AXIS D4100-VE Mk II Network Strobe Siren

用户手册

目录

安装

开始使用

⚠ 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，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. 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 5*。

有关在设备的网页界面中控件和选项的说明，请参见 *网页界面, on page 16*。

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 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

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。

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。要更好地了解 P2P 的工作方式，请参见 *点对点 SIP (P2PSIP), on page 15*。

有关设置选项的详细信息，请参见 *SIP, on page 38*。

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 15*。

有关设置选项的详细信息，请参见 *SIP, on page 38*。

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 6* 了解更多信息。

设置事件规则

了解更多信息，请参见*开始使用事件规则*。

触发操作

1. 转到**系统 > 事件**并添加响应规则。该规则可定义设备执行特定操作的时间。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. 选择触发操作时必须满足的**条件**。如果为操作规则指定多个条件，则必须满足条件才能触发操作。
4. 选择在满足条件时应执行何种**操作**。

注意

- 如果您对一条处于活动状态的规则进行了更改，则必须重新开启该规则以使更改生效。

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. 在操作列表中，选择Run light and siren 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**）。
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. 在操作列表中，选择Run light and siren 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**）。
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. 在操作列表中，选择**Run light and siren 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）**。
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：
   - **名称**：激活虚拟端口
   - **Type（类型）**：HTTP
   - **URL**：http://<IPaddress>/axis-cgi/virtualinput/activate.cgi
     将<IPaddress>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**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：
   - **名称**：停用虚拟端口
   - **Type（类型）**：HTTP
   - **URL**：http://<IPaddress>/axis-cgi/virtualinput/deactivate.cgi
     将<IPaddress>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**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**规则**，然后添加一个规则。
2. 输入以下信息：

- **名称**：激活虚拟 IO1
- **条件**：Applications（应用）> Motion Guard: Camera profile（运动保护：摄像机配置文件）
- **操作**：通知 > 通过 HTTP 发送通知
- **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：
   - **名称**：停用虚拟 IO1
   - **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**。
   - **操作**：通知 > 通过 HTTP 发送通知
   - **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：
   - **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
   - **操作**：灯光和警报声 > 在规则处于活动状态时运行灯光和警报声配置文件
   - Profile（配置文件）：选择新创建的配置文件
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名为“Strobe siren profile”（频闪警报器配置文件）的配置文件。
- 在摄像机中设置AXIS Motion Guard，并创建一个名为“Camera profile”（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：
   - **名称**：声光报警器
   - Type（类型）：HTTP
   - URL：http://<IPaddress>/axis-cgi/siren_and_light.cgi
     将<IPaddress>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**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**规则**，然后添加一个规则。
2. 输入以下信息：
   - **名称**：通过运动激活频闪警报器
   - **条件**：Applications（应用）> Motion Guard: Camera profile（运动保护：摄像机配置文件）
   - **操作**：通知 > 通过 HTTP 发送通知
   - **接收者**：频闪警报器。
     这些信息必须与您先前在**事件 > 接收者 > 名称**下输入的信息相同。
   - **方法**：POST
   - **主体**：

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

确保在“‘profile’（配置文件）：<>”下输入的信息与您在频闪警报器中创建配置文件时输入的信息相同，在这种情况下为：“Strobe siren profile”（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：
   - **名称**：通过运动停用频闪警报器
   - **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**。
   - **操作**：通知 > 通过 HTTP 发送通知
   - **接收者**：声光报警器
     这些信息必须与您先前在**事件 > 接收者 > 名称**下输入的信息相同。
   - **方法**：POST
   - **主体**：

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

确保在“‘profile’（配置文件）：<>”下输入的信息与您在频闪警报器中创建配置文件时输入的信息相同，在这种情况下为：“Strobe siren profile”（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
- **客户端 ID**:例如，摄像机 1
- **协议**：代理设置为的协议
- **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**系统 > 事件 > 规则**，然后添加一个规则。
2. 输入以下信息：
   - **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**：打开
   - 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：
   - **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**：关闭
   - 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
   - **客户端 ID**:警报声 1
   - **协议**：代理设置为的协议
   - **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**系统 > 事件 > 规则**，然后添加一个规则。

