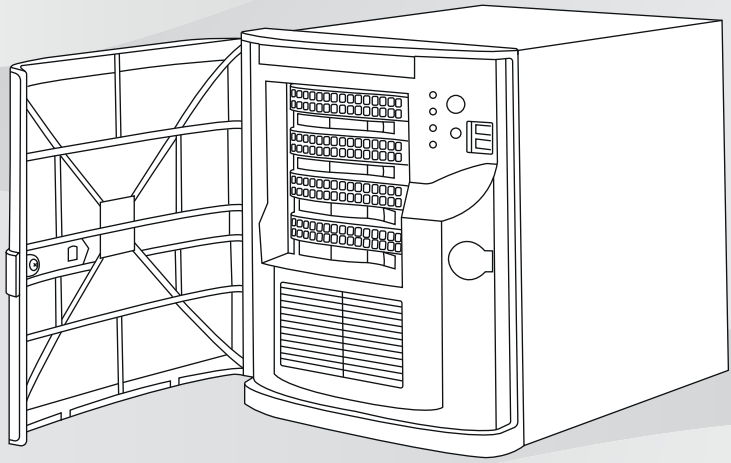
DIVAR IP all-in-one 5000

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



de Installationshandbuch

Inhaltsverzeichnis

1 Sicherheitsvorkehrungen

Beachten Sie die Sicherheitshinweise in diesem Kapitel.

1.1 Allgemeine Sicherheitsvorkehrungen

Beachten Sie diese Regeln, um die allgemeine Sicherheit zu gewährleisten:

- Halten Sie den Bereich um das System sauber und ordentlich.
- Legen Sie die obere Gehäuseabdeckung sowie ausgebaute Systemkomponenten zum Schutz vor Trittschäden in sicherer Entfernung zum System oder auf einem Tisch ab.
- Tragen Sie bei Arbeiten am System keine losen Kleidungsstücke, z. B. Krawatten oder aufgeknöpfte Hemdsärmel. Sie können mit Stromkreisen in Berührung kommen oder von einem Lüfter angesaugt werden.
- Legen Sie Schmuck oder sonstige am Körper getragene Metallgegenstände ab. Diese stellen sehr gute metallische Leiter dar, die bei Berührung mit Leiterplatten oder Strom führenden Teilen zu einem Kurzschluss und damit zu Verletzungen führen können.

Warnung!
Unterbrechung der Stromversorgung:
Spannung liegt an, sobald der Netzstecker in die Steckdose gesteckt wird.
Geräte mit einem Netzschalter sind jedoch nur betriebsbereit, wenn der Netzschalter (EIN/AUS) auf EIN steht. Wenn das Netzkabel aus der Steckdose gezogen wird, ist die Spannungszuführung zum Gerät vollkommen unterbrochen.

Warnung!

Abnehmen des Gehäuses:

Zur Vermeidung eines elektrischen Schlags darf das Gehäuse nur von qualifiziertem Wartungspersonal abgenommen werden. Vor dem Abnehmen des Gehäuses muss stets der Stecker aus der Netzsteckdose gezogen werden und bei abgenommenem Gehäuse abgezogen bleiben. Lassen Sie Wartungsarbeiten nur von qualifiziertem Wartungspersonal ausführen. Der Benutzer darf keine Reparaturen durchführen.

Warnung!

Netzkabel und AC-Adapter:

Verwenden Sie bei der Montage des Produkts die im Lieferumfang enthaltenen Verbindungskabel, Netzkabel und AC-Adapter. Die Verwendung anderer Kabel und Adapter könnte eine Störung oder einen Brand verursachen. Das Gesetz über die Sicherheit von Elektrogeräten und elektrischem Material unterbindet die Verwendung von UL- oder CSA-zertifizierten Kabeln (Kabel mit „UL/CSA“ im Code) für andere elektrische Geräte.

Warnung!

Lithium-Batterie:

Falsch eingelegte Batterien können eine Explosion verursachen. Tauschen Sie leere Batterien stets mit Batterien des gleichen oder eines vom Hersteller empfohlenen gleichwertigen Typs aus.

Gebrauchte Batterien müssen mit Sorgfalt behandelt werden. Die Batterien dürfen nicht beschädigt werden. Beschädigte Batterien können umweltgefährdende Stoffe freisetzen. Entsorgen Sie leere Batterien entsprechend den Herstelleranweisungen oder örtlichen Richtlinien.

Warnung!
Die Handhabung von in diesem Produkt verwendeten bleihaltigen Lötmetallen kann zu einer Bleiexposition führen. Diese Chemikalie wird im US-Bundesstaat Kalifornien als Ursache für Geburtsfehler oder Einschränkung der Fortpflanzungsfähigkeit eingestuft.

Hinweis!
Elektrostatisch gefährdetes Bauelement:
Um elektrostatische Entladungen zu vermeiden, sind die CMOS/MOSFET-Schutzmaßnahmen ordnungsgemäß auszuführen.
Bei der Handhabung elektrostatisch gefährdeter Leiterplatten sind geerdete Antistatikbänder zu tragen und die ESD-Sicherheitsvorkehrungen ordnungsgemäß einzuhalten.

Hinweis!
Die Installation sollte nur von qualifiziertem Kundendienstpersonal gemäß den jeweils zutreffenden elektrotechnischen Vorschriften ausgeführt werden.

Hinweis!
Das Betriebssystem enthält die neuesten Windows-Sicherheitspatches, die zu dem Zeitpunkt verfügbar waren, als das Software-Image erstellt wurde. Wir empfehlen, regelmäßig die neuesten Sicherheitspatches mit der Windows Update-Funktion zu installieren.

Entsorgung
Bei der Entwicklung und Fertigung Ihres Bosch Produkts kamen hochwertige Materialien und Bauteile zum Einsatz, die wiederverwendet werden können.
Dieses Symbol weist darauf hin, dass Elektro- und Elektronikgeräte am Ende ihrer Lebensdauer getrennt vom Hausmüll gesammelt und entsorgt werden müssen.

In der EU gibt es verschiedene Sammelsysteme für elektrische und elektronische Altgeräte. Bitte entsorgen Sie diese Geräte bei Ihrem kommunalen Abfallsammel-/Recyclingzentrum.

