

AXIS M5000-G PTZ摄像机

目录

安装	4
预览模式	4
开始使用	5
在网络上查找设备	5
浏览器支持	5
打开设备的网页界面	5
创建管理员帐户	5
安全密码	5
确保没有人篡改过设备软件	6
网页界面概览	6
配置设备	7
基本设置	7
调整图像	7
选择曝光模式	7
在低照度条件下降低噪声	7
降低低光条件下的运动模糊	7
处理具有强背光的场景	8
验证像素分辨率	8
使用隐私遮罩隐藏图像的某些部分	8
将水平转动或垂直转动位置显示为文本叠加	9
调整摄像机视图 (PTZ)	9
限制水平转动、垂直转动和变焦移动	9
创建预置位轮巡	9
查看并录制视频	9
降低带宽和存储	9
查看监视器上的实时视频流	10
设置网络存储	10
设置事件规则	10
触发操作	10
当摄像机侦测到目标时录制视频	10
当设备侦测到目标时，显示视频流中的文本叠加	11
当摄像机侦测到移动时，将摄像机定向到预设位置	11
当摄像机侦测到冲击时录制视频	12
使用 PIR 和音频来防止入侵者	12
音频	13
向录像添加音频	13
设置 Z-Wave®	13
注意事项	13
打开 Z-Wave	13
添加一个 Z-Wave 设备	13
添加包含 SmartStart 的 Z-Wave 设备	14
通过包含/排除模式删除 Z-Wave 设备	14
通过强制流程删除 Z-Wave 设备	14
从 SmartStart 列表中删除 Z-Wave 设备	14
更换 Z-Wave 设备	15
重置 Z-Wave 网络	15
将 Z-Wave 用作 I/O	15
网页界面	16
了解更多	17
取景模式	17
隐私遮罩	17
叠加	18
水平转动、垂直转动和变焦 (PTZ)	18

轮巡	18
无线 I/O (Z-Wave Plus® v2)	18
行业协会	18
命令类别	18
流传输和存储	19
视频压缩格式	19
图像、流和流配置文件设置之间的关系如何?	19
比特率控制	19
分析与应用	21
规格	22
产品概述	22
如何删除球型罩	22
LED 指示灯	22
SD 卡插槽	23
按钮	23
控制按钮	23
连接器	23
网络连接器	23
音频连接器	23
电源连接器	24
清洁您的设备	25
故障排查	26
重置为出厂默认设置	26
AXIS OS 选项	26
检查当前 AXIS OS 版本	26
升级 AXIS OS	27
技术问题和可能的解决方案	27
性能考虑	29
联系支持人员	30
网络安全	31
漏洞管理	31
安全通知	31
安全产品生命周期	31
安全组件验证 (SCV)	31

安装



要观看此视频，请转到本文档的网页版本。

如何安装产品



要观看此视频，请转到本文档的网页版本。

如何安装带天花板支架的产品

预览模式

在安装期间微调摄像机视图时，预览模式对安装者来说是非常理想。无需登录即可在预览模式下访问摄像机视图。它仅在出厂默认状态下提供，可由设备供电在有限时间使用。



要观看此视频，请转到本文档的网页版本。

该视频演示如何使用预览模式。

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 5](#)。

有关搭载 AXIS OS 的设备网页界面中大多数功能和设置的说明，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 5](#)。
3. 重新输入密码。
4. 接受许可证协议。
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 26](#)。

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 26。
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

基本设置

设置电源频率

1. 转到**视频 > 安装 > 电源线频率**。
2. 选择电源频率，然后单击**保存并重启**。

设置方向

1. 转到**视频 > 安装 > 旋转**。
2. 选择 0、90、180 或 270 度。
另请参阅。

调整图像

本部分包括配置设备的说明。如果您想要了解有关特定性能如何工作的更多信息，请转到 [了解更多](#), on page 17。

选择曝光模式

要提高特定监控场景的图像质量，请使用曝光模式。曝光模式让您能够控制光圈、快门速度和增益。转到**视频 > 图像 > 曝光**，然后在以下曝光模式之间进行选择：

- 对于大多数使用情况，请选择**自动曝光**。
- 对于使用某些人造光源（如荧光照明）的环境，请选择**无闪烁**。
选择与电流频率相同的频率。
- 对于使用某些人造光源和明亮光源的环境（例如，在夜间使用荧光照明并在白天使用日光照明的室外环境），请选择**减少闪烁**。
选择与电流频率相同的频率。
- 要锁定当前曝光设置，请选择**保持当前设置**。

在低照度条件下降低噪声

要在低照度条件下降低噪声，您可调整下面的一种或多种设置：

- 调整噪声和运动模糊之间的平衡。转到**视频 > 图像 > 曝光**，将**模糊-噪声平衡**滑块移向**低噪点**。
- 将曝光模式设置为自动。

注意

最大快门值可导致运动模糊。

- 要降低快门速度，请将最大快门设置为可能的最大值。

注意

当您降低最大增益时，图像会变得更暗。

- 将最大增益设置为更低的值。
- 如果有**Aperture（光圈）**滑块，将其移向**Open（打开）**。
- 在**视频 > 图像 > 外观**下，降低图像中的锐度。