2. 输入以下信息：
   - **名称**：检测到的动作
   - **条件**：MQTT > Stateful（**有状态**）
   - **订阅筛选器**：**运动**
   - **有效负载**：打开
   - **操作**：**灯光和警报声 > 在规则处于活动状态时运行灯光和警报声配置文件**
   - **配置文件**：选择要激活的配置文件。
3. 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>`。

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。

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。

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。

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。
- **更改帐户**：从当前帐户退出，然后登录新帐户。
- **退出**：从当前帐户退出。

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 和牌照的信息。
- **关于**：查看设备信息，包括 AXIS OS 版本和序列号。

状态

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。

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。

设备信息

显示设备相关信息，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。

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。

概述

LED 信号灯状态

显示在设备上运行的不同 LED 信号灯活动。LED 信号灯状态列表中可以同时运行高达十个活动。当同时运行两个或更多个活动时，具有较高优先级的活动显示 LED 信号灯状态。该行将在状态列表中突出显示。

警报声状态

显示在设备上运行的不同警报活动。警报声状态列表中可以同时运行高达十个活动。当同时运行两个或更多个活动时，将运行具有较高优先级的活动。该行将在状态列表中突出显示。

维护

维护模式：打开以在设备维护期间暂停灯光和警报活动。打开维护模式后，设备会显示一个三角形的白色脉动光图案，警报器也会静音。它可以保护安装人员免受听力损伤和耀眼强光的伤害。

维护优先级别为 11。只有具有更高优先级的系统特定活动才会中断维护模式。

维护模式重启后仍有效。例如，如果将时间设置为 2 小时，关闭设备并将其重新启动一小时后，设备将处于维护模式下又一个小时。

当您执行默认重置时，设备将返回到维护模式。

持续时间

- **连续**：选择让设备在关闭之前保持维护模式。
- **时间**：选择以设置将关闭维护模式的时间。

运行状况检查

检查：对设备进行健康检查，确定其灯光和警报器是否正常工作。设备将每次打开一个灯光段，并播放测试音。如果设备未通过健康检查，请查看系统日志了解更多信息。

为获得准确的结果，请确保在室温下进行健康检查。

配置文件

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。配置文件列出，以提供名称、优先级、灯光和警报器设置的概览。

创建：单击以创建配置文件。

- **预览/停止预览**：在保存配置文件之前开始或停止对其的预览。

注意

不能有两个同名的配置文件。

- **名称**：输入配置文件的名称。
- **描述**：输入配置文件的描述。
- **灯光**：从下拉菜单中选择想要的灯光的**模式**、**速度**、**强度**和**颜色**。
- **警报声**：从下拉菜单中选择想要的警报声的**模式**和**强度**。
- 仅开始或停止光线或警报的预览。
- **持续时间**：设置活动的持续时间。
  - **连续**：一旦启动，将一直运行，直到停止。
  - **时间**：为活动持续的时间设置一个指定的时间。
  - **重复**：设置活动应自我重复的次数。
- **优先级**：将活动的优先级设置为1到10之间的数字。优先级高于10的活动不能从状态列表中删除。有三种活动的优先级高于10：**维护** (11)、**识别** (12) 和**运行状况检查** (13)。

导入：添加一个或多个具有预定义配置的配置文件。

- **添加**：添加新配置文件。
- **删除和添加**：旧配置文件被删除，可以上传新的配置文件。
- **覆盖**：更新的配置文件覆盖现有配置文件。

要复制配置文件并将其保存至其他设备，选择一个或多个配置文件，然后单击**导出**。导出一个 .json 文件。

启动配置文件。配置文件及其活动出现在状态列表中。

选择Edit（**编辑**）、Copy（**复制**）、Export（**导出**）或Delete（**删除**）配置文件。

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 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。某些应用程序没有不同设置。

上下文菜单可包含以下一个或多个选项：

- **开源牌照**：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。
- **使用密钥激活牌照**：如果应用需要牌照，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。
  如果您没有牌照密钥，请转到 *axis.com/products/analytics*.您需要许可证代码和 Axis 产品序列号才能生成许可证密钥。
- **自动激活牌照**：如果应用需要牌照，则需要激活它。如果您的设备有互联网接入，请使用此选项。您需要牌照密钥来激活牌照。
- **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。

