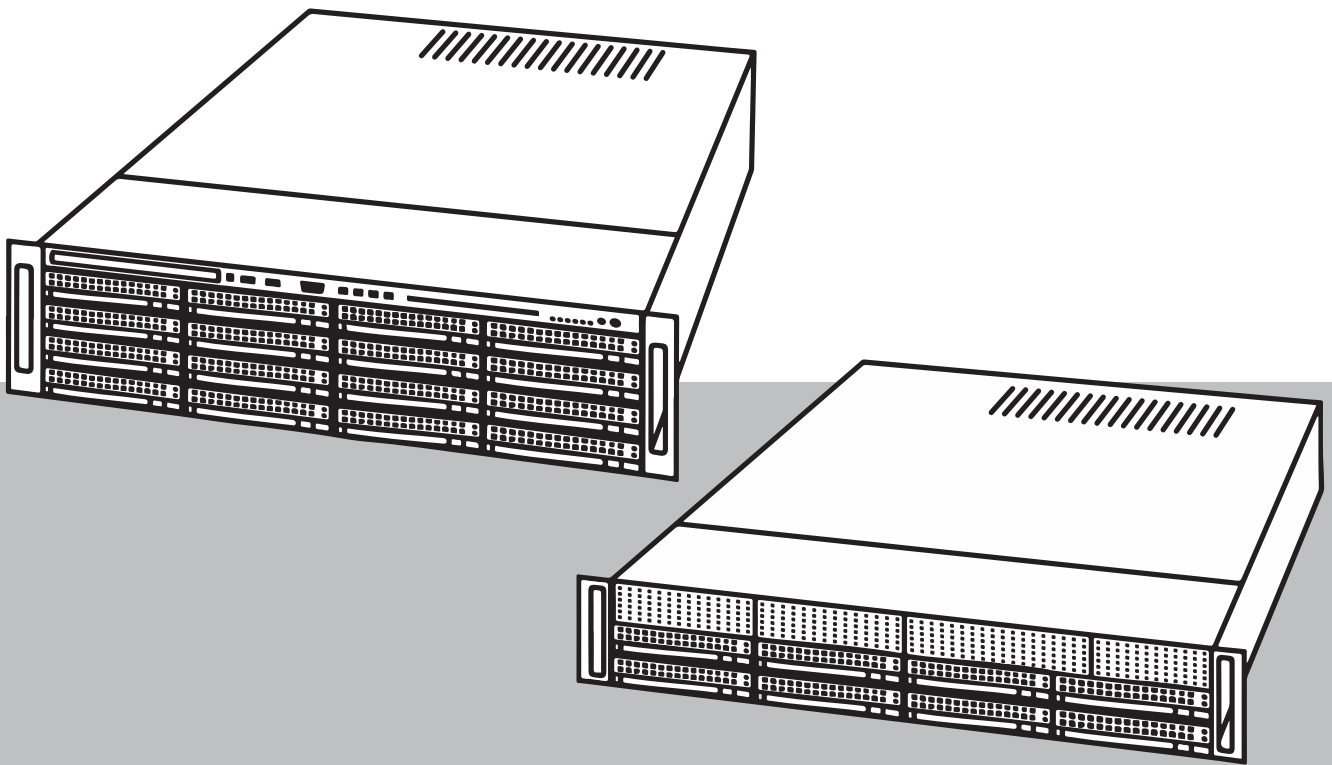


DIVAR IP all-in-one 7000 2U | DIVAR IP all-in-one 7000 3U

DIP-7380-00N | DIP-7384-8HD | DIP-7388-8HD | DIP-738C-8HD |
DIP-73G0-00N | DIP-73G8-16HD | DIP-73GC-16HD



目录

1	安全性	4
1.1	操作预防措施	4
1.2	网络安全注意事项	4
1.3	软件注意事项	4
1.3.1	使用最新软件	4
1.3.2	OSS信息	5
2	简介	6
3	系统概述	7
4	系统设置	8
4.1	默认设置	8
4.2	前提条件	8
4.3	首次登录和初始系统设置	8
5	升级软件	12
5.1	将DIVAR IP Software Center更换为DIVAR IP System Manager	12
5.2	使用System Manager升级软件	13
5.3	使用Software Center升级软件	14
6	远程连接至系统	15
6.1	保护系统，防止未经授权的访问	15
6.2	设置端口转发	15
6.3	选择合适的客户端	15
6.3.1	与BVMS Operator Client的远程连接	15
6.3.2	与Video Security App建立远程连接	16
6.4	连接到Enterprise Management Server	16
6.5	连接到Remote Portal	16
6.5.1	创建Remote Portal帐户	16
6.5.2	将DIVAR IP all-in-one设备注册到Remote Portal	17
6.5.3	从Remote Portal中取消注册DIVAR IP all-in-one设备	17
7	维护	18
7.1	登录到管理员账户	18
7.2	监控系统	18
7.2.1	采用DIVAR IP system Manager运行时使用SuperDoctor应用程序监控系统	18
7.2.2	采用DIVAR IP Software Center运行时使用SuperDoctor应用程序监控系统	18
7.2.3	使用IPMI界面监控系统	19
7.3	正在收集DIVAR IP System Manager日志文件	19
7.4	恢复装置	19
8	其它信息	21
8.1	其它文档和客户端软件	21
8.2	支持服务和博世培训学院	21

1 安全性

遵守本章中的安全预防措施。

1.1 操作预防措施

设备仅适用于专业安装。设备不适合个人或家庭操作使用。除安全信息中提到的领域外，本设备在商业和工业领域的使用不受限制。



注意!

