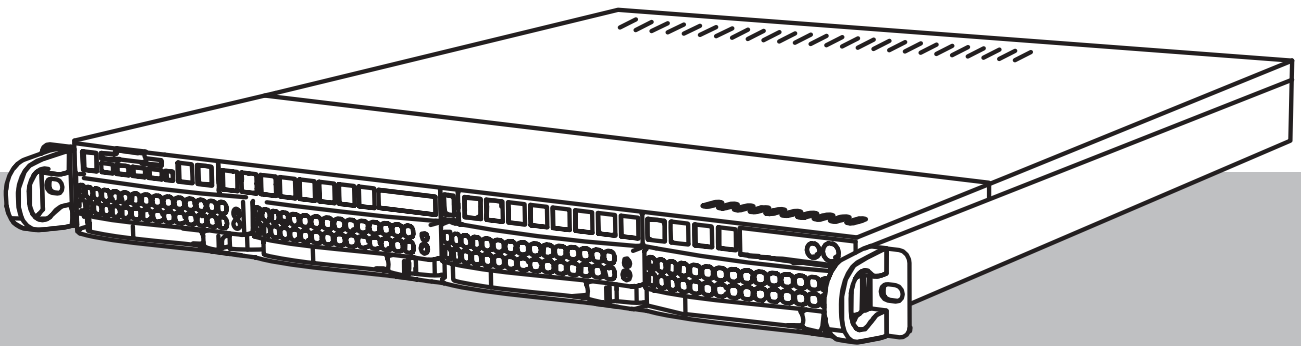


DIVAR IP all-in-one 6000

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



Sommaro

1	Sicurezza	4
1.1	Precauzioni d'uso	4
1.2	Precauzioni per la sicurezza informatica	5
1.3	Precauzioni software	6
1.3.1	Utilizzare il software più recente	6
1.3.2	Informazioni OSS	6
2	Introduzione	7
3	Panoramica del sistema	8
4	Setup del sistema	9
4.1	Impostazioni predefinite	9
4.2	Prerequisiti	9
4.3	Primo accesso e setup iniziale del sistema	9
4.3.1	Scelta della modalità operativa BVMS	11
4.3.2	Scelta della modalità operativa VRM	12
4.3.3	Scelta della modalità operativa Archiviazione iSCSI	12
5	Aggiornamento del software	13
5.1	Aggiornamento di DIVAR IP System Manager	13
5.2	Aggiornamento del software mediante DIVAR IP System Manager	13
6	Collegamento remoto al sistema	16
6.1	Proteggere il sistema da accessi non autorizzati	16
6.2	Configurazione dell'inoltro porta	16
6.3	Scegliere un client appropriato	16
6.3.1	Connessione remota a Operator Client BVMS	16
6.3.2	Connessione remota a Video Security App	17
6.4	Collegamento a un Enterprise Management Server	17
6.5	Connessione a Remote Portal	17
6.5.1	Creazione di un account Remote Portal	18
6.5.2	Registrazione dei dispositivi DIVAR IP all-in-one in Remote Portal	18
6.5.3	Annullamento della registrazione dei dispositivi DIVAR IP all-in-one da Remote Portal	18
7	Manutenzione	19
7.1	Accesso all'account amministratore	19
7.2	Monitoraggio del sistema	19
7.2.1	Monitoraggio del sistema mediante l'applicazione SuperDoctor	19
7.2.2	Monitoraggio del sistema mediante l'interfaccia IPMI	19
7.3	Sostituzione di un disco rigido difettoso e configurazione di un nuovo disco rigido	20
7.3.1	Sostituzione di un disco rigido difettoso	20
7.3.2	Ricostruzione di RAID5 con il nuovo disco rigido	21
7.4	Raccolta dei file di registro di DIVAR IP System Manager	21
7.5	Ripristino dell'unità	21
8	Informazioni aggiuntive	23
8.1	Documentazione aggiuntiva e software client	23
8.2	Servizi di supporto e Bosch Academy	23

1 Sicurezza

Osservare le norme di sicurezza descritte in questo capitolo.

1.1 Precauzioni d'uso

**Avviso!**

Destinazione d'uso

Questo prodotto è esclusivamente per uso professionale. Non è progettato per essere installato in un'area pubblica accessibile a chiunque.

**Avviso!**

Non usare questo prodotto in un punto umido o bagnato.

**Avviso!**

Adottare precauzioni per proteggere il dispositivo da sbalzi di corrente e fulmini.

**Avviso!**

Mantenere l'area intorno al dispositivo pulita e ordinata.

**Avviso!**

Aperture della custodia

Non ostruire o coprire le aperture. Le aperture della custodia sono presenti ai fini della ventilazione del dispositivo. Queste aperture evitano il surriscaldamento e garantiscono un funzionamento affidabile.

**Avviso!**

Non aprire o rimuovere il coperchio del dispositivo. L'apertura o la rimozione del coperchio può causare danni al sistema e invalidare la garanzia.

**Avviso!**

Non versare liquidi sul dispositivo.

**Avvertenza!**

Prestare attenzione durante operazioni di manutenzione ed utilizzo in prossimità del backplane. Durante il funzionamento del sistema, possono verificarsi problemi di tensione o elettricità sul backplane. Non toccare il backplane con oggetti metallici ed assicurarsi che nessun cavo a nastro tocchi il backplane.

**Avviso!**

Scollegare l'alimentazione prima di spostare il prodotto. Il prodotto deve essere spostato con cautela. L'uso di una forza eccessiva o eventuali urti possono danneggiare il prodotto e le unità disco rigido.

**Avvertenza!**

La gestione di materiali in lega di piombo utilizzati in questo prodotto potrebbe esporre l'utente al contatto con una sostanza chimica ritenuta, dallo stato della California, come causa di difetti congeniti e problemi all'apparato riproduttivo.

**Avviso!**

La perdita del segnale video è una caratteristica delle registrazioni video digitali, pertanto Bosch Security Systems non è responsabile di eventuali danni dovuti alla mancanza di informazioni video.

Per ridurre al minimo il rischio di perdita di informazioni digitali, si consiglia di utilizzare più sistemi di registrazione ridondanti ed una procedura di backup di tutte le informazioni analogiche e digitali.