1.2 Elektrische Sicherheitsvorkehrungen

Befolgen Sie zum persönlichen Schutz sowie zum Schutz des Systems grundlegende elektrische Sicherheitsvorkehrungen:

- Merken Sie sich, wo sich am Gehäuse der Netzschalter sowie im Raum der Notausschalter, der Trennschalter oder die Steckdose befinden. Dadurch können Sie das System bei einem Stromunfall schnell von der Stromversorgung trennen.
- Arbeiten Sie nie alleine an Hochspannungsbauteilen.
- Trennen Sie vor der Installation oder dem Entfernen von Komponenten (einschließlich der Rückwandplatine) die Stromkabel vom Computer.
- Bevor die Stromversorgung unterbrochen wird, schalten Sie zunächst das System aus, und ziehen Sie anschließend die Netzkabel aller Stromversorgungsmodule des Systems aus der Steckdose.
- Bei der Arbeit an freiliegenden Stromkreisen sollte eine weitere Person anwesend sein, die mit den Abschaltvorrichtungen vertraut ist und bei Bedarf die Stromversorgung unterbrechen kann.
- Arbeiten Sie nur mit einer Hand an eingeschalteten elektrischen Geräten. Dadurch wird vermieden, dass sich ein Stromkreis schließt, der zu einem elektrischen Schlag führt. Seien Sie mit Metallwerkzeugen äußerst vorsichtig, da sie elektrische Bauteile oder Platinen bei Berührung beschädigen können.
- Die Netzkabel müssen über einen Schutzkontaktstecker verfügen und an geerdete Steckdosen angeschlossen werden. Das Gerät verfügt über mehr als ein Netzkabel. Ziehen Sie vor Wartungsarbeiten beide Netzkabel ab, um einen elektrischen Schlag zu vermeiden.

– Auswechselbare Einlötsicherungen auf dem Mainboard: Die selbstrückstellenden PTC-Sicherungen (Kaltleiter) auf dem Mainboard dürfen nur von geschulten Servicemitarbeitern ausgewechselt werden. Die neue Sicherung muss den gleichen oder einen gleichwertigen Typ wie die vorherige aufweisen. Für weitere Informationen und Unterstützung wenden Sie sich an den technischen Kundendienst.

Vorsicht!

Mainboard-Batterie: Wenn die Onboard-Batterie mit umgekehrter Polarität eingesetzt wird, kann sie explodieren. Tauschen Sie diese Batterie nur gegen Batterien desselben oder eines vom Hersteller empfohlenen gleichwertigen Typs aus (CR2032). Entsorgen Sie leere Batterien entsprechend den Herstelleranweisungen.

1.3 ESD-Vorkehrungen

Wenn sich zwei Gegenstände mit unterschiedlicher elektrischer Ladung berühren, treten elektrostatische Entladungen (ESD) auf. Der Ladungsunterschied wird durch die Entladung ausgeglichen. Diese kann zu Schäden an elektronischen Bauteilen und Leiterplatten führen. Um die Geräte vor ESD zu schützen, können Ladungsunterschiede durch die folgenden Maßnahmen ausreichend ausgeglichen werden:

– Verwenden Sie zum Schutz vor elektrischen Schlägen keine Matten, die zur Verringerung elektrostatischer Entladungen dienen. Verwenden Sie stattdessen spezielle Matten, die zur elektrischen Isolierung dienen.
– Tragen Sie ein geerdetes Antistatikband.
– Entnehmen Sie Komponenten und Leiterplatten (PCBs) erst bei Gebrauch aus ihren Antistatikhüllen.
– Berühren Sie einen geerdeten Metallgegenstand, bevor Sie eine Leiterplatte aus der Antistatikhülle entnehmen.

- Lassen Sie Komponenten oder Leiterplatten nicht mit Ihrer Kleidung in Berührung kommen. Diese kann selbst beim Tragen eines Antistatikbandes eine Restladung enthalten.
- Fassen Sie Platinen ausschließlich am Rand an. Berühren Sie nicht ihre Komponenten, Peripherieschaltkreise, Speichermodule oder Kontakte.
- Berühren Sie nicht die Anschlussstifte von integrierten Schaltkreisen oder Modulen.
- Legen Sie das Mainboard und die Peripheriemodule bei Nichtgebrauch wieder in die zugehörigen Antistatikhüllen.
- Achten Sie aus Gründen der Erdung darauf, dass bei Ihrem Rechnergehäuse eine sehr gute Leitfähigkeit zwischen Stromversorgung, Gehäuse, Befestigungselementen und Mainboard besteht.

1.4 Sicherheitsvorkehrungen im Betrieb

Hinweis!
Die Gehäuseabdeckung muss bei Systembetrieb richtig angebracht sein, damit eine ausreichende Kühlung gewährleistet ist.
Wird diese Vorkehrung nicht streng beachtet, können am System Schäden entstehen, die nicht der Gewährleistung unterliegen.

Hinweis!
Gebrauchte Batterien müssen mit Sorgfalt gehandhabt werden. Die Batterien dürfen nicht beschädigt werden. Beschädigte Batterien können umweltgefährdende Stoffe freisetzen. Gebrauchte Batterien dürfen nicht im Hausmüll oder auf öffentlichen Deponien entsorgt werden. Zur ordnungsgemäßen Entsorgung von gebrauchten Batterien beachten Sie die Vorschriften Ihrer örtlichen Abfallwirtschaftsbehörde für Sondermüll.

Warnung!
Gehen Sie bei Wartung und Arbeit an der Rückwandplatine vorsichtig vor. Bei Betrieb des Systems steht die Rückwandplatine unter einer gefährlichen Spannung bzw. unter Strom. Berühren Sie die Rückwandplatine nicht mit Metallgegenständen, und stellen Sie sicher, dass keine Flachbandkabel die Rückwandplatine berühren.

1.5 Datensicherungsvorkehrungen

Beachten Sie aus Datensicherheitsgründen Folgendes:

- Nur autorisiertes Fachpersonal darf physischen Zugriff auf das System haben. Es wird dringend empfohlen, das System in einem Bereich mit Zutrittskontrolle zu platzieren, um physische Manipulationen am System zu vermeiden.
- Die Windows Update-Funktion oder die entsprechenden monatlichen Rollup-Patches für die Offline-Installation können zur Installation von BS-Sicherheitsupdates verwendet werden.
- Es wird nachdrücklich empfohlen, den Zugriff im lokalen Netzwerk auf vertrauenswürdige Geräte einzuschränken. Details finden Sie im technischen Hinweis *Netzwerkauthentifizierung – 802.1x* und im *Bosch IP-Video- und Datensicherheits-Handbuch* im Online-Produktkatalog.
- Verwenden Sie für den Zugriff über öffentliche Netzwerke nur sichere (verschlüsselte) Kommunikationskanäle.

