AXIS D4100-VE Mk II Network Strobe Siren

用户手册

目录

安装 4
..... 4
开始 5
..... 5
在网络上查找设备 5
浏览器支持 5
打开设备的网页界面 5
创建管理员帐户 5
安全密码 5
配置设备 6
在安装警报之后关闭维护模式 6
打开维护模式 6
配置一个配置文件 6
导入或导出配置文件 6
设置直连 SIP (P2P) 6
通过服务器设置 SIP (PBX) 7
设置事件规则 7
触发响应 8
触发警报时启动配置文件 8
通过 SIP 启动配置文件 8
通过 SIP 分机控制多个配置文件 8
运行两个具有不同优先级的配置文件 9
当摄像机侦测到运动时通过虚拟输入激活频闪警报器 10
当摄像机侦测到运动时通过 HTTP POST 激活频闪警报器 11
当摄像机侦测到运动时激活 MQTT 上的频闪警报器 12
网页界面 15
了解更多： 16
会话初始化协议 (SIP) 16
点对点 SIP (P2PSIP) 16
专用分支交换机 (PBX) 16
NAT 遍历 16
规格 17
产品概览 17
..... 17
LED 指示灯 17
按钮 17
控制按钮 17
连接器 17
网络连接器： 17
I/O 连接器 18
光线模式名称 18
声音模式名称 19
清洁您的设备 21
故障排查 22
重置为出厂默认设置。 22
AXIS OS 选项 22
检查当前 AXIS OS 版本 22
升级 AXIS OS 22
技术问题和可能的解决方案 23
..... 24
性能考虑 24
联系支持部门 24
网络安全 25

漏洞管理 25
安全通知 25
安全产品生命周期 25

安装



开始

⚠ 警告

闪光或闪烁的指示灯会引发光敏性癫痫患者的发作。

在网络上查找设备

有关如何查找和分配 IP 地址的更多信息，前往*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：

*:支持但有功能限制

打开设备的网页界面

1. 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。参见 *创建管理员帐户, on page 5*。

有关搭载 AXIS OS 的设备网页界面中所有功能和设置的描述，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. 输入账户。
2. 输入密码。参见 *安全密码, on page 5*。
3. 重新输入密码。
4. 接受许可协议。
5. 单击**添加帐户**。

安全密码

重要

请使用安全超文本传输协议 (HTTPS)（默认已启用）通过网络设置密码或其他敏感配置。安全超文本传输协议 (HTTPS) 可启用安全且经过加密的网络连接，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。

配置设备

在安装警报之后关闭维护模式

⚠ 警示

为防止安装者听力受损和亮光导致眩晕，建议在安装设备时启用维护模式。

首次安装设备时，默认情况下处于维护模式打开状态。当设备处于维护模式时，警报不会发出声音，而光线会产生白色脉动光模式。

转到**概览** > **维护**以关闭**维护模式**。

打开维护模式

要执行设备服务，请转到**概览** > **维护**并打开**维护模式**。常规灯光和警报器活动将暂停。

配置一个配置文件

配置文件是一组配置的集合。您可以拥有多达 30 个具有不同优先级和模式的配置文件。

要设置一个新的配置文件：

1. 转到Profiles（**配置文件**），然后单击 ＋ Create（**创建**）。
2. 输入**名称**和**描述**。
3. 选择要用于配置文件的**光线**和**警报**设置。
4. 设置灯光和警报器**优先级**，然后单击**保存**。

要编辑配置文件，请单击 ⋮ 并选择Edit（**编辑**）。

导入或导出配置文件

如果您想要使用具有预定义配置的配置文件，则您可以导入它：

1. 转到Profiles（**配置文件**），然后单击 ＋ Import（**导入**）。
2. 浏览以查找文件，或拖放要导入的文件。
3. 单击Save（**保存**）。

要复制一个或多个配置文件并保存到其他设备，您可以导出它们：

1. 选择配置文件。
2. 单击**导出**。
3. 浏览以定位 .json 文件。

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。

有关设置选项的详细信息，请参见 *SIP*。

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 Allow incoming calls（**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。有关更多信息，请参见 *NAT 穿透*。

