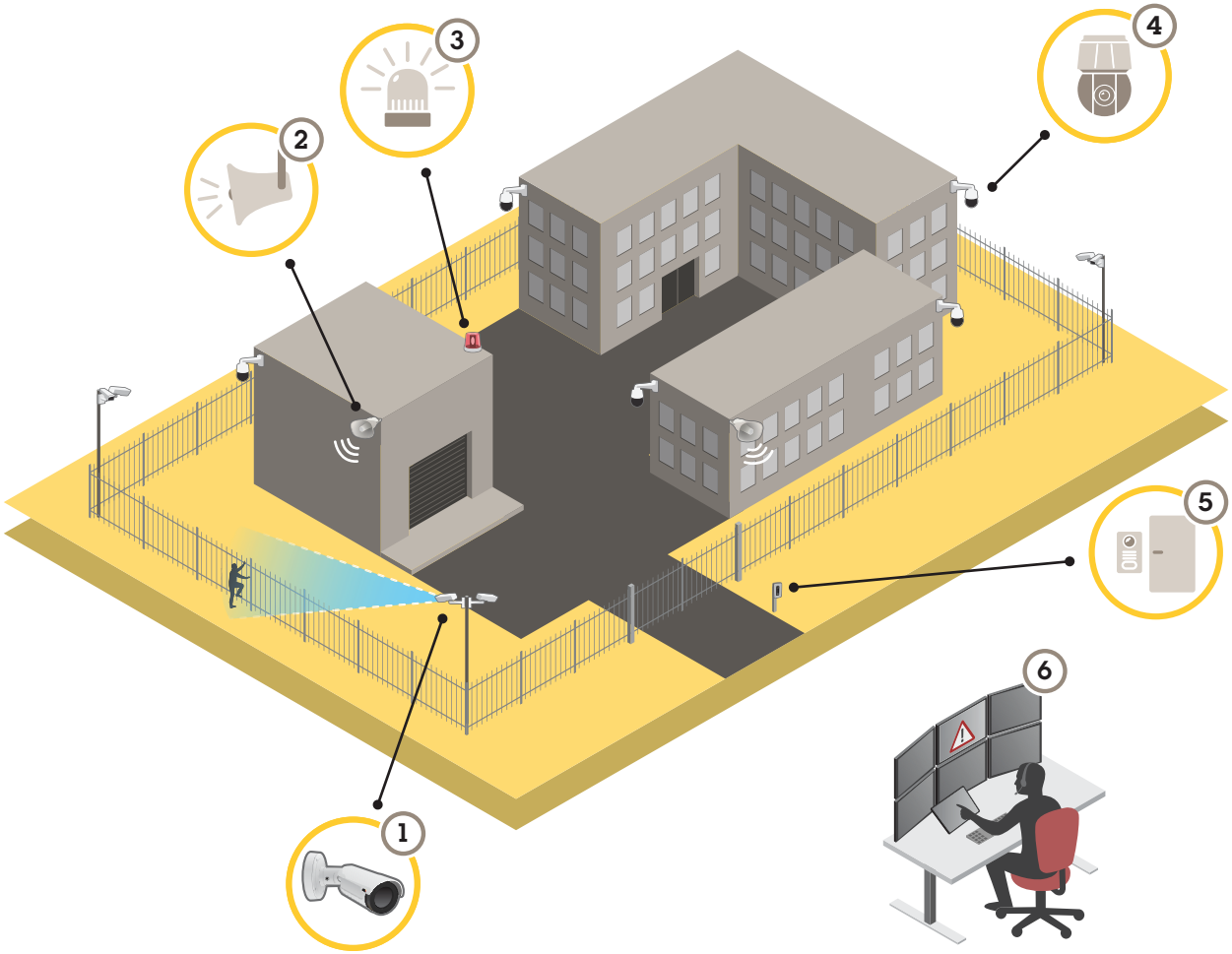
AXIS Q19热成像网络摄像机系列

AXIS Q1971-E Thermal Camera
AXIS Q1972-E Thermal Camera

User manual

目录

解决方案概述



1 *具有 AXIS Perimeter Defender 的热成像摄像机*
2 *号角扬声器*
3 *信号灯闪烁*
4 *PTZ 网络摄像机*
5 *门禁控制器*
6 *监控中心*

周界保护

对于需要入侵侦测的区域，您可以使用具有分析功能的热成像摄像机来设置周界保护。周界保护的主要物体是尽可能在早期阶段侦测到威胁或实际发生的入侵。

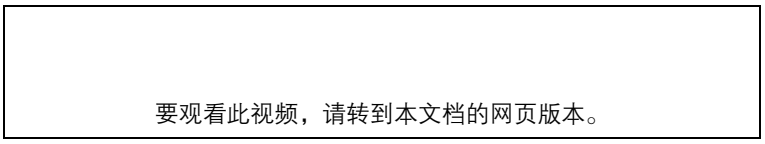
要设置周界保护，您需要在热成像摄像机上安装用于进行周界监控和保护的分析应用程序。安讯士为此提供了 AXIS Perimeter Defender 应用程序。您可以在 axis.com/products/axis-perimeter-defender 上阅读有关 *AXIS Perimeter* Defender 的更多信息

- 为了让可能出现的入侵者知道您的周界已经受到保护，请使用闪烁的信号灯 (3)。请参见 。
- 要进行警告和阻止，请连接一个播放预录制的警告消息的号角扬声器 (2)。请参见 。

安装

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。

开始使用

在网络上查找设备

若要在网络中查找 Axis 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™	Firefox®	Edge™	Safari®
Windows®	推荐	推荐	✓	
macOS ®	推荐	推荐	✓	✓
Linux®	推荐	推荐	✓	
其他操作系统	✓	✓	✓	✓*

*要在iOS 15或iPadOS 15上使用AXIS OS网页界面，请转到 **Settings（设置）> Safari > Advanced（高级）> Experimental Features（实验功能）**，并禁用NSURLSession Websocket。

如果您需要有关推荐的浏览器的更多信息，请转到 *AXIS OS Portal*。

打开设备的网页界面

1. 打开一个浏览器，键入 Axis 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，则必须创建管理员账户。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 。

创建管理员账户

首次登录设备时，您必须创建管理员账户。

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

设备没有默认账户。如果您丢失了管理员账户密码，则您必须重置设备。请参见 。

安全密码

重要

Axis 设备在网络中以明文形式发送初始设置的密码。若要在首次登录后保护您的设备，请设置安全加密的 HTTPS 连接，然后更改密码。

设备密码是对数据和服务的主要保护。Axis 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。

验证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。

网页界面概览

该视频为您提供设备网页界面的概览。

要观看此视频，请转到本文档的网页版本。

Axis 设备网页界面

配置设备

本部分介绍了安装程序在硬件安装完成后启动和运行产品所需的全部重要配置。

基本设置

设置电源频率

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

设置方向

1. 转到**视频 > 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 。

调平摄像机

要调整相对于参考区域或物体的视野，请综合使用水平网格和机械调节。

1. 转到**Video（视频）> Image（图像）>**，然后单击 。
2. 单击 显示水平网格。
3. 对摄像机进行机械调节，直到参考区域或物体的位置与水平网格对齐。

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。

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/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。

使用图像稳定功能来稳定晃动的图像

图像稳定适合在符合以下条件的环境中使用：产品安装在暴露位置，可能因为风吹或交通穿流等原因发生振动。

该功能使图像更光滑、更稳定且模糊减少。还会减小压缩图像的文件大小，并降低视频流的比特率。

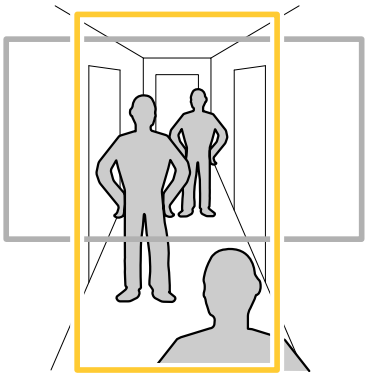
注意

当您打开图像稳定时，将对图像进行轻微的裁剪，从而降低上限分辨率。

1. 转到**视频 > 安装 > 图像校正**。
2. 打开**图像稳定**。

监控窄长区域

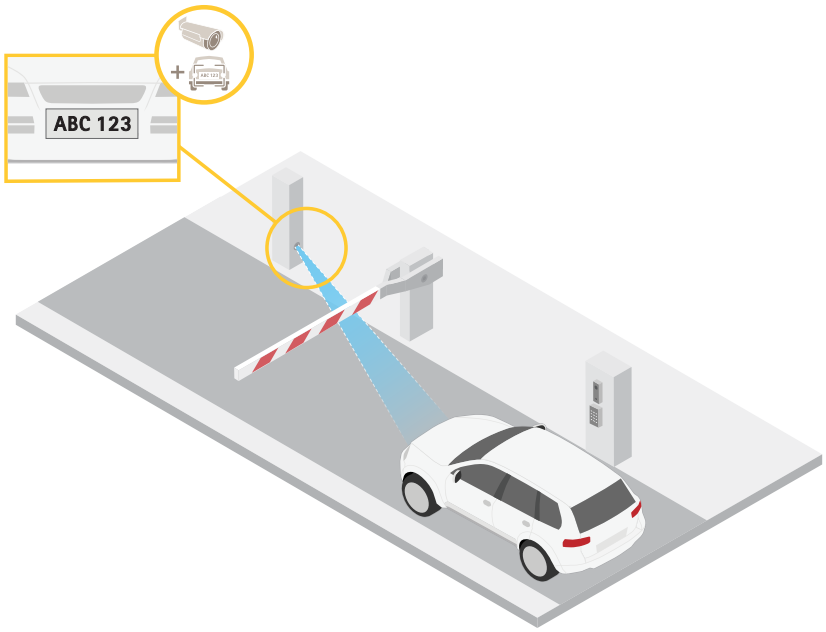
使用走廊格式可在窄长的区域（如楼梯、走廊、道路或通路）上更好地利用视野。



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° 。

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，是否能够识别车牌），您可以使用像素计数器。



1. 转到**视频 > 图像**。
2. 单击 。
3. 单击 以使用Pixel counter（**像素计数器**）。

4. 在摄像机的实时浏览中调整矩形的大小和位置，例如，在车牌可能出现的地方。
5. 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