Siehe auch

– *Fernverbindung mit dem System, Seite 30*

2 Systemüberblick

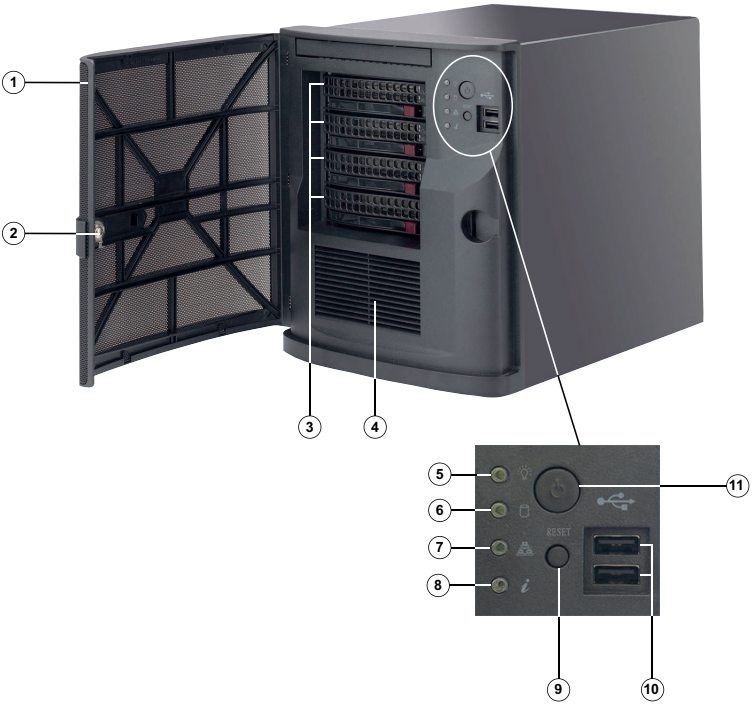
Das System DIVAR IP all-in-one 5000 ist eine einfach zu bedienende Komplettlösung zur Aufzeichnung, Wiedergabe und Verwaltung von Netzwerküberwachungssystemen.

Das DIVAR IP all-in-one 5000 ist ein intelligentes IP-Speichergerät, verfügt über die vollständige BVMS Lösung (BVMS) einschließlich Bosch Video Recording Manager (VRM) und Bosch Video Streaming Gateway (VSG) zur Integration von Drittanbieter-Kameras und kommt ohne separaten NVR-Server (Netzwerk-Videorekorder) und ohne Speicherhardware aus. BVMS verwaltet alle IP- und digitalen Video- und Audiodaten sowie alle Sicherheitsdaten, die über das IP-Netzwerk übertragen werden. Es kombiniert nahtlos IP-Kameras und IP-Encoder und stellt systemweites Ereignis- und Alarmmanagement, Systemzustandsüberwachung, Benutzer- und Prioritätsmanagement bereit.
DIVAR IP all-in-one 5000 ist eine 4-Schacht-Mini-Towereinheit mit austauschbaren SATA-Festplatten an der Vorderseite.
Es kann einfach installiert und betrieben werden. Die gesamte Systemsoftware ist vorinstalliert: Die Videomanagementanwendung ist gleich nach dem Auspacken einsatzbereit.
DIVAR IP all-in-one 5000 läuft mit Betriebssystem Windows Storage Server 2016.

2.1 Geräteansichten

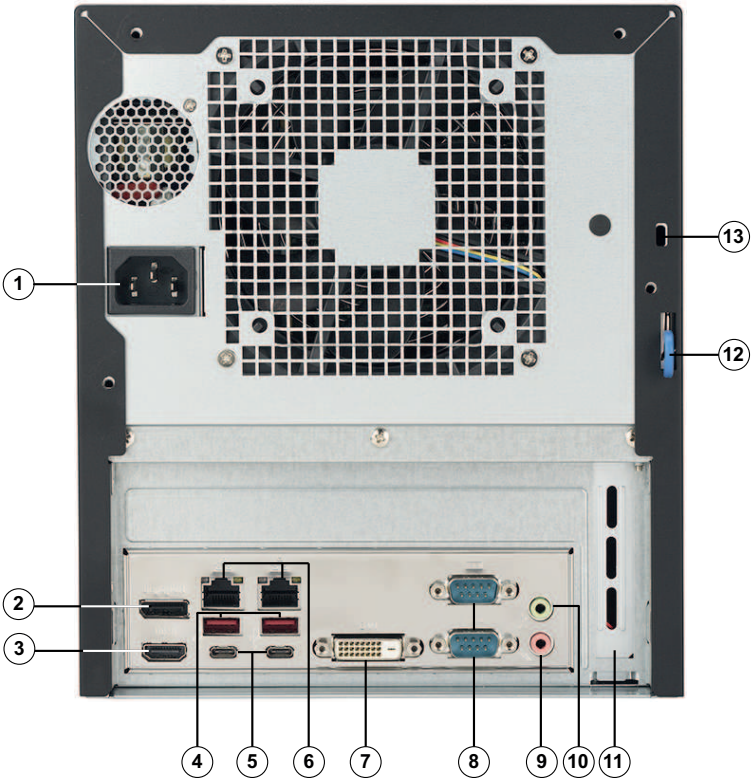
Das DIVAR IP all-in-one 5000 System befindet sich in einem kompakten Minitower-Gehäuse. Hinter der schwenkbaren Vorderabdeckung finden Sie die Festplatten und das Bedienfeld. Das vordere Bedienfeld verfügt über Netzschalter und Statusüberwachungs-LEDs.
Auf der Rückseite stehen verschiedene E/A-Anschlüsse zur Verfügung.

Vorderansicht



1	Vorderabdeckung	2	Schloss für Vorderabdeckung
3	4 x Festplattenanschlüsse (für 3,5"-Hot-Swap-Festplatten)	4	Lufteinlassfilter
5	LED für Stromzufuhr	6	HDD-LED (nicht verwendet)
7	Netzwerk-LED	8	Informations-LED
9	Rücksetztaste	10	2 x USB 2.0
11	Netzschalter		

Rückansicht



1	Netzanschluss	2	DisplayPort
3	HDMI 2.0	4	2 x USB 3.1 (Typ A)
5	2 x USB 3.1 (Typ C)	6	2 x LAN-Anschlüsse (RJ45), gebündelt **Hinweis:** Teaming-Modus nicht ändern!
7	DVI-D-Anschluss	8	2 x COM-Anschlüsse
9	Audio-Mikrofoneingang	10	Audio-Line-Ausgang

11	Zusätzliche Grafikkarte mit 4 Mini DisplayPort-Anschlüssen (die in diesem Fall für Monitorverbindungen verwendet werden sollen). **Hinweis:** nur für DIP-5240GP-00N, DIP-5244GP-4HD, DIP-5248GP-4HD und DIP-524CGP-4HD.	12	Schließband an der Gehäuserückseite (kompatibel mit vielen marktüblichen Schlössern). **Hinweis:** Schlösser sind nicht im Lieferumfang enthalten.
13	Kensington-Sicherheitsschlitz (für standardmäßiges Kensington-Schloss). **Hinweis:** Kensington-Schloss ist nicht im Lieferumfang enthalten.		