1.2**Precauzioni per la sicurezza informatica**

Per motivi di sicurezza informatica, attenersi alla seguente procedura:

- Accertarsi che l'accesso fisico al sistema sia limitato al personale autorizzato. Posizionare il sistema in un'area protetta tramite controllo degli accessi per evitare manipolazioni fisiche.
- Il sistema operativo include le ultime patch di protezione di Windows disponibili al momento in cui è stata creata l'immagine del software. Utilizzare la funzionalità di aggiornamento online di Windows o le patch corrispondenti a rilascio mensile da installare offline per installare periodicamente gli aggiornamenti di sicurezza del sistema operativo.
- Non disattivare Windows Defender e il firewall di Windows e mantenerli sempre aggiornati.
- Non installare software antivirus aggiuntivo.
- Non fornire informazioni di sistema e dati sensibili a persone che non si conoscono se non si è certi che tali persone sono autorizzate a ricevere tali dati e informazioni.
- Non inviare informazioni sensibili su Internet senza prima controllare la sicurezza di un sito web.
- Limitare l'accesso alla rete locale solo ai dispositivi attendibili. Informazioni dettagliate sono riportate nei seguenti documenti, che sono disponibili nel catalogo online dei prodotti:
 - *Autenticazione di rete 802.1X*
 - *Guida alla sicurezza informatica per i prodotti video IP Bosch*
- Per l'accesso tramite reti pubbliche, utilizzare esclusivamente canali di comunicazione (crittografati) protetti.
- L'account amministratore fornisce privilegi amministrativi completi e l'accesso illimitato al sistema. I diritti di amministrazione consentono agli utenti di installare, aggiornare o rimuovere il software e di modificare le impostazioni di configurazione. Inoltre, permettono agli utenti di accedere alle chiavi di registro del sistema e di modificarle direttamente per aggirare la gestione centralizzata e le impostazioni di sicurezza. Gli utenti che hanno eseguito l'accesso all'account amministratore possono attraversare il firewall e rimuovere il software antivirus, esponendo il sistema a virus e attacchi informatici. Ciò può comportare un rischio elevato per il sistema e la sicurezza dei dati. Per ridurre al minimo i rischi per la sicurezza informatica, procedere come segue:
 - Verificare che l'account amministratore sia protetto con una password complessa in base ai criteri password.

- Accertarsi che solo un numero limitato di utenti attendibili abbia accesso all'account amministratore.
- A causa dei requisiti di funzionamento, l'unità di sistema non deve essere crittografata. Senza la crittografia, è possibile accedere ai dati memorizzati sull'unità e rimuoverli facilmente. Per evitare furti di dati o perdite accidentali di dati, accertarsi che solo le persone autorizzate abbiano accesso al sistema e all'account amministratore.
- Per l'installazione e l'aggiornamento del software e per il ripristino del sistema potrebbe essere necessario utilizzare dispositivi USB. Pertanto, le porte USB del sistema non devono essere disabilitate. Tuttavia, il collegamento dei dispositivi USB al sistema comporta il rischio di infezione da malware. Per evitare attacchi malware, accertarsi che nessun dispositivo USB infetto sia collegato al sistema.

1.3 Precauzioni software

1.3.1 Utilizzare il software più recente

Prima di utilizzare il dispositivo per la prima volta, accertarsi di installare la versione più recente del software in uso. Per garantire funzionamento, compatibilità, prestazioni e sicurezza costanti, aggiornare regolarmente il software per tutta la durata operativa del dispositivo. Attenersi alle istruzioni fornite nella documentazione del prodotto relative agli aggiornamenti del software.

Ulteriori informazioni sono disponibili tramite i collegamenti seguenti:

- Informazioni generali: <https://www.boschsecurity.com/xc/en/support/product-security/>
- Avvertenze per la sicurezza, un elenco di vulnerabilità individuate e soluzioni proposte: <https://www.boschsecurity.com/xc/en/support/product-security/security-advisories.html>

Bosch declina ogni responsabilità per danni provocati dall'utilizzo dei prodotti con componenti software obsoleti.

Il software più recente e i pacchetti di upgrade disponibili sono reperibili nel download store di Bosch Security and Safety Systems, in: <https://downloadstore.boschsecurity.com/>

1.3.2 Informazioni OSS

Bosch utilizza software open source per i prodotti DIVAR IP all-in-one.

Le licenze dei componenti software open source dell'unità del sistema sono disponibili qui:

C:\license txt\

Le licenze dei componenti software open source utilizzate in qualsiasi altro software installato nel sistema vengono archiviate nella cartella di installazione del relativo software, ad esempio in:

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

o in:

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

2 Introduzione

DIVAR IP all-in-one 6000 è una soluzione all-in-one economica e di facile utilizzo per la registrazione, la visualizzazione e la gestione dei sistemi di sorveglianza in rete con un massimo di 64 canali (con licenza per 8 canali in dotazione).

DIVAR IP all-in-one 6000 è un'unità per installazione in rack 1U che combina funzionalità Bosch Video Management System avanzate e una gestione delle registrazioni avanzata e all'avanguardia in un solo dispositivo di registrazione facile da installare e da utilizzare e dal prezzo conveniente, per i clienti interessati alle tecnologie informatiche.

DIVAR IP all-in-one 6000 utilizza un design compatto e componenti di base ed è basato sul sistema operativo Microsoft Windows Server IoT 2022 for Storage Workgroup. DIVAR IP all-in-one 6000 presenta unità disco rigido SATA hot-swappable "dedicate all'impresa" con capacità di archiviazione globale massima di 72 TB.

3 Panoramica del sistema

Sistema operativo

Il sistema operativo Microsoft Windows Server IoT 2022 for Storage Workgroup offre un'interfaccia utente per la configurazione iniziale del server, gestione unificata dei dispositivi di archiviazione, semplice configurazione e gestione dell'archiviazione, nonché il supporto di Destinazione software iSCSI Microsoft.

Ciò rappresenta la soluzione ideale per fornire prestazioni ottimali per l'archiviazione con connessione in rete. Il sistema operativo Microsoft Windows Server IoT 2022 for Storage Workgroup offre notevoli miglioramenti relativi alla gestione di condivisione e archiviazione e all'integrazione di funzionalità e componenti per la gestione dei dispositivi di archiviazione.

DIVAR IP System Manager

L'applicazione DIVAR IP System Manager è l'interfaccia utente centrale che consente il setup, la configurazione e l'aggiornamento software semplificati del sistema.

