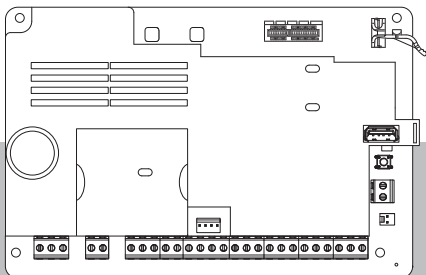


Centrales

B Series: B6512, B5512, B4512, B3512



fr Notes de version

Table des matières

1	Introduction	4
1.1	À propos de la documentation	4
1.2	Configuration requise	5
2	Firmware version 3.14.012	9
2.1	Nouveautés	10
2.2	Établissements pénitentiaires	11
2.3	Problèmes connus	13
3	Firmware version 3.12.024	15
3.1	Nouveautés	15
4	Firmware version 3.12.020	17
4.1	Nouveautés	18
4.2	Corrections	19
4.3	Problèmes connus	20
5	Historique de révision du firmware	23
5.1	Firmware version 3.11.5	23
5.2	Firmware version 3.11	24
5.3	Firmware version 3.10	28
5.4	Firmware version 3.09.050	29
5.5	Firmware version 3.08	31
6	Logiciels libres 3.14.012	34

1 Introduction

Ces *release notes* concernent la version 3.14.012 du firmware de la centrale.

1.1 À propos de la documentation

Copyright

Ce document est la propriété de Bosch Building Technologies. Il est protégé par le droit d'auteur. Tous droits réservés.


Marques commerciales

Tous les noms de matériels et logiciels utilisés dans le présent document sont probablement des marques déposées et doivent être considérés comme telles.

Dates de fabrication des produits Bosch Security Systems B.V.

Utilisez le numéro de série situé sur l'étiquette du produit et connectez-vous au site Web de Bosch Building Technologies à l'adresse : <http://www.boschsecurity.com/datecodes/>.

L'image suivante présente un exemple d'étiquette de produit et indique où trouver la date de fabrication dans le numéro de série.



BOSCH

Model Number

Mat/N: F01Uxxxxxx

7 | 82695 | 11xxx | 9

8 | 717332 | 311xxx

09216082027193xxxx

PRODUCT

QTY= 1

1.2 Configuration requise

Cette section décrit la configuration requise pour que le logiciel de paramétrage à distance (RPS) et que le récepteur/la passerelle Conettix prennent en charge cette version du firmware de la centrale.

1.2.1 Logiciel de paramétrage à distance (RPS, Remote Programming Software)

Pour utiliser toutes les nouvelles fonctionnalités de cette version du firmware, vous devez utiliser RPS version 6.12 ou ultérieure.

1.2.2 Récepteur/passerelle Conettix

Format Conettix Modem4

Lorsque vous configurez la centrale pour l'envoi de rapports au format Conettix Modem4, le récepteur/la passerelle du centre de télésurveillance Conettix et le logiciel de programmation du récepteur D6200CD peuvent nécessiter une mise à jour.

Exigences du format de génération de rapports Conettix Modem4

Récepteur/Passerelle	Version CPU	Version D6200CD
Récepteur de centre de télésurveillance D6600, 32 lignes (avec carte de ligne téléphonique D6641 installée uniquement)	01.10.00	2.10

Récepteur/Passerelle	Version CPU	Version D6200CD
Récepteur du centre de télésurveillance D6100IPV6-LT. 2 lignes, IP	01.10.00	2.10

Format Conettix ANSI-SIA Contact ID

Lorsque vous configurez la centrale pour l'envoi de rapports au format Conettix ANSI-SIA Contact ID, le récepteur/la passerelle du centre de télésurveillance Conettix et le logiciel de programmation du récepteur D6200CD peuvent nécessiter une mise à jour.

Format de rapport conforme aux normes ULC-S304 et ULC-S559

Remarque!

