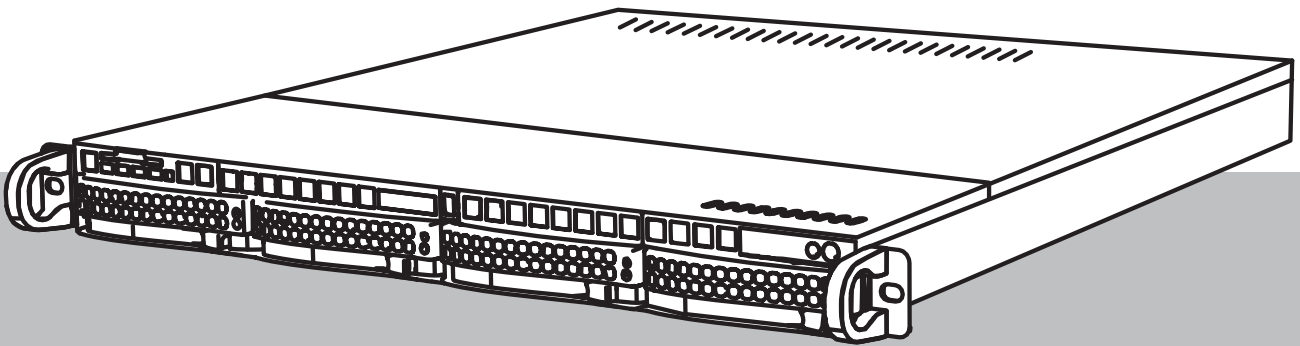


DIVAR IP all-in-one 6000

DIP-6440IG-00N | DIP-6444IG-4HD | DIP-6448IG-4HD |
DIP-644IIG-4HD



Inhaltsverzeichnis

1	Sicherheit	4
1.1	Sicherheitsvorkehrungen im Betrieb	4
1.2	Cybersicherheitsvorkehrungen	5
1.3	Sicherheitsmaßnahmen für die Software	6
1.3.1	Verwendung aktueller Software	6
1.3.2	OSS-Informationen	6
2	Einführung	8
3	Systemüberblick	9
4	Systemkonfiguration	10
4.1	Grundeinstellungen	10
4.2	Voraussetzungen	10
4.3	Erstmalige Anmeldung und erste Systemkonfiguration	10
4.3.1	Auswahl des Betriebsmodus BVMS	12
4.3.2	Auswahl des Betriebsmodus VRM	13
4.3.3	Auswahl des Betriebsmodus iSCSI-Speicher	13
5	Durchführen eines Upgrades der Software	14
6	Fernverbindung mit dem System	16
6.1	Schutz des Systems vor unbefugtem Zugriff	16
6.2	Einrichten der Portweiterleitung	16
6.3	Wählen eines geeigneten Clients	16
6.3.1	Fernverbindung mit BVMS Operator Client	16
6.3.2	Fernverbindung mit Video Security App	17
6.4	Verbindungsaufbau mit einem Enterprise Management Server	17
7	Wartung	18
7.1	Anmeldung beim Administratorkonto	18
7.2	Überwachen des Systems	18
7.2.1	Überwachung des Systems mit der Anwendung SuperDoctor	18
7.2.2	Überwachung des Systems über die IPMI-Schnittstelle	19
7.3	Ersetzen einer defekten Festplatte und Konfigurieren einer neuen Festplatte	19
7.3.1	Austausch einer defekten Festplatte	20
7.3.2	Wiederherstellung von RAID5 mit der neuen Festplatte	20
7.4	Sammeln von DIVAR IP System Manager-Logdateien	20
7.5	Wiederherstellen des Geräts	21
8	Zusatzinformationen	22
8.1	Zusätzliche Dokumentation und Client-Software	22
8.2	Supportdienstleistungen und Bosch Academy	22

1 Sicherheit

Beachten Sie die Sicherheitshinweise in diesem Kapitel.

1.1 Sicherheitsvorkehrungen im Betrieb

**Hinweis!**

Vorgesehene Verwendung

Dieses Produkt ist nur für den professionellen Gebrauch bestimmt. Es ist nicht dafür vorgesehen, in einem öffentlichen Bereich installiert zu werden, der für die allgemeine Öffentlichkeit zugänglich ist.

**Hinweis!**

Verwenden Sie dieses Produkt nicht an einem feuchten oder nassen Ort.

**Hinweis!**

Treffen Sie Sicherheitsvorkehrungen, um das Gerät vor Schäden durch Überspannung oder Blitzeinschlag zu schützen.

**Hinweis!**

Halten Sie den Bereich um das Gerät sauber und ordentlich.

**Hinweis!**

Gehäuseöffnungen

Die Öffnungen dürfen nicht blockiert oder verdeckt werden. Alle Öffnungen im Gehäuse sind für die Belüftung vorgesehen. Diese Öffnungen verhindern eine Überhitzung und gewährleisten einen zuverlässigen Betrieb.

**Hinweis!**

Die Abdeckung des Geräts darf nicht geöffnet oder entfernt werden. Das Öffnen oder Entfernen der Abdeckung kann das System beschädigen und führt zum Erlöschen der Garantie.

**Hinweis!**

Schütten Sie keine Flüssigkeit auf das Gerät.

**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.

**Hinweis!**

Trennen Sie das Gerät vom Stromnetz, bevor Sie es bewegen. Gehen Sie beim Bewegen des Produkts äußerst vorsichtig vor. Extreme Krafteinwirkung oder Erschütterungen können Schäden am Produkt und an den Festplattenlaufwerken verursachen.

**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!**

Videoverlust ist bei digitalen Videoaufzeichnungen nicht auszuschließen. Daher übernimmt Bosch Security Systems keine Haftung für Schäden, die aus verloren gegangenen Videodaten entstehen.

Um das Risiko des Datenverlusts zu minimieren, werden der Einsatz mehrerer redundanter Aufzeichnungssysteme sowie ein Verfahren zur Sicherung aller analogen und digitalen Daten empfohlen.