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 转 TCP** – 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 帐户向 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。

有关设置选项的详细信息，请参见 *SIP*。

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. 要添加新帐户，转到**系统** > **SIP** > **SIP 帐户**，然后单击 **+ 帐户**。
3. 输入您从 PBX 供应商处获得的详细信息。
4. 选择 **Registered（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。有关详细信息，请参见 *SIP*。

设置事件规则

了解更多信息，请参见*开始使用事件规则*。

触发响应

1. 转到 System（系统）> Events（事件）并单击 + Add a rule（+ 添加规则）。该规则可定义设备执行特定响应的时间。您可将规则设置为计划触发、定期触发或手动触发。
2. 输入一个**名称**。
3. 选择触发响应时必须满足的**条件**。如果为响应规则指定多个条件，则必须满足条件才能触发响应。
4. 选择满足条件时应执行何种Action（**操作**）。

触发警报时启动配置文件

本示例解释了如何在更改数字信号时触发警报。

设置端口的方向输入。

1. 转到**系统** > **附件** > I/O **端口**。
2. 转到**端口 1** > **正常状态**，然后单击**电路关闭**。

创建一个规则：

1. 转到**系统** > **事件** 并添加操作规则。
2. 为规则键入一个名称。
3. 在条件列表中，选择I/O > **数字输入激活**。
4. 选择**端口 1**。
5. 在响应列表中，选择**当规则处于活动状态时运行灯光和警报器配置文件**。
6. 选择要开始的配置文件。
7. 单击Save（**保存**）。

通过 SIP 启动配置文件

本示例解释如何使用 SIP 触发警报。

激活 SIP：

1. 转到**系统** > SIP > **事件**。
2. 选择**启用** SIP 并**允许拨入呼叫**。
3. 单击Save（**保存**）。

创建一个规则：

1. 转到**系统** > **事件** 并添加操作规则。
2. 为规则键入一个名称。
3. 在条件列表中，选择**呼叫** > **状态**。
4. 在状态列表中，选择**活动**。
5. 在响应列表中，选择**当规则处于活动状态时运行灯光和警报器配置文件**。
6. 选择要开始的配置文件。
7. 单击Save（**保存**）。

通过 SIP 分机控制多个配置文件

激活 SIP：

1. 转到**系统** > SIP > **事件**。
2. 选择**启用** SIP 并**允许拨入呼叫**。

3. 单击Save（保存）。

创建规则以启动配置文件：

1. 转到**系统** > **事件** 并添加操作规则。
2. 为规则键入一个名称。
3. 在条件列表中，选择**呼叫** > **状态更改**。
4. 在原因列表中，选择 **设备已接受**。
5. 在**呼叫方向**选项，选择**来电**。
6. 在**本地 SIP URI** 中，键入 < sip:[Ext]@[IP address]>，其中 [Ext] 是用于配置文件的扩展名，[IP address] 是设备地址。例如 sip:1001@192.168.0.90。
7. 在操作列表中，选择 Light and Siren（灯光和警报音）> Run light and siren profile（运行灯光和警报音配置文件）。
8. 选择要开始的配置文件。
9. 选择操作**开始**。
10. 单击Save（保存）。

创建规则以停止配置文件：

1. 转到**系统** > **事件** 并添加操作规则。
2. 为规则键入一个名称。
3. 在条件列表中，选择**呼叫** > **状态更改**。
4. 在原因列表中，选择**已终止**。
5. 在**呼叫方向**选项，选择**来电**。
6. 在**本地 SIP URI** 中，键入 sip:[Ext]@[IP address]，其中 [Ext] 是用于配置文件的扩展名，[IP address] 是设备地址。例如 sip:1001@192.168.0.90。
7. 在操作列表中，选择 Light and Siren（灯光和警报音）> Run light and siren profile（运行灯光和警报音配置文件）。
8. 选择要停止的配置文件。
9. 选择操作**停止**。
10. 单击Save（保存）。

