AXIS I8307-VE Network Intercom

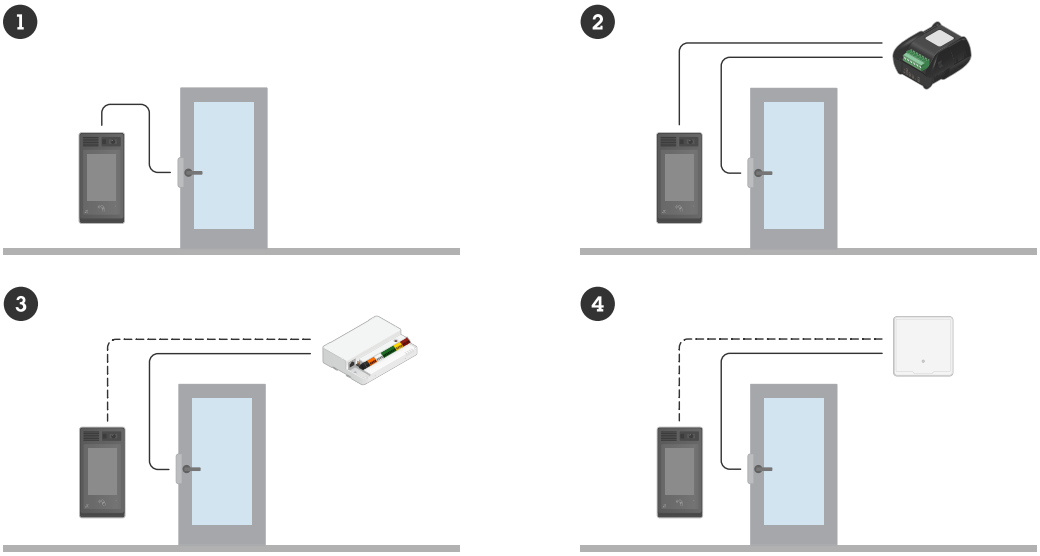
用户手册

目录

解决方案概述 4
安装 5
预览模式 5
开始 6
在网络上查找设备 6
浏览器支持 6
打开设备的网页界面 6
创建管理员帐户 6
安全密码 6
确保没有人篡改过设备软件 7
配置设备 8
校准并运行远程扬声器测试 8
设置直连 SIP (P2P) 8
通过服务器设置 SIP (PBX) 9
创建一位联系人 9
在显示屏上添加呼叫按钮 10
设置为读卡器 10
使用入口列表允许凭证持有者开门 10
使用门禁控制器设置为读卡器 11
使用卡上受保护的数据提高安全性 12
使用 DTMF 在显示屏上显示地图 12
网页界面 14
了解更多： 15
IP 语音 (VoIP) 15
会话初始化协议 (SIP) 15
点对点 SIP (P2PSIP) 15
专用分支交换机 (PBX) 16
NAT 遍历 16
设置事件规则 17
分析与应用 17
AXIS Client for Unified Communication Systems 17
规格 18
产品概览 18
LED 指示灯 19
SD 卡插槽 20
按钮 20
控制按钮 20
连接器 20
网络连接器： 20
音频连接器 20
中继连接器 20
读卡器连接器 21
I/O 连接器 21
电源连接器 22
连接设备 23
一个由 PoE (12V) 供电的继电器 23
两个由 PoE (12V) 供电的继电器 23
一个由 PoE (12V) 供电的继电器 + 一个由外部电源供电的继电器 24
一个由 PoE (12V) 供电的继电器 + 一个继电器无源触点 24
由对讲机 PoE+ 供电的 12V 断电闭门锁 25
由外部电源供电的断电闭门锁 25
一个由 PoE (24V) 供电的继电器 + 一个继电器无源触点 26
使用 OSDP 与门禁控制器连接的读卡器 26

使用 Wiegand 与门禁控制器连接的读卡器 27
使用 VAPIX 读卡器与安讯士门禁控制器连接的读卡器 27
故障排查 28
重置为出厂默认设置。 28
AXIS OS 选项 28
检查当前 AXIS OS 版本 28
升级 AXIS OS 28
技术问题和可能的解决方案 29
性能考虑 30
联系支持部门 31
安全信息 32
危险等级 32
其他消息等级 32
网络安全 33
漏洞管理 33
安全通知 33
安全产品生命周期 33

解决方案概述



1 *对讲机*
2 *与 AXIS A9801 结合的对讲机*
3 *与 AXIS A9210 结合的对讲机*
4 *与访问控制系统结合的对讲机*

安装

要观看此视频，请转到本文档的网页版本。

预览模式

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

要观看此视频，请转到本文档的网页版本。

该视频演示如何使用预览模式。

开始

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，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. 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。参见 *创建管理员帐户, on page 6*。

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 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。参见 *重置为出厂默认设置。, on page 28*。

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。

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。参见 *重置为出厂默认设置。, on page 28*。
   重置后，安全启动可保证设备的状态。
2. 配置并安装设备。

配置设备

本部分介绍了安装程序在硬件安装完成后启动和运行产品所需的全部重要配置。

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，扬声器则应重新校准。

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 *产品概览, on page 18*确认控制按钮。

设置直连 SIP (P2P)

VoIP（IP 语音）是一组支持通过 IP 网络进行语音和多媒体通信的技术。有关详细信息，请参见 *IP 语音 (VoIP), on page 15*。

在该设备中，VoIP 通过 SIP 协议启用。如需更多关于 SIP 的信息，请参见 *会话初始化协议 (SIP), on page 15*。

SIP 有两种安装形式。其中一种是点对点 (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。如需了解关于如何设置的信息，请参见 *点对点 SIP (P2PSIP), on page 15*。

1. 前往**通信 > 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**）。

注意

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

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

注意

- SIP **端口** – 对于 SIP 会话。通过此端口的信令流量为非加密。默认端口号为 5060。
- TLS **端口** – 对于 SIPS 和 TLS 保护的 SIP 会话。通过此端口的信令流量使用传输层安全协议 (TLS) 进行加密。默认端口号为 5061。
- RTP **起始端口** – SIP 呼叫中用于首个 RTP 媒体流的端口。默认起始端口为4000。有些防火墙可阻止某些端口号上的RTP通信。端口号必须在 1024 到 65535 之间。

