Bosch IP video products

zh-CHS 网络安全指导手册

目录

1 本文档的目的和目标受众

技术的发展突飞猛进，日新月异。人工智能(AI)和物联网(IoT)的飞速发展及大规模普及(AIoT)使产品和服务所面临的风险发生了改变。随着互联程度不断提高，有预谋的恶意攻击也日益猖獗。Bosch的目标是为客户提供安全可靠的产品和服务。

本指南旨在帮助集成商加强Bosch IP视频产品，以更加符合客户现有的网络安全策略和程序。

本指南将涵盖:

- 有关Bosch IP视频设备功能和基本原理的重要信息
- 可修改或禁用的特定功能
- 可激活和使用的特定功能
- 与视频系统和安全性相关的最佳做法

本指南将着重介绍如何利用Configuration Manager执行相关配置。在大多数情况下，利用BVMS Configuration Client、Configuration Manager以及视频设备的内置web界面就能完成全部配置。

2 安全概念和注意事项

在当今的网络环境中，IP视频产品变得越来越普遍。与任何放置在网络上的IP设备一样，IT管理员和安防管理员都有权全面了解设备的功能集和功能。

在使用Bosch IP视频设备时，您的第一道防线就是设备本身。Bosch编码器和摄像机的制造环境受控、安全，且持续受到审核。只能通过有效的固件上载来写入设备，这是硬件系列和芯片组所特有的。

大多数Bosch IP视频设备都带有板载安全芯片，提供类似于加密智能卡的功能和所谓的Trusted Platform Module（简称TPM）。此芯片的作用就像关键数据的保险箱，即使在有人以物理方式打开摄像机以获得访问权限的情况下，仍能保护证书、密钥、许可证等免受未经授权的访问。

Bosch IP视频设备已经过独立安防供应商执行的三万(30,000)多次漏洞和侵入测试。到目前为止，在提供适当保护的设备上尚未发生过成功的网络攻击。

3 安全安装

3.1 服务器和存储设备

所有服务器组件（例如BVMS Management Server和Video Recording Manager服务器）和存储设备应安装在安全区域。应通过门禁控制系统限制对此安全区域的访问，并进行监控。应将有权进入中央服务器机房的用户组限制为一小部分人员。
尽管服务器和存储设备安装在安全区域，但仍然必须进行保护以防止未经授权的访问。

参阅

– *强化服务器, 页面 28*
– *强化存储, 页面 27*

3.2 摄像机和前端设备

安装摄像机和前端设备时，应选择安全的安装位置和安装方向。理想情况下，在这个位置，设备不应受到有意或无意的干扰。

4 安全配置

4.1 分配IP地址

所有Bosch IP视频设备目前到货时都处于出厂默认状态，可以随时接受DHCP IP地址。
如果部署设备的活跃网络中没有DHCP服务器可用，则设备将（如果运行固件6.32或更高版本）自动从169.254.1.0至169.254.254.255或169.254.0.0/16的范围中选择一个链路本地地址。
对于较早版本的固件，它会为自己分配默认IP地址192.168.0.1。
有多个工具可用于对Bosch IP视频设备执行IP地址分配，包括：

- Bosch Configuration Manager
- BVMS Configuration Client
- BVMS Configuration Wizard

所有软件工具都提供同时为多台设备分配单个静态IPv4地址以及某个IPv4地址范围的选项。这包括子网掩码和默认网关寻址。
所有IPv4地址和子网掩码值都需要以“点分十进制表示法”输入。

注意！
要限制由未经授权的本地连接网络设备对网络进行内部网络攻击的可能性，第一步包括限制可用但未使用的IP地址。具体方法是使用IPAM（**IP A**ddress **M**anagement，IP地址管理）并对将要使用的IP地址范围划分子网。

划分子网是指从IP地址的主机部分借用位来将一个大型网络分成几个小型网络。借用的位越多，可以创建的网络就越多，但每个网络支持的主机地址越少。

后缀	主机	CIDR	借用	Binary
.255	1	/32	0	.11111111
.254	2	/31	1	.1111111**0**
.252	4	/30	2	.111111**00**
.248	8	/29	3	.11111**000**
.240	16	/28	4	.1111**0000**
.224	32	/27	5	.111**00000**
.192	64	/26	6	.11**000000**
.128	128	/25	7	.1**0000000**

自1993年以来，互联网工程任务组(IETF)提出了一种分配IPv4地址块的新概念，所采用的方法以比以前的“有类网络”寻址体系结构更灵活。这种新方法称为“无类域间路由选择”(CIDR)，也适用于IPv6地址。

IPv4有类网络被指定为A、B和C类（分别有8、16和24个网络号位）及D类（用于多播寻址）。

示例：
为了便于您理解，我们将以C类地址情景为例进行说明。C类地址的默认子网掩码为255.255.255.0。从技术上讲，并未对此掩码进行子网划分，因此最后一个八位字节整个都可用于有效的主机寻址。从主机地址借位时，我们可以选择在最后一个八位字节中使用以下掩码：
.128、.192、.224、.240、.248和.252。

如果使用255.255.255.240子网掩码（4位），我们将创建16个较小的网络，每个子网支持14个主机地址。

– 子网ID 0：
  主机地址范围192.168.1.1至192.168.1.14。广播地址192.168.1.15
– 子网ID 16：
  主机地址范围192.168.1.17至192.168.1.30。广播地址192.168.1.31
– 子网ID：32、64、96等

对于较大的网络，可能需要下一个较大的B类网络，或定义适当的CIDR块。

示例：
在部署视频安防网络之前，您可以简单地计算一下网络上需要多少个IP设备，以便为未来发展留出空间：
– 20个视频工作站
– 1个中央服务器
– 1个VRM服务器
– 15个iSCSI存储阵列
– 305个IP摄像机

总共需要342个IP地址

考虑到计算出的IP地址数量（342个），我们至少需要B类IP地址方案来容纳这么多IP地址。使用默认的B类子网掩码255.255.0.0，可在网络中使用65534个可用的IP地址。

也可以按以下方式规划网络：使用CIDR块，23位用作前缀，同时提供512个地址的地址空间，分别对应510个主机。

通过将较大的网络分成较小的部分、简单地进行子网划分或指定CIDR块，可以降低这种风险。

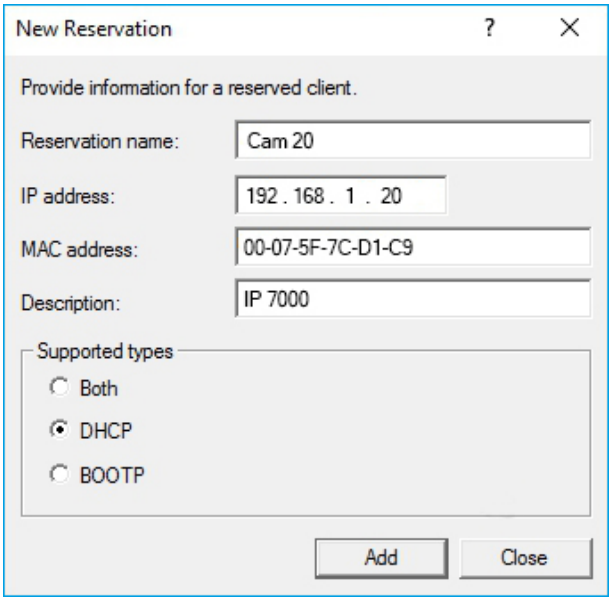
示例：

	默认	**子网**
IP 地址范围	172.16.0.0 - 172.16.255.255	172.16.8.0 - 172.16.9.255
子网掩码	255.255.0.0	255.255.254.0
CIDR表示法	172.16.0.0/16	172.16.8.0/23
子网数量	1	128
主机数量	65.534	510
多余的地址	65.192	168

4.1.1 管理DHCP

IPAM可以利用DHCP作为在环境中控制和使用IP地址的强大工具。DHCP可以配置为使用特定范围的IP地址。它还可以配置为排除某个地址范围。

如果使用DHCP，在部署视频设备时，最好基于每台设备的MAC地址配置不失效的地址保留。



注意!
即便是在使用IP地址管理跟踪IP地址的使用情况之前，网络管理的一个最佳实践是通过边缘交换机上的端口安全性限制对网络的访问，例如，仅一个特定的MAC地址可以通过某个特定的端口访问。

4.2 用户帐户和密码

所有Bosch IP视频摄像机和编码器都带有三个内置的用户帐户：

- **live**
  这是一个标准用户帐户，仅允许访问实况视频流。
- **user**
  这是一个更高级的用户帐户，允许访问实况和录制的视频，以及PTZ控制等摄像机控制。
  此帐户不允许访问配置设置。
- **service**
  这是一个管理员帐户，提供对所有设备菜单和配置设置的访问权限。

必须为每个用户帐户分配一个密码。
密码分配是保护任何网络设备的重要一步。强烈建议为所有已安装的网络视频设备分配密码。

注意!
在固件版本6.30中，用户管理得到增强，具有更大的灵活性，允许其他用户和用户名使用自己的密码。以前的帐户级别现在成为用户组级别。
固件版本6.32引入了更严格的密码策略（有关详细信息，请参阅*使用设备网页分配密码, 页面 11*）。

4.2.1 分配密码

根据视频安防系统的规模和所使用的软件，可以通过多种方式指定密码。在仅包含几台摄像机的小型安装系统中，密码可以使用设备的网页设置，也可以使用配置向导Bosch Configuration Manager进行设置，因为它支持同时进行多个设备的配置，非常方便。

注意!
如前所述，如果要保护数据免遭可能的网络攻击，密码保护至关重要。这适用于完整安全基础架构中的所有网络设备。大多数组织已经拥有强大的密码策略，但如果您正在使用没有策略的新系统，以下是实施密码保护时的一些最佳实践:
- 密码长度应在8到12个字符之间。
- 密码应包含大写和小写字母。
- 密码应至少包含一个特殊字符。
- 密码应至少包含一位数字。

示例:
使用密码短语“to be or not to be”以及我们的基本规则来生成可靠的密码。
– 2be0rnOt!t0Be

注意!
由于“@”、“&”、“<”、“>”、“:”等特殊字符在XML及其他标记语言中具有专用的含义，因此在密码中使用此类特殊字符有一些限制。尽管Web界面接受这些特殊字符，其他管理和配置软件可能会拒绝接受。

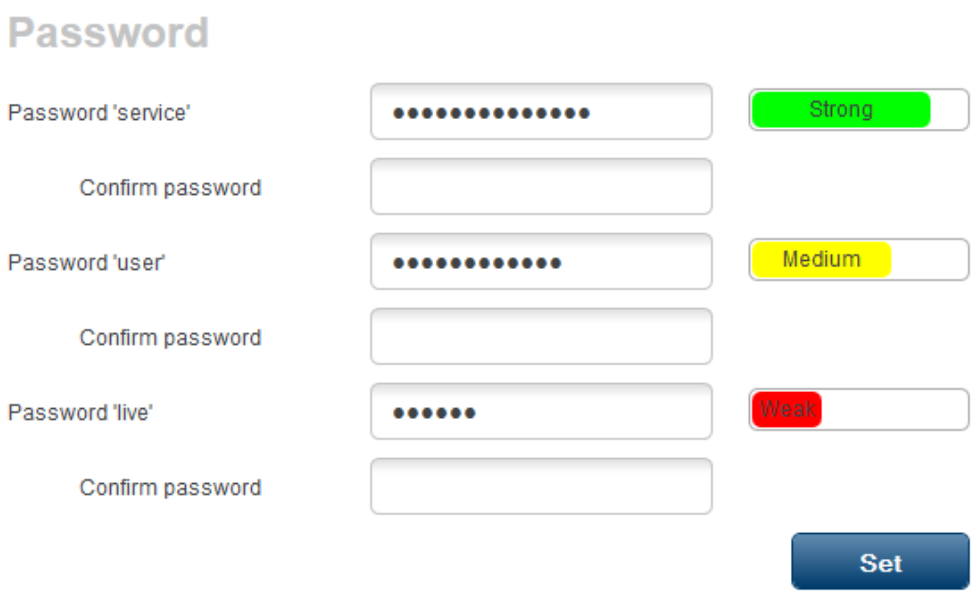
4.2.2 使用设备网页分配密码

1. 在设备网页上，导航到**配置**页面。
2. 选择**常规**菜单和**用户管理**子菜单（注意：如果固件版本低于6.30，**用户管理**子菜单的名称为**密码**）。

首次进入摄像机的网页时，会要求用户指定密码以确保最低限度的保护。
只要未设置密码，每次重新加载摄像机网页时，始终会重复出现此提示。单击**确定**将自动进入**用户管理**菜单。

