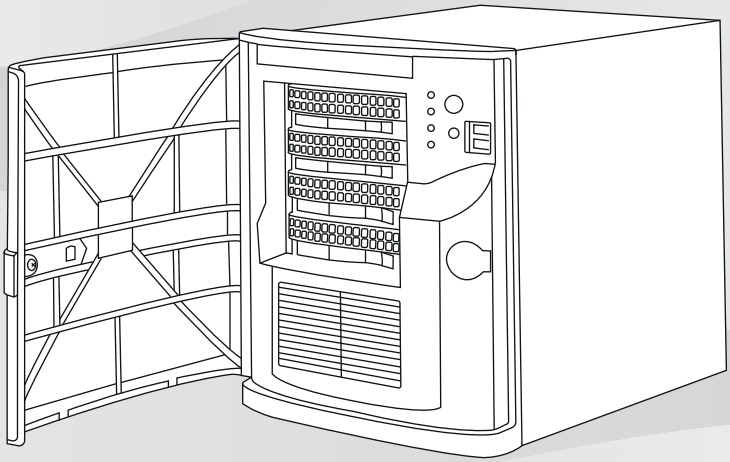
DIVAR IP all-in-one 5000

DIP-5240IG-00N | DIP-5244IG-4HD | DIP-5248IG-4HD | DIP-524CIG-4HD | DIP-5240GP-00N | DIP-5244GP-4HD | DIP-5248GP-4HD | DIP-524CGP-4HD



pt-BR Manual de instalação

Sumário

1	**Precauções de segurança**	**5**
1.1	Precauções gerais de segurança	5
1.2	Precauções elétricas de segurança	8
1.3	Precauções relativas à energia eletrostática	9
1.4	Precauções de operação	10
1.5	Precauções relativas à segurança de dados	11
2	**Visão geral do sistema**	**11**
2.1	Vistas do dispositivo	12
2.2	Elementos do painel de controle	15
3	**Instalação de uma unidade de disco rígido**	**17**
3.1	Remoção de um suporte de unidade de disco rígido de um compartimento de unidade de disco rígido	18
3.2	Instalação de uma unidade de disco rígido em um suporte de unidade de disco rígido	19
3.3	Instalação de um suporte de unidade de disco rígido em um compartimento de unidade de disco rígido	21
4	**Configuração do sistema**	**21**
4.1	Configurações padrão	21
4.2	Pré-requisitos	22
4.3	Modos de operação	22
4.4	Preparação de unidades de disco rígido para gravação de vídeos	23
4.5	Inicialização do aplicativo	24
4.5.1	Operação como sistema completo de gravação e gerenciamento de vídeos	25
4.5.2	Operação como sistema puro de gravação de vídeo	26
4.5.3	Operação como expansão de armazenamento iSCSI	26
4.6	Uso do assistente de configuração do BVMS	27
4.7	Adição de licenças adicionais	28
4.8	Uso do BVMS Operator Client	29
5	**Conexão remota com o sistema**	**29**
5.1	Proteção do sistema contra o acesso não autorizado	30
5.2	Configuração do encaminhamento de porta	30
5.3	Escolha de um cliente adequado	30

5.3.1 Conexão remota com o Operator Client 31
5.3.2 Conexão remota com o aplicativo Video Security 31
6 Manutenção 31
6.1 Monitoramento do sistema 31
6.2 Recuperação da unidade 32
6.3 Manutenção e reparo 33
7 Documentação adicional e software do cliente 34

1 Precauções de segurança

Observe as precauções de segurança neste capítulo.

1.1 Precauções gerais de segurança

Siga estas regras para garantir a segurança geral:

– Mantenha a área ao redor do sistema limpa e organizada.
– Coloque a tampa superior do chassi e todos os componentes do sistema que foram removidos longe do sistema ou em uma mesa para que não sejam pisados acidentalmente.
– Não use roupas soltas, como gravatas e mangas de camisas soltas, enquanto trabalha no sistema. Roupas soltas podem entrar em contato com circuitos elétricos ou ser sugadas por ventiladores de resfriamento.
– Remova joias ou objetos metálicos do corpo, os quais são excelentes condutores metálicos capazes de criar curtos-circuitos e causar danos se entrarem em contato com placas de circuito impresso ou áreas em que haja alimentação.

Advertência!

Interrupção da rede elétrica:

A tensão será aplicada assim que o plugue da rede for inserido na tomada da rede.

No entanto, para dispositivos com um interruptor de rede, o dispositivo só estará preparado para operação quando o interruptor da rede (LIGADO/DESLIGADO) estiver na posição LIGADO. Quando o plugue da rede for removido da tomada, a alimentação de energia ao dispositivo será completamente removida.

Advertência!

Removendo a caixa:

Para evitar choque elétrico, a caixa só deve ser removida por um técnico de manutenção qualificado.

Antes de remover a caixa, o plugue sempre deve ser removido da tomada da rede e permanecer desconectado durante a remoção da caixa. A manutenção só deve ser realizada por um técnico de manutenção qualificado. O usuário não deve realizar reparos.

Advertência!

Cabo de alimentação e adaptador de CA:

Ao instalar o produto, use os cabos de conexão fornecidos ou designados, os cabos de alimentação e os adaptadores de CA. O uso de qualquer outro cabo ou adaptador pode causar avaria ou incêndio. Leis voltadas ao uso de aparelhos elétricos e segurança de materiais proíbem o uso de cabos com certificação UL ou CSA (que apresentam UL/CSA no código) para qualquer dispositivo elétrico.

Advertência!

Bateria de lítio:

Baterias inseridas incorretamente podem causar uma explosão. Sempre troque as baterias descarregadas por baterias do mesmo tipo ou de tipo similar às recomendadas pelo fabricante.