Modalità operative

I sistemi DIVAR IP all-in-one 6000 possono funzionare in tre modalità diverse:

- Sistema completo di registrazione e gestione di video, che utilizza i componenti e i servizi di base di BVMS e Video Recording Manager.
Questa modalità offre una soluzione di videosorveglianza IP avanzata in grado di gestire in modo ottimale video, audio e dati in formato digitale su una rete IP. Combina perfettamente encoder e telecamere IP, offrendo la gestione di allarmi ed eventi nell'intero sistema, il monitoraggio dello stato del sistema e la gestione degli utenti e delle priorità. Questa modalità rappresenta il miglior Video Management System per l'utilizzo con dispositivi di videosorveglianza Bosch, sfruttando le funzionalità esclusive delle soluzioni di registrazione e delle telecamere Bosch. Include componenti Video Streaming Gateway per l'integrazione di telecamere di terze parti.
- Soluzione di videoregistrazione avanzata per un sistema BVMS, che utilizza i componenti e servizi di base di Video Recording Manager, sfruttando le funzionalità esclusive delle soluzioni di registrazione e delle telecamere Bosch. È possibile aggiungere fino a due server Video Recording Manager a un sistema BVMS in esecuzione su un dispositivo DIVAR IP all-in-one.
- Espansione di memoria iSCSI per un sistema BVMS, in esecuzione su un hardware distinto. È possibile aggiungere fino a quattro di queste espansioni di memoria iSCSI a un sistema BVMS in esecuzione su un dispositivo DIVAR IP all-in-one 6000.

Durante l'impostazione del sistema, nell'applicazione DIVAR IP System Manager è necessario scegliere la modalità operativa desiderata per configurare il sistema.

L'applicazione DIVAR IP System Manager consente inoltre di eseguire l'aggiornamento e l'upgrade del software installato.

Il software più recente e i pacchetti di upgrade disponibili sono reperibili nel download store di Bosch Security and Safety Systems, in:

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



Avviso!

I flussi video registrati devono essere configurati in modo da non superare la larghezza di banda massima del sistema (sistema base BVMS/VRM più espansioni di memoria iSCSI).

4 Setup del sistema

4.1 Impostazioni predefinite

Tutti i sistemi DIVAR IP sono preconfigurati con un indirizzo IP predefinito e impostazioni iSCSI predefinite:

- Indirizzo IP: automaticamente assegnato da DHCP (indirizzo IP di fallback: 192.168.0.200).
- Subnet Mask: automaticamente assegnata da DHCP (subnet mask di fallback: 255.255.255.0).

Impostazioni utente predefinite per l'account amministratore

- Nome utente: **BVRAdmin**
- Password: da impostare al primo accesso.
Requisiti per la password:
 - Minimo 14 caratteri.
 - Almeno una lettera maiuscola.
 - Almeno una lettera minuscola.
 - Almeno un numero.

4.2 Prerequisiti

Attenersi alle indicazioni seguenti:

- DIVAR IP deve essere dotato di un collegamento di rete attivo durante l'installazione. Accertarsi che l'interruttore di rete a cui si è collegati sia acceso.
- L'indirizzo IP predefinito non deve essere occupato da altri dispositivi nella rete. Verificare che gli indirizzi IP predefiniti dei sistemi DIVAR IP presenti nella rete vengano modificati prima di aggiungere un altro DIVAR IP.

4.3 Primo accesso e setup iniziale del sistema



Avviso!

Non modificare le impostazioni del sistema operativo. La modifica di queste impostazioni potrebbe causare il malfunzionamento del sistema.



Avviso!

Per eseguire attività di amministrazione, è necessario eseguire l'accesso all'account amministratore.



Avviso!

In caso di smarrimento della password, è necessario eseguire un ripristino del sistema, come indicato nel manuale di installazione. La configurazione deve essere effettuata da zero o deve essere importata.

Per configurare il sistema:

1. Connettere l'unità DIVAR IP all-in-one e le telecamere alla rete.
2. Accendere l'unità.


Vengono eseguite le routine di configurazione per Microsoft Windows Server IoT 2022 for Storage Workgroup. Questo processo può richiedere alcuni minuti. Non spegnere il sistema.

Al termine del processo, viene visualizzata la schermata di selezione della lingua di Windows.

3. Selezionare il proprio paese/regione, la lingua del sistema operativo desiderata e il layout della tastiera dall'elenco, quindi fare clic su **Avanti**.
Vengono visualizzati i termini della licenza software Microsoft.
4. Fare clic su **Accetta** per accettare le condizioni di licenza e attendere il riavvio di Windows. L'operazione può richiedere alcuni minuti. Non spegnere il sistema.
Dopo il riavvio, viene visualizzata la schermata di accesso di Windows.
5. Impostare una nuova password per l'account amministratore **BVRAdmin** e confermarla.
Requisiti per la password:
 - Minimo 14 caratteri.
 - Almeno una lettera maiuscola.
 - Almeno una lettera minuscola.
 - Almeno un numero.Premere Invio.
Viene visualizzata la pagina **Software Selection**.
6. Il sistema ricerca automaticamente nell'unità locale e in qualsiasi supporto di archiviazione esterno collegato il file di installazione di DIVAR IP System Manager, **SystemManager_x64_[software version].exe**, che si trova in una cartella con la seguente struttura: `Drive root\BoschAppliance\`.
La ricerca può richiedere alcuni istanti. Attendere il completamento dell'operazione.
7. Una volta che il sistema rileva il file di installazione, questo viene visualizzato nella pagina **Software Selection**. Fare clic sulla barra in cui viene visualizzato il file di installazione per avviare l'installazione.
Attenzione: accertarsi che sia installata la versione più recente di DIVAR IP System Manager. Il software più recente e i pacchetti di upgrade disponibili sono reperibili nel download store di Bosch Security and Safety Systems, in: <https://downloadstore.boschsecurity.com/>.
8. Se durante la scansione non viene trovato il file di installazione, procedere come segue:
 - Passare a <https://downloadstore.boschsecurity.com/>.
 - Nella scheda **Software**, selezionare **BVMS Appliances** nell'elenco, quindi fare clic su **Select**.
Viene visualizzato un elenco di tutti i pacchetti software disponibili.
 - Individuare il file ZIP **SystemManager_[software version].zip** e salvarlo in un supporto di memorizzazione, ad esempio un supporto USB.
 - Decomprimere il file nel supporto di memorizzazione verificando che la cartella **BoschAppliance** si trovi nella directory principale.
 - Connettere il supporto di memorizzazione al sistema DIVAR IP all-in-one.
Il sistema ricerca automaticamente il file di installazione nel supporto di memorizzazione.
La scansione può richiedere alcuni istanti. Attendere il completamento dell'operazione.
 - Una volta rilevato, il file di installazione viene visualizzato nella pagina **Software Selection**. Fare clic sulla barra che mostra il file di installazione per avviare l'installazione.
Nota: per poter essere rilevato automaticamente, il file di installazione deve trovarsi in una cartella con la seguente struttura: `Drive root\BoschAppliance\` (ad esempio `F:\BoschAppliance\`).

