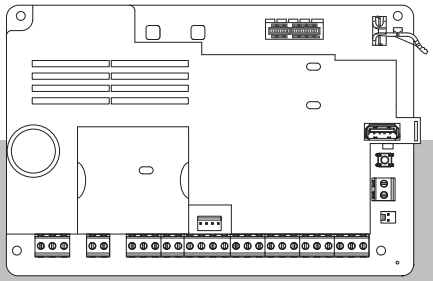
radionix

Painéis de controle

B Series: B6512, B5512, B4512, B3512



pt-BR Notas de lançamento

Sumário

1	**Introdução**	**5**
1.1	Sobre a documentação	5
1.2	Requisitos	6
2	**Firmware versão 3.15.116**	**10**
2.1	Novidades	10
2.2	Correções	10
3	**Firmware versão 3.15.110**	**11**
3.1	Novidades	11
3.2	Correções	11
4	**Firmware versão 3.15.024**	**13**
4.1	Novidades	13
4.2	Correções	15
5	**Histórico de revisão do firmware**	**19**
5.1	Firmware versão 3.14.100	19
5.2	Firmware versão 3.14.012	19
5.3	Firmware versão 3.12.024	23
5.4	Firmware versão 3.12.020	24
5.5	Firmware versão 3.11.5	28

6 Programando o painel de controle para conformidade com a SIA 30

7 Requisitos mínimos do sistema para ANSI/SIA CP-01 36

8 Software de código aberto 3.15.116 37

1 Introdução

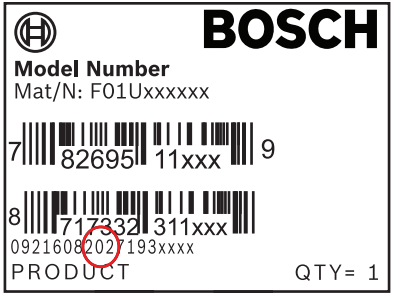
Estas *Notas de lançamento* correspondem à versão 3.15.116 do firmware do painel de controle.

1.1 Sobre a documentação

Copyright
Este documento é propriedade intelectual da Radionix e está protegido por direitos autorais. Todos os direitos reservados.

Marcas registradas
Todos os nomes de produtos de hardware e software usados neste documento provavelmente são marcas registradas e devem ser tratados de acordo.

Datas de fabricação dos produtos Radionix
Para as datas de fabricação do produto, acesse https://www.keenfinity-group.com/xc/en/datecodes/ e consulte o número de série localizado no rótulo do produto.
A imagem a seguir mostra um exemplo de uma etiqueta de produto e destaca onde encontrar a data de fabricação no número de série.



1.2 Requisitos

Esta seção mostra os requisitos para que o RPS (Remote Programming Software) e o Receptor/Gateways Conettix sejam compatíveis com esta versão do firmware do painel de controle.

1.2.1 Software de Programação Remota (RPS)

Para usar todos os novos recursos desta versão do firmware, você deve usar o RPS versão 6.15 ou posterior.

1.2.2 Receptor/Gateway Conettix

Formato Conettix Modem4

Ao configurar o painel de controle para enviar relatórios no formato Conettix Modem4, o software de programação do gateway/receptor da estação central Conettix e do D6200CD Receptor pode necessitar de uma atualização.

Requisitos do formato de relatório Conettix Modem4

Receptor/Gateway	Versão da CPU	Versão do D6200CD
D6600 Receptor da estação central, 32 linhas (somente com D6641 Placa da linha telefônica instalada)	01.10.00	2.10
D6100IPV6-LT Receptor da estação central, 2 linhas, IP	01.10.00	2.10

Formato Conettix ANSI-SIA Contact ID

Ao configurar o painel de controle para enviar relatórios no formato Contact ID Conettix ANSI-SIA, o software de programação do gateway/receptor da estação central Conettix e do D6200CD Receptor pode necessitar de uma atualização.

