AXIS P3719-PLE Network Camera

用户手册

目录

开始使用 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
确保没有人篡改过设备软件 4
创建管理员帐户 4
安全密码 5
网页界面概览 5
安装 6
预览模式 6
配置设备 7
调整图像 7
Optimize IR 照明 7
使用夜间模式，可在低光照条件下的通过红外光受益 7
在低照度条件下降低噪声 7
处理具有强背光的场景 7
监控窄长区域 8
使用隐私遮罩隐藏图像的某些部分 8
显示图像叠加 9
查看并录制视频 9
降低带宽和存储 9
设置网络存储 9
录制并观看视频 10
设置事件规则 10
触发操作 10
当摄像机侦测到物体时录制视频 10
摄像机镜头被遮挡时触发通知 11
当设备侦测到物体时，显示视频流中的文本叠加 11
音频 12
向录像添加音频 12
使用 Portcast 为您的产品添加音频功能 12
网页界面 13
状态 13
视频 15
安装 16
图像 17
流 22
叠加 25
隐私遮罩 27
录像 27
应用 28
系统 29
时间和位置 29
网络 30
安全 33
帐户 38
事件 40
MQTT 44
存储 47
流配置文件 48
ONVIF 49
分析元数据 51
侦测器 52

日志 52
普通配置 53
维护 54
了解更多 55
远程对焦和变焦 55
隐私遮罩 55
叠加 55
流传输和存储 55
视频压缩格式 55
图像、流和流配置文件设置之间的关系如何? 55
比特率控制 56
分析与应用 57
规格 58
产品概述 58
..... 58
LED 指示灯 58
对焦助手的 LED指示灯情况 58
SD 卡插槽 59
按钮 59
控制按钮 59
重启按钮 59
连接器 59
网络连接器 59
故障排查 60
重置为出厂默认设置 60
检查当前 AXIS OS 版本 60
升级 AXIS OS 60
技术问题、线索和解决方案 60
性能考虑 62

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 。

有关在设备的网页界面中控件和选项的说明，请参见 。

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 。
   重置后，安全启动可保证设备的状态。
2. 配置并安装设备。

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 。
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。请参见 。

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。

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

安装



产品的安装视频。

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。



该视频演示如何使用预览模式。

配置设备

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 。

Optimize IR 照明

根据安装环境和摄像机周围的条件（例如场景中的外部光源），有时可以通过手动调整 LED 的强度来提高图像质量。如果您遇到 LED 反射问题，可以尝试降低强度。

1. 前往**视频 > 图像 > 白天–夜间模式**。
2. 打开**允许照明**。
3. 在实时画面中单击 IR，然后选择Manual（手动）。
4. 调节亮度。

使用夜间模式，可在低光照条件下的通过红外光受益

您的摄像机使用可视光在白天提供彩色图像。但随着可见光减弱，彩色图像变得不明亮和清晰。如果在发生这种情况时转换到夜间模式，摄像机将使用可视和近红外光线，以提供明亮和详细的黑白图像。您可将摄像机设置为自转换到夜间模式。

1. 前往**视频 > 图像 > 日夜转换模式**，并确保**红外滤光片**设置为**自动**。
2. 要确定您希望摄像机转换为夜间模式的哪一种光线级别，请将**阈值**滑块移动至**明亮**或**明亮**。
3. 在摄像机为夜间模式时，要使用内置红外光，请打开**允许照明**及**同步照明**。

注意

如果将转换到夜间模式设置为在亮度较亮时，图像将保持更锐利程度，因为弱光噪点更小。如果将转换设置为在较暗时进行，则图像颜色会保持较长的水平，但由于弱光噪点，将会产生更多的图像模糊。

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。

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。



无 WDR 的图像。



有 WDR 的图像。

注意

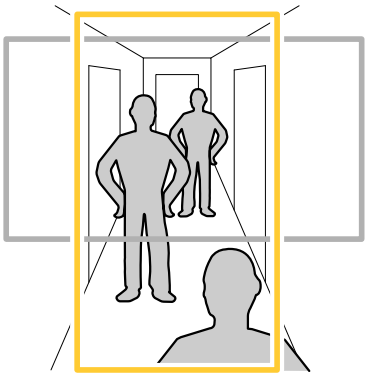
- 宽动态可能会导致图像中出现伪像。
- 宽动态并非适用于全部取景模式。

1. 转到**视频 > 图像 > 宽动态范围**。
2. 打开宽动态。
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/web-articles/wdr* 上找到更多有关宽动态以及如何使用宽动态的信息。

监控窄长区域

使用走廊格式可在窄长的区域（如楼梯、走廊、道路或通路）上更好地利用视野。



1. 根据设备的不同，请在摄像机 90° 或 270° 下转动摄像机或 3 轴镜头。
2. 如果设备没有视图的自动旋转，请转到**视频 > 安装**。
3. 旋转视野 90 ° 或 270° 。

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

显示图像叠加

您可在视频流中将图像添加为叠加。

1. 转到**视频 > 叠加**。
2. 单击**管理图片**。
3. 上传或拖放图片。
4. 单击 Upload（上传）。
5. 从下拉列表中选择**图片**，然后单击 + 。
6. 选择图像和位置。您也可在直播视图中拖动叠加图像以更改位置。

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 。

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 。
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**。

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**。

录制并观看视频

直接从摄像机录制视频

1. 转到**视频 > 流**。
2. 要开始录制，请单击 。

   如果尚未设置存储，请单击 和 。有关如何设置网络存储的说明，请参见
3. 要停止录制，再次单击 。

观看视频

1. 转到**录制**。
2. 在列表中单击 以查看您的录制内容。

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。

若要了解更多信息，请查看我们的指南*事件规则入门*。

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. 选择设备在满足条件时应执行何种**操作**。

注意

如果您对一条处于活动状态的规则进行了更改，则必须重新开启该规则以使更改生效。

当摄像机侦测到物体时录制视频

本示例解释了如何设置摄像机，当摄像机侦测到物体时开始录制到 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）。

摄像机镜头被遮挡时触发通知

本示例说明了如何设置在摄像机镜头被喷涂、覆盖或模糊时的电子邮件通知。

激活篡改侦测：

1. 转到**系统 > 侦测器 > 摄像机篡改**。
2. 为**触发延迟**设置值。该值指示发送电子邮件之前必须经过的时间。
3. 打开**黑暗图像时触发**以检测镜头是否被喷涂、覆盖或严重失焦。

添加电子邮件接受者：

4. 转到**系统 > 事件 > 接受者**，然后添加一个接受者。
5. 键入接受者的名称。
6. 选择 Email（电子邮件）作为通知类型。
7. 输入接收者的电子邮件地址。
8. 输入您想让摄像机发送通知的电子邮件地址。
9. 提供发送电子邮件账户的登录信息以及 SMTP 主机名和端口号。
10. 要测试电子邮件设置，请单击 Test（测试）。
11. 单击 Save（保存）。

创建一个规则：

12. 转到**系统 > 事件 > 规则**，然后添加一个规则。
13. 为规则键入一个名称。
14. 在条件列表中，在**视频**下，选择**篡改**。
15. 在操作列表中，在**通知**下，选择**送电子邮件通知**，然后从列表中选择接受者。
16. 键入电子邮件的主题行和消息。
17. 单击 Save（保存）。

当设备侦测到物体时，显示视频流中的文本叠加

本示例说明了当设备侦测到物体时，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）。

注意

如果您更新叠加文本，它将在视频流上动态自动更新。

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。
4. 如果对输入源进行了更改，单击**应用更改**。

编辑用于录制的流配置文件：

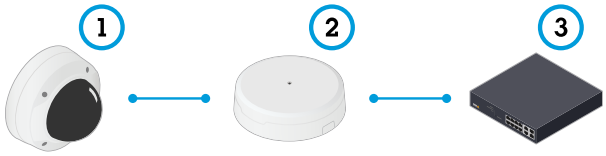
5. 转到**系统 > 流配置文件**，然后选择流配置文件。
6. 选择**包含音频**，然后将其打开。
7. 单击 Save（保存）。

