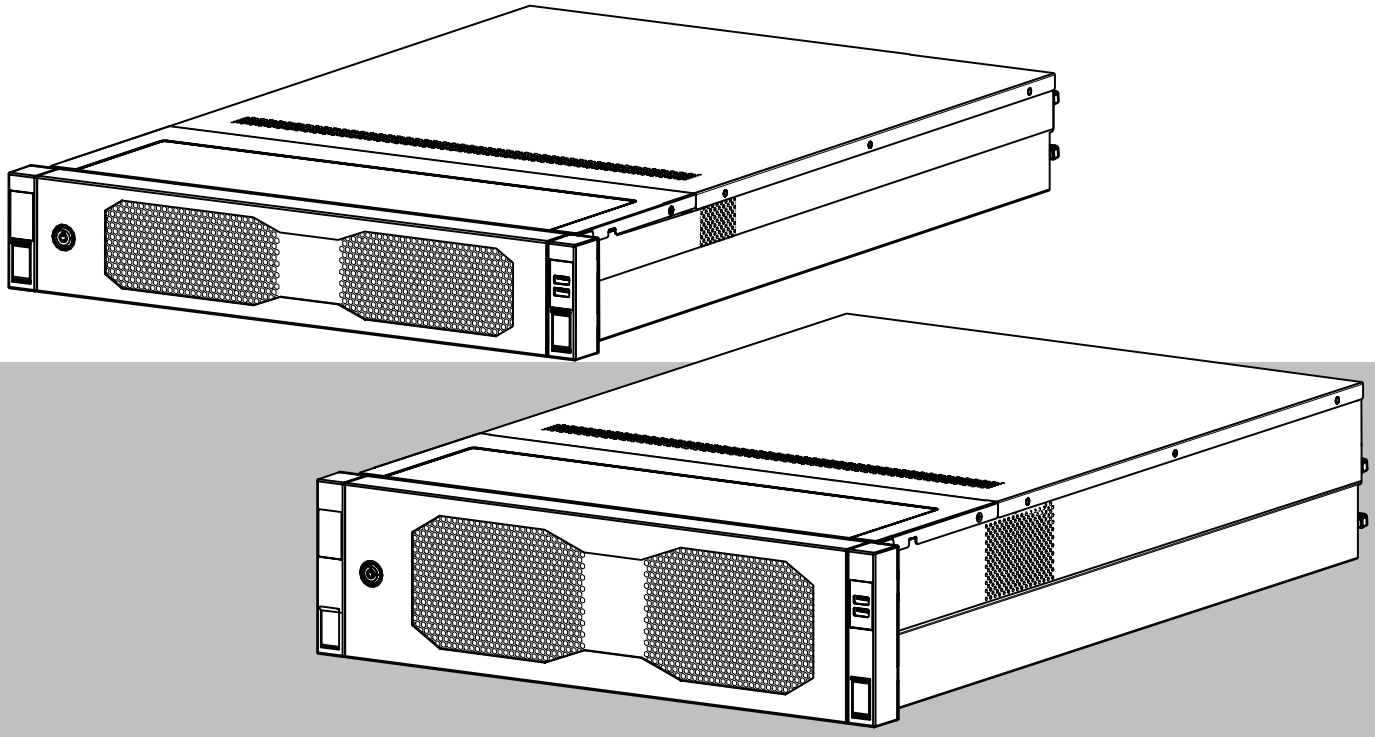
DIVAR IP all-in-one 7000 2U | DIVAR IP all-in-one 7000 3U

DIP-74C0-00N | DIP-74C4-8HD | DIP-74C8-8HD | DIP-74CI-8HD | DIP-74CI-12HD | DIP-74G0-00N | DIP-74GI-16HD



pt-BR Manual do usuário

Sumário

1 Segurança

Observe as precauções de segurança neste capítulo.

1.1 Precauções de operação

Aviso!
Uso destinado
Este produto serve somente para uso profissional. Ele não deve ser instalado em uma área pública que seja acessível à população geral.

Aviso!
Não use este produto em locais úmidos ou molhados.

Aviso!
Tome precauções para proteger o dispositivo de surtos de eletricidade e raios.

Aviso!
Mantenha a área ao redor do dispositivo limpa e organizada.

Aviso!
Aberturas do gabinete
Não bloqueie nem cubra as aberturas. As aberturas do gabinete são fornecidas para fins de ventilação. Essas aberturas impedirão o superaquecimento e garantirão uma operação confiável.

Aviso!
Não abra nem remova a tampa do dispositivo. A abertura ou remoção da tampa pode causar danos ao sistema e anulará a garantia.

Aviso!
Não deixe cair nenhum líquido no dispositivo.

Advertência!
Tenha cuidado ao fazer a manutenção e trabalhar em torno do backplane. Tensão ou energia perigosa está presente no backplane quando o sistema está em operação. Não encoste objetos metálicos no backplane e certifique-se de que nenhum cabo de fita entre em contato com o backplane.

Aviso!
Desconecte a fonte de alimentação antes de mover o produto. Mova o produto com cuidado. Força ou impactos excessivos podem danificar o produto e os discos rígidos.

Advertência!
O manuseio de materiais de solda de chumbo usados neste produto poderá expor você a chumbo, um elemento químico considerado causador de defeitos de nascimento e outros danos reprodutivos pelo estado da Califórnia.

Aviso!
A perda de vídeo é inerente à gravação de vídeo digital; portanto, a Bosch Security Systems não pode ser considerada responsável por nenhum dano resultante da perda de informações de vídeo.
Para minimizar o risco de perda de informações, recomendamos sistemas de gravação múltiplos e redundantes, bem como um procedimento de back-up de todas as informações analógicas e digitais.