Format de rapport conforme aux normes ULC-S304 et ULC-S559



Pour les formats conformes aux normes ULC-S304 et ULC-S559, le récepteur / la passerelle du centre de télésurveillance Conettix et le logiciel de programmation du récepteur D6200CD doivent utiliser la version dans le tableau.

Format ANSI-SIA DC-09

L'utilisation du format ANSI-SIA DC-09 nécessite un récepteur de centre de télésurveillance prenant en charge ce format de communication IP. Les récepteurs de centre de télésurveillance Conettix ne prennent actuellement pas en charge ce format.

2 Firmware version 3.14.012

Remarque : il n'y a pas de version 3.13 du firmware de la centrale. La version du firmware de la centrale est passée à la version 3.14 pour permettre la synchronisation numérique avec la version du logiciel RPS correspondante.

Nouveautés

- *Prise en charge du transmetteur cellulaire B444-A2, page 10*
- *Prise en charge du transmetteur cellulaire B444-V2, page 10*

Établissements pénitentiaires

- *Mise à jour de Force Arm Returnable (Armement forcé rétablissable), page 11*
- *Saisie des données des cartes d'accès de type 26 bits à partir du clavier, page 11*
- *Commande de déverrouillage de porte depuis une fonction SKED ou une fonction personnalisée, page 12*
- *La centrale ne rebasecule pas vers une connexion « Cloud via cellulaire » en cas de défaillance du DNS Ethernet, page 12*

-
- *Le fonctionnement cellulaire peut échouer si le DNS Ethernet n'est pas public, page 13*

Problèmes connus

- *Rapport d'ouverture de zone non envoyé lors du passage de l'état All-On (Activation totale) à l'état Part-On (Activation partielle), page 13*
- *Information technique - Notification personnelle par e-mail concernant les centrales G Series et B Series, page 14*

2.1 Nouveautés

Cette section examine les nouvelles fonctionnalités de cette version du firmware.

2.1.1 Prise en charge du transmetteur cellulaire B444-A2

Nouvelle prise en charge du module cellulaire enfichable B444-A2, AT&T LTE.

2.1.2 Prise en charge du transmetteur cellulaire B444-V2

Nouvelle prise en charge du module cellulaire enfichable B444-V2, Verizon LTE.

2.2 Établissements pénitentiaires

Cette section présente les corrections apportées à cette version du firmware.

2.2.1 Mise à jour de Force Arm Returnable (Armement forcé rétablissable)

Dans les versions précédentes du firmware, lorsque le paramètre Force Arm Returnable (Armement forcé rétablissable) était défini sur YES (oui), après désarmement du système, l'utilisateur devait rétablir manuellement les points forcés avec ce profil. À compter de la version 3.14.010 du firmware, lorsque le paramètre Force Arm Returnable (Armement forcé rétablissable) est défini sur YES (oui), tous les points forcés échouent automatiquement et repassent à l'état normal une fois que le système est désarmé.

2.2.2 Saisie des données des cartes d'accès de type 26 bits à partir du clavier

Dans les versions 3.11 et 3.12 du firmware, les données de carte d'accès saisies à partir d'un clavier n'étaient pas téléchargées correctement dans la centrale d'alarme.

2.2.3 Commande de déverrouillage de porte depuis une fonction SKED ou une fonction personnalisée

Dans la version 3.11 du firmware, la fonction de déverrouillage de porte permet à un utilisateur de déverrouiller une porte via une fonction SKED ou une fonction personnalisée, même si la zone est armée. Cette correction empêche la commande de déverrouillage de porte d'une fonction SKED ou personnalisée de fonctionner lorsqu'une zone est armée.

2.2.4 La centrale ne rebascule pas vers une connexion « Cloud via cellulaire » en cas de défaillance du DNS Ethernet

Si les paramètres Ethernet et cellulaires de connexion à distance au Cloud sont activés, la centrale ne basculera pas vers une connexion « Cloud via cellulaire » si la connexion « Cloud via Ethernet » présente une défaillance du DNS. Ce problème a été corrigé.