8. 单击NAT **穿越**。

9. 选择要启用 NAT 穿越功能的协议。

注意

当设备从 NAT 路由器或防火墙后方连接到网络时，使用 NAT 穿越。如需更多信息，请参见 *NAT 遍历, on page 16*。

10. 单击**Save（保存）**。

通过服务器设置 SIP (PBX)

VoIP（IP 语音）是一组支持通过 IP 网络进行语音和多媒体通信的技术。有关详细信息，请参见 *IP 语音 (VoIP), on page 15*。

在该设备中，VoIP 通过 SIP 协议启用。如需更多关于 SIP 的信息，请参见 *会话初始化协议 (SIP), on page 15*。

SIP 有两种安装形式。其中一种是 PBX 服务器。当应在 IP 网络内外的无数用户代理之间进行通信时，使用 PBX 服务器。可以在设置中添加其他功能，具体取决于 PBX 供应商。有关详细信息，请参见 *专用分支交换机 (PBX), on page 16*。

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. 前往**通信 > SIP > 帐户**，然后单击 **+ 添加帐户**。
3. 输入帐户**名称**。
4. 选择 **Registered（已注册）**。
5. 选择一种传输模式。
6. 添加 PBX 供应商提供的帐户信息。
7. 单击**Save（保存）**。
8. 使用与点对点相同的方法创建SIP设置，请参见 *设置直连 SIP (P2P), on page 8*。使用 PBX 供应商的 RTP 启动端口。

创建一位联系人

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

要创建一位新联系人：

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

注意

有关 SIP 地址的信息，请参见 *会话初始化协议 (SIP), on page 15*。

5. 选择用于发出呼叫的 SIP 账户。

注意

可用性选项在**系统** > **事件** > **时间表**中定义。

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

注意

备用联系人是一个在原始联系人未作出回应或不可用时可将电话转接的对象。

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

在显示屏上添加呼叫按钮

本示例说明如何配置显示屏，以显示供来访者按下呼叫接待处的按钮。

在您开始之前：

- 创建接待联系人。有关说明，请参见 *创建一位联系人, on page 9*。

1. 转到 Display（**显示**）> Pages（**页面**）。
2. 在 Default Homepage（**默认主页**）上，单击 ⋮ 并选择 Edit（**编辑**）。
3. 单击 **+ 添加**。
4. 在 Type（**类型**）列表中，选择 Button（**按钮**）。
5. 在联系人列表中，选择接待处。
6. 选择按钮大小。
7. 如需保存按钮，请单击 Save（**保存**）。
8. 如需保存默认主页，请单击 Save（**保存**）。

设置为读卡器

您可以将对讲机设置为读卡器，以便凭证持有者开门。

通过使用入口列表，对讲机可在本地存储凭证，并能作为独立读卡器运行，最多支持五十名凭证持有者。

当对讲机连接至门禁控制器时，对讲机仍可存储多达五十条凭证。如果在入口列表中找到请求的凭证，对讲机将管理相应的访问权限。如果请求的凭证未在入口列表中找到，且已启用 Use connected door controller（**使用已连接的门禁控制器**）选项，则请求将转发至门禁控制器，由其管理访问权限。

使用入口列表允许凭证持有者开门

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

前提条件：

- 确保在**读取器** > **芯片类型**中激活正确的芯片类型。

打开入口列表并添加凭证持有者：

1. 转到**读卡器** > **入口列表**。
2. 打开**使用入口列表**。
3. 单击 **+ 添加凭证持有者**。
4. 输入凭证持有者的名字和姓氏。名字必须是唯一的。
5. 选择**卡**。
6. 在设备上刷凭证持有者的卡，然后单击**获取新版本**。

7. 保留事件条件**授予访问权限**。
8. 在**有效期至**下，选择**次数**。
9. 在 Number of times（**次数**）中，输入 10。
10. 单击Save（**保存**）。

创建一个规则：

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

使用门禁控制器设置为读卡器

网络连接

要将对讲机用作一个读卡器，则您可将其连接至一个门禁控制器。该门控制器存储凭证并保持追踪允许进门的人员。在此情况下，我们通过网络连接设备。我们还修改允许的卡类型。

重要

网络连接仅对 Axis 门禁控制器有用。要连接至某个非 Axis 门禁控制器，您需要用电线物理连接这些设备。参见 *有线连接, on page 11*。

将对讲机设置为一个读卡器

1. 转到**读卡器 > 连接**。
2. 选择 VAPIX **阅读器**协议类型。
3. 选择用于与门禁控制器通信的协议。

注意

如果您使用的是 HTTPS，我们建议打开**验证证书**。

4. 输入门禁控制器的 IP 地址。
5. 输入门禁控制器的凭证。
6. 单击 Connect（**连接**）。
7. 选择适当门的入口读取器。
8. 单击Save（**保存**）。

有线连接

要将门站用作一个读卡器，则您可将其连接至一个门禁控制器。该门控制器存储凭证并保持追踪允许进门的人员。在此示例中，我们通过电线连接设备，我们使用 Wiegand 协议，激活蜂鸣器并使用一个适用于 LED 的 I/O 端口。我们还修改允许的卡类型。

重要

使用尚未使用的 I/O 端口。如果您使用了已经使用的 I/O 端口，那么针对这些端口创建的事件都将停止工作。

在您开始之前：

- 将对讲机连接至某个门禁控制器。
  请参见电气接线图，您可以在 *连接设备, on page 23*中找到。

- 使用针对阅读器的 Wiegand 协议配置该门禁控制器的硬件。有关说明的信息，请参见门禁控制器用户手册。

将对讲机设置为一个读卡器

1. 转到**读卡器 > 连接**。
2. 选择Wiegand作为协议类型。
3. 打开 **蜂鸣器**。
4. 在**蜂鸣器输入**下，选择 I3。
5. 在**用于 LED 控制的输入**中，选择 1。
6. 在 LED1 **输入**下，选择 I1。
7. 选择不同状态所使用的颜色。
8. 在 **按键格式**下，选择 FourBit。
9. 单击Save（保存）。
10. 转到**读卡器 > 芯片类型**并激活要使用的芯片类型。