这是 **A 类** 产品。在家庭环境中，该产品可能导致无线干扰，在这种情况下，用户可能需要采用适当的应对措施。



注意!

视频丢失是数字视频录像的固有现象；因此，博世安防系统公司对由于视频信息丢失所导致的任何损坏不负任何责任。

为了尽量减少信息丢失的风险，我们建议采用多个冗余录像系统，并采取相应的流程对所有模拟和数字信息进行备份。

1.2 网络安全注意事项

出于网络安全原因，请注意以下几点：

- 确保仅授权人员才可对系统进行物理访问。将系统置于门禁控制保护区，以避免受到物理篡改。
- 创建软件映像时，提供了包含最新Windows安全补丁的操作系统。可以使用Windows在线更新功能或相应的离线安装月度汇总补丁来定期安装操作系统安全更新。
- 请勿关闭Windows Defender和Windows防火墙，并保持最新状态。
- 请勿安装额外的防病毒软件。
- 除非您确定某人的权限，否则请勿向不认识的人员提供系统信息和敏感数据。
- 在检查网站的安全性之前，请勿通过互联网发送敏感信息。
- 设立限制，仅允许受信任的设备访问本地网络。详细信息请参见在线产品目录中提供的以下文件：
 - 《网络验证802.1X》
 - 《博世IP视频产品网络安全指南》
- 通过公共网络进行访问时，仅使用安全（加密）的通信信道。
- 管理员帐户对系统提供完全管理权限和无限访问权限。管理权限使用户能够安装、更新或删除软件，以及更改配置设置。此外，管理权限使用户能够直接访问和更改注册表项，从而绕过集中管理和安全设置。登录管理员帐户的用户可以穿越防火墙并删除防病毒软件，此操作将导致系统暴露于病毒和网络攻击。这可能对系统和数据安全构成严重风险。
为显著降低网络安全风险，请注意以下事项：
 - 确保根据密码政策，使用复杂密码来保护管理员帐户。
 - 确保只有少数受信任的用户才能访问管理员帐户。
- 由于操作需要，系统驱动器不得加密。在未加密状态下，可以轻松访问和删除此驱动器上存储的数据。为避免数据被盗或意外丢失数据，请确保只有经过授权的人员才能访问系统和管理员帐户。
- 对于安装和更新软件以及系统恢复，可能需要使用USB设备。因此，不得禁用系统的USB端口。但是，将USB设备连接到系统会带来被恶意软件感染的风险。为避免恶意软件攻击，请确保系统没有连接受感染的USB设备。

1.3 软件注意事项

1.3.1

使用最新软件

首次操作设备前，请确认您已安装可用的最新软件版本。为确保设备功能性、兼容性、安全性以及性能持续稳定，请在设备使用寿命期间定期更新软件。关于软件更新，请遵照产品文档中的说明。

访问以下链接，查看更多信息：

- 常规信息: <https://www.boschsecurity.com/xc/en/support/product-security/>
- 安全建议, 即已知漏洞及推荐的解决方案列表: <https://www.boschsecurity.com/xc/en/support/product-security/security-advisories.html>

由于所操作的博世产品软件组件过时而造成的任何损失, 博世不负任何责任。

您可以在博世安防通讯系统网站的下载商店中找到最新的软件和可用的升级软件包, 地址为:
<https://downloadstore.boschsecurity.com/>

1.3.2

OSS信息

博世在DIVAR IP all-in-one产品中使用开源软件。

您可以在以下位置找到系统驱动器上使用的开源软件组件的许可证:

C:\license txt\

在您的系统上安装的任何其他软件中使用的开源软件组件的许可证都存储在相应软件的安装文件夹中, 例如:

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

或者:

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

2 简介

DIVAR IP all-in-one 7000是一种经济实惠、易于使用的一体式录像、查看和管理解决方案，适用于具有多达256个通道的网络监控系统（其中8个通道已预先获得许可）。

DIVAR IP all-in-one 7000 2U/3U为2U/3U机架安装装置，是一款经济实惠、易于安装和操作的录像设备，兼具先进的Bosch Video Management System和出色的录像管理功能，适合具有IT意识的客户。

DIVAR IP all-in-one 7000采用嵌入式设计和核心组件，基于操作系统Microsoft Windows Server IoT 2019 for Storage Standard。DIVAR IP all-in-one 7000采用“企业级”热拔插SATA硬盘驱动器，可提供高达96/192 TB的总存储容量。

3 系统概述

操作系统

Microsoft Windows Server IoT 2019 for Storage Standard操作系统提供了用户界面，可用于服务器初始配置、存储设备统一管理、便捷设置和存储管理，以及对Microsoft iSCSI Software Target提供支持。

该软件进行了专门调整，以便为联网存储设备提供优异性能。Microsoft Windows Server IoT 2019 for Storage Standard操作系统针对存储管理进行了大幅度增强，并集成了存储设备管理组件和功能。

DIVAR IP System Manager

DIVAR IP System Manager 应用程序是一个中央用户界面，提供了一个简单的系统设置、配置和软件升级。



注意!

