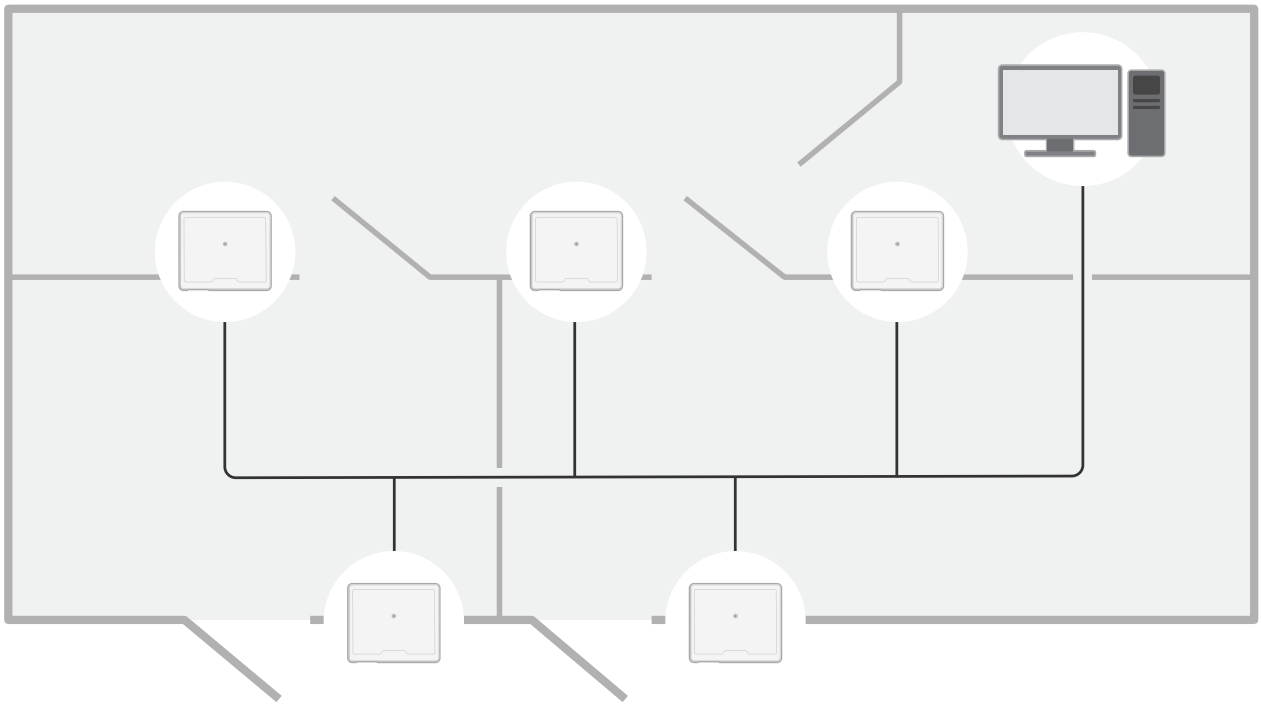
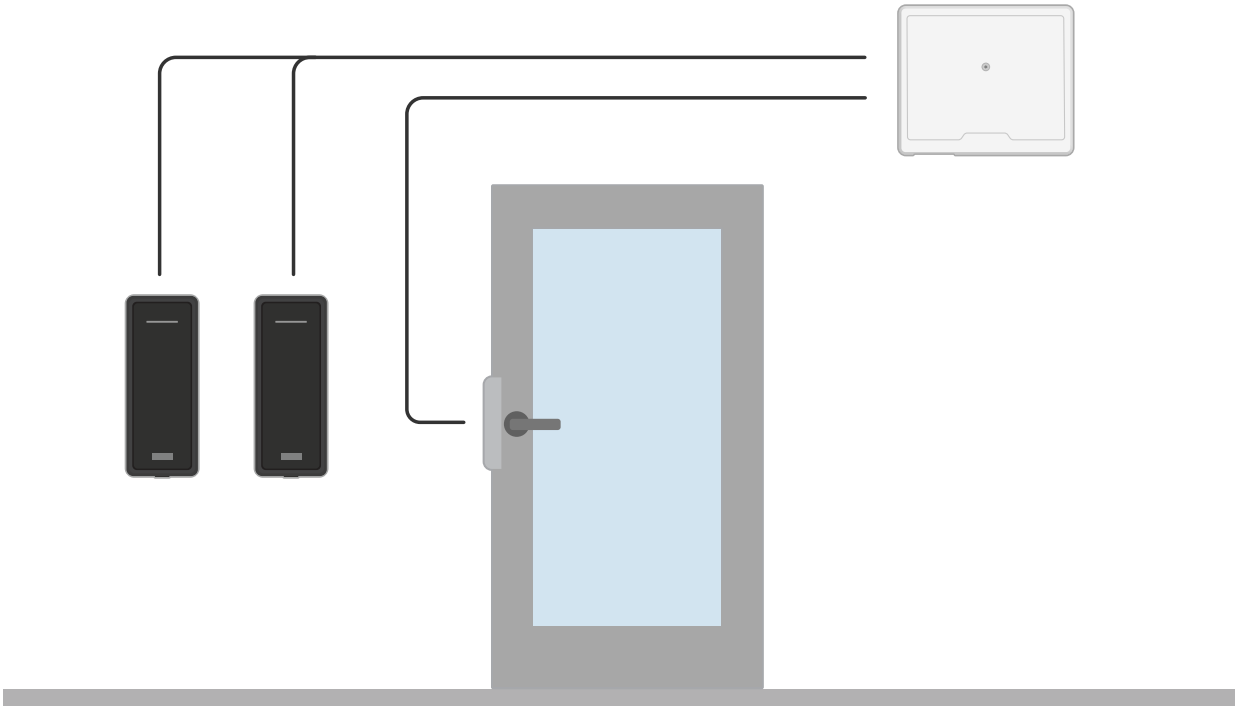
目录

