AXIS TP3604-E Cellular Back Box：

用户手册

目录

安装 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 4
配置设备 6
SIM 管理 6
设置 APN 6
验证信号强度和 IP 地址 6
测试连接情况 6
检查管理端口 6
打开转发至摄像机 7
配置摄像机的 IP 所属关系 7
本地模式 7
直通模式 8
设置事件规则 9
触发响应 9
打开外壳时触发通知 9
网页界面 10
规格 11
产品概览 11
LED 指示灯 11
按钮 12
控制按钮 12
连接器 12
PoE 输入连接器（PoE 输入） 12
网络连接器 (PoE 输出） 12
电源连接器 12
清洁您的设备 13
故障排查 14
重置为出厂默认设置。 14
AXIS OS 选项 14
检查当前 AXIS OS 版本 14
升级 AXIS OS 14
技术问题和可能的解决方案 15
联系支持部门 16
网络安全 17
漏洞管理 17
安全通知 17
安全产品生命周期 17

安装



该视频演示了如何将 AXIS TP3604–E Cellular Back Box 与 AXIS P32 Dome Camera Series 和 AXIS P14 Bullet Camera Series 配合安装。

有关涵盖大多数安装场景的说明以及安全信息，请参见安装指南：

开始

在网络上查找设备

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. 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**。

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. 配置并安装设备。

配置设备

要配置设备，您需要完成以下步骤：

1. *SIM 管理, on page 6*
2. 如果您的网络需要显式接入点名称 (APN)， *设置 APN, on page 6*
3. *验证信号强度和 IP 地址, on page 6*
4. *测试连接情况, on page 6*
5. *检查管理端口, on page 6*
6. *打开转发至摄像机, on page 7*

SIM 管理

启用 SIM PIN 时，必须进行 SIM 管理。如果已禁用 SIM PIN，则可跳过此步骤。

1. 插入 SIM 卡。转到 **Modem（调制解调器）** > **SIM management（SIM 管理）** > **SIM status（SIM 状态）**，验证调制解调器/SIM 是否已检测到。
2. 如果 SIM PIN 已锁定，请转到 **Modem（调制解调器）** > **SIM management（SIM 管理）** > **SIM PIN** > **Unlock（解锁）**，并使用正确的 PIN 进行解锁。

设置 APN

注意

仅当您的网络需要显式 APN（接入点名称）时，才需要执行此步骤。

如需设置显式 APN，请转到 **Modem（调制解调器）** > **Cellular network（蜂窝网络）** > **APN**。

验证信号强度和 IP 地址

注意

此步骤需要能够访问蜂窝网络。

1. 在 **System（系统）** > **Modem（调制解调器）** > **Cellular network（蜂窝网络）** > **Radio parameters（无线参数）** > **Signal strength index（信号强度指数）**中检查信号强度。三到四格表示信号质量良好。
2. 在 **System（系统）** > **Modem（调制解调器）** > **Cellular network（蜂窝网络）** > **User equipment IP address（用户设备 IP 地址）**中，确认已获取蜂窝网络 IP 地址。

测试连接情况

注意

此步骤需要能够访问蜂窝网络。

1. 转到 **System（系统）** > **Modem（调制解调器）** > **Cellular network（蜂窝网络）** > **Test cellular connection（测试蜂窝网络连接）**。输入主机名或 IP 地址。
2. 验证连接测试是否成功。

检查管理端口

在打开最终路由模式之前，请验证底座的管理端口。

1. 转到 **Cellular routing（蜂窝路由）** > **Back box management ports（底座管理端口）**。
2. 如果网络不支持默认端口值，请更改端口。

打开转发至摄像机

最后一步是打开转发至摄像机。

1. 转到 Cellular routing（蜂窝路由）> Main mode（主模式），然后单击 Enable forwarding to connected device（启用转发至已连接设备）。

启用转发后，常规服务端口将转发至摄像机，而底座管理功能仍可通过预留管理端口访问。

2. 测试摄像机访问：在网页浏览器中，输入蜂窝网络 IP 地址并附加端口号 80，即 `http://<cellular-ip-address>:80`。
3. 测试底盒访问：在网页浏览器中，输入蜂窝网络 IP 地址并附加端口号 11080（HTTP 默认底盒管理端口），即 `http://<cellular-ip-address>:11080`。

