AXIS S3008 Recorder

用户手册

关于您的设备

AXIS S3008 Recorder 是一款紧凑型网络视频录像机，内置 PoE 交换机，易于安装。该设备配有监控级硬盘。还包括一个 USB 端口，可轻松导出视频片段。该录像机有三种型号 – 包括 2 TB、4 TB 或 8 TB 硬盘。

可以将多少个摄像机连接到录像机?

可以将多达 8 个设备连接到录像机的 PoE 交换机。

录像机可以为摄像机提供多少功率?

以下是以太网供电 (PoE) 的限制：

- 录像机可以通过 PoE 为多达 8 个设备供电。
- 总的可用功率为：
  - 2 TB 和 4 TB：65 W
  - 8 TB：60 W
- 每个网络端口在 PoE 端口 (PSE) 支持高达 15.4 W（PoE 3 类），在摄像机端 (PD) 支持高达 12.95 W。
- 交换机根据所连接设备的 PoE 类别分配 PoE 电源。

浏览器支持

Windows®

- Chrome™（推荐）
- Firefox®
- Edge®

OS X®

- Chrome™（推荐）
- Safari®

其他

- Chrome™
- Firefox®

要查找更多有关设备使用方法的信息，请参见 *Documentation | Axis Communications* 上提供的用户手册。如果您需要更多有关推荐浏览器的信息，请转到 *Axis OS browser support | Axis Communications*。

开始使用

开始使用

注意

系统设置过程中需要访问互联网。

1. *注册 My Axis 账户 3*
2. *安装硬件 3*
3. *安装桌面应用程序 4*
4. *创建场所 4*
5. *安装移动应用程序 4*

安装完成时：

- 系统中的 Axis 设备都具有新版固件。
- 各设备都有密码。
- 使用默认设置的录制处于活动状态。
- 您可以使用远程访问。

注册 My Axis 账户

在axis.com/my-axis/login上注册*My Axis*账户。

为了使您的My Axis账户更加安全，请激活多因素身份验证 (MFA)。MFA是一种安全系统，它增加了多一层验证，以确保用户的身份。

要激活 MFA，请执行以下操作：

1. 转到 *axis.com/my-axis/login*。
2. 使用您的 My Axis 凭证登录。
3. 转到 并选择Account settings（账户设置）。
4. 单击安全设置
5. 点击处理您的两因素身份验证。
6. 输入您的 My Axis 凭据。
7. 选择 身份验证器应用程序（TOTP）或电子邮件中的一种身份验证方法，然后按照屏幕上的说明进行操作。

安装硬件

1. 安装摄像机硬件。
2. 通过 LAN 端口将录像机连接到网络。
3. 将摄像机连接到录像机的集成 PoE 交换机或外部 PoE 交换机。
4. 将计算机连接到录像机所在的同一网络。

5. 将电源连接到录像机上。

重要

您必须先将电源线连接到录像机，然后再将电源线连接到电源插座。

6. 等待几分钟，让录像机和摄像机启动后再继续。

⚠警示

将录像机放在通风良好的环境中，并在录像机周围留出足够的空间，以避免过热。

安装桌面应用程序

1. 转到*axis.com/products/axis-camera-station-edge*，然后单击Download（下载）以下载适用于Windows的。
2. 打开设置文件，然后按设置助手操作。
3. 用您的 *My Axis 帐户*登录。

创建场所

场所是监控解决方案（例如商店中的全部摄像机）的单一进入点。您可以通过一个 My Axis 帐户追踪多个场所。

1. 启动桌面应用程序。
2. 用您的 *My Axis 帐户*登录。
3. 单击Create new site（创建新场所），并为场所命名。
4. 单击下一步。
5. 选择要添加到场所的设备。
6. 单击下一步。
7. 选择存储。
8. 单击下一步。
9. 在准备安装页面上，脱机模式 和 升级固件 在默认情况下处于打开状态。如果您不想访问脱机模式或将您的设备升级到新的固件版本，您可以将其关闭。
10. 单击Install（安装）并等待配置设备。

