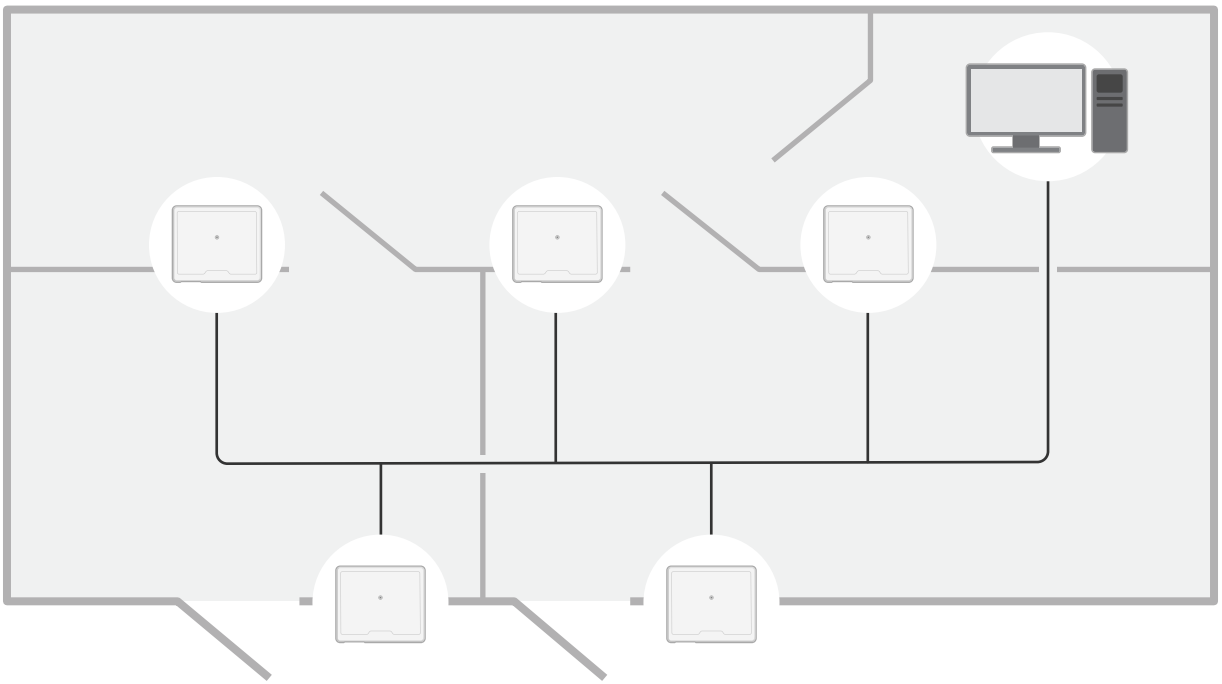
AXIS A1210 网络门禁控制器

AXIS A1210–B Network Door Controller

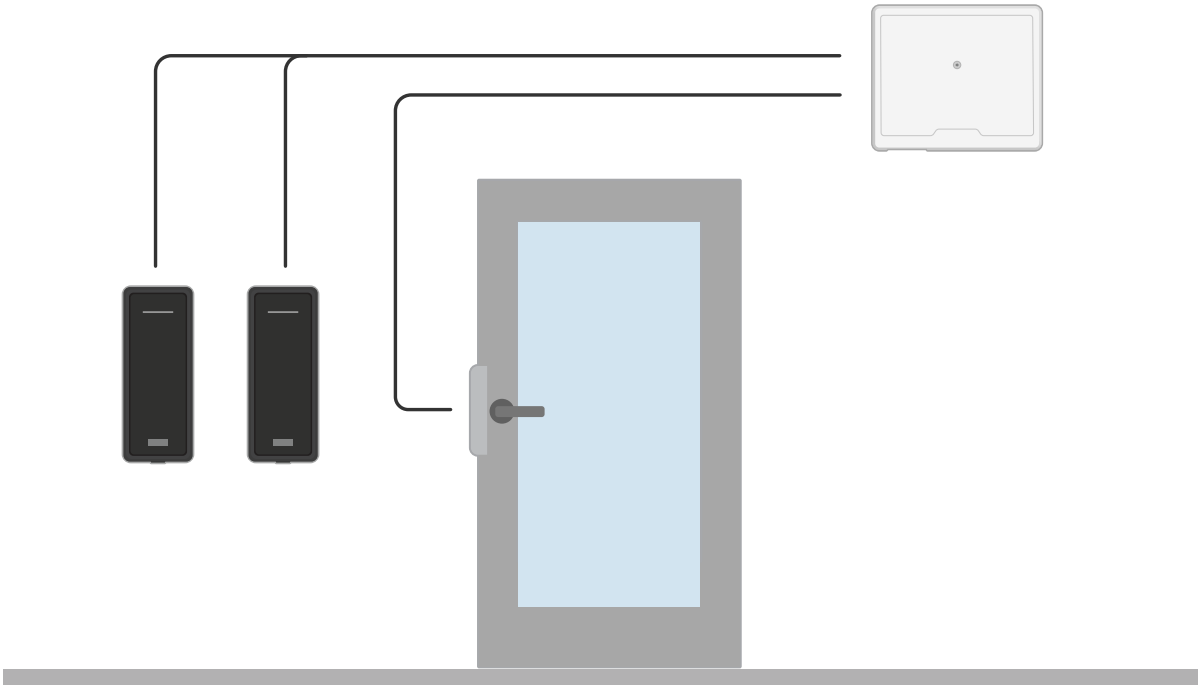
用户手册

目录

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取器。

安装

要观看此视频，请转到本文档的网页版本。

help.axis.com/?&piaId=74266&section=solution-overview

开始使用

在网络上查找设备

若要在网络中查找 Axis 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™	Firefox®	Edge™	Safari®
Windows®	推荐	推荐	✓	
macOS®	推荐	推荐	✓	✓
Linux®	推荐	推荐	✓	
其他操作系统	✓	✓	✓	✓*

**要在 iOS 15 或 iPadOS 15 上使用 AXIS OS 网页界面，请前往 设置 > Safari > 高级 > 实验功能，并禁用 NSURLSession Websocket。*

如果您需要有关推荐的浏览器的更多信息，请前往*AXIS OS Portal*。

打开设备的网页界面

1. 打开一个浏览器，键入 Axis 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。

有关在设备的网页界面中控件和选项的说明，请参见。

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。参见。
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。

安全密码

重要

Axis 设备在网络中以明文形式发送初始设置的密码。若要在首次登录后保护您的设备，请设置安全加密的 HTTPS 连接，然后更改密码。

设备密码是对数据和服务的主要保护。Axis 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。

验证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

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。

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。

注意

对本节中描述的功能和设置的支持因设备而异。此图标  指示功能或设置仅在某些设备中可用。

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。
- 注销：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。
- 旧设备界面:将设备网页界面更改为旧版本。

状态

设备信息

显示设备信息，包括 AXIS OS 版本和序列号。

升级 AXIS OS：升级设备软件。前往在其中进行升级的维护页面。

