes, badges, etc.). 									
Désignation/Fonction	Explication (case à cocher)									
RF Supervision	<p>Liste déroulante de sélection de la réaction du système d'alarme en cas de supervision RF</p> <p>Si un détecteur sans fil n'a pas de contact avec la centrale pendant plus de 20 minutes, la centrale d'alarme crée une entrée « Avertiss. RF » dans l'historique. Par ailleurs, la centrale d'alarme empêche l'activation. Lorsqu'un utilisateur ignore cet avertissement et active la centrale, une entrée "RF PB ignorée" est générée dans l'historique.</p> <p>Si un détecteur sans fil n'a pas de contact avec la centrale d'alarme pendant plus de 2 heures, les procédures suivantes s'exécutent comme suit :</p> <table border="1"> <thead> <tr> <th></th> <th>La centrale d'alarme est activée</th> <th>La centrale d'alarme est désactivée</th> </tr> </thead> <tbody> <tr> <td>Bloqué</td> <td>Aucune réaction</td> <td>Aucune réaction</td> </tr> <tr> <td>Anomalie</td> <td> <ul style="list-style-type: none"> • Consignation de cet événement dans l'historique • Pas d'affichage sur l'écran et pas de tonalités d'avertissement • Les sorties de type "RF Supervision" ou "RF Défaut" sont commutées. • La supervision est signalée </td> <td> <ul style="list-style-type: none"> • Consignation de cet événement dans l'historique • Affichage sur l'écran et tonalités d'avertissement • Les sorties de type "RF Supervision" ou "RF Défaut" sont commutées. • La supervision est signalée </td> </tr> </tbody> </table>		La centrale d'alarme est activée	La centrale d'alarme est désactivée	Bloqué	Aucune réaction	Aucune réaction	Anomalie	<ul style="list-style-type: none"> • Consignation de cet événement dans l'historique • Pas d'affichage sur l'écran et pas de tonalités d'avertissement • Les sorties de type "RF Supervision" ou "RF Défaut" sont commutées. • La supervision est signalée 	<ul style="list-style-type: none"> • Consignation de cet événement dans l'historique • Affichage sur l'écran et tonalités d'avertissement • Les sorties de type "RF Supervision" ou "RF Défaut" sont commutées. • La supervision est signalée
	La centrale d'alarme est activée	La centrale d'alarme est désactivée								
Bloqué	Aucune réaction	Aucune réaction								
Anomalie	<ul style="list-style-type: none"> • Consignation de cet événement dans l'historique • Pas d'affichage sur l'écran et pas de tonalités d'avertissement • Les sorties de type "RF Supervision" ou "RF Défaut" sont commutées. • La supervision est signalée 	<ul style="list-style-type: none"> • Consignation de cet événement dans l'historique • Affichage sur l'écran et tonalités d'avertissement • Les sorties de type "RF Supervision" ou "RF Défaut" sont commutées. • La supervision est signalée 								

	<p>Sabotage</p> <ul style="list-style-type: none"> • Consignation de cet événement dans l'historique • Antisabotage • La supervision est signalée <p>Remarque : Si "Sabotage = seulement sabotage" est bloqué, les sorties de type "Supervision" ou "Défaut" sont également commutées. Si aucun canal sabotage n'est assigné dans FF, une "alarme non confirmée" est envoyée.</p>	<ul style="list-style-type: none"> • Consignation de cet événement dans l'historique • Antisabotage • La supervision est signalée <p>Remarque Si "Sabotage = seulement sabotage" est bloqué, les sorties de type "Supervision" ou "Défaut" sont également commutées. Si aucun canal sabotage n'est assigné dans FF, une "alarme non confirmée" est envoyée.</p>												
	<p>Remarque L'option sabotage est nécessaire dans les systèmes de niveau 2 pour la conformité à EN 50131-1:2006+A1:2009</p> <p>Si l'option sabotage est utilisée et le réglage Système -> RAZ util. -> Sabotages système = Non est défini, l'utilisateur ne peut pas réinitialiser la centrale.</p>													
<p>Supervision caméra</p>	<p>Liste déroulante de sélection de la réaction du système d'alarme en cas de supervision par caméra IP</p> <p>Si une caméra n'a pas de contact avec la centrale pendant plus longtemps que le temps de réponse, la centrale crée une entrée dans l'historique et signale un avertissement (par ex. IP Zone Missing, IP-Zone Timeout).</p> <p>Temps de réponse, voir : Périphériques -> Zones IP -> Ajouter/Supprimer -> Temps de réponse</p> <p>Les procédures correspondantes s'exécutent comme suit :</p> <table border="1" data-bbox="520 1335 1536 1800"> <thead> <tr> <th></th> <th>La centrale d'alarme est activée</th> <th>La centrale d'alarme est désactivée</th> </tr> </thead> <tbody> <tr> <td>Bloqué</td> <td>Aucune réaction</td> <td>Aucune réaction</td> </tr> <tr> <td>Anomalie</td> <td> <ul style="list-style-type: none"> • Consignation de cet événement dans l'historique • Pas d'affichage sur l'écran et pas de tonalités d'avertissement </td> <td> <ul style="list-style-type: none"> • Consignation de cet événement dans l'historique • Affichage sur l'écran et tonalités d'avertissement </td> </tr> <tr> <td>Sabotage</td> <td> <ul style="list-style-type: none"> • Antisabotage • La supervision est signalée </td> <td> <ul style="list-style-type: none"> • Antisabotage • La supervision est signalée </td> </tr> </tbody> </table>			La centrale d'alarme est activée	La centrale d'alarme est désactivée	Bloqué	Aucune réaction	Aucune réaction	Anomalie	<ul style="list-style-type: none"> • Consignation de cet événement dans l'historique • Pas d'affichage sur l'écran et pas de tonalités d'avertissement 	<ul style="list-style-type: none"> • Consignation de cet événement dans l'historique • Affichage sur l'écran et tonalités d'avertissement 	Sabotage	<ul style="list-style-type: none"> • Antisabotage • La supervision est signalée 	<ul style="list-style-type: none"> • Antisabotage • La supervision est signalée
	La centrale d'alarme est activée	La centrale d'alarme est désactivée												
Bloqué	Aucune réaction	Aucune réaction												
Anomalie	<ul style="list-style-type: none"> • Consignation de cet événement dans l'historique • Pas d'affichage sur l'écran et pas de tonalités d'avertissement 	<ul style="list-style-type: none"> • Consignation de cet événement dans l'historique • Affichage sur l'écran et tonalités d'avertissement 												
Sabotage	<ul style="list-style-type: none"> • Antisabotage • La supervision est signalée 	<ul style="list-style-type: none"> • Antisabotage • La supervision est signalée 												

Désignation/Fonction	Explication (case à cocher)		
RF Brouillage	Liste déroulante de sélection de la réaction de la centrale d'alarme en cas de brouillage :		
	La centrale d'alarme peut détecter les brouillages. Les procédures correspondantes s'exécutent comme suit :		
		La centrale d'alarme est activée	La centrale d'alarme est désactivée
	Bloqué	Aucune réaction	Aucune réaction
	Anomalie	<ul style="list-style-type: none"> • Consignation de cet événement dans l'historique • Pas d'affichage sur l'écran et pas de tonalités d'avertissement 	<ul style="list-style-type: none"> • Consignation de cet événement dans l'historique • Affichage sur l'écran et tonalités d'avertissement
Sabotage	<ul style="list-style-type: none"> • Antisabotage • Le brouillage est signalé <p>Remarque : Si "Sabotage = seulement sabotage" est bloqué, les sorties de type "Brouillage" ou "Défaut" sont également commutées. Si aucun canal sabotage n'est assigné dans FF, une "alarme non confirmée" est envoyée.</p>	<ul style="list-style-type: none"> • Antisabotage • Le brouillage est signalé <p>Remarque Si "Sabotage = seulement sabotage" est bloqué, les sorties de type "Brouillage" ou "Défaut" sont également commutées. Si aucun canal sabotage n'est assigné dans FF, une "alarme non confirmée" est envoyée.</p>	
	<p>Remarque L'option sabotage est nécessaire pour la conformité à PD 6662:2010. Si l'option sabotage est utilisée et le réglage Système -> RAZ util. -> Sabotages système = Non est défini, l'utilisateur ne peut pas réinitialiser le système.</p>		
Mises à jour de niveau 4	<p>Centrale Mode Installateur -> Système -> Sécurité -> Mises à jour de niveau 4 -> Bloqué*/Autorisé</p> <p>INTERFACE WEB Mode Installateur -> Système -> Réglages de sécurité -> Mises à jour de niveau 4 -> Bloqué (désactivé, option décochée)*/Autorisé (activé, option cochée)</p> <p>Bloqué (désactivé, option décochée) Autorisé (activé, option cochée)</p> <p>Lorsque cette option est autorisée, il faut saisir un nouveau code de niveau 4. Ceci ne s'applique que si ce code de niveau 4 n'a jamais été programmé au préalable (depuis la livraison ou depuis la dernière réinitialisation de la programmation Usine). Ce code de niveau 4 comporte le même nombre de chiffres que le code installateur ou le code utilisateur.</p> <p>Entrée du « nouveau code de niveau 4 » et « confirmation du code de niveau 4 » (saisir une nouvelle fois le code pour confirmation). Un nouvel utilisateur est automatiquement créé. Voir le menu utilisateur « Utilisateur ».</p>		

Nom : « Niveau 4 »

Remarque :

Pour des raisons de sécurité, vous devez modifier le nom par défaut « Niveau 4 » de l'utilisateur de niveau 4.

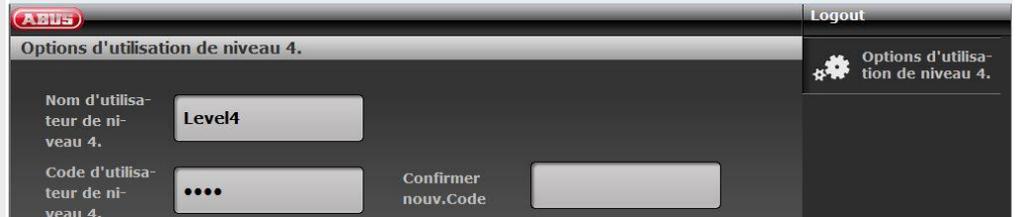
L'administrateur ou l'utilisateur lui-même peut modifier ce nom.

Lorsque vous utilisez ensuite le code de niveau 4 pour accéder à la centrale, seules les options de menu

Nom d'utilisateur de niveau 4.

Code d'utilisateur de niveau 4.

apparaissent pour autoriser cet utilisateur à modifier le nom et le code.



Voir annexe « Mise à niveau logicielle ». Cette section contient des détails sur le processus de mise à niveau logicielle.

Isoler sabotage

Si un utilisateur isole une zone, il peut être nécessaire d'isoler également le circuit anti-sabotage de cette zone.

Activé

Le contact anti-sabotage est également isolé au sein d'une zone isolée.

Désactivé

Le contact anti-sabotage continue d'être surveillé au sein d'une zone isolée.

Désignation/Fonction	Explication (case à cocher)
Armement forcé	<p>Version logicielle >= 3.01.16</p> <p>Le réglage pour Activation forcée (Off, Confirmer ou On) vaut désormais pour tous les périphériques à activer (par ex. télécommande, clavier de commande, verrou de porte supplémentaire, Secvest Key) et pour tous les avertissements qui n'empêchent pas l'activation (avertissements qui peuvent être ignorés).</p> <p>Défauts qui pourraient empêcher l'activation :</p> <ul style="list-style-type: none">• Périphérique qui ne fonctionne plus<ul style="list-style-type: none">○ Entre 20 min et 120 min, signalisation par avertissement RF○ > 120 min, signalisation par défaut de supervision, empêche toute activation• Autres défauts, par ex. défauts d'alimentation électrique ou piles vides• Zones ouvertes<ul style="list-style-type: none">○ Empêche toute activation○ Comportement spécial avec l'attribut de zone « Activation forcée isolée » <p></p> <p>Remarque</p> <p>Toutes les activations sur la centrale s'effectuent par saisie de code et interaction avec le menu. Activation rapide ignore les avertissements affichés mais les consigne. L'utilisation via l'application est une forme d'activation rapide.</p> <p><u>Périphérique qui ne fonctionne plus</u></p> <ul style="list-style-type: none">• OFF <p>Moins de 20 min après la panne d'un périphérique, une activation sans restriction ni avertissement est possible.</p> <p>Entre 20 min et 120 min, la centrale a détecté un avertissement RF d'un périphérique. Le comportement en cas de tentative d'activation est alors le suivant :</p> <p>Centrale</p> <ul style="list-style-type: none">Démarrage du processus d'activationL'avertissement RF est affichéOK est activé (l'utilisateur a pris connaissance de l'avertissement et l'ignore)La centrale est active <p>Télécommande, clavier de commande, verrou de porte supplémentaire, Secvest Key</p> <ul style="list-style-type: none">Le périphérique est activéMessage de défaut sur le périphérique selon le périphériqueLa centrale ne peut pas être activée <p>Remarque :</p> <p>Une centrale avec défaut en cours peut être activée uniquement sur la centrale.</p> <p>Cas spécial défaut de supervision > 120 min</p> <p>Centrale, télécommande, clavier de commande, verrou de porte supplémentaire, Secvest Key</p> <ul style="list-style-type: none">Message de défaut sur le périphérique selon le périphériqueLa centrale ne peut pas être activée

• **Confirmer**

Moins de 20 min après la panne d'un périphérique, une activation sans restriction ni avertissement est possible.

Entre 20 min et 120 min, la centrale a détecté un avertissement RF d'un périphérique. Le comportement en cas de tentative d'activation est alors le suivant :

Centrale

Démarrage du processus d'activation

L'avertissement RF est affiché

OK est activé (l'utilisateur a pris connaissance de l'avertissement et l'ignore)

La centrale est active

Télécommande, clavier de commande, verrou de porte supplémentaire, Secvest Key

Le périphérique est activé

Message de défaut sur le périphérique selon le périphérique

La centrale n'est pas activée

Le périphérique est activé une **deuxième fois**

La centrale est désormais active

Cas spécial défaut de supervision > 120 min

Centrale, télécommande, clavier de commande, verrou de porte supplémentaire, Secvest Key

Message de défaut sur le périphérique selon le périphérique

La centrale ne peut pas être activée

• **Allumée**

Moins de 20 min après la panne d'un périphérique, une activation sans restriction ni avertissement est possible.

Entre 20 min et 120 min, la centrale a détecté un avertissement RF d'un périphérique. Le comportement en cas de tentative d'activation est alors le suivant :

Centrale

Démarrage du processus d'activation

L'avertissement RF est affiché

OK est activé (l'utilisateur a pris connaissance de l'avertissement et l'ignore)

La centrale est active

Télécommande, clavier de commande, verrou de porte supplémentaire, Secvest Key

Le périphérique est activé

La centrale est directement active

Remarque :

En cas d'**Activation forcée = On** sur ces périphériques, l'utilisateur n'est pas informé du défaut en cours. Les défauts qui sont ignorés sont également consignés dans l'historique.

Cas spécial défaut de supervision > 120 min

Centrale, télécommande, clavier de commande, verrou de porte supplémentaire, Secvest Key

Message de défaut sur le périphérique selon le périphérique
La centrale ne peut pas être activée

Autres défauts

• OFF

Le comportement en cas de tentative d'activation est le suivant :

Centrale

Démarrage du processus d'activation

Le défaut est affiché

OK est activé (l'utilisateur a pris connaissance de l'avertissement et l'ignore)

La centrale est active

Télécommande, clavier de commande, verrou de porte supplémentaire, Secvest
Key

Le périphérique est activé

Message de défaut sur le périphérique selon le périphérique

La centrale ne peut pas être activée

Remarque :

une centrale avec défaut en cours peut être activée uniquement sur la centrale.

• Confirmer

Le comportement en cas de tentative d'activation est le suivant :

Centrale

Démarrage du processus d'activation

Le défaut est affiché

OK est activé (l'utilisateur a pris connaissance de l'avertissement et l'ignore)

La centrale est active

Télécommande, clavier de commande, verrou de porte supplémentaire, Secvest
Key

Le périphérique est activé

Message de défaut sur le périphérique selon le périphérique

La centrale n'est pas activée

Le périphérique est activé une **deuxième fois**

La centrale est désormais active

• Allumée

Le comportement en cas de tentative d'activation est le suivant :

Centrale

Démarrage du processus d'activation

Le défaut est affiché

OK est activé (l'utilisateur a pris connaissance de l'avertissement et l'ignore)

La centrale est active

Télécommande, clavier de commande, verrou de porte supplémentaire, Secvest Key

Le périphérique est activé
La centrale est directement active

Remarque :

En cas d'**Activation forcée = On** sur ces périphériques, l'utilisateur n'est pas informé du défaut en cours. Les défauts qui sont ignorés sont également consignés dans l'historique.

Zones ouvertes

• **OFF**

Le comportement en cas de tentative d'activation avec l'attribut de zone « **Activation forcée isolée** » est le suivant :

Centrale

Démarrage du processus d'activation
Le défaut est affiché
La centrale peut être activée après la fermeture de la zone.

Télécommande, clavier de commande, verrou de porte supplémentaire, Secvest Key

Le périphérique est activé
Message de défaut sur le périphérique selon le périphérique
La centrale ne peut pas être activée

Remarque :

La centrale peut être activée après la fermeture de la zone.

• **Confirmer**

Le comportement en cas de tentative d'activation avec l'attribut de zone « **Activation forcée isolée** » est le suivant :

Centrale

Démarrage du processus d'activation
Le défaut est affiché
La centrale peut être activée après la fermeture de la zone.
La zone peut aussi être masquée manuellement.

Télécommande, clavier de commande, verrou de porte supplémentaire, Secvest Key

Le périphérique est activé
Message de défaut sur le périphérique selon le périphérique
La centrale n'est pas activée
Le périphérique est activé une **deuxième fois**
La centrale est désormais active avec des zones **masquées**

• **Allumée**

Le comportement en cas de tentative d'activation avec l'attribut de zone « **Activation forcée isolée** » est le suivant :

	<p>Centrale</p> <ul style="list-style-type: none">Démarrage du processus d'activationLe défaut est affichéLa centrale peut être activée après la fermeture de la zone.La zone peut aussi être masquée manuellement. <p>Télécommande, clavier de commande, verrou de porte supplémentaire, Secvest Key</p> <ul style="list-style-type: none">Le périphérique est activéLa centrale est directement active avec des zones masquées <p>Remarque : En cas d'Activation forcée = On sur ces périphériques, l'utilisateur n'est pas informé du défaut en cours. Les défauts qui sont ignorés sont également consignés dans l'historique.</p> <p>Version logicielle < 3.01.16</p> <p>Vous pouvez permettre à un utilisateur d'activer la centrale d'alarme avec la télécommande même si une ou plusieurs zones ne fonctionnent pas ou sont ouvertes.</p> <p>Remarque Si vous autorisez l'armement forcé, la centrale ne sera plus conforme à EN 50131.</p> <p>Liste déroulante de sélection :</p> <ul style="list-style-type: none">• OFF<ul style="list-style-type: none">• L'utilisateur ne peut pas forcer l'activation de la centrale avec la télécommande, même si les zones correspondantes possèdent l'attribut Activation forcée.• Confirmer<ul style="list-style-type: none">• L'utilisateur peut forcer l'armement de la centrale avec la télécommande. Pour ce faire, il doit procéder comme suit :<ol style="list-style-type: none">1. L'utilisateur appuie sur la touche Armement de la télécommande2. Le système ne démarre pas l'activation3. L'utilisateur appuie encore une fois sur la touche de la télécommande pour confirmer qu'il souhaite activer la centrale.• Allumée<ul style="list-style-type: none">• L'utilisateur doit seulement appuyer une fois sur la touche correspondante de la télécommande pour démarrer le processus d'activation. <p>Remarque Avec les options Confirmer et ON, l'utilisateur peut également activer la centrale avec la télécommande, même si une réinitialisation était nécessaire après une alarme.</p>
<p>Désarm. télé tjs ou tps entrée</p>	<p>Choisissez si la désactivation des partitions activées via la télécommande n'est possible que si le délai de temporisation a démarré au préalable (la zone de type "Entrée/Sortie" est déclenchée)</p> <p>Liste déroulante de sélection :</p> <ul style="list-style-type: none">• Toujours

	<ul style="list-style-type: none"> • Pendant "tps d'entrée" <ul style="list-style-type: none"> • L'utilisateur peut toujours désactiver les partitions possibles sans que le temps d'entrée n'ait démarré au préalable. • L'utilisateur doit d'abord ouvrir une zone de type "Entrée/Sortie". Ceci démarre la temporisation d'entrée. L'utilisateur peut maintenant désactiver les partitions possibles. • Les partitions pour lesquelles aucune temporisation d'entrée n'a démarré restent actives.
<p>Désarm.P. télé tjs ou tps entrée</p>	<p>Choisissez si la désactivation des partitions activées en interne via la télécommande n'est possible que si le délai de temporisation a démarré au préalable (la zone de type "Entrée/Sortie" est déclenchée)</p> <p>Liste déroulante de sélection :</p> <ul style="list-style-type: none"> • Toujours • Pendant "tps d'entrée" <ul style="list-style-type: none"> • L'utilisateur peut toujours désactiver les partitions possibles sans que le temps d'entrée n'ait démarré au préalable. • L'utilisateur doit d'abord ouvrir une zone de type "Entrée/Sortie". Ceci démarre la temporisation d'entrée. L'utilisateur peut maintenant désactiver les partitions possibles. • Les partitions pour lesquelles aucune temporisation d'entrée n'a démarré restent actives.

Désignation/Fonction	Explication (case à cocher)
Clav tps d'entrée	<p>Choisissez si la désactivation des partitions activées via l'élément de commande sans fil n'est possible que si le délai de temporisation a démarré au préalable (la zone de type "Entrée/Sortie" est déclenchée)</p> <p>Liste déroulante de sélection :</p> <ul style="list-style-type: none"> • Toujours • Pendant "tps d'entrée" <ul style="list-style-type: none"> • L'utilisateur peut toujours désactiver les partitions possibles sans que le temps d'entrée n'ait démarré au préalable. • L'utilisateur doit d'abord ouvrir une zone de type "Entrée/Sortie". Ceci démarre la temporisation d'entrée. L'utilisateur peut maintenant désactiver les partitions possibles. • Les partitions pour lesquelles aucune temporisation d'entrée n'a démarré restent actives.
Clav tps d'entrée partiel	<p>Choisissez si la désactivation des partitions activées en interne via l'élément de commande sans fil n'est possible que si le délai de temporisation a démarré au préalable (la zone de type "Entrée/Sortie" est déclenchée)</p> <p>Liste déroulante de sélection :</p> <ul style="list-style-type: none"> • Toujours • Pendant "tps d'entrée" <ul style="list-style-type: none"> • L'utilisateur peut toujours désactiver les partitions possibles sans que le temps d'entrée n'ait démarré au préalable. • L'utilisateur doit d'abord ouvrir une zone de type "Entrée/Sortie". Ceci démarre la temporisation d'entrée. L'utilisateur peut maintenant désactiver les partitions possibles. • Les partitions pour lesquelles aucune temporisation d'entrée n'a démarré restent actives.
Réarmement auto	<p>S'affiche si Système->Confirmation->Mode confirmation->Basique</p> <p>Indiquez combien de fois la centrale doit se réactiver automatiquement après écoulement de la durée de sirène.</p> <p>Liste déroulante de sélection :</p> <ul style="list-style-type: none"> • Jamais • 1 x, 2 x, 3 x, 4 x, 5 x • Toujours <ul style="list-style-type: none"> • La centrale n'est pas réactivée. La centrale passe une fois seulement à l'état d'alarme. • Le système réactive toutes les zones fermées mais pas les détecteurs qui envoient toujours des signaux d'alarme. • L'un de ces réglages est nécessaire pour la conformité à EN 50131.

- Lorsque l'installation est à nouveau activée, la centrale sans fil émet une alarme acoustique interne à la place de la tonalité d'entrée habituelle quand un utilisateur entre dans la centrale via la route d'entrée.

Désignation/Fonction	Explication (case à cocher)
Avertissements silencieux (alarmes silencieuses)	<p>Cette option permet de définir l'intervalle d'émission des tonalités d'avertissement (un bip court toutes les quelques minutes).</p> <p>Liste déroulante de sélection :</p> <ul style="list-style-type: none"> • Code utilisateur <ul style="list-style-type: none"> • Des avertissements sont émis jusqu'à ce qu'un utilisateur entre son code de confirmation de l'avertissement. • 30 minutes • 60 minutes • 120 minutes <ul style="list-style-type: none"> • Des avertissements sont émis en fonction de la durée définie. L'émission des tonalités d'avertissement peut être interrompue en saisissant un code utilisateur. • Pas de signal sonore <ul style="list-style-type: none"> • Aucun signal acoustique n'est émis. <p>Remarque La centrale d'alarme n'affiche pas d'avertissement tant qu'une partition est encore active.</p>
Temps abandon	<p>Champ de saisie du temps d'abandon de l'alarme en secondes (entre 0 et 120 secondes).</p> <p>La centrale démarre toujours cette temporisation quand une alarme a été déclenchée. Si un utilisateur coupe cette alarme pendant ce délai, la réinitialisation par l'installateur n'est pas nécessaire.</p> <p>Si une alarme survient et un utilisateur désactive la centrale pendant ce délai, les sorties de type "Alarme Annulation" sont commutées et l'annulation de l'alarme est signalée.</p>
Temporisation de sirène (utilisateur)	<p>« Temporisation de sirène (utilisateur) » en minutes (valeur entre 0 et 10). 0 signifie désactivée.</p> <p></p> <p>Remarque Lorsque « Temporisation de sirène (spécifique à l'utilisateur) » est activé (> 0), le comportement global de la temporisation de sirène est bloqué dans les réglages de partition !</p> <p>Ceci n'est pas conforme à la norme EN 50131. La communication CRA/STS et le mode de confirmation ont un effet sur la temporisation de sirène dans les réglages de partition.</p> <p></p> <p>Remarque Temporisation de sirène (utilisateur) a uniquement des effets sur les sirènes d'extérieur pour les configurations suivantes :</p> <p>Partition -> Réponse alarme (Toutes actives, Active en interne, Désactivée) Sirène + Reporting STS ou</p>

	<p>Flash + TS Reporting Dans les autres variantes Interne, Sirène et Flash, cette temporisation de sirène agit pour tous les composants (centrale, sirène intérieure, module d'information, clavier de commande et sirène extérieure). Il faut donc signaler tous ces périphériques une fois la durée de temporisation écoulée.</p> <p></p> <p>Remarque En cas d'alarme incendie, agression ou 24 h, il n'y a pas de temporisation de sirène (utilisateur)</p>
<p>Entrée alarme temporisation</p>	<p>Temporisation supplémentaire si la route d'entrée n'est pas suivie.</p> <p>Si la route d'entrée n'est pas suivie, vous pouvez accorder 30 secondes supplémentaires à l'utilisateur avant le déclenchement d'une alarme externe.</p> <p>Activé La temporisation supplémentaire (30 secondes) est activée si la route d'entrée n'est pas suivie.</p> <p>Si un utilisateur s'écarte de la route d'entrée pendant le délai de temporisation d'entrée, la centrale d'alarme attend 30 secondes avant le déclenchement d'une alarme totale. Seule une alarme interne se déclenche au cours de ces 30 secondes. Si un utilisateur entre son code pendant les 30 secondes de l'alarme interne, il peut réinitialiser la centrale. Ce réglage est conforme à EN 50131.</p> <p>Désactivé Pas de temporisation supplémentaire si la route d'entrée n'est pas suivie. Une alarme se déclenche immédiatement si un utilisateur s'écarte de la route d'entrée, déclenchant ainsi un autre détecteur. Ce réglage n'est pas conforme à EN 50131.</p>

Désignation/Fonction	Explication (case à cocher)
Émission état centrale	<p>Activé</p> <p>Toute modification d'état de la centrale d'alarme est transmise à tout moment à l'élément de commande sans fil. L'élément de commande signale l'état des partitions, des alarmes et les temporisations d'entrée et de sortie "juste à temps".</p> <p>Désactivé</p> <p>L'état de la centrale est envoyé à l'élément de commande uniquement sur demande (touche "?" de l'élément de commande). L'état des partitions, des alarmes et des temporisations d'entrée et de sortie n'est pas affiché / signalé sur l'élément de commande.</p>

Mise à niveau de la centrale

Désignation/Fonction	Explication (case à cocher)
Fichier de langue	<p>Cliquez sur le bouton Parcourir pour indiquer le chemin d'accès et le nom du fichier de langue à charger.</p> <p>Cliquez sur le bouton Envoyer pour installer le fichier sélectionné dans la centrale d'alarme sans fil.</p>
Fichier d'application	<p>Cliquez sur le bouton Parcourir pour indiquer le chemin d'accès et le nom du fichier d'application à charger.</p> <p>Cliquez sur le bouton Envoyer pour installer les fichiers sélectionnés dans le système d'alarme sans fil.</p> <p>Le redémarrage de la centrale d'alarme sans fil est nécessaire.</p>

Vous trouverez également des détails sur la mise à niveau logicielle vers la version 1.01.00 dans le document « Mise à niveau logicielle » dans l'espace de téléchargement de la page Web ABUS.



Remarque

Le menu « Centrale Upgrade » n'est disponible à cet emplacement que jusqu'à la version logicielle <1.01.00. Pour des raisons de conformité avec la norme EN 50131, un autre processus a été établi à partir de la version 1.01.00.

Nouveau niveau d'autorisation « Utilisateur de niveau / niveau d'accès 4 » pour les mises à jour logicielles

- Les mises à jour logicielles via le menu Installateur du serveur Web ne sont plus possibles
- L'autorisation pour l'« utilisateur de niveau 4 » doit être attribuée dans le menu Utilisateur et installateur.
- Le code utilisateur pour l'« utilisateur de niveau 4 » est attribué après l'autorisation

Programmation/configuration

L'annexe « Mise à niveau logicielle » contient des détails à ce sujet.

Uniquement sur la centrale d'alarme

Mode Installateur -> Système -> Mise à niveau de la centrale d'alarme



Remarque

Il est obligatoire d'effectuer la mise à jour du fichier de langue AVANT la mise à jour du fichier d'application !

Voir chapitre « Mise à niveau logicielle avec nouveaux fichiers depuis la carte SD » en annexe

Après avoir appuyé sur « Sélectionner », une liste des applications logicielles disponibles apparaît.

La première ligne de la liste indique la version logicielle actuellement installée et les lignes suivantes les fichiers logiciels disponibles enregistrés sur la carte SD.

exemple

APPLICATION MISE À NIVEAU DE LA CENTRALE D'ALARME		
V3.01.14	Installée	
V1.01.00	10/02/2016	(2293760)
V2.00.00	04/10/2016	(2621440)
V2.00.06	06/03/2017	(2621440)
V2.01.08	15/06/2017	(2686976)
V3.00.04	12/12/2017	(2883584)
V3.01.01	10/05/2018	(2883584)
V3.01.11	17/10/2018	(2883584)
V3.01.14	11/03/2019	(2949120)
V3.01.16	25/11/2019	(2949120)
V3.01.17	10/12/2019	(2949120)

Sélectionnez l'application logicielle souhaitée.

Après le chargement de la version logicielle, le premier point de l'assistant de démarrage s'affiche (sélection de langue). Suivez l'assistant d'installation et de démarrage de la centrale.



Important

Version logicielle >= 3.00.06, sauvegarde et réinitialisation de la configuration

Avant que la centrale ne démarre la mise à niveau, les données de configuration et le certificat SSL sont automatiquement enregistrés dans le flash interne. Le nouveau logiciel est alors installé et la centrale est redémarrée. La programmation Usine est alors tout d'abord utilisée, mais la centrale restaure ensuite automatiquement les données de configuration et le certificat SSL du flash (tout comme si vous aviez enregistré/réinitialisé la configuration manuellement). Cela signifie que l'assistant de démarrage n'est pas exécuté et que le certificat SSL n'est pas généré à nouveau.

Contrôler la mise à niveau ?



Remarque

Pour des raisons de conformité avec la norme EN 50131, ce menu est à ce stade uniquement disponible en mode Installateur, directement sur la centrale.

Via un navigateur Web, vous ne trouverez pas ce menu en mode installateur. Ce menu s'affiche dans le menu de niveau 4. Un utilisateur de niveau 4 doit pour cela se connecter. Vous trouverez des détails à ce sujet dans le chapitre Mise à niveau logicielle en annexe.

Désignation/Fonction	Explication
Contrôler la mise à niveau ?	<p>Après avoir appuyé sur « Sélectionner », la centrale d'alarme interroge le serveur FTP ABUS : « De nouveaux logiciels sont-ils disponibles ? ».</p> <p>Si le serveur FTP répond « Oui », la remarque suivante s'affiche : « Mise à niveau disponible ».</p> <p>Si le serveur FTP répond « Non », la remarque suivante s'affiche : « Mise à niveau non disponible ».</p>
Mise à niveau disponible	<p>Si vous souhaitez poursuivre avec la mise à niveau du panneau, appuyez sur OK. Attendez jusqu'à ce que le panneau consulte les fichiers de langues. N'appuyez pas sur OK.</p> <p>Attendez jusqu'à ce que le panneau consulte le fichier d'application. N'appuyez pas sur OK.</p> <p> Remarque Ces fichiers ont été enregistrés sur la carte SD.</p> <p>Redémarrer maintenant La centrale d'alarme installe les nouveaux fichiers de la carte SD et redémarre.</p>

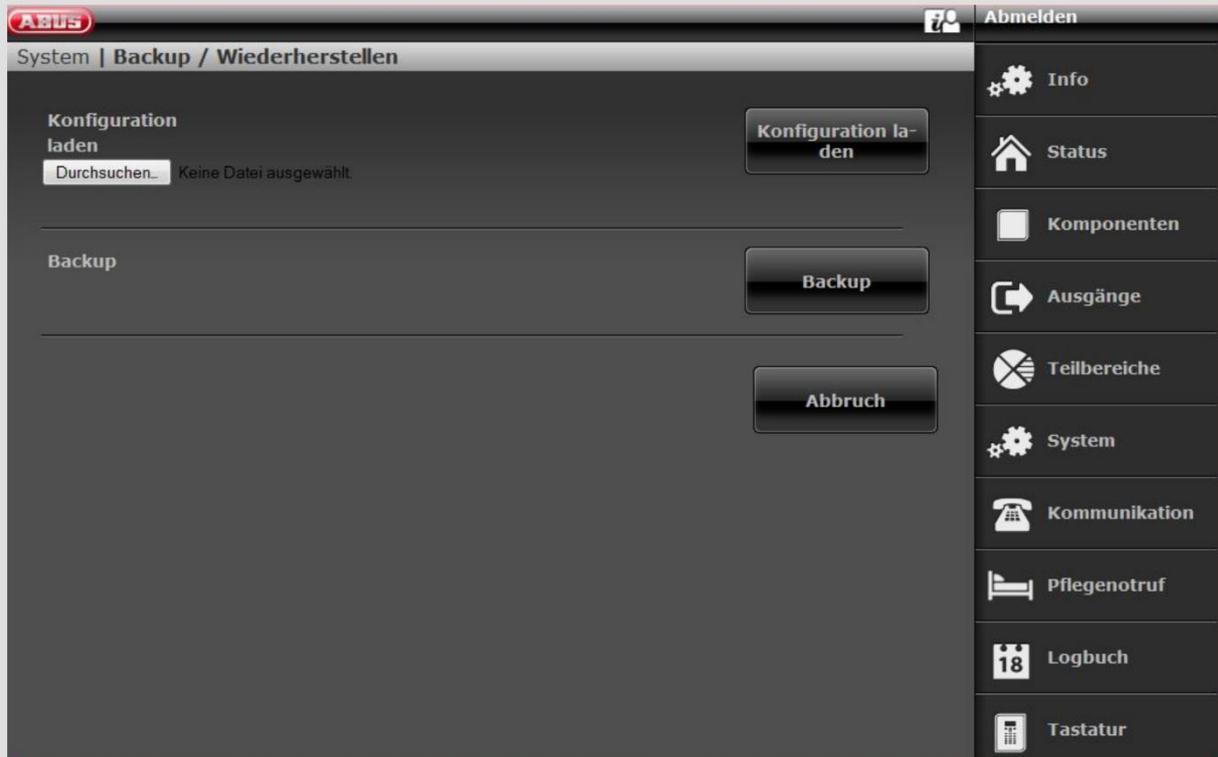


Important

Version logicielle >= 3.00.06, sauvegarde et réinitialisation de la configuration

Avant que la centrale ne démarre la mise à niveau, les données de configuration et le certificat SSL sont automatiquement enregistrés dans le flash interne. Le nouveau logiciel est alors installé et la centrale est redémarrée. La programmation Usine est alors tout d'abord utilisée, mais la centrale restaure ensuite automatiquement les données de configuration et le certificat SSL du flash (tout comme si vous aviez enregistré/réinitialisé la configuration manuellement). Cela signifie que l'assistant de démarrage n'est pas exécuté et que le certificat SSL n'est pas généré à nouveau.

Sauvegarder/Restaureur



Désignation/Fonction	Explication (case à cocher)
Charger configuration	<p>Cliquez sur le bouton Parcourir pour indiquer le chemin d'accès et le nom de fichier de la configuration à restaurer.</p> <p>Cliquez sur le bouton Charger configuration pour installer la configuration à restaurer sur la centrale d'alarme sans fil.</p> <p>Le redémarrage de la centrale d'alarme sans fil est nécessaire.</p>
Backup	<p>Cliquez sur le bouton Backup pour sauvegarder la configuration complète du système (y compris les ID des détecteurs). Le fichier de sauvegarde est enregistré dans le dossier de téléchargement par défaut.</p> <p></p> <p>Remarque</p> <p>Le fichier de configuration est enregistré au format Secvest--01-09-2017-1051.cfg. Si l'instruction jointe de modification du nom de fichier n'a pas pu être exécutée par le PC ou le navigateur Web, celle-ci est enregistrée dans la variante par défaut « config.config ».</p>

Version logicielle >=3.00.00

Sauvegarder/Restaurer (centrale d'alarme GUI uniquement)

Centrale d'alarme

Mode Installateur -> Système -> Sauvegarder/Restaurer

Config. de sauvegarde sur carte SD

Après avoir appuyé sur « Sélectionner », le fichier de configuration est enregistré sur la carte SD. À ce moment-là, l'écran affiche « **Fichier enregistré** ».

Config. de chargement depuis carte SD

Après avoir sélectionné le fichier de configuration souhaité et appuyé sur « Sélectionner », le fichier de configuration est chargé depuis la carte SD dans la centrale d'alarme. À ce moment-là, l'écran affiche « **Fichier lu** ».



Remarque

La centrale d'alarme crée un nouveau dossier intitulé « Config » sur la carte SD. Dans ce dossier sont décrits tous les fichiers de configuration. Chaque nouveau fichier reçoit un nouveau nom. Aucun fichier n'est écrasé.

La centrale d'alarme crée un nom de fichier contenant Secvest, la date et l'heure.

Exemple (version logicielle 3.00.00 jusqu'à version logicielle < 3.01.00) :

Secvest--01-09-2017-1051.cfg

01-09-2017 : Date

1051 : Heure, 10 heures 51 minutes

Exemple (version logicielle >= 3.01.01) :

Secvest—2018-11-08-0935.cfg

2018-11-08 : Date, 8 novembre 2018

0935 : Heure, 9 heures 35 minutes



Remarque

Vous pouvez également copier des fichiers de configuration enregistrés sur PC (via Internet) sur la carte SD. Copiez les fichiers de configuration dans le dossier « Config ». Si la centrale d'alarme n'a pas encore créé de dossier intitulé « Config », vous pouvez également le créer vous-même.

Pour ce faire, respectez ce qui suit :

Le fichier de configuration n'est parfois pas enregistré au format **Secvest--01-09-2017-1051.cfg** ou **Secvest--2017-09-01-1051.cfg**.

Si l'instruction jointe de modification du nom de fichier n'a pas pu être exécutée par le PC ou le navigateur Web, celle-ci est enregistrée dans la variante par défaut « config.config ».

Modifiez le nom du fichier « config.config » simplement au format suivant **Secvest--01-09-2017-1051.cfg** ou **Secvest--2017-09-01-1051.cfg**.

Important :

- l'extension du fichier doit obligatoirement être « .cfg » ;
- le nom du fichier doit commencer par Secvest et 2 traits d'union ou signes moins « **Secvest—** ».

Les fichiers dont le nom ne respecte pas cette syntaxe ne seront pas affichés dans le menu « Config. de chargement depuis carte SD » de la centrale d'alarme.

Par exemple « config.config » ou « Secvest--01-12-2017-1102.config ».



Danger

Protection des données

Tenez compte des remarques relatives à la carte SD dans le chapitre « Mise hors service de la centrale ».

Rapport

Version logicielle >=3.00.01

Interface Web uniquement



Désignation/Fonction	Explication (case à cocher)
Rapport	En cliquant sur le bouton Rapport , une fenêtre contextuelle s'ouvre dans le navigateur. Celle-ci indique de façon claire la configuration complète du système de la centrale d'alarme.

Drucken

Installation

Installation Standort:

Installation Adresse:

Errichter Name: "Firma XYZ"

Errichter Tel Nr.: "0123 4567890"

Datum: 27/11/2017

Info zu Zentrale

Version: v3.00.03

Sprache: Deutsch v1.27

Serien Nr.: SECVEST###GC028819AAB

Part No.: FUAA50000

RF Device Exclusivity: Nein

Zonen: Verfügbar: 58 Verwendet: IP: 0 FUNK: 4 VERDRAHTET: 0

Funk Bedienteil: 0

Funk Sirenen: 0

UVM: 0

Türschlösser: 0

Teilbereiche: 2

Impression

Appuyez sur le bouton « Impression » dans le formulaire en haut à gauche pour imprimer le rapport. La boîte de dialogue Windows par défaut « Impression » s'ouvre. Sélectionnez l'imprimante souhaitée.



Remarque

Le choix de l'imprimante se porte sur celles raccordées à l'ordinateur.

Par ex. « vraie » imprimante papier ou « imprimante PDF » telle que PDF-Xchange, Freepdf.

Contenu du rapport

Le rapport contient tous les réglages et informations pertinents du mode Installateur ainsi que les réglages de volume du menu utilisateur.



Remarques

Sorties de type « Défini par l'utilisateur »

Polarité : normale ou inversée, si « inversée », le mot « inversée » apparaît ici. Si « normale », aucun mot supplémentaire n'apparaît ici.

Si un planning est enregistré, les jours de la semaine sélectionnés apparaissent en lettres majuscules.

Programmation/configuration

Exemple : En continu 08:00 -> 16:00 **SmDmDfS**

Heure d'activation 08:00, heure de désactivation 16:00

S	m	D	m	D	f	S
Dim	Lu	Ma	Me	Je	Ve	Sa
oui	non	oui	non	oui	non	oui

Communication

Réseau

The screenshot displays the configuration interface for an ABUS device. At the top left, the 'ABUS' logo is visible. The main header area contains the text 'Kommunikation | Netzwerk'. Below this, four large buttons are arranged horizontally: 'Netzwerk Setup' (with a network diagram icon), 'IP Mobil Setup' (with a network diagram icon), 'E-Mail Setup' (with an envelope icon), and 'VoIP Wähler Setup' (with a 'VOIP' speech bubble and gear icon). On the right side, there is a vertical sidebar menu titled 'Abmelden' at the top. The menu items, from top to bottom, are: 'Info' (with an 'i' and gear icon), 'Status' (with a house icon), 'Komponenten' (with a square icon), 'Ausgänge' (with a right-pointing arrow icon), 'Teilbereiche' (with a circle and diagonal lines icon), 'System' (with a gear icon), 'Kommunikation' (with a telephone handset icon), 'Pflegenotruf' (with a bed icon), 'Test' (with a gear icon), 'Logbuch' (with a calendar icon showing '18'), and 'Tastatur' (with a keyboard icon).

Configuration de réseau

ABUS
Logout

Transmissions | Réseau

Port HTTP interne	<input type="text"/>	DHCP	<input type="checkbox"/>	
Port HTTPS interne	<input type="text"/>	Adresse IP	<input type="text"/>	
DNS Adresse IP primaire	<input type="text"/>	Masque sous-réseau IP	<input type="text"/>	
		Passerelle adresse IP	<input type="text"/>	

Serveur ABUS autorisé	<input checked="" type="checkbox"/>	Nom d'utilisateur serveur ABUS	<input type="text"/>
Port HTTPS externe	<input type="text"/>	Mot de passe serveur ABUS	<input type="password"/>

- INFO
- État
- Périphériques
- Sorties
- Partitions
- Système
- Transmissions
- Appel Soins de Santé
- Test
- 18 Journal de bord
- Clavier

Désignation/Fonction	Explication (case à cocher)
Port HTTP interne	<p>Port HTTP interne Valeur standard : 80</p> <p> Remarque N'effectuez pas de transfert de port au niveau du port 80 du routeur. Ceci peut entraîner un blocage du réseau. Comme cible du transfert de port, utilisez le « port HTTPS interne », par ex. 4433.</p>
Port HTTPS interne	<p>Port HTTPS interne Valeur standard : 4433</p> <p> Remarque Version logicielle >= 3.00.05 La modification du port HTTPS interne est effective uniquement après un redémarrage de la centrale. Pour cela, déconnectez-vous du mode Installateur et effectuez un redémarrage de la centrale. Consultez le chapitre « Redémarrage manuel (extinction et rallumage) » en annexe pour plus de détails.</p>

<p>DHCP</p>	<p>Activé La Secvest reprend les données IP via le serveur DHCP.</p> <p>Désactivé Saisie manuelle des données IP.</p>
<p>Adresse IP</p>	<p>Adresse IP</p> <p>Version logicielle <2.00.00 : Si vous ne saisissez rien dans ce champ, la centrale utilise automatiquement DHCP.</p> <p></p> <p>Remarque</p> <p>Il est recommandé d'attribuer une adresse IP fixe pour éviter les problèmes de transmission de port. Sur le routeur, il est possible de faire en sorte que la centrale Secvest attribue toujours la même adresse IP via DHCP à cette adresse MAC. Cependant, certains routeurs attribuent tout de même une autre adresse IP via DHCP après un certain temps.</p>
<p>Masque sous-réseau IP</p>	<p>Masque de sous-réseau IP.</p>
<p>Passerelle adresse IP</p>	<p>Passerelle adresse IP</p>
<p>DNS adresse IP primaire</p>	<p>DNS adresse IP primaire</p>
<p>Serveur ABUS autorisé</p>	<p>Activé</p> <ul style="list-style-type: none"> • Établit la connexion avec le serveur ABUS et envoie les données d'accès IP publiques. • Version logicielle >= 3.01.16 La centrale envoie un ping ICMP au serveur ABUS. <p></p> <p>Remarque</p> <ul style="list-style-type: none"> • La centrale envoie toutes les 30 minutes les informations suivantes toujours au serveur ABUS, même si aucun compte personnel n'est enregistré : L'adresse MAC, l'adresse IP publique et le port HTTPS public. Une fois le compte personnel enregistré, vous avez accès à ces données. Cela s'effectue uniquement via Ethernet, pas via Mobile IP. • Version logicielle >= 3.01.16 La centrale d'alarme envoie toutes les 30 minutes un ping ICMP au serveur ABUS. Cela s'effectue uniquement via Ethernet, pas via Mobile IP. La centrale teste ainsi le chemin IP, et particulièrement le chemin non direct au raccordement Ethernet de la centrale et dans la zone publique. Les défauts dans cette zone peuvent être : <ul style="list-style-type: none"> ○ Zone publique (WAN) Câble public vers le routeur défectueux, chantier devant la maison ○ Zone privée (LAN) Remarque : l'interface Ethernet directe sur la centrale est surveillée via « Défaut voie comm. Ethernet ». Le routeur est éteint mais le commutateur fonctionne (la centrale est raccordée directement à ce commutateur). Problèmes avec le module Wi-Fi Le Wi-Fi du routeur est hors service Pas de reconnexion au Wi-Fi après un arrêt prolongé du routeur Le Wi-Fi du routeur s'éteint entre par ex. 22h00 et 06h00 (parfois un réglage par défaut de routeurs ou une fonction d'économie d'énergie).

	<p>Si ce ping ICMP n'a pas de résultat positif, la centrale passe directement à Mobile IP. La condition requise pour ceci est l'utilisation d'un module de téléphonie mobile comme redondance et le réglage correspondant pour « Passerelle IP » (Communication -> Réseau -> Configuration Mobile IP). Mobile IP est utilisé temporairement jusqu'à ce que le ping ICMP ait à nouveau un résultat positif.</p> <p></p> <p>Remarque Si aucun module de téléphonie mobile n'existe ou si seulement Ethernet est sélectionné sous Passerelle IP, la centrale signale alors uniquement un message de défaut.</p> <p>Désactivé Fonctions impossibles.</p> <p></p> <p>Remarque Voir également les remarques relatives au serveur ABUS dans le chapitre « Mise à niveau logicielle ».</p>
Port HTTPS externe	Numéro du port externe.
Nom d'utilisateur serveur ABUS	Nom d'utilisateur sur le serveur ABUS  Remarque Entrée GUI : 31 caractères maximum Entrée interface Web : 15 caractères maximum
Mot de passe serveur ABUS	Mot de passe sur le serveur ABUS  Remarque Entrée GUI : 32 caractères maximum Entrée interface Web : 15 caractères maximum

Configuration Mobile IP

Désignation/Fonction	Explication (case à cocher)
	 <p>Remarque L'APN, le nom d'utilisateur et le mot de passe sont des données d'accès à la transmission basée sur IP dans le réseau de téléphonie mobile. Ces données dépendent du fournisseur de réseau et du fournisseur d'accès. Demandez ces données auprès de votre éditeur de cartes SIM. Alternative : ces données sont également souvent enregistrées sur la carte SIM. Introduisez la carte SIM dans un smartphone avant de l'utiliser dans le module de téléphonie mobile. Consultez les données dans le menu Réglages des données.</p>
APN	Saisissez ici le nom du point d'accès « Access Point Name ».
Nom d'utilisateur	Le nom d'utilisateur de l'accès aux données dans le réseau de téléphonie mobile.
Mot de passe	Le mot de passe de l'accès aux données dans le réseau de téléphonie mobile.
Passerelle IP	 <p>Remarque</p>  <p>Danger Les réglages de la passerelle IP concernent uniquement les communications CRA/STS basées sur IP, le transmetteur vocal et l'e-mail. Ethernet continue à être utilisé pour</p>

- L'accès au serveur Web via un navigateur Web
- L'accès à l'application
- Les notifications Push (version logicielle <= v3.01.01)
- Les caméras du réseau local



Remarque



Danger

Si le chemin de transmission « Mobile IP » est utilisé par la centrale, aucune mise à jour n'a lieu sur le serveur ABUS.



Remarque

La centrale obtient une adresse IP publique du réseau Mobile IP du réseau de téléphonie mobile. Les données et informations sont échangées une fois la communication activée via ce chemin.



Remarque

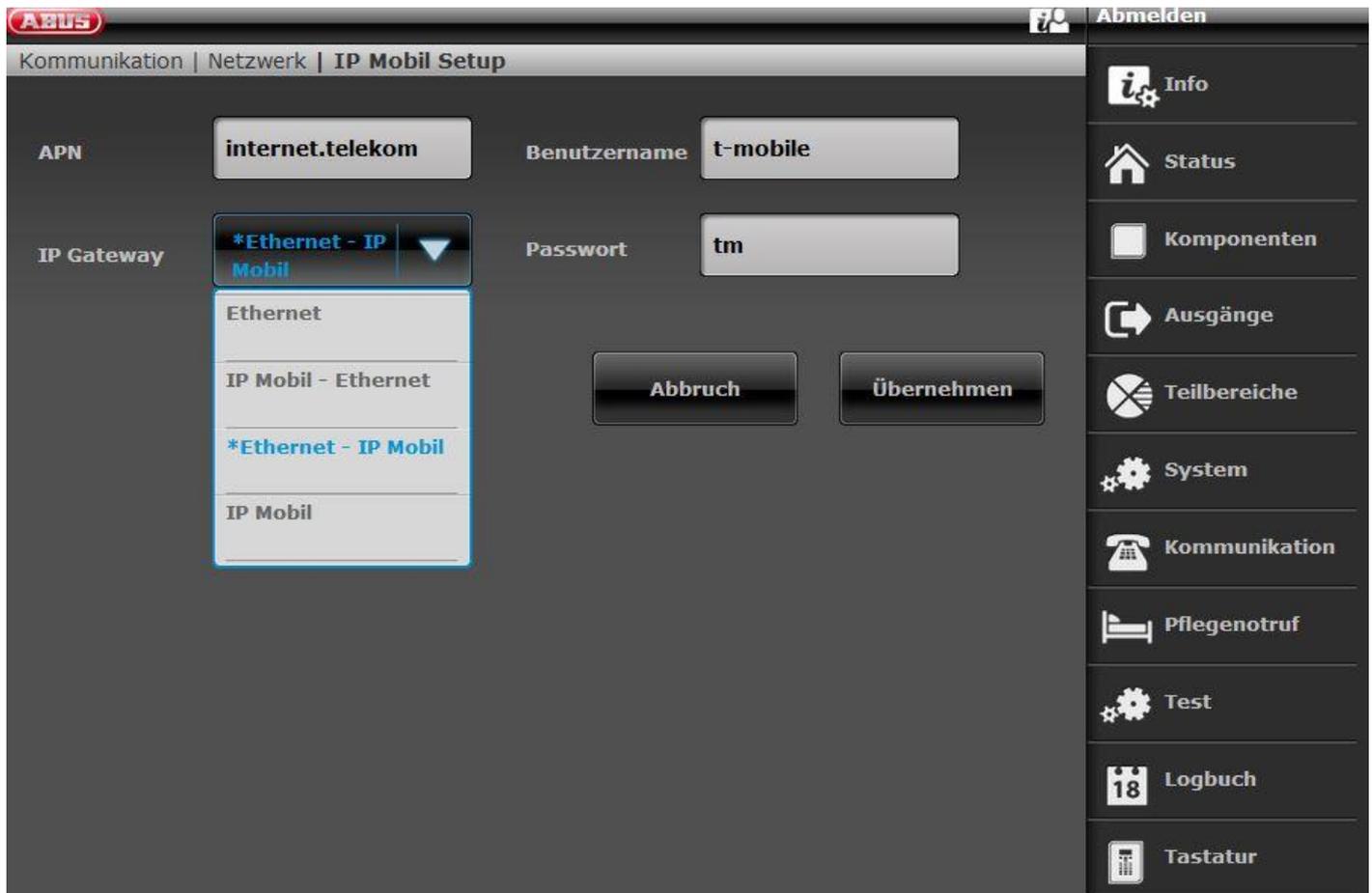
Vous trouverez en annexe quelques données d'accès. En raison des nombreux opérateurs mobiles en Europe et du nombre encore plus important d'éditeurs de cartes SIM (fournisseurs d'accès), vous y trouverez seulement quelques exemples sélectionnés.



Remarque

Version logicielle >= 3.01.16

Tenez également compte des instructions relatives au ping ICMP dans « Serveur ABUS » (Communication -> Réseau -> Configuration de réseau)



Désignation/Fonction	Explication (case à cocher)
Ethernet	<p>Seul Ethernet est utilisé, 4G/2G n'est pas utilisé.</p> <p></p> <p>Remarque Version logicielle >= 3.01.16 Tenez également compte des instructions relatives au ping ICMP dans « Serveur ABUS » (Communication -> Réseau -> Configuration de réseau)</p>
Mobile IP – Ethernet	<p>4G/2G est utilisé en premier. Ethernet est utilisé lorsqu'il n'existe pas de signal 4G/2G.</p> <p></p> <p>Remarque Un défaut 4G/2G doit d'abord avoir été détecté par la centrale.</p> <p></p> <p>Danger Ethernet continue à être utilisé pour</p> <ul style="list-style-type: none"> • L'accès au serveur Web via un navigateur Web • L'accès à l'application • Les notifications Push (version logicielle <= v3.01.01)

- Les caméras du réseau local

Il n'est pas possible d'accéder à la centrale avec l'application via le serveur ABUS et Mobile IP. Il n'est pas possible d'accéder au serveur Web de la centrale via Mobile IP.



Remarque

Notifications Push

La notification Push fonctionne uniquement via le module de téléphonie mobile (Mobile IP), lorsqu'une connexion PPP (Point to Point Protocol, Mobile IP) a déjà été active ou enregistrée pour un autre service (par ex. e-mail).

L'e-mail doit au moins être activé. Il n'est néanmoins pas nécessaire d'envoyer des e-mails. Effectuez la configuration correspondante.

Configuration du serveur ABUS, de l'application et de Push via Ethernet.

Une erreur Mobile IP (par ex. plus d'enregistrement dans un réseau de téléphonie mobile) doit être présente afin que l'empilage IP passe à Ethernet.



Remarque

Version logicielle $\geq 3.01.16$

Tenez également compte des instructions relatives au ping ICMP dans « Serveur ABUS » (Communication -> Réseau -> Configuration de réseau)

Ethernet – Mobile IP

Ethernet est utilisé en premier. 4G/2G est utilisé en cas de défaut Ethernet.

Ce réglage est recommandé pour effectuer une voie de transmission redondante basée sur IP pour le reporting CRA/STS, l'e-mail et Push.



Remarque

Un défaut Ethernet doit d'abord avoir été détecté par la centrale.



