AXIS C1410 Mk II Network Mini Speaker

用户手册

目录

解决方案概述

本手册介绍了如何使设备可访问您的音频系统，以及如何直接从其接口配置设备。

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 Pro — 用于大型系统的高级视频管理软件。
  - *AXIS Camera Station Pro 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™	Edge™	Firefox®	Safari®
Windows®	✓	✓	*	*
macOS®	✓	✓	*	*
Linux®	✓	✓	*	*
其他操作系统	*	*	*	*

✓：建议

*：支持，但有限制

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，则必须创建管理员帐户。请参见 *创建管理员帐户, on page 6*。

有关安装 AXIS OS 的设备网页界面中所有功能和设置的说明，请参阅 *AXIS OS 网页界面帮助*。

创建管理员帐户

首次登录设备时，您必须创建管理员帐户。

1. 请输入用户名。
2. 输入密码。请参见 *安全密码, on page 6*。
3. 重新输入密码。
4. 接受许可协议。
5. 单击**添加帐户**。

重要

设备没有默认帐户。如果您丢失了管理员帐户密码，则您必须重置设备。请参见 *重置为出厂默认设置, on page 21*。

安全密码

重要

使用 HTTPS（默认已启用）通过网络设置密码或其他敏感配置。HTTPS 可实现安全加密的网络连接，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。安讯士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 *重置为出厂默认设置, on page 21*。
   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

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 *产品概述, on page 18* 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 *点对点 SIP (P2PSIP), on page 14*。

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 *NAT 遍历, on page 15*。

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)

当用户代理将在 IP 网络内外进行通信时，应使用 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 *专用分支交换机 (PBX), on page 14*。

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 *设置直连 SIP (P2P), on page 8* 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。

了解更多信息，请参见*开始使用事件规则*。

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 **+ 添加接收者**。
   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 **+ 添加一个规则**。

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**）。

网页界面

要了解安装 AXIS OS 的设备网页界面中所有可用功能和设置，转到 *AXIS OS 网页界面帮助文档*。

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。

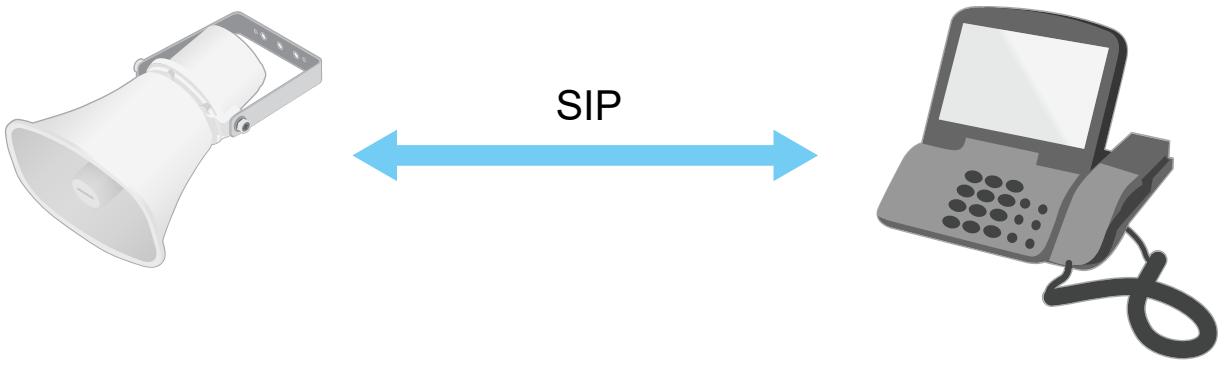
SIP 用户代理之间的实际音频或视频通过传输协议进行交换，例如 RTP（实时传输协议）。