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. 选择Image（图像）并单击 + 。
3. 点击**图像**。
4. 拖放图像。
5. 单击 Upload（上传）。
6. 单击**管理叠加**。
7. 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。

显示文本叠加

您可在视频流中将文本字段添加为叠加。例如，您可以在想要在视频流中显示日期、时间或公司名称时使用该功能。

1. 转到**视频 > 叠加**。
2. 选择Text（文本），然后单击 + 。
3. 键入要在视频流中显示的文本。
4. 选择一个位置。您也可在实时视图中拖动叠加文本字段以更改位置。

为图像添加街道名称和罗盘方向

注意

街道名称和罗盘方向将在视频流和录像上可见。

1. 转到**应用**。
2. 选择 axis-orientationaid。
3. 单击**打开**。
4. 要添加街道名称，请单击**添加文本**，然后修改文本以适合街道。
5. 要添加指南针，请单击**添加指南针**然后修改指南针以适合图像。

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：

   注意

   Zipstream 设置用于除 MJPEG 以外的所有视频编码。

   - 选择你要使用的 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**。

注意

大多数网页浏览器不支持 H.265 的解码，因此这款设备在其网页界面中不支持这种情况。相反，您可以使用支持 H.265 解码的视频管理系统或应用程序。

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 > 图像**。
2. 要开始录制，请单击 。

   如果尚未设置存储，请单击 and（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。

验证没有人篡改过视频

借助签名视频，您可以确保他人不会篡改摄像机录制的视频。

1. 转到**视频 > 流 > 常规**并打开**签名视频**。
2. 使用 AXIS Camera Station（5.46 或更高版本）或其他兼容视频管理软件录制视频。有关说明，请参见 *AXIS Camera Station 用户手册*。
3. 导出录制的视频。
4. 使用 AXIS File Player 播放视频。*下载 AXIS File Player*。

   指明没有人篡改过视频。

注意

要获取有关视频的更多信息，请右键单击视频，然后选择**显示数字签名**。

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。

请确保 AXIS Video Motion Detection 正在运行：

1. 转到**应用 > AXIS Video Motion Detection**。
2. 如果应用程序尚未运行，请将其启动。
3. 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. 在条件列表中，在**应用程序**下，选择 **VMD4**。
4. 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**。

5. 存储选项列表中，选择 SD_DISK。
6. 请选择一个摄像机和一个流配置文件。
7. 将预缓冲时间设置为 5 秒。
8. 将后缓冲时间设置为1 分钟。
9. 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”。

请确保 AXIS Video Motion Detection 正在运行：
1. 转到**应用 > AXIS Video Motion Detection**。
2. 如果应用程序尚未运行，请将其启动。
3. 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. 在条件列表中，在**应用程序**下，选择 VMD4。
4. 在操作列表中，在**叠加文本**下，选择**使用叠加文本**。
5. 选择视频通道。
6. 在**文本**中，键入“已侦测到移动动作”。
7. 设置持续时间。
8. 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。

为正在发生的事件提供视觉指示

您可以选择将 AXIS I/O Indication LED 连接到网络摄像机。此 LED 可以配置为当摄像机中发生某些事件时即打开。例如，让人们知道正在进行视频录制。

所需硬件

- AXIS I/O Indication LED
- 一台 Axis 网络视频摄像机

注意

AXIS I/O Indication LED 应该连接到输出端口。

注意

有关如何连接 AXIS I/O Indication LED 的说明，请参见产品随付的安装指南。

以下示例显示了如何配置打开 AXIS I/O Indication LED 来指示摄像机正在进行录制的规则。

1. 转到**系统 > 附件 > I/O 端口**。
2. 请确保将与 AXIS I/O Indication LED 连接的端口设置为**输出**。将正常状态设置为**开路**。
3. 转到**系统 > 事件**。
4. 创建新规则。
5. 选择触发摄像机开始录制必须满足的**条件**。例如，可以是时间表或移动侦测。
6. 在操作列表中，选择**录制视频**。选择存储空间。选择流配置文件或创建新配置文件。并根据需要设置**预缓冲**和**后缓冲**。
7. 保存规则。
8. 创建另一个规则，选择与首个规则相同的**条件**。
9. 在操作列表中，选择**当规则处于活动状态时切换 I/O**，然后选择与 AXIS I/O Indication LED 连接的端口。将状态设置为**激活**。
10. 保存规则。

可以使用 AXIS I/O Indication LED 的其他场景如：

- 将 LED 配置为在摄像机启动时打开，来指示摄像机状态。选择**系统就绪**作为条件。
- 将 LED 配置为在直播流处于活动状态时打开，来指示有人或程序正在访问摄像机中的流。选择**实时流访问**作为条件。

当摄像机侦测到大的噪音时录制视频

本示例解释了如何将摄像机设置为在侦测到大的噪音前五秒开始录制并在两分钟后停止。

打开音频：

1. 设置流配置以包括音频，请参见。

打开音频侦测：

1. 转到**系统 > 侦测器 > 音频侦测**。
2. 根据您的需求调整声音级别。

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. 在条件列表中的**音频**下，选择**音频侦测**。
4. 在操作列表中，在**录像**下，选择 **录制视频**。
5. 存储选项列表中，选择 SD_DISK。
6. 选择音频已打开的流配置文件。
7. 将预缓冲时间设置为 5 秒。
8. 将后缓冲时间设置为 2 分钟。
9. 单击 Save（**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篡改。环境或物体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**”。

侦测输入信号遮挡

本示例说明了如何在输入信号被剪切或短路时发送电子邮件。有关 I/O 连接器的详细信息，请参见 。

1. 进入 System（**系统**）>Accessories（**附件**）>I/O ports（**I/O 端口**） 并打开 Supervised（**受监控**）。

添加电子邮件接受者：

1. 转到**系统** > **事件** > **接收者**，然后添加一个接收者。
2. 键入接收者的名称。
3. 选择**电子邮件**。
4. 键入要向其发送电子邮件的电子邮件地址。
5. 摄像机没有自己的电子邮件服务器，因此必须登录到另一个电子邮件服务器才能发送电子邮件。根据您的电子邮件提供商填写其余信息。
6. 要发送测试电子邮件，单击**测试**。
7. 单击 Save（**保存**）。

创建一个规则：

1. 转到**系统** > **事件** > **规则**，然后添加一个规则。
2. 为规则键入一个名称。
3. 在条件列表中，在 **I/O**下，选择**受监督的输入篡改处于活动状态**。
4. 选择相关端口。
5. 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收者。
6. 键入电子邮件的主题和消息。
7. 单击 Save（**保存**）。

设置入侵报警

例如，使用入侵报警开关在有人打开摄像机护罩时发送通知。

在您开始之前

- 将入侵报警开关连接到摄像机 I/O 连接器的针脚 1（接地）和针脚 3（数字输入）。

配置输入端口

1. 转到**系统** > **附件** > **I/O 端口**。
2. 对于**端口 1**：

2.1. 选择**闭路**。

添加接收者:

3. 转到**系统 > 事件 > 接收者**并点击**添加接收者**。
4. 键入接收者的名称。
5. 选择**电子邮件**。
6. 键入要向其发送电子邮件的电子邮件地址。
7. 该摄像机没有自己的电子邮件服务器，因此需要登录另一个电子邮件服务器才能发送邮件。根据您的电子邮件提供商填写其余信息。
8. 要发送测试电子邮件，单击**测试**。
9. 单击 Save（保存）。

创建规则

10. 转到**系统 > 事件 > 规则**，然后添加一个规则。
11. 为规则键入一个名称。
12. 在条件列表中，在 I/O 下，选择**数字输入**。
13. 在端口列表中，选择**端口 1**。
14. 在操作列表中，在**通知**下，选择**将通知发送到电子邮件**。
15. 从列表中选择一个收件人或转到**收件人**，以创建新的收件人。

    要创建新收件人，请单击 + 。要复制现有收件人，请单击 。
16. 键入电子邮件的主题和消息。
17. 单击 Save（保存）。

如果有人喷涂镜头，自动发送电子邮件

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。

添加电子邮件接受者：

3. 转到**系统 > 事件 > 接收者**，然后添加一个接收者。
4. 键入接收者的名称。
5. 选择**电子邮件**。
6. 键入要向其发送电子邮件的电子邮件地址。
7. 摄像机没有自己的电子邮件服务器，因此必须登录到另一个电子邮件服务器才能发送电子邮件。根据您的电子邮件提供商填写其余信息。
8. 要发送测试电子邮件，单击**测试**。
9. 单击 Save（保存）。

创建一个规则：

10. 转到**系统 > 事件 > 规则**，然后添加一个规则。
11. 为规则键入一个名称。
12. 在条件列表中，在**视频**下，选择**篡改**。
13. 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收者。
14. 键入电子邮件的主题和消息。
15. 单击 Save（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。
4. 如果对输入源进行了更改，单击 Apply changes（**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**）。

连接到网络扬声器

通过网络扬声器配对，您可以使用兼容的 Axis 网络扬声器，就如同它已直接连接到摄像机。配对后，扬声器充当音频输出设备，您可以通过摄像机播放音频片段、传输声音。

重要

要使此功能与视频管理软件 (VMS) 配合使用，您必须首先将摄像机与网络扬声器配对，然后将摄像机添加到 VMS 中。

将摄像机与网络扬声器配对

1. 转到**系统 > 边缘到边缘 > 配对**。
2. 键入网络扬声器的 IP 地址、用户名和密码。
3. 选择**扬声器配对**。
4. 单击 Connect（**连接**）。显示确认消息。