DIVAR IP Software Center被用作DIVAR IP all-in-one 7000早期版本(DIP-73xx)的管理软件。强烈建议您将系统升级为DIVAR IP System Manager。将BVMS升级到11.1.1版本以上需要安装DIVAR IP System Manager 2.x。

运行模式

DIVAR IP all-in-one 7000系统可在三种不同模式下运行：

- 利用BVMS和Video Recording Manager核心组件和服务的完整视频录像和管理系统。该模式提供高级IP视频安全解决方案，可跨IP网络对数字视频、音频和数据进行无缝管理。它无缝集成IP摄像机和编码器，提供整个系统的事件和报警管理、系统运行状况监控以及用户管理和优先级管理。该模式提供了出色的视频管理系统，十分适合博世视频监控设备，可充分利用博世摄像机和录像解决方案的出色功能。它包括用于集成第三方摄像机的Video Streaming Gateway组件。
- BVMS系统的高级视频解决方案采用Video Recording Manager核心组件和服务，可充分利用博世摄像机和录像解决方案的出色功能。对于运行在DIVAR IP all-in-one设备上的BVMS系统，可添加多达两个Video Recording Manager服务器。
- BVMS或Video Recording Manager系统的iSCSI存储扩展（在不同硬件上运行）。DIVAR IP all-in-one 7000设备上运行的BVMS或Video Recording Manager系统可添加多达四个此类iSCSI存储扩展。

设置系统时，必须在DIVAR IP System Manager应用程序中选择所需的操作模式来配置系统。

使用DIVAR IP System Manager应用程序，您还可以升级已安装的软件。

您可以在博世安防通讯系统网站的下载商店中找到最新的软件和可用的升级软件包，地址为：

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



注意!

录制的视频流需要进行配置，从而不超过系统的最大带宽（BVMS/VRM基本系统加上iSCSI存储扩展）。

4 系统设置

4.1 默认设置

所有DIVAR IP系统都预先配置了默认IP地址和默认iSCSI设置：

- IP地址：由DHCP自动分配（备用IP地址：192.168.0.200）。
- 子网掩码：由DHCP自动分配（备用子网掩码：255.255.255.0）。

管理员帐户的默认用户设置

- 用户名：**BVRAdmin**
- 密码：在首次登录时设置。
密码要求：
 - 最少有14个字符。
 - 至少包含一个大写字母。
 - 至少包含一个小写字母。
 - 至少包含一个数字。

4.2 前提条件

遵守以下各项：

- DIVAR IP在安装期间需要有效的网络连接。确保要连接到的网络交换机已接通电源。
- 网络中的任何其它设备不得占用默认IP地址。添加其他DIVAR IP之前，确保网络中现有DIVAR IP系统的默认IP地址已更改。

4.3 首次登录和初始系统设置



注意！

请勿更改任何操作系统设置。更改操作系统设置可能导致系统故障。



注意！

要执行管理任务，您必须登录到管理员帐户。



注意！

如果密码丢失，您必须按照安装手册所述的步骤执行系统恢复。您必须从头开始进行配置或导入配置。

要设置系统，请执行以下操作：


1. 将DIVAR IP all-in-one装置和摄像机连接到网络。
2. 打开装置。
此时会执行Microsoft Windows Server IoT 2019 for Storage Standard的设置流程。此过程可能需要数分钟时间。请勿关闭系统。
流程执行完成后，将显示Windows语言选择屏幕。
3. 从列表中选择您的国家/地区、所需的操作系统语言和键盘布局，然后单击**下一步**。
此时将显示Microsoft软件许可条款。
4. 单击**接受**以接受许可条款，然后等待Windows重新启动。这可能需要数分钟时间。请勿关闭系统。
重新启动后，此时会显示Windows登录页面。
5. 为管理员帐户**BVRAdmin**设置新密码并确认。
密码要求：

- 最少有14个字符。
- 至少包含一个大写字母。
- 至少包含一个小写字母。
- 至少包含一个数字。

然后按下Enter。

此时将显示**Software Selection**页面。

6. 系统会自动扫描本地驱动器和任何已连接的外部存储介质，以查找安装文件 **BoschAppliance_Setup_DSC_[software version].exe**，该文件位于具有以下路径的文件夹中：Drive root\BoschAppliance\。扫描可能需要一些时间。请等待扫描完成。
7. 为了准备好装置以安装DIVAR IP System Manager，首先需要安装 **BoschAppliance_Setup_DSC_10.01.0001.exe**。
系统检测到此安装文件后，会显示在软件选择页面上。单击显示安装文件的栏以开始安装并继续执行步骤14。
如果未检测到此安装文件，请执行以下操作：
 8. 前往<https://downloadstore.boschsecurity.com/>。
 9. 在**Software**选项卡下，从列表中选择**BVMS Appliances**，然后单击**Select**。
将显示所有可用软件包的列表。
 10. 找到ZIP文件**SystemManager_[software version 2.0.0 or higher].zip**并将其保存到USB移动存储器等存储介质中。
 11. 解压存储介质上的文件，确保文件夹**BoschAppliance**放在存储介质的根目录下。
 12. 将存储介质连接到您的DIVAR IP all-in-one设备。
系统会自动扫描存储介质中的安装文件**BoschAppliance_Setup_DSC_10.01.0001.exe**。
扫描可能需要一些时间。请等待扫描完成。
 13. 系统检测到安装文件后，会显示在**Software Selection**页面上。单击显示安装文件的栏以开始安装。
注意：要实现自动检测，安装文件必须位于具有以下路径的文件夹中：Drive root\BoschAppliance\（例如F:\BoschAppliance\）。

