

AXIS I8116-E Network Video Intercom

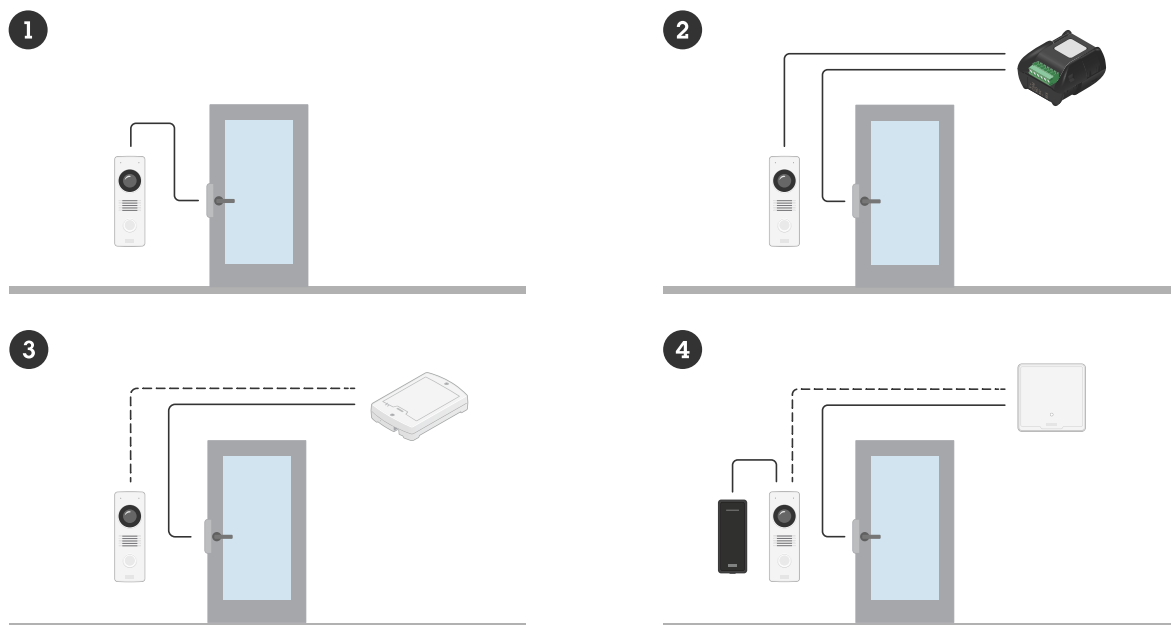
目录

设置概览	5
安装	6
预览模式	6
开始使用	7
在网络上查找设备	7
浏览器支持	7
打开设备的网页界面	7
创建管理员账户	7
安全密码	7
确保没有人篡改过设备软件	8
网页界面概览	8
配置设备	9
基本设置	9
更改root用户密码	9
设置直连 SIP (P2P)	9
通过服务器设置 SIP (PBX)	10
创建一位联系人	10
配置呼叫按钮	11
使用 DTMF 为来访者开门	11
允许凭证持有者开门	11
调整图像	12
选择曝光模式	12
在低照度条件下降低噪声	12
显示文本叠加	13
设置事件规则	13
当设备检测到物体时，显示视频流中的文本叠加	13
网页界面	14
状态	14
视频	16
安装	17
图像	17
流	21
叠加	23
隐私遮罩	25
通讯	25
联系人名单	25
SIP	25
呼叫	29
VMS 呼叫	30
分析	31
AXIS Object Analytics	31
元数据可视化	31
元数据配置	31
读卡器	31
连接	31
输出格式	33
PIN	33
入口列表	33
音频	34
设备设置	34
流	35
音频剪辑	35
录像	36

应用	37
系统	37
时间和位置	37
配置检查	39
网络	39
安全	42
账户	47
事件	49
MQTT	53
存储	56
流配置文件	57
ONVIF	58
侦测器	60
附件	61
日志	62
普通配置	63
维护	64
维护	64
故障排查	65
了解更多	66
IP 语音 (VoIP)	66
会话初始化协议 (SIP)	66
点对点 SIP (P2PSIP)	66
专用分支交换机 (PBX)	67
NAT 遍历	67
叠加	68
流传输和存储	68
视频压缩格式	68
应用	68
AXIS Object Analytics	69
元数据可视化	69
网络安全	69
签名OS	69
安全启动	69
Axis Edge Vault	69
安讯士设备ID	69
签名视频	69
规格	70
产品概述	70
LED 指示灯	70
SD 卡插槽	70
按钮	71
控制按钮	71
连接器	71
网络连接器	71
I/O、读卡器连接器和继电器	71
连接设备	73
Axis 读卡器	73
由 PoE (12V) 供电的继电器	73
由独立电源供电的继电器	73
无电势继电器	73
由对讲机 PoE 供电的 12V 断电闭门锁	74
由外部电源供电的 12V 断电闭门锁	74
故障排查	75
重置为出厂默认设置	75
AXIS OS 选项	75

检查当前 AXIS OS 版本	75
升级 AXIS OS.....	75
技术问题、线索和解决方案	76
性能考虑	77
联系支持人员	77

设置概览



- 1 对讲机
- 2 与 AXIS A9801 结合的对讲机
- 3 与 AXIS A9161 结合的对讲机
- 4 与 Axis 读卡器和门禁控制器相结合的可视对讲终端

安装



要观看此视频，请转到本文档的网页版本。

此视频演示如何安装设备

预览模式

在安装期间微调摄像机视图时，预览模式对安装者来说是非常理想。无需登录即可在预览模式下访问摄像机视图。它仅在出厂默认状态下提供，可由设备供电在有限时间使用。



要观看此视频，请转到本文档的网页版本。

该视频演示如何使用预览模式。

开始使用

在网络上查找设备

若要在网络中查找安讯士设备并为它们分配 Windows® 中的 IP 地址，请使用 AXIS IP Utility 或 AXIS Device Manager。这两种应用程序都是免费的，可以从 axis.com/support 上下载。

有关如何查找和分配 IP 地址的更多信息，请转到 [如何分配一个 IP 地址和访问您的设备](#)。

浏览器支持

您可以在以下浏览器中使用该设备：

	Chrome™	Firefox®	Edge™	Safari®
Windows®	推荐	✓	推荐	
macOS®	推荐	✓	推荐	✓*
Linux®	推荐	✓	推荐	
其他操作系统	✓	✓	✓	✓

*不完全支持。如果遇到视频流问题，请使用不同的浏览器。

打开设备的网页界面

1. 打开一个浏览器，键入安讯士设备的 IP 地址或主机名。
如果您不知道 IP 地址，请使用 AXIS IP Utility 或 AXIS Device Manager 在网络上查找设备。
2. 键入用户名和密码。如果是首次访问设备，则必须创建管理员账户。请参见。

有关在设备的网页界面中控件和选项的说明，请参见。

创建管理员账户

首次登录设备时，您必须创建管理员账户。

1. 请输入用户名。
2. 输入密码。请参见。
3. 重新输入密码。
4. 接受许可协议。
5. 单击**添加帐户**。

重要

设备没有默认账户。如果您丢失了管理员账户密码，则您必须重置设备。请参见。

安全密码

重要

使用 HTTPS（默认已启用）通过网络设置密码或其它敏感配置。HTTPS 可实现安全和加密的网络连接，从而保护密码等敏感数据。

设备密码是对数据和服务的主要保护。Axis 设备不会强加密码策略，因为它们可能会在不同类型的安装中使用。

为保护您的数据，我们强烈建议您：

- 使用至少包含 8 个字符的密码，而且密码建议由密码生成器生成。
- 不要泄露密码。

- 定期更改密码，至少一年一次。

确保没有人篡改过设备软件

要确保设备具有其原始的 AXIS OS，或在安全攻击之后控制设备，请执行以下操作：

1. 重置为出厂默认设置。请参见。
重置后，安全启动可保证设备的状态。
2. 配置并安装设备。

网页界面概览

该视频为您提供设备网页界面的概览。



Axis 设备网页界面

配置设备

本部分介绍了安装程序在硬件安装完成后启动和运行产品所需的全部重要配置。

基本设置

设置电源频率

1. 转到**视频 > 安装 > 电源线频率**。
2. 单击**更改**。
3. 选择电源频率，然后单击**保存并重启**。

更改root用户密码

1. 登录到设备界面，并转到**系统 > 用户**。
2. 对于根用户，请单击  **> Update user (更新用户)**。
3. 输入新密码并保存。

设置直连 SIP (P2P)

VoIP (IP 语音) 是一组支持通过 IP 网络进行语音和多媒体通信的技术。有关详细信息，请参见。

在该设备中，VoIP 通过 SIP 协议启用。如需了解更多关于SIP的信息，请参见

SIP有两种设置类型。直连或点对点 (P2P) 是其中之一。如果是同一 IP 网络内少数用户代理之间的通信且无需 PBX 服务器可提供的额外功能，则使用点对点。如需了解关于如何安装的信息，请参见。

1. 转到**通信 > SIP > 设置**，然后选择**启用 SIP**。
2. 要允许设备接收呼入，选择**允许呼入**。

注意

当您允许呼入时，设备会接受来自网络中不同设备的呼叫。如果可从公共网络或互联网访问该设备，我们建议您不要允许呼入。

3. 单击**呼叫处理**。
4. 在**呼叫超时**中，设置在无应答时呼叫在结束前持续的秒数。
5. 如果您已允许呼入，请在**呼入超时**中设置呼入超时前的秒数。
6. 单击**端口**。
7. 输入 **SIP 端口号**和 **TLS 端口号**。

注意

- **SIP 端口** – 对于 SIP 会话。通过此端口的信令流量为非加密。默认端口号为 5060。
 - **TLS 端口** – 对于 SIPS 和 TLS 保护的 SIP 会话。通过此端口的信令流量使用传输层安全协议 (TLS) 进行加密。默认端口号为 5061。
 - **RTP 起始端口** – SIP 呼叫中用于首个 RTP 媒体流的端口。默认开始端口为 4000。一些防火墙会拦截某些端口号上的 RTP 通信。端口号必须在 1024 到 65535 之间。
8. 单击**NAT 穿越**。
 9. 选择要启用 NAT 穿越功能的协议。

注意

当设备从 NAT 路由器或防火墙后方连接到网络时，使用 NAT 穿越。有关详细信息，请参见。

10. 单击 **Save (保存)**。

通过服务器设置 SIP (PBX)

VoIP（IP 语音）是一组支持通过 IP 网络进行语音和多媒体通信的技术。有关详细信息，请参见。
在该设备中，VoIP 通过 SIP 协议启用。如需了解更多关于 SIP 的信息，请参见

SIP 有两种设置类型。PBX 服务器是其中之一。当应在 IP 网络内外的无数用户代理之间进行通信时，使用 PBX 服务器。可以在设置中添加其他功能，具体取决于 PBX 供应商。有关详细信息，请参见。

1. 请求您的 PBX 供应商提供以下信息：
 - 用户 ID
 - 域
 - 密码
 - 身份验证 ID
 - 呼叫者 ID
 - 注册
 - RTP 开始端口
2. 转到 **通信 > SIP > 账户**，然后单击 **+ 添加账户**。
3. 输入帐户名称。
4. 选择已注册。
5. 选择一种传输模式。
6. 添加 PBX 供应商提供的帐户信息。
7. 单击 **Save（保存）**。
8. 使用与点对点相同的方法创建 SIP 设置，请参见。使用 PBX 供应商的 RTP 启动端口。

创建一位联系人

本示例说明了如何在联系人列表中创建一位新的联系人。在您开始之前，请在 **通信 > SIP** 中启用 SIP。

要创建一位新联系人：

1. 转到 **通信 > 联系人列表**。
2. 单击 **+ 添加联系人**。
3. 输入联系人的姓名。
4. 输入联系人的 SIP 地址。

注意

有关 SIP 地址的信息，请参见。

5. 选择用于发出呼叫的 SIP 账户。

注意

可用性选项在 **系统 > 事件 > 时间表** 中定义。

6. 选择联系人的**可用性**。如果在联系人不可用时呼叫，呼叫将被取消，除非有备用联系人。

注意

备用联系人是一个在原始联系人未作出回应或不可用时可将电话转接的对象。

7. 在**紧急联系人**中，选择无。
8. 单击 **Save（保存）**。

配置呼叫按钮

在默认情况下，将呼叫按钮配置为进行 VMS（视频管理软件）呼叫。如果您想保留此配置，您仅需将 Axis 对讲机添加至 VMS。

本示例说明了如何设置系统以在来访者按下呼叫按钮时呼叫联系人列表中的联系人。

1. 转到**通信 > 呼叫 > 呼叫按钮**。
2. 在**收件人**下，移除 **VMS**。
3. 在**收件人**下，选择现有联系人或创建新联系人。

要禁用呼叫按钮，关闭**启用呼叫按钮**。

使用 DTMF 为来访者开门

当某位来访者从对讲机进行呼叫时，接听人员可使用其 SIP 设备的双音多频 (DTMF) 信号发送装置来开门。门禁控制器可开门和锁门。

本示例说明了如何进行操作：

- 定义对讲机的 DTMF 信号
- 将对讲机设置为：
 - 请求门禁控制器开门，或
 - 使用内部继电器开门。

您可在对讲机网页上进行设置。

在您开始之前

- 允许从该设备进行 SIP 呼叫并创建一个 SIP 账户。请参见和。

定义对讲机的 DTMF 信号

1. 转到**通信 > SIP > DTMF**。
2. 单击**+** 添加序列。
3. 在**Sequence（序列）**中，输入**1**。
4. 在**Description（描述）**中，输入**Unlock door（打开门锁）**。
5. 在**账户**中，选择 SIP 帐户。
6. 单击 **Save（保存）**。

设置对讲机，以使用内部继电器开门

7. 转到**系统 > 事件 > 规则**，然后添加一个规则。
8. 在**Name（名称）**字段中，输入**DTMF unlock door（DTMF打开门锁）**。
9. 从条件列表中，在**呼叫**下，选择 **DTMF** 和**打开门锁**。
10. 从操作列表中，在 **I/O**下，选择 **切换 I/O 一次**。
11. 从端口列表中，选择 **继电器 1**。
12. 将**持续时间**更改为 **00:00:07**，这意味着门将打开 7 秒。
13. 单击 **Save（保存）**。

允许凭证持有者开门

通过入口列表，凭证持有者可以使用其卡或 PIN 来触发操作，例如开门。此示例说明如何添加可以使用其卡开门 10 次的凭证持有者。

前提条件

- 确保在**读卡器 > 芯片类型**中激活正确的芯片类型。

打开入口列表并添加凭证持有者：

1. 转到**读卡器 > 入口列表**。

2. 打开**使用入口列表**。
3. 单击 **+ 添加凭证持有者**。
4. 输入凭证持有者的名字和姓氏。名字必须是唯一的。
5. 选择卡。
6. 在设备上刷凭证持有者的卡，然后单击**获取新版本**。
7. 保留事件条件**授予访问权限**。
8. 在**有效期至下**，选择**次数**。
9. 在**Number of times (次数)** 中，输入**10**。
10. 单击 **Save (保存)**。

创建一个规则：

1. 转到**系统 > 事件**。
2. 在**规则**下，单击**+ 添加一个规则**。
3. 在**Name (名称)** 中，输入**Open door (开门)**。
4. 在条件列表中，选择**入口列表 > 访问权限已授予**。
5. 在操作列表中，选择**I/O > 切换 I/O 一次**。
6. 在端口列表中，选择**门**。
7. 在**状态**下，选择**活动**。
8. 设置持续时间至**00:00:07**。
9. 单击 **Save (保存)**。

调整图像

本部分包括配置设备的说明。如果您想要了解有关特定性能如何工作的更多信息，请转到。

选择曝光模式

要提高特定监控场景的图像质量，请使用曝光模式。曝光模式让您能够控制光圈、快门速度和增益。转到**视频 > 图像 > 曝光**，然后在以下曝光模式之间进行选择：

- 对于大多数使用情况，请选择**自动曝光**。
- 对于使用某些人造光源（如荧光照明）的环境，请选择**无闪烁**。
选择与电流频率相同的频率。
- 对于使用某些人造光源和明亮光源的环境（例如，在夜间使用荧光照明并在白天使用日光照明的室外环境），请选择**减少闪烁**。
选择与电流频率相同的频率。
- 要锁定当前曝光设置，请选择**保持当前设置**。

在低照度条件下降低噪声

要在低照度条件下降低噪声，您可调整下面的一种或多种设置：

- 调整噪声和运动模糊之间的平衡。转到**视频 > 图像 > 曝光**，将**模糊-噪声平衡**滑块移向**低噪声点**。
- 将曝光模式设置为自动。

注意

最大快门值可导致运动模糊。

- 要降低快门速度，请将最大快门设置为可能的最大值。

注意

当您降低最大增益时，图像会变得更暗。

- 将最大增益设置为更低的值。
- 如果有Aperture（光圈）滑块，将其移向Open（打开）。
- 在**视频 > 图像 > 外观**下，降低图像中的锐度。

显示文本叠加

您可在视频流中将文本字段添加为叠加。例如，您可以在想要在视频流中显示日期、时间或公司名称时使用该功能。

1. 转到**视频 > 叠加**。
2. 选择**Text（文本）**，然后单击 。
3. 键入要在视频流中显示的文本。
4. 选择一个位置。您也可在实时画面中拖动叠加文本字段以更改位置。

设置事件规则

您可以创建规则来使您的设备在特定事件发生时执行某项操作。规则由条件和操作组成。条件可以用来触发操作。例如，设备可以在检测到移动后开始录制或发送电子邮件，或在设备录制时显示叠加文本。

若要了解更多信息，请查看我们的指南**事件规则入门**。

当设备侦测到物体时，显示视频流中的文本叠加

本示例说明了当设备侦测到物体时，如何显示文本“Motion detected”。

请确保 AXIS Object Analytics 正在运行：

1. 转到**应用 > AXIS Object Analytics**。
2. 如果应用程序尚未运行，请将其启动。
3. 请确保已根据需要设置了应用程序。

添加叠加文本：

1. 转到**视频 > 叠加**。
2. 在**Overlays（叠加）**下，选择**Text（文本）**，然后单击 。
3. 在文本字段中，输入 #D。
4. 选择文本大小和外观。
5. 要对文本叠加进行定位，请单击  并选择一个选项。

创建一个规则：

1. 转到**系统 > 事件**并添加响应规则。
2. 为规则键入一个名称。
3. 在条件列表中的应用下，在**应用程序**下，选择 Object Analytics。
4. 在响应列表中，在**叠加文本**下，选择**使用叠加文本**。
5. 选择视频通道。
6. 在**文本**中，键入“已侦测到移动动作”。
7. 设置持续时间。
8. 单击 **Save（保存）**。

网页界面

要达到设备的网页界面，请在网页浏览器中键入设备的 IP 地址。

注意

对本节中描述的功能和设置的支持因设备而异。此图标  指示功能或设置仅在某些设备中可用。

-  显示或隐藏主菜单。
-  访问发行说明。
-  访问产品帮助页。
-  更改语言。
-  设置浅主题或深色主题。
-   用户菜单包括：
 - 有关登录用户的信息。
 -  **更改账户**：从当前账户退出，然后登录新账户。
 -  **退出**：从当前账户退出。
- ⋮ 上下文菜单包括：
 - **分析数据**：接受共享非个人浏览器数据。
 - **反馈**：分享反馈，以帮助我们改善您的用户体验。
 - **法律**：查看有关 Cookie 和许可证的信息。
 - **关于**：查看设备信息，包括 AXIS OS 版本和序列号。