- Automatic date and time (PTP)（**自动日期和时间 (PTP)**）：使用精确时间协议进行同步。
- **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。
  - **受信任的 NTS KE CA 证书**：选择用于安全 NTS KE 时间同步的受信任 CA 证书，或选择不使用任何证书。
  - **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（v4 或 v6），然后才能选择此选项。如果两种版本都可用，设备优先选择 IANA 时区而非 POSIX 时区，并优先使用 DHCPv4 而非 DHCPv6。
  - DHCPv4 选择选项 100 用于 POSIX 时区，选择选项 101 用于 IANA 时区。
  - DHCPv6 选择选项 41 用于 POSIX，选择选项 42 用于 IANA。
- **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。

网络

IPv4

自动分配 IPv4：选择 IPv4 自动获取 IP 地址 (DHCP)，即可由网络自动分配您的 IP 地址、子网掩码和路由器，无需手动配置。我们建议大多数网络采用自动 IP 分配 (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。

注意

如果禁用 DHCP，依赖自动网络配置的功能（如主机名、DNS 服务器、NTP 等）可能停止工作。

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：

- **One–click（一键）：**这是默认选项。按下设备上的控制按钮，即可连接到 O3C。根据设备型号的不同，按下并松开或按住不放，直到状态 LED 指示灯闪烁。在 24 小时内向 O3C 服务注册设备，启用 **Always（总是）**选项并保持连接。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，就会保持连接。如果无法够到控制按钮，则使用此选项。
- **No（否）：**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号。

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。

拥有人身份验证密钥 (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 目标的团体名称。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 目标（只读目标除外）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。
    - **建立连接**：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。
  - **隐私**：选择用于保护您的SNMP数据的加密方式。
  - **“initial” 帐户密码**：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。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，请转至 *help.axis.com/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：

- **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+、FIPS 140-3 Level 3）**：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）**：选择使用 TPM 2.0 来实现安全密钥库。

加密策略

加密策略定义了如何使用加密来保护数据。

激活：选择应用于设备的加密策略：

- **默认 — OpenSSL**：兼顾安全和性能，适合一般用途。
- **FIPS — 符合 FIPS 140-2 的策略**：符合 FIPS 140-2 加密标准，适用于受监管行业。

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 Axis 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

防火墙：开启以启用防火墙。

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**）：允许与设备的所有连接。默认情况下设置此选项。
- DROP（**丢弃**）：阻止与设备的所有连接。

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（**过滤**）：选择允许或阻止来自与规则中定义标准相符的设备的连接。
  - **策略**：为防火墙规则选择 Accept（**接受**）或 Drop（**丢弃**）。
  - IP range（**IP 范围**）：选择以指定允许或阻止的地址范围。在 Start（**开始**）和 End（**结束**）中使用 IPv4/IPv6。
  - 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 或两者都是）。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**）：选择以指定允许或阻止的端口范围。将它们添加到Start（**开始**）和 End（**结束**）中。
  - **端口**：输入要允许或阻止访问的端口号。端口号必须介于 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**）：从一个发送方发送到一个接收方的流量。
    - BROADCAST（**广播**）：从一个发送方发送到网络上所有设备的流量。
    - MULTICAST（**组播**）：从一个或多个发送方发送到一个或多个接收方的流量。
- LIMIT（**限制**）：选择接受来自符合规则中定义标准的设备的连接，但应用限制以减少过多流量。
  - IP range（**IP 范围**）：选择以指定允许或阻止的地址范围。在 Start（**开始**）和 End（**结束**）中使用 IPv4/IPv6。
  - 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 或两者都是）。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**）：选择以指定允许或阻止的端口范围。将它们添加到Start（**开始**）和 End（**结束**）中。
  - **端口**：输入要允许或阻止访问的端口号。端口号必须介于 1 和 65535 之间。
  - Unit（**单位**）：选择允许或阻止的连接类型。
  - Period（**时段**）：选择与 Amount（**数量**）相关的时间段。
  - Amount（**数量**）：设置设备在设定 Period（**时段**）内的最大允许连接次数。最大数量为 65535。
  - Burst（**突发**）：在设定 Period（**时段**）内，输入允许超过设定 Amount（**数量**）一次的连接次数。一旦达到这个数字，就只允许在设定时段内的设定数量。
  - Traffic type（**流量类型**）：选择要允许或阻止的流量类型。
    - UNICAST（**单播**）：从一个发送方发送到一个接收方的流量。
    - BROADCAST（**广播**）：从一个发送方发送到网络上所有设备的流量。
    - MULTICAST（**组播**）：从一个或多个发送方发送到一个或多个接收方的流量。