1.2

Cybersicherheitsvorkehrungen

Beachten Sie aus Gründen der Cybersicherheit Folgendes:

- Stellen Sie sicher, dass nur autorisiertes Fachpersonal physischen Zugriff auf das System hat. Platzieren Sie das System in einem Bereich mit Zutrittskontrolle, um physische Manipulationen daran zu vermeiden.
- Das Betriebssystem enthält die neuesten Windows-Sicherheitspatches, die zu dem Zeitpunkt verfügbar waren, als das Software-Image erstellt wurde. Verwenden Sie die Windows Update-Funktion oder die entsprechenden monatlichen Rollup-Patches für die Offline-Installation zur regelmäßigen Installation von BS-Sicherheitsupdates.
- Windows Defender und Windows Firewall dürfen nicht deaktiviert werden und müssen immer auf dem neuesten Stand sein.
- Installieren Sie keine zusätzliche Antivirensoftware.
- Geben Sie Systeminformationen und sensible Daten ausschließlich an Personen weiter, bei denen Sie zuverlässig wissen, dass diese zur Verwendung dieser Daten berechtigt sind.
- Prüfen Sie, ob eine Website sicher ist, bevor Sie sensible Informationen darüber versenden.
- Beschränken Sie den lokalen Netzwerkzugriff auf vertrauenswürdige Geräte. Details finden Sie in den folgenden Dokumenten, die im Online-Produktkatalog zur Verfügung stehen:
 - *Netzwerkauthentifizierung – 802.1X*
 - *Cybersicherheitshandbuch für Bosch IP-Videoprodukte*
- Verwenden Sie für den Zugriff über öffentliche Netzwerke nur sichere (verschlüsselte) Kommunikationskanäle.
- Das Administratorkonto hat volle Administratorrechte und uneingeschränkten Zugriff auf das System. Mit Administratorrechten können Benutzer Software installieren, aktualisieren oder entfernen und Konfigurationseinstellungen ändern. Außerdem ermöglichen Administratorrechte Benutzern einen direkten Zugriff auf und die Änderung von Registrierungsschlüsseln und damit die Umgehung von zentralen Verwaltungs- und Sicherheitseinstellungen. Mit dem Administratorkonto angemeldete Benutzer können Firewalls umgehen und Antivirensoftware entfernen, wodurch das System Viren und

Cyberattacken ausgesetzt wird. Dies kann ein ernsthaftes Risiko für das System und die Datensicherheit darstellen.

Beachten Sie zur Minimierung von Cybersicherheitsrisiken Folgendes:

- Stellen Sie sicher, dass das Administratorkonto gemäß der Passwortrichtlinie mit einem komplexen Passwort geschützt ist.
- Stellen Sie sicher, dass nur eine begrenzte Anzahl vertrauenswürdiger Benutzer Zugriff auf das Administratorkonto hat.
- Aufgrund der Betriebsanforderungen darf das Systemlaufwerk nicht verschlüsselt werden. Ohne Verschlüsselung ist der Zugriff auf die auf diesem Laufwerk gespeicherten Daten leichter möglich und die Daten könnten entfernt werden. Stellen Sie sicher, dass nur autorisierte Personen Zugriff auf das System und das Administratorkonto haben, um Datendiebstahl und versehentlichen Datenverlust zu vermeiden.
- Zur Installation und Aktualisierung der Software sowie zur Wiederherstellung des Systems müssen möglicherweise USB-Geräte verwendet werden. Daher dürfen die USB-Anschlüsse des Systems nicht deaktiviert werden. Durch das Verbinden von USB-Geräten mit dem System besteht jedoch das Risiko einer Infektion durch Malware. Stellen Sie zur Vermeidung von Malware-Angriffen sicher, dass keine infizierten USB-Geräte an das System angeschlossen werden.

1.3 Sicherheitsmaßnahmen für die Software

1.3.1 Verwendung aktueller Software

Stellen Sie vor der Erstinbetriebnahme des Geräts sicher, dass die neueste gültige Version der Software installiert ist. Sie sollten die Software während der gesamten Betriebsdauer des Geräts immer auf dem aktuellen Stand halten, um die bestmögliche Funktionalität, Kompatibilität, Leistung und Sicherheit zu erhalten. Befolgen Sie die Anweisungen zu Softwareaktualisierungen in der Produktdokumentation.

Die folgenden Links bieten weitere Informationen:

- Allgemeine Informationen: <https://www.boschsecurity.com/xc/en/support/product-security/>
- Sicherheitsanweisungen, d. h. eine Liste bekannter Sicherheitslücken und vorgeschlagene Lösungen: <https://www.boschsecurity.com/xc/en/support/product-security/security-advisories.html>

Bosch haftet nicht für Schäden, die durch den Betrieb seiner Produkte mit veralteten Softwarekomponenten verursacht werden.

Die aktuelle Software und die verfügbaren Upgrade-Pakete finden Sie im Download Store von Bosch Security and Safety Systems unter: <https://downloadstore.boschsecurity.com/>

1.3.2 OSS-Informationen

Bosch verwendet Open Source Software in DIVAR IP all-in-one Produkten.

Die Lizenzen der verwendeten Open Source Softwarekomponenten finden Sie auf dem Systemlaufwerk unter:

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

Die Lizenzen von Open-Source-Software-Komponenten, die in einer weiteren auf Ihrem System installierten Software verwendet werden, sind im Installationsordner der jeweiligen Software gespeichert, zum Beispiel unter:

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

Oder unter:

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

2 Einführung

DIVAR IP all-in-one 6000 ist eine erschwingliche und einfach zu bedienende Komplettlösung zur Aufzeichnung, Anzeige und Verwaltung von Aufnahmen mit Netzwerküberwachungssystemen mit bis zu 64 Kanälen (wird mit einer Lizenz für 8 Kanäle geliefert).

DIVAR IP all-in-one 6000 ist eine 1-HE-Rackeinheit und kombiniert die erweiterten Funktionen von Bosch Video Management System und hochmodernem Aufzeichnungsmanagement in einem einzelnen kosteneffizienten Aufzeichnungsgerät, das einfach zu installieren und zu bedienen ist.