Manuseie baterias usadas com cuidado. Não danifique a bateria de forma alguma. Uma bateria danificada pode liberar materiais perigosos no ambiente.

Descarte as baterias descarregadas de acordo com as instruções do fabricante ou as diretrizes locais.

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!
Dispositivo sensível do ponto de vista eletrostático:
Para evitar descargas eletrostáticas, as medidas de proteção CMOS/MOSFET devem ser realizadas corretamente.
Ao manusear circuitos impressos sensíveis do ponto de vista eletrostático, pulseiras antiestáticas aterradas devem ser usadas e deve-se observar as precauções de segurança relativas à energia eletrostática.

Aviso!
A instalação deve ser realizada somente por técnicos qualificados de atendimento ao cliente e de acordo com as regulamentações elétricas aplicáveis.

Aviso!
O sistema operacional inclui os mais recentes patches de segurança do Windows disponíveis no momento em que a imagem de software foi criada. Recomendamos instalar regularmente os patches de segurança mais recentes usando a função Windows Update.

Descarte
O seu produto Bosch foi desenvolvido e fabricado com materiais e componentes de alta qualidade que podem ser reutilizados. Este símbolo significa que os dispositivos elétricos e eletrônicos que atingiram o fim de sua vida útil devem ser descartados separadamente do lixo doméstico.

Na UE, já existem sistemas de coleta separados para produtos elétricos e eletrônicos usados. Descarte estes dispositivos no seu ponto de coleta de lixo local ou em um centro de reciclagem.

1.2 Precauções elétricas de segurança

Deve-se seguir as precauções de segurança elétrica básica para sua proteção e proteção do sistema contra danos:

- Esteja ciente dos locais do interruptor de ligar/desligar no chassi, bem como o interruptor de desligamento de emergência da sala, o interruptor de desconexão ou a tomada elétrica. Em caso de acidente elétrico, você poderá remover rapidamente a alimentação do sistema.
- Não trabalhe sozinho ao usar componentes de alta tensão.
- Desconecte os cabos de alimentação antes de instalar ou remover componentes do computador, incluindo o backplane.
- Ao desconectar a alimentação, primeiro é necessário desligar o sistema e depois desconectar os cabos de alimentação de todos os módulos de fonte de alimentação no sistema.
- Ao trabalhar perto de circuitos elétricos expostos, outra pessoa familiarizada com os controles de desligamento deve estar por perto para desligar a alimentação, se necessário.
- Use apenas uma mão ao trabalhar com equipamentos elétricos ligados. Isso evita o fechamento de circuito, o que causará choque elétrico. Tenha muito cuidado ao usar ferramentas metálicas, capazes de danificar facilmente qualquer componente elétrico ou placas de circuito ao contato.
- Os cabos da fonte de alimentação devem incluir um plugue de aterramento e devem ser conectados em tomadas elétricas aterradas. A unidade tem mais de um cabo da

fonte de alimentação. Desconecte ambos os cabos da fonte de alimentação antes da manutenção para evitar choque elétrico.

– Fusíveis soldados na placa principal substituíveis: os fusíveis PTC (Coeficiente positivo de temperatura) de redefinição automática na placa principal devem ser substituídos somente por técnicos de manutenção treinados. O novo fusível deve ser igual ou equivalente ao antigo. Entre em contato com o suporte técnico para obter detalhes e suporte.

Cuidado!

Bateria da placa principal: há risco de explosão caso a bateria integrada seja instalada de cabeça para baixo, o que inverterá suas polaridades. Essa bateria deve ser substituída somente pelo mesmo tipo ou por um tipo equivalente recomendado pelo fabricante (CR2032). Descarte as baterias usadas de acordo com as instruções do fabricante.

1.3 Precauções relativas à energia eletrostática

Descargas eletrostáticas (ESD) são geradas por dois objetos com cargas elétricas diferentes ao entrar em contato um com o outro. Uma descarga elétrica é criada para neutralizar essa diferença, podendo danificar componentes eletrônicos e placas de circuito impresso. As seguintes medidas costumam ser suficientes para neutralizar essa diferença antes que haja contato para proteger seu equipamento de ESD:

– Não use mantas projetadas para diminuir a descarga eletrostática como proteção contra choque elétrico. Em vez disso, use esteiras de borracha projetadas especificamente como isolantes elétricos.
– Use uma pulseira aterrada projetada para evitar descarga estática.

- Mantenha todos os componentes e as placas de circuito impresso (PCBs) em suas bolsas antiestáticas até serem usados.
- Toque em um objeto metálico aterrado antes de remover a placa da bolsa antiestática.
- Não deixe que componentes ou placas de circuito impresso entrem em contato com suas roupas, o que poderá reter uma carga mesmo que esteja usando uma pulseira.
- Manipule uma placa somente pelas bordas. Não toque nos componentes, chips periféricos, módulos de memória ou contatos.
- Ao manusear chips ou módulos, evite tocar nos pinos.
- Coloque a placa principal e os periféricos de volta em suas bolsas antiestáticas quando não utilizados.
- Para fins de aterramento, certifique-se de que o chassi do seu computador ofereça excelente condutividade entre a fonte de alimentação, a caixa, os fixadores de montagem e a placa principal.

1.4 Precauções de operação

Aviso!
A tampa do chassi deve estar encaixada quando o sistema estiver em operação para garantir o resfriamento adequado. Danos fora do escopo da garantia podem ocorrer no sistema se essa prática não for seguida.

