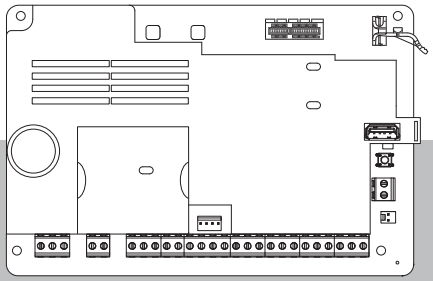
radionix

Centrales

B Series: B6512, B5512, B4512, B3512



fr Notes de version

Table des matières

1	**Introduction**	**5**
1.1	À propos de la documentation	5
1.2	Configuration requise	6
2	**Firmware version 3.15.116**	**10**
2.1	Nouveautés	10
2.2	Corrections	11
3	**Firmware version 3.15.110**	**12**
3.1	Nouveautés	12
3.2	Corrections	12
4	**Firmware version 3.15.024**	**14**
4.1	Nouveautés	14
4.2	Corrections	16
5	**Historique de révision du firmware**	**20**
5.1	Firmware version 3.14.100	20
5.2	Firmware version 3.14.012	20
5.3	Firmware version 3.12.024	25
5.4	Firmware version 3.12.020	26
5.5	Firmware version 3.11.5	30

6 Programmation de la centrale pour la conformité SIA 32

7 Configuration système minimale requise pour ANSI/SIA CP-01 39

8 Logiciels libres 3.15.116 40

1 Introduction

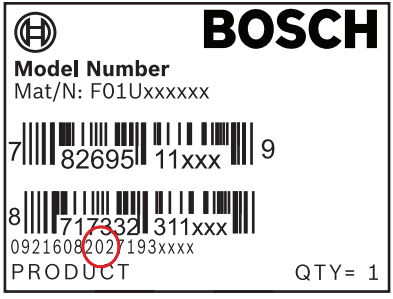
Ces *release notes* concernent la version 3.15.116 du firmware de la centrale.

1.1 À propos de la documentation

Copyright
Ce document est la propriété de Radionix et 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 Radionix
Pour connaître les dates de fabrication des produits, allez à https://www.keenfinity-group.com/xc/en/datecodes/ et reportez-vous au numéro de série situé sur l'étiquette du produit.
L'image suivante présente un exemple d'étiquette de produit et indique où trouver la date de fabrication dans le numéro de série.



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 6.15 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 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 3.15.116

Établissements pénitentiaires

- *Correction d'une erreur avec un message verrouillé « Route Group Comm Fail » non effacé après une récupération de communication, page 11*
- *Correction d'une fuite de mémoire sur le panneau, page 11*
- *Correction de l'envoi de texte en mode UTF-8, page 11*

2.1 Nouveautés

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

Cette version du firmware ne contient que des correctifs.

2.2 Corrections

2.2.1 Correction d’une erreur avec un message verrouillé « Route Group Comm Fail » non effacé après une récupération de communication

2.2.2 Correction d’une fuite de mémoire sur le panneau

2.2.3 Correction de l’envoi de texte en mode UTF-8

3 Firmware version 3.15.110

3.1 Nouveautés

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

3.1.1 Valeur par défaut de l'activation UPnP remplacée par Désactiver

La valeur par défaut a été modifiée en Désactiver UPnP pour fournir un environnement plus sécurisé et éviter les attaques par déni de service. Pour plus de protection, Keenfinity recommande de désactiver UPnP dans vos périphériques existants et de supprimer de votre routeur toutes les règles de redirection de port relatives aux produits de communication Bosch.

3.2 Corrections

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

3.2.1 Suppression du chiffrement 3DES de TLS 1.2

En raison de risques de sécurité potentiels, le chiffrement 3DES a été supprimé de TLS 1.2.

3.2.2 La centrale identifiera et mettra à jour correctement le B812

La centrale a été mise à jour pour prendre en charge la reconnaissance du B812, permettant le fonctionnement, les mises à jour du firmware et les diagnostics RPS.

3.2.3 La centrale identifie correctement le B532 dans les diagnostics RPS

La centrale a été mise à jour pour prendre en charge la reconnaissance correcte du B532 pour les diagnostics RPS.

4 Firmware version 3.15.024

Nouveautés

- *Certification UL 2610 2e édition*, *page 14*
- *Sécurité renforcée*, *page 14*
- *Compatibilité avec l'alimentation auxiliaire B532 et l'extenseur SDI2* , *page 16*
- *Prise en charge du mode 2*, *page 16*

4.1 Nouveautés

4.1.1 Certification UL 2610 2e édition

Systèmes et unités d'alarme de sécurité dans des locaux commerciaux

4.1.2 Sécurité renforcée

- Configuration de la version 1.2 minimale de TLS prise en charge ;

Avertissement!