配置摄像机的 IP 所属关系

注意

此步骤为可选步骤，仅在需要更改默认子网行为或调整子网行为时才需要执行。

蜂窝网络仅分配一个 IP 地址，并且该 IP 与 SIM 卡身份绑定。常规安装包括一个底座和一台已连接的摄像机。DHCP 模式决定摄像机“拥有”哪个 IP 地址。这是选择 DHCP 服务器模式时的关键决定。

默认情况下（本地模式），蜂窝网络 IP 保留在底座上，而摄像机会从底座本地网络中分配一个私有 IP。摄像机仍可通过蜂窝网络完全访问。对于大多数部署，这已经足够，并且能够使摄像机安全地隔离在私有网络中。

当工具从摄像机自身视角查看 IP 时，这种差异会显现出来。如果 VMS 读取摄像机上报的 IP 地址，或者摄像机被配置为将其 IP 地址叠加显示在视频画面中，那么该 IP 将是摄像机的私有局域网 IP，而不是外部访问所使用的公共蜂窝网络 IP。这两个地址不一致，因为蜂窝网络 IP 属于底座持有的 SIM 卡身份，而不是摄像机本身。

直通模式通过将蜂窝网络分配给底座的唯一 IP 转发给摄像机来解决此问题。启用“直通”后，摄像机将拥有与蜂窝网络相同的 IP 地址，因此摄像机上报（并在视频叠加中显示）的地址，与远程访问时使用的地址一致。由于摄像机现在持有蜂窝网络身份，此选择还会改变摄像机访问蜂窝网络中其他用户设备 (UE) 的方式。

本节其余部分将详细介绍各模式。

您可以通过蜂窝网络 IP 的标准端口 (`80/443/554/22`) 访问连接到底座的摄像机，同时仍可通过预留管理端口（例如 `11080/11443/11554/11022`）访问底座。

本地模式与直通模式的区别：

本地模式

- 摄像机被分配到一个私有本地子网。
- 摄像机内部 IP 地址与蜂窝网络可访问 IP 地址不同。
- 如果不确定，请使用“Local DHCP mode（本地 DHCP 模式）”选项。

直通模式

- 摄像机被分配蜂窝网络 IP 地址。

本地模式

打开本地模式

1. 在 Cellular routing（蜂窝路由）> Advanced DHCP configuration（高级 DHCP 配置）> DHCP server mode（DHCP 服务器模式）中，选择 Local（本地）。
2. 验证摄像机本地 IP 地址不会与网络中其他可访问 IP 地址冲突：Cellular routing（蜂窝路由）> Advanced DHCP configuration（高级 DHCP 配置）> Local private network configuration（本地私有网络配置）。

3. 如有需要，可在 Cellular routing（蜂窝路由）> Advanced DHCP configuration（高级 DHCP 配置）> Local private network configuration（本地私有网络配置）中更改 IP 地址。Starting IP address（起始 IP 地址）和 Ending IP address（结束 IP 地址）使用相同的值。
4. 单击Save（保存）。

直通模式

如果 UE（用户设备，即摄像机）彼此之间不通信，并且流量始终从另一个 VMS 局域网流向 UE，则不存在用于 IP 伪装的 UE 到 UE 路径。在这种情况下，从 IP 伪装的角度来看，直通模式被认为是安全的。

从宏观来看，这意味着蜂窝网络向摄像机端进行了延伸。当需要让摄像机直接显示在面向蜂窝网络的 IP 地址上时，此功能非常有用。

重要风险：直通模式下的影子 IP

该风险说明适用于单摄像机设置场景。即使只有一台摄像机，直通模式在局域网侧子网中仍需要两个 IP 地址：

- 一个 IP 地址用于摄像机。
- 一个 IP 地址用于以太网侧的底座 DHCP 服务器。

场景 1：每个 UE 分配最小子网（/30）

在此模型中，每个 UE 都拥有一个独立的小型子网。

- 一个（/30）子网可提供两个可用主机 IP 地址。
- 一个 IP 地址供摄像机使用。

剩余的 IP 地址由底座 DHCP 服务器内部使用。

针对场景 1 的建议：

- 保持每个 UE 子网相互隔离。
- 确保每个 UE 子网都是唯一的。 切勿让不同 UE 之间的子网发生重叠。

场景 2：多个 UE 共享较大的子网

某些部署会使用一个较大的子网供多个 UE 共享。如果摄像机尝试访问另一个 UE，而该 UE 使用的 IP 地址恰好与底座 DHCP 服务器的 IP 相同，则会出现“伪装冲突风险”。在这种情况下，网络流量可能会被解析到本地的底座端地址，而不是预期的远程 UE。