解决方案概述 2
安装 3
..... 3
开始 4
在网络上查找设备 4
浏览器支持 4
打开设备的网页界面 4
创建管理员帐户 4
安全密码 4
确保没有人篡改过设备软件 5
网页界面概览 5
配置设备 6
门超控 6
OSDP LED 配置文件 6
卡格式： 7
网页界面 8
了解更多： 9
网络安全 9
签名OS 9
安全启动 9
Axis Edge Vault 9
安讯士设备ID 9
规格 10
产品概览 10
..... 10
LED 指示灯 10
按钮 11
控制按钮 11
连接器 11
网络连接器： 11
电源优先级 11
读卡器连接器 11
门连接器 12
中继连接器 13
辅助连接器 14
外部连接器 14
电源连接器 15
监控输入 15
故障排查 17
重置为出厂默认设置。 17
AXIS OS 选项 17
检查当前 AXIS OS 版本 17
升级 AXIS OS 17
技术问题和可能的解决方案 18
联系支持部门 19
网络安全 20
漏洞管理 20
安全通知 20
安全产品生命周期 20

解决方案概述



网络门禁控制器可以轻松地连接到您现有的 IP 网络并由其供电，无需专用电缆。



每个网络门禁控制器都是一个智能设备，可以轻松安装在靠近门的位置。它可以供电和控制高达两个读卡器。

安装



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 4*.

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 4*.
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 17*.

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 17.*
   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。



安讯士设备网页界面

配置设备

有关如何配置设备的更多信息，请参见*AXIS Camera Station 用户手册*或第三方解决方案。

门超控

重要

此功能可直接控制门继电器，并超控 AXIS Camera Station 中的继电器配置。请仅在安迅士技术支持人员指示您这样做时使用此功能。

1. 在 AXIS Camera Station 中停止 Secure Entry 服务。
2. 在门禁控制器的网页界面中，转到 Advanced（高级）> Door override（门超控）。
3. 请仔细阅读本页信息，然后单击 I understand（我已了解）。
4. 打开 Door override（门超控），然后单击 Enable（启用）。
5. 转到门继电器页面，单击 Lock（锁定）、Unlock（解锁）或 Access（授权）以锁定门、解锁门或授予访问权限。
6. 转到要配置的继电器，然后单击 Activate（启用）或 Deactivate（停用）以启用或停用该继电器。

OSDP LED 配置文件

您可以自定义 OSDP 读卡器的 LED 配置文件，以定义不同事件所使用的灯光和声音。有关配置文件的完整列表，请参见 *LED profiles（LED 配置文件）*。

设置灯光和音频级别

1. 转到 Peripherals（外设）> Readers（读卡器）> OSDP LED profile（OSDP LED 配置文件）。
2. 展开 Light and audio levels（灯光和音频级别）下拉菜单。
3. 使用滑块调节 LED 灯条、LED 背光和声音的强度。
4. 单击Save（保存）。