1.2 Precauções relativas à segurança cibernética

Por questões de segurança cibernética, observe o seguinte:

- Verifique se o acesso físico ao sistema é restrito apenas à equipe autorizada. Coloque o sistema em uma área de controle de acesso protegida, a fim de evitar a manipulação física.
- Trave o painel frontal para impedir a remoção não autorizada dos discos rígidos. Sempre remova a chave do cadeado e guarde-a em local seguro.
- Use o recurso Sensor de intrusão do chassis para detectar qualquer acesso físico não autorizado no interior do dispositivo.
- O sistema operacional inclui os mais recentes patches de segurança do Windows disponíveis no momento em que a imagem de software foi criada. Use a funcionalidade de atualização online do Windows ou os correspondentes patches lançados mensalmente para instalação online a fim de instalar regularmente atualizações de segurança no SO.
- Para garantir que o navegador da Web esteja seguro e funcionando corretamente, mantenha-o sempre atualizado.
- Não desative o Windows Defender e o Firewall do Windows, mantendo-os sempre atualizados. Não instale software antivírus adicional que possa interromper as configurações de segurança.
- Não forneça informações sobre o sistema e dados confidenciais a pessoas desconhecidas, a não ser que você tenha certeza da autoridade de uma pessoa.
- Não envie informações confidenciais pela Internet antes de verificar a segurança de um site.
- Limite o acesso à rede local somente a dispositivos confiáveis. Os detalhes são descritos nos documentos a seguir, que estão disponíveis no catálogo de produtos online:
  - *Autenticação de rede 802.1X*
  - *Guia de segurança cibernética para produtos de vídeo IP da Bosch*
- Para obter acesso por meio de redes públicas, use apenas os canais de comunicação seguros (criptografados).
- A conta de administrador fornece privilégios administrativos completos e acesso irrestrito ao sistema. Os direitos administrativos permitem que os usuários instalem, atualizem ou removam o software e alterem as definições de configuração. Além disso, os direitos administrativos permitem que os usuários acessem e alterem diretamente as chaves do registro e, com isso, ignorem as configurações de segurança e gerenciamento central. Os usuários conectados à conta de administrador podem atravessar firewalls e

remover um software antivírus, o que vai expor o sistema a vírus e ataques cibernéticos. Isso pode representar um sério risco para a segurança do sistema e dos dados.
Para minimizar os riscos à segurança cibernética, observe o seguinte:
  - Certifique-se de que a conta de administrador esteja protegida com uma senha complexa de acordo com a política de senha.
  - Certifique-se de que somente um número limitado de usuários confiáveis tenha acesso à conta de administrador.
- Devido aos requisitos de operação, a unidade do sistema não deve ser criptografada. Sem a criptografia, os dados armazenados nessa unidade podem ser facilmente acessados e removidos. Para evitar roubo de dados ou perda acidental de dados, certifique-se de que somente pessoas autorizadas tenham acesso ao sistema e à conta de administrador.
- Para instalação e atualização de software, bem como para recuperação do sistema, talvez seja necessário usar dispositivos USB. Portanto, as portas USB do sistema não devem estar desativadas. No entanto, a conexão de dispositivos USB ao sistema representa um risco de infecção por malware. Para evitar ataques de malware, não conecte nenhum dispositivo USB infectado ao sistema.
- Não altere as configurações do BIOS UEFI. A alteração das configurações do BIOS UEFI pode comprometer ou até mesmo resultar em mau funcionamento do sistema.
- O sistema BMC não deve ser conectado à rede pública.

1.3 Precauções de software

1.3.1 Use o software mais recente

Antes de operar o dispositivo pela primeira vez, instale a versão mais recente do software aplicável. Para obter consistência de funcionalidade, compatibilidade, desempenho e segurança, atualize regularmente o software ao longo da vida útil do dispositivo. Siga as instruções na documentação do produto sobre as atualizações de software.
Os links a seguir contêm mais informações:
- Informações gerais: https://www.boschsecurity.com/xc/en/support/product-security/
- Conselhos de segurança, com uma lista de vulnerabilidades identificadas e soluções propostas: https://www.boschsecurity.com/xc/en/support/product-security/security-advisories.html
- Informações de segurança, que cobrem possíveis efeitos causados por vulnerabilidades de terceiros: https://www.boschsecurity.com/us/en/support/product-security/security-information.html

Para receber atualizações sobre novos avisos de segurança, você pode assinar os feeds RSS na página de Avisos de Segurança da Bosch Security and Safety Systems em: https://www.boschsecurity.com/xc/en/support/product-security/security-advisories.html
A Bosch não assume nenhuma responsabilidade por quaisquer danos causados pela operação de seus produtos com componentes de software desatualizados.
O software mais recente e os pacotes de atualização disponíveis encontram-se na loja de downloads do Bosch Security and Safety Systems em:
https://downloadstore.boschsecurity.com/

1.3.2 Informações sobre OSS

A Bosch usa software de código aberto nos produtos DIVAR IP all-in-one.
As licenças dos componentes de software de código aberto usados na unidade do sistema podem ser encontradas em:

```
C:\license txt\
```

As licenças de componentes do Open Source Software usadas em qualquer software adicional instalado em seu sistema são armazenadas na pasta de instalação do respectivo software, por exemplo, em:

```
C:\Program Files\Bosch\SysMgmService\apps\sysmgm-commander\[version]\License
```

ou em:

```
C:\Program Files\Bosch\SysMgmService\apps\sysmgm-executor\[version]\License
```

2 Introdução

Acessível e fácil de usar, o DIVAR IP all-in-one 7000 é uma solução multifuncional de gerenciamento, visualização e gravação para sistemas de vigilância em rede com até 256 canais (com 8 canais pré-licenciados).

O DIVAR IP all-in-one 7000 2U/3U é uma unidade para montagem em rack de 2U/3U que combina Bosch Video Management System recursos avançados e gerenciamento de gravação de última geração em um único aparelho de gravação conveniente, fácil de instalar e operar para clientes de TI.

O DIVAR IP all-in-one 7000 usa componentes de design incorporados e de núcleo, além de ser baseado no sistema operacional Microsoft Windows Server IoT 2022 for Storage Standard. Ele conta com unidades de disco rígido SATA hot-swap de “categoria corporativa”, proporcionando até 216/288 TB de capacidade de armazenamento bruta.

3 Visão geral do sistema

Sistema operacional

O sistema operacional Microsoft Windows Server IoT 2022 for Storage Standard oferece uma interface do usuário para configuração inicial do servidor, gerenciamento unificado de dispositivos de armazenamento, configuração simplificada e gerenciamento de armazenamento, além de suporte para Microsoft iSCSI Software Target.
Ele é especialmente ajustado para oferecer desempenho ideal para armazenamento conectado à rede. O sistema operacional Microsoft Windows Server IoT 2022 for Storage Standard fornece melhorias significativas em cenários de gerenciamento de armazenamento, além de integração de componentes e funcionalidades de gerenciamento do dispositivo de armazenamento.