针对场景 2 的建议：

- 检查直通设置中的底座 DHCP 服务器 IP 地址。
- 确保此 IP 地址未分配给任何其他 UE。
- 确保此 IP 地址未在网络服务门户中分配给任何 SIM 卡。

打开直通模式

注意

需要访问蜂窝网络。

1. 在 Cellular routing（蜂窝路由）> Advanced DHCP configuration（高级 DHCP 配置）> DHCP server mode（DHCP 服务器模式）中，选择 Passthrough（直通）。
2. 在 Cellular routing（蜂窝路由）> Advanced DHCP configuration（高级 DHCP 配置）> Local private network configuration（本地私有网络配置）> Server IP and prefix length（服务器 IP 和前缀长度）中，确认自动选择的服务器 IP 和子网前缀长度不会与其他可访问 IP 地址冲突。
3. 单击Save（保存）。

设置事件规则

了解更多信息，请参见*开始使用事件规则*。

触发响应

1. 转到 System（**系统**）> Events（**事件**）并单击 + Add a rule（**+ 添加规则**）。该规则可定义设备执行特定响应的时间。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. 选择触发响应时必须满足的**条件**。如果为响应规则指定多个条件，则必须满足条件才能触发响应。
4. 选择满足条件时应执行何种Action（**操作**）。

打开外壳时触发通知

本示例说明如何在设备的护罩或外壳打开时设置电子邮件通知。

添加电子邮件接收者：

1. 转到System（**系统**）> Events（**事件**）> Recipients（**接收者**）并单击Add recipient（**添加接收者**）。
2. 键入接收者的名称。
3. 选择**电子邮件**作为通知类型。
4. 输入收件人的电子邮件地址。
5. 输入您想要摄像机发送通知的电子邮件地址。
6. 提供发送电子邮件帐户的登录信息以及 SMTP 主机名和端口号。
7. 要测试您的电子邮件设置，请单击**测试**。
8. 单击Save（**保存**）。

创建一个规则：

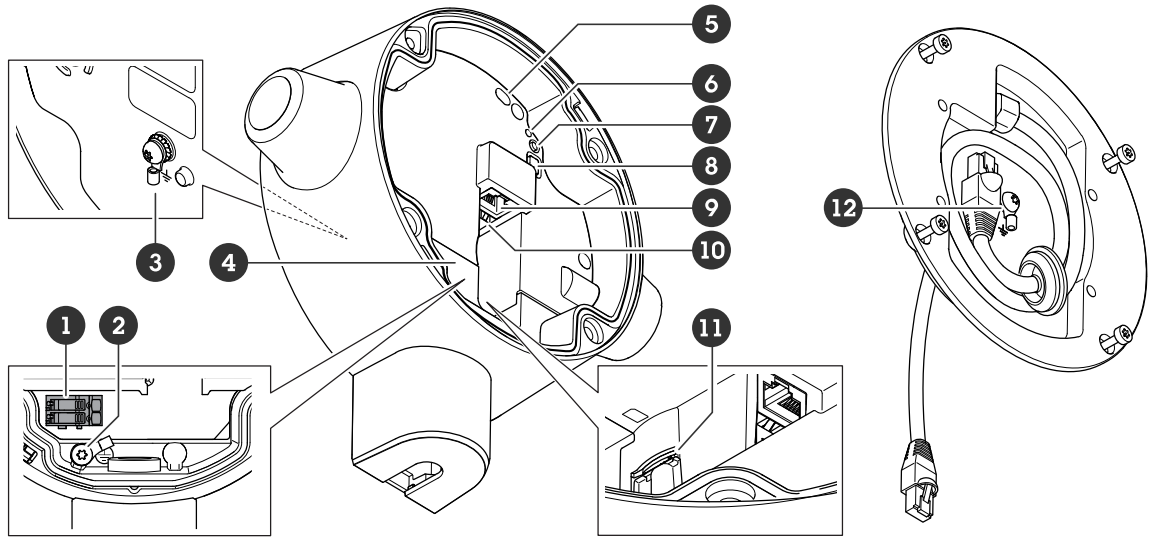
9. 转到**系统** > **事件** > **规则**并单击**添加规则**。
10. 为规则键入一个名称。
11. 在条件列表中，选择**外壳打开**。
12. 在响应列表中，选择**发送电子邮件通知**。
13. 从列表中选择接收者。
14. 输入电子邮件的主题行和消息。
15. 单击Save（**保存**）。