2.2.5 Le fonctionnement cellulaire peut échouer si le DNS Ethernet n'est pas public

Lors de la programmation d'une adresse IP de serveur DNS spécifique pour IPv4 Ethernet, celle-ci est partagée par le réseau cellulaire. Si l'adresse DNS IPv4 pour Ethernet n'est pas accessible sur le réseau public, l'interface cellulaire n'est pas en mesure de résoudre les URL.

Lors de l'utilisation de cartes Ethernet et cellulaires intégrées, un DNS IPv4 privé est requis pour Ethernet. Un paramètre DNS distinct est désormais disponible pour le plugin cellulaire.

2.3 Problèmes connus

Cette section présente les problèmes connus de cette version du firmware.

2.3.1 Rapport d'ouverture de zone non envoyé lors du passage de l'état All-On (Activation totale) à l'état Part-On (Activation partielle)

Un **rapport d'ouverture de zone** peut ne pas être envoyé si un utilisateur fait passer la zone de l'état **d'activation totale** à l'état **d'activation partielle**, puis désarme. Lorsque vous basculez de l'état **d'activation**

partielle à l'état de désarmement, les **rapports d'ouverture de zone** sont uniquement envoyés si les **rapports d'activation partielle** sont activés. Ces rapports sont désactivés par défaut. L'activation des **rapports d'activation partielle** résout ce problème.

2.3.2 Information technique - Notification personnelle par e-mail concernant les centrales G Series et B Series

Les notifications personnelles par e-mail peuvent ne plus fonctionner pour certains clients en raison des fonctionnalités de sécurité des fournisseurs de messagerie utilisant la vérification en deux étapes. Accédez à la page de sécurité du fournisseur de messagerie (Google, par exemple) pour créer un mot de passe d'application. Ce mot de passe sera utilisé dans la centrale d'alarme comme mot de passe d'authentification du serveur de messagerie pour permettre le bon fonctionnement des notifications personnelles par e-mail. Pour plus d'informations, veuillez consulter « Information technique sur les notifications personnelles concernant les centrales G Series et B Series ».

3 Firmware version 3.12.024

Nouveautés

- *Module de transmetteur cellulaire enfichable B444-A non reconnu, page 15*
- *Rapport Échec de fermeture, page 16*

Se reporter à

- *Prise en charge des informations d'identification du contrôle des accès HID 35 bits (B6512 uniquement), page 19*
- *Amélioration des communications cellulaires AT&T, page 19*

3.1 Nouveautés

Cette section examine les nouvelles fonctionnalités de cette version du firmware.

3.1.1 Module de transmetteur cellulaire enfichable B444-A non reconnu

Certains modules cellulaires B444-A peuvent être identifiés comme non valides lors de l'installation et ne seront pas reconnus par la centrale B ou G Series.

Cette version de firmware permet au dispositif hôte cellulaire de reconnaître correctement ces modules B444-A.

3.1.2 Rapport Échec de fermeture

Certains scénarios d'armement problématiques peuvent envoyer un rapport Échec de fermeture. Vous ne devez envoyer ce rapport que si la zone n'a pas été fermée en bas de la fenêtre de fermeture. Cette version du firmware résout ce problème potentiel.

4 Firmware version 3.12.020

Nouveautés

- *Prise en charge des informations d'identification du contrôle des accès HID 35 bits (B6512 uniquement), page 19*
- *Amélioration des communications cellulaires AT&T, page 19*

Corrections

- *Problème d'armement forcé avec le firmware 3.11.530, page 20*

Problèmes connus

- *Synchronisation de la sécurité des codes avec RPS et une nouvelle centrale, page 20*
- *Programmation de nouveaux types de point sur les versions de firmware antérieures à la version 3.11, page 21*
- *E-mail de notification personnelle, page 22*
- *Délai de verrouillage du clavier (blocage du clavier en cas d'échec des tentatives de code), page 22*