DIVAR IP System Manager

O aplicativo DIVAR IP System Manager é a interface de usuário central que facilita a instalação, a configuração e a atualização do software do sistema.

modos de operação

Os sistemas DIVAR IP all-in-one 7000 podem operar em três modos diferentes:

- Sistema de gravação e gerenciamento de vídeo completo, que utiliza os principais componentes e serviços do BVMS e do Video Recording Manager.
  Este modo fornece uma solução avançada de segurança de vídeo IP, que entrega um gerenciamento perfeito de vídeo digital, áudio e dados em uma rede IP. Ele combina diretamente codificadores e câmeras IP, fornece gerenciamento de alarmes e eventos do sistema, monitora a integridade do sistema e gerencia usuários e prioridades. Este modo fornece o melhor sistema de gerenciamento de vídeo para os dispositivos de vigilância por vídeo da Bosch ao aproveitar os recursos exclusivos das câmeras e das soluções de gravação da Bosch. Ele inclui componentes de Video Streaming Gateway para integrar câmeras de outros fabricantes.
- Solução avançada de gravação de vídeo para um BVMS, utilizando os componentes e os serviços principais do Video Recording Manager e os recursos exclusivos das câmeras Bosch e das soluções de gravação. Até dois servidores Video Recording Manager podem ser adicionados a um sistema BVMS executado em um dispositivo DIVAR IP all-in-one.
- Expansão de armazenamento iSCSI para um sistema BVMS, executada em um hardware diferente. Até quatro dessas expansões de armazenamento iSCSI podem ser adicionadas a um sistema BVMS em execução em um dispositivo DIVAR IP all-in-one 7000.

Ao configurar o sistema, no aplicativo DIVAR IP System Manager, você deve escolher o modo de operação desejado para configurar o sistema.
Com o aplicativo DIVAR IP System Manager, também é possível atualizar o software instalado.
O software mais recente e os pacotes de atualização disponíveis encontram-se na loja de downloads do Bosch Security and Safety Systems em:
https://downloadstore.boschsecurity.com/

Aviso!
Fluxos de vídeos gravados precisam ser configurados de modo que a largura de banda máxima do sistema (sistema base BVMS/VRM mais expansões de armazenamento iSCSI) não seja excedida.

4 Configuração do sistema

4.1 Configurações padrão

Todos os sistemas DIVAR IP são pré-configurados com um endereço IP padrão e configurações iSCSI padrão:

- Endereço IP: atribuído automaticamente por DHCP (endereço IP de fallback: 192.168.0.200).
- Máscara de sub-rede: atribuída automaticamente por DHCP (máscara de sub-rede de fallback: 255.255.255.0).

Configurações de usuário padrão para a conta de administrador

- Nome de usuário: **BVRAdmin**
- Senha: a ser configurada no primeiro logon.
  Requisitos de senha:
  - Mínimo de 14 caracteres
  - As senhas devem conter caracteres de três das seguintes quatro categorias:
    Pelo menos uma letra maiúscula.
    Pelo menos uma letra minúscula.
    Pelo menos um dígito.
    Pelo menos um caractere especial.

4.2 Pré-requisitos

Observe o seguinte:

- O DIVAR IP precisa ter uma ligação de rede ativa durante a instalação. Certifique-se de que o comutador de rede ao qual você está se conectando esteja ligado.
- O endereço IP padrão não deve estar ocupado por qualquer outro dispositivo na rede. Certifique-se de que os endereços IP padrão dos sistemas DIVAR IP existentes na rede sejam alterados antes de adicionar outro DIVAR IP.

4.3 Primeiro logon e configuração inicial do sistema

Aviso!
Não altere nenhuma configuração do sistema operacional. Alterações nas configurações do sistema operacional podem resultar no mau funcionamento do sistema.

Aviso!
Para executar tarefas administrativas, é necessário fazer logon na conta de administrador.

Aviso!
Em caso de perda de senha, deve-se realizar uma recuperação do sistema, conforme descrito no manual de instalação. A configuração deve ser feita do zero ou deve ser importada.

Aviso!
Por motivos de segurança, as caixas de diálogo UAC (Controle de Conta de Usuário) são exibidas pedindo sua confirmação para fazer as alterações pretendidas no sistema. Você só pode prosseguir com a instalação depois de confirmar que deseja fazer as alterações apropriadas.

Para configurar o sistema:

1. Conecte a unidade do DIVAR IP all-in-one e as câmeras à rede.
2. Ligue a unidade.
   Aguarde até que a tela do BIOS seja exibida e as rotinas de configuração do Microsoft Windows Server IoT 2022 for Storage Standard sejam executadas. Esse processo pode levar alguns minutos. Não desligue o sistema.
   Depois que o processo for concluído, a tela de seleção de idioma do Windows será exibida.
3. Selecione seu país/região, o idioma desejado do sistema operacional e o layout do teclado na lista e, em seguida, clique em **Avançar**.
   Os termos de licença de software da Microsoft são exibidos.
4. Clique em **Accept** para aceitar os termos de licença e aguarde o Windows ser reiniciado. Isso pode levar alguns minutos. Não desligue o sistema.
   Depois da reinicialização, a página de logon do Windows será exibida.
5. Defina uma nova senha para a conta de administrador **BVRAdmin** e confirme.
   Requisitos de senha:

– Mínimo de 14 caracteres
– As senhas devem conter caracteres de três das seguintes quatro categorias:
  – Pelo menos uma letra maiúscula.
  – Pelo menos uma letra minúscula.
  – Pelo menos um dígito.
  – Pelo menos um caractere especial.

   Pressione Enter**.**
   A página **Software Selection** é exibida.