使用 Portcast 为您的产品添加音频功能

借助 portcast 技术，您可以为您的产品添加音频功能。它允许在摄像机和接口之间通过网络电缆对音频和 I/O 通信进行数字传输。

要为您的 Axis 网络视频设备添加音频功能，请在您的设备和供电的 PoE 交换机之间连接兼容 Portcast 的 AXIS 视频设备和 I/O 接口。

1. 连接 Axis 网络视频设备（1）和 Axis Portcast 设备（2）和POE网线。
2. 连接 Axis Portcast 设备（2）和 PoE 交换机（3）和POE网线。



1 Axis 网络视频设备
2 Axis Portcast 设备
3 开关

连接这些设备后，音频选项卡立即显示在您的 Axis 网络视频设备的设置中。前往音频选项卡并打开**允许音频**。

有关详细信息，请参见 Axis Portcast 设备的用户手册。

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。
- **退出**：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。

状态

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安讯士设备理想实践的更多信息。

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。

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。

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。

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。

视频

单击以播放实时视频流。

单击以冻结实时视频流。

单击以对实时视频流进行抓拍。该文件将保存在计算机上的“下载”文件夹中。图像文件名为 [snapshot_YYYY_MM_DD_HH_MM_SS.jpg]。快照的实际大小取决于接收快照的特定网页浏览器引擎应用的压缩，因此，快照大小可能与设备中配置的实际压缩设置不同。

单击以显示 I/O 输出端口。使用开关打开或关闭端口的电路，例如测试外部设备。

单击以手动打开或关闭红外照明。

单击以手动打开或关闭白光。

单击以访问屏幕控制。启用屏幕控制组，确保用户在视频管理软件中右击实时流时可使用各组中的设置。

- **预定义控制**：列出默认的屏幕控制。
- **自定义控制**：单击 **添加自定义控制**，创建自定义屏幕控制。

启动清洗器。当程序开始时，摄像机移动到配置好的位置接受冲洗喷淋。当整个清洗程序完成时，摄像机返回至其原先的位置。此图标仅当清洗器已连接并配置时可见。

启动雨刮器。

单击并选择一个预设位置，以转到直播视图中的预设位置。或者，单击**设置**转到预置位页面。

添加或删除对焦唤醒区域。添加对焦唤醒区域时，摄像机将保存该特定水平转动/垂直转动范围内的对焦设置。如果已设置对焦唤醒区域，当摄像机在实景中进入该区域时，该摄像机将唤醒先前保存的对焦。摄像机覆盖一半区域便足以唤醒对焦。

单击以选择轮巡，然后单击Start（开始）以播放轮巡功能。或者，单击**设置**以转到轮巡功能页面。

单击以在选定的时间段内手动打开加热器。

单击开始实时视频流的连续录制。再次单击可停止录制。如果正在进行录制，它将在重启后自动恢复。

单击以显示为设备配置的存储。要配置存储，您需要以管理员身份登录。

单击以访问自动跟踪设置。若需更多设置，请单击以下图标：**分析 > 自动跟踪**。

单击以访问更多设置：

- **视频格式**：选择实景中所用编码格式。

- **自动播放**：打开以在新会话中打开设备时自动播放静音的视频流。
- **客户端流信息**：打开以显示有关显示实时视频流的浏览器所使用的视频流的动态信息。比特率信息不同于文本叠加中显示的信息，因为有不同的信息源。客户端流信息中的比特率是终末一秒的比特率，它来自设备的编码驱动程序。叠加中的比特率是终末 5 秒的平均比特率，它来自浏览器。这两个值仅覆盖原始视频流，而不是通过 UDP/TCP/HTTP 网络传输时所产生的额外带宽。
- **自适应流**：打开以将图像分辨率调整为查看客户端的实际显示分辨率，以提高用户体验并帮助防止客户端硬件可能超载。仅当您使用浏览器在网页界面中查看实时视频流时，才应用自适应流。当打开自适应流时，帧率上限为 30 fps。如果您在自适应流打开时进行抓拍，它将使用自适应流选择的图像分辨率。
- **水平网格**：单击 显示水平网格。网格可帮助您确定图像是否水平对齐。单击 以隐藏。
- **像素计数器**：单击 显示像素计数器。拖动并调整方框大小以包含关注区域。还可以在**宽度**和**高度**字段中定义方框的像素大小。
- **刷新**：单击 刷新实时浏览中的静态图像。
- **PTZ控制** ：打开以在实时画面中显示 PTZ 控件。

1:1 单击以在全分辨率下显示实时画面。如果全部分辨率超过了屏幕尺寸，请使用较小的图像以在图像中导航。

单击以全屏显示实时视频流。按ESC退出全屏模式。

安装

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。当您更改取景模式时，它可能会影响许多其他设置，例如，视点区域和隐私遮罩。

安装位置 ：图像的方向会根据您按照摄像机的方式而变化。

电源频率：要尽可能减少图像闪烁，选择您所在地区使用的频率。美国地区通常使用 60 Hz。世界上的其余地区大部分使用 50 Hz。如果您无法确定您所在地区的电源频率，请咨询当地机构。

旋转：选择理想的图像方向。

变焦：使用滑块调整缩放级别。

变焦后自动对焦：打开此选项，以在变焦缩放后自动对焦。

对焦：使用滑块手动设置对焦。

自动对焦：单击以让摄像机聚焦于所选区域。如果没有选择自动对焦区域，摄像机将聚焦于整个场景。

自动对焦区域：单击以显示自动对焦区域。此区域应包括关注区域。

重置对焦：单击以使焦点返回其初始位置。

注意

在寒冷环境中，变焦和对焦可能需要几分钟才能可用。

图像

呈现

场景配置文件：选择适合您的监控场景的场景配置文件。场景配置文件可优化特定环境或用途的图像设置，包括颜色级、亮度、锐度、对比度和局部对比度。

- Forensic：适合监控。
- **室内**：适合室内环境。
- **室外**：适合室外环境。
- **鲜明**：适用于演示目的。
- **交通概览**：适用于车辆交通监控。
- **牌照**：适用于捕捉牌照。

饱和度：使用滑块调整色彩浓度。例如，您可以获取一个灰度图像。



对比度：此滑块以调整明暗之间的差别。



亮度：使用滑块调整光线强度。这可使物体更易于查看。在捕捉图像后应用亮度，并不会影响图像的信息。要从黑暗区域获得更多详细信息，通常加大增益或增加曝光时间。



锐度：使用滑块通过调整边缘对比度以使图像中的物体显示得更锐利。如果增加锐度，可能会增加所需的比特率和存储空间量。



宽动态范围功能

WDR：打开以使图像的明暗区域均可视。

局部对比度：使用滑块调整图像对比度。较高的值会使亮度和光线区域之间的对比度更高。

色调映射：使用滑块以调整应用于图像的色调映射量。如果此值设置为零，仅应用标准灰度校正，而提高值将增加图像中更暗和更亮部分的可视性。

白平衡

如果摄像机侦测到接收的光线的色温，则可以调整图像，让颜色显得更自然。如果这还不够，您可从列表中选择合适的光源。

自动白平衡设置可通过逐渐适应变化来降低颜色闪烁的风险。若要更改照明或摄像机首次启动时，可能需要长达 30 秒来适应新光源。如果某个场景中存在多个类型的光源，即，这些光源的色温不同，则主导光源将用作自动白平衡算法的参考。通过选择与要用作参考的光源相匹配的固定白平衡设置，可以覆盖此行为。