固件6.30提供了激活**Do not show...**（请勿显示...）复选框的选项。在固件6.32中，已删除此选项，以避免出现安防疏漏。

1. 选择**用户管理**菜单，然后分别为三个帐户输入所需的密码并确认。
   请注意:
   – 首先需要在最高访问级别(**密码 'service'**)指定密码。
   – 从固件版本6.20起，引入了一种称为“密码强度表”的新指标，用于提示密码的潜在强度。这只是一个辅助工具，并不能保证密码真正符合安装系统的安防需求。
2. 单击**设置**以推送并保存更改。



固件版本6.30引入的**用户管理**提供了更大的灵活性，可以创建自由命名的用户，他们将使用自己的密码。以前的帐户级别现在代表用户组级别。

以前的用户仍然存在，仍然使用运行早期固件时指定的密码，不能删除，也不能改变其用户组级别。

单击 或 可以指定或更改密码。
只要不是所有的用户都有密码保护，就会显示警告消息。

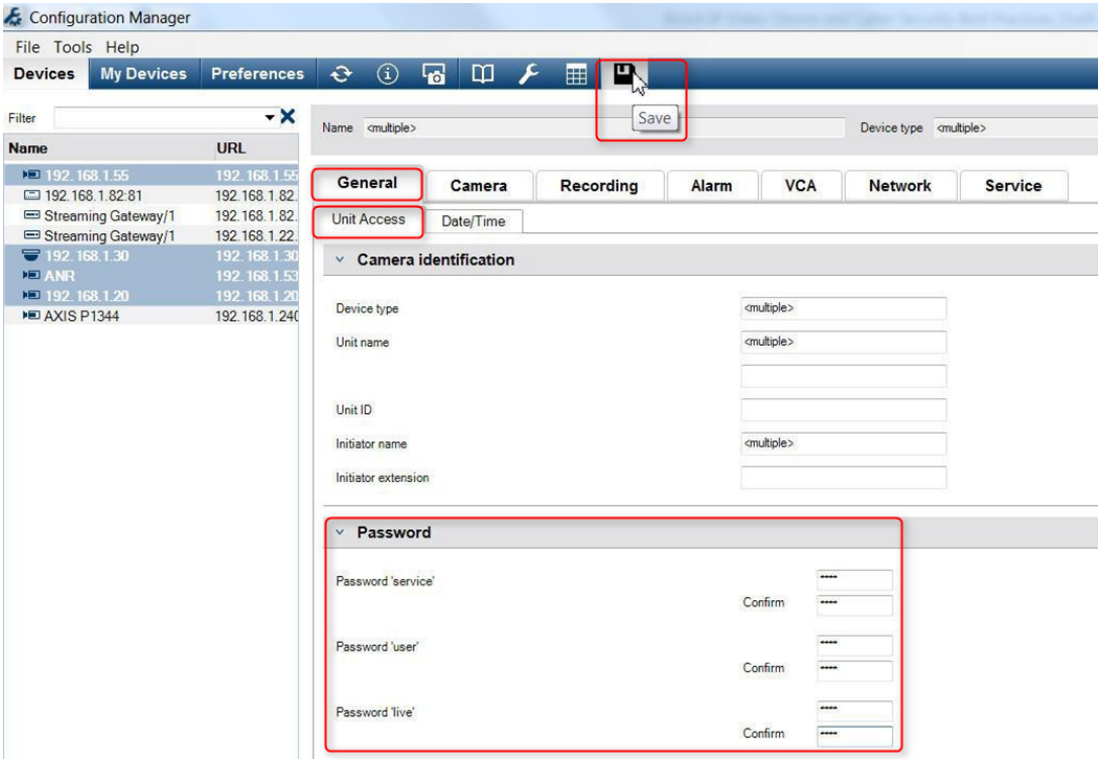
1. 要添加新用户，请单击**添加**。
   此时将出现弹出窗口。
2. 输入新凭证，并分配用户组。
3. 单击**设置**保存更改。

注意!
在固件版本6.32中，也引入了更严格的密码策略。
现在要求密码的长度最少为8个字符。

4.2.3 使用Configuration Manager分配密码

使用Bosch Configuration Manager，可以将密码轻松应用于单个设备，也可同时应用于多个设备。

1. 在Configuration Manager中，选择一个或多个设备。
2. 选择**常规**选项卡，然后选择**装置访问**。
3. 在**密码**菜单中，分别为三个帐户输入所需的密码并确认（**密码 'service'**、**密码 'user'**和**密码 'live'**）。
4. 单击  以推送并保存更改。



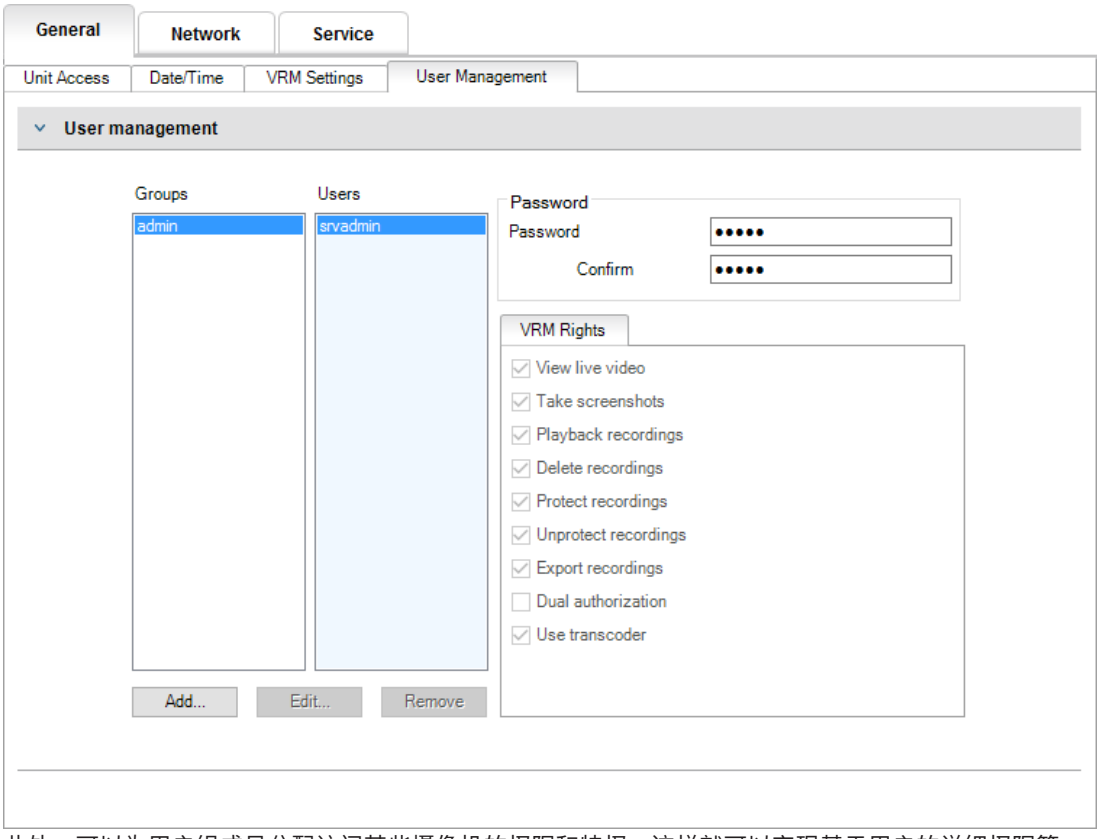
在由BVMS或安装在录制设备上的Video Recording Manager管理的大型系统中，可以对添加到系统中的所有IP视频设备应用全局密码。这样便于轻松管理并确保整个网络视频系统都有标准的安全级别。

4.2.4 为独立安装VRM分配密码

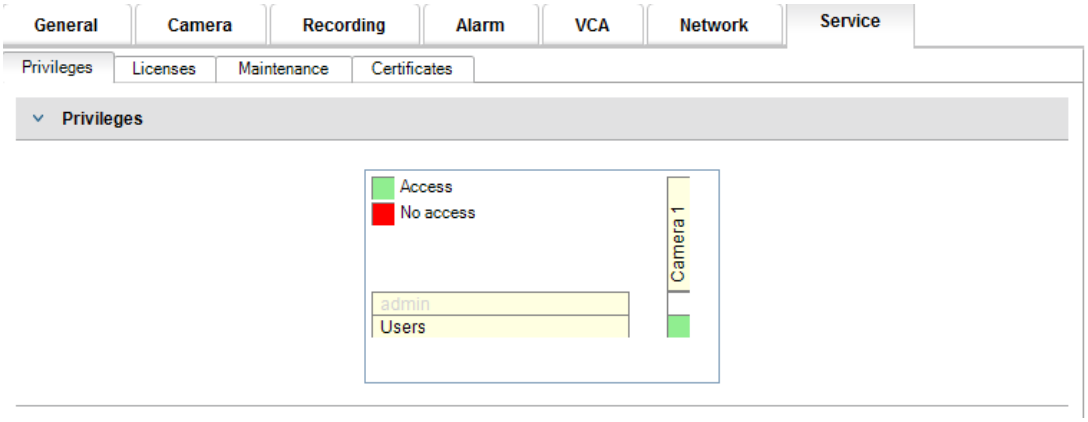
Video Recording Manager提供用户管理以增强灵活性和安全性。

默认情况下，没有为任何用户帐户分配密码。密码分配是保护任何网络设备的重要一步。强烈建议为所有已安装的网络视频设备分配密码。

这同样适用于Video Recording Manager的用户。



此外，可以为用户组成员分配访问某些摄像机的权限和特权。这样就可以实现基于用户的详细权限管理。



4.2.5 使用BVMS（在DIVAR IP或独立系统上）分配密码

设备密码保护

由BVMS管理的摄像机和编码器可以通过密码保护来防止未经授权的访问。
编码器/摄像机的内置用户帐户的密码可以通过BVMS Configuration Client进行配置。
在BVMS Configuration Client中为内置用户帐户设置密码的步骤如下：

1. 在设备树中选择所需的编码器。
2. 右击编码器，然后单击**更改密码...**。
3. 为三个内置用户帐户输入密码：live、user和service。

默认密码保护

BVMS版本5.0及更高版本能够在多达2000个IP摄像机组成的视频系统中的所有设备上实施全局密码。
您可以通过BVMS Configuration Wizard（与DIVAR IP 3000或DIVAR IP 7000录像设备一起使用时）或任何系统上的BVMS Configuration Client访问该功能。
在BVMS Configuration Client中访问全局密码菜单的步骤如下：

1. 在**硬件**菜单上，单击**使用默认密码保护设备...**。
2. 在**全局默认密码**字段中，输入密码并选择**强制用密码保护激活**。

保存并激活系统更改后，输入的密码将应用于所有设备的live、user和service帐户，包括Video Recording Manager的管理员帐户。

注意!

如果设备的其中一个帐户中已经设置了密码，则此密码不会被覆盖。
例如，如果为service设置了密码，但没有为live和user设置密码，则仅会为live和user帐户配置全局密码。

BVMS配置和VRM设置

默认情况下，BVMS使用内置管理员帐户**srvadmin**连接到具有密码保护的Video Recording Manager。为避免Video Recording Manager遭到未经授权的访问，应使用复杂的密码保护管理员帐户**srvadmin**。
在BVMS Configuration Client中修改**srvadmin**帐户密码的步骤如下：

1. 在设备树中，选择VRM设备。
2. 右击VRM设备，然后单击**更改 VRM 密码。**
   此时会显示**更改密码...**对话框。
3. 为**srvadmin**帐户输入新密码，然后单击**确定**。

与摄像机的加密通信

从BVMS版本7.0开始，可以对摄像机和BVMS Operator Client、Configuration Client、Management Server、Video Recording Manager之间的实况视频数据和控制通信加密。
在**编辑编码器**对话框中启用安全连接后，BVMS服务器、Operator Client和Video Recording Manager将使用安全的HTTPS连接来连接到摄像机或编码器。
BVMS内部使用的连接字符串将从rcpp://a.b.c.d（端口1756上的普通RCP+连接）更改为https://a.b.c.d（端口443上的HTTPS连接）。
对于不支持HTTPS的传统设备，连接字符串保持不变(RCP+)。

如果选择HTTPS通信，通信将使用HTTPS (TLS)，通过设备中的加密引擎对所有控制通信和视频负载加密。使用TLS时，将通过长度高达256位的AES加密密钥对所有HTTPS控制通信和视频负载加密。
在BVMS Configuration Client中启用加密通信的步骤如下：