Formato de relatório em conformidade com ULC-S304 e ULC-S559

Aviso!

Formato de relatório em conformidade com ULC-S304 e ULC-S559

Para formatos de relatórios em conformidade com ULC-S304 e ULC-S559, o software de programação do gateway/receptor da estação central Conettix e do D6200CD Receptor precisa usar a versão da tabela.

Formato ANSI-SIA DC-09

O uso do formato ANSI-SIA DC-09 requer um receptor de estação central que seja compatível com este formato de comunicador IP. Atualmente, os receptores de estação central Conettix da Bosch não são compatíveis com esse formato.

2 Firmware versão 3.15.116

Correções

- *Corrigido erro com uma mensagem "Falha de Comunicação do Grupo de Roteamento" travada que não apagou após a recuperação da comunicação, página 10*
- *Corrigido vazamento de memória no painel, página 10*
- *Corrigido envio de texto no modo UTF-8, página 10*

2.1 Novidades

Esta seção examina os novos recursos desta versão do firmware.
Esta versão do firmware contém apenas correções.

2.2 Correções

2.2.1 Corrigido erro com uma mensagem "Falha de Comunicação do Grupo de Roteamento" travada que não apagou após a recuperação da comunicação

2.2.2 Corrigido vazamento de memória no painel

2.2.3 Corrigido envio de texto no modo UTF-8

3 Firmware versão 3.15.110

3.1 Novidades

Esta seção examina os novos recursos desta versão do firmware.

3.1.1 Habilitar UPnP padrão alterado para Desabilitar

O padrão de fábrica foi alterado para Desabilitar UPnP, a fim de proporcionar um ambiente mais seguro e evitar ataques de Negação de serviço. Para proteção adicional, a Keenfinity recomenda desativar o UPnP nos seus dispositivos existentes e remover todas as regras de encaminhamento de portas relacionadas a produtos de comunicação Bosch do seu roteador.

3.2 Correções

Esta seção examina as correções feitas nesta versão do firmware.

3.2.1 Removida a cifra 3DES do TLS 1.2

Devido a potenciais riscos de segurança, a cifra 3DES foi removida do TLS 1.2.

3.2.2 O painel identificará e atualizará corretamente o B812

O painel de controle foi atualizado para suportar o reconhecimento do B812, permitindo operação, atualizações de firmware e diagnósticos RPS.

3.2.3 O painel identificará corretamente o B532 no diagnóstico do RPS

O painel de controle foi atualizado para suportar o reconhecimento correto do B532 para diagnósticos RPS.

4 Firmware versão 3.15.024

Novidades

– *Certificação UL 2610 2.ª Edição, página 13*
– *Segurança aprimorada, página 13*
– *Compatibilidade com fonte de alimentação auxiliar B532 e extensor SDI2 , página 15*
– *Suporte ao Modo 2, página 15*

4.1 Novidades

4.1.1 Certificação UL 2610 2.ª Edição

Unidades e Sistemas de Alarme de Segurança para Instalações Comerciais

4.1.2 Segurança aprimorada

– Configuração do TLS mínimo suportado versão 1.2;

Advertência!

Esta versão do firmware do painel aplicará o TLS 1.2. A configuração do TLS só pode ser definida como TLS 1.0 ou 1.1 usando o RPS versão 6.15 e superior. Se você dispor de ferramentas que exijam versões 1.0 ou 1.1 do TLS, NÃO atualize o firmware do painel até que você tenha o RPS 6.15 ou superior.



Observação: quando um B426 ou B450 também está em uso no sistema, esses módulos também devem atualizar seu firmware para a versão 3.15 para aplicar as configurações do TLS.

- Desativação de codificações TLS não conformes com FIPS;
- Bibliotecas TLS e pilha de protocolos atualizadas;
- Verificado para NIST CAVP (cert # A5272);
- Bloqueio programável temporário após cinco falhas consecutivas de senha de acesso remoto.