注意

当您更改灯光和音频级别时，设置将更新到连接到控制器的所有读卡器。

测试 OSDP LED 设置：

您可以使用 OSDP LED 测试菜单查看任意读卡器配置文件的音频和灯光设置。

要测试 OSDP LED 配置文件的设置：

1. 转到 Peripherals（外设）> Readers（读卡器）> OSDP LED profile（OSDP LED 配置文件）。
2. 展开 OSDP LED test（OSDP LED 测试）下拉菜单。
3. 选择一种 LED 反馈。
4. 选择您要测试的读卡器。
5. 单击开始。
6. 单击 Edit feedback（编辑反馈）以更改配置文件的灯光和音频设置。
   - 从 Color（颜色）下拉菜单中选择一种新颜色。
   - 如适用，从 Audio（音频）下拉菜单中选择一种音频频率。
   - 您还可以单击 Reset to default values（重置为默认值）来重置配置文件的设置。
   - 单击Save（保存）。

更改 OSDP LED 配置文件设置：

1. 转到 Peripherals（外设）> Readers（读卡器）> OSDP LED profile（OSDP LED 配置文件）。
2. 导航至 OSDP LED profile（OSDP LED 配置文件）。
3. 单击要编辑的配置文件旁边的 。
4. 编辑适用的设置：
   - 从 Behavior（行为）下拉菜单中选择 LED 将遵循的行为。
   - 从 Color（颜色）下拉菜单中选择 LED 的颜色。
   - 设置 LED 的 Duration on（点亮持续时间）和 Duration off（熄灭持续时间）。
   - 设置 LED 响应的 Recurrence（重复次数）。
   - 从 Audio（音频）下拉菜单中选择 Beep duration, on（蜂鸣持续时间，开启）和 Beep duration, off（蜂鸣持续时间，关闭），并设置蜂鸣器响应的 Recurrence（重复次数）。确保 Beep duration, on（蜂鸣持续时间，开启）和 Beep duration, off（蜂鸣持续时间，关闭）时长相同。
5. 单击Save（保存）。

从另一台控制器导入现有设置

1. 转到 Peripherals（外设）> Readers（读卡器）> OSDP LED profile（OSDP LED 配置文件）。
2. 单击 Import（导入）。
3. 选择您要上传的文件。
4. 单击 Import（导入）。

导出当前设置

1. 转到 Peripherals（外设）> Readers（读卡器）> OSDP LED profile（OSDP LED 配置文件）。
2. 单击 Export（导出）。
3. 选择要保存 json 文件的位置，单击 Save（保存）。

卡格式：

此功能仅供专家使用。一旦开启 Card format（卡片格式）：

- 如果您使用 37 位凭证，则最后 5 位将被移除。
- 如果您使用 64 位凭证（QR 码），则前 24 位序列将被移除。

您可以使用示例数据或读卡器来查看凭证。

1. 转到 Advanced（高级）> Card format（卡格式）。
2. 阅读警告并单击 I understand（我理解）以启用 Card format（卡格式）。
3. 在 Reader data visualization（读卡器数据可视化）下拉菜单中选择您的读卡器。
4. 单击 Get reader data（获取读卡器数据）或 Use sample data（使用示例数据）以生成卡片输出。该设置将应用于设备上的所有持卡人。
5. 开启 Trim reader data（修剪读卡器数据）以移除卡片凭证的末端位。
6. 单击**启用**。