    配置需要几分钟。

安装移动应用程序

借助 移动应用，您可以从不同位置访问设备和录制内容。您还可在发生事件或有人从对讲机中调用时获取通知。

适用于 Android

单击 *下载*或扫描以下 QR 码®。

开始使用

适用于 iOS

单击 *下载*或扫描以下 QR 码。

打开移动应用并使用您的安讯士凭证登录。

如果您没有 My Axis 帐户，则您可转到 *axis.com/my-axis* 注册新帐户。

QR 码是 Denso Wave Incorporated 在日本和其他国家/地区的注册商标。

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。
- 更改账户：从当前账户退出，然后登录新账户。
- 退出：从当前账户退出。

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

设备信息

显示设备信息，包括 AXIS OS 版本和序列号。

升级 AXIS OS：升级设备上的软件。转到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。转到可更改 NTP 设置的时间和位置页面。

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：转到*《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。

持续录制中

显示正在进行的录制及其指定的存储空间。

录像：查看正在进行的录制和过滤的录制文件及其来源。有关详细信息，请参见 显示保存录制内容的存储空间。

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特权应用程序 ：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。
  如果你没有牌照密钥，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。
- 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。
  - 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。
- 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 –。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间。

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。

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。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。

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：
- 一键式：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。
- 无：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 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 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。
  - 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。
  - “initial” 账户密码: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。

以太网供电

已分配功率：当前已分配的瓦特 (W) 数。总 PoE 消耗：消耗的瓦特 (W) 数。在记录器重启期间保持 PoE 处于活动状态：打开可以在重启录像机时为连接的设备供电。已用空间：已用空间百分比。可用空间：可用于录制的空间的百分比。可用空间：可用磁盘空间以兆字节 (MB)、千兆字节 (GB) 或兆兆字节 (TB) 显示。磁盘状态：磁盘的当前状态。磁盘温度：当前的运行温度。PoE：为每个端口打开或关闭PoE。设备连接后，您将看到以下信息：

- 昵称：昵称是在网络设置中设置的。默认名称是已连接设备的型号和媒体访问控制地址（MAC 地址）的组合。
- 功耗：当前已消耗和分配的瓦特 (W) 数。

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。

- 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+)：选择使用安全元素来实现安全密钥库。
- 受信任的平台模块 2.0（CC EAL4+、FIPS 140-2 2 级）：安全密钥库选择使用 TPM 2.0。

网络访问控制和加密

IEEE 802.1xIEEE 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 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。

＋：单击创建另一个规则。
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。
- 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。如果您将时间设置为0，规则将直接激活。

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。  ：单击可删除活动规则。  ：单击可删除各规则，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。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 Axis 可以创建自定义签名 AXIS OS 证书，因为 Axis 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。

账户

账户

＋ 添加帐户：单击以添加新账户。您可以添加多达 100 个账户。帐户:输入一个唯一的账户名。新密码：输入账户的密码。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、更新和删除其他账户。
- 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：有权访问：
  - 观看并拍摄视频流的快照。
  - 观看和导出录音。
  - 水平转动、垂直转动和变焦；使用PTZ账户权限。

⋮ 上下文菜单包括：更新账户：编辑账户的属性。删除账户：删除账户。无法删除根账户。

SSH 账户

＋ 添加SSH账户：单击以添加新 SSH 账户。
- 限制根访问：打开以限制要求根访问的功能。
- 启用 SSH:打开以使用 SSH 服务。

帐户:输入一个唯一的账户名。新密码：输入账户的密码。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 账户：编辑账户的属性。删除 SSH 账户：删除账户。无法删除根账户。

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 个接收者。

添加接收者：单击以添加接收者。名称：为接收者输入一个名称。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 Axis 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 Axis 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 Axis 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 Axis 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 账户：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：查看接收者:单击可查看各收件人详细信息。复制接收者: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。删除接收者: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。

存储

车载存储

硬盘

- 可用：可用磁盘空间。
- 状态：磁盘是否安装。
- 文件系统：磁盘使用的文件系统。
- 加密：磁盘是否加密。
- 温度：当前的硬件温度。
- 整体运行状况测试：检查磁盘运行状况后的结果。