Test rules（**测试规则**）：单击以测试已定义的规则。

- 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，单击可将防火墙回滚到之前的状态。
- Apply rules（**应用规则**）：单击此选项，可激活规则，而不执行测试。我们不建议您这样做。

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。

帐户

帐户

添加帐户：单击以添加新帐户。您可以添加多达 100 个帐户。

帐户：输入唯一的帐户名。

新密码：输入帐户的密码。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、更新和删除其他帐户。
- **操作员**：有权访问全部设置，以下各项除外：
  - 全部**系统**设置。

上下文菜单包括：

更新帐户：编辑帐户的属性。

删除帐户：删除帐户。无法删除根帐户。

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，而无需登录帐户。

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 帐户

添加SSH帐户：单击以添加新 SSH 帐户。

- **启用 SSH**：打开以使用 SSH 服务。

帐户：输入唯一的帐户名。

新密码：输入帐户的密码。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 帐户：编辑帐户的属性。

删除 SSH 帐户：删除帐户。无法删除根帐户。

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。选择以下任一方式：**基本**、**摘要**、OpenID 和**客户端凭证授予**。

HTTPS：选择使用 HTTPS。

上下文菜单包括：

- **更新虚拟主机**
- **删除虚拟主机**

客户端凭证授予配置

管理员声明：输入管理员角色的值。

验证 URL：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：单击以保存数值。

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 个操作规则。

添加规则：创建一个规则。

名称：为规则输入一个名称。

操作之间的等待时间：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。设施要执行操作必须满足的条件。如果定义了多个条件，则必须满足全部条件才能触发操作。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。

操作：从列表中选择操作，然后输入其所需的信息。有关特定操作的信息，请参见*开始使用事件规则*。

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 个接受者。

添加接受者：单击以添加接受者。

名称：为接受者输入一个名称。

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 帐户**：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：

查看接受者：单击可查看各收件人详细信息。

复制接受者：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。

删除接受者：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

终了证明（LWT）允许客户端在连接到中介时提供证明及其凭证。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。

Include condition（**包含条件**）：选择以包含描述 MQTT 主题中的条件的主题。

Include namespaces（**包含命名空间**）：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 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。
- **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。

帐户

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

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

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帐户，并将该帐户设置为默认，则您可以删除点对点帐户。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 帐户。

- **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 地址的对等帐户或域名时，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**：选择针对该帐户的 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。

帐户：选择将使用 DTMF 序列的帐户。如果选择**点对点**，则各帐户将共享相同的 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 帐户：选择要从中进行测试呼叫的帐户。

SIP 地址：输入SIP地址，然后单击测试帐户发起测试呼叫，验证帐户是否正常工作。

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。

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浏览图像的抓拍。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追踪之类敏感信息。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。
- **查看审核日志**：单击即可查看用户和系统活动的相关信息，例如，身份验证和配置的成功或失败情况。

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，向所有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 Axis 产品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。
- **自动回滚**：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