4.1.3 Compatibilidade com fonte de alimentação auxiliar B532 e extensor SDI2

4.1.4 Suporte ao Modo 2

Suporte adicional ao modo 2 para:

- Gerenciamento de usuários;
- Configuração de nível de autoridade;
- Índices de feriados;
- Abrir/fechar janelas.

4.2 Correções

4.2.1 Corrigido o POPIT ausente que ocorria durante uma atualização de programação

Trata do Boletim Técnico datado de 30 de agosto de 2024.

4.2.2 Corrigido o problema em que o telefone não podia ser restaurado após um problema de comunicação telefônica

4.2.3 Corrigido o erro "Dados fora do intervalo" ao adicionar um novo usuário com BSM

4.2.4 Melhorado o tratamento do Modo 2 de "usuários configurados"

4.2.5 Removido o registro duplo do evento "Acesso remoto inválido" quando a Ethernet é desconectada durante um RPS ou conexão de nuvem

4.2.6 Agora estão sendo enviados relatórios SDI2 para falhas de fio aberto com o Modem 4

4.2.7 Agora estão sendo enviados relatórios de "sobrecorrente" da fonte de alimentação para cada saída

4.2.8 O evento de falha CA da fonte de alimentação agora segue a configuração de falha de CA de reenvio

4.2.9 Atualizações aprimoradas do status da bateria para a fonte de alimentação B520/B532

4.2.10 Agora, o padrão de saída do teclado para se for removido da configuração do painel

4.2.11 As áreas do painel de armação do Modo 2 deixaram de ser de armação forçada, a menos que seja instruído a fazê-lo

4.2.12 Corrigida a falha de "Parâmetro de serviço" que pode ocorrer ao desabilitar pontos de um teclado

4.2.13 Já é possível eliminar o problema do B901

4.2.14 O evento de alteração do nome do usuário passou a estar registrado no log de eventos do painel

4.2.15 Corrigido o problema com o estado do ponto PIE do modo 2 que nem sempre atualizava corretamente

4.2.16 A porta automática bloqueada passou a ser enviada para o receptor

4.2.17 Tratamento atualizado de certificados TLS expirados

4.2.18 Corrigido o problema ao enviar e-mails para um servidor usando IPv6

4.2.19 Atualizações nos níveis de transmissão do modem B430

4.2.20 Quando um usuário altera uma senha no menu do instalador do teclado, ele não gera mais uma resposta de alteração de ponto

4.2.21 Atualizações para o texto B915 e B920 em caso de vários alarmes

4.2.22 Corrigido o problema em que o alarme silencioso pode se tornar audível antes das duas falhas configuradas para enviar o evento

5 Histórico de revisão do firmware

Esta seção examina os recursos importantes de revisões anteriores do firmware.

5.1 Firmware versão 3.14.100

5.1.1 Suporte para credenciais de controle de acesso HID de 32 bits — somente B6512

O suporte à credencial MIFARE Classic de 32 bits permite que os clientes que usam os cartões de acesso no formato MIFARE Classic usem esses cartões com as interfaces de controle de acesso B901 e B6512.
É um acréscimo aos formatos de 26 bits, 35 bits e 37 bits suportados anteriormente.

5.2 Firmware versão 3.14.012

5.2.1 Suporte a celular comunicador conectável B444-A2

Novo suporte de módulo celular para o módulo de celular conectável B444-A2, AT&T LTE.

5.2.2 Suporte a celular comunicador conectável B444-V2

Novo suporte de módulo celular para o módulo de celular conectável B444-V2, Verizon LTE.

5.2.3 Forçar arme retornável atualizado

Nas versões anteriores do firmware, quando o parâmetro Forçar arme retornável de um perfil de ponto era definido como SIM, depois de desarmar o sistema, o usuário tinha que reabilitar manualmente quaisquer pontos forçados com esse perfil. Com a versão de firmware 3.14.010, quando o parâmetro Forçar arme retornável for definido como YES (SIM), todos os pontos forçados serão automaticamente reabilitados e retornarão ao normal, uma vez que o sistema esteja desarmado.