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

上下文菜单包括：

- **分析数据**：接受共享非个人浏览器数据。
- **反馈**：分享反馈，以帮助我们改善您的用户体验。
- **法律**：查看有关 Cookie 和牌照的信息。
- **关于**：查看设备信息，包括 AXIS OS 版本和序列号。

状态

设备信息

显示设备信息，包括 AXIS OS 版本和序列号。

升级 AXIS OS：升级设备上的软件。转到在其中进行升级的维护页面。

时间同步状态

显示 NTP 同步信息，包括设备是否与 NTP 服务器同步以及下次同步前的剩余时间。

NTP 设置：查看并更新 NTP 设置。转到可更改 NTP 设置的**时间和位置**页面。

安全

显示活动设备的访问类型，正在使用的加密协议，以及是否允许未签约的应用。对设置的建议基于《AXIS OS 强化指南》。

强化指南：转到《*AXIS OS 强化指南*》，您可在其中了解有关如何应用 Axis 设备理想实践的更多信息。

连接的客户端

显示连接和连接的客户端数量。

查看详细信息：查看和更新已连接客户端列表。该列表显示了每个连接的 IP 地址、协议、端口、状态和 PID/进程。

持续录制中

显示正在进行的录制及其指定的存储空间。

录像： 查看正在进行的录制和过滤的录制文件及其来源。有关详细信息，请参见

显示保存录制内容的存储空间。

视频

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。

图像校正

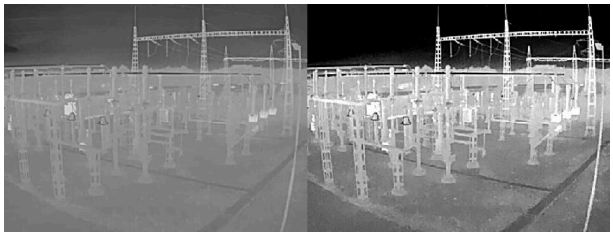
图像稳定 ：打开以生成更流畅、更稳定且不太模糊的图像。我们推荐您在符合以下条件的环境中使用图像稳定：设备安装在暴露位置中，并且可能因为风吹或人经过等因素而振动。

稳定器边界 ：使用滑块调整稳定器临界值的大小，确定振动级别以达到稳定。如果产品安装在大量振动的环境中，请将滑块向**上限**方向移动。因此，会捕捉较小的场景。如果环境的振动较少，请将滑块向 **下限**移动。

图像

呈现

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

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。

曝光

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。

增益上限：选择合适的最大增益。如果增益上限加大，则会改善低对比度图像中细节的可视级别，但也会提高噪音等级。更多噪声还可能导致使用更多带宽和存储。

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。

调色板：选择一个调色板，以使用不同颜色为图像着色，具体取决于温度。该调色板可提高精细细节的可视性。

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。

音频

包含：打开以在视频流中使用音频。

来源：选择要使用的音频源。

立体声：打开以包括内置音频以及来自外部麦克风的音频。

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视图图像中且在各视图、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。
  - : 单击以添加日期调节器 `%F`，以显示年–月–日。
  - : 单击以添加时间调节器 `%X`，以显示时: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）。
  - ：在图像中选择叠加的位置。
- **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。
  要上载图像，请单击**图像**。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。
  - : 单击以添加日期调节器 `%F`，以显示年–月–日。
  - : 单击以添加时间调节器 `%X`，以显示时: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）。
  - ：在图像中选择叠加的位置。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。
  - ：在图像中选择叠加的位置。
- **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。
- ：在图像中选择叠加的位置。
- **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。
  - ：在图像中选择叠加的位置。
  - **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。

隐私遮罩:单击此处可更改各隐私遮罩的颜色，或永久删除各隐私遮罩。

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。

遮罩 x：单击可重命名、禁用或永久删除遮罩。

分析

元数据配置

实时流协议 (RTSP) 元数据生成器

列出流传输元数据的应用程序及其使用的通道。

注意

这些设置适用于使用 ONVIF XML 的 RTSP 元数据流。在此更改不会影响元数据可视化页面。

生成器：生成元数据的应用程序。应用程序下方是应用程序从设备流传输的元数据类型的列表。

通道：应用程序使用的通道。选择以启用元数据流。出于兼容性或资源管理原因取消选择。

音频

设备设置

输入：打开或关闭音频输入。显示输入类型。

输入类型:选择输入类型，例如，麦克风或线路输入。

电源类型:选择用于输入的电源类型。

应用更改:应用您的选择。

消除回音：打开以在双向通信期间移除回声。

单独的增益控制：打开以单独调整不同输入类型的增益。

自动增益控制：打开以动态调整声音中的变化增益。

增益：使用滑块更改增益。单击麦克风图标可静音或取消静音。

流

编码：选择要用于输入源流传输的编码。只有打开了音频输入时，才能选择编码。如果音频输入已关闭，单击**启用音频输入**将其打开。

音频增强

输入

十波段图形音频均衡器：打开此项可调整一个音频信号内不同频段的级别。此功能适用于具有音频配置体验的高级用户。

对讲范围：选择操作范围以收集音频内容。提升操作范围会降低同时双向的通信能力。

声音增强：打开以增强与其他声音相关的语音内容。

录像

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。

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。

应用

添加应用：安装新应用。

查找更多应用：查找更多要安装的应用。您将被带到 Axis 应用程序的概览页面。

允许未签名的应用程序：启用允许安装未签名的应用。

允许root特权应用程序：打开以允许具有根权限的应用可对设备进行完全访问。

查看 AXIS OS 和 ACAP 应用程序中的安全更新。

注意

如果同时运行多个应用，设备的性能可能会受到影响。

使用应用名称旁边的开关可启动或停止应用。

打开：访问应用的设置。可用的设置取决于应用。某些应用程序没有设置。

上下文菜单可包含以下一个或多个选项：

- **开源牌照**:查看有关应用中使用的开放源代码许可证的信息。
- **应用日志**：查看应用事件的日志。当您与支持人员联系时，日志很有用。
- **使用密钥激活牌照**：如果应用需要牌照，则需要激活它。如果您的设备没有互联网接入，请使用此选项。
  如果你没有牌照密钥，请转到 *axis.com/products/analytics*.您需要许可证代码和 Axis 产品序列号才能生成许可证密钥。
- **自动激活牌照**：如果应用需要牌照，则需要激活它。如果您的设备有互联网接入，请使用此选项。您需要牌照密钥来激活牌照。
- **停用许可证**：停用许可证以将其替换为其他许可证，例如，当您从试用许可证更改为完整许可证时。如果要停用许可证，您还会将其从设备中移除。
- **设置**：配置参数。
- **删除**：永久从设备中删除应用。如果不首先停用许可证，则许可证将保持活动状态。

系统

时间和位置

日期和时间

时间格式取决于网页浏览器的语言设置。

注意

我们建议您将设备的日期和时间与 NTP 服务器同步。

同步：选择设备日期和时间同步选项。

- **自动日期和时间（手动 NTS KE 服务器）**：与安全 NTP 密钥建立连接至 DHCP 服务器的服务器进行同步。
  - **手动 NTS KE 服务器**：输入一个或两个 NTP 服务器的 IP 地址。当您使用两台 NTP 服务器时，设备会根据两者的输入同步并调整其时间。
  - **上限 NTP 轮询时间**：选择设备在轮询 NTP 服务器以获取更新时间之前应等待的时间上限。
  - **NTP 轮询时间下限**：选择设备在轮询 NTP 服务器以获取更新时间之前应等待的时间下限。
- **自动日期和时间（使用 DHCP 的 NTP 服务器）**：与连接到 DHCP 服务器的 NTP 服务器同步。
  - **备用 NTP 服务器**：输入一个或两个备用服务器的 IP 地址。
  - **上限 NTP 轮询时间**：选择设备在轮询 NTP 服务器以获取更新时间之前应等待的时间上限。
  - **NTP 轮询时间下限**：选择设备在轮询 NTP 服务器以获取更新时间之前应等待的时间下限。
- **自动日期和时间（手动 NTP 服务器）**：与您选择的 NTP 服务器同步。
  - **手动 NTP 服务器**：输入一个或两个 NTP 服务器的 IP 地址。当您使用两台 NTP 服务器时，设备会根据两者的输入同步并调整其时间。
  - **上限 NTP 轮询时间**：选择设备在轮询 NTP 服务器以获取更新时间之前应等待的时间上限。
  - **NTP 轮询时间下限**：选择设备在轮询 NTP 服务器以获取更新时间之前应等待的时间下限。
- **自定义日期和时间**：手动设置日期和时间。单击**从系统获取**以从计算机或移动设备获取日期和时间设置。

时区：选择要使用的时区。时间将自动调整为夏令时和标准时间。

- **DHCP**：采用 DHCP 服务器的时区。设备必须连接到 DHCP 服务器，然后才能选择此选项。
- **手动**：从下拉列表中选择时区。

注意

系统在各录像、日志和系统设置中使用日期和时间设置。

设备位置

输入设备所在的位置。视频管理系统可以使用此信息来在地图上放置设备。

- **格式化**：当您输入设备经纬度时，选择希望使用的格式。
- **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仅有的。为避免冲突，建议在分配静态 IP 地址前联系网络管理员。