Remarque

Version logicielle $\geq 3.01.16$

Tenez également compte des instructions relatives au ping ICMP dans « Serveur ABUS » (Communication -> Réseau -> Configuration de réseau)



Danger

Ethernet continue à être utilisé pour

- L'accès au serveur Web via un navigateur Web
- L'accès à l'application
- Les notifications Push (version logicielle $\leq v3.01.01$)
- Les caméras du réseau local

Il n'est pas possible d'accéder à la centrale avec l'application via le serveur ABUS et Mobile IP. Il n'est pas possible d'accéder au serveur Web de la centrale via Mobile IP.



	<p>Remarque Notifications Push La notification Push fonctionne uniquement via le module de téléphonie mobile (Mobile IP), lorsqu'une connexion PPP (Point to Point Protocol, Mobile IP) a déjà été active ou enregistrée pour un autre service (par ex. e-mail). L'e-mail doit au moins être activé. Il n'est néanmoins pas nécessaire d'envoyer des e-mails. Effectuez la configuration correspondante. Configuration du serveur ABUS, de l'application et de Push via Ethernet. Une erreur Ethernet doit être présente afin que l'empilage IP passe à Mobile IP.</p>
<p>Mobile IP</p>	<p>Seul 4G/2G est utilisé, Ethernet n'est pas utilisé.</p> <p> Remarque</p> <p> Danger Ethernet continue à être utilisé pour</p> <ul style="list-style-type: none"> • L'accès au serveur Web via un navigateur Web • L'accès à l'application • Les notifications Push (version logicielle <= v3.01.01) • Les caméras du réseau local <p>Il n'est pas possible d'accéder à la centrale avec l'application via le serveur ABUS et Mobile IP. Il n'est pas possible d'accéder au serveur Web de la centrale via Mobile IP.</p> <p> Remarque Notifications Push La notification Push fonctionne uniquement via le module de téléphonie mobile (Mobile IP), lorsqu'une connexion PPP (Point to Point Protocol, Mobile IP) a déjà été active ou enregistrée pour un autre service (par ex. e-mail). L'e-mail doit au moins être activé. Il n'est néanmoins pas nécessaire d'envoyer des e-mails. Effectuez la configuration correspondante. Configuration du serveur ABUS, de l'application et de Push via Ethernet.</p> <p> Remarque Version logicielle >= 3.01.16 La centrale d'alarme envoie toutes les 30 minutes un ping ICMP au serveur ABUS. Cela s'effectue uniquement via Ethernet, pas via Mobile IP. Pour plus de détails, consultez les instructions relatives au ping ICMP dans « Serveur ABUS » (Communication -> Réseau -> Configuration de réseau) Dans cette constellation, il est judicieux de régler le serveur ABUS sur Désactivé, afin d'éviter des dysfonctionnements. Avec le réglage Mobile IP, il n'est pas possible d'accéder à la centrale avec l'application via le serveur ABUS.</p>

Paramétrage E-mail

ABUS
Logout

Transmissions | Réseau | **Paramétrage E-mail**

Nom Serveur

Compte

Mot de Passe

Numéro port IP

Nom Utilisateur

SSL

INFO

État

Périphériques

Sorties

Partitions

Système

Transmissions

Appel Soins de Santé

Test

Journal de bord

Clavier

Désignation/Fonction	Explication (case à cocher)	Nombre max. de caractères
Nom serveur	Nom du serveur SMTP du fournisseur de messagerie électronique.	32
Numéro port IP	Numéro du port IP.	5
Compte	Nom du compte de messagerie électronique (en principe l'adresse e-mail)	90
Nom d'utilisateur	Nom d'utilisateur (selon le fournisseur, il s'agit de l'adresse e-mail complète ou d'un nom d'utilisateur spécifique).	90
Mot de passe	Mot de passe du compte de messagerie électronique.	32
	Remarque Veillez à respecter la casse !	
SSL	Activé Une connexion cryptée (SSL) est établie avec le fournisseur. Désactivé Une connexion non cryptée (SSL) est établie avec le fournisseur.	-

Vous trouverez en annexe les réglages recommandés et testés.

Dans la FAQ du fournisseur de messagerie électronique sélectionné, vous trouverez des informations complètes sur les paramètres utilisés.



Remarque

La centrale n'envoie pas d'informations. Une connexion est établie seulement lors de l'envoi concret de l'e-mail, tout d'abord avec le handshaking. Les informations sont alors envoyées selon les réglages (par ex. cryptées ou non cryptées), ainsi que les textes et événements programmés.

Setup Transmission VoIP

ABUS
Logout

Transmissions | Réseau | **Setup Transmission VoIP**

Nom domaine SIP

Proxy SIP

ID Utilisateur SIP

Mot de passe Utilisateur SIP

SIP Port

RTP Port

ID utilisateur appel test SIP

Transmission SIP autorisé

RFC 2833 Détection DTMF

INFO

État

Périphériques

Sorties

Partitions

Système

Transmissions

Appel Soins de Santé

Test

Journal de bord

Clavier

Désignation/Fonction	Explication (case à cocher)	Nombre max. de caractères
Nom domaine SIP	Nom du serveur SIP du fournisseur de services SIP propre. Par ex. sipgate.de	50
Proxy SIP	Proxy du fournisseur de services SIP propre Par ex. sipgate.de	50
ID utilisateur ID	L'ID utilisateur du fournisseur de services SIP pour votre compte.	50
Mot de passe utilisateur SIP	Mot de passe de l'utilisateur SIP du fournisseur de services SIP pour votre compte.	50
SIP port	Port du fournisseur de services SIP pour votre compte. Par défaut : 5060	5
Port RTP	Numéro du port RTP du fournisseur de services SIP pour votre compte.	5
ID utilisateur appel test SIP	ID utilisateur de la destination de l'appel test via SIP Format Version logicielle >=2.00.00 Numéro de téléphone +4982071234567 ID lorsque la destination a un compte auprès du même fournisseur de services SIP 9876543 Version logicielle <2.00.00 Numéro de téléphone +4982071234567@sipgate.de	50

	<p>sipgate.de est le fournisseur de services SIP propre, comme Nom serveur SIP</p> <p>ID lorsque la destination a un compte auprès du même fournisseur de services SIP</p> <p>9876543@sipgate.de</p>	
Transmission SIP autorisée	<p>Activé</p> <p>Le sélecteur SIP est autorisé.</p> <p></p> <p>Remarque</p> <p>La centrale n'envoie pas d'informations. Une connexion est établie seulement lors de l'appel concret, tout d'abord avec le handshaking. Les informations sont alors envoyées selon les réglages ainsi que les annonces vocales enregistrées relatives aux événements.</p> <p>Désactivé</p>	-
RFC 2833 détection DTMF	<p>Activé</p> <p>Les tonalités DTMF sont détectées avec SIP sous certaines conditions.</p> <p>Désactivé</p> <p>Pas de détection des tonalités DTMF.</p>	-



Remarque

La centrale d'alarme traite les différents types de communications dans l'ordre suivant.

1. AES/TS Reporting
2. E-mail
3. Appel Soins de santé (transmission de protocole)
4. SMS via GSM
5. Transmetteur vocal
6. SMS via RTC

La notification Push est indépendante de cette séquence et peut survenir à tout moment.

TS Reporting

ABUS
Logout

Transmissions | **TS Reporting**

Mode d'appel *Bloqué ▼

Protocole *Format rap. ▼

ID Client

Canaux FF

Plus...

Destinataire Tél. 1 Keine

Destinataire Tél. 2 Keine

Destinataire IP1 Keine Port 1792

Destinataire IP2 Keine Port 2750

Annuler
Envoyer

INFO

État

Périphériques

Sorties

Partitions

Système

Transmissions

Appel Soins de Santé

Journal de bord

Clavier

Version logicielle >=3.00.03

Désignation/Fonction	Explication (case à cocher)
Mode appel	<p>Liste déroulante de sélection :</p> <ul style="list-style-type: none"> • Bloqué • Simple • Alternatif <p></p> <p>Remarque La centrale n'envoie pas d'informations. Une connexion est établie seulement lors du reporting STS concret, tout d'abord avec le handshaking. Les informations sont alors envoyées selon les réglages (par ex. cryptées ou non cryptées).</p>
Protocole	<p>Liste déroulante de sélection :</p> <ul style="list-style-type: none"> • Format rapide • Contact ID • SIA 1 • SIA 2 • SC SIA 3 • Ex SIA 3

- Ex SIA 3 v2
- Ex SIA 3 v3
- Contact ID en SMS



Remarque

Vous trouverez une description détaillée des formats de protocole dans l'annexe « Formats de protocole AES (TS) Reporting »

TS Reporting, répertoire tél.

ABUS
Logout

Transmissions | **TS Reporting**

Mode d'appel *Bloqué ▼

Protocole *Format rap. ▼

Répertoire tél.

ID Client

Canaux FF

Plus...

Destinataire Tél. 1	<input style="width: 95%;" type="text" value="Keine"/>		
Destinataire Tél. 2	<input style="width: 95%;" type="text" value="Keine"/>		
Destinataire IP1	<input style="width: 95%;" type="text" value="Keine"/>	Port	<input style="width: 40px;" type="text" value="1792"/>
Destinataire IP2	<input style="width: 95%;" type="text" value="Keine"/>	Port	<input style="width: 40px;" type="text" value="2750"/>

Annuler

Envoyer

INFO
 État

Périphériques
 Sorties

Partitions
 Système

Transmissions
 Appel Soins de Santé

18 Journal de bord
 Clavier

Désignation/Fonction	Explication (case à cocher)
Tél. destinataire #	Lorsque vous cliquez sur ce champ, les destinataires créés dans le répertoire téléphonique (contacts) apparaissent. Sélectionnez un destinataire avec le numéro de téléphone correspondant.
Destinataire IP #	Lorsque vous cliquez sur ce champ, les destinataires créés dans le répertoire téléphonique (contacts) apparaissent. Sélectionnez un destinataire avec l'adresse IP correspondante.
Port	À droite, à côté des destinataires IP, indiquez le numéro de port que l'AES/TS vous a donné pour cette adresse IP.



Remarque

Version logicielle >= 3.01.11

Si la centrale n'a pas pu atteindre le destinataire correspondant à la première tentative d'appel, la centrale essaye 3 fois au maximum d'atteindre le destinataire correspondant.

Version logicielle < 3.01.11

La centrale essaie 16 fois au maximum d'atteindre le destinataire correspondant.



Remarque

Les contacts / destinataires utilisés pour la connexion à la station de contrôle ne sont plus « visibles » dans le répertoire téléphonique du menu utilisateur. Pour des raisons de conformité avec la norme EN 50131, les utilisateurs de niveau 2 (niveau d'accès 2) n'ont pas le droit de modifier la connexion à la station de contrôle.

TS Reporting, ID client

ABUS Logout

Transmissions | TS Reporting

Mode d'appel: ***Bloqué** | Protocole: ***Format rap.**

Répertoire tél. | **ID Client** | Canaux FF | Plus...

ID Client PART1: 000000 | ID Client PART2: 000000
 ID Client PART3: 000000 | ID Client PART4: 000000

Annuler | Envoyer

- INFO
- État
- Périphériques
- Sorties
- Partitions
- Système
- Transmissions
- Appel Soins de Santé
- Journal de bord
- Clavier

Désignation/Fonction	Explication (case à cocher)
ID client part#	<p>Champ de saisie d'un ID client jusqu'à 6 chiffres pour la partition correspondante. CID utilise des ID client à 4 chiffres</p> <p>Avec Format rapide, vous pouvez utiliser des ID client à 4, 5 ou 6 chiffres. La centrale ajoute un zéro au début pour convertir les ID client à 5 chiffres en codes à 6 chiffres.</p> <p>La centrale ne modifie pas les ID client à 4 et 6 chiffres.</p>

TS Reporting, canaux FF (uniquement avec le protocole "Format rap.")

Désignation/Fonction	Explication (case à cocher)	
Canal 1 à 8	Liste déroulante de sélection : <ul style="list-style-type: none"> • Non utilisé • Alarme intrusion • Conf. Alarme intrusion • Alarme Intrusion TB1 • Alarme Intrusion TB2 • Alarme Intrusion TB3 • Alarme Intrusion TB4 • Alarme anti-agression • Confirmer alarme agression • Code contrainte • Alarme confirmée • Incendie • Technique • Alarme annulation • Alarme médicale • Boîtier clé • Sabotage • RF Supervision • RF Brouillage • RF Pile faible • Défaut secteur • Défaut général • Début/Fin • Début • Fin • Zones isolées (lors arm.) • Zones isolées (système) 	
Programmation Usine	Canal 1 Canal 2 Canal 3 Canal 4 Canal 5 Canal 6 Canal 7 Canal 8	Incendie Alarme anti-agression Alarme intrusion Début/Fin Zones isolées (lors arm.) Sabotage Alarme confirmée Défaut général

TS Reporting, événements CID/SIA (avec tous les protocoles SAUF "Format rap.")

The screenshot shows the ABUS configuration interface. At the top, there's a header with 'ABUS' and 'Logout'. Below that, a navigation bar shows 'Transmissions | TS Reporting'. The main configuration area has two dropdown menus: 'Mode d'appel' set to '*Bloqué' and 'Protocole' set to 'Contact ID'. Below these are four buttons: 'Répertoire tél.', 'ID Client', 'Événements CID/SIA' (highlighted in blue), and 'Plus...'. The main content area contains a grid of alarm types with checkboxes:

- Alarme Feu:
- Alarme Médicale:
- Technique:
- Armement/Désarmement:
- Alarme Agression:
- Alarme Intrusion:
- Sabotages:
- Act. interne:

At the bottom of the configuration area are two buttons: 'Annuler' and 'Envoyer'. The right sidebar contains a vertical list of menu items with icons: INFO, État, Périphériques, Sorties, Partitions, Système, Transmissions, Appel Soins de Santé, Journal de bord, and Clavier.

Désignation/Fonction	Explication (case à cocher)
Incendie	Activé
Alarme Alarme	Les événements de ce groupe sont transmis au CRA ou à la STS.
Technique	
Armement/Désarmement	Désactivé
Remise à zéro	Aucun événement de ce groupe n'est transmis au CRA ou à la STS.
Exclusion	
RF Supervision	
Batt.Rad. /PSU	
Défaut secteur	
Mode installateur	
RAZ heure/date	
Alarme anti-agression	
Alarme intrusion	
Sabotages	
Act. interne	
Sortie timeout	
Boîtier clé	
RF Brouillage	
Batt. centrale	

Anomalies

Code util. changé

Supervision caméra

Cryptage

À partir de la version logicielle v3.00.03, la transmission des messages peut également être envoyée au CRA ou à la STS avec cryptage.



Remarque

Les règles du document suivant s'appliquent ici.

ANSI/SIA DC-09-2013 : Internet Protocol Event Reporting
SIA Digital Communication Standard – Internet Protocol
Event Reporting

Vous trouverez des détails à ce sujet dans le chapitre Reporting CRA/STS en annexe.



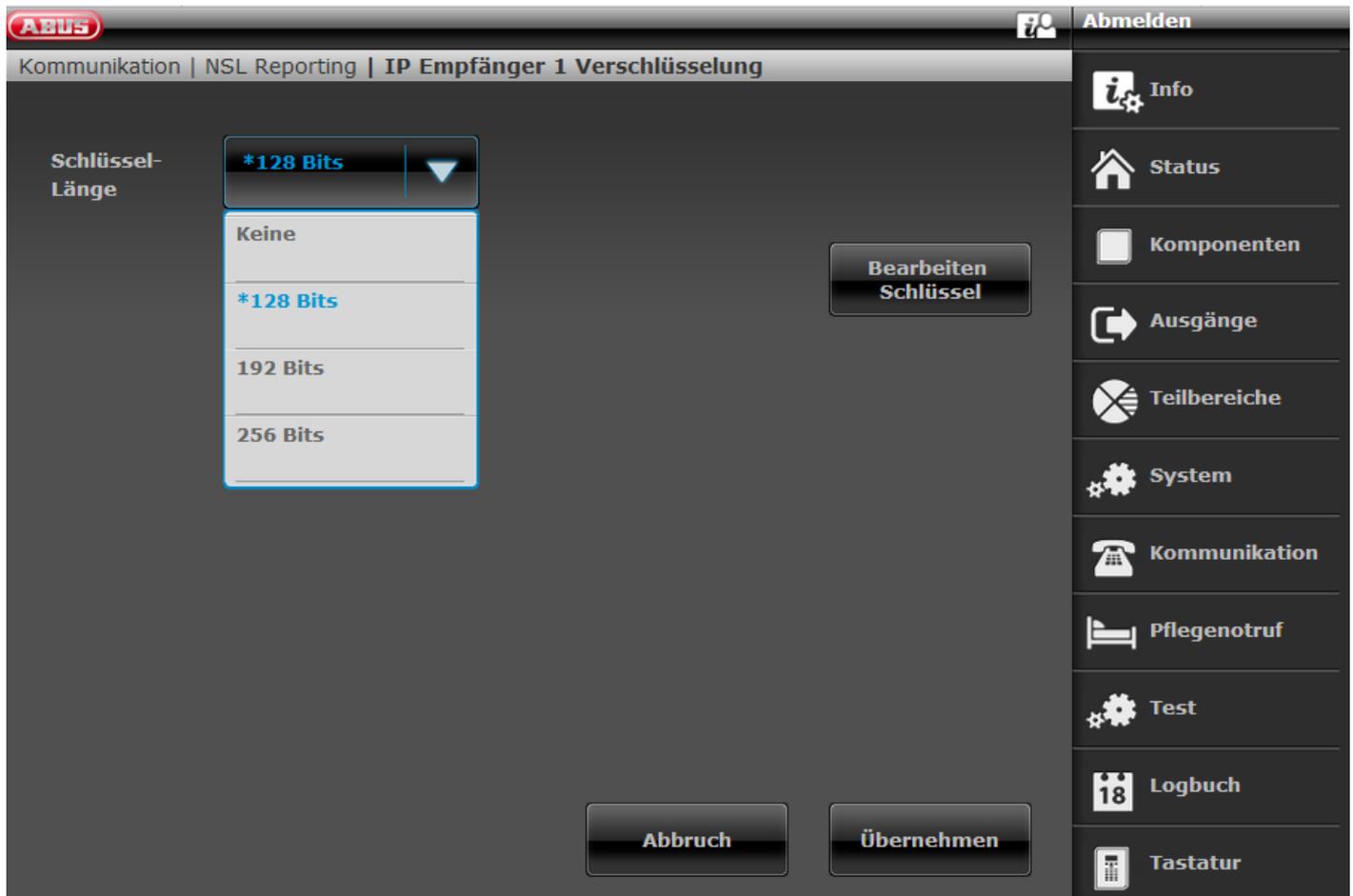
Danger

Veillez noter que l'heure de la centrale d'alarme doit bien être réglée afin que l'autorisation fonctionne correctement. Il est pour ce faire recommandé de procéder au réglage de l'heure via un serveur SNTP.

Cliquez sur le destinataire IP souhaité.

Index	Name
IP Empfänger 1	"AES TS"
IP Empfänger 2	"Keine"

Sélectionnez la longueur de clé souhaitée.



Cliquez sur « Modifier la clé » pour saisir la clé.

Désignation/Fonction	Explication (case à cocher)
Longueur de codage	Aucune
Longueur de la clé	128 bits 192 bits 256 bits
Aucune	La notification est envoyée sans cryptage.

128 bits



Remarque

Pour définir la clé, saisissez ici 32 caractères hexadécimaux.

Les caractères hexadécimaux comprennent les chiffres 0-9 et les lettres a-f.

Schlüssel:

0123

- 4567

- 89ab

- cdef -

fedc

- ba98

- 7654

- 3210

Übernehmen

Abbruch

192 bits



Remarque

Pour définir la clé, saisissez ici 48 caractères hexadécimaux.

Les caractères hexadécimaux comprennent les chiffres 0-9 et les lettres a-f.

Schlüssel:

0123	-	4567	-	89ab	-	cdef	-
fedc	-	ba98	-	7654	-	3210	-
0000	-	0000	-	0000	-	0000	-

Übernehmen

Abbruch

256 bits



Remarque

Pour définir la clé, saisissez ici 64 caractères hexadécimaux.

Les caractères hexadécimaux comprennent les chiffres 0-9 et les lettres a-f.

Schlüssel:

0123	-	4567	-	89ab	-	cdef	-
fedc	-	ba98	-	7654	-	3210	-
0000	-	0000	-	0000	-	0000	-
0000	-	0000	-	0000	-	0000	-

Übernehmen

Abbruch

Sur la **centrale d'alarme**, vous trouverez sur les réglages de cryptage sous :

Mode installateur -> Communication -> NSL Reporting -> Destinataire IP 1/2

Destinataire

Numéro port IP

Longueur de la clé

Aucune

128 bits

192 bits

256 bits

Clé



Remarque

Cette rubrique ne s'affiche **pas** si « Aucune » a été sélectionné pour la longueur de clé.

La longueur de clé 128 bits a été sélectionnée.

0000 0000 0000 0000

0000 0000 0000 0000



Remarque

Pour définir la clé, saisissez ici 32 caractères hexadécimaux.

Les caractères hexadécimaux comprennent les chiffres 0-9 et les lettres a-f.

La longueur de clé 192 bits a été sélectionnée.

0000 0000 0000 0000

0000 0000 0000 0000

0000 0000 0000 0000



Remarque

Pour définir la clé, saisissez ici 48 caractères hexadécimaux.

Les caractères hexadécimaux comprennent les chiffres 0-9 et les lettres a-f.

La longueur de clé 256 bits a été sélectionnée.

0000 0000 0000 0000

0000 0000 0000 0000

0000 0000 0000 0000

0000 0000 0000 0000



Remarque

Pour définir la clé, saisissez ici 64 caractères hexadécimaux.

Les caractères hexadécimaux comprennent les chiffres 0-9 et les lettres a-f.

TS Reporting, plus

ABUS Logout

Transmissions | TS Reporting

Mode d'appel: ***Bloqué** | Protocole: ***Format rap.**

Répertoire tél. | ID Client | Canaux FF | **Plus...**

Restaurations Réarm. Transm. Intrusion

21CN Temps Acquis: ***800ms** Appel de test dyn.

Transm. Désarm. Priorité Transm.

Annuler Envoyer

INFO

État

Périphériques

Sorties

Partitions

Système

Transmissions

Appel Soins de Santé

18 Journal de bord

Clavier

Désignation/Fonction	Explication (case à cocher)
Restaurations	<p>Si un événement entraîne une notification de la STS, deux informations sont transmises à la STS :</p> <ul style="list-style-type: none"> • le type et l'heure/la date de l'événement déclencheur • la réinitialisation de l'événement <p>la réinitialisation de l'événement est une "restauration".</p> <p>Activé Les informations sur la réinitialisation d'un événement (restauration) sont transmises à la STS.</p> <p>Désactivé Les informations sur la réinitialisation d'un événement (restauration) ne sont pas transmises à la STS.</p>
21CN temps acquis	<p>Une liaison téléphonique analogique avec la STS, établie via les nouveaux réseaux téléphoniques publics, peut exiger pour la transmission avec confirmation via le protocole Format rapide, plus de temps qu'une liaison téléphonique analogique classique.</p> <p>Cette option permet de régler le temps d'attente de la confirmation.</p> <p>Liste déroulante de sélection :</p> <ul style="list-style-type: none"> • 400 ms • 500 ms • 600 ms • 700 ms • 800 ms • 900 ms • 1 000 ms • 1 100 ms • 1 200 ms

Désignation/Fonction	Explication (case à cocher)
Transm. désarmée	<p>Activé La centrale d'alarme transmet tous les messages d'état à la STS, que la centrale soit activée ou désactivée.</p> <p>Désactivé La centrale d'alarme transmet les sabotages, panne secteur et les autres messages d'état à la STS en cas d'activation. En cas de désactivation, les messages d'état ne sont pas transmis à la STS.</p>
Réarm. Transm. Intrusion	<p>S'affiche uniquement si « Système → Confirmation → Mode confirm. = Basique » et « Protocole → transmission = Format rap. »)</p> <p>Activé</p> <ul style="list-style-type: none"> • La centrale d'alarme réactive le canal 3 dès que la durée sirène s'est écoulée. Après réactivation du canal 3, un événement peut être à nouveau transmis dès qu'il est déclenché. Le système isole automatiquement les zones déclenchées. • Remarque : Si une zone entrée/sortie est déclenchée, le canal 3 est activé à la fin du temps entrée/sortie programmé. <p>Désactivé Le canal 3 reste actif jusqu'à ce qu'un utilisateur ou un installateur remette à zéro la centrale.</p>
Appel de stat.	<p>Activé L'appel de test dynamique est activé. L'appel de test est démarré toutes les 24 heures suivant la dernière transmission.</p> <p></p> <p>Remarque L'avantage de l'appel de test dynamique est qu'une transmission test vers la station de contrôle est réalisée uniquement lorsqu'aucune transmission n'a eu lieu au sein des 24 dernières heures. Si vous avez programmé une transmission activé/désactivé, il peut arriver qu'aucune transmission test n'ait lieu pendant plusieurs jours, lorsque la centrale est activée ou désactivée une fois par jour.</p> <p>Désactivé L'appel de test dynamique est désactivé. La liste déroulante "Appel test stat." s'affiche.</p>
Priorité transmission	<p>Définissez ici dans quel ordre sont utilisées les voies de transmission.</p> <ul style="list-style-type: none"> • Ethernet/Mobile 1, 2, 3 ou Non IP • RTC 1, 2, 3 ou Non • GSM/Mobile 1, 2, 3 ou Non <p>Remarque : Le protocole DC-09 basé sur IP est automatiquement utilisé par la centrale lorsque cette dernière utilise le standard Ethernet (LAN) pour la communication sortante. Ce faisant, les données des protocoles classiques sont regroupées en paquets IP et transmises. L'annexe « Protocoles AES / TS Reporting »</p> <p>Version logicielle >= 3.00.05 Définissez ici dans quel ordre sont utilisées les voies de transmission.</p> <ul style="list-style-type: none"> • Ethernet/Mobile 1, 2, 3 ou Non IP <p></p>

	<p>Remarque Signifie transmission de données selon le réglage de la passerelle IP dans le menu « Configuration Mobile IP »</p> <p> Remarque Version logicielle >= 3.01.16 Tenez également compte des instructions relatives au ping ICMP dans « Serveur ABUS » (Communication -> Réseau -> Configuration de réseau)</p> <ul style="list-style-type: none">• RTC 1, 2, 3 ou Non• Mobile 1, 2, 3 ou Non <p> Remarque Signifie transmission de la voix classique (également DTMF et FSK) ou transmission de SMS via un réseau de téléphonie mobile.</p> <p> Remarque L'affichage varie selon le réglage de la passerelle IP dans le menu « Configuration Mobile IP ».</p>
<p>Appel de test stat. Uniquement désactivé avec "Appel de test dyn".</p>	<p>Liste déroulante de sélection :</p> <ul style="list-style-type: none">• Bloqué• Journalier• Hebdomadaire• Mensuel <p> Remarque Pour chacun des trois types d'appel, journalier, hebdomadaire et mensuel, la centrale ajoute une valeur en minutes basée sur le hasard. Cette valeur en minutes est comprise entre 0 et 16. L'appel peut donc avoir lieu jusqu'à 16 minutes après l'heure que vous avez indiquée. Cela permet de garantir que l'AES (TS) ne soit pas surchargé par une marée d'appels de test de systèmes, qui ont tous obtenu la même heure.</p>
<p>RÉGLER HEURE Uniquement avec "Appel test stat."</p> <ul style="list-style-type: none">• Journalier• Hebdomadaire• Mensuel	<p>Champ de saisie de l'heure de l'appel test journalier (hh:mm)</p> <p> Remarque Seules des heures entières sont possibles.</p>

Désignation/Fonction	Explication (case à cocher)
<p>RÉGLER JOUR Uniquement avec "Appel test stat." • Hebdomadaire</p>	<p>Liste déroulante de sélection :</p> <ul style="list-style-type: none"> • Dimanche • Lundi • Mardi • Mercredi • Jeudi • Vendredi • Samedi
<p>RÉGLER JOUR Uniquement avec "Appel test stat." • Mensuel</p>	<p>Champ de saisie du jour du mois où doit être effectué l'appel test (1 - 31)</p>

Appel d'urgence de soin
Logout

Transmissions | Appel Soins de Santé

Mode d'appel: *Bloqué ▼

Priorité Transm.: ➔

21CN Temps Acquis: *800ms ▼

Protocole: *Scancom ▼

Acquit d'appel:

Répertoire tél.
ID Client

Destinataire Tél. 1: Keine

Destinataire Tél. 2: Keine

Annuler
Envoyer

Logout

INFO

État

Périphériques

Sorties

Partitions

Système

Transmissions

Appel Soins de Santé

18 Journal de bord

Clavier

Désignation/Fonction	Explication (case à cocher)
Mode appel	<p>Liste déroulante de sélection :</p> <ul style="list-style-type: none"> • Bloqué • Simple • Alternatif <p></p> <p>Remarque La centrale n'envoie pas d'informations. Une connexion est établie seulement lors de l'envoi de l'appel d'urgence de soin concret, tout d'abord avec le handshaking. Les informations sont alors envoyées selon les réglages.</p>
Protocole	<p>Liste déroulante de sélection :</p> <ul style="list-style-type: none"> • Scancom • Scanfast • Tunstall
Priorité transmission	<p>Version logicielle < 3.00.05</p> <p>Définissez ici dans quel ordre sont utilisées les voies de transmission :</p> <ul style="list-style-type: none"> • RTC 1, 2 ou Non • GSM/Mobile 1, 2 ou Non

	<p>Version logicielle >= 3.00.05 Définissez ici dans quel ordre sont utilisées les voies de transmission.</p> <ul style="list-style-type: none"> • RTC 1, 2, 3 ou Non • Mobile 1, 2, 3 ou Non <p style="text-align: center;"></p> <p>Remarque Signifie transmission de la voix classique (également DTMF et FSK) via un réseau de téléphonie mobile.</p> <p></p> <p>Remarque L'affichage varie selon le réglage de la passerelle IP dans le menu « Configuration Mobile IP ».</p>
<p>21CN temps acquis</p>	<p>Une liaison téléphonique analogique avec la STS, établie via les nouveaux réseaux téléphoniques publics, peut exiger pour la transmission avec confirmation via le protocole Format rapide, plus de temps qu'une liaison téléphonique analogique classique.</p> <p>Cette option permet de régler le temps d'attente de la confirmation.</p> <p>Liste déroulante de sélection :</p> <ul style="list-style-type: none"> • 400 ms • 500 ms • 600 ms • 700 ms • 800 ms • 900 ms • 1 000 ms • 1 100 ms • 1 200 ms
<p>Acquit d'appel</p>	<p>Activé La transmission d'alarme de l'appel soins de santé doit être confirmée par le destinataire en appuyant sur la touche DTMF "5" ; à défaut les appels sont répétés.</p> <p>Désactivé Si la fonction est désactivée, l'appel d'urgence est considéré comme transmis lorsque la ligne appelée est décrochée.</p>

Appel soins de santé, répertoire tél.

ABUS Logout

Transmissions | Appel Soins de Santé

Mode d'appel: *Bloqué | Protocole: *Scancom

Priorité Transm.: [→] Acquit d'appel: [✓]

21CN Temps Acquis: *800ms

Répertoire tél. | ID Client

Destinataire Tél. 1: Keine

Destinataire Tél. 2: Keine

Annuler | Envoyer

Logout

INFO

État

Périphériques

Sorties

Partitions

Système

Transmissions

Appel Soins de Santé

Journal de bord

Clavier

Désignation/Fonction	Explication (case à cocher)
Tél. destinataires 1 à 2	Après avoir cliqué sur le champ de sélection, une fenêtre contextuelle s'ouvre dans laquelle le numéro de téléphone du destinataire peut être sélectionné parmi les contacts.



Remarque

Version logicielle >= 3.01.11

Si la centrale n'a pas pu atteindre le destinataire correspondant à la première tentative d'appel, la centrale essaye 3 fois au maximum d'atteindre le destinataire correspondant.

Version logicielle < 3.01.11

La centrale essaie 16 fois au maximum d'atteindre le destinataire correspondant.

Appel soins de santé, ID client

Désignation/Fonction	Explication (case à cocher)
ID client part#	<p>Enregistrement d'un ID client jusqu'à 8 chiffres (configuration par défaut = 00000000) pour la connexion à un centre d'appels soins de santé ou une station de contrôle pour la partition correspondante.</p> <p>Lors d'un appel soins de santé, l'ID client peut avoir jusqu'à 8 chiffres. Pour les types de protocole Scancom ou Scanfast, la centrale utilise les 4 à 6 derniers chiffres de l'ID client enregistré.</p> <p>Si vous saisissez 4 chiffres, la centrale utilise uniquement ces 4 chiffres. Si vous saisissez 5 chiffres, la centrale ajoute un zéro au début pour augmenter le nombre de chiffres à 6.</p> <p>Pour le type de protocole Tunstall, la centrale ajoute des zéros au début pour rallonger les ID client plus courts à 8 chiffres.</p>

Transmetteur vocal

ABUS Logout

Transmissions | Transmetteur Vocal

Autorisé Acquit d'appel

Priorité Transm.

Événement

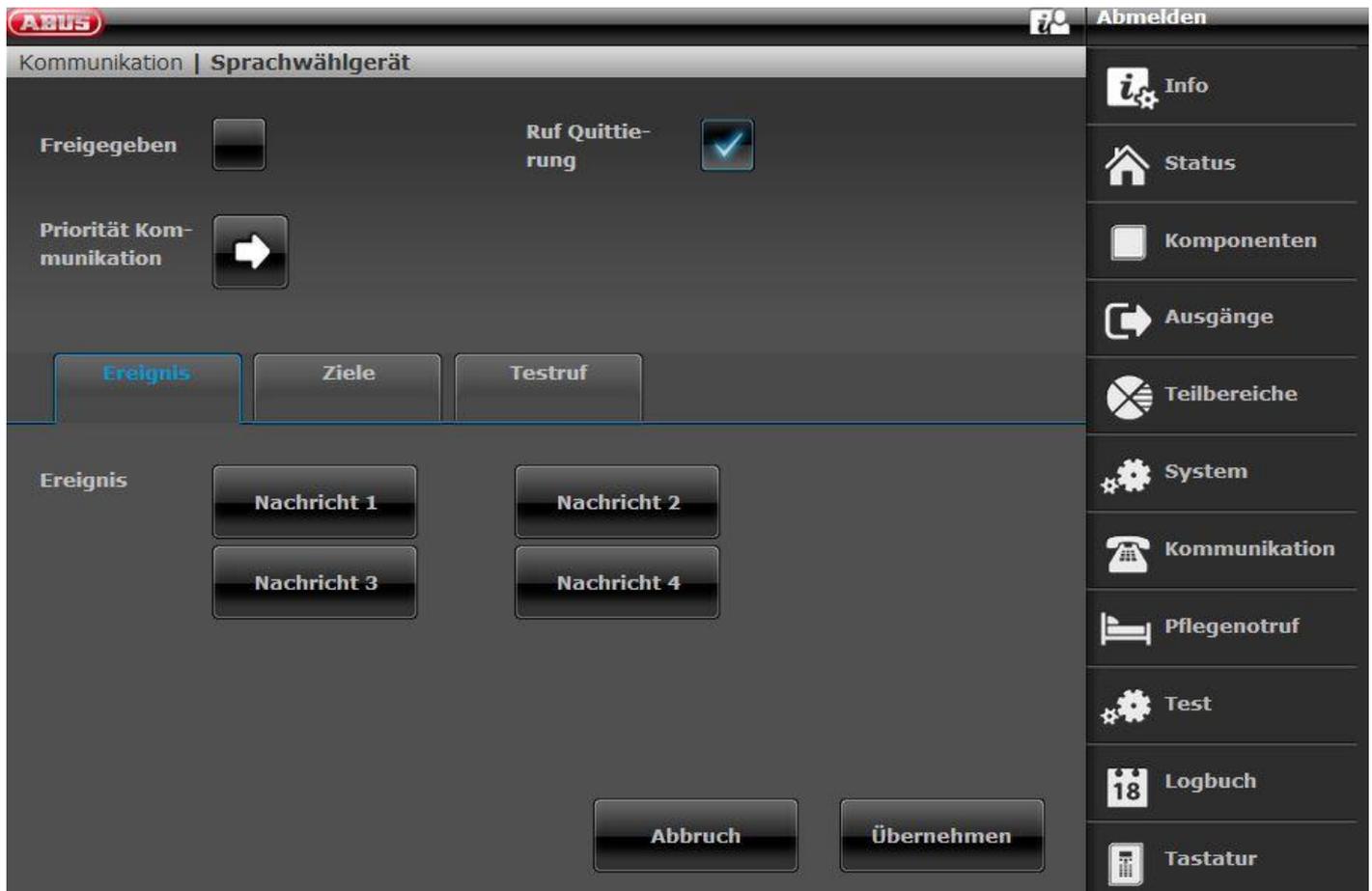
<input type="button" value="Message 1"/>	<input type="button" value="Message 2"/>
<input type="button" value="Message 3"/>	<input type="button" value="Message 4"/>

Destinations

<input type="button" value="Message 1"/>	<input type="button" value="Message 2"/>
<input type="button" value="Message 3"/>	<input type="button" value="Message 4"/>

-
-
-
-
-
-
-
-
-
-

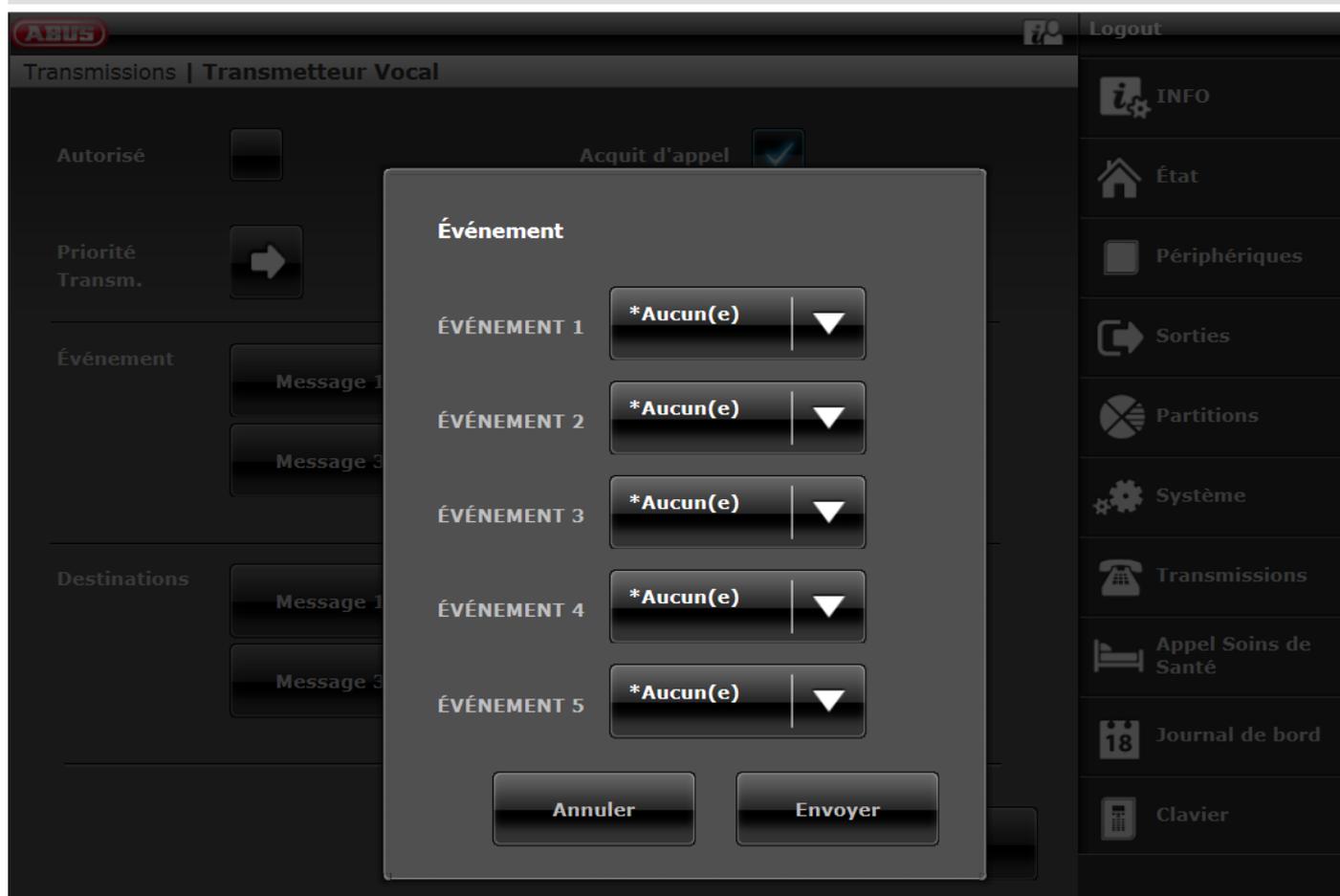
Version logicielle >= 3.00.05



Désignation/Fonction	Explication (case à cocher)
Autorisé	<p>Activé La fonction de transmetteur vocal est disponible.</p> <p>Désactivé La fonction de transmetteur vocal n'est pas disponible.</p> <p></p> <p>Remarque La centrale n'envoie pas d'informations. Une connexion est établie seulement lors de l'appel concret, tout d'abord avec le handshaking. Les informations sont alors envoyées selon les réglages ainsi que les annonces vocales enregistrées relatives aux événements.</p>
Priorité transmission	<p>Définissez ici dans quel ordre sont utilisées les voies de transmission.</p> <ul style="list-style-type: none"> • Ethernet 1, 2, 3 ou Non • RTC 1, 2, 3 ou Non • GSM/Mobile 1, 2, 3 ou Non <p>Version logicielle >= 3.00.05</p> <p>Définissez ici dans quel ordre sont utilisées les voies de transmission.</p> <ul style="list-style-type: none"> • Ethernet 1, 2, 3 ou Non • RTC 1, 2, 3 ou Non • Mobile 1, 2, 3 ou Non

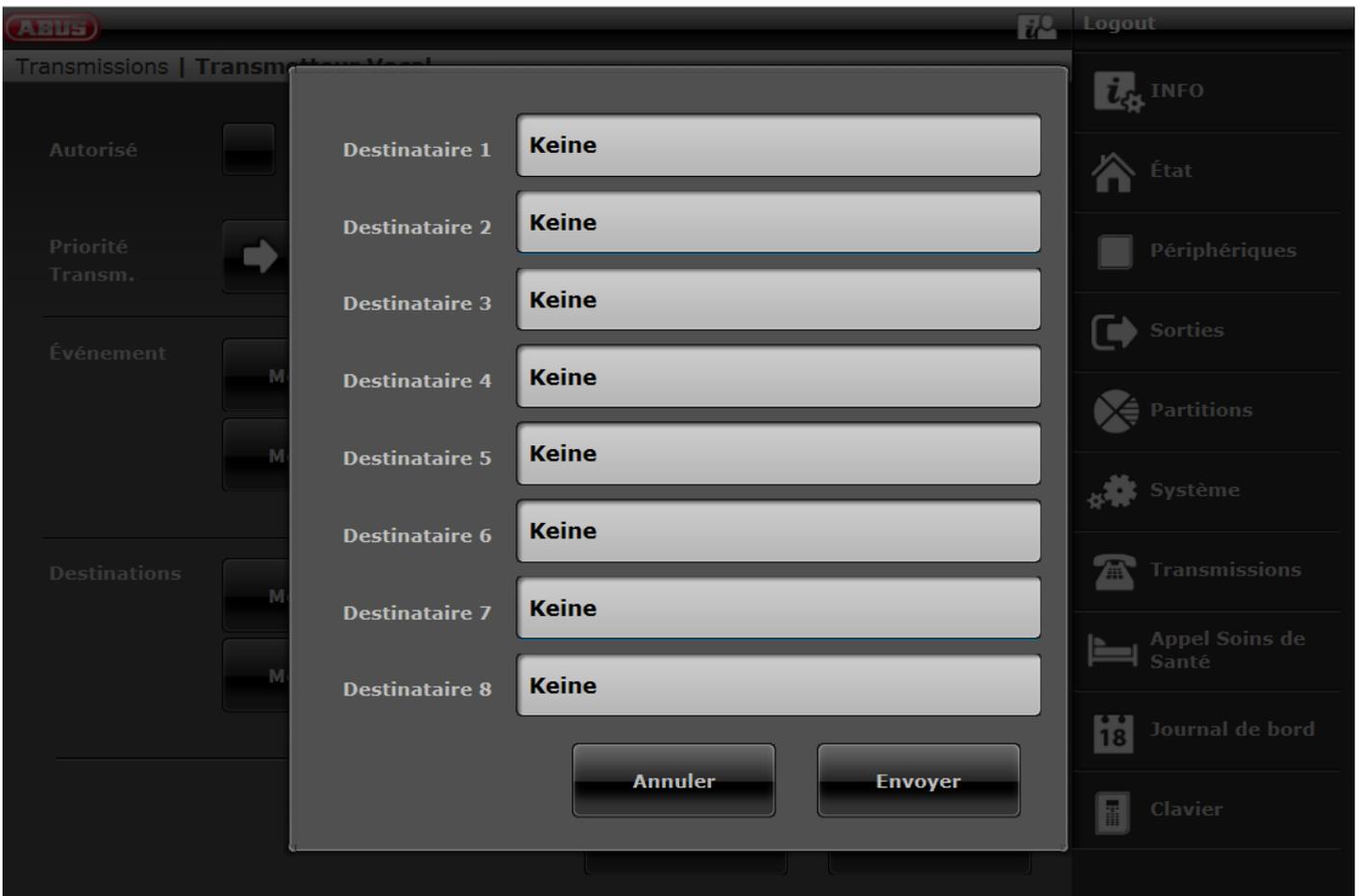
	 <p>Remarque signifie transmission de la voix classique (également DTMF et FSK) via un réseau de téléphonie mobile.</p>  <p>Remarque L'affichage varie selon le réglage de la passerelle IP dans le menu « Configuration Mobile IP ».</p>
Acquit d'appel	<p>Activé La transmission d'alarme doit être confirmée par le destinataire avec "5" ou "9". Appuyez sur la touche DTMF « 5 » : les appels à ces numéros sont terminés. À défaut, les appels sont répétés et d'autres numéros sont appelés. Appuyez sur la touche DTMF « 9 » : la procédure d'appel de la centrale d'alarme est terminée.</p>  <p>Remarque Pour la VoIP, il faut en outre avoir activé RFC 2833 Détection DTMF.</p> <p>Désactivé Si la fonction est désactivée, l'appel est considéré comme transmis lorsque la ligne appelée est décrochée.</p>
Messages	<p>Sélectionnez ces points directement sur la centrale et suivez les instructions à l'écran.</p> <p>Message de localisation (env. 12 s) Ce message est lu à chaque transmission de la voix. Vous devez ici enregistrer les données pour la localisation de la centrale sans fil (nom, rue, numéro, etc.)</p> <p>Message 1-4 (env. 8 s chacun) Enregistrement des messages pour les différents événements. Quatre messages sont disponibles. Prononcez par exemple « Alarme incendie », « Alarme agression »...</p>  <p>Remarque Il faut enregistrer au moins un message de localisation et un message d'événement. N'oubliez pas de sauvegarder les messages après l'enregistrement.</p>  <p>Remarque Tenez compte des réglages lors de l'appel de test :</p>

Transmetteur vocal, événement



Désignation/Fonction	Explication (case à cocher)
Événement #	<p>Liste déroulante de sélection :</p> <ul style="list-style-type: none"> • Aucune • Alarme intrusion • Alarme agression <ul style="list-style-type: none"> ○ Alarmes de panique et utilisation du code menace • Incendie • Alarme Alarme • Urgence soins • Inactivité soins • Technique • Défaut test détecteur • Défaut secteur • Sabotage • Brouillage • stat. <p> Remarque Tenez compte des réglages lors de l'appel de test :</p>

Transmetteur vocal, destinations



Designation/Fonction	Explication (case à cocher)
Destinataire #	Après avoir cliqué sur le champ de sélection, une fenêtre contextuelle s'ouvre dans laquelle le numéro de téléphone souhaité ou le SIP ID d'un destinataire peut être sélectionné parmi les contacts.



Remarque

Version logicielle >= 3.01.11

Si la centrale n'a pas pu atteindre le destinataire correspondant à la première tentative d'appel, la centrale essaye 3 fois au maximum d'atteindre le destinataire correspondant.

Mais chaque destinataire est testé via chaque voie disponible avant que la centrale ne poursuive avec le prochain essai.

Transmetteur vocal, appel de test

Désignation/Fonction	Explication (case à cocher)
Appel de test stat.	<p>Appel de test statique</p> <p>Après avoir cliqué sur le champ de sélection, une fenêtre contextuelle s'ouvre dans laquelle le rythme souhaité peut être sélectionné.</p> <ul style="list-style-type: none"> • Journalier • Hebdomadaire • Mensuel <p> Remarque Pour chacun des trois types d'appel, journalier, hebdomadaire et mensuel, la centrale ajoute une valeur en minutes basée sur le hasard. Cette valeur en minutes est comprise entre 0 et 16. L'appel peut donc avoir lieu jusqu'à 16 minutes après l'heure que vous avez indiquée. Cela permet de garantir que le destinataire ne soit pas surchargé par une marée d'appels de test de systèmes, qui ont tous obtenu la même heure.</p> <p> Remarque Tenez compte des réglages lors de l'événement :</p> <p> Remarque L'enregistrement d'un message vocal « Appel de test » est important pour distinguer clairement cet appel de test d'un appel d'alarme normal.</p>

<p>Heure</p>	<p>Champ de saisie de l'heure de l'appel de test journalier (format h ou hh) (0 – 23)</p> <p></p> <p>Remarque Seules des heures entières sont possibles.</p>
<p>Jours En cas d'« Appel de test stat. »</p> <ul style="list-style-type: none"> • hebdomadaire 	<p>Liste déroulante de sélection :</p> <ul style="list-style-type: none"> • Dimanche • Lundi • Mardi • Mercredi • Jeudi • Vendredi • Samedi
<p>Jours En cas d'« Appel de test stat. »</p> <ul style="list-style-type: none"> • mensuel 	<p>Champ de saisie du jour du mois où doit être effectué l'appel de test. (1 – 31)</p>

SMS

ABUS
Logout

Transmissions | SMS

Autorisé

Priorité Transm.

Événement

Destinations

Messages

SMS RTC

Événement

Message 1

Message 2

Message 3

Message 4

Annuler

Envoyer

INFO

État

Périphériques

Sorties

Partitions

Système

Transmissions

Appel Soins de Santé

18 Journal de bord

Clavier

Désignation/Fonction	Explication (case à cocher)
Autorisé	<p>Activé La fonction SMS est disponible.</p> <p>Désactivé La fonction SMS n'est pas disponible.</p> <div style="text-align: center; margin: 10px 0;"> </div> <p>Remarque La centrale n'envoie pas d'informations. Une connexion est établie seulement lors de l'envoi de SMS concret, tout d'abord avec le handshaking. Les informations sont alors envoyées selon les réglages ainsi que les textes et événements programmés.</p>
Priorité transmission	<p>Version logicielle < 3.00.05 Définissez ici dans quel ordre sont utilisées les voies de transmission.</p> <ul style="list-style-type: none"> • RTC 1, 2, 3 ou Non • GSM/Mobile 1, 2, 3 ou Non

Version logicielle >= 3.00.05

Définissez ici dans quel ordre sont utilisées les voies de transmission.

- RTC 1, 2, 3 ou Non
- Mobile 1, 2, 3 ou Non



Remarque

Signifie transmission classique de SMS via un réseau de téléphonie mobile.



Remarque

L'affichage varie selon le réglage de la passerelle IP dans le menu « Configuration Mobile IP ».

SMS, événement

ABUS
Logout

Transmissions | SMS

Autorisé

Priorité Transm.

Événement
Destinations
Messages
SMS RTC

Événement

Message 1

Message 2

Message 3

Message 4

Annuler

Envoyer

INFO

État

Périphériques

Sorties

Partitions

Système

Transmissions

Appel Soins de Santé

Journal de bord

Clavier

Désignation/Fonction	Explication (case à cocher)
Message #	<p>Après avoir cliqué sur le champ de sélection, une fenêtre contextuelle s’ouvre dans laquelle l’événement souhaité du message 1 à 4 peut être sélectionné.</p> <ul style="list-style-type: none"> • Sabotages • Alarmes • MES/MHS • Système • stat. <div style="text-align: center; margin: 10px 0;"> </div> <p>Remarque</p> <p>Tenez compte des réglages lors de l’appel de test :</p> <p>Sabotages</p> <p>Comprend tous les types de sabotage, y compris système, clavier de commande, périphériques, détecteurs, code utilisateur (sabotage de code) sirène et autres périphériques.</p> <p>Exemples : tous les sabotages sur la centrale, les détecteurs, les périphériques, la supervision (sous forme de sabotage), le brouillage (sous forme de sabotage)</p> <p>Alarmes</p> <p>Comprend tous les types d’alarme, y compris 24 heures, incendie, agression, effraction, médicale, soins, défaut de zones de test, alarme de zone et suivi zone. Cela comprend également la réinitialisation de ces alarmes. Voir</p>

également les détails de configuration de l'alarme de zone et du suivi de zone.

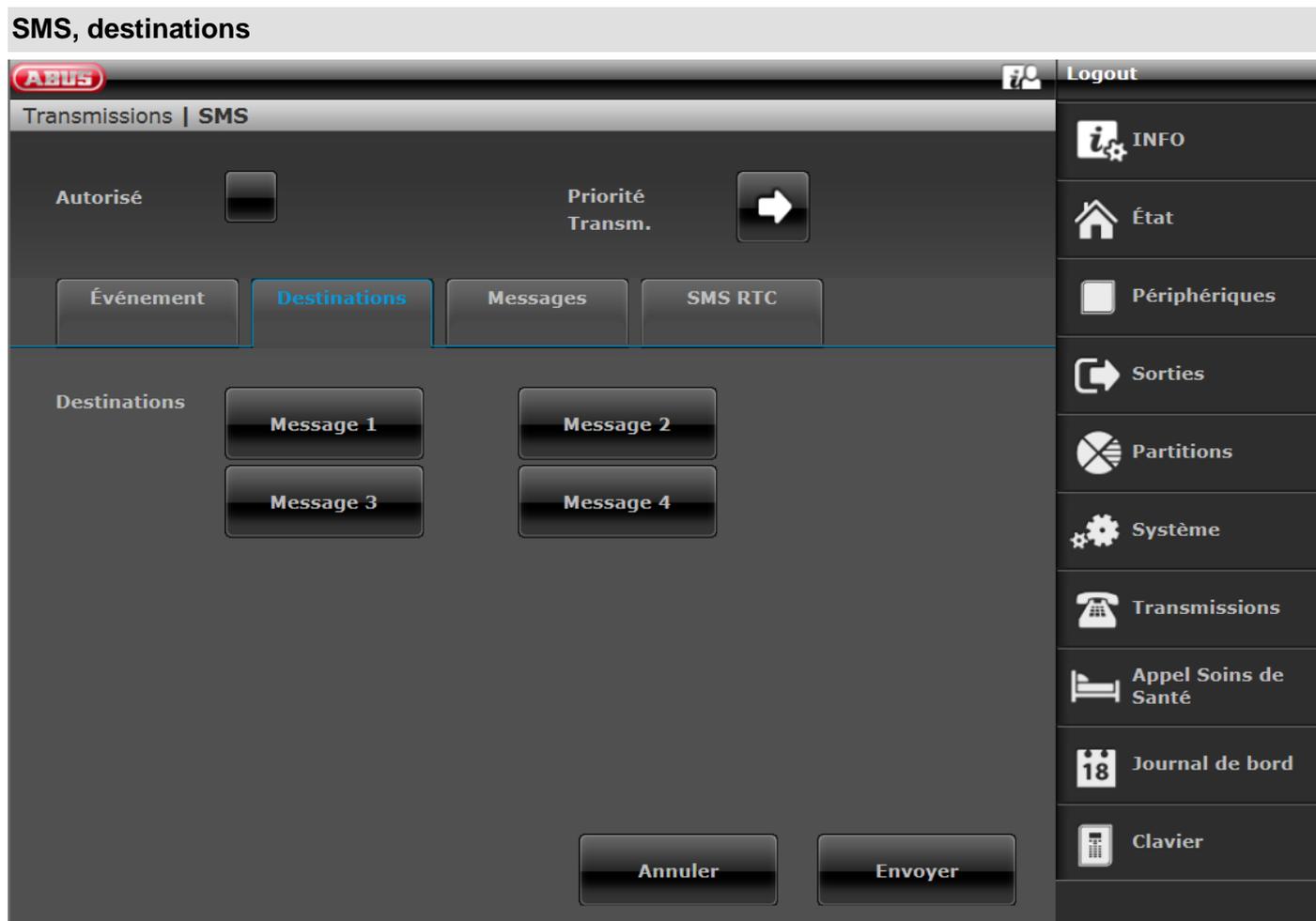
Activé/Désactivé

Comprend tous les types d'activation, activations et désactivations internes de partitions via la centrale, le clavier de commande, le verrou de porte supplémentaire, la télécommande, l'application ou via les autres périphériques pour activer et désactiver.

