AXIS C1310-E Network Horn Speaker

用户手册

解决方案概述

本手册介绍了如何使设备可供音频系统访问，以及如何直接从设备的界面配置设备（例如，当您使用不带音频或视频管理软件的设备时）。

如果您在使用音频或视频管理软件，则可以使用该软件来配置设备。以下管理软件可用于控制音频系统：

- AXIS Audio Manager Edge — 用于小型系统的音频管理软件。预装在固件版本等于或高于 10.0 的音频设备上。
  - *AXIS Audio Manager Edge 用户手册*
- AXIS Audio Manager Pro — 用于大型系统的高级音频管理软件。
  - *AXIS Audio Manager Pro 用户手册*
- AXIS Camera Station — 用于大型系统的高级视频管理软件。
  - *AXIS Camera Station 用户手册*
- AXIS Companion — 用于小型系统的视频管理软件。
  - *AXIS Companion 用户手册*

有关更多信息，请参见*音频管理软件*。



网络音频工作原理概览。

安装



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	✓	✓	✓	✓*

*要在iOS 15或iPadOS 15上使用AXIS OS网页界面，请转到 **Settings（设置）** > **Safari** > **Advanced（高级）** > **Experimental Features（实验功能）**，并禁用NSURLSession Websocket。

如果您需要有关推荐的浏览器的更多信息，请转到 *AXIS OS Portal*。

访问设备

1. 打开浏览器并输入 Axis 设备的 IP 地址或主机名。
2. 输入用户名和密码。如果您是首次访问设备，则必须设置 root 用户密码。请参见 。

为 root 用户设置一个新密码

重要

默认管理员用户名为 **root**。如果 root 的密码丢失，请将设备重置为出厂默认设置。请参见



支持提示：密码安全确认检查

1. 键入密码。请按照安全密码的相关说明操作。请参见 。
2. 重新键入密码以确认拼写。
3. 单击 **Save（保存）**。密码现在已配置完成。

安全密码

重要

Axis 设备在网络中以明文形式发送初始设置的密码。若要在首次登录后保护您的设备，请设置安全加密的 HTTPS 连接，然后更改密码。

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。

其他设置

校准并运行远程扬声器测试

您可以运行扬声器测试，从远程位置验证扬声器是否按预期工作。扬声器通过播放内置麦克风登记的一系列测试音来执行测试。每次运行测试时，都会将已登记值与校准期间登记的值进行比较。

注意

测试必须根据其在安装场所的安装位置进行校准。如果扬声器被移动或者其现场环境发生改变，例如，新增或拆除了墙壁，则应重新校准扬声器

在校准期间，建议有人员亲自在安装场所听测试音，并确保测试音清晰或未被扬声器声路中的意外障碍所阻拦。

1. 转到设备界面 > **音频 > 扬声器测试**。
2. 要校准音频设备，单击**校准**。

注意

Axis 产品校准后，可随时运行扬声器测试。

3. 要运行扬声器测试，单击**运行测试**。

注意

还可以通过按下物理设备上的控制按钮来运行校准。参见 确认控制按钮。

设置直连 SIP (P2P)

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。要更好地了解 P2P 的工作方式，请参见 。

有关设置选项的详细信息，请参见 。

1. 转到**系统** > SIP > **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**。
3. 在**呼叫处理**下，设置呼叫的超时和持续时间。
4. 在**端口**下，输入端口号。
   - **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** – 输入 SIP 呼叫中用于首个 RTP 媒体流的端口。媒体传输的默认起始端口为4000。有些防火墙可能会阻止某些端口号上的RTP通信。端口号要在 1024 到 65535 之间。
5. 在 **NAT 穿越**下，选择想要针对 NAT 穿越启用的协议。

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。

6. 在**音频**下，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。
7. 在**其他**下，选择其他选项。
   - **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。

8. 单击 **Save（保存）**。

通过服务器设置 SIP (PBX)

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。要更好地了解 P2P 的工作方式，请参见 。

有关设置选项的详细信息，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. 要添加新账户，转到**系统** > **SIP** > **SIP 账户**，然后单击 **+ 账户**。
3. 输入您从 PBX 供应商处获得的详细信息。
4. 选择**已注册**。
5. 选择一种传输模式。
6. 单击 **Save（保存）**。
7. 使用与点对点相同的方法创建 SIP 设置。请参见 了解更多信息。