光线环境：

- **自动**：自动识别和补偿光源颜色。这是推荐设置，可用于大多数情况。
- **自动 – 室外**：自动识别和补偿光源颜色。这是在多数室外场景下建议使用的设置。
- **自定义 – 室内**：固定颜色调整，用于采用人造光源（荧光照明除外）且具有约 2800 K 良好色温的房间。
- **自定义 – 室外**：固定颜色调整，用于色温约 5500 K 的晴朗天气条件。
- **固定 – 荧光 1**：固定颜色调整，用于色温约 4000 K 的荧光照明。
- **固定 – 荧光 2**：固定颜色调整，用于色温约 3000 K 的荧光照明。
- **固定 – 室内**：固定颜色调整，用于采用人造光源（荧光照明除外）且具有约 2800 K 良好色温的房间。
- **固定 – 室外 1**：固定颜色调整，用于色温约 5500 K 的晴朗天气条件。
- **固定 – 室外 2**：固定颜色调整，用于色温约 6500 K 的多云天气条件。
- **路灯 – 水银**：固定颜色调整，用于街道照明中常用汞蒸汽灯发出的紫外线。
- **路灯 – 钠**：固定颜色调整，用于补偿街道照明中常用钠蒸汽灯发出的黄橙色。
- **保持当前设置**：保持当前设置，切勿补偿光线变化。
- **手动**：借助白色物体固定白平衡。将圆圈拖曳到您想让摄像机显示为白色的实景图像中的物体上。使用**红平衡**和**蓝平衡**滑块以手动调整白平衡。

日间–夜间模式

红外滤光片：

- **自动**：选择自动打开和关闭红外过滤器。当摄像机采用白天模式时，红外滤光片被打开并阻止接收红外光，当摄像机采用夜间模式时，红外滤光片被关闭，摄像机的感光性将提高。

注意

- 某些设备在夜间模式下具有红外穿透滤光片。红外穿透滤光片提高了红外光灵敏度，但阻挡了可见光。
- **打开**：选择打开红外滤光片。图像为彩色，但是降低了感光度。
- **关闭**：选择关闭红外滤光片。图像为黑白图像，以提高感光度。

阈值：使用滑块调整摄像机从白天模式更改为夜间模式的光线阈值。

- 朝**明亮**方向移动滑块来降低红外滤光片的阈值。摄像机将较早更改为夜间模式。
- 朝**黑暗**方向移动滑块来提高红外滤光片的阈值。摄像机将较晚更改为夜间模式。

红外光

如果您的设备没有内置照明，则仅当连接支持的安讯士照明器时，这些控制才可用。

允许照明：打开此项，让摄像机在夜间模式下使用内置光线。

同步照明：打开可自动将照明与周围光线同步。日间/夜间同步仅在红外滤光片设置为**自动**或**关闭**时生效。

自动照明角度：打开以使用自动照明角度。关闭以手动设置照明角度。

照明角度：使用滑块手动设置照明角度，例如，如果角度需要不同于摄像机的视角。如果摄像机具有广阔视角，您可以将照明角度设置为较窄的视野（相当于更大的长焦位置）。这会导致图像有黑暗区域。

IR波长：选择用于红外光线的所需波长。

白光

允许照明：打开以让摄像机在夜间模式下使用白色光。

同步照明：打开可自动将照明与白光同步。

曝光

选择曝光模式以减少图像中迅速变化的不良效应，如不同光源类型产生的闪烁。我们推荐您使用自动曝光模式，或使用与电力网络相同的频率。

曝光模式：

- **自动**：摄像机自动调节光圈、增益和快门。
- **自动光圈**：摄像机自动调节光圈和增益。快门是固定的。
- **自动快门**：摄像机自动调节快门和增益。光圈是固定的。
- **保持当前设置**：锁定当前曝光设置。
- **无闪烁**：摄像机仅使用以下快门速度自动调节光圈，并仅使用以下快门速度：1/50 s (50 Hz) 和 1/60 s (60 Hz)。
- **无闪烁50 Hz**：摄像机自动调节光圈和增益，并使用快门速度 1/50 s。
- **无闪烁60 Hz**：摄像机自动调节光圈和增益，并使用快门速度 1/60 s。
- **减少闪烁**：与无闪烁相同，但摄像机可对较明亮的场景使用快于 1/100 s (50 Hz) 和 1/120 s (60 Hz) 的快门速度。
- **减少闪烁50 Hz**：这与无闪烁相同，但摄像机可对较明亮的场景使用快于 1/100 s 的快门速度。
- **减少闪烁60 Hz**：这与无闪烁相同，但摄像机可对较明亮的场景使用快于 1/120 s 的快门速度。
- **手动**：光圈、增益和快门均固定。

曝光区：使用曝光区域优化场景选定部分的曝光，例如，入口门前面的区域。

注意

曝光区域与原始图像（不旋转）相关，且区域名称将应用于原始图像。这意味着，如果视频流旋转 90° ，那么视频流中的**上方**区域将变为**右**，而**左**变为**下方**。

- **自动**：适用于大多数情况。
- **中心**：使用图像中心的固定区域来计算曝光。该区域在实景中具有固定大小和位置。
- **全屏**：使用整个实景来计算曝光。
- **向上**：使用图像上半部分具有固定大小和位置的区域来计算曝光。
- **向下**：使用图像下半部分具有固定大小和位置的区域来计算曝光。
- **左**：使用图像左半部分具有固定大小和位置的区域来计算曝光。
- **右**：使用图像右半部分具有固定大小和位置的区域来计算曝光。
- **场所**：使用实景中具有固定大小和位置的区域来计算曝光。
- **自定义**：使用实景中的一个区域来计算曝光。您可以调整该区域的大小和位置。

快门上限：选择快门速度以生成优化图像。低快门速度（曝光时间更长）可能导致运动时产生运动模糊，而过高的快门速度则可能影响图像质量。可以配合使用最大快门和最大增益来改善图像。

增益上限：选择合适的最大增益。如果增益上限加大，则会改善黑暗图像中细节的可视级别，但也会提高噪音级别。更多噪声还可能导致使用更多带宽和存储。如果将增益上限设置为较高值，且昼夜光线条件不同时，图像会差异很大。可以配合使用最大增益和最大快门以改善图像。

运动自适应曝光：选择以减少低照度条件下的运动模糊。

模糊–噪声平衡：使用滑块以调节运动模糊与噪声之间的优先级。如果您希望优先考虑低带宽，并以牺牲移动物体的细节来换取噪声降低，请将此参数调节为**低噪音**。如果您希望以牺牲噪声和带宽来优先保留移动物体的细节，请将此参数调节为**低运动模糊**。

注意

您可以通过调节曝光时间或调节增益来更改曝光。如果增加曝光时间，则会产生更多的运动模糊，并且如果增加增益，则会导致更多噪音。如果将**模糊噪声平衡功能**调整为**低噪声**，自动曝光将优先更长的曝光时间而不是增加增益，如果调整的平衡调整为**低运动模糊**，则相反。在低照度条件下，增益和曝光时间终会达到最大值，不论此参数如何设置优先级。

锁定光圈：打开以设置**光圈**滑块来保留光圈大小。关闭以让摄像机自动调整光圈大小。例如，您可以将光圈锁定在始终照亮的场景。

光圈：使用滑块来调整光圈大小，也就是说，镜头的进光量。要允许更多光线进入传感器，从而在低照度条件下生成较亮的图像，请移动滑块至**打开**。打开光圈也会降低景深，这意味着，离摄像机较近或较远的物体可能无法对焦显示。要使更多图像处于聚焦状态，请将滑块向**关闭**移动。

曝光级别：使用滑块调整图像曝光。

除雾：打开以侦测多雾天气的影响，并自动除雾以获得清晰的图像。

注意

我们建议您不要在低对比度、较大光线水平变体或自动对焦稍微熄灭的场景中打开**除雾**。这可能会影响图像质量，例如，在提高对比度时。另外，当除雾功能激活时，太多光量可能对图像质量产生负面影响。