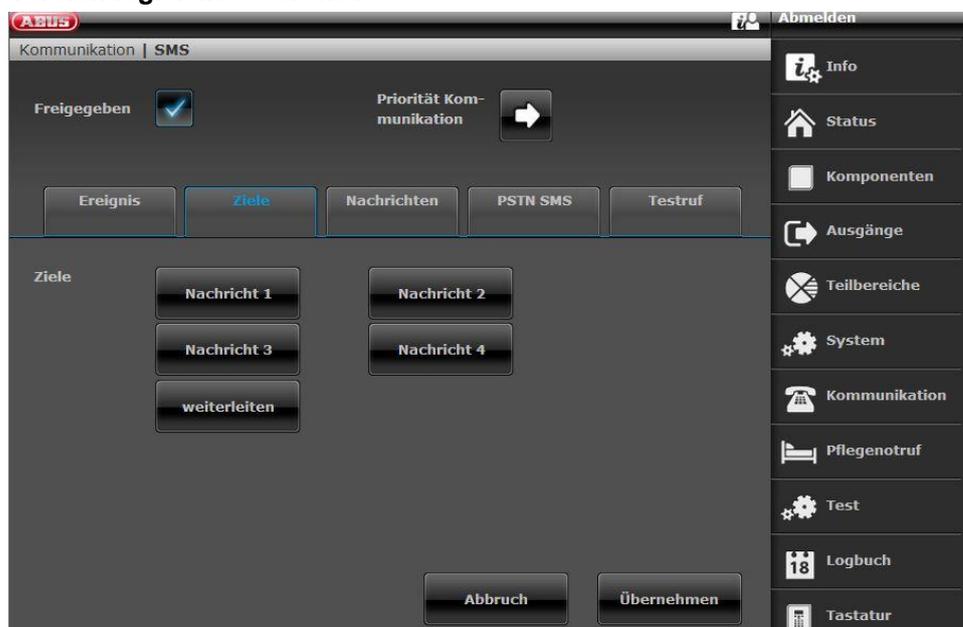
Exemples : PART. x activée/désactivée

Système

Comprend tous les types d'événements système qui ne sont pas des alarmes, sabotages ou ne concernent pas l'activation/la désactivation. Cela inclut les périphériques manquants, la supervision (sous forme de défaut), le brouillage (sous forme de défaut), les erreurs ou défauts de communication, les défauts PSU CA/CC, une batterie de système faible ou manquante, une batterie de périphériques faible ou une panne d'Aux 12 V.



Version logicielle >= 3.01.01



Désignation/Fonction	Explication (case à cocher)
Message #	Après avoir cliqué sur le champ de sélection, une fenêtre contextuelle s'ouvre dans laquelle le numéro de téléphone du destinataire peut être sélectionné parmi les contacts.
Transférer	Version logicielle >= 3.01.01

Vous permet de configurer la centrale de manière à ce que les messages SMS reçus par l'exploitant du réseau (par ex. messages d'avertissement avec crédit faible) puissent être transférés à **un** numéro de téléphone précis. Si vous sélectionnez Transférer, la liste de contacts s'affiche. Sélectionnez un contact de la liste de contacts puis un des deux numéros de téléphone définis pour ce contact.

SMS, destinations, message X

Désignation/Fonction	Explication (case à cocher)
Tél. destinataire #	Sélection du destinataire 1 à 8 pour le message 1 à 4.



Remarque

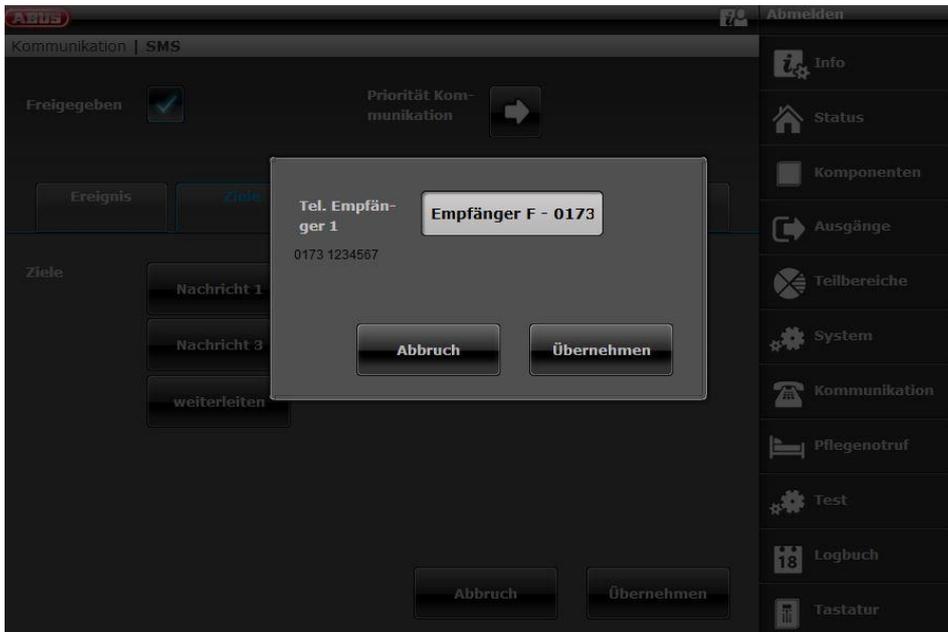
Version logicielle >= 3.01.11

Si la centrale n'a pas pu atteindre le destinataire correspondant à la première tentative d'envoi de SMS au centre de service, la centrale essaye 3 fois au maximum d'atteindre le centre de service pour le destinataire correspondant et d'envoyer le SMS.

Pour chaque essai d'envoi échoué via la première voie, la centrale essaye 3 fois au maximum d'atteindre le centre de service pour le destinataire correspondant via la deuxième voie.

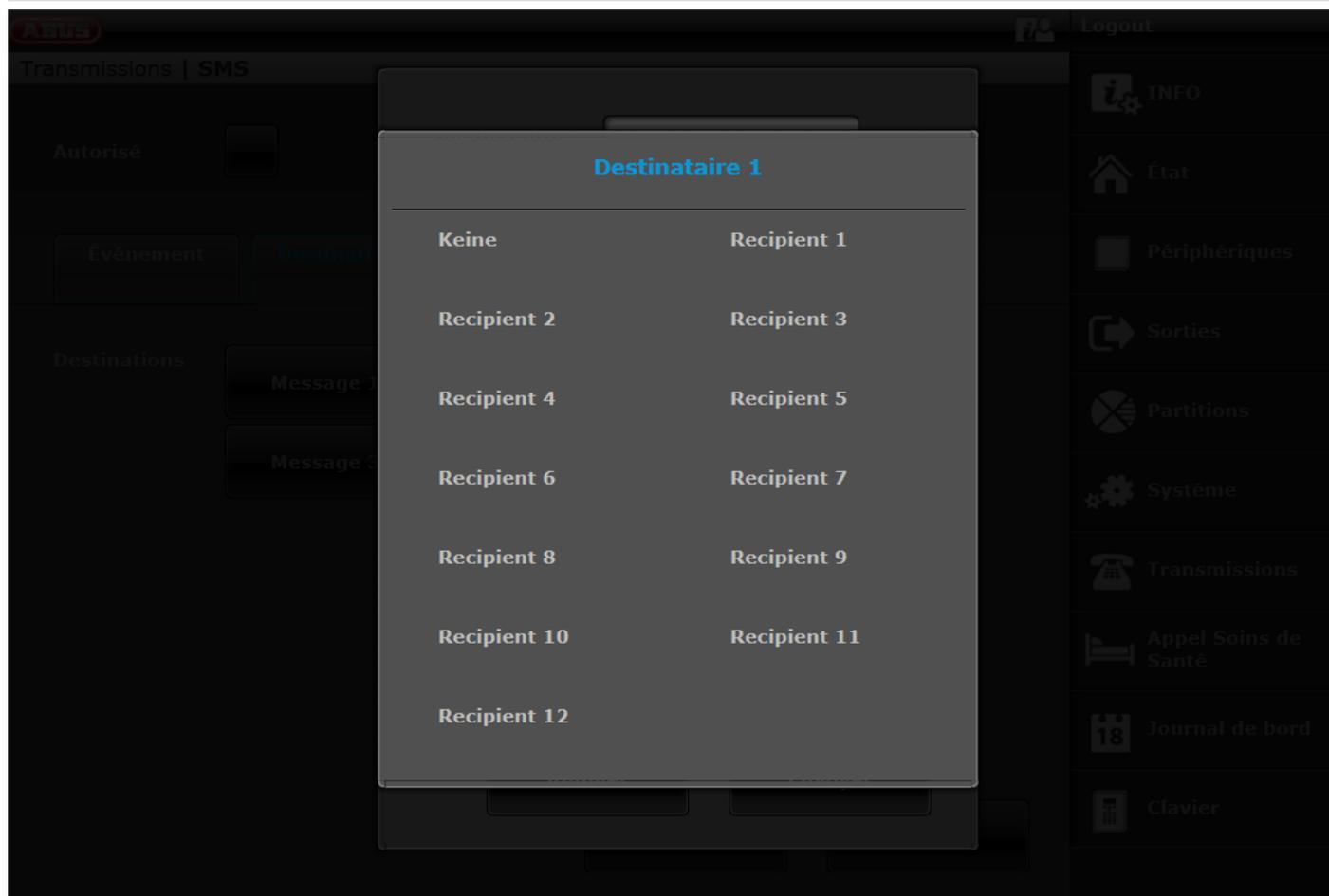
SMS, destinations, transférer

Version logicielle >= 3.01.01



Désignation/Fonction	Explication (case à cocher)
Tél. destinataire 1	Sélection d'un destinataire pour le transfert de messages SMS reçus.

SMS, destinations, message, téléphone destinataires



Désignation/Fonction	Explication (case à cocher)
Aucune	Pas de sélection de destinataire
Destinataire #	Sélection des données de contact du destinataire A à L

SMS, messages

Désignation/Fonction	Explication (case à cocher)
Message principal	Enregistrement d'un message principal (30 caractères maximum)
Message #	Enregistrement du message 1 à 4 (30 caractères maximum)

SMS, SMS RTC

ABUS Logout

Transmissions | SMS

Autorisé Priorité Transm.

Événement Destinations Messages **SMS RTC**

Protocole ***ETSI Protocole 1** Service N° Tél **1470,17094009**

- TAP 8N1
- TAP 7E1
- UCP 8N1
- UCP 7E1
- *ETSI Protocole 1**

Annuler Envoyer

INFO

État

Périphériques

Sorties

Partitions

Système

Transmissions

Appel Soins de Santé

18 Journal de bord

Clavier



Remarque

Si vous n'avez pas installé de module de téléphonie mobile, mais souhaitez envoyer des messages SMS via la ligne RTC, vous devez programmer des données supplémentaires dans ce menu.

Il est possible d'envoyer des SMS sur de nombreuses lignes fixes.

La connexion doit cependant être activée et tous les dispositifs de télécommunication commutés situés entre le point de terminaison ou la 1ère prise TAE et la centrale sans fil doivent prendre en charge la fonction CLIP.

Désignation/Fonction	Explication (case à cocher)
Protocole	<p>Sélectionnez le protocole que le centre de services SMS vous a indiqué.</p> <p>Menu déroulant avec les options de sélection suivantes :</p> <ul style="list-style-type: none"> • TAP 8N1 • TAP 7E1 • UCP 8N1 • UCP 7E1 • ETSI Protocole 1

Désignation/Fonction	Explication (case à cocher)
<p>Service n° tél</p>	<p>Indiquez ici le numéro d'appel du centre de services (F-SMSC) qui vous a été fourni.</p> <p>Le numéro d'appel du centre de services et le protocole doivent correspondre. Adressez-vous au service technique du fournisseur d'accès que vous souhaitez utiliser.</p> <p>Lorsque vous demandez le numéro du centre de services, demandez quel protocole il utilise.</p> <p>Enregistrez le numéro d'appel SMSC (numéro de la centrale des SMS du réseau fixe).</p> <p>Les numéros nationaux figurent dans l'annexe dans « Notifications par SMS ».</p> <p> Remarque Voir également le PBX avec ligne extérieure au chapitre : Options de communication – Mobile sans ligne extérieure</p> <p> Remarque Pour l'envoi de SMS à partir du réseau GSM/de téléphonie mobile (par le module de téléphonie mobile), le numéro de la centrale SMS du fournisseur correspondant figure déjà sur la carte SIM.</p> <p>Au besoin, vous pouvez vérifier le numéro enregistré avec un téléphone portable. Vous trouverez une sélection dans l'annexe dans « Notifications par SMS », seconde partie.</p>
<p>Mon n° tél</p>	<p>Certains centres de services ou protocoles ont besoin du numéro appelant avant d'accepter la demande de traitement d'un message SMS. (Permet également la facturation claire des messages SMS.) Entrez ici le numéro d'appel de la ligne de réseau fixe de la Secvest.</p> <p>Uniquement disponible si l'un des protocoles UCP suivants a été sélectionné dans le menu déroulant :</p> <ul style="list-style-type: none"> • UCP 8N1 • UCP 7E1

SMS, appel de test

Désignation/Fonction	Explication (case à cocher)
Appel de test stat.	<p>Appel de test statique</p> <p>Après avoir cliqué sur le champ de sélection, une fenêtre contextuelle s'ouvre dans laquelle le rythme souhaité peut être sélectionné.</p> <ul style="list-style-type: none"> • Journalier • Hebdomadaire • Mensuel <p> Remarque Pour chacun des trois types d'appel, journalier, hebdomadaire et mensuel, la centrale ajoute une valeur en minutes basée sur le hasard. Cette valeur en minutes est comprise entre 0 et 16. L'appel peut donc avoir lieu jusqu'à 16 minutes après l'heure que vous avez indiquée. Cela permet de garantir que le destinataire ne soit pas surchargé par une marée d'appels de test de systèmes, qui ont tous obtenu la même heure.</p> <p> Remarque Tenez compte des réglages lors de l'événement.</p>

<p>Heure</p>	<p>Champ de saisie de l'heure de l'appel de test journalier (format h ou hh) (0 – 23)</p> <p></p> <p>Remarque Seules des heures entières sont possibles.</p>
<p>Jours En cas d'« Appel de test "Appel test stat."</p> <ul style="list-style-type: none"> • Hebdomadaire 	<p>Liste déroulante de sélection :</p> <ul style="list-style-type: none"> • Dimanche • Lundi • Mardi • Mercredi • Jeudi • Vendredi • Samedi
<p>Jours En cas d'« Appel de test "Appel test stat."</p> <ul style="list-style-type: none"> • Mensuel 	<p>Champ de saisie du jour du mois où doit être effectué l'appel de test. (1 – 31)</p>

E-mail
Logout

Transmissions | E-mail

Autorisé

Priorité Transm.

Événement

Destinations

Messages

Événement

Message 1

Message 2

Message 3

Message 4

Annuler

Envoyer

- INFO
- État
- Périphériques
- Sorties
- Partitions
- Système
- Transmissions
- Appel Soins de Santé
- 18 Journal de bord
- Clavier

Désignation/Fonction	Explication (case à cocher)						
Autorisé	<p>Activé La fonction e-mail est disponible.</p> <p>Désactivé La fonction e-mail n'est pas disponible.</p> <p> Remarque La centrale n'envoie pas d'informations. Une connexion est établie seulement lors de l'envoi concret de l'e-mail, tout d'abord avec le handshaking. Les informations sont alors envoyées selon les réglages (par ex. cryptées ou non cryptées), ainsi que les textes et événements programmés.</p>						
	<p> Remarque La centrale peut envoyer des photos de la caméra TVIP41550 comme pièce jointe d'e-mail. Si un module de téléphonie mobile est utilisé, veuillez respecter les points suivants.</p> <table style="width: 100%; border: none;"> <tr> <td style="width: 50%;">Liaison de données</td> <td style="width: 50%;">Envoi d'images</td> </tr> <tr> <td>2G (GPRS)</td> <td>E-mail sans photos en pièce jointe</td> </tr> <tr> <td>4G (LTE)</td> <td>E-mail avec photos en pièce jointe</td> </tr> </table>	Liaison de données	Envoi d'images	2G (GPRS)	E-mail sans photos en pièce jointe	4G (LTE)	E-mail avec photos en pièce jointe
Liaison de données	Envoi d'images						
2G (GPRS)	E-mail sans photos en pièce jointe						
4G (LTE)	E-mail avec photos en pièce jointe						

	<p>Dans le réseau GPRS, le débit de données est trop faible pour transférer de grands volumes de données.</p>
<p>Priorité transmission</p>	<p>Définissez ici dans quel ordre sont utilisées les voies de transmission.</p> <ul style="list-style-type: none"> • Ethernet 1, 2, 3 ou Non <p>Version logicielle >= 3.00.05 Définissez ici dans quel ordre sont utilisées les voies de transmission.</p> <ul style="list-style-type: none"> • Ethernet/Mobile IP 1, 2, 3 ou Non <p> Remarque Signifie transmission de données selon le réglage de la passerelle IP dans le menu « Configuration Mobile IP »</p> <p> Remarque Version logicielle >= 3.01.16 Tenez également compte des instructions relatives au ping ICMP dans « Serveur ABUS » (Communication -> Réseau -> Configuration de réseau)</p> <p> Remarque L'affichage varie selon le réglage de la passerelle IP dans le menu « Configuration Mobile IP ».</p>

E-mail, événement

ABUS Logout

Transmissions | E-mail

Autorisé Priorité Transm. 

Événement Destinations Messages

Événement

Message 1 Message 2

Message 3 Message 4

Annuler Envoyer

-  INFO
-  État
-  Périphériques
-  Sorties
-  Partitions
-  Système
-  Transmissions
-  Appel Soins de Santé
-  18 Journal de bord
-  Clavier

Désignation/Fonction	Explication (case à cocher)
Message #	<p>Après avoir cliqué sur le champ de sélection, une fenêtre contextuelle s'ouvre dans laquelle l'événement souhaité du message 1 à 4 peut être sélectionné :</p> <ul style="list-style-type: none"> • Sabotages • Alarmes • MES/MHS • Système • stat. <p style="text-align: center;"></p> <p>Remarque</p> <p>Tenez compte des réglages lors de l'appel de test :</p> <p>Sabotages</p> <p>Comprend tous les types de sabotage, y compris système, clavier de commande, périphériques, détecteurs, code utilisateur (sabotage de code) sirène et autres périphériques.</p> <p>Exemples : tous les sabotages sur la centrale, les détecteurs, les périphériques, la supervision (sous forme de sabotage), le brouillage (sous forme de sabotage)</p> <p>Alarmes</p> <p>Comprend tous les types d'alarme, y compris 24 heures, incendie, agression, effraction, médicale, soins, défaut de zones de test, alarme de zone et suivi zone. Cela comprend également la réinitialisation de ces alarmes. Voir</p>

également les détails de configuration de l'alarme de zone et du suivi de zone.

MES/MHS

Comprend tous les types d'activation, activations et désactivations internes de partitions via la centrale, le clavier de commande, le verrou de porte supplémentaire, la télécommande, l'application ou via les autres périphériques pour activer et désactiver.

Exemples : PART. x activée/désactivée

Système

Comprend tous les types d'événements système qui ne sont pas des alarmes, sabotages ou ne concernent pas l'activation/la désactivation. Cela inclut les périphériques manquants, la supervision (sous forme de défaut), le brouillage (sous forme de défaut), les erreurs ou défauts de communication, les défauts PSU CA/CC, une batterie de système faible ou manquante, une batterie de périphériques faible ou une panne d'Aux 12 V.

E-mail, destinations

ABUS Logout

Transmissions | E-mail

Autorisé Priorité Transm. 

Événement **Destinations** Messages

Destinations

Message 1

Message 2

Message 3

Message 4

Annuler

Envoyer

-  INFO
-  État
-  Périphériques
-  Sorties
-  Partitions
-  Système
-  Transmissions
-  Appel Soins de Santé
-  18 Journal de bord
-  Clavier

Désignation/Fonction	Explication (case à cocher)
Message #	Après avoir cliqué sur le champ de sélection, une fenêtre contextuelle s'ouvre dans laquelle l'adresse e-mail souhaitée d'un destinataire peut être sélectionnée parmi les contacts.

E-mail, messages

ABUS Logout

Transmissions | E-mail

Autorisé Priorité Transm. 

Événement Destinations **Messages**

Message Principal **Secvest Lab Wall**

Message 1 **Tamper Alarm** Message 2 **Normal Alarm**

Message 3 **System Alarm** Message 4

Annuler **Envoyer**

INFO

État

Périphériques

Sorties

Partitions

Système

Transmissions

Appel Soins de Santé

Journal de bord

Clavier

Désignation/Fonction	Explication (case à cocher)
Message principal	Enregistrement d'un message principal (30 caractères maximum)
Message #	Enregistrement du message 1 à 4 (30 caractères maximum)

E-mail, appel de test

Désignation/Fonction	Explication (case à cocher)
Appel de test stat.	<p>Appel de test statique</p> <p>Après avoir cliqué sur le champ de sélection, une fenêtre contextuelle s'ouvre dans laquelle le rythme souhaité peut être sélectionné.</p> <ul style="list-style-type: none"> • Journalier • Hebdomadaire • Mensuel <p> Remarque</p> <p>Pour chacun des trois types d'appel, journalier, hebdomadaire et mensuel, la centrale ajoute une valeur en minutes basée sur le hasard. Cette valeur en minutes est comprise entre 0 et 16. L'appel peut donc avoir lieu jusqu'à 16 minutes après l'heure que vous avez indiquée. Cela permet de garantir que le destinataire ne soit pas surchargé par une marée d'appels de test de systèmes, qui ont tous obtenu la même heure.</p> <p> Remarque</p> <p>Tenez compte des réglages lors de l'événement.</p>

<p>Heure</p>	<p>Champ de saisie de l'heure de l'appel de test journalier (format h ou hh) (0 – 23)</p> <p></p> <p>Remarque Seules des heures entières sont possibles.</p>
<p>Jours En cas d'« Appel de test "Appel test stat." • Hebdomadaire</p>	<p>Liste déroulante de sélection :</p> <ul style="list-style-type: none"> • Dimanche • Lundi • Mardi • Mercredi • Jeudi • Vendredi • Samedi
<p>Jours En cas d'« Appel de test "Appel test stat." • Mensuel</p>	<p>Champ de saisie du jour du mois où doit être effectué l'appel de test. (1 – 31)</p>

options de communication

ABUS Log out

Communications | Options de communication

Ethernet Défaut Réponse Ligne	<input type="text" value="*Bloqué"/>	Ethernet Tempo Défaut ligne RTC	<input type="text" value="9"/>
RTC Défaut Réponse Ligne	<input type="text" value="*Audible"/>	RTC Tempo Défaut ligne RTC	<input type="text" value="9"/>
GSM Défaut Réponse Ligne	<input type="text" value="*Audible"/>	GSM Tempo Défaut ligne RTC	<input type="text" value="9"/>
GSM sans RTC	<input type="checkbox"/>	Contrôle Appel sortant	<input type="checkbox"/>
Contrôle Appel entrant	<input checked="" type="checkbox"/>		
Sonneries avant réponse	<input type="text" value="*5 sonneries"/>	Réponse après 1ere Sonnerie	<input type="checkbox"/>

About

Status

Devices

Outputs

Partitions

System

Communications

Social Care

View Log

Keypad

Désignation/Fonction	Explication (case à cocher)
	 <p>Remarque relative au défaut ligne réponse</p> <p>Utilisez ces options pour déterminer comment le système doit réagir lorsque la centrale enregistre un défaut sur une voie de communication. Vous pouvez saisir divers réglages pour Ethernet, RTC et Mobile IP/Mobile.</p> <p>Audible Si le système est désactivé, l'événement est consigné. Les périphériques qui en sont capables émettent un signal acoustique bref chaque minute. En saisissant un code d'accès valide, les émetteurs d'alarme sont mis en mode silencieux et l'écran affiche un défaut de la voie de communication. Malgré le défaut de voie de communication affiché, le système peut à nouveau être activé. Si le système est ensuite activé, la centrale consigne l'événement, mais n'affiche aucune notification et n'émet pas de signal acoustique. La centrale interrompt toutes les temporisations de sirène (CRA/STS) programmées dans la partition, si la voie de communication est perturbée lors du déclenchement de l'alarme.</p> <p>Remarque : ABUS recommande « Audible » pour le défaut de voie de communication.</p> <p>Silencieux Si le système est désactivé, l'écran affiche un défaut de la voie de communication. Un triangle s'affiche en bas à droite de l'écran et la centrale consigne l'événement. Malgré le défaut de voie de communication affiché, le système peut à nouveau être activé.</p>

	<p>Si le système est ensuite activé, la centrale n'affiche pas de notification et n'émet pas non plus de signal acoustique, mais consigne l'événement. Dans le menu Partition, la centrale interrompt toutes les « Temporisations de sirène (CRA/STS) » programmées, si la voie de communication est perturbée lors du déclenchement de l'alarme.</p> <p>Bloqué La centrale ne surveille pas la voie de communication.</p>
	<p></p> <p>Remarque relative à la temporisation Défaut voie comm.</p> <p>Utilisez ces options pour déterminer combien de temps la centrale attend après la détection d'un défaut voie comm. sur une de ses voies de communication avant de générer un message d'avertissement, de lancer la communication et d'activer les sorties de défaut voie comm. Vous pouvez saisir divers réglages pour Ethernet, RTC et Mobile IP/Mobile.</p> <p>Remarque : cela peut durer quelques secondes jusqu'à ce que la centrale détecte un défaut voie comm. La temporisation réelle entre l'apparition du défaut voie comm. et le message d'avertissement en résultant est donc légèrement supérieure à la valeur que vous avez indiquée.</p>
<p>Ethernet Réaction Défaut voie comm.</p>	<p>Choisissez comment la Secvest doit réagir en cas de défaut du port Ethernet :</p> <ul style="list-style-type: none"> • Bloqué • Audible • Silencieuse <p></p> <p>Remarque Version logicielle >= 3.01.16</p> <p>Une erreur WAN est forcée en cas de défaut voie comm. (Ethernet). Cela entraîne un passage direct à la voie de communication IP redondante (lors de l'utilisation d'un module de téléphonie mobile).</p> <p>Un test WAN (ping) est forcé dès que le défaut voie comm. (Ethernet) est résolu. Cela signifie que le test WAN est exécuté toutes les 30 minutes ou lors du passage du défaut voie comm. à OK.</p> <p>Tenez également compte des instructions relatives au ping ICMP dans « Serveur ABUS » (Communication -> Réseau -> Configuration de réseau)</p>
<p>Ethernet Tempo Défaut ligne RTC</p>	<p>Délai de réaction en secondes du système d'alarme en cas de défaut du port Ethernet.</p> <p>Plage de valeurs : 0 à 60 secondes</p>
<p>RTC Réaction Défaut voie comm.</p>	<p>Choisissez comment la Secvest doit réagir en cas de défaut de la ligne téléphonique :</p> <ul style="list-style-type: none"> • Bloqué • Audible

	<ul style="list-style-type: none"> • Silencieuse
RTC Tempo Défaut ligne RTC	<p>Délai de réaction en secondes de la centrale d'alarme en cas de défaut de la ligne téléphonique.</p> <p>Plage de valeurs : 0 à 60 secondes</p>
Mobile IP/Mobile Réaction Défaut voie comm. (Uniquement avec un module de téléphonie mobile)	<p>Choisissez comment la Secvest doit réagir en cas de défaut de la connexion de téléphonie mobile :</p> <ul style="list-style-type: none"> • Bloqué • Audible • Silencieuse
Mobile IP/Mobile Tempo Défaut ligne RTC (Uniquement avec un module de téléphonie mobile)	<p>Délai de réaction en secondes du système d'alarme en cas de défaut de la connexion de téléphonie mobile.</p> <p>Plage de valeurs : 0 à 60 secondes</p>
Mobile sans ligne extérieure (Uniquement avec un module de téléphonie mobile)	<p>Activé</p> <p>Sélectionnez "Activé" pour que le premier chiffre du numéro de téléphone enregistré dans le répertoire téléphonique ne soit pas composé en cas de connexion GSM/de téléphonie mobile.</p> <p>Si vous voulez téléphoner via un PBX vers le réseau téléphonique public, vous devez entrer l'indicatif réseau (numéro de ligne réseau) avant de composer le numéro de téléphone.</p> <p>Dans ce cas, l'indicatif réseau doit se trouver en 1ère position dans le répertoire téléphonique de la centrale d'alarme.</p> <p>Vient ensuite le numéro d'appel de destination.</p> <p>Les indicatifs réseau s'obtiennent auprès de l'administrateur du PBX ou dans la notice du PBX.</p> <p>Généralement, c'est le "0". En Grande-Bretagne, c'est le plus souvent le "9".</p> <p>Format du numéro de téléphone : "0 0123 4567890".</p> <p>La centrale d'alarme peut ainsi être également raccordée à un poste analogique supplémentaire d'un PBX.</p> <p>Ce poste supplémentaire ne doit pas être obligatoirement commuté sur l'accès au réseau automatique.</p> <p>Désactivé</p> <p>Si vous utilisez un poste supplémentaire d'un PBX qui est programmé sur l'accès automatique au réseau ou une connexion téléphonique analogique normale, sélectionnez "Désactivé".</p> <p>Le réglage « GSM sans ligne extérieure = activé » ou « Mobile sans ligne extérieure = activé » a des conséquences sur les numéros d'appel :</p> <ul style="list-style-type: none"> • TS Reporting • Appel d'urgence de soin • Transmetteur vocal <p></p> <p>Remarque</p> <p>Normalement, l'envoi de SMS s'effectue uniquement par GSM/téléphonie mobile. Dans le répertoire téléphonique, enregistrez le numéro normal de destination : Format du numéro de téléphone : "0123 4567890".</p>

	<p>Dans un PBX, la centrale d'alarme est raccordée à un poste supplémentaire analogique sans accès au réseau automatique.</p> <p>Si vous souhaitez réaliser un envoi de SMS qui commence au niveau de la connexion analogique de la centrale d'alarme, dans :</p> <p>Mode installateur → Transmission → SMS → SMS RTC → Service n° tél.</p> <p>programmez l'indicatif réseau avant le numéro de téléphone du centre de services. Format du numéro de téléphone : "0 0123 4567890".</p> <p>Tenez également compte des remarques au chapitre Contacts. Pour cela, les contacts doivent être enregistrés avec 2 numéros de téléphone.</p>
<p>Appel sortant Commande</p>	<p></p> <p>Remarque Le chapitre 11.4 « Utilisation par téléphone » du manuel d'utilisateur décrit les combinaisons de touches du téléphone et les fonctions correspondantes.</p> <p>Activé Si cette option est activée, l'utilisateur peut télécommander l'installation lorsqu'il répond à un appel de la centrale d'alarme.</p> <p>Désactivé Si cette option est désactivée, l'utilisateur peut encore utiliser les commandes du transmetteur vocal à distance, mais pas les commandes de télécommande.</p>
<p>Appel entrant Commande</p>	<p></p> <p>Remarque Le chapitre 11.4 « Utilisation par téléphone » du manuel d'utilisateur décrit les combinaisons de touches du téléphone et les fonctions correspondantes.</p> <p>Activé Si cette option est activée, l'utilisateur peut appeler la centrale d'alarme à distance. Une fois que l'utilisateur a envoyé à distance un code d'accès à la centrale sans fil pour s'identifier, il peut exécuter des commandes à l'aide de son clavier téléphonique.</p> <p>Désactivé Si cette option est activée, l'utilisateur ne peut plus appeler la centrale d'alarme à distance.</p>
<p>Sonneries avant réponse (Uniquement si "Contrôle appel entrant" est activé)</p>	<p>Sélectionnez quand la centrale sans fil accepte un appel.</p> <ul style="list-style-type: none"> • 3 sonneries • 5 sonneries • 7 sonneries • 10 sonneries • 15 sonneries • 255 sonneries <p>Remarque Réglez la valeur sur 255 pour que la centrale ne prenne jamais l'appel.</p>
<p>Réponse après 1 sonnerie (Uniquement si "Contrôle appel entrant" est activé)</p>	<p>Activé Si la fonction est activée, la connexion de configuration à distance s'effectue par étapes. Le téléphone appelle la centrale d'alarme, laisse sonner deux fois et raccroche. La centrale est activée pour la réponse.</p>

	Au prochain appel, la centrale sans fil répond dans un délai de 10 à 90 secondes. La fonction "Sonneries avant réponse" est alors ignorée.
	Désactivé Si cette fonction est désactivée, la fonction "Sonneries avant réponse" décroche en cas d'appel entrant.

Contacts

Transmissions | Contacts

Destinataire 1	Recipient 1	Destinataire 2	Recipient 2
Destinataire 3	Recipient 3	Destinataire 4	Recipient 4
Destinataire 5	Recipient 5	Destinataire 6	Recipient 6
Destinataire 7	Recipient 7	Destinataire 8	Recipient 8
Destinataire 9	Recipient 9	Destinataire 10	Recipient 10
Destinataire 11	Recipient 11	Destinataire 12	Recipient 12

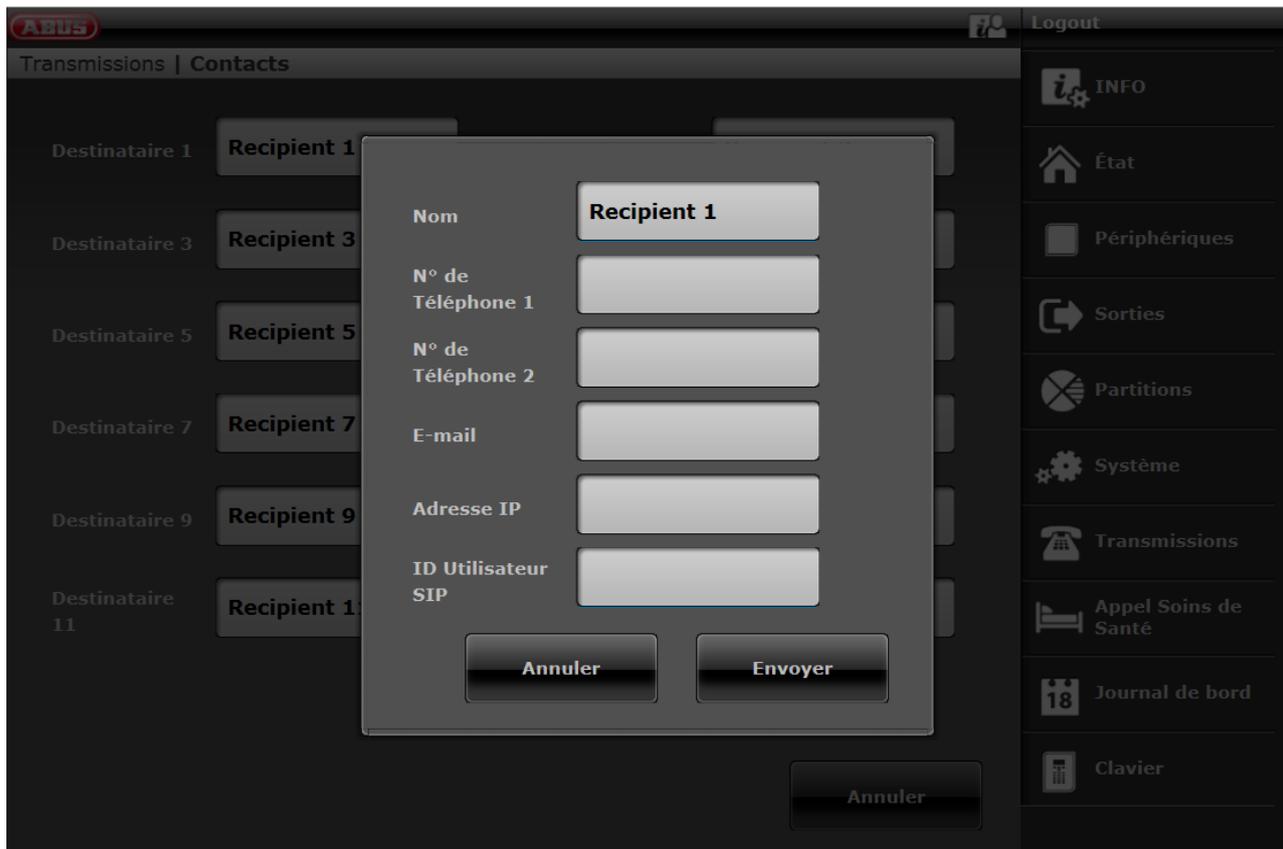
Annuler

- Logout
- INFO
- État
- Périphériques
- Sorties
- Partitions
- Système
- Transmissions
- Appel Soins de Santé
- Journal de bord
- Clavier

Jusqu'à 12 destinataires des messages peuvent être définis dans cette zone.

Un clic sur un utilisateur dans la vue d'ensemble des destinataires ouvre le profil de contact correspondant.
Entrez maintenant les données correspondantes

Version logicielle <2.00.00



Version logicielle >=2.00.00

Name	<input type="text" value="Recipient I"/>				
Teilbereiche	<input checked="" type="checkbox"/> 1	<input checked="" type="checkbox"/> 2	<input checked="" type="checkbox"/> 3	<input checked="" type="checkbox"/> 4	<input type="button" value="Alle Teilbereiche"/>
Telefon Nr. 1	<input type="text"/>				
Telefon Nr. 2	<input type="text"/>				
E-Mail	<input type="text"/>				
IP Adresse	<input type="text"/>				
SIP Ben. ID	<input type="text"/>				
	<input type="button" value="Abbruch"/>		<input type="button" value="Übernehmen"/>		

Des partitions peuvent être affectées au destinataire.

Cela signifie que le destinataire ne reçoit un message que lorsqu'un événement survient dans la partition sélectionnée.



Remarque

Cette affectation de partition s'applique uniquement au transmetteur vocal, aux SMS et aux e-mails, pas à la connexion AES/NSL.



Remarque

Les événements sans référence directe à une partition (par ex. fonctionnalité touches doubles sur la centrale d'alarme pour incendie, panique, médical et appel soins de santé) sont affectés à la partition 1.



Remarque

Panique (télécommande), panique (émetteur d'appel d'urgence), médical (émetteur d'appel d'urgence) et appel soins de santé (émetteur d'appel d'urgence)

Les événements émanant de ces composants spécifiques à l'utilisateur sont transmis aux destinataires pour lesquels les partitions sélectionnées concordent avec l'autorisation de partition de l'utilisateur.



Remarque

Clavier de commande sans fil

Fonctionnalité touches doubles pour incendie, panique, médical et appel soins de santé

Les événements émanant de ces composants sont transmis aux destinataires pour lesquels les partitions sélectionnées concordent avec l'affectation de partition du clavier de commande.



Remarque

ID utilisateur ID (utilisateur)

Format

Version logicielle $\geq 2.00.00$

Numéro de téléphone

+4982071234567

ID lorsque la destination a un compte auprès du même fournisseur de services SIP

9876543

Version logicielle $< 2.00.00$

Numéro de téléphone

+4982071234567@sipgate.de

sipgate.de est le fournisseur de services SIP propre, comme Nom serveur SIP

ID lorsque la destination a un compte auprès du même fournisseur de services SIP

9876543@sipgate.de



Remarque

Lors de l'utilisation de SMS mobile, de SMS RTC ainsi que de PBX avec ligne extérieure, 2 numéros d'appel doivent être enregistrés pour chaque destinataire.

Voir également le PBX avec ligne extérieure au chapitre :

Options de communication – **Mobile sans ligne extérieure**

Version logicielle >= 3.00.05

Name

Teilbereiche 1 2 3 4

Speech/SMS/Email De-aktiv Ak-tiv In-tern Ak-

Telefon Nr. 1

Telefon Nr. 2

E-Mail

IP Adresse

SIP Ben. ID

Désignation/Fonction	Explication (case à cocher)
Voix/SMS/E-mail	<p>Des événements ont été sélectionnés et affectés pour le transmetteur vocal, l'envoi de SMS et l'envoi d'e-mails.</p> <p>Les événements peuvent venir des groupes suivants :</p> <ul style="list-style-type: none"> • Sabotages • Alarmes • MES/MHS • Système <p>Les événements sélectionnés sont uniquement transférés à ce contact si :</p> <ul style="list-style-type: none"> • L'événement provient d'une des partitions sélectionnées • La partition présente l'état sélectionné, par exemple Désactivation et/ou Activation et/ou Activation interne • Le contact pour ces événements est affecté comme destinataire
Désactivée	<p>Oui</p> <p>En cas d'état désactivé de la partition, les événements sont transférés à ce contact</p> <p>Non</p>

	En cas d'état désactivé de la partition, les événements ne sont pas transférés à ce contact
Activation	Oui Les événements sont transférés à ce contact Non Les événements ne sont pas transférés à ce contact
Act. interne	Oui Les événements sont transférés à ce contact Non Les événements ne sont pas transférés à ce contact

Exemple 1	
Partitions	1 = Oui, 2 = Oui, 3 = Oui, 4 = Oui
Voix/SMS/E-mail	Désactivation = Non, Activation = Oui, Activation interne = Non
Événement	Incendie dans la partition 1
Partition 1 est	
Désactivée	Pas d'appel vocal, pas de SMS, pas d'e-mail à ce contact
Activée	Appel vocal, SMS et e-mail à ce contact
Activée en interne	Pas d'appel vocal, pas de SMS, pas d'e-mail à ce contact

Exemple 2	
Partitions	1 = Oui, 2 = Oui, 3 = Oui, 4 = Oui
Voix/SMS/E-mail	Désactivation = Oui, Activation = Non, Activation interne = Non
Événement	La centrale est ouverte (sabotage).
Les partitions 1 et 2 sont	Remarque : les partitions 3 et 4 ne sont pas utilisées.
Activées	Appel vocal, SMS et e-mail à ce contact !
	 <p>Remarque Aucune communication avec ce contact ne devrait normalement avoir lieu, car Activation est réglé sur Non. Mais un sabotage de boîtier est indiqué pour les 4 partitions. PART. 1 : boîtier ouvert PART. 2 : boîtier ouvert PART. 3 : boîtier ouvert PART. 4 : boîtier ouvert Les partitions 3 et 4 sont Désactivées dans ce cas, car elles ne sont pas utilisées. La communication a lieu en raison de Désactivation = Oui. Le réglage correct pour ce cas est montré à l'exemple 3.</p>

Exemple 3	
Partitions	1 = Oui, 2 = Oui, 3 = Non , 4 = Non
Voix/SMS/E-mail	Désactivation = Oui, Activation = Non, Activation interne = Non
Événement	La centrale est ouverte (sabotage).
Les partitions 1 et 2 sont	Remarque : les partitions 3 et 4 ne sont pas utilisées.
Activées	Pas d'appel vocal, pas de SMS, pas d'e-mail à ce contact

Appel d'urgence de soin

ABUS Logout

Appel Soins de Santé

Début Temps de surveillance:

Fin Temps de surveillance:

Intervalle de surveillance:

Volume langue:

-  INFO
-  État
-  Périphériques
-  Sorties
-  Partitions
-  Système
-  Transmissions
-  Appel Soins de Santé
-  18 Journal de bord
-  Clavier

Désignation/Fonction	Explication (case à cocher)
Début temps de surveillance	Début de la surveillance de soins (hh:mm).
Fin temps de surveillance	Fin de la surveillance de soins (hh:mm).
Intervalle de surveillance	Intervalle en heures.
Volume langue	Volume de l'annonce vocale.

Test

Sélectionnez la fonction correspondante.
Via l'interface Web avec version logicielle >=2.00.00.

Le tableau ci-après présente une vue d'ensemble des différentes fonctions.

The screenshot displays the 'Test' section of the ABUS web interface. At the top left is the 'ABUS' logo. The main area contains a grid of 20 test function buttons, each with an icon and a label. On the right side, there is a vertical sidebar menu with various system management options. The interface has a dark grey background with white icons and text.

Test				Logout
Test de marche	Clavier	Sirènes Ext.	Sirènes Int.	INFO
Module Sirènes	Claviers Radio	Serrures porte	Puissance du signal	État
Sorties	Badges	Télécommandes	Médailles	Périphériques
TS Reporting	Appel Soins de Santé	Transmetteur Vocal	SMS	Sorties
E-mail	Résistances Zones	PSU Centrale	Répéteur RF	Partitions
				Système
				Transmissions
				Appel Soins de Santé
				Test
				Journal de bord
				Clavier

Version logicielle >= 3.01.01

ABUS Abmelden

Test

 Geh Test	 Tastatur	 Außensirenen	 Int. Sirenen	 Sirenenmodul
 Lautsprecher	 Funk Bedienteil	 Türschlösser	 Signalstärken	 Ausgänge
 Chipschlüssel	 Fernbedienun- gen	 Notrufsender	 NSL Reporting	 Pflegetruf
 Sprachwählgerät	 SMS	 E-Mail	 Zonen Wider- stände	 Zentrale PSU
 RF Repeater				

Abmelden

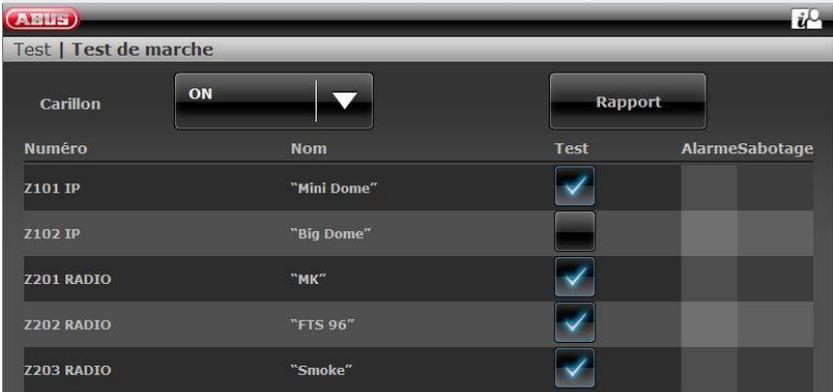
- Info
- Status
- Komponenten
- Ausgänge
- Teilbereiche
- System**
- Kommunikation
- Pflegetruf
- Test
- Logbuch
- Tastatur

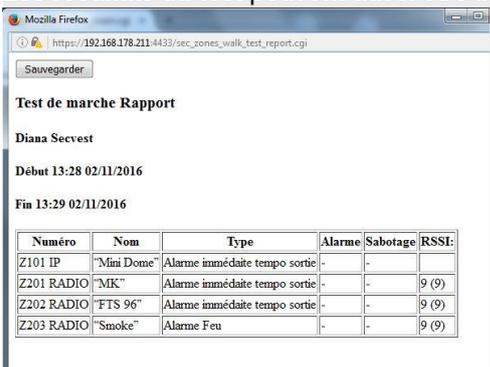
Version logicielle >= 3.01.14



Remarque

Appels de test à des destinataires externes. Veuillez le mentionner au préalable et indiquer qu'il s'agit d'un appel de test. Appel de test, par ex. station de contrôle, appels vocaux, SMS, e-mail.

Fonction	Signification
Test de détection	Carillon <ul style="list-style-type: none"> On : Une tonalité vous indique lorsque vous actionnez un détecteur. Off : Aucune tonalité ne retentit.
	<p>Ici, vous pouvez tester tous les détecteurs de la centrale. Les zones d'alarme peuvent être sélectionnées individuellement sous Test. Activez maintenant un par un tous les détecteurs installés. Lorsqu'un détecteur est identifié, la centrale d'alarme émet un signal sonore double. La colonne Alarme indique si un détecteur a détecté une alarme. La colonne Sabotage indique si un contact anti-sabotage s'est déclenché.</p> 

Test de détection (suite)	Rapport
	<p>Les résultats du test peuvent aussi être imprimés et enregistrés dans l'interface Web.</p> 

Centrale

Système

Ici, vous pouvez tester tous les détecteurs de la centrale. Activez maintenant un par un tous les détecteurs installés. Lorsqu'un détecteur est identifié, la centrale d'alarme émet un signal sonore double. Le déclenchement éventuel d'un contact anti-sabotage (S) et/ou d'une alarme (A) s'affiche également. Dans la partie supérieure de l'écran s'affiche le nombre de zones qui doivent encore être testées (alarme et sabotage).

Lorsque vous avez testé tous les détecteurs, la centrale indique Zones toutes testées.

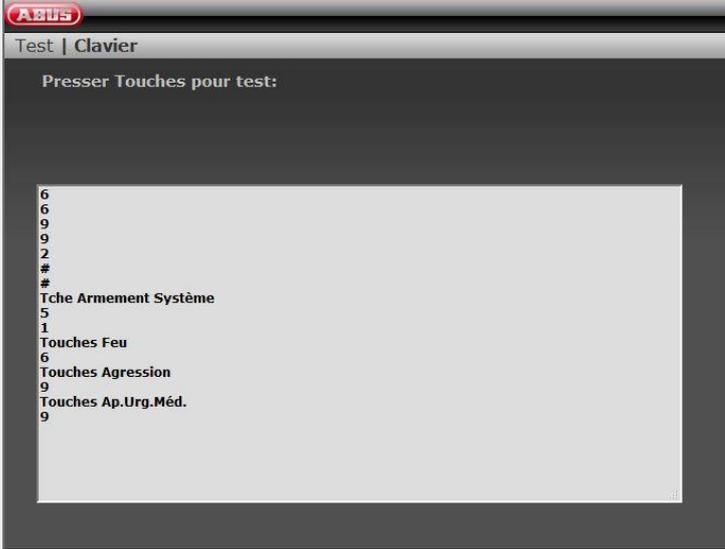
Partitions

- Ici, vous pouvez tester les détecteurs d'une partition.
- Après avoir sélectionné les partitions, seuls les détecteurs des partitions sélectionnées s'affichent.

Zones

- Vous pouvez tester ici les détecteurs sélectionnés.

La liste de tous les détecteurs s'affiche. Avec **Oui**, sélectionnez les détecteurs que vous souhaitez tester.

Fonction	Signification
Clavier	<p>Il est possible de tester le clavier à la fois sur la centrale d'alarme et dans l'interface Web.</p> <p>Activez successivement toutes les touches du panneau de commande.</p> <p>Le signe ou la fonction de la touche s'affiche en réponse.</p> <p>Appuyez simultanément sur les doubles touches (feu, agression, appel médical d'urgence ou appel soins de santé) pour les tester. La fonction de la combinaison de touches s'affiche en réponse.</p> <div data-bbox="277 414 1002 963" style="border: 1px solid black; padding: 5px; margin: 10px 0;">  </div> <p>Version logicielle >=2.01.08</p> <p>Appuyez simultanément sur les doubles touches (touches de menu gauche et droite) pour les tester. La fonction de la combinaison de touches s'affiche en réponse.</p> <div data-bbox="277 1153 335 1209" style="text-align: center;">  </div> <p>Remarque</p> <p>Le mode de nettoyage n'est pas exécuté ici. Vous trouverez des détails sur le mode de nettoyage dans le manuel d'utilisation.</p>
Sirènes et avertisseurs	<p>Le test des sirènes et avertisseurs s'effectue de la même manière dans l'interface Web et sur la centrale d'alarme.</p> <p>Sirènes int.</p> <ul style="list-style-type: none"> • Les émetteurs de la centrale d'alarme, du module d'information, de la sirène d'intérieur et de l'élément de commande radio sont commandés. <p>Sirènes radio ext.</p> <ul style="list-style-type: none"> • Les émetteurs des sirènes extérieures radio sont commandés. <div data-bbox="277 1657 335 1713" style="text-align: center;">  </div> <p>Remarque</p> <p>Concernant FUSG50100/1 (version logicielle 1.10.2 des sirènes)</p> <p>Si le boîtier de la sirène extérieure est fermé, le stroboscope et la sirène sont allumés.</p> <p>Si le boîtier de la sirène extérieure est ouvert, seul le stroboscope est allumé.</p> <p>Module sirènes</p> <ul style="list-style-type: none"> • Les émetteurs des sirènes extérieures sont commandés. Sirène extérieure associée au module universel (WAM) en tant que "module sirènes". <p>Haut-parleur</p>

- Sélectionnez « Lecture/Arrêt » pour lire successivement tous les messages enregistrés dans le système.



Fonction	Signification
Clavier de commande sans fil	<p>Le test de l'élément de commande radio s'effectue de la même manière dans l'interface Web et sur la centrale d'alarme.</p> <p>Activez successivement toutes les touches de fonction de l'élément de commande radio. Attendez 2 à 3 secondes entre chaque pression de touche afin que l'élément de commande puisse envoyer chaque message.</p> <p>Une lettre s'affiche en réponse :</p> <p>A = touche d'activation (verrou fermé) C = touche d'activation interne (*) D = touche de demande d'état (?) B = touche de désactivation (verrou ouvert)</p> <p>Sur le Web, les mêmes éléments sont visibles :</p> <ul style="list-style-type: none"> Touche Activer le système Touche Système activé en interne Demande d'état Touche Désactiver le système <p>Pour tester les touches numériques, actionnez 4 ou 6 touches numériques (selon la longueur de code définie) puis une touche de fonction. Exemple :</p> <ul style="list-style-type: none"> • Appuyez sur : 1234? • pour afficher : 1234D (interrogation d'état) <p>Appuyez simultanément sur les doubles touches (feu, agression, appel médical d'urgence ou appel soins de santé) pour les tester. L'affichage est le suivant :</p> <p>F = doubles-touches feu P = doubles-touches agression M = doubles-touches appel médical d'urgence H = doubles-touches appel soins de santé</p> <p>Sur le Web, les mêmes éléments sont visibles :</p> <ul style="list-style-type: none"> Touches Incendie Touches Panique Touches Appel d'urgence médicale Touches Soins de Santé <p>Les touches "*" et "#" au bas de l'élément de commande ne peuvent pas être testées.</p> 

Fonction	Signification																				
Verrous de porte	<p>Le test des verrous de porte s'effectue de la même manière dans l'interface Web et sur la centrale d'alarme.</p> <p>Sélectionnez le verrou de porte à tester.</p> <p>Actionnez le verrou de porte.</p> <p>Après l'ouverture, l'écran affiche "Non Verrouillée".</p> <p>Après la fermeture, l'écran affiche "Verrouillée".</p> <ul style="list-style-type: none">• Secvest Key : appuyez sur le bouton puis verrouillez.• Verrou de porte supplémentaire : n'appuyez pas sur le bouton mais verrouillez. <p>Remarque</p> <p>Ici, vous pouvez vérifier si le commutateur DIP 3 de la « Secvest Key » est bien réglé par rapport à la butée de porte.</p> <p>La puissance du signal s'affiche également.</p> <p>La signification du chiffre situé devant et dans la parenthèse est fournie dans l'explication de la puissance du signal.</p>																				
Puissance du signal	<p>Cette option permet de contrôler la puissance du signal reçu par tous les périphériques sans fil.</p> <p></p> <p>Remarque</p> <p>Pour garantir une bonne communication radio, veillez à avoir une puissance de signal supérieure à la valeur 3. Lors du test, la puissance de réception est réduite de 6 dB. La centrale d'alarme sans fil Secvest a une sensibilité d'environ -110 dBm, pour un rapport signal/bruit pondéré de 12 dB.</p> <p>Pour l'affichage de la puissance du signal sur la centrale Secvest, les valeurs de niveau suivantes s'appliquent :</p> <table><tbody><tr><td>0</td><td>< -101 dBm</td></tr><tr><td>1</td><td>< -98 dBm</td></tr><tr><td>2</td><td>< -95 dBm</td></tr><tr><td>3</td><td>< -92 dBm</td></tr><tr><td>4</td><td>< -89 dBm</td></tr><tr><td>5</td><td>< -86 dBm</td></tr><tr><td>6</td><td>< -83 dBm</td></tr><tr><td>7</td><td>< -80 dBm</td></tr><tr><td>8</td><td>≥ -77 dBm</td></tr><tr><td>9</td><td>≥ -77 dBm</td></tr></tbody></table> <p>Le chiffre qui précède la parenthèse correspond à la puissance du dernier signal reçu.</p> <p>Le chiffre dans la parenthèse correspond à la puissance de signal la plus faible après la dernière réinitialisation.</p> <p>La centrale d'alarme enregistre les puissances de signal reçu même lorsque vous n'êtes pas dans ce menu.</p> <p>Version logicielle <2.00.00</p> <p>La puissance du signal répété par le WAM est identique à celle du WAM correspondant.</p> <p>C'est la raison pour laquelle vous devez utiliser l'affichage de la puissance de signal pour le WAM correspondant pour recevoir également des informations sur la puissance des signaux répétés des périphériques sans fil.</p> <p>Version logicielle ≥2.00.00</p> <p>La puissance du signal direct des composants correspondants est visible dans la colonne de droite (WEB colonne Direct).</p> <p>La puissance du signal répété par le WAM ou par le répéteur RF est visible dans la colonne de gauche (WEB colonne Répéteur).</p>	0	< -101 dBm	1	< -98 dBm	2	< -95 dBm	3	< -92 dBm	4	< -89 dBm	5	< -86 dBm	6	< -83 dBm	7	< -80 dBm	8	≥ -77 dBm	9	≥ -77 dBm
0	< -101 dBm																				
1	< -98 dBm																				
2	< -95 dBm																				
3	< -92 dBm																				
4	< -89 dBm																				
5	< -86 dBm																				
6	< -83 dBm																				
7	< -80 dBm																				
8	≥ -77 dBm																				
9	≥ -77 dBm																				

Réinitialisation des puissances de signal pour commencer une nouvelle mesure.

WEB

Cliquez sur la ligne des composants souhaités et suivez les instructions qui apparaissent à l'écran.

Cliquez sur « Réinitialiser TOUS » et suivez les instructions qui apparaissent à l'écran. Les puissances de signal enregistrées sont alors supprimées de la liste complète correspondante.

Centrale

Touche #

Appuyez sur cette touche pour supprimer les puissances de signal enregistrées des périphériques sélectionnés.

Touche *

Appuyez sur cette touche pour supprimer les puissances de signal enregistrées de la liste complète correspondante.



Remarque

Sur le Mohy, la suppression et la mise à jour peuvent aller très vite.

**Puis-
sances de
signal
(suite)**

Détecteur

L'écran affiche les puissances de signal de chaque détecteur programmé.