状态

设备信息

显示设备信息，包括 AXIS OS 版本和序列号。

升级 AXIS OS：升级设备上的软件。转到在其中进行升级的维护页面。

时间同步状态

显示 NTP 同步信息，包括设备是否与 NTP 服务器同步以及下次同步前的剩余时间。

NTP 设置：查看并更新 NTP 设置。转到可更改 NTP 设置的**时间和位置**页面。

安全

显示活动设备的访问类型，正在使用的加密协议，以及是否允许未签约的应用。对设置的建议基于《AXIS OS 强化指南》。

强化指南：转到《AXIS OS 强化指南》，您可在其中了解有关如何应用安讯士设备理想实践的更多信息。

连接的客户端

显示连接和连接的客户端数量。

查看详细信息：查看和更新已连接客户端列表。该列表显示了每个连接的 IP 地址、协议、端口、状态和 PID/进程。

持续录制中

显示正在进行的录制及其指定的存储空间。

录像：查看正在进行的录制和过滤的录制文件及其来源。有关详细信息，请参见



显示保存录制内容的存储空间。

视频



单击以播放实时视频流。



单击以冻结实时视频流。



单击以对实时视频流拍摄快照。该文件将保存在计算机上的“下载”文件夹中。图像文件名为 [snapshot_YYYY_MM_DD_HH_MM_SS.jpg]。快照的实际大小取决于接收快照的特定网页浏览器引擎应用的压缩，因此，快照大小可能与设备中配置的实际压缩设置不同。



单击以显示 I/O 输出端口。使用开关打开或关闭端口的电路，例如测试外部设备。



单击以手动打开或关闭红外照明。



单击以手动打开或关闭白光。



单击以访问屏幕控制。启用屏幕控制组，使用户在视频管理软件中右键单击直播流时可使用各组中的设置。

- **预定义控制：**列出默认的屏幕控制。
- **自定义控制：**单击  **Add custom control (添加自定义控制)** 可创建自定义屏幕控制。



启动清洗器。当程序开始时，摄像机移动到配置好的位置接受冲洗喷淋。当整个清洗程序完成时，摄像机返回至其原先的位置。此图标仅当清洗器已连接并配置时可见。



启动雨刮器。



单击并选择一个预设位置，以转到实时画面中的预设位置。或者，单击**设置**转到预置位页面。



添加或删除对焦唤醒区域。添加对焦唤醒区域时，摄像机将保存该特定水平转动/垂直转动范围内的对焦设置。如果已设置对焦唤醒区域，当摄像机在实景中进入该区域时，该摄像机将唤醒先前保存的对焦。摄像机覆盖一半区域便足以唤醒对焦。



单击以选择轮巡，然后单击**Start (开始)**以播放轮巡功能。或者，单击**设置**以转到轮巡功能页面。



单击以在选定的时间段内手动打开加热器。



单击开始实时视频流的连续录制。再次单击可停止录制。如果正在进行录制，它将在重启后自动恢复。



单击以显示为设备配置的存储。要配置存储，您需要以管理员身份登录。



单击以访问更多设置：

- **视频格式：**选择实景中所用编码格式。

-  **自动播放**：打开以在新会话中打开设备时自动播放静音的视频流。
- **客户端流信息**：打开以显示有关显示实时视频流的浏览器所使用的视频流的动态信息。比特率信息不同于文本叠加中显示的信息，因为有不同的信息源。客户端流信息中的比特率是终末一秒的比特率，它来自设备的编码驱动程序。叠加中的比特率是终末 5 秒的平均比特率，它来自浏览器。这两个值仅覆盖原始视频流，而不是通过 UDP/TCP/HTTP 网络传输时所产生的额外带宽。
- **自适应流**：打开以将图像分辨率调整为查看客户端的实际显示分辨率，以提高用户体验并帮助防止客户端硬件可能超载。仅当您使用浏览器在网页界面中查看实时视频流时，才应用自适应流。当打开自适应流时，帧率上限为 30 fps。如果您在自适应流打开时拍摄快照，它将使用自适应流选择的图像分辨率。
- **水平网格**：单击  显示水平网格。网格可帮助您确定图像是否水平对齐。单击  以隐藏。
- **像素计数器**：单击  显示像素计数器。拖动并调整方框大小以包含关注区域。还可以在宽度和高度字段中定义方框的像素大小。
- **刷新**：单击  刷新实时画面中的静态图像。
- **PTZ控制** ：打开以在实时画面中显示 PTZ 控件。

 单击以在全分辨率下显示实时画面。如果全部分辨率超过了屏幕尺寸，请使用较小的图像以在图像中导航。

 单击以全屏显示实时视频流。按ESC退出全屏模式。

安装

取景模式 ：取景模式是一种预置配置，用于定义摄像机取景的方式。当您更改取景模式时，它可能会影响许多其他设置，例如，视点区域和隐私遮罩。

安装位置 ：图像的方向会根据您按照摄像机的方式而变化。

电源频率：要尽可能减少图像闪烁，选择您所在地区使用的频率。美国地区通常使用 60 Hz。世界上的其余地区大部分使用 50 Hz。如果您无法确定您所在地区的电源频率，请咨询当地机构。

旋转：选择理想的图像方向。

图像

外观

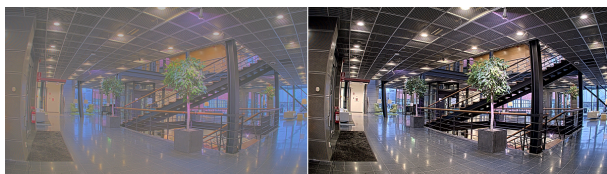
场景配置文件 ⓘ：选择适合您的监控场景的场景配置文件。场景配置文件可优化特定环境或用途的图像设置，包括颜色级、亮度、锐度、对比度和局部对比度。

- **Forensic** ⓘ：适合监控。
- **室内** ⓘ：适合室内环境。
- **室外** ⓘ：适合室外环境。
- **鲜明** ⓘ：适用于演示目的。
- **交通概览** ⓘ：适用于车辆交通监控。
- **牌照** ⓘ：适用于捕捉牌照。

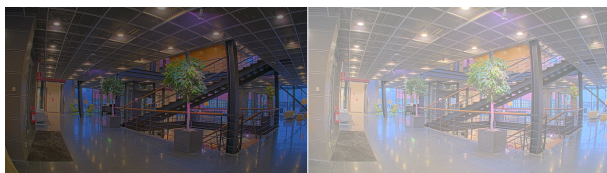
饱和度：使用滑块调整色彩浓度。例如，您可以获取一个灰度图像。



对比度：此滑块以调整明暗之间的差别。



亮度：使用滑块调整光线强度。这可使物体更易于查看。在捕捉图像后应用亮度，并不会影响图像的信息。要从黑暗区域获得更多详细信息，通常加大增益或增加曝光时间。



锐度：使用滑块通过调整边缘对比度以使图像中的物体显示得更锐利。如果增加锐度，可能会增加所需的比特率和存储空间量。



宽动态范围功能

WDR ⓘ：打开以使图像的明暗区域均可视。

局部对比度 ⓘ：使用滑块调整图像对比度。较高的值会使亮度和光线区域之间的对比度更高。

色调映射 ⓘ：使用滑块以调整应用于图像的色调映射量。如果此值设置为零，仅应用标准灰度校正，而提高值将增加图像中更暗和更亮部分的可视性。

白平衡

如果摄像机侦测到接收的光线的色温，则可以调整图像，让颜色显得更自然。如果这还不够，您可从列表中选择合适的光源。

自动白平衡设置可通过逐渐适应变化来降低颜色闪烁的风险。若要更改照明或摄像机首次启动时，可能需要长达 30 秒来适应新光源。如果某个场景中存在多个类型的光源，即，这些光源的色温不同，则主导光源将用作自动白平衡算法的参考。通过选择与要用作参考的光源相匹配的固定白平衡设置，可以覆盖此行为。

光线环境：

- **自动**：自动识别和补偿光源颜色。这是推荐设置，可用于大多数情况。
- **自动 – 室外** ⓘ：自动识别和补偿光源颜色。这是在多数室外场景下建议使用的设置。
- **自定义 – 室内** ⓘ：固定颜色调整，用于采用人造光源（荧光照明除外）且具有约 2800 K 良好色温的房间。
- **自定义 – 室外** ⓘ：固定颜色调整，用于色温约 5500 K 的晴朗天气条件。
- **固定 – 荧光 1**：固定颜色调整，用于色温约 4000 K 的荧光照明。
- **固定 – 荧光 2**：固定颜色调整，用于色温约 3000 K 的荧光照明。
- **固定 – 室内**：固定颜色调整，用于采用人造光源（荧光照明除外）且具有约 2800 K 良好色温的房间。
- **固定 – 室外 1**：固定颜色调整，用于色温约 5500 K 的晴朗天气条件。
- **固定 – 室外 2**：固定颜色调整，用于色温约 6500 K 的多云天气条件。
- **路灯 – 水银** ⓘ：固定颜色调整，用于街道照明中常用汞蒸汽灯发出的紫外线。
- **路灯 – 钠** ⓘ：固定颜色调整，用于补偿街道照明中常用钠蒸汽灯发出的黄橙色。
- **保持当前设置**：保持当前设置，切勿补偿光线变化。
- **手动** ⓘ：借助白色物体固定白平衡。将圆圈拖曳到您想让摄像机显示为白色的实景图像中的物体上。使用**红平衡**和**蓝平衡**滑块以手动调整白平衡。

曝光

选择曝光模式以减少图像中迅速变化的不良效应，如不同光源类型产生的闪烁。我们推荐您使用自动曝光模式，或使用与电力网络相同的频率。

曝光模式：

- **自动：**摄像机自动调节光圈、增益和快门。
- **自动光圈** ⓘ：摄像机自动调节光圈和增益。快门是固定的。
- **自动快门** ⓘ：摄像机自动调节快门和增益。光圈是固定的。
- **保持当前设置：**锁定当前曝光设置。
- **无闪烁** ⓘ：摄像机仅使用以下快门速度自动调节光圈，并仅使用以下快门速度：1/50 s (50 Hz) 和 1/60 s (60 Hz)。
- **无闪烁50 Hz** ⓘ：摄像机自动调节光圈和增益，并使用快门速度 1/50 s。
- **无闪烁60 Hz** ⓘ：摄像机自动调节光圈和增益，并使用快门速度 1/60 s。
- **减少闪烁** ⓘ：与无闪烁相同，但摄像机可对较明亮的场景使用快于 1/100 s (50 Hz) 和 1/120 s (60 Hz) 的快门速度。
- **减少闪烁50 Hz** ⓘ：这与无闪烁相同，但摄像机可对较明亮的场景使用快于 1/100 s 的快门速度。
- **减少闪烁60 Hz** ⓘ：这与无闪烁相同，但摄像机可对较明亮的场景使用快于 1/120 s 的快门速度。
- **手动** ⓘ：光圈、增益和快门均固定。

曝光区 ⓘ：使用曝光区域优化场景选定部分的曝光，例如，入口门前面的区域。

注意

曝光区域与原始图像（不旋转）相关，且区域名称将应用于原始图像。这意味着，如果视频流旋转 90°，那么视频流中的上方区域将变为右，而左变为下方。

- **自动：**适用于大多数情况。
- **中心：**使用图像中心的固定区域来计算曝光。该区域在实景中具有固定大小和位置。
- **全屏** ⓘ：使用整个实景来计算曝光。
- **向上** ⓘ：使用图像上半部分具有固定大小和位置的区域来计算曝光。
- **向下** ⓘ：使用图像下半部分具有固定大小和位置的区域来计算曝光。
- **左** ⓘ：使用图像左半部分具有固定大小和位置的区域来计算曝光。
- **右** ⓘ：使用图像右半部分具有固定大小和位置的区域来计算曝光。
- **场所：**使用实景中具有固定大小和位置的区域来计算曝光。
- **自定义：**使用实景中的一个区域来计算曝光。您可以调整该区域的大小和位置。

快门上限：选择快门速度以生成优化图像。低快门速度（曝光时间更长）可能导致运动时产生运动模糊，而过高的快门速度则可能影响图像质量。可以配合使用最大快门和最大增益来改善图像。

增益上限：选择合适的最大增益。如果增益上限加大，则会改善黑暗图像中细节的可视级别，但也会提高噪音级别。更多噪声还可能导致使用更多带宽和存储。如果将增益上限设置为较高值，且昼夜光线条件不同时，图像会差异很大。可以配合使用最大增益和最大快门以改善图像。

运动自适应曝光 ：选择以减少低照度条件下的运动模糊。

模糊-噪声平衡：使用滑块以调节运动模糊与噪声之间的优先级。如果您希望优先考虑低带宽，并以牺牲移动物体的细节来换取噪声降低，请将此参数调节为**低噪声**。如果您希望以牺牲噪声和带宽来优先保留移动物体的细节，请将此参数调节为**低运动模糊**。

注意

您可以通过调节曝光时间或调节增益来更改曝光。如果增加曝光时间，则会产生更多的运动模糊，并且如果增加增益，则会导致更多噪音。如果将**模糊噪声平衡功能**调整为**低噪声**，自动曝光将优先更长的曝光时间而不是增加增益，如果调整的平衡调整为**低运动模糊**，则相反。在低照度条件下，增益和曝光时间终会达到最大值，不论此参数如何设置优先级。

锁定光圈 ：打开以设置**光圈**滑块来保留光圈大小。关闭以让摄像机自动调整光圈大小。例如，您可以将光圈锁定在始终照亮的场景。

光圈 ：使用滑块来调整光圈大小，也就是说，镜头的进光量。要允许更多光线进入传感器，从而在低照度条件下生成较亮的图像，请移动滑块至**打开**。打开光圈也会降低景深，这意味着，离摄像机较近或较远的物体可能无法对焦显示。要使更多图像处于聚焦状态，请将滑块向**关闭**移动。

曝光级别：使用滑块调整图像曝光。

除雾 ：打开以侦测多雾天气的影响，并自动除雾以获得清晰的图像。

注意

我们建议您不要在低对比度、较大光线水平变体或自动对焦稍微熄灭的场景中打开**除雾**。这可能会影响图像质量，例如，在提高对比度时。另外，当除雾功能激活时，太多光量可能对图像质量产生负面影响。

流

概述

分辨率：选择适合监控场景的图像分辨率。更高的分辨率会增加带宽和存储。

帧率：为了避免网络带宽问题或降低存储容量，可将帧速限制为一个固定值。如果将帧速保留为零，则帧速将保持在当前条件下可能的帧速上限。更高的帧速要求更多带宽和存储容量。

P 帧：P 帧是仅显示图像与前一帧的变化的预测图像。输入所需的 P 帧数量。该数量越高，所需带宽越少。但是，如果出现网络拥塞，视频质量可能会明显下降。

压缩：使用滑块调整图像压缩。高压压缩导致更低的比特率和更差的图像质量。低级别的压缩可提高图像质量，但在录制时会使用更多带宽和存储。

签名视频 ：打开以将签名视频功能添加到视频。签名视频通过向视频添加加密签名来保护视频免受篡改。

Zipstream

Zipstream 是一种针对视频监控进行了优化的比特率降低技术，能够实时降低 H.264 或 H.265 流中的平均比特率。Axis Zipstream 在具有多个关注区域的场景（例如，有移动物体的场景）中应用高比特率。当场景更加静态时，Zipstream 使用更低的比特率，从而减少所需存储。要了解更多信息，请参见以 *Axis Zipstream 降低比特率*

选择比特率降低强度：

- **关闭：** 比特率没有降低。
- **低：** 在大部分场景中没有可见的质量降低。这是默认选项，可用于各类型的场景以降低比特率。
- **中：** 通过在较低关注度区域内噪声减少且细节水平略低（例如，没有移动）的某些场景中的可视效果。
- **高：** 通过在较低关注度区域内噪声减少且细节水平降低（例如，没有移动）的某些场景中的可视效果。我们为使用本地存储的云连接设备和设备推荐此级别。
- **更高：** 通过在较低关注度区域内噪声减少且细节水平降低（例如，没有移动）的某些场景中的可视效果。
- **非常高：** 在大多数场景中具有可见效果。比特率已针对存储下限进行了优化。

优化存储： 打开以在保持质量的同时尽可能降低比特率。优化不应用于网络客户端中显示的流。仅当您的 VMS 支持 B 帧时，才可使用此选项。打开**优化存储**还会打开**动态 GOP**。

动态 FPS（每秒帧数）： 打开以允许带宽因场景中的活动级别而异。更多的活动需要更多带宽。

下限： 输入一个值，以根据场景运动调整 fps 下限和流默认 fps 之间的帧速。我们建议您在很少运动的场景中使用下限，帧速可降至 1 或更低。

动态图片组 (GOP)（图片组）： 打开以根据场景中的活动级别动态调整 I 帧之间的间隔。

上限： 输入 GOP 长度上限，即两个 I 帧之间的 P 帧数上限。I 帧是独立的图像帧，不依赖于其他帧。

比特率控制

- **平均：** 选择以在更长的时间内自动调整比特率，并根据可用存储提供理想图像质量。
 -  单击以根据可用存储空间、保留时间和比特率限制计算目标比。
 - **目标比特率：** 输入所需的目标比特率。
 - **保留时间：** 输入录制内容的保留天数。
 - **存储：** 显示可用于流的预计存储空间。
 - **比特率上限：** 打开以设置比特率限制。
 - **比特率限制：** 键入一个高于目标比特率的比特率限制。
- **上限：** 选择以根据您的网络带宽设置流的即时比特率上限。
 - **上限：** 输入比特率上限。
- **可变：** 选择以允许比特率根据场景中的活动级别而变化。更多的活动需要更多带宽。我们建议在大多数情况下选择此选项。