光学器件

Temperature compensation（**温度补偿**）：如果您希望根据光学器件中的温度来纠正对焦位置的调整，请打开。

IR compensation（**红外补偿**）：如果您希望在红外滤光片关闭和有红外线时对焦位置进行校正，请打开。

校准对焦和变焦：单击可将光学器件和变焦和对焦设置重置为出厂默认位置。如果光学器件在运输过程中失去了校准，或者设备已暴露于高振动，则需要执行此操作。

概述

名称：为选定摄像机输入一个名称。

流

概述

分辨率：选择适合监控场景的图像分辨率。更高的分辨率会增加带宽和存储。

帧率：为了避免网络带宽问题或降低存储容量，可将帧速限制为一个固定值。如果将帧速保留为零，则帧速将保持在当前条件下可能的帧速上限。更高的帧速要求更多带宽和存储容量。

P 帧：P 帧是仅显示图像与前一帧的变化的预测图像。输入所需的 P 帧数量。该数量越高，所需带宽越少。但是，如果出现网络拥塞，视频质量可能会明显下降。

压缩：使用滑块调整图像压缩。高压缩导致更低的比特率和更差的图像质量。低级别的压缩可提高图像质量，但在录制时会使用更多带宽和存储。

签名视频：打开以将签名视频功能添加到视频。签名视频通过向视频添加加密签名来保护视频免受篡改。

Zipstream

Zipstream 是一种针对视频监控进行了优化的比特率降低技术，能够实时降低 H.264 或 H.265 流中的平均比特率。Axis Zipstream 在具有多个关注区域的场景（例如，有移动物体的场景）中应用高比特率。当场景更加静态时，Zipstream 使用更低的比特率，从而减少所需存储。要了解更多信息，请参见*以 Axis Zipstream 降低比特率*

选择比特率降低**强度**：

- **关闭**：比特率没有降低。
- **低**：在大部分场景中没有可见的质量降低。这是默认选项，可用于各类型的场景以降低比特率。
- **中**：通过在较低关注度区域内噪声减少且细节水平略低（例如，没有移动）的某些场景中的可视效果。
- **高**：通过在较低关注度区域内噪声减少且细节水平降低（例如，没有移动）的某些场景中的可视效果。我们为使用本地存储的云连接设备和设备推荐此级别。
- **更高**：通过在较低关注度区域内噪声减少且细节水平降低（例如，没有移动）的某些场景中的可视效果。
- **非常高**：在大多数场景中具有可见效果。比特率已针对存储下限进行了优化。

优化存储：打开以在保持质量的同时尽可能降低比特率。优化不应用于网络客户端中显示的流。仅当您的 VMS 支持 B 帧时，才可使用此选项。打开**优化存储**还会打开**动态 GOP**。

动态 FPS（每秒帧数）：打开以允许带宽因场景中的活动级别而异。更多的活动需要更多带宽。

下限：输入一个值，以根据场景运动调整 fps 下限和流默认 fps 之间的帧速。我们建议您在很少运动的场景中使用下限，帧速可降至 1 或更低。

动态图片组 (GOP)（图片组）：打开以根据场景中的活动级别动态调整 I 帧之间的间隔。

上限：输入 GOP 长度上限，即两个 I 帧之间的 P 帧数上限。I 帧是独立的图像帧，不依赖于其他帧。

比特率控制

- **平均**：选择以在更长的时间内自动调整比特率，并根据可用存储提供理想图像质量。
  - 单击以根据可用存储空间、保留时间和比特率限制计算目标比。
  - **目标比特率**：输入所需的目标比特率。
  - **保留时间**：输入录制内容的保留天数。
  - **存储**：显示可用于流的预计存储空间。
  - **比特率上限**：打开以设置比特率限制。
  - **比特率限制**：键入一个高于目标比特率的比特率限制。
- **上限**：选择以根据您的网络带宽设置流的即时比特率上限。
  - **上限**：输入比特率上限。
- **可变**：选择以允许比特率根据场景中的活动级别而变化。更多的活动需要更多带宽。我们建议在大多数情况下选择此选项。

方向

镜像：打开以镜像图像。

叠加

：单击以添加叠加。从下拉列表中选择叠加类型：

- **文本**：选择以显示集成在实时浏览图像中且在各视图、录制和快照中可见的文本。您可以输入自己的文本，也可以包括预先配置的调节器，以自动显示示例时间、日期及帧速。
  - ：单击以添加日期显示符 %F，显示年-月-日。
  - ：单击以添加时间调节器 %X，显示时:分:秒（24 小时制）。
  - **调节器**：单击以选择列表中显示的任一调节器，以将其添加到文本框中。例如，%a 显示星期几。
  - **尺寸**：选择所需字体大小。
  - **呈现**：选择文本颜色和背景色，如白色文本加黑色背景（默认）。
  - ：选择叠加在图像中的位置，或单击并拖动叠加，使其在实时画面中四处移动。
- **图像**：选择以显示通过视频流叠加的静态图像。您可以使用 bmp、.png、jpeg 或 svg 文件。
  要上载图片，请单击**管理图片**。在上载图像之前，您可以选择：
  - **使用分辨率缩放**：选择自动缩放叠加图像以适合视频分辨率。
  - **使用透明色**：选择并输入该颜色的 RGB 十六进制值。使用 RRGGBB 格式。十六进制值的示例：FFFFFF 表示白色，000000 表示黑色，FF0000 表示红色，6633FF 表示蓝色，669900 表示绿色。仅适用于 .bmp 图像。
- **场景填充**：选择以在视频流中显示叠加在同一位置的文本，即使摄像机向另一个方向平移或倾斜也是如此。您可以选择仅在特定缩放级别内显示叠加层。
  - ：单击以添加日期显示符 %F，显示年-月-日。
  - ：单击以添加时间调节器 %X，显示时:分:秒（24 小时制）。
  - **调节器**：单击以选择列表中显示的任一调节器，以将其添加到文本框中。例如，%a 显示星期几。
  - **尺寸**：选择所需字体大小。
  - **呈现**：选择文本颜色和背景色，如白色文本加黑色背景（默认）。
  - ：选择叠加在图像中的位置，或单击并拖动叠加，使其在实时画面中四处移动。叠加将被保存并保留在该位置的平移和倾斜坐标中。
  - **变焦级别 (%) 之间的注释**：设置叠加层显示的缩放级别。
  - **注释符号**：选择当摄像机不在设置的缩放级别内时显示的符号而不是叠加层。
- **流传输指示器**：选择以显示通过视频流叠加的动画。动画显示视频流是实时的，即使场景中没有移动。
  - **呈现**：选择动画的颜色和背景色，如红色文本加透明背景（默认）。
  - **尺寸**：选择所需字体大小。
  - ：选择叠加在图像中的位置，或单击并拖动叠加，使其在实时画面中四处移动。
- **小部件：折线图**：显示一个图表，显示测量值如何随时间变化。
  - **标题**：输入小部件的标题。

- **叠加调节器**：选择叠加调节器作为数据源。如果您创建了 MQTT 叠加，它们将位于列表的末尾。
- ：选择叠加在图像中的位置，或单击并拖动叠加，使其在实时画面中四处移动。
- **尺寸**：选择叠加的大小。
- **在各频道上可见**：关闭以仅在您当前选择的频道上显示。打开以在各活动频道上显示。
- **更新间隔**：选择数据更新之间的时间。
- **透明度**：设置整个叠加的透明度。
- **背景透明度**：仅设置叠加层背景的透明度。
- **点**：启用以在数据更新时向图表线条添加点。
- X axis
  - **标签**：输入 x 轴的文本标签。
  - **时间窗口**：输入数据可视化的时间。
  - **时间单位**：输入 x 轴的时间单位。
- Y axis
  - **标签**：输入 y 轴的文本标签。
  - **动态缩放**：开启以便缩放会自动适应数据值。关闭以手动输入固定比例的值。
  - **低警报阈值**和**高警报阈值**：这些值将为图表添加水平参考线，以便更容易看到数据值何时变得过高或过低。