Aviso!
Manuseie as baterias usadas com cuidado. Não danifique a bateria de forma alguma. Uma bateria danificada pode liberar materiais perigosos no ambiente. Não descarte uma bateria usada no lixo ou em aterros públicos. Cumpra as regulamentações definidas pela agência local de gestão de resíduos perigosos a fim de descartar sua bateria usada adequadamente.

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.

1.5 Precauções relativas à segurança de dados

Por questões de segurança de dados, observe o seguinte:

– O acesso físico ao sistema deve ser restrito apenas à equipe autorizada. É altamente recomendado colocar o sistema em uma área protegida por controle de acesso, a fim de impedir a manipulação física do sistema.
– A funcionalidade de atualização online do Windows ou os correspondentes patches lançados mensalmente para instalação online podem ser usados para instalar atualizações de segurança no SO.
– Recomenda-se fortemente limitar o acesso à rede local aos dispositivos confiáveis. Os detalhes estão descritos na Nota técnica *Autenticação de rede 802.1X* e no *Guia de segurança de dados e vídeo IP da Bosch*, disponíveis no catálogo de produtos online.
– Para obter acesso através de redes públicas, use apenas os canais de comunicação seguros (criptografados).

Veja também

– *Conexão remota com o sistema, página 29*

2 Visão geral do sistema

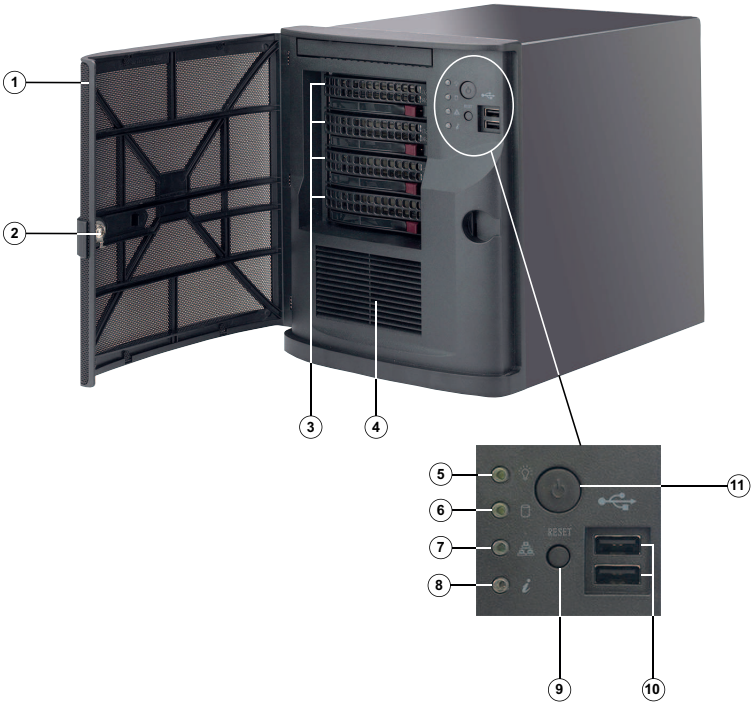
O sistema DIVAR IP all-in-one 5000 é uma solução de gravação, exibição e gerenciamento "tudo em um" e fácil de usar para sistemas de vigilância em rede.
Executando a solução completa BVMS (BVMS) e baseado no software Bosch Video Recording Manager (VRM) que inclui o Bosch Video Streaming Gateway (VSG) para integrar câmeras de

terceiros, DIVAR IP all-in-one 5000 é um dispositivo de armazenamento IP inteligente que elimina a necessidade de servidor de Gravador de vídeo em rede (NVR) e hardware de armazenamento separados.
O BVMS gerencia todo o vídeo e áudio IP e digital, além dos dados de segurança transmitidos via sua rede IP. Ele combina diretamente câmeras IP e codificadores, fornece gerenciamento de alarmes e eventos do sistema, monitora a integridade do sistema e gerencia usuários e prioridades.
O DIVAR IP all-in-one 5000 é uma unidade de minitorre com 4 compartimentos que apresenta unidades de disco rígido SATA substituíveis pela frente.
É fácil de instalar e operar. Todo o software do sistema é pré-instalado — criando um dispositivo de gerenciamento de vídeo pronto para uso.
DIVAR IP all-in-one 5000 utiliza o sistema operacional Windows Storage Server 2016.

2.1 Vistas do dispositivo

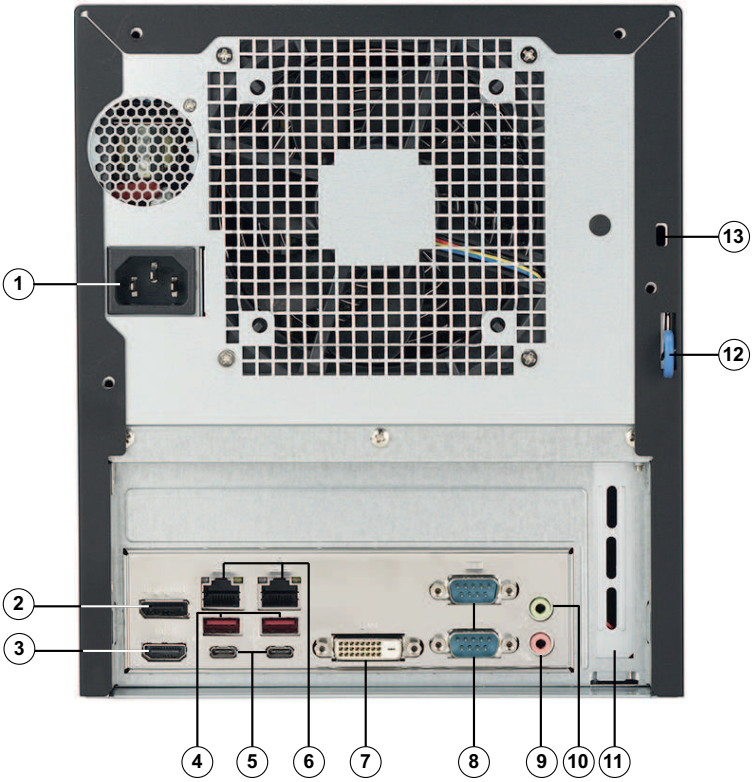
O sistema DIVAR IP all-in-one 5000 possui um chassi de minitorre compacto. Possui uma tampa frontal articulada que esconde as unidades de disco rígido e o painel de controle.
O painel de controle localizado na parte frontal apresenta botões de alimentação e LEDs de monitoramento de status.
Na parte traseira há várias portas de E/S.

