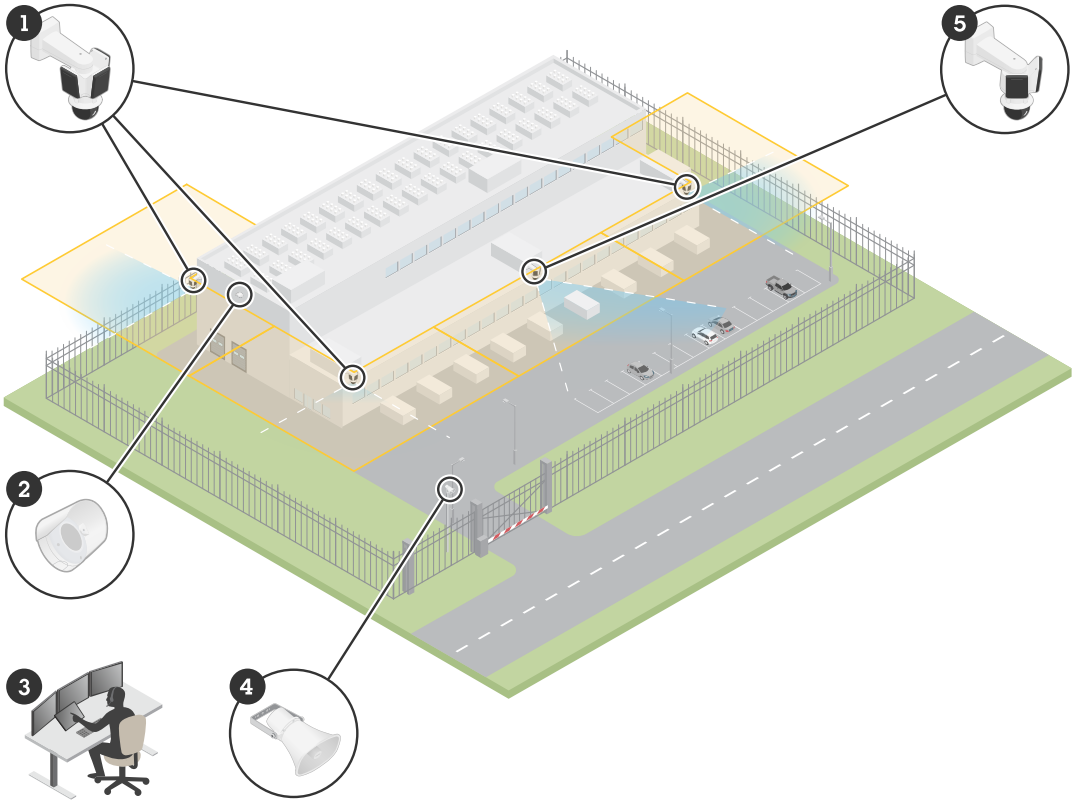
AXIS D21-VE Radar 系列

AXIS D2122-VE Radar
AXIS D2123-VE Radar

用户手册

目录

解决方案概述



数据中心监控解决方案的示例。

1 *AXIS D2123–VE Radar 与 AXIS Q6358–LE PTZ 摄像机配对*
2 *AXIS D4200–VE Strobe speaker*
3 *监控中心*
4 *AXIS C1310–E horn speaker*
5 *AXIS D2122–VE Radar 与 AXIS Q6358–LE PTZ 摄像机配对*

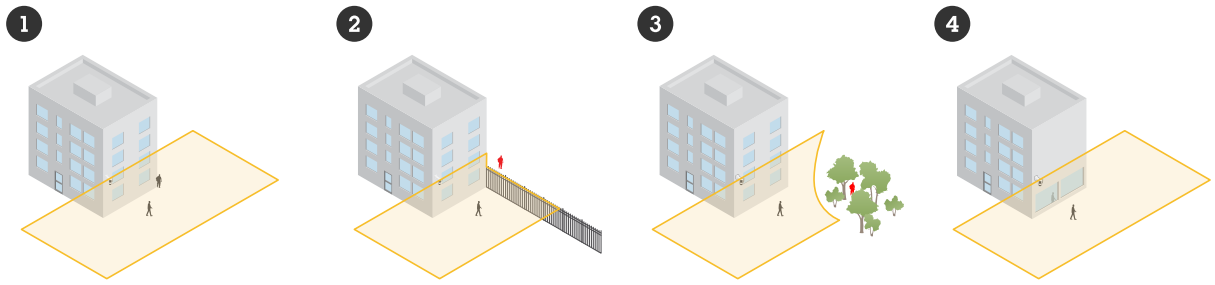
安装

要观看此视频，请转到本文档的网页版本。

本视频演示了如何安装 AXIS D21–VE Radar 系列。有关大多数安装场景的说明及安全信息，请参见安装指南。

注意事项

- 雷达用于监控开阔区域 (1)。场景中不同类型的固体目标（如墙壁、围栏、树木或大型灌木）都会在其后方创建盲区，即所谓的雷达阴影 (2, 3)。安装高度影响雷达阴影的大小。
- 对于更复杂的场景（例如存在反射表面时），我们建议采用雷达视频融合技术，并搭配选择的 PTZ 摄像机。
- 雷达在地面覆盖有沥青等铺装表面时效果更佳。当地面覆盖砾石或草坪时，侦测性能可能会受到影响。
- 若将雷达安装在墙面上，请保障雷达左右一米（三英尺）范围内无其他目标或装置。此类目标可反射无线电波，从而影响雷达的性能。
- 若将雷达安装在立杆上，请保障立杆足够稳固。该雷达配备可启用的稳定机制，但启用后可能影响雷达灵敏度或侦测移动目标所需的时间。
- 场景中的金属物体或反射表面可能反射在其附近移动的人员或车辆，从而产生反射雷达轨迹或虚假轨迹 (4)。这会影响雷达进行相对精确分类的能力，并导致假警报。您可以使用排除区域来过滤掉此类反射。若将摄像机与雷达配对，也可尽可能减少反射的影响。
- 建议安装高度详见 *axis.com* 上的设备数据表。

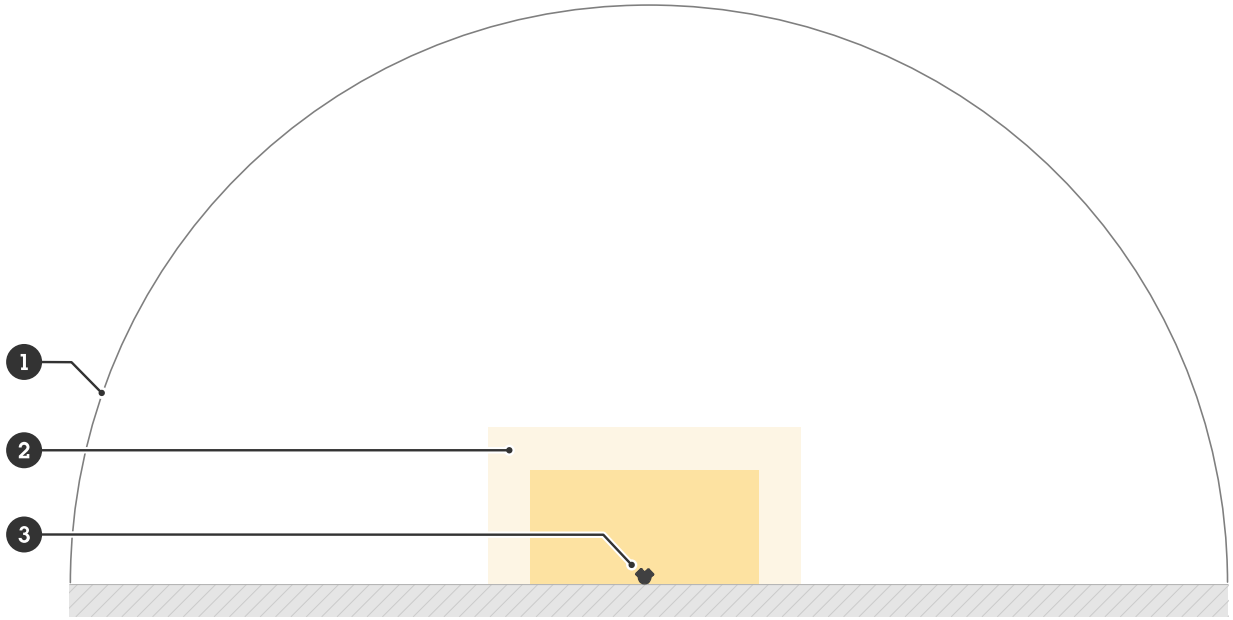


监视场景

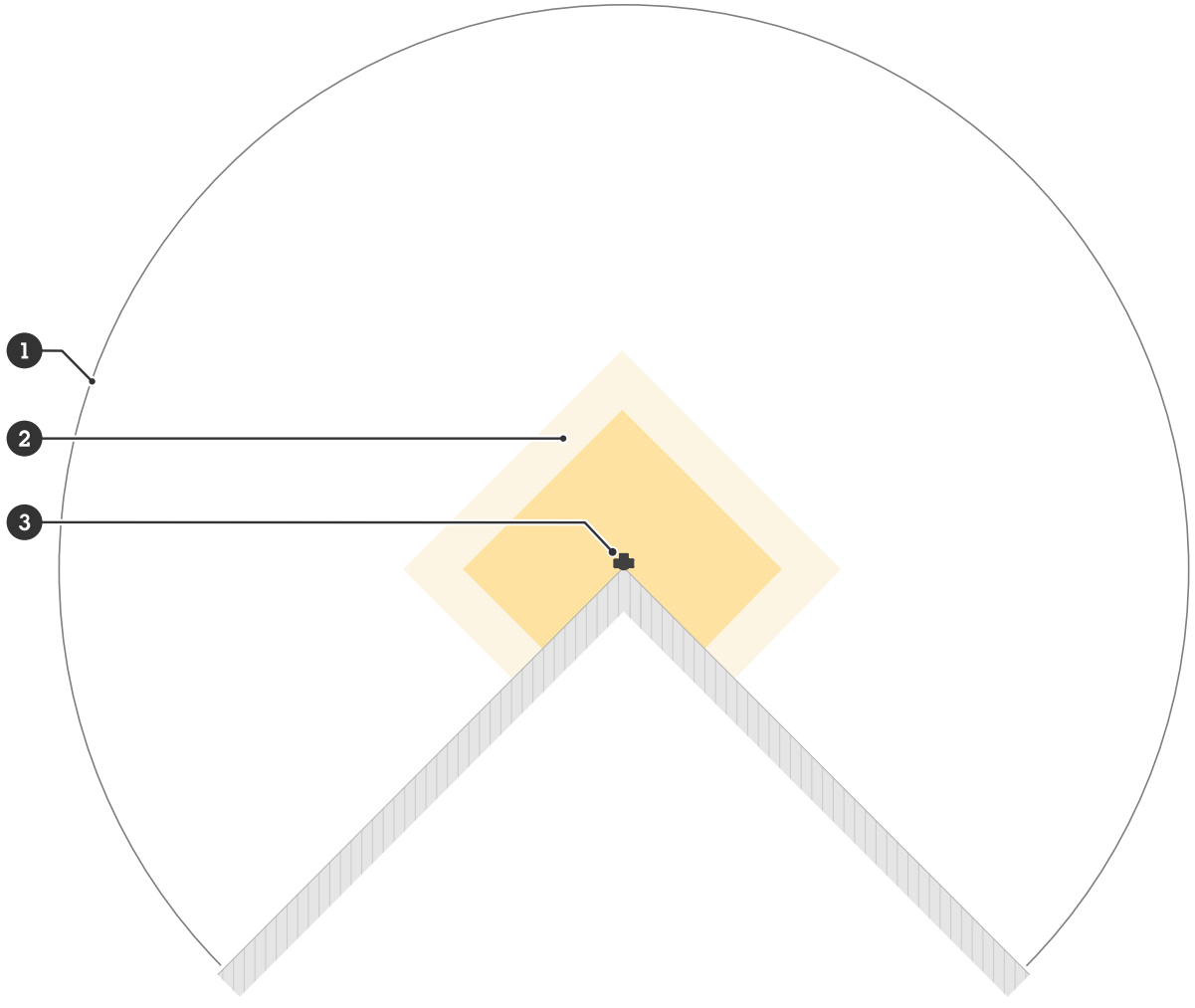
该雷达能够侦测移动目标，并将其分类为人、车辆或未知目标。监视区域时，请使用**区域监控**配置文件。