6. O sistema verificará automaticamente a unidade local e qualquer mídia de armazenamento externa conectada em busca do arquivo de instalação **SystemManager_x64_[software version].exe** do DIVAR IP System Manager, que está localizado em uma pasta com a seguinte estrutura: `Drive root\BoschAppliance\`.
   A verificação pode levar algum tempo. Aguarde a conclusão.
7. Depois que o sistema detectar o arquivo de instalação, ele será exibido na página **Software Selection**. Clique na barra que exibe o arquivo de instalação para iniciar a instalação.
   Aviso: Verifique se a versão mais recente do DIVAR IP System Manager está instalada. Você pode encontrar o software e os pacotes de atualização mais recentes disponíveis na loja de download da Bosch Security and Safety Systems em: https://downloadstore.boschsecurity.com/.
8. Se o arquivo de instalação não for encontrado durante o processo de digitalização, continue da seguinte maneira:
   – Acesse https://downloadstore.boschsecurity.com/.
   – Na guia **Software,** selecione **BVMS Appliances** na lista e clique em **Select**.
     Uma lista de todos os pacotes de software disponíveis é exibida.
   – Localize o arquivo ZIP **SystemManager_[software version].zip** e salve-o em uma mídia de armazenamento, como um dispositivo USB.
   – Descompacte o arquivo na mídia de armazenamento, certificando-se de que a pasta **BoschAppliance** seja colocada na raiz da mídia de armazenamento.
   – Conecte a mídia de armazenamento ao seu sistema DIVAR IP all-in-one.
     O sistema verificará automaticamente a mídia de armazenamento em busca do arquivo de instalação.
     A verificação pode levar algum tempo. Aguarde a conclusão.

- Assim que o arquivo de instalação for detectado, ele será exibido na página **Software Selection**. Clique na barra que exibe o arquivo de instalação para iniciar a instalação.
  Observação: Para ser detectado automaticamente, o arquivo de instalação deve estar localizado em uma pasta com a seguinte estrutura: `Drive root\BoschAppliance\` (por exemplo, `F:\BoschAppliance\`).
  Se o arquivo de instalação estiver localizado em outro local que não corresponda à estrutura de pastas predefinida, clique em  para navegar para o respectivo local. Depois, clique no arquivo de instalação para iniciar a instalação.

9. Antes de a instalação começar, a caixa de diálogo **End User License Agreement (EULA)** é exibida. Leia os termos de licença e clique em **Accept** para continuar.
10. Nas caixas de diálogo Controle de conta de usuário a seguir, clique em **Yes** para continuar. A instalação é iniciada.
11. Após a conclusão da instalação, o sistema é reinicializado e você é direcionado para a página de logon do Windows. Faça logon na conta de administrador.
12. O navegador Microsoft Edge é aberto e a página **DIVAR IP - Configuração do sistema** é exibida. A página mostra o tipo de dispositivo e o número de série do dispositivo, bem como os três modos de operação e as versões de software disponíveis para cada modo de operação.
    Você deve escolher o modo de operação desejado e a versão de software desejada para configurar seu sistema DIVAR IP all-in-one.
    Observação: Se a versão de software desejada para o respectivo modo de operação não estiver disponível em uma unidade local, proceda da seguinte forma:
    - Acesse https://downloadstore.boschsecurity.com/.
    - Na guia **Software,** selecione **BVMS Appliances** na lista e clique em **Select**.
      Uma lista de todos os pacotes de software disponíveis é exibida.
    - Localize os arquivos ZIP dos pacotes de software desejados (por exemplo, **BVMS_[BVMS version]_SystemManager_package_[package version].zip**) e salve-os em uma mídia de armazenamento, como um pen-drive.
    - Descompacte os arquivos na mídia de armazenamento. Não altere a estrutura de pastas dos arquivos descompactados.
    - Conecte a mídia de armazenamento ao seu sistema DIVAR IP all-in-one.

Aviso!
A alteração do modo de operação depois da instalação requer uma redefinição de fábrica completa.

4.3.1 Escolha do modo de operação BVMS

Para operar o sistema DIVAR IP all-in-one como um sistema completo de gravação e gerenciamento de vídeos:

1. Na página **DIVAR IP - Configuração do sistema**, selecione o modo de operação **BVMS** e a versão do BVMS que você deseja instalar e clique em **Instalar modo de operação**.
   O contrato de licença BVMS será exibido.
2. Leia e aceite o contrato de licença e clique em **Sim, instalar** para continuar.
   A instalação é iniciada e a caixa de diálogo da instalação mostra o andamento da instalação. Não desligue o sistema e não remova a mídia de armazenamento durante o processo de instalação.

3. Depois que todos os pacotes de software forem instalados com êxito, o sistema será reiniciado. Depois da reinicialização, você é direcionado para a área de trabalho do BVMS.
4. Na área de trabalho do BVMS, clique no aplicativo desejado para configurar o sistema.

Aviso!
Para obter mais detalhes, consulte o respectivo treinamento baseado na Web do DIVAR IP all-in-one e a documentação do BVMS.
O treinamento pode ser encontrado em: www.boschsecurity.com/xc/en/support/training/

4.3.2 Escolha do modo de operação VRM

Para operar o sistema DIVAR IP all-in-one como um sistema de gravação de vídeo puro:

1. Na página **DIVAR IP - Configuração do sistema**, selecione o modo de operação **VRM** e a versão do VRM que você deseja instalar e clique em **Instalar modo de operação**.
   O contrato de licença VRM será exibido.
2. Leia e aceite o contrato de licença e clique em **Sim, instalar** para continuar.
   A instalação é iniciada e a caixa de diálogo da instalação mostra o andamento da instalação. Não desligue o sistema e não remova a mídia de armazenamento durante o processo de instalação.
3. Depois que todos os pacotes de software forem instalados com êxito, o sistema será reiniciado. Depois da reinicialização, você é direcionado para a tela de logon do Windows.

Aviso!
Para obter mais detalhes, consulte a documentação do VRM.

4.3.3 Escolha do modo de operação de armazenamento iSCSI

Para operar o sistema DIVAR IP all-in-one como uma expansão de armazenamento iSCSI:

1. Na página **DIVAR IP - Configuração do sistema**, selecione o modo de operação **armazenamento iSCSI** e a versão de armazenamento iSCSI que deseja instalar e clique em **Instalar modo de operação**.
   A caixa de diálogo de instalação é exibida.
2. Na caixa de diálogo de instalação, clique em **Sim, instalar** para continuar.
   A instalação é iniciada e a caixa de diálogo da instalação mostra o andamento da instalação. Não desligue o sistema e não remova a mídia de armazenamento durante o processo de instalação.
3. Depois que todos os pacotes de software forem instalados com êxito, o sistema será reiniciado. Depois da reinicialização, você é direcionado para a tela de logon do Windows.
4. Adicione o sistema como uma expansão de armazenamento iSCSI a um servidor externo do BVMS ou do VRM usando o BVMS Configuration Client ou o Configuration Manager.

Aviso!
Para obter mais detalhes, consulte o BVMS ou a documentação do Configuration Manager.