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。前往可更改 NTP 设置的日期和时间页面。

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：前往*《AXIS OS 强化指南》*，您可在其中了解有关如何应用 Axis 设备理想实践的更多信息。

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。

设备

警报

移动设备：打开当检测到设备移动时在系统中触发警报。外壳打开  ：打开当检测到门禁控制器的外壳打开时在系统中触发警报。关闭裸机门禁控制器的此设置。外部篡改  ：当检测到外部篡改时，打开以在系统中触发警报。例如，当外部机柜打开或关闭时。

- 监控输入  ：打开以监控输入状态，并配置线路上的电阻。
  - 要使用并联首次连接，请选择带有 22 KΩ 并联电阻器和 4.7 KΩ 串联电阻器的并联首次连接。
  - 要使用串行首次连接，请选择串行首次连接，然后从电阻值下拉列表中选择电阻值。

联网

读取器

+ 添加读取器：单击以添加新读取器。名称：为连接的读取器输入一个名称。读取器:从下拉列表中选择读取器。IP 地址：手动输入读取器的 IP 地址。用户名：输入用户名。密码：输入密码。忽略服务器证书验证：开启此选项以忽略验证。

升级读取器

升级读取器：单击将读取器升级到新的 AXIS OS 版本。只有受支持的读取器在线时才能升级该功能。

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。允许 root 权限应用程序  ：打开以允许具有根权限的应用可对设备进行完全访问。  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。

如果您没有许可证密钥，请访问*axis.com/products/analytics*。您需要有许可证代码和安讯士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。
- 自动日期和时间（手动 NTS KE 服务器）：与连接到 DHCP 服务器的安全 NTP 密钥建立服务器同步。
  - 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。
  - 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，然后才能选择此选项。
- 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 代表正北方。
- 标签：为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：选择此设置可让网络路由器自动分配设备的 IP 地址。我们建议大多数网络采用自动 IP（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仅有的。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 –。

