AXIS A9210 Network I/O Relay Module

用户手册

开始使用

在网络上查找设备

若要在网络中查找安讯士设备并为它们分配 Windows® 中的 IP 地址，请使用 AXIS IP Utility 或 AXIS Device Manager。这两种应用程序都是免费的，可以从 *axis.com/support* 上下载。

有关如何查找和分配 IP 地址的更多信息，请转到*如何分配一个 IP 地址和访问您的设备*。

浏览器支持

您可以在以下浏览器中使用该设备：

	Chrome™	Edge™	Firefox®	Safari®
Windows®	✓	✓	*	*
macOS®	✓	✓	*	*
Linux®	✓	✓	*	*
其他操作系统	*	*	*	*

✓：建议

*：支持，但有限制

打开设备的网页界面

1. 打开一个浏览器，键入安讯士设备的 IP 地址或主机名。
   如果您不知道 IP 地址，请使用 AXIS IP Utility 或 AXIS Device Manager 在网络上查找设备。
2. 键入用户名和密码。如果是首次访问设备，则必须创建管理员帐户。请参见 *创建管理员帐户, on page 2*。

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

创建管理员帐户

首次登录设备时，您必须创建管理员帐户。

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

重要

设备没有默认帐户。如果您丢失了管理员帐户密码，则您必须重置设备。请参见 *重置为出厂默认设置, on page 15*。

安全密码

重要

使用 HTTPS（默认已启用）通过网络设置密码或其他敏感配置。HTTPS 可实现安全加密的网络连接，从而保护密码等敏感数据。

设备密码是对数据和服务的主要保护。安讯士设备不会强加密码策略，因为它们可能会在不同类型的安装中使用。

为保护您的数据，我们强烈建议您：

- 使用至少包含 8 个字符的密码，而且密码建议由密码生成器生成。
- 不要泄露密码。
- 定期更改密码，至少一年一次。

确保没有人篡改过设备软件

要确保设备具有其原始的 AXIS OS，或在安全攻击之后控制设备，请执行以下操作：

1. 重置为出厂默认设置。请参见 *重置为出厂默认设置, on page 15*。
   重置后，安全启动可保证设备的状态。
2. 配置并安装设备。

网页界面概览

该视频为您提供设备网页界面的概览。

Axis 设备网页界面

配置设备

配置 I/O 端口

1. 转到**设备 > I/O 和继电器 > AXIS A9210 > I/O**。
2. 单击 以展开 I/O 端口设置。
3. 重命名端口。
4. 配置正常状态。单击 开路，或 闭路。
5. 要将 I/O 端口配置为输入：
   5.1. 在**方向**下，单击 。
   5.2. 要监控输入状态，请开启**受监督**。请参见 *监控输入, on page 13*。

注意

在 API 中，受监督的 I/O 端口的工作方式与受监督的输入端口不同。有关更多信息，请转到 *VAPIX® 库*。

6. 要将 I/O 端口配置为输出：
   6.1. 在**方向**下，单击 。
   6.2. 要查看要激活和停用连接的设备的 URL，请转到**切换端口 URL**。

配置继电器

1. 转到**设备 > I/O 和继电器> AXIS A9210>继电器**。
2. 单击 以展开继电器设置。
3. 打开 **Relay（继电器）**。
4. 重命名继电器。
5. 要查看要激活和停用继电器的 URL，请转到**切换端口 URL**。

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。

网页界面

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

了解更多

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 Door Monitoring

该应用程序监控门状态，显示门开着还是关着，以及门是否长时间保持开着。例如，可以在不需要锁具但需要知道门是否打开的防火安全门上使用此应用程序。

普通门有门位传感器、REX、以及锁具和读卡器，需配合门禁控制器使用。

监控门仅需配备门位传感器和REX，即可通过网络 I/O 继电器模块进行监控。每个网络 I/O 继电器模块最多可连接五个监控门。

限制

该应用程序仅适用于 AXIS A9210。REX 模块仅可连接至 I/O 1 和 I/O 2，无法在 I 3、I 4 或 I 5 端口上配置 REX 模块。

AXIS Monitoring Door 配置

名称	说明
门	门的数量。
DPS 输入	门的 DPS 输入。
REX 输入	门的 REX 输入。
门打开时间过长（秒）	允许门保持打开状态的秒数。
访问时间（秒）	在授予访问权限后门应保持解锁的秒数。
状态	门的状态。