方向

镜像： 打开以镜像图像。

音频

包含： 打开以在视频流中使用音频。

来源 ：选择要使用的音频源。

立体声 ：打开以包括内置音频以及来自外部麦克风的音频。

叠加



：单击以添加叠加。从下拉列表中选择叠加类型：

- **文本**：选择以显示集成在实时画面图像中且在各画面、录像和快照中可见的文本。您可以输入自己的文本，也可以包括预先配置的调节器，以自动显示示例时间、日期及帧速。
 - ：单击以添加日期修饰符 %F，以显示年-月-日。
 - ：单击以添加时间修饰符 %X，以显示时:分:秒（24 小时制）。
 - **修饰符**：单击以选择列表中显示的任一修饰符，以将其添加到文本框中。例如，%a 显示星期几。
 - **尺寸**：选择所需字体大小。
 - **外观**：选择文本颜色和背景色，如白色文本加黑色背景（默认）。
 - ：选择叠加在图像中的位置，或单击并拖动叠加，使其在实时画面中四处移动。
- **图像**：选择以显示通过视频流叠加的静态图像。您可以使用 bmp、.png、jpeg 或 svg 文件。要上传图像，请单击 **Manage images（管理图像）**。在上传图像之前，您可以选择：
 - **使用分辨率缩放**：选择自动缩放叠加图像以适合视频分辨率。
 - **使用透明色**：选择并输入该颜色的 RGB 十六进制值。使用 RRGGBB 格式。十六进制值的示例：FFFFFF 表示白色，000000 表示黑色，FF0000 表示红色，6633FF 表示蓝色，669900 表示绿色。仅适用于 .bmp 图像。
- **场景填充** ：选择以在视频流中显示叠加在同一位置的文本，即使摄像机向另一个方向平移或倾斜也是如此。您可以选择仅在特定缩放级别内显示叠加层。
 - ：单击以添加日期修饰符 %F，以显示年-月-日。
 - ：单击以添加时间修饰符 %X，以显示时:分:秒（24 小时制）。
 - **修饰符**：单击以选择列表中显示的任一修饰符，以将其添加到文本框中。例如，%a 显示星期几。
 - **尺寸**：选择所需字体大小。
 - **外观**：选择文本颜色和背景色，如白色文本加黑色背景（默认）。
 - ：选择叠加在图像中的位置，或单击并拖动叠加，使其在实时画面中四处移动。叠加将被保存并保留在该位置的平移和倾斜坐标中。
 - **变焦级别 (%) 之间的注释**：设置叠加层显示的缩放级别。
 - **注释符号**：选择当摄像机不在设置的缩放级别内时显示的符号而不是叠加层。
- **流传输指示器** ：选择以显示通过视频流叠加的动画。动画显示视频流是实时的，即使场景中没有移动。
 - **外观**：选择动画的颜色和背景色，如红色文本加透明背景（默认）。
 - **尺寸**：选择所需字体大小。
 - ：选择叠加在图像中的位置，或单击并拖动叠加，使其在实时画面中四处移动。
- **小部件：折线图** ：显示一个图表，显示测量值如何随时间变化。
 - **标题**：输入小部件的标题。

- **叠加调节器**：选择叠加调节器作为数据源。如果您创建了 MQTT 叠加，它们将位于列表的末尾。
- ：选择叠加在图像中的位置，或单击并拖动叠加，使其在实时画面中四处移动。
- **尺寸**：选择叠加的大小。
- **在各频道上可见**：关闭以仅在您当前选择的频道上显示。打开以在各活动频道上显示。
- **更新时间隔**：选择数据更新之间的时间。
- **透明度**：设置整个叠加的透明度。
- **背景透明度**：仅设置叠加层背景的透明度。
- **点**：启用以在数据更新时向图表线条添加点。
- **X axis**
 - **标签**：输入 x 轴的文本标签。
 - **时间窗口**：输入数据可视化的时间。
 - **时间单位**：输入 x 轴的时间单位。
- **Y axis**
 - **标签**：输入 y 轴的文本标签。
 - **动态缩放**：开启以便缩放会自动适应数据值。关闭以手动输入固定比例的值。
 - **低警报阈值和高警报阈值**：这些值将为图表添加水平参考线，以便更容易看到数据值何时变得过高或过低。
- **小部件：计量器** ：显示近期测量的数据值的条形图。
 - **标题**：输入小部件的标题。
 - **叠加调节器**：选择叠加调节器作为数据源。如果您创建了 MQTT 叠加，它们将位于列表的末尾。
 - ：选择叠加在图像中的位置，或单击并拖动叠加，使其在实时画面中四处移动。
 - **尺寸**：选择叠加的大小。
 - **在各频道上可见**：关闭以仅在您当前选择的频道上显示。打开以在各活动频道上显示。
 - **更新时间隔**：选择数据更新之间的时间。
 - **透明度**：设置整个叠加的透明度。
 - **背景透明度**：仅设置叠加层背景的透明度。
 - **点**：启用以在数据更新时向图表线条添加点。
 - **Y axis**
 - **标签**：输入 y 轴的文本标签。
 - **动态缩放**：开启以便缩放会自动适应数据值。关闭以手动输入固定比例的值。
 - **低警报阈值和高警报阈值**：这些值将为条形图添加水平参考线，以便更容易看到数据值何时变得过高或过低。

隐私遮罩



：单击以创建新的隐私遮罩。

隐私遮罩:单击此处可更改各隐私遮罩的颜色，或永久删除各隐私遮罩。



遮罩 x：单击可重命名、禁用或永久删除遮罩。

通讯

联系人名单

联系人



单击可将联系人列表下载为 json 文件。



单击导入联系人列表（json）。



Add contact（添加联系人）：单击此处，将新联系人添加到联系人列表中。

上传图像 ：单击上传代表联系人的图像。

名字：输入联系人的名字。

姓氏：输入联系人的姓氏。

Speed dial（快速拨号） ：输入联系人的可用快速拨号号码。此号码用于从设备呼叫联系人。

SIP 地址：若您使用 SIP，请输入联系人的 IP 地址或分机号。



：单击以进行测试呼叫。当应答时，呼叫将自动结束。

SIP 账户:若您使用 SIP，选择要用于从设备呼叫联系人的 SIP 账户。

可用性：选择联系人的可用性时间表。您可以在**系统 > 事件 > 时间表**中添加或调整时间表。如果在联系人不可用时尝试呼叫，呼叫将被取消，除非有备用联系人。

备用：如果适用，请从列表中选择一个备用联系人。

备注：添加有关联系人的可选信息。



上下文菜单包括：

编辑联系人：编辑联系人的属性。

删除联系人：删除联系人。

SIP

设置

会话初始协议 (SIP) 用于用户间的交互式通信会话。该会话可包含音频和视频。

SIP 设置助手：单击以逐步设置和配置 SIP。

启用 SIP：选中此选项，可以初始化和接收 SIP 呼叫。

允许呼入：勾选此选项以允许来自其他 SIP 设备的呼入。

呼叫处理

- **呼叫超时：**设置无人应答时尝试呼叫的持续时间上限。
- **呼入持续时间：**设置一个呼入可持续的时间上限（上限为 10 分钟）。
- **在这之后结束呼叫：**设置一个呼叫可持续的上限时间（上限为 60 分钟）。如果您不想限制呼叫长度，请选择**无限期呼叫持续时间**。

端口

端口号要在 1024 到 65535 之间。

- **SIP 端口：**用于 SIP 通信的网络端口。通过此端口的信令流量为非加密。默认端口号为 5060。如果需要，请输入不同的端口号。
- **TLS 端口：**用于已加密 SIP 通信的网络端口。通过此端口的信令流量使用传输层安全协议 (TLS) 进行加密。默认端口号为 5061。如果需要，请输入不同的端口号。
- **RTP 起始端口：**SIP 呼叫中用于第一个 RTP 媒体流的网络端口。默认开始端口号为 4000。有些防火墙会阻止某些端口号上的 RTP 通信。

NAT 遍历

当设备位于某个专用网络 (LAN)，并且您希望使它在该网络之外可用时，则使用 NAT（网络地址转换）穿透。

注意

要使 NAT 穿透发挥作用，则要使用支持其的路由器。该路由器还必须支持 UPnP®。

每个 NAT 穿越协议可单独使用或组合使用，具体取决于网络环境。

- **ICE：**ICE（交互式连接建立）协议可增加找到对等设备之间进行成功通信的更有效路径的机率。如果您还启用了 STUN 和 TURN，则您可提高 ICE 协议的机会。
- **STUN：**STUN（NAT 会话遍历实用程序）是一个客户端服务器网络协议，可让设备确定是否其位于 NAT 或防火墙的后方，如果是的话，则获取映射的公共 IP 地址和分配用于连接至远程主机的端口号。输入 STUN 服务器地址，例如，IP 地址。
- **TURN：**TURN（通过中继方式穿越 NAT）是一个可让 NAT 路由器或防火墙后方的设备通过 TCP 或 UDP 接收其他主机的呼入数据的协议。输入 TURN 服务器地址和登录信息。

音频和视频

- **音频编解码器优先级：**针对 SIP 呼叫选择至少一个具有所需音频质量的音频编解码器。拖放可更改优先级。

注意

所选编解码器必须与呼叫接收编解码器匹配，因为进行呼叫时，接收编解码器起着决定性作用。

- **音频指导：**选择允许的音频方向。
- **H.264 packetization 模式：**选择要使用的 packetization 模式。
 - **自动：**（推荐）该设备决定要使用哪种 packetization 模式。
 - **无：**未设置 packetization 模式。此模式通常被解释为模式 0。
 - **0：**非隔行模式。
 - **1：**单 NAL 单元模式。
- **视频方向：**选择允许的视频方向。
- **在通话中显示视频 **：在设备显示屏上显示传入的视频流。

其他

- **UDP-to-TCP 转换：**选择以允许暂时将传输协议从 UDP（用户数据报协议）转换成 TCP（传输控制协议）的呼叫。转换的原因是为了避免分片，如果请求在传输单元 (MTU) 上限的 200 字节内或大于 1300 字节，则可以进行切换。
- **允许通过重写：**选择以发送本地 IP 地址，而不是路由器的公共 IP 地址。
- **允许触点重写：**选择以发送本地 IP 地址，而不是路由器的公共 IP 地址。
- **每次向服务器登记：**设置您希望设备就现有 SIP 账户向 SIP 服务器登记的频率。
- **DTMF 有效负载类型：**更改 DTMF 的默认有效负载类型。
- **重新传输率上限：**设置设备在停止尝试之前尝试连接到 SIP 服务器的最大次数。
- **故障恢复之前秒数：**设置设备在故障转移到辅助 SIP 服务器后在尝试重新连接到主 SIP 服务器之前间隔的秒数。

账户

当前的 SIP 账户都列在**SIP 账户**下。针对已注册账户，彩色圆圈可使您了解其状态。

- 该账户通过 SIP 服务器成功注册。
- 该帐户存在问题。原因可能是授权失败、账户证书错误或 SIP 服务器无法找到该账户。

点对点（默认）帐户是一个自动创建的帐户。如果您至少创建了一个其他账户，并将该账户设置为默认，则您可以删除点对点账户。在未指定从哪个 SIP 帐户呼叫的情况下，进行 VAPIX® 应用程序接口 (API) 呼叫时，始终使用默认帐户。

+ **添加帐户：**单击以创建新的 SIP 账户。

- **激活：**选择能够使用该帐户。
- **设为默认：**选择将此帐户设为默认帐户。必须设置一个默认帐户，且仅能存在一个默认帐户。
- **自动应答：**选择自动接听呼入。
- **IPv6优先于IPv4 **：选择此选项可优先处理 IPv6 地址而不是 IPv4 地址。当您连接到同时解析 IPv4 和 IPv6 地址的对等账户或域名时，这非常有用。对于映射到 IPv6 地址的域名，您只能优先考虑 IPv6。
- **名称：**输入一个描述性名称。例如，此名称可以是一个姓名、一个角色或一个地点。该名称可重复。
- **用户 ID：**输入分配给设备的仅有的扩展名或电话号码。
- **点对点：**用于本地网络上向另一个 SIP 设备进行直接呼叫。
- **已注册：**用于通过 SIP 服务器向本地网络外的 SIP 设备进行呼叫。
- **域：**如可用，请输入公共域名。呼叫其他帐户时，它将显示为 SIP 地址的一部分。
- **密码：**输入与 SIP 帐户关联的密码，以根据 SIP 服务器进行鉴定。
- **鉴定 ID：**输入用于针对 SIP 服务器进行验证的身份验证 ID。如果它与用户 ID 相同，则您无需输入身份验证 ID。
- **呼叫者 ID：**从设备向呼叫接收人所显示的名称。
- **注册服务器：**输入注册服务器的 IP 地址。
- **传输模式：**选择针对该账户的 SIP 传输模式：UDP、TCP 或 TLS。
- **TLS 版本（仅与 TLS 传输模式一同使用）：**选择要使用的 TLS 版本。**v1.2** 和 **v1.3** 版本安全性高。**自动**选择系统可处理的高安全版本。
- **媒体加密（仅与 TLS 传输模式一同使用）：**选择 SIP 呼叫中媒体（音频和视频）的加密类型。
- **证书（仅与 TLS 传输模式一同使用）：**选择一个证书。
- **验证服务器证书（仅与 TLS 传输模式一同使用）：**选中以验证该服务器证书。
- **辅助 SIP 服务器：**若在主 SIP 服务器上注册失败，如果您想让设备在一台辅助 SIP 服务器上注册，则打开。
- **SIP 安全：**选择使用安全会话初始协议 (SIPS)。SIPS 使用 TLS 传输模式来加密通信。
- **代理**
 - **+** **代理：**单击添加代理。
 - **优先排序：**如果您已添加两个或更多代理，请单击以对其进行优先排序。
 - **服务器地址：**输入 SIP 代理服务器的 IP 地址。
 - **用户名：**如果需要，输入 SIP 代理服务器的用户名。
 - **密码：**如果需要，输入 SIP 代理服务器的密码。

- **视频** ⓘ
 - **视点区域**：选择用于视频呼叫的视点区域。如果您选择无，则使用原始视图。
 - **分辨率**：选择用于视频呼叫的分辨率。该分辨率会影响所需带宽。
 - **帧率**：选择视频通话的每秒帧数。帧速会影响所需带宽。
 - **H.264 配置文件**：选择用于视频通话的配置文件。

DTMF

+ **添加序列**：单击以创建新的双音多频（DTMF）序列。要创建通过按键激活的规则，请转到 **事件>规则**。

序列：输入字符以激活规则。允许的字符：0–9、A–D、# 和 *。

描述：输入以序列触发操作的描述。

账户：选择将使用 DTMF 序列的帐户。如果选择**点对点**，则各账户将共享相同的 DTMF 序列。

协议

选择要用于每个帐户的协议。各点对点帐户共享相同的协议设置。

使用 RTP (RFC2833)：打开以允许 RTP 数据包中的双音多频 (DTMF) 信令、其他音调信号和电话事件。

使用 SIP INFO (RFC2976)：打开以使 SIP 协议中包含 INFO 方法。INFO 方法会添加通常与会话有关的可选应用程序层信息。

测试呼叫

SIP 账户：选择要从中进行测试呼叫的账户。

SIP 地址：输入 SIP 地址，然后单击  **测试账户** 发起测试呼叫，验证账户是否正常工作。

访问列表

使用访问列表：开启以限制谁可以拨打设备电话。

策略：

- **允许**：选择此选项仅允许来自访问列表中源的传入呼叫。
- **阻止**：选择阻止来自访问列表中源的传入呼叫。

+ **Add source (添加源)**：单击可在访问列表中创建新条目。

SIP 源：键入源的主叫方 ID 或 SIP 服务器地址。

呼叫

呼叫按钮

使用呼叫按钮：打开以使用呼叫按钮。

呼叫期间的按钮功能：选择从设备开始呼叫后呼叫按钮的功能。

- **结束呼叫：**来访者在呼出期间按下呼叫按钮时，呼叫就会结束。使用此选项可让来访者随时结束呼叫。
- **呼叫结束前无功能：**来访者在呼出期间按下呼叫按钮时，什么都不会发生。使用此选项可禁止来访者结束呼叫。
- **结束呼叫前的延迟：**来访者开始呼叫后，在**延迟**中设置的时间内按下呼叫按钮，什么都不会发生。如果延迟时间已过，按下呼叫按钮即可结束呼叫。使用此选项可防止来访者因重复按键而意外结束呼叫。
 - **延迟（秒）：**输入第二次按呼叫按钮结束呼叫前必须经过的时间。

备用光：在呼叫按钮周围为内置光选择一个选项。

- **Auto（自动）** ：设备根据周围光线的情况打开和关闭内置光。
- **On（打开）：**当设备处于备用模式下时，内置灯始终处于打开状态。
- **关闭：**当设备处于备用模式下时，内置灯始终处于关闭状态。

接收者：选择或创建一个或多个要呼叫的联系人，以便在某人按下呼叫按钮时进行呼叫。如果您添加多个接收者，则呼叫将同时对各接收者进行。SIP 呼叫接收者数量上限为 6，而 VM 呼叫接收者数量不限。

备用：如果没有接收者回复，则从列表中添加备用联系人。

概述

音频

注意

- 所选音频剪辑仅在在进行呼叫时播放。
- 如果在正在进行的呼叫过程中更改音频剪辑或增益，则直到下一个呼叫才会生效。

铃声：选择要在有人呼叫设备时播放的音频剪辑。使用滑块调整增益。

回铃音：选择要在有人从设备呼叫时播放的音频剪辑。使用滑块调整增益。

VMS 呼叫

VMS 呼叫

Allow calls in the video management software (VMS)（允许在视频管理软件 (VMS) 中呼叫）：选择以允许从设备呼叫VMS。即使关闭SIP，您也可以进行VMS呼叫。

呼叫超时：设置无人应答时尝试呼叫的持续时间上限。

分析

AXIS Object Analytics

开始：单击以开始 AXIS Object Analytics。应用将在后台运行，您可以根据应用的当前设置为事件创建规则。

打开：单击以打开 AXIS Object Analytics。应用程序将在新的浏览器标签页中打开，您可以在其中配置其设置。

- **未安装：**AXIS Object Analytics 未在此设备上安装。将 AXIS OS 升级到新版本以获取新版本的应用。

元数据可视化

摄像机可侦测移动物体，并根据物体类型对其进行分类。在视图中，已分类对象周围有一个彩色边界框以及为其分配的 ID。

ID（标识号）：已识别对象和类型的唯一标识号。此数字同时显示在列表和视图中。

类型：将移动对象分类为人、人脸、汽车、公共汽车、卡车、自行车或牌照。边界框的颜色取决于类型分类。

置信度：该条形表示对象类型分类的置信度。

元数据配置

实时流协议 (RTSP) 元数据生成器

列出流传输元数据的应用程序及其使用的通道。

注意

这些设置适用于使用 ONVIF XML 的 RTSP 元数据流。在此更改不会影响元数据可视化页面。

生成器：生成元数据的应用程序。应用程序下方是应用程序从设备流传输的元数据类型的列表。

通道：应用程序使用的通道。选择以启用元数据流。出于兼容性或资源管理原因取消选择。

读卡器

连接

外部读卡器（输入）

使用外部 OSDP 读卡器：打开以将设备与外部读卡器配合使用。将读卡器连接至读卡器连接器（IO1、IO2、12V 和 GND）。

状态：

- **已连接：**设备已连接到活动的外部读卡器。
- **正在连接：**设备正在尝试连接到外部读卡器。
- **Not connected（未连接）：**OSDP 已关闭。