降低低光条件下的运动模糊

要在低照度条件下降低运动模糊，可调整下面的一种或多种设置：**视频 > 图像 > 曝光**：

注意

当增益提高时，图像噪点也将增加。

- 将**最大快门**设置为更短的时间，将**最大增益**设置为更高的值。

如果仍存在运动模糊的问题，请执行以下操作：

- 提高场景中的照度等级。
- 安装摄像机，让目标相对于其的移动是正面靠近或远离而非侧面移动。

处理具有强背光的场景

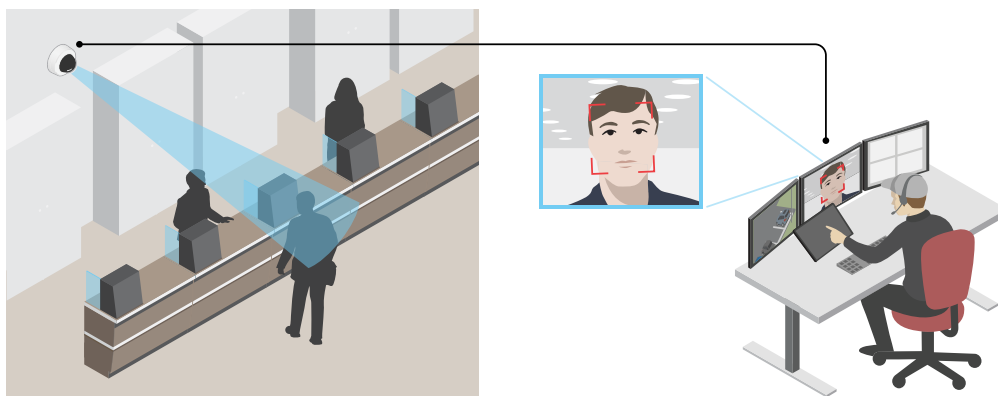
动态范围是图像亮度水平的差异。在某些情况下，黑暗和明亮区域之间的差异可能很明显。结果通常会产生黑暗或明亮区域均可视的图像。宽动态范围 (WDR) 可使图像的明暗区域均可视。

1. 转到**视频 > 图像 > 宽动态范围**。
2. 使用**局部对比度**滑块调整宽动态量。
3. 如果仍有问题，请转到**曝光**并调节**曝光区域**以覆盖关注区域。

可以在 axis.com/solutions/wide-dynamic-range-wdr 上找到更多有关宽动态以及如何使用宽动态的信息。

验证像素分辨率

为了验证图像已定义的部分是否包含足够的像素，例如，为能够识别人脸，您可以使用像素计数器。



1. 转到**Video (视频) > Image (图像)**，然后单击 .
2. 单击  以使用**Pixel counter (像素计数器)**。
3. 在摄像机的实时画面中调整矩形的大小和位置，例如，在人脸可能出现的地方。您可以查看矩形每条边的像素数量，并确定这些值是否满足您的需求。

使用隐私遮罩隐藏图像的某些部分

您可以创建一个或多个隐私遮罩，以隐藏部分图像。

1. 转到**视频 > 隐私遮罩**。
2. 单击 .
3. 单击新遮罩并输入一个名称。
4. 根据您的需求调整隐私遮罩的大小和放置。
5. 要更改隐私遮罩的颜色，单击**隐私遮罩**，然后选择一个颜色。

另请参阅 **隐私遮罩**, on page 17

将水平转动或垂直转动位置显示为文本叠加

您可以将水平转动或垂直转动位置显示为图像中的叠加。

1. 转到**Video (视频) > Overlays (叠加)**，然后单击 。
2. 在文本字段中，键入 #x 以显示水平转动位置。
键入 #y 以显示垂直转动位置。
3. 选择外观、文本大小和对齐方式。
4. 当前的水平转动和垂直转动位置显示在实时视图图像和录制内容中。

调整摄像机视图 (PTZ)

限制水平转动、垂直转动和变焦移动

如果您不希望摄像机到达场景的某些部分，则可限制水平转动、垂直转动和变焦移动。例如，您希望在位于您打算监控的停车场附近的单元建筑中保护派驻人员的隐私。

要限制变焦移动：

1. 转到**PTZ > 限制**。
2. 根据需要设置限制。

创建预置位轮巡

轮巡按预定顺序或随机地显示在可配置的时间段来自不同预置位的视频流。

1. 前往 **PTZ > 轮巡**。
2. 单击  **Guard tour (轮巡)**。
3. 选择**预置位**并单击**创建**。
4. 在**常规设置**下：
 - 键入轮巡的名称，然后指定各轮巡之间的暂停时间长度。
 - 如果希望轮巡随机前往预置位，请打开**随机开始轮巡**。
5. 在**步骤设置**下：
 - 设置预置位的持续时间。
 - 设置移动速度，其控制移至下一个预置位的速度。
6. 前往**预置位**。
 - 6.1. 在您的轮巡中选择您所需的预置位。
 - 6.2. 将其拖到查看顺序区域，然后单击**完成**。
7. 要计划轮巡，前往**系统 > 事件**。

查看并录制视频

本部分包括配置设备的说明。要了解有关流和存储的工作原理的更多信息，请转到 [流传输和存储](#), on page 19。

降低带宽和存储

重要

降低带宽可能导致图像中的细节损失。

1. 转到**视频 > 流**。

2. 在直播视图中单击  A。
3. 如果设备支持**视频格式 AV1**，请选择此格式。否则选择 **H.264**。
4. 转到**视频 > 流 > 常规**并增加**压缩**。
5. 转到**视频 > 流 > Zipstream**并执行以下一个或多个操作：
 - 选择您要使用的 **Zipstream 级别**。
 - 打开**存储优化**。仅当视频管理软件支持 B 帧时，才可使用此选项。
 - 打开**动态 FPS**。
 - 打开**动态 GOP**并设置高 GOP 长度值的**上限**。

查看监视器上的实时视频流

设置网络存储

要在网络上存储录制内容，您需要设置网络存储。

1. 转到**系统 > 存储**。
2. 单击  **添加网络存储**（在**Network storage（网络存储）**下）。
3. 输入主机服务器的 IP 地址。
4. 在**网络共享**下键入主机服务器上共享位置的名称。
5. 键入用户名和密码。
6. 选择 SMB 版本或将其保留在**自动**状态。
7. 如果遇到临时连接问题或尚未配置共享，选中**添加共享而不测试**。
8. 单击**添加**。

设置事件规则

您可以创建规则来使您的设备在特定事件发生时执行某项操作。规则由条件和操作组成。条件可以用来触发操作。例如，设备可以在检测到移动后开始录制或发送电子邮件，或在设备录制时显示叠加文本。

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

- 如果更改规则中所用流配置文件的定义，则您需要重启使用该流配置文件的操作规则。

当摄像机侦测到目标时录制视频

本示例解释了如何设置摄像机，当摄像机侦测到目标时开始录制到 SD 卡。该录制内容将包括侦测前 5 秒到侦测结束后一分钟之间的画面。

在您开始之前：

- 请确保您已安装 SD 卡。

1. 如果应用程序尚未运行，请将其启动。
2. 请确保已根据需要设置了应用程序。

创建一个规则：

1. 转到**系统 > 事件**并添加响应规则。
2. 为规则键入一个名称。
3. 在操作列表中，在**录制**下，选择在**规则处于活动状态时录制视频**。
4. 存储选项列表中，选择 **SD_DISK**。
5. 请选择一个摄像机和一个流配置文件。
6. 将预缓冲时间设置为 5 秒。
7. 将后缓冲时间设置为 1 分钟。
8. 单击 **Save (保存)**。

