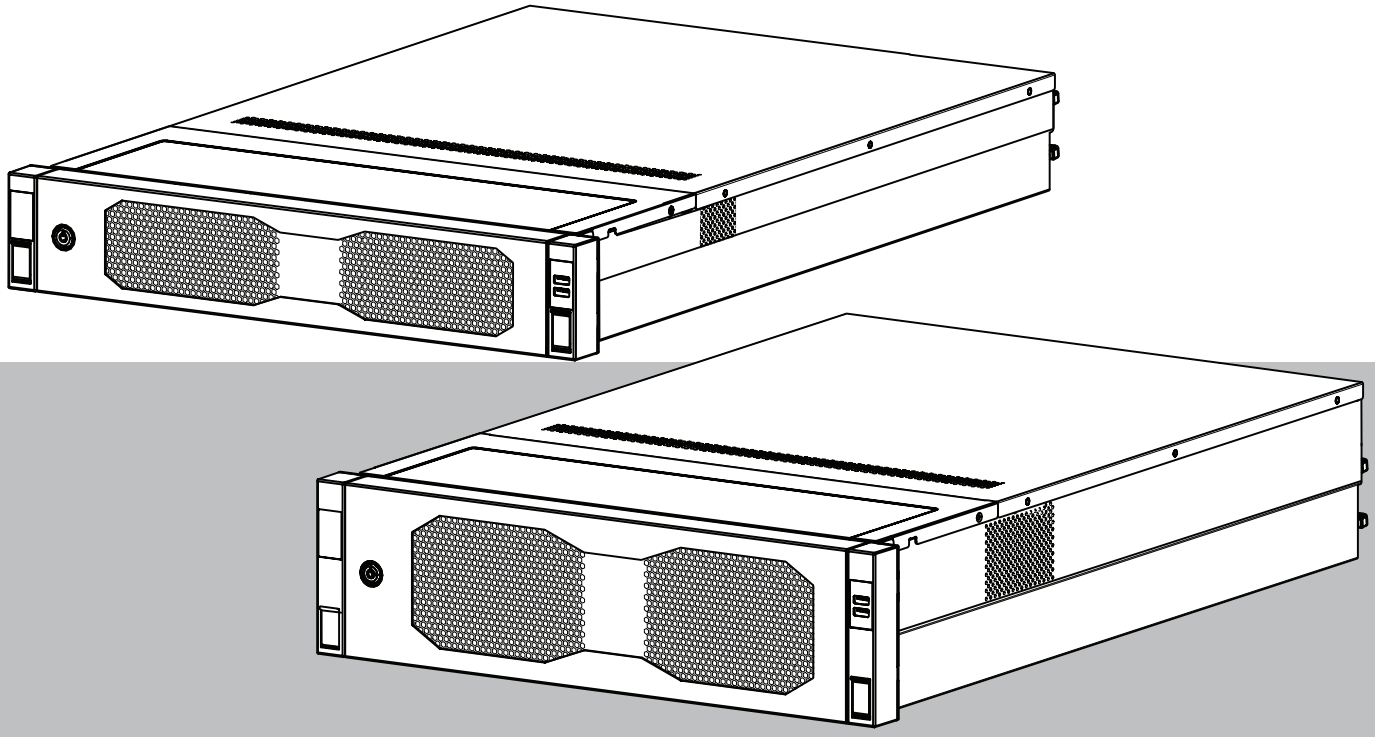
DIVAR IP all-in-one 7000 2U | DIVAR IP all-in-one 7000 3U