Se reporter à

- *Module de transmetteur cellulaire enfichable B444-A non reconnu, page 15*

-
- *Rapport Échec de fermeture, page 16*
 - *Connectivité améliorée au réseau Verizon, page 23*
 - *Types de point environnementaux, page 24*
 - *Prise en charge des certificats de centrale B Series et G Series mis à jour, page 27*
 - *Sécurité des codes configurable, page 25*
 - *Firmware de la centrale compatible FIPS, page 26*
 - *Code temporaire, page 25*
 - *Type de point Panique, page 24*
 - *Support d'entrée filaire pour la caméra IP, page 25*
 - *Corruption de l'historique pendant la mise à jour du firmware, page 24*
 - *Index des congés 2, page 23*

4.1 Nouveautés

Cette section examine les nouvelles fonctionnalités de cette version du firmware.

4.1.1 Prise en charge des informations d'identification du contrôle des accès HID 35 bits (B6512 uniquement)

La prise en charge des informations d'identification HID 35 bits permet aux clients qui utilisent le format d'entreprise Corporate 1000 d'utiliser ces cartes avec les centrales Bosch et l'interface de contrôle des accès B901. Les cartes au format 26 bits et 37 bits restent prises en charge. Notez que cette fonction n'est disponible que pour la centrale B6512.

4.1.2 Amélioration des communications cellulaires AT&T

Le fonctionnement de B444-A a fait l'objet d'améliorations et prend en compte les changements apportés au réseau cellulaire AT&T en vue de l'arrêt de la 3G.

4.2 Corrections

Cette section présente les corrections apportées à cette version du firmware.

4.2.1 Problème d'armement forcé avec le firmware 3.11.530

La version 3.12 du firmware corrige un problème concernant la fonction d'armement forcé dans nos centrales B9512G, B8512G, B6512, B5512, B4512 et B3512 pouvant provoquer le contournement de points armés de manière forcée sans aucune indication sur le clavier. Notez que ce problème n'existe qu'avec la version 3.11.530 du firmware.

4.3 Problèmes connus

Cette section présente les problèmes connus de cette version du firmware.

4.3.1 Synchronisation de la sécurité des codes avec RPS et une nouvelle centrale

Lorsque vous vous connectez à une nouvelle centrale à l'aide du firmware 3.11 et de RPS 6.11, et que vous recevez la configuration de la nouvelle centrale, l'option d'envoi/de réception suivante ouvre la fenêtre Synchronisation de la centrale car le paramètre Sécurité des codes de la centrale ne correspond pas au paramètre Sécurité des codes du logiciel RPS.

Si vous activé l'option **Voir les différences de données** dans la fenêtre Synchronisation de la centrale, vous ne verrez pas de différence concernant le paramètre Sécurité des codes dans le logiciel RPS et dans la centrale.

Recommandation

Transmettez la configuration de RPS à la centrale pour que les paramètres Sécurité des codes de la centrale et de RPS correspondent.

4.3.2 Programmation de nouveaux types de point sur les versions de firmware antérieures à la version 3.11

Lorsque vous utilisez le logiciel RPS 6.11 pour programmer un nouveau point Panique ou un nouveau point environnemental (Eau, Temp. élevée, Temp. faible) sur une centrale équipée d'un firmware d'une version antérieure à 3.11, le système ne génère aucune alarme ou condition attendue.

Dans certains cas, le type de point Temp. faible génère un défaut et dans tous les cas les types de point Panique, Eau et Temp. élevée ne génèrent aucune condition.

Recommandation

Mettez le firmware de la centrale à niveau vers la version 3.11 ou une version ultérieure si ces nouveaux types de point sont nécessaires.

4.3.3 E-mail de notification personnelle

Lorsque les notifications personnelles par e-mail sont utilisées, certaines options de configuration serveur (par exemple, la vérification en 2 étapes de Gmail ou la désactivation de l'option autorisant des applications moins sécurisées) peuvent ne pas fonctionner correctement. Afin de garantir le fonctionnement, désactivez d'autres options de serveur de messagerie.