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。

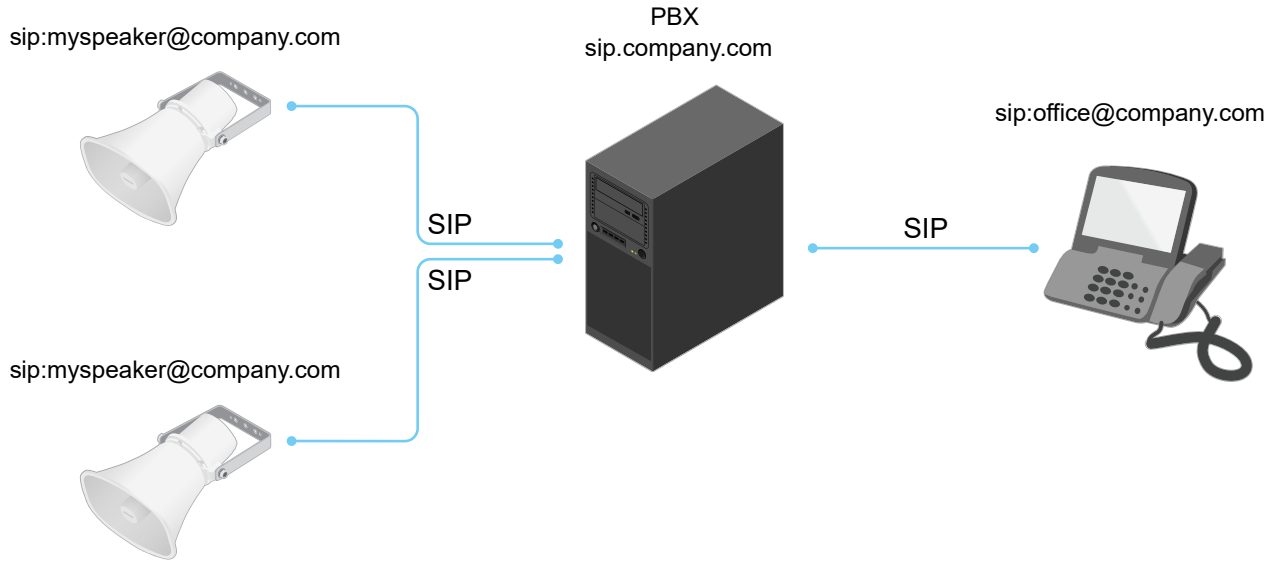
专用分支交换机 (PBX)

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。

分析与应用

借助分析与应用，您可以更充分地利用您的 Axis 设备。AXIS Camera Application Platform (ACAP) 是一个开放平台，使第三方能够为 Axis 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 Axis 分析与应用的用户手册，请转到 *help.axis.com*。

AXIS Audio Analytics

AXIS Audio Analytics 可在安装它的设备范围内侦测音量的突然增加和特定类型的声音，如尖叫声或喊叫声。这些检测可以配置为触发响应，例如录制视频、播放音频消息或向安保人员发出警报。要了解有关应用程序如何工作的更多信息，请参见 *AXIS Audio Analytics 用户手册*。

AXIS Client for Unified Communication Systems

通过此应用，您可以在支持 SIP 的 Axis 设备与关联的 Microsoft® Teams 账户之间进行通话。如需了解更多信息，请参阅 *AXIS Client for Unified Communication Systems 用户手册*。

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*。

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授权访问。它依托加密计算模块（安全元素和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。

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。

安全密钥库

一个防篡改保护的环境，可保护私钥并安全执行加密操作。在存在安全漏洞的情况下，它可防止非法访问和恶意提取。根据安全要求，安讯士设备可配备一个或多个基于硬件的加密计算模块，用于提供硬件保护型安全密钥库。根据安全要求，一个安讯士设备可拥有一个或多个基于硬件的加密计算模块，如 TPM 2.0（受信任的平台模块）或安全元素，以及/或用于提供硬件保护安全密钥库的 TEEE 型（受信任执行环境）。此外，所选的 Axis 产品具有一种 FIPS 140–2 2 级认证的安全密钥库。

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

加密文件系统

安全密钥库可通过对文件系统实施强效加密，以防止恶意信息提取和配置篡改。这可确保在设备未使用、实现对设备的未授权访问和/或安讯士设备被盗时，无法提取或篡改存储在文件系统中的数据。在安全启动过程中，可对读/写文件系统进行解密，并可将其安装并供安讯士设备使用。

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。

Axis 安全通知服务

Axis 提供通知服务，其中包含有关漏洞以及适用于安讯士设备的其他安全相关事项的信息。要接收通知，您可以在 *axis.com/security–notification–service* 订阅。