工具

- 检查：检查存储设备是否存在错误，并尝试进行自动修复。
- 修复：修复存储设备。在修复期间，活进行中的录制将暂停。修复存储设备可能导致数据丢失。
- 格式化：擦除全部录制内容并格式化存储设备。选择一个文件系统。
- 加密：加密存储的数据。
- 解密：解密存储的数据。系统将擦除存储设备上的全部文件。
- 更改密码：更改磁盘加密的密码。更改密码不会中断正在进行的录制。

- 使用工具：单击以运行选定的工具

卸载  ：请在从系统上断开设备之前单击。这将停止正在进行的录制。写保护：打开以保护存储设备防止内容被覆盖。自动格式化  ：磁盘将使用 ext4 文件系统自动格式化。

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。

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。CA 证书已设置：查看当前设置或添加证书。

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

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。

故障排查

Ping：要检查设备是否能到达特定地址，请输入希望运行 Ping 命令的主机名或 IP 地址，然后单击启动。端口检查：要验证设备与特定 IP 地址和 TCP/UDP 端口的连通性，请输入希望检查的主机名或 IP 地址和端口号，然后单击启动。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追踪持续时间，并单击 下载。

配置设备

已分配功率

录像机为每个端口保留一定功率。总保留功率不能超过功率总和。如果录像机尝试保留比可用数量更多的功率，端口将不会启动。这样做可确保已连接的设备都处于通电状态。

PoE 电源可通过以下方式分配至连接的设备：

- PoE 级别 — 每个端口根据所连接设备的 PoE 级别自动确定要保留的功率。
- LLDP — 每个端口通过使用 LLDP 协议交换 PoE 信息来确定保留的功率。

注意

仅含 LLDP 的功率分配仅适用于具有固件 9.80 或更高版本的支持设备，适用于具有固件 10.2 或更高版本的 AXIS S3008 Recorder 。

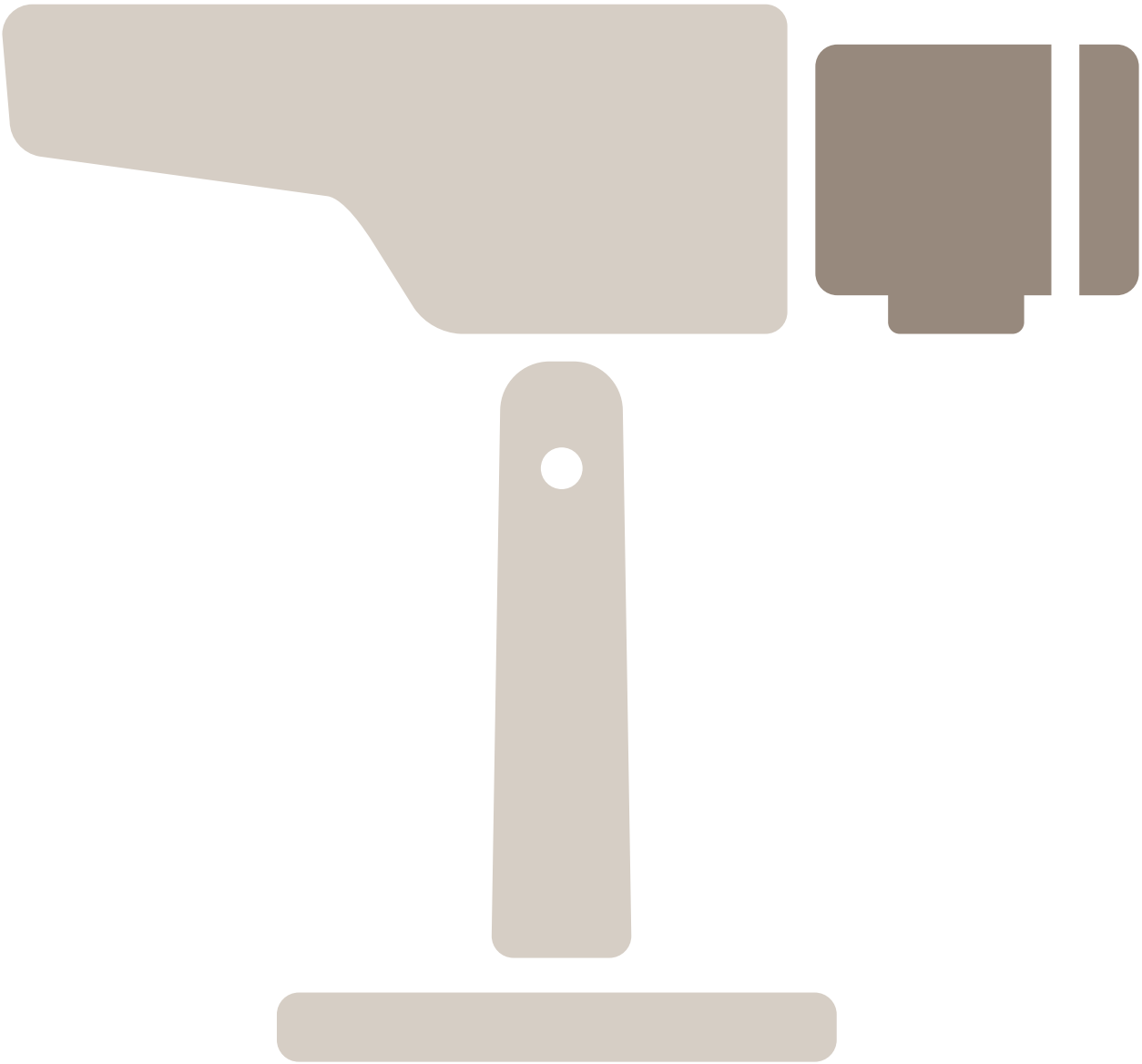
LLDP 在 AXIS S3008 Recorder 中始终处于活动状态，但必须在已连接设备上激活。如果在连接的设备关闭或不支持 LLDP，则将改用 PoE 级别保留。