安装多个雷达

要监视建筑物周围或围栏外的缓冲区等区域，可将多个雷达安装在相邻位置。每个雷达可在半径 500 米（1640 英尺）范围内与最多 11 个其他 AXIS D2122–VE 或 AXIS D2123–VE 雷达共存，从而构成共存区。您也可以将此雷达型号安装在之前 Axis 雷达型号的共存区内，因为它们彼此之间不会产生干扰。有关共存区的详细信息，请参见 *共存区, on page 62*。



1 共存区
2 侦测区域
3 Axis D2122–VE Radar



1 共存区

2 侦测区域
3 Axis D2123–VE Radar

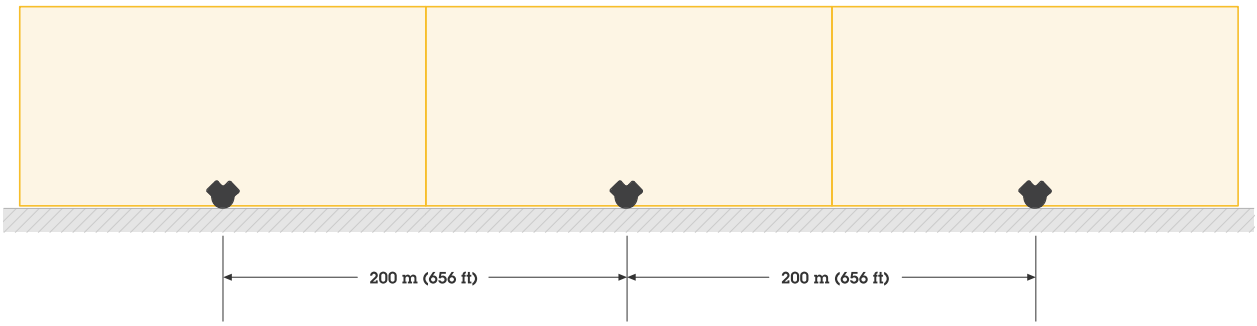
注意

共存区域中雷达的性能可能受环境和雷达相对围栏、建筑物或相邻雷达的方向的影响。

安装示例

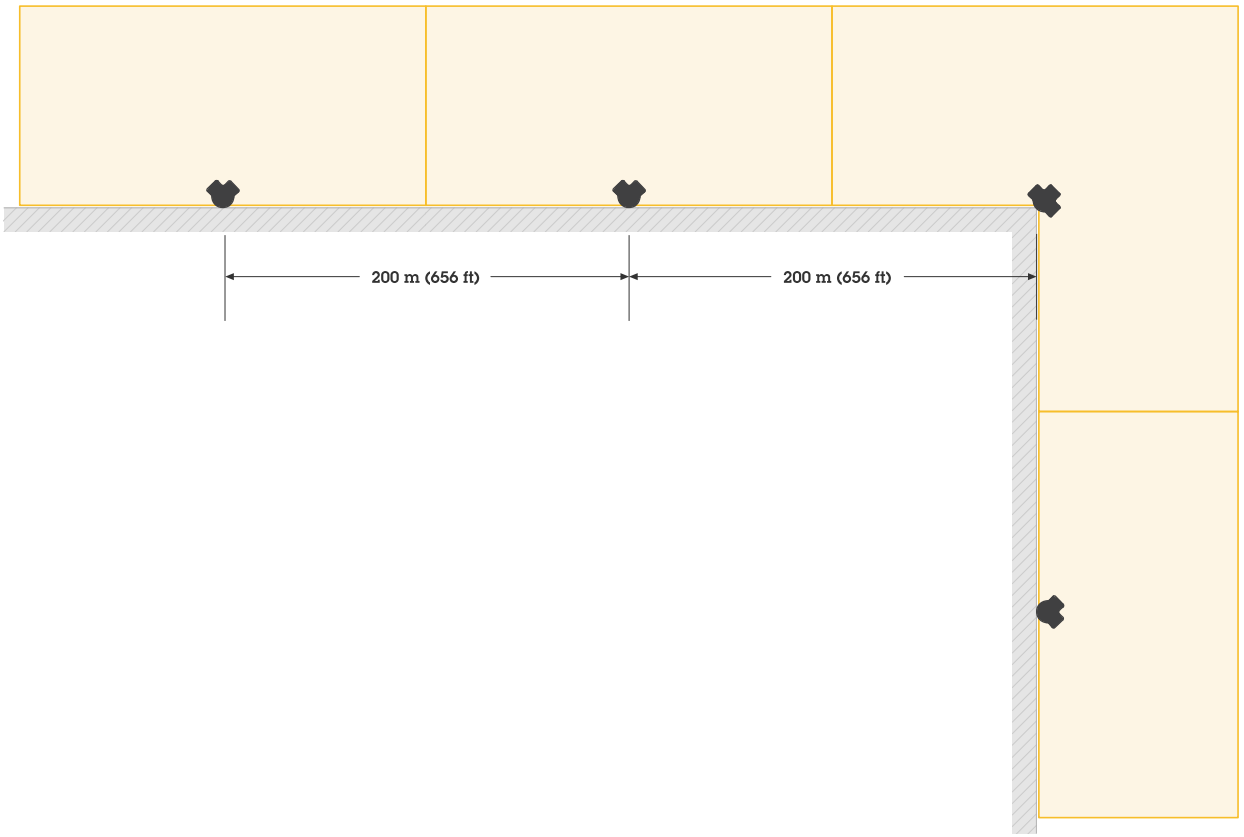
使用多个雷达创建虚拟围栏

要沿建筑物创建虚拟围栏，应并排放置多个雷达。我们建议雷达之间保持 200 米（656 英尺）的间距。



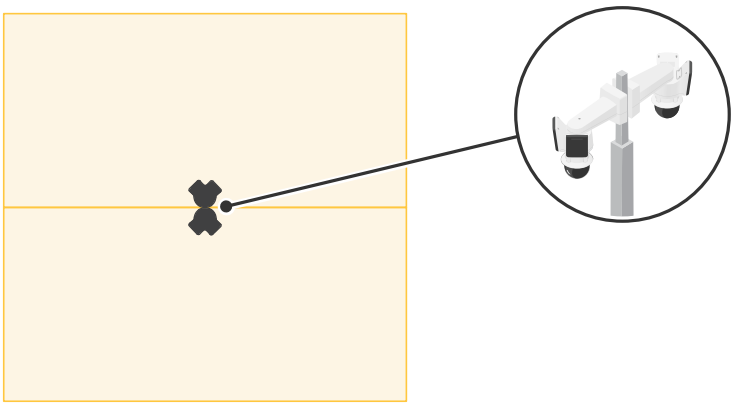
覆盖建筑物周围区域

要监视建筑物周围区域，请将雷达放在建筑物对外的墙上。



覆盖开放区域

要监视一个较大的开放区域，请使用两个立杆托架将两个 AXIS D2122–VE Radar 背靠背安装。

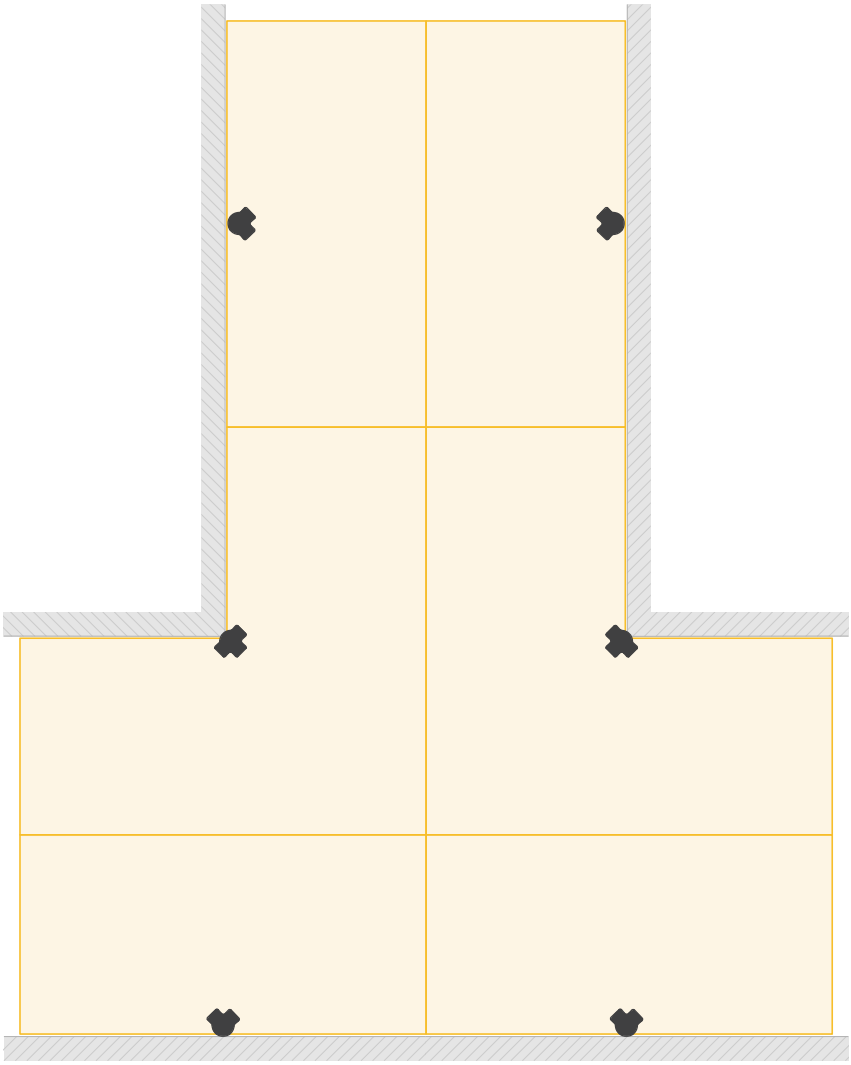


注意

当雷达由 90 瓦中跨设备供电时，每个雷达可提供高达 60 瓦的 PoE 输出功率。PoE 输出需符合以太网供电 IEEE 802.3bt 4 型 8 类。

安装彼此相对的多个雷达

要监视建筑物之间的区域，请将雷达设备彼此相对放置。在同一共存区内，最多可有 12 个雷达彼此相对放置。

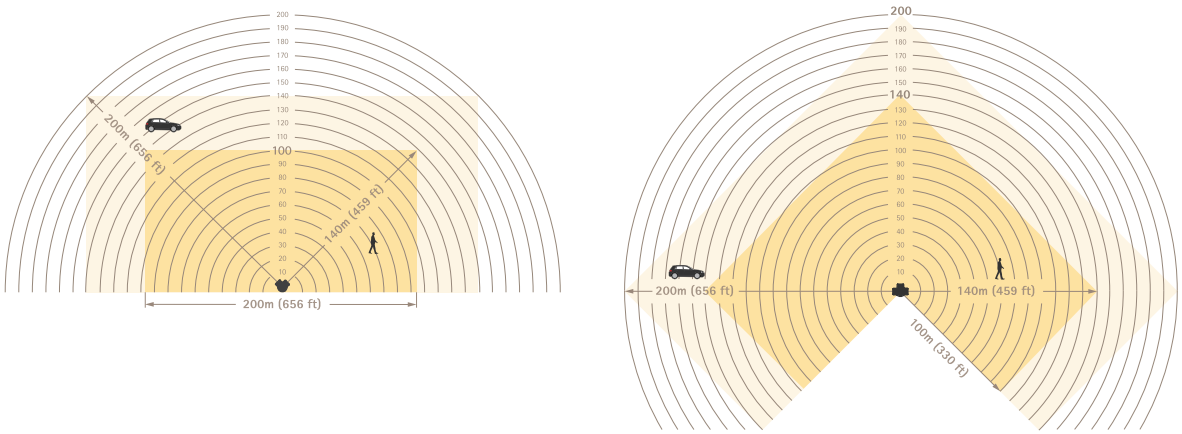


识别与侦测距离

在采用理想安装高度安装雷达时：

- 在识别区域内，您可侦测距离雷达 100 至 140 米（330 至 459 英尺）范围内的人并将其分类，具体距离取决于人相对于雷达的位置。
- 在侦测区域内，您可侦测距离雷达 140 至 200 米（459 至 656 英尺）范围内的车辆，具体取决于：
  - 车辆的速度