漏洞管理

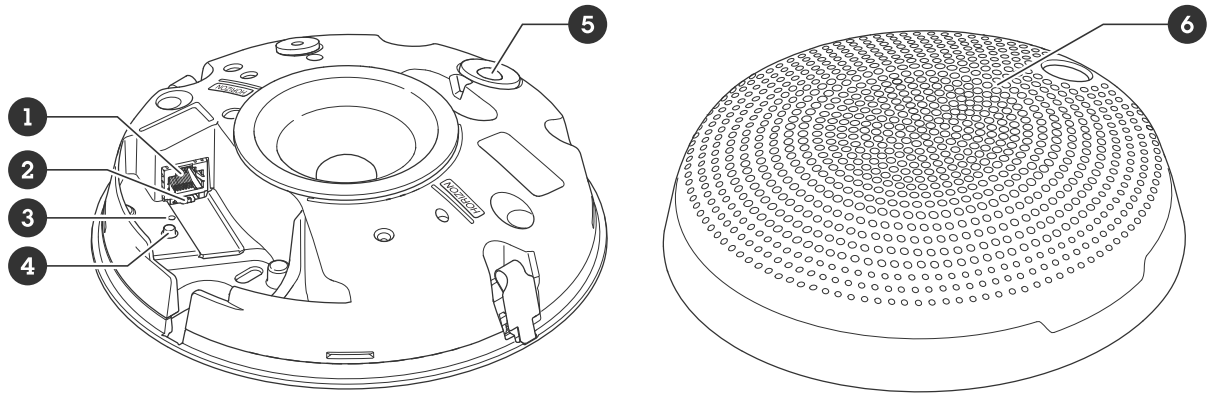
为了尽可能降低客户曝光风险、安讯士作为**常见漏洞和曝光 (CVE) 编号颁发机构 (CNA)**），遵循行业标准来管理和响应我们的设备、软件和服务中发现的漏洞。有关 Axis 漏洞管理策略、如何报告安全漏洞、已披露漏洞以及相应安全通报的更多信息，请参见 *axis.com/vulnerability–management*。

安讯士设备的安全操作

带有出厂默认设置的安讯士设备预配置了安全默认保护机制。我们建议您在安装设备时使用更多安全配置。如需了解有关安讯士网络安全方法的更多信息，包括保护设备安全的最佳实践、资源和指南，请转到 *axis.com/about–axis/cybersecurity*。

规格

产品概述



1 *网络连接器*
2 *麦克风开关*
3 *状态 LED 指示灯*
4 *控制按钮*
5 *PIR 传感器和前置 LED*
6 *外壳*

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 *重置为出厂默认设置, on page 21*。

麦克风禁用开关

若要了解麦克风禁用开关的位置，请参见 *产品概述, on page 18*。

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

网络连接器

采用以太网供电 (PoE) 的 RJ45 以太网连接器。

注意

该设备应使用隐蔽式网络电缆 (STP) 进行连接。将设备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。

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® 控制安讯士设备中提供的功能。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

在网络浏览器中输入命令，并将 <deviceIP> 替换为您设备的 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`

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 *产品概述, on page 18*。
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**。

AXIS OS 选项

Axis 可根据主动追踪或长期支持 (LTS) 追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，则建议使用主动追踪中的 AXIS OS。如果您使用第三方集成，则建议使用 LTS 追踪，其未针对主动追踪进行连续验证。使用 LTS，产品可维护网络安全，而无需引入重大功能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

- 升级设备软件时，您的预配置和自定义设置将被保存。安讯士公司无法保证设置会被保存，即使新版 AXIS OS 支持这些功能。
- 从 AXIS OS 12.6 开始，您必须安装设备当前版本与目标版本之间的各个 LTS 版本。例如，如果当前安装的设备软件版本为 AXIS OS 11.2，则必须先安装 LTS 版本 AXIS OS 11.11，才能将设备升级至 AXIS OS 12.6。有关更多信息，请参见：*AXIS OS 门户：升级路径*。
- 确保设备在整个升级过程中始终连接到电源。

注意

- 使用活动追踪中的新 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。

技术问题和可能的解决方案

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载了错误的 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

无法设置 IP 地址

- 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 地址可能已被其他设备使用。检查：
  1. 从网络上断开安讯士设备。
  2. 在 Command/DOS 窗口中，键入 `ping` 和设备的 IP 地址。
  3. 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。
  4. 如果您收到：`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。
- 可能与同一子网中的另一台设备存在 IP 地址冲突。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。

设备访问问题

通过浏览器访问设备时无法登录

启用 HTTPS 后，需在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`。

如果您遗失了根帐户密码，则必须将设备重置为出厂默认设置。有关说明，请参见 *重置为出厂默认设置, on page 21*。

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。

如有需要，您可以手动分配静态 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**。

该浏览器不受支持

有关推荐浏览器的列表，请参阅 *浏览器支持, on page 6*。

无法从外部访问设备

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 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*。

音频文件问题

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。请使用具有相同增益的剪辑。

MQTT 问题

无法通过 SSL 通过端口 8883 进行连接，MQTT 通过 SSL

防火墙会拦截使用 8883 端口的流量，因为该端口被判定为存在安全风险。

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。

设备操作问题

前加热器和雨刮器不工作

如果前加热器或雨刮器无法打开，请确认顶部外壳已正确固定在护罩单元底部。

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。

性能考虑

当您设置系统时，考虑不同设置和情况对所需带宽（比特率）的影响，这非常重要。

需要考虑的更重要的因素：

- 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。

联系支持人员

如果您需要更多帮助，请转到 *axis.com/support*。

T10208067_zh

2026-02 (M11.2)