1. 在设备树中选择所需的编码器/摄像机。

2. 右击编码器/摄像机，然后单击**编辑编码器**。
3. 在**编辑编码器**对话框中，启用**安全连接。**
4. 保存并激活配置。

启用与编码器的安全连接后，可以禁用其他协议（参见*一般网络端口的使用和视频传输, 页面 16*）。

注意!
BVMS仅支持默认的HTTPS端口443，不支持使用其他端口。

4.3 强化设备访问

所有Bosch IP视频设备都带有内置的多用途网页。设备专用的网页支持实况和回放视频功能，以及一些可能无法通过视频管理系统访问的特定配置设置。内置的用户帐户具有对专用网页不同部分的访问权限。虽然无法通过网页本身完全禁用网页访问 - 可使用Configuration Manager，但有几种方法可以隐藏设备的存在、限制访问和管理视频端口的使用。

4.3.1 一般网络端口的使用和视频传输

所有Bosch IP视频设备都使用Remote Control Protocol Plus (RCP+)进行检测、控制和通信。
RCP+是一种专有的Bosch协议，使用特定的静态端口 - 1756、1757和1758 - 对Bosch IP视频设备进行检测并与之通信。与BVMS或其他通过Bosch VideoSDK与Bosch IP视频设备集成的第三方供应商视频管理系统一起使用时，所列端口必须可从IP视频设备所在的网络上访问，才能正常工作。

从设备流式传输视频的方式有多种：UDP（动态）、HTTP (80)或HTTPS (443)。
HTTP和HTTPS端口的用法可以修改（参见*HTTP、HTTPS和视频端口使用, 页面 17*）。在对端口进行任何修改之前，必须配置所需的设备通信形式。可以使用Configuration Manager访问通信菜单。

1. 在Configuration Manager中，选择所需的设备。
2. 选择**常规**选项卡，然后选择**装置访问**。
3. 找到页面的**设备访问**部分。

4. 在**协议**列表中，选择所需的协议：

- RCP+
- HTTP（默认）
- HTTPS

如果选择HTTPS通信，Configuration Manager与视频设备之间的通信将使用HTTPS (TLS)，通过最大长度为256位的AES加密密钥加密有效载荷。这是一项免费的基本功能。使用TLS时，所有HTTPS控制通信和视频有效载荷均通过设备中的加密引擎进行加密。

注意!
加密专用于“传输路径”。软件或硬件解码器接收视频之后，将对视频流进行永久解密。

4.3.2 最低TLS版本

一些旧版的客户端可能需要使用安全性较低的早期TLS版本。但如有可能，请为TLS定义一个最低版本，以避免客户端强制设备进入安全性较低的访问模式。
选择尽可能最高的TLS版本作为最低版本。

注意!
在定义从客户端软件访问设备的最低安全级别时，请确保设备中允许更低访问级别的所有端口和协议都已关闭或禁用。

4.3.3 HTTP、HTTPS和视频端口使用

可以更改或关闭所有设备上的HTTP和HTTPS端口的使用。可以通过禁用RCP+端口和HTTP端口来强制执行加密通信，强制所有通信使用加密。如果关闭HTTP端口的使用，HTTPS将保持打开状态，无论如何尝试关闭它都将失败。

1. 在Configuration Manager中，选择所需的设备。
2. 选择**网络**选项卡，然后选择**网络访问**。
3. 找到页面的**详细资料** 部分。

4. 在**详细资料**部分，使用下拉菜单修改HTTP和HTTPS浏览器端口及RCP+端口：
   - HTTP浏览器端口修改：将80或端口10000改为10100
   - HTTPS浏览器端口修改：将443或端口10443改为10543
   - RCP+端口1756：**开启**或**关闭**

注意!
在固件版本6.1x中，如果禁用HTTP端口，并尝试访问设备的网页，则会将该请求定向到当前定义的HTTPS端口。
在固件版本6.20及更高版本中，将省略重定向功能。如果禁用HTTP端口，并且已将HTTPS端口修改为使用443以外的端口，则只能通过导航到设备IP地址加上分配的端口完成网页访问。

示例:
https://192.168.1.21:10443。任何连接到默认地址的尝试都将失败。

4.3.4 视频软件和端口选择

在您的LAN中使用视频管理软件时，调整这些设置也会影响用于视频传输的端口。
如果所有IP视频设备均设置为HTTP端口10000（举个例子），且为“TCP数据通道”配置BVMS Operator Client，则网络上发生的所有视频传输将通过HTTP端口10000完成。

注意!
设备中的端口设置更改必须与管理系统及其组件以及客户端中的设置相匹配。

注意!
根据系统的部署方案和安全目标，最佳实践可能会有所不同。禁用和重定向HTTP或HTTPS端口的使用有它的优点。更改任一协议中的端口都有助于避免向NMAP（网络映射器、免费安全扫描器）等网络工具提供信息。诸如NMAP之类的应用程序通常用作侦察工具，以识别网络上任何设备的弱点。这种技术与强密码实施相结合，增加了系统的整体安全性。

4.3.5 SSH数据通道

对于使用BVMS Operator Client通过公共网络进行远程设备访问的情况，BVMS提供Secure Shell (SSH)数据通道以确保安全（加密）通信。
SSH数据通道可以构建通过SSH协议/套接字连接建立的加密通道。该加密通道可以传输加密和未加密的流量。博世SSH还可以使用Omni-Path协议实现，这是由Intel开发的高性能低延迟通信协议。

有关如何在BVMS中配置SSH服务的更多信息，请参见BVMS文档。
有关如何在BVMS Operator Client中配置DIVAR IP系统安全远程访问的更多信息，请参见DIVAR IP文档。

4.3.6 Telnet访问

Telnet是一种应用层协议，通过虚拟终端会话提供与设备的通信，用于维护和故障排除。所有Bosch IP视频设备都支持Telnet，版本6.1x及以下的固件版本中，均默认启用Telnet支持。从固件版本6.20开始，默认禁用Telnet端口。

注意!
自2011年以来，利用Telnet协议实施的网络攻击日益猖獗。在当今的环境中，最佳实践表明应在所有设备上禁用Telnet支持，除非为了进行维护或故障排除而需要启用。

1. 在Configuration Manager中，选择所需的设备。
2. 选择**网络**选项卡，然后选择**网络访问**。
3. 找到页面的**详细资料** 部分。

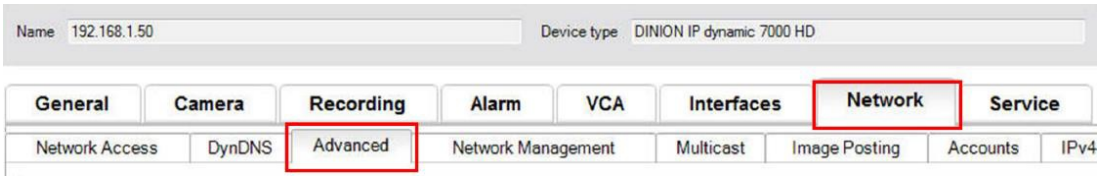
4. 在**详细资料**部分，使用下拉菜单**开启**或**关闭Telnet 支持**。

注意!
从固件版本6.20开始，通过使用安全HTTPS连接的“web套接字”也可以支持Telnet。Web套接字不使用标准Telnet端口，而是在需要时提供一种安全访问IP设备命令行界面的方式。

4.3.7 RTSP：实时流传输协议

实时流协议(RTSP)是ONVIF协议向符合ONVIF标准的视频管理系统提供流视频和设备控制时所使用的主要视频组件。各种第三方视频应用程序也使用RTSP实现基本流式传输功能，在某些情况下，RTSP还可用于设备和网络故障排除。所有Bosch IP视频设备都能够使用RTSP协议提供流式传输。
使用 Configuration Manager可轻松修改RTSP服务。

1. 在Configuration Manager中，选择所需的设备。
2. 选择**网络**选项卡，然后选择**高级**。



3. 找到页面的**RTSP**部分。
4. 在**RTSP 端口**下拉菜单中，关闭或修改RSTP服务：

- RTSP默认端口：554
- RTSP端口修改：10554改为10664

注意!
近年来有过利用RTSP堆栈溢出缓冲区攻击实施网络攻击的报告。这些攻击是针对特定供应商的设备而编写的。最佳实践是，如果符合ONVIF标准的视频管理系统不使用该服务或在基本的实时流中不使用该服务，则应禁用该服务。
或者，在接收客户端允许的情况下，可以使用HTTPS连接作为RTSP通信的传输通道，这是迄今为止传输加密RTSP数据的唯一方法。

注意!
有关RTSP的更多详细信息，请参阅博世智能建筑科技在线产品目录中的应用说明*博世VIP设备的RTSP用法*，链接如下：
https://resources-boschsecurity-cdn.azureedge.net/public/documents/RTSP_VIP_Application_note_enUS_9007200806939915.pdf

4.3.8 UPnP：通用即插即用

Bosch IP视频设备能够通过**通用即插即用**与网络设备进行通信。该功能主要用于仅包含几台摄像机的小型系统中，在此类系统中，摄像机会自动出现在PC的网络目录中，因此可以很容易地找到。但它们对网络中的任何设备都会执行此操作。
通用即插即用可使用Configuration Manager关闭。

1. 在Configuration Manager中，选择所需的设备。
2. 选择**网络**选项卡，然后选择**网络管理**。

3. 找到页面的**通用即插即用**部分。
4. 在**通用即插即用**下拉菜单中，选择**关闭**以禁用**通用即插即用**。

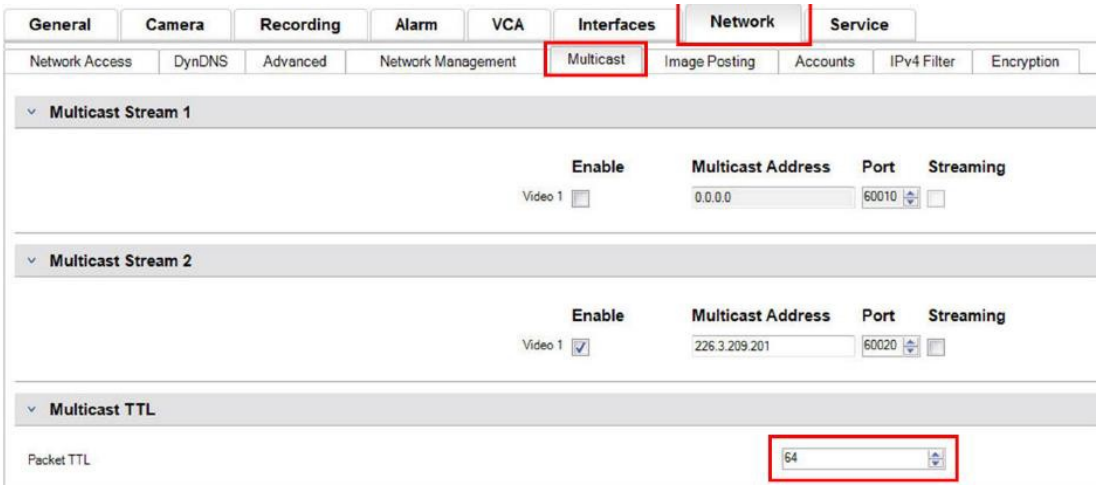
注意!
由于大量的注册通知以及非必要访问或攻击的潜在风险，**通用即插即用**不应用于大型系统。

4.3.9 多播

所有Bosch IP视频设备都能够提供“按需组播”或“组播流”视频。单播视频传输以目的地为基础，而组播以源为基础，这可能在网络级别引发安全问题，包括：组访问控制、组中心信任和路由器信任。虽然路由器配置不在本指南的讨论范围内，但有一种安全解决方案可以从IP视频设备本身实施。
TTL（生存时间）范围定义允许组播流量在网络中流动的位置和距离，每一跳将TTL减小1。配置IP视频设备用于组播时，可以修改设备的数据包TTL。

1. 在Configuration Manager中，选择所需的设备。
2. 选择**网络**选项卡，然后选择**组播**。
3. 找到页面的**组播 TTL**部分。
4. 使用以下TTL值和范围限制，调整**数据包 TTL**设置：
   - TTL值0 = 仅限本地主机
   - TTL值1 = 仅限同一子网
   - TTL值15 = 仅限同一站点
   - TTL值64（默认）= 仅限同一区域
   - TTL值127 = 全球范围
   - TTL值191 = 全球范围，使用有限带宽

– TTL值255 = 无限制数据

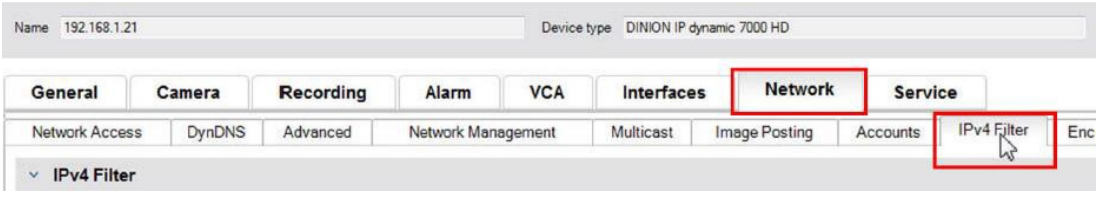


注意!
处理视频监控数据时，最佳做法是将TTL设置设置为15，限制为同一站点。或者更好的方法是，如果您知道确切的最大跳距数，请将此作为TTL值。

4.3.10 IPv4过滤

您可以通过称为IPv4过滤的功能，限制对任何Bosch IP视频设备的访问。IPv4过滤利用“子网划分”的基本原理来定义最多两个允许的IP地址范围。定义范围之后，它将拒绝来自这些范围之外的任何IP地址的访问。