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：

网络安全

有关网络安全的产品特定信息，请参见 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*。

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。

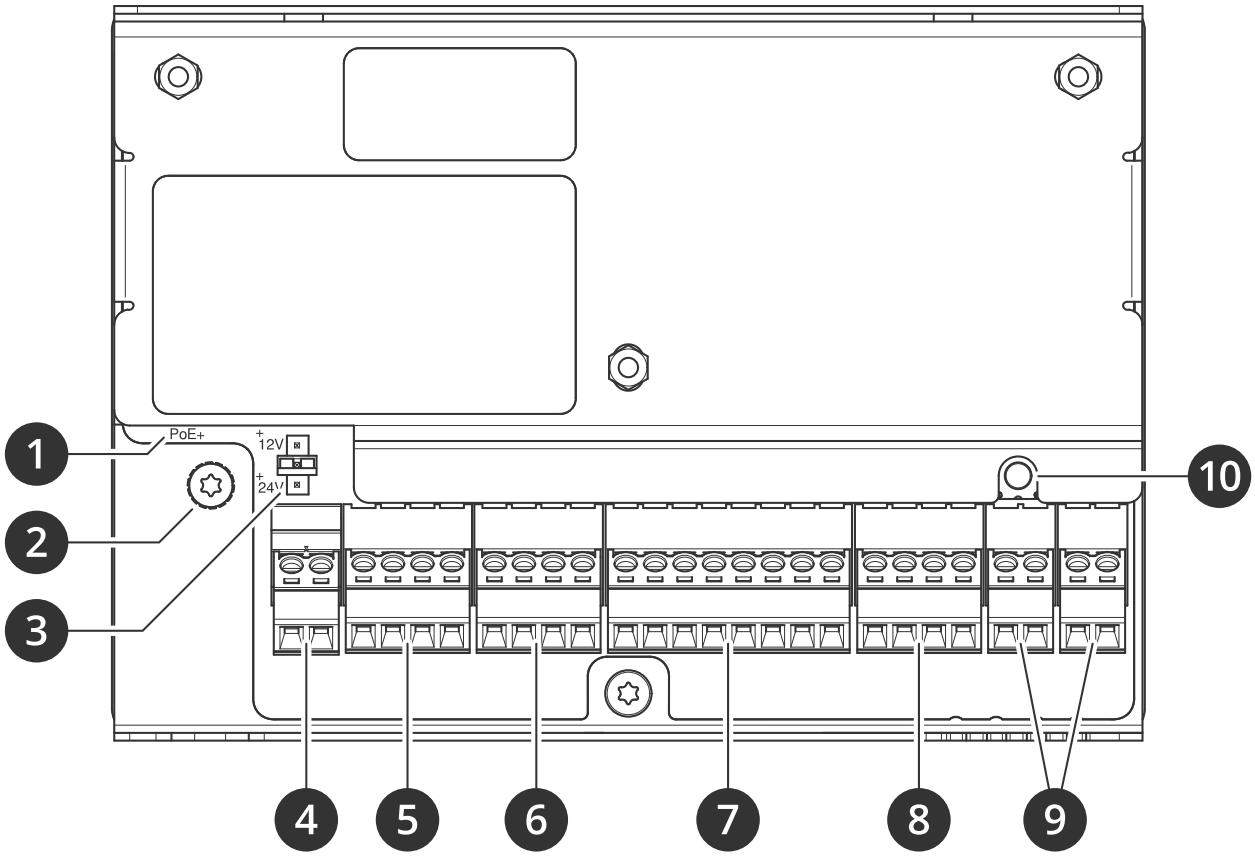
Axis Edge Vault

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（安全元件和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。

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

产品概览



1 网络连接器：
2 接地位置
3 继电器跳线
4 电源连接器
5 中继连接器
6 门连接器
7 读卡器连接器
8 辅助连接器
9 外部连接器
10 控制按钮

LED 指示灯

LED	颜色	指示
状态：	绿色	稳定绿色表示正常工作。
	琥珀色	在启动期间和还原设置时常亮。
	红色	缓慢闪烁表示升级失败。
网络：	绿色	稳定表示连接到 100 MBit/s 网络。闪烁表示网络活动。
	琥珀色	稳定表示连接到 10 MBit/s 网络。闪烁表示网络活动。
	熄灭	无网络连接。
电源	绿色	正常工作.

	琥珀色	在固件升级过程中呈绿色/橙色闪烁。
继电器：	绿色	继电器激活。[1]
	熄灭	继电器不活动。

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 17*.

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。

UL：以太网供电 (PoE) 应由以太网供电 IEEE 802.3af/802.3at 1 型 3 类或以太网供电增强版 (PoE+) IEEE 802.3at 2 型 4 类限制电源馈电器（提供 44–57 V DC、15.4 W / 30 W）供电。以太网供电 (PoE) 已由 UL 使用 AXIS T8133 Midspan 30 W 1–port 进行过评估。

电源优先级

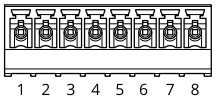
此设备可由 PoE 或 DC 输入供电。请参见 *网络连接器：, on page 11*和 *电源连接器, on page 15*。