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，设备可以根据时间计划或在其收到呼叫后播放某个音频片段，或在设备更改 IP 地址时发送一封电子邮件。

若要了解更多信息，请查看我们的指南*事件规则入门*。

如果扬声器测试失败，发送电子邮件

在本示例中，音频设备配置为在扬声器测试失败时向规定的接收者发送电子邮件。扬声器测试配置为在每天 18:00 进行。

1. 设置扬声器测试时间表：
   1.1. 转到设备界面 > **系统** > **事件** > **时间表**。
   1.2. 创建开始时间为每天 18:00 且结束时间为每天 18:01 的时间表。将其命名为“每天下午 6 点”。
2. 创建电子邮件接收者：
   2.1. 转到设备界面 > **系统** > **事件** > **接收者**。
   2.2. 单击**添加接收者**。
   2.3. 将接收者命名为“扬声器测试接收者”
   2.4. 在**类型**下，选择**电子邮件**。
   2.5. 在**发送电子邮件至**下，输入接收者的电子邮件地址。使用逗号分隔多个地址。
   2.6. 输入发送者的电子邮件帐户详细信息。
   2.7. 单击**测试**发送测试电子邮件。

注意

某些电子邮件提供商拥有可防止用户接收或查看大型附件、接收预定电子邮件及类似内容的安全过滤器。检查电子邮件提供商的安全策略，以避免出现投递问题，防止电子邮件账户被锁定。

2.8. 单击 Save（保存）。

3. 创建自动扬声器测试：
   3.1. 转到设备界面 > **系统** > **事件** > **规则**。
   3.2. 单击**添加规则**。
   3.3. 为规则输入一个名称。
   3.4. 在**条件**下，选择**时间表**，然后从触发器列表中进行选择
   3.5. 在**时间表**下，选择您的时间表（“每天下午 6 点”）。
   3.6. 在**操作**下，选择**运行自动扬声器测试**。
   3.7. 单击 Save（保存）。
4. 设置条件，在扬声器测试失败时发送电子邮件。
   4.1. 转到设备界面 > **系统** > **事件** > **规则**。
   4.2. 单击**添加规则**。
   4.3. 为规则输入一个名称。
   4.4. 在**条件**下，选择**扬声器测试结果**。
   4.5. 在**扬声器测试状态**下，选择**未通过测试**。
   4.6. 在**操作**下，选择**发送电子邮件通知**。
   4.7. 在**接收者**下，选择您的接收者（“扬声器测试接收者”）
   4.8. 输入主题和消息，然后单击**保存**。

摄像机侦测到移动时播放音频

该示例解释了如何安装音频设备，从而在 Axis 网络摄像机侦测到移动时播放音频剪辑。

前提条件

- Axis 音频设备和 Axis 网络摄像机位于同一个网络。
- 已在摄像机中配置移动侦测应用程序且其正在运行。

1. 准备一个音频剪辑链接：
   1.1. 转到**音频** > **音频剪辑**。
   1.2. 单击 ⋮ > Create link（**创建链接**）选择音频片段。
   1.3. 设置音量和重复该剪辑的次数。
   1.4. 单击复制图标以复制链接。
2. 创建操作规则：
   2.1. 转到**系统** > **事件** > **接收者**。
   2.2. 单击 **+ 添加接受者**。
   2.3. 键入接收者的名称，例如“扬声器”。
   2.4. 从**类型**下拉列表中选择 HTTP。
   2.5. 在 URL 字段中粘贴音频设备中配置好的链接。
   2.6. 输入音频设备的用户名和密码。
   2.7. 单击 Save（保存）。
   2.8. 转到**规则**并单击 **+ 添加一条规则**。
   2.9. 键入操作规则的名称，例如“播放剪辑”。