  - 车辆相对于雷达的方向
  - 地面的平坦度
  - 地面材料

有关该区域的详细信息，请参见 *识别与侦测区域, on page 62*。



识别与侦测距离

注意

- 校准雷达时，请在设备的网页界面中输入实际安装高度。
- 识别和侦测距离受场景影响。
- 不同目标类型的识别与侦测距离有所差异。

识别与侦测距离在以下条件下进行测量：

- 该距离是在平坦的水平地面上测量的。
- 该雷达安装时未进行垂直转动调整。
- 目标为身高 170 厘米（5 英尺 7 英寸）的人。
- 雷达拥有观测该人员的清晰视线。
- 雷达灵敏度设置为**中**。

雷达无法侦测距离小于侦测距离下限的目标。侦测距离下限取决于雷达的安装高度：

安装高度	**侦测距离下限**
4 米 （9.8 英尺）	4 米 （9.8 英尺）
5 米 （16.4 英尺）	6 米 （19.7 英尺）
6 米 （19.7 英尺）	8 米 （26英尺）

7 米 （ 23英尺 ）	11 米 （ 36英尺 ）
8 米 （ 26英尺 ）	13 米 （ 42.7 英尺 ）
9 米 （ 29.5 英尺 ）	15 米 （ 49.2 英尺 ）
10 米 （ 32.8.5 英尺 ）	18 米 （ 59英尺 ）

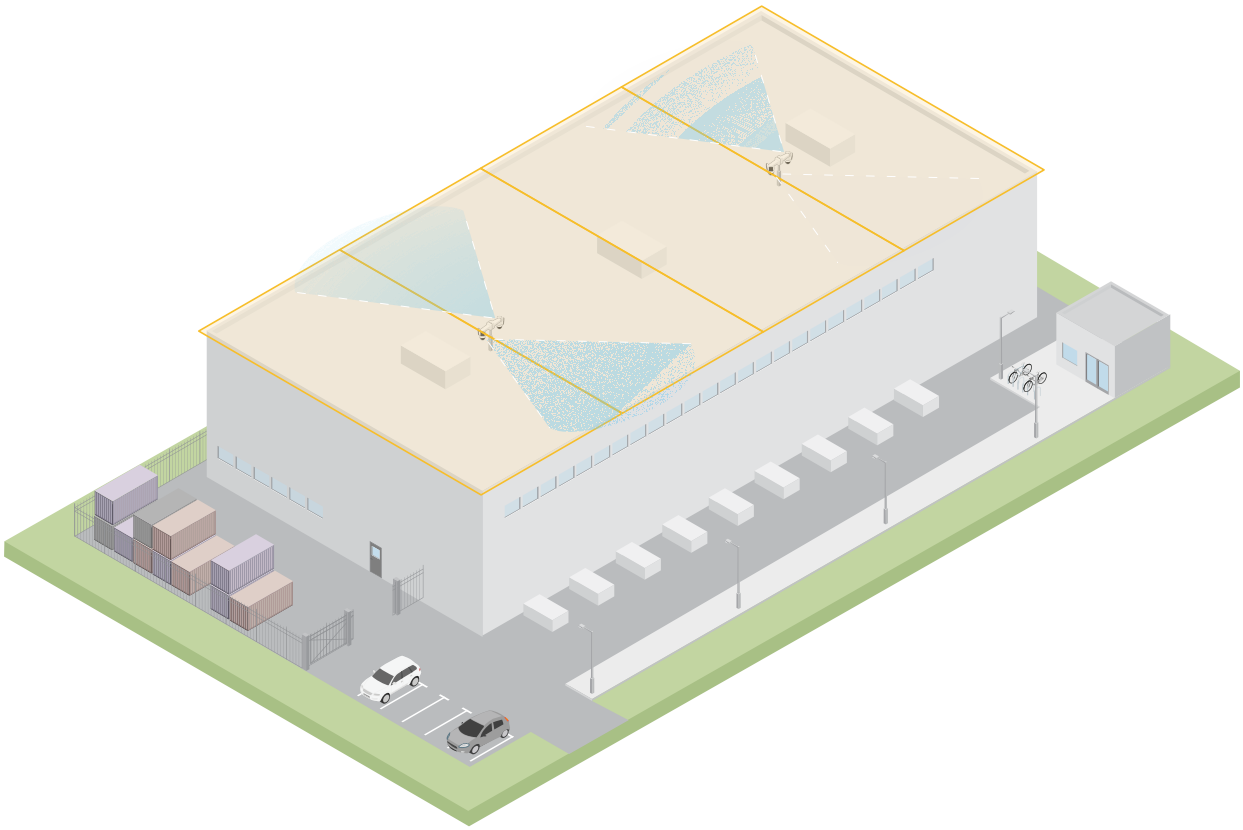
注意

将雷达与 PTZ 摄像机配对时，即使在雷达的侦测距离下限内，摄像机仍能持续追踪目标。

用例

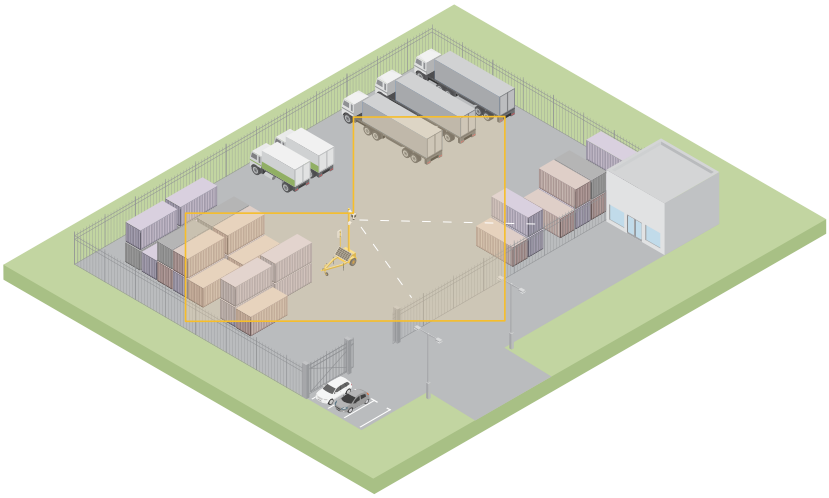
屋顶区域覆盖

某大型配送中心希望利用雷达覆盖屋顶区域。雷达与 ARTPEC–9 PTZ 摄像机配对，背靠背安装在立杆上，覆盖整个屋顶。雷达探测到屋顶上的移动目标并将其分类，引导摄像机对准目标，并让摄像机验证分类结果。摄像机利用自动追踪持续追踪目标。



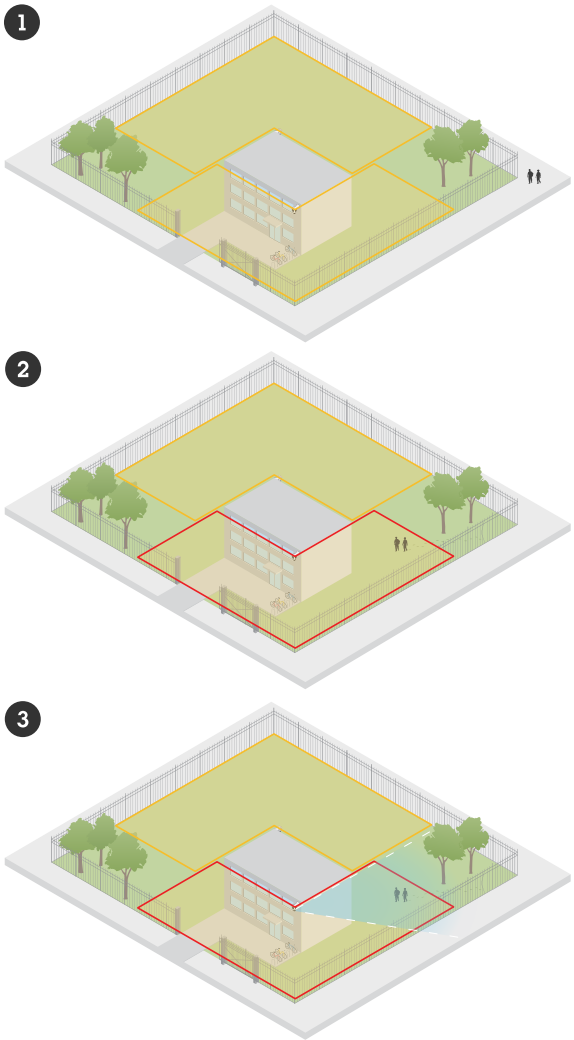
使用移动监控拖车覆盖大面积开放区域

一家五金店的户外庭院在营业时间结束后已发生数起盗窃事件。每次都有一名安保人员值班，但需要加强夜间的安保措施，而不会增加聘用更多员工成本。他们决定在移动监控拖车上背靠背安装两个雷达，以覆盖整个院区。雷达经配置可提醒当值安保人员有可疑行为，以便其能够调查场景。他们还考虑安装由雷达触发的频闪扬声器，以威慑入侵者。