如果安装文件位于与预定义文件夹路径不匹配的其他位置，请单击  导航到相应的位置。然后单击安装文件开始安装。

14. 安装开始。安装过程可能需要数分钟时间。请勿在安装过程中关闭系统，也不要移除存储介质。安装成功完成后，系统将重新启动，您将会转到Windows登录页面。
15. 登录管理员帐户BVRAdmin。
此时会显示**Software Selection**页面，显示DIVAR IP System Manager2.x安装文件 **SystemManager_x64_[software version].exe**。
16. 单击显示安装文件的栏以开始安装。
17. 在安装开始之前，系统将显示**End User License Agreement (EULA)**对话框。阅读许可条款，然后单击**Accept**以继续。
安装开始。
安装成功完成后，系统将重新启动，您将会转到Windows登录页面。
18. 登录到管理员帐户BVRAdmin。
此时将打开Microsoft Edge浏览器并显示**DIVAR IP - 系统设置**页面。该页面显示设备类型和设备序列号，以及三种操作模式和每种操作模式的可用软件版本。
您必须选择所需的操作模式和所需的软件版本来配置您的DIVAR IP all-in-one系统。
19. 如果本地驱动器上没有相应操作模式所需的软件版本，请执行以下操作：
 - 前往<https://downloadstore.boschsecurity.com/>。
 - 在**Software**选项卡下，从列表中选择**BVMS Appliances**，然后单击**Select**。
将显示所有可用软件包的列表。

- 找到所需软件包的ZIP文件，例如**BVMS [BVMS version]_SystemManager_package_[package version].zip**，并将它们保存到USB移动存储器等存储介质中。
- 解压存储介质上的文件。不要更改解压文件的文件夹结构。
- 将存储介质连接到您的DIVAR IP all-in-one设备。

**注意!**

首次操作设备前，请确认您已安装可用的最新软件版本。您可以在博世智能建筑科技网站的下载商店中找到最新的软件和可用的升级软件包，地址为：<https://downloadstore.boschsecurity.com/>。

选择操作模式BVMS

要作为完整的视频录像和管理系统运行DIVAR IP all-in-one系统，请执行以下操作：

1. 在**DIVAR IP - 系统设置**页面中，选择**BVMS**操作模式和想要安装的BVMS版本，然后单击**下一步**。
此时将显示BVMS许可协议。
2. 阅读并接受许可协议，然后单击**安装**以继续。
安装开始，安装对话框将显示安装进度。请勿在安装过程中关闭系统，也不要移除存储媒体。
3. 所有软件包安装成功后，系统将重新启动。重新启动后，您将会转到BVMS桌面。
4. 在BVMS桌面上，单击所需的应用程序来配置系统。

**注意!**

有关详细信息，请参阅相应的DIVAR IP all-in-one线上培训和BVMS文档。

您可以在以下位置找到培训：www.boschsecurity.com/xc/en/support/training/

选择操作模式VRM

要将DIVAR IP all-in-one系统作为纯视频录像系统来运行，请执行以下操作：

1. 在**DIVAR IP - 系统设置**页面中，选择**VRM**操作模式和想要安装的VRM版本，然后单击**下一步**。
此时将显示VRM许可协议。
2. 阅读并接受许可协议，然后单击**安装**以继续。
安装开始，安装对话框将显示安装进度。请勿在安装过程中关闭系统，也不要移除存储媒体。
3. 所有软件包安装成功后，系统将重新启动。重新启动后，您将会转到Windows登录屏幕。

**注意!**

有关详情，请参阅VRM文档。

选择操作模式iSCSI存储

要将DIVAR IP all-in-one系统作为iSCSI存储扩展来运行，请执行以下操作：

1. 在**DIVAR IP - 系统设置**页面中，选择**iSCSI存储**操作模式以及想要安装的所需iSCSI存储版本，然后单击**下一步**。
此时将显示安装对话框。
2. 在安装对话框中，单击**安装**以继续。
安装开始，安装对话框将显示安装进度。请勿在安装过程中关闭系统，也不要移除存储介质。
3. 所有软件包安装成功后，系统将重新启动。重新启动后，您将会转到Windows登录屏幕。
4. 使用BVMS Configuration Client或Configuration Manager，将系统作为iSCSI存储扩展添加到外部BVMS或VRM服务器。



注意!

有关详情，请参阅BVMS或Configuration Manager文档。

5 升级软件



注意!