Cette version du firmware de la centrale impose l'utilisation de TLS 1.2. Le paramètre TLS ne peut être défini sur TLS 1.0 ou 1.1 qu'à l'aide de RPS version 6.15 et ultérieure. Si vous disposez d'outils qui nécessitent les versions TLS 1.0 ou 1.1, NE METTEZ PAS à jour le firmware de la centrale tant que vous n'avez pas RPS version 6.15 et ultérieure.

Remarque : Lorsqu'un B426 ou un B450 est également utilisé dans le système, ces modules doivent également mettre à jour leur firmware vers la version 3.15 pour appliquer les paramètres TLS.

- Désactivation des chiffrements TLS non compatibles FIPS ;
- Mise à jour des bibliothèques TLS et de la pile réseau ;
- Vérifié au NIST CAVP (cert # A5272) ;
- Verrouillage temporaire programmable après cinq échecs consécutifs du mot de passe d'accès à distance.

4.1.3 Compatibilité avec l'alimentation auxiliaire B532 et l'extenseur SDI2

4.1.4 Prise en charge du mode 2

Prise en charge supplémentaire du mode 2 pour :

- Gestion des utilisateurs ;
- Configuration du niveau d'autorité ;
- Index des congés ;
- Périodes d'ouverture/de fermeture.

4.2 Corrections

4.2.1 Correction du POPIT manquant qui s'est produit lors d'une mise à jour de programmation

Réponse au bulletin technique du 30 août 2024.

4.2.2 Correction d'un défaut où le téléphone ne pouvait pas être restauré après un défaut de communication téléphonique

4.2.3 Correction de l'erreur « Données hors plage » lors de l'ajout d'un nouvel utilisateur avec BSM

4.2.4 Amélioration de la gestion des utilisateurs configurés en mode 2

4.2.5 Suppression de la double consignation de l'événement « Accès à distance non valide » lorsque Ethernet est déconnecté pendant une connexion RPS ou Cloud

4.2.6 Les rapports SDI2 pour les défauts de câble ouvert avec le modem 4 sont maintenant envoyés

4.2.7 Des rapports de surintensité d'alimentation sont maintenant envoyés pour chaque sortie

4.2.8 L'événement Défaut secteur suit désormais le paramètre de renvoi de défaillance secteur

4.2.9 Mises à jour améliorées de l'état de la batterie pour l'alimentation B520/B532

4.2.10 La configuration de sortie du clavier s'arrête maintenant si elle est retirée de la configuration de la centrale

4.2.11 Le mode 2 Armer les partitions de la centrale n'est plus un armement forcé, sauf indication contraire

4.2.12 Correction d'une erreur de paramètre de service pouvant se produire lors du contournement de points à partir d'un clavier

4.2.13 Le défaut B901 peut maintenant être résolu

4.2.14 L'événement de changement du nom d'utilisateur est maintenant consigné dans le journal des événements de la centrale

4.2.15 Correction d'un défaut avec l'état du point PIE Mode 2 qui n'était pas toujours mis à jour correctement

4.2.16 Le verrouillage de porte automatique est désormais transmis au récepteur

4.2.17 Gestion mise à jour des certificats TLS expirés

4.2.18 Correction du défaut d'envoi d'e-mails à un serveur via IPv6

4.2.19 Mises à jour des niveaux de transmission du modem B430

4.2.20 Lorsqu'un utilisateur change un code à partir du menu d'installation du clavier, cela ne génère plus de réponse de changement de point

4.2.21 Mises à jour du texte B915 et B920 lorsque plusieurs alarmes sont présentes

4.2.22 Correction d'un défaut où une alarme silencieuse pouvait devenir audible avant les deux échecs configurés pour envoyer l'événement

5 Historique de révision du firmware

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

5.1 Firmware version 3.14.100

5.1.1 Prise en charge des informations d'identification du contrôle des accès HID 32 bits (B6512 uniquement)

La prise en charge des informations d'identification MIFARE Classic 32 bits permet aux clients qui utilisent les cartes d'accès au format MIFARE Classic d'utiliser ces cartes avec la centrale B6512 et l'interface de contrôle d'accès B901.
Il s'agit d'un ajout aux formats 26 bits, 35 bits et 37 bits déjà prises en charge.