5 Atualização do software

Atualize DIVAR IP System Manager para a versão mais recente.

5.1 Atualizar o DIVAR IP System Manager

1. Acesse https://downloadstore.boschsecurity.com/.
2. Na guia **Software,** selecione **BVMS Appliances** na lista e clique em **Select**.
   Uma lista de todos os pacotes de software disponíveis é exibida.
3. Localize o arquivo ZIP **SystemManager_[software version 2.3.0 or higher].zip** e salve-o em um meio de armazenamento, como um USB.
4. Descompacte o arquivo na mídia de armazenamento.
5. Conecte a mídia de armazenamento ao seu dispositivo DIVAR IP all-in-one.
6. Inicie o DIVAR IP System Manager:
   - Se você estiver conectado ao Windows com a conta de administrador do **BVRAdmin**, clique duas vezes no ícone DIVAR IP System Manager da área de trabalho do Windows. O
     DIVAR IP System Manager será iniciado.
   - Se o seu sistema estiver sendo executado no modo de operação do BVMS, clique no ícone DIVAR IP System Manager na área de trabalho BVMS e efetue login na conta de administrador BVRAdmin. O DIVAR IP System Manager é aberto em uma caixa de diálogo tela cheia (é possível sair da caixa de diálogo pressionando Alt+ F4).
7. A página **Pacotes de software** é exibida. Escolha o pacote de software DIVAR IP System Manager, depois clique em **Instalar pacote** para prosseguir.
   A caixa de diálogo de instalação será exibida.
8. Na caixa de diálogo de instalação, clique em **Sim, instalar** para prosseguir.
   A instalação começará.
   O processo de instalação pode demorar alguns minutos. Não desligue o sistema nem remova a mídia de armazenamento durante o processo de instalação.
   Observe as notificações que são exibidas no topo da página.

5.2 Atualizar o software usando o DIVAR IP System Manager

Com o aplicativo DIVAR IP System Manager, é possível atualizar o software instalado no seu sistema.
O software mais recente e os pacotes de atualização disponíveis encontram-se na loja de downloads do Bosch Security and Safety Systems em:
https://downloadstore.boschsecurity.com/

Aviso!
Não há suporte para reverter o software instalado para uma versão anterior.

Para atualizar o software instalado:

1. Acesse https://downloadstore.boschsecurity.com/.
2. Na guia **Software,** selecione **BVMS Appliances** na lista e clique em **Select**.
   Uma lista de todos os pacotes de software disponíveis é exibida.
3. Localize os arquivos ZIP dos pacotes de software desejados (por exemplo, **BVMS_[BVMS version]_SystemManager_package_[package version].zip**) e salve-os em uma mídia de armazenamento, como um pen-drive.

4. Descompacte os arquivos na mídia de armazenamento. Não altere a estrutura de pastas dos arquivos descompactados.
5. Inicie o DIVAR IP System Manager:
   – Se você estiver conectado ao Windows com a conta de administrador do **BVRAdmin**, clique duas vezes no ícone DIVAR IP System Manager da área de trabalho do Windows. O
   DIVAR IP System Manager será iniciado.
   – Se o seu sistema estiver sendo executado no modo de operação do BVMS, clique no ícone DIVAR IP System Manager na área de trabalho BVMS e efetue login na conta de administrador BVRAdmin. O DIVAR IP System Manager é aberto em uma caixa de diálogo tela cheia (é possível sair da caixa de diálogo pressionando Alt+ F4).
6. A página **Pacotes de software** será exibida, mostrando o tipo de dispositivo e o número de série do dispositivo no topo da página.

– Na coluna **Nome do pacote de software**, você pode ver todos os aplicativos de software do DIVAR IP System Manager que já estão instalados no sistema, bem como todos os aplicativos de software do DIVAR IP System Manager que foram detectados pelo sistema, na unidade **Images** ou em uma mídia de armazenamento.
– Na coluna **Versão instalada,** você pode ver a versão do aplicativo de software instalada atualmente no sistema.
– Na coluna **Estado**, você pode ver o status do respectivo aplicativo de software:
  – O ícone  indica que nenhuma versão posterior do aplicativo de software instalado foi detectada pelo sistema na unidade **Images** ou em uma mídia de armazenamento.
  Observação: Para garantir que você esteja usando a versão mais recente do software, verifique as versões de software disponíveis no armazenamento de downloads do Bosch Security and Safety Systems em:
  https://downloadstore.boschsecurity.com/
  – O ícone indica que o sistema não detectou nenhuma versão posterior do aplicativo de software instalado na unidade **Images** ou em uma mídia de armazenamento.
  O ícone também será exibido se o sistema detectar um aplicativo de software que ainda não foi instalado no sistema.
– Na coluna **Versão disponível**, você pode ver as versões posteriores dos aplicativos de software instalados. Essas versões foram detectadas pelo sistema na unidade **Images** ou em uma mídia de armazenamento.
  A coluna também exibe as versões disponíveis dos aplicativos de software detectados ainda não instalados no sistema.
  Observação: Serão exibidas somente as versões posteriores dos aplicativos de software instalados. Não há suporte para reverter o aplicativo de software para uma versão anterior.

7. Na coluna **Nome do pacote de software**, clique no respectivo botão de opção para selecionar o aplicativo de software que você deseja atualizar ou instalar.
8. Na coluna **Versão disponível**, selecione a versão desejada para a qual deseja atualizar o aplicativo de software ou que deseja instalar e clique em **Instalar pacote**.
   Se aplicável, uma caixa de diálogo do contrato de licença será exibida.

9. Leia e aceite o contrato de licença e, depois, clique em **Sim, instalar** para continuar.
   A instalação será iniciada, e a caixa de diálogo da instalação mostrará o andamento da instalação. Não desligue o sistema e não remova a mídia de armazenamento durante o processo de instalação.
10. Após todos os pacotes de software terem sido instalados, você receberá uma confirmação de que a instalação foi bem-sucedida.
11. Se a instalação falhar, você verá uma mensagem com instruções sobre como proceder.

6 Conexão remota com o sistema

Você pode fazer uma conexão remota com o sistema DIVAR IP all-in-one e acessá-lo pela Internet.

Para criar uma conexão remota, é necessário fazer o seguinte:

1. *Proteção do sistema contra o acesso não autorizado, página 17*.
2. *Configuração do encaminhamento de porta, página 17*.
3. *Escolha de um cliente adequado, página 17*.