DIVAR IP all-in-one 6000 nutzt integrierte Design- und Kernkomponenten und basiert auf dem Betriebssystem Microsoft Windows Server IoT 2022 for Storage Workgroup. DIVAR IP all-in-one 6000 bietet für Unternehmen ausgelegte, unterbrechungsfrei austauschbare SATA-Festplatten mit bis zu 72 TB Bruttospeicherkapazität.

3 Systemüberblick

Betriebssystem

Das Microsoft Windows Server IoT 2022 for Storage Workgroup Betriebssystem bietet eine Schnittstelle für die Erstkonfiguration des Servers, eine einheitliche Verwaltung von Speichergeräten, die vereinfachte Einrichtung und Speicherverwaltung sowie Unterstützung für Microsoft iSCSI-Softwareziele.

Es ist speziell optimiert, um für über Netzwerkdienste bereitgestellte Speichersysteme (Network Attached Storage, NAS) die bestmögliche Leistung zu liefern. Das Microsoft Windows Server IoT 2022 for Storage Workgroup Betriebssystem bietet signifikante Verbesserungen für Speicherverwaltungsszenarios sowie eine Integration der Komponenten und der Funktionalität für die Verwaltung von Speichergeräten.

DIVAR IP System Manager

Die Anwendung DIVAR IP System Manager ist die zentrale Schnittstelle für einfache Systemeinrichtung, Konfiguration und Softwareaktualisierung.

Betriebsarten

DIVAR IP all-in-one 6000 Systeme können in drei verschiedenen Modi betrieben werden:

- Vollständiges Videoaufzeichnungs- und -managementsystem mit BVMS und Video Recording Manager Kernkomponenten und -diensten.
Dieser Modus bietet eine fortschrittliche IP-Videoüberwachung, die eine nahtlose Verwaltung von digitalem Video, Audio und Daten über ein IP-Netzwerk ermöglicht. Er kombiniert nahtlos IP-Kameras und IP-Encoder und stellt systemweites Ereignis- und Alarmmanagement, Systemzustandsüberwachung, Benutzer- und Prioritätsmanagement bereit. Dieser Modus bietet das beste Videomanagementsystem für den Einsatz mit Videoüberwachungsgeräten von Bosch und nutzt die einzigartigen Funktionen der Kameras und Aufzeichnungslösungen von Bosch. Er beinhaltet Video Streaming Gateway-Komponenten zur Integration von Drittanbieterkameras.
- Reines Videoaufzeichnungssystem mit Video Recording Manager Kernkomponenten und -diensten, das die einzigartigen Funktionen der Kameras und Aufzeichnungslösungen von Bosch nutzt.
- iSCSI-Speichererweiterung für ein BVMS oder Video Recording Manager System, das auf einer anderen Hardware ausgeführt wird. Bis zu vier dieser iSCSI-Speichererweiterungen können zu einem BVMS oder Video Recording Manager System hinzugefügt werden, das auf einem DIVAR IP all-in-one 6000 ausgeführt wird.

Bei der Einrichtung des Systems müssen Sie in der Anwendung DIVAR IP System Manager den gewünschten Betriebsmodus auswählen, um Ihr System zu konfigurieren.

Mit der Anwendung DIVAR IP System Manager können Sie auch die installierte Software aktualisieren.

Die aktuelle Software und die verfügbaren Upgrade-Pakete finden Sie im Download Store von Bosch Security and Safety Systems unter:

<https://downloadstore.boschsecurity.com/>



Hinweis!

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

4 Systemkonfiguration

4.1 Grundeinstellungen

Alle DIVAR IP Systeme sind mit einer Standard-IP-Adresse und mit den iSCSI-Standardinstellungen 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

- Benutzername: **BVRAdmin**
- Passwort: wird bei der ersten Anmeldung festgelegt
Passwort-Anforderungen:
 - Mindestens 14 Zeichen.
 - Mindestens ein Großbuchstabe.
 - Mindestens ein Kleinbuchstabe
 - Mindestens eine Zahl

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.

4.3 Erstmalige Anmeldung und erste Systemkonfiguration



Hinweis!

Ändern Sie keine Einstellungen des Betriebssystems. Ein Ändern der Betriebssystemeinstellungen kann zu Fehlfunktionen im System führen.



Hinweis!

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



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.

So konfigurieren Sie das System:


1. Schließen Sie das DIVAR IP all-in-one Gerät und die Kameras an das Netzwerk an.
2. Schalten Sie das Gerät ein.

Konfigurationsroutinen für Microsoft Windows Server IoT 2022 for Storage Workgroup werden durchgeführt. Dieser Vorgang kann einige Minuten dauern. Schalten Sie das System nicht aus.

Nachdem der Vorgang abgeschlossen ist, wird der Bildschirm mit der Windows-Sprachauswahl angezeigt.

