AXIS D8204-E PoE++ Switch

用户手册

目录

关于本手册 3
缩写 3
解决方案概述 4
开始 5
通过浏览器访问产品 5
了解产品网页 5
了解产品的内置帮助 6
设置示例 7
设置访问 VLAN 7
基于 MAC 地址保留 IP 地址 8
在交换机之间建立冗余链路，以实现网络冗余 8
使用 VAPIX 打开或关闭端口的 PoE 功能 9
配置 MACsec 9
静态 CAK 9
动态 CAK 10
连接 1Gbps SFP 模块 11
维护系统 12
重新启动产品 12
重置为出厂默认设置。 12
升级设备软件 13
恢复到备用的软件映像 13
规格 14
产品概览 14
故障排查 15
网络安全 16
漏洞管理 16
安全通知 16
安全产品生命周期 16

关于本手册

注意

该产品旨在供负责操作和维护网络设备的网络管理员使用。需要了解常规的交换机功能、安全性、网际协议 (IP) 和简单网络管理协议 (SNMP) 的基本工作知识。

本用户手册将为您提供有关如何进行以下操作的信息：

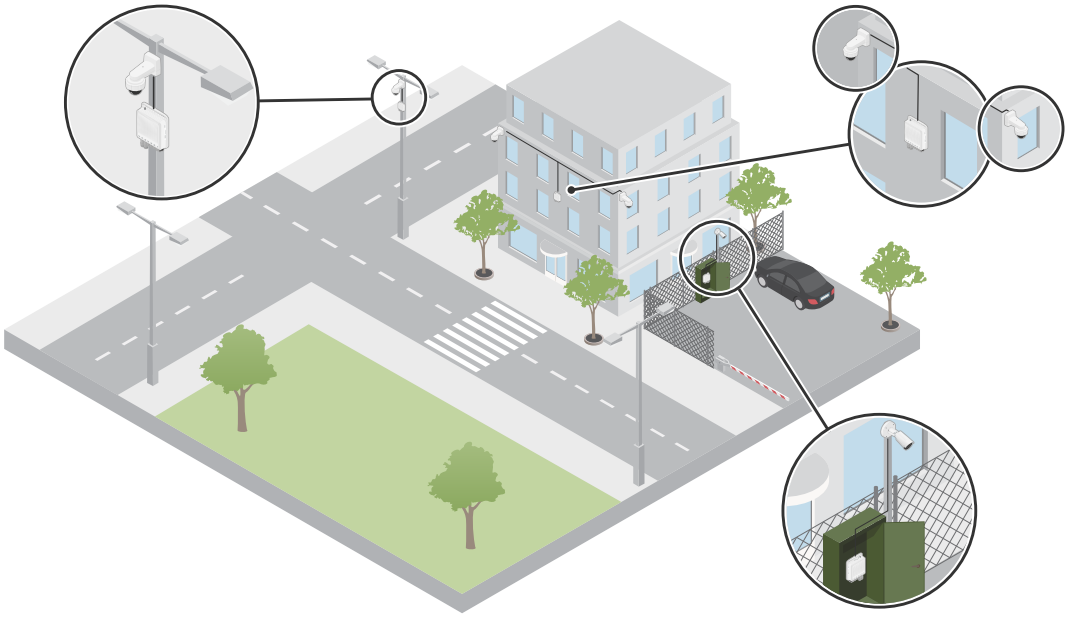
- 访问产品
- 配置指定的设置示例
- 对产品进行维护

产品功能及其设置在与上下文相关的内置帮助中有更详细的介绍。

缩写

缩写	说明
MACsec	媒体访问控制安全
802.1X	网络访问控制
802.1AE	与 MACsec 相同
CAK	连接关联密钥
CKN	连接密钥名称
DHCP	动态主机配置协议
OpenSSL	开源软件库
PoE	以太网供电
半径：	远程身份验证拨入用户服务
SFP：	光纤接口，小型可插拔模块
SFP+	增强型，小型可插拔模块
SNMP	简单网络管理协议
SSL	安全套接字层
TLS	传输层安全协议
虚拟局域网 (VLAN)	虚拟局域网