要在 PoE 设备上打开 LLDP，请执行以下操作：

1. 打开设备网页。
2. 转到 设置 > 系统 > 普通配置 > 网络 。
3. 在 LLDP POE 下 ，选择 LLDP 发送最大 PoE 复选框。

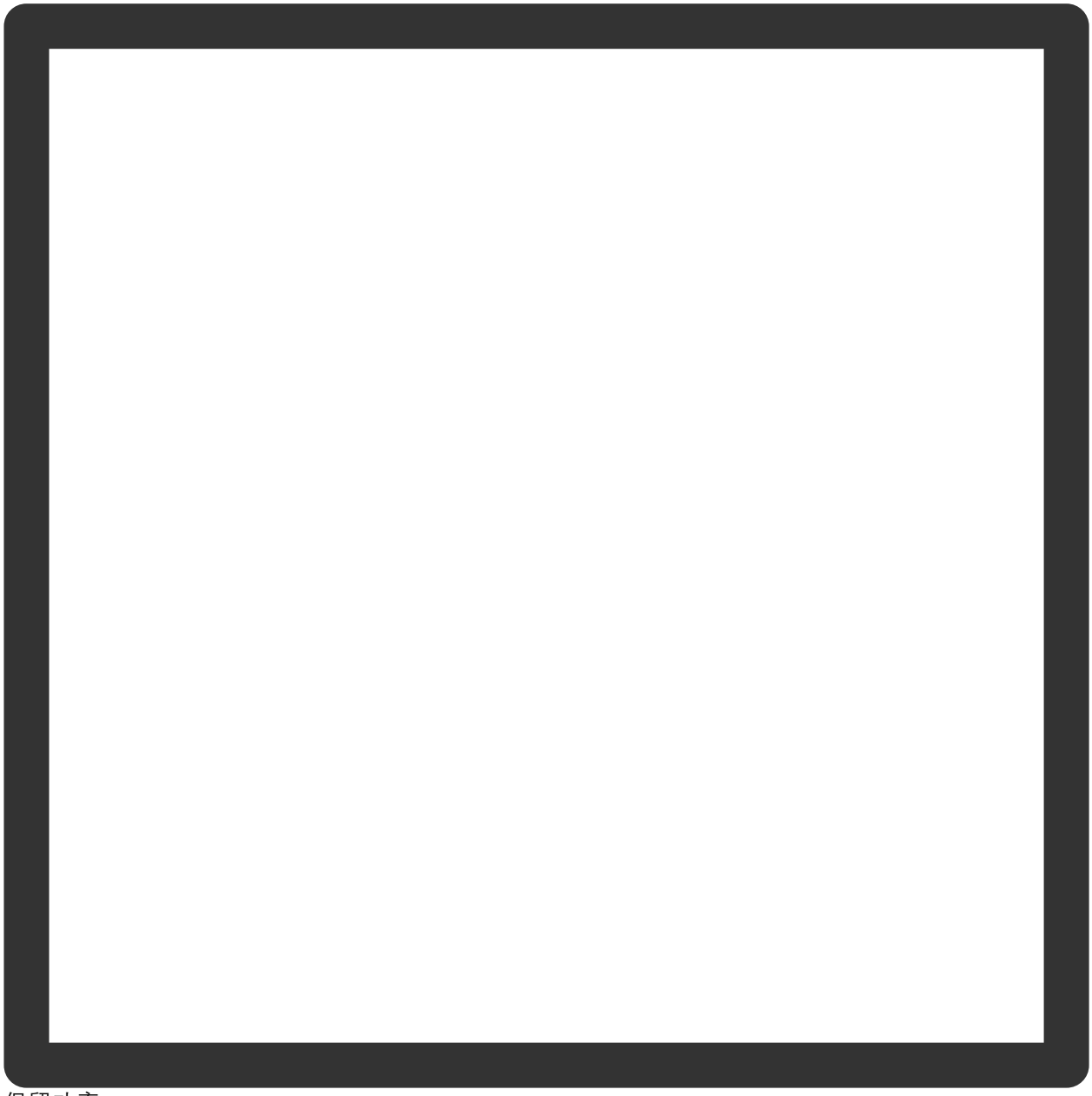
示例:
在此示例中，AXIS S3008 Recorder 的功率总和为 65 W。