4.3.4 Délai de verrouillage du clavier (blocage du clavier en cas d'échec des tentatives de code)

Si la valeur de la temporisation de blocage dépasse 6 553 secondes, le verrouillage du clavier risque de ne pas fonctionner correctement. Pour garantir le bon fonctionnement, réglez la temporisation de blocage à moins de 6 553 secondes.

5 Historique de révision du firmware

Cette section analyse les principales fonctionnalités des versions antérieures de ce firmware.

5.1 Firmware version 3.11.5

5.1.1 Connectivité améliorée au réseau Verizon

Le firmware version 3.11.5 améliore la gestion de l'APN Verizon lors de l'utilisation des transmetteurs cellulaires B444-V ou B444, ce qui renforce la fiabilité de la connexion.

5.1.2 Index des congés 2



Remarque!

Cela ne s'applique qu'au B6512.

L'index des congés 2 ne s'est pas exécuté tel que programmé et a été corrigé dans cette version du firmware.

5.1.3 Corruption de l'historique pendant la mise à jour du firmware

Les mises à jour du firmware de la centrale version 3.06 ou antérieure vers les versions 3.07 à 3.09 peuvent entraîner la perte d'événements consignés dans l'historique. Ce problème se produit lors de la réinitialisation ou du redémarrage de la centrale. L'historique de l'ancienne centrale doit être téléchargé avant la mise à niveau vers les versions 3.07 à 3.09. La version 3.10 résout ce problème et empêche toute corruption de l'historique.

5.2 Firmware version 3.11

5.2.1 Type de point Panique

Le type de point Panique est ajouté à la centrale, ce qui correspond à une alarme cambriolage sur 24 heures destinée à un dispositif de saisie Panique.

5.2.2 Types de point environnementaux

De nouveaux types de point sont disponibles :

- Eau - Alarme indiquant une fuite d'eau.
- Temp. élevée - Alarme indiquant une température élevée.

-
- Temp. faible - Alarme indiquant une température faible.

5.2.3 Sécurité des codes configurable

L'auto-surveillance des codes utilisateur est désormais configurable pour les claviers et les clients en mode Automatisation afin de détecter les tentatives d'authentification non valides et de réagir suite à un certain nombre de ces tentatives.

5.2.4 Code temporaire

Un code unique autorisant le désarmement peut être attribué à un utilisateur pour une ou plusieurs zones de la centrale dans le cadre d'un temporaire. Le niveau d'autorisation associé définit l'utilisateur comme un utilisateur temporaire et lui permet uniquement de désarmer le système une fois, avant expiration du code/ de l'autorisation.

5.2.5 Support d'entrée filaire pour la caméra IP

La nouvelle source de point Caméra IP comprend désormais 2 entrées filaires pour une caméra IP.

Configurez les sources de caméra IP en affectations de point RPS dans les groupes de points. Par exemple, les points 10 et 19 de la caméra IP 1, les points 20 et 29 de la caméra IP 2, les points 30 et 39 de la caméra IP 3, jusqu'au nombre de caméras disponibles sur chaque type de centrale.

5.2.6 Firmware de la centrale compatible FIPS

Le logiciel RPS a été mis à jour pour fonctionner dans un environnement Windows sécurisé, tel que le FIPS (Federal Information Processing Standard).

- Un progiciel de firmware chiffré AES/SHA supplémentaire est disponible pour les centrales B Series et G Series dans la section Téléchargements > Logiciels du catalogue de produits de détection d'intrusion Bosch. Ce firmware peut être utilisé dans toute instance de RPS 6.11 ou version ultérieure.
- Le fichier chiffré du firmware est nommé selon le type de centrale, le numéro de version du firmware portant l'extension `_SHA.fwr` pour indiquer le chiffrement SHA (*B3512_B4512_ B5512_ B6512_FW_3.11.xxx_SHA.fwr*).