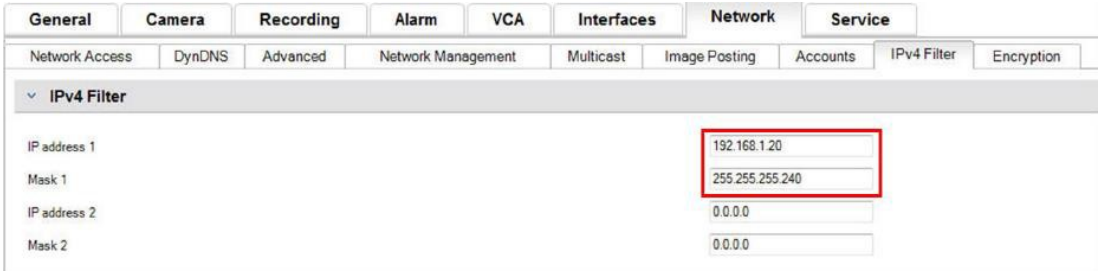
1. 在Configuration Manager中，选择所需的设备。
2. 选择**网络**选项卡，然后选择**IPv4 过滤器**。



注意!
要成功配置此功能，您必须对子网划分有基本的了解，或者有权访问子网计算器。在此设置中输入不正确的值可能会限制对设备本身的访问，并且可能需要执行出厂默认重置，才能重新获得访问权限。

3. 要添加过滤器规则，请输入以下两项：
   – 输入在您创建的子网规则范围内的基本IP地址。
     基本IP地址用于指定您允许的子网，且必须在所需范围内。
   – 输入用于定义IP地址的子网掩码，IP视频设备将通过该IP地址接受通信。

在下面的示例中，已输入**IP 地址 1** 192.168.1.20和**遮挡 1** 255.255.255.240。此设置将限制来自定义的IP范围（192.168.1.16到192.168.1.31）内的设备的访问。



使用**IPv4 过滤器**功能时，能够通过RCP+对设备进行扫描，但不能通过允许的IP地址范围以外的客户端访问配置设置和视频。其中包括网页浏览器访问。
IP视频设备本身并不需要位于允许的地址范围内。

注意!
使用**IPv4 过滤器**选项可以使设备在非必要情况下在网络上不可见，具体取决于系统设置。如果启用此功能，请确保记录设置以供将来参考。
请注意，仍然可以通过IPv6访问设备，因此IPv4过滤仅在纯IPv4网络中有效果。

4.3.11 SNMP

简单网络管理协议(SNMP)是一种监控系统运行状况的通用协议。这样的监控系统通常有一个中央管理服务器，它从系统的兼容组件和设备收集所有数据。
SNMP提供两种获取系统运行状况的方法：

- 网络管理服务器可以通过SNMP请求轮询设备的运行状况。
- 在出现错误或警报状况时，设备可以通过向SNMP服务器发送SNMP陷阱的方式，主动通知网络管理服务器其系统运行状况。此类陷阱必须在设备内部配置。

此外，SNMP也允许在设备和组件内配置一些变量。
关于设备支持哪些消息以及可以发送哪些陷阱的信息，是从管理信息库（即所谓的MIB文件）导出的，该文件随产品一起提供，可轻松集成到网络监控系统中。

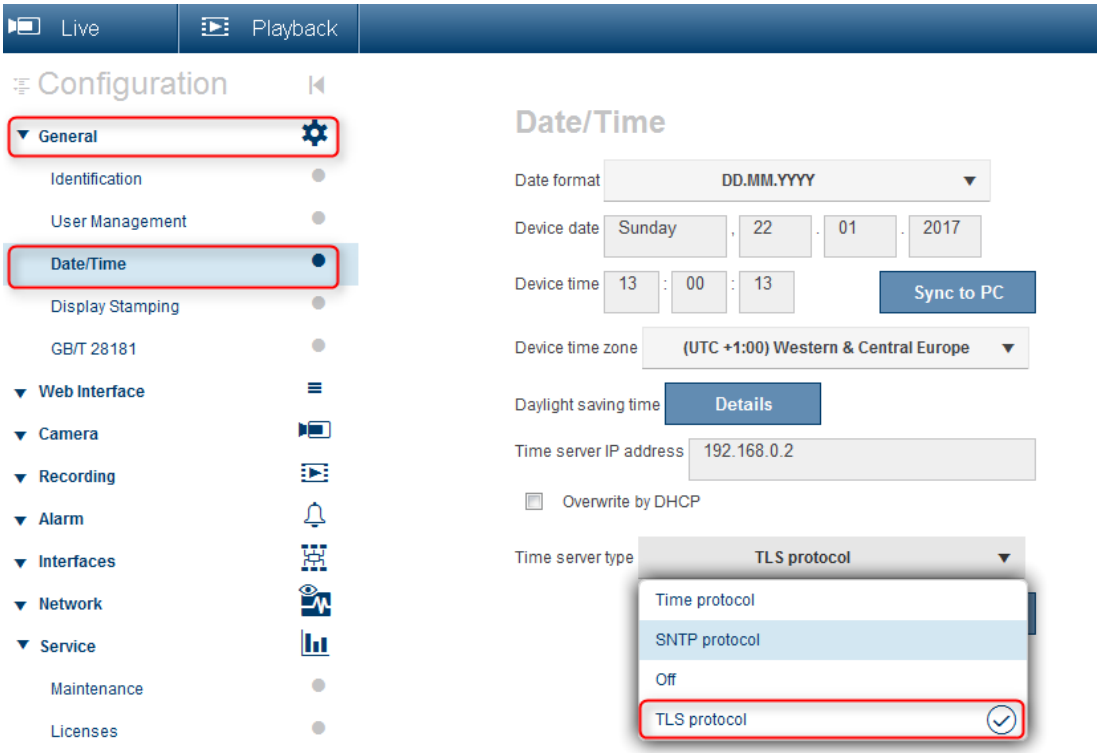
有三种不同版本的SNMP协议：

- SNMP版本1
  SNMP版本1(SNMPv1)是SNMP协议的初始实施。该版本获得了广泛使用，已成为网络管理和监控的实际标准协议。
  但由于SNMPv1缺乏安防功能，已经受到威胁。它只使用“*团体字符串*”作为一种密码，以明文形式传输。
  因此，只有在能够保证网络受到物理保护，可防止未经授权的访问时，才能使用SNMPv1。
- SNMP版本2
  SNMP版本2(SNMPv2)包括安全性和机密性等方面的改进，并引入了批量请求，可在单次请求中检索大量数据。不过，它的安防方法被认为过于复杂，因而无法获得广泛接受。
  因此，它很快就被版本SNMPv2c取而代之，后者相当于SNMPv2，但没有使用其备受争议的安全模型，而是恢复到SNMPv1基于团体的方法，同样缺乏安全性。
- SNMP版本3
  SNMP版本3(SNMPv3)主要增加了安全性和远程配置增强功能。其中包括通过对数据包进行加密、消息完整性和身份验证来提高机密性。
  该版本还解决了SNMP的大规模部署问题。

注意!
由于缺乏安全功能，SNMPv1和SNMPv2c都受到威胁。它们只使用“社区字符串”作为一种密码，以明文形式传输。
因此，只有在确保网络获得物理保护可以防止未经授权的访问时，才应使用SNMPv1或SNMPv2c。
博世摄像机目前仅支持SNMPv1。如果不使用SNMP，请确保将其关闭。

4.3.12 安防时间基准

除了时间协议和SNTP（两者都是非安全协议）之外，固件版本6.20还引入了时间服务器客户端的第三种模式，使用TLS协议。这种方法通常也称为*TLS日期*。
在这种模式下，任意HTTPS服务器都可用作时间服务器。时间值作为HTTPS握手过程副作用导出。传输是受TLS保护的。可以将HTTPS服务器的可选根证书加载到摄像机的证书存储区，以对服务器进行验证。



注意!
请确保输入的时间服务器IP地址本身具有稳定且不受损害的时基。

4.3.13 基于云的服务

所有Bosch IP视频设备均可与Bosch的基于云的服务（例如Remote Portal）通信。这将允许IP视频设备使用诸如Remote Device Management或Cloud VMS等服务将警报和其他数据转发到中心站，具体取决于部署区域。
如需更多信息，请参阅博世智能建筑科技知识库：
https://community.boschsecurity.com。

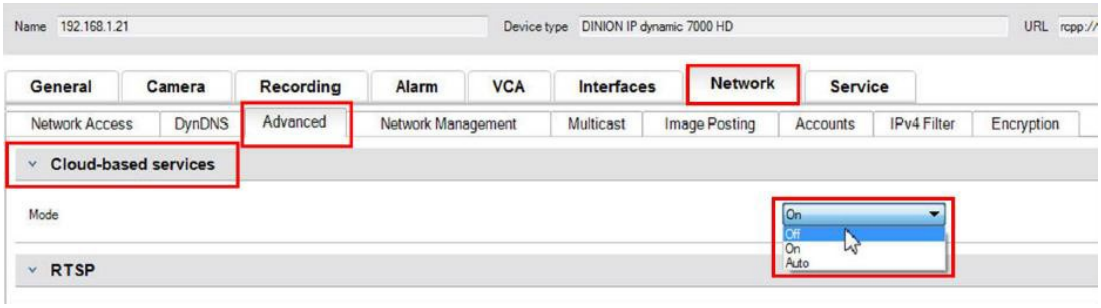
基于云的服务有三种操作模式：

– **开启**：
  视频设备将不断轮询云服务器。

– **自动**（默认）：
视频设备将尝试轮询云服务器几次，如果不成功，它将停止尝试访问云服务器。
– **关闭**：
不进行轮询。

使用Configuration Manager可以轻松关闭基于云的服务。

1. 在Configuration Manager中，选择所需的设备。
2. 选择**网络**选项卡，然后选择选项卡**高级**。
3. 找到页面的**基于云的服务**部分，然后从列表中选择**Off**。



注意!
如果您使用的是博世基于云的服务，请保留默认配置。
在所有其他情况下，将基于云的服务模式切换为**Off**。

4.4 强化IP摄像机

博世IP摄像机出厂时采用默认配置，可轻松集成到不同环境中。
根据目标环境及其预期的安全级别，可能需要更改某些摄像机设置以提高网络和数据安全性。
但是，操作环境可能存在限制，要求使用某种安全性较低的协议或功能（例如SNMPv1）。

4.4.1 强化级别

指定了两种强化级别：*提升*和*严格*。
强化级别 - *严格* - 设置设备的方式更安全，但设备的使用可能会受到限制，因为自动发现设备等功能被禁用。应针对每个功能评估是否可以应用设置*提升*或*严格*。

4.4.2 强化概述

网络 - 网络服务	默认	提升	严格
HTTP	启用	禁用	禁用
HTTPS	启用	启用	启用
RTSP	启用	可选	禁用
RCP	启用	禁用	禁用
SNMPv1	禁用	禁用	禁用
SNMPv3	禁用	启用	启用
iSCSI	启用	可选	禁用
UPnP	禁用	禁用	禁用
NTP服务器	禁用	禁用	禁用
Discovery	启用	启用	禁用

网络 - 网络服务	默认	提升	严格
ONVIF Discovery	启用	启用	禁用
GBT/28181	禁用	禁用	禁用
密码重置机制	启用	禁用	禁用
Ping响应	启用	启用	禁用
RTSPS	启用	启用	启用
HTTP	启用	禁用	禁用

网络 - 网络访问	默认	提升	严格
最低TLS版本	1.0	1.2	1.2
HSTS	禁用	启用	启用

网络 - 高级	默认	提升	严格
802.1x	禁用	可选	启用
Syslog	禁用	TCP	TLS

网络 - 网络管理	默认	提升	严格
SNMPv3模式	禁用	SHA1 / AES	SHA1 / AES

网络 - IPv4 过滤器	默认	提升	严格
IPv4过滤器	禁用	启用	启用

常规 - 日期/时间	默认	提升	严格
日期/时间（NTP客户端）	禁用	SNTP/TLS日期	TLS日期

连接 - 云服务	默认	提升	严格
Remote Portal	禁用	启用	启用

服务 - 日志	默认	提升	严格
软件密封	禁用	启用	启用

4.4.3 功能描述和强化建议

HTTP

HTTP在默认情况下启用，但未加密，因此如果使用凭证或设置，将在未加密的情况下传输。

建议：应禁用普通HTTP，优先使用加密HTTPS，尤其是在网络不受信任的情况下。

HTTPS
HTTPS已加密，应是访问Web界面或访问基于Web的RCP API时的默认选择。建议使用自己的PKI和证书。
建议：HTTPS是用于配置的默认安全协议，应保持启用。