配置设备



PoE 级别 2 设备。要求 7 W 的功率，但实际消耗 5 W。

PoE 级别 3 设备。要求 15.5 W 的功率，但实际消耗 7.5 W。



保留功率。

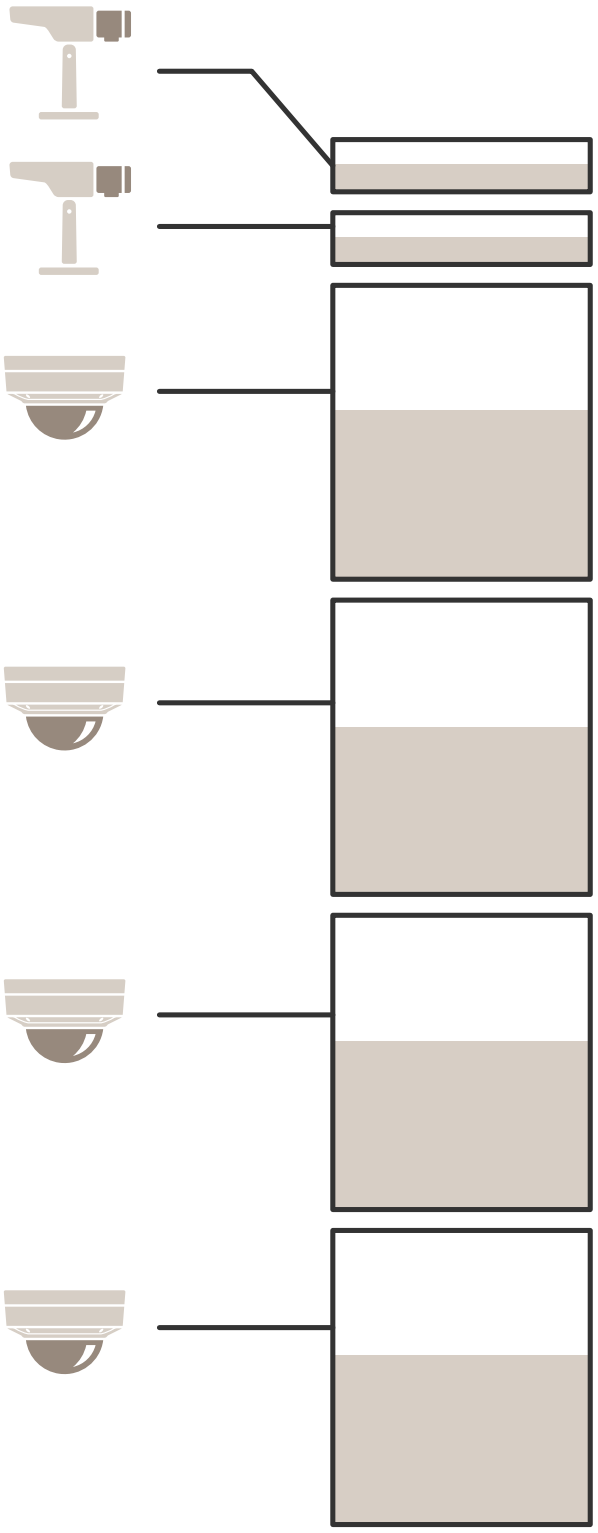
实际功耗。

按 PoE 级别分配功率

配置设备

保留功率

实际功耗



- 每个端口根据设备的 PoE 级别保留功率。
- 录像机可为 2 台 PoE 3 级设备和 4 台 PoE 2 级设备供电。
- 总功率为 (2 x 15.5) + (4 x 7) =59 W。
- 实际功耗为 (2 x 7.5) + (4 x 5) = 35 W。