重复上述步骤，为您要通过 SIP 控制的每个配置文件创建开始和停止规则。

运行两个具有不同优先级的配置文件

如果您运行两个具有不同优先级的配置文件，则具有较高优先级编号的配置文件将以较低的优先级编号中断配置文件。

注意

如果您运行两个具有相同优先级的配置文件，则新的配置文件将取消前一个。

本示例解释了如何设置设备，以在数字 I/O 端口触发时，优先级为 4 的配置文件的显示优先于另一个优先级为 3 的配置文件。

创建配置文件：

1. 创建优先级为 3 的配置文件。
2. 使用优先级 4 创建另一个配置文件。

创建一个规则：

1. 转到**系统** > **事件** 并添加操作规则。
2. 为规则键入一个名称。

3. 在条件列表中，选择I/O > **数字输入激活**。
4. 选择端口。
5. 在响应列表中，选择**当规则处于活动状态时运行灯光和警报器配置文件**。
6. 选择具有上限优先级编号的配置文件。
7. 单击Save（保存）。
8. 转到**配置文件**，并以下限优先级编号启动配置文件。

当摄像机侦测到运动时通过虚拟输入激活频闪警报器

本示例说明了如何将摄像机连接到频闪警报器，并在安装在摄像机中的应用程序 AXIS Motion Guard 侦测到运动时激活频闪警报器中的配置文件。

在您开始之前：

- 在频闪警报器中创建一个具有操作员或管理员角色的新账号。
- 在频闪警报器中创建一个配置文件。
- 在摄像机中设置 AXIS Motion Guard，并创建一个名为“摄像机配置文件”的配置文件。

在摄像机中创建两个接收者：

1. 在摄像机的设备界面中，转到**系统 > 事件 > 接收者**，然后添加一名接收者。
2. 输入以下信息：
   - Name（名称）：激活虚拟端口
   - Type（类型）：HTTP
   - URL：http://<IPaddress>/axis-cgi/virtualinput/activate.cgi
     将<IPaddress（IP 地址）>替换为频闪警报器的地址。
   - 新创建的频闪警报器的账号及密码。
3. 单击Test（测试），确保这些数据均有效。
4. 单击Save（保存）。
5. 使用以下信息添加第二个接收者：
   - Name（名称）：停用虚拟端口
   - Type（类型）：HTTP
   - URL：http://<IPaddress>/axis-cgi/virtualinput/deactivate.cgi
     将<IPaddress（IP 地址）>替换为频闪警报器的地址。
   - 新创建的频闪警报器的账号及密码。
6. 单击Test（测试），确保这些数据均有效。
7. 单击Save（保存）。

在摄像机中创建两个规则:

1. 转到 Rules（规则），然后添加一个规则。
2. 输入以下信息：
   - Name（名称）：激活虚拟 IO1
   - Condition（条件）：Applications（应用）> Motion Guard: Camera profile（运动保护：摄像机配置文件）
   - Action（响应）：通知 > 通过 HTTP 发送通知
   - Recipient（接收者）：激活虚拟端口
   - Query string suffix（查询字符串后缀）：schemaversion=1&port=1
3. 单击Save（保存）。

4. 使用以下信息添加另一个规则：
   - Name（名称）：停用虚拟 IO1
   - Condition（条件）：Applications（应用）> Motion Guard: Camera profile（运动保护：摄像机配置文件）
   - 选择**反转此条件**。
   - Action（响应）：通知 > 通过 HTTP 发送通知
   - Recipient（接收者）：停用虚拟端口
   - Query string suffix（查询字符串后缀）：schemaversion=1&port=1
5. 单击**Save（保存）**。

在频闪警报器中创建一个规则:

1. 在频闪警报器的网页界面中，转到**系统 > 事件**，然后添加一个规则。
2. 输入以下信息：
   - Name（名称）：在虚拟输入 1 上触发
   - Condition（条件）：I/O > Virtual input（虚拟输入）
   - Port（端口）：1
   - Action（响应）：Light and siren（灯光和警报器）> Run light profile while the rule is active（当规则处于活动状态时运行灯光和警报器配置文件）
   - **配置文件**：选择新建的配置文件
3. 单击**Save（保存）**。