覆盖有围栏的建筑物

在以下场景中，将 PTZ 摄像机与雷达配合使用，通过雷达视频融合技术实现报警验证并提供相对精确的分类。



1. 入侵者正在围栏外行走，未触发报警。
2. 入侵者翻越围栏闯入，雷达探测到他们并触发报警。
3. 雷达将 PTZ 摄像机转向入侵者，并通过视频分析功能让摄像机验证报警。

有关详细信息，请参见 *自动追踪, on page 63*。

开始使用

在网络上查找设备

若要在网络中查找安讯士设备并为它们分配 Windows® 中的 IP 地址，请使用 AXIS IP Utility 或 AXIS Device Manager。这两种应用程序都是免费的，可以从 *axis.com/support* 上下载。

有关如何查找和分配 IP 地址的更多信息，请转到*如何分配一个 IP 地址和访问您的设备*。

浏览器支持

您可以在以下浏览器中使用该设备：

	Chrome™	Edge™	Firefox®	Safari®
Windows®	✓	✓	*	*
macOS®	✓	✓	*	*
Linux®	✓	✓	*	*
其他操作系统	*	*	*	*

✓：建议

*：支持，但有限制

打开设备的网页界面

1. 打开一个浏览器，键入安讯士设备的 IP 地址或主机名。
   如果您不知道 IP 地址，请使用 AXIS IP Utility 或 AXIS Device Manager 在网络上查找设备。
2. 键入用户名和密码。如果是首次访问设备，则必须创建管理员帐户。请参见 *创建管理员帐户, on page 12*。

有关在设备的网页界面中控件和选项的说明，请参见 *网页界面, on page 20*。

创建管理员帐户

首次登录设备时，您必须创建管理员帐户。

1. 请输入用户名。
2. 输入密码。请参见 *安全密码, on page 12*。
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 *重置为出厂默认设置, on page 70*。

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。

配置设备

为充分利用您的设备，我们建议您执行以下步骤：

1. *设置安装高度, on page 14*
2. 若将多个雷达安装在彼此相邻的位置： *设置相邻雷达的数量, on page 14*
3. *添加地图供参考, on page 14*
4. *创建一个用于侦测目标的场景, on page 15*
5. *大幅度减少假警报, on page 16*
6. *验证您的安装, on page 16*

设置安装高度

在网页界面中设置雷达的安装高度。正确的安装高度对于雷达能够准确侦测并测量目标经过时的速度至关重要。自动追踪功能正常运行也至关重要。

尽可能准确地测量从地面到雷达的高度。对于表面不平整的场景，请设置代表场景中平均高度的值。

1. 转到**雷达 > 设置 > 常规**。
2. 在**安装高度**下设置高度。

设置相邻雷达的数量

若在该雷达的共存区内安装其他同型号雷达，请在每个雷达的网页界面中定义相邻雷达的数量。这样可提高雷达的性能，并尽可能降低干扰风险。

1. 转到**雷达 > 设置 > 共存**。
2. 选择该雷达共存区内相邻雷达的数量。

添加地图供参考

为便于设置场景并理解场景中目标的移动位置，可选择将地图作为雷达流的背景。您可以使用显示雷达覆盖区域的平面图或航拍照片。调整并校准地图，使雷达视图适配地图的位置、方向和比例，如果您对场景的特定部分感兴趣，还可以将地图放大。

您可以使用设置助手一步步完成地图校准，也可以单独编辑每个设置。

使用设置助手：

1. 转到**雷达 > 地图校准**。
2. 单击Setup assistant（**设置助手**）并按说明操作。

要删除上传的地图和您添加的设置，请单击Reset calibration（**重置校准**）。

单独编辑每个设置：

调整每个设置后，地图可逐渐校准。

1. 转到Radar（**雷达**）> Map calibration（**地图校准**）> Map（**地图**）。
2. 选择要上传的图像，或将其拖放到指定区域。
   要以当前水平转动和变焦缩放设置重新使用地图图像，请单击Download map（**下载地图**）。
3. 在Rotate map（**旋转地图**）下方，使用滑块将地图旋转到位。
4. 转到Scale and distance on a map（**地图上的比例尺和距离**），单击地图上的两个预定点。
5. 在Distance（**距离**）下，添加您添加到地图上的两点之间的实际距离。
6. 转到Pan and zoom map（**水平转动和变焦缩放地图**），使用按钮水平转动地图图像或放大、缩小地图图像。

注意

- 变焦缩放功能不会改变雷达视图。即使在变焦缩放后部分视图不可见，雷达仍能侦测整个视图范围内的移动目标。排除侦测到的移动情况的唯一方法是添加排除区域。
- 您可随时通过**地图校准**、**排除区域**或**场景**页面调整水平转动和变焦缩放功能，单击 即可操作。

7. 转到Radar position（**雷达位置**），使用按钮移动或旋转雷达在地图上的位置。

要删除上传的地图和您添加的设置，请单击Reset calibration（**重置校准**）。

视频举例显示了如何在安讯士雷达或雷达视频融合摄像机中校准参考地图。

创建一个用于侦测目标的场景

通过场景，您可以侦测或识别场景中移动的目标。要在场景条件满足时触发响应，请在**事件**中创建规则。您可以创建多个场景来侦测不同行为或覆盖场景的不同部分。

1. 转到**雷达 > 场景**。
2. 单击**添加场景**。
3. 键入场景的名称。
4. 如果您希望目标在区域中移动时或目标跨线时触发，请选择此选项。
5. 单击 Next（**下一步**）。
6. 对于**区域内移动**场景：
   6.1. 选择区域形状。
   使用鼠标来移动和调整区域，从而覆盖雷达视图或参考地图中所需的部分。
7. 对于**越线**场景：
   7.1. 在场景中定位线。
   使用鼠标移动和调整线条。
   7.2. 要更改侦测方向，请启用**更改方向**。
   7.3. 要使目标越过两条线才能触发响应，请打开**需要越过两条线**。
   在场景中定位第二条线。
8. 单击 Next（**下一步**）。
9. 添加侦测设置。
   9.1. 对于**区域内移动**场景和**越线**场景（一条线），请在**忽略短暂停留的目标**中添加延迟时间以尽可能减少假警报。
   9.2. 对于**越线**场景（两条线），请在**最大越线间隔时间**中设置越过第一条线与第二条线的间隔时间限制。
   9.3. 在**对象类型触发**下选择要触发的对象类型。
   9.4. 在**速度限制**下添加速度范围。
10. 单击 Next（**下一步**）。
11. 在**触发持续时间下限**下设置警报的下限持续时间。
    对于**越线**场景，如果希望使目标在越线时立即触发响应，请将持续时间降为 0 秒。
12. 单击 Save（**保存**）。

大幅度减少假警报

若频繁出现假警报，可尝试通过更改为不同设置来尽可能减少假警报。例如，您可以过滤掉特定类型的移动或目标，调整目标触发报警的区域，或调节侦测灵敏度。

- 调整雷达的侦测灵敏度：
  转到**雷达 > 设置 > 侦测** 并降低**侦测灵敏度**。
  灵敏度设置会影响大多数区域。
  - 当场景中存在大量金属物体或大型车辆时，较低的侦测灵敏度更为适用。这样可降低假警报的风险，但也削弱了雷达对小型目标的分别能力。
  - 更高的侦测灵敏度适用于没有金属物体的开阔场景，例如田野。
- 修改包含区域与排除区域：
  场景中的硬质表面可能产生反射，导致单个物理目标被多次侦测到。您可以调整场景中的包含区域形状，也可以添加通用排除区域来忽略场景的特定部分。
- 在目标跨越两条线（而非一条线）时触发：
  若在越线场景中存在摆动的目标或动物，则存在此类目标越线并触发假警报的风险。在这种情况下，您可以将场景调整为仅在目标跨越两条线时触发。
- 特定移动过滤：
  - 为尽可能减少场景中树木、灌木丛和旗帜引发的假警报，请转到**雷达 > 设置 > 侦测**，开启**忽略摆动的目标**。
  - 为尽可能减少场景中猫和兔子等小型目标引发的假警报，请转到**雷达 > 设置 > 侦测**，开启**忽略小型目标**。此设置可在区域监控配置文件中找到。
- 时间过滤：
  - 转到**雷达 > 场景**。
  - 选择一个场景，然后单击 ⋮ 修改其设置。
  - 增加**触发前秒数**。这是从雷达开始跟踪某个目标到其触发警报之间的延迟时间。当雷达侦测到目标时计时器开始计时（并非从目标进入场景中的包含区域时开始）。
- 按对象类型过滤：
  - 转到**雷达 > 场景**。
  - 选择一个场景，然后单击 ⋮ 修改其设置。
  - 要避免触发特定的目标类型，清除不会触发该场景警报的目标类型。

验证您的安装

验证雷达的安装

在开始使用雷达之前，我们建议您先验证安装是否正确。验证功能可帮助您识别安装过程中的问题，或管理场景中的静态目标（如树木或反射表面）。

注意

在验证时适用的条件下对安装进行验证。场景中的条件改变可能影响安装的日常性能。

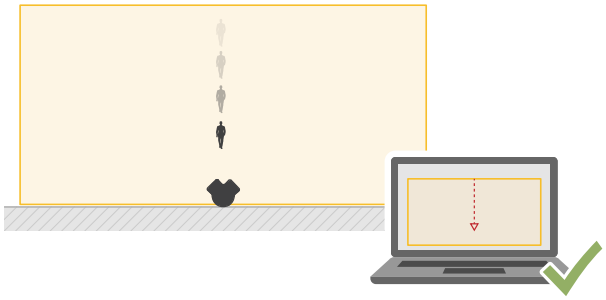
检查是否有误侦测

1. 检查识别区域内是否没有人员活动。
2. 请等待几分钟，保障雷达在识别区域内未侦测到不同静态目标。
3. 若出现不必要的侦测，您可以过滤掉特定类型的移动或目标，调整目标触发报警的区域，或调节侦测灵敏度。有关说明，请参见 *大幅度减少假警报, on page 16*。

检查符号、移动方向及地图上的位置是否正确。

1. 在雷达的网页界面中，开始录制。有关说明，请参见 *录制并观看视频, on page 18*。

2. 从识别区域外开始行走，并直接朝雷达方向前进。
3. 检查当人员进入识别区域时是否显示人体分类符号。
4. 检查雷达的网页界面是否显示了正确的移动方向。



5. 检查人员的实际位置是否与地图上的位置一致。

创建一个与以下表格类似的表，帮助您记录验证数据。

测试	通过/失败	备注
1.检查区域畅通无物时是否出现不想要的侦测。		
2.检查当人员进入识别区域时是否显示人体分类符号。		
3.检查移动方向是否正确。		
4.保障人员的实际位置与地图上的位置一致。		