读卡器协议

阅读器协议类型：选择要用于读卡器功能的协议。

- **VAPIX 阅读器：**仅可与 Axis 门禁控制器一起使用。
 - **协议：**选择 HTTPS 或 HTTP。
 - **门禁控制器地址：**输入门禁控制器的 IP 地址。
 - **用户名：**输入门禁控制器的用户名。
 - **密码：**输入门禁控制器的密码。
 - **连接：**单击以连接到门禁控制器。
 - **选择读取器：**选择适当门的入口阅读器。
- **OSDP：**
 - **OSDP 地址：**输入OSDP读卡器地址。0是默认地址，也是单读卡器最常用的地址。
- **Wiegand 
 - **寻呼机：**打开以激活寻呼机输入。
 - **寻呼机输入：**选择用于寻呼机的 I/O 端口。
 - **LED 控制输入：**选择在设备上用于控制 LED 反馈的输入/输出端口数量。
 - **Input for LED1/LED2 (LED1/LED2的输入)：**选择LED输入要使用的I/O端口。
 - **空闲的颜色：**如果没有用于控制 LED 的 I/O 端口，则您可以选择要在读卡器指示器带上显示的静态颜色。
 - **Color for state low/high (低/高状态的颜色)：**如果一个I/O端口用于LED控制，请分别选择显示低和高状态的颜色。
 - **空闲颜色/LED1 颜色/LED2 颜色/LED1 + LED2 颜色：**如果两个 I/O 端口用于 LED 控制，请分别为空闲、LED1、LED2 和 LED1 + LED2 选择要显示的颜色。
 - **按键格式：**选择将 PIN 发送至访问控制单元时如何格式化。
 - **FourBit：**个人识别码 1234 被编码为 0x1 0x2 0x3 0x4 发送。这是默认和最常见的行为。
 - **EightBitZeroPadded：**个人识别码 1234 被编码为 0x01 0x02 0x03 0x04 发送。
 - **EightBitInvertPadded：**个人识别码 1234 被编码为 0xE1 0xD2 0xC3 0xB4 发送。
 - **Wiegand26：**PIN以Wiegand26格式编码，具有8位功能码和一个16位的识别码。
 - **Wiegand34PIN**以Wiegand34格式编码，具有16位功能码和一个16位的识别码。
 - **Wiegand37：**PIN采用35位识别码的Wiegand37格式 (H10302) 编码。
 - **Wiegand37FacilityCode：**PIN以Wiegand37格式 (H10304) 编码，具有16位功能码和一个19位的识别码。
 - **设施代码：**输入要发送的设施代码。此选项仅适用于某些按键格式。**

输出格式

选择数据格式：选择将卡数据发送到访问控制单元的格式。

- **原始：**按原样传输卡数据。
- **Wiegand26：**以Wiegand26格式编码卡数据，具有8位功能码和一个16位的识别码。
- **Wiegand34：**以Wiegand34格式编码卡数据，具有16位功能码和一个16位的识别码。
- **Wiegand37：**使用35位识别码Wiegand37格式（H10302）对卡数据进行编码。
- **Wiegand37FacilityCode：**以Wiegand37格式（H10304）编码卡数据，具有16位功能码和一个19位的识别码。
- **自定义：**定义您自己的格式。

设施代码覆盖模式：选择用于覆盖设施代码的选项。

- **自动：**不覆盖设施代码，并从输入数据自动侦测创建设施代码。使用卡的原始设施代码，或放弃其超出卡号的多余位。
- **可选：**使用输入数据中的设施代码，或使用配置的可选值重写。
- **覆盖：**始终以指定的设施代码覆盖。

PIN

PIN 设置必须与在访问控制单元中配置的设置相匹配。

Length (0–32) (长度 (0–32))：输入PIN的位数。如果用户在使用读卡器时不需要使用PIN，请将长度设置为0。

Timeout (seconds, 3–50) (超时 (秒, 3–50))：输入在未收到PIN时设备返回到空闲模式之前需要的秒数。

入口列表

通过入口列表，您可以将设备设置为允许凭证持有者使用其卡或 PIN 执行不同的操作，例如开门。将凭证本地存储在设备中。您还可以将此功能与外部门禁控制器结合使用。

凭证持有者

使用入口列表：打开以使用入口列表功能。

使用已连接的门禁控制器：如果设备已连接到门禁控制器，请打开。如果有人提供的凭证在入口列表中不存在，我们会将请求发送到已连接的门禁控制器。我们不发送入口列表中可用的凭证。

添加凭证持有者：单击以添加新的凭证持有者。

名字：输入名字。

姓氏：输入姓氏。

凭证类型：

- **PIN：**
 - **PIN：**输入唯一 PIN 码或单击**生成**自动创建一个。
- **卡：**
 - **UID：**输入卡的UID和位长度，或单击**Get latest（获取上一次）**以从上一次刷卡中获取数据。

事件条件：选择凭证持有者使用其凭证时要触发的一个或多个条件。要设置生成的操作，请转到**系统>事件**并使用您在此处选择的相同条件创建规则。

生效日期：选择当前设备时间以立即激活凭证。清除以指定何时激活凭证。

有效期至：

- **没有结束日期：**凭证无限期有效。
- **结束日期：**指定凭证无效的日期和时间。
- **播放次数：**指定凭证持有者可以使用凭证的次数。字段中的值会随着凭证的使用而减小，以显示剩余的可用值。

备注：输入可选信息。

暂停：选择此选项可使凭证暂时无效。

事件日志

事件登录显示一个入口列表事件的列表。登录文件的最大大小为 2 MB，约等于 6000 个事件。

导出全部：单击可导出列表中的所有事件。如要仅导出子集，请选择您感兴趣的事件。事件会导出到 CSV 文件中。

过滤器：单击可显示特定时间范围内发生的事件。

：键入可在列表中搜索所有匹配内容。

音频

设备设置

输入：打开或关闭音频输入。显示输入类型。

输入类型 ：选择输入类型，例如，内部麦克风或线路输入。

电源类型 ：选择用于输入的电源类型。

应用更改 ：应用您的选择。

降噪：打开以通过消除背景噪音来提高音频质量。

消除回音 ：打开以在双向通信期间移除回声。

单独的增益控制 ：打开以单独调整不同输入类型的增益。

自动增益控制 ：打开以动态调整声音中的变化增益。

增益：使用滑块更改增益。单击麦克风图标可静音或取消静音。

输出：显示输出类型。

增益：使用滑块更改增益。单击扬声器图标可静音或取消静音。

自动音量控制 ：打开可使设备根据周围噪音等级自动动态调节增益。自动音量控制会影响所有音频输出，包括线路输出和电传线圈输出。

流

消除回音：打开以在双向通信期间移除回声。

音频剪辑

+ **添加片段**：添加新的音频剪辑。您可以使用 au、.mp3、opus、vorbis、.wav 文件。

 **播放音频片段。**

 **停止播放音频片段。**

⋮

上下文菜单包括：

- **重命名**：更改音频剪辑的名称。
- **创建链接**：创建一个 URL，并在使用时在设备上播放音频剪辑。指定音量和播放剪辑的次数。
- **下载**：将音频剪辑下载到您的电脑上。
- **删除**：从设备上删除音频剪辑。

录像

正在进行的录制内容：显示设备上全部正在进行的录制。

- 开始在设备上录制。



选择要保存到哪个存储设备。

- 停止在设备上录制。

触发的录制将在手动停止或设备关闭时结束。

连续录制将继续，直到手动停止。即使设备关闭，录制也会在设备再次启动时继续。



播放录制内容。



停止播放录制内容。



显示或隐藏有关录制内容的信息和选项。

设置导出范围：如果只想导出部分录制内容，输入时间跨度。请注意，如果您工作的时区与设备所在地的时区不同，时间跨度将基于设备所在的时区。

加密：选择此选项可为导出的录制文件设置密码。如果没有密码，将无法打开导出的文件。



单击以删除一个录制内容。

导出：导出全部或部分录制文件。



单击以过滤录制内容。

从：显示在某个时间点之后完成的录制内容。

到：显示在某个时间点之前的录制内容。

来源 ⓘ：显示基于源的录制内容。源是指传感器。

事件：显示基于事件的录制内容。

存储：显示基于存储类型的录制内容。

应用



添加应用：安装新应用。

查找更多应用：查找更多要安装的应用。您将被带到 Axis 应用程序的概览页面。



允许未签名的应用程序：启用允许安装未签名的应用。



查看 AXIS OS 和 ACAP 应用程序中的安全更新。

注意

如果同时运行多个应用，设备的性能可能会受到影响。

使用应用名称旁边的开关可启动或停止应用。

打开：访问应用的设置。可用的设置取决于应用。某些应用程序没有设置。



上下文菜单可包含以下一个或多个选项：

- **开源许可证：**查看有关应用中使用的开放源代码许可证的信息。
- **应用日志：**查看应用事件的日志。当您与支持人员联系时，日志很有用。
- **使用密钥激活许可证：**如果应用需要许可证，则需要激活它。如果您的设备没有互联网接入，请使用此选项。
如果您没有许可证密钥，请转到 axis.com/products/analytics。您需要许可证代码和安讯士产品序列号才能生成许可证密钥。
- **自动激活许可证：**如果应用需要许可证，则需要激活它。如果您的设备有互联网接入，请使用此选项。您需要许可证密钥来激活许可证。
- **停用许可证：**停用许可证以将其替换为其他许可证，例如，当您从试用许可证更改为完整许可证时。如果要停用许可证，您还会将其从设备中移除。
- **设置：**配置参数。
- **删除：**永久从设备中删除应用。如果不首先停用许可证，则许可证将保持活动状态。

系统

时间和位置

日期和时间

时间格式取决于网页浏览器的语言设置。

注意

我们建议您将设备的日期和时间与 NTP 服务器同步。

同步：选择设备日期和时间同步选项。

- **自动日期和时间（手动 NTP KE 服务器）：**与安全 NTP 密钥建立连接至 DHCP 服务器的服务器进行同步。
 - **手动 NTP KE 服务器：**输入一个或两个 NTP 服务器的 IP 地址。当您使用两台 NTP 服务器时，设备会根据两者的输入同步并调整其时间。
 - **上限 NTP 轮询时间：**选择设备在轮询 NTP 服务器以获取更新时间之前应等待的时间上限。
 - **NTP 轮询时间下限：**选择设备在轮询 NTP 服务器以获取更新时间之前应等待的时间下限。
- **自动日期和时间（使用 DHCP 的 NTP 服务器）：**与连接到 DHCP 服务器的 NTP 服务器同步。
 - **备用 NTP 服务器：**输入一个或两个备用服务器的 IP 地址。
 - **上限 NTP 轮询时间：**选择设备在轮询 NTP 服务器以获取更新时间之前应等待的时间上限。
 - **NTP 轮询时间下限：**选择设备在轮询 NTP 服务器以获取更新时间之前应等待的时间下限。
- **自动日期和时间（手动 NTP 服务器）：**与您选择的 NTP 服务器同步。
 - **手动 NTP 服务器：**输入一个或两个 NTP 服务器的 IP 地址。当您使用两台 NTP 服务器时，设备会根据两者的输入同步并调整其时间。
 - **上限 NTP 轮询时间：**选择设备在轮询 NTP 服务器以获取更新时间之前应等待的时间上限。
 - **NTP 轮询时间下限：**选择设备在轮询 NTP 服务器以获取更新时间之前应等待的时间下限。
- **自定义日期和时间：**手动设置日期和时间。单击**从系统获取**以从计算机或移动设备获取日期和时间设置。

时区：选择要使用的时区。时间将自动调整为夏令时和标准时间。

- **DHCP：**采用 DHCP 服务器的时区。设备必须连接到 DHCP 服务器，然后才能选择此选项。
- **手动：**从下拉列表中选择时区。

注意

系统在各录像、日志和系统设置中使用日期和时间设置。

设备位置

输入设备所在的位置。视频管理系统可以使用此信息来在地图上放置设备。

- **格式化：**选择输入设备纬度和经度时使用的格式。
- **纬度：**正值代表赤道以北。
- **经度：**正值代表本初子午线以东。
- **朝向：**输入设备朝向的指南针方向。0 代表正北。
- **标签：**为您的设备输入一个描述性名称。
- **保存：**单击此处，以保存您的设备位置。

配置检查

交互式设备图像：单击图像中的按钮模拟实际按键。这允许您尝试配置或排除硬件故障，而无需物理访问设备。

Latest credentials (上次凭证) ：显示有关上次注册的凭证的信息。

  显示新的凭证数据。

  上下文菜单包括：

- **Reverse UID (翻转UID)：**反转UID的字节顺序。
- **Revert UID (恢复UID)：**将UID的字节顺序恢复为原始顺序。
- **复制到剪贴板：**复制 UID。

Check credentials (检查凭证) ：输入 UID 或 PIN 并提交以检查凭证。系统的响应方式与您在设备上使用凭证的方式相同。如果同时需要 UID 和 PIN，请先输入 UID。

网络

IPv4

自动分配 IPv4：选择此设置可让网络路由器自动分配设备的 IP 地址。我们建议大多数网络采用自动 IP (DHCP)。

IP 地址：为设备输入唯一的 IP 地址。在独立的网络中可随机分配静态 IP 地址，只要每个指定地址是唯一的。为避免冲突，建议在分配静态 IP 地址前联系网络管理员。

子网掩码：输入子网掩码，以定义局域网内的地址。局域网之外的地址都通过路由器。

路由器：输入默认路由器（网关）的 IP 地址用于连接已连接至不同的网络和网段的设备。

如果 DHCP 不可用，退回到静态 IP 地址：如果希望在 DHCP 不可用且无法自动分配 IP 地址时，添加要用作备用静态 IP 地址，请选择此项。

注意

如果 DHCP 不可用且设备使用备用静态地址，则静态地址配置范围有限。

IPv6

自动分配 IPv6：选择打开 IPv6 并让网络路由器自动分配设备的 IP 地址。

主机名

自动分配主机名称：选择让网络路由器自动分配设备的主机名称。

主机名称：手动输入主机名称，作为访问设备的另一种方式。服务器报告和系统日志使用主机名。允许的字符是 A-Z, a-z, 0-9 和 -。

启动动态 DNS 更新：允许设备在 IP 地址更改时自动更新其域名服务器记录。

注册 DNS 名称：输入指向设备 IP 地址的唯一域名。允许的字符是 A-Z, a-z, 0-9 和 -。

TTL：生存时间 (TTL) 设置 DNS 记录在需要更新之前保持有效的时长。

DNS 服务器

自动分配 (DNS):选择以让 DHCP 网络路由器自动向设备分配搜索域和 DNS 服务器地址。我们建议大多数网络采用自动 DNS (DHCP)。

搜索域:当您使用不完全合格的主机名时,请单击**添加搜索域**并输入一个域,以在其中搜索设备使用的主机名称。

DNS 服务器:单击**添加 DNS 服务器**并输入 DNS 服务器的 IP 地址。此服务器提供主机名到网络上 IP 地址的转换。

HTTP 和 HTTPS

HTTPS 是一种协议,可为来自用户的页面请求和网络服务器返回的页面提供加密。加密的信息交换使用 HTTPS 证书进行管理,这保证了服务器的真实性。

要在设备上使用 HTTPS,必须安装 HTTPS 证书。转到**系统 > 安全**以创建和安装证书。

允许访问浏览:选择是否允许用户通过 HTTP、HTTPS 或同时通过 HTTP 和 HTTPS 协议连接到设备。

注意

如果通过 HTTPS 查看加密的网页,则可能会出现性能下降,尤其是您首次请求页面时。

HTTP 端口:输入要使用的 HTTP 端口。设备允许端口 80 或范围 1024–65535 中的端口。如果您以管理员身份登录,则您还可以输入 1–1023 范围内的端口。如果您使用此范围内的端口,您将收到警告。

HTTPS 端口:输入要使用的 HTTPS 端口。设备允许端口 443 或范围 1024–65535 中的端口。如果您以管理员身份登录,则您还可以输入 1–1023 范围内的端口。如果您使用此范围内的端口,您将收到警告。

证书:选择要为设备启用 HTTPS 的证书。

网络发现协议

Bonjour®:打开允许在网络中执行自动发现。

Bonjour 名称:键入要在网络中显示的昵称。默认名称为设备名加 MAC 地址。

UPnP®:打开允许在网络中执行自动发现。

UPnP 名称:键入要在网络中显示的昵称。默认名称为设备名加 MAC 地址。

WS 发现:打开允许在网络中执行自动发现。

LLDP 和 CDP:打开允许在网络中执行自动发现。关闭 LLDP 和 CDP 可能会影响 PoE 电源协商。若要解决 PoE 电源协商问题,请仅为硬件 PoE 电源协商配置 PoE 交换机。

全局代理

Http proxy (Http代理)：根据允许的格式指定全局代理主机或IP地址。

Https proxy (Https代理)：根据允许的格式指定全局代理主机或IP地址。

http和https代理支持的格式：

- http(s)://host:port
- http(s)://user@host:port
- http(s)://user:pass@host:port

注意

重启设备以应用全局代理设置。

No proxy (无代理)：使用**No proxy (无代理)**以绕过全局代理。输入列表中的一个选项，或输入多个选项，以逗号分隔：

- 留空
- 指定IP地址
- 以CIDR格式指定IP地址
- 指定域名，例如：www.<域名>.com
- 指定特定域中的所有子域，例如.<域名>.com

一键云连接

一键式云连接 (O3C) 与 O3C 服务结合使用，可从不同位置通过互联网安全地访问实时视频和录制的视频。有关详细信息，请参见 axis.com/end-to-end-solutions/hosted-services。

允许 O3C：

- **一键式**：这是默认选项。要连接至 O3C，请按下设备上的控制按钮。根据设备型号，按下并松开或按住不放，直到状态 LED 闪烁。在 24 小时内注册设备使其连接 O3C 服务，**始终**启用并保持连接。如果不注册，设备将断开与 O3C 的连接。
- **总是**：设备将不断尝试通过互联网连接到 O3C 服务。一旦注册设备，它就会保持连接。如果无法够到控制按钮，则使用此选项。
- **无**：断开 O3C 服务。

代理设置：如果需要，请输入代理设置以连接到代理服务器。

主机：输入代理服务器的地址。

端口：输入用于访问的端口数量。

登录和密码：如果需要，请输入代理服务器的用户名和密码。

身份验证方法：

- **基本**：此方法是 HTTP 兼容的身份验证方案。它的安全性不如**摘要**方法，因为它将用户名和密码发送到服务器。
- **摘要**：此方法一直在网络中传输加密的密码，因此更安全。
- **自动**：借助此选项，可使设备根据支持的方法自动选择身份验证方法。**摘要**方法优先于**基本**方法。

所有者身份验证密钥 (OAK)：单击**Get key (获取密码)**以获取所有者的身份验证密钥。只有在没有防火墙或代理的情况下设备连接到互联网时，才可能发生这种情况。

SNMP

简单网络管理协议 (SNMP) 允许远程管理网络设备。

SNMP:选择要使用的 SNMP 版本。

- **v1 和 v2c:**
 - **读取团体:** 输入可只读访问支持的 SNMP 对象的团体名称。默认值为**公共**。
 - **编写社区:** 输入可读取或写入访问支持全部的 SNMP 物体（只读物体除外）的团体名称。默认值为**写入**。
 - **激活陷阱:** 打开以激活陷阱报告。该设备使用陷阱发送重要事件或更改状态的消息到管理系统。在网页界面中，您可以设置 SNMP v1 和 v2c 的陷阱。如果您更改为 SNMP v3 或关闭 SNMP，陷阱将自动关闭。如果使用 SNMP v3，则可通过 SNMP v3 管理应用程序设置陷阱。
 - **陷阱地址:** 输入管理服务器的 IP 地址或主机名。
 - **陷阱团体:** 输入设备发送陷阱消息到管理系统时要使用的团体。
 - **陷阱:**
 - **冷启动:** 设备启动时发送陷阱消息。
 - **连接:** 链接自下而上发生变更时，发送陷阱消息。
 - **断开连接:** 链接自上而下发生变更时，发送陷阱消息。
 - **身份验证失败:** 验证尝试失败时，发送陷阱消息。