DIVAR IP Software Center被用作DIVAR IP all-in-one 7000早期版本(DIP-73xx)的管理软件。强烈建议您将系统升级为DIVAR IP System Manager。将BVMS升级到11.1.1版本以上需要安装DIVAR IP System Manager 2.x。



注意!

首次操作设备前，请确认您已安装可用的最新软件版本。您可以在博世智能建筑科技网站的下载商店中找到最新的软件和可用的升级软件包，地址为：<https://downloadstore.boschsecurity.com/>。

5.1 将DIVAR IP Software Center更换为DIVAR IP System Manager

要将DIVAR IP Software Center更换为DIVAR IP System Manager 2.0（或更高版本），请执行以下步骤：

1. 启动DIVAR IP Software Center。
2. 按如下方式升级操作模式软件：
 - 如果您的系统在BVMS操作模式下运行，请将BVMS版本升级到**BVMS 11.1.1**。
 - 如果您的系统在VRM操作模式下运行，请将VRM版本升级到**VRM 4.03.0025**。
 - 有关使用DIVAR IP Software Center升级软件的更多详细信息，请参阅*使用Software Center升级软件*，页面 14。
3. 前往<https://downloadstore.boschsecurity.com/>。
4. 在**Software**选项卡下，从列表中选择**BVMS Appliances**，然后单击**Select**。
将显示所有可用软件包的列表。
5. 找到ZIP文件**SystemManager_[software version 2.0.0 or higher].zip**并将其保存到USB移动存储器等存储介质中。
6. 解压存储介质上的文件。
7. 将存储介质连接到您的DIVAR IP all-in-one设备。
8. 在存储介质上找到安装文件**SystemManager_x64_software version].exe**，双击文件开始安装。
9. 安装开始前，会显示许可协议对话框。阅读许可协议，选中复选框以接受该协议，然后单击**安装**以继续。
此时会显示**DIVAR IP System Manager setup**对话框，请求更新SuperDoctor。



注意!

更新SuperDoctor服务

DIVAR IP System Manager 2.0（或更高版本）需要更新SuperDoctor服务。更新将覆盖现有的SuperDoctor设置。您必须在更新后重新应用各项特定设置。在开始更新之前，请务必记下您的设置。更新后，SuperDoctor服务将禁用，SuperDoctor密码也将重置为默认密码**DivaripSD5**。Bosch强烈建议在首次登录SuperDoctor后立即更改默认密码。

10. 单击**Install**以继续。

DIVAR IP System Manager安装开始。

安装过程可能需要数分钟时间。请勿在安装过程中关闭系统，也不要移除存储介质。

注：在DIVAR IP System Manager 2.0（或更高版本）安装期间，DIVAR IP Software Center会自动卸载。

在DIVAR IP System Manager 2.0（或更高版本）安装期间，SuperDoctor监控服务将禁用。您必须在安装完成后启用该服务。

启用SuperDoctor服务

要启用SuperDoctor服务，请执行以下操作：

1. 在桌面上**Tools**文件夹中，右击**startSD5Service**脚本，然后单击**Run with PowerShell**。
2. 双击桌面上的**SuperDoctor 5 Web**图标。
3. 使用以下默认凭据登录web界面：
 - 用户名: **admin**
 - 密码: **DivaripSD5**
4. 单击**Configuration**选项卡，然后单击**Account Setting**并更改默认密码。
注：博世强烈建议在首次登录**SuperDoctor**应用程序后立即更改默认密码。
5. 重新应用在更换DIVAR IP Software Center之前应用的SuperDoctor设置。

5.2 使用System Manager升级软件



使用DIVAR IP System Manager应用程序，您还可以升级在您的系统已安装的软件。




注意！

不支持将已安装的软件降级到早期版本。

要升级已安装的软件，请执行以下操作：

1. 前往<https://downloadstore.boschsecurity.com/>。
2. 在**Software**选项卡下，从列表中选择**BVMS Appliances**，然后单击**Select**。
将显示所有可用软件包的列表。
3. 找到所需软件包的ZIP文件，例如**BVMS_[BVMS version]_SystemManager_package_[package version].zip**，并将它们保存到USB移动存储器等存储介质中。
4. 解压存储介质上的文件。不要更改解压缩文件的文件夹结构。
5. 启动DIVAR IP System Manager：
 - 如果您使用**BVRAAdmin**管理员帐户登录Windows，请双击Windows桌面上的DIVAR IP System Manager图标。
DIVAR IP System Manager将启动。
 - 如果您的系统在BVMS操作模式下运行，请单击BVMS桌面上的DIVAR IP System Manager图标并登录BVRAAdmin管理员帐户。此时DIVAR IP System Manager会在全屏对话框中打开（您可以按Alt+ F4退出对话框）。
6. 将显示**软件包**页面，在页面顶部显示设备类型和设备序列号。
 - 在**名称**列中，您可以看到系统上已安装的所有DIVAR IP System Manager软件应用程序，以及系统在**Images**驱动装置或存储介质上检测到的所有其他DIVAR IP System Manager软件应用程序。
 - 在**已安装的版本**列中，您可以看到系统上当前安装的软件应用程序版本。
 - 在**状态**列中，您可以看到各个软件应用程序的状态：
 -  图标表示系统在**Images**驱动装置或存储介质上未检测到安装的软件应用程序的更新版本。
注：为确保您使用的是最新的软件版本，请仔细检查博世智能建筑科技下载商店中的可用软件版本，网址为：
<https://downloadstore.boschsecurity.com/>
 -  图标表示系统在**Images**驱动装置或存储介质上检测到安装的软件应用程序的更新版本。
如果系统检测到尚未安装在系统上的软件应用程序，也会显示该图标。