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。

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。前往系统> 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。该设备允许使用端口 80 或 1024–65535 范围内的任何端口。如果您以管理员身份登录，您还可以输入 1–1023 范围内的任何端口。如果使用此范围内的端口，将会收到警告。HTTPS 端口：输入要使用的 HTTPS 端口。该设备允许使用端口 443 或 1024–65535 范围内的任何端口。如果您以管理员身份登录，您还可以输入 1–1023 范围内的任何端口。如果使用此范围内的端口，将会收到警告。证书：选择要为设备启用 HTTPS 的证书。

网络发现协议

Bonjour®：开启该选项以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®：开启该选项以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–Discovery：开启该选项以允许在网络中执行自动发现。LLDP 和 CDP：开启该选项以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。要解决 PoE 电源协商的任何问题，请仅为硬件 PoE 电源协商配置 PoE 交换机。

一键云连接

一键式云连接 (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：

- 单击：这是默认设置。按住设备上的控制按钮，以通过互联网连接到 O3C 访问。按下控制按钮后 24 小时内，您需要向 O3C 服务注册设备。否则，设备将从 O3C 服务断开。一旦您注册了设备，一直将被启用，您的设备会一直连接到 O3C 服务。
- 总是：设备将不断尝试通过互联网连接到 O3C 服务。一旦您注册了设备，它会一直连接到 O3C 服务。如果无法够到设备上的控制按钮，则使用此选项。
- 否：禁用 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数量。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：此方法是与 HTTP 最为兼容的身份验证方案。它的安全性相比 Digest 较差，因为它会将未加密的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。

所有者身份验证密钥 (OAK)：单击 Get key（获取密钥）以获取所有者身份验证密钥。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 对象的团体名称。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 物体（只读物体除外）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，您可以为 SNMP v1 和 v2c 设置陷阱。如果更改为 SNMP v3 或关闭 SNMP，陷阱会自动关闭。如果使用 SNMP v3，则可以通过 SNMP v3 管理应用程序来设置陷阱。
  - 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。
  - 热启动：更改 SNMP 设置时发送陷阱消息。
  - 连接：链接自下而上发生变更时，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 是一个更安全的版本，提供加密和安全密码。要使用 SNMP v3，我们建议您激活 HTTPS，因为密码随后会通过 HTTPS 发送。这还可以防止未经授权者访问未加密的 SNMP v1 和 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。
  - “initial”帐户的密码：为“initial”帐户输入 SNMP 密码。虽然无需激活 HTTPS 即可发送密码，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，当设备连接到受 IEEE 802.1X 保护的网络时，用于验证身份验证服务器的身份。设备已预装多个 CA 证书。

支持以下格式：
- 证书格式：.PEM、.CER 和 .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。

- 更多 ⌄：显示更多要填充或选择的栏。
- 安全密钥库：选择使用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/en-us/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 ⓘ：

- 安全元件 (CC EAL6+)：选择使用安全元件作为安全密钥库。
- 可信平台模块 2.0 (CC EAL4+、FIPS 140–2 级别 2)：选择使用 TPM 2.0 作为安全密钥库。

网络访问控制和加密

IEEE 802.1xIEEE 802.1x 是对基于端口的网络准入控制的 IEEE 标准，可为有线和无线网络设备提供安全身份验证。IEEE 802.1x 是基于 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 MACsecIEEE 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：选择要使用 IEEE 802.1x 的客户端证书。身份验证服务器使用该证书来验证客户端。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：选择使用 IEEE 802.1x 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

激活：打开防火墙。
默认策略：选择防火墙的默认状态。

- 允许：允许与设备的各连接。默认情况下设置此选项。
- 拒绝：拒绝与设备的各连接。

要对默认策略进行例外处理，您可以创建允许或拒绝从特定地址、协议和端口连接到设备的规则。

- 地址：输入要允许或拒绝访问的 IPv4/IPv6 或 CIDR 格式的地址。
- 协议：选择要允许或拒绝访问的协议。
- 端口：输入要允许或拒绝访问的端口号。您可以添加介于 1 和 65535 之间的端口号。
- 策略：选择规则的策略。