Você também pode se conectar ao seu DIVAR IP all-in-one via Bosch Remote Portal e utilizar os recursos atuais e futuros disponível por meio Remote Portal. Para obter mais informações, consulte *Conexão ao Remote Portal, página 18*.

6.1 Proteção do sistema contra o acesso não autorizado

Para proteger o sistema contra o acesso não autorizado, siga as regras de senha forte antes de se conectar ao sistema pela Internet. Quanto mais forte a senha, mais protegido seu sistema estará contra pessoas não autorizadas e malware.

6.2 Configuração do encaminhamento de porta

Para acessar um sistema DIVAR IP all-in-one pela Internet por meio de um roteador NAT/PAT adequado, você deve configurar o encaminhamento de porta no sistema DIVAR IP all-in-one e no roteador.

Para configurar o encaminhamento de porta:

- ▸ Insira as seguintes regras de portas nas configurações de encaminhamento de porta do seu roteador de Internet:
  - porta 5322 para acesso ao túnel SSH usando BVMS Operator Client.
    Observações: Essa conexão é aplicável somente ao modo de operação BVMS.
  - porta 443 para acesso HTTPS ao VRM usando o Video Security Client ou o Video Security App.
    Observação: Essa conexão é aplicável somente ao modo de operação BVMS ou VRM.

Seu DIVAR IP all-in-one está sendo acessado pela Internet.

6.3 Escolha de um cliente adequado

Há duas opções para fazer uma conexão remota com seu sistema DIVAR IP all-in-one:

- *Conexão remota com o Operador cliente do BVMS, página 17*.
- *Conexão remota com o aplicativo Video Security, página 18*.

Aviso!
A compatibilidade das versões do BVMS Operator Client ou Video Security App é determinada pelas versões do software BVMS ou VRM instalado no DIVAR IP.
Para obter informações detalhadas, consulte os respectivos materiais de treinamento e documentação do software.

6.3.1 Conexão remota com o Operador cliente do BVMS

Aviso!
Essa conexão é aplicável somente ao modo de operação BVMS.

Para realizar uma conexão remota com o BVMS Operator Client:

1. Instale o BVMS Operator Client na estação de trabalho do cliente.
2. Após concluir a instalação com êxito, inicie o Operator Client usando o atalho da área de trabalho  .
3. Insira o seguinte e clique em **OK**.
   Nome do usuário: admin (ou outro usuário, caso já tenha sido configurado)
   Senha: senha do usuário
   Conexão: ssh://[public-IP-address-of-DIVAR-IP_all-in-one]:5322

6.3.2 Conexão remota com o aplicativo Video Security

Aviso!
Essa conexão é aplicável somente ao modo de operação BVMS ou VRM.

Para realizar uma conexão remota com o Video Security App:
1. Na App Store da Apple, pesquise Bosch Video Security.
2. Instale o aplicativo Video Security em seu dispositivo iOS.
3. Inicie o aplicativo Video Security.
4. Selecione **Adicionar**.
5. Insira o endereço IP público ou o nome dynDNS.
6. Verifique se Secure Connection (SSL) está habilitada.
7. Selecione **Adicionar**.
8. Insira o seguinte:
   Nome do usuário: admin (ou outro usuário, caso esteja configurado)
   Senha: senha do usuário

6.4 Conexão a um Enterprise Management Server

Para um gerenciamento centralizado de vários sistemas DIVAR IP all-in-one no modo de operação BVMS, você pode usar um BVMS Enterprise Management Server instalado em um servidor diferente.
Para obter informações detalhadas sobre a configuração e a operação do BVMS Enterprise System, consulte os materiais de treinamento e a documentação do BVMS.

6.5 Conexão ao Remote Portal

É possível se conectar a um dispositivo DIVAR IP all-in-one pelo Bosch Remote Portal e usar as funcionalidades atuais e futuras, como o serviço Bosch Remote System Management que está disponível no Remote Portal.
Para obter informações detalhadas sobre o serviço Remote System Management, consulte a documentação e os materiais de treinamento do Remote System Management.

Pré-requisitos

Conexão com o Remote Portal
Para conectar dispositivos DIVAR IP all-in-one ao Remote Portal, certifique-se de que os seguintes pré-requisitos se aplicam:
– O DIVAR IP System Manager 2.3.0 (ou superior) deve ser instalado no dispositivo.
– Uma conta do Remote Portal deve ser criada.

Comunicação com o Remote Portal
Requisitos de conectividade para a comunicação com o Remote Portal.
Aviso: todas as conexões são de saída.

HTTPS (Porta 443)

– https://api.remote.boschsecurity.com/rest/iot/devices
– https://sw-repo-remote.s3.eu-central-1.amazonaws.com

MQTTS (Porta 8883)

– tls://a1j83emmuys8gs-ats.iot.eu-central-1.amazonaws.com:8883

6.5.1 Criando uma conta do Remote Portal

Para criar uma conta do Remote Portal:

1. Acesse https://remote.boschsecurity.com/login.
2. Clique em **Sign up**.
3. Insira o nome e o email da sua empresa.
4. Selecione a região da sua empresa.
5. Leia os termos e condições e o aviso de proteção de dados e, em seguida, marque as caixas de seleção para aceitá-las.
6. Clique em **Sign up** para criar uma conta.

6.5.2 Registrando dispositivos DIVAR IP all-in-one devices no Remote Portal

Para registrar um dispositivo DIVAR IP all-in-one no Remote Portal:

1. Inicie o DIVAR IP System Manager.
2. Clique na guia **Conexão Remote Portal**.
3. Se você tiver uma conta existente do Remote Portal, insira seu e-mail e sua senha e clique em **Registrar-se** para registrar seu dispositivo DIVAR IP all-in-one no Remote Portal.
4. Caso o seu e-mail esteja atribuído a diversas contas empresariais com privilégios de administrador, será exibida uma caixa de diálogo de seleção com as respectivas contas empresariais.
   Nessa caixa de diálogo, escolha a conta empresarial na qual deseja registrar o dispositivo DIVAR IP all-in-one.

Aviso!

SingleKey ID

A Bosch introduziu o SingleKey ID como um provedor de identidade (IdP) para permitir uma entrada central em todos os aplicativos, serviços e plataformas da Bosch.

Para conectar o dispositivo ao Remote Portal usando o SingleKey ID, siga as instruções na tela.