解决方案概述



安讯士前端设备安装在现场，通过以太网连接到安讯士交换机。交换机通过光纤连接。

开始

通过浏览器访问产品

注意

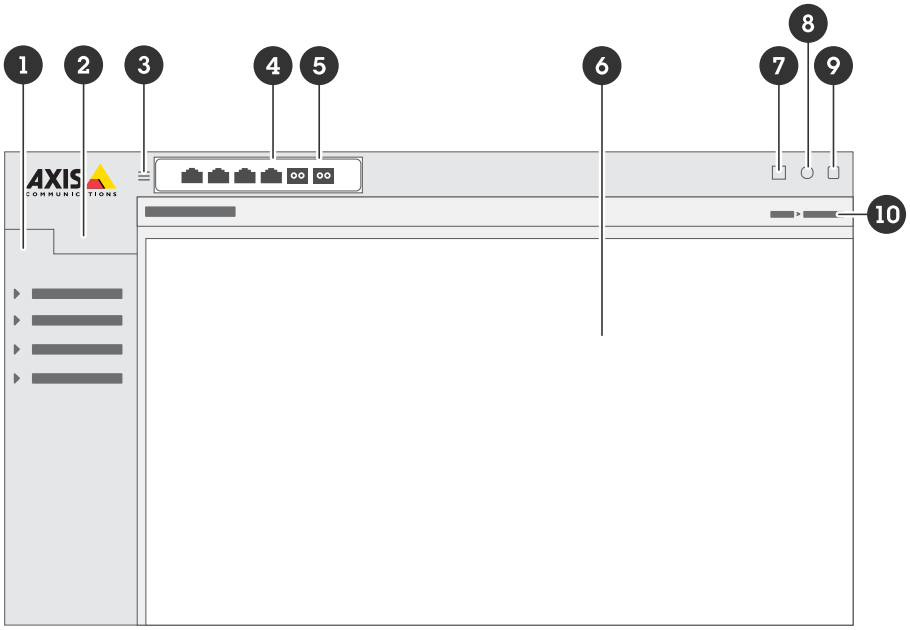
- 按照安装指南中的规定，安装、连接设备和为设备供电。
- 按照本节中的步骤操作后，您将进入该产品的网页，并能够对该产品进行配置和管理。

1. 使用 AXIS IP Utility 或 AXIS Device Manager 在网络上查找设备。有关如何查找设备的更多信息，请访问*axis.com/support*.
2. 输入产品标签上提供的用户名和密码。
   默认用户名为root。
3. 按照安装向导中的步骤进行操作：

– 更改密码（为了安全起见，建议您更改）
– 通过 DHCP 或者手动设置 IP 地址
– 设置日期和时间信息
– 设置系统信息

4. 单击**Save（保存）**。
5. 使用新密码重新登录。

了解产品网页



1 基本功能
2 高级功能
3 Toggle（切换）按钮 – 隐藏或取消隐藏菜单
4 RJ45 端口状态指示灯
5 SFP 端口状态指示灯
6 基本/高级功能的内容区域
7 Save（保存）按钮 – 将设置保存到启动配置文件中
8 帮助按钮 – 访问与上下文相关的内置帮助
9 退出按钮
10 菜单路径