5.2.7 Prise en charge des certificats de centrale B Series et G Series mis à jour

Le firmware de centrale v3.11 introduit un nouveau certificat de sécurité avant l'expiration du certificat actuel en avril 2022. Ce certificat est utilisé pour la plupart des connexions d'automatisation (intégration) et TLS RPS à la centrale. Le certificat cloud de la centrale n'est pas affecté. Toutes les connexions cloud continueront de fonctionner comme elles le font aujourd'hui.

RPS v6.11 a été mis à jour pour tenir compte automatiquement de ce nouveau certificat de sécurité de centrale.

Remarque!

Info.



Les clients qui améliorent ou installent des centrales avec le firmware v3.11 doivent mettre à niveau RPS vers la version 6.11, puis vérifier les autres applications intégrées (Bosch ou tierces) qui doivent utiliser le nouveau certificat Bosch, afin de maintenir les connexions TCP à la centrale après mars 2022.

Les clients qui utilisent RPS avec le firmware de centrale 3.10 ou une version antérieure ne sont pas concernés par l'expiration du certificat et leurs opérations se seront pas interrompues.

5.3 Firmware version 3.10

5.3.1 Sorties configurables

Les profils de sortie prennent en charge la programmation personnalisée et fournissent un moyen pour les sorties de fonctionner selon les exigences uniques des applications.

Une fois qu'un profil de sortie est créé, il peut être réutilisé et affecté à plusieurs sorties, ce qui permet une programmation rapide des sorties.

Vous pouvez créer des profils de sortie pour définir le mode de fonctionnement d'une sortie lorsque des événements spécifiques se produisent. Les profils de sortie offrent un moyen d'attribuer et d'utiliser des effets de sortie homogènes dans le système.

5.3.2 UL 985 - 6ème édition

Cette version du firmware prend désormais en charge la dernière édition de :

- UL 985 - Systèmes d'alarme incendie de maison familiale

5.4 Firmware version 3.09.050

5.4.1 Prise en charge B444-A et B444-V

Le système prend désormais en charge le module cellulaire enfichable B444-A, AT&T LTE, B444-V et Verizon LTE.

Activation de la carte SIM B444-A/B444-V

Attention!



Activez la carte SIM B444-A/B444-V avant de l'insérer. Dans le cas contraire, des erreurs de communication à la centrale/au module peuvent se produire. Dès la première mise sous tension du B444-A/B444-V, le processus d'activation peut prendre jusqu'à 15 minutes.

5.4.2 Format ANSI-SIA DC-09

Le système prend désormais en charge les formats de transmetteur réseau suivants :

- Conettix Modem4
 - Conettix ANSI-SIA Contact ID
-

– ANSI-SIA DC-09



Remarque!

APPLICATIONS HOMOLOGUÉES UL et ULC

Le format ANSI-SIA DC-09 n'est pas disponible pour les applications homologuées UL et ULC.

5.4.3 Sécurité des dispositifs connectés

Pour être en conformité avec le Security of Connected Devices Act (TITLE 1.81.26. Security of Connected Devices) et la législation associée, ce produit utilise un mot de passe de connexion unique.

Le « code RPS » de la connexion initiale à ce produit doit correspondre à l'ID de cloud unique du produit. Assurez-vous que votre opérateur RPS utilise l'ID de cloud unique qui est libellé sur le produit et qui figure sur la carte dans la zone du produit.

5.4.4 Fonctionnement du type de réponse de sortie

Dans le firmware de centrale v3.09.024, les sélections de configuration 1 et 2 de l'opération de type de réponse de sortie ne fonctionnaient pas correctement. Cela a été corrigé dans le firmware de centrale v3.09.050.

Si vous avez apporté des modifications dans le firmware de centrale v3.09.024 pour assurer le bon fonctionnement, ces changements ne sont plus nécessaires.

- ▶ Dans le fonctionnement du type de réponse de sortie, les sélections de configuration 1 et 2 retrouvent leur configuration prévue, et documentée.