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*。

规格

产品概览



1 交流电源接头
2 保护接地
3 接地螺丝
4 保护罩 (AC)
5 外壳打开侦测器
6 重置按钮
7 状态 LED
8 控制按钮
9 PoE 输出（数据）
10 PoE 输入
11 SIM 卡插槽
12 接地螺丝（摄像机）

LED 指示灯

设置模式下的状态 LED

状态 LED	指示
熄灭	外壳检测红外线 (IR) 被遮挡。
绿色	运行正常，以太网接口已就绪。
琥珀色	在启动期间稳定。在设备软件升级过程中或重置为出厂默认设置时闪烁。
琥珀色/红色	无以太网连接，调制解调器正在启动期间进行配置。
红色	设备软件升级失败。

连接模式下的状态 LED

状态 LED	指示
熄灭	外壳检测红外线 (IR) 被遮挡。
绿色	调制解调器已连接到网络。
琥珀色	在启动期间稳定。在设备软件升级过程中或重置为出厂默认设置时闪烁。

琥珀色/红色	启动过程中正在配置调制解调器。
红色	设备软件升级失败。

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 14*。
- 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

PoE 输入连接器（PoE 输入）

带以太网供电 (PoE) IEEE 802.3af/802.3at/802.3bt Type 3 Class 5 的 RJ45 以太网连接器。

注意

此连接器仅用于电源输入，不提供网络连接。

注意

- PoE IEEE 802.3at Type 2 Class 4 输出需要交流输入电源。
- 对于 PoE IEEE 802.3af Type 1 Class 3 输出，需要 IEEE 802.3at Type 2 Class 4 或更高等级。
- 对于 PoE IEEE 802.3af Type 1 Class 3 输入，设备可正常运行，但不输出电源。

注意

以太网电缆最大长度为 20 m。

网络连接器 (PoE 输出）

RJ45 以太网连接器。

注意

- PoE IEEE 802.3at Type 2 Class 4 输出需要交流输入电源。
- 对于 PoE IEEE 802.3af Type 1 Class 3 输出，需要 IEEE 802.3at Type 2 Class 4 或更高等级。
- 对于 PoE IEEE 802.3af Type 1 Class 3 输入，设备可正常运行，但不输出电源。

注意

以太网电缆最大长度为 20 m。

电源连接器

用于连接交流电源的接线端子。

注意

PoE IEEE 802.3at Type 2 Class 4 输出需要交流输入电源。

清洁您的设备

您可以使用温水和温和的非研磨性肥皂清洁设备。

注意

- 刺激性化学品会损坏设备。请勿使用窗户清洁剂或丙酮等化学品来清洁设备。
- 避免在阳光直射或高温下清洁，因为这可能会导致污渍。

1. 使用罐装压缩空气，将灰尘及散落的灰尘从设备上移除。
2. 如有必要，请使用蘸有温水和温和的非研磨性肥皂的柔软超细纤维布清洁设备。
3. 为去除残留的清洁剂，请用蘸有温水的柔软超细纤维布擦拭设备。
4. 为避免污渍，请用干净的非研磨性布擦干设备。

如需更详细地了解安讯士设备的清洁，请参阅白皮书*常见清洁剂的化学耐受性*。

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。参见 *产品概览, on page 11*。
3. 按住控制按钮15–30秒，直到状态LED指示灯闪烁琥珀色。
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、设置密码和访问设备。
   安装和管理软件工具可在*axis.com/support* 的支持页上获得。

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*。

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。

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 14*。

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。

T10233346_zh

2026-10 (M2.2)

© 2026 Axis Communications AB