3. Wählen Sie Ihr Land/Ihre Region, die gewünschte Sprache des Betriebssystems und das Tastaturlayout aus der Liste aus und klicken Sie dann auf **Weiter**.
Die Microsoft Software-Lizenzbedingungen werden angezeigt.
4. Klicken Sie auf **Annehmen**, um die Lizenzbedingungen zu akzeptieren, und warten Sie, bis Windows neu gestartet wird. Dies kann einige Minuten dauern. Schalten Sie das System nicht aus.
Nach dem Neustart wird die Windows-Anmeldeseite angezeigt.
5. Legen Sie ein neues Passwort für das Administrator-Konto **BVRAdmin** fest und bestätigen Sie es.
Passwort-Anforderungen:
 - Mindestens 14 Zeichen
 - Mindestens ein Großbuchstabe
 - Mindestens ein Kleinbuchstabe.
 - Mindestens eine Zahl.Drücken Sie dann auf Eingabe.
Die Seite **Software Selection** wird angezeigt.
6. Das System durchsucht automatisch das lokale Laufwerk und alle angeschlossenen externen Speichermedien nach der Installationsdatei **SystemManager_x64_[software version].exe** für DIVAR IP System Manager, die sich in einem Ordner mit folgender Struktur befindet: *Drive root\BoschAppliance*.
Die Suche kann einige Zeit in Anspruch nehmen. Warten Sie, bis der Vorgang abgeschlossen ist.
7. Sobald das System die Installationsdatei erkannt hat, wird sie auf der Seite **Software Selection** angezeigt. Klicken Sie auf die Leiste, die die Installationsdatei anzeigt, um die Installation zu starten.
8. Wenn die Installationsdatei beim Scannen nicht gefunden wird, gehen Sie wie folgt vor:
 - Gehen Sie zu <https://downloadstore.boschsecurity.com/>.
 - Wählen Sie auf der Registerkarte **Software** die Option **BVMS Appliances** aus der Liste und klicken Sie dann auf **Select**.
Es wird eine Liste mit allen verfügbaren Softwarepaketen angezeigt.
 - Suchen Sie die ZIP-Datei **SystemManager_[software version].zip** und speichern Sie sie auf einem Speichermedium wie z. B. einem USB-Stick.
 - Entpacken Sie die Datei auf dem Speichermedium, indem Sie sicherstellen, dass sich der Ordner **BoschAppliance** im Stammverzeichnis des Speichermediums befindet.
 - Schließen Sie das Speichermedium an Ihr DIVAR IP all-in-one-System an.
Das System sucht automatisch auf dem Speichermedium nach der Installationsdatei. Die Suche kann einige Zeit in Anspruch nehmen. Warten Sie, bis der Vorgang abgeschlossen ist.
 - Sobald die Installationsdatei erkannt wird, wird sie auf der Seite **Software Selection** angezeigt. Klicken Sie auf die Leiste, die die Installationsdatei anzeigt, um die Installation zu starten.

Hinweis: Um automatisch erkannt zu werden, muss sich die Installationsdatei in einem Ordner mit der folgenden Struktur befinden: *Drive root\BoschAppliance* (zum Beispiel *F:\BoschAppliance*).

Wenn sich die Installationsdatei an einem anderen Ort befindet, der nicht der vordefinierten Ordnerstruktur entspricht, klicken Sie auf , um zu dem entsprechenden Ort zu navigieren. Klicken Sie dann auf die Installationsdatei, um die Installation zu starten.

9. Bevor die Installation beginnt, wird das Dialogfeld **End User License Agreement (EULA)** angezeigt. Lesen Sie die Lizenzbedingungen und klicken Sie dann auf **Accept**, um fortzufahren. Die Installation beginnt.
10. Nach Abschluss der Installation wird das System neu gestartet und Sie werden zur Windows-Anmeldeseite weitergeleitet. Melden Sie sich bei dem Administratorkonto an.
11. Der Microsoft Edge-Browser wird geöffnet und die Seite **DIVAR IP - Systemkonfiguration** wird angezeigt. Die Seite zeigt den Gerätetyp und die Seriennummer des Geräts sowie die drei Betriebsmodi und die für jeden Betriebsmodus verfügbaren Softwareversionen an.

Sie müssen den gewünschten Betriebsmodus und die gewünschte Softwareversion auswählen, um Ihr DIVAR IP all-in-one-System zu konfigurieren.

Hinweis: Wenn die gewünschte Softwareversion für den jeweiligen Betriebsmodus nicht auf einem lokalen Laufwerk vorhanden ist, gehen Sie wie folgt vor:

- Gehen Sie zu <https://downloadstore.boschsecurity.com/>.
- Wählen Sie auf der Registerkarte **Software** die Option **BVMS Appliances** aus der Liste und klicken Sie dann auf **Select**.
Es wird eine Liste mit allen verfügbaren Softwarepaketen angezeigt.
- Suchen Sie die ZIP-Dateien der gewünschten Softwarepakete, z. B. **BVMS_[BVMS version]_SystemManager_package_[package version].zip**, und speichern Sie sie auf einem Speichermedium wie z. B. einem USB-Stick.
- Entpacken Sie die Dateien auf dem Speichermedium. Die Ordnerstruktur der entpackten Dateien darf nicht verändert werden.
- Schließen Sie das Speichermedium an Ihr DIVAR IP all-in-one-System an.



Hinweis!

Die Änderung des Betriebsmodus nach der Installation erfordert ein komplettes Zurücksetzen auf Werkseinstellungen.

4.3.1

Auswahl des Betriebsmodus BVMS

So bedienen Sie das DIVAR IP all-in-one-System als vollständiges Videoaufzeichnungs- und Videomanagementsystem:

1. Wählen Sie auf der Seite **DIVAR IP - Systemkonfiguration** den Betriebsmodus **BVMS** und die gewünschte BVMS-Version, die Sie installieren möchten, und klicken Sie dann auf **Weiter**.
Die BVMS-Lizenzvereinbarung wird angezeigt.
2. Lesen und akzeptieren Sie die Lizenzvereinbarung und klicken Sie dann auf **Installieren**, um fortzufahren.
Die Installation beginnt und das Installationsdialogfeld zeigt den Fortschritt der Installation an. Schalten Sie das System nicht aus und entfernen Sie die Speichermedien nicht während des Installationsvorgangs.
3. Nachdem alle Softwarepakete erfolgreich installiert worden sind, startet das System neu. Nach dem Neustart werden Sie auf den BVMS Desktop weitergeleitet.
4. Klicken Sie auf dem BVMS Desktop auf die gewünschte Anwendung, um das System zu konfigurieren.



Hinweis!

Weitere Einzelheiten finden Sie in der jeweiligen DIVAR IP all-in-one Webschulung und in der BVMS Dokumentation.

Sie finden die Schulung unter: www.boschsecurity.com/xc/en/support/training/

4.3.2 Auswahl des Betriebsmodus VRM

So bedienen Sie das DIVAR IP all-in-one System als reines Videoaufzeichnungssystem:

1. Wählen Sie auf der Seite **DIVAR IP - Systemkonfiguration** den Betriebsmodus **VRM** und die gewünschte VRM-Version, die Sie installieren möchten, und klicken Sie dann auf **Weiter**.
Die VRM-Lizenzvereinbarung wird angezeigt.
2. Lesen und akzeptieren Sie die Lizenzvereinbarung und klicken Sie dann auf **Installieren**, um fortzufahren.
Die Installation beginnt und das Installationsdialogfeld zeigt den Fortschritt der Installation an. Schalten Sie das System nicht aus und entfernen Sie die Speichermedien nicht während des Installationsvorgangs.
3. Nachdem alle Softwarepakete erfolgreich installiert worden sind, startet das System neu. Nach dem Neustart werden Sie zum Windows-Anmeldebildschirm weitergeleitet.