Se il file di installazione si trova in un'altra posizione non corrispondente alla



struttura delle cartelle predefinita, fare clic su  per passare alla relativa posizione. Quindi fare clic sul file di installazione per avviare l'installazione.

9. Prima dell'avvio dell'installazione, viene visualizzata la finestra di dialogo **End User License Agreement (EULA)**. Leggere i termini di licenza, quindi fare clic su **Accept** per continuare. L'installazione inizia.
10. Al termine dell'installazione, il sistema viene riavviato e si viene indirizzati alla pagina di accesso di Windows. Accedere all'account amministratore.
11. Viene aperto il browser Microsoft Edge e viene visualizzata la pagina **DIVAR IP - Configurazione del sistema**. Nella pagina vengono visualizzati il tipo di dispositivo, il numero di serie, le tre modalità operative e le versioni software disponibili per ciascuna di esse.

Per configurare il sistema DIVAR IP all-in-one, è necessario scegliere la modalità operativa e la versione software desiderate.

Nota: se la versione software desiderata per una determinata modalità non è disponibile in un'unità locale, seguire questa procedura:

- Passare a <https://downloadstore.boschsecurity.com/>.
- Nella scheda **Software**, selezionare **BVMS Appliances** nell'elenco, quindi fare clic su **Select**. Viene visualizzato un elenco di tutti i pacchetti software disponibili.
- Individuare i file ZIP dei pacchetti software desiderati, ad esempio **BVMS_[BVMS version]_SystemManager_package_[package version].zip**, e salvarli in un supporto di memorizzazione, ad esempio un supporto USB.
- Decomprimere i file nel supporto di memorizzazione. Non modificare la struttura delle cartelle dei file compressi.
- Collegare quindi il supporto di memorizzazione al sistema DIVAR IP all-in-one.



Avviso!

La modifica della modalità operativa dopo l'installazione richiede un ripristino completo delle impostazioni di fabbrica.

4.3.1

Scelta della modalità operativa BVMS

Per utilizzare DIVAR IP all-in-one come sistema completo di registrazione e gestione di video:

1. Nella pagina **DIVAR IP - Configurazione del sistema**, selezionare la modalità operativa **BVMS** e la versione di BVMS che si desidera installare, quindi fare clic su **Successivo**. Viene visualizzato il contratto di licenza di BVMS.
2. Leggere e accettare il contratto di licenza, quindi fare clic su **Installa** per continuare. Viene avviata l'installazione e una finestra di dialogo mostra lo stato dell'installazione. Durante il processo di installazione non spegnere il sistema e non rimuovere i supporti di archiviazione.
3. Una volta installati tutti i pacchetti software, il sistema viene riavviato. Dopo il riavvio, viene visualizzato il desktop di BVMS.
4. Sul desktop di BVMS, fare clic sull'applicazione desiderata per configurare il sistema.

**Avviso!**

Per ulteriori informazioni, consultare il corso di formazione DIVAR IP all-in-one sul Web e la documentazione di BVMS.

Il corso di formazione è disponibile al seguente indirizzo: www.boschsecurity.com/xc/en/support/training/

4.3.2**Scelta della modalità operativa VRM**

Per utilizzare il sistema DIVAR IP all-in-one unicamente come sistema di registrazione video:

1. Nella pagina **DIVAR IP - Configurazione del sistema**, selezionare la modalità operativa **VRM** e la versione di VRM che si desidera installare, quindi fare clic su **Successivo**. Viene visualizzato il contratto di licenza di VRM.
2. Leggere e accettare il contratto di licenza, quindi fare clic su **Installa** per continuare. Viene avviata l'installazione e una finestra di dialogo mostra lo stato dell'installazione. Durante il processo di installazione non spegnere il sistema e non rimuovere i supporti di archiviazione.
3. Una volta installati tutti i pacchetti software, il sistema viene riavviato. Dopo il riavvio, viene visualizzata la schermata di accesso di Windows.

**Avviso!**

Per ulteriori informazioni, fare riferimento alla documentazione di VRM.

4.3.3**Scelta della modalità operativa Archiviazione iSCSI**

Per utilizzare il sistema DIVAR IP all-in-one come espansione di memoria iSCSI:

1. Nella pagina **DIVAR IP - Configurazione del sistema**, selezionare la modalità operativa **Archiviazione iSCSI** e la versione corrispondente che si desidera installare, quindi fare clic su **Successivo**. Viene visualizzata la finestra di dialogo di installazione.
2. Nella finestra di dialogo di installazione, fare clic su **Installa** per continuare. L'installazione inizia e viene visualizzata una finestra di dialogo che ne indica lo stato. Durante il processo di installazione, non spegnere il sistema e non rimuovere il supporto di memorizzazione.
3. Una volta installati tutti i pacchetti software, il sistema viene riavviato. Dopo il riavvio, viene visualizzata la schermata di accesso di Windows.
4. Aggiungere il sistema come espansione di memoria iSCSI su un sistema BVMS esterno o su server VRM mediante BVMS Configuration Client o Configuration Manager.

**Avviso!**

Per ulteriori informazioni, fare riferimento alla documentazione di BVMS o Configuration Manager.

5 Aggiornamento del software

Accertarsi di eseguire l'aggiornamento di DIVAR IP System Manager alla versione più recente.