RTSP
RTSP用于视频流，但通常未加密。如果接收视频流的软件可以使用RTSPS，建议禁用普通RTSP。使用其他博世组件（例如解码器/BVMS/VRM/DIVAR IP）时，可以为RTSP启用博世专有加密以保证安全传输。
建议：如果可以在不加密的情况下或通过博世加密传输视频，则采用基于风险的方法。如果可能，使用加密的RTSPS。

RCP
博世专有Remote Control Protocol Plus是博世IP摄像机的配置协议。普通RCP未加密，因此传输设置时将不加密。所有博世工具现在都有一段时间使用RCP over HTTPS进行通信，但仍然依赖于此协议的第三方集成工具或脚本工具可能需要它。
建议：如果第三方工具或旧系统不使用RCP，则禁用它。

SNMPv1
SNMP是一种常见的网络监控协议，用于查询设备的运行状况信息或向远程接收器发送陷阱，但未加密。
建议：如果不需要进行运行状况监控或存在其他兼容性原因，则保持禁用。如果可能，使用SNMPv3。

SNMPv3
SNMPv3是SNMPv1的后续版本，也可以加密使用。
建议：如果必须实施SNMP监控，则建议使用。

iSCSI
禁用内部iSCSI服务器，该服务器用于在可通过iSCSI访问的摄像机上进行内部录制。iSCSI是一种未加密的协议。
建议：如果在摄像机上未使用，则禁用iSCSI服务器。

UPnP
使摄像机可通过UPnP协议发现。
建议：如果不需要，则禁用UPnP。

NTP服务器
在摄像机上启用NTP服务器，以便其他设备或摄像机可以同步时间。如果可能，应使用专用设备为摄像机网络提供时间，从而实现服务分离。如果没有其他设备可用，可以通过摄像机来提供时间。
建议：如果不需要，应禁用NTP服务器。

Discovery
使用博世专有机制使摄像机可被博世软件（例如Configuration Manager）发现。
建议：使用动态IP地址时，此功能应保持启用。在具有固定IP地址的环境中工作时，可以关闭此功能。

ONVIF Discovery
支持通过ONVIF Discovery协议发现摄像机设备

建议：使用动态IP地址和ONVIF兼容工具时，此功能应保持启用。在具有固定IP地址的固定环境中工作时，可以关闭此功能。

GBT/28181
GBT/28181是中国对于不同设备间互操作性的标准。
建议：如果不需要，则保持禁用。

密码重置机制
IP摄像机可能安装在非常偏僻的位置，因此如果摄像机的访问权限被锁定，则很难进行维护工作或恢复出厂设置。博世提供的功能可通过质询-响应机制（基于安全公钥/私钥机制）来重置摄像机密码。
建议：如果不需要该功能，建议禁用。

Ping响应
配置摄像机是否响应网络中的ping请求。可以帮助调试。在安全性高的网络中，可以禁用此功能来避免通过ping扫描进行设备枚举，但攻击者可以使用其他几种设备发现方式。
建议：基于风险的方法，对于安全性高的网络可以禁用。

RTSPS
RTSPS是RTSP的加密版本，用于视频流。在接收软件支持的情况下，RTSPS应该总是优先于普通RTSP。由于许多RTSP客户端不支持安全版本，因此仍然为1级安全性启用RTSP。
建议：尽可能使用RTSPS。

最低TLS版本
IP摄像机不允许使用不安全的SSLv3或更早版本的连接。TLS 1.0和1.1已被IETF弃用，并且存在已知的潜在安全问题（BEAST、FREAK）。
CPP4、CPP6、CPP7和CPP7.3摄像机支持安全的TLS 1.2，应将其设置为最低版本要求。
CPP13和CPP14摄像机不允许使用早于1.2的TLS版本。它们还支持更新的TLS 1.3规范。
建议：将最低TLS版本设置为1.2。

HSTS
HTTP Strict Transport Security (HSTS)是网站为了防止中间人攻击和协议降级攻击而设置的策略。它允许网站告诉浏览器在此连接中仅允许使用HTTPS连接，不允许使用任何未加密的HTTP连接。
建议：在摄像机上启用HSTS。

802.1x
802.1x是网络访问控制(NAC)标准。它允许设备在网络中进行验证，只向经过验证的设备授予对网络的访问权限。博世IP摄像机支持802.1x的密码或基于证书的验证，首选基于证书的验证。要使用802.1x，网络交换机必须支持此标准，并且需要使用验证服务器。
建议：在网络基础设施允许的情况下，使用802.1x进行网络验证。

Syslog
由于摄像机仅提供有限的空间用于日志消息，因此应将日志消息发送到中央位置并在那里进行分析，以检测任何攻击或错误配置。
建议：使用TCP Syslog避免因丢包而丢失消息。使用Syslog和TLS加密和验证消息。

SNMPv3模式
SNMPv3是SNMPv1的后续版本，可实现安全的验证和信息传输。

建议：使用SNMPv3时，使用SHA1作为验证协议，使用AES作为隐私协议（如果支持）。

IP过滤器

在IP过滤器中，可以定义多个IP地址（单个主机或网络子网），允许其访问摄像机。建议在此处定义访问摄像机的计算机或网络。

建议：建议使用IP过滤器来定义允许的主机或网络。

日期/时间

要在日志和视频数据上显示正确的时间戳，建议将时间同步到中央时间服务器。SNTP和TLS日期都可以用于实现此目的。SNTP的优点是时间同步更精确。TLS日期的优点是可以检查正确的证书，因而是一种安全性更高的解决方案。

建议：使用安全的时间同步方法，可以使用SNTP日期或TLS日期。

基于云的服务

博世提供自有的基于云的服务，以通过博世云(Remote Portal)管理摄像机。云服务不会自动连接到Remote Portal，默认情况下处于禁用状态。每台摄像机需要先连接到Remote Portal才可以使用。Remote Portal与摄像机之间的连接已经获得了全方位的安全保护，因此如有需要，Remote Portal在任何环境下都能使用。

建议：可以根据是否使用云解决方案来使用Remote Portal。

软件密封

IP摄像机配置完成后，不应更改设备的设置。可以启用软件密封以通知设备配置更改。

建议：如果不计划更改配置，则应启用软件密封。

4.4.4 纵深防御

纵深防御是一种分层的安全方法，它是指不依靠任何一种单一的措施来单独负责保护产品的安全，攻击者需要突破多层安全防护才能攻击产品。在每次发布产品时，都会评估是否需要增加新功能来防卫新的攻击手段或提高产品的整体安全性。

以下概述了IP摄像机的主要安全功能。

- **固件签名**
  每个固件更新文件均由博世证书加密和签名。摄像机上只能安装博世发布的更新，从而避免安装恶意固件。
- **安全启动**
  CPP13、CPP14或更新平台的摄像机具有安全启动机制。安全启动会检查整个系统的完整性，首先检查启动加载程序，然后继续检查摄像机上的固件本身。从不可更改的硬件信任根开始，启动过程的每一步都会验证下一步。这样可以防止攻击者修改设备上的启动加载程序或固件。
- **登录防火墙**
  为了防止密码暴力破解，同时允许管理员登录，并防御拒绝服务(DoS)攻击，登录防火墙会基于行为分析检查登录尝试，并动态阻止或允许基于IP地址的访问。
- **摄像机验证**
  为了标识和验证摄像机的唯一身份，在生产每台摄像机时都会创建一张博世设备证书。该证书可用于检查正在通信的设备是否为正版博世设备。此外，用户还可以在摄像机上上传或创建自定义证书，以便与PKI环境集成，防止中间人攻击。

4.5 强化存储

由于Bosch IP摄像机或编码器能够直接与iSCSI驱动器建立iSCSI会话并将视频数据写入iSCSI驱动器，因此必须将iSCSI单元连接到与Bosch外围设备相同的LAN或WAN。

为避免未经授权访问录制的视频数据，必须保护iSCSI装置避免未经授权的访问：

- 使用CHAP密码验证以确保仅允许已知设备访问iSCSI目标。在iSCSI目标上设置CHAP密码，然后在VRM配置中输入已配置的密码。CHAP密码对VRM有效，并且将自动发送至所有设备。如果在BVMS VRM环境中使用CHAP密码，则必须将所有存储系统配置为使用相同的密码。
- 从iSCSI目标中删除所有默认用户名和密码。
- 对iSCSI目标的管理用户帐户使用强密码。
- 禁用管理员通过Telnet访问iSCSI目标的访问权限。改用SSH访问。
- 通过强密码保护控制台对iSCSI目标的访问。
- 禁用未使用的网络接口卡。
- 通过第三方工具监视iSCSI存储的系统状态以识别异常。

4.5.1 在iSCSI设备上设置CHAP密码

在BVMS Configuration Client中设置全局CHAP密码时，该密码会自动传输到所有编码器、解码器和VSG设备。

某些iSCSI设备不支持此功能。您必须在这些设备上手动设置CHAP密码。

注意!

在将它们添加到BVMS之前，您必须在iSCSI设备上设置全局CHAP密码。

如果iSCSI设备已激活全局CHAP密码，则不能将其添加到BVMS配置中。

要在基于最新版本的Microsoft Windows Server操作系统的iSCSI设备（例如DIVAR IP）上手动设置CHAP密码，请执行以下操作:

1. 打开**Server Manager**并导航到**File and Storage Services > iSCSI**。
2. 在**ISCSI TARGETS**列表中，右击所需的iSCSI目标并单击**Properties**。
   此时将显示**Properties**对话框。
3. 在**Properties**对话框中，单击**Security**，然后选中复选框**Enable CHAP**。
4. 输入以下内容:
   - **用户名:** 用户
   - **密码:** 输入BVMS Configuration Client中给出的全局CHAP密码（位于菜单**Hardware > Protect iSCSI storages with CHAP password...**下）。
5. 单击**OK**。
   CHAP密码便已分配给iSCSI目标。

4.6 强化服务器

4.6.1 服务器硬件推荐设置

- 服务器的BIOS提供了设置较低级别密码的功能。
  这些密码可以限制人们启动计算机、从可移动设备启动，以及未经许可更改BIOS或UEFI（统一可扩展固件接口）设置。
- 为了防止向服务器传输数据，应禁用USB端口和CD/DVD驱动器。
  此外，还应禁用未使用的NIC端口，并应禁用或通过密码保护HP ILO (HP Integrated Lights-Out)接口或控制台端口等管理端口。

4.6.2 Windows操作系统推荐安全设置

服务器应该是Windows域的一部分。

将服务器集成到Windows域之后，用户权限应分配给由中央服务器管理的网络用户。由于这些用户帐户通常会实施密码强度和到期规则，因此这种集成可以提高不具有此类限制的本地帐户的安全性。

4.6.3 Windows更新

应安装Windows软件补丁和更新并保持最新。Windows更新通常包括针对新发现的安全漏洞提供的补丁，例如影响了全球数百万台计算机的Heartbleed SSL漏洞。应安装针对这些重大问题提供的补丁。

4.6.4 安装防病毒软件

安装防病毒和防间谍软件，并保持最新。

4.6.5 Windows操作系统推荐设置

以下本地组策略设置是在Windows服务器操作系统中推荐使用的组设置。要更改默认的本地计算机策略(LCP)，请使用本地组策略编辑器。
您可以使用命令行或使用Microsoft管理控制台(MMC)打开本地组策略编辑器。

从命令行打开本地组策略编辑器:

- 单击**开始**，在**开始**搜索框中键入**gpedit.msc**，然后按Enter键。

以MMC管理单元的形式打开本地组策略编辑器:

1. 单击**开始**，在**开始**搜索框中键入**mmc**，然后按Enter键。
2. 在**添加或删除管理单元**对话框中，单击**组策略对象编辑器**，然后单击**添加**。
3. 在**选择组策略对象**对话框中，单击**浏览**。
4. 单击**此电脑**编辑本地组策略对象，或单击**用户**编辑管理员、非管理员或每用户本地组策略对象。
5. 单击**完成**。

4.6.6 激活服务器上的用户帐户控制

Local Computer Policies -> Computer Configuration -> Windows Settings -> Security Settings -> Local Policies -> Security Options