- 在**可用版本**列中，您可以看到安装的软件应用程序的更高版本。系统在**Images**驱动装置或存储介质上检测到这些版本。
该列还显示系统上尚未安装的检测到的软件应用程序的可用版本。
注：仅显示安装的软件应用程序的更高版本。不支持将软件应用程序降级到早期版本。
- 7. 在**名称**列中，单击相应的选项按钮，选择要升级或安装的软件应用程序。
- 8. 在**可用版本**列中，选择要升级软件应用程序或要安装的所需版本，然后单击**下一步**。
如果适用，将显示许可协议对话框。
- 9. 阅读并接受许可协议，然后单击**安装**以继续。
安装开始，安装对话框显示安装进度。请勿在安装过程中关闭系统，也不要移除存储介质。
- 10. 成功安装所有软件包后，您将在页面顶部收到消息**成功完成安装**。
- 11. 如果安装不成功，您将收到消息**安装失败**。并将显示  图标。在这种情况下，按F5返回**软件包**页面。再次下载相应的软件包并重试。
如果问题仍然存在，请联系技术支持。

5.3 使用Software Center升级软件

升级软件

要升级已安装的软件，请执行以下操作：

1. 从**下载区**下载所需的软件包，然后将其保存在本地驱动器或存储介质上。然后将存储介质连接到系统。
2. 启动DIVAR IP Software Center。
此时会显示**已安装的软件**页面。
3. **升级**部分中将显示可用的升级。单击**升级**以升级所需的软件。
此时将显示**升级**对话框，显示升级中包含的软件包。
注：升级将保存您的所有设置，更新软件并重新启动系统。
4. 单击**安装**以继续。
开始安装软件包。这可能需要数分钟时间。请勿关闭系统，也不要移除存储介质。
安装完成后，系统将重新启动。

6 远程连接至系统

您可以远程连接到DIVAR IP all-in-one系统，并从互联网访问它。

要创建远程连接，必须执行以下操作：

1. 保护系统，防止未经授权的访问，[页面 15](#)。
2. 设置端口转发，[页面 15](#)。
3. 选择合适的客户端，[页面 15](#)。

您还可以通过BoschRemote Portal连接到DIVAR IP all-in-one，并通过Remote Portal使用当前和未来功能。有关详细信息，请参阅[连接到Remote Portal](#)，[页面 16](#)。

6.1 保护系统，防止未经授权的访问

为了保护系统免受未经授权的访问，请确保在将系统连接到互联网之前遵循严格的密码规则。密码越强，系统保护就越强，不易受到未经授权的人员和恶意软件的攻击。

6.2 设置端口转发

要通过支持NAT/PAT的路由器从互联网访问DIVAR IP all-in-one系统，必须在DIVAR IP all-in-one系统和路由器上配置端口转发。

要设置端口转发，请执行以下操作：

- ▶ 在互联网路由器的端口转发设置中输入以下端口规则：
 - 端口5322用于SSH隧道访问，使用BVMS Operator Client。
注：此连接仅适用于BVMS操作模式。
 - 对用于HTTPS的端口443，使用Video Security Client或Video Security App访问VRM。
注：此连接仅适用于BVMS或VRM操作模式。

现在可以从互联网访问您的DIVAR IP all-in-one。

6.3 选择合适的客户端

有两个选项可以远程连接到DIVAR IP all-in-one系统：

- 与BVMS Operator Client的远程连接，[页面 15](#)。
- 与Video Security App建立远程连接，[页面 16](#)。



注意！

BVMS Operator Client或Video Security App版本的兼容性由DIVAR IP中安装的BVMS或VRM软件版本决定。

有关详细信息，请参阅相应的软件文档和培训材料。


6.3.1 与BVMS Operator Client的远程连接



注意！

此连接仅适用于BVMS操作模式。

要与BVMS Operator Client建立远程连接，请执行以下操作：

1. 在客户端工作站上安装BVMS Operator Client。
2. 成功完成安装后，使用桌面快捷方式  启动Operator Client。
3. 输入以下内容，然后单击**OK**。

用户名： admin（或配置的其他用户）

密码： 用户密码

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

6.3.2 与Video Security App建立远程连接



注意!