5.1 Aggiornamento di DIVAR IP System Manager

1. Passare a <https://downloadstore.boschsecurity.com/>.
2. Nella scheda **Software**, selezionare **BVMS Appliances** nell'elenco, quindi fare clic su **Select**.
Viene visualizzato un elenco di tutti i pacchetti software disponibili.
3. Individuare il file ZIP **SystemManager_ [versione software 2.0.0 o superiore].zip** e salvarlo in un supporto di memorizzazione, ad esempio un supporto USB.
4. Decomprimere il file nel supporto di memorizzazione.
5. Collegare il supporto di memorizzazione al dispositivo DIVAR IP all-in-one.
6. Avviare DIVAR IP System Manager:
 - Se è stato effettuato l'accesso a Windows con l'account amministratore **BVRAdmin**, fare doppio clic sull'icona DIVAR IP System Manager sul desktop di Windows. DIVAR IP System Manager viene avviato.
 - Se il sistema è in esecuzione nella modalità operativa BVMS, fare clic sull'icona DIVAR IP System Manager sul desktop BVMS e accedere all'account amministratore BVRAdmin. DIVAR IP System Manager si apre in una finestra di dialogo a tutto schermo (è possibile chiudere la finestra di dialogo premendo Alt+ F4).
7. Viene visualizzata la pagina **Pacchetti software**. Selezionare il pacchetto software **DIVAR IP System Manager Commander**, quindi fare clic su **Successivo** per continuare.
Viene visualizzata la finestra di dialogo di installazione.
8. Nella finestra di dialogo di installazione, fare clic su **Installa** per continuare.
Viene avviata l'installazione e l'interfaccia utente viene aggiornata. Il processo può richiedere alcuni minuti. Non spegnere il sistema e non rimuovere il supporto di memorizzazione.
Osservare le notifiche visualizzate nella parte superiore della pagina. Se la riconnessione non riesce, ricaricare la pagina.
9. Al termine dell'installazione, nella pagina **Pacchetti software** selezionare il pacchetto software **DIVAR IP System Manager Executor**, quindi fare clic su **Successivo** per continuare.
Viene visualizzata la finestra di dialogo di installazione.
10. Nella finestra di dialogo di installazione, fare clic su **Installa** per continuare.
Viene avviata l'installazione.
Il processo di installazione può richiedere alcuni minuti. Non spegnere il sistema e non rimuovere il supporto di memorizzazione durante il processo di installazione.
Osservare le notifiche visualizzate nella parte superiore della pagina.

5.2 Aggiornamento del software mediante DIVAR IP System Manager

Con l'applicazione DIVAR IP System Manager è possibile aggiornare il software installato sul sistema.



Il software più recente e i pacchetti di upgrade disponibili sono reperibili nel download store di Bosch Security and Safety Systems, in:

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

**Avviso!**


Il downgrade del software installato a una versione precedente non è supportato.

Per aggiornare il software installato:

1. Passare a <https://downloadstore.boschsecurity.com/>.
2. Nella scheda **Software**, selezionare **BVMS Appliances** nell'elenco, quindi fare clic su **Select**.
Viene visualizzato un elenco di tutti i pacchetti software disponibili.
3. Individuare i file ZIP dei pacchetti software desiderati, ad esempio **BVMS_[BVMS version]_SystemManager_package_[package version].zip**, e salvarli in un supporto di memorizzazione, ad esempio un supporto USB.
4. Decomprimere i file nel supporto di memorizzazione. Non modificare la struttura delle cartelle dei file compressi.
5. Avviare DIVAR IP System Manager:
 - Se è stato effettuato l'accesso a Windows con l'account amministratore **BVRAdmin**, fare doppio clic sull'icona DIVAR IP System Manager sul desktop di Windows. DIVAR IP System Manager viene avviato.
 - Se il sistema è in esecuzione nella modalità operativa BVMS, fare clic sull'icona DIVAR IP System Manager sul desktop BVMS e accedere all'account amministratore BVRAdmin. DIVAR IP System Manager si apre in una finestra di dialogo a tutto schermo (è possibile chiudere la finestra di dialogo premendo Alt+ F4).
6. Viene visualizzata la pagina **Pacchetti software**, nella cui parte superiore sono indicati il tipo e il numero di serie del dispositivo.
 - Nella colonna **Nome** è possibile vedere tutte le applicazioni software DIVAR IP System Manager già installate sul sistema, nonché tutte le ulteriori applicazioni software DIVAR IP System Manager rilevate dal sistema sull'unità **Images** o su un supporto di memoria.
 - Nella colonna **Versione installata**, viene indicata la versione dell'applicazione software installata sul sistema.
 - Nella colonna **Stato** viene indicato lo stato della rispettiva applicazione software:
 - L'icona  indica che il sistema non ha rilevato nessuna versione successiva dell'applicazione software installata sull'unità **Images** o su un supporto di memoria. **Nota:** per essere sicuri di utilizzare la versione più recente del software, controllare le versioni software disponibili nel negozio di download di Bosch Security and Safety Systems all'indirizzo: <https://downloadstore.boschsecurity.com/>
 - L'icona  indica che il sistema ha rilevato delle versioni successive dell'applicazione software installata sull'unità **Images** o su un supporto di memoria. L'icona viene visualizzata anche se il sistema ha rilevato un'applicazione software non ancora installata nel sistema.
 - Nella colonna **Versione disponibile** sono indicate le versioni successive delle applicazioni software installate. Queste versioni sono state rilevate dal sistema sull'unità **Images** o su un supporto di memoria.
Nella colonna sono inoltre indicate le versioni disponibili delle applicazioni software rilevate non ancora installate nel sistema.

Nota: vengono visualizzate solo le versioni successive delle applicazioni software installate. Il downgrade di un'applicazione software a una versione precedente non è supportato.

7. Nella colonna **Nome**, fare clic sul relativo pulsante delle opzioni per selezionare l'applicazione software che si desidera aggiornare o installare.
8. Nella colonna **Versione disponibile**, selezionare la versione desiderata a cui si desidera aggiornare l'applicazione software o che si desidera installare, quindi fare clic su **Successivo**.
Se applicabile, viene visualizzata una finestra di dialogo dell'accordo di licenza.
9. Leggere e accettare il contratto di licenza, quindi fare clic su **Installa** per continuare. L'installazione viene avviata e si apre una finestra di dialogo che indica lo stato dell'installazione. Durante il processo di installazione non spegnere il sistema e non rimuovere i supporti di archiviazione.
10. Dopo aver installato tutti i pacchetti software, viene visualizzato un messaggio **Installazione completata con successo** in alto nella pagina.
11. Se l'installazione non va a buon fine, viene visualizzato il messaggio **Installazione non**

riuscita. e compare l'icona . In questo caso, premere F5 per tornare alla pagina **Pacchetti software**. Scaricare nuovamente i pacchetti software, quindi riprovare. Se il problema persiste, contattare l'assistenza tecnica.