当设备侦测到目标时，显示视频流中的文本叠加

本示例说明了当设备侦测到目标时，如何显示文本 “Motion detected”。

1. 如果应用程序尚未运行，请将其启动。
2. 请确保已根据需要设置了应用程序。

添加叠加文本：

1. 转到**视频 > 叠加**。
2. 在**Overlays (叠加)**下，选择**Text (文本)**，然后单击 。
3. 在文本字段中，输入 #D。
4. 选择文本大小和外观。
5. 要对文本叠加进行定位，请单击  并选择一个选项。

创建一个规则：

1. 转到**系统 > 事件**并添加响应规则。
2. 为规则键入一个名称。
3. 在操作列表中，在**叠加文本**下，选择**使用叠加文本**。
4. 选择视频通道。
5. 在**文本**中，键入“已侦测到移动动作”。
6. 设置持续时间。
7. 单击 **Save (保存)**。

当摄像机侦测到移动时，将摄像机定向到预设位置

本示例解释了如何设置摄像机，使其在侦测到图像中的运动时转到预置位。

1. 如果应用程序尚未运行，请将其启动。
2. 请确保已根据需要设置了应用程序。

添加预置位：

转到 **PTZ**，然后通过创建预置位来设置摄像机的定向位置。

创建一个规则：

1. 转到**系统 > 事件**并添加响应规则。
2. 为规则键入一个名称。
3. 在操作列表中，选择**转到预置位**。

4. 选择您希望摄像机转到的预置位。
5. 单击“保存”。

当摄像机侦测到冲击时录制视频

冲击侦测允许摄像机侦测由振动或冲击导致的遮挡。环境或目标造成的振动可触发操作，具体取决于冲击灵敏度范围，该范围可设置为0至100。在此场景中，有人在下班后向摄像机投掷石块，您希望获得事件的视频片段。

打开冲击侦测：

1. 转到**系统 > 侦测器 > 冲击侦测**。
2. 开启冲击侦测，并调节冲击的灵敏度。

创建一个规则：

3. 转到**系统 > 事件 > 规则**，然后添加一个规则。
4. 为规则键入一个名称。
5. 在条件列表中，在**设备状态**下，选择**侦测到冲击**。
6. 单击 + 添加第二个条件。
7. 在条件列表中，在**计划和重复**下选择**计划**。
8. 在时间表列表中，选择**下班后**。
9. 在操作列表中，在**录制**下，选择**在规则处于活动状态时录制视频**。
10. 选择保存录制内容的位置。
11. 选择**摄像机**。
12. 将预缓冲时间设置为 5 秒。
13. 将后缓冲时间设置为 50 秒。
14. 单击“保存”。

使用 PIR 和音频来防止入侵者

本示例解释了如何将摄像机设置为在 PIR 传感器侦测到超出办公室时间的移动时，播放狗吠音频剪辑。

在您开始之前：

- 向设备添加狗吠的音频剪辑。有关详细信息，请参见。

创建一个规则：

1. 转到**系统 > 事件**并添加响应规则。
2. 为规则输入一个名称。
3. 在条件列表中，选择**设备状态 > PIR 传感器**。
4. 单击 + 添加第二个条件。
5. 在条件列表中，选择**计划和重复 > 计划**。
6. 在时间表列表中，选择**下班后**。
7. 在操作列表中，选择**音频剪辑 > 播放音频剪辑**。
8. 在剪辑列表中，选择**狗吠**。
9. 单击“保存”。

音频

向录像添加音频

打开音频：

1. 转到**视频 > 流 > 音频**，并包含音频。
2. 如果设备有多个输入源，在**源**中选择正确的源。
3. 转到**音频 > 设备设置**，然后打开正确的输入源。

编辑用于录制的流配置文件：

4. 转到**系统 > 流配置文件**，然后选择流配置文件。
5. 选择**包含音频**，然后将其打开。
6. 单击 **Save (保存)**。

设置 Z-Wave®

有关 Z-Wave 的更多信息，请访问 *无线 I/O (Z-Wave Plus® v2), on page 18*。

注意事项

在使用 Z-Wave Plus v2 的无线 I/O 之前，请考虑以下事项：

- 您要是管理员才能执行 Z-Wave 配置。
- 当对产品网页执行与 Z-Wave 相关的操作时（如添加、删除和替换 Z-Wave 设备或重置 Z-Wave 网络），我们建议您不要在操作过程开始时重新加载页面或将其从其移走。如果完成，操作的实际和显示状态可能会有所不同。要进行恢复，可能需要等待几分钟，然后再次重新加载页面。
- 复制（即，将网络信息复制到另一个控制设备）作为包含过程的一部分执行。
- 本产品忽略基本命令类中的命令。

打开 Z-Wave

1. 转到**系统 > Z-Wave**。
2. 转到 **网关设置无线 I/O**，然后打开 Z-Wave。可能需要等待几分钟后，Z-Wave 才会激活。

添加一个 Z-Wave 设备

尽管不受 Z-Wave Plus v2 协议的限制，但产品的事件系统允许在任意给定时间添加 Z-Wave 设备。如果达到上限数量，您需要先删除一个 Z-Wave 设备，然后才能添加新的。有关 Z-Wave 设备上限数量的信息，请参见产品数据表。

1. 转到**系统 > Z-Wave**。
2. 转到**Device management (设备管理)**，然后单击 **+ Add device (添加设备)**。该产品开始在 Z-Wave 网络中寻找 Z-Wave 设备。
3. 按照其用户手册中所述，将 Z-Wave 设备设置为添加到包含/排除模式。
4. 如果需要，请输入随 Z-Wave 设备提供的 PIN，然后单击**确定**。
5. 等待直到添加过程如网页上的通知所示完成。