Vista frontal



1	Tampa frontal	2	Trava da tampa frontal
3	4 x portas de unidade de disco rígido hot-swap (para unidades de disco rígido de 3,5 pol.)	4	Filtro de entrada de ar
5	LED de alimentação	6	LED de HDD (não usado)
7	LED de rede	8	LED de informação
9	Botão de reinicialização	10	2 x USB 2.0
11	Botão de ligar/desligar		

Vista traseira



1	Conexão da rede elétrica	2	Porta de vídeo
3	HDMI 2.0	4	2 x USB 3.1 (tipo A)
5	2 x USB 3.1 (tipo C)	6	2 x portas LAN (RJ45), agrupadas **Observação:** Não altere o modo de agrupamento!
7	Porta DVI-D	8	2 x portas COM
9	Entrada de microfone de áudio	10	Saída de linha de áudio

11	Placa de GPU adicional com 4x portas Mini Display (neste caso, as portas Mini Display devem ser usadas para a conexão de monitor). **Observação:** Disponível somente para DIP-5240GP-00N, DIP-5244GP-4HD, DIP-5248GP-4HD e DIP-524CGP-4HD.	12	Ferrolho de chassi traseiro (compatível com uma variedade de travas comumente disponíveis). **Observação:** As travas não estão inclusas.
13	Slot de segurança Kensington (para trava Kensington padrão). **Observação:** Trava Kensington não inclusa.		

2.2 Elementos do painel de controle

O painel de controle localizado na parte frontal do chassi apresenta botões de alimentação e LEDs de monitoramento de status.

Botões do painel de controle

Botão	Descrição
Alimentação	O botão de alimentação é usado para ligar ou desligar o sistema. **Observação:** Desligar a alimentação do sistema com esse botão remove a alimentação da rede, mas mantém a alimentação de espera. **Para remover toda a alimentação, desconecte o sistema antes de realizar tarefas de manutenção.**

Botão	Descrição
Reinicializar	O botão de reinicialização é usado para reinicializar o sistema.

LEDs do painel de controle

LED	Descrição	
Alimentação	Este LED indica que há alimentação para as unidades de fontes de alimentação do sistema. Este LED normalmente deve estar aceso quando o sistema estiver em operação.	
HDD	Este LED não é usado.	
Rede	Este LED indica atividade da rede quando estiver piscando.	
Informação	Este LED indica o status do sistema.	
	Status do sistema	**Descrição**
	Aceso continuamente e vermelho	Ocorreu uma condição de superaquecimento. (Isso pode ser causado pelo acúmulo de cabos.)
	Vermelho piscando (1 Hz)	Falha da ventoinha: verifique se a ventoinha está inoperante.

LED	Descrição	
	Vermelho piscando (0,25 Hz)	Falha da alimentação: verifique se a fonte de alimentação está inoperante.
	Azul sólido	A UID local foi ativada. Use essa função para localizar a unidade em um ambiente de racks.
	Azul piscando (300 ms)	A UID remota foi ativada. Use essa função para localizar a unidade de uma localização remota.

3 Instalação de uma unidade de disco rígido

O sistema DIVAR IP all-in-one 5000 possui quatro unidades de disco rígido substituíveis pela frente. As unidades de disco rígido são montadas em suportes para simplificar sua instalação e remoção do chassi. Esses suportes de unidades de disco rígido também ajudam a promover um fluxo de ar adequado para os compartimentos das unidades de disco rígido.

Procedimento

Para instalar uma unidade de disco rígido, é preciso realizar as seguintes etapas:

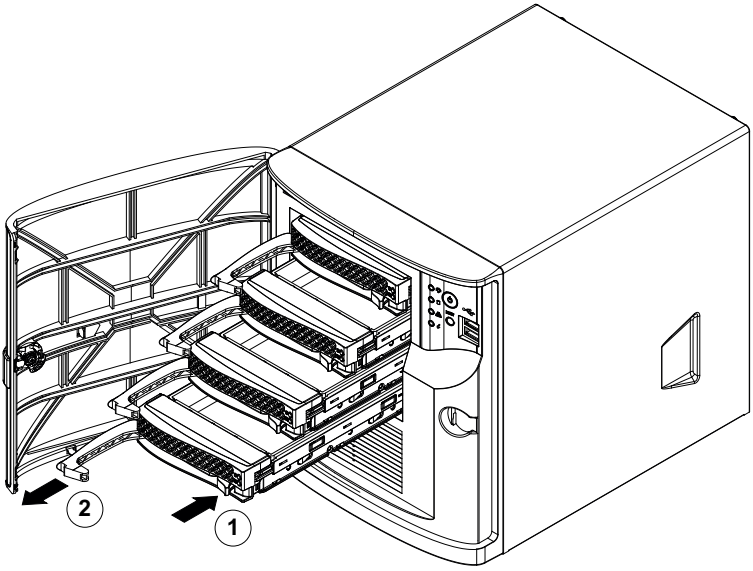
1. *Remoção de um suporte de unidade de disco rígido de um compartimento de unidade de disco rígido, página 18*
2. *Instalação de uma unidade de disco rígido em um suporte de unidade de disco rígido, página 19*
3. *Instalação de um suporte de unidade de disco rígido em um compartimento de unidade de disco rígido, página 21*

Aviso!
Revise os avisos e as precauções listadas neste manual antes de realizar trabalhos no chassi.