5.2.4 Digitando dados de acesso do tipo de cartão de 26 bits do teclado

No firmware versão 3.11 e 3.12, os dados do cartão de acesso inseridos por um teclado não foram carregados no painel de controle com precisão.

5.2.5 Comando de desbloqueio de porta de uma função SKED ou personalizada

No firmware versão 3.11, o recurso de desbloqueio de porta permitiu que um usuário desbloqueasse uma porta por meio de uma SKED ou função personalizada, mesmo que a área estivesse armada. Essa correção impede o comando de desbloqueio de porta de uma função SKED ou personalizada durante um estado armado.

5.2.6 O painel não retornará à conexão "nuvem sobre celular" se ocorrer falha de DNS Ethernet

Se os parâmetros Ethernet e celular do Cloud Remote Connect estiverem ativados, o painel não mudará para “nuvem sobre celular” se a conexão “nuvem sobre Ethernet” tiver uma falha de DNS. Esse problema foi corrigido.

5.2.7 A operação celular pode falhar se o DNS Ethernet não for público

Ao programar um endereço IP de servidor DNS específico para Ethernet IPv4, o endereço será compartilhado por celular. Se o endereço DNS IPv4 para Ethernet não estiver acessível na rede pública, a interface do celular não poderá resolver URLs.

Ao usar Ethernet integrada e celular, um DNS IPv4 privado é necessário para usar Ethernet. Uma configuração de DNS separada para o plugin celular já está disponível.

5.2.8 Relatório de abertura de área não enviado ao alternar do estado All-On para Part-On

Um **Relatório de área aberta** pode não ser enviado se um usuário alterar a área de **All-On**, depois para **Part-On** e, em seguida, desarmar. Ao alternar de **Part-On para desarmar**, os **Relatórios de abertura de área** são enviados apenas se os **Relatórios de Part-On** estiverem ativados. Esses relatórios são desativados por padrão. A ativação dos **Relatórios de Part-On** resolve esse problema.

5.2.9 Boletim Técnico - E-mail de notificação pessoal de G Series e B Series

As mensagens de e-mail de notificação pessoal podem parar de funcionar para alguns clientes devido aos recursos de segurança do provedor de e-mail que usam a verificação em duas etapas. Use a página de segurança do provedor de e-mail (Google, por exemplo) para criar uma senha de aplicativo. Essa senha será usada no painel de controle, como a senha de autenticação do servidor de e-mail, para

permitir que os e-mails de notificação pessoal funcionem. Consulte o “Boletim Técnico - E-mail de notificação pessoal de G Series e B Series” para obter mais informações.

5.3 Firmware versão 3.12.024

5.3.1 Novidades

Esta seção examina os novos recursos desta versão do firmware.

5.3.1.1 O módulo do comunicador celular conectável B444-A não é reconhecido

Alguns módulos celulares B444-A podem reportar como "inválidos" durante a instalação e não serão reconhecidos pelo painel de controle da B Series ou G Series. Esta versão de firmware permite que o dispositivo host celular reconheça corretamente esses módulos B444-A.

5.3.1.2 Relatório de falha ao fechar

Alguns cenários problemáticos de armação podem enviar um relatório de falha ao fechar. Este relatório só deve ser enviado se a área não estiver fechada no final da janela de fechamento. Esta versão de firmware resolve esse problema potencial.

5.4 Firmware versão 3.12.020

5.4.1 Novidades

Esta seção examina os novos recursos desta versão do firmware.