2.10. 从**条件**列表中，选择**应用**下的视频移动侦测替代选择。

注意

如无针对视频移动侦测的选项，那么请转到**应用**，单击 AXIS Video Motion Detection 并打开移动侦测。

2.11. 从**操作**列表中，选择**通过 HTTP 发送通知**。

2.12. 在**接收者**下选择您的接收者。

2.13. 单击“**保存**”。

通过 DTMF 停止播放音频

本示例说明了如何进行操作：

- 在一个设备上配置 DTMF。
- 设置一个事件，在 DTMF 命令发送至设备时停止播放音频。

1. 转到**系统** > SIP > **事件**。
2. 确保**启用** SIP 已打开。
   如果需要将其打开，记住在之后单击**保存**。
3. 转到 **SIP 帐户**。
4. 在SIP账户旁边，单击 ⋮ > Edit（**编辑**）。
5. 在 DTMF 下，单击 **+ DTMF 序列**。
6. 在**序列**下，输入“1”。
7. 在**描述**下，输入“停止音频”。
8. 单击 Save（**保存**）。
9. 转到**系统** > **事件** > **规则**，然后单击 **+ 添加规则**。
10. 在**名称**下，输入“DTMF 停止音频”。
11. 在**条件**下，选择 DTMF。
12. 在 DTMF **事件 ID** 下，选择**停止音频**。
13. 在**操作**下，选择**停止播放音频剪辑**。
14. 单击 Save（**保存**）。

设置用于传入 SIP 呼叫的音频

您可以设置一个在接收到 SIP 呼叫时播放音频剪辑的规则。

您还可以设置一个附加规则，以在音频剪辑结束后自动回答 SIP 呼叫。当警报操作员想要引起靠近音频设备的人的关注并建立线路通信时，这可能非常有用。这是通过向音频设备进行 SIP 呼叫来完成的，这将播放音频剪辑，以提醒音频设备附近的人员。当音频剪辑停止播放时，SIP 呼叫将由音频设备自动应答，且警报操作员和靠近音频设备的人员之间可进行通信。

启用 SIP 设置：

1. 通过在 Web 浏览器中输入 IP 地址，转到扬声器的设备界面。
2. 转到System（**系统**）> SIP > SIP settings（SIP**设置**），然后选择Enable SIP（**启用** SIP）。
3. 要允许设备接收呼入，选择Allow incoming calls（**允许呼入**）。
4. 单击Save（**保存**）。
5. 转到SIP accounts（SIP**账户**）。
6. 在SIP账户旁边，单击 ⋮ > Edit（**编辑**）。

7. 取消选择**自动应答**。

在收到 SIP 呼叫时播放音频：

1. 转到Settings（**设置**）> System（**系统**）> Events（**事件**）> Rules（**规则**），然后添加一个规则。
2. 为规则键入一个名称。
3. 在条件列表中，选择State（**状态**）。
4. 在状态列表中，选择**铃声**。
5. 在操作列表中，选择Play audio clip（**播放音频片段**）。
6. 在剪辑列表中，选择要播放的音频剪辑。
7. 选择重复音频剪辑的次数。0 表示“播放一次”。
8. 单击Save（**保存**）。

在音频片段结束后，自动应答 SIP 呼叫：

1. 转到Settings（**设置**）> System（**系统**）> Events（**事件**）> Rules（**规则**），然后添加一个规则。
2. 为规则键入一个名称。
3. 在条件列表中，选择Audio clip playing（**音频片段播放**）。
4. 选择**使用此条件作为触发器。**
5. 选择**反转此条件。**
6. 单击 **+ 添加条件**，向事件中添加第二个条件。
7. 在条件列表中，选择State（**状态**）。
8. 在状态列表中，选择**铃声**。
9. 在操作列表中，选择Answer call（**回答呼叫**）。
10. 单击Save（**保存**）。

了解更多

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。

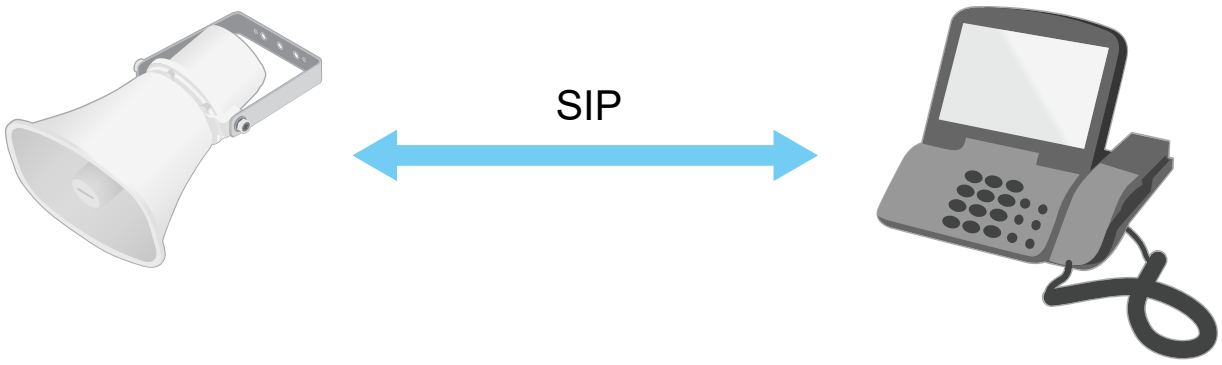
SIP 用户代理之间的实际音频或视频通过传输协议进行交换，例如 RTP（实时传输协议）。