5. Se você ainda não tiver uma conta do Remote Portal, comece clicando em **Criar conta** para criar uma conta do Remote Portal. Consulte .

6.5.3 Cancelando o registro de dispositivos DIVAR IP all-in-one do Remote Portal

Para cancelar o registro de um dispositivo DIVAR IP all-in-one do Remote Portal:

1. Inicie o DIVAR IP System Manager.
2. Clique na guia **Remote Portal connection**.
3. Clique em **Cancelar registro** para cancelar o registro do dispositivo DIVAR IP all-in-one do Remote Portal.
   Nota: o cancelamento do registro do dispositivo do Remote Portal não exclui a configuração do dispositivo no Remote Portal. Para excluir a configuração do dispositivo, efetue login na conta da empresa correspondente do Remote Portal.

7 Manutenção

7.1 Logon na conta de administrador

Logon na conta de administrador no modo de operação BVMS

Para fazer logon na conta de administrador no modo de operação BVMS:

1. Na área de trabalho do BVMS, pressione Ctrl+Alt+Del.
2. Mantenha pressionada a tecla Shift à esquerda imediatamente depois de clicar em **Alternar usuário**.
3. Pressione Ctrl+Alt+Del novamente.
4. Selecione o usuário **BVRAdmin** e insira a senha definida durante a configuração do sistema. Depois, pressione Enter.

Observação: Para voltar à área de trabalho do BVMS, pressione Ctrl+Alt+Del e clique em **Alternar usuário** ou **Sair**. O sistema retornará automaticamente para a área de trabalho do BVMS sem reiniciar o sistema.

Logon na conta de administrador no modo de operação VRM or iSCSI

Para fazer logon na conta de administrador no modo de operação VRM ou iSCSI:

- Na tela de logon do Windows, pressione Ctrl+Alt+Del e insira a senha **BVRAdmin**.

7.2 Monitoramento do sistema

7.2.1 Monitoramento do sistema usando o aplicativo ASUS Inband Tool

Os sistemas DIVAR IP all-in-one acompanham o aplicativo ASUS **Inband Tool** pré-instalado, que pode ser usado para monitorar o sistema.

O serviço do aplicativo é ativado por padrão.

Para iniciar o aplicativo:

1. Faça logon na conta de administrador (consulte *Logon na conta de administrador, página 20*).
2. Na área de trabalho, abra a pasta **Ferramentas** e clique duas vezes no atalho ASUS Inband Tool.
   O aplicativo será inicializado.
3. Use as credenciais padrão para fazer login:

– Conta: **admin**
– Senha: **admin**

4. Após o primeiro login, você terá que alterar essa senha inicial.
   Informe uma nova senha e confirme-a.
   Guarde a sua nova senha em um local seguro.
   Considere os seguintes requisitos para a senha:

– As senhas devem ter, no mínimo, 14 caracteres.
– As senhas devem conter pelo menos uma letra maiúscula.
– As senhas devem conter pelo menos uma letra minúscula.
– As senhas devem conter pelo menos um caractere especial.
– As senhas devem conter pelo menos um número.

5. Depois de confirmar a nova senha, a página **Painel** será exibida e apresentará o status geral do sistema.
6. No painel **MENU** do lado esquerdo, é possível selecionar as respectivas páginas para receber informações detalhadas a respeito do status de integridade do sistema.
7. No item de menu **SNMP** , é possível definir usuários SNMP e destinos SNMP.
8. Na página **Relatório**, é possível gerar um relatório que contenha as informações adequadas que você escolheu.

7.2.2 Monitoramento do sistema usando a interface da Web BMC

A unidade DIVAR IP all-in-one 7000 possui uma porta BMC dedicada na parte traseira.
Cada unidade DIVAR IP all-in-one 7000 é fornecida com o nome de usuário padrão da BMC **admin** e uma senha inicial da BMC. A senha inicial da BMC é exclusiva para cada unidade. Você pode encontrá-la na etiqueta na parte traseira da unidade, abaixo da porta BMC.
Após o primeiro login na interface web BMC, você terá que alterar essa senha inicial. Guarde a nova senha em um local seguro.
Observe os seguintes requisitos de senha:

– As senhas devem ter, no mínimo, 14 caracteres.
– As senhas devem conter pelo menos uma letra maiúscula.
– As senhas devem conter pelo menos uma letra minúscula.
– As senhas devem conter pelo menos um caractere especial.
– As senhas devem conter pelo menos um número.

Aviso!
Por razões de segurança, nunca conecte o dispositivo em uma rede pública por meio da porta BMC.

Definição das configurações da BMC

Para definir as configurações da BMC:

1. Ligue a unidade e pressione Del para entrar na configuração do BIOS.

Aviso!
Senha BIOS
A senha inicial do BIOS é exclusiva para cada unidade. Você pode encontrá-la na etiqueta na parte traseira da unidade. A Bosch recomenda veementemente alterar essa senha inicial. Guarde a nova senha em um local seguro.
Observe os seguintes requisitos de senha:
- As senhas devem ter, no mínimo, 14 caracteres.
- As senhas devem conter pelo menos uma letra maiúscula.
- As senhas devem conter pelo menos uma letra minúscula.
- As senhas devem conter pelo menos um caractere especial.
- As senhas devem conter pelo menos um número.

2. Na configuração do BIOS, navegue até a guia **Server Mgmt**.
3. Selecione a opção **BMC Network Configuration** e pressione Enter.
4. Na próxima caixa de diálogo, selecione a opção **Configuration Address source** e pressione Enter.
   A caixa de diálogo **Configuration Address source** é exibida.
5. Na caixa de diálogo **Configuration Address source**, selecione a opção desejada de como o endereço BMC deve ser configurado e pressione Enter.
6. Defina os parâmetros de configuração de rede desejados.
7. Pressione F4 e Enter para salvar e sair.
   A unidade DIVAR IP all-in-one 7000 é reiniciada.

Operação remota utilizando a interface BMC iKVM

Por padrão, os dispositivos DIVAR IP all-in-one 7000 devem funcionar com um ou dois monitores locais, conectados às interfaces HDMI na parte traseira da unidade
Se não houver nenhum monitor local conectado às interfaces HDMI, a unidade poderá ser controlada remotamente pela interface BMC iKVM.