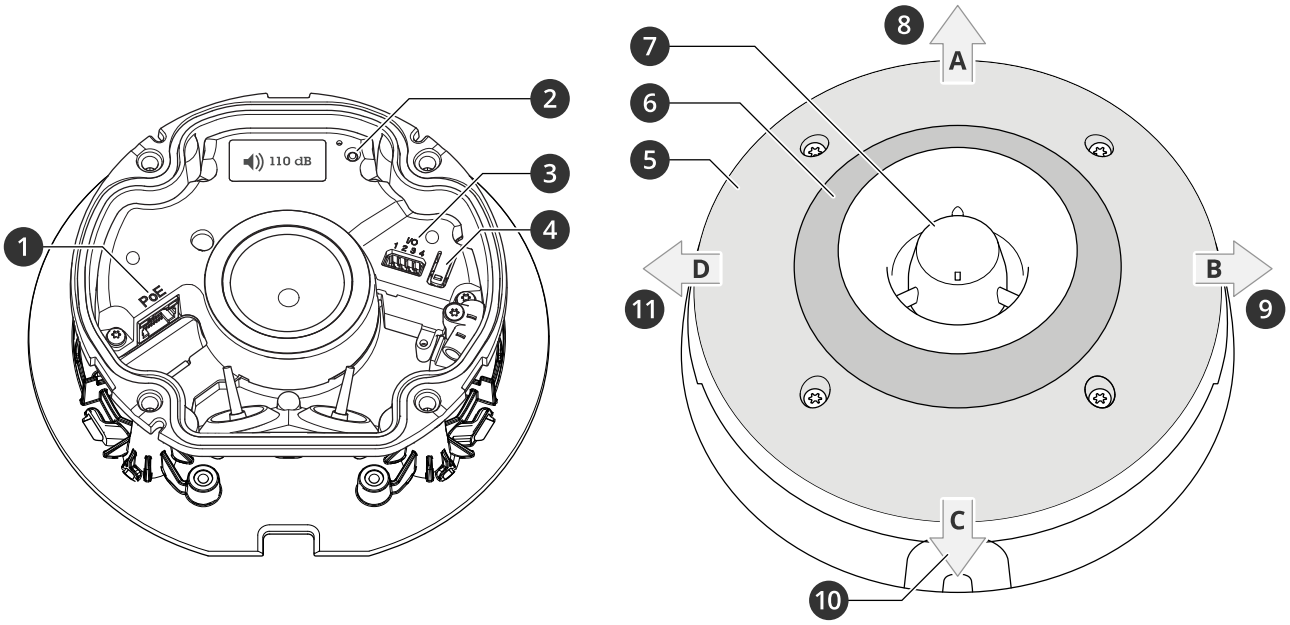
网络追踪文件可能包含敏感信息，例如证书或密码。

通过录制网络上的活动，网络追踪文件可帮助您排除问题。

追踪时间：选择以秒或分钟为单位的追踪持续时间，并单击**下载**。

规格

产品概述



1 网络连接器 PoE
2 状态 LED 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 报警器
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。
淡黄色	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。请参见 *重置为出厂默认设置, on page 51*。
- 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

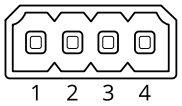
采用以太网供电 (PoE) 的 RJ45 以太网连接器。

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。

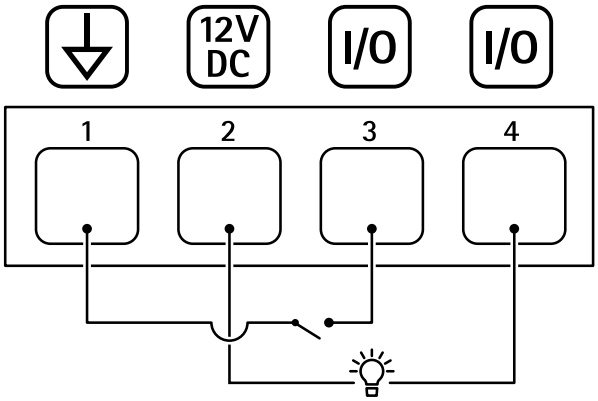
数字输出 – 用于连接继电器和 LED 等外部设备。已连接的设备可由 VAPIX® 应用程序编程接口、通过事件或从设备网页接口进行激活。

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。	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

关闭
稳定
稳定白色 + 闪烁颜色
其他

脉冲
升级 3 个步骤
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

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：接受
通知：正在呼叫
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。
- 请勿将洗涤剂直接喷洒在设备上。相反，在非研磨性布上喷洒洗涤剂并用它来清洁设备。
- 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. 为避免污渍，请用干净的非研磨性布擦干设备。

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 46*。
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 51*。

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 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，请转到 *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/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。

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。

联系支持人员

如果您需要更多帮助，请转到 *axis.com/support*。

T10223803_zh

2026-01 (M4.2)

© 2025 Axis Communications AB