子网掩码：输入子网掩码，以定义局域网内的地址。局域网之外的地址都通过路由器。

路由器：输入默认路由器（网关）的 IP 地址用于连接已连接至不同的网络和网段的设备。

如果 DHCP 不可用，退回到静态 IP 地址:如果希望在 DHCP 不可用且无法自动分配 IP 地址时，添加要用作备用静态 IP 地址，请选择此项。

注意

如果 DHCP 不可用且设备使用备用静态地址，则静态地址配置范围有限。

IPv6

自动分配 IPv6：选择打开 IPv6 并让网络路由器自动分配设备的 IP 地址。

主机名

自动分配主机名称：选择让网络路由器自动分配设备的主机名称。

主机名称：手动输入主机名称，作为访问设备的另一种方式。服务器报告和系统日志使用主机名。允许的字符是 A–Z, a–z, 0–9 和 –。

启动动态 DNS 更新： 允许设备在 IP 地址更改时自动更新其域名服务器记录。

注册 DNS 名称：输入指向设备 IP 地址的唯一域名。允许的字符是 A–Z, a–z, 0–9 和 –。

TTL：生存时间 (TTL) 设置 DNS 记录在需要更新之前保持有效的时长。

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，您将得到一个警告。

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，您将得到一个警告。

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。要解决 PoE 电源协商的任何问题，请仅为硬件 PoE 电源协商配置 PoE 交换机。

全局代理

Http proxy（Http代理）：根据允许的格式指定全局代理主机或IP地址。

Https proxy（Https代理）：根据允许的格式指定全局代理主机或IP地址。

http和https代理支持的格式：

- http(s)://host:port
- http(s)://user@host:port
- http(s)://user:pass@host:port

注意

重启设备以应用全局代理设置。

No proxy（无代理）：使用**No proxy（无代理）**以绕过全局代理。输入列表中的一个选项，或输入多个选项，以逗号分隔：

- 留空
- 指定IP地址
- 以CIDR格式指定IP地址
- 指定域名，例如：www.<域名>.com
- 指定特定域中的所有子域，例如.<域名>.com

一键云连接

一键式云连接 (O3C) 与 O3C 服务结合使用，可从不同位置通过互联网安全地访问实时视频和录制的视频。有关详细信息，请参见 *axis.com/end–to–end–solutions/hosted–services*。

允许 O3C：

- **一键式：**这是默认设置。按住设备上的控制按钮，以通过互联网连接到 O3C 访问。按下控制按钮后 24 小时内，您需要向 O3C 服务注册设备。否则，设备将从 O3C 服务断开。一旦您注册了设备，**一直**将被启用，您的设备会一直连接到 O3C 服务。
- **总是：**设备将不断尝试通过互联网连接到 O3C 服务。一旦您注册了设备，它会一直连接到 O3C 服务。如果无法够到设备上的控制按钮，则使用此选项。
- **无：**禁用 O3C 服务。

代理设置：如果需要，请输入代理设置以连接到代理服务器。

主机：输入代理服务器的地址。

端口：输入用于访问的端口数量。

登录和**密码：**如果需要，请输入代理服务器的用户名和密码。

身份验证方法：

- **基本：**此方法是 HTTP 兼容的身份验证方案。它的安全性不如 **Digest（摘要）**方法，因为它将用户名和密码发送到服务器。
- **摘要：**此方法一直在网络中传输加密的密码，因此更安全。
- **自动：**借助此选项，可使设备根据支持的方法自动选择身份验证方法。**摘要**方法优先于**基本**方法。

拥有人身份验证密钥 (OAK):单击**Get key（获取密码）**以获取所有者的身份验证密钥。只有在没有防火墙或代理的情况下设备连接到互联网时，才可能发生这种情况。

SNMP

简单网络管理协议 (SNMP) 允许远程管理网络设备。

SNMP:选择要使用的 SNMP 版本。

- **v1 和 v2c**:
  - **读取团体**：输入可只读访问支持的 SNMP 对象的团体名称。默认值为**公共**。
  - **编写社区**：输入可读取或写入访问支持全部的 SNMP 物体（只读物体除外）的团体名称。默认值为**写入**。
  - **激活陷阱**：打开以激活陷阱报告。该设备使用陷阱发送重要事件或更改状态的消息到管理系统。在网页界面中，您可以设置 SNMP v1 和 v2c 的陷阱。如果您更改为 SNMP v3 或关闭 SNMP，陷阱将自动关闭。如果使用 SNMP v3，则可通过 SNMP v3 管理应用程序设置陷阱。
  - **陷阱地址**：输入管理服务器的 IP 地址或主机名。
  - **陷阱团体**：输入设备发送陷阱消息到管理系统时要使用的团体。
  - **陷阱**:
    - **冷启动**：设备启动时发送陷阱消息。
    - **热启动**：更改 SNMP 设置时发送陷阱消息。
    - **连接**：链接自下而上发生变更时，发送陷阱消息。
    - **身份验证失败**：验证尝试失败时，发送陷阱消息。

注意

打开 SNMP v1 和 v2c 陷阱时，将启用 Axis Video MIB 陷阱。有关更多信息，请参见 *AXIS OS Portal > SNMP*。

- **v3**:SNMP v3 是一个提供加密和安全密码的更安全版本。若要使用 SNMP v3，我们建议激活 HTTPS，因为密码将通过 HTTPS 发送。这还会防止未授权方访问未加密的 SNMP v1 及 v2c 陷阱。如果使用 SNMP v3，则可通过 SNMP v3 管理应用程序设置陷阱。
  - **“initial” 账户密码**:输入名为'initial'的帐户的 SNMP 密码。尽管可在不激活 HTTPS 的情况下发送密码，但我们不建议这样做。SNMP v3 密码仅可设置一次，并且推荐仅在 HTTPS 启用时。一旦设置了密码，密码字段将不再显示。要重新设置密码，则设备必须重置为出厂默认设置。

安全

认证

证书用于对网络上的设备进行身份验证。该设备支持两种类型的证书：

- **客户端/服务器证书**
  客户端/服务器证书用于验证设备身份，可以是自签名证书，也可以是由证书颁发机构颁发的证书。自签名证书提供有限的保护，可在获得 CA 颁发的证书之前使用。
- **CA 证书**
  您可以使用 CA 证书来验证对等证书，例如，在设备连接到受 IEEE 802.1X 保护的网络时，用于验证身份验证服务器的身份。设备具有几个预装的 CA 证书。

支持以下格式：

- 证书格式：.PEM、.CER、.PFX
- 私钥格式：PKCS#1 和 PKCS#12

重要

如果将设备重置为出厂默认设置，将删除各证书。预安装的 CA 证书将重新安装。

添加证书：单击添加证书。

- **更多** ：显示更多要填充或选择的栏。
- **安全密钥库**：选择使用**安全元件**或**可信平台模块 2.0** 来安全存储私钥。有关选择哪个安全密钥库的更多信息，请转至 *help.axis.com/en-us/axis-os#cryptographic-support*。
- **秘钥类型**：从下拉列表中选择默认或其他加密算法以保护证书。

上下文菜单包括：

- **证书信息**：查看已安装证书的属性。
- **删除证书**：删除证书。
- **创建证书签名请求**：创建证书签名请求，发送给注册机构以申请数字身份证书。

安全密钥库：

- **安全元件 (CC EAL6+)**：选择使用安全元素来实现安全密钥库。
- **受信任的平台模块 2.0（CC EAL4+、FIPS 140-2 2 级）**：安全密钥库选择使用 TPM 2.0。

网络访问控制和加密

IEEE 802.1x

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

激活：打开防火墙。

默认策略：选择防火墙的默认状态。
- **允许**：允许与设备的各连接。默认情况下设置此选项。
- **拒绝**：拒绝与设备的各连接。

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

- **地址**：输入要允许或拒绝访问的 IPv4/IPv6 或 CIDR 格式的地址。
- **协议**：选择要允许或拒绝访问的协议。
- **端口**：输入要允许或拒绝访问的端口号。您可以添加介于 1 和 65535 之间的端口号。
- **策略**：选择规则的策略。

＋：单击创建另一个规则。

添加规则：单击此项可添加已定义的规则。
- **时间（秒）**：设置测试规则的时间限制。默认时间限制设置为300秒。要立即激活规则，请将时间设置为0。
- **确认规则**：确认规则及其时间限制。如果您将时间限制设置为 1 秒以上，则规则将在此期间处于活动状态。如果您将时间设置为0，规则将直接激活。

待处理规则：您尚未确认的经过测试的新检测规则概述。

注意

具有时间限制的规则将显示在**活动规则**下，直到显示的计时器用完或确认它们为止。如果不进行确认，一旦计时器用完，它们将显示在**待处理规则**下，并且防火墙将恢复为之前定义的设置。如果您确认，它们将替换当前有效的规则。

确认规则：单击以激活挂起的规则。

活动规则：当前在设备上运行的规则概述。

：单击可删除活动规则。

：单击可删除各规则，包括挂起规则和活动规则。

自定义签名的 AXIS OS 证书

要在设备上安装来自 Axis 的测试软件或其他自定义软件，您需要自定义签名的 AXIS OS 证书。证书验证软件是否由设备权利人和 Axis 批准。软件只能在由其单一序列号和芯片 ID 标识的特定设备上运行。只有 Axis 可以创建自定义签名 AXIS OS 证书，因为 Axis 持有对其进行签名的密钥。

安装：单击安装以安装证书。在安装软件之前，您需要安装证书。

⋮ 上下文菜单包括：

- **删除证书**：删除证书。

账户

账户

添加帐户：单击以添加新账户。您可以添加多达 100 个账户。

帐户:输入一个唯一的账户名。

新密码：输入账户的密码。密码必须为 1 到 64 个字符长。密码仅允许包含可打印的 ASCII 字符（代码 32–126），如字母、数字、标点符号和某些符号。

确认密码：再次输入同一密码。

优先权：

- **管理员**：可完全访问全部设置。管理员也可以添加、更新和删除其他账户。
- **操作员**：有权访问全部设置，以下各项除外：
  - 全部 System（**系统**）设置。
- **浏览者**：有权访问：
  - 观看并拍摄视频流的快照。
  - 观看和导出录音。
  - 水平转动、垂直转动和变焦；使用**PTZ账户**权限。