了解产品的内置帮助

您的产品具有与上下文相关的内置帮助。该帮助提供了产品的基本和高级功能及其设置的更详细信息。要访问指定视图的帮助内容，请单击

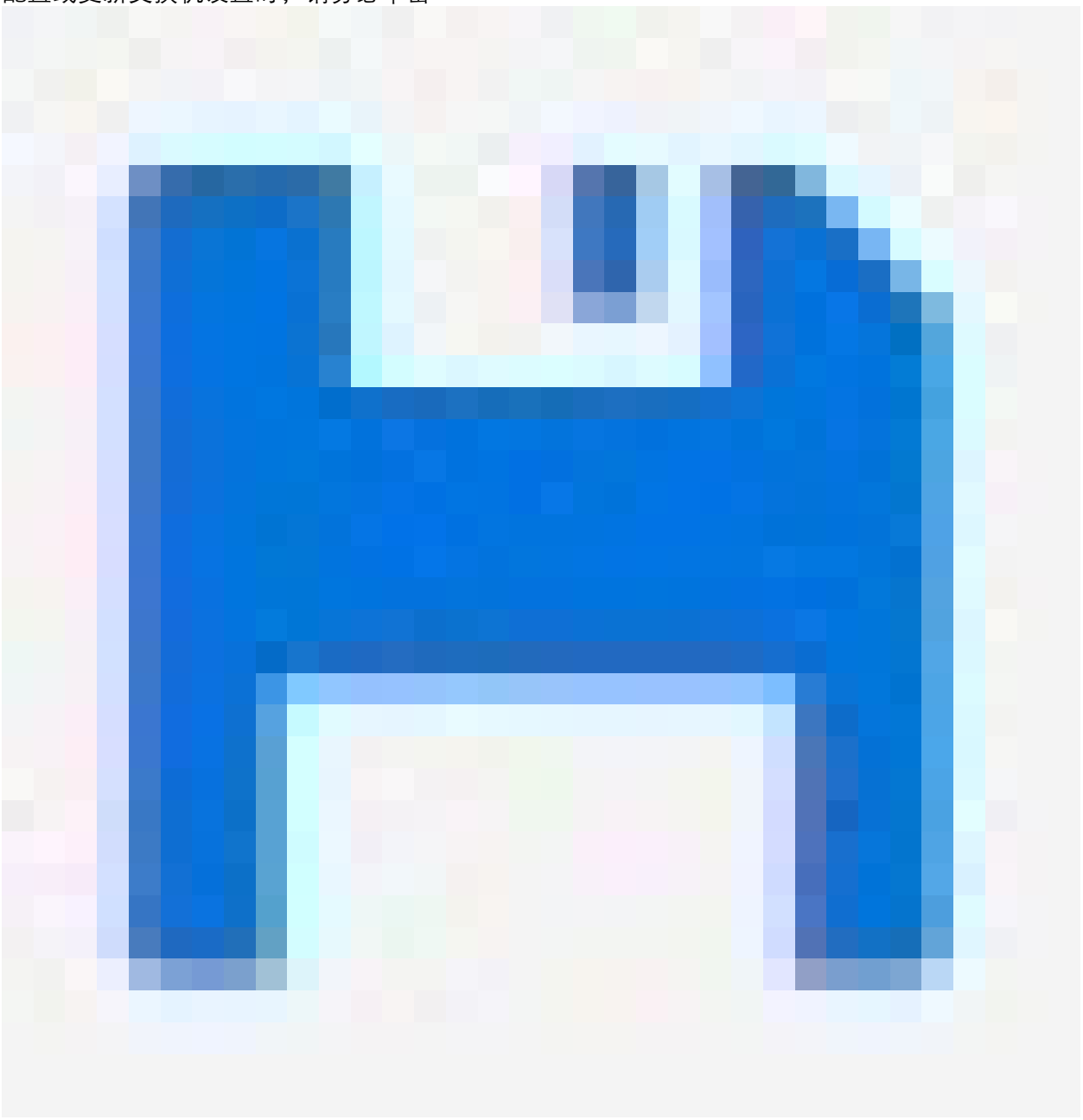


。某些帮助内容还包括可单击的术语和缩略语，在内置词汇表中会有更详细的说明。

设置示例

注意

配置或更新交换机设置时，请务必单击



以将更新保存到启动配置文件。

重新开始或重新启动交换机后启动配置文件会保留，但在将交换机恢复为出厂默认设置后不会保留。

设置访问 VLAN

VLAN 通常用于在大型网络中创建多个广播域，但也可用于隔离网络流量。例如，视频流量可以属于某个 VLAN，而其他网络流量属于另一个 VLAN。

1. 转到 **Advanced（高级）** > **VLANs** > **Configuration（配置）**。
2. 在 **Global VLAN Configuration（全局 VLAN 配置）**下方，在 **Allowed Access VLANs（允许访问的 VLAN）**字段中，输入要创建的 VLAN ID。例如，如果您输入：1、10–13、200、300，将创建以下 VLAN ID：1、10、11、12、13、200 和 300。

3. 要向在**端口 VLAN 配置**下创建的 VLAN ID 分配一个指定端口，请在**端口 VLAN** 字段中输入此 ID。
4. 单击**Save（保存）**。