+ ：单击以创建另一项规则。
添加规则：单击此项可添加已定义的规则。

- 时间（秒）：设置测试规则的时间限制。默认时间限制设置为 300 秒。要立即激活规则，请将时间设置为 0 秒。

- 确认规则：确认规则及其时间限制。如果您将时间限制设置为 1 秒以上，则规则将在此期间处于活动状态。如果将时间设置为 0，规则将立即生效。

待处理规则：您尚未确认的经过测试的新检测规则概述。

注意

具有时间限制的规则将显示在活动规则下，直到显示的计时器用完或确认它们为止。如果不进行确认，一旦计时器用完，它们将显示在待处理规则下，并且防火墙将恢复为之前定义的设置。如果您确认，它们将替换当前有效的规则。

确认规则：单击以激活挂起的规则。活动规则：当前在设备上运行的规则概述。 ：单击以删除活动规则。 ：单击以删除所有规则，包括挂起规则和活动规则。

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。该软件只能在由其唯一序列号和芯片 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的 AXIS OS 证书，因为安讯士拥有用以签名这些证书的密钥。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:输入一个唯一的帐户名。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。
- 浏览者：无法访问更改设置。

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。

SSH 帐户

添加 SSH 帐户：单击以添加新 SSH 帐户。

- 限制根访问：打开以限制要求根访问的功能。
- 启用 SSH：打开此选项以使用 SSH 服务。

帐户:输入一个唯一的帐户名。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。在基本、摘要和打开 ID 之间选择。 ⋮ 上下文菜单包括：
- 更新：更新虚拟主机。
- 删除：删除虚拟主机。

已禁用：服务器已禁用。

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据。

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：打开此选项以关闭当前连接并允许来自提供商 URL 的设备身份验证。

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。Axis 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，即客户端和代理。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。您可在*AXIS OS Portal* 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。这用于通过与其他协议（例如 HTTP）共用端口来启用 MQTT 流量。在某些情况下，可能不会为 MQTT 通信开放专用端口。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。
- MQTT over TCP 的默认值是 1883。
- 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 代理提供商提供的 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。客户端标识符在客户端连接到服务器时发送到服务器。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据。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。包括主题名称：选择以包含描述 MQTT 主题中的条件的主题。包括主题命名空间：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。

附件

I/O 端口

数字输入用于连接可在开路和闭路之间切换的外部设备，例如 PIR 传感器、门或窗传感器和玻璃破碎探测器。

使用数字输出连接外部设备，例如继电器和 LED。您可以通过 VAPIX® 应用程序编程接口 (API) 或网页界面激活连接的设备。

端口名称：编辑文本来重命名端口。方向： 指示端口是输入端口。 指示端口是输出端口。如果端口可配置，则您可以单击这些图标以在输入和输出之间进行切换。正常状态：如果是开路，单击 ，闭路则单击 。当前状态：显示端口的当前状态。在当前状态并非正常状态时，将激活输入或输出。当断开连接或电压高于 1 V DC 时，设备上的输入为开路。

注意

在重启过程中，输出电路为开路。当重启完成时，电路将恢复为正常位置。如果更改此页面上设置，无论是否存在活动的触发器，输出电路都将返回其正常位置。

受监控 ：如果有人篡改连接到数字 I/O 设备，请打开，以侦测并触发操作。除了侦测某个输入是否打开或关闭外，您还可以侦测是否有人篡改了该输入（即，剪切或短路）。监控连接功能要求外部 I/O 回路中存在其他硬件（线尾电阻器）。

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的快照。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跟踪之类敏感信息。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。

网络追踪

重要

网络跟踪文件可能包含敏感信息，例如证书或密码。

通过记录网络上的活动，网络追踪文件可帮助您排除问题。跟踪时间：选择以秒或分钟为单位的跟踪持续时间，并单击下载。

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。

- 安讯士
- 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。CA 证书已设置：查看当前设置或添加证书。

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

各 Axis 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 Axis 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，请前往*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。
- 自动还原：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。