完成验证

成功完成验证的第一部分后，请执行以下测试以完成验证过程。

1. 请确保您已根据说明配置了雷达。
2. 保障您已添加并校准了参考地图。
3. 设置雷达场景在侦测到人时触发。默认情况下，**触发前秒数**设置为两秒，但如果需要，您可以更改此设置。
4. 设置雷达以在侦测到适当的目标时录制视频。
   有关说明，请参见 *录制并观看视频, on page 18*。
5. 转到**雷达 > 设置 > 目标可视化**，将**轨迹寿命**设置为一小时，以使其安全地超过您离开座位、进入监控区域并返回到您的座位所需的时间。轨迹寿命将在雷达的实时视图中保持轨道的设置时间，在完成验证后，可以将其禁用。
6. 沿识别区域的边框进行遍历，保障系统上的尾随与您走进的路线相匹配。
7. 如果您对验证结果不满意，请重新校准参考图并重复验证。

调整雷达图像

本部分包括配置雷达图像的说明。如果您想要了解有关特定性能如何工作的更多信息，请转到 *了解更多, on page 62*。

显示图像叠加

您可在雷达流中叠加图片。

1. 转到**雷达 > 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 *流传输和存储, on page 63*。

录制并观看视频

直接从雷达录制视频

1. 转到**雷达 > 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。

了解更多信息，请参见*开始使用事件规则*。

触发操作

1. 转到**系统 > 事件**并添加响应规则。该规则可定义设备执行特定操作的时间。您可将规则设置为计划触发、定期触发或手动触发。
2. 输入一个**名称**。
3. 选择触发操作时必须满足的**条件**。如果为操作规则指定多个条件，则必须满足条件才能触发操作。
4. 选择在满足条件时应执行何种**操作**。

注意

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

激活雷达上的扫频红灯

您可以使用雷达前端的动态 LED 灯带来指示该区域受到监控。

此示例说明如何在工作日下班后激活扫频红灯。

创建一个时间表：

1. 转到**系统 > 事件 > 时间表**，然后添加一个时间表。
2. 键入时间表的名称，例如 `Weekday nights`。
3. 在**类型**下，选择**时间表**。
4. 在**重复**下，选择**每日**。
5. 将开始时间设为 06:00 PM。
6. 将结束时间设为 06:00 AM。
7. 在**日期**下，选择星期一至星期五。
8. 单击 **Save（保存）**。

创建一个规则：

1. 转到**系统 > 事件**并添加响应规则。
2. 键入规则的名称，例如 `Red sweeping light`。
3. 在条件列表中，在**计划和重复**下选择**计划**。
4. 在时间表列表中，选择**工作日夜晚**。
5. 在操作列表中，在**雷达**下，选择**动态 LED 灯带**。
6. 选择模式**扫频红色**。
7. 将持续时间设置为 12 小时。
8. 单击 **Save（保存）**。

如果有人用金属物体覆盖雷达，请发送电子邮件

此示例说明如何创建一个规则，该规则在有人用金属物体（如金属箔或金属板）覆盖雷达以篡改雷达时发送电子邮件通知。

添加电子邮件接受者：

1. 转到**系统 > 事件 > 接受者**，然后添加一个接受者。
2. 键入接受者的名称。
3. 在**类型**下，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. 根据您的电子邮件提供商填写其余信息。
   雷达设备没有自己的电子邮件服务器，因此需要登录到一个电子邮件服务器才能发送电子邮件。
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：

8. 转到**系统 > 事件**并添加响应规则。
9. 键入规则的名称，例如 `Tampering mail`。
10. 从条件列表中的**设备状态**下，选择**雷达数据故障**。
11. 在**原因**下，选择 **篡改**。
12. 在操作列表中，在**通知**下，选择**将通知发送到电子邮件**。
13. 选择您创建的收件人。
14. 键入电子邮件的主题和消息。
15. 单击 **Save（保存）**。

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

设备信息

显示设备相关信息，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安讯士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 *录像, on page 28*

显示保存录制内容的存储空间。

功率状态

显示电源状态信息，包括电流电源、平均功率和上限功率。

电源设置：查看和更新设备的电源设置。将前往可更改电源设置的电源设置页面。

雷达

设置

概述

无线电传输：用于完全关闭雷达模块。

通道：如果您遇到多个设备相互干扰的问题，请为最多四个彼此靠近的设备选择同一信道。对于大多数装置，选择**自动**让设备自动协商使用哪个信道。

安装高度：输入产品的安装高度。

注意

输入安装高度时尽可能具体。这有助于设备在图像中的正确位置可视化雷达侦测。

共存

邻近雷达的数量：选择在同一个共存区域内安装的邻近雷达的数量。这有助于避免干扰。

- **0–3**：如果您在同一个共存区域中安装一个到四个雷达，请选择此选项。
- **4–5**：如果您在同一个共存区域中安装五个到六个雷达，请选择此选项。
- **6–11**：如果您在同一个共存区域中安装七个到十二个雷达，请选择此选项。

侦测

侦测灵敏度：选择雷达的灵敏程度。值越高，侦测范围就越长，但出现假警报的风险也越高。较低的灵敏度将消除假警报的数量，但可能会缩短侦测范围。

雷达配置文件：选择适合您关注区域的配置文件。

- **区域监控**：以较低的速度在开放区域中移动大小目标。
  - **忽略静止的旋转对象**：打开此选项可尽可能地减少具有旋转运动的静止目标（如风扇或涡轮机）发出的误报。
  - **忽略小型目标**：打开以尽可能减少来自小型目标（如猫或兔子）的假警报。
  - **忽略摆动的目标**：打开以尽量减少摆动的目标（如树木、灌木丛或旗杆）发出的假警报。
  - **忽略未知目标**：打开以尽量减少因雷达无法进行分类的目标引发的假警报。
- **道路监控**：跟踪在市内区域和次级城市道路上以更高的速度移动的车辆
  - **忽略静止的旋转对象**：打开此选项可尽可能地减少具有旋转运动的静止目标（如风扇或涡轮机）发出的误报。
  - **忽略摆动的目标**：打开以尽量减少摆动的目标（如树木、灌木丛或旗杆）发出的假警报。
  - **忽略未知目标**：打开以尽量减少因雷达无法进行分类的目标引发的假警报。

查看

信息说明：打开以显示包含雷达可侦测和跟踪的目标类型的图例。拖放可移动信息图例。

区域透明度：选择覆盖区域应有的不透明或透明程度。

网格透明度：选择网格应有的不透明或透明程度。

颜色方案：为雷达可视化选择一个主题。

旋转：选择雷达图像的首选方向。

目标可视化

轨迹寿命：选择所跟踪的目标的轨迹在雷达视图中可见的时间。

图标风格：在雷达视图中选择所跟踪目标的图标样式。对于普通三角形，请选择 **三角形** 。对于代表符号，请选择**符号**。无论采用哪种样式，这些图标都将指向所跟踪目标移动的方向。

用图标显示信息：选择要显示在跟踪对象图标旁边的信息：
- **目标类型**：显示雷达检测到的目标类型。
- **分类概率**：显示雷达对目标分类是否正确的确定程度。
- **速度**：显示目标移动的快慢。

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。

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。

地图校准

使用地图校准上传和校准参考地图。校准的结果是一张参考地图，以适当的比例显示雷达覆盖范围，从而更容易看清目标移动的位置。

设置助手：单击可打开设置助手，引导您逐步完成校准。

重置校准：单击可删除当前地图图像和雷达在地图上的位置。

地图

上传地图：选择或拖放要上传的地图图像。

下载地图：单击可下载地图。

Rotate map（**旋转地图**）：使用滑块来旋转地图图像。

地图上的比例尺和距离

距离：添加您添加到地图上的两点之间的距离。

水平转动和变焦缩放地图

水平转动：单击按钮可水平转动地图图像。

变焦：单击按钮可变焦缩放地图图像。

重置水平转动和变焦缩放：单击可移除水平转动和变焦缩放设置。

雷达位置

位置：单击按钮在地图上移动雷达。

旋转：单击按钮在地图上旋转雷达。

排除区域

排除区域是忽略移动目标的区域。如果场景内存在触发大量不必要的警报的区域，请使用排除区域。

 ：单击以创建新的排除区域。

要修改排除区域，请在列表中选择它。

跟踪正在通过的对象：打开以跟踪穿过排除区域的目标。经过的对象会保留其轨迹 ID，并且在整个区域中可见。将不会跟踪从排除区域内显示的目标。

区域形状预设：选择排除区域的初始形状。

- **覆盖全部**：选择以设置覆盖整个雷达覆盖区域的排除区域。
- **重置为方框**：选择以在覆盖区域的中间放置一个矩形排除区域。

要修改区域形状，请拖放这些线上的点。要删除点，请在其上单击鼠标右键。

场景

场景是触发条件以及场景和检测设置的组合。

＋：单击以创建新方案。您可以创建多达 20 个场景。

触发条件：选择将会触发警报的条件。
- **区域内移动**：如果您希望场景在目标在区域中移动时触发，请选择此选项。
- **越线**：如果您希望场景在目标跨越一条或两条线时触发，请选择此项。

场景：在移动目标将触发报警的场景中，定义区域或线。
- 对于**区域内移动**，选择一个形状预设以修改区域。
- 对于**越线**，请将该行拖放到场景中。要在线上创建更多点，请单击并拖动线上的任一位置。要删除点，请在其上单击鼠标右键。
  - **需要跨越两条线**：在触发警报前，如果目标必须跨越两条线，请打开。
  - **更改方向**：如果您希望场景在目标沿其他方向跨越线时处触发警报，请打开此项。

侦测设置：定义场景的触发条件。
- 对于**区域内移动**：
  - **忽略短暂停留的目标**：设置从雷达侦测到场景触发警报时的时间间隔（以秒为单位）。这有助于减少假警报。
  - **按对象类型触发**：选择希望场景触发的目标类型(人、车辆、位置)。
  - **速度限制**：以特定范围内的速度移动的目标触发。
    - **翻转**：选择要在设置速度限制的上方和下方触发速度。
- 对于**越线**：
  - **忽略短暂停留的目标**：设置从雷达侦测到场景触发操作时的时间间隔（以秒为单位）。这有助于减少假警报。此选项不适用于跨越两条线的目标。
  - **跨越两条线之间的时间上限**：设置从跨越首条线到第二条线之间的时间间隔上限。此选项仅适用于跨越两条线的目标。
  - **按对象类型触发**：选择希望场景触发的目标类型(人、车辆、位置)。
  - **速度限制**：以特定范围内的速度移动的目标触发。
    - **翻转**：选择要在设置速度限制的上方和下方触发速度。