- **小部件：计量器** ：显示近期测量的数据值的条形图。
  - **标题**：输入小部件的标题。
  - **叠加调节器**：选择叠加调节器作为数据源。如果您创建了 MQTT 叠加，它们将位于列表的末尾。
  - ：选择叠加在图像中的位置，或单击并拖动叠加，使其在实时画面中四处移动。
  - **尺寸**：选择叠加的大小。
  - **在各频道上可见**：关闭以仅在您当前选择的频道上显示。打开以在各活动频道上显示。
  - **更新间隔**：选择数据更新之间的时间。
  - **透明度**：设置整个叠加的透明度。
  - **背景透明度**：仅设置叠加层背景的透明度。
  - **点**：启用以在数据更新时向图表线条添加点。
  - Y axis
    - **标签**：输入 y 轴的文本标签。
    - **动态缩放**：开启以便缩放会自动适应数据值。关闭以手动输入固定比例的值。
    - **低警报阈值**和**高警报阈值**：这些值将为条形图添加水平参考线，以便更容易看到数据值何时变得过高或过低。

隐私遮罩

：单击以创建新的隐私遮罩。

Privacy masks x/32（**隐私遮罩** x/32）：单击此标题栏可更改**全部**隐私遮罩的颜色，或永久删除**全部**隐私遮罩。

单元格大小： 如果选择马赛克颜色，隐私遮罩将显示为像素化模式。使用滑块可更改像素的大小。

Mask x（**遮罩** x）：单击单个遮罩名称/编号可重命名、禁用或永久删除该遮罩。

Use zoom level（**使用变焦级别**）：打开此项可使隐私遮罩仅在达到创建时的变焦级别时显示。缩小图像会再次隐藏遮罩。

录像

单击以过滤录制内容。

从：显示在某个时间点之后完成的录制内容。

到：显示在某个时间点之前的录制内容。

来源：显示基于源的录制内容。源是指传感器。

事件：显示基于事件的录制内容。

存储：显示基于存储类型的录制内容。

正在进行的录制内容：显示设备上全部正在进行的录制。

开始在设备上进行录制。

选择要保存到哪个存储设备。

停止在设备上进行录制。

触发的录制将在手动停止或设备关闭时结束。

连续录制将继续，直到手动停止。即使设备关闭，录制也会在设备再次启动时继续。

播放录制内容。

停止播放录制内容。

显示或隐藏有关录制内容的信息和选项。

设置导出范围：如果只想导出部分录制内容，输时间跨度。请注意，如果您工作的时区与设备所在地的时区不同，时间跨度将基于设备所在的时区。

加密：选择此选项可为导出的录制文件设置密码。如果没有密码，将无法打开导出的文件。

单击以删除一个录制内容。

导出：导出全部或部分录制文件。

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。

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。某些应用程序没有任何设置。

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。
  - **受信任的 NTS KE CA 证书**：选择用于安全 NTS KE 时间同步的受信任 CA 证书，或选择不使用任何证书。
  - **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**：为您的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唯一的。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长。

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。转到**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。设备允许端口 80 或范围 1024–65535 中的端口。如果您以管理员身份登录，则您还可以输入 1–1023 范围内的端口。如果您使用此范围内的端口，您将收到警告。

HTTPS 端口：输入要使用的 HTTPS 端口。设备允许端口 443 或范围 1024–65535 中的端口。如果您以管理员身份登录，则您还可以输入 1–1023 范围内的端口。如果您使用此范围内的端口，您将收到警告。

证书：选择要为设备启用 HTTPS 的证书。

网络发现协议

Bonjour®：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。若要解决 PoE 电源协商问题，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：

- **One–click（一键）**：这是默认选项。按下设备上的控制按钮，即可连接到 O3C。根据设备型号的不同，按下并松开或按住不放，直到状态 LED 指示灯闪烁。在 24 小时内向 O3C 服务注册设备，启用 **Always（总是）**选项并保持连接。如果不注册，设备将断开与 O3C 的连接。
- **总是**：设备将不断尝试通过互联网连接到 O3C 服务。一旦注册设备，就会保持连接。如果无法够到控制按钮，则使用此选项。
- **No（否）**：断开 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。
    - **建立连接**：链接自下而上发生变更时，发送陷阱消息。
    - **断开连接**：链接自上而下发生变更时，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” 帐户密码**：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。

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。分步指南打开。

- **更多** ：显示更多要填充或选择的栏。
- **安全密钥库**：选择使用**可信执行环境 (SoC TEE)**、**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/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：

- **可信执行环境 (SoC TEE)**：选择使用 SoC TEE 来实现安全密钥库。
- **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 802.1x

IEEE 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 MACsec

IEEE 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

防火墙：开启以启用防火墙。

默认策略：选择希望防火墙如何处理规则未涵盖的连接请求。

- ACCEPT（**接受**）：允许与设备的所有连接。默认情况下设置此选项。
- DROP（**丢弃**）：阻止与设备的所有连接。

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

+ New rule（**+ 新规则**）：单击以创建规则。

Rule type（**规则类型**）：

- FILTER（**过滤**）：选择允许或阻止来自与规则中定义标准相符的设备的连接。
  - **策略**：为防火墙规则选择 Accept（**接受**）或 Drop（**丢弃**）。
  - IP range（IP **范围**）：选择以指定允许或阻止的地址范围。在 Start（**开始**）和 End（**结束**）中使用 IPv4/IPv6。
  - IP **地址**：输入要允许或阻止的地址。使用 IPv4/IPv6 或 CIDR 格式
  - **协议**：选择要允许或阻止的网络协议（TCP、UDP 或两者都是）。如果选择协议，还必须指定端口。
  - MAC: 输入要允许或阻止的设备的 MAC 地址。
  - Port range（**端口范围**）：选择以指定允许或阻止的端口范围。将它们添加到Start（**开始**）和 End（**结束**）中。
  - **端口**：输入要允许或阻止访问的端口号。端口号必须介于 1 和 65535 之间。
  - Traffic type（**流量类型**）：选择要允许或阻止的流量类型。
    - UNICAST（**单播**）：从一个发送方发送到一个接收方的流量。
    - BROADCAST（**广播**）：从一个发送方发送到网络上所有设备的流量。
    - MULTICAST（**组播**）：从一个或多个发送方发送到一个或多个接收方的流量。
- LIMIT（**限制**）: 选择接受来自符合规则中定义标准的设备的连接，但应用限制以减少过多流量。
  - IP range（IP **范围**）：选择以指定允许或阻止的地址范围。在 Start（**开始**）和 End（**结束**）中使用 IPv4/IPv6。
  - IP **地址**：输入要允许或阻止的地址。使用 IPv4/IPv6 或 CIDR 格式
  - **协议**：选择要允许或阻止的网络协议（TCP、UDP 或两者都是）。如果选择协议，还必须指定端口。
  - MAC: 输入要允许或阻止的设备的 MAC 地址。
  - Port range（**端口范围**）：选择以指定允许或阻止的端口范围。将它们添加到Start（**开始**）和 End（**结束**）中。
  - **端口**：输入要允许或阻止访问的端口号。端口号必须介于 1 和 65535 之间。
  - Unit（**单位**）：选择允许或阻止的连接类型。
  - Period（**时段**）：选择与 Amount（**数量**）相关的时间段。
  - Amount（**数量**）：设置设备在设定 Period（**时段**）内的最大允许连接次数。最大数量为 65535。
  - Burst（**突发**）：在设定 Period（**时段**）内，输入允许超过设定 Amount（**数量**）一次的连接次数。一旦达到这个数字，就只允许在设定时段内的设定数量。
  - Traffic type（**流量类型**）：选择要允许或阻止的流量类型。
    - UNICAST（**单播**）：从一个发送方发送到一个接收方的流量。
    - BROADCAST（**广播**）：从一个发送方发送到网络上所有设备的流量。
    - MULTICAST（**组播**）：从一个或多个发送方发送到一个或多个接收方的流量。