注意

您可以保留默认的芯片类型集，但我们建议根据您的具体需求修改该列表。

11. 单击**添加数据集** 以指定不同芯片类型的数据组。
12. 单击Save（保存）。

使用卡上受保护的数据提高安全性

为了提高访问控制系统的安全性，您可以选择使用存储在某些类型卡上的安全卡数据。数据受密钥保护。要读取卡数据，您需要将密钥和有关卡的其他信息存储在设备上。

1. 转到**读卡器 > 芯片类型**。
2. 在**数据集**下，选择要编辑的芯片类型，然后单击**添加数据集**。
3. 输入有关卡数据的信息。输入什么信息取决于卡的类型和登记方式。
4. 如果使用 OSDP 或 Wiegand 协议，请选择**作为 UID 使用**以 UID/CSN 而不是普通卡 UID/CSN 的形式发送安全数据。
5. 要仅允许符合指定卡数据的卡发送到门禁控制器，请选择**所需的数据**。不符合要求的卡片会被读卡器静默忽略。
6. 单击Save（保存）。

使用 DTMF 在显示屏上显示地图

当来访者用对讲机拨打电话需要方向指引时，接听人可以使用 DTMF（双音多频）信号在对讲机的显示屏上显示地图。

本示例说明了如何进行操作：

- 将地图图像上传到对讲机。
- 在对讲机中创建一个包含地图图像的页面。
- 定义对讲机的 DTMF 序列。
- 设置对讲机显示地图页面 30 秒，作为对 DTMF 序列的响应。

在您开始之前：

- 允许从该设备进行 SIP 呼叫并创建一个 SIP 账户。有关说明，请参见 *设置直连 SIP (P2P), on page 8*和 *通过服务器设置 SIP (PBX), on page 9*。

上传地图图像

1. 转到 Media（媒体）。

2. 单击 **+ 添加**。
3. 拖放显示建筑物地图的图像。建议图像分辨率为 480x800 像素，最大分辨率为 2048x2048 像素。
4. 单击**Save（保存）**。

为显示屏创建地图页面

5. 转到 **Display（显示）> Pages（页面）**。
6. 单击 **+ 添加**。
7. 键入页面名称，例如 Map page（地图页面）。
8. 单击 **+ 添加**。
9. 在类型列表中，选择 **Image（图像）**。
10. 键入图像名称，例如 Map page（地图图像）。
11. 在图像列表中，选择地图图像。
12. 单击**Save（保存）**。
13. 再次单击 **Save（保存）**。

定义 DTMF 序列

14. 前往**通信** > SIP> DTMF。
15. 单击**+ 添加序列**。
16. 在 **Sequence（序列）**中，键入 9。
17. 在 **Description（描述）**中，键入 Show map（显示地图）。
18. 选择账户。
19. 单击**Save（保存）**。

创建一个规则。

20. 转到 **System（系统）> Events（事件）> Rules（规则）**，然后添加一项规则。
21. 键入规则名称，例如 Use DTMF to show map（使用 DTMF 显示地图）。
22. 在条件列表中，选择 **Call（呼叫）> DTMF**。
23. 在 DTMF 事件 ID 列表中，选择 **Show map（显示地图）**。
24. 在响应列表中，选择 **Display（显示）> Show page（显示页面）**。
25. 在页面列表中，选择 **Map page（地图页面）**。
26. 在 **Duration（持续时间）**中，输入 00:00:30 显示地图 30 秒。
27. 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*。

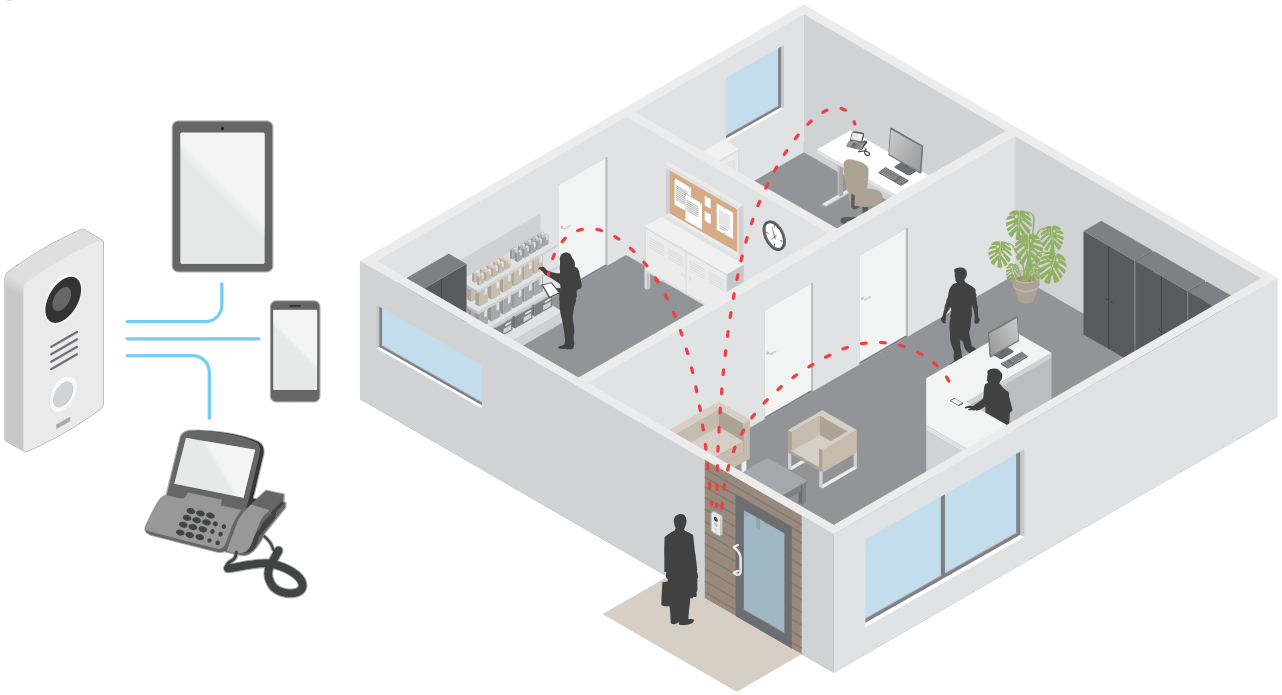
了解更多：

IP 语音 (VoIP)

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

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

示例：



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

会话初始化协议 (SIP)