DIP-74C0-00N | DIP-74C4-8HD | DIP-74C8-8HD | DIP-74CI-8HD | DIP-74CI-12HD | DIP-74G0-00N | DIP-74GI-16HD



zh-CHS 用户手册

目录

1 安全标准

遵守本章中的安全预防措施。

1.1 操作预防措施

注意!
预期用途
本产品仅供专业人员使用。本产品不得安装在普通人群可以进入的公共区域。

注意!
请勿在任何潮湿地带使用本产品。

注意!
采取预防措施，防止设备免遭电源或雷电浪涌损坏。

注意!
设备周围的区域应清洁整齐。

注意!
外壳开口
请勿阻塞或盖住任何开口。外壳上的任何开口均用于通风。这些开口将避免设备过热并确保可靠运行。

注意!
请勿打开或取下设备盖。打开或取下设备盖可能会损坏系统并导致保修失效。

注意!
请勿让任何液体溅到设备上。

警告!
维修底板以及在底板周围工作时，请务必小心。 当系统工作时，底板上存在危险电压或能量。 切勿用任何金属物体接触底板，确保没有带状电缆接触底板。

注意!
移动设备之前应断开电源。移动产品时应小心谨慎。用力过度或撞击可能会对本产品和硬盘驱动器造成损坏。

警告!
处理本产品中使用的铅焊接材料可能会使您接触到铅。铅是加利福尼亚州已知会导致出生缺陷和其他生殖危害的化学物质。

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。
- 锁定前挡板，以防止未经授权拆卸硬盘驱动器。勿将钥匙留在锁中，请取出钥匙并存放在安全地点。
- 使用机箱入侵传感器功能，检测任何未经授权的物理访问设备内部的情况。
- 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。
- 为确保网页浏览器安全且正常工作，请始终保持最新状态。
- 请勿关闭Windows Defender和Windows防火墙，并保持最新状态。切勿安装其他防病毒软件，否则可能会破坏安全配置。
- 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制访问权限。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。
- 切勿更改BIOS UEFI设置。更改BIOS UEFI设置可能会损坏系统，甚至导致系统故障。
- 不得将BMC系统接入公共网络。

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
- 安全信息，其中包括第三方漏洞造成的潜在影响：https://www.boschsecurity.com/us/en/support/product-security/security-information.html

要接收新安全建议的更新，您可以订阅博世智能建筑科技安全建议页面上的RSS源：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 2022 for Storage Standard。该设备采用“企业级”热拔插SATA硬盘驱动器，可提供高达216/288 TB的总存储容量。

3 系统概述

操作系统

Microsoft Windows Server IoT 2022 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 2022 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。

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系统的iSCSI存储扩展（在不同硬件上运行）。对于运行在DIVAR IP all-in-one 7000设备上的BVMS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：
  – 不低于14个字符
  – 密码必须包含以下四类字符中的三类：
    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。
    至少包含一个特殊字符。

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。

注意!
出于安全原因，将显示用户帐户控制(UAC)对话框，要求您确认对系统进行所需更改。您只有在确认要进行适当的更改后，才能继续安装。

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. 打开设备。
   等待BIOS屏幕显示并执行Microsoft Windows Server IoT 2022 for Storage Standard设置程序。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：
   - 不低于14个字符
   - 密码必须包含以下四类字符中的三类：
     - 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。
     - 至少包含一个特殊字符。

   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连接的外部存储媒体，以查找DIVAR IP System Manager安装文件**SystemManager_x64_[software version].exe**， 该文件 位于具有以下结构的文件夹中：`Drive root\BoschAppliance\`。
   扫描可能需要一些时间。等待扫描完成。
7. 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：确保最新版本的DIVAR IP System Manager已安装。您可以在Bosch智能建筑科技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. 如果在扫描过程中找不到安装文件，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ZIP文件**SystemManager_[software version].zip**并将其保存到USB移动存储器等存储介质中。
   - 解压存储介质上的文件，确保文件夹**BoschAppliance**放在存储介质的根目录下。
   - 将存储介质连接到您的DIVAR IP all-in-one系统。
     系统会自动扫描存储介质中的安装文件。
     扫描可能需要一些时间。等待扫描完成。
   - 检测到安装文件后，相关文件将显示在**Software Selection**页面上。单击显示安装文件的栏以开始安装。
     注意：要自动检测，安装文件必须位于具有以下结构的文件夹中：`Drive root\BoschAppliance\`（例如`F:\BoschAppliance\`）。

     如果安装文件位于与预定义文件夹结构不匹配的其他位置，请单击  导航到相应的位置。然后单击安装文件开始安装。
9. 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。
10. 在以下用户帐户控制对话框中，单击**Yes**以继续。安装开始。
11. 安装完成后，系统重新启动，您将转到Windows登录页面。登录到管理员帐户。
12. Microsoft Edge浏览器将打开并且显示**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。
    注意：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。不要更改解压缩文件的文件夹结构。
- 将存储介质连接到您的DIVAR IP all-in-one系统。

注意!
安装后若要更改操作模式，需要完全恢复出厂设置。

4.3.1 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**操作模式和需要安装的BVMS版本，然后单击**安装操作模式**。
   此时将显示BVMS许可协议。
2. 阅读并接受许可协议，然后单击**是，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/

4.3.2 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**操作模式和需要安装的VRM版本，然后单击**安装操作模式**。
   此时将显示VRM许可协议。
2. 阅读并接受许可协议，然后单击**是，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。