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：



您可以安装一部已启用 SIP 的电话来呼叫同一网络上采用点对点 SIP 设置的音频设备。

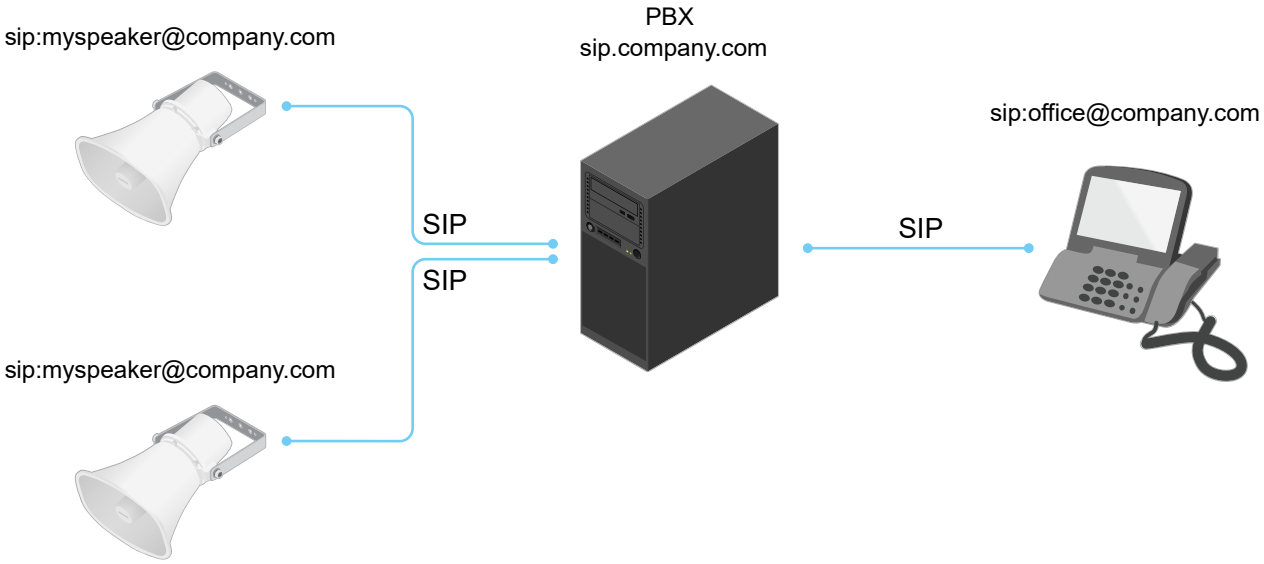
专用分支交换机 (PBX)

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：



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。

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*。

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

音频系统信息

仅针对属于 AXIS Audio Manager Edge 场所的设备显示此信息。

AXIS Audio Manager Edge：启动 AXIS Audio Manager Edge。

定位设备

显示定位设备信息，包括序列号和 IP 地址。

定位设备：播放有助于识别扬声器的声音。对于某些产品，设备上会闪烁 LED 。

扬声器测试

显示扬声器是否已校准。

扬声器测试： : 校准扬声器测试。带您进入**扬声器测试**页面，您可以在其中进行校准并运行扬声器测试。

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**日期和时间**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。