Para possibilitar o controle remoto do sistema:

1. Garanta que não haja nenhum monitor HDMI local conectado ao sistema.
2. Faça login na interface web BMC.
3. No painel de menus do lado esquerdo, escolha a página **Controle remoto**.
4. Clique no botão **Inicializar H5Viewer**.
   Uma janela será aberta, apresentando a saída do monitor do dispositivo DIVAR IP all-in-one 7000 e oferecendo controle ao mouse e ao teclado da máquina remota.

7.3 Substituição de um disco rígido com defeito e configuração de um novo disco rígido

Aviso!
A Bosch não se responsabiliza por perda de dados ou danos, nem falhas de sistema em unidades equipadas com discos rígidos não fornecidos pela Bosch. A Bosch não poderá fornecer suporte se discos rígidos não fornecidos pela Bosch forem consideradas a causa do problema. Para solucionar possíveis problemas de hardware, a Bosch exige que sejam instalados discos rígidos fornecidos pela Bosch.

7.3.1 Substituição de um disco rígido com defeito

Para substituir um disco rígido com defeito:

- Remova o disco rígido com defeito da unidade e instale o novo disco rígido.
  Consulte o capítulo *Instalação de um disco rígido SATA* no manual de instalação.

7.3.2 Recriação de RAID5 com o novo disco rígido

Recriação automática de RAID5

1. Na área de trabalho do DIVAR IP all-in-one, clique duas vezes no atalho **Launch LSA**.
   O aplicativo **LSI Storage Authority** será iniciado, e a página **Remote Server Discovery** será exibida.
2. Faça logon com as credenciais da conta de administrador **BVRAdmin**.
   Uma caixa de diálogo será exibida, mostrando que há um controlador, que possui um problema crítico.
3. No topo da página, clique em **Selecionar controlador**, depois selecione a barra **Controller ID:** para abrir as configurações do controlador.
   - Se ainda não removeu o disco rígido com defeito, ela será exibida em **Drives** > **Foreign Drives** > **Unconfigured Drives.**
   - Depois de remover o disco rígido com defeito e instalar o novo disco rígido, o sistema iniciará automaticamente a recriação de RAID5 com o novo disco rígido, e uma barra de progresso mostrará o andamento da recriação.
4. Após a conclusão da recriação, o ícone  será exibido.

Recriação manual de RAID5

Se a recriação de RAID5 no novo disco rígido não for iniciada automaticamente, faça o seguinte:

1. Na caixa de diálogo de configurações do controlador, em **Drives** > **Foreign Drives** > **Unconfigured Drives**, selecione o disco rígido com o status **Unconfigured Bad** e, no painel direito, selecione **Make Unconfigured Good**.
   Uma caixa de diálogo será exibida.

2. Marque a caixa de seleção **Confirm** e clique em **Yes, Make Unconfigured Good** para continuar.
   O sistema iniciará a recriação de RAID5 com o novo disco rígido.
3. Após a conclusão da recriação, o ícone  será exibido.

7.4 Coleta de arquivos de log do DIVAR IP System Manager

O aplicativo DIVAR IP System Manager inclui um script dedicado que simplifica a coleta de arquivos de log.

Para coletar arquivos de log do DIVAR IP System Manager:
1. Faça logon na conta de administrador (consulte Logon na conta de administrador).
2. No menu **Iniciar** do Windows, clique com o botão direito do mouse em **Export System Manager Logs** e execute o script como administrador.
   O script exportar os arquivos de log para a pasta `Documents\Bosch` e cria um arquivo ZIP com a seguinte estrutura de nomenclatura `SysMgrLogs-[date]_[time]`.
   Você pode usar esse arquivo ZIP para anexá-lo à descrição detalhada do erro.

7.5 Recuperação da unidade

Para recuperar a unidade:
1. Ligue a unidade e pressione F7 durante o autoteste de inicialização do BIOS para entrar no Windows PE.
   A caixa de diálogo **System Management Utility** é exibida.
2. Selecione uma das seguintes opções:
   - **System factory default**: esta opção formatará as partições de dados de vídeo e restaurará a partição do sistema operacional com a imagem padrão de fábrica. Esse processo vai levar alguns minutos.
   - **Full data overwrite and system factory default**: esta opção formatará as partições de dados de vídeo, substituirá completamente os dados existentes e restaurará a partição do sistema operacional com a imagem padrão de fábrica.
     Observação: este processo pode levar vários dias.
   - **OS system recovery only**: esta opção restaurará a partição do sistema operacional com a imagem padrão de fábrica e importará discos rígidos virtuais existentes de partições de dados de vídeo existentes.
     Esse processo vai levar vários minutos.

   Observação:
   A opção **OS system recovery only** não exclui as gravações de vídeo que são armazenadas em HDDs de dados. No entanto, ela substitui toda a partição do sistema operacional (incluindo as configurações do sistema de gerenciamento de vídeo) por uma configuração padrão. Para acessar as gravações em vídeo existentes após a recuperação, a configuração do sistema de gerenciamento de vídeo precisará ser exportada antes da recuperação do sistema e importada novamente depois.

Aviso!
Não desligue a unidade durante o processo. Isso danificará a mídia de recuperação.

3. Confirme a opção selecionada.
   O sistema inicia a formatação e o processo de recuperação da imagem.

4. Depois da conclusão do processo de recuperação, confirme a reinicialização do sistema.
   O sistema é reiniciado e as rotinas de instalação são executadas.
5. Depois da conclusão do processo, a tela de seleção de idioma do Windows é exibida.
6. Continue com a configuração inicial do sistema.

8 Informações adicionais

8.1 Documentação adicional e software do cliente

Para mais informações, download de software e documentação, acesse a página do produto correspondente no catálogo de produtos:
http://www.boschsecurity.com
O software mais recente e os pacotes de atualização disponíveis encontram-se na loja de downloads do Bosch Security and Safety Systems em:
https://downloadstore.boschsecurity.com/

8.2 Serviços de suporte e Bosch Academy

Suporte

Acesse nossos **serviços de suporte** em www.boschsecurity.com/xc/en/support/.

Bosch Building Technologies Academy

Visite o site da Bosch Building Technologies Academy e tenha acesso a **cursos de treinamento, tutoriais em vídeo** e **documentos**: www.boschsecurity.com/xc/en/support/training/

Bosch Security Systems B.V.
Torenallee 49
5617 BA Eindhoven
Netherlands
www.boschsecurity.com

Soluções prediais para uma vida melhor

202404171736