现在，设备管理列表中显示已添加的 Z-Wave 设备。

注意

如果找不到 Z-Wave 设备，则添加流程将自动终止。

要查看所添加的 Z-Wave 设备的详细状态信息，请在设备管理列表中展开设备信息。

注意

根据设备类型，所添加的 Z-Wave 设备的状态信息会有所不同。有关详细信息，请参见在线帮助 。

您可以对产品进行设置，以触发具有指定 Z-Wave 触发条件的规则。可用的 Z-Wave 条件和操作根据所添加的 Z-Wave 设备类型而有所不同。

添加包含 SmartStart 的 Z-Wave 设备

您可以将 Z-Wave 设备添加至包含 SmartStart 的 Z-Wave 网络。添加至 SmartStart 列表的 Z-Wave 设备在网络附近通电后 10 分钟内自动添加到设备管理列表中。

1. 转到 **系统 > Z-Wave**。
2. 转到 **SmartStart**，然后单击 **+ Add device information (添加设备信息)**。
3. 键入设备特定密钥和可选信息。
4. 单击 **确定**。

通过包含/排除模式删除 Z-Wave 设备

注意

这是推荐的删除操作。

1. 转到 **系统 > Z-Wave**。
2. 转到 **Device management (设备管理)**，然后单击 。该产品开始在 Z-Wave 网络中寻找 Z-Wave 设备。
3. 按照其用户手册中所述，将要删除的 Z-Wave 设备设置为包含/排除模式。
4. 等待直到删除过程如网页上的通知所示完成。

现已从设备管理列表中删除 Z-Wave 设备。

注意

删除的 Z-Wave 设备中与产品相关的信息都将被删除。

注意

如果找不到 Z-Wave 设备，则删除流程将自动终止。

通过强制流程删除 Z-Wave 设备

可能会出现通信故障，例如，由于电池电量耗尽，因此您可能无法通过将 Z-Wave 设备设置为包含/排除模式来将其删除。您可以强制删除在设备管理列表中显示 **关闭** 状态的 Z-Wave 设备。

1. 转到 **系统 > Z-Wave**。
2. 转到 **设备管理**，然后展开要删除的 Z-Wave 设备的设备信息。
3. 转到 **Node (节点) > Status (状态)**，然后单击 。
4. 等待直到排除过程如网页上的通知所示完成。

现已从设备管理列表中删除 Z-Wave 设备。

注意

删除的 Z-Wave 设备中与产品相关的信息都将被保留。

从 SmartStart 列表中删除 Z-Wave 设备

注意

如果从 SmartStart 列表中删除 Z-Wave 设备，该设备不会从设备管理列表中删除。

1. 转到 **系统 > Z-Wave**。

2. 转到 **SmartStart**。
3. 将鼠标悬停在列表中的设备上以显示垃圾桶图标：。
4. 单击要从SmartStart列表中删除的Z-Wave设备旁边的.

更换 Z-Wave 设备

可能会出现通信故障，例如，由于 Z-Wave 设备故障，您想用另一个设备来替换该设备。您可以强制更换在设备管理列表中显示为关闭状态的 Z-Wave 设备。

1. 转到**系统 > Z-Wave**。
2. 转到**设备管理**，然后展开要更换的 Z-Wave 设备的设备信息。
3. 转到**Node (节点) > Status (状态)**，然后单击。该产品开始在 Z-Wave 网络中寻找 Z-Wave 设备。
4. 设置 Z-Wave 设备，将现有设备替换为其用户手册中所述的包括/排除模式。
5. 等待直到替代过程如网页上的通知所示完成。

新的带某些状态信息的 Z-Wave 设备现在显示在设备管理列表中。

注意

节点 ID 和事件操作信息将传递到新的Z-Wave 设备。其他信息将被删除。

注意

如果找不到 Z-Wave 设备，则更换流程将自动终止。

重置 Z-Wave 网络

重要

- 此过程会删除产品中的 Z-Wave 设备。
- 重置 Z-Wave 网络后，您还需要删除每个 Z-Wave 设备或将其重置为出厂默认设置，然后才能将其再次添加到其他网络。
- 仅当网络主控制器丢失或无法操作时，才使用此程序。

1. 转到**系统 > Z-Wave**。
2. 转到**Device management (设备管理)**，然后单击.
3. 在下拉菜单中选择**重置网络**。

已添加的全部 Z-Wave 设备现在均已从产品中删除，并且设备管理列表为空。

将 Z-Wave 用作 I/O

本产品没有物理 I/O 连接器，但您可在 I/O 界面使用 Z-Wave 功能。

您可以将一个 I/O 端口号分配给高达六个相连的 Z-Wave 设备。要查看端口号，请转到**系统 > 附件 > I/O 端口**。可在 Z-Wave 设备的信息窗口中更改 I/O 端口号。