3.1 Remoção de um suporte de unidade de disco rígido de um compartimento de unidade de disco rígido

Para remover um suporte de unidade de disco rígido de um compartimento de unidade de disco rígido:

1. Destrave a tampa frontal e abra-a.
2. Pressione o botão de liberação à direita do suporte de unidade de disco rígido. Fazer isso estende a alça do suporte de unidade de disco rígido.
3. Use a alça para puxar o suporte de unidade de disco rígido para fora do chassi.



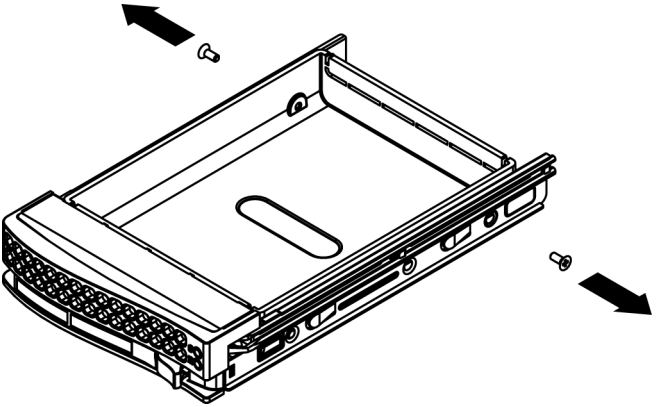
1	Botão de liberação	2	Alça do suporte de unidade de disco rígido

Aviso!
Não opere a unidade com os suportes de unidades de disco rígido removidos dos compartimentos.

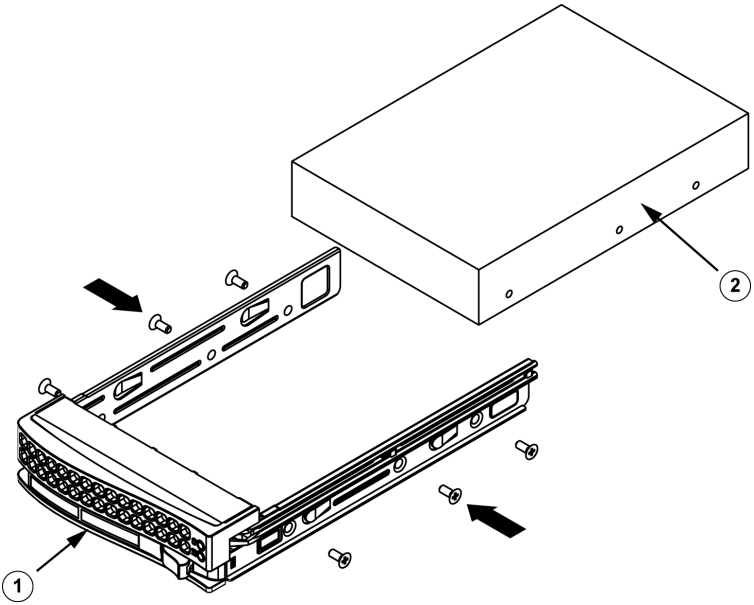
3.2 Instalação de uma unidade de disco rígido em um suporte de unidade de disco rígido

Para instalar uma unidade de disco rígido em um suporte de unidade de disco rígido:

1. Remova os parafusos que prendem a unidade falsa no suporte de unidade de disco rígido.



2. Remova a unidade falsa do suporte de unidade de disco rígido e coloque o suporte de unidade de disco rígido em uma superfície plana.
3. Deslize uma nova unidade de disco rígido no suporte de unidade de disco rígido com o lado da placa de circuito impresso voltado para baixo.
4. Alinhe os orifícios de montagem no suporte de unidade de disco rígido e na unidade de disco rígido.
5. Prenda a unidade de disco rígido no suporte com os seis parafusos.



1	Suporte da unidade de disco rígido	2	Unidade de disco rígido SATA

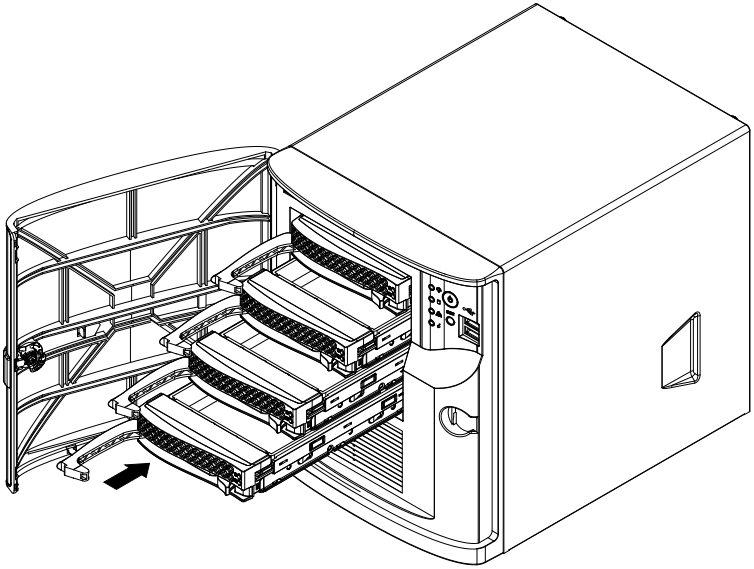
Aviso!