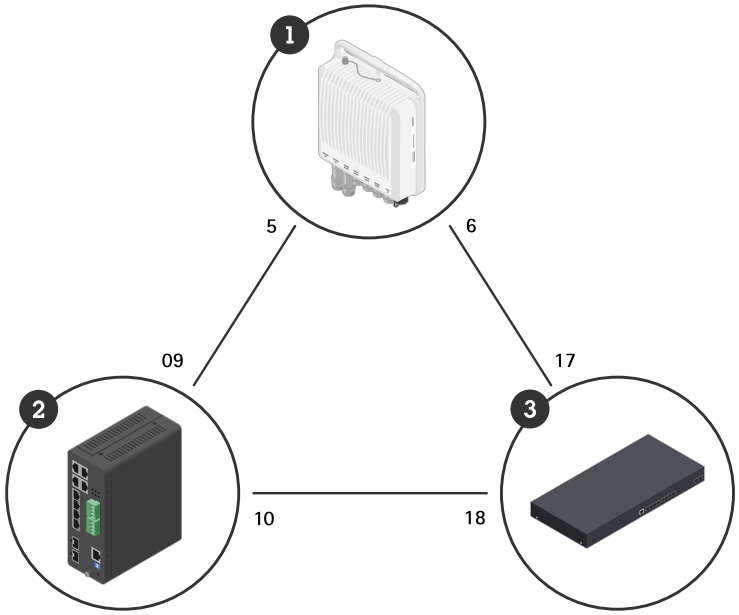
基于 MAC 地址保留 IP 地址

1. 转到 **高级** > DHCP > **服务器** > **配置** > **地址池**。
2. 单击**添加新地址池**。
3. 输入地址池的名称，然后单击**保存**。名称中不允许使用空格。
4. 要访问地址池设置，请单击已添加的名称。
5. 在**类型**下拉菜单中，选择**主机**。
6. 输入其他所需设置，如IP地址、**子网掩码**和**默认路由器**。
7. 在**客户端标识符**下拉菜单中，选择MAC。
8. 在**Hardware Address（硬件地址）**字段中，输入设备的 MAC 地址。
9. 单击**Save（保存）**。

在交换机之间建立冗余链路，以实现网络冗余

如果需要网络冗余，您可以使用生成树配置在交换机之间建立冗余链路。

示例：
在此示例中，交换机 AXIS D8204–E (1)、AXIS D8208–R (2) 和 AXIS T8516 (3) 通过一条冗余链路连接，且未配置额外的虚拟局域网 (VLAN)。如果交换机之间有上行链接出现故障，则会激活冗余链路并提供网络连接。



设备名称：	**型号名称**	CIST 端口
交换机 – 01	AXIS D8204–E	5, 6
交换机 – 02	AXIS D8208–R	9, 10
交换机 – 03	AXIS T8516	17, 18

在每台交换机的网页上建立冗余链路：

1. 转到 **高级** > **生成树** > **配置** > **桥接设置**。
2. 在**协议版本**下拉菜单中的**基本设置**下，选择 RSTP，然后单击**保存**。
3. 转到 **高级** > **生成树** > **配置** > CIST **端口**。
4. 在CIST Normal Port Configuration（CIST**正常端口配置**）下，务必为交换机的端口选择 STP Enabled（**启用**STP），如下所示：

– 交换机 – 01：端口 5 和 6
– 交换机 – 02：端口 9 和 10
– 交换机 – 03：端口 17 和 18

5. 单击Save（**保存**）。

注意

如果必须将某个端口用作主通信链接，请在CIST Normal Port Configuration（CIST**正常端口配置**）下为该端口输入Path Cost（**路径成本**）。如果未指定，交换机将自动选择端口。例如，如果要使用端口 17 作为主通信链接，请在端口 6 输入Path Cost（**路径成本**）值 10，然后在端口 18 输入Path Cost（**路径成本**）值 50。

使用 VAPIX 打开或关闭端口的 PoE 功能

您可以在 VAPIX 中使用以下命令来打开或关闭特定端口的 PoE 功能：

- Turn PoE on（开启 PoE）：
  `http://[IP address of the switch]/axis-cgi/nvr/poe/setportmode.cgi?port=[number of the port on the switch]&enabled=yes&schemaversion=1`
- Turn PoE off（关闭 PoE）：
  `http://[IP address of the switch]/axis-cgi/nvr/poe/setportmode.cgi?port=[number of the port on the switch]&enabled=no&schemaversion=1`

配置 MACsec

MACsec 配置可在两台支持 MACsec 的设备之间建立安全连接，确保设备之间的通信具有保密性、经过身份验证，并能抵御重放攻击。

静态 CAK

连接关联密钥（CAK）是一种加密密钥，用于确保设备之间实现安全通信。128 位密钥必须由 32 个十六进制字符组成，256 位密钥则必须由 64 个十六进制字符组成。