网络安全

有关网络安全的产品特定信息，请参阅Axis.com上该产品的数据表。

有关AXIS OS网络安全的深度信息，请阅读*AXIS OS强化配置指南*。

Axis Edge Vault

Axis Edge Vault为保障安讯士设备安全提供了基于硬件的网络安全平台。它有保证设备的身份和完整性的功能，并保护您的敏感信息免遭未授权访问。它依托加密计算模块（安全元素和TPM）和SoC安全（TEE和安全启动）的强大基础，与前端设备安全的相关专业知识相结合。

签名OS

已签名的操作系统由软件供应商实施，并使用私钥对 AXIS OS 映像进行签名。将签名附加到操作系统后，设备将在安装软件之前对其进行验证。如果设备侦测到软件完整性受损，AXIS OS 升级将被拒绝。

安全启动

安全启动是一种由加密验证软件的完整链组成的启动过程，始于不可变的内存（启动ROM）。安全启动基于签名操作系统的使用，可确保设备仅能使用已授权的软件启动。

安全密钥库

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

安讯士设备ID

能够验证设备来源是建立设备身份信任的关键。在生产期间，配备 AXIS Edge Vault 的设备被分配到具有唯一性、由工厂预置且符合 IEEE 802.1AR 标准的安讯士设备 ID 证书。其原理与护照相似，旨在证明设备来源。设备ID作为经安讯士根证书签名的证书，安全且永久存储在安全密钥库中。客户的 IT 基础设施可以利用设备 ID 实现自动安全设备板载和安全设备确认