5.2 Firmware version 3.14.012

5.2.1 Prise en charge du transmetteur cellulaire B444-A2

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

5.2.2 Prise en charge du transmetteur cellulaire B444-V2

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

5.2.3 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.

5.2.4 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.

5.2.5 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.

5.2.6 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.

5.2.7 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.

5.2.8 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.

5.2.9 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 ».

5.3 Firmware version 3.12.024

5.3.1 Nouveautés

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

5.3.1.1 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.

5.3.1.2 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.

5.4 Firmware version 3.12.020

5.4.1 Nouveautés

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

5.4.1.1 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.

5.4.1.2 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.

5.4.2 Corrections

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

5.4.2.1 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.

5.4.3 Problèmes connus

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

5.4.3.1 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.

5.4.3.2 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.

5.4.3.3 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.

5.4.3.4 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.

5.5 Firmware version 3.11.5

5.5.1 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.

5.5.2 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.

5.5.3 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.

6 Programmation de la centrale pour la conformité SIA

Nom du paramètre	Paramètres de centrale requis pour la conformité SIA	Valeur par défaut
Num télé.	(Préfixer le numéro de téléphone de secours avec la commande Appel en instance[1] désactivée)	{Blank}
Type de contrainte	Option 3[2]	0 (Désactivé)
Rapports d'annulation	Oui	Oui
Durée de la temporisation de sortie	45 à 255 secondes	60 secondes
Contrainte activée	Oui	Non

Redémarrage de la temporisation de sortie	Oui ou Non	Oui
Activation totale - Aucune sortie	Oui ou Non	Oui
Règle de présence de deux personnes ?	Non	Non
Contrainte en avance ?	Non	Non
Avertissement de temporisation de sortie	Oui	Oui

Tonalité d'entrée	Oui	Oui
Tonalité de sortie	Oui ou Non	Oui
Abandonner l'affichage	Oui ou Non	Oui
Annuler l'affichage	Oui ou Non	Oui
Vérifier l'heure	10 à 60 secondes	60 secondes
Fonction de saisie du code	Armer/Désarmer	Armer/ Désarmer
Activation totale instantanée	- (Désactivé)	- (Désactivé)

Armement partiel instantané	- (Désactivé)	- (Désactivé)
Envoyer la contrainte	- (Désactivé) ou E (Activé)	E (Désactivé)
Désarmer	- (Désactivé) ou E (Activé)	E (Désactivé)
Désarmement du code	- (Désactivé) ou E (Activé)	E (Désactivé)
Temporisation d'entrée	30 à 240 secondes	30 secondes
Abandon de l'alarme	Oui ou Non	Oui
Période d'interruption	15 à 45 secondes	30 secondes
Longueur du code	3 à 6 chiffres	désactivé

Nombres d'inhibitions automatiques	1 à 2 trajets[3]	2 trajets
Avertissement à distance	Oui	Oui
Minuterie de points de croisement	5 à 255 secondes	20 secondes
Point de croisement	Oui ou Non[4]	Non
Test de la détection (tous les points intrusion sauf incendie)	E (Désactivé)	E (Désactivé)

Test de détection de tous les points incendie	E (Désactivé)	E (Désactivé)
Réponse de temporisation, désarmée	00:00	00:00
Réponse temporisation, armé	00:00	00:00

[1]Appel en instance ne s'applique pas aux réseaux cellulaires ni aux communications PSDN (Public Switched Data Network). Une commande de désactivation de l'appel en instance sur une ligne sans appel en instance empêchera la connexion centre de télésurveillance.
[2]L14 est le niveau d'autorité sous contrainte par défaut.
[3]Le nombre d'inhibitions automatiques est programmable jusqu'à 4 trajets. Pour la conformité SIA, réglez sur 1 ou 2.

[4]Les points de croisement doivent se chevaucher (protéger la même zone) afin qu'un seul point puisse protéger la zone individuellement.

7 Configuration système minimale requise pour ANSI/SIA CP-01

Configuration système minimale requise pour la classification conforme à ANSI/SIA CP-01 :

- Unité de commande homologuée UL B6512, B5512, B4512 ou B3512
- Modèle de clavier homologué et classé UL B942/B942W, B930, B921C/B921CW, B920 ou B915/B915I
- Sonnerie locale homologuée UL
- Moyens de transmission hors site

8 Logiciels libres 3.15.116

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

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.

Radionix B.V.
Achtseweg Zuid 173
5651 GW Eindhoven
The Netherlands
www.radionix.com
© Radionix 2026

Radionix LLC
130 Perinton Pkwy.
Fairport, NY 14450
USA
www.radionix.com
© Radionix 2026

202611021246