5.5 Firmware version 3.08

5.5.1 Prise en charge des langues

Ajoute la prise en charge du néerlandais, de l'allemand et du suédois.

Lorsque la première langue de la centrale et la seconde langue sont définies sur le néerlandais, l'anglais, le français, l'allemand, le hongrois, l'italien, le portugais, l'espagnol ou le suédois, le système utilise le jeu de caractères standard Latin-1.

Lorsque la première langue de la centrale ou la seconde langue est définie sur le chinois, le grec ou le polonais, le système utilise étendu le jeu de caractères étendu UTF-8 Unicode.

Remarque!

Seuls les claviers B915/B915i et B942 prennent en charge le jeu de caractères étendu UTF-8



Seuls les claviers B915/B915i avec le firmware version 1.01.010 ou ultérieure et les claviers B942 avec le firmware version 1.02.022 ou ultérieure prennent en charge le jeu de caractères étendu UTF-8

5.5.2 Durée de shuntage de la porte

La sélection la plus longue possible pour la durée de shuntage de la porte est comprise entre 240 secondes et 8 heures.

Cette option est disponible avec les versions de firmware suivantes :

- Firmware de centrale version 3.08 ou ultérieure
- Firmware de Remote Programming Software version 6.08 ou ultérieure
- Firmware B901 version 1.05 ou ultérieure

5.5.3 Dispositifs de destination de sauvegarde

La centrale peut envoyer des rapports à quatre groupes de destinataire différents en utilisant un groupe principal et jusqu'à trois dispositifs de destination de sauvegarde pour chaque groupe de destinataire.

5.5.4 Rapport de test personnalisé

Vous pouvez envoyer un rapport de test normal ou un rapport de test personnalisé :

- Rapport de test normal : inclut tous les groupes de destinataires pour lesquels la fonction de rapport de test est activée, indépendamment du dispositif de destination utilisé pour communiquer. Le rapport de test est envoyé au premier dispositif de destination réussi dans un groupe de destinataires.
- Rapport de test personnalisé : vous pouvez sélectionner le groupe de destinataires et le dispositif de destination que vous souhaitez tester. Vous pouvez tester un dispositif de destination par groupe de destinataires ou tous les dispositifs de destination configurés pour un groupe de destinataires.

6 Logiciels libres 3.14.012

Bosch inclut les modules logiciels libres listés ci-dessous dans le firmware de cette centrale. L'inclusion de ces modules ne limite pas la garantie Bosch.

Digital Equipment Corporation

Portions Copyright (c) 1993 by Digital Equipment Corporation.

Permission to use, copy, modify, and distribute this software for any purpose with or without fee is hereby granted, provided that the above copyright notice and this permission notice appear in all copies, and that the name of Digital Equipment Corporation not be used in advertising or publicity pertaining to distribution of the document or software without specific, written prior permission.

THE SOFTWARE IS PROVIDED "AS IS" AND DIGITAL EQUIPMENT CORP. DISCLAIMS ALL WARRANTIES WITH REGARD TO THIS SOFTWARE, INCLUDING ALL IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS. IN NO EVENT SHALL DIGITAL EQUIPMENT CORPORATION BE LIABLE FOR ANY SPECIAL, DIRECT, INDIRECT, OR CONSEQUENTIAL DAMAGES OR ANY DAMAGES WHATSOEVER RESULTING FROM LOSS OF USE, DATA

OR PROFITS, WHETHER IN AN ACTION OF CONTRACT, NEGLIGENCE OR OTHER TORTIOUS ACTION, ARISING OUT OF OR IN CONNECTION WITH THE USE OR PERFORMANCE OF THIS SOFTWARE.

Digital historical

Copyright 1987 by Digital Equipment Corporation, Maynard, Massachusetts, and the Massachusetts Institute of Technology, Cambridge, Massachusetts.

All Rights Reserved

Permission to use, copy, modify, and distribute this software and its documentation for any purpose and without fee is hereby granted, provided that the above copyright notice appear in all copies and that both that copyright notice and this permission notice appear in supporting documentation, and that the names of Digital or MIT not be used in advertising or publicity pertaining to distribution of the software without specific, written prior permission.