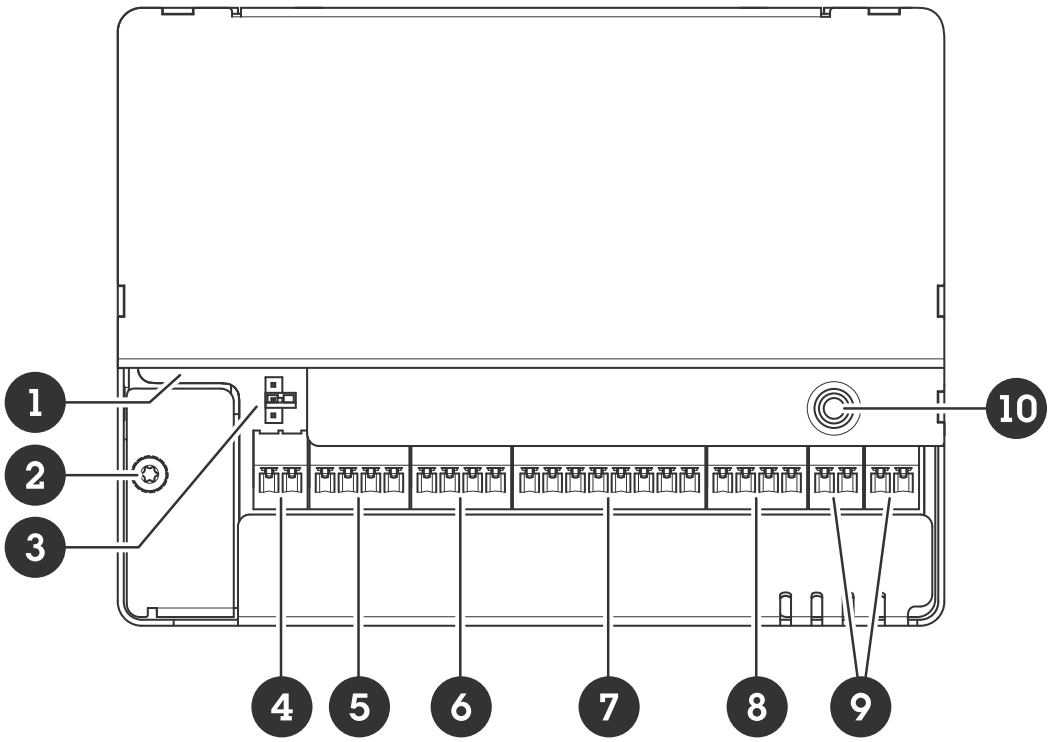
加密文件系统

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

要了解有关安讯士设备中网络安全功能的更多信息，请转到 *axis.com/learning/white–papers* 并搜索网络安全。

规格

产品概述



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 输入 1 连接器
7 RS485 和 I/O 连接器
8 I/O 连接器
9 输入 2 连接器
10 控制按钮

LED 指示灯

LED	彩色	指示
状态	绿色	稳定绿色表示正常工作。
	淡黄色	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。
	淡黄色	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	工作正常。

	淡黄色	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。请参见 *重置为出厂默认设置, on page 15*。
- 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 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 9*和 *电源连接器, on page 9*。

- 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。

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)。

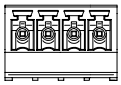
功能	针脚	注意	规格
DC 接地 (GND)	1		0 V DC
DC 输入	2	在未使用以太网供电时，可用于给设备供电。 注意：此针脚只能用作电源输入。	12 V DC, 上限 36 W

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。

1. 当 *COM* 连接到 *NO* 时继电器处于活动状态。

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。如果与电感负载（如锁）一起使用，则将整流管与负载并联连接，以防止电压瞬变。



功能	针脚	注意	规格
DC 接地 (GND)	1		0 V DC
NO	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。

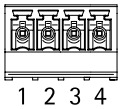
它可以用于连接 GND 和 NO 或 GND 和 NC 针之间的锁。

电源	12 V DC 时的上限功率	24 V DC 时的上限功率
DC 输入	2 000 mA	1 000 mA
PoE	350 mA	150 mA
PoE+	1100 mA	500 mA

输入 1 连接器

一个 4 针接线端子，用于输入。

它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，则安装线尾电阻器。使用连接图来安装监控输入。请参见 *监控输入, on page 13*。



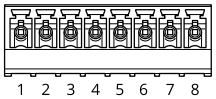
功能	针脚	注意	规格
DC 接地	1, 3		0 V DC
输入	2, 4	数字输入或监控输入 – 分别连接至引脚 1 或 3 以启用，或保留浮动状态（断开连接）以停用。	0 至最大 30 V DC

重要

如果满足以下电缆要求，电缆长度不超200 米（656 英尺）：AWG 24。

RS485 和 I/O 连接器

一个 8 针接线端子，包括 4 针 RS485 和 4 针 I/O。



RS485

功能	针脚	注意	规格
DC 接地 (GND)	1		0 V DC
DC 输出 (+12 V)	2	为辅助设备供电，例如 Modbus 传感器。	12 V DC，上限200 mA
A	3		
B	4		

I/O

功能	针脚	注意	规格
数字输出	5	如果与电感负载（如继电器）一起使用，则将整流管与负载并联连接，以防止电压瞬变。	0 至最大 30 V DC，漏极开路，100 mA
数字输出	6	如果与电感负载（如继电器）一起使用，则将整流管与负载并联连接，以防止电压瞬变。	0 至最大 30 V DC，漏极开路，100 mA
输入	7	数字输入或监控输入 – 连接至针脚 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
数字输出	8	如果与电感负载（如继电器）一起使用，则将整流管与负载并联连接，以防止电压瞬变。	0 至最大 30 V DC，漏极开路，100 mA