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 上的产品数据表。

有关 AXIS OS 网络安全的详细信息，请阅读*AXIS OS 强化指南*。

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。

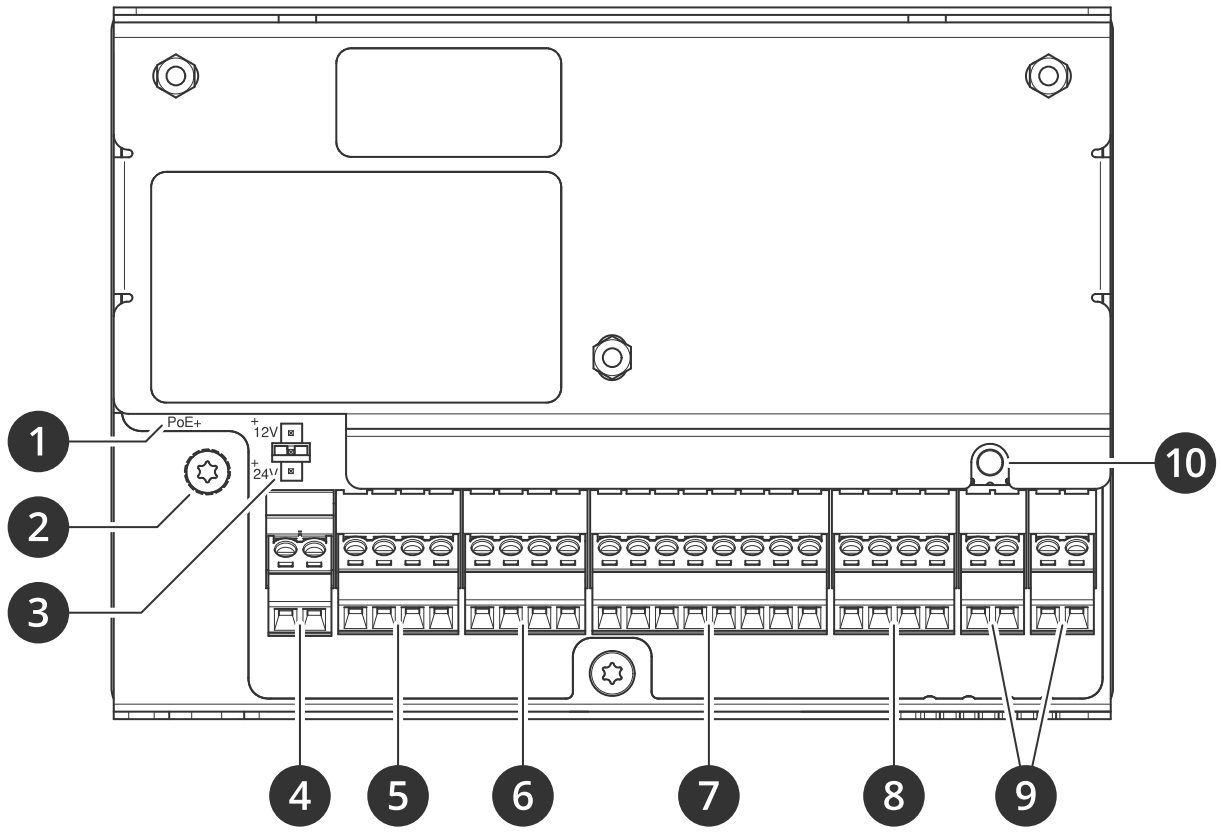
安讯士设备ID

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

要了解有关 Axis 设备中网络安全功能的更多信息，请前往*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 门连接器
7 读取器连接器
8 辅助连接器
9 外部连接器
10 控制按钮

LED 指示灯

LED	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。

1. 当 COM 连接到 NO 时继电器处于活动状态。

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。

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

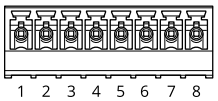
此设备可由 PoE 或 DC 输入供电。参见和。

- 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。

读取器连接器

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

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



为一个 OSDP 读取器配置

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

为两个 OSDP 读取器配置（多点）

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

重要

- 当读取器由控制器供电时，电缆长度不超 200 米（656 英尺）。仅针对 Axis 读取器进行验证。
- 当读取器不是由控制器供电时，如果满足以下电缆要求，读取器数据的合格电缆长度可达 1000 米（3280.8 英尺）：1 对屏蔽双绞线，AWG 24，120 欧姆阻抗。仅针对 Axis 读取器进行验证。

为一个 Wiegand 读取器配置

功能	引脚	注意	规格
DC 接地 (GND)	1		0 V DC
DC 输出 (+12 V)	2	为读取器供电。	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

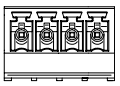
重要

- 当读取器由控制器供电时，电缆长度不超 150 米（500 英尺）。
- 当读取器不是由控制器供电时，如果满足以下电缆要求，读取器数据的合格电缆长度可达 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，则安装线尾电阻器。使用连接图来安装监控输入。参见 。



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，电缆长度不超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

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	常见	
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

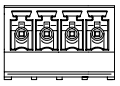
在外部设备结合了移动侦测、事件触发和报警通知等功能的情况下，使用辅助连接器。除0 V DC 参考点和电源（DC 输出）外，辅助连接器还提供连接至以下模块的接口：