当摄像机侦测到运动时通过 HTTP POST 激活频闪警报器

本示例说明了如何将摄像机连接到频闪警报器，并在安装在摄像机中的应用程序 AXIS Motion Guard 侦测到运动时激活频闪警报器中的配置文件。

在您开始之前：

- 在频闪警报器中创建一个具有操作员或管理员角色的新用户。
- 在频闪警报器中创建一个配置文件名为：“频闪警报器配置文件”。
- 在摄像机中设置 AXIS Motion Guard，并创建一个名为“摄像机配置文件”的配置文件。
- 确保使用安装了 10.8.0 或更高版本固件的 AXIS Device Assistant。

在摄像机中创建接收者：

1. 在摄像机的设备界面中，转到**系统 > 事件 > 接收者**，然后添加一名接收者。
2. 输入以下信息：
   - Name（名称）：声光报警器
   - Type（类型）：HTTP
   - URL：http://<IPaddress>/axis-cgi/siren_and_light.cgi
     将<IPaddress（IP 地址）>替换为频闪警报器的地址。
   - 新创建的频闪警报器用户的用户名和密码。
3. 单击**Test（测试）**，确保这些数据均有效。
4. 单击**Save（保存）**。

在摄像机中创建两个规则:

1. 转到 **Rules（规则）**，然后添加一个规则。
2. 输入以下信息：
   - Name（名称）：通过运动激活频闪警报器

- Condition（条件）：Applications（应用）> Motion Guard: Camera profile（运动保护：摄像机配置文件）
- Action（响应）：通知 > 通过 HTTP 发送通知
- Recipient（接收者）：闪光警报器.
  这些信息必须与您先前在 Events（事件）> Recipients（接收者）> Name（名称）下输入的信息相同。
- Method（方法）：POST
- 主体：

```
{  "apiVersion": "1.0",  "method": "start",  "params": {
"profile" : "Strobe siren profile"  } }
```

请确保在"profile" : <>下输入的信息与您在闪光警报器中创建配置文件时输入的信息一致，在本例中为：“频闪警报器配置文件”。

3. 单击Save（保存）。
4. 使用以下信息添加另一个规则：
   - Name（名称）：通过运动停用频闪警报器
   - Condition（条件）：Applications（应用）> Motion Guard: Camera profile（运动保护：摄像机配置文件）
   - 选择反转此条件。
   - Action（响应）：通知 > 通过 HTTP 发送通知
   - Recipient（接收者）：闪光警报器
     这些信息必须与您先前在 Events（事件）> Recipients（接收者）> Name（名称）下输入的信息相同。
   - Method（方法）：POST
   - 主体：

```
{  "apiVersion": "1.0",  "method": "stop",  "params": {    "profile" : "Strobe siren
profile"  } }
```

请确保在"profile" : <>下输入的信息与您在闪光警报器中创建配置文件时输入的信息一致，在本例中为：“频闪警报器配置文件”。

5. 单击Save（保存）。

当摄像机侦测到运动时激活 MQTT 上的频闪警报器

本示例说明了如何将摄像机连接到 MQTT 上的频闪警报器，并在安装在摄像机中的应用程序 AXIS Motion Guard 侦测到运动时激活频闪警报器中的配置文件。

在您开始之前：

- 在频闪警报器中创建一个配置文件。
- 设置 MQTT 代理并获取代理的 IP 地址、用户名和密码。
- 在摄像机中设置 AXIS Motion Guard。

在摄像机中设置 MQTT 客户端:

1. 在摄像机的设备界面中，转到系统 > MQTT > MQTT 客户端 > 代理，然后输入以下信息：
   - 主机：代理 IP 地址
   - Client ID（客户端 ID）:例如，摄像机 1
   - 协议：代理设置为的协议
   - Port（端口）：代理使用的端口号
   - 代理用户名和密码
2. 单击保存并连接。

在摄像机中创建两个用于 MQTT 发布的规则:

1. 转到 System（系统）> Events（事件）> Rules（规则），然后添加一项规则。
2. 输入以下信息：
   - Name（名称）：检测到的动作
   - 条件：应用 > 运动报警
   - 响应：MQTT > Send MQTT publish message（发送MQTT发布消息）
   - 主题：运动
   - 有效负载：开
   - QoS：0, 1 或 2
3. 单击Save（保存）。
4. 使用以下信息添加另一个规则：
   - Name（名称）：无运动
   - 条件：应用 > 运动报警
     - 选择反转此条件。
   - 响应：MQTT > Send MQTT publish message（发送MQTT发布消息）
   - 主题：运动
   - 有效负载：关
   - QoS：0, 1 或 2
5. 单击Save（保存）。

在明暗闪动警报中设置 MQTT 客户端：

1. 在明暗闪动警报的设备界面中，转到系统 > MQTT > MQTT 客户端 > 代理，然后输入以下信息：
   - 主机：代理 IP 地址
   - Client ID（客户端 ID）:警报声 1
   - 协议：代理设置为的协议
   - Port（端口）：代理使用的端口号
   - 用户名和密码
2. 单击保存并连接。
3. 转到 MQTT 订阅并添加订阅。
   输入以下信息：
   - 订阅筛选器：运动
   - 订阅类型：有状态
   - QoS：0, 1 或 2
4. 单击Save（保存）。

在用于 MQTT 订阅的明暗闪动警报中创建规则：

1. 转到 System（系统）> Events（事件）> Rules（规则），然后添加一项规则。
2. 输入以下信息：
   - Name（名称）：检测到的动作
   - 条件：MQTT > Stateful（有状态）
   - 订阅过滤器：运动
   - 有效负载：开

- Action（响应）：Light and siren（灯光和警报器）> Run light profile while the rule is active（当规则处于活动状态时运行灯光和警报器配置文件）
- 配置文件：选择要激活的配置文件。

3. 单击Save（保存）。

网页界面

如需阅读搭载 AXIS OS 的设备在网页界面中提供的所有功能和设置，请转到 *AXIS OS 网页界面帮助*。

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>`。

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。在这种情况中，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。