重要

- 如果满足以下电缆要求，RS485 的合格电缆长度可达1000 米（3281 英尺）：1 条屏蔽双绞线，AWG 24，阻抗120 欧姆。
- 适用于 I/O 的合格电缆长度可达 200 米（656 英尺）。

I/O 连接器

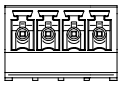
在外部设备结合了移动侦测、事件触发和报警通知等功能的情况下，使用辅助连接器。除0 V DC 参考点和电源（DC 输出）外，辅助连接器还提供连接至以下模块的接口：

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。

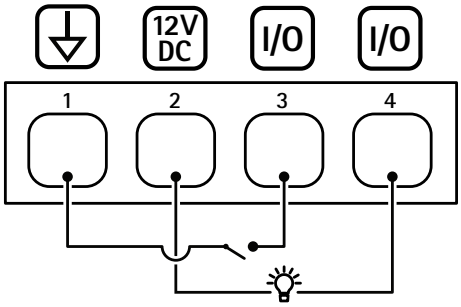
监控输入 – 能够侦测对数字输入进行的篡改。

数字输出 – 用于连接继电器和 LED 等外部设备。连接的设备可以通过 VAPIX® 应用可编程接口 (API) 或从产品网页激活。

4 针接线端子



功能	针脚	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 – 连接至针脚 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（例如继电器）一起使用，请在负载上并联一个二极管，以防止电压瞬变。如果使用内部 12 V DC 输出（引脚 2），则输入/输出 (I/O) 能够驱动 12 V DC、50 mA（最大组合电流）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

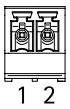


1 DC 接地
2 DC 输出12 V
3 I/O 配置为输入
4 I/O 配置为输出

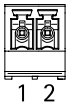
输入 2 连接器

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	针脚	注意	规格
DC 接地	1		0 V DC
输入	2	数字输入或监控输入 – 连接至针脚 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



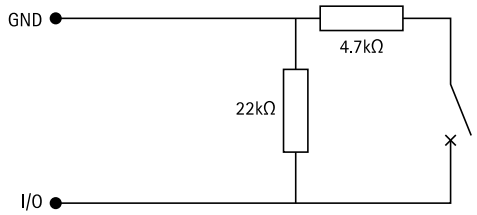
功能	针脚	注意	规格
DC 接地	1		0 V DC
输入	2	数字输入或监控输入 – 连接至针脚 1 以启用，或保留浮动状态（断开连接）以停用。	0 至最大 30 V DC

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。

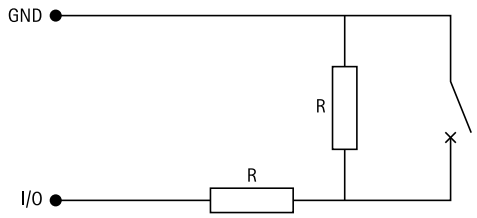
并联优先连接

电阻值要为 4.7 kΩ 和 22 kΩ。



串行首次连接

电阻器值必须相同，可能的值为 1 kΩ、2.2 kΩ、4.7 kΩ 和 10 kΩ、1%、¼ 瓦特标准。



注意

建议使用绞合屏蔽电缆。将屏蔽件连接至 0 V DC。

状态	说明
打开	监控开关处于打开模式。
已关闭	监控开关处于关闭模式。

短	I/O 或输入 1–5 电缆短路至接地。
切断	I/O 或输入 1–5 电缆被切断并保持打开状态，没有通向 GND 的电流路径。

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 8*。
3. 按住控制按钮 25 秒，直到状态 LED 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：
   - **使用AXIS OS 12.0及更高版本的设备：** 从链路本地地址子网获取 (169.254.0.0/16)
   - **使用AXIS OS 11.11及更早版本的设备：** 192.168.0.90/24
5. 使用安装和管理软件工具分配 IP 地址、设置密码和访问产品。