4.3.3 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**操作模式以及需要安装的iSCSI存储版本，然后单击**安装操作模式**。
   此时将显示安装对话框。
2. 在安装对话框中，单击**是，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

确保您将DIVAR IP System Manager升级为最新版本。

5.1 升级DIVAR IP System Manager

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ZIP文件**SystemManager_[software version 2.3.0 or higher].zip**并将其保存到USB移动存储器等存储介质中。
4. 解压存储介质上的文件。
5. 将存储介质连接到您的DIVAR IP all-in-one设备。
6. 启动DIVAR IP System Manager:
   - 如果您使用**BVRAdmin**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BVRAdmin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）。
7. 此时会显示**软件包**页面。选择软件包DIVAR IP System Manager，然后单击**安装软件包**以继续。
   此时将显示安装对话框。
8. 在安装对话框中，单击**是，安装**以继续。
   安装随即开始。
   安装过程可能需要几分钟时间。安装过程中请勿关闭系统，也不要移除存储介质。
   观察页面顶部显示的通知。

5.2 使用DIVAR IP 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。
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!
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**BVRAdmin**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BVRAdmin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**软件包名称**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**软件包名称**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**安装软件包**。
   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**是，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，您将收到安装成功的确认消息。
11. 如果安装不成功，您将收到一条相应的消息，告知您在这种情况下如何继续操作。

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*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Remote Portal

您可以通过BoschRemote Portal连接到DIVAR IP all-in-one设备，并通过Remote Portal使用当前和未来功能，例如BoschRemote System Management服务。
有关Remote System Management服务的详细信息，请参阅Remote System Management文档和培训材料。

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 2.3.0（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）
– tls://a1j83emmuys8gs-ats.iot.eu-central-1.amazonaws.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连接**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**Register**以将DIVAR IP all-in-one设备注册到Remote Portal。
4. 如果您的电子邮件被分配给多个具有管理员权限的公司帐户，则会显示一个选择对话框，其中显示相应的公司帐户。
   在选择对话框中，选择您想要注册DIVAR IP all-in-one设备的公司帐户。

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。

5. 如果您还没有Remote Portal帐户，请先单击**Create account**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 使用ASUS Inband工具应用程序监控系统

DIVAR IP all-in-one系统附带预安装的ASUS **Inband工具**应用程序，您可以使用它来监控您的系统。该应用程序服务默认开启。

要启动应用程序，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. 在桌面上的**Tools**文件夹中，双击快捷方式ASUS Inband Tool。
   应用程序随即启动。
3. 使用以下默认凭据登录：

– 账号:**admin**
– 密码：**admin**

4. 首次登录后，系统会要求您更改此初始密码。
   输入新密码并确认。
   确保将新密码存储在安全位置。
   请遵守以下密码要求：

– 密码长度不低于14个字符。
– 密码必须包含至少一个大写字母。
– 密码必须包含至少一个小写字母。
– 密码必须包含至少一个特殊字符。
– 密码必须包含至少一个数字。

5. 确认新密码后，将显示**Dashboard**页面，为您展示系统的整体状态。
6. 在左侧的**MENU**窗格中，您可以选择相应的页面来接收有关系统运行状况的详细信息。
7. 在**SNMP**菜单项中，您可以设置SNMP用户和SMMP目标。
8. 在**Report**页面上，您可以生成包含您选择的适当信息的报告。

7.2.2 使用BMC Web界面监控系统

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

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

首次登录BMC Web界面后，系统会要求您更改初始密码。确保将新密码存储在安全的位置。

请遵守以下密码要求：

– 密码长度不低于14个字符。
– 密码必须包含至少一个大写字母。

– 密码必须包含至少一个小写字母。
– 密码必须包含至少一个特殊字符。
– 密码必须包含至少一个数字。

注意!
出于安全原因，请勿通过BMC端口将设备连接到公共网络。

配置BMC设置
要配置BMC设置，请执行以下操作:
1. 打开装置并按下Del进入BIOS设置。

注意!
BIOS 密码
每个装置均有唯一的初始BIOS密码。可以在装置背面的标签上找到该密码。博世强烈建议更改此初始密码。确保将新密码存储在安全的位置。
请遵守以下密码要求:
- 密码长度不低于14个字符。
- 密码必须包含至少一个大写字母。
- 密码必须包含至少一个小写字母。
- 密码必须包含至少一个特殊字符。
- 密码必须包含至少一个数字。