Version logicielle <2.00.00 Les noms de zone d'alarme s'affichent. Pour voir les numéros de zone, appuyez sur la touche de menu droite.

Clavier de commande sans fil

L'écran affiche la puissance de signal de chaque élément de commande programmé.

Sirènes d'extérieur

L'écran affiche la puissance de signal de chaque sirène extérieure sans fil programmée.

Générateur de signal int.

L'écran affiche la puissance de signal de chaque générateur de signal intérieur programmé.

WAM

L'écran affiche la puissance de signal de chaque WAM programmé.

Verrous de porte

L'écran affiche la puissance de signal de chaque verrou de porte programmé.

Module hybride

L'écran affiche les puissances de signal de chaque module hybride programmé.

Vous trouvez ici 2 affichages.

Signal centrale d'al.

Il s'agit de la puissance du signal du module hybride sur la centrale.

Signal MoHy

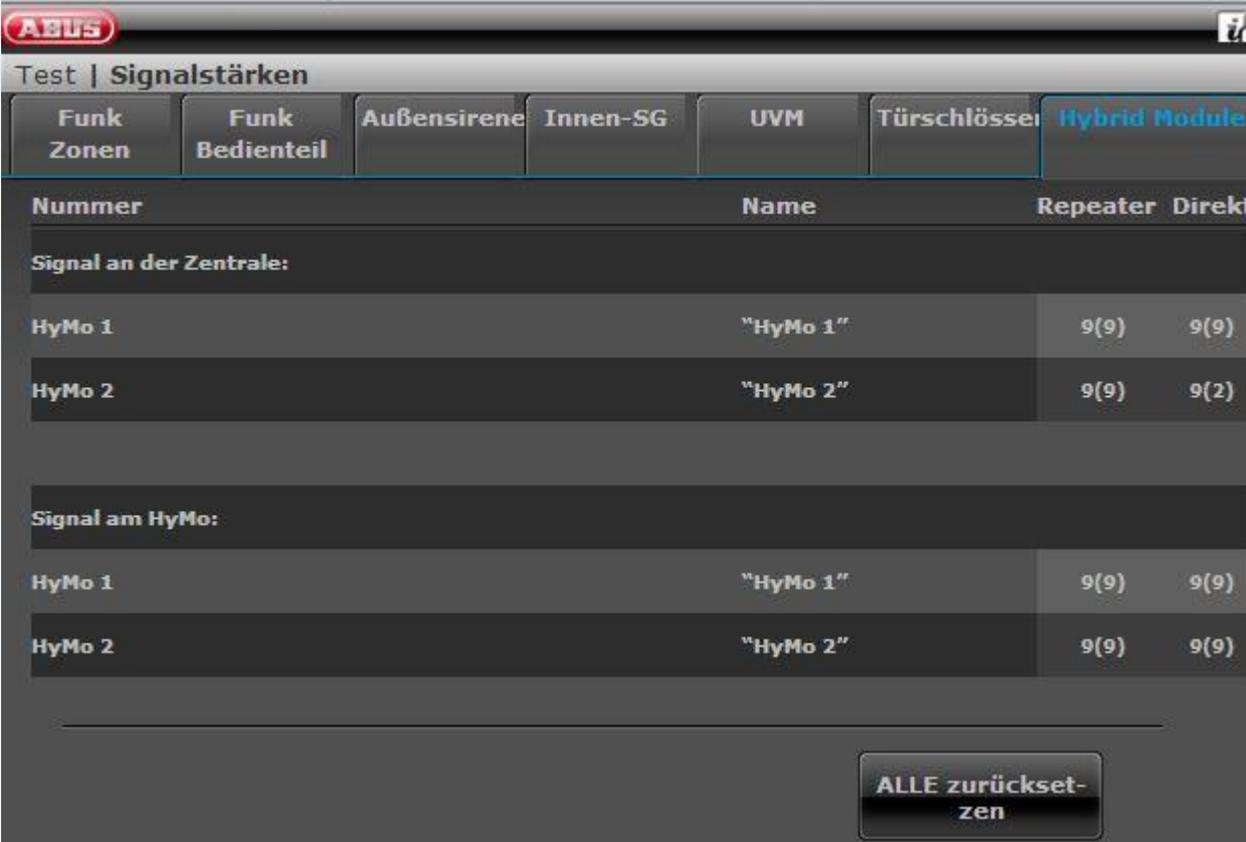
Il s'agit de la puissance du signal de la centrale sur le module hybride.



Remarque

Les deux puissances de signal sont similaires. Les puissances de signal centrale -> MoHy et MoHy -> centrale peuvent cependant être légèrement différentes. Les causes sont les suivantes :

des structures d'antennes différentes pour la centrale et le MoHy ;
des conditions de propagation des ondes radio différentes dans la direction correspondante.



The screenshot shows the 'Signalstärken' (Signal Strength) section of the ABUS web interface. It features a navigation bar with tabs for 'Funk Zonen', 'Funk Bedienteil', 'Außensirene', 'Innen-SG', 'UVM', 'Türschlösser', and 'Hybrid Module'. The main content area is divided into two sections: 'Signal an der Zentrale:' and 'Signal am HyMo:'. Each section contains a table with columns for 'Nummer', 'Name', 'Repeater', and 'Direkt'. The 'Signal an der Zentrale:' section shows two rows for 'HyMo 1' and 'HyMo 2', both with a signal strength of 9(9) for the Repeater and 9(9) for the Direkt column. The 'Signal am HyMo:' section also shows two rows for 'HyMo 1' and 'HyMo 2', both with a signal strength of 9(9) for the Repeater and 9(9) for the Direkt column. A button labeled 'ALLE zurücksetzen' is located at the bottom right of the interface.

Nummer	Name	Repeater	Direkt
Signal an der Zentrale:			
HyMo 1	"HyMo 1"	9(9)	9(9)
HyMo 2	"HyMo 2"	9(9)	9(2)
Signal am HyMo:			
HyMo 1	"HyMo 1"	9(9)	9(9)
HyMo 2	"HyMo 2"	9(9)	9(9)

Répéteur RF (centrale d'alarme uniquement)

L'écran affiche la puissance de signal de chaque répéteur RF programmé.

Vous trouverez ci-dessous, au niveau de Répéteur RF, des explications sur les affichages sur le WEB.

Périphériques répéteur RF (centrale d'alarme uniquement)

Vous trouverez ci-dessous, au niveau de Répéteur RF, des explications sur les affichages sur le WEB.

L'écran affiche sur le répéteur RF la puissance de signal de chaque périphérique attribué pour le répéteur RF correspondant.

Vous trouverez ci-dessous, au niveau de Répéteur RF, des explications sur les affichages sur le WEB.

Répéteur centrale d'alarme

Vous trouvez ici la puissance du signal des messages reçus sur le répéteur de la **centrale d'alarme**.

Répéteur détecteurs

Vous trouvez ici les puissances de signal des messages reçus sur le répéteur des **détecteurs**.

Répéteur claviers de commande sans fil

Vous trouvez ici les puissances de signal des messages reçus sur le répéteur des **claviers de commande sans fil**.

Répéteur générateur de signal int.

	<p>Vous trouvez ici les puissances de signal des messages reçus sur le répéteur des générateurs de signal intérieurs.</p> <p>Répéter sirènes d'extérieur Vous trouvez ici les puissances de signal des messages reçus sur le répéteur des sirènes d'extérieur.</p> <p>Répéter verrous de porte Vous trouvez ici les puissances de signal des messages reçus sur le répéteur des verrous de porte.</p> <p>Répéter MoHy Vous trouvez ici les puissances de signal des messages reçus sur le répéteur des modules hybrides.</p>
<p>Sorties</p>	<p>Sorties sans fil</p> <ul style="list-style-type: none"> • Cette fonction permet de contrôler toutes les sorties radio programmées. <p>Sorties filaires</p> <ul style="list-style-type: none"> • Cette fonction permet de contrôler toutes les sorties filaires programmées. <p>Sorties MoHy</p> <ul style="list-style-type: none"> • Cette fonction permet de contrôler toutes les sorties filaires MoHy programmées. <p>Une fois que vous avez quitté le menu, toutes les sorties éventuellement commutées reviennent à l'état de base programmé.</p>
<p>Badge</p>	<p>Le test des badges s'effectue de la même manière dans l'interface Web et sur la centrale d'alarme. Passez le badge sur la zone de lecture dans la partie inférieure de la centrale d'alarme (à hauteur du logo ABUS).</p> <p>Vous pouvez voir</p> <ul style="list-style-type: none"> • quel utilisateur est assigné à ce badge ou • que ce badge est inconnu de la centrale d'alarme
<p>Télécommandes</p>	<p>Le test de la télécommande s'effectue de la même manière dans l'interface Web et sur la centrale d'alarme.</p> <p>Appuyez sur n'importe quelle touche de la télécommande.</p> <p>L'écran affiche :</p> <ul style="list-style-type: none"> • le numéro séquentiel de la télécommande • une lettre ou un caractère correspondant à la touche enfoncée A = touche d'activation (verrou fermé) * = touche d'activation interne ou de commutation d'une sortie de type « Défini par U » (*) ? = touche de consultation de l'état (?) D = touche de désactivation (verrou ouvert) • à quel utilisateur est assignée cette télécommande • la fonction de la touche enfoncée <ul style="list-style-type: none"> - Tout activer - Activ. int. ou Sortie ON (Off ou Commuter) xyz - Interrog. état - Tout désactiver • la puissance du signal reçu (RSSI) <p>Exemple FB001,D:utilisateur 002 Tout est désactivé RSSI : 9</p>

Fonction	Signification
Émetteur d'appel d'urgence	<p>Le test de la télécommande s'effectue de la même manière dans l'interface Web et sur la centrale d'alarme.</p> <p>Appuyez sur la touche d'un médaillon.</p> <p>L'écran affiche</p> <ul style="list-style-type: none">à quel utilisateur est assigné cet émetteur d'appel d'urgencela fonction exécutée par cet émetteur d'appel d'urgence AA = alarme agression Médical = appel médical d'urgence Alarme ASS = appel soins de santéla puissance du signal reçu (RSSI) <p>Exemple</p> <p>Utilisateur : Utilisateur 002 Fonc : Médical RSSI : 9</p>
TS Reporting	<p>Le test de la fonction TS Reporting s'effectue de la même manière dans l'interface Web et sur la centrale d'alarme.</p> <p>TS Reporting doit être activé et les contacts doivent être enregistrés dans le répertoire téléphonique.</p> <p>Mode installateur->Transmission->TS Reporting ->Mode appel ->Simple (ou altern.)</p> <p>La liste des voies de transmission raccordées disponibles s'affiche :</p> <p>Ethernet, Ethernet/Mobile IP</p> <ul style="list-style-type: none">Après la sélection, les 2 destinataires programmés possibles (destinataire IP 1, destinataire IP 2) s'affichent avec le nom de contact depuis le répertoire téléphonique enregistré.Défilez jusqu'au contact souhaité. Appuyez sur la touche « Sélectionner » ou « Démarrer » dans l'interface Web.La centrale envoie un appel test à ce destinataire.L'événement test est transmis selon le protocole défini. <p>RTC</p> <ul style="list-style-type: none">Après la sélection, les 2 destinataires programmés possibles (destinataire tél. 1, destinataire tél. 2) s'affichent avec le nom de contact depuis le répertoire téléphonique enregistré.Défilez jusqu'au contact souhaité. Appuyez sur la touche « Sélectionner » ou « Démarrer » dans l'interface Web.La centrale envoie un appel test à ce destinataire.L'événement test est transmis selon le protocole défini. <p>GSM/Mobile</p> <ul style="list-style-type: none">Après la sélection, les 2 destinataires programmés possibles (destinataire tél. 1, destinataire tél. 2) s'affichent avec le nom de contact depuis le répertoire téléphonique enregistré.Défilez jusqu'au contact souhaité. Appuyez sur la touche « Sélectionner » ou « Démarrer » dans l'interface Web.La centrale envoie un appel test à ce destinataire.L'événement test est transmis selon le protocole défini. <p>Pendant l'appel test, l'écran affiche une suite de messages de progression.</p> <p>Si l'appel test a échoué, l'écran affiche un message court précisant la cause de l'erreur.</p>

Fonction	Signification
Appel d'urgence de soin	<p>Le test de la fonction Urgence de soin s'effectue de la même manière dans l'interface Web et sur la centrale d'alarme.</p> <p>L'urgence de soin doit être activée et les contacts doivent être enregistrés dans le répertoire téléphonique.</p> <p>Mode installateur->Transmission->TS Reporting ->Mode appel ->Simple (ou altern.)</p> <p>La liste des voies de transmission raccordées disponibles s'affiche :</p> <p>RTC</p> <ul style="list-style-type: none"> • Après la sélection, les 2 destinataires programmés possibles (destinataire tél. 1, destinataire tél. 2) s'affichent avec le nom de contact depuis le répertoire téléphonique enregistré. • Défilez jusqu'au contact souhaité. Appuyez sur la touche « Sélectionner » ou « Démarrer » dans l'interface Web. • La centrale envoie un appel test à ce destinataire. • L'événement test est transmis selon le protocole défini. <p>GSM/Mobile</p> <ul style="list-style-type: none"> • Après la sélection, les 2 destinataires programmés possibles (destinataire tél. 1, destinataire tél. 2) s'affichent avec le nom de contact depuis le répertoire téléphonique enregistré. • Défilez jusqu'au contact souhaité. Appuyez sur la touche « Sélectionner » ou « Démarrer » dans l'interface Web. • La centrale envoie un appel test à ce destinataire. • L'événement test est transmis selon le protocole défini. <p>Pendant l'appel test, l'écran affiche une suite de messages de progression.</p> <p>Si l'appel test a échoué, l'écran affiche un message court précisant la cause de l'erreur.</p>

Fonction	Signification
Transmetteur vocal	<p>Le transmetteur vocal doit être activé. Mode installateur->Transmission->Transmetteur vocal->Mode d'appel ->Autorisé</p> <p>La liste des voies de transmission raccordées disponibles s'affiche</p> <p>Ethernet</p> <ul style="list-style-type: none">Après la sélection, entrez un ID Utilisateur SIP valide.Par ex. +498207123456789@sipgate.deAppuyez sur la touche "OK".La centrale d'alarme établit une connexion avec ce raccordement. Si l'appel est accepté par ce destinataire, celui-ci entend le "Message principal" et le "Message 1" jusqu'au "Message 4". <p>Version logicielle >=2.00.00</p> <ul style="list-style-type: none">Après la sélection, les destinataires programmés s'affichent avec le nom de contact depuis le répertoire téléphonique enregistré.Défilez jusqu'au contact souhaité. Appuyez sur la touche « Sélectionner » ou « Démarrer » dans l'interface Web.La centrale envoie un appel test à ce destinataire. <p>RTC</p> <ul style="list-style-type: none">Après cette sélection, entrez un numéro d'appel.Appuyez sur la touche "OK".La centrale d'alarme établit une connexion avec ce raccordement. Si l'appel est accepté par ce destinataire, celui-ci entend le "Message principal" et le "Message 1" jusqu'au "Message 4". <p>Version logicielle >=2.00.00</p> <ul style="list-style-type: none">Après la sélection, les destinataires programmés s'affichent avec le nom de contact depuis le répertoire téléphonique enregistré.Défilez jusqu'au contact souhaité. Appuyez sur la touche « Sélectionner » ou « Démarrer » dans l'interface Web.La centrale envoie un appel test à ce destinataire. <p>GSM/Mobile</p> <ul style="list-style-type: none">Après cette sélection, entrez un numéro d'appel.Appuyez sur la touche "OK".La centrale d'alarme établit une connexion avec ce raccordement. Si l'appel est accepté par ce destinataire, celui-ci entend le "Message principal" et le "Message 1" jusqu'au "Message 4". <p>Version logicielle >=2.00.00</p> <ul style="list-style-type: none">Après la sélection, les destinataires programmés s'affichent avec le nom de contact depuis le répertoire téléphonique enregistré.Défilez jusqu'au contact souhaité. Appuyez sur la touche « Sélectionner » ou « Démarrer » dans l'interface Web.La centrale envoie un appel test à ce destinataire. <p>Si l'acquiescement d'appel est activé :</p> <ul style="list-style-type: none">La sélection de Mode installateur->Transmission->Transmetteur vocal->Acquiescement d'appel ->Autorisé permet au destinataire d'acquiescer et de terminer l'appel avec 5 ou 9.Pendant l'appel test, l'écran affiche une suite de messages de progression. <p>Si l'appel test a échoué, l'écran affiche un message court précisant la cause de l'erreur.</p>
SMS	<p>Les SMS doivent être activés et les contacts doivent être enregistrés dans le répertoire téléphonique : Mode installateur->Transmission->SMS->Mode d'appel ->Autorisé</p>

La liste des voies de transmission raccordées disponibles s'affiche :

RTC

- Après la sélection, les destinataires programmés possibles s'affichent avec le nom de contact depuis le répertoire téléphonique enregistré.
- Défilez jusqu'au contact souhaité. Appuyez sur la touche « Sélectionner » ou « Démarrer » dans l'interface Web.
- La centrale d'alarme envoie un SMS test à ce destinataire.

GSM/Mobile

- Après la sélection, les destinataires programmés possibles s'affichent avec le nom de contact depuis le répertoire téléphonique enregistré.
- Défilez jusqu'au contact souhaité. Appuyez sur la touche « Sélectionner » ou « Démarrer » dans l'interface Web.
- La centrale d'alarme envoie un SMS test à ce destinataire.
- Le destinataire reçoit un SMS sous la forme suivante :
<Message principal> : 10:56 21/01/2015 Appel de test SMS
- Pendant l'appel test, l'écran affiche une suite de messages de progression.
- Si l'appel test a échoué, l'écran affiche un message court précisant la cause de l'erreur.

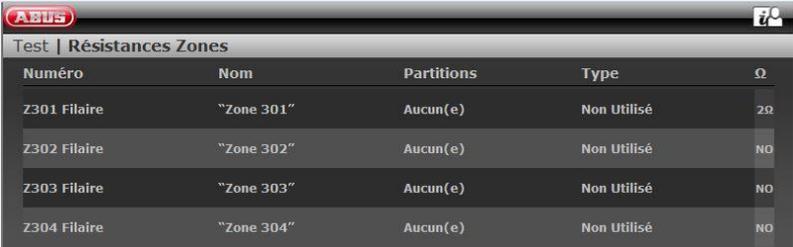
E-mail

L'e-mail doit être activé et les contacts doivent être enregistrés dans le répertoire téléphonique :
Mode installateur->Transmission->E-mail->Mode d'appel ->Autorisé

La liste des voies de transmission raccordées disponibles s'affiche (uniquement sur l'interface Web) :

Ethernet, Ethernet/Mobile IP

- Après la sélection, les destinataires programmés possibles s'affichent avec le nom de contact depuis le répertoire téléphonique enregistré.
- Défilez jusqu'au contact souhaité. Appuyez sur la touche « Sélectionner » ou « Démarrer » dans l'interface Web.
- La centrale d'alarme envoie un e-mail à ce destinataire.
- Le destinataire reçoit un e-mail sous la forme suivante :
Objet :
 <Message principal> : E-mail de test appel
Texte :
 <Message principal> :
 11:09 21/01/2015 E-mail de test
- Pendant l'appel test, l'écran affiche une suite de messages de progression.
Si l'appel test a échoué, l'écran affiche un message court précisant la cause de l'erreur.

Fonction	Signification
Résistances zones	<p>Les valeurs de résistance actuelles des zones filaires (centrale et modules hybrides) s'affichent ici.</p> <p>Affichage sur la centrale d'alarme :</p> <p>Les noms de zone s'affichent. Pour voir les numéros de zone, appuyez sur la touche de menu droite.</p> <p>Testez ici toutes les variantes selon le type de câblage pour savoir si elles répondent aux exigences :</p> <ul style="list-style-type: none"> • Contact d'alarme ouvert / fermé • Contact anti-sabotage ouvert / fermé • Courts-circuits • (Circuits électriques coupés) ouverts <p>0k00 correspond à 0 ohm ou NC</p>  <p>Remarque</p> <p>Type de câblage « 4 fils NC »</p> <p>Centrale</p> <p>L'affichage alterne entre résistance circuit d'alarme (A) et résistance circuit anti-sabotage (S).</p> <p>INTERFACE WEB</p> <p>Vous voyez ici simultanément les deux valeurs dans le champ, la résistance circuit d'alarme (A) et la résistance circuit anti-sabotage (S).</p> <p>Exemple pour une zone "2 fils FSL 2K2/4K7"</p> <ul style="list-style-type: none"> • Contact d'alarme fermé (repos) 2k18 • Contact d'alarme ouvert 6k89 • Contact d'alarme ouvert et résistance de série court-circuitée 4k68 • Court-circuit dans le câble vers les détecteurs 0k00 • Coupure de câble NO
PSU centrale	<p>Vous obtenez ici des informations sur les valeurs de tension de l'alimentation électrique. L'affichage est le même sur la centrale d'alarme et dans l'interface Web :</p> <p>Tension d'entrée CC extérieure</p> <ul style="list-style-type: none"> • La valeur de tension de la source de tension continue externe. <p>Batt. centrale d'alarme 1</p> <ul style="list-style-type: none"> • La valeur de tension de la première batterie <p>Batt. centrale 2</p> <ul style="list-style-type: none"> • La valeur de tension de la seconde batterie <p>Aux. tension out</p> <ul style="list-style-type: none"> • La valeur de tension sur le raccordement de borne 0V / 12V AUX <p>Exemple (Dans cet exemple, la batterie 2 n'est pas raccordée)</p>

- Tension d'entrée CC extérieure 14,1 V
- Batt. centrale d'alarme 1 8,3 V
- Batt. centrale d'alarme 2 0,1 V
- Aux. tension out 13,9 V

PSU MoHy Vous voyez ici la valeur de tension de la source de tension continue externe au niveau du raccordement de borne 0 V/12 V IN du module hybride.

Interface Web :



The screenshot shows the ABUS web interface with a table titled "Test | HyMo PSU". The table has five columns: "Nummer", "Name", "Teilbereiche", "Lautsprecher Teilbereiche", and "DC Spannung".

Nummer	Name	Teilbereiche	Lautsprecher Teilbereiche	DC Spannung
HyMo 1	"HyMo 1"	3	1-4	13.6V
HyMo 2	"HyMo 2"	1	1-4	13.7V

Vous obtenez ici des informations supplémentaires sur

Numéro

le numéro interne au sein du logiciel de la centrale

Nom

le nom unique choisi pour ce module hybride

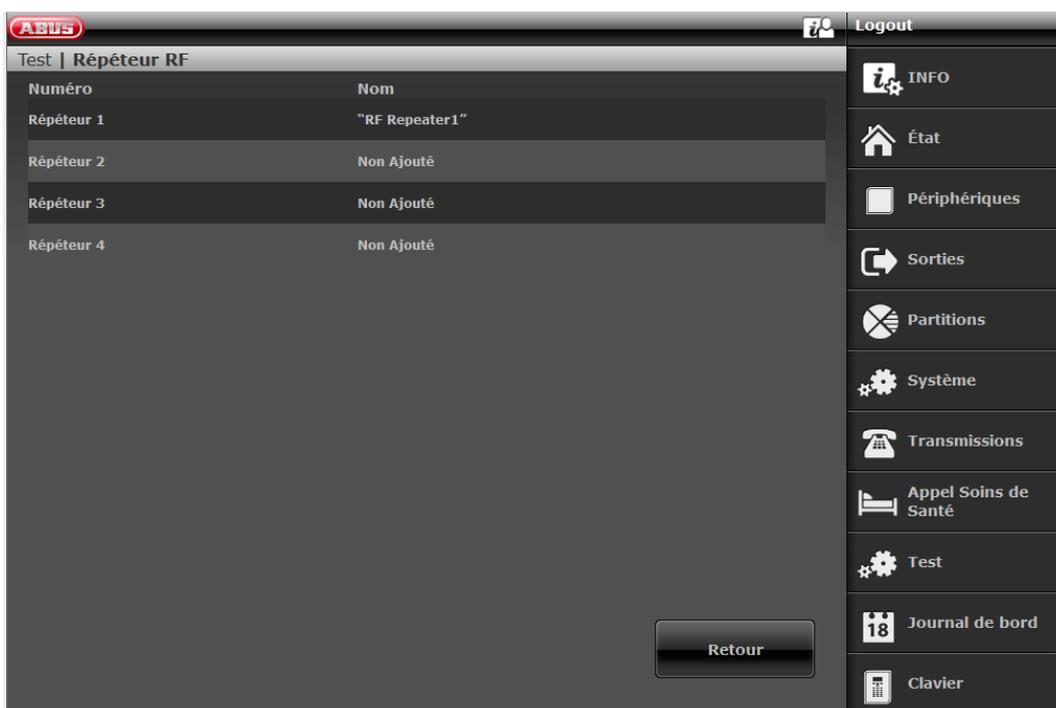
Partitions

les numéros des partitions auxquelles est assigné le module hybride

Partitions haut-parleur

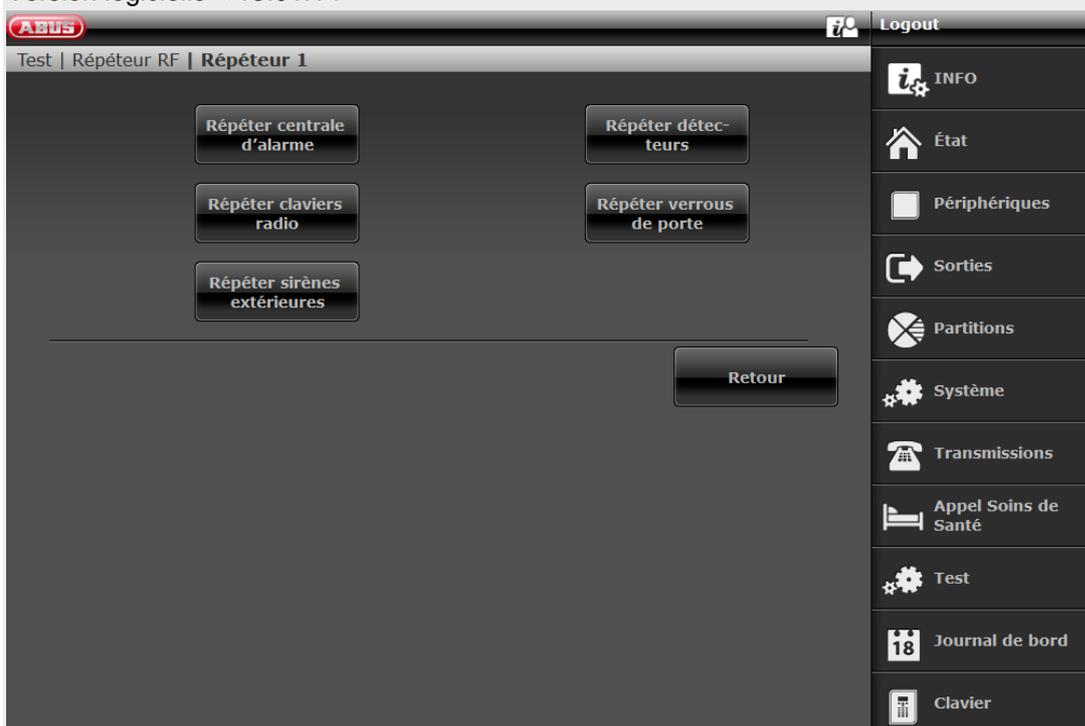
les partitions pour lesquelles le haut-parleur raccordé en option émet des signaux

Répéteur RF Vous obtenez ici des informations sur les puissances de signal des périphériques sur le répéteur. Il s'agit de la puissance de signal sur le répéteur des messages reçus des périphériques. L'affichage est le même sur la centrale d'alarme et dans l'interface Web.

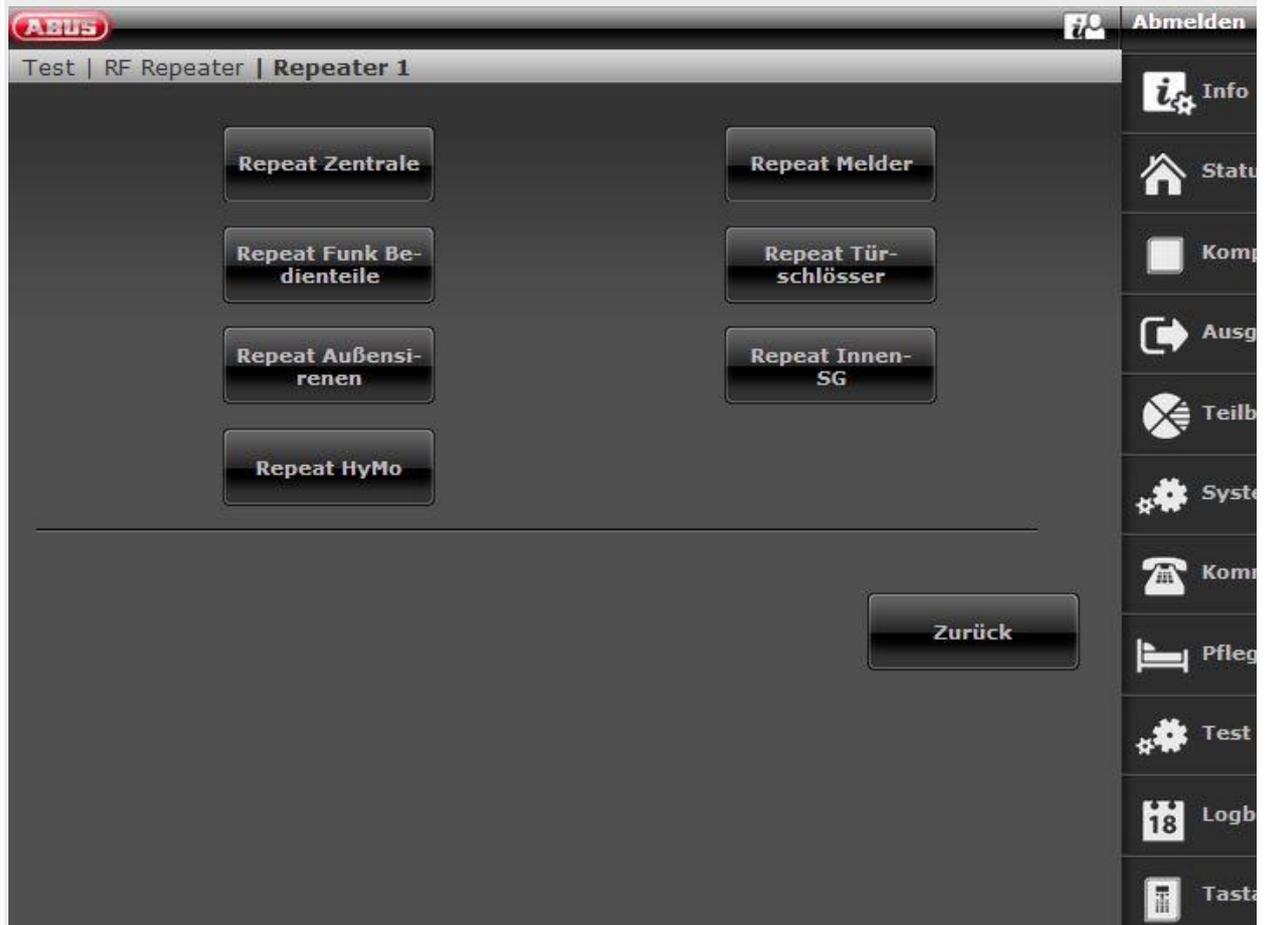


Cliquez sur la ligne du répéteur souhaité. Le message suivant s'affiche ensuite :

Version logicielle < v3.01.14



Version logicielle >= v3.01.14



Cliquez sur le type de périphérique souhaité. Vous trouverez ci-dessus des détails sur l'affichage de la puissance du signal dans Test -> Puissances de signal.

Répéter centrale d'alarme

Vous trouvez ici 2 affichages.

Répéteur RF

Il s'agit de la puissance du signal du répéteur sur la centrale d'alarme.

Répéter centrale d'alarme

Il s'agit de la puissance du signal de la centrale d'alarme sur le répéteur.



Remarque

Les deux puissances de signal sont similaires. Les puissances de signal Centrale d'alarme->Répéteur et Répéteur->Centrale d'alarme peuvent cependant être légèrement différentes. Les causes sont les suivantes :

- des structures d'antennes différentes pour la centrale d'alarme et le répéteur ;
- des conditions de propagation des ondes radio différentes dans la direction correspondante.

The screenshot shows the ABUS configuration interface. At the top, there is a navigation bar with the ABUS logo, a user icon, and a 'Logout' button. Below the navigation bar, the breadcrumb trail reads 'Test | Répéteur RF | Répéteur 1 | Puissance du signal'. The main content area displays a table with two rows of data:

Numéro	Nom	Puissance du signal
Répéteur RF		9(9)
Répéter centrale d'alarme		-(-)

Below the table is a 'Retour' button. On the right side, there is a vertical menu with the following items: INFO, État, Périphériques, Sorties, Partitions, Système, Transmissions, Appel Soins de Santé, Test, Journal de bord, and Clavier.

Répéter détecteurs

Vous trouvez ici les puissances de signal des messages reçus sur le répéteur des **détecteurs**.

The screenshot shows the ABUS configuration interface. At the top, there is a navigation bar with the ABUS logo, a user icon, and a 'Logout' button. Below the navigation bar, the breadcrumb trail reads 'Test | Répéteur RF | Répéteur 1 | Zones'. The main content area displays a table with one row of data:

Numéro	Nom	Puissance du signal
Zone 201	"Zone 201"	9(9)

Below the table is a 'Retour' button. On the right side, there is a vertical menu with the following items: INFO, État, Périphériques, Sorties, Partitions, Système, Transmissions, Appel Soins de Santé, Test, Journal de bord, and Clavier.

Répéter claviers de commande sans fil

Vous trouvez ici les puissances de signal des messages reçus sur le répéteur des **claviers de commande sans fil**.

Répéter verrous de porte

Vous trouvez ici les puissances de signal des messages reçus sur le répéteur des **verrous de porte**.

Répéter sirènes d'extérieur

Vous trouvez ici les puissances de signal des messages reçus sur le répéteur des **sirènes d'extérieur**.

Répéter générateur de signal int.

Vous trouvez ici les puissances de signal des messages reçus sur le répéteur des **générateurs de signal intérieurs**.

Répéter MoHy

Vous trouvez ici les puissances de signal des messages reçus sur le répéteur des **modules hybrides**.

Historique

Version logicielle <= v2.01.08

ABUS  Logout

Journal de bord

Date	Heure	
04/01/2014	21:01:04	U000 Login(9999)
04/01/2014	21:01:04	U000 Présent (Web)(9999)
04/01/2014	20:18:29	U000 Logout(9999)
04/01/2014	20:18:29	U000 Absent (Web)(9999)
04/01/2014	18:59:03	U000 Login(9999)
04/01/2014	18:59:03	U000 Présent (Web)(9999)
04/01/2014	03:43:15	U000 Logout(9999)
04/01/2014	03:43:15	U000 Absent (Web)(9999)
04/01/2014	01:41:16	U000 Login(9999)
04/01/2014	01:41:16	U000 Présent (Web)(9999)

Navigation:   **1**      

-  INFO
-  État
-  Périphériques
-  Sorties
-  Partitions
-  Système
-  Transmissions
-  Appel Soins de Santé
-  **18** Journal de bord
-  Clavier

Version logicielle >= v3.00.03

The screenshot shows the ABUS software interface. At the top left is the ABUS logo. The main area is titled 'Logbuch' and contains a table of events. Below the table are buttons for 'Speichern' and 'Drucken'. At the bottom of the table are navigation buttons (back, home, 1-5, forward). On the right side, there is a sidebar menu with options: Abmelden, Info, Status, Komponenten, Ausgänge, Teilbereiche, System, Kommunikation, Pflegenotruf, Test, Logbuch (highlighted with a calendar icon showing '18'), and Tastatur.

Datum	Zeit	
14/11/2017	13:28:32	B000 Einstellung geändert(2419)
14/11/2017	13:20:05	Ben 000 Log in(2419)
14/11/2017	13:20:05	Ben000 Log in (Web)(2419)
14/11/2017	13:04:47	Ben 000 Log out(2419)
14/11/2017	13:04:37	B000 Einstellung geändert(2419)
14/11/2017	13:03:55	Ben 000 Log in(2419)
14/11/2017	13:00:38	Ben 000 Log out(2419)
14/11/2017	13:00:38	Ben 000 TB 1 rückgesetzt(2419)
14/11/2017	13:00:38	B000 Einstellung geändert(2419)
14/11/2017	13:00:33	Codes zurückgesetzt

Dans ce menu, vous pouvez consulter le « journal des événements ».

Le journal des événements contient toutes les données, accompagnées de la date et de l'heure, concernant la centrale d'alarme.

La mémoire peut contenir jusqu'à 600 entrées.

Si elle est pleine, l'événement le plus ancien est supprimé et remplacé par la nouvelle entrée (« principe FiFo » : First in – First out, premier entré, premier sorti).

Dans l'annexe, vous trouverez une vue d'ensemble des entrées de journal possibles.

Bouton « Enregistrer » (version logicielle >= v3.00.03)

Appuyez sur le bouton « Enregistrer » pour enregistrer le journal. La boîte de dialogue Windows par défaut « Ouvrir/Enregistrer » s'ouvre. Sélectionnez « Ouvrir avec » ou « Enregistrer le fichier ».

Le nom de fichier par défaut est « log.csv ».



Remarque

Pour ouvrir et modifier un fichier « log.csv », nous vous recommandons d'utiliser MS Excel.

Pour convertir un fichier « .csv » (comma separated values) en un fichier « .xlsx », procédez comme suit :

Marquez ligne 5/colonne A à ligne x/colonne A.

Cliquez sur l'onglet **Données** dans le groupe **Outils de données**, puis sur **Texte des colonnes**.

Suivez les instructions de l'assistant de conversion de texte pour définir la répartition du texte dans les colonnes.

Enregistrez le fichier au format « .xlsx ».

Vous avez maintenant un fichier à 3 colonnes pour une recherche et lisibilité optimisées des données.

Bouton « Impression » (version logicielle >= v3.00.03)

Appuyez sur le bouton « Impression » pour imprimer le journal. La boîte de dialogue Windows par défaut « Impression » s'ouvre. Sélectionnez l'imprimante souhaitée.



Remarque

Le choix de l'imprimante se porte sur celles raccordées à l'ordinateur.

Par ex. « vraie » imprimante papier ou « imprimante PDF » telle que PDF-Xchange, Freepdf.



Remarque

Lors de l'enregistrement ou de l'impression, toutes les entrées de stockage sont exportées, de la page actuellement sélectionnée jusqu'à la dernière page.

Exemple :

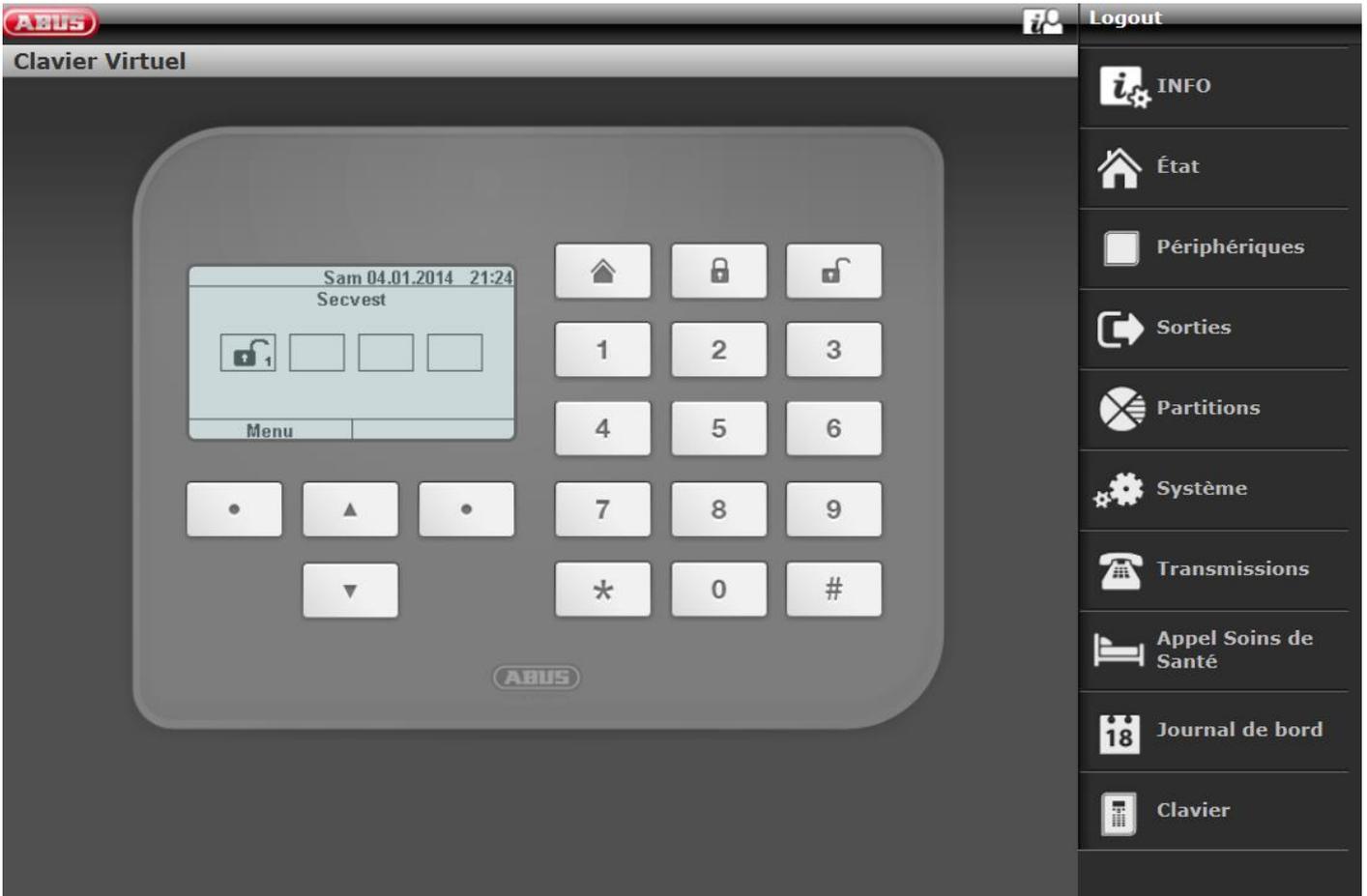
Le journal possède actuellement 51 pages de 10 lignes chacune. Vous avez sélectionné la page 41. Lors de l'enregistrement ou de l'impression, seul le contenu des pages 41 à 51 est exporté. Vous obtenez ensuite ces 100 unités de stockage (100 lignes) dans les fichiers respectifs.

Les 4 premières lignes contiennent des informations sur la centrale. Les lignes suivantes comportent le contenu du journal.

Exemple :

```
ABUS Secvest, (texte écran)
Secvest 3.01.11,
heure de la centrale 11:39, date : 08/11/2018,
Le système est configuré en tant que : Partitions,
08/11/2018,10:45:19,Util. 000 Connexion (2925)
08/11/2018,10:45:19,Util. 000 Connexion
(Web)(2925)
08/11/2018,10:45:09,Util. 000 Déconnexion (2925)
...
...
...
```

Clavier virtuel



Le clavier virtuel regroupe toutes les fonctions du clavier et de l'écran de la centrale d'alarme.

Sur la centrale d'alarme, vous appuyez sur les touches correspondantes.

Sur le clavier virtuel, vous cliquez sur les touches correspondantes.

Les affichages de l'écran virtuel correspondent également à ceux de l'écran de la centrale.

Veillez noter :

Si vous vous êtes connecté au serveur Web en tant qu'installateur, vous pouvez accéder au clavier virtuel après avoir saisi un code installateur en mode installateur.

Si vous vous êtes connecté au serveur Web en tant qu'utilisateur/administrateur, vous pouvez accéder au clavier virtuel après avoir saisi un code utilisateur dans le menu utilisateur.

Annexe

Caractéristiques techniques

Généralités

Nom du produit	Secvest
Description du produit	Système d'alarme sans fil
Fabricant	ABUS Security-Center GmbH & Co. KG Linker Kreuthweg 5 86444 Affing ALLEMAGNE
Classe d'environnement	II (EN 50131-1 + A1:2009 §7, EN 50131-3:2009 §7)
Indice de protection, type de protection IP	IP30 (intérieur, à l'état monté) IP = International Protection ou Ingress Protection (protection contre les corps étrangers) 3 = Protection contre les corps étrangers : protection contre les corps étrangers solides de diamètre > 2,5 mm Protection contre le contact : protection contre l'accès avec un outil et contre des fils Ø > 2,5 mm 0 = Protection contre l'infiltration d'eau : pas de protection
Température de fonctionnement	0 °C à 40 °C
Température de stockage	0 °C à 40 °C
Humidité de l'air, max.	Humidité relative moyenne d'env. 75 % sans condensation
Matériau du boîtier	ABS
Dimensions (L x H x P)	205 x 285 x 48 mm
Poids	1 453 g (sans batteries) 1 543 g (avec une batterie) Poids d'une batterie seule : 90 g
Généralités	Ce produit doit être installé, entretenu et maintenu par un technicien de service qualifié. Les travaux de nettoyage extérieurs peuvent être exécutés par l'utilisateur.

Capacité

Zones	
Zones IP	3 6 (version logicielle 1.01.00 et supérieures) modèles de caméra ABUS définis, voir annexe sur les instructions d'installation « Équipement compatible »
Zones sans fil	48
Zones filaires	4 (2 fils RFL/DEOL ou 2 fils NC) 2 (4 fils NC)
Claviers de commande sans fil	8
Sirènes d'extérieur	
Sirènes sans fil	4
Sirènes filaires	1
Générateur de signal intérieur	4
Modules d'informations/Sirènes d'intérieur	∞
WAM	8
Verrous de porte	8

Répéteur RF	4
Nombre de composants par répéteur	10 Les télécommandes et les émetteurs d'appel d'urgence (agression, médical, soin) sont toujours répétés.
Sorties	
Sorties IP	0
Sorties sans fil	32
Sorties filaires	4
Sorties mixtes	10
Partitions	4 (chacune avec l'option Act. interne)
Utilisateur	50
Noms d'utilisateur	50 (+ nom de l'installateur)
Codes utilisateur	50 (+ code de l'installateur)
Badges Proximity (clés électroniques)	50 (un par utilisateur)
Télécommandes	50 (une ou plusieurs par utilisateur)
Émetteur d'alarme panique	50 (un par utilisateur)
Émetteur d'appel d'urgence médicale	50 (un par utilisateur)
Émetteur d'appel d'urgence pour soins	50 (un par utilisateur)
Répertoire téléphonique	12 contacts Nom Partitions 1-4 Voix/SMS/E-mail – Désactivation, Activation, Act. interne 2 n° tél. 1 adresse e-mail 1 adresse IP 1 identifiant VoIP/SIP
Calendrier Arm./Désarm.	160 événements 20 exceptions
Capacité de l'historique	Jusqu'à 600 événements 500 événements prioritaires 100 événements non prioritaires Sauvegarde dans la mémoire EEPROM (mémoire non volatile, non-volatile memory - NVM), disponible pendant au moins 10 ans sans alimentation électrique. L'intégralité de l'historique sauvegarde ses enregistrements pendant au moins 10 ans sans alimentation électrique. Remarque : l'historique est protégé et ne peut pas être supprimé par un installateur, un administrateur ou un utilisateur normal.
Horloge interne	1 Commandée par quartz et synchronisation temporelle via un serveur de temps (synchronisation temporelle SNTP) Précision, lorsque la centrale n'utilise pas de synchronisation temporelle via un serveur de temps : ± 5 minutes sur un an @ 20 °C de température nominale < ± 10 minutes sur un an @ 20 °C de température nominale selon EN 50131-1 chapitre 8.10
Haut-parleur	1
Microphone	1
Messages vocaux	33 messages vocaux pour chaque langue installée dans la centrale 5 messages enregistrés par l'utilisateur (transmetteur vocal du mode installateur)

	<p>Message de localisation de 12 s 8 s pour chaque message 1-4</p> <p>1 mémo (menu utilisateur) 30 s</p> <p>58/56 noms de zones (menu utilisateur) 2 s pour chaque zone 6 zones IP 48 zones sans fil 4/2 zones filaires</p>
Sirène interne	1 (sirène ou avertisseur piezo intégré) Pression acoustique > 96 dB(A) @ 1 m
Modules de communication, enfichables	1
Ports	1x Ethernet 1x a/b 1x USB 1x SD-Card, carte SD
Batteries de secours	2
Écran	3,5", surface efficace 84 mm x 45 mm, LCD 240 x 128 pixels monochromes (niveau de gris), rétroéclairage blanc

Protection et sécurité

Degré de sécurité	niveau 2 (EN 50131-1 + A1:2009 §6, EN 50131-3:2009 §6)
Classe d'environnement	II (EN 50131-1 + A1:2009)
Sécurité anti-sabotage (détection/protection)	Type B (EN 50131-3:2009 §8.7)
Composants sans fil, distinction	16,777,214 ($2^{24} - 2$) ID différents par type de périphérique
Surveillance sans fil	Programmable
Codes d'accès	Il n'y a aucun code utilisateur réglé en usine. Il n'y a aucun code administrateur réglé en usine. Version logicielle $\leq 1.01.00$ Le code par défaut (utilisateur administrateur : 1234 ou 123456) doit impérativement être modifié au cours de l'installation.
Nombre de codes d'accès	50 + un code installateur
Distinction entre les codes d'accès	10 000 variantes de codes à 4 chiffres (0000-9999) Chaque chiffre de code est un nombre compris entre 0 et 9. $10^4 = 10 \times 10 \times 10 \times 10 = 10\,000$ (combinaisons différentes)
	1 000 000 variantes de codes à 6 chiffres (000000-999999) Chaque chiffre de code est un nombre compris entre 0 et 9. $10^6 = 10 \times 10 \times 10 \times 10 \times 10 \times 10 = 1\,000\,000$ (combinaisons différentes)
Nombre de badges de proximité (badges)	50
Distinction entre les badges Proximity	4,294,967,296 (2^{32} , 2^{32})

Autorisation temporaire d'accès utilisateur	Aucune possibilité n'a été prévue pour une mise à disposition d'une autorisation temporaire (par ex. code PIN ou badge Proximity valable uniquement pendant une durée limitée ou pour un certain nombre de fois).														
Blocage d'accès/du code	Le clavier est bloqué pendant 5 minutes après 3 codes erronés d'affilée. Le clavier est bloqué pendant 5 minutes après 3 badges Proximity d'affilée.														
Clés mécaniques															
Claviers de commande															
Interrupteur à clé sans fil	FUBE50061, FUBE50060, FU8165														
Distinction entre les clés mécaniques	30,000														
Verrous de porte															
Verrou de porte supplémentaire	FUFT5001x-2x, 7010E 7025E														
Distinction entre les clés mécaniques	30,000														
Cylindre sans fil Secvest Key	FUSK53030-58080, FUBE5XXXX														
Distinction entre les clés mécaniques	789.024														
Longueur du nom d'utilisateur Web	12 chiffres														
Distinction entre les noms d'utilisateur Web	88 ¹² (215 671 155 821 681 003 462 656, 88 ¹² , >1 000 000) Tous les chiffres peuvent être des caractères alphanumériques et des caractères spéciaux.														
	<table border="1"> <tr> <td>A-Z</td> <td>26</td> </tr> <tr> <td>a-z</td> <td>26</td> </tr> <tr> <td>0-9</td> <td>10</td> </tr> <tr> <td>Espace Apostrophe ():.-!&@+_*#</td> <td>14</td> </tr> <tr> <td>Æ Å Ä Ø Ö Ü (majuscule)</td> <td>6</td> </tr> <tr> <td>æ å ä ø ö ü (minuscule)</td> <td>6</td> </tr> <tr> <td></td> <td>88 Σ</td> </tr> </table>	A-Z	26	a-z	26	0-9	10	Espace Apostrophe ():.-!&@+_*#	14	Æ Å Ä Ø Ö Ü (majuscule)	6	æ å ä ø ö ü (minuscule)	6		88 Σ
A-Z	26														
a-z	26														
0-9	10														
Espace Apostrophe ():.-!&@+_*#	14														
Æ Å Ä Ø Ö Ü (majuscule)	6														
æ å ä ø ö ü (minuscule)	6														
	88 Σ														
Cryptage Web	HTTPS TLS 1.2 < 2.0.0 : Algorithme de signature : SHA1 >= 2.0.0 : Algorithme de signature : SHA256 (SHA 2) > 3.01.01 : mbedTLS library V2.6.0														
Compatibilité électromagnétique Résistance électromagnétique	Conforme à EN 50130-4														
Compatibilité électromagnétique Émissions parasites électromagnétiques	Conforme à EN 61000-6-3														
Sécurité électrique	Conforme à EN 60950-1														

Alimentation électrique

Type d'alimentation électrique	Type A selon EN 50131-1:2006+A1:2009 §9 et EN 50131-6:2008+A1:2014 §4.1 Secvest contient un bloc d'alimentation intégré (type A). Ce bloc d'alimentation délivre des tensions internes différentes sur les circuits imprimés pour alimenter le circuit en électricité. Au niveau de la sortie AUX 0 V/12 V, ce bloc d'alimentation délivre une tension de 13,8 V avec une intensité max. de 600 mA.
Alimentation/fréquence de service	110 V/230 V CA, 50/60 Hz, (85-265 V CA, 50/60 Hz) 13,8 V CC (13,0-14,5 V CC)
Puissance absorbée / consommation d'énergie maximales	I CA MAX : 430 mA rms @ 85 V CA 190 mA rms @ 230 V CA 170 mA rms @ 265 V CA
Puissance absorbée/consommation d'énergie nominales	6,9 W 6,9 W x 24 x 365 = 60 kWh par an 55 mA rms @ 230 V CA (défini avec 200 mA de charge auxiliaire et batteries complètement chargées) 300 mA @ 13,8 V
Défaut entrée Ext CC si	12,5 V OK si 12,7 V
PSU externe	13,0-14,5 V CC, au moins 1,7 A
Consommations électriques typiques	Veille centrale : 100 mA Rétroéclairage désactivé Rétroéclairage : Élevé : 100 mA Moyen : 40 mA Faible : 15 mA Sirène interne dans l'alarme et volume max. : +70 mA GSM/Mobile veille : +15 mA @ 12 VCC GSM/Mobile activé : +240 mA @ 12 VCC Courant de charge par batterie : 220 mA
Alimentation de secours	
Batterie	Lithium-ion polymère, 7,4 V
Capacité	2 500 mAh, 18,5 Wh
Durée minimale en mode de secours (temps de veille)	plus de 12 heures plus de 24 heures avec deuxième batterie en option
Durée de recharge maximale	moins de 72 heures selon EN 50131-1:2006+A1:2009 §9 tableau 24
Durée maximale pour recharger la batterie à 80 %	24 heures
Valeur seuil de sous-tension de la batterie	7,2 V Défaut « Batterie vide » si < 7,2 V
Protection contre la décharge profonde si	6 +/- 0,2 V
Sortie de l'alimentation électrique auxiliaire	I max. 700 mA (problème ACCI principal < 7) I max. 600 mA (problème ACCI principal >= 7) Fonctionnement avec raccordement au réseau électrique (85-265 V CA, 50/60 Hz)

	<p>13,9 V max, attente 13,4 V min, pleine charge (@ 600 mA)</p> <p>Fonctionnement avec entrée CC @ 13,0 V 12,8 V max, attente 12,2 V min, pleine charge (@ 600 mA)</p> <p>@ 13,8 V 13,6 V max, attente 13,0 V min, pleine charge (@ 600 mA)</p> <p>@ 14,5 V 14,3 V max, attente 13,7 V min, pleine charge (@ 600 mA)</p> <p></p> <p>Remarque En cas de coupure de courant, cette sortie n'est pas sauvegardée par la batterie. En cas de coupure de courant, la tension de sortie est de 0 V.</p>
Défaut sortie de l'alimentation électrique auxiliaire si	11,5 V OK si 12,0 V
Protection contre la surtension Tension de déclenchement	Aucune entrée au niveau 2
Surveillance PSU	La surveillance couvre les défauts CA et CC externe. Cela entraîne une notification du défaut CA ou du défaut CC externe à la centrale lorsque l'alimentation électrique est perturbée ou coupée. La centrale continue alors de fonctionner sur batterie, mais la centrale et l'utilisateur en sont informés. La surveillance comprend la sous-tension de la batterie Lorsque la batterie est vide, la centrale et l'utilisateur en sont informés et la centrale envoie un message d'avertissement.