用作数字输入端口事件时，Z-Wave 设备只能使用一个功能。默认功能取决于设备类型。要更改要使用的功能，请转到设备信息窗口。

有关使用 I/O 端口的详细信息，请参见产品的内置帮助。

网页界面

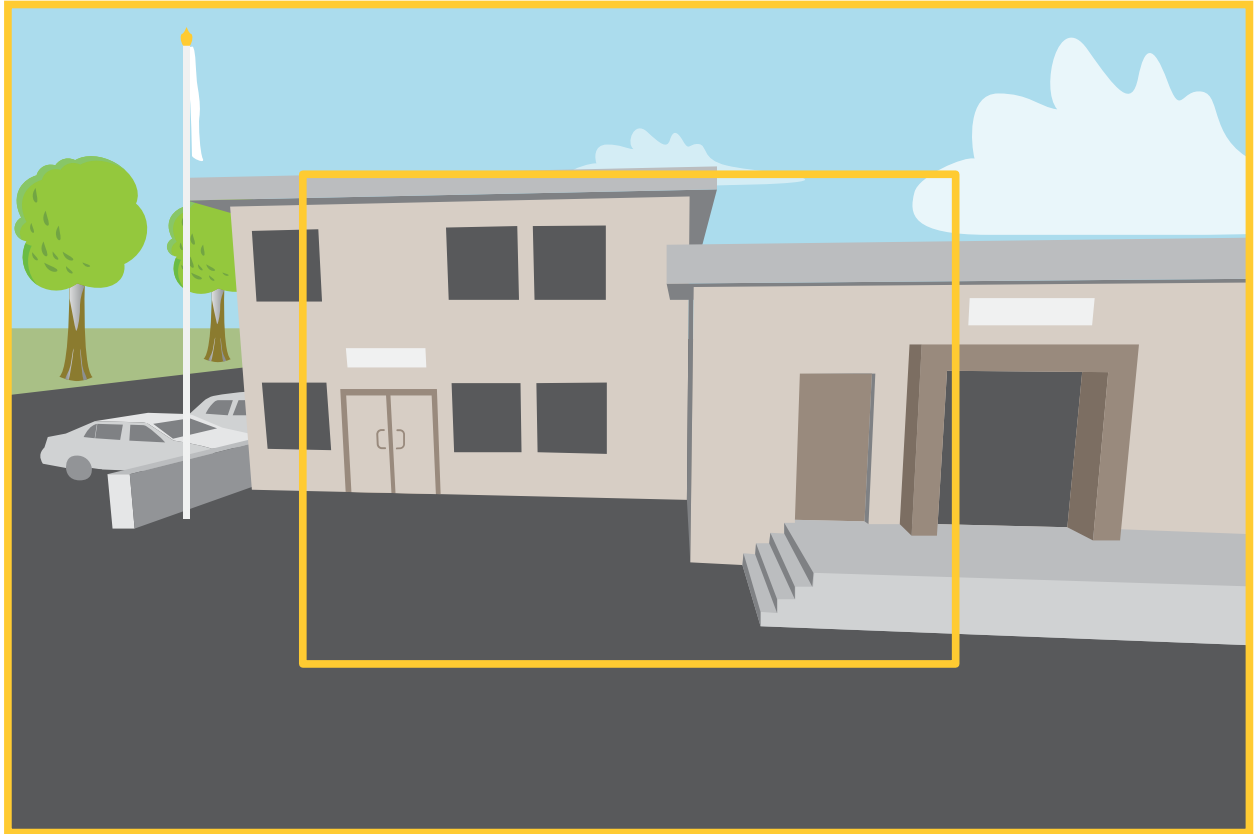
要了解配备 AXIS OS 的设备网页界面中所有可用功能和设置，转到 [AXIS OS 网页界面帮助](#)。

了解更多

取景模式

取景模式是一种预设配置，用于定义摄像机取景的方式。取景模式设置可能会影响摄像机的视野和屏幕纵横比。快门速度也可能会受到影响，这反过来影响到感光性。

较低分辨率的取景模式可根据原始分辨率进行采样，也可从原始分辨率中裁掉，在此情况下，视野可能也会受到影响。



该图像显示了在两种不同的取景模式下，视野和纵横比是如何变化的。

选择何种取景模式取决于特定监控设置的帧速和分辨率要求。有关可用取景模式的规格，请参见 axis.com 的产品数据表。

隐私遮罩

隐私遮罩是用户定义的区域，可防止用户查看监控区域的某个部分。在视频流中，隐私遮罩显示为纯色块。

隐私遮罩是相对于水平转动、垂直转动和变焦坐标的，因此无论摄像机指向何处，隐私遮罩都将覆盖相同的位置或目标。

您将在快照、录制的视频和实时流上看到隐私遮罩。

您可以使用 VAPIX® 应用程序编程接口（API）来隐蔽隐私遮罩。

重要

如果使用多个隐私遮罩，可能会影响产品的性能。

您可以创建多个隐私遮罩。每个遮罩可包含 3–10 个锚点。

叠加

叠加是指叠印在视频流上。叠加用于在录制期间或产品安装和配置期间提供额外信息（如时间戳）。您可以添加文本或图像。

水平转动、垂直转动和变焦（PTZ）

轮巡

轮巡按预定顺序或随机地显示在可配置的时间段来自不同预置位的视频流。一旦开始，轮巡将持续运行，直到您将其停止，即使在没有客户端（Web 浏览器）查看图像时也是如此。

无线 I/O (Z-Wave Plus® v2)

这是一款支持安全的 Z-Wave Plus® v2 产品，可以使用加密的 Z-Wave Plus v2 消息与支持安全的 Z-Wave Plus v2 设备进行通信。该产品可以在任意 Z-Wave® 网络中与其他制造商兼容的 Z-Wave 认证设备一起运行。为了提高网络可靠性，网络中各供应商的非电池供电的 Z-Wave 设备均作为中继器使用。此产品用作控制设备，添加到其中的 Z-Wave 设备用作辅助设备。

行业协会

- 本产品支持一个关联组，组标识符 = 1 (Lifeline)。
- 可添加至关联组的设备数量上限 = 1。
- 组标识符 1 用于发送设备重置本地报告。

命令类别

本产品支持以下命令类别：

- COMMAND_CLASS_APPLICATION_STATUS
- COMMAND_CLASS_ASSOCIATION_V3 (安全)
- COMMAND_CLASS_ASSOCIATION_GRP_INFO_V3 (安全)
- COMMAND_CLASS_CRC_16_ENCAP
- COMMAND_CLASS_DEVICE_RESET_LOCALLY (安全)
- COMMAND_CLASS_FIRMWARE_UPDATE_MD_V5 (安全)
- COMMAND_CLASS_INCLUSION_CONTROLLER
- COMMAND_CLASS_INDICATOR_V3 (安全)
- COMMAND_CLASS_MANUFACTURER_SPECIFIC_V2 (安全)
- COMMAND_CLASS_MULTI_CHANNEL_ASSOCIATION_V4 (安全)
- COMMAND_CLASS_MULTI_CMD
- COMMAND_CLASS_NETWORK_MANAGEMENT_BASIC_V2 (安全)
- COMMAND_CLASS_NETWORK_MANAGEMENT_INCLUSION_V4 (安全)
- COMMAND_CLASS_NETWORK_MANAGEMENT_INSTALLATION_MAINTENANCE_V4 (安全)
- COMMAND_CLASS_NETWORK_MANAGEMENT_PROXY_V4 (安全)
- COMMAND_CLASS_NODE_PROVISIONING (安全)
- COMMAND_CLASS_POWERLEVEL (安全)
- COMMAND_CLASS_SECURITY
- COMMAND_CLASS_SECURITY_2
- COMMAND_CLASS_SUPERVISION

- COMMAND_CLASS_TIME
- COMMAND_CLASS_TRANSPORT_SERVICE_V2
- COMMAND_CLASS_VERSION_V3 (安全)
- COMMAND_CLASS_ZWAVEPLUS_INFO_V2 (安全)