2.2 Bedienfeld-Steuerelemente

Das Bedienfeld an der Gehäusevorderseite verfügt über Netzschalter und Statusüberwachungs-LEDs.

Bedienfeld-Tasten

Taste	Beschreibung
 **Stromversorgung**	Der Netzschalter wird dazu verwendet, das System vom Netzteil aus mit Strom zu versorgen bzw. die Stromversorgung zu unterbrechen. **Hinweis:** Beim Ausschalten des Systems mit dieser Taste wird die Hauptstromversorgung unterbrochen, die Standby-Stromversorgung des Systems wird jedoch aufrechterhalten.

Taste	Beschreibung
	Trennen Sie das System von der Stromversorgung, bevor Sie Wartungsaufgaben durchführen.
 **Zurücksetzen**	Mit der Rücksetztaste wird das System neu gestartet.

Bedienfeld-LEDs

LED	Beschreibung	
 **Stromversorgung**	Diese LED zeigt an, dass die Netzteile des Systems mit Strom versorgt werden. Im Normalfall sollte diese LED bei Systembetrieb leuchten.	
 **Festplatte**	Diese LED wird nicht verwendet.	
 **Netzwerk**	Diese LED weist durch Blinken auf eine Netzwerkaktivität hin.	
 **Information**	Diese LED zeigt den Systemstatus an.	
	Systemstatus	**Beschreibung**

LED	Beschreibung	
	Permanent ein, rot	Eine Überhitzung ist aufgetreten. (Dies kann durch überlastete Kabel verursacht werden.)
	Blinkend, rot (1 Hz)	Lüfterausfall: Prüfen Sie, ob ein Lüfter ausgefallen ist.
	Blinkend, rot (0,25 Hz)	Stromausfall: Prüfen Sie, ob ein Netzteil ausgefallen ist.
	Permanent ein, blau	Lokale UID wurde aktiviert. Mit dieser Funktion können Sie das Gerät in einer Rack-Umgebung finden.
	Blinkend, blau (300 ms)	Remote-UID wurde aktiviert. Mit dieser Funktion können Sie das Gerät von einem entfernten Standort finden.

3 Einbauen einer Festplatte

Das DIVAR IP all-in-one 5000 System verfügt über vier austauschbare Festplatten an der Vorderseite. Die Festplatten befinden sich in Festplattenträgern, damit sie leichter eingebaut und aus dem Gehäuse entfernt werden können. Die Festplattenträger sorgen außerdem für eine ausreichende Belüftung der Festplattenschächte.

Vorgehensweise

Gehen Sie zum Einbau einer Festplatte wie folgt vor:

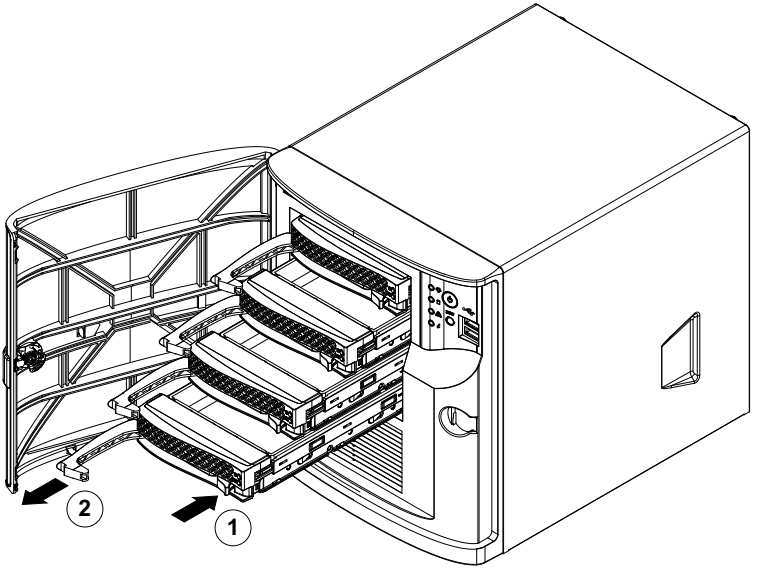
1. *Entfernen eines Festplattenträgers aus einem Festplattenschacht, Seite 18*
2. *Einbauen einer Festplatte in einem Festplattenträger, Seite 19*
3. *Einbauen eines Festplattenträgers in einen Festplattenschacht, Seite 20*

Hinweis!
Lesen Sie vor Arbeiten am Gehäuse die Warn- und Sicherheitshinweise in diesem Handbuch.

3.1 Entfernen eines Festplattenträgers aus einem Festplattenschacht

So entfernen Sie einen Festplattenträger aus einem Festplattenschacht:

1. Entsperren und öffnen Sie die Vorderabdeckung.
2. Drücken Sie die Entriegelungstaste rechts neben dem Festplattenträger. Der Griff des Festplattenträgers klappt aus.
3. Ziehen Sie den Festplattenträger mit dem Griff aus dem Gehäuse.



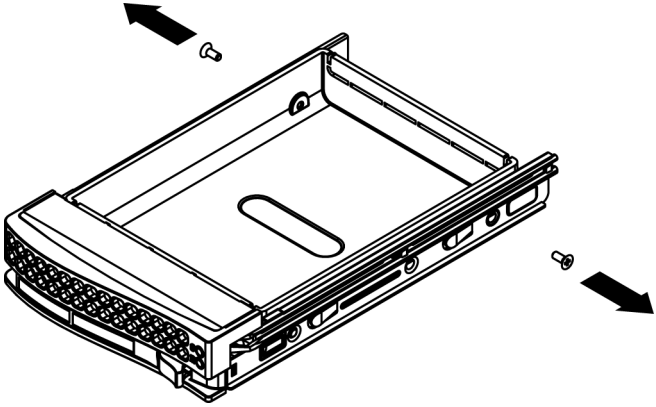
1	Entriegelungstaste	2	Griff des Festplattenträgers

Hinweis!
Lassen Sie das Gerät nicht laufen, solange sich die Festplattenträger nicht in den Schächten befinden.