A Bosch recomenda usar as respectivas unidades de disco rígido da Bosch. As unidades de disco rígido são componentes críticos e, por isso, são selecionadas cuidadosamente pela Bosch com base nos índices de falhas disponíveis. As unidades de disco rígido não entregues pela Bosch não são compatíveis. Para obter mais informações sobre as unidades de disco rígido compatíveis, consulte a ficha técnica no Catálogo de produtos online da Bosch em:
www.boschsecurity.com

3.3 Instalação de um suporte de unidade de disco rígido em um compartimento de unidade de disco rígido

Para instalar um suporte de unidade de disco rígido em um compartimento de unidade de disco rígido:

1. Insira o suporte de unidade de disco rígido horizontalmente no compartimento de unidade de disco rígido, orientando o suporte de unidade de disco rígido para que o botão de liberação fique à direita.
2. Pressione o suporte de unidade de disco rígido no compartimento até que a alça se retraia e o suporte de unidade de disco rígido encaixe na posição travada.
3. Feche e trave a tampa frontal.



4 Configuração do sistema

4.1 Configurações padrão

Os sistemas DIVAR IP são fornecidos com um Assistente de configuração pré-instalado de fábrica.

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 conta de administrador
– Usuário: BVRAdmin
– Senha: WSS4Bosch

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.
– Determine se a instalação inicial está em uma rede DHCP. Se esse não for o caso, será necessário atribuir endereços IP válidos aos dispositivos de vídeo. Consulte o administrador de TI local para obter um intervalo de endereços IP válidos a ser usado com o DIVAR IP e dispositivos associados.
– As configurações iSCSI padrão são otimizadas para o uso com VRM.

4.3 Modos de operação

O sistema DIVAR IP pode operar em três modos diferentes:
– Sistema completo de gravação e gerenciamento de vídeos, utilizando os principais componentes e serviços do BVMS e do VRM: este modo habilita recursos avançados de gerenciamento de vídeos, como tratamento de eventos e alarmes.

– Sistema puro de gravação de vídeo, utilizando os principais componentes e serviços do VRM.
– Expansão de armazenamento iSCSI para um sistema BVMS ou VRM, executada em um hardware diferente.

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.

4.4 Preparação de unidades de disco rígido para gravação de vídeos

Os sistemas pré-equipados com unidades de disco rígido de fábrica são fornecidos prontos para gravar.
As unidades de disco rígido que foram adicionadas a um sistema vazio precisam ser preparadas (formatadas) antes de usá-las para a gravação de vídeo.

Para formatar uma unidade de disco rígido, você tem as seguintes opções:

– Realizar a configuração de fábrica inicial: consulte *Recuperação da unidade, página 32*.
– Executar o script de formatação.

Execução do script de formatação

Para executar o script de formatação, é necessário fazer login na conta de administrador (BVRAdmin).

1. Inicialize o sistema.
2. Na tela padrão do BVMS, pressione CTRL+ALT+DEL.
3. Com a tecla SHIFT pressionada, clique em **Alternar usuário** e mantenha SHIFT pressionado durante cinco segundos.
4. Insira o nome de usuário e a senha de administrador.
5. Na Área de Trabalho, na pasta **Ferramentas**, clique com o botão direito do mouse no script **Format_data_hard_drives** e clique em **Executar como administrador**.

6. Siga as instruções.
7. Depois de formatar você pode adicionar o armazenamento à configuração de gerenciamento de vídeo.

Aviso!
Formatar uma unidade de disco rígido exclui todos os dados existentes na unidade de disco rígido.

4.5 Inicialização do aplicativo

O aplicativo fornece uma solução fácil de instalar e intuitiva de usar para sistemas de vigilância em rede.

Para iniciar o aplicativo:

1. Conecte a unidade e as câmeras à rede.
2. Ligue a unidade.
   O processo de configuração do Windows Storage Server 2016 é iniciado.
3. Selecione o idioma apropriado para a instalação e clique em **Próximo**.
4. Nas listas **País ou região**, **Hora e moeda** e **Layout do teclado**, clique nos itens apropriados e clique em **Próximo**.
   São exibidos o Microsoft Software License Terms e o EULA (Contrato de licença do usuário final).
5. Aceite os termos da licença e clique em **Iniciar**. O Windows é reiniciado.
6. Após o reinício, pressione CTR+ALT+DELETE. A página de logon do Windows é exibida.
7. Insira a senha padrão **WSS4Bosch**.
8. Depois de inserir a senha, é exibida uma mensagem informando que a senha deve ser alterada antes do primeiro login. Para confirmar, clique em **OK**.
9. Altere a senha.
   Uma série de scripts realiza tarefas importantes de configuração. Isso pode levar alguns minutos. Não desligue o computador.
   A tela padrão do BVMS é exibida.

Agora você pode decidir em qual modo deseja operar o sistema:

– *Operação como sistema completo de gravação e gerenciamento de vídeos, página 25*
– *Operação como sistema puro de gravação de vídeo, página 26*
– *Operação como expansão de armazenamento iSCSI, página 26*

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!
Recomendamos enfaticamente não alterar as configurações do sistema operacional. Alterações nas configurações do sistema operacional podem resultar no mau funcionamento do sistema.

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

4.5.1 Operação como sistema completo de gravação e gerenciamento de vídeos

Para operar o sistema DIVAR IP como sistema completo de gravação e gerenciamento de vídeos:

1. Na tela padrão do BVMS, clique duas vezes no ícone do Config Wizard do BVMS para iniciar o Config Wizard. A página **Welcome** é exibida.
2. Configure o sistema usando o Config Wizard.