2. 在BIOS设置中，导航到选项卡**Server Mgmt**.
3. 选择**BMC Network Configuration**选项，然后按下Enter。
4. 在下一个对话框中，选择选项**Configuration Address source**，然后按下Enter。
   此时会显示**Configuration Address source**对话框。
5. 在**Configuration Address source**对话框中，按需要选择BMC地址的配置方式，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。

使用BMC iKVM接口进行远程操作
默认情况下，DIVAR IP all-in-one 7000设备旨在与连接到设备背面HDMI接口的一台或两台本地监视器一起运行。
如果没有本地监视器连接到HDMI接口，则可以使用BMC iKVM接口远程控制设备。
要远程控制系统:
1. 确保没有本地HDMI监视器连接到系统。
2. 登录到BMC Web界面。
3. 在左侧菜单窗格中，选择**Remote Control**页面。
4. 单击**Launch H5Viewer**按钮。
   此时将打开一个窗口，显示DIVAR IP all-in-one 7000监视器输出并实现对远程机器鼠标和键盘的操作控制。

7.3 更换故障硬盘驱动装置并配置新硬盘驱动装置

注意!
对于配备非博世提供的硬盘驱动器的装置，如发生任何数据丢失、损坏，或系统故障，博世概不负责。如果非博世提供的硬盘驱动器被认定为诱发问题的原因，博世将无法提供支持。为解决潜在的硬件问题，博世要求安装博世提供的硬盘驱动器。

7.3.1 更换有故障的硬盘驱动装置

更换有故障的硬盘驱动装置:

- 从装置上卸下故障硬盘驱动装置，然后安装新硬盘驱动装置。
  请参阅安装手册中的安装*SATA*硬盘驱动装置 一章。

7.3.2 使用新硬盘驱动装置重建RAID5

自动RAID5重建

1. 在DIVAR IP all-in-one桌面上，双击**Launch LSA**快捷方式。
   LSI Storage Authority应用程序启动，此时将显示**Remote Server Discovery**页面。
2. 使用**BVRAdmin**管理员帐户凭据登录。
   将显示一个对话框，显示存在一个存在严重问题的控制器。
3. 在页面顶部，单击**Select Controller**，然后单击**Controller ID:**栏打开控制器设置。
   - 如果尚未卸下故障硬盘驱动装置，它将显示在**Drives** > **Foreign Drives** > **Unconfigured Drives下。**
   - 卸下故障硬盘驱动装置并安装新硬盘驱动装置后，系统会自动使用新硬盘驱动装置启动RAID5重建，并且进度条会显示重建进度。
4. 重建成功完成后，将显示  图标。

手动RAID5重建

如果新硬盘驱动装置的RAID5重建没有自动启动，请执行以下操作:

1. 在控制器设置对话框中，在**Drives** > **Foreign Drives** > **Unconfigured Drives**下，选择具有**Unconfigured Bad**状态的硬盘驱动装置，然后在右侧窗格中，选择**Make Unconfigured Good**。
   将显示一个对话框。
2. 选中复选框**Confirm**，然后单击**Yes, Make Unconfigured Good**继续。
   系统使用新硬盘驱动装置启动RAID5重建。
3. 重建成功完成后，将显示  图标。

7.4 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. 登录到管理员帐户（请参见登录到管理员账户）。
2. 在Windows**开始**菜单上，右击**Export System Manager Logs**并以管理员身份运行脚本。
   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。

7.5 恢复装置

要恢复装置:

1. 打开装置，在BIOS开机自检期间按下F7以进入Windows PE。
   此时将显示**System Management Utility**对话框。
2. 选择以下选项之一:
   - **System factory default**：此选项将格式化视频数据分区并使用出厂默认图像恢复操作系统分区。
     完成此过程需要数分钟时间。

- **Full data overwrite and system factory default**：此选项将格式化视频数据分区，完全覆盖现有数据，并使用出厂默认图像恢复操作系统分区。
  注意：完成此过程可能需要几天时间。
- **OS system recovery only**：此选项将使用出厂默认图像恢复操作系统分区，并从现有视频数据分区导入现有虚拟硬盘驱动器。
  完成此过程可能需要数分钟时间。

注意：

OS system recovery only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. 确认所选的选项。
   系统开始格式化和图像恢复过程。
4. 恢复过程完成后，确认系统重新启动。
   系统重新启动并执行设置流程。
5. 该过程完成后，将显示Windows语言选择屏幕。
6. 继续进行初始系统设置。

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

建智能方案，筑更美生活

202404171736