上下文菜单包括：

更新账户：编辑账户的属性。

删除账户：删除账户。无法删除根账户。

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，而无需登录账户。

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 账户

添加SSH账户：单击以添加新 SSH 账户。

- **限制根访问**：打开以限制要求根访问的功能。
- **启用 SSH**:打开以使用 SSH 服务。

帐户:输入一个唯一的账户名。

新密码：输入账户的密码。密码必须为 1 到 64 个字符长。密码仅允许包含可打印的 ASCII 字符（代码 32–126），如字母、数字、标点符号和某些符号。

确认密码：再次输入同一密码。

注释：输入注释（可选）。

上下文菜单包括：

更新 SSH 账户：编辑账户的属性。

删除 SSH 账户：删除账户。无法删除根账户。

OpenID 配置

重要

如果无法使用 OpenID 登录，请使用配置 OpenID 登录时使用的摘要或基本凭据。

客户端 ID:输入 OpenID 用户名。

外发代理:输入 OpenID 连接的代理地址以使用代理服务器。

管理员声明:输入管理员角色的值。

提供商 URL:输入 API 端点身份验证的网页链接。格式应为 https://[insert URL]/.well–known/openid–configuration

操作员声明:输入操作员角色的值。

需要声明:输入令牌中应包含的数据。

浏览者声明:输入浏览者角色的值。

远程用户:输入一个值以标识远程用户。这有助于在设备的网页界面中显示当前用户。

范围:可以是令牌一部分的可选作用域。

客户端密码:输入 OpenID 密码

保存：单击以保存 OpenID 值。

启用 OpenID:打开以关闭当前连接并允许来自提供商 URL 的设备身份验证。

事件

规则

规则定义产品执行操作触发的条件。该列表显示产品中当前配置的全部规则。

注意

您可以创建多达 256 个操作规则。

添加规则：创建一个规则。

名称：为规则输入一个名称。

操作之间的等待时间：输入必须在规则激活之间传输的时间下限（hh：mm：ss）。如果规则是由夜间模式条件激活，以避免日出和日落期间发生的小的光线变化会重复激活规则，此功能将很有用。

条件：从列表中选择条件。设施要执行操作必须满足的条件。如果定义了多个条件，则必须满足全部条件才能触发操作。有关特定条件的信息，请参见*开始使用事件规则*。

使用此条件作为触发器：选择以将此首个条件作为开始触发器。这意味着一旦规则被激活，不管首个条件的状态如何，只要其他条件都将保持有效，它将一直保持活动状态。如果未选择此选项，规则将仅在全部条件被满足时即处于活动状态。

反转此条件：如果希望条件与所选内容相反，请选择此选项。

添加条件：单击以添加附加条件。

操作：从列表中选择操作，然后输入其所需的信息。有关特定操作的信息，请参见*开始使用事件规则*。

接受者

您可以设置设备以通知收件人有关事件或发送文件的信息。

注意

如果将设备设置为使用 FTP 或 SFTP，请不要更改或删除添加到文件名中的唯一序列号。如果这样做，每个事件只能发送一副图像。

该列表显示产品中当前配置的全部收件人以及有关其配置的信息。

注意

您可以创建多达 20 个接收者。

添加接收者：单击以添加接收者。

名称：为接收者输入一个名称。

类型：从列表中选择：

- FTP
  - **主机**：输入服务器的 IP 地址或主机名。如果输入主机名，请确保在 **System（系统）>Network（网络）>IPv4 and IPv6（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 **System（系统）>Network（网络）>IPv4 and IPv6（IPv4 和 IPv6）**下指定 DNS 服务器。
  - **端口**：输入 SFTP 服务器使用的端口号。默认为 22。

- **文件夹**：输入要存储文件的目录路径。如果 SFTP 服务器上不存在此目录，则上载文件时将出现错误消息。
- **用户名**：输入登录用户名。
- **密码**：输入登录密码。
- **SSH 主机公共密钥类型 (MD5)**：输入远程主机的公共密钥（32 位十六进制的数字串）指纹。SFTP 客户端通过 RSA、DSA、ECDSA 和 ED25519 主机密钥类型支持 SFTP 服务器使用 SSH-2 协议。在协商期间，RSA 是理想方法，然后是 ECDSA、ED25519 和 DSA。要确保输入您的 SFTP 服务器使用的正确 MD5 主机密钥。虽然 Axis 设备同时支持 MD5 和 SHA-256 哈希密钥，但我们建议使用 SHA-256，因为安全性比 MD5 更安全。有关如何配置带 Axis 设备的 SFTP 服务器的详细信息，请转到 *AXIS OS Portal*。
- **SSH 主机公共密钥类型 (SHA256)**：输入远程主机的公共密钥（43 位 Base64 的编码字符串）指纹。SFTP 客户端通过 RSA、DSA、ECDSA 和 ED25519 主机密钥类型支持 SFTP 服务器使用 SSH-2 协议。在协商期间，RSA 是理想方法，然后是 ECDSA、ED25519 和 DSA。要确保输入您的 SFTP 服务器使用的正确 MD5 主机密钥。虽然 Axis 设备同时支持 MD5 和 SHA-256 哈希密钥，但我们建议使用 SHA-256，因为安全性比 MD5 更安全。有关如何配置带 Axis 设备的 SFTP 服务器的详细信息，请转到 *AXIS OS Portal*。
- **使用临时文件名**:选择以临时自动生成的文件名上传文件。上载完成时，这些文件将重命名为所需的名称。如果上传中止或中断，您不会获得损坏的文件。但是，您仍然可能会获得临时文件。这样，您就知道带有所需名称的文件都是正确的。

- SIP或VMS：
  SIP：选择进行 SIP 呼叫。
  VMS：选择进行 VMS 呼叫。
  - **从 SIP 账户**：从列表中选择。
  - **至 SIP 地址**：输入 SIP 地址。
  - **测试**：单击以测试呼叫设置是否有效。
- **电子邮件**
  - **发送电子邮件至**：键入电子邮件的收件地址。如果要输入多个地址，请用逗号将地址分隔开。
  - **从以下位置发送电子邮件**：输入发件服务器的电子邮件地址。
  - **用户名**：输入邮件服务器的用户名。如果电子邮件服务器不需要身份验证，请将此字段留空。
  - **密码**：输入邮件服务器的密码。如果电子邮件服务器不需要身份验证，请将此字段留空。
  - **电子邮件服务器 (SMTP)**：输入 SMTP 服务器的名称，例如，smtp.gmail.com 和 smtp.mail.yahoo.com。
  - **端口**：使用 0–65535 范围内的值输入 SMTP 服务器的端口号。默认值为 587。
  - **加密**：要使用加密，请选择 SSL 或 TLS。
  - **验证服务器证书**：如果使用加密，请选择验证设备的身份。证书可以是自签名的或由证书颁发机构 (CA) 颁发。
  - **POP 身份验证**：打开输入 POP 服务器的名称，例如，pop.gmail.com。

注意

某些电子邮件提供商拥有安全过滤器，可防止用户接收或查看大量附件、接收计划的电子邮件及类似内容。检查电子邮件提供商的安全策略，以避免您的电子邮件帐户被锁定或错过预期的电子邮件。

- TCP

- **主机**：输入服务器的 IP 地址或主机名。如果输入主机名，请确保在 **System（系统）>Network（网络）>IPv4 and IPv6（IPv4 和 IPv6）**下指定 DNS 服务器。
- **端口**：输入用于访问服务器的端口号。

测试：单击以测试设置。

⋮ 上下文菜单包括：

查看接收者:单击可查看各收件人详细信息。

复制接收者:单击以复制收件人。当您进行复制时，您可以更改新的收件人。

删除接收者:单击以永久删除收件人。

时间计划表

时间表和脉冲可用作规则中的条件。该列表显示产品中当前配置的全部时间表和脉冲以及有关其配置的信息。

＋ **添加时间表**：单击以创建时间表或脉冲。

手动触发器

可使用手动触发以手动触发规则。手动触发器可用于验证产品安装和配置期间的行为等。

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。Axis 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。

您可在 *AXIS OS Portal* 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据。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 Axis 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**域\用户名**。
- **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 Axis 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为介于 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 账户

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 账户，即可自动启用 ONVIF 通信。使用该账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。

添加账户：单击以添加新 ONVIF 账户。

帐户:输入一个唯一的账户名。

新密码：输入账户的密码。密码必须为 1 到 64 个字符长。密码仅允许包含可打印的 ASCII 字符（代码 32–126），如字母、数字、标点符号和某些符号。

确认密码：再次输入同一密码。

角色：

- **管理员**：可完全访问全部设置。管理员也可以添加、更新和删除其他账户。
- **操作员**：有权访问全部设置，以下各项除外：
  - 全部System（**系统**）设置。
  - 添加应用。
- **媒体账户**：仅允许访问视频流。

上下文菜单包括：

更新账户：编辑账户的属性。

删除账户：删除账户。无法删除根账户。

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。

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。关闭时，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。

音频侦测

这些设置可用于每个音频输入。

声音级别:调整声音级别设置在 0–100 的范围内，其中 0 是敏感上限，而 100 是敏感下限。在设置声音级别时，请使用活动指示器作为指导。在创建事件时，您可以将声音级别用作条件。如果声音级别高于、低于或超过设定值，您可以选择触发操作。