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

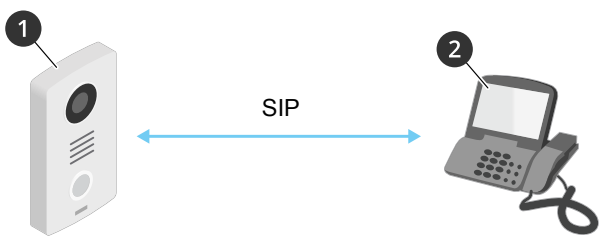
SIP 用户代理之间的实际音频或视频通过传输协议进行交换，例如 RTP（实时传输协议）。

您可以使用点对点设置在本地网络上或使用 PBX 在各网络间进行呼叫。

点对点 SIP (P2PSIP)

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

示例：



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

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

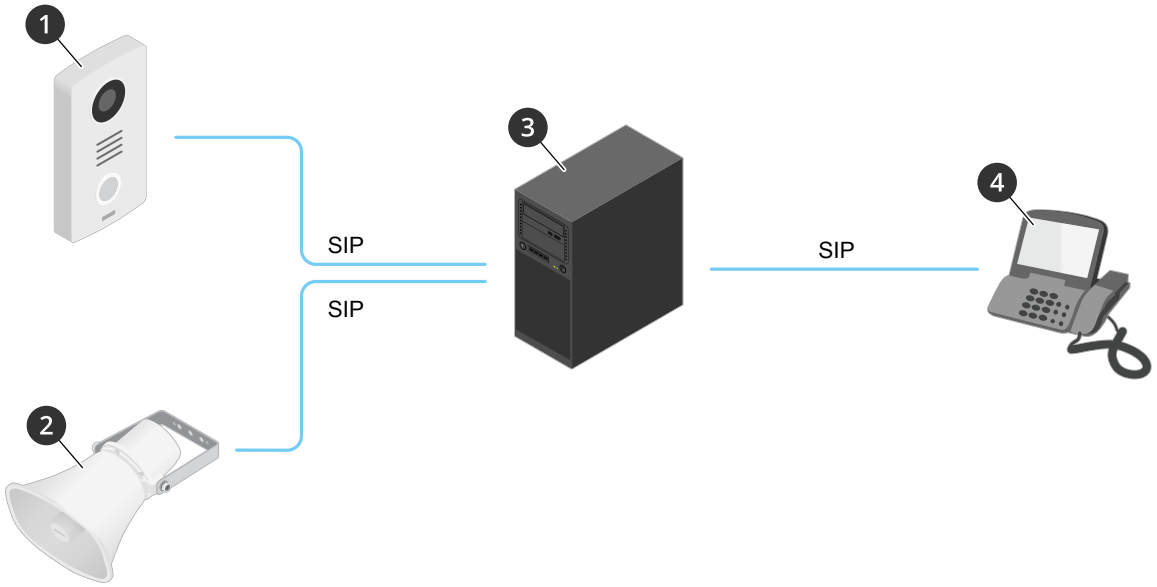
专用分支交换机 (PBX)

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

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

每个 SIP 用户代理都需注册 PBX，随后才能拨打正确的电话分机联系其他人。在这种情况中，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。

示例:



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

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

NAT 遍历

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

注意

路由器要支持 NAT 穿越和 UPnP®。

每个 NAT 穿越协议可单独使用或组合使用，具体取决于网络环境。

- **ICE** ICE（交互式连接建立）协议可增加找到对等设备之间进行成功通信的更有效路径的机率。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。

设置事件规则

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

了解更多信息，请参见*开始使用事件规则*。

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。

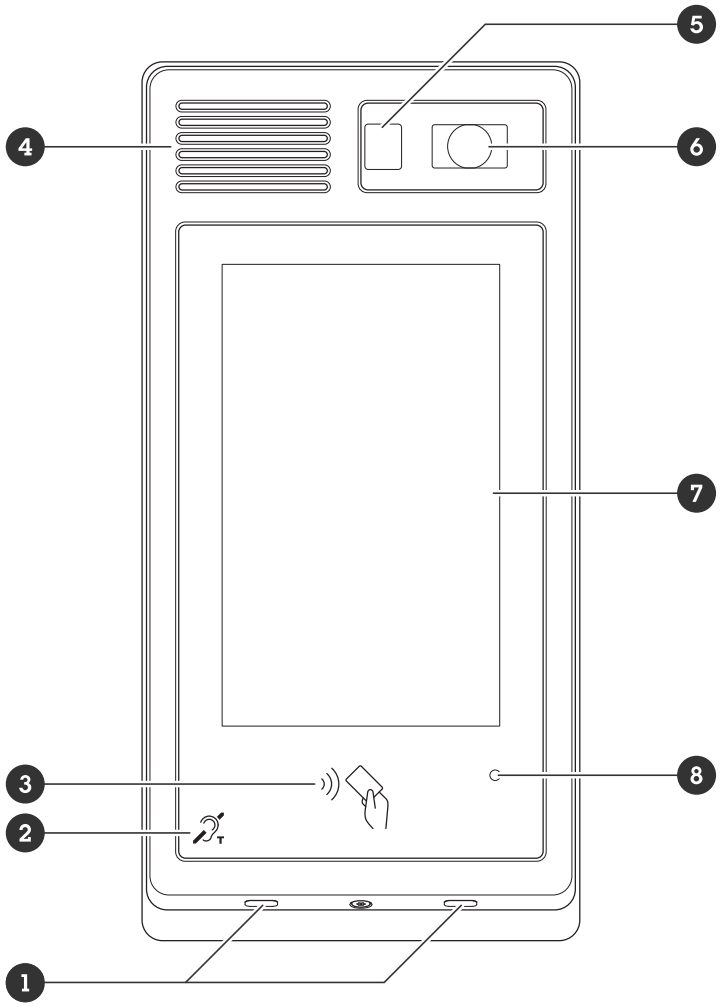
要查找 Axis 分析与应用的用户手册，请转到 *help.axis.com*。