此连接仅适用于BVMS或VRM操作模式。

要与Video Security App建立远程连接，请执行以下操作：

1. 在Apple App Store搜索Bosch Video Security。
2. 在您的iOS设备上安装Video Security应用程序。
3. 启动Video Security应用程序。
4. 选择**添加**。
5. 输入公共IP地址或DynDNS名称。
6. 确保安全连接(SSL)已打开。
7. 选择**添加**。
8. 输入以下内容：
用户名： admin (或其他用户，如果配置了一个)
密码： 用户密码

6.4 连接到Enterprise Management Server

要在BVMS操作模式下集中管理多个DIVAR IP all-in-one系统，可以使用安装在单独服务器上的BVMS Enterprise Management Server。

有关BVMS Enterprise System配置和操作的详细信息，请参阅BVMS文档和培训材料。

6.5 连接到Remote Portal

前提条件

Remote Portal连接

要将DIVAR IP all-in-one设备连接到Remote Portal，请确保满足以下前提条件：

- 设备上必须安装DIVAR IP System Manager 2.0 (或更高版本)。
- 要安装DIVAR IP System Manager 2.0 (或更高版本)，DIVAR IP设备必须运行BVMS 11.1.1或更高版本。
- 必须创建Remote Portal帐户。

Remote Portal通信

Remote Portal通信在连接方面具有一定要求。

注： 所有连接均为传出连接。

HTTPS (端口443)

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

MQTTS (端口8883)

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

6.5.1 创建Remote Portal帐户

要创建Remote Portal帐户，请执行以下操作：

1. 前往<https://remote.boschsecurity.com/login>。
2. 单击**Sign up**。
3. 输入您的公司名称和电子邮件。
4. 选择您公司所在的区域。
5. 阅读条款和条件以及数据保护声明，然后选中复选框以接受。
6. 单击**Sign up**以创建帐户。

6.5.2 将DIVAR IP all-in-one设备注册到Remote Portal

要将DIVAR IP all-in-one设备注册到Remote Portal，请执行以下操作：

1. 启动DIVAR IP System Manager。
2. 单击**Remote Portal connection**选项卡。
3. 如果您当前已有Remote Portal帐户，请输入您的电子邮件和密码，然后单击以将DIVAR IP all-in-one设备注册到Remote Portal。



注意!

SingleKey ID

Bosch引入了SingleKey ID作为身份提供商(IdP)，允许集中登录Bosch所有的应用程序、服务和平台。

要使用SingleKey ID将设备连接到Remote Portal，请按照屏幕上的说明进行操作。



注意!

Default commissioning company设置

如果您的电子邮件被分配给多个公司帐户，请确保您将DIVAR IP all-in-one设备注册到正确的公司帐户。

- 登录您的Remote Portal帐户。

- 转到**User settings > My companies**，选择所需的帐户，然后选择选项**Default commissioning company**。

注： **Default commissioning company**设置将会在12小时后自动失效。

4. 如果您还没有Remote Portal帐户，请先单击以创建一个Remote Portal帐户。请参阅。

6.5.3 从Remote Portal中取消注册DIVAR IP all-in-one设备

要从Remote Portal中取消注册DIVAR IP all-in-one设备，请执行以下操作：

1. 启动DIVAR IP System Manager。
2. 单击**Remote Portal connection**选项卡。
3. 单击**取消注册**以从Remote Portal中取消注册DIVAR IP all-in-one设备。

注： 从Remote Portal中取消注册设备不会删除Remote Portal中的设备配置。要删除设备配置，请登录相应的Remote Portal公司帐户。

7 维护

7.1 登录到管理员账户

登录到BVMS操作模式中的管理员帐户

要登录到BVMS操作模式中的管理员帐户：

1. 在BVMS桌面，按Ctrl+Alt+Del键。
2. 单击**切换用户**后，立即长按左Shift键。
3. 再次按Ctrl+Alt+Del键。
4. 选择**BVRAdmin**用户，然后输入系统设置时设定的密码。然后按Enter。

注意：要回到BVMS桌面，请按Ctrl+Alt+Del键并单击**切换用户**或者**登出**。系统会自动返回没有系统重启的BVMS桌面。

登录到VRM或者iSCSI操作模式中的管理员帐户

要登录到VRM或者iSCSI操作模式中的管理员帐户：

- ▶ 在Windows登录屏幕上，按Ctrl+Alt+Del键并输入**BVRAdmin**密码。

7.2 监控系统

7.2.1 采用DIVAR IP system Manager运行时使用SuperDoctor应用程序监控系统

DIVAR IP all-in-one系统附带预安装的应用程序**SuperDoctor**，您可以使用它来监控您的系统。

激活监控功能

要激活监视功能，请执行以下操作：

1. 登录到管理员帐户（请参见**登录到管理员账户**，[页面 18](#)）。
2. 在桌面上**Tools**文件夹中，右击**startSD5Service**脚本，然后单击**Run with PowerShell**。
3. 双击桌面上的**SuperDoctor 5 Web**图标。
4. 使用以下默认凭据登录web界面：
 - 用户名：**admin**
 - 密码：**DivaripSD5**
5. 单击**Configuration**选项卡，然后单击**Account Setting**并更改默认密码。
注：博世强烈建议在首次登录**SuperDoctor**应用程序后立即更改默认密码。
6. 在**Configuration**选项卡下，单击**Alert Configuration**。
7. 激活**SNMP Trap**功能，并为SNMP陷阱的接收器指定IP地址。

停用监控功能

要停用监视功能，请执行以下操作：

1. 登录到管理员帐户（请参见**登录到管理员账户**，[页面 18](#)）。
2. 在桌面上**Tools**文件夹中，右击**stopSD5Service**脚本，然后单击**Run with PowerShell**。