6 Collegamento remoto al sistema

È possibile stabilire una connessione remota al sistema DIVAR IP all-in-one ed accedervi da Internet.

Per creare una connessione remota, è necessario effettuare le seguenti operazioni:

1. *Proteggere il sistema da accessi non autorizzati, pagina 16.*
2. *Configurazione dell'inoltro porta, pagina 16.*
3. *Scegliere un client appropriato, pagina 16.*

È inoltre possibile connettersi al proprio DIVAR IP all-in-one tramite Bosch Remote Portal e utilizzare le funzionalità future e attualmente disponibili mediante Remote Portal. Per ulteriori informazioni, vedere Connessione a Remote Portal.

6.1 Proteggere il sistema da accessi non autorizzati

Per proteggere il sistema da accessi non autorizzati, seguire le regole di complessità della password prima di collegare il sistema a Internet. Più la password è robusta, più protetto sarà il sistema da persone non autorizzate e malware.

6.2 Configurazione dell'inoltro porta

Per accedere a un sistema DIVAR IP all-in-one da Internet attraverso un router NAT/PAT, è necessario configurare l'inoltro porta sul sistema DIVAR IP all-in-one e sul router.

Per configurare l'inoltro porta:

- ▶ Inserire le seguenti regole porta nelle impostazioni di inoltro porta del router Internet:
 - Porta 5322 per l'accesso a tunnel SSH mediante BVMS Operator Client.
Nota: questa connessione è applicabile solo alla modalità operativa BVMS.
 - porta 443 per l'accesso HTTPS a VRM con Video Security Client o Video Security App.
Nota: questa connessione è applicabile solo alla modalità operativa BVMS o VRM.

DIVAR IP all-in-one è ora accessibile da Internet.

6.3 Scegliere un client appropriato

Per effettuare una connessione remota al sistema DIVAR IP all-in-one, sono disponibili due opzioni:

- *Connessione remota a Operator Client BVMS, pagina 16.*
- *Connessione remota a Video Security App, pagina 17.*



Avviso!

La compatibilità delle versioni di BVMS Operator Client o Video Security App è determinata dalle versioni del software BVMS o VRM installato su DIVAR IP.

Per informazioni dettagliate, consultare la documentazione software e il materiale formativo corrispondenti.

6.3.1 Connessione remota a Operator Client BVMS



Avviso!

Questa connessione è applicabile solo alla modalità operativa BVMS.

Per effettuare una connessione remota con BVMS Operator Client:

1. Installare BVMS Operator Client sulla workstation client.

- Al termine dell'installazione, avviare Operator Client mediante il collegamento sul desktop



- Digitare i dati seguenti, quindi fare clic su **OK**.

Nome utente: admin (o altro nome utente, se configurato)

Password: inserire la password utente

Connessione: ssh://[public-IP-address-of-DIVAR-IP_all-in-one]:5322

6.3.2 Connessione remota a Video Security App



Avviso!

Questa connessione è applicabile solo alla modalità operativa BVMS o VRM.

Per effettuare una connessione remota con Video Security App:

- Nell'App Store di Apple, cercare Bosch Video Security.
- Installare l'app Video Security sul proprio dispositivo iOS.
- Avviare l'app Video Security.
- Selezionare **Aggiungi**.
- Immettere l'indirizzo IP pubblico o il nome dynDNS.
- Verificare che la connessione protetta (SSL) sia abilitata.
- Selezionare **Aggiungi**.
- Digitare i dati seguenti:

Nome utente: admin (o altro nome utente, se configurato)

Password: inserire la password utente

6.4 Collegamento a un Enterprise Management Server

Per una gestione centrale di più sistemi DIVAR IP all-in-one in modalità operativa BVMS, è possibile utilizzare un Enterprise Management Server di BVMS installato su un server separato. Per informazioni dettagliate sulla configurazione ed il funzionamento di BVMS Enterprise System, consultare la documentazione di BVMS ed il materiale formativo.

6.5 Connessione a Remote Portal

Prerequisiti

Connessione a Remote Portal

Per connettere i dispositivi DIVAR IP all-in-one a Remote Portal, assicurarsi che vengano soddisfatti i seguenti prerequisiti:

- DIVAR IP System Manager 2.0 (o versione successiva) deve essere installato sul dispositivo.
- È necessario creare un account Remote Portal.

Comunicazione con Remote Portal

Requisiti di connettività per la comunicazione con Remote Portal.

Avviso: tutte le connessioni sono in uscita.

HTTPS (porta 443)

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

MQTTS (porta 8883)

- [mqtt://mqtt.bosch-iot-hub.com:8883](https://mqtt.bosch-iot-hub.com:8883)

6.5.1 Creazione di un account Remote Portal

Per creare un account Remote Portal:

1. Accedere a <https://remote.boschsecurity.com/login>.
2. Fare clic su **Sign up**.
3. Immettere il nome dell'azienda e l'indirizzo e-mail.
4. Selezionare l'area geografica dell'azienda.
5. Leggere i termini e le condizioni e l'avviso sulla protezione dei dati, quindi selezionare le caselle di controllo per accettarli.
6. Fare clic su **Sign up** per creare un account.

6.5.2 Registrazione dei dispositivi DIVAR IP all-in-one in Remote Portal

Per registrare un dispositivo DIVAR IP all-in-one in Remote Portal:

1. Avviare DIVAR IP System Manager.
2. Fare clic sulla scheda **Remote Portal connection**.
3. Se si dispone di un account Remote Portal esistente, immettere il proprio indirizzo e-mail e la password, quindi fare clic su per registrare il dispositivo DIVAR IP all-in-one in Remote Portal.



Avviso!

SingleKey ID

Bosch ha introdotto SingleKey ID come provider di identità (IdP) per consentire l'accesso centrale a tutti i servizi, le applicazioni e le piattaforme Bosch.

Per connettere il dispositivo a Remote Portal mediante SingleKey ID, seguire le istruzioni visualizzate sullo schermo.



Avviso!