警报设置：定义报警条件。
- **触发持续时间下限**：设置触发警报的持续时间下限。

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。

动态 LED 灯带

动态 LED 灯带模式

使用此页面测试动态 LED 灯带的模式。

模式：选择要测试的模式。

持续时间：指定测试持续时间。

测试：单击以启动要测试的模式。

停止：单击以停止测试。如果您在播放模式时离开页面，该模式将自动停止。

要激活用于指示或威慑目的的模式，请转到**系统 > 事件**，然后创建一个规则。有关示例，请参见 *激活雷达上的扫频红灯, on page 18*。

分析

元数据配置

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。

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。

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。某些应用程序没有不同设置。

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。

- Automatic date and time (PTP)（**自动日期和时间 (PTP)**）：使用精确时间协议进行同步。
- **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（v4 或 v6），然后才能选择此选项。如果两种版本都可用，设备优先选择 IANA 时区而非 POSIX 时区，并优先使用 DHCPv4 而非 DHCPv6。
  - DHCPv4 选择选项 100 用于 POSIX 时区，选择选项 101 用于 IANA 时区。
  - DHCPv6 选择选项 41 用于 POSIX，选择选项 42 用于 IANA。
- **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。

区域设置

设置要在全部系统使用的单位制。

Metric（公制）（m、km/h）：选择米作为距离测量单位，公里/小时为速度测量单位。

U.S. customary（美国常用）（ft、mph）：选择英尺为距离测量单位，英里/小时为速度测量单位。

网络

IPv4

自动分配 IPv4：选择 IPv4 自动获取 IP 地址 (DHCP)，即可由网络自动分配您的 IP 地址、子网掩码和路由器，无需手动配置。我们建议大多数网络采用自动 IP 分配 (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。

注意

如果禁用 DHCP，依赖自动网络配置的功能（如主机名、DNS 服务器、NTP 等）可能停止工作。

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。

网络端口

Power and ethernet（电源和以太网）：选择此选项以打开交换机端口的网络。

Power only（仅电源）：选择此选项以关闭交换机端口的网络。端口仍通过以太网供电。

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号。

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 目标的团体名称。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 目标（只读目标除外）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。
  - **隐私**：选择用于保护您的SNMP数据的加密方式。
  - **“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+、FIPS 140-3 Level 3）**：选择使用安全元件来实现安全密钥库。
- **受信任的平台模块 2.0（CC EAL4+、FIPS 140-2 2 级）**：选择使用 TPM 2.0 来实现安全密钥库。

加密策略

加密策略定义了如何使用加密来保护数据。

激活：选择应用于设备的加密策略：

- **默认 — OpenSSL**：兼顾安全和性能，适合一般用途。
- **FIPS — 符合 FIPS 140-2 的策略**：符合 FIPS 140-2 加密标准，适用于受监管行业。

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**：没有更改设置的访问权限。

⋮ 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。选择以下任一方式：**基本**、**摘要**、OpenID 和**客户端凭证授予**。

HTTPS：选择使用 HTTPS。

上下文菜单包括：

- **更新虚拟主机**
- **删除虚拟主机**

客户端凭证授予配置

管理员声明：输入管理员角色的值。

验证 URL：输入 API 端点身份验证的网页链接。

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。

保存：单击以保存数值。

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*。

您的产品可能具有以下预配置的规则：

Front–facing LED Activation: LiveStream（**前置指示灯激活：直播**）：当麦克风打开并且接收到直播流时，音频设备上的前置指示灯 将变为绿色。

Front–facing LED Activation: Recording（**前置指示灯激活：录制**）：当麦克风打开并且正在进行录制时，音频设备上的前置指示灯 将变为绿色。

Front–facing LED Activation: SIP（**前置指示灯激活：SIP**）：当麦克风打开并且 SIP 呼叫处于活动状态时，音频设备上的前置指示灯将变为绿色。必须先在音频设备上启用 SIP，然后才能触发此事件。

Pre–announcement tone: Play tone on incoming call（**预提示音：来电时播放提示音**）：当对音频设备发起 SIP 呼叫时，设备将播放预定义的音频片段。必须要为音频设备启用 SIP。要使 SIP 呼叫者在音频播放音频片段时听到铃声，必须要将音频设备的 SIP 帐户配置为不自动应答呼叫。

Pre–announcement tone: Answer call after incoming call–tone（**预提示音：来电提示音后接听来电**）：当音频片段结束时，应答传入的 SIP 呼叫。必须要为音频设备启用 SIP。

响亮的铃声：当对音频设备发起 SIP 呼叫时，只要规则处于活动状态，就会播放预定义的音频片段。必须要为音频设备启用 SIP。

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。

Include condition（**包含条件**）：选择以包含描述 MQTT 主题中的条件的主题。

Include namespaces（**包含命名空间**）：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

Network storage（**网络存储**）：打开以使用网络存储。

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。

车载存储

硬盘

- **可用**：可用磁盘空间。
- **状态**：磁盘是否安装。
- **文件系统**：磁盘使用的文件系统。
- **加密**：磁盘是否加密。
- **温度**：当前的硬件温度。
- **整体运行状况测试**：检查磁盘运行状况后的结果。

工具

- **检查**：检查存储设备是否存在错误，并尝试进行自动修复。
- **修复**：修复存储设备。在修复期间，活进行中的录制将暂停。修复存储设备可能导致数据丢失。
- **格式化**：擦除全部录制内容并格式化存储设备。选择一个文件系统。
- **加密**：加密存储的数据。
- **解密**：解密存储的数据。系统将擦除存储设备上的全部文件。
- **更改密码**：更改磁盘加密的密码。更改密码不会中断正在进行的录制。
- **使用工具**：单击以运行选定的工具

卸载：请在从系统上断开设备之前单击。这将停止正在进行的录制。

写保护：打开以保护存储设备防止内容被覆盖。

自动格式化：磁盘将使用 ext4 文件系统自动格式化。

车载存储

RAID

- **可用**：可用磁盘空间。
- **状态**：磁盘是否安装。
- **文件系统**：磁盘使用的文件系统。
- **加密**：磁盘是否加密。
- **温度**：当前的硬件温度。
- **整体运行状况测试**：检查磁盘运行状况后的结果。
- **RAID 级别**：用于存储的 RAID 级别。支持的 RAID 级别为 0、1、5、6、10。
- **RAID 状态**：存储的 RAID 状态。可能的值包括**联机**、**降级**、**同步**和 **失败**。同步过程可能需要数小时。

工具

注意

运行以下工具时，请务必等到操作完成后再关闭页面。

- **检查**：检查存储设备是否存在错误，并尝试进行自动修复。
- **修复**：修复存储设备。在修复期间，活进行中的录制将暂停。修复存储设备可能导致数据丢失。
- **格式化**：擦除全部录制内容并格式化存储设备。选择一个文件系统。
- **加密**：加密存储的数据。存储设备上的文件都将被擦除。
- **解密**：解密存储的数据。存储设备上的文件都将被擦除。
- **更改密码**：更改磁盘加密的密码。更改密码不会中断正在进行的录制。
- **更改 RAID 级别**：擦除全部录像，并更改存储的 RAID 级别。
- **使用工具**：单击以运行选定的工具。

硬盘状态：单击以查看硬盘状态、容量和序列号。

写保护：为存储设备启用写保护以防止内容被覆盖。

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 *叠加, on page 26*。

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。

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。
  - 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。

侦测器

撞击检测

冲击侦测器：打开以在目标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。

电源设置

功率状态

显示电源状态信息。信息因产品而异。

电源设置

Delayed shutdown（**延迟关机**）：如果要在关闭电源前设置一个延迟时间，则需打开。

Delay time（**延迟时间**）：设置一个介于 1 和 60 分钟之间的延迟时间。

Power saving mode（**节能模式**）：打开以使设备进入节能模式。当打开节能模式时，红外照明范围会降低。

设置电源配置：通过选择不同的 PoE 级别选项来更改电源配置。单击**保存并重启**以保存更改。

注意

如果您将电源配置设置为 PoE 3 级，则建议您在设备具有该选项时选择**低功率配置**。

Dynamic power mode（**动态电源模式**）：打开以在设备处于非活动状态时降低功耗。

Power warning overlay（**电源警告叠加**）：打开以在设备电量不足时显示电量警告叠加层。

I/O port power（**I/O 端口电源**）：打开以向连接至 I/O 端口的外部设备提供 12 V 电源。关闭以优先考虑内部功能，如红外、加热和冷却。因此，需要 12 V 电源的设备和传感器将停止正常工作。

电表

能源使用

显示当前的电源使用情况、平均电源使用情况、上限电源使用情况以及时间的功率消耗。

上下文菜单包括：

- **导出**：单击可导出图表数据。

边缘到边缘

配对

配对让您使用兼容的安讯士设备，如同它是主设备的一部分。

添加：添加要配对的设备。

Discover devices（**发现设备**）：单击此选项，可查找网络上的设备。网络扫描完成后，将显示可用设备列表。

注意

列表将显示找到的所有安讯士设备，而不仅仅是可以配对的设备。

只有启用了 Bonjour 的设备才能被找到。要为设备启用 Bonjour，请打开设备的网页界面，进入System（**系统**）> Network（**网络**）> Network discovery protocols（**网络发现协议**）。

注意

已配对的设备会显示信息图标。将鼠标悬停在图标上，可获得与已激活的配对有关的信息。

音频配对可让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。

要配对列表中的设备，请单击 。

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。

PTZ **配对** 允许您将雷达与 PTZ 摄像机配对以使用自动追踪。雷达 PTZ 自动追踪使 PTZ 摄像机根据雷达提供的有关目标位置的信息跟踪目标。

要配对列表中的设备，请单击 + 。

选择配对类型：从下拉列表中进行选择。

地址：输入主机名或 PTZ 摄像机的 IP 地址。

用户名：输入 PTZ 摄像机的用户名。

密码：输入 PTZ 摄像机帐户的密码。

Close（**关闭**）：单击以清除各字段。

连接：单击以建立与 PTZ 摄像机的连接。

配置雷达自动追踪：单击以打开并配置自动追踪。您也可以转到**雷达** > **雷达 PTZ 自动追踪**进行配置。

Generic pairing（**通用配对**）可让您与具备灯光和警报功能的设备进行配对。

要配对列表中的设备，请单击 + 。

选择配对类型：从下拉列表中进行选择。

地址：输入设备的主机名称或IP地址。

用户名：请输入用户名。

密码：输入密码。

Certificate name（**证书名称**）：输入证书名称。

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追踪之类敏感信息。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。

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

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。

故障排查

重置 PTR：如果由于某种原因**水平转动**、**垂直转动**或**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。