按 LLDP 分配功率

注意

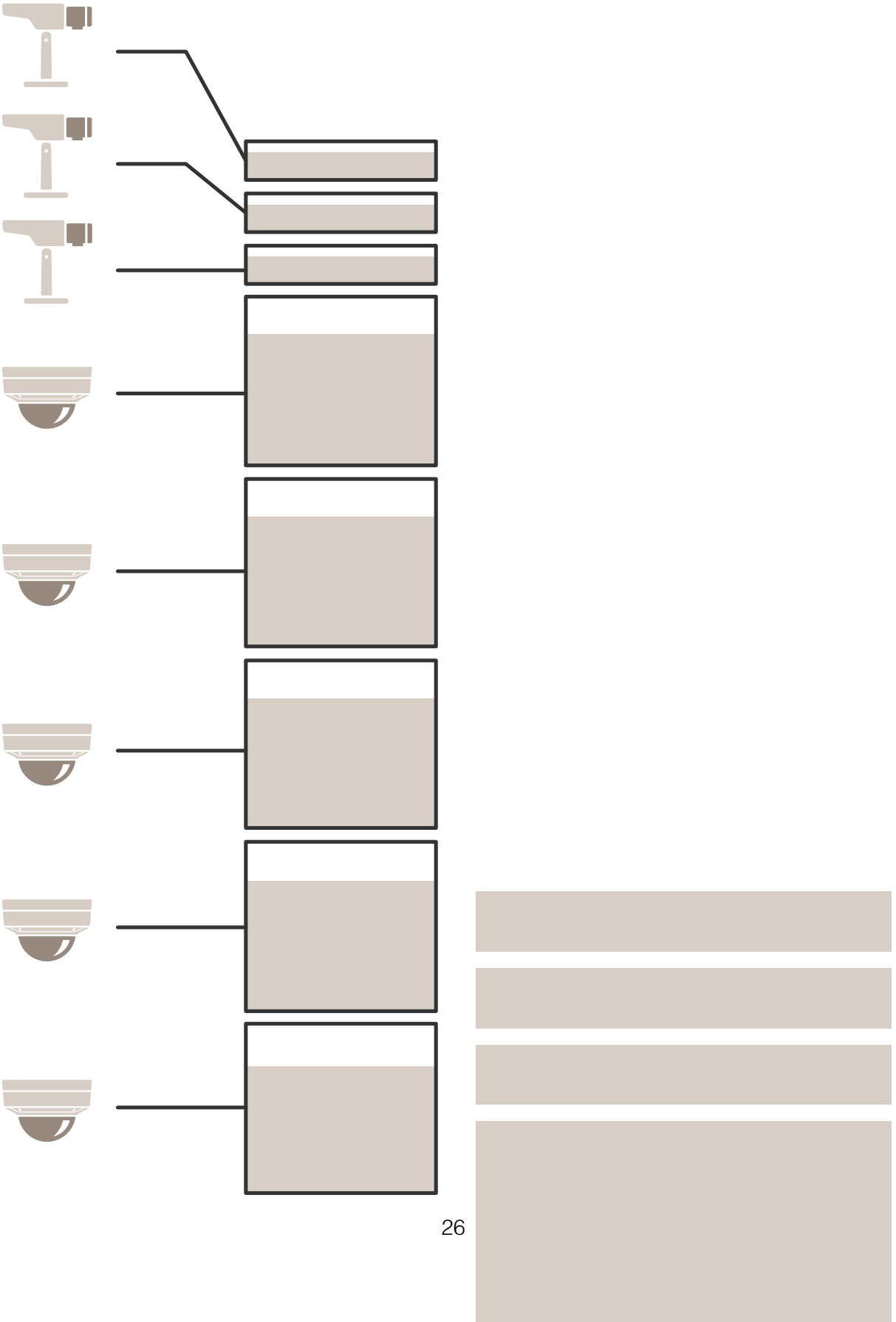
通过 LLDP 进行的功率分配将超过网络电缆上发生的较坏情况下的功率损失。

PoE 级别	1	2	3
摄像机最大功率	3.84	6.49	12.95
电缆损失最大功率	0.14	0.41	1.92
录像机需要功率	3.98	6.90	14.87
该级别最大功率	4.00	7.00	15.40
录像机保留功率	4 W	7 W	15.5 W

配置设备

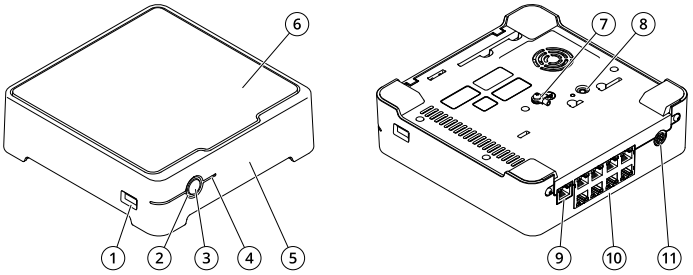
保留功率

实际功耗



- 最大功率由所连接的设备决定。
- 每个端口根据设备的最大 PoE 功耗保留功率。
- 如果最大功率要求在限制范围内，录像机可为多达 8 台设备供电。
- LLDP 下，8 台 PoE 3 级设备所保留的总功率为 (8 x 7.5) = 60 W。
- LLDP 下，8 台 PoE 3 级设备实际功耗为 (8 x 7) = 56 W。
- 以这种方式，更紧缩的 PoE 预算分配允许连接更多的设备。

产品概述



1 USB 端口
2 状态LED
3 电源按钮
4 硬盘 LED
5 报警蜂鸣器
6 硬盘
7 接地
8 控制按钮
9 LAN 端口
10 PoE 端口（8 个）
11 电源输入

电源按钮

- 要关闭录像机，请长按电源按钮，直到蜂鸣器发出短暂的声音。
- 要使蜂鸣器静音，请短按电源按钮。

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 *硬重置录像机 30*。
- 通过互联网连接到一键云连接 (O3C) 服务。若要连接，请按住该按钮约 3 秒，直到 LED 状态指示灯呈绿色闪烁。

故障排除

LED 状态指示灯为您提供以下信息：

状态LED	指示
绿色	录像机已打开，状态正常。
橙色	录像机正在启动，或固件正在升级。等待 LED 变绿。
红色	这可能意味着超过了 PoE 预算。如果您刚刚将一个设备连接到录像机，请再试着将其移除。有关 PoE 限制的详细信息，请参见*录像机可以为摄像机提供多少功率？ 2*。