Veja também

– *Uso do assistente de configuração do BVMS, página 27*

4.5.2 Operação como sistema puro de gravação de vídeo

Para operar o sistema DIVAR IP como sistema puro de gravação de vídeo, é necessário fazer login na conta de administrador (BVRAdmin) a fim de executar as etapas de configuração necessárias.

1. Na tela padrão do BVMS, pressione CTRL+ALT+DEL.
2. Com a tecla SHIFT pressionada, clique em **Alternar usuário** e mantenha SHIFT pressionado durante cinco segundos.
3. Insira o nome de usuário e a senha de administrador.
4. Na Área de Trabalho, na pasta **Ferramentas**, clique com o botão direito do mouse no script **Disable_BVMS** e clique em **Executar como administrador**.
5. Configure o Video Recording Manager (VRM) a partir de um sistema externo usando o BVMS Configuration Client ou o Configuration Manager.

4.5.3 Operação como expansão de armazenamento iSCSI

Para operar o sistema DIVAR IP como uma expansão de armazenamento iSCSI, é necessário fazer login na conta de administrador (BVRAdmin) a fim de executar as etapas de configuração necessárias.

1. Na tela padrão do BVMS, pressione CTRL+ALT+DEL.
2. Com a tecla SHIFT pressionada, clique em **Alternar usuário** e mantenha SHIFT pressionado durante cinco segundos.
3. Insira o nome de usuário e a senha de administrador.
4. Na Área de Trabalho, na pasta **Ferramentas**, clique com o botão direito do mouse no script **Disable_BVMS_and_VRM** e clique em **Executar como administrador**.
5. 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.

4.6 Uso do assistente de configuração do BVMS

O uso pretendido do Config Wizard é a rápida e fácil configuração de um sistema menor. O Config Wizard ajuda você a alcançar um sistema configurado, incluindo VRM, sistema iSCSI, câmeras, perfis de gravação e grupos de usuários.
Os grupos de usuários e suas permissões são configurados automaticamente. É possível adicionar ou remover usuários e definir senhas.
Config Wizard consegue acessar o Management Server somente no computador local.
Você pode salvar uma configuração ativada para fins de backup e importar essa configuração posteriormente. Você pode alterar essa configuração importada após a importação.
O Config Wizard adiciona o VRM local automaticamente.

Restrições:
As tarefas a seguir não podem ser feitas com o Config Wizard. Em vez disso, use o Configuration Client do BVMS.
- ajuste de cronogramas
- configuração de sistemas sem ou com vários Video Recording Manager
- configuração de dispositivos de armazenamento externo
- adição de Video Streaming Gateway
- todas as configurações avançadas além da configuração básica (mapas ou alarmes, por exemplo)

Para obter uma configuração rápida usando o Config Wizard:
1. Na tela padrão do BVMS, clique duas vezes no ícone do Config Wizard. A página **Welcome** é exibida.
2. Siga o assistente e observe as instruções na tela.

Aviso!
Para as tarefas que não puderem ser feitas com o Config Wizard e para obter informações detalhadas sobre o próprio Config Wizard, consulte o manual do BVMS disponível no catálogo de produtos online.

Veja também

– *Documentação adicional e software do cliente, página 34*

4.7 Adição de licenças adicionais

Você pode adicionar licenças adicionais usando o Configuration Client.

Para ativar o software:

1. Inicie o Configuration Client.
2. No menu **Ferramentas**, clique em **Gestor de Licenças...**.
   A caixa de diálogo **Gestor de Licenças** é exibida.
3. Clique nas caixas de seleção do pacote de software, dos recursos e das expansões que deseja ativar. Para as expansões, insira o número de licenças.
   Se você recebeu um arquivo de Informações de pacote, clique em **Importar Infor. do Pacote** para importá-lo.
4. Clique em **Activar**.
   A caixa de diálogo **Licença Activação** é exibida.
5. Anote a assinatura do computador ou copie e cole-a em um arquivo de texto.
6. Em um computador com acesso à Internet, insira o seguinte URL no seu navegador:
   https://activation.boschsecurity.com
   Caso você não tenha uma conta para acessar o Centro de ativação de licenças da Bosch, crie uma nova conta (recomendado) ou clique no link para ativar uma nova licença sem fazer login. Se você criar uma conta e fizer login antes de ativar, o License Manager manterá um registro de suas ativações. Depois, isso poderá ser revisado a qualquer momento.
   Siga as instruções para obter a Chave de ativação de licença.
7. Volte para o software BVMS. Na caixa de diálogo **Licença Activação**, digite a Chave de ativação de licença obtida no License Manager e clique em **Activar**.
   O pacote de software é ativado.

4.8 Uso do BVMS Operator Client

Use o BVMS Operator Client para verificar as funcionalidades ao vivo, gravação e reprodução do DIVAR IP.

Para verificar a funcionalidade de imagem ao vivo no Operator Client

1. Na tela padrão do BVMS, clique duas vezes no ícone do Operator Client . O aplicativo é iniciado.
2. Insira o seguinte e clique em **OK**.
   Nome do usuário: admin
   Senha: não é necessária (caso não tenha sido definida no assistente)
   Conexão: 127.0.0.1
3. Clique no ícone de imagem ao vivo. A Árvore lógica com as câmeras é exibida.
4. Selecione uma câmera e arraste-a para uma janela de imagens. A imagem da câmera será exibida se a câmera estiver atribuída corretamente.
   Observação:
   As câmeras na janela de imagens com um ponto vermelho no ícone da câmera são exibidas ao vivo.