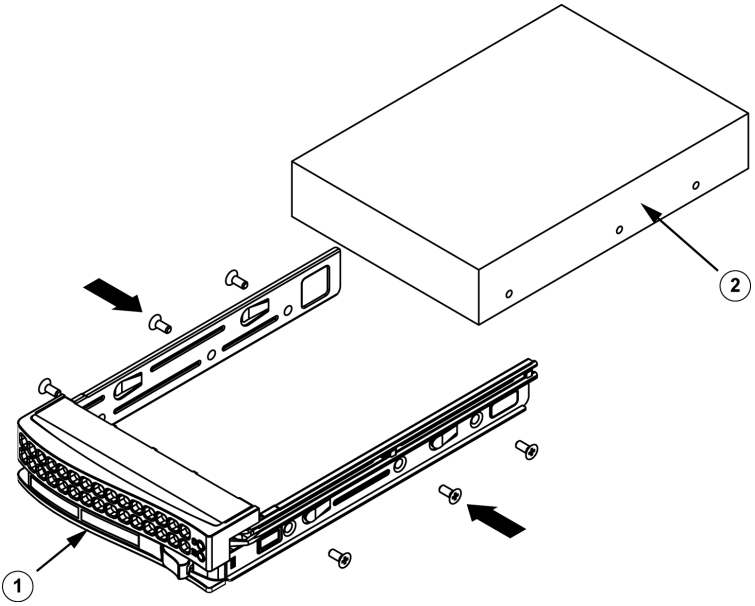
3.2 Einbauen einer Festplatte in einem Festplattenträger

So bauen Sie eine Festplatte in einem Festplattenträger ein:

1. Entfernen Sie die Schrauben, mit denen das Laufwerkdummy am Festplattenträger befestigt ist.



2. Entfernen Sie das Laufwerkdummy aus dem Festplattenträger und legen Sie den Festplattenträger auf eine ebene Fläche.
3. Schieben Sie eine neue Festplatte mit nach unten gerichteter Leiterplatte in den Festplattenträger.
4. Richten Sie die Befestigungslöcher von Festplattenträger und Festplatte aus.
5. Befestigen Sie die Festplatte mit den sechs Schrauben am Festplattenträger.



1	Festplattenträger	2	SATA-Festplatte

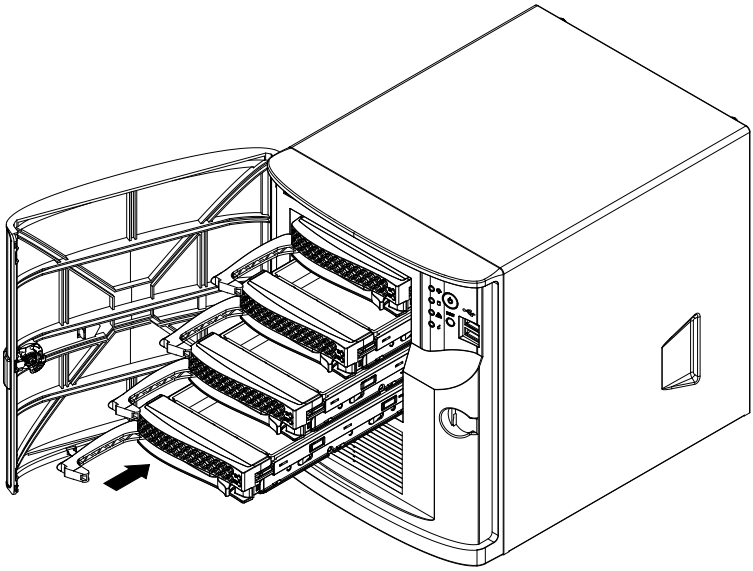
Hinweis!
Bosch empfiehlt die Verwendung der jeweiligen Festplatten von Bosch. Als eine der kritischen Komponenten werden die Festplatten von Bosch basierend auf verfügbaren Ausfallquoten sorgfältig ausgewählt. Nicht von Bosch gelieferte Festplatten werden nicht unterstützt.
Weitere Informationen zu unterstützten Festplatten finden Sie im Datenblatt im Online-Produktkatalog von Bosch unter: www.boschsecurity.com

3.3 Einbauen eines Festplattenträgers in einen Festplattenschacht

So bauen Sie einen Festplattenträger in einen Festplattenschacht ein:

1. Setzen Sie den Festplattenträger horizontal und mit der Entriegelungstaste rechts in den Festplattenschacht ein.

2. Drücken Sie den Festplattenträger in den Schacht, bis der Griff eingefahren wird und der Festplattenträger einrastet.
3. Schließen Sie die Vorderabdeckung und schließen Sie sie ab.



4 Systemkonfiguration

4.1 Standardeinstellungen

DIVAR IP-Systeme werden mit einem werkseitig vorinstallierten Konfigurationsassistenten geliefert.
Alle DIVAR IP Systeme sind mit einer Standard-IP-Adresse und mit den iSCSI-Standardeinstellungen vorkonfiguriert:

– IP-Adresse: automatisch durch DHCP zugewiesen (Fallback-IP-Adresse: 192.168.0.200).
– Subnetzmaske: automatisch durch DHCP zugewiesenen (Fallback-Subnetzmaske: 255.255.255.0).

Standard-Benutzereinstellungen für Administrator-Konto

– Benutzer: BVRAdmin
– Passwort: WSS4Bosch

4.2 Voraussetzungen

Dabei ist zu beachten:

- DIVAR IP muss während der Installation eine aktive Netzwerkverbindung haben. Stellen Sie sicher, dass der Netzwerk-Switch, mit dem Sie eine Verbindung herstellen möchten, in Betrieb ist.
- Die Standard-IP-Adresse darf nicht von einem anderen Gerät im Netzwerk belegt sein. Stellen Sie sicher, dass die Standard-IP-Adressen von vorhandenen DIVAR IP Systemen im Netzwerk geändert werden, bevor Sie ein weiteres DIVAR IP hinzufügen.
- Legen Sie fest, ob die Erstinstallation auf einem DHCP-Netzwerk stattfinden soll. Ist dies nicht der Fall, müssen Sie gültige IP-Adressen an die Videogeräte vergeben. Wenden Sie sich an Ihren IT-Administrator, um einen gültigen IP-Adressbereich für DIVAR IP und die zugehörigen Geräte zu erhalten.
- Die iSCSI-Standardeinstellungen sind für die Verwendung mit VRM optimiert.

4.3 Betriebsarten

Das DIVAR IP System kann in drei verschiedenen Modi betrieben werden:

- Vollständiges Videoaufzeichnungs- und -managementsystem mit BVMS und VRM Kernkomponenten und -diensten: Dieser Modus ermöglicht erweiterte Videomanagement-Funktionen, z. B. Ereignis- und Alarmverarbeitung.
- Reines Videoaufzeichnungssystem mit VRM-Kernkomponenten und -diensten.
- iSCSI-Speichererweiterung für ein BVMS oder VRM System, das auf einer anderen Hardware ausgeführt wird.

Hinweis!
Aufgezeichnete Videostreams müssen so konfiguriert sein, dass die maximale Bandbreite des Systems (BVMS/VRM Basissystem plus iSCSI-Speichererweiterungen) nicht überschritten wird.