用户帐户控制：用于内置管理员帐户的管理员批准模式	启用
用户帐户控制：允许UIAccess应用程序在不使用安全桌面的情况下提示提升权限	禁用
用户帐户控制：管理员批准模式中管理员的提升权限提示行为	许可提示
用户帐户控制：标准用户的提升权限提示行为	在安全桌面上输入凭证的提示
用户帐户控制：检测应用程序安装并提示提升权限	启用
用户帐户控制：只提升签名并验证的可执行文件	禁用
用户帐户控制：以管理员批准模式运行所有管理员	启用
用户帐户控制：提示提升权限时切换到安全桌面	启用
用户帐户控制：将文件和注册表写入失败虚拟化到各个用户位置	启用

Local Computer Policies -> Computer Configuration -> Administrative Templates -> Windows Components -> Credential User Interface

提升权限时枚举管理员帐户	禁用

4.6.7 停用自动播放

Local Computer Policies -> Computer Configuration -> Administrative Templates -> Windows Components -> AutoPlay Policies

关闭自动播放	启用所有驱动器
自动运行的默认行为	启用，不执行任何自动运行命令

关闭非卷设备的自动播放	启用

4.6.8 外部设备

Local Computer Policies -> Computer Configuration -> Windows Settings -> Security Settings -> Local Policies -> Security Options

设备：无需登录即可断开坞接	禁用
设备：允许格式化和弹出可移除介质	管理员
设备：阻止用户安装打印机驱动程序	启用
设备：仅限本地登录用户访问CD-ROM	启用
设备：仅限本地登录用户访问软盘	启用

4.6.9 配置用户权限分配

Local Computer Policies -> Computer Configuration -> Windows Settings -> Security Settings -> Local Policies -> User Rights Assignment

将Access Credential Manager作为受信任的调用者	没有人
从网络访问此计算机	验证用户
作为操作系统的一部分	没有人
将工作站添加到域	没有人
允许通过远程桌面服务登录	管理员，远程桌面用户
更改系统时间	管理员
更改时区	管理员，本地服务
创建页面文件	管理员
创建令牌对象	没有人
创建永久共享对象	没有人
拒绝从网络访问此计算机	匿名登录，访客组
拒绝批量登录	匿名登录，访客组
拒绝服务登录	没有人
拒绝本地登录	匿名登录，访客组
拒绝通过远程桌面服务登录	匿名登录，访客
允许信任计算机和用户帐户以进行委派	没有人
从远程系统强制关闭	管理员
生成安全审计	本地服务，网络服务
提高调度优先级	管理员
加载和卸载设备驱动程序	管理员
修改对象标签	没有人
修改固件环境值	管理员

执行卷维护任务	管理员
配置文件单进程	管理员
从坞站移除计算机	管理员
恢复文件和目录	管理员
关闭系统	管理员
同步目录服务数据	没有人
获取文件或其他对象的所有权	管理员

4.6.10 屏幕保护程序

– 激活受密码保护的屏保程序并定义超时时间:
Local Computer Policies -> User Configuration -> Administrative Templates -> Control Panel -> Personalization

启用屏保程序	启用
密码保护屏保程序	启用
屏保程序超时	1800秒

4.6.11 激活密码策略设置

– 启用密码策略设置可确保用户密码满足最低密码要求

Local Computer Policies -> Windows Settings -> Security Settings -> Account Policies -> Password Policy

强制执行密码历史记录	记住10个密码
密码最长使用期限	90 天
密码最短使用期限	1 天
最小密码长度	10个字符
密码必须满足复杂性要求	启用
使用可逆加密为域中的所有用户存储密码	禁用

4.6.12 禁用非必需的Windows服务

– 禁用非必要的Windows服务可提高安全级别并更大限度减少攻击点。

应用层网关服务	禁用
应用程序管理	禁用
计算机浏览器	禁用
分布式链接跟踪客户端	禁用
功能发现提供程序主机	禁用
功能发现资源发布	禁用
人机接口设备访问	禁用
互联网连接共享(ICS)	禁用

链路层拓扑发现映射器	禁用
多媒体类计划程序	禁用
脱机文件	禁用
远程访问自动连接管理器	禁用
远程访问连接管理器	禁用
路由和远程访问	禁用
Shell硬件检测	禁用
Special Administration Console Helper	禁用
SSDP发现	禁用

4.6.13 Windows操作系统用户帐户

必须使用复杂的密码保护Windows操作系统用户帐户。
通常通过Windows管理员帐户管理和维护服务器，应确保使用强密码来保护管理员帐户。

密码必须包含以下三个类别的字符:

- 欧洲语言的大写字母（A到Z，带变音符号，希腊语和西里尔字符）
- 欧洲语言的小写字母（a到z，sharp-s，带变音符号，希腊语和西里尔字符）
- 10个基本数字（0到9）
- 非字母数字字符：~!@#$%^&*_-+=`|\(){}[]:;"'<>,.?/
- 任何被归类为字母字符，但不属于大写或小写的Unicode字符。这包括来自亚洲语言的Unicode字符。

使用Windows帐户锁定，使密码猜测攻击更难成功。
Windows 8.1安全基线建议是10/15/15:

- 10次失败的尝试
- 15分钟锁定时间
- 15分钟后计数器重置

Local Computer Policies -> Computer Configuration -> Windows Settings -> Security Settings -> Account Policies -> Account Lockout Policy

帐户锁定持续时间	帐户锁定持续时间
15分钟帐户锁定阈值10次登录尝试失败	15分钟帐户锁定阈值10次登录尝试失败
之后重置帐户锁定计数器	之后重置帐户锁定计数器

- 确保使用新的强密码替换服务器和Windows操作系统的所有默认密码。

4.6.14 在服务器上启用防火墙

▶ 根据BVMS端口，启用BVMS标准端口的通信。

注意!
关于相关端口的设置和使用，请参阅BVMS文档。请务必仔细检查有关固件或软件升级的设置。

4.7 强化Windows客户端

4.7.1 Windows工作站

用于BVMS客户端应用程序（例如BVMS Operator Client或Configuration Client）的Windows桌面操作系统安装在安全区域之外。工作站必须强化以保护视频数据、文档以及其他应用程序免受未经授权的访问。
应当应用或检查以下设置。

4.7.2 Windows工作站硬件推荐设置

- 设置BIOS/UEFI密码，以限制人们启动替代操作系统。
- 为了防止向客户端传输数据，应禁用USB端口和CD/DVD驱动器。此外，还应禁用未使用的NIC端口。

4.7.3 Windows操作系统推荐安全设置

- 工作站应该是Windows域的一部分。
  将工作站集成到Windows域中，可以集中管理安防相关设置。
- Windows更新
  始终安装最新的Windows操作软件修补程序和更新。
- 安装防病毒软件
  安装防病毒和防间谍软件，并保持最新。

4.7.4 Windows操作系统推荐设置

以下本地组策略设置是在Windows服务器操作系统中推荐使用的组设置。要更改默认的本地计算机策略(LCP)，请使用本地组策略编辑器。
您可以使用命令行或使用Microsoft管理控制台(MMC)打开本地组策略编辑器。

从命令行打开本地组策略编辑器:

- 单击**开始**，在**开始**搜索框中键入**gpedit.msc**，然后按Enter键。

以MMC管理单元的形式打开本地组策略编辑器:

1. 单击**开始**，在**开始**搜索框中键入**mmc**，然后按Enter键。
2. 在**添加或删除管理单元**对话框中，单击**组策略对象编辑器**，然后单击**添加**。
3. 在**选择组策略对象**对话框中，单击**浏览**。
4. 单击**此电脑**编辑本地组策略对象，或单击**用户**编辑管理员、非管理员或每用户本地组策略对象。
5. 单击**完成**。

4.7.5 激活服务器上的用户帐户控制

Local Computer Policies -> Computer Configuration -> Windows Settings -> Security Settings -> Local Policies -> Security Options

用户帐户控制：用于内置管理员帐户的管理员批准模式	启用
用户帐户控制：允许UIAccess应用程序在不使用安全桌面的情况下提示提升权限	禁用
用户帐户控制：管理员批准模式中管理员的提升权限提示行为	许可提示
用户帐户控制：标准用户的提升权限提示行为	在安全桌面上输入凭证的提示
用户帐户控制：检测应用程序安装并提示提升权限	启用
用户帐户控制：只提升签名并验证的可执行文件	禁用

用户帐户控制：以管理员批准模式运行所有管理员	启用
用户帐户控制：提示提升权限时切换到安全桌面	启用
用户帐户控制：将文件和注册表写入失败虚拟化到各个用户位置	启用

Local Computer Policies -> Computer Configuration -> Administrative Templates -> Windows Components -> Credential User Interface

提升权限时枚举管理员帐户	禁用

4.7.6 停用自动播放

Local Computer Policies -> Computer Configuration -> Administrative Templates -> Windows Components -> AutoPlay Policies

关闭自动播放	启用所有驱动器
自动运行的默认行为	启用，不执行任何自动运行命令
关闭非卷设备的自动播放	启用

4.7.7 外部设备

Local Computer Policies -> Computer Configuration -> Windows Settings -> Security Settings -> Local Policies -> Security Options

设备：无需登录即可断开坞接	禁用
设备：允许格式化和弹出可移除介质	管理员
设备：阻止用户安装打印机驱动程序	启用
设备：仅限本地登录用户访问CD-ROM	启用
设备：仅限本地登录用户访问软盘	启用

4.7.8 配置用户权限分配

Local Computer Policies -> Computer Configuration -> Windows Settings -> Security Settings -> Local Policies -> User Rights Assignment

将Access Credential Manager作为受信任的调用者	没有人
从网络访问此计算机	验证用户
作为操作系统的一部分	没有人
将工作站添加到域	没有人
允许通过远程桌面服务登录	管理员，远程桌面用户
更改系统时间	管理员
更改时区	管理员，本地服务
创建页面文件	管理员
创建令牌对象	没有人
创建永久共享对象	没有人

拒绝从网络访问此计算机	匿名登录，访客组
拒绝批量登录	匿名登录，访客组
拒绝服务登录	没有人
拒绝本地登录	匿名登录，访客组
拒绝通过远程桌面服务登录	匿名登录，访客
允许信任计算机和用户帐户以进行委派	没有人
从远程系统强制关闭	管理员
生成安全审计	本地服务，网络服务
提高调度优先级	管理员
加载和卸载设备驱动程序	管理员
修改对象标签	没有人
修改固件环境值	管理员
执行卷维护任务	管理员
配置文件单进程	管理员
从坞站移除计算机	管理员
恢复文件和目录	管理员
关闭系统	管理员
同步目录服务数据	没有人
获取文件或其他对象的所有权	管理员

4.7.9 屏幕保护程序

– 激活受密码保护的屏保程序并定义超时时间:
Local Computer Policies -> User Configuration -> Administrative Templates -> Control Panel -> Personalization

启用屏保程序	启用
密码保护屏保程序	启用
屏保程序超时	1800秒

4.7.10 激活密码策略设置

– 启用密码策略设置可确保用户密码满足最低密码要求

Local Computer Policies -> Windows Settings -> Security Settings -> Account Policies -> Password Policy

强制执行密码历史记录	记住10个密码
密码最长使用期限	90 天
密码最短使用期限	1 天
最小密码长度	10个字符
密码必须满足复杂性要求	启用

使用可逆加密为域中的所有用户存储密码	禁用

4.7.11 禁用非必需的Windows服务

– 禁用非必要的Windows服务可提高安全级别并更大限度减少攻击点。

应用层网关服务	禁用
应用程序管理	禁用
计算机浏览器	禁用
分布式链接跟踪客户端	禁用
功能发现提供程序主机	禁用
功能发现资源发布	禁用
人机接口设备访问	禁用
互联网连接共享(ICS)	禁用
链路层拓扑发现映射器	禁用
多媒体类计划程序	禁用
脱机文件	禁用
远程访问自动连接管理器	禁用
远程访问连接管理器	禁用
路由和远程访问	禁用
Shell硬件检测	禁用
Special Administration Console Helper	禁用
SSDP发现	禁用

4.7.12 Windows操作系统用户帐户

必须使用复杂的密码保护Windows操作系统用户帐户。
通常通过Windows管理员帐户管理和维护服务器，应确保使用强密码来保护管理员帐户。

密码必须包含以下三个类别的字符：
– 欧洲语言的大写字母（A到Z，带变音符号，希腊语和西里尔字符）
– 欧洲语言的小写字母（a到z，sharp-s，带变音符号，希腊语和西里尔字符）
– 10个基本数字（0到9）
– 非字母数字字符：~!@#$%^&*_-+=`|\(){}[]:;"'<>,.?/
– 任何被归类为字母字符，但不属于大写或小写的Unicode字符。这包括来自亚洲语言的Unicode字符。

使用Windows帐户锁定，使密码猜测攻击更难成功。
Windows 8.1安全基线建议是10/15/15：
– 10次失败的尝试
– 15分钟锁定时间
– 15分钟后计数器重置