Sécurités

Sécurité réseau (entrée CA)	Coupe-circuit (fusible) remplaçable
Désignation	T1AL250V
Caractéristique	T = inerte
Courant nominal	1 A
Capacité de coupure	L = faible
Tension nominale	250 V
Structure	Tube de verre 5 x 20 mm

Transmission de signaux sans fil

Fréquence de fonctionnement	868,6625 MHz
	Conformité aux normes : EN 50131-5-3 Grade 2 EN 300 220-1 V.2.1.1 EN 300 220-2 V.2.1.1 EN 300 220-3 V.1.1.1
	Fréquence réservée aux applications de sécurité
Modulation	FM
Largeur de bande	+/- 10 kHz Bas débit, espacement entre canaux 25 kHz
Puissance d'émission	Max. 10 mW
Sensibilité	env. -110 dBm
Rapport signal/bruit	12 dB
Antenne	Technologie d'antennes duplex intégrée
Portée	Intérieur : env. 30 m Dépend des conditions ambiantes Extérieur : env. 100 m
Caractéristiques particulières	Identification individuelle Contrôle de supervision Détection brouillage

Lecteur de jour de badges Proximity RFID

Système	Mifare Classic
Fréquence de fonctionnement	13,56 MHz
Puissance d'émission	Max. 55 mW
	Conformité aux normes : EN 300 330-2
Caractéristiques particulières	Identification individuelle

Raccordements

L  N	<p>Connexion réseau 110 V/230 V CA, 50/60 Hz, (85-265 V CA, 50/60 Hz) L – Phase (noir ou marron)  – Conducteur de protection (jaune/vert) N – Conducteur neutre (bleu)</p>
- CC IN + 13,8 V	<p>Entrée PSU externe 13,8 V CC, PSU externe d'au moins 1,7 A Voir section « Alimentation électrique » pour plus de détails</p>
0 V 12 V AUX	<p>Sortie de tension 13,8 V CC jusqu'à 700 mA, problème ACCI principal < 7 jusqu'à 600 mA, problème ACCI principal >= 7</p> <p>Ondulation résiduelle de sortie maximale (tension d'ondulation) : 0,2 V p-p Défaut sortie auxiliaire si 11,5 V, OK si 12,0 V Voir section « Alimentation électrique » pour plus de détails</p> <p> Remarque En cas de coupure de courant, cette sortie n'est pas sauvegardée par la batterie. En cas de coupure de courant, la tension de sortie est de 0 V.</p>
+BATT1 ,+BATT2	Batterie lithium-ion polymère, 7,4 V, 2 500 mAh
OP 301, OP 302	<p>Sortie de relais Sans potentiel, contact à bascule NO/C/NC Capacité de charge de contact max. : 500 mA @ 24 V CA rms ou 30 V CC</p>
OP 303, OP 304	<p>Sortie de transistor Open-drain Capacité de charge de contact max. : 500 mA @ 13,8 V CC</p> <p> Remarque En cas de coupure de courant, ces sorties chutent à 0 V.</p>
TR	<p>Une entrée anti-sabotage négative L'entrée passe en état faible inactif (potentiel de masse) via la sirène raccordée. La tension seuil est activée > 4 V, inactivée <3,6 V.</p>
TRB	<p>Une entrée anti-défaut négative L'entrée passe en état faible inactif (potentiel de masse) via la sirène raccordée. La tension seuil est activée > 4 V, inactivée <3,6 V.</p>
10/100 LAN	<p>Ethernet/LAN Câble Patch Cat5e, mâle RJ45 Fiche à chaque extrémité, adaptée pour 10/100 Base-T</p>
USB TYPE B	<p>Fiche USB Mini-B pour centrale Fiche USB-A pour PC Longueur max. 3 m</p>
A B	<p>Interface pour ligne téléphonique analogique vers le réseau téléphonique public, une installation téléphonique ou un périphérique d'accès (routeur communément appelé IAD, comme vodafone Easybox xyz ou FRITZ!Box vwxy)</p>

	Certification télécommunication d'après TBR-21/CTR21 (ETSI ES203021) > 18 V REN rating 1 Débits de données RTC jusqu'à 1 200 bps (V.22)
Micro SD	Secure Digital Memory Card Micro SD 11 mm x 15 mm x 1,0 mm Micro SDHC 4 Go
Z301, Z302, Z303, Z304	Zones filaires 2 fils FSL 2K2/4K7 2 fils FSL 1K/1K 2 fils FSL 2K2/2K2 2 fils FSL 4K7/4K7 2 fils NC
Z301A/Z301T, Z302A/Z302T	Zones filaires 4 fils NC

Zones de résistance spécifiques pour l'état de repos, d'alarme et anti-sabotage (les valeurs sont données en ohms).
Valeurs de résistance directement sur les bornes à vis.

Résistance de conduction recommandée du câble : doit être inférieure à 100 ohms.

	2 fils FSL 2K2/4K7	2 fils FSL 1K/1K	2 fils FSL 2K2/2K2	2 fils FSL 4K7/4K7
Anti-sabotage O/C	8 281-∞	2 401-∞	5 281-∞	11 281-∞
Alarme	4 081 - 8 280	1 401 - 2 400	3 081 - 5 280	6 581 - 11 280
Repos	1 760 - 4 080	800 - 1 400	1 760 - 3 080	3 760 - 6 580
Anti-sabotage S/C	0 - 1 759	0 - 799	0 - 1 759	0 - 3 759

	4 fils NC	2 fils CC
Ouvert/Alarme/Anti-sabotage	1 001-∞	1 001-∞
Fermé/Repos	0 - 1 000	0 - 1 000

Communication

Moyens de communication (canaux)									
Interface a/b	Interface pour ligne téléphonique analogique vers le réseau téléphonique public, une installation téléphonique ou un périphérique d'accès (IAD)								
Ethernet	10/100 LAN								
GSM/GPRS (2G)	Module enfichable, en option FUMO50000 FUMO50001 Bande Quad GSM : 850/900/1800/1900 MHz								
GSM/GPRS (2G) LTE (4G)	Module enfichable, en option ESMO50000 2G GSM : 900 et 1 800 MHz 4G LTE : B3 (1 800 MHz), B8 (900 MHz), B20 (800 MHz)								
Types de communication									
Serveur Web	Accès Internet, APP et serveur ABUS								
AES/TS Reporting									
Destinataire	2 n° tél., 2 adresses IP								
Protocoles	Basé sur DTMF Format rapide, Contact ID Basé sur FSK SIA 1, SIA 2, Ex SIA 3, Ex SIA 3 V2, Ex SIA 3 V3 Basé sur SMS CID en SMS IP Compatible avec « SIA IP Reporting (TCP-2013) » DC-09 (SIA-IP), avec format rapide, Contact ID, SIA <table border="1" data-bbox="762 1173 1228 1451"> <thead> <tr> <th>Protocole</th> <th>Jeton</th> </tr> </thead> <tbody> <tr> <td>FF</td> <td>« SCN-S8 »</td> </tr> <tr> <td>CID</td> <td>« ADM-CID »</td> </tr> <tr> <td>SIA 1, SIA 2, SIA 3, Ex SIA 3, Ex SIA 3 V2, Ex SIA 3 V3</td> <td>« SIA-DCS »</td> </tr> </tbody> </table> TCP, uniquement sans cryptage (version logicielle <=3.00.03), sans cryptage et crypté (version logicielle >=3.00.03) Remarque : Voir annexe « Formats de protocole AES (NSL) Reporting » pour plus de détails.	Protocole	Jeton	FF	« SCN-S8 »	CID	« ADM-CID »	SIA 1, SIA 2, SIA 3, Ex SIA 3, Ex SIA 3 V2, Ex SIA 3 V3	« SIA-DCS »
Protocole	Jeton								
FF	« SCN-S8 »								
CID	« ADM-CID »								
SIA 1, SIA 2, SIA 3, Ex SIA 3, Ex SIA 3 V2, Ex SIA 3 V3	« SIA-DCS »								
Appel d'urgence de soin									
Destinataire	2 n° tél.								
Protocoles	Basé sur DTMF Scancom, Scanfast, Tunstall								
Transmetteur vocal									
Destinataire	8 n° tél. ou identifiants VoIP/SIP								
MFV/DTMF détection VoIP/SIP Accusé de réception	RFC 2833								
Codec VoIP/SIP	PCM G711 A law (RTP AV Profile 8) ITU-T G.711 PCM A-Law audio 64 Ko/s								

	Référence RFC 3551
SMS	
Destinataire	8
Protocole RTC SMS	TAP 8N1 TAP 7E1 UCP 8N1 UCP 7E1 ETSI Protocole 1
E-mail	
Destinataire	8
Pilotage à distance par téléphone	Oui
Installation de transmission d'alarme Catégories et classifications Catégories de systèmes de transmission d'alarme (ATS), classification SPT (Supervised Premises Transceiver)	La centrale contient un communicateur SP2 (ATS2) intégré, afin de répondre à la norme EN 50131 pour le degré de sécurité 2. L'installation de transmission d'alarme est conforme à la norme EN 50136-1:2012 comme communicateur SP2 (ATS2). La centrale prend en charge les options A, B et C pour le niveau 2, comme indiqué dans le tableau 10 de la norme EN 50131-1:2006+A1:2009
Classification de la durée de transmission	D2 -> SP2
Durée de transmission, valeur la plus élevée	M2 -> SP2
Classification de la durée du message	T2 -> SP2
Classification de la disponibilité	A0 (aucune exigence)-> SP2 (en option) Il n'y a aucune méthodologie pour atteindre la conformité avec la norme EN 50136-1:2012, 6.7.3 (non disponibilité de l'installation de transmission d'alarme) car A0, aucune exigence.
Sécurité contre l'échange	S0 (aucune mesure) -> SP2 (en option) Il n'y a aucune méthodologie pour atteindre la conformité avec la norme EN 50136-1:2012, 6.7.2 (redondance / doublement) car S0, aucune mesure
Sécurité des informations	I0 (aucune mesure)-> SP2 (en option) Il n'y a aucune méthodologie pour atteindre la conformité avec la norme EN 50136-1:2012, 6.8.3 (sécurité des informations) car I0, aucune mesure.
Surveillance a/b, Ethernet et GSM/téléphonie mobile	Voir les instructions d'installation au chapitre Options de communication. Mode installateur -> Communication -> Options comm. -> Réaction Défaut voie comm. Ethernet, RTC (a/b), GSM/mobile Mode installateur -> Communication -> Options comm. -> Tempo défaut ligne Ethernet, RTC (a/b), GSM/mobile
Procédure pour l'échange des certificats	Mode de fonctionnement/Procédure : Pass-through (EN 50136-2:2013 chapitre 6 Fonctionnement)

Version logicielle >= 3.00.06

Fonction	RTC	Ethernet LAN	2G GSM, GPRS	4G LTE
Module de téléphonie mobile et raccordements	a/b	LAN	ESMO50000 FUMO50001 FUMO50000	ESMO50000
AES/NSL Reporting (basé sur DTMF et FSK)	oui	non	oui	non
AES/NSL Reporting (basé sur IP, par ex. DC-09)	non	oui	oui	oui
Appel urgence de soin (basé sur DTMF)	oui	non	oui	non
Transmetteur vocal (analogique)	oui	non	oui	2G fallback
Transmetteur vocal (VoIP/SIP)	non	oui	non	non
Transmetteur vocal (VoLTE)	non	non	non	non
Communication à 2 voies	oui	oui	oui	2G fallback
Contrôle par téléphone	oui	non	oui	2G fallback
SMS	oui	non	oui	oui si l'exploitant du réseau le prend en charge
E-mail (avec photos)	non	oui	non	oui
E-mail (sans photos)	non	oui	oui	oui
Serveur Web	non	oui	non	non
Serveur DynDNS ABUS	non	oui	non	non
SNTP (synchronisation horaire)	non	oui	oui	oui
Caméra IP	non	oui	non	non
« Application » smartphone	non	oui	non	non
Notifications Push	non	oui	oui	oui

Autres

Configuration	Navigateur Web via le serveur Web intégré ou directement sur la centrale

Directives européennes

RED : 2014/53/UE
EMV : 2014/30/UE
RoHS : 2011/65/UE
WEEE : 2012/19/UE
ErP : 2009/125/UE
Sous-tension : 2014/35/UE
Sécurité générale : 2001/95/CE

Déclarations de conformité

Pour les systèmes de centrales d'alarme sans fil Secvest FUAA50000, FUAA50500, FUAA50010, FUAA50510, FUAA50100, FUAA50600, FUAA50110, FUAA50610.

Normes et standards auxquels la centrale se conforme.

Organisme de certification/Certification body : **Telefication B.V.**

EN 50131-1:2006+A1:2009
EN 50131-3:2009
EN 50131-5-3:2005+A1:2008
EN 50131-6:2008+A1:2014
EN 50131-10:2014
EN 50136-2:2013

Organisme de certification/Certification body : **ANPI**

INCERT TO31 édition 2014

Niveau de sécurité : niveau 2

Classe d'environnement : classe II

En cas d'installation correcte de la centrale, la Secvest est en mesure d'être conforme à la norme EN 50131 niveau 2.

La Secvest est conforme aux normes EN 50131-1 et EN 50130-5 de classe d'environnement II.

Le bloc d'alimentation est conforme aux normes EN 50131-1:2006+A1 2009 §9 et EN 50131-6:2008+A1:2014 en cas d'installation correcte de la centrale.

L'installation de transmission d'alarme (en anglais ATS) est conforme à la norme EN 50136-1:2012 comme communicateur SP2.

Au niveau 2, le communicateur SP2 intégré permet à la Secvest d'avoir un communicateur conforme, à condition que

- a) Elle soit installée conformément aux instructions d'installation.
- b) Le RTC, LAN et GSM/téléphonie mobile qui y sont connectés fonctionnent normalement.
- c) Le centre de réception des alarmes soit équipé de manière appropriée.

Le module de téléphonie mobile (types voir Données techniques -> Communication) peut être utilisé comme communicateur en option pour le niveau 2.

Version logicielle > 3.00.06

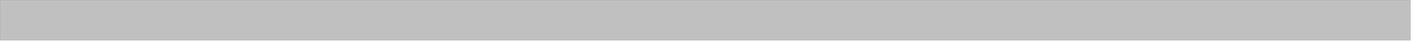
	Variante 1	Variante 2
Interface réseau de remplacement DT	Communicateur	Module de téléphonie mobile

Interface réseau de remplacement DT	Module de téléphonie mobile	Communicateur
--	-----------------------------	---------------

La centrale prend en charge les options A, B et C pour le niveau 2, comme indiqué dans le tableau 10 de la norme EN 50131-1:2006+A1:2009

Si l'installateur sélectionne une configuration non conforme, l'étiquetage de conformité doit alors être retiré ou corrigé.

Le contrôle des conformités par un tiers a été effectué par ANPI et Telefication B.V.



Équipement compatible

Périphériques radio

Nom	Référence de l'article	Remarque
Détecteur		
Détecteur d'ouverture CC (marron)	FUMK50000B	
Détecteur d'ouverture CC (blanc)	FUMK50000W	
Détecteur d'ouverture RFL (marron)	FUMK50010B	
Détecteur d'ouverture RFL (blanc)	FUMK50010W	
Serrure de porte supplémentaire avec bouton de porte 7010 E (marron)	FUFT50010B	
Serrure de porte supplémentaire avec bouton de porte – 7010 E (argent)	FUFT50010S	
Serrure de porte supplémentaire avec bouton de porte 7010 E (blanc)	FUFT50010W	
Serrure de porte supplémentaire avec bouton de porte 7010 E (marron)	FUFT50011B	
Serrure de porte supplémentaire avec bouton de porte – 7010 E (argent)	FUFT50011S	
Serrure de porte supplémentaire avec bouton de porte 7010 E (blanc)	FUFT50011W	
Serrure de porte supplémentaire avec barillet interne 7025 E (marron)	FUFT50020B	
Serrure de porte supplémentaire avec barillet interne 7025 E (argent)	FUFT50020S	
Serrure de porte supplémentaire avec barillet interne 7025 E (blanc)	FUFT50020W	
Serrure de porte supplémentaire avec barillet interne 7025 E (marron)	FUFT50021B	
Serrure de porte supplémentaire avec barillet interne 7025 E (argent)	FUFT50021S	
Serrure de porte supplémentaire avec barillet interne 7025 E (blanc)	FUFT50021W	
Mini-détecteur d'ouverture (marron)	FUMK50020B	
Mini-détecteur d'ouverture (argent)	FUMK50020S	
Mini-détecteur d'ouverture (blanc)	FUMK50020W	
Détecteur d'ouverture fin (blanc)	FUMK50030W	
Détecteur d'ouverture fin (blanc)	FUMK50031W	
Protection de fenêtre sans fil FTS 96 E - AL0089 (marron)	FUFT50000B	
Protection de fenêtre sans fil FTS 96 E - AL0089 (blanc)	FUFT50000W	
Protection de fenêtre sans fil FTS 96 E - AL0125 (marron)	FUFT50001B	
Protection de fenêtre sans fil FTS 96 E - AL0125 (blanc)	FUFT50001W	
Protection de fenêtre sans fil FTS 96 E - AL0145 (marron)	FUFT50002B	
Protection de fenêtre sans fil FTS 96 E - AL0145 (blanc)	FUFT50002W	
Kit de mise à niveau pour FTS 96 (marron)	FUFT50008B	
Kit de mise à niveau pour FTS 96 (blanc)	FUFT50008W	
Poignée de fenêtre FG 350 E (marron)	FUFT50040B	
Poignée de fenêtre FG 350 E (argent)	FUFT50040S	
Poignée de fenêtre FG 350 E (blanc)	FUFT50040W	
Verrou de crémone de fenêtre FOS 550 E - AL0089 (marron)	FUFT50030B	
Verrou de crémone de fenêtre FOS 550 E - AL0089 (blanc)	FUFT50030W	

Verrou de crémone de fenêtre FOS 550 E - AL0125 (marron)	FUFT50031B	
Verrou de crémone de fenêtre FOS 550 E - AL0125 (blanc)	FUFT50031W	
Verrou de crémone de fenêtre FOS 550 E - AL0145 (marron)	FUFT50032B	
Verrou de crémone de fenêtre FOS 550 E - AL0145 (blanc)	FUFT50032W	
Kit de mise à niveau pour FOS 550 - AL0089 (marron)	FUFT50036B	
Kit de mise à niveau pour FOS 550 - AL0089 (blanc)	FUFT50036W	
Kit de mise à niveau pour FOS 550 - AL0125 (marron)	FUFT50037B	
Kit de mise à niveau pour FOS 550 - AL0125 (blanc)	FUFT50037W	
Kit de mise à niveau pour FOS 550 - AL0145 (marron)	FUFT50038B	
Kit de mise à niveau pour FOS 550 - AL0145 (blanc)	FUFT50038W	
Protection de poignée de fenêtre FO 400 E - AL0089 (marron)	FUFT50050B	
Protection de poignée de fenêtre FO 400 E - AL0089 (blanc)	FUFT50050W	
Protection de poignée de fenêtre FO 400 E - AL0125 (marron)	FUFT50051B	
Protection de poignée de fenêtre FO 400 E - AL0125 (blanc)	FUFT50051W	
Kit de mise à niveau pour FO 400	FUFT50058	
Détecteur de mouvement PIR	FUBW50000	
Détecteur de mouvement (PET)	FUBW50010	
Détecteur de mouvement extérieur	FUBW50020 FUBW50021 FUBW50022	
Détecteur autonome avertisseur de fumée	FURM50000	
Détecteur de bris de glace	FUGB50000	
Détecteur de vibrations	FUEM50000	
Détecteur d'inondation	FUWM50000	
Bouton d'alarme panique	FUAT50010	Détecteur d'agression
Bouton d'alarme incendie	FUAT50020	
Claviers de commande		
Clavier de commande	FUBE50000	Activer / Désactiver (activation / désactivation)
Clavier de commande avec RC	FUBE50001	Activer / Désactiver (activation / désactivation) Version logicielle >= V2.00.06
Interrupteur à clé	FUBE50060	Activer / Désactiver (activation / désactivation)
Interrupteur à clé avec RC	FUBE50061	Activer / Désactiver (activation / désactivation) Version logicielle >= V2.00.06
Sirènes d'extérieur		
Sirène d'extérieur	FUSG50000	
Sirène d'extérieur	FUSG50100	Sirènes version logicielle 1.8 Remarque : Aucun répéteur possible.
Sirène d'extérieur	FUSG50101	Sirènes version logicielle >= 1.10

Annexe

Générateur de signal intérieur		
Générateur de signal intérieur	FUSG50110	Version logicielle >= 3.00.05
Modules d'informations / Sirènes d'intérieur		
Module d'information	FUMO50030	
Sirène d'intérieur	FUSG50010	
WAM		
Module universel (MAW)	FUMO50020	
Verrous de porte		
Serrure de porte supplémentaire avec bouton de porte 7010 E (marron)	FUFT50010B	Activer / Désactiver (activation / désactivation)
Serrure de porte supplémentaire avec bouton de porte – 7010 E (argent)	FUFT50010S	Activer / Désactiver (activation / désactivation)
Serrure de porte supplémentaire avec bouton de porte 7010 E (blanc)	FUFT50010W	Activer / Désactiver (activation / désactivation)
Verrou de porte supplémentaire avec bouton de porte 7010 E (marron) avec RC	FUFT50011B	Activer / Désactiver (activation / désactivation) Version logicielle >= V2.00.06
Verrou de porte supplémentaire avec bouton de porte 7010 E (argent) avec RC	FUFT50011S	Activer / Désactiver (activation / désactivation) Version logicielle >= V2.00.06
Verrou de porte supplémentaire avec bouton de porte 7010 E (blanc) avec RC	FUFT50011W	Activer / Désactiver (activation / désactivation) Version logicielle >= V2.00.06
Serrure de porte supplémentaire avec barillet interne 7025 E (marron)	FUFT50020B	Activer / Désactiver (activation / désactivation)
Serrure de porte supplémentaire avec barillet interne 7025 E (argent)	FUFT50020S	Activer / Désactiver (activation / désactivation)
Serrure de porte supplémentaire avec barillet interne 7025 E (blanc)	FUFT50020W	Activer / Désactiver (activation / désactivation)
Verrou de porte supplémentaire avec barillet interne 7025 E (marron) avec RC	FUFT50021B	Activer / Désactiver (activation / désactivation) Version logicielle >= V2.00.06
Verrou de porte supplémentaire avec barillet interne 7025 E (argent) avec RC	FUFT50021S	Activer / Désactiver (activation / désactivation) Version logicielle >= V2.00.06
Verrou de porte supplémentaire avec barillet interne 7025 E (blanc) avec RC	FUFT50021W	Activer / Désactiver (activation / désactivation) Version logicielle >= V2.00.06
Secvest Key	FUSK5xxxx	Activer / Désactiver (activation / désactivation)
Secvest Key avec RC	FUKE53030-58080	Activer / Désactiver (activation / désactivation) Version logicielle >= V2.00.06
Répéteur RF		
Module répéteur Secvest	FUMO50010	Version logicielle >= V2.01.08
Module hybride		
Module hybride Secvest	FUMO50110	Version logicielle >= V3.01.14
Sorties		
Prise	FUHA50010	

Badge		
Clé Proximity	FUBE50020	Activer / Désactiver (activation / désactivation)
Télécommandes		
Télécommande	FUBE50010 FUBE50011 FUBE50012 FUBE50013	Activer / Désactiver (activation / désactivation)
Télécommande avec RC	FUBE50014 FUBE50015	Activer / Désactiver (activation / désactivation) Version logicielle >= V2.00.06
Médaille anti-agression		
Émetteur d'appel d'urgence	FUAT50000	Émetteur anti-agression
Médaille Méd.		
Émetteur d'appel d'urgence	FUAT50000	
Émett.appel d'urg.soins		
Émetteur d'appel d'urgence	FUAT50000	
Périphériques de test		
Boîte de test	FU3801	

Périphériques filaires, accessoires

Nom	Référence de l'article	Remarque
Caméra TVIP41550		
Caméra réseau PIR	TVIP41550	
Caméras IP		
Dôme IP intérieur IR 3 MPx	IPCA33500	Version logicielle >= V1.01.00
Boîtier IP 2 MPx (1080 p, 3 x WDR)	IPCA52010	
Boîtier IP Universel 3MPx	IPCA53000	Version logicielle >= V1.01.00
Boîtier IP 8 MPx (4K, 3 x WDR)	IPCA58000	
Tube IP 2 MPx (1080 p, 3 – 9 mm, 3 x WDR)	IPCA62510	
Tube IP 2 MPx (1080 p, 5 – 50 mm, 3 x WDR)	IPCA62515	
Tube IP Extérieur IR Ultra Low-Light 1080 p	IPCA62520	Version logicielle >= V1.01.00
Tube IP extérieur IR 3 MPx	IPCA63500	Version logicielle >= V1.01.00
Tube IP extérieur IR 6 MPx	IPCA66500	Version logicielle >= V1.01.00
Tube IP 8 MPx (4K, 4,3 – 8,6 mm, 3 x WDR)	IPCA68500	
Dôme IP 2 MPx (1080 p, 3 – 9 mm, 3 x WDR)	IPCA72510	
Dôme IP 2 MPx (1080 p, 5 – 50 mm, 3 x WDR)	IPCA72515	
Dôme IP Extérieur IR Ultra Low-Light 1080 p	IPCA72520	Version logicielle >= V1.01.00
Dôme IP extérieur IR 3 MPx	IPCA73500	Version logicielle >= V1.01.00
Dôme IP extérieur IR 6 MPx	IPCA76500	Version logicielle >= V1.01.00
Dôme IP 8 MPx (4K, 4,3 – 8,6 mm, 3 x WDR)	IPCA78500	
Mini Dôme IP Extérieur IR 1080 p	IPCB42500 IPCB42501	Version logicielle >= V1.01.00
Mini Dôme IP 2 MPx (1080 p, 2,8 mm)	IPCB42510A	
Mini Dôme IP 2 MPx (1080 p, 4 mm)	IPCB42510B	
Mini Dôme IP 2 MPx (1080 p, 6 mm)	IPCB42510C	
Mini Dôme IP Wi-Fi 2 MPx (1080 p, 2,8 mm)	IPCB42515A	
Mini Dôme IP Extérieur IR Wi-Fi 1080 p	IPCB42550 IPCB42551	Version logicielle >= V1.01.00
Mini Dôme IP 4 MPx (2,8 mm)	IPCB44510A	
Mini Dôme IP 4 MPx (4 mm)	IPCB44510B	
Mini Dôme IP 4 MPx (6 mm)	IPCB44510C	
Mini Tube IP Universel IR 1080 p	IPCB62500	Version logicielle >= V1.01.00
Mini Tube IP 2 MPx (1080 p, 2,8 mm)	IPCB62510A	
Mini Tube IP 2 MPx (1080 p, 4 mm)	IPCB62510B	
Mini Tube IP 2 MPx (1080 p, 6 mm)	IPCB62510C	
Tube IP 2 MPx (1080 p, 2,8 – 12 mm)	IPCB62520	
Mini Tube IP 4 MPx (2,8 mm)	IPCB64510A	
Mini Tube IP 4 MPx (4 mm)	IPCB64510B	

Mini Tube IP 4 MPx (6 mm)	IPCB64510C	
Tube IP 4 MPx (2,8 – 12 mm)	IPCB64520	
Mini Tube IP 8 MPx (4K, 2,8 mm)	IPCB68510A	
Mini Tube IP 8 MPx (4K, 4 mm)	IPCB68510B	
Mini Tube IP 8 MPx (4K, 6 mm)	IPCB68510C	
Tube IP 8 MPx (4K, 2,8 – 12 mm)	IPCB68520	
Dôme IP Universel IR 720 p	IPCB71500	Version logicielle >= V1.01.00
Dôme IP Universel IR 1080 p	IPCB72500 IPCB72501	Version logicielle >= V1.01.00
Dôme IP 2 MPx (1080 p, 2,8 mm)	IPCB72515A	
Dôme IP 2 MPx (1080 p, 2,8 – 12 mm)	IPCB72520	
Dôme IP 4 MPx (4 mm)	IPCB74515B	
Dôme IP 4 MPx (2,8 – 12 mm)	IPCB74520	
Dôme IP 8 MPx (4K, 2,8 mm)	IPCB78515A	
Dôme IP 8 MPx (4K, 2,8 – 12 mm)	IPCB78520	
Encodeur Dual Flex	IPCS10020	
Tube IP Ultra Low-Light IR 1080 p	IPCS62520	Version logicielle >= V1.01.00
Dôme IP Ultra Low-Light IR 1080 p	IPCS72520	Version logicielle >= V1.01.00
PTZ IP 2 MPx (1080 p, 20x)	IPCS82500	
PTZ IP 2 MPx (1080 p, 23x, Ultra Low-Light)	IPCS82520	
PTZ IP 3 MPx (36x)	IPCS83500	
Mini PTZ IP 4 MPx (4x)	IPCS84510	
Caméra intérieure compacte 2 MPx Wi-Fi pour vidéosurveillance IP	TVIP11560 TVIP11561	
Caméra intérieure pan tilt zoom Wi-Fi HD 720 p	TVIP21560	
Caméra dôme réseau d'extérieur IR HD 720 p	TVIP41500	
Caméra dôme d'extérieur Wi-Fi HD 720 p	TVIP41560	
Caméra dôme PTZ Wi-Fi HD 720 p	TVIP41660	
Mini caméra dôme Wi-Fi 2 MPx pour vidéosurveillance IP ABUS	TVIP42560	
Caméra réseau WDR jour/nuit HD 1080 p	TVIP52502	
Caméra réseau d'extérieur IR HD 720 p	TVIP61500	
Caméra réseau d'extérieur Wi-Fi IR HD 720 p	TVIP61550	
Caméra d'extérieur Wi-Fi HD 720 p	TVIP61560	
Mini caméra tube Wi-Fi 2 MPx pour vidéosurveillance IP ABUS	TVIP62560	
Caméra dôme réseau jour/nuit PTZ 720 p	TVIP81000	
Caméra dôme réseau d'extérieur jour/nuit PTZ 720 p	TVIP81100	
Caméra dôme réseau jour/nuit PTZ 1080 p	TVIP82000	
Caméra dôme réseau d'extérieur jour/nuit PTZ 1080 p	TVIP82100	
Réseau intérieur de caméra Fisheye HD 1080 p	TVIP82900	
Fisheye IP 3 MPx	TVIP83900	

Annexe

Caméra hémisphérique d'extérieur dôme IP 6 MPx	TVIP86900	
Périphériques de communication		
Module de téléphonie mobile	FUMO50000	
Module de téléphonie mobile	FUMO50001	Version logicielle >= V1.01.00
Module de téléphonie mobile	ESMO50000	Version logicielle >= V3.00.05
Antenne mobile	AZ6310W	
Carte SIM		SIM standard 1,8 V/3,0 V Micro SIM FUMO50001 ESMO50000
Adaptateur Wi-Fi	FUMO50040	Ethernet <-> Wi-Fi
PSU externe		
Bloc d'alimentation 13,8 V/1,7 A	AZZU10000 AZZU10030 FU3819	
Bloc d'alimentation 13,8 V/2 A	TVAC35500	
Bloc d'alimentation 13,8 V/3 A	TVAC35510	
Bloc d'alimentation 13,8 V/5 A	TVAC35520	
Alimentation de secours		
Batterie de rechange 7,4 V/2 500 mAh	FUBT50000	
Carte SD		
Carte Micro SD 4 Go	TVAC40970	Micro SDHC 4 Go
Touch Cover		
Secvest Touch Cover individuel	FUZU50000	Version logicielle >=2.01.08

Périphériques filaires satisfaisant aux spécifications électriques des raccordements correspondants (zones, sorties, entrées).

Logiciel d'utilisation, de commande et de communication

Nom	Référence de l'article	Remarque
Navigateur		
IE8		IE7 et les navigateurs antérieurs ne sont pas compatibles
Firefox		
Chrome		
Safari		
Appli		
Application Secvest (iOS)	APP50000	Version 2.3.1 2.1.1 2.1.0 2.0.1 1.3.5 1.3.1 1.2.5 1.2.2 1.1.7 1.1.2 iOS 10 ou version supérieure iPhone, iPad, iPod touch
Application Secvest (Android)	APP50200	Version 2.3.1 2.1.1 2.1.0 2.0.1 1.3.40 1.3.38 1.3.1 1.2.1 1.1.6 Android 5.0 (Lollipop) ou version supérieure
Mise à jour logicielle		
Utilitaire de mise à jour Secvest		Version 1.02.05 ou supérieure

Valeurs par défaut/Réglages d'usine matériel

À la livraison, un pontage à fil est raccordé entre le raccordement TR (Tamper Return) et 0 V ainsi qu'entre le raccordement TRB (Trouble) et 0 V.

Ainsi, aucun message d'erreur (sabotage ou défaut) n'apparaît si aucune sirène filaire n'est raccordée.

Valeurs par défaut/Réglages d'usine logiciel



Remarque

La centrale Secvest satisfait aux exigences de la norme EN 50131 lorsque les valeurs par défaut sont conservées et que les remarques sont prises en compte. Si vous modifiez ces réglages, la conformité de l'installation est compromise. Si la centrale Secvest n'est plus conforme à la norme EN 30131, vous devez éliminer tous les indicateurs de défaut de conformité.

Mode installateur

Option de menu	Programmation Usine Valeurs par défaut	Observations
1. COMPOSANTS		
Détecteur		
Zones IP		
Ajouter/supprimer détecteurs		
Zone 1nn		Zone 101 à 103 Zone 101 à 106 (version logicielle 1.01.00 et versions supérieures)
Type de périphérique	Série IPCx	
Mode Trigger	Externe	
Trigger événements	Non	(Apparaît uniquement en « mode Trigger » = « Externe » ou « Int. + Ext. »)
Action de la caméra	Vidéos Non Images Oui	Apparaît uniquement dans la série IPCx
Trigger partitions	Partition 1 Oui Partition 2 Oui Partition 3 Oui Partition 4 Oui Toutes Partitions Oui	(Apparaît uniquement en « mode Trigger » = « Externe » ou « Int. + Ext. »)
Adresse IP	Vide	
HTTP Port Interne	80	
HTTP Port Externe	Vide	
RTSP Port Interne	554	
RTSP Port Externe	Vide	
Nom d'utilisateur	Vide	
Mot de passe	Vide	
Temps de réponse	20 s	Plage de 1 s à 99 s
Éditer zones		
Nom	Zone 10x	Zone 101 à 103 Zone 101 à 106 (version logicielle 1.01.00 et versions supérieures)

Type	Non utilisé		
Partitions	Aucune		Apparaît uniquement lorsque le type de zones n'est pas « Non utilisé ».
Propriétés	Aucune		Apparaît uniquement si un type autre que « Non utilisé » a été attribué à la zone. Certaines propriétés ne sont disponibles que pour certains types de zones.
	Surveillance interne	Dé-sac-tivée	
	Carillon de porte	Dé-sac-tivé	
	Test 14 Jours	Dé-sac-tivé	
	Surveillance d'activité	Dé-sac-tivée	
	Armement Forcé Isolé	Dé-sac-tivé	
	Sabotage ignoré	Dé-sac-tivé	
	Isoler est Possible	Dé-sac-tivé	
	Inversion	Dé-sac-tivée	
Supervision	Allu-mée		
Supprimer tous			
Zones sans fil			
Ajouter/supprimer détec-teurs			
Zone 2nn			Zone 201 à 248
Éditer zones			
Nom	Zone 2xy		Zone 201 à 248
Type	Non utilisé		
Partitions	Aucune		Apparaît uniquement lorsque le type de zones n'est pas « Non utilisé ».
Propriétés	Aucune		Apparaît uniquement si un type autre que « Non utilisé » a été attribué à la zone. Certaines propriétés ne sont disponibles que pour certains types de zones.
	Surveillance interne	Dé-sac-tivée	
	Carillon de porte	Dé-sac-tivé	
	Test 14 Jours	Dé-sac-tivé	

	Surveillance d'activité	Dé- sac- tivée	
	Armement Forcé Isolé	Dé- sac- tivé	
	Sabotage ignoré	Dé- sac- tivé	
	Isoler est Possible	Dé- sac- tivé	
	Supervision Version logicielle >= 3.01.16	Allu- mée	
Supprimer tous			
Zones filaires			
Éditer zones			
Nom	Zone 30x		Zone 301 à 304
Type	Non utilisé		
Partitions	Aucune		Apparaît uniquement lorsque le type de zones n'est pas « Non utilisé ».
Propriétés	Aucune		Apparaît uniquement si un type autre que « Non utilisé » a été attribué à la zone. Certaines propriétés ne sont disponibles que pour certains types de zones.
	Surveillance interne	Dé- sac- tivée	
	Carillon de porte	Dé- sac- tivé	
	Test 14 Jours	Dé- sac- tivé	
	Surveillance d'activité	Dé- sac- tivée	
	Armement Forcé Isolé	Dé- sac- tivé	
	Sabotage ignoré	Dé- sac- tivé	
	Isoler est Possible	Dé- sac- tivé	
	Inversion	Dé- sac- tivée	
Supprimer tous			
Zones MoHy			
Éditer zones			
Nom	Zone 40x		Zone 401 à 420
Type	Non utilisé		

Partitions	Aucune	Apparaît uniquement lorsque le type de zones n'est pas « Non utilisé ».	
Propriétés	Aucune	Apparaît uniquement si un type autre que « Non utilisé » a été attribué à la zone. Certaines propriétés ne sont disponibles que pour certains types de zones.	
	Surveillance interne		Dé-sactivée
	Carillon de porte		Dé-sactivé
	Test 14 Jours		Dé-sactivé
	Surveillance d'activité		Dé-sactivée
	Armement Forcé Isolé		Dé-sactivé
	Sabotage ignoré		Dé-sactivé
	Isoler est Possible		Dé-sactivé
Inversion	Dé-sactivée		
Supprimer tous			
Clavier de commande sans fil			
Ajouter/supprimer CLAV			
CLAVIER RADIO 0n		CLAVIER RADIO 01 à 08	
Éditer Clavier			
Nom	CLAVIER RADIO 0x	CLAVIER RADIO 01 à 08	
Partitions	Partition 1-4 : Oui Toutes Partitions : Oui		
Touche C	Act. interne		
Armement immédiat	Oui		
Supprimer tous			
Sirènes d'extérieur			
Sirènes sans fil			
Ajouter/supprimer Sirène			
Sirène radio 0n		Sir. radio 01 à 04	
Éditer Sirène			
Nom	Sir. radio 0n	Sir. radio 01 à 04	
Partitions	Partition 1-4 : Oui Toutes Partitions : Oui		
Supprimer tous			
Sirènes filaires			
Sirène filaire 01			

Nom	Sirène filaire 01	
Générateur de signal intérieur		
Ajouter/Supprimer		
Générateur de signal int. 0n		Générateur de signal int. 01 à 04
Éditer		
Nom	Générateur de signal int. 0n	Générateur de signal int. 01 à 04
Partitions	Partition 1 : Oui Partitions 2-4 : Non Toutes Partitions : Non	
Supprimer tous		
Sirènes d'intérieur/Module d'information		
Ajouter Centrale		
Actualisation	Bloqué	
LED prêt	Bloqué	
WAM		
Ajouter/supprimer MAW		
MAW 0n		MAW 01 à 08
Éditer MAW		
Nom	MAW 0x	MAW 01 à 08
Mode		
Supprimer tous		
Verrous de porte		
Ajouter/Supprimer verrou porte		
Verrou porte 0n		Verrou porte 01 à 08
Éditer verrou porte		
Nom	Verrou porte 0x	Verrou porte 01 à 08
Partitions	Partition 1-4 : Oui Toutes Partitions : Oui	
Désactivé après effraction	Oui	Version logicielle >= 3.01.16
Supprimer tous		
Répéteur RF		
Ajouter/Supprimer répéteur RF		
Répéteur RF 1 à 4		Répéteur RF 1 à 4
Éditer verrou porte		
Nom	Répéteur RF 1 à 4	Répéteur RF 1 à 4
Répéter centrale d'alarme	Non	

Répéter détecteurs	Non	Après l'ajout d'un répéteur, tous les détecteurs programmés de la centrale d'alarme s'affichent.
Répéter claviers de commande sans fil	Non	Après l'ajout d'un répéteur, tous les claviers de commande sans fil programmés de la centrale d'alarme s'affichent.
Répéter générateur de signal int.	Non	Après l'ajout d'un répéteur, tous les générateurs de signal intérieurs programmés de la centrale s'affichent.
Répéter sirènes d'extérieur	Non	Après l'ajout d'un répéteur, toutes les sirènes d'extérieur programmées de la centrale d'alarme s'affichent.
Répéter verrous de porte	Non	Après l'ajout d'un répéteur, tous les verrous de porte programmés de la centrale d'alarme s'affichent.
Répéter MoHy	Non	Après l'ajout d'un répéteur, tous les modules hybrides programmés de la centrale s'affichent.
Supprimer tous		
Modules hybrides		
Ajouter/Supprimer		
MoHy n		Module hybride 1 à 2
Éditer		
Nom	MoHy x	Module hybride 1 à 2
Partitions	Partition 1-4 : Oui Toutes Partitions : Oui	
Type de zone filaire	2 fils FSL 2K2/4K7	
Options haut-parleur		
Partitions	Partition 1-4 : Oui Toutes Partitions : Oui	
Supprimer tous		
2. SORTIES		
Sorties sans fil		
Ajouter Sorties		
Sortie 2nn		Sortie 201 à 232
Éditer sorties		
Nom	Sortie 2nn	Sortie 201 à 232
Type	Non utilisé	
Polarité	Normal	
Partitions	Partition 1-4 : Oui Toutes Partitions : Oui	
Supprimer tous		
Sorties filaires		
Éditer sorties		
Nom	Sortie 3nn	Sortie 301 à 304

Type	Non utilisé	
Polarité	Normal	
Partitions	Partition 1-4 : Oui Toutes Partitions : Oui	
Supprimer tous		
Sorties MoHy		
Éditer sorties		
Nom	Sortie 40n	Sortie 401 à 408
Type	Non utilisé	
Polarité	Normal	
Partitions	Partition 1-4 : Oui Toutes Partitions : Oui	
Supprimer tous		
Sorties mixtes		
Sorties mixtes 1-10		
Mode	Un (OU)	
Entrées 1-10	Non utilisé	
3. PARTITIONS		
Partition 1-4		
Nom	Partition n	Partition 1 à 4
Tous act.		
Mode Sortie	Armement temporisé	
Temps de sortie	40 secondes	Apparaît uniquement lorsque que le mode Sortie est « Armement temporisé » ou « Arm. silencieux ».
Temps supplémentaire	15 secondes	Apparaît uniquement lorsque le mode Sortie est « Sortie Finale Armement », « Verrou activ. » ou « Annulation Tempor. Stie ».
Temps d'entrée	40 secondes	Pour la conformité avec la norme EN 50131-1, clause 8.3.8.2, 45 s max.
Réponse alarme	Sirène + transmission	Alarme interne comprise
Retard sirène	0 minute	
Durée sirène extérieure	15 minutes 3 minutes lorsque le pays est l'Allemagne	Pour la conformité avec la norme EN 50131-1, clause 8.6, 90 s min., 15 min max.
Flash arm.	Désactivé	Ce réglage est nécessaire pour la conformité à la norme EN 50131.
Flash désarm.	Désactivé	
Bip arm	Désactivé	Ce réglage est nécessaire pour la conformité à la norme EN 50131.
Bip désarm	Désactivé	
Durée sirène int.	Indéfini	

Act. interne		
Mode Sortie	Armement immédiat	
Temps de sortie	40 secondes	Apparaît uniquement lorsque que le mode Sortie est « Armement temporisé » ou « Arm. silencieux ».
Temps supplémentaire	15 secondes	Apparaît uniquement lorsque le mode Sortie est « Sortie Finale Armement », « Verrou activ. » ou « Annulation Tempor. Sti »
Temps d'entrée	40 secondes	Pour la conformité avec la norme EN 50131-1, clause 8.3.8.2, 45 s max.
Réponse alarme	Sirène	Alarme interne comprise Ce réglage est nécessaire pour la conformité à la norme EN 50131.
Retard sirène	0 minute	
Durée sirène extérieure	15 minutes 3 minutes lorsque le pays est l'Allemagne	Pour la conformité avec la norme EN 50131-1, clause 8.6, 90 s min., 15 min max.
Sortie finale arm. part.	Entrée/sortie	
Route entrée arm. part	Route d'entrée	
Flash arm.	Désactivé	Ce réglage est nécessaire pour la conformité à la norme EN 50131.
Flash désarm.	Désactivé	
Bip arm	Désactivé	Ce réglage est nécessaire pour la conformité à la norme EN 50131.
Bip désarm	Désactivé	
Durée sirène int.	Indéfini	
Désactivée		Version logicielle >=2.00.00
Réponse alarme	Sirène + transmission	Alarme interne comprise
Retard sirène	0 minute	
Durée sirène extérieure	15 minutes 3 minutes lorsque le pays est l'Allemagne	Pour la conformité avec la norme EN 50131-1, clause 8.6, 90 s min., 15 min max.
Durée sirène int.	Indéfini	
Réaction agression	Silencieuse (version logicielle >= 2.00.00) Sonore (version logicielle < 2.00.00)	
Lien arm. compl.	Partitions 2-4 : Non Toutes Partitions : Non	La partition 1 est la partition commune.
4. SYSTEME		
Généralités		
Langue	Français	Cette valeur dépend de votre réponse à la question portant sur la langue, lors de la première mise en service.
Texte écran	Secvest	

Réinitialiser		
Programmation Usine		
Programmation pays		Apparaît uniquement dans le cadre du processus de programmation Usine.
Défaut secteur		
Message défaut CA	Allumée	Ce réglage est nécessaire pour la conformité à la norme EN 50131.
Retard Défaut A/C	0 minute	Ce réglage est nécessaire pour la conformité à la norme EN 50131.
Message Défaut DC externe	Allumée	Ce réglage est nécessaire pour la conformité à la norme EN 50131.
Retard Défaut DC externe	0 minute	Ce réglage est nécessaire pour la conformité à la norme EN 50131.
Installateur détails		
Nom de l'installateur		Cette valeur dépend de votre réponse aux questions « Longueur code d'accès » et « Nouv. code installateur », lors de la première mise en service.
Code installateur		Cette valeur dépend de votre réponse aux questions « Longueur code d'accès » et « Nouv. code installateur », lors de la première mise en service.
Installateur No tél.		
Accès utilisateur		
Enregistrement mémo	Oui	
Fonction touches doubles	Non	
Touches Soins de Santé	Non	
Masquer tous/tes	Oui	
Armement rapide	Non	Ce réglage est nécessaire pour la conformité à la norme EN 50131.
Isoler rapidement	Non	
Code utilisateur requis	Oui	Ce réglage est nécessaire pour la conformité à la norme EN 50131. Norme EN 50131-1, section 8.3.1 (lien avec la norme EN 50131-3, section 8.3.1)
Réponse 2WAY	Oui	
Téléco arm immédiat	Oui	
Contrainte ON	Non	Modifiez l'option Utilisation Code Contrainte sur Oui
RAZ Util.		
Zone alarmes	Oui	Cette option apparaît uniquement lorsque le mode de confirmation est « Basique ».
Sabotages zone	Oui	Pour la reconnaissance INCERT, définir sur NON.
Sabotages système	Non	Pour la reconnaissance INCERT, définir sur NON.
Confirmation		
Mode de confirmation		

Base	Standard pour les systèmes hors Royaume-Uni	Cette valeur dépend de votre réponse à la question portant sur la « programmation pays », lors de la première mise en service.
DD243		
BS8243	Standard pour les systèmes britanniques, lorsque le Royaume-Uni est sélectionné comme pays.	Cette valeur dépend de votre réponse à la question portant sur la « programmation pays », lors de la première mise en service.
Durée de confirmation	30 minutes	Visible pour DD243 ou BS8243. Peut être réglée entre 1 et 60 minutes. Notez que seule une valeur supérieure ou égale à 30 minutes est conforme au mode de confirmation DD243 ou BS8243.
Après entrée	1 Zone	Visible pour DD243 ou BS8243. Le réglage par défaut passe à 2 zones lorsque le mode de confirmation = DD243.
Clav bloqué tempo entrée	Désactivé	Visible pour DD243 ou BS8243.
Sirène ON	Ne pas confirmer	Visible pour DD243, BS8243 et Basique.
Sirène ON	Ne pas confirmer	Visible pour DD243, BS8243 et Basique.
RAZ non confirmée	Utilisateur	Visible pour DD243 ou BS8243.
RAZ confirmée	Installateur	Visible pour DD243 ou BS8243.
Confirmation temps alarme agression	8 heures	Visible uniquement pour BS8243. La valeur doit être comprise entre 8 et 20 heures pour être conforme à BS8243:2010.
Sabotage= seulement sabotage	Autorisé	Visible pour BS8243.
Hardware		
Type de zone filaire	2 fils FSL 2K2/4K7	Cette valeur dépend de votre réponse à la question « Type Zone Filaire », lors de la première mise en service.
Options sirènes radio	Sirène + Flash	
Batt. 2	Bloqué	
Carte SD		
Antenne GSM/mobile	Interne	
Sécurité		
Supervision	Anomalie Sabotage, lorsque le pays est le Royaume-Uni	« SABOTAGE » pour le Royaume-Uni, pour satisfaire PD6662:2010
Brouillage	Anomalie Sabotage, lorsque le pays est le Royaume-Uni	« SABOTAGE » pour le Royaume-Uni, pour satisfaire PD6662:2010
Mises à jour de niveau 4	Bloqué	
Isoler sabotage	Bloqué	Ce réglage est nécessaire pour la conformité à la norme EN 50131.

Armement forcé	Désactivé	Si vous autorisez l'activation forcée, le système ne sera plus conforme à la norme EN 50131.
Désarm. télé tjs ou tps entrée	Toujours	
Désarm.P. Télé Tjs ou Tps Entrée	Toujours	
Clav tps d'entrée	Toujours	
Clav Tps d'entrée Partiel	Toujours	
Réarmement auto	Jamais	Ce réglage est nécessaire pour la conformité à la norme EN 50131. Apparaît uniquement lorsque le mode de confirmation est basique.
Avertissements silencieux	Code utilisateur	
Temps abandon	120 secondes	
Retard sirène (Util)	0 minute	
Retard Alarme Entrée	Autorisé	Ce réglage est nécessaire pour la conformité à la norme EN 50131-1 8.3.8.2.
Émission état centrale	Non	
Mise à niveau de la centrale		« V3.00.03 – installée »
Contrôler la mise à niveau ?		Après la sélection, la centrale d'alarme vérifie automatiquement si une nouvelle version logicielle est disponible sur le serveur FTP ABUS.
Sauvegarder/Restaurer		
Config. de sauvegarde sur carte SD		
Config. de chargement depuis carte SD		« Secvest—04-12-2017-0932.cfg »
Rapport		Sur interface Web uniquement
5. COMMUNICATION		
Réseau		
Configuration de réseau		
Serveur Web	Autorisé	
DHCP	Allumé	
Adresse IP	Vide	Cette option est uniquement affichée, version logicielle >=2.00.00 DHCP=OFF
Numéro port IP	80	Version logicielle <2.00.00
Port HTTP interne	80	
Port HTTPS interne	4433	
Masque sous-réseau IP	Vide	Cette option est uniquement affichée, version logicielle <2.00.00 en cas de saisie d'une adresse IP. version logicielle >=2.00.00 DHCP=OFF

Passerelle adresse IP	Vide	Cette option est uniquement affichée, version logicielle <2.00.00 en cas de saisie d'une adresse IP. version logicielle >=2.00.00 DHCP=OFF
DNS adresse IP primaire	Vide	Cette option est uniquement affichée, version logicielle <2.00.00 en cas de saisie d'une adresse IP. version logicielle >=2.00.00 DHCP=OFF
Serveur DYNDNS ABUS		
État	Autorisé	
Nom d'utilisateur	Vide	
Mot de passe	Vide	
Port externe	443	Version logicielle <2.00.00
Port HTTPS externe	4433	
Configuration Mobile IP		Version logicielle >= 3.01.01 Cette option est uniquement affichée si un module de téléphonie mobile est installé.
APN	Vide	
Nom d'utilisateur	Vide	
Mot de passe	Vide	
Passerelle IP	Ethernet	
Paramétrage E-mail		
Nom serveur	Vide	
N° port serveur IP	587	
Compte	Vide	
Nom d'utilisateur	Vide	
Mot de passe	Vide	
SSL	Bloqué	
Setup Transmission VoIP		
SIP Appel de Test		
Destination SIP ID U	Vide	
Start Test		
Nom serveur SIP	Vide	Version logicielle <2.00.00
Nom domaine SIP	Vide	
Proxy SIP	Vide	
ID utilisateur SIP	Vide	
Mot de passe utilisateur SIP	Vide	
SIP port	5060	
Port RTP	10000	
RFC 2833 détection DTMF	Autorisé	

Transmission SIP autorisée	Autorisé		
TS Reporting			
Mode appel	Simple		Le réglage « Simple » ou « Altern. » est nécessaire pour la conformité à la norme EN 50131.
Protocole	Format rapide		
Priorité transmission	Ethernet 2 RTC 1		
Destinataire	Aucun		
Cryptage	Aucun		
ID client	ID client PART. 1 : 000000 ID client PART. 2 : 000000 ID client PART. 3 : 000000 ID client PART. 4 : 000000		Un ID client par partition
Canaux format rapide	Canal 1 : Incendie Canal 2 : Alarme anti-agression Canal 3 : Alarme intrusion Canal 4 : Ouvert / Fermé Canal 5 : Zones isolées (système) Canal 6 : Sabotage Canal 7 : Alarme confirmée Canal 8 : Défaut général		Apparaît uniquement lorsque le protocole = Format rapide
Événements CID/SIA	Incendie	Oui	Remarques : 1. Apparaît lorsque le protocole = CID ou SIA. 2. Ce réglage est nécessaire pour la conformité à la norme EN 50131.
	Alarme anti-agression	Oui	
	Alarme Alarme	Oui	
	Alarme intrusion	Oui	
	Technique	Non	
	Sabotages	Oui	
	Armement/Désarmement	Oui voir remarque 2	
	Act. interne	Oui voir remarque 2	
	Remise à zéro	Oui voir remarque 2	
	Sortie timeout	Oui	
	Exclusion	Oui	
	Boîtier clé	Non	
	RF Supervision	Oui	
	RF Brouillage	Oui voir remarque 2	
	Batt.Rad. /PSU	Oui voir remarque 2	
	Batt. centrale	Oui voir remarque 2	
	Défaut secteur	Oui voir remarque 2	
Anomalies	Oui voir remarque 2		
Mode installateur	Oui voir remarque 2		
Code util. changé	Oui		
RAZ heure/date	Non		

	Supervision ca- méra	Non	
Restaurations	Autorisé		
Réarm. Transm. Intrusion	Autorisé		Apparaît uniquement lorsque le protocole = Format rapide ET que le mode de confirmation = « Basique ».
21CN temps acquis	800 ms		Apparaît uniquement lorsque le protocole = Format rapide.
Sabotage = Intrusion	Bloqué		Apparaît uniquement lorsque le protocole = CID ou SIA.
Appel de stat.	Autorisé		Apparaît uniquement lorsque l'appel test statique est bloqué
Appel de test stat.	Bloqué		Apparaît uniquement lorsque l'appel test dynamique est bloqué. En vue du respect de la norme EN 50131, l'appel de test statique ou dynamique doit être activé.
Transm. désarmée	Autorisé		
Appel d'urgence de soin			
Mode appel	Bloqué		
Protocole	Scancom		
Priorité transmission	RTC 1		
Destinataire	Aucun		
ID Client	ID client PART. 1 : 000000 ID client PART. 2 : 000000 ID client PART. 3 : 000000 ID client PART. 4 : 000000		Un ID client par partition
Acquit d'appel	Autorisé		
21CN temps acquis	800 ms		Apparaît uniquement lorsque le protocole = Scancom ou Scanfast
Transmetteur vocal			
Mode appel	Bloqué		
Priorité transmission	Ethernet 2 RTC 1		
Messages	Aucun		
Événement	Aucun		
Message 1	Événement 1 : Aucun Événement 2 : Aucun Événement 3 : Aucun Événement 4 : Aucun Événement 5 : Aucun		
Message 2	Événement 1 : Aucun Événement 2 : Aucun Événement 3 : Aucun Événement 4 : Aucun Événement 5 : Aucun		
Message 3	Événement 1 : Aucun Événement 2 : Aucun Événement 3 : Aucun Événement 4 : Aucun Événement 5 : Aucun		
Message 4	Événement 1 : Aucun		

	Événement 2 : Aucun Événement 3 : Aucun Événement 4 : Aucun Événement 5 : Aucun	
Destinations	Aucune	
Acquit d'appel	Autorisé	
Appel de test stat.	Mensuel, jour : 1, heure : 12:00	
SMS		
Mode appel	Bloqué	
Priorité transmission	RTC 1	
Messages	Vide	
Événement	Aucun	
SMS RTC		
Protocole	ETSI Protocole 1	
Service n° tél	1470,17094009	EC
Mon n° tél	Vide	Apparaît uniquement lorsque le protocole = UCP
Destinations	Aucune	
Appel de test stat.	Mensuel, jour : 1, heure : 12:00	
E-mail		
Mode appel	Bloqué	
Priorité transmission	Ethernet 1	
Messages	Vide	
Événement	Aucun	
Destinations	Aucune	
Appel de test stat.	Mensuel, jour : 1, heure : 12:00	
Niveau Options		
Réaction Défaut voie comm.	Ethernet = audible RTC = audible Mobile IP/Mobile = audible	
Tempo Défaut ligne RTC	Ethernet = 9 secondes RTC = 9 secondes Mobile IP/Mobile = 9 secondes	Ce réglage est nécessaire pour la conformité à la norme EN 50131. Mobile IP/Mobile visible uniquement en cas d'intégration d'un module de téléphonie mobile. Plage de valeurs : 0 à 60 secondes
Contrôle par téléphone		
Contrôle Appel sortant	Désactivé	
Contrôle Appel entrant	Désactivé	
Sonneries avant réponse	5 sonneries	Apparaît uniquement lorsque le contrôle d'appel entrant est activé
Réponse après 1 sonnerie	Désactivée	Apparaît uniquement lorsque le contrôle d'appel entrant est activé
GSM/Mobile sans ligne extérieure	Non	Apparaît uniquement en cas d'intégration d'un module de téléphonie mobile.