音频

AXIS Audio Manager Edge

AXIS Audio Manager Edge：启动应用程序。

音频场所安全

CA 证书：选择要向音频场所添加设备时使用的证书。您必须在 AXIS Audio Manager Edge 中启用 TLS 身份验证。

保存：激活并保存您的选择。

设备设置

输入：打开或关闭音频输入。显示输入类型。

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。

输入类型  ：选择输入类型。

电源类型  ：选择供电类型。

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。

流

编码：选择要用于输入源流传输的编码。只有打开了音频输入时，才能选择编码。如果音频输入已关闭，单击**启用音频输入**将其打开。

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。

监听和录制

单击以进行侦听。

开始实时音频流的连续录制。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。

注意

只有当设备的输入打开时，才能进行监听和录制。转到**音频 > 设备设置**，确保您已经打开输入。

显示设备的已配置存储。要配置存储，您需要以管理员身份登录。

扬声器测试

您可以使用扬声器测试来远程验证扬声器按预期工作。

校准：首次测试前，您需要先校准扬声器。校准时，扬声器播放一系列由内置麦克风记录的测试音。校准扬声器时，要将其安装在其尾端。如果之后移动扬声器或者其环境发生改变，例如，新砌或拆除了墙壁，则应重新校准扬声器。

进行测试:播放校准期间播放的相同系列的测试音，并将其与校准的注册值进行比较。

录像

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。

正在进行的录制内容：显示设备上全部正在进行的录制。

开始在设备上进行录制。

选择要保存到哪个存储设备。

停止在设备上进行录制。

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。

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。您将被带到安讯士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。

允许root特权应用程序：打开以允许具有根权限的应用可对设备进行完全访问。

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 NTS 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 NTS 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。

- **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。

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 –。

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，您将得到一个警告。

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，您将得到一个警告。

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。要解决 PoE 电源协商的任何问题，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：**这是默认设置。按住设备上的控制按钮，以通过互联网连接到 O3C 访问。按下控制按钮后 24 小时内，您需要向 O3C 服务注册设备。否则，设备将从 O3C 服务断开。一旦您注册了设备，**一直**将被启用，您的设备会一直连接到 O3C 服务。
- **总是：**设备将不断尝试通过互联网连接到 O3C 服务。一旦您注册了设备，它会一直连接到 O3C 服务。如果无法够到设备上的控制按钮，则使用此选项。
- **无：**禁用 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。
    - **热启动**：更改 SNMP 设置时发送陷阱消息。
    - **连接**：链接自下而上发生变更时，发送陷阱消息。
    - **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。

- **更多** ：显示更多要填充或选择的栏。
- **安全密钥库**：选择使用**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/en-us/axis-os#cryptographic-support*。
- **秘钥类型**：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：

- **安全元件 (CC EAL6+)**：选择使用安全元素来实现安全密钥库。
- **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 保护的网络，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，不管网络是否连接，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络，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 802.1 x。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，无论连接到哪个网络，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 802.1 x 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

激活：打开防火墙。

默认策略：选择防火墙的默认状态。
- **允许**：允许与设备的各连接。默认情况下设置此选项。
- **拒绝**：拒绝与设备的各连接。

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

- **地址**：输入要允许或拒绝访问的 IPv4/IPv6 或 CIDR 格式的地址。
- **协议**：选择要允许或拒绝访问的协议。
- **端口**：输入要允许或拒绝访问的端口号。您可以添加介于 1 和 65535 之间的端口号。
- **策略**：选择规则的策略。

＋：单击创建另一个规则。

添加规则：单击此项可添加已定义的规则。
- **时间（秒）**：设置测试规则的时间限制。默认时间限制设置为300秒。要立即激活规则，请将时间设置为0。
- **确认规则**：确认规则及其时间限制。如果您将时间限制设置为 1 秒以上，则规则将在此期间处于活动状态。如果您将时间设置为0，规则将直接激活。

待处理规则：您尚未确认的经过测试的新检测规则概述。

注意

具有时间限制的规则将显示在**活动规则**下，直到显示的计时器用完或确认它们为止。如果不进行确认，一旦计时器用完，它们将显示在**待处理规则**下，并且防火墙将恢复为之前定义的设置。如果您确认，它们将替换当前有效的规则。

确认规则：单击以激活挂起的规则。

活动规则：当前在设备上运行的规则概述。

：单击可删除活动规则。

：单击可删除各规则，包括挂起规则和活动规则。

自定义签名的 AXIS OS 证书

要在设备上安装来自安讯士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安讯士批准。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:输入一个唯一的账户名。