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

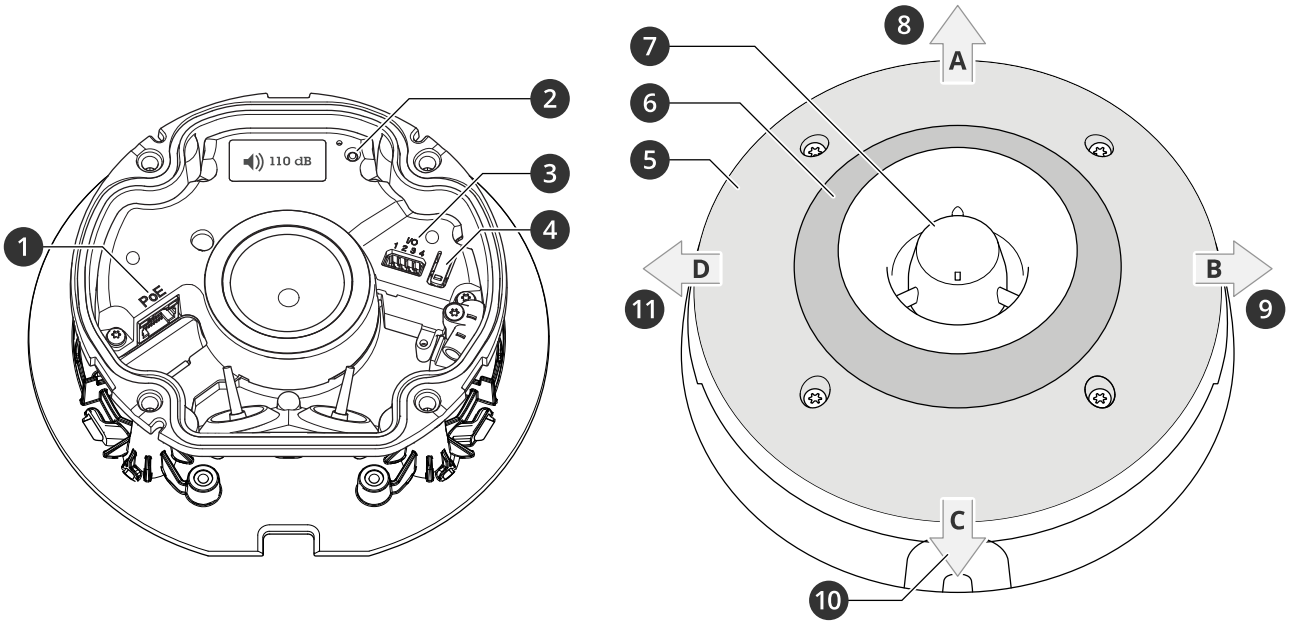
路由器要支持 NAT 穿越和 UPnP®。

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。

规格

产品概览



1 网络连接器 PoE
2 状态指示灯指示灯
3 I/O 连接器
4 控制按钮
5 白色 Led
6 RGBA（红色、蓝色、绿色、琥珀色）LED
7 警报声：
8 光线方向 A
9 光线方向 B
10 光线方向 C
11 光线方向 D

LED 指示灯

状态 LED	指示
绿色	启动完成后，将稳定显示绿色 10 秒，以表示正常工作。
琥珀色	在启动期间、重置为出厂默认设置过程中或在还原设置时常亮。

按钮

控制按钮

控制按钮用于：

- 将产品重置为出厂默认设置。参见 *重置为出厂默认设置。, on page 22*。
- 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：

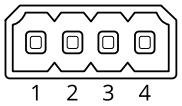
采用以太网供电 (PoE) 的 RJ45 以太网连接器。

I/O 连接器

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。

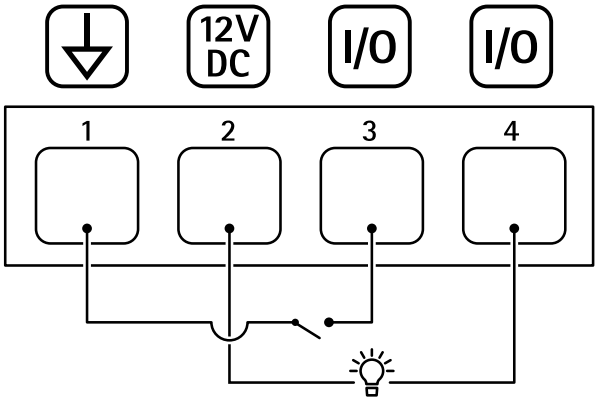
数字输出 – 用于连接继电器和 LED 等外部设备。已连接的设备可由 VAPIX® 应用程序编程接口、通过事件或从设备网页接口进行激活。

4 针接线端子



功能	针脚	注意	规格
DC 接地	1		0 VDC
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 VDC 最大负载 = 50 mA
可配置（输入或输出）	3–4	数字输入 – 连接到针 1 以启用，或保留浮动状态（断开连接）以停用。	0 至最大 30 VDC
		数字输出 – 启用时内部连接至引脚 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。	0 至最大 30 VDC，开漏，100 mA

示例:



1 *DC 接地*
2 *DC 输出 12 V，最大 50 mA*
3 *I/O 配置为输入*
4 *I/O 配置为输出*

光线模式名称

关
稳定
稳定白色 + 闪烁颜色
其他
脉冲

升级 3 个步骤
闪烁
闪烁 3x
闪烁 4x
闪烁 3x 淡出
闪烁 4x 淡化
闪烁 1x
闪烁 3x
闪烁 1x 白色 + 稳定颜色
闪烁 3x 白色 + 稳定颜色
方向 A + 稳定颜色
方向 B + 稳定颜色
方向 C + 稳定颜色
方向 D + 稳定颜色
旋转白色 + 稳定颜色
旋转尾白色 + 稳定颜色
随机白色 + 稳定颜色
旋转白色 + 稳定颜色
稳定白色 + 稳定颜色

声音模式名称

关
报警:警报高音调
报警:警报低音调
报警:鸟
报警:船喇叭
报警:汽车警报
报警:汽车警报快速
报警:传统时钟
报警:首个出席者
报警:恐怖
报警:工业
报警:单声报警音
报警:软故障四声报警音
报警:柔和三重音
报警:三重高音