Contacts		
Destinataires A-L		
Nom	Destinataires A-L	
Partitions	1-4	Version logicielle >= 2.00.00
Voix/SMS/E-mail	Désactivé : Oui Activé : Oui Act. interne : Oui	Version logicielle >= 3.01.01
N° de tél. 1	Vide	
N° de tél. 2	Vide	
E-mail	Vide	
Adresse IP	Vide	
ID utilisateur SIP	Vide	
6. APPEL D'URGENCE DE SOIN		
Début temps de surveillance	08:00 (hh:mm)	
Fin temps de surveillance	20:00 (hh:mm)	
Intervalle de Contrôle	4 heures	
Volume	Centrale – Intermédiaire, Web - 5	
7. TEST		
Test de détection	Pas de zones utilisées	
Clavier		
Sirènes et avertisseurs		
Sirènes int.	Désactivé	
Tension d'entrée CC externes	Pas de Périph.!	
Module Sirènes	Pas de Périph.!	
Haut-parleur	Arrêté	
Clavier de commande sans fil		
Verrous de porte	Pas de Périph.!	
Puissance du signal		
Détecteur	Pas de détecteurs	
Clavier de commande sans fil	Pas de Périph.!	
Sirènes d'extérieur	Pas de Périph.!	
Générateur de signal int.	Pas de Périph.!	
WAM	Pas de Périph.!	
Verrous de porte	Pas de Périph.!	
Modules hybrides	Pas de Périph.!	
Répéteur RF	Pas de Périph.!	
Périphériques répéteur RF	Pas de Périph.!	

Sorties		
Sorties sans fil	Pas de sorties disponibles	
Sorties filaires	Pas de sorties disponibles	
Badge	Aucun badge lu	
Télécommandes	Pas de Téléco enregistrée	
Émetteur d'appel d'urgence	Pas de médaillon enregistré	
TS Reporting		
Ethernet	Pas de destinataires!	
RTC	Pas de destinataires!	
GSM/Mobile	Pas de destinataires!	Apparaît uniquement en cas d'intégration d'un module de téléphonie mobile.
Transmetteur vocal	Communication pas activée	
SMS	Communication pas activée	
E-mail	Communication pas activée	
Résistances zones	Pas de zones utilisées	
PSU centrale		
Tension d'entrée CC extérieure	p. ex. 14,2 volts	La valeur de tension apparaît uniquement lorsque le PSU externe est raccordé.
Batt. centrale d'alarme 1	p. ex. 8,3 volts	
Batt. centrale d'alarme 2	p. ex. 0,1 Volt	
Aux. tension out	p. ex. 13,9 volts	
PSU MoHy		
	Pas de Périph.!	
8. HISTORIQUE		
Tous les événements		
Évén.Prioritaires		
Évén.Non Prioritaires		
Enregistrer		Disponible sur interface Web uniquement
Impression		Disponible sur interface Web uniquement
9. INFO		
Centrale		
Version		Indique la version logicielle, S/N, le n° de partition et la langue.
Customisation		Indique le code pour l'ajustement de centrale spécifique du client.
Communication		
RTC		
GSM/Mobile		Apparaît uniquement en cas d'intégration d'un module de téléphonie mobile.

Annexe

Réseau		Indique l'opérateur de réseau mobile et le RSSI (intensité de la réception)
IMEI		
N° de client		
IMSI		
Version	p. ex. 13.210.11.07.00	Firmware du modem du module de téléphonie mobile
Remise à zéro		
Ethernet		
Adresse IP		
Masque sous-réseau IP		
Passerelle adresse IP		
DNS adresse IP primaire		
Adresse MAC		
État Com.IP		
Modules hybrides		
	Pas de Périph.!	

Menu utilisateur

Option de menu	Programmation Usine Valeurs par défaut	Observations
1. UTILISATEUR		
Ajouter Utilisateur		Visible uniquement pour l'administrateur
Éditer Utilisateur		
« Utilisateur 001 »		Ne peut pas être supprimé
Nom		Cette valeur dépend de votre réponse aux questions « Longueur code d'accès » et « Code administrateur » lors de la première mise en service.
Type	Administrateur	
Partitions	1-4	
Code		Cette valeur dépend de votre réponse aux questions « Longueur code d'accès » et « Code administrateur » lors de la première mise en service.
Badge	Aucun	
Télécommande	Aucune	
Alarme anti-agression	Aucune	
Médaille Méd.	Aucun	
Émett.appel d'urg.soins	Aucun	
Supprimer Util.		Visible uniquement pour l'administrateur
2. MÉMO VOCAL		
Enregistrement		Temps d'enregistrement maximal = 30 s
Lecture	Aucune	
Effacer message		
3. ISOLER DES ZONES		
	Pas de Zones Isolables	
4. SORTIES ON/OFF		Apparaît uniquement lorsque l'installateur a configuré des sorties de type « Défini par U ».
5. CONFIGURATION		
Fonctions		Surface avant à touches
Carillon	Allumée	

Annexe

Annonce vocale	Allumée	
Moniteur d'activité	Désactivé	
Contraste de l'écran	100 %	
Luminosité du rétroéclairage	Élevée	
Rétroéclairage de l'écran LCD	Allumée	
Rétroéclairage des touches de menu	Désactivé	
Rétroéclairage des touches actives	Désactivé	
Rétroéclairage des touches numériques	Désactivé	
Annonce des noms de zone		Temps d'enregistrement maximal = 2 s pour chaque zone
Autorisé	Désactivé	
Zones IP	Enregistrement Lecture : Aucune Effacer message	Zone 101 à 106
Zones sans fil	Enregistrement Lecture : Aucune Effacer message	Zone 201 à 248
Zones filaires	Enregistrement Lecture : Aucune Effacer message	Zone 301 à 304
Redémarrer centrale		Visible uniquement pour l'administrateur et si : <ul style="list-style-type: none"> il n'y a aucune transmission à ce moment-là la centrale est désarmée.
Tonalités des touches	Allumée	Version logicielle >= 2.01.08
Fonctions		Touch Cover , version logicielle >= 2.01.08
Carillon	Allumée	
Annonce vocale	Allumée	
Moniteur d'activité	Désactivé	
Contraste de l'écran	100 %	
Luminosité du rétroéclairage	Élevée	
Rétroéclairage	Selon le délai	
Annonce des noms de zone		Temps d'enregistrement maximal = 2 s pour chaque zone
Autorisé	Désactivé	
Zones IP	Enregistrement Lecture : Aucune Effacer message	Zone 101 à 106
Zones sans fil	Enregistrement Lecture : Aucune Effacer message	Zone 201 à 248
Zones filaires	Enregistrement	Zone 301 à 304

	Lecture : Aucune Effacer message	
Redémarrer centrale		Visible uniquement pour l'administrateur et si : <ul style="list-style-type: none"> il n'y a aucune transmission à ce moment-là la centrale est désarmée.
Tonalités des touches	Allumée	
Rétroéclairage dynamique	Allumée	
Mode Nettoyage	Allumée	
Date et heure		Visible uniquement pour l'administrateur
Sync. heure SNTP		
Sync. heure SNTP	Désactivé	
Mode manuel		
RÉGLER DATE	01/01/2015	
RÉGLER L'HEURE	00:00 (hh:mm)	
ÉTÉ/HIVER	Automatique	
Éditer sorties		Visible uniquement pour l'administrateur et apparaît uniquement lorsque l'installateur a configuré des sorties de type « Défini par U ».
Télécommandes	Aucune	Visible uniquement pour l'administrateur
Réglages Volume		Visible uniquement pour l'administrateur
Tonalités opérateur	5	
Tonalités info	5	
Tonalités alarme	10	
Volume langue	50 %	
Volume Message	33 %	
Accès Web	Autorisé	Visible uniquement pour l'administrateur
Mises à jour de niveau 4	Bloqué	Visible uniquement pour l'administrateur
Calendrier Arm./Désarm.		Visible uniquement pour l'administrateur
Autorisé	Non	
Hebdomadaire		Événements : 160 Exceptions : 20
Notification Push	Aucune	
6. CONTACTS		Visible uniquement pour l'administrateur
Destinataires A-L		
Nom	Destinataires A-L	
N° de tél. 1	Vide	
N° de tél. 2	Vide	
E-mail	Vide	

Adresse IP	Vide	
ID utilisateur ID	Vide	
7. TEST		Visible uniquement pour l'administrateur
Test de détection	Pas de zones utilisées	
Sirènes et avertisseurs		
Sirènes int.	Désactivé	
Tension d'entrée CC externes	Pas de Périph.!	
Module Sirènes	Pas de Périph.!	
Haut-parleur	Arrêté	
Verrous de porte	Pas de Périph.!	
Sorties	Pas de sorties disponibles	
Badge	Aucun badge lu	
Télécommandes	Pas de Téléco enregistrée	
Émetteur d'appel d'urgence	Pas de médaillon enregistré	
Appel téléphonique	Vide	
8. HISTORIQUE		
9. INFO		Visible uniquement pour l'administrateur
Centrale		
Version		Indique la version logicielle, S/N, le n° de partition et la langue.
Communication		
RTC		
GSM/Mobile		Apparaît uniquement en cas d'intégration d'un module de téléphonie mobile.
Réseau		Indique l'opérateur de réseau mobile et le RSSI (intensité de la réception)
IMEI		
N° de client		
IMSI		
Version	p. ex. 13.210.11.07.00	Firmware du modem du module de téléphonie mobile
Remise à zéro		
Ethernet		
Adresse IP		
Masque sous-réseau IP		
Passerelle adresse IP		
DNS adresse IP primaire		
Adresse MAC		
État Com.IP		

Assistant de démarrage

LANGUE

APPLICATION MISE À NIVEAU DE LA CENTRALE D'ALARME

PROGRAMMATION PAYS

RÉGLER DATE

RÉGLER L'HEURE

HEURE D'ÉTÉ/HIVER

Automatique (réglage par défaut)

Manuel

MESSAGE DÉFAUT CA

OFF

ON (réglage par défaut)

MESSAGE DÉFAUT CC EXT.

OFF

ON (réglage par défaut)

BATTERIE 2

TYPE DE ZONE FILAIRE

SERVEUR WEB

Bloqué

Déverrouillé (réglage par défaut)

DHCP

Éteinte

Si OFF sélectionné

ADRESSE IP

MASQUE SOUS-RÉSEAU IP

PASSERELLE ADRESSE IP

DNS ADRESSE IP PRIMAIRE

On

(réglage par défaut)

PORT HTTP INTERNE

APERÇU

MODE D'APPEL (REPORTING CRA/STS)

Bloqué

Simple (réglage par défaut *en raison des exigences de la norme EN 50131*)

Alternatif

LONGUEUR DES CODES D'ACCÈS

Remarque

Ce menu vous permet également de supprimer tous les utilisateurs.

Veillez respecter pour cela les instructions sous Système -> Sécurité -> Code utilisateur à 6 chiffres.

CODE INSTALLATEUR

CONFIRMATION CODE INSTALLATEUR

CODE UTILISATEUR ADMINISTRATEUR

CONFIRMATION CODE UTILISATEUR ADMINISTRATEUR

IDENTIFICATION

Remarque à l'écran :

« Veuillez vérifier si de nouvelles versions logicielles sont disponibles. »

Remarque à l'écran :

Pour l'utilisation de codes sûrs.

Remarque à l'écran :

Établissement de certificats

Veille écran (avec date et heure)

Signaux sonores, acoustiques

La centrale peut générer une vaste gamme de signaux sonores acoustiques. Sur les périphériques tels que le clavier de commande, les sirènes d'intérieur/le module d'information, les générateurs de signal intérieurs et le haut-parleur du module hybride, ils ressemblent aux tonalités d'alarme, d'information et de commande de la centrale d'alarme sans fil.

Le tableau suivant fournit un aperçu des tonalités de signalisation et leur affectation de groupe correspondante.

Signaux sonores	Signification
Tonalités alarme	Cambriolage/Agression
	Incendie
	Alarme médicale
	Appel d'urgence de soin
Tonalités info	Carillon de porte
	Tonalité de sortie p. ex. Long bip continu (biiiiiiiiip) : Pendant la temporisation de sortie. Toutes les zones sont fermées, la centrale d'alarme est activée après écoulement de la temporisation.
	Tonalité de sortie en cas de défaut p. ex. Bips intermittents (bip...bip...bip) : Une zone a été ouverte pendant la temporisation de sortie. Elle doit être fermée avant le début de la temporisation.
	Tonalité d'entrée p. ex. Bips intermittents (bip...bip...bip) : Pendant la temporisation d'entrée.
	Avertissement d'appel d'urgence de soin, avertissement d'inactivité
Tonalités opérateur	Acquittement/Confirmation p. ex. Double bip (bip, bip) : La centrale d'alarme a bien été activée.
	Erreur p. ex. Court bip (bip) : Défaut au niveau de l'installation, la centrale d'alarme ne peut pas être activée



Remarque

Le volume des signaux sonores est réglable séparément pour chaque groupe.

Menu utilisateur -> Configuration -> Réglages Volume

Tonalités opérateur 0-10

Tonalités info 0-10

Tonalités alarme 0-10



Remarque

Ces réglages de volume ont simultanément un effet sur le volume de la centrale **et** du générateur de signal intérieur **et** du haut-parleur du module hybride.

Maintenance et entretien

Maintenance et entretien par l'installateur

La centrale d'alarme doit être vérifiée au moins une fois par an. À chaque inspection :

- Contrôlez la présence de signes manifestes de dommages sur le boîtier de Secvest ou à l'avant de ce dernier.
- Contrôlez le fonctionnement du bouton anti-sabotage du boîtier et du bouton anti-sabotage mural (contact d'arrachement mural)
- Vérifiez l'état des batteries de secours
- Vérifiez la présence de dommages ou les signes d'usure du câblage
- Vérifiez les signes manifestes de dommages sur le clavier
- Testez le fonctionnement de tous les boutons du clavier
- Nettoyez le clavier, l'écran et le boîtier
 - Après le nettoyage, essuyez la surface à l'aide d'un chiffon doux et sec.
 - N'utilisez pas d'eau, de solvants ni de produits de nettoyage.
- Contrôlez la puissance du signal et l'état des batteries/piles de tous les détecteurs, claviers de commande, sirènes d'extérieur et d'intérieur, générateurs de signal intérieurs, MAW, verrous de porte, modules hybrides, télécommandes, médaillons anti-agression, médaillons médicaux et médaillons de soins.
- Remplacez les piles ou batteries conformément aux instructions du fabricant.
- Testez chaque composant.
- Nettoyez soigneusement les objectifs de tous les détecteurs PIR et de toutes les caméras à l'aide d'un chiffon doux et sec propre.
- N'utilisez pas d'eau, de solvants ni de produits de nettoyage.
- Réalisez un test de détection de tous les détecteurs.
- Testez toutes les alarmes externes
- Testez la transmission.
- Par ailleurs, il convient de veiller au respect de la norme EN 50131-7 « Systèmes d'alarme - Systèmes d'alarme contre l'intrusion et les cambriolages - Partie 7 : Règles d'application ».

Utilisez les fonctions de test dans Mode Installateur -> Test

Aucune vérification des calibrages ou ajustements n'est nécessaire.

Maintenance et entretien par l'utilisateur

L'administrateur utilise les fonctions de test dans menu utilisateur -> Test

- Nettoyez la sirène
 - Après le nettoyage, essuyez la surface à l'aide d'un chiffon doux et sec.
 - N'utilisez pas d'eau, de solvants ni de produits de nettoyage.
- L'utilisateur ne doit pas effectuer d'autres travaux de maintenance.

Mise à niveau logicielle



Remarque

Version logicielle $\geq 3.00.03$

Il existe quatre possibilités de mise à niveau logicielle.

- Mise à niveau logicielle avec nouveaux fichiers enregistrés sur la carte SD.
- Mise à niveau logicielle avec nouveaux fichiers enregistrés sur le PC.
- Mise à niveau logicielle avec nouveaux fichiers déposés sur le serveur FTP.
- Mise à niveau logicielle avec Secvest Update Utility



Remarque

Mise à jour logicielle de 3.01.14 à 3.01.17

Mise à jour logicielle de versions antérieures à 3.01.17

- La centrale d'alarme sans fil Secvest peut revenir aux réglages d'usine lors de la mise à jour à V3.01.17.
- Par conséquent, il faut **impérativement sauvegarder la configuration** de la centrale au préalable. À l'issue de la mise à jour, la configuration peut être rétablie (ainsi que tous les ID de périphériques).
- Il est obligatoire d'effectuer la mise à jour du fichier de langue AVANT la mise à jour du fichier d'application !
- Niveau d'autorisation « Utilisateur de niveau 4 » pour les mises à jour logicielles
 - Les mises à jour logicielles via le menu Installateur du serveur Web ne sont plus possibles.
 - L'autorisation pour « Utilisateur de niveau 4 » doit être attribuée dans le menu utilisateur et installateur.
 - Le code utilisateur pour « Utilisateur de niveau 4 » est attribué après l'autorisation.
- Les réglages PUSH sont éventuellement perdus en raison de la mise à jour et doivent être contrôlés et testés !

Enregistrement sur le serveur ABUS

- Si la centrale d'alarme sans fil Secvest est utilisée en combinaison avec le serveur ABUS, celle-ci doit éventuellement être supprimée manuellement dans le compte du serveur ABUS.
 - Pour le contrôle, vous pouvez utiliser la fonction Trace. Avec X = 4 = « Client HTTPS », vous voyez le protocole de communication entre la centrale et le serveur ABUS. Si « MAC already in use » (MAC déjà en utilisation) y apparaît, la centrale doit être supprimée du compte du serveur ABUS. La centrale peut ensuite être saisie à nouveau.
- L'enregistrement s'effectue automatiquement sur le serveur ABUS au maximum 30 minutes après la réinitialisation de la configuration.

Historique de navigation

- Veuillez effacer le cache (historique de navigation) pour vous assurer que les fichiers JavaScript, CSS et d'images les plus récents sont chargés par la centrale.

Temps d'attente – Accès au serveur Web après redémarrage

- Après un redémarrage de la centrale, attendez au moins trois minutes avant d'accéder au serveur Web de la centrale.
- Lors du premier accès, le certificat https ainsi que d'autres caractéristiques de sécurité sont « échangés ».

Sauvegarde et réinitialisation de la configuration



Important

Lors d'une mise à jour importante, la programmation Usine du système d'alarme sans fil Secvest sont rétablis.

Par conséquent, il faut impérativement sauvegarder la configuration de la centrale au préalable :

1. « Mode Installateur »
2. « Système »
3. « Backup/Restaurer »
4. « Backup »

À l'issue de la mise à jour, la configuration peut être rétablie (ainsi que tous les ID de composants) :

5. « Mode installateur »
6. « Système »
7. « Backup/Restaurer »
8. « Charger configuration »



Remarque

Lorsqu'un processus de mise à niveau est en cours, vous voyez les 3 opérations suivantes sur la centrale d'alarme.

- 1)
 - Les touches de menu sont allumées.
 - Les touches activation/désactivation clignotent.
 - Les touches numériques sont sombres.
- 2)
 - Les touches de menu sont allumées.
 - Les touches activation/désactivation sont sombres.
 - Les touches numériques clignotent.
- 3)
 - Les touches de menu sont sombres.
 - Les touches activation/désactivation clignotent à nouveau pour signaler que le processus de mise à niveau se termine.
 - Les touches numériques sont sombres.

Le premier point de l'assistant de démarrage s'affiche (sélection de langue).



Important

Attendez que ce processus soit entièrement terminé. N'interrompez en aucun cas l'alimentation électrique pendant le processus de mise à niveau. Cela peut entraîner une panne/défaillance totale du logiciel.

Si une surface avant tactile est montée, aucune touche n'est allumée pendant ce processus.



Important

Attendez jusqu'à ce que quelque chose s'affiche à nouveau à l'écran. N'interrompez en aucun cas l'alimentation électrique pendant le processus de mise à niveau. Cela peut entraîner une panne/défaillance totale du logiciel.

Set de fichiers logiciels pour V3.01.17

Logiciel Titre	Logiciel Version	Logiciel Noms de fichier	Taille de fichier sur le disque
			Affichage PC du système d'exploitation
Core	V3_01_17	13410164_FUAA50XXX_App_V3_01_17.bin	2 880 Ko
		Taille de fichier en octets Affichage GUI : 2.949.120	
Langues			
Français	V1_42	13404974_FUAA50XXX_Deutsch_V1_42.Ing	2 347 Ko
English	V1_35	13404973_FUAA50XXX_English_V1_35.Ing	1 864 Ko
Néerlandais	V1_17	13404976_FUAA50XXX_Nederlands_V1_17.Ing	2 281 Ko
Français	V1_17	13404975_FUAA50XXX_Francais_V1_17.Ing	2 328 Ko
Italien	V1_16	13404978_FUAA50XXX_Italiano_V1_16.Ing	2 521 Ko
Danois	V1_19	13404977_FUAA50XXX_Dansk_V1_19.Ing	1 791 Ko
Suédois	V1_13	13405100_FUAA50XXX_Svenska_V1_13.Ing	2 346 Ko
Espagnol	V1_13	13404979_FUAA50XXX_Espanol_V1_13.Ing	2 379 Ko
Polonais	V1_13	13405101_FUAA50XXX_Polski_V1_13.Ing	2 177 Ko
Russe	V1_10	13405102_FUAA50XXX_Pycck_V1_10.Ing	2 534 Ko
Test de confiance			
ConfTest	V1_03	12551477_FUAA50XXX_ConfTest_V1_03.Ing	32 Ko
Programmes d'aide Accessoires			
Configuration utilitaire de mise à jour Secvest 32	V1.02.05	Setup Secvest Update Utility 1_02_05 (32 bit).msi	
Configuration utilitaire de mise à jour Secvest 64	V1.02.05	Setup Secvest Update Utility 1_02_05 (64 bit).msi	
Bootloader	V1_00_00	12526869_FUAA50XXX_Boot_V1_00_00.bin	42

Mise à niveau logicielle avec nouveaux fichiers depuis la carte SD

Centrale

Mode Installateur -> Système -> Généralités-> Langue

Mode Installateur -> Système -> Mise à niveau de la centrale



Remarque

Il est obligatoire d'effectuer la mise à jour du fichier de langue AVANT la mise à jour du fichier d'application !

La note de publication correspondante « Secvest_Software_Release_Notes_Va_bc_de_yyyy_mm_dd » vous indique quelle version de fichier de langue est compatible avec quelle version de fichier d'application.

exemple

Mode Installateur -> Système -> Mise à niveau de la centrale

APPLICATION MISE À NIVEAU DE LA CENTRALE D'ALARME		
V3.01.14	Installée	
V1.01.00	10/02/2016	(2293760)
V2.00.00	04/10/2016	(2621440)
V2.00.06	06/03/2017	(2621440)
V2.01.08	15/06/2017	(2686976)
V3.00.04	12/12/2017	(2883584)
V3.01.01	10/05/2018	(2883584)
V3.01.11	17/10/2018	(2883584)
V3.01.14	11/03/2019	(2949120)
V3.01.16	25/11/2019	(2949120)

Mise à niveau logicielle avec nouveaux fichiers sur le PC



Important

Sauvegarde et réinitialisation de la configuration

Lors d'une mise à jour importante, la programmation Usine du système d'alarme sans fil Secvest sont rétablis.

Par conséquent, il faut impérativement sauvegarder la configuration de la centrale au préalable :

1. Serveur Web « Mode Installateur »
2. « Système »
3. « Backup/Restaurer »
4. « Backup »

À l'issue de la mise à jour, la configuration peut être rétablie (ainsi que tous les ID de composants) :

5. Serveur Web « Mode Installateur »
6. « Système »
7. « Backup/Restaurer »
8. « Charger configuration »



Important

Version logicielle >= 3.00.06, sauvegarde et réinitialisation de la configuration

Avant que la centrale ne démarre la mise à niveau, les données de configuration et le certificat SSL sont automatiquement enregistrés dans le flash interne. Le nouveau logiciel est alors installé et la centrale est redémarrée. La programmation Usine est alors tout d'abord utilisée, mais la centrale restaure ensuite automatiquement les données de configuration et le certificat SSL du flash (tout comme si vous aviez enregistré/réinitialisé la configuration manuellement). Cela signifie que l'assistant de démarrage n'est pas exécuté, que le certificat SSL n'est pas généré à nouveau, et plus important encore, que l'installateur ne doit pas se rendre sur place pour répondre aux exigences de saisie de l'assistant de démarrage.



Important

Avec la version logicielle 2.00.00, des modifications ont été apportées dans les menus suivants

- Setup Transmission VoIP
- Contacts -> ID utilisateur SIP
- Sorties -> Type « Défini par U »
- AES/NSL Reporting -> Port IP

Après lecture, veuillez contrôler la configuration de ce menu et adapter les réglages en conséquence.

Mises à jour de niveau 4

Préparation :

Ajouter un nouvel « utilisateur de niveau 4 »

Centrale

Mode Installateur -> Système -> Sécurité -> Mises à jour de niveau 4 -> Autorisé

ou

INTERFACE WEB

Mode Installateur -> Système -> Réglages de sécurité -> Mises à jour de niveau 4 -> Autorisé (coché)

Lorsque cette option est autorisée, il faut saisir un nouveau code de niveau 4. Ceci ne s'applique que si ce code de niveau 4 n'a jamais été programmé au préalable (depuis la livraison ou depuis la dernière réinitialisation de la programmation Usine). Ce code de niveau 4 comporte le même nombre de chiffres que le code installateur ou le code utilisateur.

Entrée du « nouveau code de niveau 4 » et « confirmation du code de niveau 4 » (saisir une nouvelle fois le code pour confirmation).

Un nouvel utilisateur est automatiquement créé. Voir le menu utilisateur « Utilisateur ».

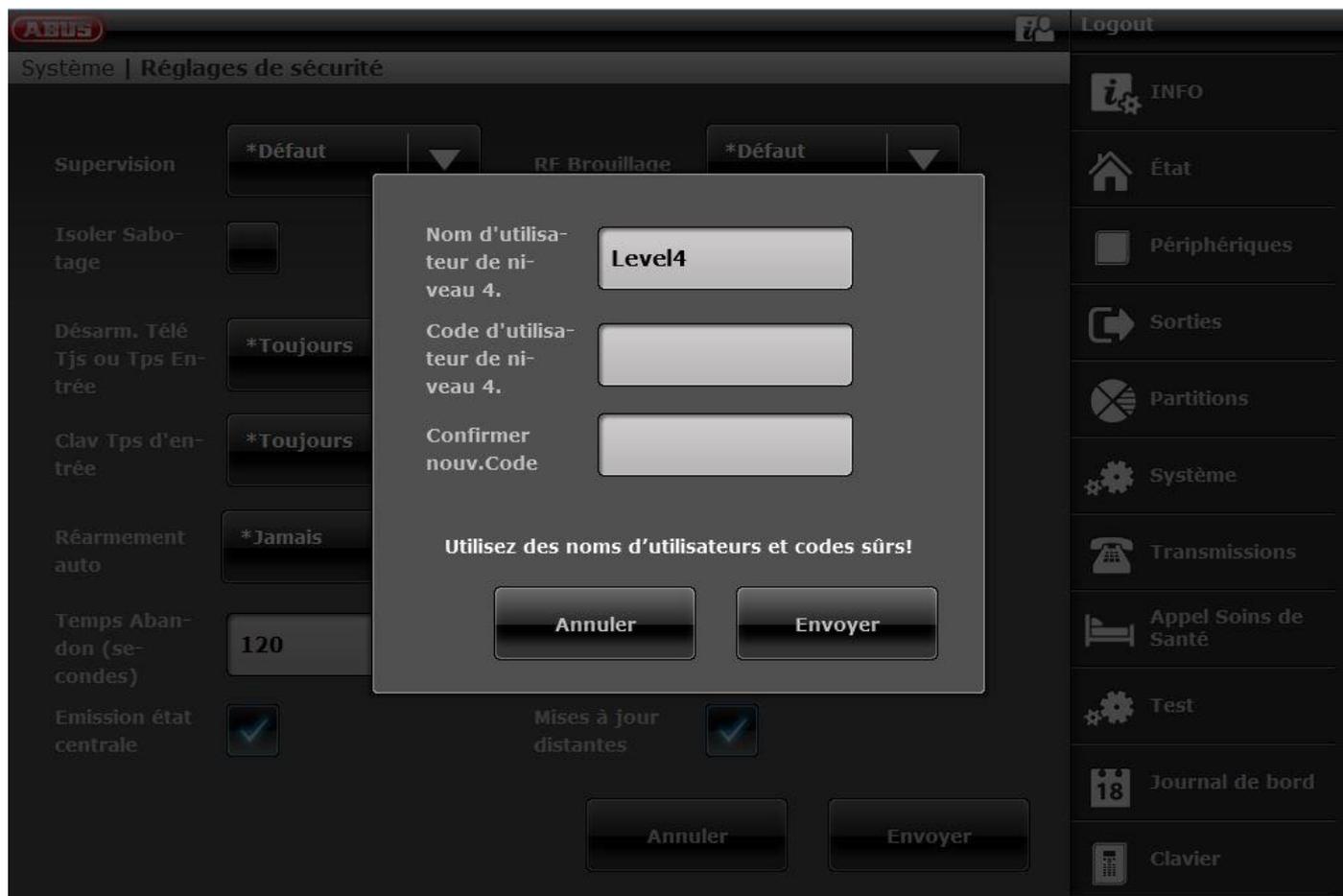
Nom : « Niveau 4 »

Remarque :

Pour des raisons de sécurité, vous devez modifier le nom par défaut « Niveau 4 » de l'utilisateur de niveau 4.

Remarque :

Vous trouverez des détails supplémentaires dans les descriptions des menus, dans les instructions correspondantes.



Début de la procédure de « Mise à jour distante » :

Assurez-vous que

Centrale

Mode Installateur -> Système -> Sécurité -> Mises à jour de niveau 4 -> Autorisé

Menu utilisateur -> Configuration -> Mises à jour de niveau 4 -> Autorisé

ou

INTERFACE WEB

Mode Installateur -> Système -> Réglages de sécurité -> Mises à jour de niveau 4 -> Autorisé (coché)

Menu utilisateur -> Configuration -> Réglages de sécurité -> Mises à jour de niveau 4 -> Autorisé (coché)

Lorsqu'un utilisateur de niveau 4 se connecte au serveur Web à l'aide de son nom et de son code d'utilisateur de niveau 4, si les deux options de « mise à jour distante » sont autorisées, seules trois options de menu sont affichées pour cet utilisateur :

Coordonnées de l'utilisateur de niveau 4 pour modification

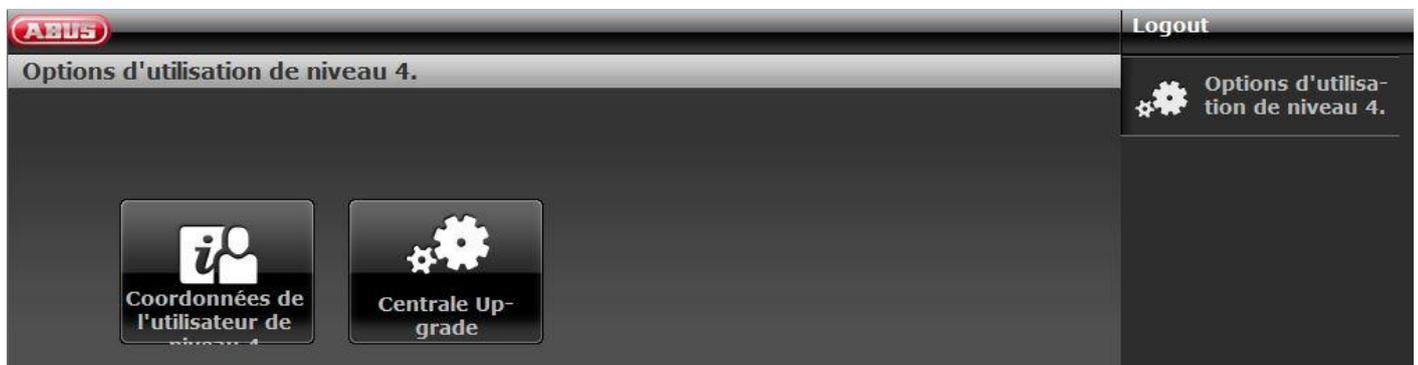
Nom d'utilisateur de niveau 4.

Code d'utilisateur de niveau 4.

et

Mise à niveau de la centrale

Ces options ne sont pas affichées si vous vous connectez en tant qu'installateur.



Version logicielle >= 3.00.03

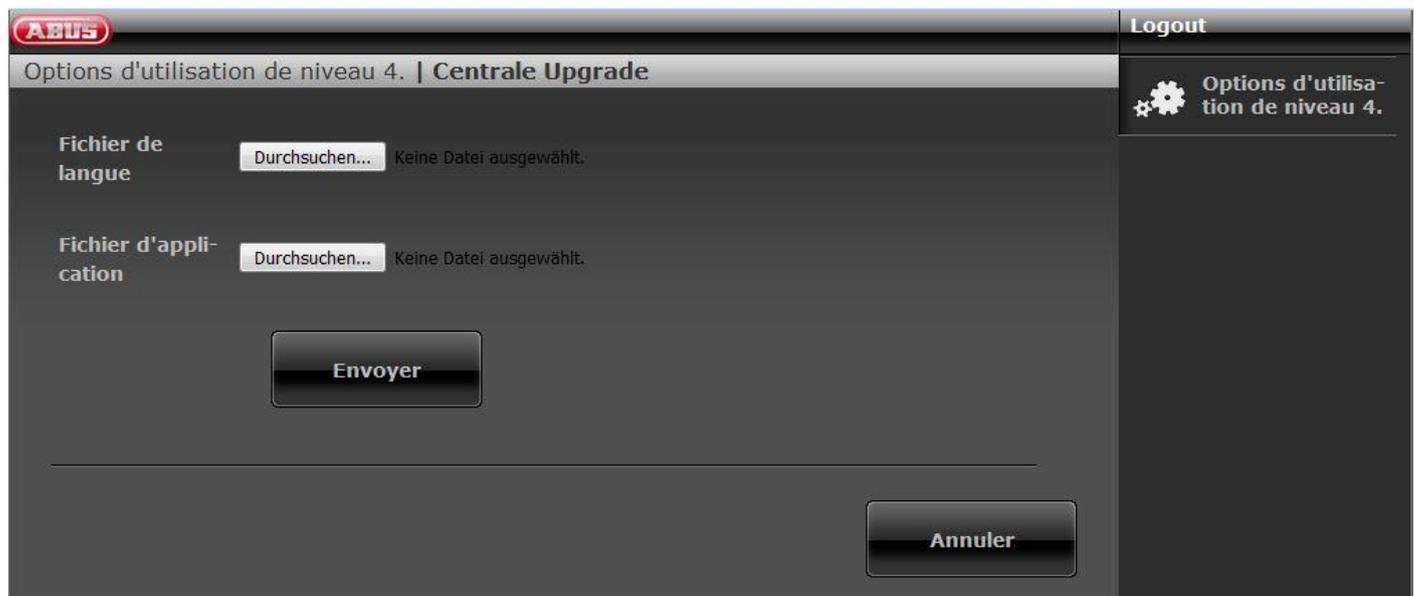


Remarque



En cliquant sur ce symbole, vous obtenez le fichier « Notes de publication » au format PDF.

Cliquez sur « Centrale Upgrade »



Version logicielle >= 3.00.03



Important

Veillez à charger uniquement

- un fichier de langue compatible avec le fichier d'application existant ou
- un fichier d'application compatible avec le fichier de langue existant
- un fichier de langue et un fichier d'application compatibles entre eux

Consultez les notes de publication à ce sujet.

Sélectionnez un « fichier de langue »

Cliquez sur le bouton « **Parcourir** » pour indiquer le chemin d'accès et le nom du fichier de langue à charger.
Cliquez sur le bouton « **Envoyer** » pour importer le fichier sélectionné dans le système d'alarme sans fil.

Sélectionnez un « fichier d'application »

Cliquez sur le bouton « **Parcourir** » pour indiquer le chemin d'accès et le nom du fichier d'application à charger.
Cliquez sur le bouton « **Envoyer** » pour importer le fichier sélectionné dans le système d'alarme sans fil.

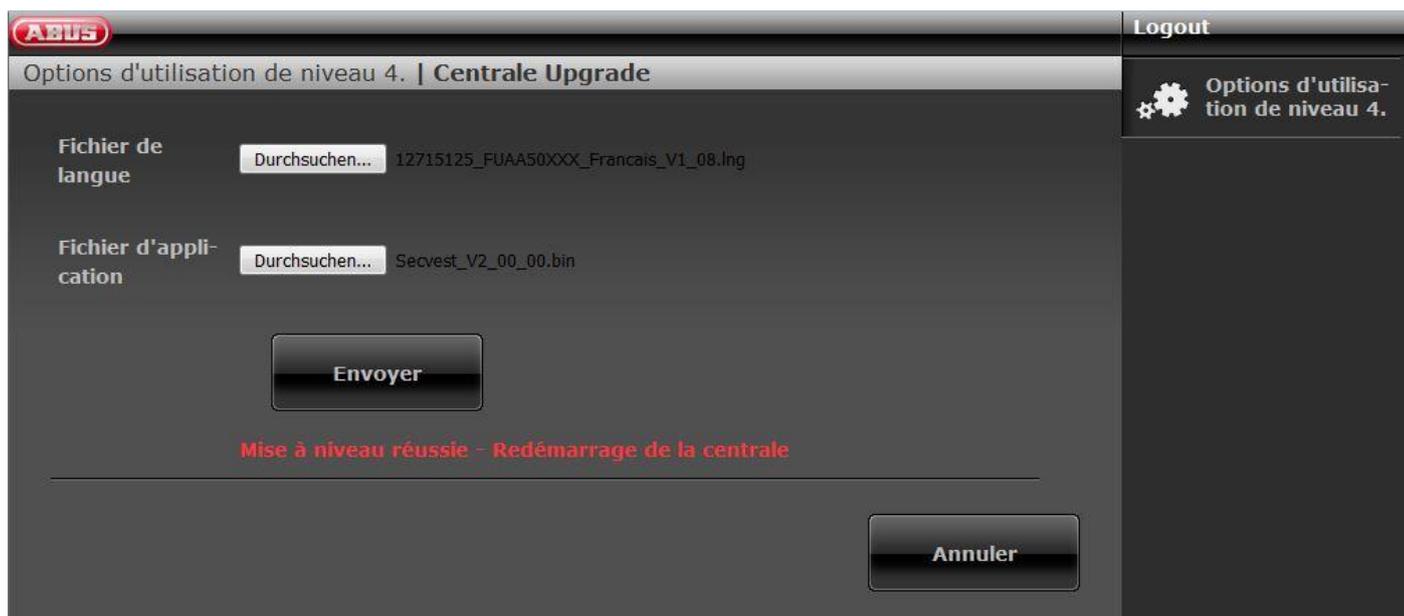
Vous pouvez également effectuer ces deux actions simultanément.

Sélectionnez un « fichier de langue ».

Sélectionnez un « fichier d'application ».

Cliquez sur « Envoyer ».

Une fois le téléchargement terminé, la centrale compare le numéro de configuration du logiciel actuel avec le numéro de configuration du logiciel téléchargé. S'ils concordent, la centrale redémarre automatiquement et installe le nouveau logiciel.



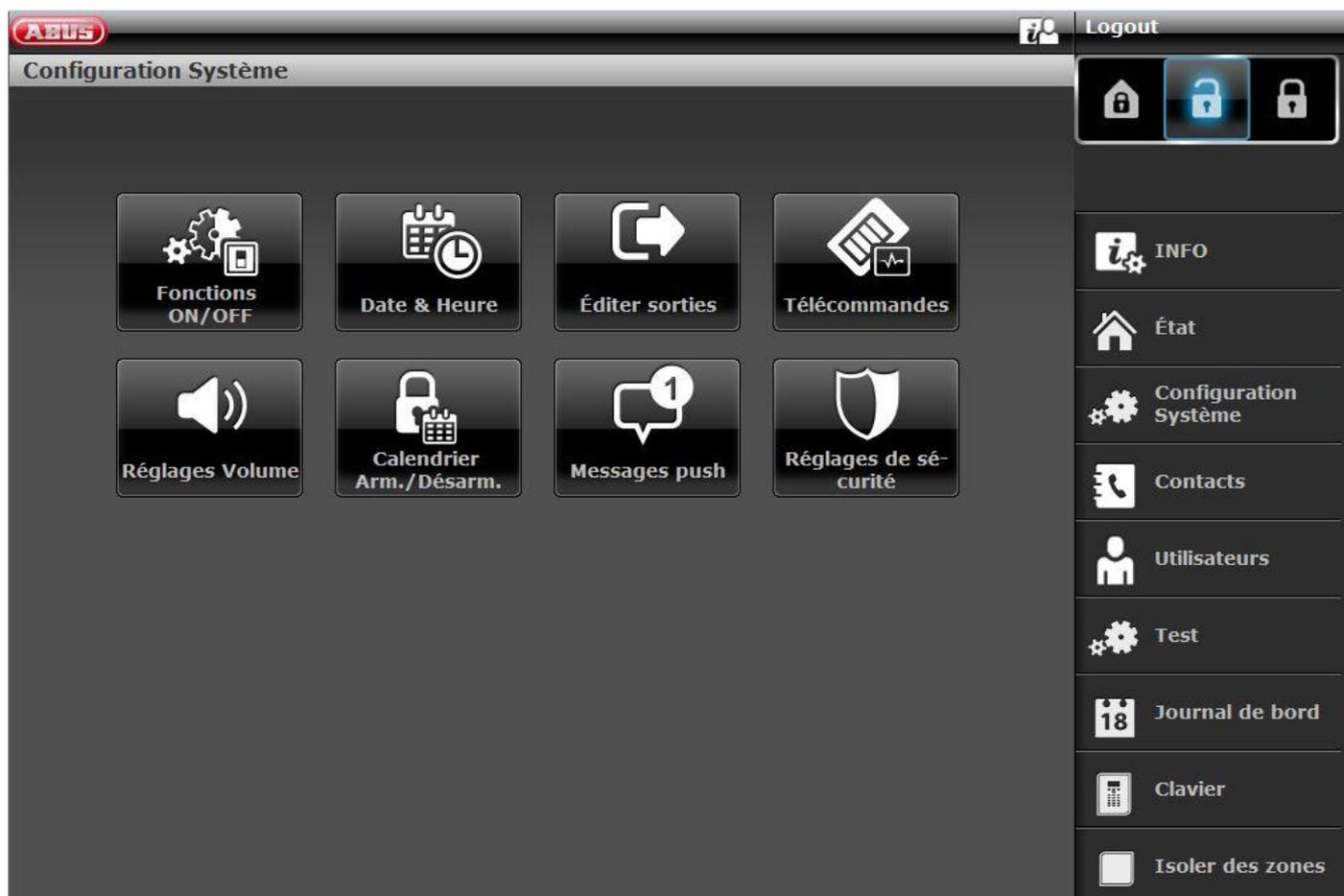
S'ils ne concordent pas, le serveur Web avertit l'utilisateur que la centrale va redémarrer, que sa configuration va être réinitialisée et que l'installateur être sur place pour la reconfigurer (la centrale reste au niveau de l'« assistant de démarrage »).

Si l'utilisateur choisit l'option « Non », le fichier téléchargé est supprimé de la carte SD.

Cela permet d'éviter qu'un utilisateur de niveau 3 se présente sur place et installe le nouveau logiciel à partir de la carte SD sans ouvrir la centrale. Cette opération est interdite pour un utilisateur de niveau 3, à moins que la centrale soit ouverte.

Notez que le contrôle du numéro de configuration mentionné ci-dessus est effectué uniquement sur les centrales sur lesquelles une version du logiciel a déjà cette fonction (version 1.01.00 et supérieures).

Voir également le manuel d'utilisation chapitre Mises à jour distantes/Mises à jour de niveau 4.





Centrale

Menu utilisateur -> Configuration -> Mises à jour de niveau 4

ou

INTERFACE WEB

Menu utilisateur -> Configuration -> Réglages de sécurité -> Mises à jour de niveau 4

Bloqué (désactivé - option décochée)

Un utilisateur de niveau 4 peut uniquement modifier le « code de niveau 4 » et le « nom d'utilisateur de niveau 4 ».

Autorisé (activé, option cochée)

Lorsqu'un utilisateur de niveau 4 se connecte au serveur Web à l'aide de son nom et de son code d'utilisateur de niveau 4, si l'option de « mise à jour distante » est autorisée en mode Installateur, seules trois options de menu sont affichées pour cet utilisateur :

Coordonnées de l'utilisateur de niveau 4 pour modification

Nom d'utilisateur de niveau 4.

Code d'utilisateur de niveau 4.

et

Mise à niveau de la centrale



Remarque

Création du certificat SSL en cours, ceci peut durer quelques minutes (env. 3 minutes).
Les fonctions réseau ne sont pas disponibles pendant ce temps.



Remarque

Le message suivant s'affiche : Initialisation réseau, veuillez patienter...



Remarque

Lorsqu'un processus de mise à niveau est en cours, vous voyez les 3 opérations suivantes sur la centrale d'alarme.

- 1)
 - Les touches de menu sont allumées.
 - Les touches activation/désactivation clignotent.
 - Les touches numériques sont sombres.
- 2)
 - Les touches de menu sont allumées.
 - Les touches activation/désactivation sont sombres.
 - Les touches numériques clignotent.
- 3)
 - Les touches de menu sont sombres.
 - Les touches activation/désactivation clignotent à nouveau pour signaler que le processus de mise à niveau se termine.
 - Les touches numériques sont sombres.

Le premier point de l'assistant de démarrage s'affiche (sélection de langue).



Important

Attendez que ce processus soit entièrement terminé. N'interrompez en aucun cas l'alimentation électrique pendant le processus de mise à niveau. Cela peut entraîner une panne/défaillance totale du logiciel.

Si une surface avant tactile est montée, aucune touche n'est allumée pendant ce processus.



Important

Attendez jusqu'à ce que quelque chose s'affiche à nouveau à l'écran. N'interrompez en aucun cas l'alimentation électrique pendant le processus de mise à niveau. Cela peut entraîner une panne/défaillance totale du logiciel.

Mise à niveau logicielle avec nouveaux fichiers depuis le serveur FTP

Version logicielle \geq 3.00.03



Remarque

Tenez également compte des remarques contenues dans le chapitre ci-dessus.

Cette fonction est également disponible directement sur la centrale d'alarme. Vous trouverez des détails à ce sujet dans le chapitre Système -> Contrôle de la mise à niveau ?

Connectez-vous au serveur Web en tant qu'utilisateur de niveau 4.

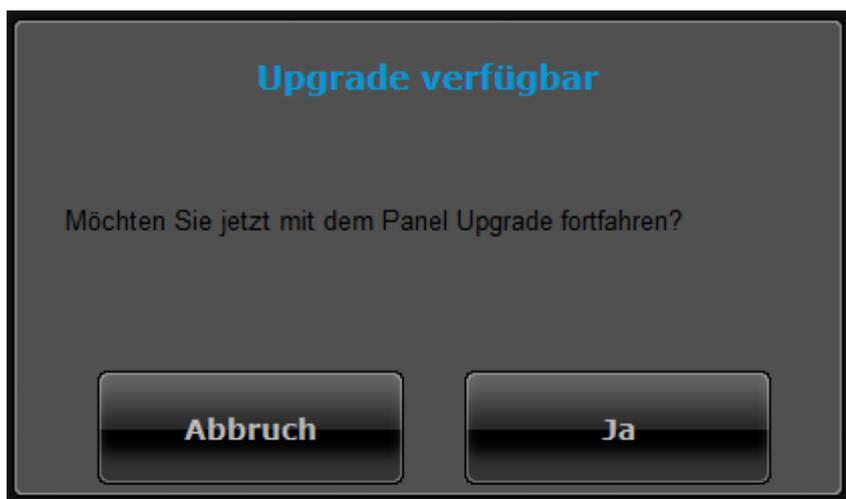


Après connexion, le logiciel interroge automatiquement le serveur FTP ABUS : « De nouveaux logiciels sont-ils disponibles ? ».

Vous pouvez également redémarrer cette opération manuellement.

Cliquez sur « Contrôle de la mise à niveau ? ».

Si le serveur FTP répond « Oui », les menus contextuels suivants s'ouvrent.





Remarque

Le logiciel actuel comprend un nouveau fichier d'application et un nouveau fichier de langue. Ces fichiers ont été enregistrés sur la carte SD.



Cliquez sur « Redémarrage de la centrale d'alarme ». La centrale d'alarme installe les nouveaux fichiers et redémarre.



Important

Version logicielle >= 3.00.06, sauvegarde et réinitialisation de la configuration

Avant que la centrale ne démarre la mise à niveau, les données de configuration et le certificat SSL sont automatiquement enregistrés dans le flash interne. Le nouveau logiciel est alors installé et la centrale est redémarrée. La programmation Usine est alors tout d'abord utilisée, mais la centrale restaure ensuite automatiquement les données de configuration et le certificat SSL du flash (tout comme si vous aviez enregistré/réinitialisé la configuration manuellement). Cela signifie que l'assistant de démarrage n'est pas exécuté, que le certificat SSL n'est pas généré à nouveau, et plus important encore, que l'installateur ne doit pas se rendre sur place pour répondre aux exigences de saisie de l'assistant de démarrage.

Mise à niveau logicielle avec Secvest Update Utility

Cette variante est conçue pour des cas spéciaux.

Pour plus de détails, consultez les installateurs spécialisés de notre assistance

AES / TS Reporting

Formats de protocole AES/TS Reporting

Remarque :

En vue de la conformité avec la norme EN 50131, AES (TS) Reporting doit être activé.

La centrale utilise automatiquement les protocoles classiques si elle utilise le standard RTC ou GSM/Mobile pour la communication sortante.

Format rapide

Lors de l'utilisation du format rapide, chaque message transmis à AES (TS) se compose des éléments suivants :

un ID client à 4, 5 ou 6 chiffres.

8 canaux de données.

Chaque canal indique l'état d'une sortie. Le type de la sortie (canal) est défini dans le menu « Canaux FF » (voir page xyz). Chaque canal peut transmettre les valeurs suivantes :

1 = nouvelle alarme non déclenchée jusqu'à présent

2 = sortie ouverte/désactivée

3 = alarme réinitialisée et non déclenchée jusqu'à présent

4 = sortie fermée/activée

5 = aucune alarme

6 = alarme déjà déclenchée plus tôt

Signal de test ou état

Contact ID

Le format Contact ID transmet les données des entrées du journal de bord à AES (TS). Exemples de messages au format Contact ID :

Exemple 1

1234 18 1137 01 015 2

1234	est l'ID client tel que spécifié dans le menu ID Client (page xyz).
18	est le type de message utilisé pour identifier le message en tant que Contact ID.
1137	est le numéro d'événement d'un nouvel événement (1), suivi du code d'événement d'une alarme de sabotage du système (137)
01	correspond au numéro de la partition
015	correspond au numéro de zone
2	numéro de somme de contrôle dont AES (TS) a besoin pour vérifier et confirmer qu'un message valide a été reçu

Exemple 2

1234 18 3137 01 015 3

L'unique différence entre cet exemple et le premier est le 3 qui caractérise le numéro d'événement pour afficher une réinitialisation de l'alarme de sabotage du système, et celui correspondant à la valeur de la somme de contrôle.

SIA 1, SIA 2, SIA 3, Extended SIA 3 et Extended SIA 3 V2

Les formats SIA transmettent les données des entrées du journal de bord à AES (TS).

Les quatre formats SIA se distinguent selon la quantité des données transmises avec chaque message.

Type	Format
SIA1	#AAAAAA NCCcc
SIA2	#AAAAAA Nidnnn/rinn/CCcc
SIA3	#AAAAAA Ntiah:mm/idnnn/rinn/CCcc #AAAAAA AS
Extended SIA 3	#AAAAAA Ntiah:mm/idnnn/rinn/CCcc/AS
Extended SIA 3 V2	#AAAAAA Ntiah:mm idnnn rinn CCcc AS
Extended SIA 3 V3	#AAAAAA Ntiah:mm/idnnn/rinn/CCcc^AS^

Où :

AAAAAA	ID client réglable à 6 chiffres (123456, p. ex.).
"N"	Nouvel événement (toujours N)
"ti"hh:mm/	Heure (ti10:23/, p. ex.).
"id"nnn/	Numéro utilisateur, si applicable, sinon, non envoyé (id123/ ou id6/, p. ex.)
"ri"nn/	Numéro de partition (ri12/ ou ri3, p. ex.).
NC	Code d'événement (p. exemple, FA = Alarme Feu).
cc	Numéro de zone ou de claviers, si applicable, sinon, non envoyé (p. ex. 23 ou 5)
"A"S	Description de l'événement, en général la description de l'événement de journal de bord

Remarque :

La centrale d'alarme envoie les caractères figurant entre « et » représentés ci-dessus de façon fidèle, tels qu'ils sont répertoriés dans le tableau ci-dessus.

exemple

Dans le cas d'une alarme incendie de la zone 2 de la partition 4 à 10:15 avec l'ID client 10 pour la partition 4, les différents formats pour le protocole SIA se présentent comme suit :

SIA1	#000010 NFA2
SIA2	#000010 N/ri4/FA2
SIA3	#000010 Nti10:15/ri4/FA2 #000010 AFire Zone 2
Extended SIA3	#000010 Nti10:15/ri4/FA2/AFire Zone 2
Extended SIA3 V2	#000010 Nti10:15 ri4 FA2 AFire Zone 2
Extended SIA3 V3	#000010 Nti10:15/ri4/FA2^AFire Zone 2^

Remarque concernant le format Extended SIA3 V2 :

Certaines versions logicielles à l'œuvre dans les destinataires SIA ne détectent pas toujours le séparateur de texte « / ». Cela peut provoquer des problèmes. Des messages « erreur réseau » indus apparaissent au niveau de l'AES (TS). Cela peut se produire lors de l'activation ou de la désactivation de la centrale ou de l'activation ou de la désactivation du mode Installateur.

Par conséquent, dans la version 2 du format Extended SIA3, le séparateur de texte « / » a été remplacé par « | ».

Ainsi, la chaîne :

#000010|Nti10:15/ri4/FA2/AFire Zone 2

devient :

#000010|Nti10:15|ri4|FA2|AFire Zone 2

Si vous rencontrez des problèmes de messages d'« erreur réseau » incorrects, testez cette option SIA3 V2 étendue.

Remarque concernant le format Extended SIA3 V3 :

Certaines versions logicielles à l'œuvre dans les destinataires SIA ne détectent pas toujours le séparateur de texte « / ». Cela peut provoquer des problèmes.

Par conséquent, dans la version 3 du format Extended SIA3, le séparateur de texte « / » a été remplacé à deux positions et complété par un séparateur de texte « ^ ».

Ainsi, la chaîne :

#000010|Nti10:15/ri4/FA2/AFire Zone 2

devient :

#000010|Nti10:15/ri4/FA2^AFire Zone 2^

DC-09



Remarque

Les règles du document suivant s'appliquent ici.

**ANSI/SIA DC-09-2013 : Internet Protocol Event Reporting
SIA Digital Communication Standard – Internet Protocol
Event Reporting**

Version logicielle <= v3.00.03 Les messages sont envoyés **sans cryptage (non cryptés)**.

Version logicielle >= v3.00.03 Les messages peuvent également être envoyés **avec cryptage**.

Le protocole DC-09 basé sur IP est automatiquement utilisé par la centrale lorsque cette dernière utilise le standard Ethernet (LAN) pour la communication sortante.

Ce faisant, les données des protocoles classiques sont regroupées en paquets IP et transmises.

Remarque :

Vous pouvez trouver des détails dans les spécifications DC-09 et DC-07 de SIA et dans les standards applicables mentionnés dans ce document.

Les **jetons** utilisés sont les suivants :

Protocole	Jeton	Définition
FF	« SCN-S8 »	Scancom 4-8-1, 5-8-1, 6-8-1
CID	« ADM-CID »	Ademco Contact ID
SIA 1, SIA 2, SIA 3, Ex SIA 3, Ex SIA 3 V2, Ex SIA 3 V3	« SIA-DCS »	SIA DCS

TCP

Lors de la transmission, le protocole Internet **TCP** est utilisé.



Remarque

TCP utilise le port 9999.

Si les messages ne peuvent être envoyés, il peut arriver dans certaines circonstances que le pare-feu verrouille également différents ports **sortants**. Contrôlez par conséquent les réglages du pare-feu au niveau du routeur ou d'IAD.

Remarques relatives à l'implémentation dans la Secvest par rapport au chapitre 5.5.1 « Event Messages (PE) » des spécifications DC-09.

Sommaire	Chapitre DC-09-Spéc.	Utilisation dans la Secvest	Remarques
LF	5.5.1.1	Oui	
CRC	5.5.1.2	Oui	
0LLL	5.5.1.3	Oui	
ID	5.5.1.4	Oui	Jeton, voir ci-dessus
Séq.	5.5.1.5	Oui	
Rrcvr	5.5.1.6.3	Non	Aucun envoi
Receiver Number			
Lpref	5.5.1.6.2	Non	L0 a été envoyé
Préfixe Account			
#acct	5.5.1.6.1	Oui	
Account Number			
Pad	5.5.1.7	Oui	Entre parenthèses « [» et «] »
Données	5.5.1.7	Oui	Entre parenthèses « [» et «] »
Horodatage	5.5.1.9	Oui	Messages cryptés uniquement. Correspond à GMT L'écart (inexactitude) entre le temps de la centrale d'alarme et le temps du destinataire CRA/STS peut être de +20 à -40 secondes maximum.
CR	5.5.1.10	Oui	

**Remarque**

Un fuseau horaire est une zone composée de plusieurs États et de parties d'États plus grands dans laquelle la même heure réglementée officiellement s'applique.