AXIS Client for Unified Communication Systems

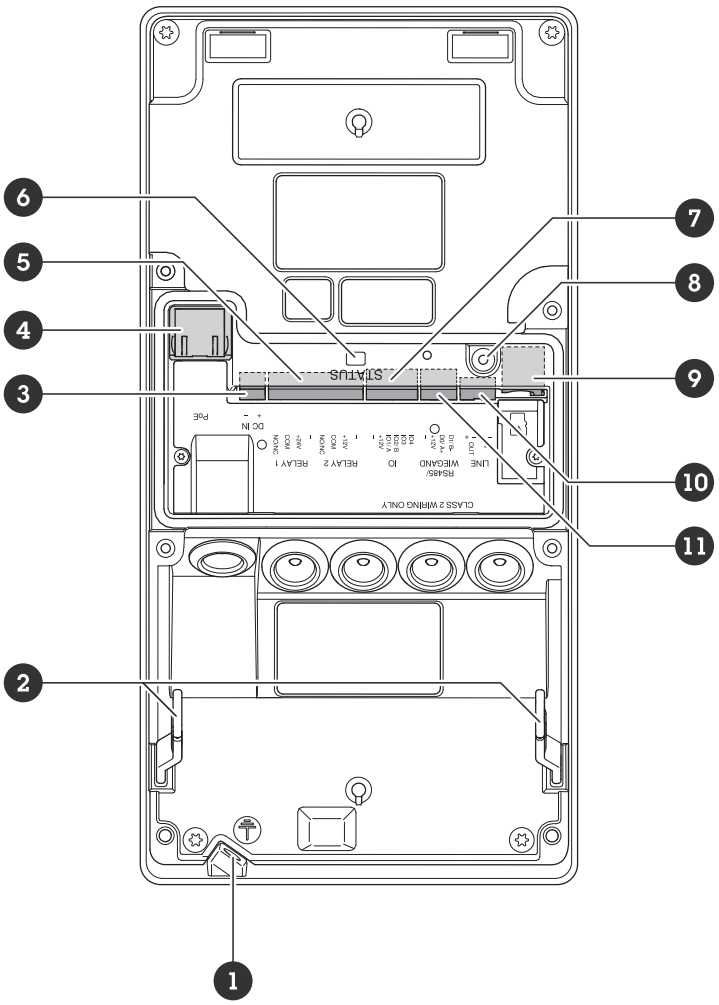
通过此应用，您可以在支持 SIP 的 Axis 设备与关联的 Microsoft® Teams 账户之间进行通话。如需了解更多信息，请参阅 *AXIS Client for Unified Communication Systems 用户手册*。

规格

产品概览



1 *麦克风（2 个）*
2 *T–coil*
3 *RFID 读卡器*
4 *扬声器*
5 *PIR 传感器*
6 *摄像机*
7 *显示*
8 *光传感器*



1 *接地螺丝*
2 *安装铰链*
3 *电源连接器*
4 *网络连接器：*
5 *中继连接器 (2 个)*
6 *状态 LED*
7 *I/O 连接器*
8 *控制按钮*
9 *SD 卡插槽 (microSD)*
10 *音频连接器*
11 *读卡器连接器*

LED 指示灯

状态 LED	指示
绿色	稳定绿色表示正常工作。

SD 卡插槽

注意

- SD 卡可能损坏。插拔 SD 卡时，请勿使用尖锐工具、金属物品或用力过猛。请用手指捏住 SD 卡进行插拔。
- 数据丢失和录制内容损坏的风险。移除 SD 卡之前，请从设备的网页接口上卸载 SD 卡。产品运行时，请勿取出 SD 卡。

本设备支持 microSD/microSDHC/microSDXC 卡。

有关 SD 卡的建议，请参见 *axis.com*。

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

按钮

控制按钮

控制按钮用于：

- 将产品重置为出厂默认设置。参见 *重置为出厂默认设置。, on page 28*。

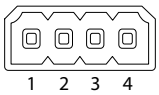
连接器

网络连接器：

采用以太网供电 增强版 (PoE+) 的 RJ45 以太网连接器。

音频连接器

用于音频输入和输出的 4 针接线端子。

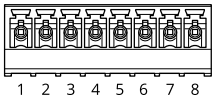


功能	引脚	注意
线路输入	1	线路输入（单声道）
接地	2	音频接地
线路输出	3	线路输出
接地	4	音频接地

中继连接器

用于可通过以下方式使用的固态继电器的 8 针接线端子：

- 作为开启和关闭辅助电路的一个标准继电器。
- 直接控制一个锁。
- 通过一个安全继电器控制一个锁。在门的安全侧上使用一个安全继电器可避免线路发热。



功能	引脚	注意	规格
NO/NC	1	常开/常闭 用于连接中继设备。 这两个继电器引脚与其余电路电位隔离。	最大电流1 A 最大电压30 V DC
COM	2	公共	
24 V DC	3	用于为辅助设备供电。 注意:此针只能用作电源输出。	输出电压 24 V DC 最大电流50 mA[1] 最大电流300 mA[2]
DC 接地	4		0 V DC
NO/NC	5	常开/常闭 用于连接中继设备。 这两个继电器引脚与其余电路电位隔离。	最大电流1 A 最大电压30 V DC
COM	6	公共	
12 V DC	7	用于为辅助设备供电。 注意:此针只能用作电源输出。	输出电压12 V DC 最大电流100 mA[1] 最大电流600 mA[2]
DC 接地	8		0 V DC

读卡器连接器

用于连接外部阅读器的 4 针接线端子。

功能	引脚	注意	规格
DC 接地	1		0 V DC
12 V DC	2	用于为辅助设备供电。 注意:此针只能用作电源输出。	输出电压 12 V DC
D0/A+	3	Wiegand:DATA0输出 RS485：A+	
D1/B–	4	Wiegand:DATA1输出 RS485：B–	

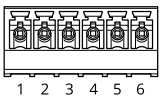
I/O 连接器

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 VDC 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。

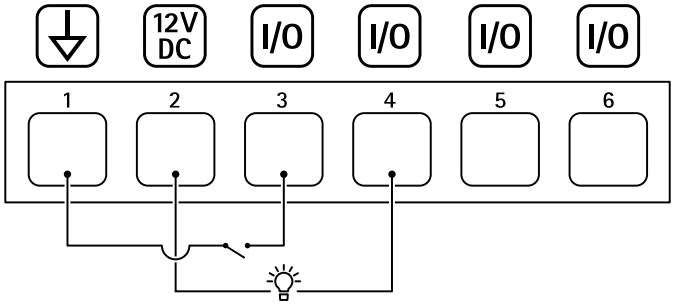
数字输出 – 用于连接继电器和 LED 等外部设备。已连接的设备可由 VAPIX® 应用程序编程接口、通过事件或从设备网页接口进行激活。