4.4 Vorbereiten der Festplatten für die Videoaufzeichnung

Systeme mit werkseitig eingebauten Festplatten sind nach dem Auspacken sofort für die Aufzeichnung bereit.
Festplatten, die zu einem leeren System hinzugefügt wurden, müssen vor der Verwendung für Videoaufzeichnungen vorbereitet (formatiert) werden.

So können Sie eine Festplatte formatieren:

– Durchführen der erstmaligen Einrichtung ab Werk: siehe *Wiederherstellen des Geräts, Seite 33*.
– Führen Sie das Formatierungsskript aus.

Ausführen des Formatierungsskripts

Zum Ausführen des Formatierungsskripts müssen Sie sich mit dem Administrator-Konto (BVRAdmin) anmelden.

1. Starten Sie das System.
2. Drücken Sie auf dem BVMS Standardbildschirm die Tastenkombination Strg+Alt+Entf.
3. Halten Sie die Umschalttaste gedrückt, klicken Sie auf **Benutzer wechseln** und lassen Sie die Umschalttaste noch ca. fünf Sekunden lang gedrückt.
4. Geben Sie Administrator-Benutzernamen und -Passwort ein.
5. Klicken Sie auf dem Desktop im Ordner **Tools** mit der rechten Maustaste auf das Skript **Format_data_hard_drives** und klicken Sie dann auf **Als Administrator ausführen**.
6. Befolgen Sie die Anweisungen.
7. Nach der Formatierung können Sie den Speicher zur Videomanagement-Konfiguration hinzufügen.

Hinweis!
Beim Formatieren einer Festplatte werden alle darauf vorhandenen Daten gelöscht.

4.5 Starten der Anwendung

Die Anwendung bietet eine einfach zu installierende, benutzerfreundliche Lösung zur Netzwerküberwachung.

So starten Sie die Anwendung:

1. Schließen Sie das Gerät und die Kameras an das Netzwerk an.
2. Schalten Sie das Gerät ein.
   Der Einrichtungsprozess für Windows Storage Server 2016 wird gestartet.
3. Wählen Sie die gewünschte Sprache für die Installation, und klicken Sie dann auf **Weiter**.
4. Klicken Sie in den Listen **Land oder Region**, **Zeit und Währung** und **Tastaturlayout** auf das entsprechende Element. Klicken Sie dann auf **Weiter**.
   Die Microsoft Software License Terms und die EULA (Endbenutzer-Lizenzvereinbarung) werden angezeigt.
5. Akzeptieren Sie die Lizenzvereinbarung, und klicken Sie dann auf **Start**. Windows wird neu gestartet.
6. Nachdem der Neustart abgeschlossen ist, drücken Sie die Tastenkombination Strg+Alt+Entf. Der Windows-Anmeldebildschirm wird angezeigt.
7. Geben Sie das Standardpasswort **WSS4Bosch** ein.
8. Nach der Eingabe des Passworts werden Sie dazu aufgefordert, das Passwort zu ändern, damit Sie sich zum ersten Mal anmelden können. Klicken Sie zum Bestätigen auf **OK**.
9. Ändern Sie das Passwort.

Eine Reihe von Skripts führt wichtige Einstellungen durch. Dies kann einige Minuten dauern. Schalten Sie den Computer nicht aus.
Der BVMS Standardbildschirm wird angezeigt.
Sie können nun entscheiden, in welchem Modus das System betrieben werden soll:

- *Betrieb als vollständiges Videoaufzeichnungs- und -managementsystem, Seite 25*
- *Betrieb als reines Videoaufzeichnungssystem, Seite 26*
- *Betrieb als iSCSI-Speichererweiterung, Seite 26*

Hinweis!
Wenn Sie Ihr Passwort einmal vergessen haben sollten, muss eine Systemwiederherstellung durchgeführt werden. Diese wird im Installationshandbuch beschrieben. Die Konfiguration muss dann von Grund auf neu erfolgen oder importiert werden.

Hinweis!
Wir empfehlen ausdrücklich, keine Einstellungen am Betriebssystem zu ändern. Ein Ändern der Betriebssystemeinstellungen kann zu Fehlfunktionen im System führen.

Hinweis!
Zum Durchführen von administrativen Aufgaben müssen Sie sich mit dem Administrator-Konto anmelden.

4.5.1 Betrieb als vollständiges Videoaufzeichnungs- und -managementsystem

Für den Betrieb des DIVAR IP Systems als vollständiges Videoaufzeichnungs- und -managementsystem:

1. Doppelklicken Sie auf dem BVMS Standardbildschirm auf das Symbol BVMS Config Wizard  , um den Config Wizard zu starten.
   Die Seite **Welcome** wird angezeigt.

2. Konfigurieren Sie das System mit dem Config Wizard.

Siehe auch

– *Verwendung des BVMS Config Wizard, Seite 27*

4.5.2 Betrieb als reines Videoaufzeichnungssystem

Für den Betrieb des DIVAR IP Systems als reines Videoaufzeichnungssystem müssen Sie sich mit dem Administrator-Konto (BVRAdmin) anmelden, um die erforderlichen Konfigurationsschritte durchzuführen.

1. Drücken Sie auf dem BVMS Standardbildschirm die Tastenkombination Strg+Alt+Entf.
2. Halten Sie die Umschalttaste gedrückt, klicken Sie auf **Benutzer wechseln** und lassen Sie die Umschalttaste noch ca. fünf Sekunden lang gedrückt.
3. Geben Sie Administrator-Benutzernamen und -Passwort ein.
4. Klicken Sie auf dem Desktop im Ordner **Tools** mit der rechten Maustaste auf das Skript **Disable_BVMS** und klicken Sie dann auf **Als Administrator ausführen**.
5. Konfigurieren Sie den Video Recording Manager (VRM) über ein externes System mit dem BVMS Configuration Client oder Configuration Manager.

4.5.3 Betrieb als iSCSI-Speichererweiterung

Für den Betrieb des DIVAR IP Systems als iSCSI-Speichererweiterung müssen Sie sich mit dem Administrator-Konto (BVRAdmin) anmelden, um die erforderlichen Konfigurationsschritte durchzuführen.

1. Drücken Sie auf dem BVMS Standardbildschirm die Tastenkombination Strg+Alt+Entf.
2. Halten Sie die Umschalttaste gedrückt, klicken Sie auf **Benutzer wechseln** und lassen Sie die Umschalttaste noch ca. fünf Sekunden lang gedrückt.
3. Geben Sie Administrator-Benutzernamen und -Passwort ein.

4. Klicken Sie auf dem Desktop im Ordner **Tools** mit der rechten Maustaste auf das Skript **Disable_BVMS_and_VRM** und klicken Sie dann auf **Als Administrator ausführen**.
5. Fügen Sie das System als eine iSCSI-Speichererweiterung mit BVMS Configuration Client oder Configuration Manager zu einem externen BVMS oder VRM Server hinzu.