7.2.2 采用DIVAR IP Software Center运行时使用SuperDoctor应用程序监控系统

该系统提供运行状态监控工具。

要激活监控功能，您必须登录到管理员帐户(**BVRAdmin**)。

1. 登录到管理员帐户**BVRAdmin**。有关详细信息，请参阅**登录到管理员账户**，[页面 18](#)。
2. 在桌面上的**Tools**文件夹中，右击**Enable_SuperDoctor_5_Service**脚本，然后单击**以管理员身份运行**。
3. 双击同一文件夹中的**SuperDoctor 5 Web**图标。
4. 使用以下默认凭证登录到Web界面：
 - 用户名：**admin**
 - 密码：**DivaripSD5**
5. 单击**Configuration**选项卡，然后单击**Password Settings**并更改默认密码。
6. 单击**Configuration**选项卡，然后单击**Alert Configuration**。
7. 激活**SNMP Trap**功能，并为SNMP陷阱的接收器指定IP地址。

7.2.3 使用IPMI界面监控系统

DIVAR IP all-in-one 7000背面有一个专用的IPMI端口。

您可以使用IPMI界面作为远程服务器访问、监视、诊断和管理DIVAR IP all-in-one 7000系统。

每个DIVAR IP all-in-one 7000装置交付时带有默认用户名ADMIN和初始密码。每个装置均带有唯一的初始密码。可以在装置背面、IPMI端口下方的标签上找到。

博世强烈建议在IPMI配置期间更改初始密码，并将新密码存储到安全位置。



注意!

出于安全原因，请勿通过IPMI端口将设备永久连接到公共网络。

要配置IPMI设置:

1. 打开装置并按下Del进入BIOS设置。
2. 在BIOS设置中，导航到选项卡IPMI。
3. 选择**BMC Network Configuration**选项，然后按下Enter。
4. 在下一个对话框中，选择**Update IPMI LAN Configuration**选项，然后按下Enter。
此时将显示**Update IPMI LAN Configuration**对话框。
5. 在**Update IPMI LAN Configuration**对话框中，选择**Yes**，然后按下Enter。
6. 设置所需的网络配置参数。
7. 按下F4和Enter以保存并退出。

DIVAR IP all-in-one 7000装置将重新启动。

7.3 正在收集DIVAR IP System Manager日志文件

DIVAR IP System Manager应用程序包括一个专用脚本，可以简化日志文件收集。

要收集DIVAR IP System Manager日志文件，请执行以下操作:

1. 登录到管理员账户（请参见[登录到管理员账户](#)，[页面 18](#)）。
2. 在Windows**开始**菜单上，单击**Export System Manager Logs**。
脚本将日志文件导出到文件夹Documents\Bosch并创建具有以下名称结构的ZIP文件
`SysMgrLogs-[date]_[time].`
您可以使用此ZIP文件将其附加到详细的错误描述中。

7.4 恢复装置

按照下述流程操作以恢复出厂默认图像。

要将装置恢复到出厂默认图像，请执行以下操作:

1. 启动装置，在BIOS开机自检期间按下**F7**以进入Windows PE。
此时将显示“恢复”菜单。
2. 选择以下选项之一：
 - **初始出厂设置（将丢失所有系统数据）**：该选项将删除所有硬盘分区的数据，并以出厂默认图像覆盖操作系统分区。
 - **初始出厂设置（覆盖现有数据）**：该选项将删除并覆盖所有硬盘分区的数据，并以出厂默认图像覆盖操作系统分区。
注意：该过程可能会花费较长时间。
 - **系统恢复（恢复为出厂默认设置）**：该选项将以出厂默认图像覆盖操作系统分区，并在恢复期间从硬盘中导入现有的虚拟硬盘驱动器。

注意：

系统恢复选项不会删除存储在数据硬盘上的视频画面，但仍然会将整个操作系统分区（包括视频管理系统设置）更改为默认配置。为了在恢复后访问现有视频画面，需要在系统恢复前导出视频管理系统配置，然后在恢复后再行导入。

**注意！**

过程中请不要关闭装置。否则将损坏恢复介质。

3. 装置从恢复介质启动。如果设置成功，则按是重新启动系统。
4. Windows将执行操作系统的初始化设置。
Windows完成设置后，装置重新启动。
5. 重新启动装置之后，将安装出厂设置。

8 其它信息

8.1 其它文档和客户端软件

如需获得更多信息、下载软件或获取文档，请访问产品目录中的相应产品页面：

<http://www.boschsecurity.com>

您可以在博世安防通讯系统网站的下载商店中找到最新的软件和可用的升级软件包，地址为：

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

8.2 支持服务和博世培训学院



支持

访问www.boschsecurity.com/xc/en/support/，获取支持服务。



博世智能建筑科技培训学院

访问博世智能建筑科技培训学院网站，获取培训课程、视频教程和文档：www.boschsecurity.com/xc/en/support/training/

Bosch Security Systems B.V.

Torenallee 49

5617 BA Eindhoven

Netherlands

www.boschsecurity.com

© Bosch Security Systems B.V.2023

Building solutions for a better life.

202309021111