1. 通过*IEEE 802.3af/802.3at 1*型*3*类以太网供电时。
2. 通过*IEEE 802.3at 2*型*4*类增强型以太网供电 *(PoE+)* 或直流电源输入供电时。



功能	引脚	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）	3–6	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*
5 *可配置的 I/O*
6 *可配置的 I/O*

电源连接器

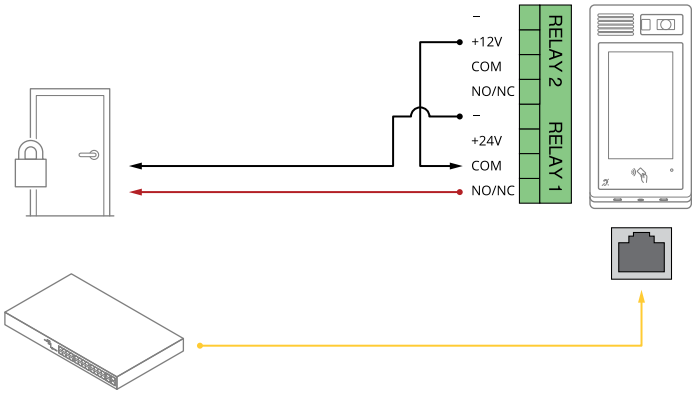
用于 DC 电源输入的双针接线端子。使用额定输出功率限制为 ≤100 W或额定输出电流限制为 ≤5 A 且符合安全超低电压 (SELV) 要求的限制电源 (LPS)。



功能	引脚	注意	规格
DC 接地	1		0 V DC
DC 输入	2	在未使用以太网供电时，可用于给控制器供电。 注意:此引脚只能用作电源输入。	18–28 V DC，最大 22 W 输出上的最大负载9 W

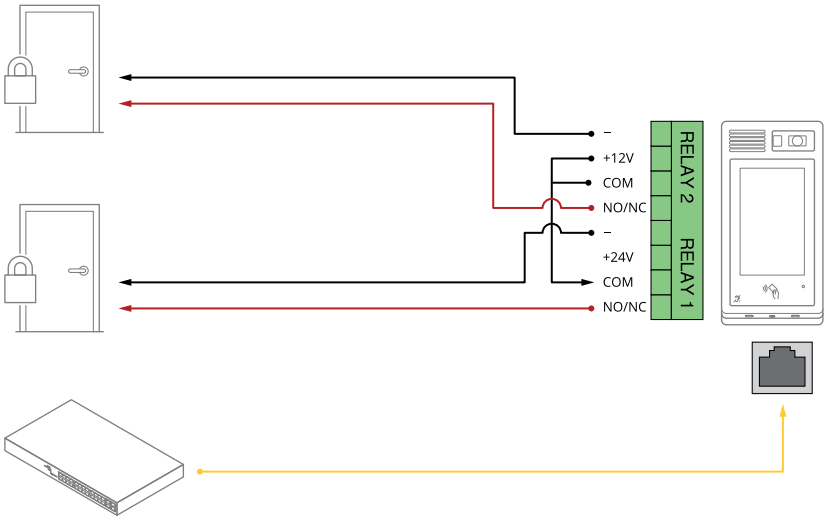
连接设备

一个由 PoE (12V) 供电的继电器



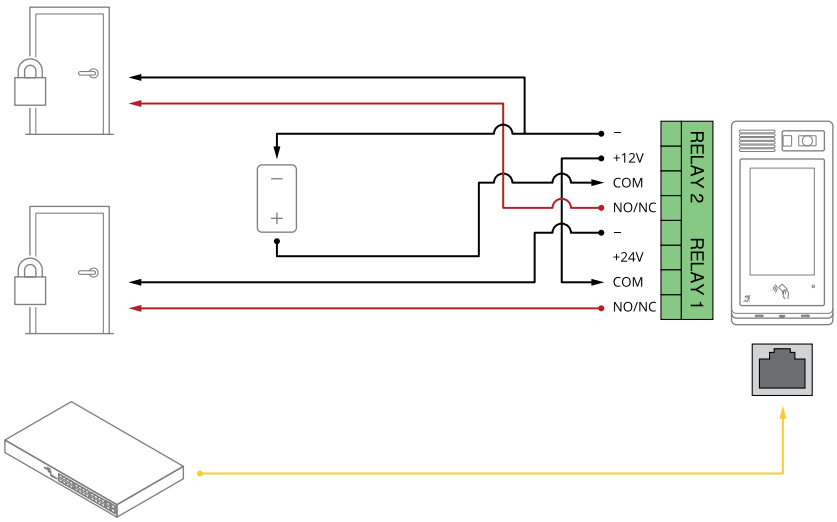
1. 要检查继电器状态，前往**系统 > 附件**，并找到继电器端口。
2. 将**正常状态**设置为：
   - ，适用于断电闭门锁。
   - ，适用于自动防故障锁。