4.6 Verwendung des BVMS Config Wizard

Der Config Wizard dient zur schnellen und einfachen Konfiguration kleinerer Systeme. Der Config Wizard verhilft Ihnen zu einem konfigurierten System einschließlich VRM, iSCSI-System, Kameras, Aufzeichnungsprofilen und Benutzergruppen. Benutzergruppen und ihre Freigaben werden automatisch konfiguriert. Sie können Benutzer hinzufügen oder entfernen und Passwörter festlegen.
Der Config Wizard kann nur auf dem lokalen Computer auf Management Server zugreifen.
Sie können eine aktivierte Konfiguration als Sicherungskopie speichern und diese Konfiguration später importieren. Sie können die importierte Konfiguration nach dem Importieren ändern.
Der Config Wizard fügt den lokalen VRM automatisch hinzu.

Einschränkungen:
Die folgenden Aufgaben können nicht mit dem Config Wizard ausgeführt werden. Verwenden Sie stattdessen den BVMS Configuration Client.

- Anpassen der Zeitpläne
- Konfigurieren von Systemen ohne oder mit mehreren Video Recording Manager
- Konfigurieren der externen Speichergeräte
- Hinzufügen von Video Streaming Gateway
- alle erweiterten Konfigurationen, die über eine grundlegende Konfiguration hinausgehen (z. B. Karten oder Alarme)

Zur schnellen Konfiguration mithilfe des Config Wizard:

1. Doppelklicken Sie auf dem BVMS Standardbildschirm auf das Config Wizard-Symbol. Die Seite **Welcome** wird angezeigt.
2. Folgen Sie den Anweisungen des Assistenten auf dem Bildschirm.

Hinweis!
Weitere Informationen zu Aufgaben, die nicht mit Config Wizard ausgeführt werden können, und Informationen zu Config Wizard finden Sie im BVMS Handbuch im Online-Produktkatalog.

Siehe auch

– *Zusätzliche Dokumentation und Client-Software, Seite 35*

4.7 Hinzufügen von zusätzlichen Lizenzen

Sie können zusätzliche Lizenzen mit Configuration Client hinzufügen.

So aktivieren Sie die Software:

1. Starten Sie Configuration Client.
2. Klicken Sie im Menü **Werkzeuge** auf **Lizenz-Manager...**. Das Dialogfeld **Lizenz-Manager** wird angezeigt.
3. Klicken Sie auf die Kontrollkästchen des Software-Pakets, der Funktionen und der Erweiterungen, die Sie aktivieren möchten. Geben Sie für die Erweiterungen die Anzahl der Lizenzen ein.
   Wenn Sie eine Bundle-Informationsdatei erhalten haben, klicken Sie zum Importieren der Datei auf **Bundle Info importieren**.
4. Klicken Sie auf **Aktivieren**.
   Das Dialogfeld **Lizenz Aktivierung** wird angezeigt.
5. Notieren Sie sich die Computer-Signatur, oder kopieren Sie sie, und fügen Sie sie in eine Textdatei ein.
6. Geben Sie auf einem Computer mit Internetzugang folgende URL im Browser ein:
   https://activation.boschsecurity.com

Wenn Sie kein Zugangskonto für das Bosch License Activation Center besitzen, können Sie zwischen zwei Möglichkeiten wählen: Erzeugen Sie ein neues Konto (empfohlen), oder klicken Sie auf den Link, um die neue Lizenz ohne Anmeldung zu aktivieren. Wenn Sie vor der Aktivierung ein Konto erzeugen und sich anmelden, protokolliert der Lizenz-Manager Ihre Aktivierungen. Sie können dies jederzeit überprüfen.
Folgen Sie den Anweisungen, um den Lizenz-Aktivierungsschlüssel zu erhalten.

7. Wechseln Sie wieder zur BVMS-Software. Geben Sie im Dialogfeld **Lizenz Aktivierung** den vom Lizenz-Manager abgerufenen Lizenz-Aktivierungsschlüssel ein, und klicken Sie auf **Aktivieren**.
   Das Software-Paket wird aktiviert.

4.8 Verwenden des BVMS Operator Client

Verwenden Sie den BVMS Operator Client, um die Live-, Aufzeichnungs- und Wiedergabefunktionalität von DIVAR IP zu überprüfen.

So überprüfen Sie die Live-Bild-Funktion im Operator Client

1. Doppelklicken Sie auf dem BVMS Standardbildschirm auf das Operator Client-Symbol  . Die Anwendung wird gestartet.
2. Geben Sie die folgenden Angaben ein und klicken Sie auf **OK**.
   Benutzername: admin
   Passwort: kein Passwort erforderlich (falls nicht mit dem Assistenten eingerichtet)
   Verbindung: 127.0.0.1
3. Klicken Sie auf das Live-Bild-Symbol. Der logische Baum mit den Kameras wird angezeigt.

4. Wählen Sie eine Kamera aus und ziehen Sie sie in ein Bildfenster. Das Bild der Kamera wird angezeigt, wenn die Kamera richtig zugewiesen ist.
   Hinweis:
   Kameras im Bildfenster mit einem roten Punkt im Kamerasymbol werden live angezeigt.

So überprüfen Sie die Aufzeichnungsfunktion im Operator Client

- Kameras im logischen Baum mit einem roten Punkt im Kamerasymbol werden aufgezeichnet.

So überprüfen Sie die Wiedergabefunktion im Operator Client

- Die Zeitleiste bewegt sich, wenn die Kamera im Wiedergabemodus angezeigt wird.

Informationen zum Durchführen weitere Funktionen finden Sie im BVMS Handbuch im Online-Produktkatalog.

5 Fernverbindung mit dem System

In diesem Abschnitt werden die erforderlichen Schritte für den Zugriff auf das DIVAR IP System über das Internet beschrieben.

5.1 Schutz des Systems vor unbefugtem Zugriff

Um das System vor unbefugtem Zugriff zu schützen, empfehlen wir, ein starkes Passwort festzulegen, bevor Sie das System mit dem Internet verbinden. Je stärker das Passwort ist, desto besser wird Ihr System vor dem Zugriff durch unbefugte Personen und Malware geschützt.

5.2 Einrichten der Portweiterleitung

Um aus dem Internet über einen NAT/PAT-fähigen Router auf ein DIVAR IP System zugreifen zu können, muss die Portweiterleitung auf dem DIVAR IP System und dem Router konfiguriert werden.

So richten Sie die Portweiterleitung ein:

- Geben Sie die folgenden Portregeln in den Einstellungen für die Portweiterleitung Ihres Routers ein:
- Port 5322 für SSH-Tunnelzugriff mit BVMS Operator Client.
- Port 443 für HTTPS-Zugriff auf VRM mit Video Security Client oder Video Security App.