撞击检测

冲击侦测器:打开以在物体击中设备或被遮挡时生成警报。

敏感度级别:移动滑块以调整设备应生成警报的敏感度级别。低值表示设备仅在击中力很强的情况下才生成警报。较高的值意味着即使有轻度的干预，设备也会生成警报。

附件

I/O 端口

数字输入用于连接可在开路和闭路之间切换的外部设备，例如 PIR 传感器、门或窗传感器和玻璃破碎探测器。

数字输出用于连接继电器和 LED 等外部设备。您可通过 VAPIX® 应用程序编程接口或网页界面激活已连接的设备。

端口

名称：编辑文本来重命名端口。

方向：指示端口是输入端口。指示它是一个输出端口。如果端口可配置，则您可以单击这些图标以在输入和输出之间进行切换。

正常状态：单击开路，单击闭路。

当前状态：显示端口的当前状态。在当前状态并非正常状态时，将激活输入或输出。当断开连接或电压高于 1 VDC 时，设备上的输入为开路。

注意

在重启过程中，输出电路为开路。当重启完成时，电路将恢复为正常位置。如果更改此页面上设置，无论是否存在活动的触发器，输出电路都将返回其正常位置。

受监控：如果有人篡改连接到数字 I/O 设备，请打开，以侦测并触发操作。除了侦测某个输入是否打开或关闭外，您还可以侦测是否有人篡改了该输入（即，剪切或短路）。监控连接功能要求外部 I/O 回路中存在其他硬件（线尾电阻器）。

边缘到边缘

配对

自动配对允许你使用兼容的 Axis 网络扬声器，就如同它是主设备的一部分。

Audio pairing（**音频配对**）允许您与网络扬声器或麦克风配对。配对后，网络扬声器充当音频输出设备，您可以通过摄像机播放音频片段、传输声音。网络麦克风将占用周围区域的声音，并使其作为音频输入设备提供，可用于媒体流和录制内容。

重要

要使此功能与视频管理软件 (VMS) 配合使用，您要首先将摄像机与扬声器或麦克风配对，然后将摄像机添加到 VMS 中。

当您在以“音频检测”为条件且以“播放音频剪辑”为操作的事件规则中使用网络配对音频设备时，请在事件规则中设置“在操作之间等待（hh：mm：ss）”限制。这将帮助您避免在捕音麦克风从扬声器采集音频时进行检测。

添加：添加希望配对的设备。

Select pairing type（**选择配对类型**）：从下拉列表中进行选择。

扬声器配对:选择配对网络扬声器。

麦克风配对：选择配对麦克风。

地址：输入网络扬声器的主机名称或 IP 地址。

用户名：请输入用户名。

密码：输入用户的密码。

Close（**关闭**）：单击以清除各字段。

连接：单击以建立与要配对设备的连接。

日志

报告和日志

报告

- **查看设备服务器报告**：在弹出窗口中查看有关产品状态的信息。服务器报告中自动包含访问日志。
- **下载设备服务器报告**：将创建一个 .zip 文件，其中包含 UTF–8 格式的完整服务器报告文本文件以及当前实时浏览的快照。当您与支持人员联系时，请始终提供服务器报告 .zip 文件。
- **下载崩溃报告**：下载和存档有关服务器状态的详细信息。崩溃报告中包含服务器报告中的信息和详细的调试信息。此报告中可能包含网络跟踪之类敏感信息。可能需要几分钟时间才生成此报告。

日志

- **查看系统日志**：单击以查看有关系统事件（如设备启动、警告和重要消息）的信息。
- **查看访问日志**：单击以查看访问设备的全部失败尝试，例如，使用了错误的登录密码。

远程系统日志

系统日志是消息日志记录的标准。它允许分离生成消息的软件、存储消息的系统以及报告和分析这些消息的软件。每个消息都标有设施代码，指示生成消息的软件类型，并为其分配一个严重性等级。

服务器：单击以添加新服务器。

主机：输入服务器的主机名或 IP 地址。

格式化：选择要使用的 syslog 消息格式。

- Axis
- RFC 3164
- RFC 5424

协议：选择要使用的协议：

- UDP（默认端口为 514）
- TCP（默认端口为 601）
- TLS（默认端口为 6514）

端口：编辑端口号以使用其他端口。

严重程度：选择触发时要发送哪些消息。

CA 证书已设置：查看当前设置或添加证书。

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

维护

重启：重启设备。这不会影响当前设置。正在运行的应用程序将自动重启。

恢复：将大部分设置恢复为出厂默认值。之后，您必须重新配置设备和应用，重新安装未预安装的应用，并重新创建事件和预设。

重要

重置后保存的仅有设置是：

- 引导协议（DHCP 或静态）
- 静态 IP 地址
- 默认路由器
- 子网掩码
- 802.1X 设置
- O3C 设置
- DNS 服务器 IP 地址

出厂默认设置：将全部恢复为出厂缺省值。之后，您必须重置 IP 地址，以便访问设备。

注意

各个 Axis 设备软件均经过数字签名以确保仅在设备上安装经过验证的软件。这会进一步提高 Axis 设备的总体网络安全级别门槛。有关详细信息，请参见 *axis.com* 上的白皮书“Axis Edge Vault”。

AXIS OS 升级：升级到新的 AXIS OS 版本。新版本中可能包含改进的功能、补丁和全新功能。建议您始终使用新 AXIS OS 版本。要 下载更新版本，请转到 *axis.com/support*。

升级时，您可以在三个选项之间进行选择：

- **标准升级**：升级到新的 AXIS OS 版本。
- **出厂默认设置**：更新并将设置都恢复为出厂默认值。当您选择此选项时，无法在升级后恢复到以前的 AXIS OS 版本。
- **自动还原**：在规定时间内升级并确认升级。如果您没有确认，设备将恢复到以前的 AXIS OS 版本。

AXIS OS 回滚：恢复为先前安装的 AXIS OS 版本。

故障排查

Reset PTR（重置 PTR）：如果由于某种原因 Pan（水平转动）、Tilt（垂直转动）**或** Roll（滚转）**设置无法按预期工作，则重置**PTR。始终在新摄像机中校准 PTR 电机。但是，如果摄像机断电或电机被手动移除，则可能会丢失校准。重置 PTR 时，摄像机将重新校准，并返回到其出厂默认位置。

Calibration（校准）：单击 **Calibrate（校准）**可重新校准水平转动、垂直转动和滚动电机至它们默认的位置。

Ping：要检查设备是否能到达特定地址，请输入要 Ping 的主机名或 IP 地址，然后单击**开始**。

端口检查：要验证设备与特定 IP 地址和 TCP/UDP 端口的连接性，请输入要检查的主机名或 IP 地址和端口编号，然后单击**开始**。

网络追踪

重要

网络跟踪文件可能包含敏感信息，例如证书或密码。

通过记录网络上的活动，网络追踪文件可帮助您排除问题。

跟踪时间：选择以秒或分钟为单位的跟踪持续时间，并单击**下载**。

了解更多

调色板

为了帮助人眼区分热图像中的细节，可以将调色板应用于图像。调色板中的颜色是人工创建的假色，用于强调温度差异。

此产品有多个调色板可供选择。如果操作员观看视频流，您可以随意选择调色板。如果视频流仅由应用程序使用，请选择白热成像调色板。

隐私遮罩

隐私遮罩是覆盖部分监视区域的用户定义区域。在视频流中，隐私遮罩显示为纯色块或使用马赛克图案。

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。

视频流指示器是另一种类型的叠加。它显示实时视野视频流是实时的。

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

注意

为了确保支持 Opus 音频编解码器，始终通过 RTP 发送 Motion JPEG 流。

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，但是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。

H.265 或 MPEG–H Part 2/HEVC

与 H.264 标准相比，H.265 可将数字视频文件的大小减少 25% 以上。

注意

- H.265 是一种许可制技术。Axis 产品包括一个 H.265 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。
- 大多数网页浏览器不支持 H.265 的解码，因此这款摄像机在其网页界面中不支持这种情况。相反，您可以使用支持 H.265 解码的视频管理系统或应用程序。

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。

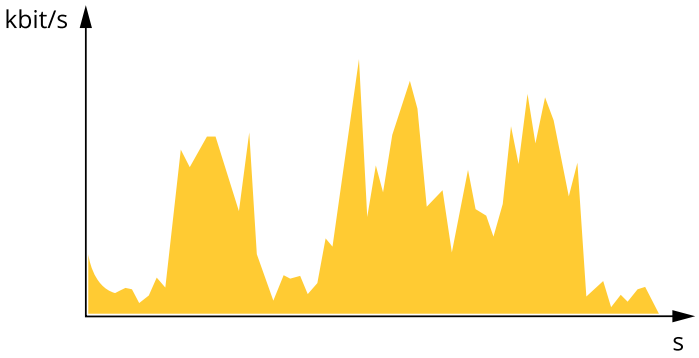
流选项卡包含视频流的设置。如果您从产品请求视频流，但未指定示例分辨率或帧率，则可获得这些设置。当您更改**流**选项卡中的设置时，它不会影响正在进行的流，但它将在开始新流时生效。

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。

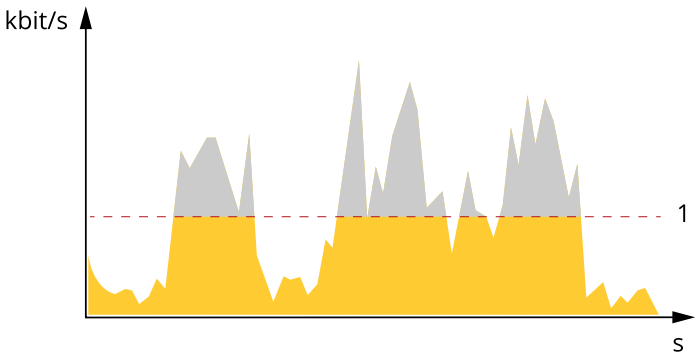
比特率控制

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，但您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。

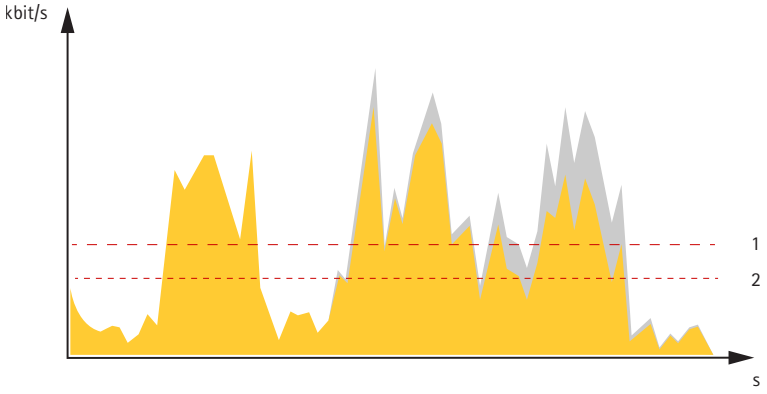


1 目标比特率

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。这样，您就可以满足指定目标，并根据可用存储提供更佳的视频质量。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