两个由 PoE (12V) 供电的继电器



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

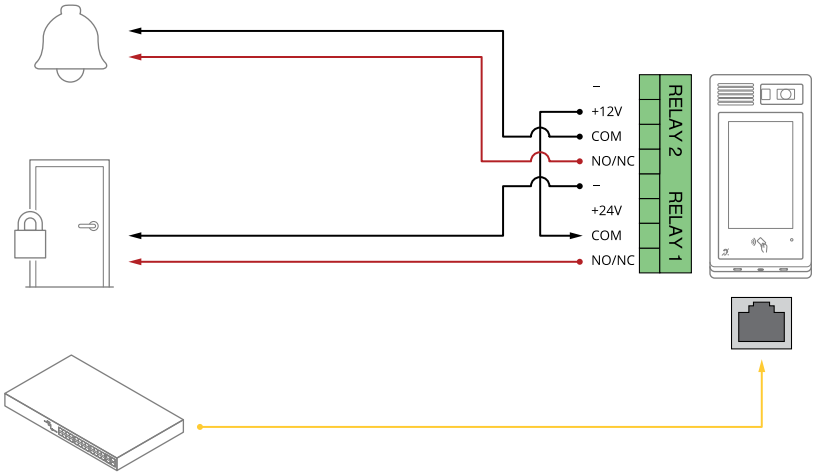
一个由 PoE (12V) 供电的继电器 + 一个由外部电源供电的继电器



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

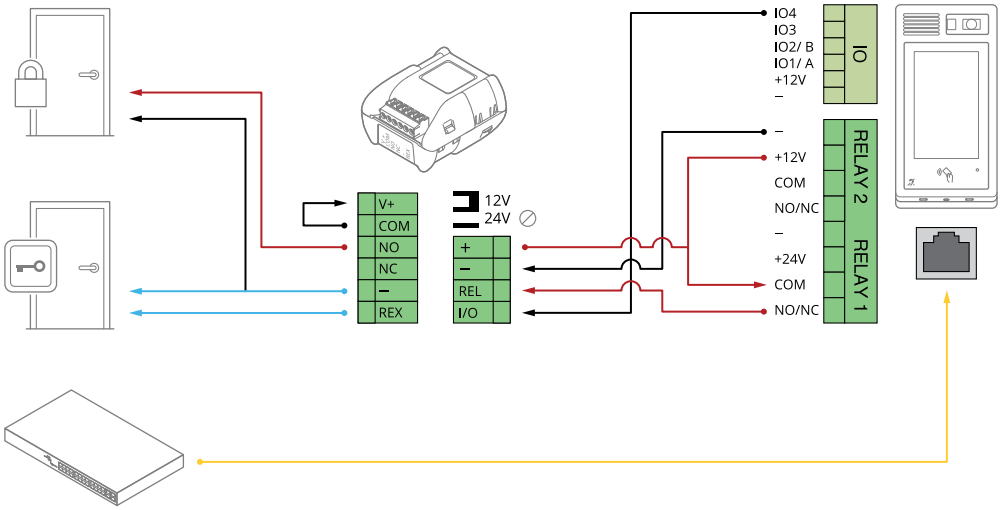
一个由 PoE (12V) 供电的继电器 + 一个继电器无源触点

无源触点可以是门铃等。



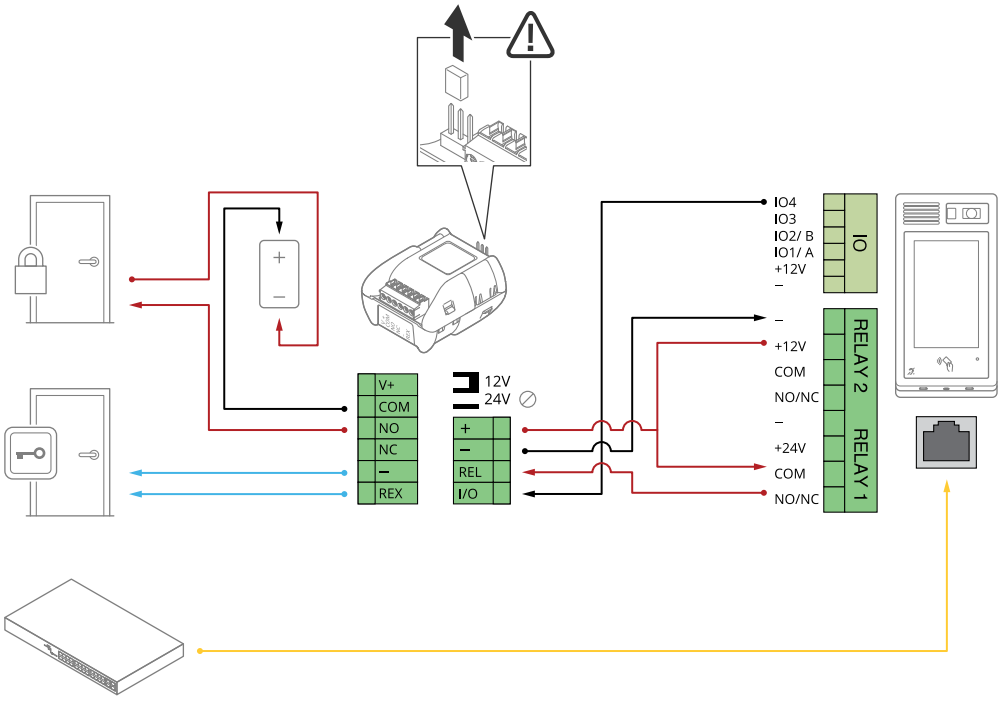
1. 要检查继电器状态，前往**系统 > 附件**，并找到继电器端口。
2. 将**正常状态**设置为：
   - ，适用于断电闭门锁。
   - ，适用于自动防故障锁。