Le temps zonal indique l'écart entre l'heure locale et le TUC (temps universel coordonné) ou GMT (Greenwich Mean Time, temps moyen de Greenwich).

Exemple pour la France :

- Heure d'hiver : UTC/GMT +1
- Heure d'été : UTC/GMT +2

Événements CID / SIA

Ce menu apparaît uniquement si vous sélectionnez « Contact ID » ou une autre version SIA à l'emplacement suivant :
Mode Installateur -> Transmission -> TS Reporting -> Protocole

Vous trouverez une description détaillée des formats CID et SIA dans l'annexe « Formats de protocole AES (TS) Reporting »

Pour faciliter la programmation, les événements CID/SIA possibles sont rassemblés dans des groupes. Les tableaux 1 et 3 présentent les événements CID/SIA et l'affectation de groupe correspondante. Les tableaux 2 et 4 présentent les groupes et les événements CID/SIA correspondants.

Si vous autorisez un groupe avec Oui, la centrale peut envoyer chaque événement de ce groupe.

Remarques :

Les transmissions d'alarme CID/SIA nécessitent beaucoup plus de temps que le format rapide Scancom, étant donné que le système transfère des données d'alarme étendues au centre de réception des alarmes (AES, TS).



Remarque

La centrale reporte le TS Reporting ou l'entrée dans le journal de bord d'environ 15 à 22 minutes (choix aléatoire) en cas de panne de réseau (coupure de courant) ou lorsque vous quittez le mode Installateur en présence d'une panne de réseau (coupure de courant).

La centrale reporte le TS Reporting ou l'entrée dans le journal de bord d'environ 60 à 90 secondes (choix aléatoire), en cas de rétablissement de l'alimentation électrique ou lorsque vous quittez le mode Installateur et que l'alimentation électrique est rétablie.

Tableau 1 Codes CID - Groupes de rapport CID

Code CID	Contient :	Groupe de rapport CID
100	Alarme médicale	Alarme Alarme
101	Appel Soins de santé (urgence soins)	Alarme Alarme
110	Feu et Feu OK	Incendie
120	Agression zone (panique) et OK Agression (panique) silence et OK Agression clavier (panique) et OK Agression RF (panique) et OK Agression clavier sans fil (panique) et OK	Alarme anti-agression
121	Alarme code contrainte	Alarme anti-agression
129	Alarme agression (panique) confirmée	Alarme anti-agression
130	Intrusion et Intrusion OK	Alarme intrusion
131	Enveloppe extérieure/périmètre et enveloppe extérieure/périmètre OK Tentative d'effraction par levier et bris de glace par ex. du FTSE	Alarme intrusion
137	Sabotage du boîtier de la centrale et OK Sabotage du clavier et OK Sabotage du détecteur et OK Sabotage du clavier et OK Sabotage de la sirène et OK Sabotage du clavier sans fil et OK Sabotage des sirènes externes et OK Sabotage MAW et OK Sabotage du verrou de la porte et OK	Sabotages
139	Confirmation alarme	Alarme intrusion
150	Alarme technique et OK	Technique
150	Boîtier clé ouvert et fermé	Boîtier clé
300	Défaut et OK pour : AUX 12 V, système 12 V	Anomalies
301	Défaut secteur A/C et OK Centrale, MoHy	Défaut secteur
302	Batt. centrale vide/défaut et OK	Batt. centrale
305	Système ou partition réinitialisé(e)	Remise à zéro
311	Batt. centrale vide/manquante et OK	Batt. centrale
311	Défaut batterie externe et OK	Anomalies
320	Défaut zone sirène externe et OK Défaut MAW et OK	Anomalies
337	Générateur de signal int., clavier de commande, répéteur, MoHy, détecteur autonome avertisseur de fumée, MAW Défaut PSU et OK	Batt.Rad. /PSU
337	Défaut PSU externe et OK via zone n MoHy	Anomalies
338	Sirène externe, MAW, répéteur	Batt.Rad. /PSU

Annexe

	Défaut batterie/pile vide et OK	
338	PSU externe tension faible via zone n	Anomalies
342	Défaut A/C PSU externe et OK	Anomalies
344	Défaut brouillage et ok 1)	RF Brouillage
351	Défaut voie de communication et OK	Anomalies
373	Défaut détecteur de fumée et OK	Anomalies
375	Défaut zone périphérique agression et OK	Anomalies
380	Défaut supervision caméra de zone IP et OK (par ex. IP Zone Missing, IP-Zone Timeout).	Supervision caméra
381	Défaut supervision de zone et OK Défaut supervision du clavier sans fil et OK Défaut supervision de sirène externe et OK 1) Défaut supervision de générateur de signal int. et OK Défaut supervision MAW et OK Défaut supervision de verrou de porte et OK Défaut supervision de répéteur et OK Défaut supervision MoHy et OK	RF Supervision
384	Défaut zone batterie vide et OK	Batt.Rad. /PSU
401	Système ou partition activé(e) et désactivé(e)	Armement/Désarmement
401	Système ou partition activé(e) en interne	Act. interne
406	Alarme annulation	Alarme intrusion
409	Système ou partition activé(e) et désactivé(e) avec un interrupteur à clé	Armement/Désarmement
409	Système ou partition activé(e) en interne avec un interrupteur à clé	Act. interne
412	Téléchargement réussi	Télécharger
457	Sortie timeout et OK	Sortie timeout
461	Saisie de 4 codes utilisateur consécutifs erronés (également appelés « Code sabotage utilisateur »)	Sabotages
573	Zone utilisateur/système masquée, zone affichée	Exclusion
601	Rapport de test de déclenchement manuel 2)	/
602	Rapport de test périodique/automatique 2)	/
625	Nouveau réglage de la date et de l'heure	RAZ heure/date
627	Mode Installateur Démarrage centrale (Web)	Mode installateur
628	Mode Installateur Fin centrale (Web)	Mode installateur

Remarque :

- 1) La centrale d'alarme transmet le brouillage et la supervision lorsque le système est désactivé.
- 2) Indépendant d'un groupe/sans lien avec un groupe

Tableau 2 Groupes de rapport CID – Codes CID

Groupe de rapport CID	Code CID	Contient :
Incendie	110	Feu et Feu OK
Alarme anti-agression	120	Agression zone (panique) et OK Agression (panique) silence et OK Agression clavier (panique) et OK Agression RF (panique) et OK Agression clavier sans fil (panique) et OK
Alarme anti-agression	121	Alarme code contrainte
Alarme anti-agression	129	Alarme agression (panique) confirmée
Alarme Alarme	100	Alarme médicale
Alarme Alarme	101	Appel Soins de santé (urgence soins)
Alarme intrusion	130	Intrusion et Intrusion OK
Alarme intrusion	131	Enveloppe extérieure/Périmètre et enveloppe extérieure/Périmètre OK Tentative d'effraction par levier et bris de glace par ex. du FTSE
Alarme intrusion	139	Confirmation alarme
Alarme intrusion	406	Alarme annulation
Technique	150	Alarme technique et OK
Sabotages	137	Sabotage du boîtier de la centrale et OK Sabotage du clavier et OK Sabotage du détecteur et OK Sabotage du clavier et OK Sabotage de la sirène et OK Sabotage du clavier sans fil et OK Sabotage des sirènes externes et OK Sabotage MAW et OK Sabotage du verrou de la porte et OK
Sabotages	461	Saisie de 4 codes utilisateur consécutifs erronés (également appelés « Code sabotage utilisateur »)
Armement/Désarmement	401	Système ou partition activé(e) et désactivé(e)
Armement/Désarmement	409	Système ou partition activé(e) et désactivé(e) avec un interrupteur à clé
Act. interne	401	Système ou partition activé(e) en interne
Act. interne	409	Système ou partition activé(e) en interne avec un interrupteur à clé

Annexe

Remise à zéro	305	Système ou partition réinitialisé(e)
Sortie timeout	457	Sortie timeout et OK
Exclusion	573	Zone utilisateur/système masquée, zone affichée
Boîtier clé	150	Boîtier clé ouvert et fermé
RF Supervision	381	Défaut supervision de zone et OK Défaut supervision du clavier sans fil et OK Défaut supervision de sirène externe et ok 1) Défaut supervision de générateur de signal int. et OK Défaut supervision MAW et OK Défaut supervision de verrou de porte et OK Défaut supervision de répéteur et OK Défaut supervision MoHy et OK
RF Brouillage	344	Défaut brouillage et ok 1)
Batt.Rad. /PSU	337	Générateur de signal int., clavier de commande, répéteur, MoHy, détecteur autonome avertisseur de fumée, MAW Défaut PSU et OK
Batt.Rad. /PSU	338	Sirène externe, MAW, répéteur Défaut batterie/pile vide et OK
Batt.Rad. /PSU	384	Défaut zone batterie vide et OK
Batt. centrale	302	Batt. centrale vide/défaut et OK
Batt. centrale	311	Batt. centrale vide/manquante et OK
Défaut secteur	301	Défaut secteur A/C et OK Centrale, MoHy
Anomalies	300	Défaut et OK pour : AUX 12 V, système 12 V
Anomalies	311	Défaut batterie externe et OK
Anomalies	320	Défaut zone sirène externe et OK Défaut MAW et OK
Anomalies	337	Défaut PSU externe et OK via zone n MoHy
Anomalies	338	PSU externe tension faible via zone n
Anomalies	342	Défaut A/C PSU externe et OK
Anomalies	351	Défaut voie de communication et OK
Anomalies	373	Défaut détecteur de fumée et OK
Anomalies	375	Défaut zone périphérique agression et OK
Mode installateur	627	Mode Installateur Démarrage centrale (Web)

Mode installateur	628	Mode Installateur Fin centrale (Web)
Code util. changé	/	/
RAZ heure/date	625	Nouveau réglage de la date et de l'heure
Supervision caméra	380	Défaut supervision caméra de zone IP et OK (par ex. IP Zone Missing, IP-Zone Timeout).
Télécharger	412	Téléchargement réussi
/	601	Rapport de test de déclenchement manuel 2)
/	602	Rapport de test périodique/automatique 2)

Remarque :

- 1) La centrale d'alarme transmet le brouillage et la supervision lorsque le système est désactivé.
- 2) Indépendant d'un groupe/sans lien avec un groupe

Tableau 3 Codes SIA - Groupes de rapport SIA

Code SIA	Contient :	Groupe de rapport SIA
AT, AR	Défaut secteur et OK Centrale, MoHy	Défaut secteur
AT, AR	Défaut A/C PSU externe et OK Centrale, MoHy	Anomalies
BA, BR	Intrusion et Intrusion OK	Alarme intrusion
BA, BR	Enveloppe extérieure/Périmètre et enveloppe extérieure/Périmètre OK Tentative d'effraction par levier et bris de glace par ex. du FTSE	Alarme intrusion
BA, BR	Boîtier clé ouvert et fermé	Boîtier clé
BB, BU	Zone utilisateur/système masquée, zone affichée	Exclusion
BC	Alarme annulation	Alarme intrusion
BV	Confirmation alarme	Alarme intrusion
BZ	Défaut supervision de zone et OK Défaut supervision du clavier sans fil et OK Défaut supervision de sirène externe et ok 1) Défaut supervision de générateur de signal int. et OK Défaut supervision MAW et OK Défaut supervision de verrou de porte et OK Défaut supervision de répéteur et OK Défaut supervision MoHy et OK	RF Supervision
BZ	Défaut supervision caméra de zone IP et OK (par ex. IP Zone Missing, IP-Zone Timeout).	Supervision caméra
CA, OA	Activation du calendrier, désactivation du calendrier	Armement/Désarmement
CE	Activation de l'agenda repoussée dans le temps	Armement/Désarmement
CL	Système ou partition activé(e) en interne	Act. interne
CL, OP	Système ou partition activé(e) et désactivé(e)	Armement/Désarmement
CS	Système ou partition activé(e) en interne avec un interrupteur à clé	Act. interne
CS, OS	Système ou partition activé(e) et désactivé(e) avec un interrupteur à clé	Armement/Désarmement
EA	Sortie timeout et OK	Sortie timeout
FA, FR	Feu et Feu OK	Incendie
FT, FJ	Défaut détecteur de fumée et OK	Anomalies
HA, HR	Contrainte et OK	Alarme anti-agression
HV	Alarme agression (panique) confirmée	Alarme anti-agression
JA	Saisie de 4 codes utilisateur consécutifs erronés (également appelés « Code sabotage utilisateur »)	Sabotages
JT	Nouveau réglage de la date et de l'heure	RAZ heure/date
JV	L'utilisateur A a modifié le code de l'utilisateur B	Code util. changé
JX	L'utilisateur A a supprimé l'utilisateur B	Code util. changé
LB (RB)	Mode Installateur Démarrage centrale (Web)	Mode installateur

LS (RS)	Mode Installateur Fin centrale (Web)	Mode installateur
LT, LR	Défaut voie de communication et OK	Anomalies
MA, MH	Alarme médicale et OK	Alarme Alarme
OA, CA	Désactivation du calendrier, activation du calendrier	Armement/Désarmement
OR	Système ou partition réinitialisé(e)	Remise à zéro
PA, PR	Agression zone (panique) et OK Agression clavier (panique) et OK Agression RF (panique) et OK Agression clavier sans fil (panique) et OK	Alarme anti-agression
PT, PJ	Défaut zone périphérique agression et OK	Anomalies
QA, QH	Appel Soins de santé (urgence soins)	Alarme Alarme
RH	Code utilisateur réinitialisé	Code util. changé
RP	Rapport de test périodique/automatique 2)	/
RS	Téléchargement réussi	Télécharger
RU	Échec du téléchargement	Télécharger
RX	Rapport de test de déclenchement manuel 2)	/
TA, TR	Sabotage du clavier et OK Sabotage du détecteur et OK Sabotage du boîtier de la centrale et OK Sabotage de la sirène et OK Sabotage du clavier sans fil et OK Sabotage des sirènes externes et OK Sabotage MAW et OK Sabotage du clavier et OK Sabotage du verrou de la porte et OK	Sabotages
TA, TR	Défaut MAW et OK	Anomalies
UA, UR	Alarme technique et OK	Technique
XQ, XH	Défaut brouillage et ok 1)	RF Brouillage
XT, XR	Défaut zone batterie vide et OK	Batt.Rad. /PSU
YA, YH	Défaut zone sirène externe et OK	Anomalies
YM, YR	Batt. centrale vide/manquante et OK	Batt. centrale
YM, YR	Défaut batterie externe et OK	Anomalies
YP, YQ	Générateur de signal int., clavier de commande, répéteur, détecteur autonome avertisseur de fumée, MAW Défaut PSU et OK	Batt.Rad. /PSU
YP, YQ,	Défaut et OK pour : AUX 12 V, système 12 V	Anomalies
YP, YQ	Défaut PSU externe et OK via zone n	Anomalies
YT, YR	Sirène externe, MAW, répéteur Défaut batterie/pile vide et OK	Batt.Rad. /PSU
YT, YR	Batt. centrale vide/défaut et OK	Batt. centrale
YT, YR	PSU externe tension faible via zone n MoHy	Anomalies
YW	Erreur système	Anomalies

Remarque

- 1) La centrale d'alarme transmet le brouillage et la supervision lorsque le système est désactivé.
- 2) Indépendant d'un groupe/sans lien avec un groupe

Tableau 4 Groupes de rapport SIA - Codes SIA

Groupe de rapport SIA	Code SIA	Contient :
Incendie	FA, FR	Feu et Feu OK
Alarme anti-agression	HA, HR	Contrainte et OK
Alarme anti-agression	HV	Alarme agression (panique) confirmée
Alarme anti-agression	PA, PR	Agression zone (panique) et OK Agression clavier (panique) et OK Agression RF (panique) et OK Agression clavier sans fil (panique) et OK
Alarme Alarme	MA, MH	Alarme médicale et OK
Alarme Alarme	QA, QH	Appel Soins de santé (urgence soins)
Alarme intrusion	BA, BR	Intrusion et Intrusion OK
Alarme intrusion	BA, BR	Enveloppe extérieure/Périmètre et enveloppe extérieure/Périmètre OK Tentative d'effraction par levier et bris de glace par ex. du FTSE
Alarme intrusion	BC	Alarme annulation
Alarme intrusion	BV	Confirmation alarme
Technique	UA, UR	Alarme technique et OK
Sabotages	JA	Saisie de 4 codes utilisateur consécutifs erronés (également appelés « Code sabotage utilisateur »)
Sabotages	TA, TR	Sabotage du clavier et OK Sabotage du détecteur et OK Sabotage du boîtier de la centrale et OK Sabotage de la sirène et OK Sabotage du clavier sans fil et OK Sabotage des sirènes externes et OK Sabotage MAW et OK Sabotage du clavier et OK Sabotage du verrou de la porte et OK
Armement/Désarmement	CA, OA	Activation du calendrier, désactivation du calendrier
Armement/Désarmement	CE	Activation de l'agenda repoussée dans le temps
Armement/Désarmement	CL, OP	Système ou partition activé(e) et désactivé(e)
Armement/Désarmement	CS, OS	Système ou partition activé(e) et désactivé(e) avec un interrupteur à clé
Act. interne	CL	Système ou partition activé(e) en interne

Annexe

Act. interne	CS	Système ou partition activé(e) en interne avec un interrupteur à clé
Remise à zéro	OR	Système ou partition réinitialisé(e)
Sortie timeout	EA	Sortie timeout et OK
Exclusion	BB, BU	Zone utilisateur/système masquée, zone affichée
Boîtier clé	BA, BR	Boîtier clé ouvert et fermé
RF Supervision	BZ	Défaut supervision de zone et OK Défaut supervision du clavier sans fil et OK Défaut supervision de sirène externe et OK 1) Défaut supervision de générateur de signal int. et OK Défaut supervision MAW et OK Défaut supervision de verrou de porte et OK Défaut supervision de répéteur et OK Défaut supervision MoHy et OK
RF Brouillage	XQ, XH	Défaut brouillage et ok 1)
Batt.Rad. /PSU	XT, XR	Défaut zone batterie vide et OK
Batt.Rad. /PSU	YP, YQ	Générateur de signal int., clavier de commande, répéteur, détecteur autonome avertisseur de fumée, MAW Défaut PSU et OK
Batt.Rad. /PSU	YT, YR	Sirène externe, MAW, répéteur Défaut batterie/pile vide et OK
Batt. centrale	YM, YR	Batt. centrale vide/manquante et OK
Batt. centrale	YT, YR	Batt. centrale vide/défaut et OK
Défaut secteur	AT, AR	Défaut secteur et OK Centrale, MoHy
Anomalies	AT, AR	Défaut A/C PSU externe et OK Centrale, MoHy
Anomalies	FT, FJ	Défaut détecteur de fumée et OK
Anomalies	LT, LR	Défaut voie de communication et OK
Anomalies	PT, PJ	Défaut zone périphérique agression et OK
Anomalies	TA, TR	Défaut MAW et OK
Anomalies	YA, YH	Défaut zone sirène externe et OK
Anomalies	YM, YR	Défaut batterie externe et OK
Anomalies	YP, YQ,	Défaut et OK pour : AUX 12 V, système 12 V
Anomalies	YP, YQ	Défaut PSU externe et OK via zone n
Anomalies	YT, YR	PSU externe tension faible via zone n

		MoHy
Anomalies	YW	Erreur système
Mode installateur	LB (RB)	Mode Installateur Démarrage centrale (Web)
Mode installateur	LS (RS)	Mode Installateur Fin centrale (Web)
Code util. changé	JV	L'utilisateur A a modifié le code de l'utilisateur B
Code util. changé	JX	L'utilisateur A a supprimé l'utilisateur B
Code util. changé	RH	Code utilisateur réinitialisé
RAZ heure/date	JT	Nouveau réglage de la date et de l'heure
Supervision caméra	BZ	Défaut supervision caméra de zone IP et OK (par ex. IP Zone Missing, IP-Zone Timeout).
Télécharger	RS	Téléchargement réussi
Télécharger	RU	Échec du téléchargement
/	RP	Rapport de test périodique/automatique 2)
/	RX	Rapport de test de déclenchement manuel 2)

Remarque

- 1) La centrale d'alarme transmet le brouillage et la supervision lorsque le système est désactivé.
- 2) Indépendant d'un groupe/sans lien avec un groupe

Messages d'erreur par e-mail

Le tableau suivant comprend les codes de réponse du serveur SMTP :

200	non standard success response, see RFC876
211	System status, or system help reply
214	Help message
220	<domain> service ready
221	<domain> service closing transmission channel
235	successful authentication
250	Requested mail action OK, completed
251	User not local, will forward to <forward-path>
252	Cannot VRFY user, but will accept message and attempt delivery
253	Pending message for node started
334	server challenge
354	Start mail input, end with <CRLF>.<CRLF>
355	Octet offset is the transaction offset
421	<domain> service not available, closing transmission channel
432	A password transition is needed
450	Requested mail action not taken: mailbox unavailable
451	Requested action aborted: error in processing
452	Requested action not taken: insufficient system storage
453	no mail
454	TLS not available due to temporary reason. Encryption required for requested authentication mechanism
455	Server unable to accommodate parameters
458	Unable to queue message for node
459	Node not allowed: <reason>
500	Syntax error, command unrecognized
501	Syntax error in parameters or arguments
502	Command not implemented
503	Bad sequence of commands
504	Command parameter not implemented
510	Check the recipient address
512	<domain> cannot be found. Unknown host
515	Destination mailbox address invalid
517	Problem with senders mail attribute, check properties
521	<domain> does not accept mail (see RFC1846)
522	Recipient has exceeded mailbox limit
523	Server limit exceeded. Message too large
530	Encryption required for authentication mechanism
531	Mail system full
533	Remote server has insufficient disk space to hold email
534	Authentication mechanism is too weak. Message too big
535	Authentication unsuccessful/Bad username or password
538	Encryption required for authentication mechanism
550	Requested action not taken: mailbox unavailable
551	User not local, please try <forward-path>
552	Requested mail action aborted: exceeded storage allocation
553	Requested action not taken: mailbox name not allowed
554	Transaction failed
555	MAIL FROM/RCPT TO parameters not recognised or not implemented

Messages d'erreur par TCP/IP

Le tableau suivant comprend les messages d'erreur TCP/IP :

1001	General Error
1002	Invalid socket descriptor
1003	Invalid parameter
1004	It would have blocked
1005	Not enough memory in memory pool
1006	Connection is closed or aborted
1007	Socket is locked in RTX environment
1008	Socket, Host Resolver timeout
1009	Host Name resolving in progress
1010	Host Name not existing

Vue d'ensemble des messages SSL

Le tableau suivant comprend les messages SSL que nous utilisons dans l'empilage SSL – Ils peuvent changer en cas de mise à niveau :

10064	Failed to get an IP address for the given hostname
10066	Failed to open a socket
10068	The connection to the given server / port failed
10070	Binding of the socket failed
10072	Could not listen on the socket
10074	Could not accept the incoming connection
10076	Reading information from the socket failed
10078	Sending information through the socket failed
10080	Connection was reset by peer
10082	Connection requires a read call
10084	Connection requires a write call
37520	A counter would wrap (eg, too many messages exchanged).
37648	Internal error (eg, unexpected failure in lower-level module)
37776	Unknown identity received (eg, PSK identity)
37904	Public key type mismatch (eg, asked for RSA key exchange and presented EC key)
38032	Session ticket has expired.
38160	Processing of the NewSessionTicket handshake message failed.
38288	Handshake protocol not within min/max boundaries
38416	Processing of the compression / decompression failed
38544	Hardware acceleration function skipped / left alone data
38800	The requested feature is not available
38928	Bad input parameters to function
39056	Verification of the message MAC failed
39184	An invalid SSL record was received
39312	The connection indicated an EOF
39440	An unknown cipher was received
39568	The server has no ciphersuites in common with the client
39696	No RNG was provided to the SSL module
39824	No client certification received from the client, but required by the authentication mode
39952	Our own certificate(s) is/are too large to send in an SSL message
40080	The own certificate is not set, but needed by the server
40208	The own private key or pre-shared key is not set, but needed
40336	No CA Chain is set, but required to operate
40464	An unexpected message was received from our peer
40592	A fatal alert message was received from our peer
40720	Verification of our peer failed

40848	The peer notified us that the connection is going to be closed
40976	Processing of the ClientHello handshake message failed
41104	Processing of the ServerHello handshake message failed
41232	Processing of the Certificate handshake message failed
41360	Processing of the CertificateRequest handshake message failed
41488	Processing of the ServerKeyExchange handshake message failed
41616	Processing of the ServerHelloDone handshake message failed
41744	Processing of the ClientKeyExchange handshake message failed
41872	Processing of the ClientKeyExchange handshake message failed in DHM / ECDH Read Public
42000	Processing of the ClientKeyExchange handshake message failed in DHM / ECDH Calculate Secret
42128	Processing of the CertificateVerify handshake message failed
42256	Processing of the ChangeCipherSpec handshake message failed
42384	Processing of the Finished handshake message failed
42512	Memory allocation failed
42640	Hardware acceleration function returned with error

Messages d'erreur par VOIP

Le tableau suivant comprend les messages d'erreur importants pour l'utilisateur :

VOIP_CALL_NO_RESULT	0
VOIP_CALL_FAIL_NO_LINK	1
VOIP_CALL_FAIL_NO_LOCAL_ADDRESS	2
VOIP_CALL_REJECTED	3
VOIP_CALL_TIMEOUT_NO_ANSWER	4
VOIP_CALL_CANCELLED	5
VOIP_CALL_DECLINED	6
VOIP_CALL_FORBIDDEN	7
VOIP_CALL_NOT_FOUND	8
VOIP_CALL_INIT_SIP_URL_ERROR	9
VOIP_CALL_CALLER_ABORT	10
VOIP_CALL_DISCONNECT	11
VOIP_CALL_PASSWORD_ERROR	12
VOIP_CALL_LINK_LOST_ERROR	13

Le tableau suivant comprend les messages d'erreur internes :

VOIP_CALL_INIT_PARAM_ERROR	14
VOIP_CALL_PJSIP_APP_ERROR	15
VOIP_CALL_ICE_CREATE_ERROR	16
VOIP_CALL_ICE_PROCEDURE_ERROR	17
VOIP_CALL_ICE_INVITE_CREATION_ERROR	18
VOIP_CALL_ICE_REINVITE_CREATION_ERROR	19
VOIP_CALL_ICE_REINVITE_SEND_ERROR	20
VOIP_CALL_ICE_UPDATE_CREATION_ERROR	21
VOIP_CALL_ICE_UPDATE_SEND_ERROR	22
VOIP_CALL_ICE_SDP_POINTER_ERROR	23
VOIP_CALL_ICE_NEGOTIATION_FAIL_ERROR	24
VOIP_CALL_REGISTRATION_CREATION_ERROR	25
VOIP_CALL_REGISTRATION_INIT_ERROR	26
VOIP_CALL_REGISTRATION_CRED_ERROR	27
VOIP_CALL_REGISTRATION_REG_ERROR	28
VOIP_CALL_REGISTRATION_SEND_ERROR	29
VOIP_CALL_REGISTRATION_SERVER_RESPONSE_TIMEOUT	30
VOIP_CALL_REGISTRATION_RESULT_INTERNAL_ERROR	31
VOIP_CALL_REGISTRATION_SERVER_RESPONSE_ERROR	32
VOIP_CALL_PJSIP_ASSERT_ERROR	33
VOIP_CALL_AUDIO_PLAYBACK_NOT_CONNECTED_ERROR	40

Messages d'erreur GSM CME/CMS

Les tableaux suivants comprennent les messages d'erreur importants pour l'utilisateur :

Codes d'erreur CME

Codes d'erreur liés au matériel GSM

0	Phone failure
1	No connection to phone
2	Phone-adapter link reserved
3	Operation not allowed
4	Operation not supported
5	PH-SIM PIN required
6	PH-FSIM PIN required
7	PH-FSIM PUK required
10	SIM not inserted
11	SIM PIN required
12	SIM PUK required
13	SIM failure
14	SIM busy
15	SIM wrong
16	Incorrect password
17	SIM PIN2 required
18	SIM PUK2 required
20	Memory full
21	Invalid index
22	Not found
23	Memory failure
24	Text string too long
25	Invalid characters in text string
26	Dial string too long
27	Invalid characters in dial string
30	No network service
31	Network timeout
32	Network not allowed - emergency call only
40	Network personalization PIN required
41	Network personalization PUK required
42	Network subset personalization PIN required
43	Network subset personalization PUK required
44	Service provider personalization PIN required
45	Service provider personalization PUK required
46	Corporate personalization PIN required
47	Corporate personalization PUK required
48	Hidden key required
49	EAP method not supported
50	Incorrect parameters
99	Resource limitation
100	Unknown
103	Illegal MS
106	Illegal ME

107	GPRS services not allowed
111	PLMN not allowed
112	Location area not allowed
113	Roaming not allowed in this location area
132	Service option not supported
133	Requested service option not subscribed
134	Service option temporarily out of order
148	Unspecified GPRS error
149	PDP authentication failure
150	Invalid mobile class
201	Alternate SIM conflict
256	Operation temporarily not allowed
257	Call barred
258	Phone is busy
259	User abort
260	Invalid dial string
261	SS not executed
262	SIM Blocked
263	Invalid block
500	CTS Handover on Progress
501	Cellular Protocol Stack Out of service state
502	CTS Unspecified Error
650	General AVMS error
651	Communication error
652	Session in progress
654	RDMS services are in "deactivated" state
655	RDMS services are in "prohibited" state
656	RDMS services are in "to be provisioned" state; no available NAP
772	SIM powered down
800	SIM Security unspecified error
902	No more sockets available; the maximum number has been reached
903	Memory problem
904	DNS error
905	TCP disconnection by the server
906	TCP/UDP connection error
907	Generic error
908	Fail to accept client request's
909	Data send by KTCPSND/KUDPSND are incoherent
910	Bad session ID
911	Session is already running
912	No more sessions can be used (maximum session is 32)
913	Socket connection timer timeout
914	Control socket connection timer timeout
915	A parameter is not expected
916	A parameter has an invalid range of values
917	A parameter is missing
918	Feature is not supported
919	Feature is not available
920	Protocol is not supported
921	Error due to invalid state of bearer connection
922	Error due to invalid state of session
923	Error due to invalid state of terminate port data mode
924	Error due to session busy, retry later
925	Failed to decode HTTP header's name, missing ':'
926	Failed to decode HTTP header's value, missing '\r\lf'

927	HTTP header's name is an empty string
928	HTTP header's value is an empty string
929	Format of input data is invalid
930	Content of input data is invalid or not supported
931	The length of a parameter is invalid
932	The format of a parameter is invalid

Codes d'erreur CMS

Codes d'erreur liés au réseau GSM

1	Unassigned (unallocated) number
8	Operator determined barring
10	Call barred
21	Short message transfer rejected
27	Destination out of service
28	Unidentified subscriber
29	Facility rejected
30	Unknown subscriber
38	Network out of order
41	Temporary failure
42	Congestion
47	Resources unavailable, unspecified
50	Requested facility not subscribed
69	Requested facility not implemented
81	Invalid short message transfer reference value
95	Invalid message, unspecified
96	Invalid mandatory information
97	Message type non-existent or not implemented
98	Message not compatible with short message protocol state
99	Information element non-existent or not implemented
111	Protocol error, unspecified
127	Interworking, unspecified
128	Telematic interworking not supported
129	Short message Type 0 not supported
130	Cannot replace short message
143	Unspecified TP-PID error
144	Data coding scheme (alphabet) not supported
145	Message class not supported
159	Unspecified TP-DCS error
160	Command cannot be executed
161	Command unsupported
175	Unspecified TP-Command error
176	TPDU not supported
192	SC busy
193	No SC subscription
194	SC system failure
195	Invalid SME address
196	Destination SME barred
197	SM Rejected-Duplicate SM
198	TP-VPF not supported
199	TP-VP not supported
208	D0 SIM SMS storage full

209	No SMS storage capability in SIM
210	Error in MS
211	Memory Capacity Exceeded
212	SIM Application Toolkit Busy
213	SIM data download error
255	Unspecified error cause
300	ME failure
301	SMS service of ME reserved
302	Operation not allowed
303	Operation not supported
304	Invalid PDU mode parameter
305	Invalid text mode parameter
310	SIM not inserted
311	SIM PIN required
312	PH-SIM PIN required
313	SIM failure
314	SIM busy
315	SIM wrong
316	SIM PUK required
317	SIM PIN2 required
318	SIM PUK2 required
320	Memory failure
321	Invalid memory index
322	Memory full
330	SMSC address unknown
331	no network service
332	Network timeout
340	NO +CNMA ACK EXPECTED
500	Unknown error
512	User abort
513	Unable to store
514	Invalid Status
515	Device busy or Invalid Character in string
516	Invalid length
517	Invalid character in PDU
518	Invalid parameter
519	Invalid length or character
520	Invalid character in text
521	Timer expired
522	Operation temporary not allowed
532	SIM not ready
534	Cell Broadcast error unknown
535	Protocol stack busy
538	Invalid parameter
615	Network failure
616	network is down
639	service type not yet available
640	operation of service temporary not allowed
764	missing input value
765	invalid input value
767	operation failed

Historique

Entrées de journal de bord

Cette annexe fournit de brèves explications sur les messages qui peuvent s'afficher dans le journal de la centrale d'alarme.

Notez qu'une grande partie de ces messages se réfèrent à des périphériques spécifiques avec le numéro de périphérique correspondant. Il est donc impossible d'afficher dans cette liste les messages de journal exacts, tels que vous les verrez dans une certaine installation.

Les messages de la liste sont triés par ordre alphabétique. La colonne « Entrée du journal des événements » affiche « == » ou parfois « # ». Ces caractères correspondent au numéro de zone, d'utilisateur ou de périphérique que la centrale d'alarme a enregistré pour l'événement. Dans la colonne « Explication », celui-ci est indiqué par « nn » ou « n ». Dans les messages de communication répertoriés, « \$m » représente le type de la voie de communication utilisée.

Entrées du journal des événements	Explication
« \$m alarme OK »	Transfert d'alarme au CRA ou à la STS réussi via le chemin de transmission correspondant (RTC/IP/GSM/Mobile)
"\$m défaut e-mail"	\$m défaut e-mail
"\$m voie de comm. ok"	Voie de communication rétablie
"\$m défaut voie de comm."	Voie de communication perturbée
"\$m défaut modem"	\$m modem perturbé
"\$m modem de nouveau ok"	\$m modem de nouveau ok
"Protocole PAUS défaut \$m"	Protocole du poste central défaut de communication de \$m
"\$m défaut protocole de soin"	Défaut \$M lors de l'envoi du protocole de soin
"\$m défaut SMS"	\$m défaut communication SMS
"\$m défaut transm. vocal"	\$m transmetteur vocal perturbé
« \$m défaut WAN »	Défauts de la voie de communication IP <ul style="list-style-type: none"> ○ Zone publique (WAN) ○ Zone privée (LAN) En supplément de « Ligne réponse Ethernet » directement sur la centrale
« \$m WAN OK »	Voie de communication IP rétablie
"== Défaut A/C"	Extension == défaut de l'alimentation électrique
"== Défaut A/C ok"	Extension == alimentation électrique rétablie
"== Aux. fus. manq."	Extension == fusible manquant
"== Aux. fus. réinit."	Extension == fusible ok
"== Aux1 err. syst."	Extension == tension de la sortie 1 perturbée
"== Aux1 sort. ok"	Extension == tension de la sortie 1 ok
"== Aux2 err. syst."	Extension == tension de la sortie 2 perturbée
"== Aux2 sort. ok"	Extension == tension de la sortie 2 ok
"== Pile 1 manq."	Extension == pile 1 manquante
"== Pile 1 OK"	Extension == pile 1 ok
"== Pile 2 manq."	Extension == pile 2 manquante
"== pile 2 OK"	Extension == pile 2 ok

"== Code sabotage ok"	Le sabotage dû à un nombre trop élevé de saisies d'un code erroné a été réinitialisé.
"== App. charg. 1 err."	Extension == erreur appareil de chargement pile 1
"== App. charg. 1 OK"	Extension == appareil de chargement pile 1 ok
"== App. charg. 2 err."	Extension == erreur appareil de chargement pile 2
"== App. charg. 2 OK"	Extension == appareil de chargement pile 2 ok
"== Chargement 1 OK"	Extension == chargement de la batterie 1 ok
"== Chargement 2 OK"	Extension == chargement de la batterie 2 ok
"== Défaut test charge batt.1"	Extension == chargement de la batterie 1 perturbé
"== Défaut test charge batt.2"	Extension == chargement de la batterie 2 perturbé
"== Tension basse"	Extension == alimentation électrique basse
"== Pile 1 faible"	Extension == pile 1 chargement faible
"== Pile 2 faible"	Extension == pile 2 chargement faible
"== Err. tens. syst."	Extension == erreur dans la tension du système
"== Tens. syst. ok"	Extension == tension du système ok
"== Transm. sort. OK"	Extension == sortie de communication ok
"== ErrTransmSort."	Extension == erreur sortie de communication
"== Tension OK"	Extension == alimentation électrique ok
"12 V aux. ok"	Sortie 12 V de la centrale ok
"12 V aux. défaut"	Sortie 12 V de la centrale perturbée
"12 V clav. ok"	Clavier défaut de l'alimentation 12 V ok
"24 h Z=== Alarme"	Alarme 24 heures dans la zone n.
"24 h Z=== ok"	Alarme 24 heures réinitialisée dans la zone n.
"24 h Z== Alarme"	Alarme 24 heures dans la zone n.
"24 h Z== OK"	Alarme 24 heures réinitialisée dans la zone n.
"Déconnexion"	Déconnecté du serveur Web
"A/C OK"	L'erreur de tension secteur a été réinitialisée
"Défaut A/C ok part. ##"	Le défaut de l'alimentation électrique dans la partition ## a été réinitialisé
"Défaut A/C part. ##"	Défaut de l'alimentation électrique dans la partition ##
"Défaut A/C"	Absence de tension secteur
"Chargement batt. # OK"	Batterie # chargée
"Défaut chargement batt. #"	Défaut de charge de la batterie #
"Charge batt. # OK"	Test de charge de la batterie # OK
"Défaut test charge batt. #"	Test de charge de la batterie # perturbé
"Défaut batt. # OK"	Défaut de la batterie # de nouveau ok
"Batt. # entièrement déchargée/manquante"	La batterie # est entièrement déchargée ou manquante
"Défaut test charge batt. #"	Test de charge de la batterie non réussi
"Batt. entièrement déchargée/manquante"	La batterie est entièrement déchargée ou manquante
"Défaut d'activation Z=="	Activation impossible, zone == perturbée ou ouverte
"Alarme conf. serveur Web"	Alarme confirmée par serveur Web

Annexe

"Alarme conf. Z=="	Alarme confirmée par la zone ==
"Alarme conf. "	Alarme confirmée par clavier
"Alarme conf. aux. #"	Alarme confirmée par contact anti-sabotage sur l'appareil #
"Alarme conf.==ER"	Alarme confirmée par lecteur de proxy externe ==ER
"Conf. alarme =="	Alarme confirmée par extension ==
"Alarme appel de test"	Alarme appel de test déclenchée
"Annulation d'alarme U--"	Annulation d'alarme par l'utilisateur --
"Confalarme Clav=="	Alarme confirmée clavier de commande ==
"Confalarme clav. rad.=="	Alarme confirmée clavier de commande sans fil ==*
"Confalarme sonnerie #"	Alarme confirmée générateur de signal#
"Confalarme bip sonore"	Alarme confirmée bip sonore
"Confalarme sir. =="	Alarme confirmée sirène ==
"Confalarme MAW =="	Alarme confirmée MAW ==
"Confalarme Z==="	Alarme confirmée zone ===
"Confalarme boîtier centrale"	Alarme confirmée sabotage centrale d'alarme
"Confalarme aux."	Alarme confirmée accessoire raccordé
"Confirmation d'alarme"	Alarme confirmée
"Conf. alm RPT=="	Alarme confirmée répéteur
"Alm conf.cen. brouill."	Alarme confirmée brouillage de la centrale d'alarme
"Connexion"	Connecté au serveur Web
"ATE L.F. tous"	Toutes les lignes des unités de transmission d'alarme sont perturbées
"ATE L.F. individuel"	Une ligne des unités de transmission d'alarme est perturbée
"ATE L.F. ok"	Toutes les lignes des unités de transmission d'alarme sont rétablies
"Auto act. int. #"	Système activé # automatiquement en interne
"Auto syst. désact."	Système désactivé automatiquement
"Auto système act."	Système activé automatiquement
"Auto part. # act."	Partition # activée automatiquement
"Auto part. # désact."	Partition # désactivée automatiquement
"Act. autom. désact. part. #"	L'activation automatique de la partition # est désactivée
"Act. autom. act. part. #"	L'activation automatique de la partition # est activée
"Act. autom. ret. U--"	L'activation automatique a été décalée par l'utilisateur --
"Act. autom. retardée U-- P#"	L'utilisateur -- a retardé l'activation automatique de la partition #
"Act. autom. désact."	L'activation automatique est désactivée
"Act. autom. act."	L'activation automatique est activée
"Act. autom. autom. part. #"	L'activation automatique de la partition # est perturbée
"Auto part. # act. int."	Partition # activée automatiquement en interne
"Aux. # sabo ok"	Sabotage de l'alimentation électrique sur l'appareil externe # réinitialisé
"Aux. 14V4 # défaut"	Sortie 14 V de la centrale perturbée
"Aux. sabo ok"	Sabotage de l'alimentation électrique sur un appareil externe réinitialisé
"Aux. # sabotage"	Sabotage de l'alimentation électrique sur l'appareil externe #
"Aux. 14V4 # OK"	Sortie 14 V de la centrale ok
"Aux. sabotage"	Sabotage de l'alimentation électrique sur un appareil externe
"U -- syst. act. int. #"	L'utilisateur -- a activé le système en interne

"U-- activ. ignorer"	L'utilisateur -- a interrompu l'activation du système
"U-- défaut téléch."	Utilisateur == téléchargement perturbé
"U-- Réglage modifié"	Configuration modifiée par l'utilisateur ==
"U--- int. S # sortie"	L'utilisateur -- a démarré la temporisation de la sortie #
"U--- Alarme médicale"	Alarme d'urgence médicale déclenchée par l'utilisateur --
"U-- redémarrage centrale"	L'utilisateur == a redémarré la centrale
"U--- contrainte OK"	Alarme de contrainte de l'utilisateur == réinitialisée
"U--- contrainte"	Alarme de contrainte de l'utilisateur==
"U--- code shunt"	Code shunt saisi par l'utilisateur --
"U-- TrVoc. = mod."	L'utilisateur -- a modifié un numéro du transmetteur vocal
"U--- sortie système"	L'utilisateur -- a démarré la temporisation de la sortie
"U--- part. ## sortie"	L'utilisateur -- a activé la temporisation de la sortie dans la partition ##
"U--- part. ## contrainte ok"	Alarme de contrainte de l'utilisateur == dans la partition ## réinitialisée
"U--- part. ## contrainte"	Alarme de contrainte de l'utilisateur == dans la partition ##
"U-- ignorer"	L'utilisateur -- a activé la partition # malgré l'avertissement
"Pile faible Z==="	Pile faible zone ===
"Pile faible Z===ok"	Pile zone === ok
"Pile ent. Z==ok"	Pile zone == ok
"Pile faible Z=="	Pile faible zone ==
"Pile ok"	La pile est ok
"Pile faible"	Pile faible
"Clav incendie ok"	Alarme incendie sur le clavier == réinitialisée
"Clav.== code sabotage"	Sabotage dû à un nombre trop élevé de saisies d'un code erroné sur le clavier de commande ==
"Clav== incendie"	Alarme incendie sur le clavier == déclenchée
"Clav== méd."	Clavier == alarme médicale déclenchée
"Clav== AA"	Clavier == alarme agression déclenchée
"Occup. act. avec#"	Journal des événements utilisé par #
"Util. -- modif. util. =="	L'utilisateur -- a modifié le code de l'utilisateur ==
"Util. -- connexion"	L'utilisateur -- a appelé le menu
"Util. -- déconnexion"	L'utilisateur -- a quitté le menu
"Util. -- suppr. util. =="	L'utilisateur -- a supprimé l'utilisateur ==
"Util. -- système act."	L'utilisateur -- a activé le système
"Util. -- système désact."	Système désactivé par l'utilisateur --
"Util. -- réinit. système"	L'utilisateur -- a réinitialisé le système
"Util. -- part. # act."	L'utilisateur -- a activé la partition #
"Util. -- part. # désact."	L'utilisateur -- a désactivé la partition #
"Util. -- part. # act. int."	L'utilisateur -- a activé la partition # en interne
"Util. -- part. # réinit."	L'utilisateur -- a réinitialisé la partition #
"Util.-- connexion (Web)"	L'utilisateur -- a appelé le menu Web
"Util.-- déconnexion (Web)"	L'utilisateur -- a quitté le menu Web
"Util.-- date/heure"	L'utilisateur == a modifié la date/heure
"Util.-- zone== masquée"	L'utilisateur -- a masqué la zone ==
"Util.--- zone=== masquée ok"	L'utilisateur --- a réactivé la zone ===

Annexe

"Util.-- zone=== masquée"	L'utilisateur --- a masqué la zone ===
"Util.--- zone=== agression masquée"	Zone === agression masquée par utilisateur ---
"Util.-- appel soins de santé"	L'utilisateur -- a déclenché un appel de soins de santé
"U--téléch. dist."	Utilisateur == téléchargement distant réussi
"Clav. == trouvé"	Nouveau clavier == trouvé
"Clav. == supprimé"	Clavier == supprimé
"Clav. == ajouté"	Le clavier == a été ajouté
"Clav.== code sabotage"	Sabotage dû à un nombre trop élevé de saisies d'un code erroné sur le clavier de commande ==
"Clav.== manquant"	Clavier == manquant
"Clav.== ok"	Le clavier == est ok
"U--part. # ignorer"	L'utilisateur -- a activé le système malgré l'avertissement
"Soins P-- pile faible"	Émetteur d'appel de soins de santé pile faible
"CO Z== alarme"	CO alarme zone ==
"CO Z== ok"	CO alarme zone == réinitialisé
"Code sabotage"	Sabotage dû à un nombre trop élevé de saisies d'un code erroné
« Codes réinitialisés »	Les codes ont été réinitialisés au réglage usine. Les codes ont été supprimés puis de nouveau saisis.
"Téléchargement bloqué"	Téléchargement bloqué
"Sirène filaire== défaut"	Défaut sur la sirène filaire== Contrôlez également le câblage entre le raccordement TRB (Trouble) et 0 V.
"Sirène filaire== défaut OK"	Défaut sur la sirène filaire== a été réinitialisé
"Dup. == OK"	L'erreur "Adresse attribuée en double" est corrigée
"Dupliquer =="	Erreur "Adresse attribuée en double"
"Intrusion Z== alarme"	Alarme intrusion zone ==
"Intr. Z== OK."	Alarme intrusion zone == réinitialisée
"Intrusion Z=== alarme"	Alarme intrusion zone ===
"Intrusion Z=== ok"	Alarme intrusion zone === réinitialisée
"Entr. dém. Z==="	Temporisation d'entrée zone === démarrée
"Route entr. quittée Z=="	La route d'entrée a été quittée, zone === déclenchée
"Entrée déviation Z==="	La route d'entrée a été quittée, zone == déclenchée
"Régl.Z===shunt."	Les réglages de la zone === ont été shuntés
"Réglage modifié"	La configuration a été modifiée
"Erreur e-mail ---"	Erreur e-mail ---
"Erreur e-mail \$w"	Erreur e-mail "w
"E-mail appel de test"	E-mail appel de test
"Ext. == trouvée"	Nouvelle extension == trouvée
"Ext. == supprimée"	L'extension == a été supprimée
"Ext. == ajoutée"	La nouvelle extension == a été ajoutée
"Rét. A/C ext. Z=="	Alimentation électrique externe Z== rétablie
"Rét. A/C ext. Z==="	Alimentation électrique externe Z=== rétablie
"Défaut A/C ext. Z=="	Défaut externe de l'alimentation électrique Z==
"Défaut A/C ext. Z==="	Défaut externe de l'alimentation électrique Z===
"Défaut pile ext. Z=="	Erreur pile externe Z==
"Déf. pile ext. Z==="	Erreur pile externe Z===

"Rét. pile ext. Z=="	Pile externe Z== ok
"Rét. pile ext. Z==="	Pile externe Z=== ok
"CC ext. ok part. ##"	Courant continu externe rétabli dans la partition ##
"Défaut CC ext. part. ##"	Courant continu externe perturbé dans la partition ##
"Tens. faible ext. Z=="	Tension faible de l'alimentation électrique externe Z==
"Tens. faible ext. Z==="	Tension faible de l'alimentation électrique externe Z===
"Défaut PSU ext. Z=="	Défaut de l'alimentation électrique externe Z==
"Rét. PSU ext. Z==="	Alimentation électrique externe Z=== ok
"Rét. PSU ext. Z=="	Alimentation électrique externe Z== ok
"Défaut PSU ext. zone =="	Défaut de l'alimentation électrique externe Z===
"Rét. tens. ext. Z==="	Alimentation électrique externe Z=== ok
"Rét. tens. ext. Z=="	Alimentation électrique externe Z== ok
"Défaut CC externe"	Défaut externe du courant continu
"TC util. -- pile faible"	Utilisateur -- la pile de la télécommande est faible
"Clav. rad.== défaut de supervision"	Clavier radio == surveillance radio perturbée constatée
"Clav. rad.== surv. ok"	Clavier radio == surveillance radio ok
"Manquant == OK"	Extension == de nouveau dans le système
"Manquant == ok"	Le clavier manquant == est de nouveau accessible
"Manquant =="	Extension == manquante
"Manquant =="	Clavier == manquant
"Manquant ==ER ok"	Lecteur proxy externe == sur le clavier ok
"Manquant ==ER"	Lecteur proxy externe == manquant sur le clavier
"Réinit. dist."	Le système a été réinitialisé à distance
"Téléservice réussi"	Téléservice terminé avec succès
"L'erreur incendie a été réinitialisée part.#"	Alarme incendie partition # ok
"Incendie OK"	L'alarme incendie a été réinitialisée
"Incendie OK"	Alarme incendie réinitialisée sur le clavier
"Incendie réinitialisation"	L'alarme incendie a été réinitialisée
"Incendie Z== alarme"	Alarme incendie zone ==
"Incendie Z== OK"	L'alarme incendie zone == a été réinitialisée
"Incendie Z=== alarme"	Alarme incendie zone ===
"Incendie Z=== ok"	L'alarme incendie zone === a été réinitialisée
"Alarme incendie"	Alarme incendie déclenchée sur le clavier
"Incendie clav.== alarme"	Alarme incendie déclenchée sur le clavier ==
"Clav. rad.## appel soins de santé"	Clavier radio ## appel soins de santé déclenché
"Clav. rad.== 4/6 divergence"	Clavier radio == longueur de code (4/6) erronée
"Clav. rad.== pile faible"	Pile faible clavier radio ==
"Clav. rad.== code sabotage ok"	Le sabotage dû à un nombre trop élevé de saisies d'un code erroné sur le clavier de commande sans fil == a été réinitialisé.
"Clav. rad.== PSU ok"	Clavier radio == alimentation électrique externe établie
"Clav. rad.== défaut PSU"	Clavier radio == alimentation électrique externe perturbée
"Clav. rad.== RF OK"	Clavier sans fil == liaison sans fil ok
"Clav. rad.== avertissement RF"	Clavier de commande sans fil == plus de 15 min sans liaison radio avec la centrale d'alarme

Annexe

"Clav. rad.== supervision ok"	Surveillance radio perturbée clavier radio == réinitialisée
"Clav. rad.== défaut de supervision"	Surveillance radio perturbée clavier radio ==
"Autorisé =="	...est autorisé
"Clav. radio == sabo ok"	Clavier radio == sabotage réinitialisé
"Clav. radio == sabo"	Clavier radio == sabotage déclenché
"Sir. radio == pile ok"	Sirène radio == pile ok
"Sir. radio == pile faible"	Sirène radio == pile faible
"Sir. radio == sabo ok"	Sirène radio == l'erreur de sabotage a été réinitialisée
"Sir. radio == sabo"	Sirène radio == sabotage
"Sir. radio == défaut de supervision"	Sirène externe == surveillance radio ok
"Défaut radio OK"	Défaut radio résolu
"Défaut radio"	Défaut radio
"Sabo boîtier OK"	Le sabotage du boîtier de la centrale a été réinitialisé
"Sabotage boîtier"	Sabotage du boîtier de la centrale
"Bloqué =="	...est bloqué
"Bris glace ok Z==="	La zone de bris de glace == a été supprimée
"Bris glace Z==="	Bris de glace détecté par la zone ==
"GSM CME info --"	GSM CME info --
"GSM CME info \$w"	GSM CME info \$w
"GSM CMS info --"	GSM CMS info --
"GSM CMS info \$w"	GSM CMS info \$w
"M/H== sabo."	Boîtier ouvert au niveau du module hybride
"M/H== sabo. OK"	Boîtier fermé au niveau du module hybride
"M/H== batterie PSU vide"	Batterie vide de l'alimentation électrique du module hybride
"M/H== batterie PSU OK"	Batterie OK de l'alimentation électrique du module hybride
"M/H== défaut sup."	Plus de 2 h sans liaison sans fil avec le module hybride
"M/H== sup. OK"	Liaison sans fil OK avec le module hybride
"M/H== avertissement RF"	Plus de 20 min sans liaison sans fil avec le module hybride
"M/H== RF OK"	Liaison sans fil OK avec le module hybride
"M/H== brouillage"	Brouillage détecté par le module hybride
"M/H== brouillage OK"	Plus de brouillage sur le module hybride
"M/H== défaut CA PSU"	Défaut d'alimentation électrique 230 V sur le module hybride
"M/H== CA PSU OK"	Alimentation électrique 12 V à nouveau OK sur le module hybride
"M/H== défaut CC"	Défaut d'alimentation électrique 12 V sur le module hybride
"M/H== CC OK"	Alimentation électrique 12 V à nouveau OK sur le module hybride
"M/H== défaut Aux"	Défaut d'alimentation électrique sortie 12 V sur le module hybride
"M/H== Aux OK"	Alimentation électrique sortie 12 V à nouveau OK sur le module hybride
"M/H== sabo. sir."	Boîtier de générateur de signal ouvert, entrée TR au niveau du module hybride
"M/H== sabo. sir. OK"	Boîtier de générateur de signal fermé, entrée TR au niveau du module hybride
"Inactivité soin part. #"	Appel de soins de santé déclenché dans la partition # par l'inactivité
"Générateur de signal int.== sabotage"	Boîtier ouvert au niveau du générateur de signal intérieur

"Générateur de signal int.== sabotage OK"	Boîtier fermé au niveau du générateur de signal intérieur
"Générateur de signal int.== pile faible"	Piles vides au niveau du générateur de signal intérieur
"Générateur de signal int.== pile faible OK"	Piles OK au niveau du générateur de signal intérieur
"Générateur de signal int.== défaut sup. TL"	Plus de 2 h sans liaison sans fil avec le générateur de signal intérieur
"Générateur de signal int.== défaut sup. TL OK"	Liaison sans fil OK avec le générateur de signal intérieur
"Générateur de signal int.== Avertissement RF"	Plus de 20 min sans liaison sans fil avec le générateur de signal intérieur
"Générateur de signal int.== RF OK"	Liaison sans fil OK avec le générateur de signal intérieur
"Générateur de signal int.== brouillage"	Brouillage détecté par le générateur de signal intérieur
"Générateur de signal int.== brouillage OK"	Plus de brouillage sur le générateur de signal intérieur
"Générateur de signal int.== défaut PSU"	Défaut d'alimentation électrique 12 V sur le générateur de signal intérieur
"Générateur de signal int.== défaut PSU OK"	Alimentation électrique 12 V à nouveau OK sur le générateur de signal intérieur
"Périphérique IP déconnecté"	Périphérique IP déconnecté
"Périphérique IP connecté"	Périphérique IP connecté
"IP Polling ok"	IP Polling rétablie
"IP Polling défaut"	IP Polling défaut
"Z IP=== err. HTTP"	Zone IP === erreur HTTP
"Z IP=== réinit. manq."	Zone IP === connexion rétablie
"Z IP=== manquante"	Zone IP === zone manquante
"Z IP=== temporisation"	Zone IP === temporisation
"Z IP=== IP err. 404"	Zone IP === erreur IP "Page non accessible"
"Z IP=== err. auth. IP"	Zone IP === erreur autorisation IP
"Brouillage == OK"	Extension == brouillage ok
"Brouillage =="	Extension == brouillage constaté
"Communication 12 V défaut ok"	Communication alimentation 12 V de nouveau ok
"Communication 12 V défaut"	Communication défaut de l'alimentation 12 V
"Défaut de communication"	Communication perturbée
"Défaut de configuration"	Configuration erronée
"Bip sonore # 12 V OK"	Bip sonore # 12 V de nouveau disponible
"Bip sonore # 12 V défaut"	Défaut 12 V bip sonore #
"Batterie vide # ok"	La batterie # est ok
"Batterie vide #"	La batterie # est vide
"CO"	La connexion a été interrompue
"Blocage Z=== act."	La zone de blocage === a été activée
"Blocage Z=== désact."	La zone de blocage === a été désactivée
"Journal événement types"	Journal événement types
"Recherche journal effacée"	Recherche du journal terminée
"Masque OK Z==="	Surveillance de masquage perturbée zone === rétablie
"Masque Z==="	Masquage zone ===
"Masquage défaut zone ==="	Surveillance de masquage perturbée zone ===