- 当 PoE 和 DC 在设备加电之前均已连接时，将使用 PoE 供电。
- PoE 和 DC 已连接，PoE 当前正在供电。当 PoE 丢失时，设备使用 DC 供电，而无需重启。
- PoE 和 DC 已连接，DC 当前正在供电。DC 丢失时，设备将重新启动并使用 PoE 供电。
- 当在启动过程中使用 DC 并且 PoE 在设备启动后连接时，将使用 DC 供电。
- 当在启动过程中使用 PoE 并且 DC 在设备启动后连接时，将使用 PoE 供电。

读卡器连接器

支持用于与读卡器通信的 OSDP 和 Wiegand 协议的一个 8 针接线端子。

它最多可以连接两个 OSDP 读卡器（多点）或一个 Wiegand 读卡器。所有连接到门禁控制器的读卡器都预留了 500 mA（12 V 直流电压）的电流。



为一个 OSDP 读卡器配置

功能	引脚	注意	规格
DC 接地 (GND)	1		0 V DC
DC 输出 (+12 V)	2	为读卡器供电。	12 V DC，上限500 mA
A	3	半双工	
B	4	半双工	

为两个 OSDP 读卡器配置（多点）

1. 当 *COM* 连接到 *NO* 时继电器处于活动状态。

功能	引脚	注意	规格
DC 接地 (GND)	1		0 V DC
DC 输出 (+12 V)	2	为两个读卡器供电。	两个读卡器组合 12 V DC，上限500 mA
A	3	半双工	
B	4	半双工	

重要

- 当读卡器由控制器供电时，电缆长度不超 200 米（656 英尺）。仅针对安讯士读卡器进行验证。
- 当读卡器不是由控制器供电时，则如果满足以下电缆要求，读卡器数据的电缆长度不超 1000 米（(3280,8 英尺）：1 对带屏蔽双绞线，AWG 24，120 欧姆阻抗。仅针对安讯士读卡器进行验证。

为一个 Wiegand 读卡器配置

功能	引脚	注意	规格
DC 接地 (GND)	1		0 V DC
DC 输出 (+12 V)	2	为读卡器供电。	12 V DC，上限500 mA
D0	3		
D1	4		
LED 1	5	红色 LED	
LED 2	6	绿色 LED	
篡改	7	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 V DC
蜂鸣器	8	数字输出 — 如果与电感负载（如继电器）一起使用，则将二极管与负载并联连接，以防止电压瞬变。	0 至最大 30 V DC，漏极开路，100 mA

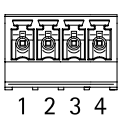
重要

- 当读卡器由控制器供电时，电缆长度不超 150 米（500 英尺）。
- 当读卡器不是由控制器供电时，则如果满足以下电缆要求，读卡器数据电缆长度不超150 米（500 英尺）：AWG 22。

门连接器

用于门禁监控设备的一个 4 针接线端子（数字输入）。

门监视器支持使用线尾电阻器监控。如果连接中断，将触发报警。要使用监控输入，安装线尾电阻器。使用连接图来安装监控输入。参见*page 15*。



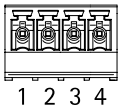
功能	引脚	注意	规格
DC 接地	1, 3		0 V DC
输入	2, 4	用于与门禁监控器通信。 数字输入或监控输入 – 分别连接至引脚 1 或 3 以启用，或保留浮动状态（断开连接）以停用。	0 至最大 30 V DC

重要

如果满足以下电缆要求，合格电缆长度可达200 米（656 英尺）：AWG 24。

中继连接器

C 型继电器的一个 4 针接线端子可以用于控制大门的锁或接口等。



功能	引脚	注意	规格
DC 接地 (GND)	1		0 V DC
否	2	常开。 用于连接中继设备。在 NO 和 DC 接地之间连接断电闭门锁。 如果不使用跳线，则两个继电器引脚与电路的其余部分电气隔离。	最大电流 = 2 A 最大电压 = 30 V DC
COM	3	公共	
NC	4	常闭。 用于连接中继设备。在 NC 和 DC 接地之间连接自动防故障锁。 如果不使用跳线，则两个继电器引脚与电路的其余部分电气隔离。	