注意

本产品支持 COMMAND_CLASS_INDICATOR_V3，但无可见的指示器。

流传输和存储

视频压缩格式

决定使用何种压缩方式取决于您的查看要求及网络属性。可用选项包括：

Motion JPEG

Motion JPEG 或 MJPEG 是由一系列单张 JPEG 图像组成的数字视频序列。然后将按照足以创建流的速度显示和更新这些图像，从而连续显示更新的运动。为了让浏览者感知运动视频，速度必须至少为每秒 16 个图像帧。每秒 30 (NTSC) 或 25 (PAL) 帧时即可感知完整运动视频。

Motion JPEG 流使用大量带宽，但可以提供出色的图像质量并访问流中包含的每个图像。

H.264 或 MPEG-4 Part 10/AVC

注意

H.264 是一种许可证制技术。Axis 产品包括一个 H.264 查看客户端牌照。禁止安装其他未经许可证的客户端副本。要购买其他许可证，请与您的 Axis 分销商联系。

与 Motion JPEG 格式相比，H.264 可在不影响图像质量的情况下将数字视频文件的大小减少 80% 以上；而与旧的 MPEG 格式相比，可减少多达 50%。这意味着视频文件需要更少的网络带宽和存储空间。或者，从另一个角度来看，在给定的比特率下，能够实现更高的视频质量。

图像、流和流配置文件设置之间的关系如何？

图像选项卡包含影响来自产品的视频流的摄像机设置。如果您在此选项卡中进行了更改，它将影响视频流和录制内容。

流选项卡包含视频流的设置。如果您从产品请求视频流，但未指定示例分辨率或帧率，则可获得这些设置。当您更改**流选项卡**中的设置时，它不会影响正在进行的流，但它将在开始新流时生效。

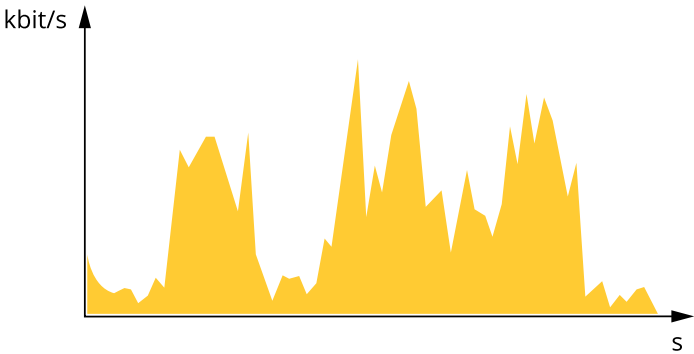
流配置文件设置将重写**流选项卡**中的设置。如果您请求具有特定流配置文件的流，则流包含该配置文件的设置。如果您在未指定流配置文件的情况下请求流，或请求流配置文件在产品中不存在，则流将包含**流选项卡**中的设置。

比特率控制

比特率控制帮助您管理视频流的带宽消耗。

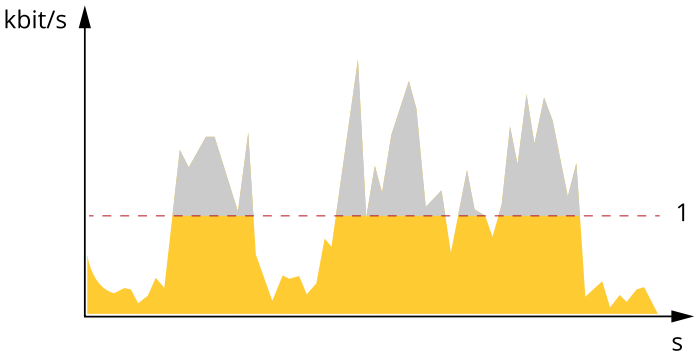
可变比特率 (VBR)

可变比特率允许带宽消耗根据场景中的活动水平而变化。活动越多，需要的带宽就越大。借助可变比特率，您可保证图像质量恒定，但需要确保具有存储容量。



最大比特率 (MBR)

上限比特率让您可设置一个目标比特率，以处理系统中的比特率限制。当即时比特率保持低于指定目标比特率时，您可能会看到图像质量或帧速下降。您可以选择确定图像质量或帧速的优先顺序。我们建议将目标比特率配置为比预期比特率更高的值。这样可在场景中存在高水平的活动时提供边界。

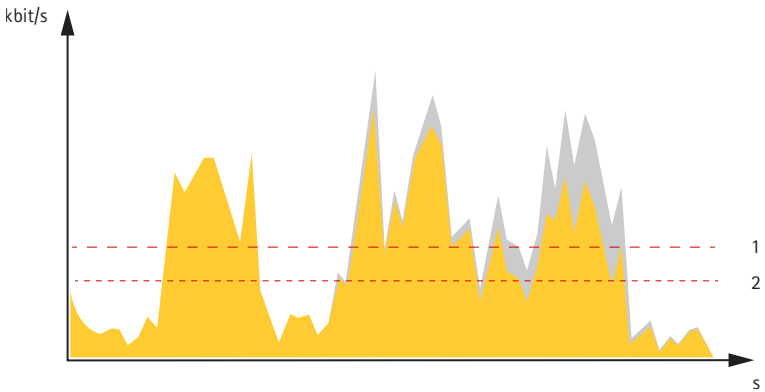


1 目标比特率

平均比特率 (ABR)

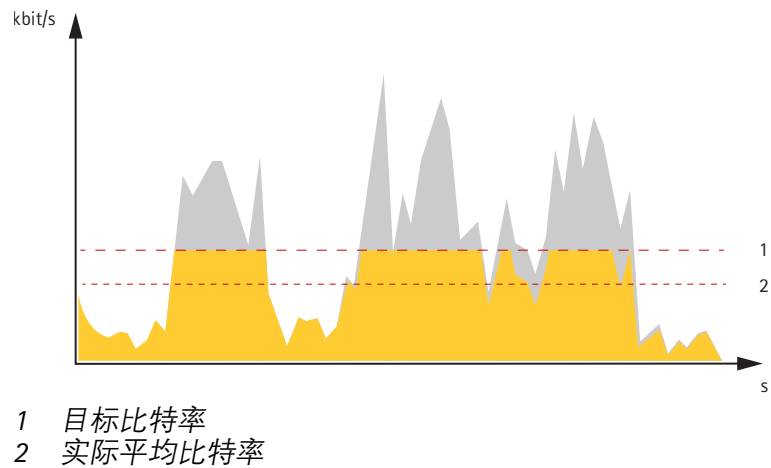
根据平均比特率，比特率可通过更长的时间段自动调整。由此，您就可以满足指定目标，并根据可用存储提供更佳视频质量。与静态场景相比，比特率在具有大量活动的场景中更高。在有大量活动的场景中，如果您使用平均比特率选项，那么您更有可能获得更高的图像质量。当调整图像质量以满足指定的目标比特率时，您可以定义存储视频流所需的总存储量（保留时间）。以下列方式之一指定平均比特率设置：