校准：单击**校准**可将水平转动、垂直转动和滚转电机重新校准到其默认位置。

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

网络追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。

追踪时间：选择以秒或分钟为单位的追踪持续时间，并单击**下载**。

了解更多

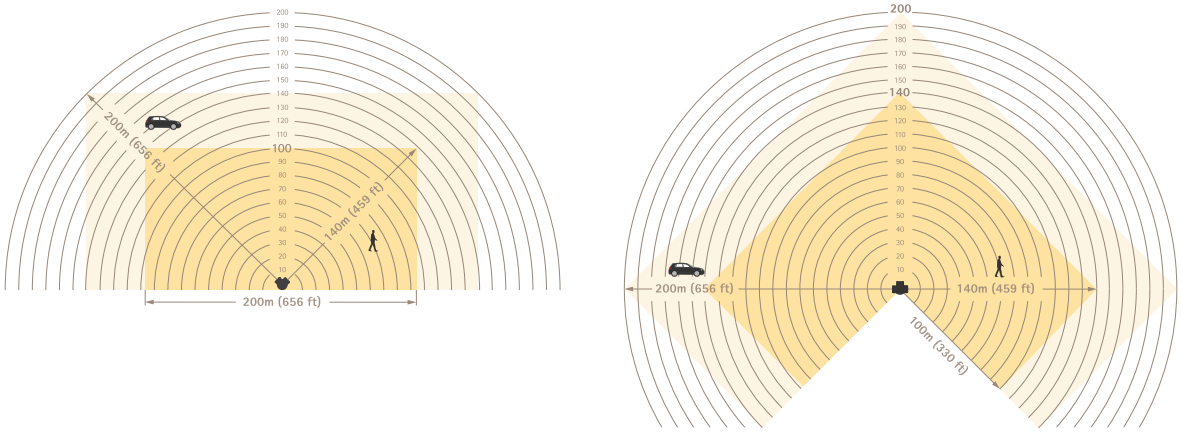
雷达

识别与侦测区域

识别区域是指雷达能够确切将目标分类为人或车辆的区域。

侦测区域是指雷达能够侦测快速移动车辆的区域。

每个区域的大小取决于安装高度及其他因素。



识别区域为深黄色，侦测区域为浅黄色。

场景、包含区域与排除区域

场景包括一组条件，移动目标必须满足这些条件才能触发事件系统中的规则。其中一些条件如下：

- 目标类型（人、车辆、未知）
- 目标行为（区域内移动或越线）
- 场景的一部分（包含区域或虚拟线）
- 目标速度

包含区域是场景中用于侦测和分类“区域内移动”场景中目标的部分。

若场景中存在不希望移动目标触发报警的区域，可创建**排除区域**。若包含区域内存在引发大量不必要报警的区域，您也可使用排除区域。在排除区域内，移动目标将被忽略。使用这些功能可过滤掉诸如路边摇曳的树叶，或是由金属围栏等雷达反射材料构成的目标所产生的虚假轨迹。

共存区

您可以安装多个雷达，以覆盖超过单个雷达具体侦测区域的更大范围。使用相同无线电频率的雷达可能造成电磁干扰，从而影响其性能。每种 AXIS 雷达型号都有一个指定的共存区。在此区域内，可安装若干雷达而不会造成干扰。要了解共存区的半径和推荐的最大雷达数量，请前往 *axis.com* 参阅设备数据表。

雷达视频融合技术

雷达视频融合技术将 Axis 雷达与 Axis 摄像机的优势相结合。这种组合能提供出色的态势感知能力，并减少假警报。当您通过摄像机的网页界面将 ARTPEC–9 PTZ 摄像机与 ARTPEC–9 雷达配对时，雷达可探测到移动目标并将其分类，引导摄像机转向目标，并让摄像机验证分类结果。摄像机随后可通过自动追踪功能继续追踪目标，具体操作请参阅 PTZ 摄像机的用户手册。

自动追踪

您可以利用不同目标位置的雷达数据，使 PTZ 摄像机实现目标追踪。有三个不同的选项：

- 如果您希望连接多个 PTZ 摄像机和雷达，请使用应用 AXIS Radar Autotracking for PTZ。有关详细信息，请参见 *使用 AXIS Radar Autotracking for PTZ 控制 PTZ 摄像机, on page 63*。
- 如果您希望连接安装位置相邻的一个雷达与一个 ARTPEC–7 PTZ 摄像机，请使用摄像机配对功能以启用内置的雷达自动追踪。
- 如果您希望连接安装在一起的一个雷达与一个 ARTPEC–9 PTZ 摄像机，请使用雷达配对功能以启用内置的雷达视频融合自动追踪。该选项结合了人工智能驱动的雷达与视频分析技术，以尽可能减少假警报。有关如何设置雷达视频融合自动追踪的说明，请前往 *help.axis.com/axis–q6325–le* 参阅 PTZ 摄像机的用户手册。

使用 AXIS Radar Autotracking for PTZ 控制 PTZ 摄像机

AXIS Radar Autotracking for PTZ 是一款基于服务器的解决方案，可以在跟踪目标时处理不同的设置：

- 使用一个雷达控制多个 PTZ 摄像机。
- 控制具有多个雷达的 PTZ 摄像机。
- 控制具有多个雷达的多个 PTZ 摄像机。
- 当安装在覆盖相同区域的不同位置时，使用一台雷达控制一个 PTZ 摄像机。

该应用与一组特定的 PTZ 摄像机兼容。有关更多信息，请参见 *axis.com/products/axis–radar–autotracking–for–ptz#compatible–products*。

下载应用，参阅用户手册了解如何设置应用。有关更多信息，请参见 *axis.com/products/axis–radar–autotracking–for–ptz/support*。

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。

AV1

AV1 (AOMedia Video 1) 是一种免许可证的视频编码格式，针对流媒体进行了优化。即使在带宽受限的环境中，AV1 也可提供高质量的视频流。通过降低视频的比特率，AV1 既能保持视频质量，又能最大限度地减少数据用量。

AV1 支持所有主流流浏览器、计算机操作系统和移动平台。

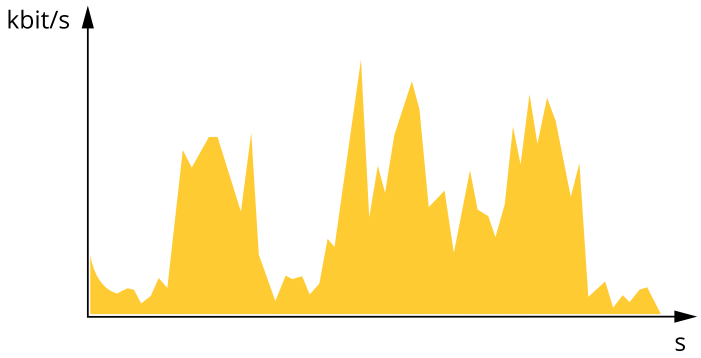
注意

与其他一些编解码器相比，AV1 需要更强的处理能力进行编码和解码。

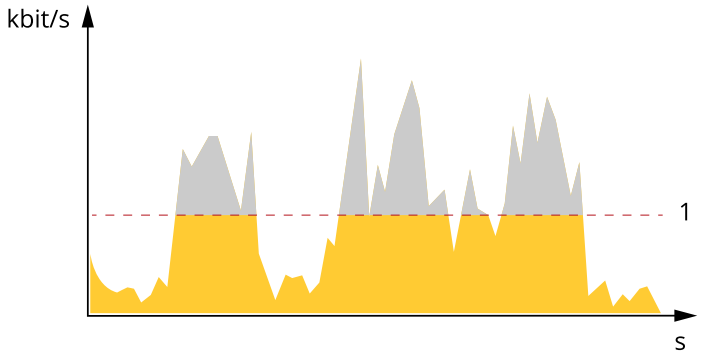
比特率控制

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。



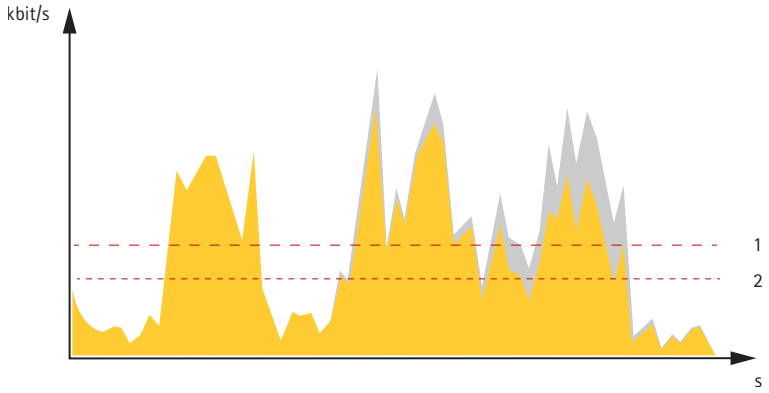
最大比特率 (MBR)
上限比特率让您可设置一个目标比特率，以处理系统中的比特率限制。当即时比特率保持低于指定目标比特率时，您可能会看到图像质量或帧速下降。您可以选择确定图像质量或帧速的优先顺序。我们建议将目标比特率配置为比预期比特率更高的值。这样可在场景中存在高水平的活动时提供边界。



1 目标比特率

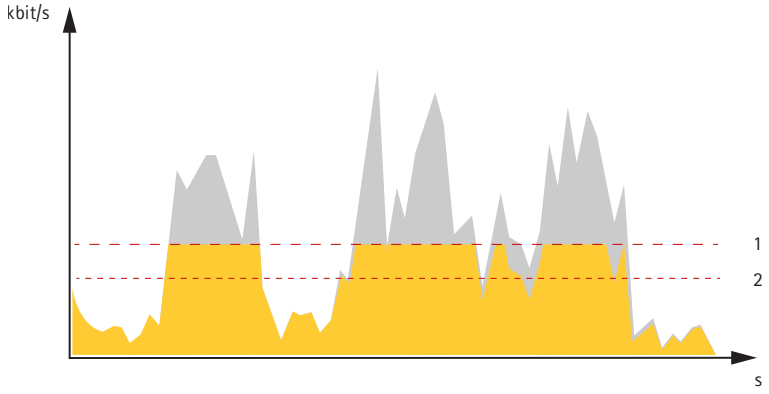
平均比特率 (ABR)
根据平均比特率，比特率可通过更长的时间段自动调整。由此，您就可以满足指定目标，并根据可用存储提供更佳视频质量。与静态场景相比，比特率在具有大量活动的场景中更高。在有大量活动的场景中，如果您使用平均比特率选项，那么您更有可能获得更高的图像质量。当调整图像质量以满足指定的目标比特率时，您可以定义存储视频流所需的总存储量（保留时间）。以下列方式之一指定平均比特率设置：

- 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

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。

如需了解更多信息，请参阅白皮书“边缘到边缘技术”（网址：*whitepapers.axis.com/edge-to-edge-technology*）。

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。

麦克风配对

边缘对边缘麦克风配对可让您将兼容的安讯士麦克风当作摄像机自带设备来使用。配对后，麦克风将立即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。

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 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安讯士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