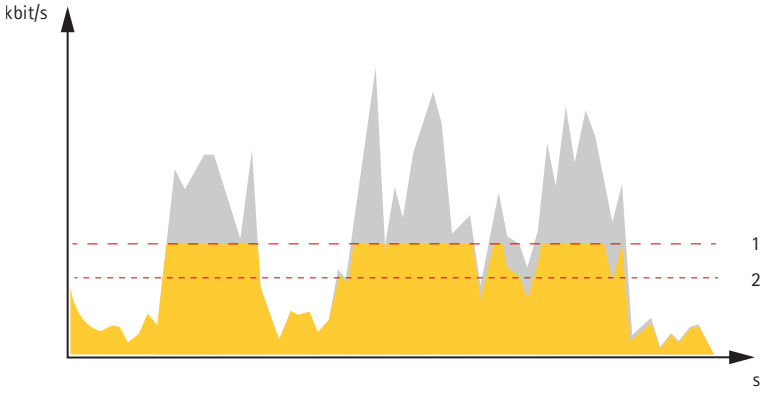
动的场景中，如果您使用平均比特率选项，那么您更有可能获得更高的图像质量。当调整图像质量以满足指定的目标比特率时，您可以定义存储视频流所需的总存储量（保留时间）。以下列方式之一指定平均比特率设置：

- 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

边缘到边缘技术

从边缘到边缘是一种使 IP 设备直接相互通信的技术。例如，Axis 摄像机和 Axis 音频或雷达产品等之间提供了智能配对功能。

有关该技术的更多信息，请转到 *axis.com/learning/white-papers* 并查看白皮书“边缘到边缘”。

扬声器配对

边缘到边缘扬声器配对，可使您能够使用兼容的 Axis 网络扬声器，就如同它是摄像机的一部分。配对后，扬声器的功能将集成到摄像机的网页界面中，网络扬声器可用作音频输出设备，您可以在其中播放音频剪辑并通过摄像机传输声音。

摄像机会向 VMS 识别自己为具有集成音频输出的摄像机，并将所播放的音频重定向到扬声器。

应用

借助应用，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 应用程序的用户手册，请转到 *help.axis.com*。

注意

- 多个应用程序可以同时运行，但某些应用程序可能无法彼此兼容。在并行运行时，某些应用程序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。

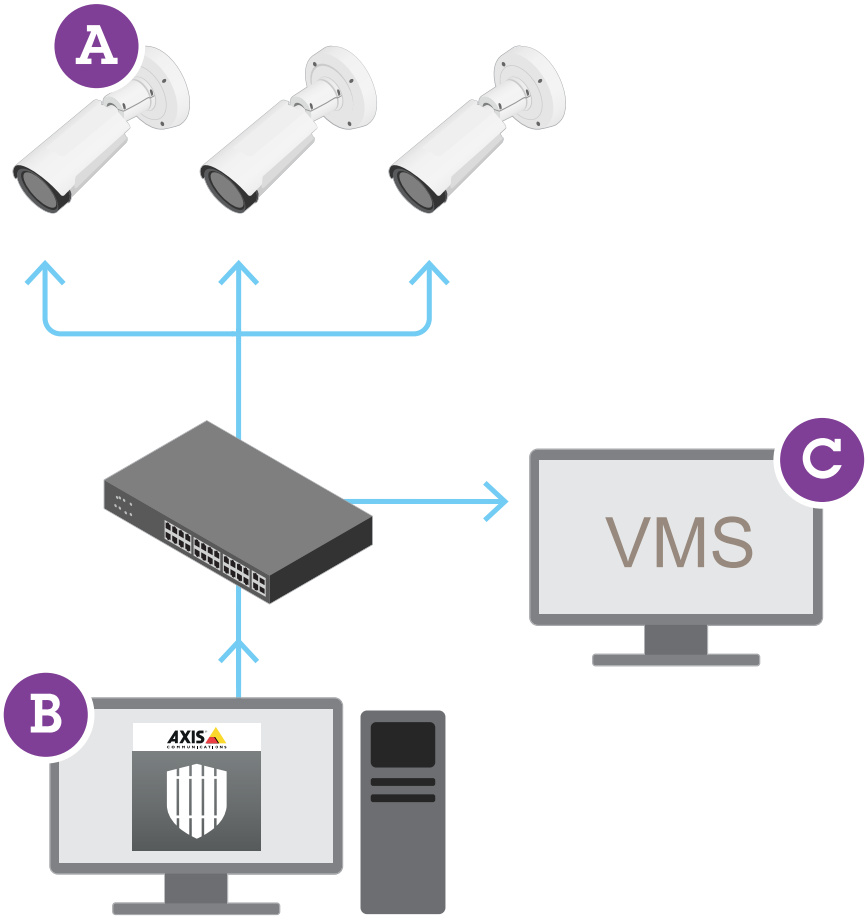
AXIS Perimeter Defender

AXIS Perimeter Defender是用于周界监控和保护的应用程序。它很适用于高度安全的周界保护，其需要增强具有可靠入侵侦测功能的物理访问控制系统。

AXIS Perimeter Defender 主要是针对所谓的无菌区域保护而设计，例如，沿标记边界的围栏进行监控。术语“无菌区域”是指不应该有人进入的区域。

在室外环境中使用 AXIS Perimeter Defender 可以：

- 侦测移动的人。
- 侦测移动的车辆，不区分车辆类型。



这款摄像机可在校准模式、人工智能模式或两种模式相结合的情况下运行该应用程序。如果选择仅在人工智能模式下运行，摄像机安装更灵活，无需校准摄像机。

AXIS Perimeter Defender 包括一个桌面界面 (B)，您可从中在摄像机 (A) 上安装和设置应用程序。然后，您可以将系统配置为向视频管理软件 (C) 发送警报。

AXIS Perimeter Defender PTZ Autotracking是AXIS Perimeter Defender应用程序的一个插件，使用相同的桌面界面。借助此插件，您可以将固定视觉摄像机或热成像摄像机与 Axis Q-line PTZ 摄像

机配对。之后，您可以通过固定摄像机维护场景的连续侦测覆盖范围，PTZ 摄像机可以自动跟踪侦测到的物体并为您提供侦测到的物体的近景视图。

重要

AXIS Perimeter Defender PTZ Autotracking 需要对固定摄像机和 PTZ 摄像机进行校准。

AXIS Perimeter Defender 提供以下类型的侦测场景：

- Intrusion（入侵）：当有人或车辆进入地面界定区域（从不同的方向，以各种轨迹）时，会触发警报。
- Loitering（徘徊）：当有人或车辆在地面上定义的区域内停留的时间超过预定义的秒数时，触发警报。
- Zone-crossing（穿越区域）：当有人或车辆以指定顺序经过地面上定义的两个或多个区域时，触发警报。
- Conditional（条件）：当有人或车辆进入地面上定义的区域，而没有先经过地面上定义的另一个或多个区域时，触发警报。

网络安全

有关网络安全的产品特定信息，请参阅Axis.com上该产品的数据表。

有关AXIS OS网络安全的深度信息，请阅读*AXIS OS强化配置指南* 。

Axis Edge Vault

Axis Edge Vault为保障安讯士设备安全提供了基于硬件的网络安全平台。它有保证设备的身份和完整性的功能，并保护您的敏感信息免遭未授权访问。它依托加密计算模块（安全元素和TPM）和SoC安全（TEE和安全启动）的强大基础，与前端设备安全的相关专业知识相结合。

签名OS

已签名的操作系统由软件供应商实施，并使用私钥对 AXIS OS 映像进行签名。将签名附加到操作系统后，设备将在安装软件之前对其进行验证。如果设备侦测到软件完整性受损，AXIS OS 升级将被拒绝。

安全启动

安全启动是一种由加密验证软件的完整链组成的启动过程，始于不可变的内存（启动ROM）。安全启动基于签名操作系统的使用，可确保设备仅能使用已授权的软件启动。

安全密钥库

一个防篡改保护的环境，可保护私钥并安全执行加密操作。在存在安全漏洞的情况下，它可防止非法访问和恶意提取。根据安全要求，安讯士设备可配备一个或多个基于硬件的加密计算模块，用于提供硬件保护型安全密钥库。根据安全要求，一个 Axis 设备可拥有一个或多个基于硬件的加密计算模块，如 TPM 2.0（受信任的平台模块）或安全元素，以及/或用于提供硬件保护安全密钥库的 TEEE 型（受信任执行环境）。此外，所选的 Axis 产品具有一种 FIPS 140-2 2 级认证的安全密钥库。

安讯士设备ID

能够验证设备来源是建立设备身份信任的关键。在生产期间，配备 AXIS Edge Vault 的设备被分配到具有唯一性、由工厂预置且符合 IEEE 802.1AR 标准的安讯士设备 ID 证书。其原理与护照相似，旨在证明设备来源。设备ID作为经安讯士根证书签名的证书，安全且永久存储在安全密钥库中。客户的 IT 基础设施可以利用设备 ID 实现自动安全设备板载和安全设备确认

签名视频

签名视频能够在无需证明视频文件保管链的情况下，证实视频证据未遭到篡改。摄像机使用安全地存储在安全密钥库中的唯一签名密钥将签名添加到视频流中。播放视频时，文件播放器将显示视频是否完好。签名视频让视频追溯可达摄像机源头，并确定视频在离开摄像机后未遭到篡改。