Hinweis!

Weitere Informationen finden Sie in der VRM Dokumentation.

4.3.3 Auswahl des Betriebsmodus iSCSI-Speicher

So bedienen Sie das DIVAR IP all-in-one System als iSCSI-Speichererweiterung:

1. Wählen Sie auf der Seite **DIVAR IP - Systemkonfiguration** den Betriebsmodus **iSCSI-Speicher** und die gewünschte iSCSI-Speicherversion, die Sie installieren möchten, und klicken Sie dann auf **Weiter**.
Das Dialogfeld für die Installation wird angezeigt.
2. Klicken Sie im Installationsdialogfeld auf **Installieren**, um fortzufahren.
Die Installation beginnt und das Installationsdialogfeld zeigt den Fortschritt der Installation an. Schalten Sie das System nicht aus und entfernen Sie die Speichermedien nicht während des Installationsvorgangs.
3. Nachdem alle Softwarepakete erfolgreich installiert worden sind, startet das System neu. Nach dem Neustart werden Sie zum Windows-Anmeldebildschirm weitergeleitet.
4. Fügen Sie das System als eine iSCSI-Speichererweiterung mit BVMS Configuration Client oder Configuration Manager zu einem externen BVMS oder VRM Server hinzu.



Hinweis!

Weitere Informationen finden Sie in der BVMS oder Configuration Manager Dokumentation.

5 Durchführen eines Upgrades der Software

Mit der Anwendung DIVAR IP System Manager können Sie die installierte Software auf Ihrem System aktualisieren.

Die aktuelle Software und die verfügbaren Upgrade-Pakete finden Sie im Download Store von Bosch Security and Safety Systems unter:


<https://downloadstore.boschsecurity.com/>





Hinweis!

Ein Downgrade der installierten Software auf eine frühere Version wird nicht unterstützt.

So führen Sie ein Upgrade der installierten Software durch:

1. Gehen Sie zu <https://downloadstore.boschsecurity.com/>.
2. Wählen Sie auf der Registerkarte **Software** die Option **BVMS Appliances** aus der Liste und klicken Sie dann auf **Select**.
Es wird eine Liste mit allen verfügbaren Softwarepaketen angezeigt.
3. Suchen Sie die ZIP-Dateien der gewünschten Softwarepakete, z. B. **BVMS_[BVMS version]_SystemManager_package_[package version].zip**, und speichern Sie sie auf einem Speichermedium wie z. B. einem USB-Stick.
4. Entpacken Sie die Dateien auf dem Speichermedium. Die Ordnerstruktur der entpackten Dateien darf nicht verändert werden.
5. So starten Sie die Anwendung DIVAR IP System Manager:
 - Wenn Sie in Windows mit dem Administratorkonto **BVRAdmin** angemeldet sind, doppelklicken Sie auf das DIVAR IP System Manager-Symbol auf dem Windows-Desktop.
Die Anwendung DIVAR IP System Manager wird gestartet.
 - Wenn Ihr System im Betriebsmodus BVMS läuft, klicken Sie auf das DIVAR IP System Manager-Symbol auf dem BVMS-Desktop und melden sich beim BVRAdmin-Administratorkonto an. Die Anwendung DIVAR IP System Manager wird in einem Vollbild-Dialogfeld geöffnet (Sie können das Dialogfeld mit der Taste Alt+ F4 verlassen).
6. Die Seite **Softwarepakete** wird angezeigt. Oben auf der Seite werden der Gerätetyp und die Seriennummer des Geräts angezeigt.
 - In der Spalte **Name** sehen Sie alle DIVAR IP System Manager-Softwareanwendungen, die bereits auf Ihrem System installiert sind, sowie alle weiteren DIVAR IP System Manager-Softwareanwendungen, die vom System auf dem **Images**-Laufwerk oder auf einem Speichermedium erkannt wurden.
 - In der Spalte **Installierte Version** sehen Sie die Version der Softwareanwendung, die derzeit auf Ihrem System installiert ist.
 - In der Spalte **Status** sehen Sie den Status der jeweiligen Softwareanwendung:
 - Das -Symbol zeigt an, dass das System keine neueren Versionen der installierten Softwareanwendung auf dem **Images**-Laufwerk oder auf einem Speichermedium gefunden hat.
Hinweis: Um sicherzustellen, dass Sie die neueste Softwareversion verwenden, überprüfen Sie die verfügbaren Softwareversionen im Download Store von Bosch Security and Safety Systems unter:
<https://downloadstore.boschsecurity.com/>