Local Computer Policies -> Computer Configuration -> Windows Settings -> Security Settings -> Account Policies -> Account Lockout Policy

帐户锁定持续时间	帐户锁定持续时间
15分钟帐户锁定阈值10次登录尝试失败	15分钟帐户锁定阈值10次登录尝试失败
之后重置帐户锁定计数器	之后重置帐户锁定计数器

– 确保使用新的强密码替换服务器和Windows操作系统的所有默认密码。
– 禁用未使用的Windows操作系统帐户。
– 禁用对客户端工作站的远程桌面访问。
– 以非管理员权限运行工作站，以避免标准用户更改系统设置。

4.7.13 在工作站上启用防火墙

▸ 根据BVMS端口，启用BVMS标准端口的通信。

注意!
关于相关端口的设置和使用，请参阅BVMS文档。请务必仔细检查有关固件或软件升级的设置。

4.8 保护网络访问

目前，许多中小型IP视频监控系统只是以“另一个IT应用”的形式部署在客户的现有网络基础结构上。尽管这种部署方式具有成本和维护方面的优势，但也会使安防系统面临不必要的威胁，包括内部威胁。需要采取适当的措施，并避免将事件视频泄露到互联网或社交媒体上等类的情况。此类事件不仅可能侵犯隐私，还可能对公司造成损害。

有两种主要的技术可用于创建网络中的网络。IT基础结构架构师将选择哪种技术主要取决于现有网络基础结构、所部署的网络设备，以及所要求的功能和网络拓扑。

4.8.1 VLAN：虚拟LAN

虚拟LAN是通过将LAN细分为多个网段而创建的。网络分段是通过网络交换机或路由器配置完成的。VLAN的优点是无需重新布设设备网络连接即可满足资源需求。
应用于视频监控等特定领域的服务质量方案可能不仅有助于提高安全性，还有助于提高性能。

VLAN在数据链路层（OSI第2层）上实现，类似于在网络层（OSI第3层）发生的IP子网划分（请参阅 *分配IP地址, 页面 8*）。

4.8.2 VPN：虚拟专用网络

虚拟专用网络是一个分离的（专用）网络，通常跨越公共网络或互联网。有各种协议可用于创建VPN，通常是承载受保护流量的数据通道。虚拟专用网络可能设计为点对点数据通道、任意到任意连接或多点连接。VPN可以部署加密通信，或者仅依赖VPN本身的安全通信。

VPN可用于通过广域网(WAN)连接来连接远程站点，同时还可以保护隐私并提高局域网(LAN)的安全性。由于VPN充当一个单独的网络，因此添加到VPN的所有设备都将如同在一个典型网络上一样无缝工作。VPN不仅为监控系统增加了额外的保护层，而且还额外带来了划分生产网络业务流量和视频流量的好处。

注意!
如果适用，VLAN或VPN可提高合并到现有IT基础设施中的监控系统的安全级别。

除了保护监控系统免于共享IT基础结构上未经授权的访问之外，还需要考虑谁可以连接到网络。

4.8.3 禁用未使用的交换机端口

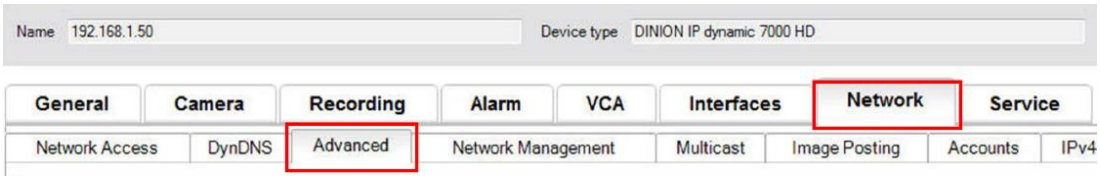
禁用未使用的网络端口可确保未经授权的设备无法访问网络。这可以降低此类风险：有人试图通过将其设备插入交换机或未使用的网络套接字来访问安全子网。禁用特定端口的选项是一种常见选项，在低成本和企业级托管交换机中均提供。

4.8.4 802.1x保护的网络

所有Bosch IP视频设备都可以配置为802.1x客户端。这样一来，它们可以通过验证连接到RADIUS服务器并加入安全网络。在将视频设备加入到安全网络之前，您需要从技术人员的笔记本电脑直接连接到视频设备，以输入有效凭证，详细步骤如下。

802.1x服务可通过Configuration Manager轻松配置。

1. 在Configuration Manager中，选择所需的设备。
2. 选择**网络**选项卡，然后选择**高级**。



3. 找到页面的**802.1x**部分。
4. 在**802.1x**下拉菜单中，选择**开启**。
5. 输入有效的**标识**和**密码**。
6. 保存更改。
7. 断开设备，并将设备放置到安全网络上。

注意！

802.1x本身并不提供请求方与身份验证服务器之间的安全通信。

因此，用户名和密码可能会遭到来自网络的“嗅探”。802.1x可使用EAP-TLS来确保安全通信。

可扩展身份验证协议 - 传输层安全

可扩展身份验证协议(EAP)支持多种身份验证方法。传输层安全(TLS)提供相互验证、完整性获得保护的密码套件协商以及两个端点之间的密钥交换。EAP-TLS包括支持基于证书的相互验证和密钥派生。也就是说，EAP-TLS囊括了服务器端和客户端互相发送证书的过程。

注意！

请参阅特定的技术白皮书*网络验证 - 802.1x - 保护网络边缘*，其位于Bosch Security Systems在线产品目录的如下位置：

http://resource.boschsecurity.com/documents/WP_802.1x_Special_enUS_22335867275.pdf。

5 安全操作

5.1 网络分离

如果可能，设备应在具有访问限制的单独网络（例如使用VLAN）中运行，以限制广播流量并保护设备免受网络攻击。

5.2 硬件保管库中的安全密钥存储

当来自证书的私钥安全地存储在硬件组件或硬件保管库中时，能够得到更安全的保护。即使设备机身被强行打开以获得访问权限，此类芯片也可以防止未经授权访问私钥。
在博世摄像机中，此类密钥存储在单独的加密协处理器或安全元件(SE)中。两者都提供安全存储和加密功能，绝不会将私钥暴露在可能被检索到的位置或内存中。
在工作站和服务器上，通常提供可信平台模块(TPM)芯片。加密库和函数应配置为尽可能使用TPM存储。

5.3 唯一设备证书

尽管每台支持TLS或HTTPS的设备一般都能使用自签名默认证书，但不应认为仅使用此证书进行验证就足够了，因为它不能防止中间人(MITM)攻击。

如果设备所部署的环境需要采取额外步骤来对每一台IP视频设备进行身份验证，则可以创建新证书和私钥并将其加载到视频设备本身。您可以从证书颁发机构(CA)获得新证书，也可以使用OpenSSL工具包创建新证书。

如果在公共网络中使用设备，建议从公共证书颁发机构获取证书，或者拥有由此类机构签署的自己的证书，这也能够验证设备证书的来源和有效性，即可信度。

多年来，所有Bosch摄像机都预装了唯一的设备证书和私钥，此类设备证书和私钥从Bosch根证书派生并安装在安全的生产环境中，证明摄像机是“原始制造的”Bosch设备。该证书自动用于HTTPS连接，也可用于识别和验证设备，方法为对一直到Bosch根证书的证书链进行验证。

注意!
证书应用于验证单台设备。建议为每台设备创建一个从根证书派生的特定证书。

更安全的证书部署方法是在设备上生成证书签名请求(CSR)，并从内部或外部证书颁发机构请求获得证书。
对于证书签名请求，设备在内部保存私钥，只公开证书的其余部分以供证书颁发机构签名。私钥安全地存储在摄像机的安全元件(SE)中或设备的可信平台模块(TPM)等位置。
因此，每当设备允许使用CSR时，都应优先采用该方式创建证书。

可以使用视频设备的设备网页或使用Configuration Manager将证书上传到设备。

通过设备网页上传证书
可以使用视频设备的设备网页上传证书。
在设备网页的**证书**页面，可以添加新证书和删除证书并指定证书的用法。

使用Configuration Manager上传证书
在Configuration Manager中，可以轻松地将证书上传到单台设备或同时上传到多台设备。
上传证书的具体步骤如下：
1. 在Configuration Manager中，选择一台或多台设备。

2. 右击，然后依次单击**文件上载**和**SSL 证书...**。
   Windows Explorer窗口将打开，找到要上传的证书。

对于较小的系统，Configuration Manager提供一个名为**MicroCA**的支持功能，它允许创建或使用根CA并从中派生设备证书，或者用于签署设备的证书签名请求，也可以同时用于多台设备。有关详情，请参阅Configuration Manager用户手册。

参阅

– *使用证书建立信任, 页面 40*

5.4 检查日志文件

监控日志文件是安全分析或维护活动的重要组成部分。定期查看日志文件可以发现配置问题或安全违规，例如错误登录。
要分析日志文件并长期保存，建议将设备的日志文件发送到系统日志服务器或SIEM系统，例如，摄像机将保留固定空间用于内部日志记录，但如果该空间已满，它将覆盖旧日志。

5.5 SIEM系统

安全信息和事件管理(SIEM)系统用于收集和分析来自不同设备和系统的信息。这些设备可以与SIEM系统集成，具体方式是通过syslog协议发送日志。分析这些日志有助于进行维护并发现配置错误或对设备的攻击（例如错误登录）。

5.6 PKI

公钥基础设施(PKI)是指生成和管理数字证书所需的系统。对于HTTPS、802.1x网络验证、使用证书进行用户验证以及其他加密功能，可以在设备上安装自定义证书。

5.7 AD FS

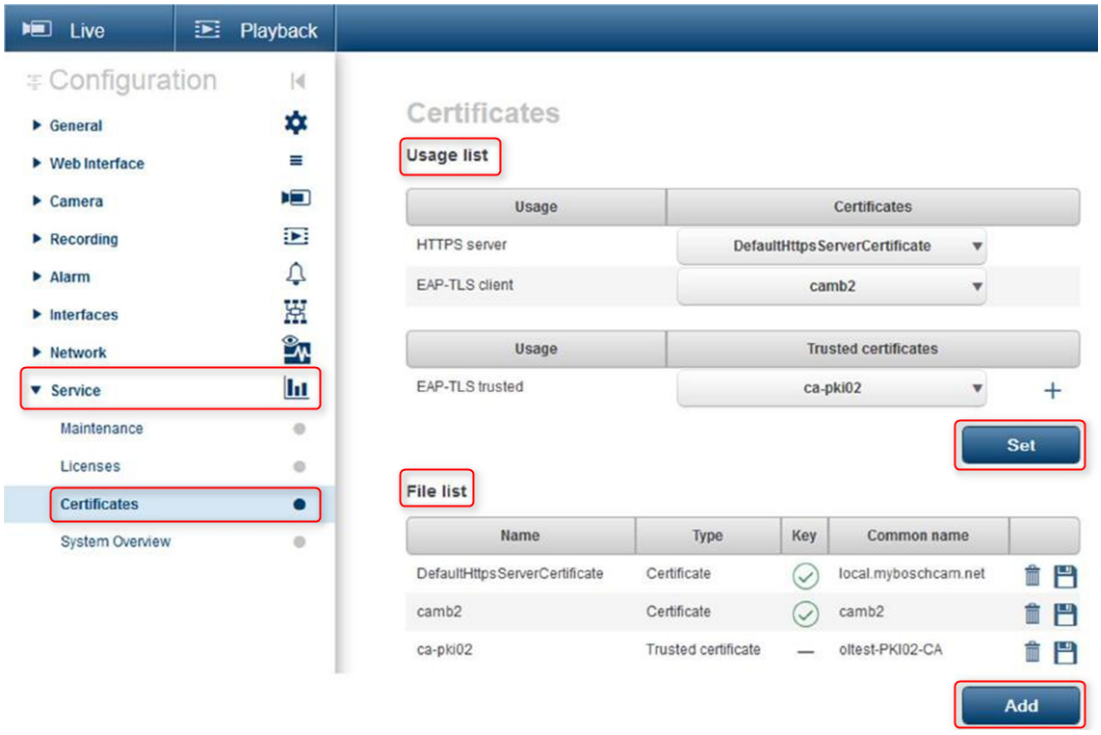
Active Directory Federation Services (AD FS)是Microsoft提供的一项服务，允许进行本地Active Directory（使用AD FS服务器）或Azure Cloud验证。除了使用密码或基于证书的验证进行本地用户验证外，还可以使用AD FS将设备集成到Active Directory域中，以集中进行验证和管理用户访问。

5.8 IP摄像机的安全运行

5.8.1 使用证书建立信任

所有运行固件6.10或更高版本的Bosch IP摄像机均使用证书存储区，可在摄像机配置的**服务**菜单下找到。
可将特定的服务器证书、客户端证书和可信证书添加到存储区。
将证书添加到存储区：