Test rules（**测试规则**）：单击以测试已定义的规则。

- Test time in seconds（**测试时间（秒）**）：设置测试规则的时间限制。
- **还原**：在测试规则之前，单击可将防火墙回滚到之前的状态。
- Apply rules（**应用规则**）：单击此选项，可激活规则，而不执行测试。我们不建议您这样做。

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。只有安讯士可以创建自定义签名 AXIS OS 证书，因为安讯士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。

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**：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帐户**权限。

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。

匿名访问

允许匿名浏览：打开以允许其他人以查看者的身份访问设备，而无需登录帐户。

允许匿名PTZ操作：打开允许匿名用户平移、倾斜和缩放图像。

SSH 帐户

添加SSH帐户：单击以添加新 SSH 帐户。

- **启用 SSH**：打开以使用 SSH 服务。

帐户：输入唯一的帐户名。

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证。

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 个接受者。

添加接受者：单击以添加接受者。

名称：为接受者输入一个名称。

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。虽然安讯士设备同时支持 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。有关如何配置带安讯士设备的 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。虽然安讯士设备同时支持 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。有关如何配置带安讯士设备的 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 帐户**：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：

查看接受者：单击可查看各收件人详细信息。

复制接受者：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。

删除接受者：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。

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。安讯士设备软件中的 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、客户端和中间件。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。

您可以在 *AXIS OS Knowledge Base* 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。这用于在使用其他协议（如 HTTP）的同一个端口上启用 MQTT 流量。在某些情况下，可能没有为 MQTT 通信打开专用端口。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。

- 1883 是 **TCP 的 MQTT** 的默认值
- 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 代理供应商提供的 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。客户端连接到服务器时，客户端标识符发送给服务器。

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证。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。

MQTT 叠加

注意

在添加 MQTT 叠加调节器之前，请连接到 MQTT 代理。

添加叠加调节器：单击以添加新的叠加调节器。

主题过滤器：添加包含要在叠加中显示的数据的 MQTT 主题。

数据字段：为要在叠加中显示的消息有效负载指定密钥，默认消息为 JSON 格式。

调节器：当您创建叠加时，请使用结果调节器。

- 以 **#XMP** 开头的调节器显示从主题接收到的数据。
- 以 **#XMD** 开头的调节器显示数据字段中指定的数据。

存储

网络存储

忽略：打开以忽略网络存储。

添加网络存储：单击以添加网络共享，以便保存记录。

- **地址**：键入主机服务器的 IP 地址或主机名称，通常为 NAS（网络连接存储）。我们建议您将主机配置为使用固定 IP 地址（非 DHCP，因为动态 IP 地址可能会更改），或者使用 DNS。不支持 Windows SMB/CIFS 名称。
- **网络共享**：在主机服务器上键入共享位置的名称。因为每台安讯士设备都有自己的文件夹，因此，多个设备可以使用同一个共享网络。
- **用户**：如果服务器需要登录，请输入用户名。要登录到特定域服务器，请键入 `DOMAIN\username`。
- **密码**：如果服务器需要登录，请输入密码。
- **SMB 版本**：选择 SMB 存储协议版本以连接到 NAS。如果您选择**自动**，设备将尝试协商其中一个安全版本 SMB：3.02, 3.0, 或 2.1.选择 1.0 或 2.0 以连接到不支持更高版本的较早的 NAS。您可以*在此*了解安讯士设备中有关 SMB 支持的更多信息。
- **添加共享而不测试**：即使在连接测试中发现错误，也选择添加网络共享。例如，错误可能是即便服务器需要密码，而您没有输入密码。

删除网络存储：单击以卸载、取消绑定及删除与网络共享的连接。这将删除网络共享的设置。

取消绑定：单击以取消绑定并断开网络共享。
Bind（绑定）：单击以绑定并连接网络共享。

卸载：单击此处卸载网络共享。
Mount（安装）：单击以安装网络共享。

写保护：打开停止写入到网络共享并防止录制内容被移除。无法格式化写保护的网络共享。

保留时间：选择保留录音的时间、限制旧录音的数量，或遵守有关数据存储的法规。如果网络存储已满，则会在选定时间段过去之前删除旧录音。

工具

- **测试连接**：测试网络共享的连接。
- **格式化**：格式化网络共享，例如，需要快速擦除数据时。CIFS 是可用的文件系统选项。

使用工具：单击以激活选定的工具。

车载存储

重要

数据丢失和录制内容损坏的风险。设备正在运行时，请勿取出 SD 卡。在删除 SD 卡之前将其卸载。

卸载：单击以安全删除 SD 卡。

写保护：打开停止写入到 SD 卡并防止录制内容被移除。您无法格式化写保护 SD 卡。

自动格式化：打开以自动格式化新插入的 SD 卡。它将文件系统格式化为 ext4。

忽略：打开以停止在 SD 卡上存储录音。当您忽略 SD 卡时，设备不再识别卡的存在。该设置仅适用于管理员。

保留时间：选择保留录像的时间、限制旧录像的数量，或遵守相关数据存储法规。当SD卡满时，它会在旧录像的保留时间未到期之前将其删除。

工具

- **检查**：检查 SD 卡上是否存在错误。
- **修复**：修复文件系统中的错误。
- **格式化**：格式化SD卡，更改文件系统并擦除所有数据。您只能将SD卡格式化为ext4文件系统。需要使用第三方ext4驱动程序或应用程序以从Windows®访问文件系统。
- **加密**：使用此工具格式化 SD 卡并启用加密。这会擦除SD卡上存储的数据。存储在SD卡上的新数据都将被加密。
- **解密**：使用此工具在不加密的情况下格式化 SD 卡。这会擦除SD卡上存储的数据。存储在SD卡上的新数据都不会被加密。
- **更改密码**：更改加密 SD 卡所需的密码。

使用工具：单击以激活选定的工具。

损耗触发器：设置要触发操作的 SD 卡损耗水平的值。损耗级别范围为 0–200%。从未使用过的新 SD 卡的损耗级别为 0%。100% 的损耗级别表示 SD 卡接近其预期寿命。当损耗达到 200% 时，SD 卡性能不良的风险很高。我们建议将损耗触发器设置在 80–90% 之间。这为您提供了下载录制内容以及在可能损耗之前替换 SD 卡的时间。使用损耗触发器，您可以设置事件并在磨损级别达到设置值时获得通知。

流配置文件

流配置文件是一组影响视频流的设置。您可以在不同情况下使用流配置文件，例如，在您创建事件和使用规则进行记录时。

添加流配置文件：单击以创建新的流配置文件。

预览：带有您选择的流配置文件设置的视频流的预览。更改页面上的设置时，预览会更新。如果您的设备具有不同的视图区域，则您可在图像左下角的下拉框中更改视图区域。

名称：为您的配置文件添加一个名称。

描述：添加您的配置文件的描述。

视频编解码器：选择应适用于配置文件的视频编解码器。

分辨率：有关该设置的说明，请参见。

帧率：有关该设置的说明，请参见。

压缩：有关该设置的说明，请参见。

Zipstream：有关该设置的说明，请参见。

优化存储：有关该设置的说明，请参见。

动态FPS：有关该设置的说明，请参见。

动态GOP：有关该设置的说明，请参见。

镜像：有关该设置的说明，请参见。

GOP长度：有关该设置的说明，请参见。

比特率控制：有关该设置的说明，请参见。

包括叠加：选择要包含的叠加类型。有关如何添加叠加的信息，请参见 。

包含音频：有关该设置的说明，请参见。

ONVIF

ONVIF 帐户

ONVIF（Open Network Video Interface Forum）是一个全球的接口标准，终端用户、集成商、顾问和制造商可通过此接口轻松利用网络视频技术带来的可能性。ONVIF 可实现不同供应商产品之间的互操作性，提高灵活性，降低成本以及提供面向未来的系统。

创建 ONVIF 帐户，即可自动启用 ONVIF 通信。使用该帐户名和密码用于与设备的全部 ONVIF 通信。有关详细信息，请参见 *axis.com* 上的 Axis 开发者社区。