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**：没有权限更改设置。

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。

- **限制根访问**：打开以限制要求根访问的功能。
- **启用 SSH**:打开以使用 SSH 服务。

帐户:输入一个唯一的账户名。

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。

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据。

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。

观看者声明:输入观看者角色的值。

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

规则定义产品执行响应触发的条件。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*。

您的产品可能具有以下预配置的规则：

Front–facing LED Activation: LiveStream（**前置指示灯激活：直播**）：当麦克风打开并且接收到直播流时，音频设备上的前置指示灯 将变为绿色。

Front–facing LED Activation: Recording（**前置指示灯激活：录制**）：当麦克风打开并且正在进行录制时，音频设备上的前置指示灯 将变为绿色。

Front–facing LED Activation: SIP（**前置指示灯激活：SIP**）：当麦克风打开并且 SIP 呼叫处于活动状态时，音频设备上的前置指示灯将变为绿色。必须先在音频设备上启用 SIP，然后才能触发此事件。

Pre–announcement tone: Play tone on incoming call（**预提示音：来电时播放提示音**）：当对音频设备发起 SIP 呼叫时，设备将播放预定义的音频片段。必须要为音频设备启用 SIP。要使 SIP 呼叫者在音频播放音频片段时听到铃声，必须要将音频设备的 SIP 帐户配置为不自动应答呼叫。

Pre–announcement tone: Answer call after incoming call–tone（**预提示音：来电提示音后接听来电**）：当音频片段结束时，应答传入的 SIP 呼叫。必须要为音频设备启用 SIP。

响亮的铃声：当对音频设备发起 SIP 呼叫时，只要规则处于活动状态，就会播放预定义的音频片段。必须要为音频设备启用 SIP。

接受者

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，则上载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。上载完成时，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，则上载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。上载完成时，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。

您可在 *AXIS OS Portal* 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

终了证明（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。

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

- **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。

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：UPD、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 服务器上进行注册，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。

组播控制器

使用组播控制器：打开以激活多播控制器。

音频编解码器:选择音频解码。

来源：增加新的组播控制器源。

- **标签**：输入尚未被源使用的标签名称。
- **来源**：输入源。
- **端口**：输入端口。
- **优先级**：选择优先级。
- **配置文件**：选择一个配置文件。
- **SRTP 键**：输入 SRTP 键。

上下文菜单包括：

编辑：编辑组播控制器源。

删除：删除多播控制器源。

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网络共享。

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。

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:输入一个唯一的账户名。

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，包括多画面、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

音频侦测

这些设置可用于每个音频输入。

声音级别:调整声音级别设置在 0–100 的范围内，其中 0 是敏感上限，而 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，您可以选择触发响应。

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。

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 V DC 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。

监控 ：如果有人篡改连接到数字 I/O 设备，请打开，以侦测并触发响应。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。

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**。

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。

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

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置。

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 10 秒，直到 LED 状态指示灯再次变成橙色。
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、设置密码和访问产品。

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**。

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。

固件升级问题	
固件升级失败	如果固件升级失败，该设备将重新加载以前的固件。比较常见的原因是上载了错误的固件文件。检查固件文件名是否与设备相对应，然后重试。

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 root 用户的密码丢失，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。

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，我们建议使用以下其中一种适用于 Windows® 的应用程序：

- AXIS CameraStation：30 天免费试用版，适用于小中型系统。

有关说明和下载文件，请转到 *axis.com/vms*。

声音文件的问题

无法上传媒体剪辑	支持以下音频剪辑格式： • au 文件格式，以 µ 定律编码并使用 8 或 16 kHz 进行采样。 • wav 文件格式，编码在 PCM 音频中。它支持将编码为 8 个或 16–bit 单声道或立体声，采样率为 8 至 48 kHz。 • mp3 文件格式，采用单声道或立体声，比特率为 64 kbps 到 320 kbps，采样率为 8 到 48 kHz。
媒体剪辑是使用不同的音量播放的	录制声音文件时有一定增益。如果您的音频剪辑创建时具有不同增益，播放时会有不同响度。请确保使用具有相同增益的剪辑。