1. 在设备网页上，导航到**配置**页面。
2. 选择**服务**菜单，然后选择**证书**子菜单。
3. 在**文件列表**部分，单击**添加**。
4. 上载所需的证书。
   上载完成后，证书将出现在**使用列表**部分。
5. 在**使用列表**部分，选择所需的证书。
6. 要激活证书的使用，必须重新启动摄像机。要重新启动摄像机，请单击**设置**。



图片 5.1: 示例：存储在Bosch摄像机（固件6.11）中的EAP/TLS证书

证书可以采用*.pem、*.cer或*.crt格式，并且必须采用base64编码。它们可以作为一个合并文件上传，也可以拆分为证书和密钥这两部分，并按此顺序作为单独的文件上传，然后自动重新合并。

从固件版本6.20开始，系统支持受密码保护的PKCS#8私钥（AES加密），并且必须以base64编码的*.pem格式上传。

5.8.2 视频验证

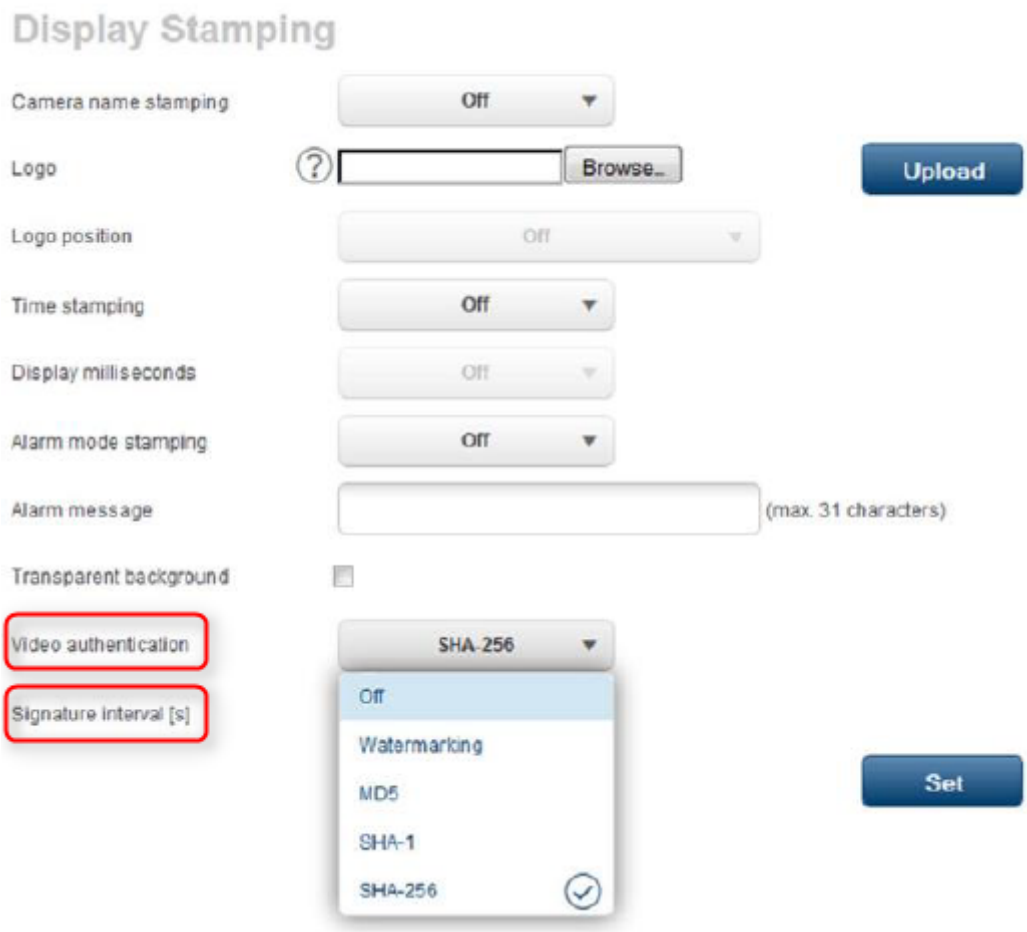
一旦系统中的设备获得保护并正确完成验证，就值得同时关注从它们传输的视频数据。这种方法称为视频验证。

视频验证仅涉及验证视频真实性的方法。在任何情况下，视频验证都不涉及视频或数据的传输。

在固件5.90发布之前，水印是通过视频流上的简单校验和算法进行的。处理基本水印时，不会使用证书或加密。校验和是对文件“数据稳定性”的基线测量，可以验证文件的完整性。

配置视频验证（例如在网页浏览器中）：

1. 导航到**常规**菜单，然后选择**显示标记**。
2. 在**视频验证**下拉菜单中，选择所需的选项：
   除了标准的添加水印之外，固件版本5.9及更高版本在视频验证中还提供了三个选项：
   - MD5：用于生成128位哈希值的消息摘要。
   - SHA-1：由美国国家安全局设计，也是由美国NIST发布的美国联邦信息处理标准。SHA-1可生成160位哈希值。
   - SHA-256：SHA-256算法可生成几乎唯一、固定大小的256位（32字节）哈希。



注意!
哈希是一种单向函数 - 不能反过来对其进行解密。

使用视频验证时，视频流中的每个数据包都经过哈希处理。这些哈希嵌入在视频流中，且本身与视频数据一起经过哈希处理。这可以确保流内容的完整性。

哈希按照由签名间隔定义的一定期间，使用设备TPM内存储证书的私钥进行签名。在iSCSI录像中的报警录像和块变化均以签名结尾，以确保连续的视频真实性。

注意!
计算数字签名需要计算能力，如果计算过于频繁，可能会影响摄像机的整体性能。因此，应选择合理的间隔。

由于哈希和数字签名嵌入在视频流中，因此也将存储在录像中，从而在播放和导出时也能进行视频验证。

6 安全更新管理

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。

您可以在博世智能建筑科技下载商店中找到最新的固件和软件版本：
https://downloadstore.boschsecurity.com/
对于连接到Remote Portal的设备，用户可以通过远程警报服务接收有关可用固件更新的电子邮件通知。
更全面的下载包通过博世智能建筑科技产品目录分发：
https://www.boschsecurity.com

7 安全监控

由于要求不断变化，因此无法100%保证安全。为此，博世确立了结构明晰的漏洞和事件管理流程，以专业地管理潜在的产品安全漏洞和事件。

对于我们而言，专业、系统地处理报告的安全漏洞并确保对我们的客户透明非常重要。所以我们会调查所有漏洞报告。我们根据通用漏洞评分系统(CVSS)评估产品安全漏洞。CVSS是一项免费、开放的行业标准，用于评估计算机系统安全漏洞的严重程度。分数是根据公式计算得出的，该公式取决于多个指标，这些指标能够大致衡量漏洞攻击的难易程度和影响。分数范围为0到10分，其中10表示严重程度最高。

如果确认存在漏洞，我们会发布安全通告，告知客户产品或解决方案中已识别的安全漏洞及其补救措施。所有安全通告均包含以下内容:

- 使用常见漏洞和暴露(CVE)参考及CVSS分数对漏洞进行描述。
- 指明已知受影响的产品和软件/硬件版本。
- 有关预防办法和备用预案的信息。
- 可用修复或其他补救措施的时间安排和位置。

您可以在我们的网站上找到已发布的安全通告的列表：https://www.boschsecurity.com/xc/en/support/product-security/security-advisories.html。
一旦您认为自己发现了与博世产品或服务相关的漏洞或任何其他安全问题，请联系博世产品安全事件响应团队(PSIRT)：https://psirt.bosch.com。

8 安全处置和停用

在产品或系统生命周期的特定时间点，可能需要更换或停用设备或组件。由于设备或组件可能包含敏感数据，如凭证或证书，因此请确保安全地彻底删除这些数据。

您可以将大多数设备设置为出厂默认设置。
对于大多数IP摄像机和编码器，您可以使用重置按钮执行此操作。如果没有重置按钮，请通过Web界面使用出厂默认功能，然后从网络上卸载设备。
所有用户及其各自的密码都将被删除，设置将恢复为出厂默认设置。存储在TPM或安全元件中的所有证书及相应的密钥也将被删除。

其他设备可能有不同的选项用于将设备设置为出厂默认设置。有关正确的处置程序，请参阅相应用户文档中的说明。
服务器和工作站也可能存储了证书和凭证。使用适当的工具和方法确保在停用设备期间或处置设备之前安全地删除您的相关数据。

建议将设备设置为出厂默认设置，以防设备必须转移到可能使用其他凭证或证书的其他系统中。

注意!
有关正确的处置程序，请参阅相应用户文档中的说明。

9 其它信息

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

词汇

802.1x

IEEE 802.1x 标准可以为 IEEE 802 网络提供常规的验证和授权方法。验证通过验证程序来执行，此程序将使用验证服务器来检查传输的验证信息（参见 RADIUS 服务器），然后相应地批准或拒绝用户访问提供的服务（LAN、VLAN 或 WLAN）。

DHCP

Dynamic Host Configuration Protocol（动态主机配置协议）的缩写：使用适当的服务器来为网络中的计算机动态分配 IP 地址和其它网络参数。

HTTP

Hypertext Transfer Protocol（超文本传输协议）的缩写：用于通过网络传输数据的协议

HTTPS

Hypertext Transfer Protocol Secure（安全超文本传输协议）的缩写：用于对 Web 服务器与浏览器之间的通信进行加密和验证。

IPv4地址

唯一定义互联网中每个装置的 4 字节数字。通常用小数点记号加以分隔，例如“209.130.2.193”。

Net mask（网络掩码）

一种掩码，用于解释 IP 地址的哪一部分是网络地址，哪一部分是主机地址。通常用小数点记号加以分隔，例如“255.255.255.192”。

ONVIF

开放式网络视频接口论坛。网络视频产品的全球标准。符合ONVIF标准的设备之间可以交换实况视频、音频、元数据和控制信息，并确保它们会被自动识别并连接至视频管理系统等网络应用。

RADIUS 服务器

Remote Authentication Dial-In User Service（远程验证拨号用户服务）的缩写：这是一种客户端/服务器协议，用于在计算机网络中为拨号连接用户提供验证、授权和帐号设置服务 。 RADIUS 是拨号连接中央认证的非官方标准，拨号连接途径有 Modem（调制解调器）、 ISDN、VPN、无线 LAN（参见 802.1x）和 DSL。

RCP+

远程控制协议：博世专有协议，使用特定静态端口检测博世IP视频设备并与之通信

RTSP

Real Time Streaming Protocol（实时数据流协议）的缩写。 这种网络协议可以控制音频和视频数据或软件在 IP 网络上的连续传输。

SNMP

Simple Network Management Protocol（简单网络管理协议）的缩写；一种网络管理协议，用于管理和监视网络组件

SSL

Secure Sockets Layer（安全套接字层），是在IP网络中传输数据的一种过时的加密协议（参见TLS）。

TCP

传输控制协议。 以连接为导向的通信协议，用于通过 IP 网络传输数据。 提供可靠和有序的数据传输。

Telnet

一种登录协议，通过它，用户可以访问互联网上的远程计算机（主机）

TLS

传输层安全。TLS 1.0和1.1是SSL 3.0的标准高级开发（参见SSL）。现代设备使用TLS 1.2或1.3

TTL

Time-To-Live（生存时间）的缩写；数据包在站传输器中的生命周期

UDP

用户数据报文协议。无连接协议，用于通过IP网络交换数据。传输视频时，由于UDP的开销较低，因此它比TCP更为高效。

VPN

虚拟专用网络(VPN)在公共网络（例如互联网）中实现专用网络。VPN中的网络流量经过加密，可以防止间谍活动。

Wide Area Network（广域网）

用于扩展或连接远程局域网的长距离链路

局域网

Local Area Network（局域网）的缩写。此网络连接的设备位于有界限的地理区域内。

强化

该过程通过以下手段来提高系统安全性：仅使用系统运行所必需的专用软件，应用特定保护设置以及删除非必需软件。

设备

摄像机、编码器/解码器、NVR、DiBos、模拟矩阵、ATM/POS桥接器等硬件组件。

身份验证

验证视频流真伪的过程。用户可以启用验证过程。如果发现不可信的数据，则会显示一条信息。

用户组

用户组用于定义常规用户属性，如权限、特权和 PTZ 控制优先级等。 成为某个组的一员后，用户会自动继承该组的所有属性。

组播

网络上单个收发器与多个接收器之间的通信。它将网络的单个数据流分发到已定义组中的多个接收器。 组播操作的必要条件是实施 UDP 协议和 IGMP 协议且与组播兼容的网络。

Bosch Sicherheitssysteme GmbH
Robert-Bosch-Ring 5
85630 Grasbrunn
Germany
www.boschsecurity.com

Building solutions for a better life.

202302091957