添加帐户：单击以添加新 ONVIF 帐户。

帐户：输入唯一的帐户名。

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。

角色：

- **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。
  - 添加应用。
- **媒体帐户**：仅允许访问视频流。

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。

ONVIF 媒体配置文件

ONVIF 媒体配置文件包括一组您可用于更改媒体流设置的配置。您可以使用自己的配置创建新的配置文件，也可以使用预配置的配置文件进行快速设置。

添加媒体配置文件：单击以添加新的 ONVIF 媒体配置文件。

配置文件名称：为媒体配置文件添加一个名称。

视频源：选择适合您的配置的视频源。

- **选择配置**：从列表中选择一个用户定义的配置。下拉列表中的配置对应于设备的视频通道，包括多视图、视点区域和虚拟通道。

视频编码器：选择适合您的配置的视频编码格式。

- **选择配置**：从列表中选择一个用户定义的配置并调整编码设置。下拉列表中的配置作为视频编码器配置的标识符/名称。选择用户 0 到 15 以应用您自己的设置，或者如果您想要对特定编码格式使用预定义设置，请选择一个默认用户。

注意

在设备中启用音频，以获得选择音频源和音频编码器配置的选项。

音频源：选择适合您的配置的音频输入源。

- **选择配置**：从列表中选择一个用户定义的配置并调整音频设置。下拉列表中的配置对应于设备的音频输入。如果设备只有一个音频输入，则为用户 0。如果设备有多个音频输入，则列表中将会有其他用户。

音频编码器：选择适合您的配置的音频编码格式。

- **选择配置**：从列表中选择一个用户定义的配置并调整音频编码设置。下拉列表中的配置作为音频编码器配置的标识符/名称。

音频解码器：选择适合您的配置的音频解码格式。

- **选择配置**：从列表中选择一个用户定义的配置并调整设置。下拉列表中的配置作为配置的标识符/名称。

音频输出：选择适合您的配置的音频输出格式。

- **选择配置**：从列表中选择一个用户定义的配置并调整设置。下拉列表中的配置作为配置的标识符/名称。

元数据：选择要包含在配置中的元数据。

- **选择配置**：从列表中选择一个用户定义的配置并调整元数据设置。下拉列表中的配置作为元数据配置的标识符/名称。

PTZ：选择适合您的配置的 PTZ 设置。

- **选择配置**：从列表中选择一个用户定义的配置并调整 PTZ 设置。下拉列表中的配置对应于支持 PTZ 的设备视频通道。

创建：单击以保存您的设置并创建配置文件。

取消：单击以取消配置并清除全部设置。

profile_x：单击配置文件名称以打开并编辑预配置的配置文件。

分析元数据

实时流协议 (RTSP) 元数据生成器

查看和管理传输元数据的通道及其使用的协议。

注意

这些设置适用于使用 ONVIF XML 的 RTSP 元数据流。此处更改的设置不会影响元数据可视化页面。

生成器：使用实时流协议 (RTSP) 传输元数据的通道。

通道：用于从生成器发送元数据的通道。启用此选项可开启元数据流。出于兼容性或资源管理原因，可以禁用此选项。

侦测器

摄像机防篡改

当场景发生变化时，例如，镜头被覆盖、喷涂或严重超出对焦，且**触发延迟**时间已过，摄像机遮挡侦测器将生成警报。只有在摄像机至少 10 秒未移动时，遮挡侦测器才会激活。在此期间，侦测器将设置场景模型，用作侦测当前图像中遮挡的比较。要正确设置场景模型，请确保摄像机已对焦，照明条件良好，并且摄像机未指向缺少轮廓的场景（如，空白的墙壁）。摄像机遮挡也可用作触发操作的条件。

触发延迟：输入报警触发前必须激活篡改条件的下限时间。这有助于防止影响图像的已知条件的假警报。

在黑暗图像上触发：当摄像机镜头被喷涂时，很难获得警报，因为无法将此情况与图像同样变暗的其他情况（例如，当光线条件变化时）区分开来。打开此参数将为图像变黑暗的全部情况生成警报。关闭后，当图像变暗时，设备不会生成警报。

注意

用于在静态和非拥挤场景中侦测篡改尝试。

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图像的抓拍。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。
- **查看审核日志**：单击即可查看用户和系统活动的相关信息，例如，身份验证和配置的成功或失败情况。

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。

通过录制网络上的活动，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。

- 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。

类型：选择要发送的日志类型。

Test server setup（测试服务器设置）：保存设置前，向所有服务器发送测试消息。

CA 证书已设置：查看当前设置或添加证书。

普通配置

普通配置适用于具有 Axis 产品配置经验的高级用户。大多数参数均可在此页面进行设置和编辑。

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

安讯士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。这会进一步提高安讯士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。
- **自动回滚**：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

远程对焦和变焦

借助远程对焦和变焦功能，您可以从电脑对摄像机进行对焦和调整。这种方式可方便地用于确保场景对焦、视角和分辨率的优化，而无需去摄像机的安装现场。

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。

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。

重要

在创建隐私遮罩之前，请设置变焦和对焦。

注意

您不能向四画面视频流中添加隐私遮罩，但会在单独的视频通道中显示大多数配置的隐私遮罩。

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。

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。

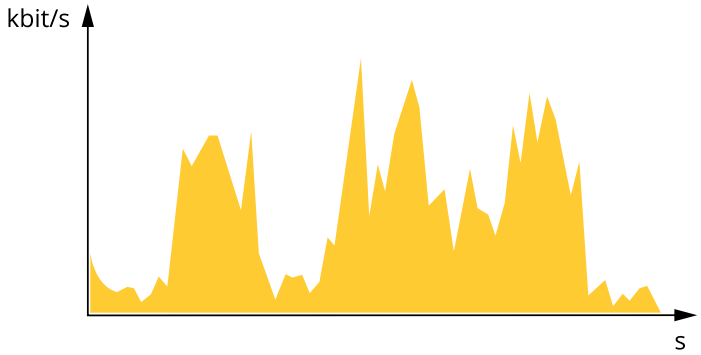
流选项卡包含视频流的设置。如果您从产品请求视频流，但未指定示例分辨率或帧率，则可获得这些设置。当您更改**流**选项卡中的设置时，它不会影响正在进行的流，但它将在开始新流时生效。

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。

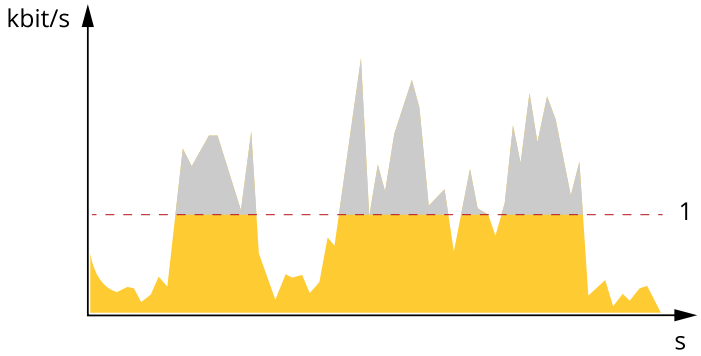
比特率控制

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。



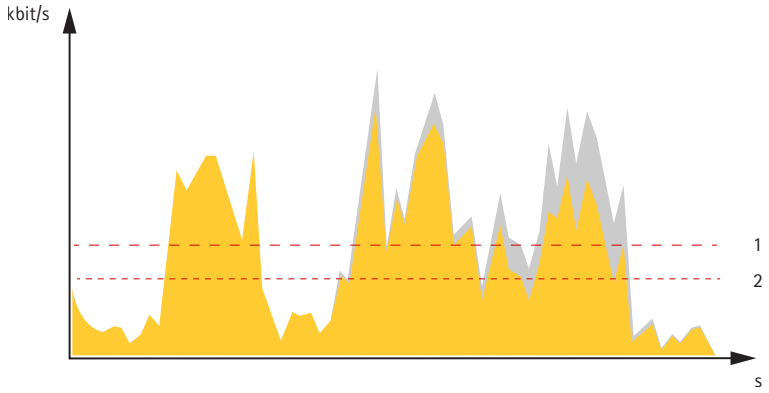
最大比特率 (MBR)
上限比特率让您可设置一个目标比特率，以处理系统中的比特率限制。当即时比特率保持低于指定目标比特率时，您可能会看到图像质量或帧速下降。您可以选择确定图像质量或帧速的优先顺序。我们建议将目标比特率配置为比预期比特率更高的值。这样可在场景中存在高水平的活动时提供边界。