Para verificar a funcionalidade de gravação no Operator Client

- As câmeras na Árvore lógica com um ponto vermelho no ícone da câmera estão gravando.

Para verificar a funcionalidade de reprodução no Operator Client

- A linha do tempo se move se a câmera estiver sendo visualizada no modo de reprodução.

Para realizar funcionalidades adicionais, consulte o manual do BVMS disponível no catálogo de produtos online.

5 Conexão remota com o sistema

Esta seção descreve as etapas necessárias para acessar o sistema DIVAR IP pela Internet.

5.1 Proteção do sistema contra o acesso não autorizado

Para proteger o sistema contra o acesso não autorizado, recomendamos que você 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.

5.2 Configuração do encaminhamento de porta

Para acessar um sistema DIVAR IP pela Internet por meio de um roteador NAT/PAT adequado, o encaminhamento de porta deve ser configurado no sistema DIVAR IP 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 de túnel SSH usando o BVMS Operator Client.
  - porta 443 para acesso HTTPS ao VRM usando o Video Security Client ou o Video Security App.

O sistema DIVAR IP agora está acessível pela Internet.

5.3 Escolha de um cliente adequado

Este capítulo descreve as maneiras para permitir conexão remota a um sistema DIVAR IP pela Internet.

Há duas maneiras de realizar uma conexão remota:

- *Conexão remota com o Operator Client, página 31*.
- *Conexão remota com o aplicativo Video Security, página 31*.

Aviso!
Use o BVMS Operator Client ou o Video Security App somente na versão que corresponda ao DIVAR IP. Outros clientes ou softwares de aplicativos podem funcionar, mas não são compatíveis.

5.3.1 Conexão remota com o Operator Client

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: insira a senha do usuário
   Conexão: ssh://[public-IP-address-of-DIVAR-IP_all-in-one]:5322

5.3.2 Conexão remota com o aplicativo Video Security

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: insira a senha do usuário

6 Manutenção

6.1 Monitoramento do sistema

O sistema oferece ferramentas para o monitoramento da integridade.
Para ativar a funcionalidade de monitoramento, é necessário fazer login na conta de administrador (BVRAdmin).

1. Na tela padrão do BVMS, pressione CTRL+ALT+DEL.
2. Com a tecla SHIFT pressionada, clique em **Alternar usuário** e mantenha SHIFT pressionado durante cinco segundos.
3. Insira o nome de usuário e a senha.
4. Na Área de Trabalho, na pasta **Ferramentas**, clique com o botão direito do mouse no script **Enable_SuperDoctor_5_Service** e clique em **Executar como administrador**.
5. Clique duas vezes no ícone **SuperDoctor 5 Web** na mesma pasta.
6. Faça login na interface da web usando as seguintes credenciais padrão:
   Nome do usuário: ADMIN
   Senha: ADMIN
7. Clique na guia **Configuração**, clique em **Configurações de senha** e altere a senha padrão.
8. Clique na guia **Configuração** e clique em **Configuração de alerta**.
9. Ative o recurso **Interceptação de SNMP** e especifique o endereço IP do receptor para interceptações de SNMP.

6.2 Recuperação da unidade

O procedimento a seguir descreve como restaurar a imagem padrão de fábrica.

Para restaurar a unidade para a imagem padrão de fábrica:

1. Inicie a unidade e pressione **F7** durante o autoteste de inicialização do BIOS.
   O menu de recuperação é exibido.
2. Selecione uma das seguintes opções:
   – **Configuração de fábrica inicial:** restaura para a imagem padrão de fábrica e exclui todos os dados nos HDDs.
     ou

– **Recuperação do sistema (voltar para os Padrões de fábrica):** restaura para a imagem padrão de fábrica; os dados nos HDDs não serão excluídos.

Observação:
embora a opção de **Recuperação do sistema** não exclua as gravações em vídeo armazenadas nos HDDs de dados, ainda assim substitui toda a partição do SO (incluindo as configurações de VMS) por uma configuração padrão. Para acessar as gravações em vídeo existentes após a recuperação, a configuração do VMS precisa 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. A unidade é iniciada a partir da Mídia de recuperação. Se a configuração for bem-sucedida, pressione **Sim** para reiniciar o sistema.
4. O Windows realiza a configuração inicial do sistema operacional. A unidade é reiniciada após a conclusão da configuração pelo Windows.
5. Após o reinício da unidade, as configurações de fábrica são instaladas.

6.3 Manutenção e reparo

O sistema de armazenamento tem garantia de 3 anos. Os problemas serão tratados de acordo com as diretrizes do Serviço e suporte da Bosch.
O equipamento de armazenamento é enviado com um contrato original de Serviço e Suporte do fabricante.
O Suporte técnico da Bosch é o único ponto de contato em caso de falha, mas as obrigações relacionadas a serviço e suporte são cumpridas pelo fabricante ou um parceiro.

Para permitir que a organização de Serviço e suporte do fabricante atenda aos Níveis de serviço definidos, o sistema deverá ser registrado novamente. Caso contrário, o nível de serviço definido não poderá ser fornecido, mas somente com base no "melhor esforço".
Uma descrição sobre quais informações são necessárias e onde enviá-las está inclusa fisicamente em cada envio. A descrição também está disponível eletronicamente no catálogo de produtos online da Bosch.

7 Documentação adicional e software do cliente

Para obter mais informações, download de software e documentação, acesse www.boschsecurity.com e vá até a página do produto correspondente.

Bosch Security Systems B.V.
Torenallee 49
5617 BA Eindhoven
Netherlands
www.boschsecurity.com
© Bosch Security Systems B.V., 2019