连接密钥名称 (CKN) 用于标识建立设备间安全 MACsec 连接的密钥，并仅允许授权设备参与安全通信。CKN 必须由 2 到 64 个十六进制字符组成，且字符长度必须为偶数。CKN 识别应使用哪个 CAK，且 CAK 和 CKN 必须在链路的两端相匹配，才能建立 MACsec 通信。

您可以手动创建 CAK 和 CKN，也可以使用 OpenSSL 生成它们。

使用 OpenSSL 生成 CAK 和 CKN

1. 在已安装 OpenSSL 的计算机上打开命令提示符。
2. 生成一个 CAK：
   – 类型 `openssl rand –hex 16`。
   – 按下回车键。
3. 生成一个 CKN：
   – 类型 `openssl rand –hex 8`。
   – 按下回车键。
4. 保存 CAK 和 CKN。您以后会需要用到它们。

配置 AXIS OS 设备

1. 在设备的网页界面中，转到 **系统** > **安全** > **网络访问控制和加密**。
2. 对于**身份验证方法**，请选择 IEEE 802.1AE MACsec（**静态 CAK/预共享密钥**）。
3. 对于**密钥协议连接关联密钥名称**，输入 CKN。
4. 对于**密钥协议连接关联密钥**，输入 CAK。
5. 单击Save（**保存**）。

配置交换机

1. 在交换机的网页界面中，转到 **高级** > **安全** > MACsec > **配置** > **策略**。
2. 单击 Add Policy（**添加策略**）。
3. 为该策略输入一个名称。
4. 选择 **启用**，并输入您生成的 CAK 和 CKN。
5. 单击Save（**保存**）。
6. 转到 **高级** > **安全** > MACsec > **配置** > **接口**。
   - 对于连接到设备的**接口**，请从下拉列表中选择新策略。
   - 单击Save（**保存**）。

验证连接

1. 在交换机的网页界面中，转到 **系统** > **安全** > MACsec > **状态** > **状态**。
2. 请确认**状态**的状态指示器为绿色。

动态 CAK

CAK 是通过采用 IEEE 802.1X 和认证服务器进行的身份验证及密钥管理流程生成的。借助此功能，您可以动态生成并管理密钥，从而无需手动配置长期密钥。

注意

- 请确保网络上已配置 RADIUS 服务器且可访问。
- 在 RADIUS 服务器上安装*安讯士设备 ID CA 证书*。

配置连接设备

1. 在设备的网页界面中，转到 **系统** > **安全** > **网络访问控制和加密**。
2. 在**身份验证方法**中，选择 IEEE 802.1X EAP–TLS / IEEE 802.1AE MACsec（**动态 CAK**）。
3. 对于**客户端证书**，选择 RADIUS 服务器信任的安讯士设备 ID 证书<。使用证书可验证身份验证服务器的身份。
4. 对于**CA 证书**，当未选择任何证书时，设备将自动完成身份验证，无论其连接的是哪个网络。
5. 对于 **EAP 身份**，输入与客户端证书关联的用户身份。EAP 身份必须与所选客户端证书中的通用名称 (CN) 字段相匹配。
6. 在 **EAPOL 版本**列表中，选择网络交换机所使用的版本。
7. 开启**使用 IEEE 802.1x** 以使用 IEEE 802.1 x 协议。
8. 单击Save（**保存**）。

在交换机上配置 802.1X

1. 在交换机的网页界面中，转到 **高级** > **安全**>Radius > **配置**。
2. 单击**添加新服务器**，然后输入主机名和密码。
3. 单击Save（**保存**）。
4. 转到 **高级** > **生成树** > **配置** > CIST **端口**。
5. 清除连接到您设备端口的**启用** STP 复选框。

6. 单击Save（保存）。
7. 转到 高级 > 安全> 802.1X > 配置。
8. 在 Mode（模式）列表中，选择 Enabled（启用）。
9. 对于相关端口，将 Admin state（管理状态）设置为 Port–based 802.1X（基于端口的 802.1X）。
10. 单击Save（保存）。