通知：已拒绝
通知：完成
通知：记录
通知：失败
通知：赶快
通知：消息
通知：下一步
通知：打开
警报声：其他
警报声：弹性的
警报声：Evac
警报声：下降的音调
警报声：家庭柔和

清洁您的设备

您可以使用温水和温和的非研磨性肥皂清洁设备。

注意

- 刺激性化学品会损坏设备。请勿使用窗户清洁剂或丙酮等化学品来清洁设备。
- 避免在阳光直射或高温下清洁，因为这可能会导致污渍。

1. 使用罐装压缩空气，将灰尘及散落的灰尘从设备上移除。
2. 如有必要，请使用蘸有温水和温和的非研磨性肥皂的柔软超细纤维布清洁设备。
3. 为去除残留的清洁剂，请用蘸有温水的柔软超细纤维布擦拭设备。
4. 为避免污渍，请用干净的非研磨性布擦干设备。

如需更详细地了解安讯士设备的清洁，请参阅白皮书*常见清洁剂的化学耐受性*。

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。参见 *产品概览, on page 17*。
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：
   - **运行 AXIS OS 12.0 及更高版本的设备：**从本地链接地址子网 (169.254.0.0/16) 获取
   - **采用 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。前往**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 Axis 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. 前往设备的网页界面 > **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 生命周期指南：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，前往 *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. 前往**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

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 22*。

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，前往 *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。前往**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 5*。

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，前往 *axis.com/vms*。

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/代理可能不会提供用于 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/代理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。

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.

声音问题	
设备不会像预期那样大	检查设备是否已正确关闭，以及在触角或扬声器元素上是否没有障碍物。
设备不发出声音	检查设备是否处于**维护模式**。如果处于维护模式，请将其关闭。

光线问题	
设备不会像预期那样明亮	检查是否使用了 PoE 4 类电源。 检查设备的周边温度。如果设备安装在高温环境中，则光线将自动变暗。

性能考虑

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。

联系支持部门

如果您需要更多帮助，前往 *axis.com/support*。

网络安全

网络安全助力确保成功的产品生命周期管理，并将风险降至最低。您可以在 *axis.com/about–axis/cybersecurity* 上查阅有关我们网络安全策略的详细信息和文档。请遵循以下网络安全指南，以便接收安讯士发送的产品安全通知，并配置您的产品，以确保其整个生命周期及退役过程的安全。

在 *Axis Trust Center* 上，您可以了解安讯士如何落实安全合规、透明度、数据保护和隐私保护的信息。

漏洞管理

安讯士是*通用漏洞披露 (CVE) 编号授权机构 (CNA)* 之一。为了最大限度降低您所面临的风险，在对我们设备、软件及服务中的漏洞进行识别和修复时，我们始终遵循行业标准。如需了解我们漏洞管理政策的相关信息或报告漏洞，请访问 *axis.com/vulnerability–management*。

安全通知

请访问 *axis.com/security–notification–service* 订阅安讯士安全通知电子邮件。我们将向您发送有关您所使用的安讯士i产品中存在的漏洞、相应的安全公告及其他安全相关事项的信息。

安全产品生命周期

安讯士通过安全生命周期管理，在产品全生命周期内将风险降至最低。请访问 *help.axis.com* 查阅我们的强化配置指南，以更安全地配置和操作您的安讯士产品，并了解以下信息：

首次使用安全 – 安讯士产品预配置高强度默认保护，以确保从一开始就能实现安全的初始化及加密通信。

预期用途与常见配置错误 – 我们的指南提供有关安讯士产品预期用途的信息，包括应避免的常见安全相关误用和配置错误。

漏洞与供应链透明度管理 – 每次软件发布时，都会在 *axis.com* 上发布一份软件物料清单 (SBOM)，以披露漏洞并提高供应链透明度。

产品退役与数据安全擦除 – 当产品到达生命周期终点时，为实现安全退役，请将其恢复为出厂默认设置。这会擦除您的配置、存储数据和敏感信息。

T10223803_zh

2026-10 (M7.2)

© 2025 – 2026 Axis Communications AB