注意

打开 SNMP v1 和 v2c 陷阱时，将启用 Axis Video MIB 陷阱。有关更多信息，请参见 *AXIS OS Portal > SNMP*。

- **v3:**SNMP v3 是一个提供加密和安全密码的更安全版本。若要使用 SNMP v3，我们建议激活 HTTPS，因为密码将通过 HTTPS 发送。这还会防止未授权方访问未加密的 SNMP v1 及 v2c 陷阱。如果使用 SNMP v3，则可通过 SNMP v3 管理应用程序设置陷阱。
 - **“initial” 账户密码:**输入名为'initial'的帐户的 SNMP 密码。尽管可在不激活 HTTPS 的情况下发送密码，但我们不建议这样做。SNMP v3 密码仅可设置一次，并且推荐仅在 HTTPS 启用时。一旦设置了密码，密码字段将不再显示。要重新设置密码，则设备必须重置为出厂默认设置。

安全

认证

证书用于对网络上的设备进行身份验证。该设备支持两种类型的证书：

- **客户端/服务器证书**
客户端/服务器证书用于验证设备身份，可以是自签名证书，也可以是由证书颁发机构颁发的证书。自签名证书提供有限的保护，可在获得 CA 颁发的证书之前使用。
- **CA 证书**
您可以使用 CA 证书来验证对等证书，例如，在设备连接到受 IEEE 802.1X 保护的的网络时，用于验证身份验证服务器的身份。设备具有几个预装的 CA 证书。

支持以下格式：

- 证书格式：.PEM、.CER、.PFX
- 私钥格式：PKCS#1 和 PKCS#12

重要

如果将设备重置为出厂默认设置，将删除各证书。预安装的 CA 证书将重新安装。



添加证书：单击添加证书。分步指南打开。

- **更多** ：显示更多要填充或选择的栏。
- **安全密钥库：**选择使用可信执行环境 (SoC TEE)、安全元件或可信平台模块 2.0 来安全存储私钥。有关选择哪个安全密钥库的更多信息，请转到 help.axis.com/axis-os#cryptographic-support。
- **密钥类型：**从下拉列表中选择默认或其他加密算法以保护证书。



上下文菜单包括：

- **证书信息：**查看已安装证书的属性。
- **删除证书：**删除证书。
- **创建证书签名请求：**创建证书签名请求，发送给注册机构以申请数字身份证书。

安全密钥库 ：

- **可信执行环境 (SoC TEE)：**选择使用 SoC TEE 来实现安全密钥库。
- **安全元件 (CC EAL6+)：**选择使用安全元件来实现安全密钥库。
- **受信任的平台模块 2.0 (CC EAL4+、FIPS 140-2 2 级)：**安全密钥库选择使用 TPM 2.0。

网络访问控制和加密

IEEE 802.1x

IEEE 802.1x 是针对基于端口的网络管理控制一种 IEEE 标准，可提供有线和无线网络设备的安全身份验证。IEEE 802.1x 基于 EAP（可扩展身份验证协议）。

要访问受 IEEE 802.1x 保护的网路，网络设备必须对其自身进行身份验证。该身份验证由身份验证服务器执行，通常是 RADIUS 服务器（例如，FreeRADIUS 和 Microsoft Internet Authentication Server）。

IEEE 802.1AE MACsec

IEEE 802.1AE MACsec 是一项针对媒体访问控制（MAC）安全性的 IEEE 标准，它定义了媒体访问独立协议无连接数据的机密性和完整性。

认证

在不配置 CA 证书时，这意味将禁用服务器证书验证，不管网路是否连接，设备都将尝试进行自我身份验证。

在使用证书时，在安讯士的实施中，设备和身份验证服务器通过使用 EAP-TLS（可扩展身份验证协议 - 传输层安全）的数字证书对其自身进行身份验证。

要允许设备访问通过证书保护的网路，您必须在设备上安装已签名的客户端证书。

身份验证方法：选择用于身份验证的 EAP 类型。

客户端证书：选择客户端证书以使用 IEEE 802.1x。使用证书可验证身份验证服务器的身份。

CA 证书：选择一个 CA 证书来验证身份验证服务器的身份。未选择证书无时，无论连接到哪个网路，设备都将尝试进行自我身份验证。

EAP 身份：输入与客户端的证书关联的用户标识。

EAPOL 版本：选择网络交换机中使用的 EAPOL 版本。

使用 IEEE 802.1x:选择以使用 IEEE 802.1x 协议。

仅当您使用 IEEE 802.1x PEAP-MSCHAPv2 作为身份验证方法时，这些设置才可用：

- **密码：**输入您的用户标识密码。
- **Peap 版本：**选择网络交换机中使用的 Peap 版本。
- **标签：**选择 1 使用客户端 EAP 加密；选择 2 使用客户端 PEAP 加密。选择使用 Peap 版本 1 时网络交换机使用的标签。

仅当您使用 IEEE 802.1ae MACsec（静态 CAK/预共享密钥）作为身份验证方法时，这些设置才可用：

- **密钥协议连接关联密钥名称：**输入连接关联名称 (CKN)。必须为 2 到 64（可被 2 整除）个十六进制字符。必须在连接关联中手动配置 CKN，而且链路两端的 CKN 必须匹配，才能初始启用 MACsec。
- **密钥协议连接关联密钥：**输入连接关联密钥 (CAK)。其长度应为 32 或 64 个十六进制字符。必须在连接关联中手动配置 CAK，而且链路两端的 CAK 必须匹配，才能初始启用 MACsec。

防止蛮力攻击

正在阻止:开启以阻止强力攻击。强力攻击使用试验和错误来猜测登录信息或加密密钥。

阻止期:输入阻止暴力攻击的秒数。

阻止条件:输入在阻止开始之前每秒允许的身份验证失败次数。您可设置页面级和设备级上所允许的失败次数。

防火墙

Firewall (防火墙) : 打开此项可激活防火墙。

默认策略 : 选择希望防火墙如何处理规则未涵盖的连接请求。

- **ACCEPT (接受)** : 允许与设备的各连接。默认情况下设置此选项。
- **DROP (丢弃)** : 阻止与设备的各连接。

要对默认策略进行例外处理, 您可以创建允许或阻止从特定地址、协议和端口连接到设备的规则。

+ New rule (新规则) : 单击以创建规则。

Rule type (规则类型) :

- **FILTER (筛选)** : 选择允许或阻止符合规则定义条件的设备建立连接。
 - **策略** : 选择Accept (接受) 或Drop (丢弃) 防火墙规则。
 - **IP range (IP 范围)** : 选择此项可指定允许或阻止的地址范围。在Start (起始) 和End (结束) 中使用IPv4/IPv6 格式。
 - **IP 地址** : 输入要允许或阻止的地址。使用IPv4/IPv6 或CIDR 格式。
 - **协议** : 选择要允许或阻止的网络协议 (TCP、UDP 或两者)。如果选择协议, 还必须指定端口。
 - **MAC** : 输入要允许或阻止的设备的MAC 地址。
 - **Port range (端口范围)** : 选择此项可指定允许或阻止的端口范围。将其添加到Start (起始) 和End (结束) 中。
 - **端口** : 输入要允许或阻止的端口号。端口号必须在1 和65535 之间。
 - **Traffic type (流量类型)** : 选择要允许或阻止的流量类型。
 - **UNICAST (单播)** : 从单一发送方至单一接收方的流量。
 - **BROADCAST (广播)** : 从单一发送方至网络全部设备的流量。
 - **MULTICAST (组播)** : 从一个或多个发送方至一个或多个接收方的流量。
- **LIMIT (限制)** : 选择以接受符合规则定义条件的设备建立连接, 但应用限制以减少过多流量。
 - **IP range (IP 范围)** : 选择此项可指定允许或阻止的地址范围。在Start (起始) 和End (结束) 中使用IPv4/IPv6 格式。
 - **IP 地址** : 输入要允许或阻止的地址。使用IPv4/IPv6 或CIDR 格式。
 - **协议** : 选择要允许或阻止的网络协议 (TCP、UDP 或两者)。如果选择协议, 还必须指定端口。
 - **MAC** : 输入要允许或阻止的设备的MAC 地址。
 - **Port range (端口范围)** : 选择此项可指定允许或阻止的端口范围。将其添加到Start (起始) 和End (结束) 中。
 - **端口** : 输入要允许或阻止的端口号。端口号必须在1 和65535 之间。
 - **Unit (单位)** : 选择允许或阻止的连接类型。
 - **Period (时期)** : 选择与Amount (数量) 相关的时间段。
 - **Amount (数量)** : 设置在所设定Period (时期) 内允许设备连接的最大次数。上限为65535 次。
 - **Burst (突发)** : 在设定的Period (时期) 内, 输入允许单次超过设定Amount (数量) 的连接数。达到此数值后, 后续连接将被限制为设定时期内的设定数量。
 - **Traffic type (流量类型)** : 选择要允许或阻止的流量类型。
 - **UNICAST (单播)** : 从单一发送方至单一接收方的流量。
 - **BROADCAST (广播)** : 从单一发送方至网络全部设备的流量。
 - **MULTICAST (组播)** : 从一个或多个发送方至一个或多个接收方的流量。

Test rules (测试规则) : 单击此项可测试已定义的规则。

- **Test time in seconds (测试时间 (秒))**：设置测试规则的时间限制。
- **还原**：在测试规则之前，单击此项可将防火墙还原到之前的状态。
- **Apply rules (应用规则)**：单击以激活规则，无需测试。不建议您这样操作。

自定义签名的 AXIS OS 证书

要在设备上安装来自 Axis 的测试软件或其他自定义软件，您需要自定义签名的 AXIS OS 证书。证书验证软件是否由设备权利人和 Axis 批准。软件只能在由其单一序列号和芯片 ID 标识的特定设备上运行。只有安讯士可以创建自定义签名 AXIS OS 证书，因为安讯士持有对其进行签名的密钥。

安装：单击安装以安装证书。在安装软件之前，您需要安装证书。

⋮

上下文菜单包括：

- **删除证书**：删除证书。

账户

账户



添加帐户：单击以添加新账户。您可以添加多达 100 个账户。

帐户：输入唯一的账户名。

新密码：输入账户的密码。密码必须为 1 到 64 个字符长。密码仅允许包含可打印的 ASCII 字符（代码 32–126），如字母、数字、标点符号和某些符号。

确认密码：再次输入同一密码。

优先权：

- **管理员**：可完全访问全部设置。管理员也可以添加、更新和删除其他账户。
- **操作员**：有权访问全部设置，以下各项除外：
 - 全部系统设置。
- **观看者**：有权访问：
 - 观看并拍摄视频流的快照。
 - 观看和导出录音。
 - 水平转动、垂直转动和变焦；使用PTZ账户权限。

⋮

上下文菜单包括：

更新账户：编辑账户的属性。

删除账户：删除账户。无法删除根账户。

匿名访问

允许匿名浏览：打开以允许其他人以查看者的身份访问设备，而无需登录账户。

允许匿名PTZ操作 ：打开允许匿名用户平移、倾斜和缩放图像。

SSH 账户

 **添加SSH账户：**单击以添加新 SSH 账户。

- **启用 SSH：**打开以使用 SSH 服务。

帐户：输入唯一的账户名。

新密码：输入账户的密码。密码必须为 1 到 64 个字符长。密码仅允许包含可打印的 ASCII 字符（代码 32–126），如字母、数字、标点符号和某些符号。

确认密码：再次输入同一密码。

注释：输入注释（可选）。

⋮ 上下文菜单包括：

更新 SSH 账户：编辑账户的属性。

删除 SSH 账户：删除账户。无法删除根账户。

虚拟主机

 **添加虚拟主机：**单击以添加新的虚拟主机。

已启用：选择以使用此虚拟主机。

服务器名称：输入服务器的名称。仅使用数字 0–9、字母 A–Z 和连字符 (-)。

端口：输入服务器连接到的端口。

类型：选择要使用的身份验证类型。在**基本**、**摘要**和**打开 ID**之间选择。

⋮ 上下文菜单包括：

- **更新：**更新虚拟主机。
- **删除：**删除虚拟主机。

已禁用：服务器已禁用。

客户端凭证授予配置

管理员声明：输入管理员角色的值。

Verification URI（身份验证 URI）：输入 API 端点身份验证的网页链接。

操作员声明：输入操作员角色的值。

需要声明：输入令牌中应包含的数据。

浏览者声明：输入浏览者角色的值。

保存：单击以保存值。

OpenID 配置

重要

如果无法使用 OpenID 登录，请使用配置 OpenID 登录时使用的摘要或基本凭证。

客户端 ID: 输入 OpenID 用户名。

外发代理: 输入 OpenID 连接的代理地址以使用代理服务器。

管理员声明: 输入管理员角色的值。

提供商 URL: 输入 API 端点身份验证的网页链接。格式应为 https://[insert URL]/.well-known/openid-configuration

操作员声明: 输入操作员角色的值。

需要声明: 输入令牌中应包含的数据。

浏览者声明: 输入浏览者角色的值。

远程用户: 输入一个值以标识远程用户。这有助于在设备的网页界面中显示当前用户。

范围: 可以是令牌一部分的可选作用域。

客户端密码: 输入 OpenID 密码

保存: 单击以保存 OpenID 值。

启用 OpenID: 打开以关闭当前连接并允许来自提供商 URL 的设备身份验证。

事件

规则

规则定义产品执行操作触发的条件。该列表显示产品中当前配置的全部规则。

注意

您可以创建多达 256 个响应规则。



添加规则: 创建一个规则。

名称: 为规则输入一个名称。

响应之间的等待时间: 输入必须在规则激活之间传输的时间下限 (hh; mm; ss)。如果规则是由夜间模式条件激活, 以避免日出和日落期间发生的小的光线变化会重复激活规则, 此功能将很有用。

条件: 从列表中选择条件。设施要执行响应必须满足的条件。如果定义了多个条件, 则必须满足全部条件才能触发响应。有关特定条件的信息, 请参见 *开始使用事件规则*。

使用此条件作为触发器: 选择以将此首个条件作为开始触发器。这意味着一旦规则被激活, 不管首个条件的状态如何, 只要其他条件都将保持有效, 它将一直保持活动状态。如果未选择此选项, 规则将仅在全部条件被满足时即处于活动状态。

反转此条件: 如果希望条件与所选内容相反, 请选择此选项。



添加条件: 单击以添加附加条件。

响应: 从列表中选择响应, 然后输入其所需的信息。有关特定响应的信息, 请参见 *开始使用事件规则*。

接收者

您可以设置设备以通知收件人有关事件或发送文件的信息。

注意

如果将设备设置为使用 FTP 或 SFTP，请不要更改或删除添加到文件名中的唯一序列号。如果这样做，每个事件只能发送一副图像。

该列表显示产品中当前配置的全部收件人以及有关其配置的信息。

注意

您可以创建多达 20 个接收者。



添加接收者：单击以添加接收者。

名称：为接收者输入一个名称。

类型：从列表中选择：

- **FTP** 
 - **主机：**输入服务器的 IP 地址或主机名。如果输入主机名，请确保在**系统 > 网络 > IPv4 和 IPv6** 下指定 DNS 服务器。
 - **端口：**输入 FTP 服务器使用的端口号。默认为 21。
 - **文件夹：**输入要存储文件的目录路径。如果 FTP 服务器上不存在此目录，则上传文件时将出现错误消息。
 - **用户名：**输入登录用户名。
 - **密码：**输入登录密码。
 - **使用临时文件名：**选择以临时自动生成的文件名上传文件。上传完成时，这些文件将重命名为所需的名称。如果上传中止/中断，您不会获得损坏的文件。但是，您仍然可能会获得临时文件。这样您就知道带有所需名称的文件都是正确的。
 - **使用被动 FTP：**正常情况下，产品只需向目标 FTP 服务器发送请求便可打开数据连接。设施将主动启动 FTP 控制以及与目标服务器的数据连接。如果设施和目标 FTP 服务器之间存在防火墙，通常需要执行此操作。
- **HTTP**
 - **URL：**输入 HTTP 服务器的网络地址以及处理请求的脚本。例如：http://192.168.254.10/cgi-bin/notify.cgi。
 - **用户名：**输入登录用户名。
 - **密码：**输入登录密码。
 - **代理：**如果必须通过代理服务器连接到 HTTPS 服务器，请打开并输入所需信息。
- **HTTPS**
 - **URL：**输入 HTTPS 服务器的网络地址以及处理请求的脚本。例如：https://192.168.254.10/cgi-bin/notify.cgi。
 - **验证服务器证书：**选中以验证由 HTTPS 服务器创建的证书。
 - **用户名：**输入登录用户名。
 - **密码：**输入登录密码。
 - **代理：**如果必须通过代理服务器连接到 HTTPS 服务器，请打开并输入所需信息。
- **网络存储** 

您可添加 NAS（网络附加存储）等网络存储，并将其用作存储文件的接受方。这些文件以 Matroska (MKV) 文件格式保存。

 - **主机：**输入网络存储的 IP 地址或主机名。
 - **共享：**在主机上输入共享的名称。
 - **文件夹：**输入要存储文件的目录路径。
 - **用户名：**输入登录用户名。
 - **密码：**输入登录密码。
- **SFTP** 
 - **主机：**输入服务器的 IP 地址或主机名。如果输入主机名，请确保在**系统 > 网络 > IPv4 和 IPv6** 下指定 DNS 服务器。
 - **端口：**输入 SFTP 服务器使用的端口号。默认为 22。

- **文件夹：**输入要存储文件的目录路径。如果 SFTP 服务器上不存在此目录，则上传文件时将出现错误消息。
 - **用户名：**输入登录用户名。
 - **密码：**输入登录密码。
 - **SSH 主机公共密钥类型 (MD5)：**输入远程主机的公共密钥（32 位十六进制的数字串）指纹。SFTP 客户端通过 RSA、DSA、ECDSA 和 ED25519 主机密钥类型支持 SFTP 服务器使用 SSH-2 协议。在协商期间，RSA 是理想方法，然后是 ECDSA、ED25519 和 DSA。要确保输入您的 SFTP 服务器使用的正确 MD5 主机密钥。虽然安讯士设备同时支持 MD5 和 SHA-256 哈希密钥，但我们建议使用 SHA-256，因为安全性比 MD5 更安全。有关如何配置带安讯士设备的 SFTP 服务器的详细信息，请转到 *AXIS OS Portal*。
 - **SSH 主机公共密钥类型 (SHA256)：**输入远程主机的公共密钥（43 位 Base64 的编码字符串）指纹。SFTP 客户端通过 RSA、DSA、ECDSA 和 ED25519 主机密钥类型支持 SFTP 服务器使用 SSH-2 协议。在协商期间，RSA 是理想方法，然后是 ECDSA、ED25519 和 DSA。要确保输入您的 SFTP 服务器使用的正确 MD5 主机密钥。虽然安讯士设备同时支持 MD5 和 SHA-256 哈希密钥，但我们建议使用 SHA-256，因为安全性比 MD5 更安全。有关如何配置带安讯士设备的 SFTP 服务器的详细信息，请转到 *AXIS OS Portal*。
 - **使用临时文件名：**选择以临时自动生成的文件名上传文件。上传完成时，这些文件将重命名为所需的名称。如果上传中止或中断，您不会获得损坏的文件。但是，您仍然可能会获得临时文件。这样，您就知道带有所需名称的文件都是正确的。
- **SIP或VMS**  :
SIP：选择进行 SIP 呼叫。
VMS：选择进行 VMS 呼叫。
 - **从 SIP 账户：**从列表中选择。
 - **至 SIP 地址：**输入 SIP 地址。
 - **测试：**单击以测试呼叫设置是否有效。
 - **电子邮件**
 - **发送电子邮件至：**键入电子邮件的收件地址。如果要输入多个地址，请用逗号将地址分隔开。
 - **从以下位置发送电子邮件：**输入发件服务器的电子邮件地址。
 - **用户名：**输入邮件服务器的用户名。如果电子邮件服务器不需要身份验证，请将此字段留空。
 - **密码：**输入邮件服务器的密码。如果电子邮件服务器不需要身份验证，请将此字段留空。
 - **电子邮件服务器 (SMTP)：**输入 SMTP 服务器的名称，例如，smtp.gmail.com 和 smtp.mail.yahoo.com。
 - **端口：**使用 0-65535 范围内的值输入 SMTP 服务器的端口号。默认值为 587。
 - **加密：**要使用加密，请选择 SSL 或 TLS。
 - **验证服务器证书：**如果使用加密，请选择验证设备的身份。证书可以是自签名的或由证书颁发机构 (CA) 颁发。
 - **POP 身份验证：**打开输入 POP 服务器的名称，例如，pop.gmail.com。