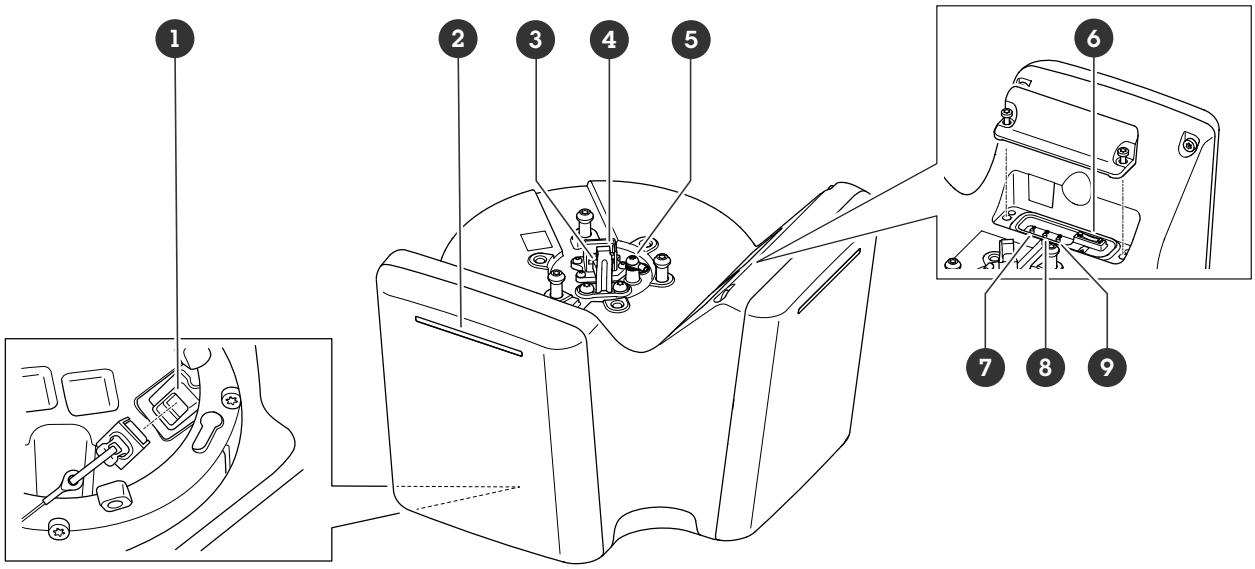
为了尽可能降低客户曝光风险、安讯士作为**常见漏洞和曝光 (CVE) 编号颁发机构 (CNA)**），遵循行业标准来管理和响应我们的设备、软件和服务中发现的漏洞。有关 Axis 漏洞管理策略、如何报告安全漏洞、已披露漏洞以及相应安全通报的更多信息，请参见 *axis.com/vulnerability–management*。

安讯士设备的安全操作

带有出厂默认设置的安讯士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。如需了解有关安讯士网络安全方法的更多信息，包括保护设备安全的最佳实践、资源和指南，请转到 *axis.com/about–axis/cybersecurity*。

规格

产品概述



1 *网络连接器（PoE 输出）*
2 *动态 LED 灯带*
3 *安全线挂钩*
4 *网络连接器（PoE 输入）*
5 *接地螺丝*
6 *microSD 卡插槽*
7 *控制按钮*
8 *操作按钮*
9 *功能按钮（未使用）*

LED 指示灯

状态LED	指示
绿色	稳定绿色表示正常工作。
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。

动态 LED 灯带模式
红色
蓝色
绿色
黄色
白色款
扫频红色
扫频蓝色
扫频绿色
闪烁红色、蓝色、白色

SD 卡插槽

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 *重置为出厂默认设置, on page 70*。

连接器

网络连接器（PoE 输入）

带以太网供电 IEEE 802.3bt 4 型 8 类的 RJ45 以太网连接器。

注意

PoE 输出需要以太网供电 IEEE 802.3bt 4 型 8 类。当不为第二个设备供电时，以太网供电 IEEE 802.3at 2 型 4 类就足够。

网络连接器（PoE 输出）

以太网供电 IEEE 802.3bt 3 型 6 类。

此连接器用于为其他 PoE 设备（例如，摄像机、喇叭扬声器或另一个 Axis 雷达）供电。

注意

- 通过以太网供电 IEEE 802.3bt 4 型 8 类标准为雷达供电，可支持为另一个采用以太网供电 IEEE 802.3bt 3 型 6 类标准的设备供电。
- 通过以太网供电 IEEE 802.3bt 3 型 6 类标准为雷达供电，可支持为另一个采用以太网供电 IEEE 802.3bt 2 型 4 类标准的设备供电。
- 若采用以太网供电 IEEE 802.3bt 2 型 4 类标准为雷达供电，则 PoE 输出将被禁用。

注意

最大以太网电缆长度为 100 米（ PoE 进出总计）。您可以使用 PoE 扩展器来延长。

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。

故障排查

重置为出厂默认设置

重要

重置为出厂默认设置时应谨慎。重置为出厂默认设置会将全部设置（包括 IP 地址）重置为出厂默认值。

将产品重置为出厂默认设置：

1. 断开产品电源。
2. 按住控制按钮，同时重新连接电源。请参见 *产品概述, on page 67*。
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**。

确保没有人篡改过设备软件

要确保设备具有其原始的 AXIS OS，或在安全攻击之后控制设备，请执行以下操作：

1. 重置为出厂默认设置。请参见 *重置为出厂默认设置, on page 70*。
   重置后，安全启动可保证设备的状态。
2. 配置并安装设备。

AXIS OS 选项

Axis 可根据主动追踪或长期支持 (LTS) 追踪提供设备软件管理。处于主动追踪意味着可以持续访问新产品特性，而 LTS 追踪则提供一个定期发布主要关注漏洞修复和安保升级的固定平台。

如果您想访问新特性，或使用安讯士端到端系统产品，则建议使用主动追踪中的 AXIS OS。如果您使用第三方集成，则建议使用 LTS 追踪，其未针对主动追踪进行连续验证。使用 LTS，产品可维护网络安全，而无需引入重大功能改变或影响现有集成。如需有关安讯士设备软件策略的更多详细信息，请转到 *axis.com/support/device–software*。

检查当前 AXIS OS 版本

AXIS OS 决定了我们设备的功能。当您进行问题故障排查时，我们建议您从检查当前 AXIS OS 版本开始。新版本可能包含能修复您的某个特定问题的校正。

要检查当前 AXIS OS 版本：

1. 转到设备的网页界面 > **状态**。
2. 请参见**设备信息**下的 AXIS OS 版本。

升级 AXIS OS

重要

- 升级设备软件时，您的预配置和自定义设置将被保存。安讯士公司无法保证设置会被保存，即使新版 AXIS OS 支持这些功能。
- 从 AXIS OS 12.6 开始，您必须安装设备当前版本与目标版本之间的各个 LTS 版本。例如，如果当前安装的设备软件版本为 AXIS OS 11.2，则必须先安装 LTS 版本 AXIS OS 11.11，才能将设备升级至 AXIS OS 12.6。有关更多信息，请参见：*AXIS OS 门户：升级路径*。
- 确保设备在整个升级过程中始终连接到电源。
- 请确保在升级过程中装上外盖，以避免安装失败。

注意

- 使用活动追踪中的新 AXIS OS 升级设备时，产品将获得可用的新功能。在升级前，始终阅读每个新版本提供的升级说明和版本注释。要查找新 AXIS OS 和发布说明，请转到 *axis.com/support/device-software*。

1. 将 AXIS OS 文件下载到您的计算机，该文件可从 *axis.com/support/device-software* 免费获取。
2. 以管理员身份登录设备。
3. 转到**维护 > AXIS OS 升级**，然后单击**升级**。

升级完成后，产品将自动重启。

技术问题和可能的解决方案

升级 AXIS OS 时出现问题

AXIS OS 升级失败

如果升级失败，该设备将重新加载以前的版本。比较常见的原因是上载了错误的 AXIS OS 文件。检查 AXIS OS 文件名是否与设备相对应，然后重试。

AXIS OS 升级后出现的问题

如果您在升级后遇到问题，请从**维护**页面回滚到之前安装的版本。

设置 IP 地址时出现问题

无法设置 IP 地址

- 如果用于设备的 IP 地址和用于访问该设备的计算机 IP 地址位于不同子网上，则无法设置 IP 地址。请联系网络管理员获取 IP 地址。
- 该 IP 地址可能已被其他设备使用。检查：
  1. 从网络上断开安讯士设备。
  2. 在 Command/DOS 窗口中，键入 `ping` 和设备的 IP 地址。
  3. 如果收到：`Reply from <IP address>: bytes=32; time=10...`，这意味着网络上其他设备可能已使用该 IP 地址。请从网络管理员处获取新的 IP 地址，然后重新安装该设备。
  4. 如果您收到：`Request timed out`，这意味着该 IP 地址可用于此安讯士设备。请检查布线并重新安装设备。
- 可能与同一子网中的另一台设备存在 IP 地址冲突。在 DHCP 服务器设置动态地址之前，将使用安讯士设备中的静态 IP 地址。这意味着，如果其他设备也使用同一默认静态 IP 地址，则可能在访问该设备时出现问题。

设备访问问题

通过浏览器访问设备时无法登录

启用 HTTPS 后，需在登录时使用正确的协议（HTTP 或 HTTPS）。您可能需要在浏览器的地址字段中手动键入 `http` 或 `https`。

如果您遗失了根帐户密码，则必须将设备重置为出厂默认设置。有关说明，请参见 *重置为出厂默认设置, on page 70*。

通过DHCP修改了IP地址。

从 DHCP 服务器获得的 IP 地址是动态的，可能会更改。如果 IP 地址已更改，请使用 AXIS IP Utility 或 安讯士设备管理器在网络上找到设备。使用设备型号或序列号或根据 DNS 名称（如果已配置该名称）来识别设备。

如有需要，您可以手动分配静态 IP 地址。如需说明，请转到 *axis.com/support*。

使用 IEEE 802.1X 时出现证书错误

要使身份验证正常工作，则安讯士设备中的日期和时间设置必须与 NTP 服务器同步。转到**系统 > 日期和时间**。

该浏览器不受支持

有关推荐浏览器的列表，请参阅 *浏览器支持, on page 12*。

无法从外部访问设备

如需从外部访问设备，我们建议您使用以下其中一种适用于 Windows® 的应用程序：

- AXIS Camera Station Edge：免费，适用于有基本监控需求的小型系统。
- AXIS Camera Station Pro：90 天试用版免费，适用于小中型系统。

有关说明和下载文件，请转到 *axis.com/vms*。

MQTT 问题

无法通过 SSL 通过端口 8883 进行连接，MQTT 通过 SSL

防火墙会拦截使用 8883 端口的流量，因为该端口被判定为存在安全风险。

在某些情况下，服务器/中介可能不会提供用于 MQTT 通信的特定端口。仍然可以使用通常用于 HTTP/HTTPS 通信的端口上的 MQTT。

- 如果服务器/代理支持 websocket/Websocket Secure (WS/WSS)，通常在端口 443 上，请改用此协议。与服务器/中介提供商确认是否支持 WS/WSS以及要使用哪个端口和 basepath。
- 如果服务器/代理支持ALPN，则可通过开放端口（如443）协商使用MQTT。请咨询服务器/代理提供商，了解是否支持ALPN以及使用哪个ALPN协议和端口。

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。

图像问题

图像降级或图像丢失

- 检查设备服务器报告，查看您丢失到传感器单元的链接的次数。
- 检查传感器单元和主机之间的连接器电缆是否已拧紧。
- 更换为新的传感器单元电缆。

设备自动关闭的问题

设备关闭

- 断开并重新连接设备电源。
- **检查延迟关机**是否打开。如果其处于打开状态，则主机将根据设置的延迟时间关闭。您有 300 秒可在设备再次关闭之前关闭**延迟关机**。

性能考虑

当您设置系统时，考虑不同设置和情况对所需带宽（比特率）的影响，这非常重要。

需要考虑的更重要的因素：

- 拆下或安装盖子都会重启摄像机。
- 由于基础设施差而导致的网络利用率重负会影响带宽。

联系支持人员

如果您需要更多帮助，请转到 *axis.com/support*。

T10223326_zh

2026-01 (M1.36)