验证 802.1x 连接

1. 在雷达的网页界面中，转到 System（系统）> Security（安全）。
2. 请确认 802.1X 已授权的状态指示器为绿色。

在交换机上配置 MACsec

1. 在交换机的网页界面中，转到 高级 > 安全 > MACsec > 配置 > 策略。
2. 单击 Add policy（添加策略），然后为该策略输入一个名称。
3. 单击Save（保存）。
4. 转到 高级 > 安全 > MACsec > 配置 > 接口。
5. 对于连接到设备的接口，请从列表中选择新创建的策略。
6. 单击Save（保存）。

验证 MACsec 连接

1. 转到 系统 > 安全 > MACsec > 状态 > 状态。
2. 请确认状态的状态指示器为绿色。

注意

如果连接状态一直显示为“待处理”，请重启设备。

连接 1Gbps SFP 模块

1. 转到 Advanced（高级）> Ports（端口）> Configuration（配置）。
2. 用于连接模块的端口（5 或 6），请将其配置为 1 Gbps FDX。

注意

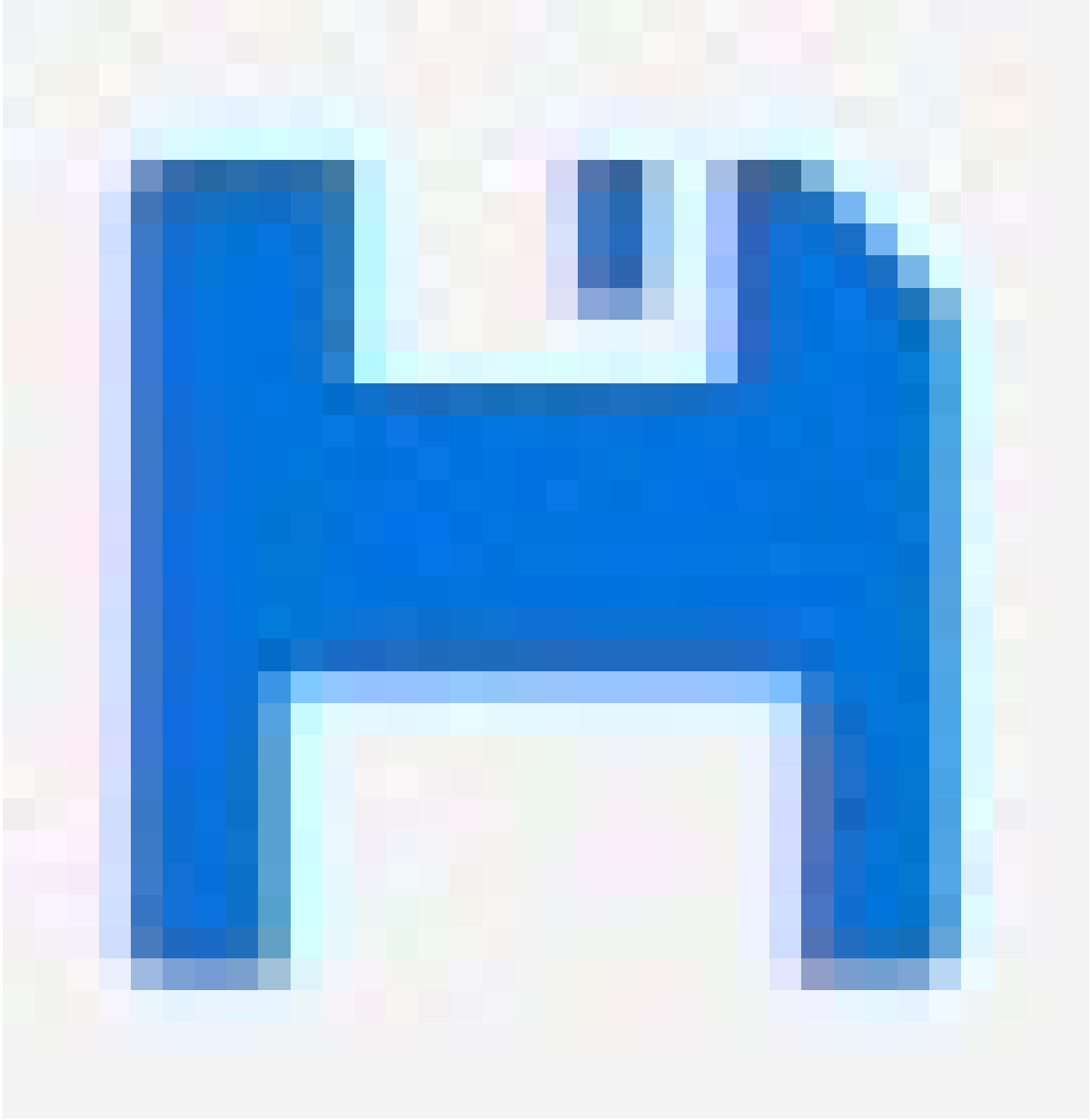
如果将端口设置为自动，则 SFP 和 SFP+ 将能够正常工作。

维护系统

重新启动产品

注意

- 重启期间，通过产品的流量会受到影响。
- 重启设备之前，单击



将设置保存到启动配置文件中。

1. 转到 Advanced（高级）> Maintenance（维护）> Restart Device（重启设备）。
2. 单击Yes（是）。重启后，产品将正常启动。

重置为出厂默认设置。

重要

任何保存的配置都将恢复为出厂默认值。

1. 转到 **高级** > **维护** > **出厂默认设置**。
2. 单击Yes（是）。

如果您忘记了密码，请按照以下步骤将其恢复为出厂默认设置：

1. 将所有设备从交换机上断开，包括电源。
2. 用一条 RJ45 网线将端口 1 和端口 2 连接起来。
3. 连接电源线，给交换机通电。
4. 5 分钟后，拔下 RJ45 网线。电源线应保持连接。
5. 将该单元连接到计算机后，IP 地址应恢复为默认 IP 地址 192.168.0.254。