由对讲机 PoE+ 供电的 12V 断电闭门锁



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

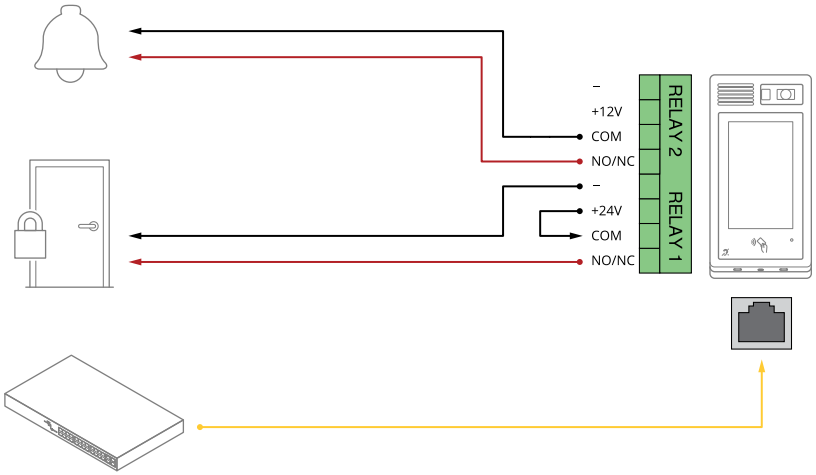
由外部电源供电的断电闭门锁



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

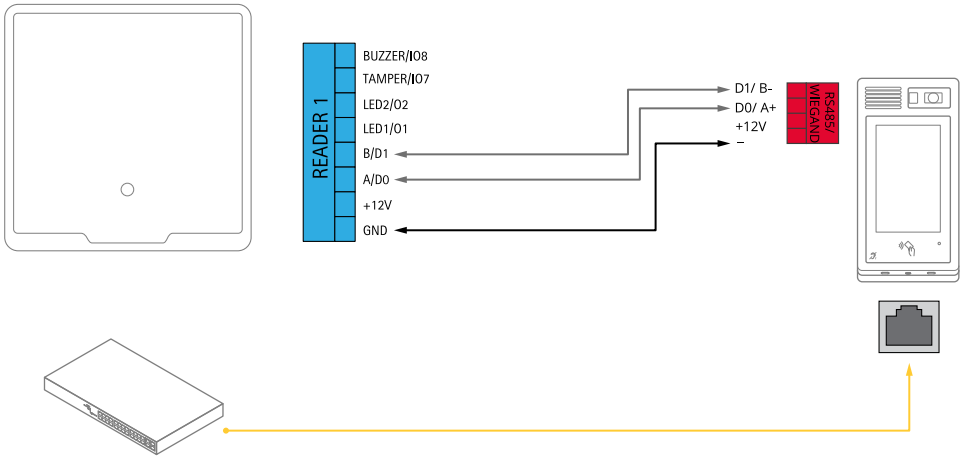
一个由 PoE (24V) 供电的继电器 + 一个继电器无源触点

无源触点可以是门铃等。



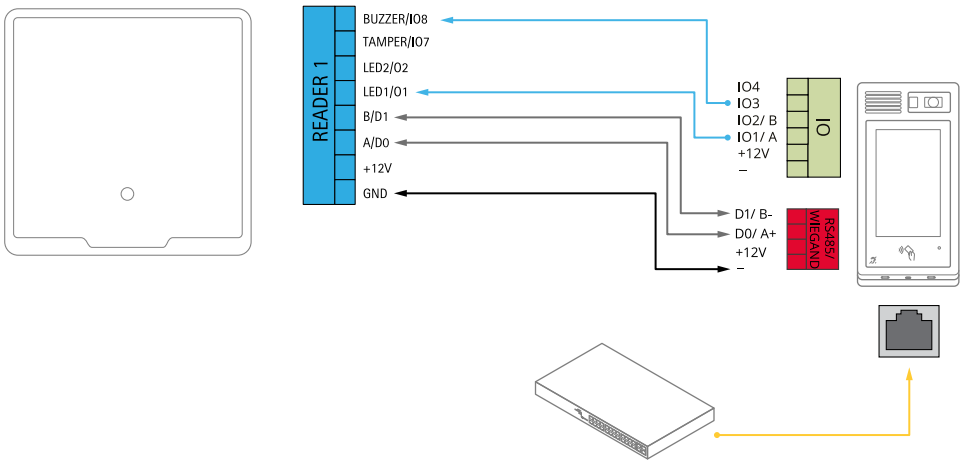
1. 要检查继电器状态，前往**系统 > 附件**，并找到继电器端口。
2. 将**正常状态**设置为：
   - ，适用于断电闭门锁。
   - ，适用于自动防故障锁。

使用 OSDP 与门禁控制器连接的读卡器



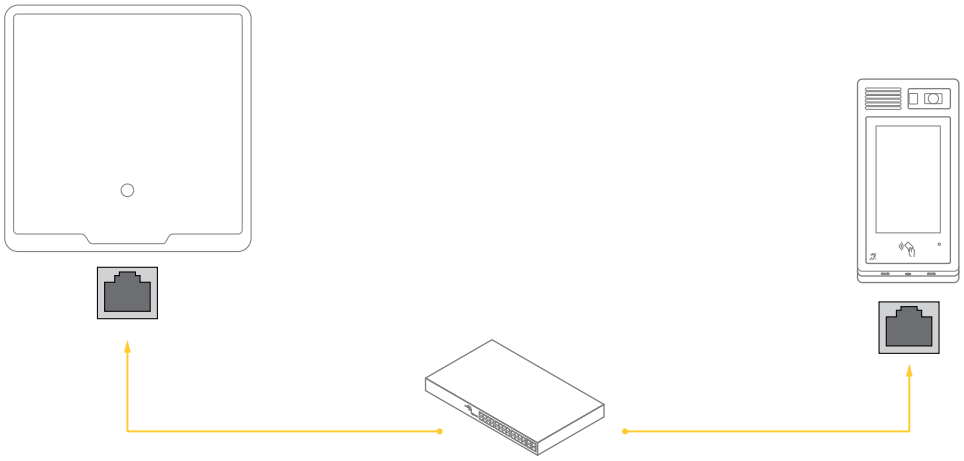
1. 转到 Reader（读卡器）> Connection（连接）> Reader protocol（读卡器协议）。
2. 将 Reader protocol type（读卡器协议类型）设置为 OSDP，然后单击 Save（保存）。

使用 Wiegand 与门禁控制器连接的读卡器



1. 转到 Reader（读卡器）> Connection（连接）> Reader protocol（读卡器协议）。
2. 将 Reader protocol type（读卡器协议类型）设置为 Wiegand。
3. 打开 **蜂鸣器**。
4. 在 Input for beeper（蜂鸣器输入）中，选择 I3。
5. 在**用于 LED 控制的输入**中，选择 1。
6. 在 Input for LED1（LED1 输入）中，选择 I1。
7. 调整其他设置，然后单击 Save（保存）。

使用 VAPIX 读卡器与安讯士门禁控制器连接的读卡器



1. 转到 Reader（读卡器）> Connection（连接）> Reader protocol（读卡器协议）。
2. 将 Reader protocol type（读卡器协议类型）设置为 VAPIX reader（VAPIX 读卡器）。
3. 连接到安讯士门禁控制器。

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 18*。
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 28*。

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 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，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.

性能考虑

当您设置系统时，考虑不同设置和情况对性能的影响，这非常重要。一些因素影响带宽（比特率），一些因素影响帧速，还有一些因素同时影响两者。

需要考虑的更重要的因素：

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

联系支持部门

如果您需要更多帮助，前往 *axis.com/support*。

安全信息

危险等级

⚠ 危险
表示如果不避免则会导致死亡或严重伤害的危险情况。

⚠ 警告
表示如果不避免则可能导致死亡或严重伤害的危险情况。

⚠ 警示
表示如果不避免则可能导致轻微或中度伤害的危险情况。

注意
表示如果不避免则可能导致财产损失的情况。

其他消息等级

重要
表示产品正常工作所必需的重要信息。

注意
表示有助于充分利用产品的有用信息。

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。

T10213214_zh

2026-10 (M12.2)

© 2025 – 2026 Axis Communications AB