Impostazione di **Default commissioning company**

Se l'indirizzo e-mail è assegnato a più account aziendali, assicurarsi di registrare il dispositivo DIVAR IP all-in-one sull'account aziendale corretto.

- Accedere al proprio account Remote Portal.

- Accedere a **User settings > My companies**, selezionare l'account desiderato, quindi selezionare l'opzione **Default commissioning company**.

Nota: l'impostazione **Default commissioning company** scade automaticamente dopo 12 ore.

4. Se non si dispone ancora di un account Remote Portal, innanzitutto fare clic su per creare un account Remote Portal. Consultare .

6.5.3 Annullamento della registrazione dei dispositivi DIVAR IP all-in-one da Remote Portal

Per annullare la registrazione di un dispositivo DIVAR IP all-in-one da Remote Portal:

1. Avviare DIVAR IP System Manager.
2. Fare clic sulla scheda **Remote Portal connection**.
3. Fare clic su **Annulla registrazione** per annullare la registrazione del dispositivo DIVAR IP all-in-one da Remote Portal.

Nota: l'annullamento della registrazione del dispositivo da Remote Portal non elimina la configurazione del dispositivo in Remote Portal. Per eliminare la configurazione del dispositivo, accedere all'account aziendale Remote Portal corrispondente.

7 Manutenzione

7.1 Accesso all'account amministratore

Accesso all'account amministratore in modalità operativa BVMS

Per accedere all'account amministratore in modalità operativa BVMS:

1. sul desktop di BVMS, premere Ctrl+Alt+Canc.
2. Tenere premuto il tasto Maiusc sinistro subito dopo aver fatto clic su **Cambia utente**.
3. Premere di nuovo Ctrl+Alt+Canc.
4. Selezionare l'utente **BVRAdmin** e inserire la password impostata durante il setup del sistema. quindi premere Invio.

Nota: per tornare al desktop di BVMS, premere Ctrl+Alt+Canc e fare clic su **Cambia utente** o **Disconnetti**. Il sistema torna automaticamente al desktop di BVMS senza richiedere il riavvio.

Accesso all'account amministratore in modalità operativa VRM o iSCSI

Per accedere all'account amministratore in modalità operativa VRM o iSCSI:

- ▶ nella schermata di accesso di Windows, premere Ctrl+Alt+Canc e inserire la password di **BVRAdmin**.

7.2 Monitoraggio del sistema

7.2.1 Monitoraggio del sistema mediante l'applicazione SuperDoctor

I sistemi DIVAR IP all-in-one vengono utilizzati con l'applicazione **SuperDoctor** preinstallata, che può essere utilizzata per monitorare il sistema.

Attivazione della funzione di monitoraggio

Per attivare la funzione di monitoraggio:

1. Accedere all'account amministratore (vedere *Accesso all'account amministratore, pagina 19*).
2. Sul desktop, nella cartella **Tools**, fare clic con il pulsante destro del mouse sullo script **startSD5Service**, quindi fare clic su **Run with PowerShell**.
3. Fare doppio clic sull'icona di **SuperDoctor 5 Web** sul desktop
4. Accedere all'interfaccia Web utilizzando le seguenti credenziali predefinite:
 - Nome utente: **admin**
 - Password: **DivaripSD5**
5. Fare clic sulla scheda **Configuration**, quindi fare clic su **Account Setting** e modificare la password predefinita.

Nota: Bosch consiglia vivamente di modificare la password predefinita subito dopo il primo accesso all'applicazione **SuperDoctor**.
6. Nella scheda **Configuration**, fare clic su **Alert Configuration**.
7. Attivare la funzione **SNMP Trap** e specificare l'indirizzo IP del ricevitore di trap SNMP.

Disattivazione della funzione di monitoraggio

Per disattivare la funzione di monitoraggio:

1. Accedere all'account amministratore (vedere *Accesso all'account amministratore, pagina 19*).
2. Sul desktop, nella cartella **Tools**, fare clic con il pulsante destro del mouse sullo script **stopSD5Service**, quindi fare clic su **Run with PowerShell**.

7.2.2 Monitoraggio del sistema mediante l'interfaccia IPMI

DIVAR IP all-in-one 6000 presenta una porta IPMI dedicata nella parte posteriore.

È possibile utilizzare l'interfaccia IPMI per accedere, monitorare, diagnosticare e gestire il sistema DIVAR IP all-in-one 6000 come server remoto.

Ogni unità DIVAR IP all-in-one 6000 viene fornita con il nome utente predefinito ADMIN e una password iniziale. La password iniziale è univoca per ogni unità. La password è riportata sull'etichetta sul retro dell'unità, sotto la porta IPMI.

Bosch consiglia vivamente di modificare la password iniziale durante la configurazione IPMI e di archiviare la nuova password in una posizione protetta.

**Avviso!**

Per motivi di sicurezza, non collegare il dispositivo a una rete pubblica tramite la porta IPMI in modo permanente.

Per configurare le impostazioni IPMI:

1. Accendere l'unità e premere Canc per accedere alla configurazione del BIOS.
2. Nella configurazione del BIOS, andare nella scheda **IPMI**.
3. Selezionare l'opzione **BMC Network Configuration**, quindi premere Invio.
4. Nella finestra di dialogo successiva, selezionare l'opzione **Update IPMI LAN Configuration**, quindi premere Invio.
Viene visualizzata la finestra di dialogo **Update IPMI LAN Configuration**.
5. Nella finestra di dialogo **Update IPMI LAN Configuration**, selezionare **Yes**, quindi premere Invio.
6. Impostare i parametri della configurazione di rete desiderati.
7. Premere F4 e Invio per salvare e uscire.

L'unità DIVAR IP all-in-one 6000 si riavvia.

7.3

Sostituzione di un disco rigido difettoso e configurazione di un nuovo disco rigido

Se si verifica un errore su un disco rigido installato sul sistema DIVAR IP all-in-one 6000, il LED del relativo vassoio si illumina in rosso. In tal caso, è necessario effettuare le seguenti operazioni:

1. *Sostituzione di un disco rigido difettoso, pagina 20.*
2. *Ricostruzione di RAID5 con il nuovo disco rigido, pagina 21.*

**Avviso!**

Questa procedura si applica solo a una configurazione RAID5 predefinita ed esclusivamente laddove vi siano guasti a un solo disco rigido della configurazione RAID5. Solo in questo caso è possibile garantire che nessun dato andrà perso.