注意

某些电子邮件提供商拥有安全过滤器，可防止用户接收或查看大量附件、接收计划的电子邮件及类似内容。检查电子邮件提供商的安全策略，以避免您的电子邮件帐户被锁定或错过预期的电子邮件。

- **TCP**

- **主机：**输入服务器的 IP 地址或主机名。如果输入主机名，请确保在**系统 > 网络 > IPv4 和 IPv6** 下指定 DNS 服务器。
- **端口：**输入用于访问服务器的端口号。

测试：单击以测试设置。



上下文菜单包括：

查看接收者：单击可查看各收件人详细信息。

复制接收者：单击以复制收件人。当您进行复制时，您可以更改新的收件人。

删除接收者：单击以永久删除收件人。

时间计划表

时间表和脉冲可用作规则中的条件。该列表显示产品中当前配置的全部时间表和脉冲以及有关其配置的信息。



添加时间表：单击以创建时间表或脉冲。

手动触发器

可使用手动触发以手动触发规则。手动触发器可用于验证产品安装和配置期间的行为等。

MQTT

MQTT（消息队列遥测传输）是用于物联网（IoT）的标准消息协议。它旨在简化IoT集成，并在不同行业中使用，以较小的代码需求量和尽可能小的网络带宽远程连接设备。安讯士设备软件中的 MQTT 客户端可使设备中的数据和事件集成至非视频管理软件 (VMS) 系统的流程简化。

将设备设置为 MQTT 客户端。MQTT 通信基于两个实体、客户端和中间件。客户端可以发送和接收消息。代理负责客户端之间路由消息。

您可以在 *AXIS OS Knowledge Base* 中了解有关 MQTT 的更多信息。

ALPN

ALPN 是一种 TLS/SSL 扩展，允许在客户端和服务器之间的连接信号交换阶段中选择应用协议。这用于在使用其他协议（如 HTTP）的同一个端口上启用 MQTT 流量。在某些情况下，可能没有为 MQTT 通信打开专用端口。这种情况下的解决方案是使用 ALPN 来协商将 MQTT 用作标准端口上的应用协议（由防火墙允许）。

MQTT 客户端

连接：打开或关闭 MQTT 客户端。

状态：显示 MQTT 客户端的当前状态。

代理

主机：输入 MQTT 服务器的主机名或 IP 地址。

协议：选择要使用的协议。

端口：输入端口编号。

- 1883 是 TCP 的 MQTT 的默认值
- 8883 是 SSL 的 MQTT 的默认值
- 80 是 WebSocket 的 MQTT 的默认值
- 443 是 WebSocket Secure 的 MQTT 的默认值

ALPN 协议：输入 MQTT 代理供应商提供的 ALPN 协议名称。这仅适用于 SSL 的 MQTT 和 WebSocket Secure 的 MQTT。

用户名：输入客户将用于访问服务器的用户名。

密码：输入用户名的密码。

客户端 ID:输入客户端 ID。客户端连接到服务器时，客户端标识符发送给服务器。

清理会话:控制连接和断开时间的行为。选定时，状态信息将在连接及断开连接时被丢弃。

HTTP 代理：最大长度为 255 字节的 URL。如果您不想使用 HTTP 代理，则可以将该字段留空。

HTTPS 代理：最大长度为 255 字节的 URL。如果您不想使用 HTTPS 代理，则可以将该字段留空。

保持活动状态间隔:让客户端能够在无需等待长 TCP/IP 超时的情况下，侦测服务器何时停用。

超时：允许连接完成的时间间隔（以秒为单位）。默认值：60

设备主题前缀：在 MQTT 客户端选项卡上的连接消息和 LWT 消息中的主题默认值中使用，以及在 MQTT 发布选项卡上的发布条件中使用。

自动重新连接：指定客户端是否应在断开连接后自动重新连接。

连接消息

指定在建立连接时是否应发送消息。

发送消息:打开以发送消息。

使用默认设置:关闭以输入您自己的默认消息。

主题：输入默认消息的主题。

有效负载:输入默认消息的内容。

保留：选择以保留此主题的客户端状态

QoS:更改数据包流的 QoS 层。

最后证明消息

终止证明（LWT）允许客户端在连接到代理时提供证明及其凭据。如果客户端在某点后仓促断开连接（可能是因为电源失效），它可以让代理向其他客户端发送消息。此终止了证明消息与普通消息具有相同的形式，并通过相同的机制进行路由。

发送消息:打开以发送消息。

使用默认设置:关闭以输入您自己的默认消息。

主题: 输入默认消息的主题。

有效负载: 输入默认消息的内容。

保留: 选择以保留此主题的客户端状态

QoS: 更改数据包流的 QoS 层。

MQTT 出版

使用默认主题前缀: 选择以使用默认主题前缀，即在 **MQTT 客户端** 选项卡中的设备主题前缀的定义。

包括主题名称: 选择以包含描述 MQTT 主题中的条件的主题。

包括主题命名空间: 选择以将 ONVIF 主题命名空间包含在 MQTT 主题中。

包含序列号: 选择以将设备的序列号包含在 MQTT 有效负载中。

+ 添加条件: 单击以添加条件。

保留: 定义将哪些 MQTT 消息作为保留发送。

- **无:** 全部消息均以不保留状态发送。
- **性能:** 仅将有状态消息发送为保留。
- **全部:** 将有状态和无状态消息作为保留发送。

QoS: 选择 MQTT 发布所需的级别。

MQTT 订阅

+ 添加订阅: 单击以添加一个新的 MQTT 订阅。

订阅筛选器: 输入要订阅的 MQTT 主题。

使用设备主题前缀: 将订阅筛选器添加为 MQTT 主题的前缀。

订阅类型:

- **无状态:** 选择以将 MQTT 消息转换为无状态消息。
- **有状态:** 选择将 MQTT 消息转换为条件。负载用作状态。

QoS: 选择 MQTT 订阅所需的级别。

MQTT 叠加

注意

在添加 MQTT 叠加调节器之前，请连接到 MQTT 代理。

+ 添加叠加调节器: 单击以添加新的叠加调节器。

主题过滤器: 添加包含要在叠加中显示的数据的 MQTT 主题。

数据字段: 为要在叠加中显示的消息有效负载指定密钥，默认消息为 JSON 格式。

调节器: 当您创建叠加时，请使用结果调节器。

- 以 **#XMP** 开头的调节器显示从主题接收到的数据。
- 以 **#XMD** 开头的调节器显示数据字段中指定的数据。

存储

网络存储

忽略：打开以忽略网络存储。

添加网络存储：单击以添加网络共享，以便保存记录。

- **地址：**键入主机服务器的 IP 地址或主机名称，通常为 NAS（网络连接存储）。我们建议您将主机配置为使用固定 IP 地址（非 DHCP，因为动态 IP 地址可能会更改），或者使用 DNS。不支持 Windows SMB/CIFS 名称。
- **网络共享：**在主机服务器上键入共享位置的名称。因为每台安讯士设备都有自己的文件夹，因此，多个设备可以使用同一个共享网络。
- **用户：**如果服务器需要登录，请输入用户名。要登录到特定域服务器，请键入 DOMAIN \username。
- **密码：**如果服务器需要登录，请输入密码。
- **SMB 版本：**选择 SMB 存储协议版本以连接到 NAS。如果您选择**自动**，设备将尝试协商其中一个安全版本 SMB：3.02, 3.0, 或 2.1.选择 1.0 或 2.0 以连接到不支持更高版本的较早的 NAS。您可以在此了解安讯士设备中有关 SMB 支持的更多信息。
- **添加共享而不测试：**即使在连接测试中发现错误，也选择添加网络共享。例如，错误可能是即便服务器需要密码，而您没有输入密码。

删除网络存储：单击以卸载、取消绑定及删除与网络共享的连接。这将删除网络共享的设置。

取消绑定：单击以取消绑定并断开网络共享。

Bind（绑定）：单击以绑定并连接网络共享。

卸载：单击此处卸载网络共享。

Mount（安装）：单击以安装网络共享。

写保护：打开停止写入到网络共享并防止录制内容被移除。无法格式化写保护的共享。

保留时间：选择保留录音的时间、限制旧录音的数量，或遵守有关数据存储的法规。如果网络存储已满，则会在选定时间段过去之前删除旧录音。

工具

- **测试连接：**测试网络共享的连接。
- **格式化：**格式化网络共享，例如，需要快速擦除数据时。CIFS 是可用的文件系统选项。

使用工具：单击以激活选定的工具。

车载存储

重要

数据丢失和录制内容损坏的风险。设备正在运行时，请勿取出 SD 卡。在删除 SD 卡之前将其卸载。

卸载：单击以安全删除 SD 卡。

写保护：打开停止写入到 SD 卡并防止录制内容被移除。您无法格式化写保护 SD 卡。

自动格式化：打开以自动格式化新插入的 SD 卡。它将文件系统格式化为 ext4。

忽略：打开以停止在 SD 卡上存储录音。当您忽略 SD 卡时，设备不再识别卡的存在。该设置仅适用于管理员。

保留时间：选择保留录像的时间、限制旧录像的数量，或遵守相关数据存储法规。当SD卡满时，它会在旧录像的保留时间未到期之前将其删除。

工具

- **检查：**检查 SD 卡上是否存在错误。
- **修复：**修复文件系统错误。
- **格式化：**格式化SD卡，更改文件系统并擦除所有数据。您只能将SD卡格式化为ext4文件系统。需要使用第三方ext4驱动程序或应用程序以从Windows®访问文件系统。
- **加密：**使用此工具格式化 SD 卡并启用加密。这会擦除SD卡上存储的数据。存储在SD卡上的新数据都将被加密。
- **解密：**使用此工具在不加密的情况下格式化 SD 卡。这会擦除SD卡上存储的数据。存储在SD卡上的新数据都不会被加密。
- **更改密码：**更改加密 SD 卡所需的密码。

使用工具：单击以激活选定的工具。

损耗触发器：设置要触发响应的 SD 卡损耗水平的值。损耗级别范围为 0–200%。从未使用过的新 SD 卡的损耗级别为 0%。100% 的损耗级别表示 SD 卡接近其预期寿命。当损耗达到 200% 时，SD 卡性能不良的风险很高。我们建议将损耗触发器设置为介于 80–90% 之间。这为您提供了下载录制内容以及在可能损耗之前替换 SD 卡的时间。使用损耗触发器，您可以设置事件并在磨损级别达到设置值时获得通知。

流配置文件

流配置文件是一组影响视频流的设置。您可以在不同情况下使用流配置文件，例如，在您创建事件和使用规则进行记录时。



添加流配置文件：单击以创建新的流配置文件。

预览：带有您选择的流配置文件设置的视频流的预览。更改页面上的设置时，预览会更新。如果您的设备具有不同的视图区域，则您可在图像左下角的下拉框中更改视图区域。

名称：为您的配置文件添加一个名称。

描述：添加您的配置文件的描述。

视频编解码器：选择应适用于配置文件的视频编解码器。

分辨率：有关该设置的说明，请参见。

帧率：有关该设置的说明，请参见。

压缩：有关该设置的说明，请参见。

Zipstream ：有关该设置的说明，请参见。

优化存储 ：有关该设置的说明，请参见。

动态FPS ：有关该设置的说明，请参见。

动态GOP ：有关该设置的说明，请参见。

镜像 ：有关该设置的说明，请参见。

GOP长度 ：有关该设置的说明，请参见。

比特率控制：有关该设置的说明，请参见。

包括叠加 ：选择要包含的叠加类型。有关如何添加叠加的信息，请参见。

包含音频 ：有关该设置的说明，请参见。

ONVIF

ONVIF 账户

ONVIF（Open Network Video Interface Forum）是一个全球的接口标准，终端用户、集成商、顾问和制造商可通过此接口轻松利用网络视频技术带来的可能性。ONVIF 可实现不同供应商产品之间的互操作性，提高灵活性，降低成本以及提供面向未来的系统。

创建 ONVIF 账户，即可自动启用 ONVIF 通信。使用该账户名和密码用于与设备的全部 ONVIF 通信。有关详细信息，请参见 axis.com 上的安讯士开发者社区。



添加账户：单击以添加新 ONVIF 账户。

帐户：输入唯一的账户名。

新密码：输入账户的密码。密码必须为 1 到 64 个字符长。密码仅允许包含可打印的 ASCII 字符（代码 32–126），如字母、数字、标点符号和某些符号。

确认密码：再次输入同一密码。

角色：

- **管理员：**可完全访问全部设置。管理员也可以添加、更新和删除其他账户。
- **操作员：**有权访问全部设置，以下各项除外：
 - 全部系统设置。
 - 添加应用。
- **媒体账户：**仅允许访问视频流。



上下文菜单包括：

更新账户：编辑账户的属性。

删除账户：删除账户。无法删除根账户。

ONVIF 媒体配置文件

ONVIF 媒体配置文件包括一组您可用于更改媒体流设置的配置。您可以使用自己的配置创建新的配置文件，也可以使用预配置的配置文件进行快速设置。



添加媒体配置文件：单击以添加新的 ONVIF 媒体配置文件。

配置文件名称：为媒体配置文件添加一个名称。

视频源：选择适合您的配置的视频源。

- **选择配置：**从列表中选择一个用户定义的配置。下拉列表中的配置对应于设备的视频通道，包括多视图、视点区域和虚拟通道。

视频编码器：选择适合您的配置的视频编码格式。

- **选择配置：**从列表中选择一个用户定义的配置并调整编码设置。下拉列表中的配置作为视频编码器配置的标识符/名称。选择用户 0 到 15 以应用您自己的设置，或者如果您想要对特定编码格式使用预定义设置，请选择一个默认用户。

注意

在设备中启用音频，以获得选择音频源和音频编码器配置的选项。

音频源 ：选择适合您的配置的音频输入源。

- **选择配置：**从列表中选择一个用户定义的配置并调整音频设置。下拉列表中的配置对应于设备的音频输入。如果设备只有一个音频输入，则为用户 0。如果设备有多个音频输入，则列表中将会有其他用户。

音频编码器 ：选择适合您的配置的音频编码格式。

- **选择配置：**从列表中选择一个用户定义的配置并调整音频编码设置。下拉列表中的配置作为音频编码器配置的标识符/名称。

音频解码器 ：选择适合您的配置的音频解码格式。

- **选择配置：**从列表中选择一个用户定义的配置并调整设置。下拉列表中的配置作为配置的标识符/名称。

音频输出 ：选择适合您的配置的音频输出格式。

- **选择配置：**从列表中选择一个用户定义的配置并调整设置。下拉列表中的配置作为配置的标识符/名称。

元数据：选择要包含在配置中的元数据。

- **选择配置：**从列表中选择一个用户定义的配置并调整元数据设置。下拉列表中的配置作为元数据配置的标识符/名称。

PTZ ：选择适合您的配置的 PTZ 设置。

- **选择配置：**从列表中选择一个用户定义的配置并调整 PTZ 设置。下拉列表中的配置对应于支持 PTZ 的设备视频通道。

创建：单击以保存您的设置并创建配置文件。

取消：单击以取消配置并清除全部设置。

profile_x：单击配置文件名称以打开并编辑预配置的配置文件。

侦测器

摄像机遮挡

当场景发生变化时，例如，镜头被覆盖、喷涂或严重超出对焦，且**触发延迟**时间已过，摄像机遮挡侦测器将生成警报。只有在摄像机至少 10 秒未移动时，遮挡侦测器才会激活。在此期间，侦测器将

设置场景模型，用作侦测当前图像中遮挡的比较。要正确设置场景模型，请确保摄像机已对焦，照明条件良好，并且摄像机未指向缺少轮廓的场景（如，空白的墙壁）。摄像机遮挡也可用作触发响应的条件。

触发延迟：输入报警触发前必须激活篡改条件的下限时间。这有助于防止影响图像的已知条件的假警报。

在黑暗图像上触发：当摄像机镜头被喷涂时，很难获得警报，因为无法将此情况与图像同样变暗的其他情况（例如，当光线条件变化时）区分开来。打开此参数将为图像变黑暗的全部情况生成警报。关闭时，当图像变暗时，设备不会生成警报。

注意

用于在静态和非拥挤场景中侦测篡改企图。

音频侦测

这些设置可用于每个音频输入。

声音级别：将声音级别调整到 0–100 范围内的值，其中 0 是敏感上限，100 是敏感下限。在设置声音级别时，请使用活动指示器作为指导。在创建事件时，您可以将声音级别用作条件。如果声音级别高于、低于或超过设定值，您可以选择触发操作。

撞击检测

冲击侦测器：打开以在物体击中设备或被遮挡时生成警报。

敏感度级别：移动滑块以调整设备应生成警报的敏感度级别。低值表示设备仅在击中力很强的情况下才生成警报。较高的值意味着即使有轻度的干预，设备也会生成警报。

附件

I/O 端口

数字输入用于连接可在开路和闭路之间切换的外部设备，例如 PIR 传感器、门或窗传感器和玻璃破碎探测器。

数字输出用于连接继电器和 LED 等外部设备。您可通过 VAPIX® 应用程序编程接口或网页界面激活已连接的设备。

端口

名称：编辑文本来重命名端口。

使用：继电器端口的默认选项是门。对于有指示器图标的设备，当状态发生变化并且门解锁时会变成绿色。如果您将继电器用于门以外的其他用途，并且不希望状态更改时图标亮起，则您可以为端口选择其他选项。

方向：  指示端口是输入端口。  指示它是一个输出端口。如果端口可配置，则您可以单击这些图标以在输入和输出之间进行切换。

正常状态：单击  开路，单击  闭路。

当前状态：显示端口的当前状态。在当前状态并非正常状态时，将激活输入或输出。当断开连接或电压高于 1 VDC 时，设备上的输入为开路。

注意

在重启过程中，输出电路为开路。当重启完成时，电路将恢复为正常位置。如果更改此页面上设置，无论是否存在活动的触发器，输出电路都将返回其正常位置。

受监控 ：如果有人篡改连接到数字 I/O 设备，请打开，以侦测并触发操作。除了侦测某个输入是否打开或关闭外，您还可以侦测是否有人篡改了该输入（即，剪切或短路）。监控连接功能要求外部 I/O 回路中存在其他硬件（线尾电阻器）。