加密文件系统

安全密钥库可通过对文件系统实施强效加密，以防止恶意信息提取和配置篡改。这可确保在设备未使用、实现对设备的未授权访问和/或 Axis 设备被盗时，无法提取或篡改存储在文件系统中的数据。在安全启动过程中，可对读/写文件系统进行解密，并可将其安装并供 Axis 设备使用。

要了解有关 Axis 设备中网络安全功能的更多信息，请转到 *axis.com/learning/white-papers* 并搜索网络安全。

Axis 安全通知服务

Axis 提供通知服务，其中包含有关漏洞以及适用于 Axis 设备的其他安全相关事项的信息。要接收通知，您可以在 *axis.com/security-notification-service* 订阅。

漏洞管理

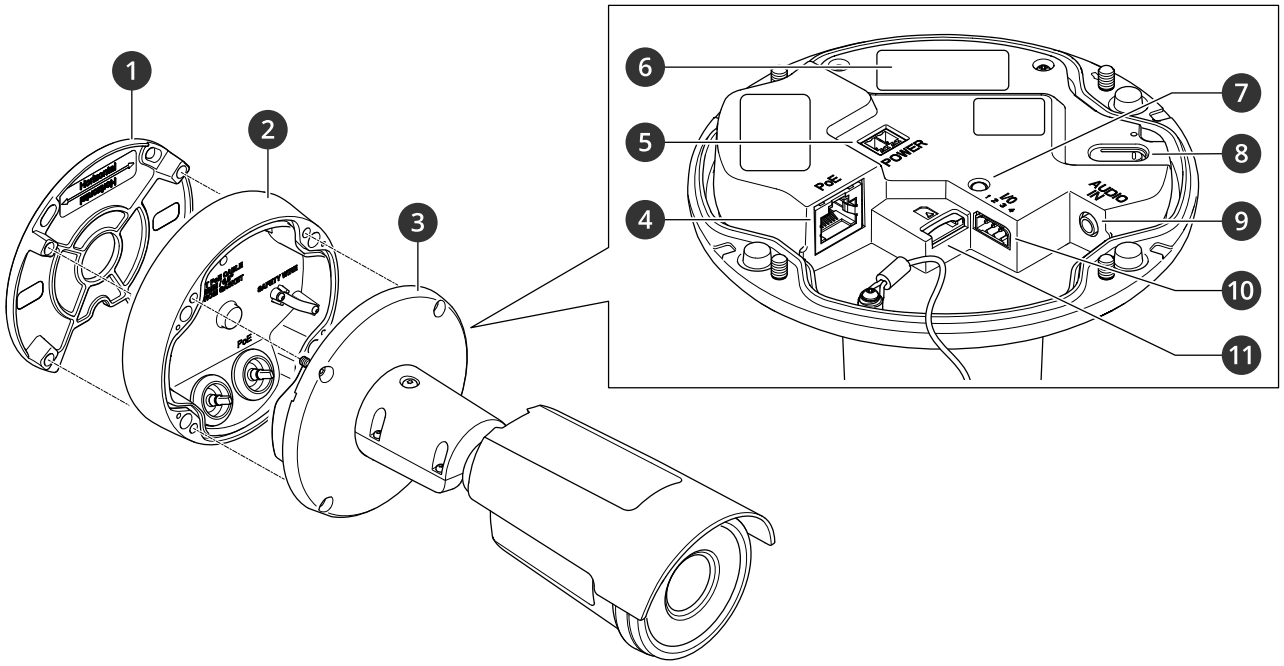
为了尽可能降低客户曝光风险、安讯士作为**常见漏洞和曝光 (CVE) 编号颁发机构 (CNA)**），遵循行业标准来管理和响应我们的设备、软件和服务中发现的漏洞。有关 Axis 漏洞管理策略、如何报告安全漏洞、已披露漏洞以及相应安全通报的更多信息，请参见 *axis.com/vulnerability-management* 。

Axis 设备的安全操作

带有出厂默认设置的 Axis 设备预配置了安全默认保护机制。我们建议您在安装设备时使用更多安全配置。要了解有关 Axis 强化指南以及其他网络安全相关文档的更多信息，请转到 *axis.com/support/cybersecurity/resources* 。

规格

产品概述



1 安装支架
2 连接盖
3 摄像机装置
4 网络连接器 (PoE)
5 电源连接器
6 零件号 (P/N) 和序列号 (S/N)
7 状态 LED 指示灯
8 控制按钮
9 音频连接器
10 I/O 连接器
11 SD 存储卡插槽

LED 指示灯

状态LED	指示
熄灭	连接和正常工作。
绿色	连接和正常工作。
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。
红色	设备软件升级失败。

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 microSD/microSDHC/microSDXC 卡。

有关 SD 卡的建议，请参见 *axis.com*。

microSD、microSDHC 和 microSDXC 徽标是 SD–3C LLC 的商标。microSD、microSDHC、microSDXC 是 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 。
- 通过互联网连接到一键云连接 (O3C) 服务。若要连接，请按住该按钮约 3 秒，直到 LED 状态指示灯呈绿色闪烁。

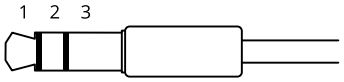
连接器

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

- **音频输入** – 3.5 毫米输入，用于数字麦克风、模拟单声道麦克风或线路输入单声道信号（左声道用于立体声信号）。



音频输入

1 尖部	2 中间环	3 尾段
非平衡麦克风（带/不带电子电源）或线路输入	可选择电子电源	接地
数字信号	可选择环形电源	接地

连接时使用外部麦克风。

I/O 连接器

使用 I/O 连接器连接外部设备，并结合应用移动侦测、事件触发和报警通知等功能。除 0 VDC 参考点和电源（12 V DC 输出）外，I/O 连接器还提供连接至以下模块的接口：

数字输入 – 用于连接可在开路和闭路之间切换的设备，例如 PIR 传感器、门/窗磁和玻璃破碎侦测器。

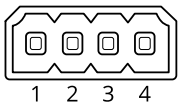
监控输入 – 能够侦测对数字输入进行的篡改。

数字输出 – 用于连接继电器和 LED 等外部设备。已连接的设备可由 VAPIX® 应用程序编程接口、通过事件或从设备网页接口进行激活。

注意

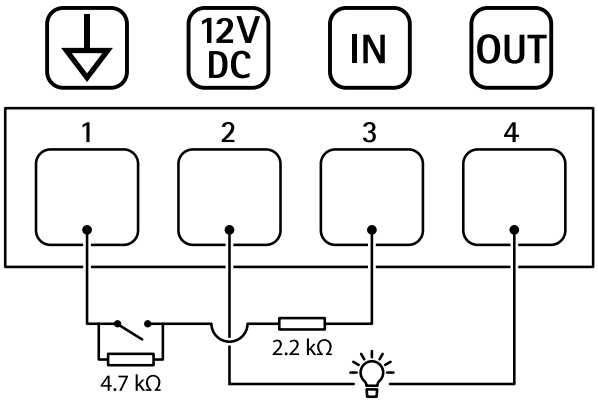
I/O 连接器在交货时已连接到护罩（风扇/加热器）。在风扇或加热器出现故障的情况下，将在摄像机中触发输入信号。在摄像机中设置操作规则，以配置信号将触发的操作。

4 针接线端子



功能	针脚	注意	规格
DC 接地	1		0 VDC
DC 输出	2	可用于为辅助设备供电。 注意：此针只能用作电源输出。	12 VDC 最大负载 = 25 mA
数字输入或监控输入	3	连接至针脚 1 以启用，或保留浮动状态（断开连接）以停用。要使用监控输入，则安装线尾电阻器。有关如何连接电阻器的信息，请参见连接图。	0 至最大 30 VDC
数字输出	4	启用时内部连接至针 1（DC 接地），停用时保留浮动状态（断开连接）。如果与电感负载（如继电器）一起使用，则将二极管与负载并联连接，以防止电压瞬变。	0 至最大 30 VDC，开漏，100 mA

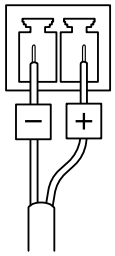
示例：



1 DC 接地
2 DC 输出 12 V，最大 25 mA
3 监控输入
4 数字输出

电源连接器

用于 DC 电源输入的双针脚接线盒。使用额定输出功率限制为≤100 W或额定输出电流限制为≤5 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。
- 请勿将洗涤剂直接喷洒在设备上。相反，在非研磨性布上喷洒洗涤剂并用它来清洁设备。
- 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. 为避免污渍，请用干净的非研磨性布擦干设备。

故障排除

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。请参见 。
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 可根据主动跟踪或长期支持 (LTS) 跟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 Axis 端到端系统产品，则建议使用主动跟踪中的 AXIS OS。如果您使用第三方集成，则建议使用 LTS 跟踪，其未针对主动跟踪进行连续验证。使用 LTS，产品可维持网络安全，而无需引入重大功能性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. 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 Axis 设备。运行 Ping 命令（在 Command/DOS 窗口中，键入 `ping` 和设备的 IP 地址）： • 如果收到消息：`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。 • 如果收到消息：`Request timed out`，这意味着该 IP 地址可用于此 Axis 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 Axis 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`。 如果根账户的密码丢失，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 AXIS 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 Axis 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 Axis 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。
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。 • 每秒的帧数上限取决于 Axis 设备的使用频率 (60/50 Hz)。
无法在实时浏览中选择 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。

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。

以下因素是重要的考虑因素：

- 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 用户或单播 H.264/H.265/AV1 用户访问会影响带宽。
- 不同用户同时查看不同流（分辨率、压缩率）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。
- 使用调色板会影响产品的 CPU 负载，从而影响帧速。

联系支持人员

如果您需要更多帮助，请转到 *axis.com/support*。

T10209446_zh

2025-02 (M4.2)