**Avviso!**

Bosch non è responsabile di eventuali perdite di dati, danni o errori di sistema delle unità dotate di unità disco rigido non fornite da Bosch. Bosch non può fornire assistenza se le unità disco rigido non fornite da Bosch sono ritenute la causa del problema. Per risolvere i potenziali problemi hardware, Bosch richiede che siano installate unità disco rigido fornite da Bosch.

7.3.1


Sostituzione di un disco rigido difettoso

Per sostituire un disco rigido difettoso:

- ▶ Rimuovere il disco rigido guasto dall'unità ed installare il nuovo disco rigido.
Vedere il capitolo *Installazione di un disco rigido SATA* nel manuale di installazione.


7.3.2 Ricostruzione di RAID5 con il nuovo disco rigido

Ricostruzione RAID5 automatica

1. Sul desktop DIVAR IP all-in-one, fare doppio clic sul collegamento rapido **Launch LSA**. L'applicazione **LSI Storage Authority** si avvia e viene visualizzata la pagina **Remote Server Discovery**.
2. Accedere con le credenziali dell'account amministratore **BVRAdmin**. Si apre una finestra di dialogo che mostra indica la presenza di un problema critico su una unità di controllo.
3. Fare clic sulla barra **Controller ID**: per aprire le impostazioni dell'unità di controllo.
 - Se non è stato ancora rimosso, il disco rigido guasto viene visualizzato in **Drives > Foreign Drives > Unconfigured Drives**.
 - Una volta rimosso il disco rigido guasto e installato quello nuovo, viene avviata automaticamente la ricostruzione RAID5 con il nuovo disco rigido e su una barra di avanzamento viene mostrato l'avanzamento della ricostruzione.
4. Al termine della ricostruzione, viene visualizzata l'icona .

Ricostruzione manuale di RAID5

Se la ricostruzione RAID5 del nuovo disco rigido non si avvia automaticamente, procedere come segue:

1. Nella finestra di dialogo delle impostazioni dell'unità di controllo, alla voce **Drives > Foreign Drives > Unconfigured Drives**, selezionare il disco rigido con lo stato **Unconfigured Bad** quindi, nel riquadro di destra, selezionare **Make Unconfigured Good**. Si apre una finestra di dialogo.
2. Selezionare la casella di controllo **Confirm**, quindi fare clic su **Yes, Make Unconfigured Good** per continuare. Viene avviata la ricostruzione del sistema RAID5 con il nuovo disco rigido.
3. Al termine della ricostruzione, viene visualizzata l'icona .

7.4 Raccolta dei file di registro di DIVAR IP System Manager

L'applicazione DIVAR IP System Manager include uno script dedicato che semplifica la raccolta di file di registro.

Per raccogliere i file di registro di DIVAR IP System Manager:

1. Accedere all'account amministratore (vedere *Accesso all'account amministratore, pagina 19*).
2. Nel menu **Start** di Windows, fare clic su **Export System Manager Logs**. Lo script consente di esportare i file di registro nella cartella `Documents\Bosch` e crea un file ZIP con la seguente struttura nome: `SysMgrLogs-[date]_[time]`. È possibile utilizzare il file ZIP per allegarlo alla descrizione dettagliata dell'errore.

7.5 Ripristino dell'unità

Per ripristinare l'unità:

1. Avviare l'unità e premere F7 durante la fase di POST del BIOS per accedere a Windows PE. Viene visualizzata la finestra di dialogo **System Management Utility**.
2. Selezionare una delle opzioni seguenti:

- **System factory default:** questa opzione consente di formattare le partizioni dei dati video e ripristinare la partizione del sistema operativo dall'immagine predefinita. Questa procedura potrebbe richiedere fino a 5 minuti.
- **Full data overwrite and system factory default:** questa opzione consente di formattare le partizioni dei dati video, sovrascrivendo completamente i dati esistenti e ripristinando la partizione del sistema operativo dall'immagine predefinita.
Nota: questo processo può richiedere fino a 110 ore.
- **OS system recovery only:** questa opzione consente di ripristinare la partizione del sistema operativo dall'immagine predefinita e di importare le unità disco rigido virtuali esistenti dalle partizioni dei dati video esistenti.
Il processo potrebbe richiedere fino a 5 minuti.

Nota:

l'opzione **OS system recovery only** non elimina le registrazioni video archiviate sulle unità disco rigido contenenti i dati. Tuttavia, sostituisce l'intera partizione del sistema operativo (incluse le impostazioni del sistema di gestione video) con una configurazione predefinita. Per accedere alle registrazioni video esistenti dopo il ripristino, la configurazione del sistema di gestione video deve essere esportata prima del ripristino del sistema e reimportata dopo il ripristino.

**Avviso!**

Non spegnere l'unità durante il processo. In caso contrario, il supporto di ripristino viene danneggiato.

3. Confermare l'opzione selezionata.
Il sistema avvia il processo di formattazione e ripristino dell'immagine.
4. Al termine del processo di ripristino, confermare il riavvio del sistema.
Il sistema si riavvia e vengono eseguite le normali procedure di setup.
5. Al termine del processo, viene visualizzata la schermata di selezione della lingua di Windows.
6. Procedere alla configurazione iniziale del sistema.

Fare riferimento a

- *Primo accesso e setup iniziale del sistema, pagina 9*

8 Informazioni aggiuntive

8.1 Documentazione aggiuntiva e software client

Per ulteriori informazioni, download del software e documentazione, consultare la rispettiva pagina del prodotto nel catalogo dei prodotti:

<http://www.boschsecurity.com>

Il software più recente e i pacchetti di upgrade disponibili sono reperibili nel download store di Bosch Security and Safety Systems, in:

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

8.2 Servizi di supporto e Bosch Academy



Supporto

I **servizi di supporto** sono disponibili all'indirizzo www.boschsecurity.com/xc/en/support/.



Bosch Building Technologies Academy

Visitare il sito Web di Bosch Building Technologies Academy e accedere a **corsi di formazione**, **esercitazioni video** e **documenti**: www.boschsecurity.com/xc/en/support/training/

Bosch Security Systems B.V.

Torenallee 49

5617 BA Eindhoven

Paesi Bassi

www.boschsecurity.com

© Bosch Security Systems B.V., 2023

Building solutions for a better life.

202309021046