硬盘 LED 为您提供以下信息：

硬盘 LED	指示
绿色	当数据写入硬盘时，LED 呈绿色闪烁。
红色	发生录制中断。有关更多信息，请转到系统>存储。

蜂鸣器响起的原因为：

- 超过了 PoE 预算。如果您刚刚将一个设备连接到录像机，请再试着将其移除。有关 PoE 限制的详细信息，请参见*录像机可以为摄像机提供多少功率？ 2*

注意

您可以短按电源按钮来停止蜂鸣器。

录像机关闭：

- 录像机严重过热。

技术问题、线索和解决方案

颁发	解决方案
录制不可用。	转到*解决常见问题 29*。
无法连接到摄像机。	转到*解决常见问题 29*。
我收到错误通知：“无联系”。	转到*解决常见问题 29*。
场所没有在移动应用中显示。	确保您使用的是 AXIS Companion 版本 4 移动应用。

解决常见问题

在重启、配置或重置设备之前，我们建议您保存一份系统报告。

请参见 *保存系统报告 31*。

1. 检查摄像机和录像机是否通电。
2. 检查是否已连接到互联网。
3. 检查网络是否运行正常。
4. 检查摄像机是否与计算机连接到同一个网络，除非您处于远程状态。

仍无法正常工作?

5. 请确保摄像机、录像机和 AXIS Companion 桌面应用程序装有更新的固件和软件更新。
   请参见*升级固件 30*。
6. 重启 AXIS Companion 桌面应用程序。
7. 重启摄像机和录像机。

仍无法正常工作?

8. 对摄像机和录像机进行硬重置，使其恢复到出厂默认设置。
   请参见 *硬重置录像机 30*。
9. 再次将重置的摄像机添加到您的场所。

仍无法正常工作?

10. 更新您的显卡驱动。

仍无法正常工作?

11. 保存系统报告并联系*安讯士技术支持*。
    请参见 *保存系统报告 31*。

升级固件

新的固件更新为您带来更新和经过改进的特性、功能和安全性增强。

1. 转到主设备的网页界面。
2. 转到 维护 > 固件升级，然后单击升级。
3. 按屏幕说明操作。

硬重置录像机

重要

在开机状态下时，小心地移动录像机。突然移动或冲击可能会损坏硬盘。

注意

- 硬重置将重置全部设置，包括 IP 地址。
- 硬重置不会删除您的录制内容。

1. 关闭录像机：
   按住录像机前面的电源按钮 4–5 秒，直到听到一声蜂鸣声。
2. 等到录像机关闭后，再将其翻转以访问控制按钮。

3. 按住控制按钮。按下并松开电源按钮以启动录像机。15–30 秒后，当 LED 指示灯呈淡黄色闪烁时，松开控制按钮。
4. 小心地将录像机放回原位。
5. 当状态LED指示灯变绿时，此过程完成。产品已重置为出厂默认设置。如果网络上没有可用的 DHCP 服务器，则默认 IP 地址为 `192.168.0.90`
6. 重置连接到录像机的设备。
7. 如果您的硬盘已加密，则必须在录像机重置后手动安装该硬盘：

   7.1 转到设备的网页界面。

   7.2 转到系统>存储，然后单击安装。

   7.3 输入加密硬盘时使用的加密密码。

无法登录产品网页界面

如果您在配置过程中为产品设置了密码，并且稍后将该产品添加到一个场所，则无法再使用已设置的密码登录产品网页界面。这是因为 AXIS Companion 软件会更改场所中全部设备的密码。

要登录场所中的设备，请键入用户名根和场所密码。

如何擦除全部录制内容

1. 在设备的网页界面中，转到系统 > 存储。
2. 选择格式化，然后单击使用工具。

注意

此过程将擦除硬盘上的全部录制内容，但是录像机和场所的配置不会改变。

保存系统报告

1. 在中，转到  > Save system report（保存系统报告）。
2. 在 Axis 帮助台上登记新事例时，请附上系统报告。

需要更多帮助?

实用的链接

- *AXIS Companion 用户手册*

联系支持人员

如果您需要更多帮助，请转到 *axis.com/support*。

用户手册
AXIS S3008 Recorder

版本 M30.2
日期： 1月 2025
零件号 T10152902