日志

报告和日志

报告

- **查看设备服务器报告：**在弹出窗口中查看有关产品状态的信息。服务器报告中自动包含访问日志。
- **下载设备服务器报告：**将创建一个 .zip 文件，其中包含 UTF-8 格式的完整服务器报告文本文件以及当前实时画面的快照。当您与支持人员联系时，请始终提供服务器报告 .zip 文件。
- **下载崩溃报告：**下载和存档有关服务器状态的详细信息。崩溃报告中包含服务器报告中的信息和详细的调试信息。此报告中可能包含网络跟踪之类敏感信息。可能需要几分钟时间才生成此报告。

日志

- **查看系统日志：**单击以查看有关系统事件（如设备启动、警告和重要消息）的信息。
- **查看访问日志：**单击以查看访问设备的全部失败尝试，例如，使用了错误的登录密码。

远程系统日志

系统日志是消息日志记录的标准。它允许分离生成消息的软件、存储消息的系统以及报告和分析这些消息的软件。每个消息都标有设施代码，指示生成消息的软件类型，并为其分配一个严重性等级。



服务器：单击以添加新服务器。

主机：输入服务器的主机名或 IP 地址。

格式化：选择要使用的 syslog 消息格式。

- Axis
- RFC 3164
- RFC 5424

协议：选择要使用的协议：

- UDP (默认端口为 514)
- TCP (默认端口为 601)
- TLS (默认端口为 6514)

端口：编辑端口号以使用其他端口。

严重程度：选择触发时要发送哪些消息。

类型：选择要发送的日志类型。

Test server setup (测试服务器设置)：保存设置前，向全部服务器发送测试消息。

CA 证书已设置：查看当前设置或添加证书。

普通配置

普通配置适用于具有安讯士设备配置经验的高级用户。大多数参数均可在此页面进行设置和编辑。

维护

维护

重启：重启设备。这不会影响当前设置。正在运行的应用程序将自动重启。

恢复：将大部分设置恢复为出厂默认值。之后，您必须重新配置设备和应用，重新安装未预安装的应用，并重新创建事件和预设。

重要

重置后保存的仅有设置是：

- 引导协议（DHCP 或静态）
- 静态 IP 地址
- 默认路由器
- 子网掩码
- 802.1X 设置
- O3C 设置
- DNS 服务器 IP 地址

出厂默认设置：将全部恢复为出厂缺省值。之后，您必须重置 IP 地址，以便访问设备。

注意

安讯士设备软件均经过数字签名以确保仅在设备上安装经过验证的软件。这会进一步提高安讯士设备的总体网络安全级别门槛。有关详细信息，请参见 axis.com 上的白皮书“Axis Edge Vault”。

AXIS OS 升级：升级到新的 AXIS OS 版本。新版本中可能包含改进的功能、补丁和全新功能。建议您始终使用新 AXIS OS 版本。要下载更新版本，请转到 axis.com/support。

升级时，您可以在三个选项之间进行选择：

- **标准升级：**升级到新的 AXIS OS 版本。
- **出厂默认设置：**更新并将设置都恢复为出厂默认值。当您选择此选项时，无法在升级后恢复到以前的 AXIS OS 版本。
- **自动还原：**在规定时间内升级并确认升级。如果您没有确认，设备将恢复到以前的 AXIS OS 版本。

AXIS OS 回滚：恢复为先前安装的 AXIS OS 版本。

故障排查

重置 PTR ：如果由于某种原因**水平转动**、**垂直转动**或**滚转**设置无法按预期工作，则重置 PTR。始终在新摄像机中校准 PTR 电机。但是，如果摄像机断电或电机被手动移除，则可能会丢失校准。重置 PTR 时，摄像机将重新校准，并返回到其出厂默认位置。

校准 ：单击**校准**可将水平转动、垂直转动和滚转电机重新校准到其默认位置。

Ping：要检查设备是否能到达特定地址，请输入要 Ping 的主机名或 IP 地址，然后单击**开始**。

端口检查：要验证设备与特定 IP 地址和 TCP/UDP 端口的连接性，请输入要检查的主机名或 IP 地址和端口编号，然后单击**开始**。

网络追踪

重要

网络跟踪文件可能包含敏感信息，例如证书或密码。

通过记录网络上的活动，网络追踪文件可帮助您排除问题。

跟踪时间：选择以秒或分钟为单位的跟踪持续时间，并单击**下载**。

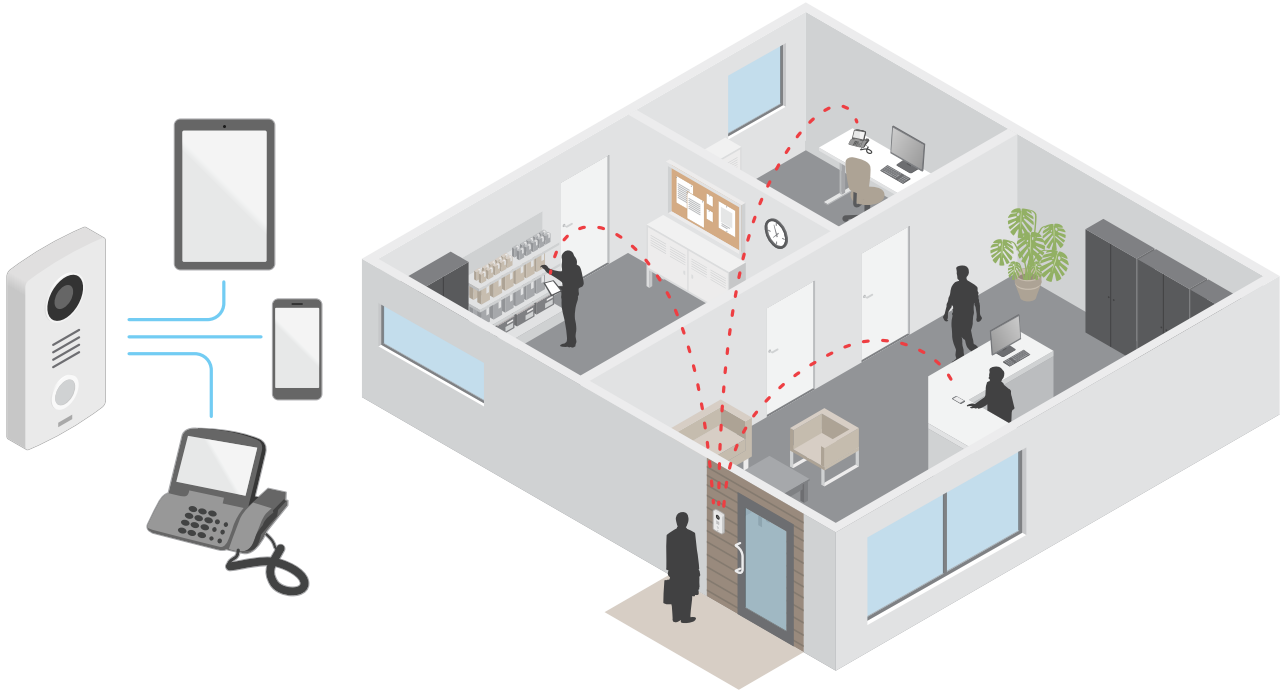
了解更多

IP 语音 (VoIP)

IP 语音 (VoIP) 是一组支持通过 IP 网络（如互联网）进行语音通信和多媒体会话的技术。在传统的电话呼叫中，模拟信号在公共交换电话网络 (PSTN) 上通过电路传输发送。在 VoIP 呼叫中，模拟信号被转化成数字信号，使其可以在本地 IP 网络或互联网间以数据包的形式发送。

在安讯士产品中，VoIP 已通过会话初始化协议 (SIP) 和双音多频 (DTMF) 信号启用。

示例：



当您按下 Axis 对讲机上的呼叫按钮时，会向一个或多个预定的接收者发起呼叫。接收者应答时，就建立了呼叫。音频和视频通过 VoIP 技术进行传输。

会话初始化协议 (SIP)

会话初始化协议 (SIP) (SIP) 用于创建、维持和终止 VoIP 呼叫。您可以在两方或多方（称为 SIP 用户代理）之间进行呼叫。如需进行 SIP 呼叫，您可以使用（例如）SIP 电话、软件电话或已启用 SIP 的安讯士设备。

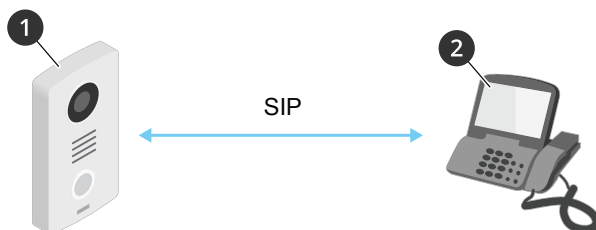
SIP 用户代理之间的实际音频或视频通过传输协议进行交换，例如 RTP（实时传输协议）。

您可以使用点对点设置在本地网络上或使用 PBX 在各网络间进行呼叫。

点对点 SIP (P2PSIP)

基本的 SIP 通信类型会直接发生在两个或多个 SIP 用户代理之间。这称为点对点 SIP (P2PSIP)。如果这发生在本地网络上，则只需用户代理的 SIP 地址。在这种情况下，SIP 地址通常为 sip:<local-ip>。

示例：



- 1 用户代理 A – 对讲机。SIP地址: sip:192.168.1.101
- 2 用户代理 B – 支持 SIP 的电话。SIP地址: sip:192.168.1.100

您可以安装 Axis 对讲机来呼叫，比如同一网络上采用点对点 SIP 设置且支持 SIP 的电话。

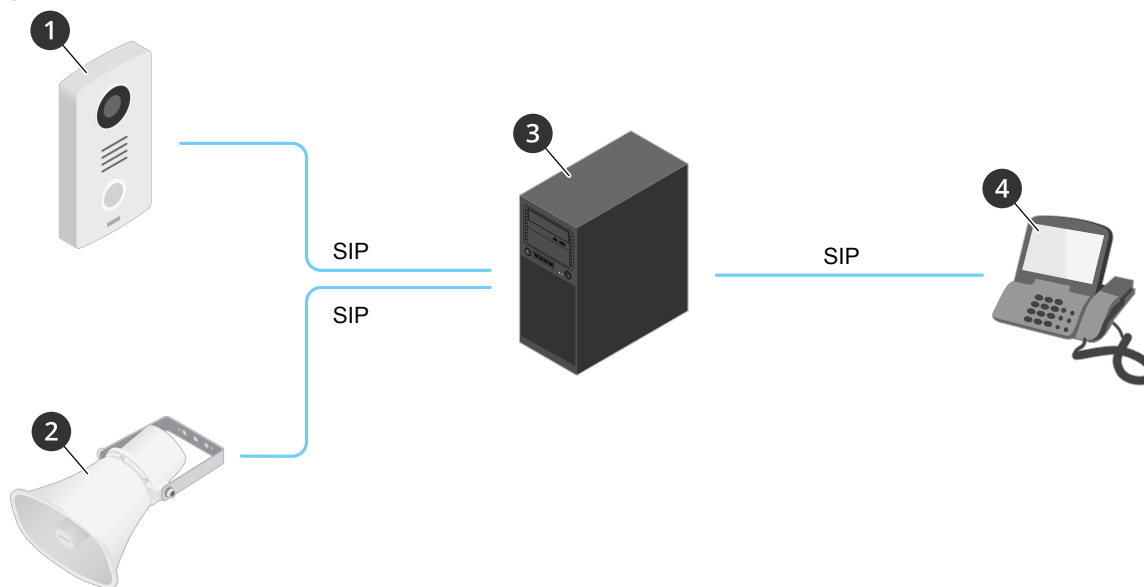
专用分支交换机 (PBX)

当您在本地 IP 网络外进行 SIP 呼叫时，专用分支交换机 (PBX) 可用作一个中央集线器。PBX 的主要元件是 SIP 服务器，也称为 SIP 代理服务器或注册服务器。PBX 的工作方式与传统交换机相同，会显示客户的当前状态，且可允许（例如）呼叫转移、语音邮件和重定向。

PBX SIP 服务器可安装为一个本地实体或异地实体。它可以托管在内联网上或由第三方提供商进行托管。当您在网络之间进行 SIP 呼叫时，呼叫会通过一组 PBX 进行传输，PBX 会查询要到达的 SIP 地址的位置。

每个 SIP 用户代理都需注册 PBX，随后才能拨打正确的电话分机联系其他人。在这种情况下，SIP 地址通常为 sip:<user>@<domain> 或 sip:<user>@<registrar-ip>。SIP 地址独立于其 IP 地址，PBX 使设备在 PBX 上注册期间可访问。

示例：



- 1 sip:mydoor@company.com
- 2 sip:myspeaker@company.com
- 3 PBX sip.company.com
- 4 sip:office@company.com

当您按下 Axis 对讲机上的呼叫按钮时，呼叫通过一个或多个 PBX 传输到本地 IP 网络或互联网上的 SIP 地址。

NAT 遍历

当安讯士设备位于某个专用网络 (LAN) 上，并且您想从该网络外部访问它时，使用 NAT（网络地址转换）穿越。

注意

路由器要支持 NAT 穿越和 UPnP®。

每个 NAT 穿越协议可单独使用或组合使用，具体取决于网络环境。

- ICE ICE（交互式连接建立）协议可增加找到对等设备之间进行成功通信的更有效路径的几率。如果您还启用了 STUN 和 TURN，则您可提高 ICE 协议的机会。

- **STUN** – STUN (NAT 会话遍历实用程序) 是一个客户端-服务器网络协议，可让安讯士设备确定其是否位于 NAT 或防火墙的后方，如果是的话，则获取映射的公共 IP 地址和分配用于连接至远程主机的端口编号。输入 STUN 服务器地址，例如，IP 地址。
- **TURN** – TURN (通过中继方式穿越 NAT) 是一个可让 NAT 路由器或防火墙后方的设备通过 TCP 或 UDP 接收其他主机的呼入数据的协议。输入 TURN 服务器地址和登录信息。

叠加

注意

使用 SIP 呼叫时，视频流中不包括叠加。

叠加是指叠印在视频流上。叠加用于在录制期间或产品安装和配置期间提供额外信息（如时间戳）。您可以添加文本或图像。

流传输和存储

视频压缩格式

决定使用何种压缩方式取决于您的查看要求及网络属性。可用选项包括：

Motion JPEG

Motion JPEG 或 MJPEG 是由一系列单张 JPEG 图像组成的数字视频序列。然后将按照足以创建流的速度显示和更新这些图像，从而连续显示更新的运动。为了让观看者感知运动视频，速度必须至少为每秒 16 个图像帧。每秒 30 (NTSC) 或 25 (PAL) 帧时即可感知完整运动视频。

Motion JPEG 流使用大量带宽，但是可以提供出色的图像质量并访问流中包含的图像。

H.264 或 MPEG-4 Part 10/AVC

注意

H.264 是一种许可制技术。安讯士产品包括一个 H.264 查看客户端许可证。禁止安装其他未经许可的客户端副本。要购买其他许可证，请与您的安讯士经销商联系。

与 Motion JPEG 格式相比，H.264 可在不影响图像质量的情况下将数字视频文件的大小减少 80% 以上；而与旧的 MPEG 格式相比，可减少多达 50%。这意味着视频文件需要更少的网络带宽和存储空间。或者，从另一个角度来看，在给定的比特率下，能够实现更高的视频质量。

H.265 或 MPEG-H Part 2/HEVC

与 H.264 标准相比，H.265 可将数字视频文件的大小减少 25% 以上。

注意

- H.265 是一种许可制技术。安讯士产品包括一个 H.265 查看客户端许可证。禁止安装其他未经许可的客户端副本。要购买其他许可证，请与您的安讯士经销商联系。
- 大多数网页浏览器不支持 H.265 的解码，因此这款摄像机在其网页界面中不支持这种情况。相反，您可以使用支持 H.265 解码的视频管理系统或应用程序。

应用

借助应用，您可以更充分地利用您的安讯士设备。AXIS Camera Application Platform (ACAP) 是一个开放平台，使第三方能够为安讯士设备开发分析及其他应用。应用可以预装在设备上，可以免费下载，或收取许可费。

要查找安讯士应用程序的用户手册，请转到 help.axis.com。

注意

- 多个应用程序可以同时运行，但某些应用程序可能无法彼此兼容。在并行运行时，某些应用程序组合可能需要很高的处理能力或很多内存资源。在部署之前验证应用程序能否协同工作。

AXIS Object Analytics

AXIS Object Analytics 是摄像机上预装的分析应用程序。它侦测场景中移动的物体，并将其分类为人或车辆等。您可以设置该应用程序，以发送不同类型的物体的警报。要了解有关应用程序如何工作的更多信息，请参见 *AXIS Object Analytics 用户手册*。

元数据可视化

分析元数据可用于场景中的移动对象。所支持的对象类通过对象周围的边界框在视频流中可视化，以及有关对象类型和分类置信度的信息。要了解有关如何配置和使用分析元数据的更多信息，请参见 *AXIS Scene Metadata 集成指南*。

网络安全

有关网络安全的产品特定信息，请参阅Axis.com上该产品的数据表。

有关AXIS OS网络安全的深度信息，请阅读 *AXIS OS 强化配置指南*。

签名OS

已签名的操作系统由软件供应商实施，并使用私钥对 AXIS OS 映像进行签名。将签名附加到操作系统后，设备将在安装软件之前对其进行验证。如果设备侦测到软件完整性受损，AXIS OS 升级将被拒绝。

安全启动

安全启动是一种由加密验证软件的完整链组成的启动过程，始于不可变的内存（启动ROM）。安全启动基于签名操作系统的使用，可确保设备仅能使用已授权的软件启动。

Axis Edge Vault

Axis Edge Vault为保障安讯士设备安全提供了基于硬件的网络安全平台。它有保证设备的身份和完整性的功能，并保护您的敏感信息免遭未经授权访问。它依托加密计算模块（安全元件和TPM）和SoC安全（TEE和安全启动）的强大基础，与前端设备安全的相关专业知识相结合。

安讯士设备ID

能够验证设备来源是建立设备身份信任的关键。在生产期间，配备 AXIS Edge Vault 的设备被分配到具有唯一性、由工厂预置且符合 IEEE 802.1AR 标准的安讯士设备 ID 证书。其原理与护照相似，旨在证明设备来源。设备ID作为经安讯士根证书签名的证书，安全且永久存储在安全密钥库中。客户的 IT 基础设施可以利用设备 ID 实现自动安全设备板载和安全设备确认