- Das  -Symbol zeigt an, dass das System neuere Versionen der installierten Softwareanwendung auf dem **Images**-Laufwerk oder auf einem Speichermedium erkannt hat.
Das Symbol wird auch angezeigt, wenn das System eine Softwareanwendung erkannt hat, die noch nicht auf Ihrem System installiert ist.
- In der Spalte **Verfügbare Version** sehen Sie die neueren Versionen der installierten Softwareanwendungen. Diese Versionen wurden vom System auf dem **Images**-Laufwerk oder auf einem Speichermedium erkannt.
In dieser Spalte werden auch die verfügbaren Versionen der erkannten Softwareanwendungen angezeigt, die noch nicht auf Ihrem System installiert sind.
Hinweis: Es werden nur neuere Versionen der installierten Softwareanwendungen angezeigt. Das Downgrade einer Softwareanwendung auf eine frühere Version wird nicht unterstützt.
- 7. Klicken Sie in der Spalte **Name** auf das entsprechende Optionsfeld, um die Softwareanwendung auszuwählen, die Sie aktualisieren oder installieren möchten.
- 8. Wählen Sie in der Spalte **Verfügbare Version** die gewünschte Version aus, auf die Sie Ihre Softwareanwendung aktualisieren oder die Sie installieren möchten, und klicken Sie dann auf **Weiter**.
Falls zutreffend, wird ein Dialogfeld mit einer Lizenzvereinbarung angezeigt.
- 9. Lesen und akzeptieren Sie die Lizenzvereinbarung und klicken Sie dann auf **Installieren**, um fortzufahren.
Die Installation beginnt, und das Dialogfeld für die Installation zeigt den Fortschritt der Installation an. Schalten Sie das System nicht aus und entfernen Sie die Speichermedien nicht während des Installationsvorgangs.
- 10. Nachdem alle Softwarepakete erfolgreich installiert wurden, erhalten Sie die Meldung **Installation erfolgreich abgeschlossen**. oben auf der Seite.
- 11. Wenn die Installation nicht erfolgreich war, erhalten Sie die Meldung **Installation fehlgeschlagen**. und das  -Symbol wird angezeigt. In diesem Fall drücken Sie F5, um zur Seite **Softwarepakete** zurückzukehren. Laden Sie die jeweiligen Softwarepakete herunter, und versuchen Sie es erneut.
Wenn das Problem weiterhin besteht, wenden Sie sich an den technischen Support.

6 Fernverbindung mit dem System

Sie können eine Fernverbindung zu Ihrem DIVAR IP all-in-one System herstellen und über das Internet darauf zugreifen.

Um eine Fernverbindung herzustellen, müssen Sie Folgendes tun:

1. *Schutz des Systems vor unbefugtem Zugriff, Seite 16.*
2. *Einrichten der Portweiterleitung, Seite 16.*
3. *Wählen eines geeigneten Clients, Seite 16.*

6.1 Schutz des Systems vor unbefugtem Zugriff

Um das System vor unbefugtem Zugriff zu schützen, sollten Sie strenge Passwortregeln einhalten, 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.

6.2 Einrichten der Portweiterleitung

Um vom Internet aus über einen NAT/PAT-fähigen Router auf ein DIVAR IP all-in-one System zuzugreifen, müssen Sie auf Ihrem DIVAR IP all-in-one System und auf dem Router eine Portweiterleitung konfigurieren.

So richten Sie die Portweiterleitung ein:

- ▶ Geben Sie die folgenden Portregeln in den Einstellungen für die Portweiterleitung Ihres Routers ein:
 - Port 5322 für den SSH-Tunnelzugang mit BVMS Operator Client.
Hinweis: Diese Verbindung ist nur im Betriebsmodus BVMS anwendbar.
 - Port 443 für HTTPS-Zugriff auf VRM mit Video Security Client oder Video Security App.
Hinweis: Diese Verbindung ist nur für den Betriebsmodus BVMS oder VRM anwendbar.
- Ihre DIVAR IP all-in-one ist jetzt über das Internet zugänglich.

6.3 Wählen eines geeigneten Clients

Es gibt zwei Möglichkeiten, eine Fernverbindung zu Ihrem DIVAR IP all-in-one System herzustellen:

- *Fernverbindung mit BVMS Operator Client, Seite 16.*
- *Fernverbindung mit Video Security App, Seite 17.*



Hinweis!

Die Kompatibilität der Versionen von BVMS Operator Client oder Video Security App wird durch die im BVMS oder VRM installierten Versionen der Software DIVAR IP bestimmt. Ausführliche Informationen finden Sie in der jeweiligen Software-Dokumentation und im Schulungsmaterial.

6.3.1 Fernverbindung mit BVMS Operator Client




Hinweis!

Diese Verbindung ist nur für den Betriebsmodus BVMS anwendbar.

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 Folgendes ein und klicken Sie dann auf **OK**.
Benutzername: admin (oder ein anderer Benutzer, falls einer konfiguriert ist)
Passwort: Benutzerpasswort
Verbindung: ssh://[public-IP-address-of-DIVAR-IP_all-in-one]:5322

6.3.2 Fernverbindung mit Video Security App



Hinweis!

Diese Verbindung ist nur für den Betriebsmodus BVMS oder VRM anwendbar.

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 Folgendes ein:
Benutzername: admin (oder ein anderer Benutzer, falls einer konfiguriert ist)
Passwort: Benutzerpasswort

6.4 Verbindungsaufbau mit einem Enterprise Management Server

Für eine zentrale Verwaltung mehrerer DIVAR IP all-in-one Systeme im Betriebsmodus BVMS können Sie einen BVMS Enterprise Management Server verwenden, der auf einem separaten Server installiert ist.

Ausführliche Informationen zur Konfiguration und zum Betrieb von BVMS Enterprise System finden Sie in der BVMS-Dokumentation und im Schulungsmaterial.

7 Wartung

7.1 Anmeldung beim Administratorkonto

Anmeldung beim Administratorkonto im BVMS-Betriebsmodus

So melden Sie sich bei dem Administratorkonto im BVMS-Betriebsmodus an:

1. Drücken Sie auf dem BVMS-Desktop Strg+Alt+Entf.
2. Halten Sie die linke Umschalt-Taste gedrückt, unmittelbar nachdem Sie auf **Benutzer wechseln** geklickt haben.
3. Drücken Sie erneut Strg+Alt+Entf.
4. Wählen Sie den **BVRAdmin**-Benutzer und geben Sie das Passwort ein, das bei der Systemkonfiguration festgelegt wurde. Drücken Sie dann Eingabe.

Hinweis: Um zum BVMS-Desktop zurückzukehren, drücken Sie Strg+Alt+Entf und klicken Sie auf **Benutzer wechseln** oder **Abmelden**. Das System kehrt automatisch zum BVMS-Desktop zurück, ohne dass ein Systemneustart erforderlich ist.

Anmeldung mit dem Administratorkonto im Betriebsmodus VRM oder iSCSI

So melden Sie sich bei dem Administratorkonto im VRM- oder iSCSI-Betriebsmodus an:

- ▶ Drücken Sie auf dem Windows-Anmeldebildschirm Strg+Alt+Entf und geben Sie das **BVRAdmin**-Passwort ein.