5.4.1.1 Suporte para credenciais de controle de acesso HID de 35 bits (somente B6512)

O suporte de credenciais HID de 35 bits permite que os clientes que usam o formato Corporate 1000 usem esses cartões com painéis da Bosch e a interface de controle de acesso B901. Isso se soma aos cartões de formato de 26 bits e 37 bits que já eram compatíveis. Observe que este recurso está disponível somente para o painel de controle B6512.

5.4.1.2 Melhores comunicações celulares da AT&T

Melhorias foram adicionadas para melhorar a operação B444-A e acomodar mudanças na rede celular da AT&T associada ao futuro 3G sunset.

5.4.2 Correções

Esta seção examina as correções feitas nesta versão do firmware.

5.4.2.1 Problema de armação forçada com a versão 3.11.530 do firmware

A versão de firmware 3.12 corrige um problema em relação ao recurso de armação forçada em nossos painéis de controle B9512G, B8512G, B6512, B5512, B4512 e B3512, que podia fazer com que os pontos que tivessem sido armados à força permanecessem ignorados sem nenhuma indicação no teclado. Observe que esse problema existe apenas na versão 3.11.530 do firmware.

5.4.3 Problemas conhecidos

Esta seção examina os problemas conhecidos desta versão do firmware.

5.4.3.1 Sincronização da segurança por senha com RPS e novo painel

Ao conectar a um novo painel de controle com firmware v3.11 usando o RPS v6.11 e receber a configuração do novo painel, a próxima opção de envio/recebimento abrirá a janela

“Sincronização de painéis” porque o parâmetro “Segurança por senha” no painel de controle não corresponde à configuração do parâmetro “Segurança por senha” no RPS. Clicar na opção **Ver diferenças de dados** na janela “Sincronização de painéis” não mostra diferença entre o parâmetro “Segurança por senha” no RPS e no painel de controle.

Recomendação

Envie a configuração do RPS para o painel a fim de corresponder os parâmetros “Segurança por senha” no RPS e no painel.

5.4.3.2 Programação de novos tipos de ponto em versões de firmware anteriores à v3.11

Ao usar o RPS 6.11 para programar um novo ponto de pânico ou ponto ambiental (água, alta temperatura, baixa temperatura) em um sistema de painel de controle com versões de firmware anteriores à v3.11, o sistema não vai gerar alertas e condições conforme esperado.

Em alguns cenários, o tipo de ponto “Baixa temperatura” gerará um evento de problema; em todos os cenários, os tipos de ponto “Pânico”, “Água” e “Alta temperatura” não vão gerar nenhuma condição de evento.

Recomendação

Atualize o firmware do painel de controle para a versão v3.11 ou posterior se esses novos tipos de ponto forem necessários.

5.4.3.3 E-mail de notificação pessoal

Ao usar notificações pessoais por e-mail, algumas opções de configuração do servidor (por exemplo, a verificação de duas etapas do Gmail, Permitir aplicativos menos seguros: Desligado) podem não funcionar corretamente. Para garantir a operação, desabilite opções adicionais do servidor de e-mail.

5.4.3.4 Período de travamento do teclado (o teclado trava após as tentativas de senha inválida)

Se o valor do tempo de travamento for maior do que 6.553 segundos, a operação de travamento do teclado poderá falhar. Para garantir a operação correta, ajuste o tempo de travamento abaixo de 6.553 segundos.

5.5 Firmware versão 3.11.5

5.5.1 Conectividade melhorada com a rede Verizon

O FW V3.11.5 melhora o gerenciamento da Verizon APN ao usar os Comunicadores Celulares B444-V ou B444, resultando em maior confiabilidade da conexão.

5.5.2 Índice de Feriados 2

Aviso!
Isso se aplica apenas ao B6512.

O Índice de Feriados 2 não foi executado conforme programado e foi fixado nesta versão do firmware.