Annexe

"Méd. U-- pile faible"	L'émetteur d'appel d'urgence médicale de l'utilisateur -- a une pile faible
"Médical clavier alarme"	Alarme d'appel d'urgence médicale déclenchée par le clavier
"Médical OK part.#"	La partition d'alarme médicale # a été supprimée
"Médical OK"	L'alarme médicale a été supprimée
"ClavUrgMéd==alarme"	Alarme d'appel d'urgence médicale déclenchée par le clavier ==
"Err. dét. Z==="	Zone === erreur rés. finale
"Détecteur OK Z==="	Zone === erreur de résistance finale réinitialisée
"Défaut test détecteur Z=="	Défaut test de détecteur zone ==
"Historique seul"	Historique seul
"Défaut de pile ok"	Défaut de pile de nouveau ok
"OK défaut CC externe"	Défaut externe du courant continu ok
"Avert. périm. Z=="	Zone d'avertissement de périmètre ==
"Appel soins de santé clav."	Appel soins de santé déclenché par le clavier
"ASS util. -- pile faible"	L'émetteur d'appel de soins de santé de l'utilisateur -- a une pile faible
"Somme de contrôle erronée"	Somme de contrôle erronée
"RTC voie comm. OK"	Défaut de communication ligne téléphonique résolu
"RTC défaut voie de comm."	Défaut de communication ligne téléphonique
"REP== Pile faible"	Répéteur == pile vide
"REP== Brouillage OK"	Répéteur == pas de brouillage sur le répéteur
"REP== Brouillage"	Répéteur == brouillage constaté
"REP== Défaut PSU OK"	Répéteur == pas de défaut d'alimentation électrique sur l'entrée de 12 V
"REP== Défaut PSU"	Répéteur == défaut d'alimentation électrique sur l'entrée de 12 V
"REP== Avertissement RF"	Répéteur == plus de 15 min sans liaison radio avec la centrale d'alarme
"REP== Sabotage OK"	Répéteur == sabotage ok
"REP== Sabotage"	Répéteur == sabotage
"REP== Défaut sup. OK"	Répéteur == la surveillance sans fil perturbée a été réinitialisée.
"REP== Défaut sup."	Répéteur == surveillance sans fil perturbée
"Brouillage RF OK"	Brouillage radio ok
"Brouillage RF"	Brouillage radio
"Sabo ==ER ok"	Le sabotage du lecteur de proxy externe == a été réinitialisé
"Sabo ==ER"	Sabotage du lecteur de proxy externe ==
"Sabotage == OK"	Extension == l'erreur de sabotage a été réinitialisée
"Sabotage == ok"	Clavier == l'alarme anti-sabotage a été réinitialisée
"Sabotage =="	Extension == sabotage déclenché
"Sabotage =="	Alarme anti-sabotage du clavier ==
"Sabotage clav. == ok"	Clavier == l'alarme anti-sabotage a été réinitialisée
"Sabotage clav.=="	Clavier == alarme anti-sabotage
"Sabotage Z== OK"	Zone de sabotage == réinitialisée
"Sabotage Z=="	Zone de sabotage ==
"Sabotage Z==="	Zone de sabotage ===
"Sabotage Z===ok"	Zone de sabotage === réinitialisée
"Sirène # sabotage ok"	Le générateur de signal # de l'alarme anti-sabotage a été réinitialisé
"Sirène # sabotage"	Générateur de signal # alarme anti-sabotage

"Sirène sabotage ok"	Le générateur de signal de l'alarme anti-sabotage a été réinitialisé
"Sirène sabotage"	Générateur de signal alarme anti-sabotage
"Boît. clé ouv. Z=="	Boîtier clé ouvert zone =====
"Boîtier clé fermé Z=="	Boîtier clé fermé zone ==
"Boîtier clé ouvert Z=="	Boîtier clé ouvert zone ===
"Boît. clé fer. Z===="	Boîtier clé fermé zone ===
"Cadenas tent. effr. ok Z===="	Zone de tentative d'effraction ==
"Cadenas tent. effr. Z===="	La zone de tentative d'effraction == a été supprimée
"Int. clé part. # act."	La partition # a été activée par l'interrupteur à clé
"Int. clé part. # désact."	La partition # a été désactivée par l'interrupteur à clé
"Int. clé syst. act."	Le système a été activé par l'interrupteur à clé
"Int. clé syst. désact."	Le système a été désactivé par l'interrupteur à clé
"Int. clé syst. act. int."	Le système a été activé en interne par l'interrupteur à clé
"Int. clé part. # act. int."	La partition # a été activée en interne par l'interrupteur à clé
"Erreur de carte SD ou carte non insérée"	Erreur de carte SD ou carte non insérée
"Grp shunt ##DÉSACT."	Shunter groupe ## désactivé
"Grp shunt ##ACT."	Shunter groupe ## activé
"Sir. == supervision ok"	Sirène radio == surveillance radio ok
"Sir. == défaut de supervision"	Sirène radio == surveillance radio perturbée
"Sir. == surv. Ok"	Sirène externe == surveillance radio perturbée
"SIR== brouillage ok"	Sirène radio == brouillage ok
"SIR== brouillage"	Sirène radio == brouillage constaté
"SIR== défaut ok"	Sirène radio == défaut ok
"SIR== défaut"	Sirène radio == défaut
"Logiciel modifié"	Le logiciel a été modifié
"Tr. vocal = tout acq."	Réglages transmetteur vocal : tous les utilisateurs appelés doivent confirmer
"Tr. vocal = aucun acq."	Réglages transmetteur vocal : aucune confirmation requise
"Transm. vocal = acq."	Réglages transmetteur vocal : un utilisateur appelé doit confirmer
"Sir. == RF OK"	Sirène sans fil == liaison sans fil ok
"Sir. == avertissement RF"	Sirène sans fil == plus de 15 min sans liaison radio avec la centrale d'alarme
"Module enfichable voie comm. OK"	Le module enfichable de la centrale signale que les voies de communication sont ok
"Module enfichable défaut voie de comm."	Le module enfichable de la centrale signale un défaut de la voie de communication
"Défaut 12 V clavier"	Clavier défaut de l'alimentation 12 V
"Défaut activation Z=="	Activation impossible, zone === perturbée ou ouverte
"Défaut activation autom."	L'activation automatique est perturbée
"Défaut générateur de signal ext. Z===="	Défaut du générateur de signal filaire externe Z ===
"Défaut communication téléservice"	Défaut de communication du téléservice
"Défaut test détecteur Z==== alarme"	Défaut test de détecteur zone === alarme déclenchée
"Défaut test détecteur Z==== sabotage"	Défaut test de détecteur zone === sabotage déclenché
"Défaut ok générateur de signal ext. Z===="	Générateur de signal filaire externe Z === ok

Annexe

"Défaut test Z==="	Défaut test de détecteur zone ===
"Système 12 V ok"	12 V alimentation système rétablie
"Défaut système 12 V"	Défaut système 12 V
"Sabotage système OK"	Le sabotage du système a été réinitialisé
"Sabotage système"	Sabotage du système déclenché
"Système réactivé"	Le système a été réactivé
"Erreur système"	Défaut du processeur principal de la centrale. Essayez de redémarrer.
"Démarrage du système"	Le système a été redémarré après une coupure de courant (alimentation électrique principale et batterie).
"Part. # téléc. réinit."	La partition # a été réinitialisée par une télécommande
"Alarme tech. Z=="	Alarme technique dans la zone ==
"Tech. Z== OK"	L'alarme technique dans la zone == a été réinitialisée
"Alarme tech. Z==="	Alarme technique dans la zone ===
"Tech. Z===OK"	L'alarme technique dans la zone === a été réinitialisée
"Partition # réactivée"	La partition # a été réactivée
"Appel test OK"	Appel de test réussi
"Défaut appel test"	Échec de l'appel de test
"Appel test soin"	Appel de soins de santé de test effectué
"Appel test SMS"	Appel de test SMS effectué
"Appel test langue"	Appel test transmetteur vocal effectué
"Bip sonore # sabo. OK"	Le bip sonore # de l'alarme anti-sabotage a été réinitialisé
"Bip sonore # sabo."	Bip sonore # alarme anti-sabotage Contrôlez également le câblage entre le raccordement TR (Tamper Return) et 0 V.
"Bip sonore sabo. OK"	Le bip sonore de l'alarme anti-sabotage a été réinitialisé
"Bip sonore sabo."	Bip sonore alarme anti-sabotage Contrôlez également le câblage entre le raccordement TR (Tamper Return) et 0 V.
"Trace =="	Trace ==
"Porte défaut PSU Z==="	Porte défaut de l'alimentation électrique zone ==
"Porte PSU OK Z==="	Alimentation électrique porte zone == de nouveau OK
"Verrou de porte # pile vide"	Pile vide avec verrou de porte #
"Tr. toutes voies err."	Transmission toutes voies de communication perturbée
"Tr. toutes voies OK"	Transmission toutes voies de communication de nouveau OK
"Tr. prim. chem. err."	Chemin de transmission primaire perturbé
"Tr. prim. chem. OK"	Chemin de transmission primaire de nouveau ok
"Tr. chem. sec. err."	Chemin de transmission secondaire perturbé
"Tr. chem. sec. OK"	Chemin de transmission secondaire de nouveau ok
"AA clav.== alarme"	Alarme agression déclenchée sur le clavier ==
"Conf. AA ==ER"	Alarme agression confirmée par lecteur de proxy externe ==
"AA conf. cen. br."	Alarme agression confirmée par le brouillage radio de la centrale
"AA ok part.#"	L'alarme agression de la partition # a été réinitialisée
"AA ok"	Agression réinitialisée
"AA OK"	L'alarme agression a été réinitialisée.
"AA ok"	L'alarme agression a été réinitialisée

"AA Z.=== alarme"	Alarme agression dans la zone ===
"AA Z===ok"	L'alarme agression de la zone === a été réinitialisée
"AA Z.== alarme"	Alarme agression dans la zone ==
"AA Z==OK"	L'alarme agression de la zone == a été réinitialisé
"Défaut agression ok Z==="	Le défaut de la zone d'agression === a été réinitialisé
"Alarme agression conf. =="	Alarme agression confirmée par détecteur de sabotage sur MAW--
"Alarme agression conf. =="	Alarme agression confirmée par clavier ==
"Alarme agression conf. aux. #"	Alarme agression confirmée par l'alimentation électrique externe sur l'appareil #
"Alarme agression conf. aux."	Alarme agression confirmée par l'alimentation électrique externe sur l'appareil
"Alarme agression conf. clav. rad.=="	Alarme agression confirmée par clavier radio #
"Alarme agression conf. HD=="	Alarme agression confirmée par émetteur panique
"Alarme agression conf. bip sonore #"	Alarme agression confirmée par le bip sonore #
"Alarme agression conf. bip sonore"	Alarme agression confirmée par le bip sonore
"Alarme agression conf. émetteur appel urgence U--"	Alarme agression confirmée par émetteur d'appel d'urgence utilisateur ==
"Alarme agression conf. agr. clav. rad.=="	Alarme agression confirmée par touches al. agr. du clavier radio.
"Alarme agression conf. SIR=="	Alarme agression confirmée par sirène externe--
"Alarme agression conf. bouton homme-mort U--"	Alarme agression confirmée par bouton homme-mort utilisateur ==
"Alarme agression conf. MAW=="	Alarme agression confirmée par MAW
"Alarme agression conf. serveur Web"	Alarme agression confirmée par serveur Web
"Alarme agression conf. Z==="	Alarme agression confirmée par zone ===
"Alarme agression conf. centrale"	Alarme agression confirmée par le contact anti-sabotage de la centrale
"Alarme agression"	Alarme agression déclenchée sur le clavier
"Défaut agression Z==="	Défaut de la zone d'agression ===
"Ignorer"	Le système a été activé malgré l'avertissement
"AGR util. -- alarme"	Alarme par télécommande utilisateur --
"AGR util. -- pile faible"	La télécommande de l'utilisateur -- indique une pile faible
"Non valide"	Non valide
"MAW == défaut de supervision"	MAW == surveillance radio perturbée
"MAW== batterie ok"	MAW== batterie ok
"MAW== batterie faible"	MAW== batterie faible
"MAW== PSU ok"	MAW== défaut de l'alimentation électrique
"MAW== défaut PSU"	MAW== alimentation électrique ok
"MAW== RF OK"	MAW== liaison sans fil ok
"MAW== avert. RF"	MAW == plus de 15 min sans liaison radio avec la centrale d'alarme
"MAW== sabo ok"	MAW== sabotage ok
"MAW== sabo"	MAW== sabotage
"MAW== sir. sabo"	MAW== sirènes sabotage
"MAW== défaut sir."	MAW== défaut sirènes
"MAW== sir. sabo ok"	MAW== sirènes sabotage ok
"MAW== déf. sir. ok"	MAW== défaut sirènes ok
"MAW== supervision ok"	MAW== surveillance radio ok

Annexe

"MAW== supervision ok"	MAW== surveillance radio ok
"MAW== défaut de supervision"	MAW== surveillance radio perturbée
"Fluide Z== alarme"	Détecteur d'inondation zone == alarme
"Fluide Z== ok"	Le détecteur d'inondation zone == a été réinitialisé
"Serveur Web code sabotage"	Sabotage dû à un nombre trop élevé de saisies d'un code erroné sur l'accès au serveur Web
"Serv. Web code sabo ok"	Le sabotage dû à un nombre trop élevé de saisies d'un code erroné sur l'accès au serveur Web a été réinitialisé.
"Réglages usine chargés"	Système défini sur les réglages usine
"SirF== réinit. trouble"	Le défaut de la sirène filaire a été réinitialisé
"SirF== trouble"	Défaut sirène filaire
"Z== suivi photos"	Les photos ont été enregistrées car la zone a déclenché ==.
"Z== bloc alim. ok"	Défaut bloc alim. détecteur de fumée zone == réinitialisé
"Z== err. bloc alim."	Défaut bloc alim. détecteur de fumée zone ==
"Z== fumée PSU ok"	Défaut bloc alim. détecteur de fumée zone === réinitialisé
"Z== défaut PSU fumée"	Défaut bloc alim. détecteur de fumée zone ===
"Z== déf. fumée ok"	Défaut détecteur de fumée zone === réinitialisé
"Z== défaut fumée ok"	Défaut détecteur de fumée zone == réinitialisé
"Z== défaut fumée"	Défaut détecteur de fumée zone ==
"Z== RF OK"	Zone === liaison sans fil ok
"Z== avert. RF"	Zone == plus de 15 min sans liaison radio avec la centrale d'alarme
"Z== supervision OK"	Surveillance radio zone == ok
"Z== défaut de supervision"	Surveillance radio perturbée zone ==
"Z=== ouvert"	La zone === est ouverte
"Z=== fermée"	Zone === fermée
"Z=== non shuntée"	La zone === n'a pas été shuntée
"Z=== défaut fumée"	Défaut détecteur de fumée zone ===
"Z=== avert. RF"	Zone === plus de 15 min sans liaison radio avec la centrale d'alarme
"Z=== supervision ok"	Surveillance radio zone === ok
"Z=== défaut de supervision"	Surveillance radio perturbée zone ===
"Z=== shuntée"	La zone === a été shuntée
"Z==surv. OK"	Surveillance radio zone == ok
"Centrale A/C OK"	L'alimentation électrique de la centrale est ok
"Centrale défaut A/C"	Défaut d'alimentation électrique de la centrale
"Centrale code sabotage OK"	Le sabotage dû à un nombre trop élevé de saisies d'un code erroné sur la centrale d'alarme a été réinitialisé.
"Centrale code sabotage"	Sabotage dû à un nombre trop élevé de saisies d'un code erroné sur la centrale d'alarme
"CC ext. centrale ok"	Alimentation électrique externe de la centrale ok
"Défaut CC ext. centrale"	Défaut de l'alimentation électrique externe de la centrale

Numéros utilisateur

Version logicielle >=1.01.00

Numéro utilisateur	Explication
00	Installateur
01	Administrateur
02-50	Utilisateur
51	Armement rapide / touches d'armement rapide enfoncées
52	Niveau 4 / Utilisateur de niveau d'accès 4
53	<p>Système / Centrale</p> <p>p. ex. lors du passage à l'heure d'été/hiver</p> <p>B053 Date/Heure</p> <p>Système</p> <p>03:00:00 27/03/2015</p>
54	Interrupteur à clé
55	Accès à distance AES/TS, réinitialisation
56	Téléchargement
57	Clavier virtuel via interface Web
58	Processus RF
59	Appel sortant de la centrale (sans code utilisateur), changements d'état de la centrale
60	<p>Trouver IP, programme d'installation IP d'ABUS</p> <p>Ce numéro utilisateur fait l'objet d'un protocole lorsque l'application Trouver IP est utilisée pour trouver la Secvest dans le réseau. Le nom, l'adresse IP, le type, l'état et l'adresse MAC peuvent être déterminés avec Trouver IP.</p>
61	<p>Client DDNS de serveur ABUS</p> <p>Ce numéro utilisateur fait l'objet d'un protocole lors de la modification de la configuration, pendant la réception des ID attribués après l'ajout de l'appareil sur le serveur Abus.</p>

Version logicielle <1.01.00

Numéro utilisateur	Explication
00	Installateur
01	Administrateur
02-50	Utilisateur
51	Armement rapide / touches d'armement rapide enfoncées
52	<p>Système / Centrale</p> <p>p. ex. lors du passage à l'heure d'été/hiver</p> <p>B053 Date/Heure</p> <p>Système</p> <p>03:00:00 27/03/2015</p>
53	Interrupteur à clé
54	Accès à distance AES/TS, réinitialisation
55	Téléchargement
56	Clavier virtuel via interface Web
57	Processus RF
58	Appel sortant de la centrale (sans code utilisateur), changements d'état de la centrale
59	<p>Trouver IP, programme d'installation IP d'ABUS</p> <p>Ce numéro utilisateur fait l'objet d'un protocole lorsque l'application Trouver IP est utilisée pour trouver la Secvest dans le réseau. Le nom, l'adresse IP, le type, l'état et l'adresse MAC peuvent être déterminés avec Trouver IP.</p>

60	Client DDNS de serveur ABUS Ce numéro utilisateur fait l'objet d'un protocole lors de la modification de la configuration, pendant la réception des ID attribués après l'ajout de l'appareil sur le serveur Abus.
----	--

Dépannage et recherche d'erreurs

Redémarrage manuel (extinction et rallumage)

Version logicielle >= 1.01.00

En cas de problèmes, cela peut s'avérer utile pour remettre la centrale dans un état de sortie défini. Tous les réglages et les configurations sont conservés.



Remarque

Le redémarrage n'est possible que lorsque
Toutes les partitions sont désactivées.
La centrale a interrompu tous les transferts, communications et actions importants.

3 possibilités s'offrent à vous

- [1] Dans le menu utilisateur de la centrale d'alarme, au niveau de l'accès administrateur
- [2] Dans le menu utilisateur, au niveau de l'accès au serveur Web en tant qu'administrateur
- [3] Au niveau de la centrale d'alarme, en appuyant sur la touche de navigation « Haut »/« Bas »

[1] Centrale - menu utilisateur

Menu utilisateur -> Configuration -> Fonctions -> Redémarrage de la centrale
Vous pouvez effectuer ici un redémarrage manuel de la centrale.



Remarque

ce menu n'est visible que par l'administrateur. Cela signifie que ce dernier doit s'être connecté au système.

Sélectionnez « Redémarrage de la centrale » en appuyant sur la touche de menu « Modifier ».

Vous êtes invité à confirmer le redémarrage.

Appuyez sur la touche de menu « Oui ».

À ce stade, vous pouvez encore interrompre le redémarrage.

Cliquez sur « Retour ».

[2] Menu utilisateur de l'interface Web

Menu utilisateur -> Configuration -> Fonctions -> Redémarrage de la centrale
Vous pouvez effectuer ici un redémarrage manuel de la centrale.



Remarque

ce menu n'est visible que par l'administrateur. Cela signifie que ce dernier doit s'être connecté au système.

jointe : Redémarrage_centrale d'alarme_1

Configuration Système | Fonctions ON/OFF

Carillon	<input checked="" type="checkbox"/>	Annonce vocale	<input checked="" type="checkbox"/>
Moniteur d'activité	<input type="checkbox"/>	Annonce nom de Zone	<input type="checkbox"/>
Contraste Ecran	10	Rétroéclairage Luminosité	*Haut
Rétroéclairage LCD	*ON	Rétroéclairage Touches Menu	*ON Période
Rétroéclairage Touches Act.	*ON Période	Rétroéclairage Chiffre	*ON Période

Redémarrer centrale

Annuler Envoyer

Logout

- INFO
- État
- Configuration Système
- Contacts
- Utilisateurs
- Test
- Journal de bord
- Clavier
- Isoler des zones

Cliquez sur « Redémarrage de la centrale ».
 Vous êtes invité à confirmer le redémarrage.

jointe : Redémarrage_centrale d'alarme_2

Configuration Système | Fonctions ON/OFF

Confirmer le redémarrage

Annuler le redémarrage Redémarrer maintenant

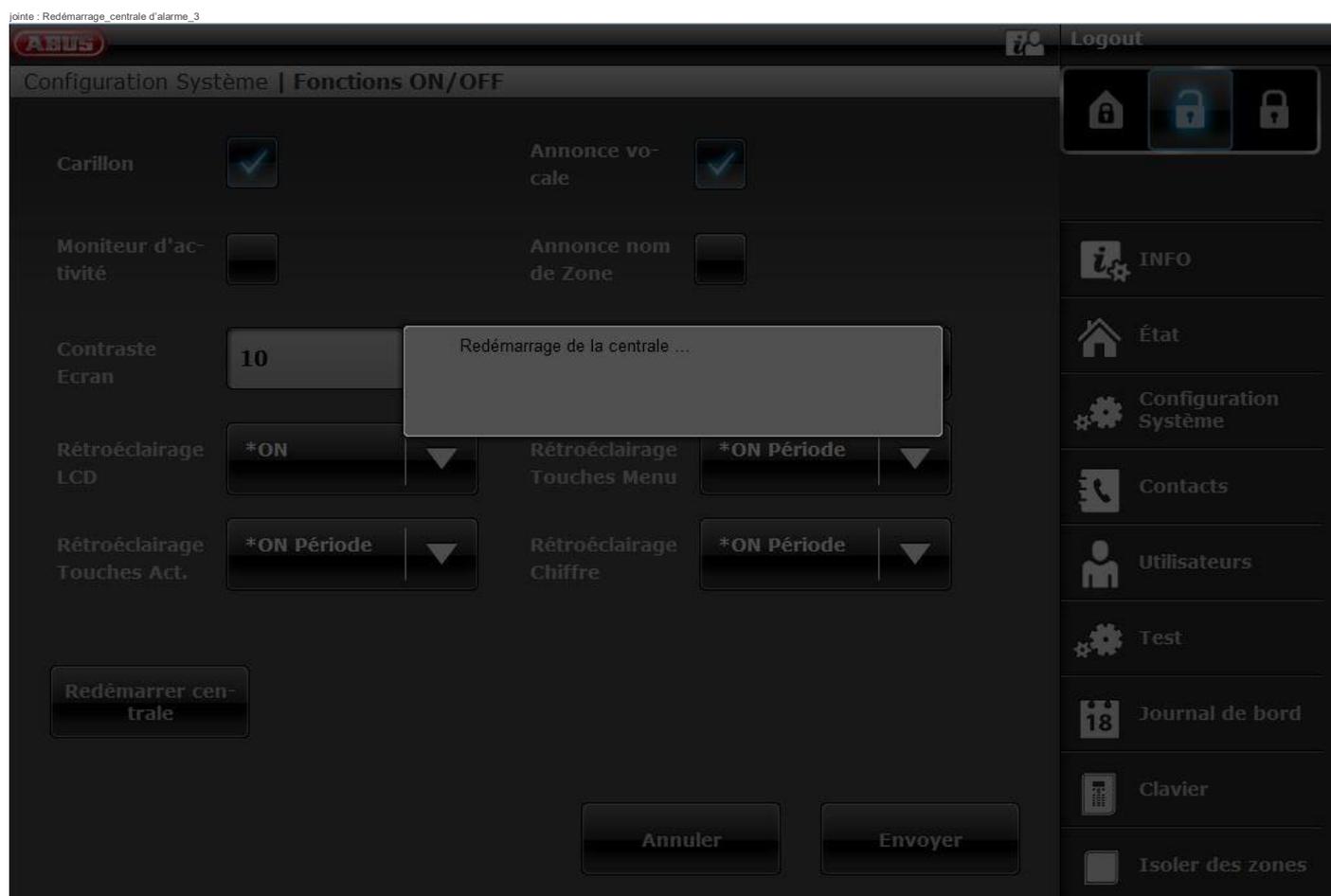
Annuler Envoyer

Logout

- INFO
- État
- Configuration Système
- Contacts
- Utilisateurs
- Test
- Journal de bord
- Clavier
- Isoler des zones

Cliquez à nouveau sur « Redémarrage de la centrale ».
 À ce stade, vous pouvez encore interrompre le redémarrage.
 Cliquez sur « Interrompre le redémarrage ».

Le redémarrage s'affiche comme suit.



Après le redémarrage, vous êtes automatiquement déconnecté du serveur Web. Si vous souhaitez continuer de travailler sur le serveur Web, reconnectez-vous avec votre nom d'utilisateur et votre mot de passe.

[3] Centrale d'alarme - Touches de navigation « Haut »/« Bas »

Appuyez simultanément et de manière prolongée sur les touches de navigation « Haut »/« Bas » pendant plus de 5 s.

L'installateur se trouve dans le mode installateur

Si vous appuyez simultanément et de manière prolongée sur les touches de navigation « Haut »/« Bas » pendant plus de 5 s, la centrale d'alarme est immédiatement redémarrée.

L'administrateur se trouve dans le menu utilisateur

Si vous appuyez simultanément et de manière prolongée sur les touches de navigation « Haut »/« Bas » pendant plus de 5 s, la centrale d'alarme est immédiatement redémarrée.

La centrale se trouve en mode Veille

Si vous appuyez simultanément et de manière prolongée sur les touches de navigation « Haut »/« Bas » pendant plus de 5 s, un écran permettant de saisir un code d'accès apparaît.

Après la saisie d'un code installateur ou administrateur valide et une nouvelle confirmation en cliquant sur « Oui », la centrale d'alarme est redémarrée.



Remarque

Création du certificat SSL en cours, ceci peut durer quelques minutes.
Les fonctions réseau ne sont pas disponibles pendant ce temps.

**Remarque**

Le message suivant s'affiche : Initialisation réseau, veuillez patienter...

Effectuer un appel test GSM/mobile manuellement, carte prépayée



Danger

et



Remarque

Vous utilisez une carte SIM prépayée avec un tarif prépayé.

Exemple : CallYa, Xtra, MagentaMobil-Start

Veillez effectuer **tous les mois** ou **tous les trois mois** un appel test GSM/mobile et/ou envoyer un SMS test GSM/mobile.

En cas de non-utilisation prolongée du réseau GSM/mobile, il peut arriver

Qu'aucun appel d'alarme ne soit passé par GSM/mobile.

Qu'aucun SMS d'alarme ne soit envoyé par GSM/mobile.

Que la carte soit bloquée momentanément par l'exploitant du réseau.

La carte ne peut plus s'inscrire au réseau GSM/mobile.

Un message de dérangement sur la centrale vous l'indique.

Par conséquent, **aucun appel d'alarme** ni **SMS d'alarme** ne peut être effectué. Par ailleurs, la centrale **n'est plus accessible** via GSM/mobile.

En cas de non-utilisation prolongée, l'exploitant du réseau peut également agir de manière similaire pour les cartes contractuelles.

Veillez donc effectuer également **tous les mois** ou **tous les trois mois** un appel test GSM/mobile et/ou envoyer un SMS test GSM/mobile.

Module GSM/de téléphonie mobile et module Wi-Fi



Danger

Pour l'installation supplémentaire du module Wi-Fi, utilisez impérativement **Externe** pour l'antenne de téléphonie mobile.

Système -> Matériel -> Antenne mobile -> **Externe**

L'antenne de téléphonie mobile interne sur la platine peut influencer voire empêcher la connexion du signal Wi-Fi.

LED de diagnostic sur la platine principale et le module GSM/de téléphonie mobile

Identification des LED sur la platine	Explication
HEART BEAT	<p>Affichage de l'état de fonctionnement Clignote (en vert) 1 Hz Fonctionnement normal</p> <p>Utilitaire de mise à jour Secvest utilisé : La LED « battements de cœur » doit clignoter rapidement pour indiquer que la centrale Secvest fonctionne en mode « Mise à jour ».</p> <p>BOM : LED9 Y/G</p>
3V3	<p>Tension d'alimentation interne 3,3 V Allumée (verte) La tension d'alimentation interne de 3,3 V est correcte.</p> <p>BOM : LED7 Y/G</p>
13V8	<p>Tension d'alimentation interne 13,8 V Allumée (verte) La tension d'alimentation interne de 13,8 V est correcte.</p> <p>BOM : LED6 Y/G</p>
ACTIVITY	<p>Activité Ethernet Désactivé Pas de connexion Allumée (verte) Connexion Clignote (en vert) Activité</p> <p>BOM : LED10 Y/G</p>
B1 STATUS	<p>État Batt.1 Allumée (rouge) Rechargement – Traitement préalable ou courant continu (CC Constant Current) ou tension régulée CV (Constant Voltage). Désactivé Rechargement terminé Clignote (en rouge) 0,1 Hz Défaut temps ou défaut température de cellule</p> <p>BOM : LED2 red</p>
B2 STATUS	<p>État Batt.2 Allumée (rouge) Rechargement – Traitement préalable ou courant continu (CC Constant Current) ou tension régulée CV (Constant Voltage). Désactivé Rechargement terminé Clignote (en rouge) 0,1 Hz Défaut temps ou défaut température de cellule</p> <p>BOM : LED1 red</p>
OFF HOOK	RTC ou état de câble a/b

	<p>Allumé L'installation a « décroché le combiné du téléphone » pour RTC</p> <p>Désactivé L'installation a « raccroché le combiné du téléphone » pour RTC</p> <p>BOM : LED3 red</p>
RFTX	<p>État émetteur RF</p> <p>Allumé Émetteur RF actif</p> <p>Désactivé Émetteur RF inactif</p> <p>BOM : LED4 red</p>
ÉTAT (module GSM/de téléphonie mobile)	<p>État du module GSM/de téléphonie mobile</p> <p>Désactivé Mode veille</p> <p>Clignotement de 0,1 s pendant une durée d'1 s Recherche réseau ou aucun état réseau (y compris le cas où la carte SIM n'est pas insérée et celui où le code PIN est autorisé)</p> <p>Clignotement de 0,1 s pendant une durée de 3 s Connecté à un réseau 2G</p> <p>Clignotement de 0,1 s pendant une durée de 0,125 s Service de données GPRS</p> <p>Allumé Appel vocal</p> <p>BOM : LEDx red</p>

Trace, enregistrement des processus de communication

Dans la centrale, accédez au menu suivant :

Mode Installateur -> Info -> Transmission

Appuyez sur la touche *, puis sur la touche chiffrée <x>. Les chiffres pouvant être remplacés par « x » sont indiqués ci-dessous.

Un tampon de trace en direct (mode direct) est affiché.

Lors de l'affichage de la trace

Appuyez sur la touche # pour consulter l'horodatage.

Appuyez sur la touche * pour prendre un instantané (mode Instantané). Utilisez les touches Haut/Bas pour faire défiler le tampon de trace. Appuyez sur la touche * pour revenir au mode direct.

Appuyez sur la touche de menu de droite en mode direct ou en mode Instantané pour vous déplacer horizontalement vers la droite. Pour revenir au centre, appuyez sur la touche Haut ou Bas.

Pour enregistrer la trace pertinente sur la carte SD, appuyez sur la touche 0 en mode direct ou en mode Instantané. Une fois la carte SD retirée, la trace peut également être analysée en veille sur un ordinateur.

La trace est enregistrée au format suivant :

\\TRACE\trace_0X.txt

Les chiffres pouvant être remplacés par « x » sont indiqués ci-dessous.

Remarque :

« > » signifie « vers l'extérieur », envoyé par la centrale ou transmis par cette dernière.

« < » signifie « vers l'intérieur », reçu par la centrale ou transmis à cette dernière.

Version logicielle <= v2.01.08

X = 0 = GSM/mobile (p. exemple « GSM – HUAWEI MG 323-B » ou « module enfichable »)

La communication entre la platine principale et le module GSM/de téléphonie mobile, les commandes AT, etc.

Exemple :

Commande AT CSQ
< +CSQ : <rssi>,<ber>

Description des paramètres

<rssi> : indicateur d'intensité du signal reçu

0 : ≤ -113 dBm

1 : -111 dBm

2...30 : -109...-53 dBm (incréments de 2 dBm)

31 : ≥ 51 dBm

99 : inconnu ou incommensurable

<ber> : taux d'erreurs sur les bits en pourcentage. La valeur de **ber** ne peut être interrogée que pendant le traitement des appels. Sinon, seule la valeur **0** ou **99** est renvoyée. Actuellement, seule la valeur **99** est renvoyée.

Ex.

+CSQ : 14,99

14 = -85 dBm (affichage Secvest RSSI 4)

La plage de valeurs ci-dessus de 0 à 31 correspond à la plage de valeurs de la Secvest de 0 à 9

X = 1 = E-mail

Protocole de communication entre la centrale et le serveur SMTP.

X = 2 = Voip SIP

Protocole de communication entre la centrale et le serveur VoIP.

X = 3 = Appel téléphonique

Protocole téléphonique du transmetteur vocal via a/b (RTC) ou GSM/mobile
ou

Protocole téléphonique du reporting CRA/STS via a/b (RTC) ou GSM/mobile

Remarque

Il n'existe pas de protocole de communication lié à DC-09 (transfert IP AES/TS).

Si vous souhaitez réaliser une trace du transfert IP AES/TS, utilisez un outil réseau adapté, par exemple Wireshark. Certains routeurs permettent également de réaliser un enregistrement réseau. Il est également possible d'utiliser Wireshark pour l'analyse.

X = 4 = Client HTTPS

Protocole de communication entre la centrale et le serveur ABUS.

X = 5 = Serveur HTTPS

Cet écran présente toutes les cinq secondes un instantané des connexions HTTPS au serveur Web actives.

Exemple d'instantané :

```
00001286.98:< # 4 | up 4 | idle 1 | host 192.168.1.204:10510 | system/partitions _=1432112428380
00001286.98:< # 3 | up 4 | idle 3 | host 192.168.1.194:54252 | logs--1
00001286.98:< # 2 | up 4 | idle 3 | host 192.168.1.194:53100 | system/partitions-2/zones
00001286.98:<HTTP(S) stats 00:21:28
```

Il indique

- combien de temps la connexion TCP a duré (en secondes)
- combien de temps la connexion TCP était en attente (en secondes)
- l'adresse IP hôte et le port
- le nom de fichier demandé, le chemin d'accès et la chaîne de demande.

X = 6 = SNTP

Protocole de communication entre la centrale d'alarme et le serveur NTP.

exemple

```
>***Timesync from ntp.exnet.com***
```

Version logicielle >= v3.00.03

X = 0 = GSM/mobile (p. exemple « GSM – HUAWEI MG 323-B » ou « module enfichable »)

Voir ci-dessus

Mobile IP/Mobile

```
>AT+CESQ
```

```
<+CESQ : 99, 99, 255, 255, 24, 47
```

```
<+CESQ : <a>, <b>, <c>, <d>, <e>, <f>
```

a, b

Indique la puissance de signal et la qualité en **2G**

Lorsque la cellule téléphonique mobile actuelle **n'est pas** une cellule 2G, **99** est écrit ici

Plage de valeurs

a = puissance de signal, 0 (très mauvaise) - 63 (très bonne)

b = qualité, 0 (très mauvaise) - 7 (très bonne)

c, d

Indique la puissance de signal et la qualité en **3G**

Lorsque la cellule téléphonique mobile actuelle **n'est pas** une cellule 3G, **255** est écrit ici

e, f

Indique la puissance de signal et la qualité en **4G**

Lorsque la cellule téléphonique mobile actuelle **n'est pas** une cellule 4G, **255** est écrit ici

Plage de valeurs

e = qualité, 0 (très mauvaise) - 34 (très bonne)

f = puissance de signal, 0 (très mauvaise) - 97 (très bonne)

X = 1 = E-mail

Voir ci-dessus

X = 2 = Voip SIP

Voir ci-dessus

X = 3 = Appel téléphonique

Voir ci-dessus

X = 4 = Client HTTPS

Voir ci-dessus

X = 5 = Serveur HTTPS

Voir ci-dessus

X = 6 = SIA-IP (DC-09)

Protocole de communication entre la centrale d'alarme et AES/TS. Les messages DC-09 réels figurent dans ASCII Notation. La représentation des messages DC-09 est similaire aux exemples du chapitre « Annexe B : Exemple Message Frames » des spécifications DC-09.

```
>A38700b6**SIA-DCS"0013L0#7128[c499a115.....]....
```



Remarque

Se référer à GMT pour l'horodatage, tel qu'exigé pour DC-09.

X = 7 = SNTP

Protocole de communication entre la centrale d'alarme et le serveur NTP.

exemple

```
>***Timesync from ntp.exnet.com***
```

X = 8 = PPP

Protocole point à point

Principalement pour la transmission mobile

exemple

```
>ATDT*99***1H
```

```
<CONNECT
```

tone dialing

X = 9 = Connexion au cloud

Le protocole de communication entre la centrale d'alarme et le cloud ABUS.

Exemple :

```
>ID Panneau : U0yVq7k.....
```

X = 10 = système (**version logicielle >= v3.01.01**)

10 = appuyez pour cela sur la touche de menu ▲ « Haut ».

Cet affichage montre les erreurs système

X = 11 = caméras (**version logicielle >= v3.01.09**)

11 = appuyez pour cela sur la touche de menu ▲ « Bas ».

Cet affichage montre les erreurs de communication entre la centrale et les caméras.

X = 12 = ping ICMP (**version logicielle >= v3.01.16**)

12 = appuyez pour cela sur la touche de menu « Retour ».

Cet affichage montre le protocole de communication ping entre la centrale et le serveur ABUS.

Exemple quand tout est OK :

- Ping triggered
- Trying DNS for ping.abus-server.com
- Sent ping request to 91.250.95.198
- Ping reply OK



Remarque

(Version logicielle >= v3.01.16)

Utilisez * suivi de la touche 1 et appuyez ensuite à nouveau sur le 1 pour effectuer des enregistrements (les écrans) de chaque processus de communication.

Routeur, IAD, pare-feu

Reporting CRA/STS et DC-09



Remarque

Lors de la transmission, le protocole Internet **TCP** est utilisé. TCP utilise le port 9999.

Si les messages ne peuvent être envoyés, il peut arriver dans certaines circonstances que le pare-feu verrouille également différents ports sortants. Contrôlez par conséquent les réglages du pare-feu au niveau du routeur ou d'IAD.

Le port TCP 9999 utilise le Transmission Control Protocol. TCP est un des protocoles principaux dans les réseaux TCP/IP. TCP est un protocole orienté sur la connexion nécessitant une pression de la main pour paramétrer les communications de bout en bout. Une fois la connexion paramétrée, les données d'utilisateur peuvent être envoyées en deux voies via la connexion.

Attention ! TCP garantit la livraison de paquets de données au port 9999 dans l'ordre dans lequel ils ont été envoyés. Une communication garantie via le port TCP 9999 est la différence principale entre TCP et UDP.

Fuseaux horaires

Un fuseau horaire est une zone composée de plusieurs états et de parties d'états plus grands dans laquelle la même heure réglementée officiellement s'applique.

Le temps zonal indique l'écart entre l'heure locale et le TUC (temps universel coordonné) ou GMT (Greenwich Mean Time, temps moyen de Greenwich).

Exemple pour la France :

- Heure d'hiver : UTC/GMT +1
- Heure d'été : UTC/GMT +2

Centre de notification du réseau fixe

Allemagne

Exploitant F-SMSC	Protocole	Service n° tél
Materna	UCP 8N1	09003 266 9002
Telekom		01930105

Vous trouverez des informations complètes sur les liens suivants :

Materna

<http://www.sms-im-festnetz.de/sms/>

Telekom

<http://hilfe.telekom.de/hsp/cms/content/HSP/de/12556/Startseite/SMS;jsessionid=1620596013AB81A8BADD3E34609A213F>

<http://hilfe.telekom.de/hsp/cms/content/HSP/de/12538>

Centre de notification du réseau GSM

Pour pouvoir envoyer un SMS à un numéro de téléphone prédéfini en cas d'événement, vous devez enregistrer le numéro de la centrale SMS sur la carte SIM.

Voici une vue d'ensemble des opérateurs de réseau mobile et le numéro de leur centrale SMS.



Remarque

Pour plus de précisions, consultez votre opérateur réseau mobile.

Notification par SMS

Opérateur	Réseau mobile	Centrale SMS
Telekom (D1)	Telekom	+491710760000
Vodafone (D2)	Vodafone	+491722270333 (n° alternatif : +491722270000)
o2	o2	+491760000443
BASE (E-Plus)	E-Plus	+491770610000
mobilcom- debitel	Telekom	+491710760315
	Vodafone	+491722270880
	o2	+491760000462
	E-Plus	+491770602300
1&1	Vodafone	+491722270333 (n° alternatif : +491722270000)
blau.de	E-Plus	+491770610000
callmobile	Telekom	+491710760000
	Vodafone	+491722270333
congstar	Telekom	+491710760000
FONIC	o2	+491760000443
klarmobil	Telekom	+491710760000
	o2	+491760000466
McSIM	Vodafone	+491722270333 (n° alternatif : +491722270000)
PHONEX	o2	+491760000443
simyo	E-Plus	+491770610000

* Données non contractuelles

Notification par e-mail / setup e-mail

Pour pouvoir envoyer un e-mail à une adresse e-mail prédéfinie en cas d'événement, vous devez enregistrer les données de connexion SMTP du compte de messagerie dans la Secvest.



Remarque

La fonctionnalité SMTP n'est pas gratuite chez tous les fournisseurs.

Voici une liste de fournisseurs de services de messagerie gratuits.

- GMX
- web.de
- Yahoo
- T-Online
- Google Mail
- Outlook

*Données non contractuelles

Arcor

Nom serveur	mail.arcor.de
N° port serveur IP	25 ou 587
Compte	< Adresse e-mail > par ex. dupont@arcor.de
Nom d'utilisateur	< Adresse e-mail > par ex. dupont@arcor.de
Mot de passe	< Mot de passe du compte de messagerie électronique >
SSL	Bloqué

GMX

Nom serveur	mail.gmx.net
N° port serveur IP	465
Compte	< Adresse e-mail > par ex. dupont@gmx.de
Nom d'utilisateur	< Adresse e-mail > par ex. dupont@gmx.de
Mot de passe	< Mot de passe du compte de messagerie électronique >
SSL	Autorisé

GMX

Nom serveur	mail.gmx.net
N° port serveur IP	25 ou 587
Compte	< Adresse e-mail > par ex. dupont@gmx.de
Nom d'utilisateur	< Adresse e-mail > par ex. dupont@gmx.de
Mot de passe	< Mot de passe du compte de messagerie électronique >
SSL	Bloqué

Googlemail

Nom serveur	smtp.gmail.com
N° port serveur IP	465
Compte	< Adresse e-mail > par ex. dupont@gmail.com
Nom d'utilisateur	< Adresse e-mail > par ex. dupont@gmail.com
Mot de passe	< Mot de passe du compte de messagerie électronique >
SSL	Autorisé

Annexe

Googlemail

Nom serveur	smtp.gmail.com
N° port serveur IP	25 ou 587
Compte	< Adresse e-mail > par ex. dupont@gmail.com
Nom d'utilisateur	< Adresse e-mail > par ex. dupont@gmail.com
Mot de passe	< Mot de passe du compte de messagerie électronique >
SSL	Bloqué

T-Online

Nom serveur	securesmtp.t-online.de
N° port serveur IP	465
Compte	< Adresse e-mail > par ex. dupont@t-online.de
Nom d'utilisateur	< Adresse e-mail > par ex. dupont@t-online.de
Mot de passe	< Mot de passe du compte de messagerie électronique >
SSL	Autorisé

T-Online

Nom serveur	securesmtp.t-online.de
N° port serveur IP	25 ou 587
Compte	< Adresse e-mail > par ex. dupont@t-online.de
Nom d'utilisateur	< Adresse e-mail > par ex. dupont@t-online.de
Mot de passe	< Mot de passe du compte de messagerie électronique >
SSL	Bloqué

Web.de

Nom serveur	smtp.web.de
N° port serveur IP	25 ou 587
Compte	< Adresse e-mail > par ex. dupont@web.de
Nom d'utilisateur	< Adresse e-mail > par ex. dupont@web.de
Mot de passe	< Mot de passe du compte de messagerie électronique >
SSL	Bloqué

Yahoo.de

Nom serveur	smtp.mail.yahoo.de
N° port serveur IP	465
Compte	< Adresse e-mail > par ex. dupont@yahoo.de
Nom d'utilisateur	< Adresse e-mail > par ex. dupont@yahoo.de
Mot de passe	< Mot de passe du compte de messagerie électronique >
SSL	Autorisé

Yahoo.de

Nom serveur	smtp.mail.yahoo.de
N° port serveur IP	25 ou 587
Compte	< Adresse e-mail > par ex. dupont@yahoo.de
Nom d'utilisateur	< Adresse e-mail > par ex. dupont@yahoo.de
Mot de passe	< Mot de passe du compte de messagerie électronique >
SSL	Bloqué

Configuration Mobile IP/Communication données mobiles



Remarque

Vous trouverez ici quelques données d'accès. En raison des nombreux opérateurs mobiles en Europe et du nombre encore plus important d'éditeurs de cartes SIM (fournisseurs d'accès), vous trouverez ici seulement quelques exemples sélectionnés.

Données non contractuelles

Vodafone Allemagne

APN	web.vodafone.de
Nom d'utilisateur	Sans/Vide
Mot de passe	Sans/Vide

Telekom Allemagne

APN	internet.telekom
Nom d'utilisateur	t-mobile
Mot de passe	tm

blau Allemagne

APN	internet.eplus.de
Nom d'utilisateur	blau
Mot de passe	blau

Eplus Allemagne

APN	internet.eplus.de
Nom d'utilisateur	eplus
Mot de passe	internet

Aldi Talk Allemagne

APN	internet.eplus.de
Nom d'utilisateur	eplus
Mot de passe	gprs

Sipgate (par ex. VoIP)

APN	internet
Nom d'utilisateur	sipgate
Mot de passe	sipgate

Service après-vente et support

Consommateur final

En cas de questions, veuillez vous adresser à votre revendeur ou à votre installateur.

Revendeur spécialisé/Installateur

En cas de questions, veuillez vous adresser au numéro d'assistance téléphonique correspondant.

Pour obtenir plus d'informations sur le produit, rendez-vous sur notre site Internet.

ABUS Security-Center GmbH & Co. KG

86444 Affing

Linker Kreuthweg 5

ALLEMAGNE

www.abus.com

info@abus-sc.com

Mise hors service de la centrale

- Sélectionnez :
Menu -> Mode Installateur
- Ouvrez la centrale
- Retirez la ou les batterie(s) de secours
- Débranchez l'alimentation électrique, la connexion réseau ou le PSU externe
- Retirez les installations et démontez la centrale

Protection des données



Danger



Remarque

Lors de la transmission, de l'envoi pour réparation et de la mise hors service de la centrale, veuillez noter que les dossiers

CONFIG

et

IMG_X

de la carte SD doivent **impérativement être supprimés**.

ou que la carte SD doit être **retirée**.

La carte SD peut contenir des informations importantes concernant l'utilisateur et sa propriété.

Le dossier

CONFIG

contient la configuration de la centrale lors de la sauvegarde via le GUI.

La configuration contient par ex.

Les données d'accès (mot de passe) au serveur ABUS

Les données d'accès (mot de passe) au compte e-mail

Les données d'accès (mot de passe) VoIP

Les données d'accès (mot de passe) des caméras

Les coordonnées du répertoire

Le dossier

IMG_X

contient les images de la caméra TVIP41550.

Selon le lieu de montage de la caméra, il s'agit d'images de votre vie privée.

Élimination



Éliminez l'appareil et les batteries conformément à la directive UE relative aux déchets d'équipements électriques et électroniques 2012/19/UE – WEEE (Waste Electrical and Electronic Equipment). En cas de doute, veuillez vous adresser aux autorités communales compétentes en matière d'élimination. Vous recevrez les informations sur les points de reprise de vos vieux appareils par ex. auprès de l'administration communale ou municipale locale, des entreprises locales d'élimination des déchets ou auprès de votre revendeur.

Éliminez l'emballage conformément aux directives locales.

- 2014/53/UE 3, 15
- ABUS Security-Center GmbH & Co. KG 8, 439
- Accès à distance 25
- Act. interne 134
- Activation 32
- Activation, désactivation 21
- Activée 125
- Adresse MAC 57
- AES/TS Reporting 374
- Affectation des touches 18
- Affichage d'état 62
- Aide en ligne 47
- Aide en ligne 22
- Alarme locale 29
- Alarme sans fil bidirectionnelle 22
- Alerte
 - Externe 24
- Alerte interne 27
- Alerte silencieuse 33
- Alimentation électrique
 - Dangers 11
- Appel d'urgence de soin 234, 280
- Appel test GSM 417
- Appel test mobile 417
- Assistant de démarrage 354
- Assistant, assistant de démarrage 354
- Avertissement
 - Danger 9
 - Important 9
 - Remarque 9
- Avertisseur combiné 28
- Badge 23
 - Badge Proximity 23
- Bande de fréquence de sécurité 32
- Barre d'informations 47
- Bloc d'alimentation 11, 40
- Bouton
 - Connexion 48
- Bouton de connexion 47
- Broches de réinitialisation de code 19, 152, 157
- Calendrier Arm./Désarm. 46, 125, 134
- Caractéristiques techniques 306
- Carte micro-SD 42
- Carte SD 42
- Centrale 51
- Centrale d'alarme, centrale 21
- Centrale SMS 426
- Centre de notification 425, 426
- Certifications 36
- Champ de saisie
 - Mot de passe 48
 - Nom d'utilisateur 48
- Clavier de commande sans fil 86
- Clavier de commande sans fil 25
- Clavier virtuel 305
- Codage des signaux radio 23
- Code d'administrateur par défaut 10
- Code d'installateur par défaut 10
- Code tournant 31
- Codes CID 379, 381
- Codes SIA 384, 387
- Commande
 - Lecteur de clé Proximity 17
 - Touche Désactiver 17
 - Touche MES totale 17
- Communication 55, 201
- Communication données mobiles 430
- Composants 63
- Composants 28
- Conditions de temps 37
- Configuration Mobile IP 430
- Configurer
 - Périphérie du système d'alarme sans fil 8
- Conformité 320
- Connexion
 - à la Secvest 44
- Connexion/déconnexion 8
- Contact ID 374
- Contenu de la livraison 16
- Customisation 61
- DC-09 376
- Déclaration de conformité 3
- Déconnexion
 - de la Secvest 45
- Demande d'état 33
- Dépannage 413
- Désactivation 32
- Détecteur 67
- Détecteur câblé 24
- Détecteur d'alarme 21

- Détecteur d'inondation 35
- Détecteur d'ouverture 30
- Détecteur de bris de glace 22, 25
- Détecteur de danger 25
- Détecteur de mouvement 22
- Détecteur de vibrations 24
- Détecteur filaire 24
- Détecteur sans fil 25
- Détecteur sismique 32
- Détecteurs autonomes avertisseurs de fumée 31
- DHCP 23, 203
- Diagnostic d'erreur 413
- Directives européennes 320
- Dommmages techniques 34
- Données communication mobile 430
- Données d'accès aux systèmes de sécurité 10
- Écran 23
- Écran d'authentification 44, 48
- Éléments de commande 47
- Élimination 433
- E-mail 260
- Emballage 16
- EN 50131-3 §9.1 gg 46, 331
- EN 50131-3 §9.1 hh 46, 331
- EN 50131-3 §9.1 jj 331
- EN 50131-3 §9.1 m 46, 331
- EN 50131-3 §9.1 p 16
- EN 50131-3 §9.1 x 46, 125, 134
- EN 50131-3 §9.1 y 46, 125, 134
- Enregistrement des processus de communication 420
- Enregistrement des réglages 45
- Entrées de journal de bord 398
- Équipement compatible 322
- État 33, 62
- Ethernet 57
- Événements CID/SIA 378
- Événements SIA/CID 378
- Extensions de communication 28
- Fausses alertes 11
- FDL 24
- Filtre antiparasite 11
- Fin de ligne double 24
- Format rapide 374
- Formats de protocole AES/TS Reporting 374
- Formats de protocole TS/AES Reporting 374
- Fuseaux horaires 424
- Garantie 3
- Générateur de signal – Intérieur 90
- Générateur de signal intérieur 90
- Groupes de rapport CID 379, 381
- Groupes de rapport SIA 384, 387
- GUI 26
- Guide de démarrage rapide 8
- Heure GMT 377, 424
- Heure TUC 377, 424
- Historique 302, 398
- IAD 423
- Identification individuelle 24
- Implantation 15
- Index 434
- Indication d'état 33
- Info 51
- Installation 27
 - Périphérie du système d'alarme sans fil 8
 - Secvest 8
 - Système d'alarme sans fil 8
- INTERFACE WEB 35
- Interrupteur à clé sans fil 25
- Interrupteur anti-sabotage du boîtier 41
- Lecteur de clé Proximity 17
- LED de diagnostic 418
- Limite de la responsabilité 2
- Maintenance et entretien 357
- Manipulation 32, 34
- Menus principaux 47
- Messages d'erreur CME/CMS 394
- Messages d'erreur GSM CME/CMS 394
- Messages d'erreur par e-mail 390
- Messages d'erreur par TCP/IP 391
- Messages d'erreur par VoIP 393
- Messages SSL 391
- Mise à niveau logicielle 358
- Mise hors service 432
- Mobile 58
- Mode Nettoyage 285
- Mode sans fil 15
 - Conformité R&TTE 15
 - Licence radio 15
- Module d'information 93
- Module hybride 26
- Modules hybrides 60
- Modules hybrides 103
- Montage du module de téléphonie mobile 41

- Mot de passe 44, 48
- Niveau 1-4 29, 36, 363
- Niveau d'accès 1-4 36, 363
- Nom d'administrateur 10
- Nom d'installateur 10
- Normes et standards 320
- Notification par e-mail 427
- Numéros utilisateur 411
- Numéroteur téléphonique 16, 34
- options de communication 268
- Paramétrage E-mail 427
- Pare-feu 423
- Partitions 34, 124
- Périphériques d'activation 32
- Plaque de montage
 - Fixation murale 40
- Portée sans fil 25
- Première mise en service 43
- Présentation de l'appareil 17
- Priorité d'édition 16
- Programmation 31
 - Secvest 8
- Programmation Usine 43, 151, 153
- Protection anti-effraction active 21
- Protection anti-sabotage 32
- Protection de fenêtre sans fil 25
- Protection de l'enveloppe extérieure 22
- Protection des données 432
- Protection intérieure 27
- Protocole de transmission 8
- Raccordement
 - des périphériques 41
- Raccordements 15
- RC 31
- Réaction agression 148
- RED 3, 15
- Redémarrage 413
- Réglages d'usine à niveaux 152
- Réglages d'usine logiciel 331
- Réglages d'usine matériel 330
- Réinitialiser 151
- Réinitialiser broches de code 19, 152, 157
- Remarques concernant la batterie 13
- Répéteur 99
- Répéteur RF 99
- Réseau mobile 426
- Rétablissement de la configuration d'origine 43
- Routeur 423
- RTC 56
- Sabotage 32
- Secteur extérieur abrité 25
- Sécurité 9
- Secvest
 - Activation/désactivation 8
 - Implantation 15
- Sélection de partition 62
- Service après-vente et support 431
- SIA 375
- Signaux sonores, acoustiques 355
- Sirène 21, 32
- Sirènes – Sirènes d'extérieur 22, 88
- Sirènes – Sirènes d'intérieur 27, 93
- SMS 246
- SMSC 425, 426
- Sommaire 4
- Sorties 107
- Sorties filaires 117
- Sorties mixtes 121
- Sorties module hybride 118
- Sorties relais 31
- Sorties sans fil 108
- Sous-menus 47
- Surface avant à touches 42
- Surface avant tactile 42
- Surveillance de périmètre 31
- Surveillance des erreurs et du sabotage de la centrale 37
- Symboles 9
- Système 150
- Système anti-effraction 24
- Système d'alarme 21, 24
- Système d'alarme sans fil 25**
- Système de détection de danger 25
- Télécommande sans fil 25
- Téléservice 25
- Termes, définitions 21
- Test 281
- Test de fonctionnement
 - Secvest 8
- Trace 420
- Transmetteur vocal 33, 238
- TS Reporting 215
- TS/AES Reporting 374
- Type d'alarme 21

UE 3
Urgence médicale 29
Utilisateur 22
 Connexion/déconnexion 8
 Installateur 44, 48
Utilisation conforme 9
Utilisation intuitive 27
Valeurs par défaut logiciel 331
Valeurs par défaut matériel 330
VdS 112
Verrous de porte 97
Vue avant 17
WAM 95
Zone 36
Zone d'alarme 21
Zone d'alarme filaire 24
Zone d'alarme sans fil 24, 25
Zone filaire 24
Zone radio 25
Zones filaires 82
Zones IP 67
Zones module hybride 83
Zones sans fil 80

Système d'alarme sans fil ABUS

Secvest

V3.01.17

Fabricant
ABUS Security-Center GmbH & Co. KG
Linker Kreuthweg 5
D-86444 Affing