7.2 Überwachen des Systems

7.2.1 Überwachung des Systems mit der Anwendung SuperDoctor

Die DIVAR IP All-in-One Systeme werden mit der vorinstallierten Anwendung **SuperDoctor** geliefert, mit der Sie Ihr System überwachen können.

Aktivieren der Überwachungsfunktion

So aktivieren Sie die Überwachungsfunktion:

1. Melden Sie sich beim Administratorkonto an (siehe *Anmeldung beim Administratorkonto, Seite 18*).
2. Klicken Sie auf dem Desktop im Ordner **Tools** mit der rechten Maustaste auf das Skript **startSD5Service** und dann auf **Run with PowerShell**.
3. Doppelklicken Sie auf das **SuperDoctor 5 Web**-Symbol auf dem Desktop.
4. Melden Sie sich an der Webschnittstelle mit den folgenden Standard-Anmeldedaten an:
 - Benutzername: **admin**
 - Passwort: **DivaripSD5**
5. Klicken Sie auf die Registerkarte **Configuration** und dann auf **Account Setting** und ändern Sie das Standardpasswort.
Hinweis: Bosch empfiehlt dringend, das Standardpasswort unmittelbar nach der ersten Anmeldung bei der Anwendung **SuperDoctor** zu ändern.
6. Klicken Sie unter der Registerkarte **Configuration** auf **Alert Configuration**.
7. Aktivieren Sie die Funktion **SNMP Trap** und geben Sie die IP-Adresse des Empfängers für SNMP-Traps an.

Deaktivieren der Überwachungsfunktion

So deaktivieren Sie die Überwachungsfunktion:

1. Melden Sie sich beim Administratorkonto an (siehe *Anmeldung beim Administratorkonto, Seite 18*).
2. Klicken Sie auf dem Desktop im Ordner **Tools** mit der rechten Maustaste auf das Skript **stopSD5Service** und dann auf **Run with PowerShell**.

7.2.2

Überwachung des Systems über die IPMI-Schnittstelle

Das DIVAR IP all-in-one 6000 verfügt über einen speziellen IPMI-Anschluss an der Rückseite. Sie können die IPMI-Schnittstelle verwenden, um auf Ihr DIVAR IP all-in-one 6000 System zuzugreifen, es zu überwachen, zu diagnostizieren und als Remote-Server zu verwalten. Jedes DIVAR IP all-in-one 6000 Gerät wird mit dem Standardbenutzernamen ADMIN und einem Initialpasswort geliefert. Das Initialpasswort ist bei jedem Gerät einzigartig. Sie finden es auf dem Etikett an der Geräterückseite unter dem IPMI-Anschluss. Bosch empfiehlt ausdrücklich, das Initialpasswort während der IPMI-Konfiguration zu ändern und das neue Passwort an einem sicheren Ort zu speichern.



Hinweis!

Aus Sicherheitsgründen sollte das Gerät nicht dauerhaft über den IPMI-Anschluss mit einem öffentlichen Netzwerk verbunden sein.

So konfigurieren Sie die IPMI-Einstellungen:

1. Schalten Sie das Gerät ein und drücken Sie die Entf-Taste, um in das BIOS-Setup zu gelangen.
2. Navigieren Sie im BIOS-Setup zur Registerkarte **IPMI**.
3. Wählen Sie die Option **BMC Network Configuration** aus und drücken Sie dann die Eingabe-Taste.
4. Wählen Sie im nächsten Dialogfeld die Option **Update IPMI LAN Configuration** aus und drücken Sie dann die Eingabe-Taste.
Das Dialogfeld **Update IPMI LAN Configuration** wird angezeigt.
5. Wählen Sie im Dialogfeld **Update IPMI LAN Configuration** die Option **Yes** aus und drücken Sie dann die Eingabe-Taste.
6. Legen Sie die gewünschten Netzwerkkonfigurationsparameter fest.
7. Drücken Sie die Tasten F4 und Eingabe, um zu speichern und das BIOS-Setup zu verlassen.

Das DIVAR IP all-in-one 6000 Gerät wird neu gestartet.

7.3

Ersetzen einer defekten Festplatte und Konfigurieren einer neuen Festplatte

Wenn eine Festplatte, die in Ihrem DIVAR IP all-in-one 6000 System installiert ist, defekt ist, leuchtet die entsprechende LED des Festplattenfachs rot. In diesem Fall müssen Sie wie folgt vorgehen:

1. *Austausch einer defekten Festplatte, Seite 20.*
2. *Wiederherstellung von RAID5 mit der neuen Festplatte, Seite 20.*



Hinweis!

Dieses Verfahren gilt nur für eine Standard-RAID5-Konfiguration und nur für den Fall, dass eine einzelne Festplatte in der RAID5-Konfiguration defekt ist. Nur in diesem Fall kann sichergestellt werden, dass keine Daten verloren gehen.



Hinweis!

Bosch haftet nicht für Datenverluste, Schäden oder Systemausfälle von Geräten, die mit Festplatten ausgestattet sind, die nicht von Bosch geliefert wurden. Bosch kann keine Unterstützung leisten, wenn nicht von Bosch gelieferte Festplatten als Ursache für das Problem angesehen werden. Für die Fehlersuche bei möglichen Hardwareproblemen müssen von Bosch gelieferte Festplatten installiert werden.


7.3.1 Austausch einer defekten Festplatte

So ersetzen Sie eine defekte Festplatte:

- ▶ Entfernen Sie die defekte Festplatte aus dem Gerät und installieren Sie die neue Festplatte.
Lesen Sie das Kapitel *Installation einer SATA-Festplatte* im Installationshandbuch.