您还可以通过设备网页界面将参数重置为出厂默认设置。转到**维护** > **出厂默认设置**，然后单击**默认**。

AXIS OS 选项

Axis 可根据主动追踪或长期支持 (LTS) 追踪提供设备软件管理。处于主动追踪意味着可以持续访问新产品特性，而 LTS 追踪则提供一个定期发布主要关注漏洞修复和安保升级的固定平台。

如果您想访问新特性，或使用安讯士端到端系统产品，则建议使用主动追踪中的 AXIS OS。如果您使用第三方集成，则建议使用 LTS 追踪，其未针对主动追踪进行连续验证。使用 LTS，产品可维护网络安全，而无需引入重大功能改变或影响现有集成。如需有关安讯士设备软件策略的更多详细信息，请转到 *axis.com/support/device-software*。

检查当前 AXIS OS 版本

AXIS OS 决定了我们设备的功能。当您进行问题故障排查时，我们建议您从检查当前 AXIS OS 版本开始。新版本可能包含能修复您的某个特定问题的校正。

要检查当前 AXIS OS 版本：

1. 转到设备的网页界面 > **状态**。
2. 请参见**设备信息**下的 AXIS OS 版本。

升级 AXIS OS

重要

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

注意

- 使用活动追踪中的新 AXIS OS 升级设备时，产品将获得可用的新功能。在升级前，始终阅读每个新版本提供的升级说明和版本注释。要查找新 AXIS OS 和发布说明，请转到 *axis.com/support/device-software*。

1. 将 AXIS OS 文件下载到您的计算机，该文件可从 *axis.com/support/device–software* 免费获取。
2. 以管理员身份登录设备。
3. 转到**维护 > AXIS OS 升级**，然后单击**升级**。

升级完成后，产品将自动重启。

技术问题和可能的解决方案

升级 AXIS OS 时出现问题

AXIS OS 升级失败

如果升级失败，该设备将重新加载以前的版本。比较常见的原因是上载了错误的 AXIS OS 文件。检查 AXIS OS 文件名是否与设备相对应，然后重试。

AXIS OS 升级后出现的问题

如果您在升级后遇到问题，请从**维护**页面回滚到之前安装的版本。

设置 IP 地址时出现问题

无法设置 IP 地址

- 如果用于设备的 IP 地址和用于访问该设备的计算机 IP 地址位于不同子网上，则无法设置 IP 地址。请联系网络管理员获取 IP 地址。
- 该 IP 地址可能已被其他设备使用。检查：
  1. 从网络上断开安讯士设备。
  2. 在 Command/DOS 窗口中，键入 `ping` 和设备的 IP 地址。
  3. 如果收到：`Reply from <IP address>: bytes=32; time=10...`，这意味着网络上其他设备可能已使用该 IP 地址。请从网络管理员处获取新的 IP 地址，然后重新安装该设备。
  4. 如果您收到：`Request timed out`，这意味着该 IP 地址可用于此安讯士设备。请检查布线并重新安装设备。
- 可能与同一子网中的另一台设备存在 IP 地址冲突。在 DHCP 服务器设置动态地址之前，将使用安讯士设备中的静态 IP 地址。这意味着，如果其他设备也使用同一默认静态 IP 地址，则可能在访问该设备时出现问题。

设备访问问题

通过浏览器访问设备时无法登录

启用 HTTPS 后，需在登录时使用正确的协议（HTTP 或 HTTPS）。您可能需要在浏览器的地址字段中手动键入 `http` 或 `https`。

如果您遗失了根帐户密码，则必须将设备重置为出厂默认设置。有关说明，请参见 *重置为出厂默认设置, on page 15*。

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 2*。

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 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。

设备操作问题

前加热器和雨刮器不工作

如果前加热器或雨刮器无法打开，请确认顶部外壳已正确固定在护罩单元底部。

如果您无法在此处找到您要寻找的信息，请尝试在 *axis.com/support* 上的故障排除部分查找。

联系支持人员

如果您需要更多帮助，请转到 *axis.com/support*。

T10202445_zh

2026-02 (M7.2)