- 要计算预计存储需求，请设置目标比特率和保留时间。
- 使用目标比特率计算器，根据可用存储和所需的保留时间计算平均比特率。



1 目标比特率
 2 实际平均比特率

您也可打开最大比特率，并在平均比特率选项中指定目标比特率。



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，或收取许可证费。

要查找 Axis 分析与应用的用户手册，请转到 help.axis.com。

注意

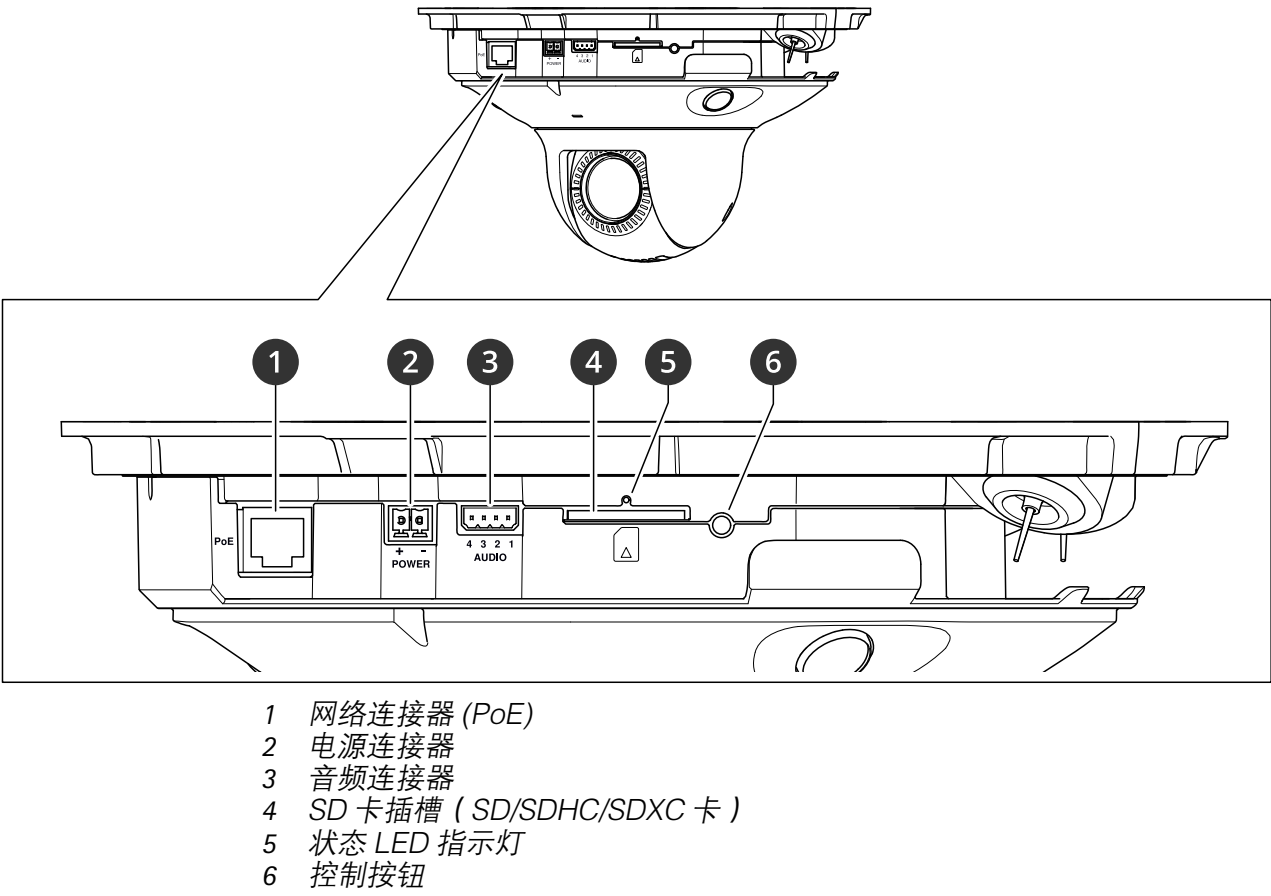
- 可同时运行多个应用，但某些应用可能无法彼此兼容。在并行运行时，某些应用组合可能需要很高的处理能力或很多内存资源。在部署之前验证应用程序能否协同工作。

重要

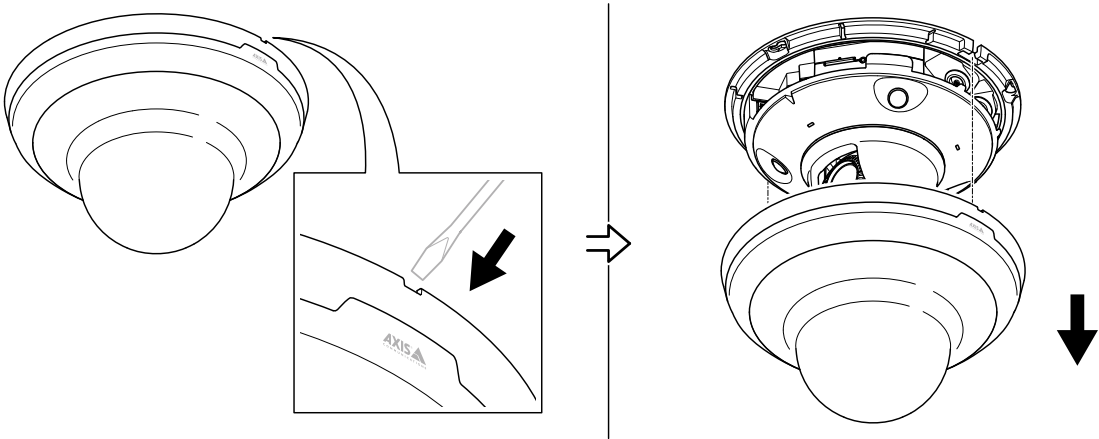
AXIS 3D People Counter 是一款嵌入设备中的应用。我们不建议您在此设备上运行其他应用，因为这会影响 AXIS 3D People Counter 的性能。