DIGITAL DISCLAIMS ALL WARRANTIES WITH REGARD TO THIS SOFTWARE, INCLUDING ALL IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS, IN NO EVENT SHALL DIGITAL BE LIABLE FOR ANY SPECIAL, INDIRECT OR CONSEQUENTIAL DAMAGES OR ANY DAMAGES WHATSOEVER RESULTING FROM

LOSS OF USE, DATA OR PROFITS, WHETHER IN AN ACTION OF CONTRACT, NEGLIGENCE OR OTHER TORTIOUS ACTION, ARISING OUT OF OR IN CONNECTION WITH THE USE OR PERFORMANCE OF THIS SOFTWARE.

OpenSSL License

Copyright (c) 1998-2008 The OpenSSL Project. All rights reserved.

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

1. Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.
2. Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.
3. All advertising materials mentioning features or use of this software must display the following acknowledgment:

"This product includes software developed by the OpenSSL Project for use in the OpenSSL Toolkit.
(<http://www.openssl.org/>)"

4. The names "OpenSSL Toolkit" and "OpenSSL Project" must not be used to endorse or promote products derived from this software without prior written permission. For written permission, please contact openssl-core@openssl.org.

5. Products derived from this software may not be called "OpenSSL" nor may "OpenSSL" appear in their names without prior written permission of the OpenSSL Project.

6. Redistributions of any form whatsoever must retain the following acknowledgment:

"This product includes software developed by the OpenSSL Project for use in the OpenSSL Toolkit
(<http://www.openssl.org/>)"

THIS SOFTWARE IS PROVIDED BY THE OpenSSL PROJECT "AS IS" AND ANY EXPRESSED OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE OpenSSL PROJECT OR ITS CONTRIBUTORS BE LIABLE FOR ANY

DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

This product includes cryptographic software written by Eric Young (eay@cryptsoft.com). This product includes software written by Tim Hudson (tjh@cryptsoft.com). Pour plus d'informations, reportez-vous à la licence OpenSSL sur le site www.boschsecurity.com, sous Catalogue de produits.

Regents of the University of California

Copyright (c) 1985, 1993

The Regents of the University of California. All rights reserved.

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

1. Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.
2. Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.
3. All advertising materials mentioning features or use of this software must display the following acknowledgement: This product includes software developed by the University of California, Berkeley and its contributors.
4. Neither the name of the University nor the names of its contributors may be used to endorse or promote products derived from this software without specific prior written permission.

THIS SOFTWARE IS PROVIDED BY THE REGENTS AND CONTRIBUTORS ``AS IS" AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE REGENTS OR CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR

CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

RSA data security

Copyright © 1991-2, RSA Data Security, Inc. Created 1991. All rights reserved.

The "RSA Data Security, Inc. MD5 Message-Digest Algorithm" is included in the control panel firmware. RSA Data Security, Inc. makes no representations concerning either the merchantability of this software or the suitability of this software for any particular purpose. It is provided "as is" without express or implied warranty of any kind.

Time routines

Copyright © 2002 Michael Ringgaard. All rights reserved.

This software [Time routines] is provided by the copyright holders and contributors "as is" and any express or implied warranties, including, but not limited to, the implied warranties of merchantability and fitness for a particular purpose are disclaimed. In no event shall the copyright owner or contributors be liable for any direct, indirect, incidental, special, exemplary, or consequential damages (including, but not limited to, procurement of substitute goods or services; loss of use, data, or profits; or business interruption) however caused and on any theory of liability, whether in contract, strict liability, or tort (including negligence or otherwise) arising in any way out of the use of this software, even if advised of the possibility of such damage.

Bosch Security Systems B.V.

Torenallee 49

5617 BA Eindhoven

Pays-Bas

www.boschsecurity.fr

© Bosch Security Systems B.V., 2023

Building solutions for a better life.

202304141014