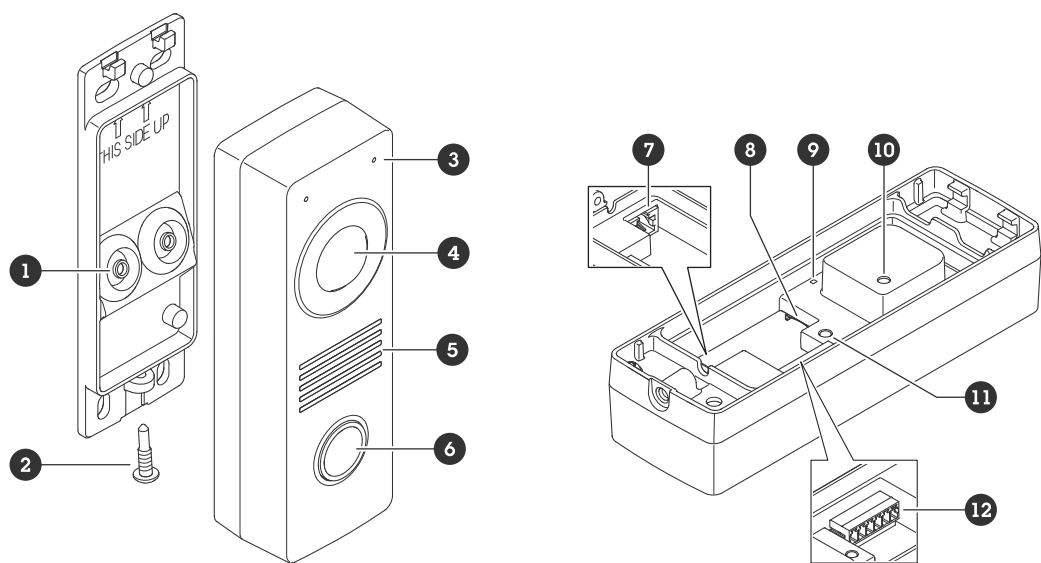
签名视频

签名视频能够在无需证明视频文件保管链的情况下，证实视频证据未遭到篡改。摄像机使用安全地存储在安全密钥库中的唯一签名密钥将签名添加到视频流中。播放视频时，文件播放器将显示视频是否完好。签名视频让视频追溯可达摄像机源头，并确定视频在离开摄像机后未遭到篡改。

要了解有关安讯士设备中网络安全功能的更多信息，请转到 axis.com/learning/white-papers 并搜索网络安全。

规格

产品概述



- 1 垫圈 (2x)
- 2 螺丝 (TR20)
- 3 Microphone (2x)
- 4 摄像机
- 5 扬声器
- 6 呼叫按钮
- 7 网络连接器 (PoE)
- 8 SD 卡插槽
- 9 状态LED
- 10 防破坏按钮
- 11 控制按钮
- 12 I/O、继电器和读卡器连接器

LED 指示灯

状态LED	指示
绿色	稳定绿色表示正常工作。

SD 卡插槽

注意

- 损坏 SD 卡的风险。插入或取出 SD 卡时，请勿使用锋利的工具、金属物体或用力过大。使用手指插入和取出该卡。
- 数据丢失和录制内容损坏的风险。移除 SD 卡之前，请从设备的网页接口上卸载 SD 卡。产品运行时，请勿取出 SD 卡。

本设备支持 microSD/microSDHC/microSDXC 卡。

有关 SD 卡的建议，请参见 axis.com。

   microSD、microSDHC 和 microSDXC 徽标是 SD-3C LLC 的商标。microSD、microSDHC、microSDXC 是 SD-3C, LLC 在美国和/或其他国家/地区的商标或注册商标。

按钮

控制按钮

- 控制按钮用于：
- 将产品重置为出厂默认设置。请参见。
 - 通过互联网连接到一键云连接 (O3C) 服务。若要连接，请按下并松开按钮，然后等待 LED 状态灯闪烁三次绿灯。

连接器

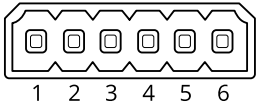
网络连接器

采用以太网供电 (PoE) 的 RJ45 以太网连接器。

I/O、读卡器连接器和继电器

您可以将此连接器用于 I/O 和中继，或用于读卡器连接。

6 针接线端子



- 1 -
- 2 12V
- 3 A/IO1
- 4 B/IO2
- 5 NO/NC
- 6 CO

功能	针脚	注意	规格
DC 接地	1		0 V DC
DC 输出	2	可用于为辅助设备供电。 注意：此针只能用作电源输出。	12 V DC I/O：最大负载 = 50 mA Reader/relay（读卡器/继电器）：最大负载 = 350 mA
I/O：可配置（输入或输出） Reader（读卡器）：A	3	I/O：数字输入 – 连接至针脚1以启用，或保留浮动状态（断开连接）以停用。数字输出 – 启用时内部连接至针脚 1（DC 接地），停用时保留浮动状态（断开连接）。如果与电感负载（如继电器）一起使用，则将二极管与负载并联连接，以防止电压瞬变。 Reader（读卡器）：RS485 – A	I/O：输入 – 0至最大值30 V DC 输出 – 0 至 30 V DC，开漏 100 mA)
I/O：可配置（输入或输出） Reader（读卡器）：B	4	I/O：与针脚 3 相同 Reader（读卡器）：RS485 – B	I/O：与针脚 3 相同

Relay (继电器): NO/NC	5	正常开/正常闭。用于连接中继设备。这两个继电器针脚与其余电路电位隔离。	上限电流 = 700mA 上限电压 = +30 V DC
Relay (继电器): CO	6	公共	

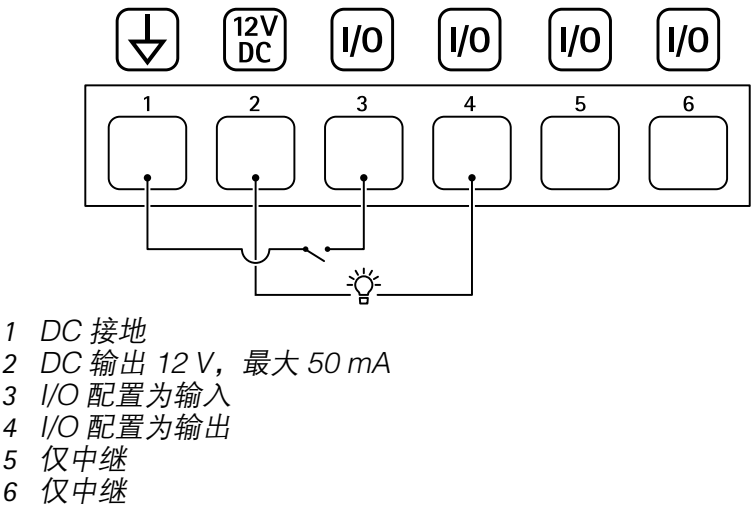
I/O 连接器

一个选项是将 I/O 连接器用于外部设备，例如与运动侦测、事件触发和警报通知结合使用。除 0 V DC 参考点和电源（12 V DC 输出）外，I/O 连接器还提供连接至以下模块的接口：

数字输入 – 用于连接可在开路和闭路之间切换的设备，例如 PIR 传感器、门/窗磁和玻璃破碎侦测器。

数字输出 – 用于连接继电器和LED等外部设备。已连接的设备可由VAPIX®应用程序编程接口、通过事件或从设备接口进行激活。

示例:



中继连接器

结合 I/O，您可以将连接器用作中继连接器来连接固态继电器，并使用它：

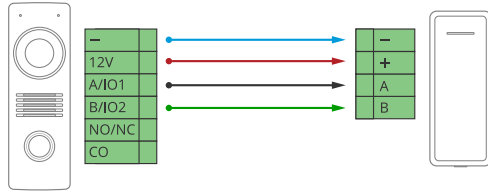
- 作为开启和关闭辅助电路的一个标准继电器，
- 直接控制一个锁，
- 通过安全继电器控制一个锁。在门的安全侧上使用一个安全继电器可避免线路发热。

读卡器连接器

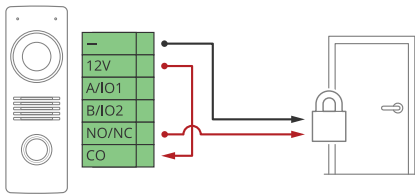
第三个选项是将连接器用作读卡器连接器来连接外部读卡器。

连接设备

Axis 读卡器

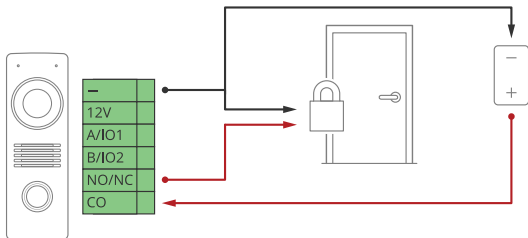


由 PoE (12V) 供电的继电器



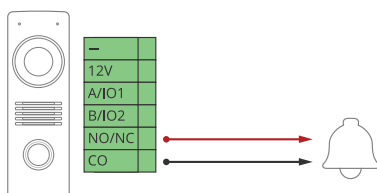
1. 要检查继电器状态，转到**系统 > 附件**，并找到继电器端口。
2. 将**正常状态**设置为：
 - ，适用于断电闭门锁。
 - ，适用于自动防故障锁。

由独立电源供电的继电器



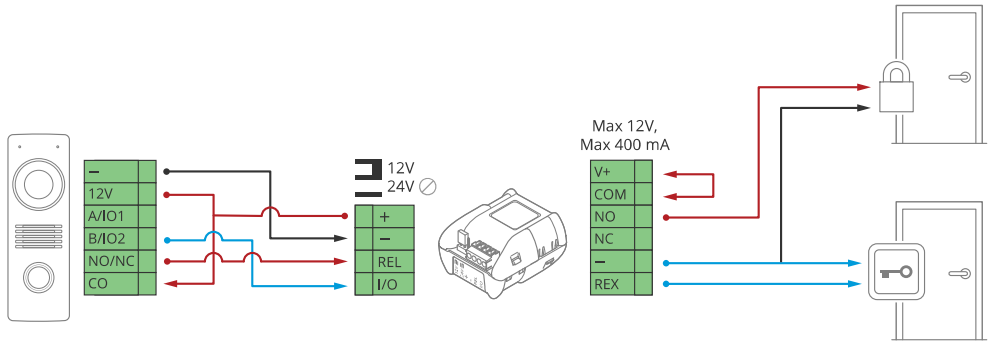
1. 要检查继电器状态，转到**系统 > 附件**，并找到继电器端口。
2. 将**正常状态**设置为：
 - ，适用于断电闭门锁。
 - ，适用于自动防故障锁。

无电势继电器



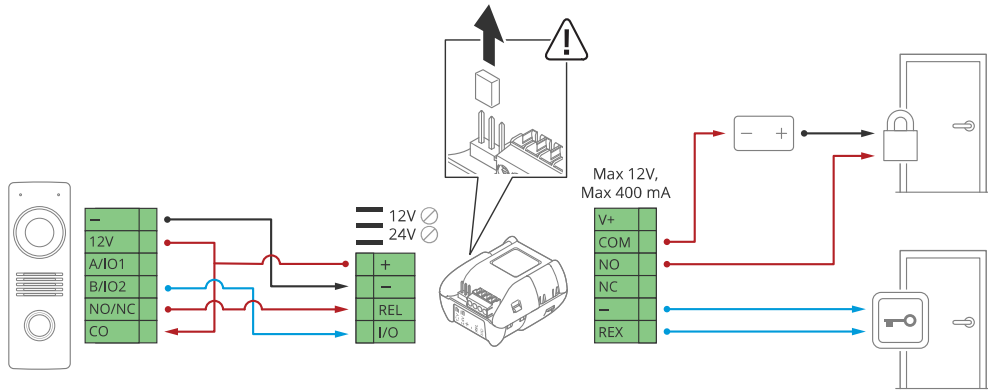
- 要检查继电器状态，转到**系统 > 附件**，并找到继电器端口。
- 将**正常状态**设置为：
 - ，适用于断电闭门锁。
 - ，适用于自动防故障锁。

由对讲机 PoE 供电的 12V 断电闭门锁



- 要检查继电器状态，转到**系统 > 附件**，并找到继电器端口。
- 将**正常状态**设置为：
 - ，适用于断电闭门锁。
 - ，适用于自动防故障锁。

由外部电源供电的 12V 断电闭门锁



- 要检查继电器状态，转到**系统 > 附件**，并找到继电器端口。
- 将**正常状态**设置为：
 - ，适用于断电闭门锁。
 - ，适用于自动防故障锁。

故障排查

重置为出厂默认设置

重要

重置为出厂默认设置时应谨慎。重置为出厂默认设置会将全部设置（包括 IP 地址）重置为出厂默认值。

将产品重置为出厂默认设置：

1. 断开产品电源。
2. 按住控制按钮，同时重新连接电源。请参见 。
3. 按住控制按钮15–30秒，直到状态LED指示灯闪烁琥珀色。
4. 释放控制按钮。当状态LED指示灯变绿时，此过程完成。如果网络上没有可用的DHCP服务器，设备IP地址将默认为以下之一：
 - 使用AXIS OS 12.0及更高版本的设备：从链路本地地址子网获取 (169.254.0.0/16)
 - 使用AXIS OS 11.11及更早版本的设备：192.168.0.90/24
5. 使用安装和管理软件工具分配 IP 地址、设置密码和访问设备。
安装和管理软件工具可在 axis.com/support 的支持页上获得。

您还可以通过设备网页界面将参数重置为出厂默认设置。转到**维护 > 出厂默认设置**，然后单击**默认**。

AXIS OS 选项

Axis 可根据主动跟踪或长期支持 (LTS) 跟踪提供设备软件管理。处于主动追踪意味着可以持续访问新产品特性，而 LTS 追踪则提供一个定期发布主要关注漏洞修复和安保升级的固定平台。

如果您想访问新特性，或使用安讯士端到端系统产品，则建议使用主动跟踪中的 AXIS OS。如果您使用第三方集成，则建议使用 LTS 跟踪，其未针对主动跟踪进行连续验证。使用 LTS，产品可维持网络安全，而无需引入重大功能性改变或影响现有集成。如需有关安讯士设备软件策略的更多详细信息，请转到 axis.com/support/device-software。

检查当前 AXIS OS 版本

AXIS OS 决定了我们设备的功能。当您进行问题故障排查时，我们建议您从检查当前 AXIS OS 版本开始。新版本可能包含能修复您的某个特定问题的校正。

要检查当前 AXIS OS 版本：

1. 转到设备的网页界面 > **状态**。
2. 请参见**设备信息**下的 AXIS OS 版本。

升级 AXIS OS

重要

- 在升级设备软件时，将保存预配置和自定义设置（如果这些功能在新 AXIS OS 中可用），但 Axis Communications AB 不对此做保证。
- 确保设备在整个升级过程中始终连接到电源。

注意

使用活动跟踪中的新 AXIS OS 升级设备时，产品将获得可用的新功能。在升级前，始终阅读每个新版本提供的升级说明和版本注释。要查找新 AXIS OS 和发布说明，请转到 axis.com/support/device-software。

1. 将 AXIS OS 文件下载到您的计算机，该文件可从 axis.com/support/device-software 免费获取。
2. 以管理员身份登录设备。

3. 转到**维护** > **AXIS OS 升级**，然后单击**升级**。

升级完成后，产品将自动重启。

技术问题、线索和解决方案

如果您无法在此处找到您要寻找的信息，请尝试在 axis.com/support 上的故障排除部分查找。

升级 AXIS OS 时出现问题

AXIS OS 升级失败	如果升级失败，该设备将重新加载以前的版本。比较常见的原因是上传了错误的 AXIS OS 文件。检查 AXIS OS 文件名是否与设备相对应，然后重试。
AXIS OS 升级后出现的问题	如果您在升级后遇到问题，请从 维护 页面回滚到之前安装的版本。

设置 IP 地址时出现问题

设备位于不同子网掩码上	如果用于设备的 IP 地址和用于访问该设备的计算机 IP 地址位于不同子网上，则无法设置 IP 地址。请联系网络管理员获取 IP 地址。
该 IP 地址已用于其他设备	从网络上断开安讯士设备。运行 Ping 命令（在 Command/DOS 窗口中，键入 ping 和设备的 IP 地址）： - 如果收到 Reply from <IP address>: bytes=32; time=10...，这意味着网络上其他设备可能已使用该 IP 地址。请从网络管理员处获取新的 IP 地址，然后重新安装该设备。 - 如果收到 Request timed out，这意味着该 IP 地址可用于此安讯士设备。请检查布线并重新安装设备。
可能的 IP 地址与同一子网上的其他设备发生冲突	在 DHCP 服务器设置动态地址之前，将使用安讯士设备中的静态 IP 地址。这意味着，如果其他设备也使用同一默认静态 IP 地址，则可能在访问该设备时出现问题。

无法通过浏览器访问该设备

无法登录	启用 HTTPS 时，请确保在尝试登录时使用正确的协议（HTTP 或 HTTPS）。您可能需要在浏览器的地址字段中手动键入 http 或 https。 如果根账户的密码丢失，则设备必须重置为出厂默认设置。请参见。
通过DHCP修改了IP地址。	从 DHCP 服务器获得的 IP 地址是动态的，可能会更改。如果 IP 地址已更改，请使用 AXIS IP Utility 或 安讯士设备管理器在网络上找到设备。使用设备型号或序列号或根据 DNS 名称（如果已配置该名称）来识别设备。 如果需要，可以手动分配静态 IP 地址。如需说明，请转到 axis.com/support。
使用 IEEE 802.1X 时出现证书错误	要使身份验证正常工作，则安讯士设备中的日期和时间设置必须与 NTP 服务器同步。转到 系统 > 日期和时间 。

可以从本地访问设备，但不能从外部访问

如需从外部访问设备，我们建议您使用以下其中一种适用于 Windows® 的应用程序：

- AXIS Camera Station Edge：免费，适用于有基本监控需求的小型系统。
- AXIS Camera Station 5：30 天试用版免费，适用于小中型系统。
- AXIS Camera Station Pro：90 天试用版免费，适用于小中型系统。

有关说明和下载文件，请转到 axis.com/vms。

无法通过 SSL 通过端口 8883 进行连接，MQTT 通过 SSL

防火墙会阻止使用端口 8883 的通信，因为它被认为是不安全的。

在某些情况下，服务器/中介可能不会提供用于 MQTT 通信的特定端口。仍然可以使用通常用于 HTTP/HTTPS 通信的端口上的 MQTT。

- 如果服务器/代理支持 websocket/Websocket Secure (WS/WSS)，通常在端口 443 上，请改用此协议。与服务器/中介提供商确认是否支持 WS/WSS 以及要使用哪个端口和 basepath。
- 如果服务器/代理支持 ALPN，则可通过开放端口（如 443）协商使用 MQTT。请咨询服务器/代理提供商，了解是否支持 ALPN 以及使用哪个 ALPN 协议和端口。

性能考虑

设置系统时，务必考虑不同设置和情况对性能的影响。一些因素会影响所需带宽大小（比特率），另一些因素可能会影响帧速，还有一些因素可能会同时影响这两者。如果 CPU 的负载达到最大值，也会影响帧速。

以下因素是重要的考虑因素：

- 图像分辨率较高或压缩级别较低都会导致图像含更多数据，从而影响带宽。
- 大量 Motion JPEG 客户端或单播 H.264/H.265/AV1 用户访问会影响带宽。
- 使用不同客户端同时查看不同流（分辨率、压缩）会同时影响帧速和带宽。尽量使用相同流来保持高帧速。流配置文件可用于确保流是相同的。
- 同时访问不同编解码器的视频流会影响帧速和带宽。为获得理想性能，请使用编解码器相同的视频流。
- 大量使用事件设置会影响产品的 CPU 负载，从而影响帧速。
- 使用 HTTPS 可能降低帧速，尤其是流传输 Motion JPEG 时。
- 由于基础设施差而导致的网络利用率重负会影响带宽。
- 在性能不佳的客户端计算机上进行查看会降低帧速，影响用户体验。
- 同时运行多个 AXIS Camera Application Platform (ACAP) 应用程序可能会影响帧速和整体性能。

联系支持人员

如果您需要更多帮助，请转到 axis.com/support。

T10183848_zh

2025-06 (M11.2)

© 2023 – 2025 Axis Communications AB