5.5.3 Corrupção do log de histórico durante a atualização do firmware

Atualizações do firmware do painel da versão v3.06, ou anterior, para as versões v3.07 a v3.09 pode causar perda de eventos do log de histórico. Esse problema ocorre durante a reinicialização do painel de controle. O log de histórico do painel mais antigo deve ser carregado antes de realizar a atualização para as versões v3.07 a v3.09.
A versão V3.10 corrige esse problema e remova qualquer corrupção no log de histórico.

6 Programando o painel de controle para conformidade com a SIA

Nome do parâmetro	Configurações necessárias do painel de controle para conformidade com a SIA	Padrão
Nº Tel.	(Insira o comando de desativação de chamada em espera[1] no número de telefone de backup)	{Em branco}
Tipo de coação	Opção 3[2]	0 (Desativado)
Cancelar reportes	Sim	Sim
Tempo de atraso na saída	45 a 255 segundos	60 segundos
Habilitar coação	Sim	Não

Reinício de atraso na saída	Sim ou Não	Sim
Armar total - Sem saída	Sim ou Não	Sim
Regra de duas pessoas?	Não	Não
Emboscada inicial?	Não	Não
Alerta de atraso na saída	Sim	Sim
Tom de entrada	Sim	Sim
Tom de saída	Sim ou Não	Sim

Abortar exibição	Sim ou Não	Sim
Cancelar exibição	Sim ou Não	Sim
Verifique a hora	10 a 60 segundos	60 segundos
Função de senha	Arm./desarm.	Arm./ desarm.
Armar total imediato	- (Desativado)	- (Desativado)
ArmPerím imediato	- (Desativado)	- (Desativado)
Enviar coação	- (Desativado) ou E (Ativado)	E (Ativado)
Desarmar	- (Desativado) ou E (Ativado)	E (Ativado)
Desarmar senha	- (Desativado) ou E (Ativado)	E (Ativado)

Atraso para entrada	30 a 240 segundos	30 segundos
Abortar alarme	Sim ou Não	Sim
Janela Abortar	15 a 45 segundos	30 segundos
Número de dígitos da senha	3 a 6 dígitos	Desativado
Contagem para desabilitar oscilador	1 a 2 acionamentos[3]	2 acionamentos
Alerta remoto	Sim	Sim
Temporizador de ponto cruzado	5 a 255 segundos	20 segundos

Ponto cruzado	Sim ou Não[4]	Não
Teste de passagem (todos os pontos de intrusão que não forem incêndios	E (Ativado)	E (Ativado)
Teste de caminhada em todos os pontos de incêndio	E (Ativado)	E (Ativado)
Resposta de atraso, Desarmado	00:00	00:00

Resposta de atraso, Armado	00:00	00:00

[1]A chamada em espera não se aplica a redes celulares nem à comunicação PSDN (Rede Pública de Dados Comutada). O comando de desativação de chamada em espera em uma linha telefônica sem chamadas impedirá a conexão bem-sucedida com a estação central.

[2]L14 é o nível de autoridade de coação padrão.

[3]A contagem para desabilitar oscilador é programável até 4 acionamentos. Para conformidade com a SIA, defina como 1 ou 2.

[4]Os pontos cruzados devem se sobrepor (proteger a mesma área) para que um único ponto possa proteger a área individualmente.

7 Requisitos mínimos do sistema para ANSI/SIA CP-01

Requisitos mínimos do sistema para classificação de acordo com ANSI/SIA CP-01:

- Unidade de controle listada e classificada pela UL, modelos B6512, B5512, B4512 ou B3512
- Teclado listado e classificado pela UL Modelos B942/ B942W, B930, B921C/B921CW, B920 ou B915/B915I
- Campainha local listada pela UL.
- Meios de transmissão fora das instalações

8 Software de código aberto 3.15.116

A Radionix inclui os módulos de software de código aberto listados abaixo no firmware deste painel de controle. A inclusão desses módulos não limita a garantia da 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).

Para obter mais informações, consulte a Licença OpenSSL em www.boschsecurity.com, em Catálogo do Produto.

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

202611021237