7.3.2 Wiederherstellung von RAID5 mit der neuen Festplatte

Automatischer RAID5-Neuaufbau

1. Doppelklicken Sie auf dem DIVAR IP all-in-one-Desktop auf die **Launch LSA**-Verknüpfung. Die Anwendung **LSI Storage Authority** wird gestartet und die Seite **Remote Server Discovery** wird angezeigt.
2. Melden Sie sich mit den Anmeldedaten des Administratorkontos **BVRAdmin** an. Es wird ein Dialogfeld angezeigt, das darauf hinweist, dass es einen Controller gibt, der ein kritisches Problem hat.
3. Klicken Sie auf die Leiste **Controller ID:**, um die Controller-Einstellungen zu öffnen.
 - Wenn Sie die defekte Festplatte noch nicht entfernt haben, wird sie unter **Drives > Foreign Drives > Unconfigured Drives** angezeigt.
 - Sobald Sie die defekte Festplatte entfernt und die neue Festplatte installiert haben, beginnt das System automatisch mit dem Wiederaufbau des RAID5 mit der neuen Festplatte und ein Fortschrittsbalken zeigt den Fortschritt des Wiederaufbaus an.
4. Nach erfolgreichem Abschluss des Neuaufbaus wird das -Symbol angezeigt.

Manueller RAID5-Neuaufbau

Wenn der RAID5-Rebuild der neuen Festplatte nicht automatisch startet, gehen Sie wie folgt vor:

1. Wählen Sie im Dialogfeld „Controller-Einstellungen“ unter **Drives > Foreign Drives > Unconfigured Drives**, die Festplatte mit dem Status **Unconfigured Bad** aus, und wählen Sie dann im rechten Fensterbereich **Make Unconfigured Good** aus. Es wird ein Dialogfeld angezeigt.
2. Aktivieren Sie das Kontrollkästchen **Confirm**, und klicken Sie auf **Yes, Make Unconfigured Good**, um fortzufahren. Das System beginnt den RAID5-Neuaufbau mit der neuen Festplatte.
3. Nach erfolgreichem Abschluss des Neuaufbaus wird das -Symbol angezeigt.

7.4 Sammeln von DIVAR IP System Manager-Logdateien

Die Anwendung DIVAR IP System Manager enthält ein spezielles Skript, das die Sammlung von Logdateien vereinfacht.

So Sammeln Sie DIVAR IP System Manager-Logdateien:

1. Melden Sie sich beim Administratorkonto an (siehe *Anmeldung beim Administratorkonto, Seite 18*).
2. Klicken Sie im Windows-**Startmenü** auf **Export System Manager Logs**. Das Skript exportiert die Logdateien in den Ordner *Documents\Bosch* und erstellt eine ZIP-Datei mit folgender Namensstruktur *SysMgrLogs-[date]_[time]*. Sie können diese ZIP-Datei verwenden, um sie an die detaillierte Fehlerbeschreibung anzuhängen.

7.5 Wiederherstellen des Geräts

So stellen Sie das Gerät wieder her:

1. Schalten Sie das Gerät ein und drücken Sie während des BIOS-Power-On-Self-Tests (Selbsttest beim Einschalten) die F7-Taste, um Windows PE zu öffnen.
Das Dialogfeld **System Management Utility** wird angezeigt.
2. Wählen Sie eine der folgenden Optionen aus:
 - **System factory default:** Mit dieser Option werden Videodatenpartitionen formatiert und die Betriebssystempartition mit dem Standard-Image des Geräts wiederhergestellt.
Dieser Vorgang kann bis zu 5 Minuten dauern.
 - **Full data overwrite and system factory default:** Mit dieser Option werden Videodatenpartitionen formatiert, vorhandene Daten vollständig überschrieben und die Betriebssystempartition mit dem Standard-Image des Geräts wiederhergestellt.
Hinweis: Dieser Vorgang kann bis zu 110 Stunden dauern.
 - **OS system recovery only:** Mit dieser Option werden die Betriebssystempartition mit dem Standard-Image des Geräts wiederhergestellt und vorhandene virtuelle Festplatten aus vorhandenen Videodatenpartitionen importiert.
Dieser Vorgang kann bis zu 5 Minuten dauern.

Hinweis:

Mit der Option **OS system recovery only** wird kein Videomaterial gelöscht, das auf den Daten-Festplatten gespeichert ist. Durch den Vorgang wird jedoch die gesamte Betriebssystempartition (einschließlich der Einstellungen des Videomanagementsystems) durch eine Standardkonfiguration ersetzt. Damit Sie nach der Wiederherstellung auf das vorhandene Videomaterial zugreifen können, muss die Konfiguration des Videomanagementsystems vor der Systemwiederherstellung exportiert und danach erneut importiert werden.



Hinweis!

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

3. Bestätigen Sie die ausgewählte Option.
Das System beginnt mit dem Prozess der Formatierung und Image-Wiederherstellung.
4. Bestätigen Sie nach abgeschlossener Wiederherstellung den Systemneustart.
Das System wird neu gestartet und es werden Konfigurationsroutinen durchgeführt.
5. Nachdem der Vorgang abgeschlossen ist, wird der Bildschirm mit der Windows-Sprachauswahl angezeigt.
6. Fahren Sie mit der Ersteinrichtung des Systems fort.

Siehe

- *Erstmalige Anmeldung und erste Systemkonfiguration, Seite 10*

8 Zusatzinformationen

8.1 Zusätzliche Dokumentation und Client-Software

Weitere Informationen, Software und Dokumentation finden Sie unter <http://www.boschsecurity.com> im Produktkatalog auf der entsprechenden Produktseite.

Die aktuelle Software und die verfügbaren Upgrade-Pakete finden Sie im Download Store von Bosch Security and Safety Systems unter:

<https://downloadstore.boschsecurity.com/>

8.2 Supportdienstleistungen und Bosch Academy



Support

Supportdienstleistungen erhalten Sie unter www.boschsecurity.com/xc/en/support/.



Bosch Building Technologies Academy

Besuchen Sie die Website der Bosch Building Technologies Academy und erhalten Sie Zugang zu **Schulungskursen, Videoanleitungen** und **Dokumenten**: www.boschsecurity.com/xc/en/support/training/

Bosch Security Systems B.V.

Torenallee 49

5617 BA Eindhoven

Niederlande

www.bosch-sicherheitssysteme.de

© Bosch Security Systems B.V., 2022

Building solutions for a better life.

202211241306