6. 转到 **高级** > **维护** > **出厂默认设置**。
7. 单击**Yes（是）**。

升级设备软件

重要

软件升级可能需要 10 分钟。在此期间，请勿重新启动设备或关闭设备电源。

注意

升级期间，通过产品的流量会受到影响。

1. 转到 **Advanced（高级）** > **Maintenance（维护）** > **Device Software（设备软件）** > **Software Upgrade（软件升级）**。
2. 要从指定位置选择软件文件，请单击 **选择文件...**。
3. 单击**升级**。

软件升级后，产品将正常重启。

恢复到备用的软件映像

您可以选择使用备用（备份）软件映像，而不使用产品中的活动（主要）软件映像。两个映像的信息表都显示在**高级>维护>设备软件>软件选择**下。

注意

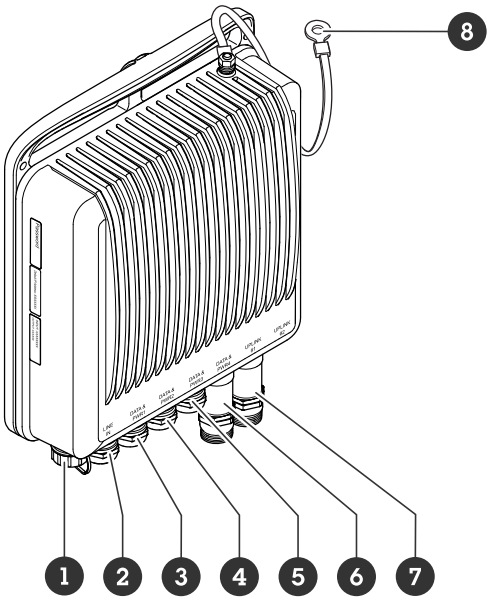
- 如果已将活动映像设置为备用映像，则仅显示**活动映像**表，并且**激活备用映像**按钮将被禁用。
- 如果已将备用映像设置为活动映像（因手动设置或因主映像损坏），并将新的软件映像上传至产品，则新映像将自动设置为活动映像。
- 对于较旧版本的软件，软件版本和日期信息可能为空。这是正常现象。

要将备用映像设置为活动映像，请执行以下操作：

1. 前往 **高级 > 维护 > 设备软件 > 软件选择**。
2. 单击**激活备用映像**。

规格

产品概览



1 电源连接器端口
2 – 5.RJ45 PoE 端口
6 – 7.SFP插槽
8 接地电缆

故障排查

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 12*。

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。

如果您需要更多帮助，请转到 *axis.com/support* 或查阅*安讯士网络交换机配置指南*。

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。

T10231182_zh

2026-11 (M1.17)

© 2025 – 2026 Axis Communications AB