规格

产品概述



如何删除球型罩



LED 指示灯

状态LED	指示
熄灭	连接和正常工作。
绿色	启动完成后，将稳定显示绿色 10 秒，以表示正常工作。

淡黄色	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。
橙色/红色	如果网络连接不可用或丢失，则呈橙色/红色闪烁。

无线 LED	指示
熄灭	有线模式。
绿色	常亮表示连接到无线网络。闪烁表示网络活动。
红色	常亮表示没有无线网络连接。扫描无线网络时闪烁。
淡黄色	在无线网络配对时常亮或闪烁。

SD 卡插槽

注意

- 损坏 SD 卡的风险。插入或取出 SD 卡时，请勿使用锋利的工具、金属物体或用力过大。使用手指插入和取出该卡。
- 数据丢失和录制内容损坏的风险。移除 SD 卡之前，请从设备的网页接口上卸载 SD 卡。产品运行时，请勿取出 SD 卡。

本设备支持 SD/SDHC/SDXC 卡。

有关 SD 卡的建议，请参见 axis.com。

 SD、SDHC 和 SDXC 标志均为 SD-3C LLC 的商标。SD、SDHC 和 SDXC 均为 SD-3C LLC 在美国和/或其他国家/地区的商标或注册商标。

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 26。
- 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 (PoE) 的 RJ45 以太网连接器。

音频连接器

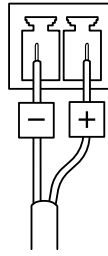
用于音频输入和输出的 4 针脚接线盒。请参见 [产品概述](#), on page 22。

对于音频输入，左声道用于立体声信号。

功能	针脚	注意
接地	1	音频 GND
NC	2	未连接
音频输入	3	音频线路输入
音频输出	4	音频线路输出

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 $\leq 100\text{ W}$ 或额定输出电流限制为 $\leq 5\text{ A}$ 且符合安全超低电压 (SELV) 要求的限制电源 (LPS)



清洁您的设备

您可以用温水清洁设备。

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，请使用软纤维布蘸温水清洁设备。
 3. 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

如果您使用的是 Z-Wave 网络，则要先重置 Z-Wave 网络，然后才能将设备重置为出厂默认设置。请参见 [重置 Z-Wave 网络](#), on page 15。

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。

注意

此摄像机已通过 AXIS License Plate Verifier 预配置。如果恢复至出厂默认设置，您需要重新安装许可证密钥。请参见。

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 22。
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：
 - 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。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 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，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。

您可以使用 AXIS Device Manager 同时升级多个设备。更多信息请访问 axis.com/products/axis-device-manager。

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 26。

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 5。

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，请转到 axis.com/vms。

流传输问题

组播 H.264 仅供本地客户端访问

检查您的路由器是否支持组播，或者是否需要配置客户端和设备之间的路由器设置。您可能需要增大 TTL（生存时间）值。

客户端中未显示组播 H.264

请与网络管理员确认安讯士设备使用的组播地址是否对您的网络有效。

请与网络管理员确认是否存在阻止查看的防火墙。

H.264 图像渲染不佳

请确保您的显卡使用新驱动程序。通常可以从制造商的网站下载新驱动程序。

H.264 和 Motion JPEG 中的色彩饱和度不同

修改图形适配器的设置。有关更多信息，请查看适配器的文档。

帧速低于预期

- 请参见 *性能考虑*, on page 29。
- 减少客户端计算机上运行的应用程序数量。
- 限制同时浏览的人数。
- 请与网络管理员确认是否有足够的可用带宽。
- 降低图像分辨率。
- 登录到设备网页界面并设置优先考虑帧速的取景模式。如果要更改取景模式以优先考虑帧速, 这可能会降低分辨率上限, 具体取决于所使用的设备和可用的取景模式。

无法在实时画面中选择 H.265 编码

网页浏览器不支持 H.265 解码。使用支持 H.265 解码的视频管理系统或应用程序。

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。

性能考虑

当您设置系统时, 考虑不同设置和情况对性能的影响, 这非常重要。一些因素影响带宽 (比特率), 一些因素影响帧速, 还有一些因素同时影响两者。

需要考虑的更重要的因素:

- 图像分辨率较高或压缩级别较低都会导致图像含更多数据, 从而影响带宽。
- 旋转 GUI 中的图像可能增加产品的 CPU 负载。
- 大量 Motion JPEG 客户端或单播 H.264/H.265/AV1 用户访问会影响带宽。
- 使用不同客户端同时查看不同流 (分辨率、压缩) 会同时影响帧速和带宽。尽量使用相同流来保持高帧速。流配置文件可用于确保流是相同的。
- 同时访问不同编解码器的视频流会影响帧速和带宽。为获得理想性能, 请使用编解码器相同的视频流。
- 大量使用事件设置会影响产品的 CPU 负载, 从而影响帧速。
- 使用 HTTPS 可能降低帧速, 尤其是流传输 Motion JPEG 时。

- 由于基础设施差而导致的网络利用率重负会影响带宽。
- 在性能不佳的客户端计算机上进行查看会降低帧速，影响用户体验。
- 同时运行多个 AXIS Camera Application Platform (ACAP) 应用程序可能会影响帧速和整体性能。

联系支持人员

如果您需要更多帮助，请转到 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。您可以在以下链接中查阅有关我们网络安全策略的详细信息和文档：axis.com/about-axis/cybersecurity。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，并配置您的产品以实现安全生命周期和退役。

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，在对我们的设备、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产品存在的漏洞、相应的安全通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。

安全组件验证 (SCV)

您的设备随附一份 SCV 证书，该证书可验证您收到的设备是否正确，并确认该设备自出厂以来未被篡改。该证书由制造商签名，并存储在 iDRAC 中。

收到设备后，请使用 AXIS Recorder Toolbox 验证设备的 SCV 证书。有关 SCV 的更多信息，请访问 dell.com。

T10169100_zh

2026-07 (M18.2)

© 2021 – 2026 Axis Communications AB