1 目标比特率

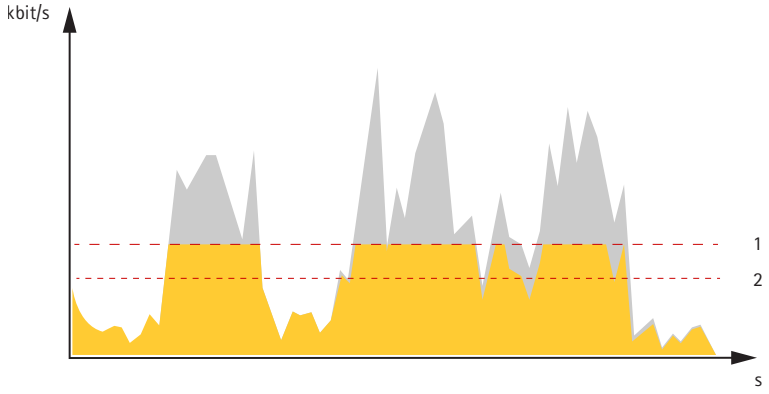
平均比特率 (ABR)
根据平均比特率，比特率可通过更长的时间段自动调整。由此，您就可以满足指定目标，并根据可用存储提供更佳视频质量。与静态场景相比，比特率在具有大量活动的场景中更高。在有大量活动的场景中，如果您使用平均比特率选项，那么您更有可能获得更高的图像质量。当调整图像质量以满足指定的目标比特率时，您可以定义存储视频流所需的总存储量（保留时间）。以下列方式之一指定平均比特率设置：

- 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。



1 目标比特率
2 实际平均比特率

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。

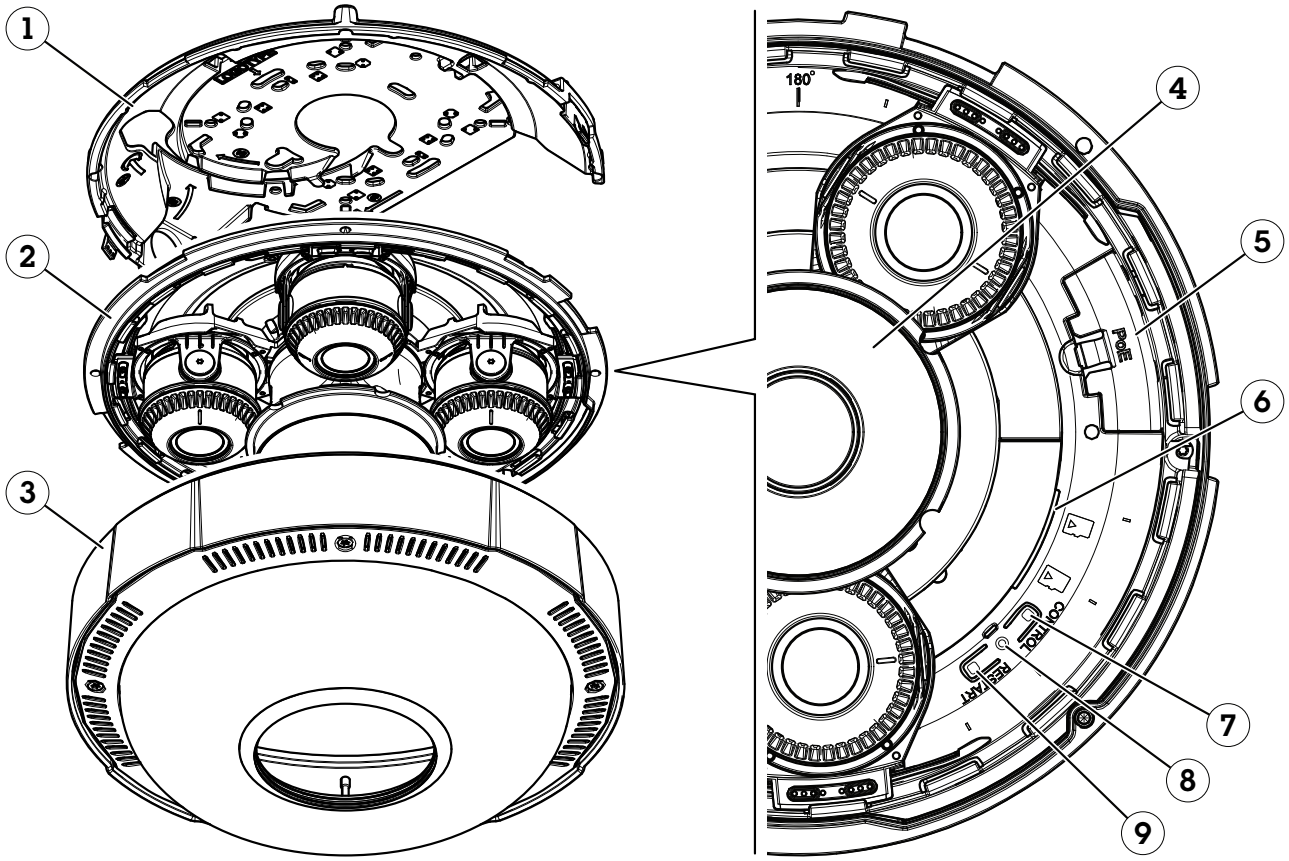
要查找 Axis 分析与应用的用户手册，请转到 *help.axis.com*。

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能否协同工作。

规格

产品概述



1 安装支架
2 摄像机装置
3 球型罩
4 红外照明
5 网络连接器 (PoE)
6 SD卡插槽
7 控制按钮
8 状态 LED 指示灯
9 重启按钮

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。

对焦助手的 LED指示灯情况

当对焦助手处于活动状态时， LED指示灯 闪烁。

彩色	指示
红色	图像失焦。 调整镜头。
淡黄色	图像接近对焦。 镜头需要微调。
绿色	图像已对焦。

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 。

重启按钮

按下重启按钮以重启产品。

连接器

网络连接器

采用高功率以太网供电 (High PoE) 的 RJ45。

故障排查

重置为出厂默认设置

⚠ 警告

⚠ 本产品可能会发出有害的光辐射。可能伤害眼睛。请勿注视正在工作的灯。

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. 同时按住控制按钮和重启按钮。
2. 释放重启按钮，但继续按住控制按钮 15–30 秒，直到 LED 状态指示灯呈琥珀色闪烁。
3. 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
4. 使用安装和管理软件工具分配 IP 地址、设置密码和访问视频流。

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**。

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

- 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、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	从网络上断开安讯士设备。运行 Ping 命令（在 Command/DOS 窗口中，键入 `ping` 和设备的 IP 地址）： • 如果您收到：`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。 • 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。

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。请参见 。
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 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。 如果需要，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**。

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 Camera Station Edge：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，请转到适配器的文档。
帧速低于预期	• 请参见 。 • 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。

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。

性能考虑

设置系统时，务必考虑不同设置和情况对性能的影响。一些因素会影响所需带宽大小（比特率），另一些因素可能会影响帧速，还有一些因素可能会同时影响这两者。如果 CPU 的负载达到最大值，也会影响帧速。

以下是重要的考虑因素：

- 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。

T10168322_zh

2024-06 (M11.2)

© 2021 – 2024 Axis Communications AB