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。

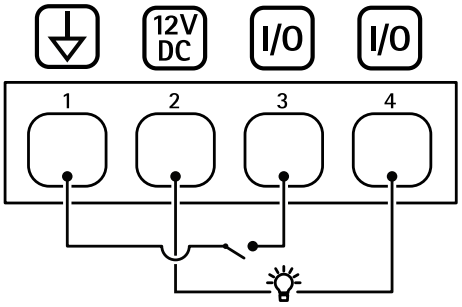
数字输出 – 用于连接继电器和 LED 等外部设备。连接的设备可以通过 VAPIX® 应用可编程接口 (API) 或从产品网页激活。

4 针接线端子



功能	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 = 总计 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 – 启用时内部连接至针 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



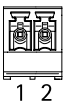
1 DC 接地
2 DC 输出 12 V
3 I/O 配置为输入
4 I/O 配置为输出

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 电源输入的双引脚接线盒。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

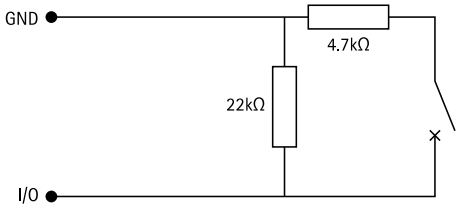
UL：使用具有适当额定功率的 UL 603 上市电源供应器提供 DC 电源，具体取决于应用。

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。

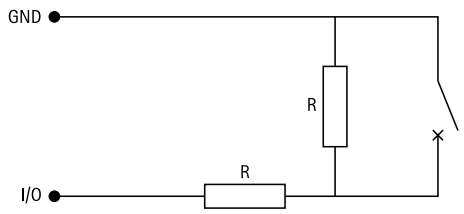
并联优先连接

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。



注意

建议使用绞合屏蔽电缆。将屏蔽件连接至 0 V DC。

故障排除

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。
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：
   - 采用 AXIS OS 12.0 及更高版本的设备：从链路本地地址子网 (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 可根据主动跟踪或长期支持 (LTS) 跟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 Axis 端到端系统产品，则建议使用主动跟踪中的 AXIS OS。如果您使用第三方集成，则建议使用 LTS 跟踪，其未针对主动跟踪进行连续验证。使用 LTS，产品可维持网络安全，而无需引入重大功能性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，请前往*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

- 在升级设备软件时，将保存预配置和自定义设置（如果这些功能在新 AXIS OS 中可用），但 Axis Communications AB 不对此做保证。
- 确保设备在整个升级过程中始终连接到电源。

注意

使用活动跟踪中的新 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，请前往*axis.com/support/device-software*。

注意

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、线索和解决方案

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。

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	
设备位于不同子网掩码上	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 地址已用于其他设备	从网络上断开 Axis 设备。运行 Ping 命令（在 Command/DOS 窗口中，键入 `ping` 和设备的 IP 地址）： • 如果收到消息：**来自 <IP 地址>的回复**：`bytes=32; time=10...` 这意味着该 IP 地址可能已被网络上的另一台设备占用。请从网络管理员处获取新的 IP 地址，然后重新安装该设备。 • 如果收到消息：`Request timed out`，这意味着该 IP 地址可用于此 Axis 设备。请检查布线并重新安装设备。
可能的 IP 地址与同一子网上的其他设备发生冲突	在 DHCP 服务器设置动态地址之前，将使用 Axis 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。

无法通过浏览器访问该设备	
无法登录	启用 HTTPS 时，请确保在尝试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`。如果根帐户的密码丢失，则设备必须重置为出厂默认设置。参见。

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AXIS 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。如果需要，可以手动分配静态 IP 地址。如需说明，请前往*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 Axis 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。

可以从本地访问设备，但不能从外部访问

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 Companion：免费，适用于有基本监控需求的小型系统。
- AXIS Camera Station 5：30 天试用版免费，适用于小中型系统。
- 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，请前往*axis.com/vms*。

无法通过 SSL 通过端口 8883 进行连接，MQTT 通过 SSL

防火墙会阻止使用端口 8883 的通信，因为它被认为是不安全的。	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 MQTT 的使用。请与服务器/代理提供商确认是否支持 ALPN 以及要使用的 ALPN 协议和端口。

联系支持人员

如果您需要更多帮助，请前往*axis.com/support*。

用户手册

版本 M7.3
日期： 10月 2024
零件号 T10181041