Das DIVAR IP System ist jetzt über das Internet erreichbar.

5.3 Wählen eines geeigneten Clients

In diesem Kapitel erfahren Sie, wie Sie eine Fernverbindung mit einem DIVAR IP System über das Internet herstellen können.

Es gibt zwei Möglichkeiten, um eine Fernverbindung herzustellen:

- *Fernverbindung mit Operator Client, Seite 31*.
- *Fernverbindung mit Video Security App, Seite 32*.

Hinweis!
Verwenden Sie nur BVMS Operator Client oder Video Security App in der Version, die DIVAR IP entspricht. Andere Clients oder Anwendungssoftware funktionieren möglicherweise, werden aber nicht unterstützt.

5.3.1 Fernverbindung mit Operator Client

So stellen Sie eine Fernverbindung mit BVMS Operator Client her:

1. Installieren Sie BVMS Operator Client auf der Client-Arbeitsstation.
2. Nachdem Sie die Installation erfolgreich abgeschlossen haben, starten Sie Operator Client über die Desktop-Verknüpfung  .
3. Geben Sie die folgenden Angaben ein und klicken Sie dann auf **OK**.
   Benutzername: admin (oder ein anderer Benutzer, falls konfiguriert)

Passwort: Benutzerpasswort eingeben
Verbindung: ssh://[öffentliche-IP-Adresse-des-DIVAR-IP_all-in-one]:5322

5.3.2 Fernverbindung mit Video Security App

So stellen Sie eine Fernverbindung mit der Video Security App her:

1. Suchen Sie im App Store von Apple nach Bosch Video Security.
2. Installieren Sie die Video Security App auf Ihrem iOS-Gerät.
3. Starten Sie die Video Security App.
4. Wählen Sie **Hinzufügen** aus.
5. Geben Sie die öffentliche IP-Adresse oder den DynDNS-Namen ein.
6. Stellen Sie sicher, dass die SSL-Verbindung aktiviert ist.
7. Wählen Sie **Hinzufügen** aus.
8. Geben Sie die folgenden Angaben ein:
   Benutzername: admin (oder ein anderer Benutzer, falls konfiguriert)
   Passwort: Benutzerpasswort eingeben

6 Wartung

6.1 Überwachen des Systems

Das System bietet Tools zur Überwachung des Systemzustands. Zum Aktivieren der Überwachungsfunktion müssen Sie sich mit dem Administrator-Konto (BVRAdmin) anmelden.

1. Drücken Sie auf dem BVMS Standardbildschirm die Tastenkombination Strg+Alt+Entf.
2. Halten Sie die Umschalttaste gedrückt, klicken Sie auf **Benutzer wechseln** und lassen Sie die Umschalttaste noch ca. fünf Sekunden lang gedrückt.
3. Geben Sie Benutzername und Passwort ein.

4. Klicken Sie auf dem Desktop im Ordner **Tools** mit der rechten Maustaste auf das Skript **Enable_SuperDoctor_5_Service** und klicken Sie dann auf **Als Administrator ausführen**.
5. Doppelklicken Sie auf das **SuperDoctor 5 Web**-Symbol im selben Ordner.
6. Melden Sie sich mit den folgenden Standard-Anmeldeinformationen auf der Weboberfläche an:
   Benutzername: ADMIN
   Passwort: ADMIN
7. Klicken Sie auf die Registerkarte **Konfiguration**, dann auf **Passworteinstellungen**, und ändern Sie anschließend das Standardpasswort.
8. Klicken Sie auf die Registerkarte **Konfiguration** und dann auf **Alarmkonfiguration**.
9. Aktivieren Sie die Funktion **SNMP-Trap** und geben Sie die IP-Adresse des Empfängers für SNMP-Traps an.

6.2 Wiederherstellen des Geräts

Im Folgenden wird beschrieben, wie das Standardbild wiederhergestellt wird.

So stellen Sie das Standardbild des Geräts wieder her:

1. Starten Sie das Gerät und drücken Sie während des BIOS-Power-On-Self-Tests (Selbsttest beim Einschalten) auf **F7**. Das Wiederherstellungsmenü wird nun angezeigt.
2. Wählen Sie eine der folgenden Optionen aus:
   - **Erstmalige Einrichtung ab Werk:** stellt das Standardbild wieder her und löscht alle Daten auf den Festplatten.
     oder
   - **Systemwiederherstellung (zurück auf Werkseinstellungen):** stellt das Standardbild wieder her; Daten auf den Festplatten werden nicht gelöscht.

Hinweis:
Auch wenn bei der Option **Systemwiederherstellung** kein Videomaterial von den Festplatten gelöscht wird, wird trotzdem die gesamte Betriebssystem-Partition (einschließlich VMS-Einstellungen) durch eine Standardkonfiguration ersetzt. Damit Sie nach der Wiederherstellung auf das vorhandene Videomaterial zugreifen können, muss die VMS-Konfiguration vor der Wiederherstellung des Systems exportiert und danach erneut importiert werden.

Hinweis!
Schalten Sie das Gerät während des Vorgangs nicht aus. Dies würde das Wiederherstellungsmedium beschädigen.

3. Das Gerät wird über das Wiederherstellungsmedium gestartet. Wenn die Einrichtung erfolgreich war, drücken Sie auf **Ja**, um das System neu zu starten.
4. Die Ersteinrichtung des Betriebssystems wird von Windows durchgeführt. Anschließend wird das Gerät automatisch neu gestartet.
5. Nach dem Neustart des Geräts werden die Werkseinstellungen installiert.

6.3 Wartung und Reparatur

Das Speichersystem ist durch eine 3-jährige Garantie geschützt. Garantiefälle werden gemäß den Service- und Support-Richtlinien von Bosch bearbeitet.
Die Speichergeräte werden mit einem Service- und Support-Vertrag vom Originalhersteller geliefert.
Der Technische Kundendienst von Bosch ist der Ansprechpartner bei Ausfällen, aber die Service- und Supportarbeiten werden vom Hersteller oder einem Partner durchgeführt.

Damit die Service- und Support-Abteilung des Herstellers das angegebene Serviceniveau erfüllen kann, muss das System neu registriert werden. Andernfalls kann nicht das definierte Serviceniveau, sondern nur entsprechend den besten Bemühungen geliefert werden.
Eine Beschreibung der geforderten Informationen und der Zielort sind in jeder Lieferung in Papierform enthalten. Die Beschreibung ist auch elektronisch im Bosch Online-Produktkatalog verfügbar.

7 Zusätzliche Dokumentation und Client-Software

Weitere Informationen, Software und Dokumentation finden Sie unter www.boschsecurity.com auf der entsprechenden Produktseite.

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