继电器电源跳线

当安装继电器电源跳线时，它将12 V DC 或24 V DC 连接到继电器 COM 针。

它可以用于连接 GND 和 NO 或 GND 和 NC 针之间的锁。

电源	12 V DC 时的上限功率	24 V DC 时的上限功率
DC 输入	1 600 mA	800 mA
PoE	900 mA	450 mA

注意

如果锁无极性，建议您增加外部续流二极管。

辅助连接器

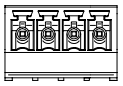
在外部设备结合了移动侦测、事件触发和报警通知等功能的情况下，使用辅助连接器。除0 V DC 参考点和电源（DC 输出）外，辅助连接器还提供连接至以下模块的接口：

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。

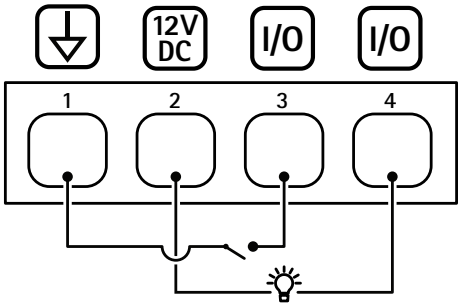
监控输入 – 能够侦测对数字输入进行的篡改。

数字输出 – 用于连接继电器和 LED 等外部设备。已连接的设备可通过 VAPIX® 应用程序编程接口或从产品网页进行激活。

4 针接线端子



功能	引脚	注意	规格
DC 接地	1		0 V DC
DC 输出	2	可用于为辅助设备供电。 注意:此针只能用作电源输出。	12 V DC 最大负载 = 共50 mA
可配置（输入或输出）	3–4	数字输入或监控输入 – 连接至引脚 1 以启用，或保留浮动状态（断开连接）以停用。要使用监控输入，则安装线尾电阻器。有关如何连接电阻器的信息，请参见连接图。	0 至最大 30 V DC
		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。如果使用内部 12 V DC 输出（引脚 2），I/O 能够驱动 12 V DC (50 mA)（合并最大）外部负载。如果结合外部电源使用开漏连接，每个 I/O 则可以管理 0–30 V DC、100 mA 的直流供电。	0 至最大 30 V DC，开漏，100 mA



1 DC 接地
2 DC 输出12 V
3 I/O 配置为输入
4 I/O 配置为输出

外部连接器

两个用于外部设备的 2 针接线端子，例如，玻璃破碎或火灾侦测器。

UL：此连接器尚未由 UL 进行防窃或防火报警使用方面的评估。



功能	引脚	注意	规格
DC 接地	1		0 V DC
篡改	2	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 V DC



功能	引脚	注意	规格
DC 接地	1		0 V DC
报警	2	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 V DC

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 (GND)	1		0 V DC
DC 输入	2	在未使用以太网供电时，可用于给设备供电。 注意:此引脚只能用作电源输入。	12 V DC, 上限 36 W

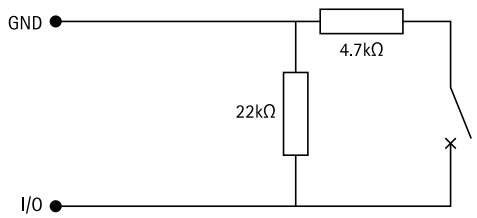
UL：使用具有适当额定功率的 UL 603 上市电源供应器提供 DC 电源，具体取决于应用。

监控输入

要使用监控输入，则根据下面的图表安装线尾电阻器。

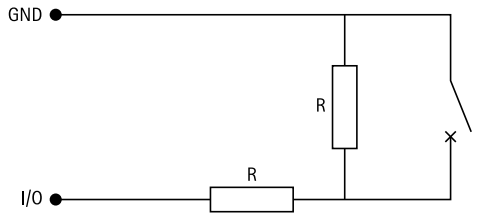
并联优先连接：

电阻值要为 4.7 kΩ 和 22 kΩ。



串联优先连接：

电阻器值必须相同，可能的值为 1 kΩ、2.2 kΩ、4.7 kΩ和 10 kΩ。



注意

建议使用绞合屏蔽电缆。将屏蔽件连接至 0 V DC。

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 10*.
3. 按住控制按钮 25 秒，直到状态指示灯指示灯再次变成淡黄色。
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。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*。

- 由于用户、组、凭证和其他数据的数据库将在 AXIS OS 升级后更新，因此首次启动可能需要几分钟才能完成。所需时间取决于数据量。

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。

4. 产品重启之后，将清除网页浏览器的缓存。

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 17*。

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 4*。

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.

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。

T10181041_zh

2026-10 (M11.6)

© 2022 – 2026 Axis Communications AB