性能考虑

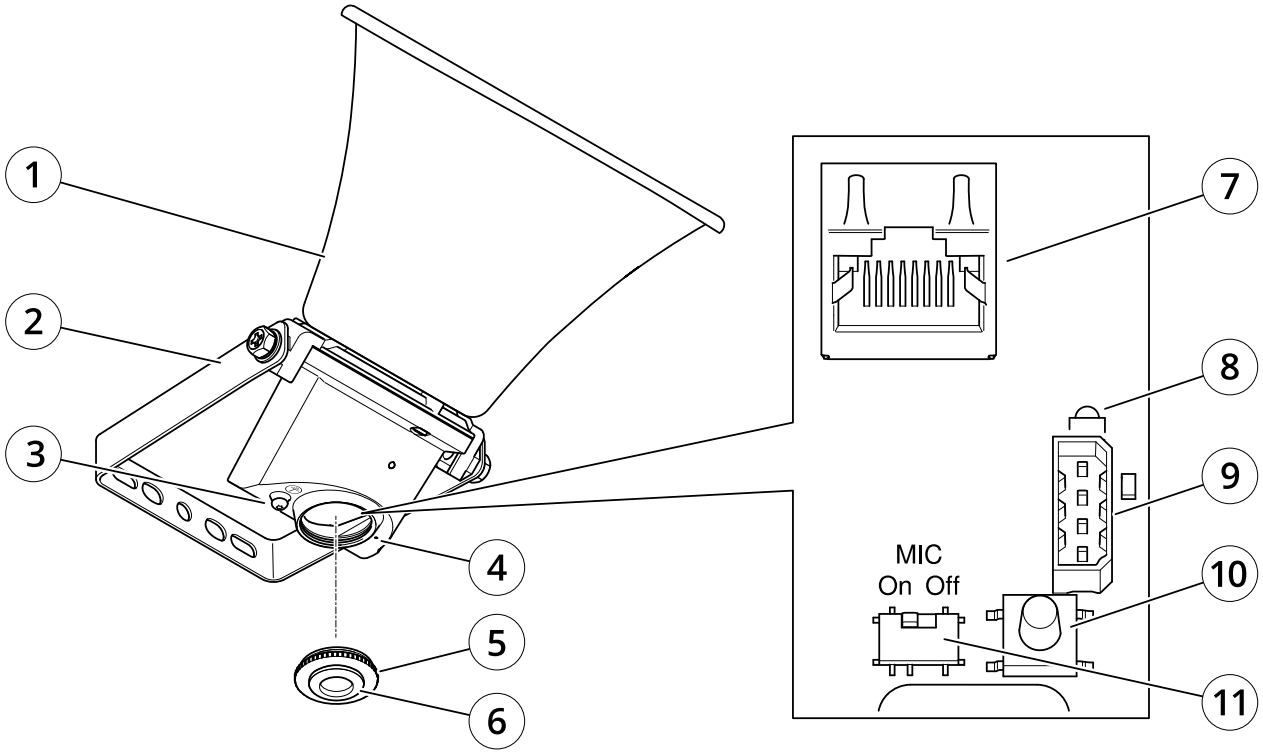
设置系统时，务必考虑不同设置和情况对所需带宽量（比特率）的影响。

以下因素是重要的考虑因素：

- 由于基础设施差而导致的网络利用率重负会影响带宽。
- 同时运行多个 AXIS Camera Application Platform (ACAP) 应用可能会影响整体性能。

规格

产品概述



1 喇叭型
2 支架
3 保护性接地端子
4 麦克风
5 盖帽
6 垫圈
7 网络连接器
8 状态 LED 指示灯
9 I/O端口
10 控制按钮
11 麦克风禁用开关

LED 指示灯

状态LED	指示
熄灭	正常运行时不亮。
绿色	启动完成后，指示灯稳定亮起10秒，表示正常工作。
淡黄色	在启动期间稳定。在设备软件升级过程中或重置为出厂默认设置时闪烁。
橙色/红色	如果网络连接不可用或丢失，指示灯闪烁。
红色	如果升级失败，指示灯缓慢闪烁。
红色/绿色	选择Locate device（本地设备）时快速闪烁。

按钮

控制按钮

控制按钮用于：

- 校准扬声器测试。按下并松开控制按钮，将播放测试音。
- 将产品重置为出厂默认设置。请参见 。

麦克风禁用开关

若要了解麦克风禁用开关的位置，请参见。

麦克风禁用开关用于机械**打开**或**关闭**麦克风。此开关的出厂默认设置为**开**。

连接器

保护性接地端子

⚠ 危险

触点危险。产品应使用接地线接地。确保接地线的两端与其各自的接地表面接触。

确保接地线尽可能较短，从而尽可能缩短电流通道。

网络连接器

采用以太网供电 (PoE) 的 RJ45 以太网连接器。

注意

该产品应使用屏蔽网络电缆 (STP) 进行连接。将产品连接到网络的电缆应用于其特定用途。确保根据制造商的说明安装网络设备。有关法规要求的信息，请参见 *www.axis.com* 上的安装指南。

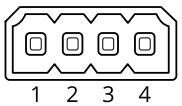
I/O 连接器

使用 I/O 连接器连接外部设备，并结合应用移动侦测、事件触发和报警通知等功能。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、通过事件或从设备网页接口进行激活。

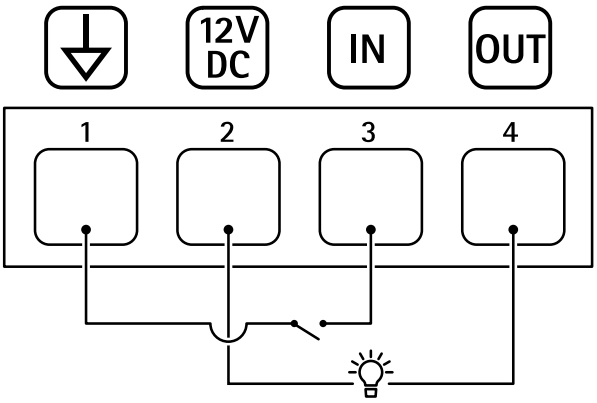
4 针接线端子



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 最大负载 = 25 mA

数字输入	3	连接至针脚 1 以启用，或保留浮动状态（断开连接）以停用。	0 至最大 30 V DC
数字输出	4	启用时内部连接至针 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。	0 至最大 30 V DC，开漏，100 mA

示例：



1 DC 接地
2 DC 输出 12 V，最大 25 mA
3 数字输入
4 数字输出

API 命令

VAPIX® 是 Axis 自有的开放式 API（应用程序编程接口）。您可以通过 VAPIX® 控制 Axis 设备中提供的功能。如需访问完整的VAPIX®文档，在*axis.com/developer–community*上加入安讯士开发人员社区

在网页浏览器中输入命令，并将 <deviceIP> 替换为设备的 IP 地址或主机名。

重要

API 命令会立即执行。如果您还原或重置您的设备，各设置都将会丢失。例如操作规则。

示例: Request
重启设备
Request
`http://<deviceIP>/axis-cgi/restart.cgi`

示例: Request
还原设备。该请求会使大多数设置恢复为默认值，但会保留 IP 编号。
Request
`http://<deviceIP>/axis-cgi/factorydefault.cgi`

示例: Request
重置设备。该请求会使包括 IP 编号在内的各设置恢复为默认值。
Request
`http://<deviceIP>/axis-cgi/hardfactorydefault.cgi`

示例: Request
请参见设备参数的列表。
Request
`http://<deviceIP>/axis-cgi/param.cgi?action=list`

示例: Request
获得调试档案
Request
`http://<deviceIP>/axis-cgi/debug/debug.tgz`

示例: Request
获得服务器报告
Request
`http://<deviceIP>/axis-cgi/serverreport.cgi`

示例: Request
获得 300 秒的网络追踪
Request
`http://<deviceIP>/axis-cgi/debug/debug.tgz?cmd=pcapdump&duration=300`

示例: Request
启用 FTP
Request
`http://<deviceIP>/axis-cgi/param.cgi?action=update&Network.FTP.Enabled=yes`

示例: Request
禁用 FTP
Request
`http://<deviceIP>/axis-cgi/param.cgi?action=update&Network.FTP.Enabled=no`

示例: Request
启用 SSH
Request
`http://<deviceIP>/axis-cgi/param.cgi?action=update&Network.SSH.Enabled=yes`

示例: Request
禁用 SSH
Request
`http://<deviceIP>/axis-cgi/param.cgi?action=update&Network.SSH.Enabled=no`

T10145506_zh

2024-09 (M20.2)

© 2020 – 2024 Axis Communications AB