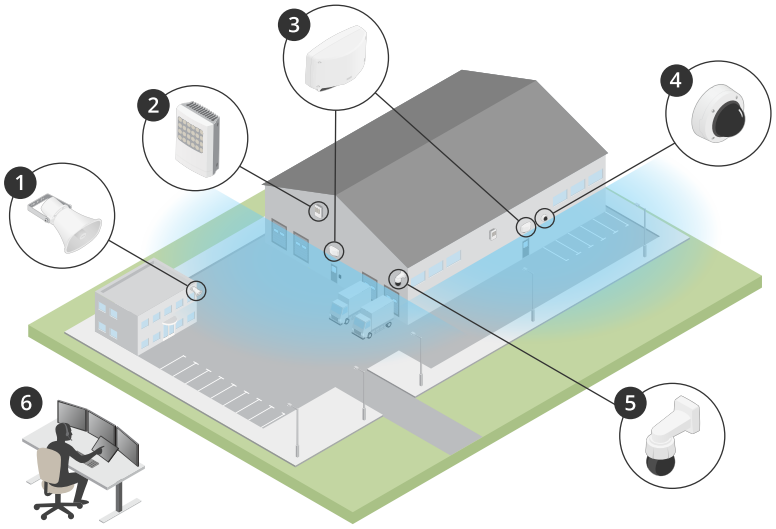
AXIS D2110–VE Security Radar

用户手册

目录

目录

解决方案概览



1 C1310–E 喇叭扬声器
2 门禁控制器
3 D2110–VE Security Radar
4 固定半球摄像机
5 PTZ 摄像机
6 监控中心

雷达配置文件

注

要使用雷达配置文件，设备必须运行固件版本 10.11 或更高版本。转到 以更新您的固件。

用户手册的设置可帮助您使用雷达，具体取决于您所需的功能。AXIS D2110–VE Security Radar 有两个配置文件：

- 区域监控配置文件可跟踪以低于 55 km/h（34 英里小时）的速率移动的大小物体。
- 用于跟踪移动速度高达 105 km/h（65 英里小时）的车辆的道路监控配置文件

本用户手册中的不属于区域监控配置文件或道路监控配置文件的信息都是两个配置文件通用的，无论您使用哪一种，均可参考。

产品安装位置

- 雷达用于监视开阔区域。覆盖区域内的大多数实体物体（如墙体、围栏、树木或大灌木丛）背后会形成盲点（雷达阴影）。
- 将雷达安装在没有其他物体或装置的稳定立杆或墙面的一个点上。雷达图左侧和右侧 1 米（3 英尺）以内的物体，可反映无线电波，从而影响雷达的性能。
- 视野中的金属物体导致反射会影响雷达执行分类的能力。
- 如果要在同一个共存区域中安装两个以上的雷达，请参见 *安装多个雷达 6*。

解决方案概览

覆盖范围

AXIS D2110–VE 的水平区域覆盖范围为 180°。该侦测范围对应于用于车辆的 11300 平方米（122000 平方英尺）和用于人的 5600 平方米（61000 平方英尺）。

注

理想区域覆盖范围适用于安装在 3.5–4 米（11–13 英尺）处的雷达。安装高度将影响雷达下方的盲点的大小。

区域监控配置文件

区域监控配置文件

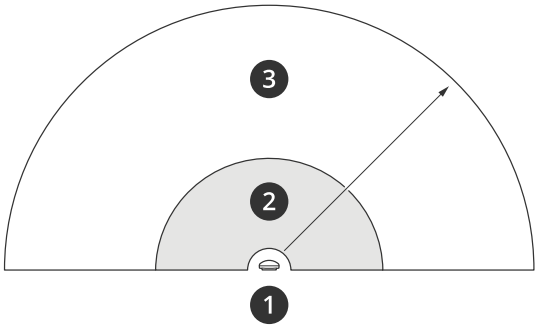
区域监控配置文件针对移动速度高达 55 公里/小时（34 英里/小时）的物体进行了优化。此配置文件让您能够侦测到某个物体是人、车辆还是未知。可以设置一个规则，在侦测到这些物体中的任意一个时触发操作。要跟踪以更高速度行驶的车辆，请使用 *道路监控配置文件 13*。

安装多个雷达

您可以安装多个雷达，以覆盖诸如建筑周围或围栏外的缓冲区域等区域。

共存

当您将两个以上的雷达放在同一个共存区域中时，区域中雷达的无线电波会引起干扰，并影响性能。共存区域半径为 350 米（380 码）。



1 雷达
2 侦测区域
3 共存区域

注

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

在同一个共存区域中安装 2-3 个雷达

当您将两个或三个雷达放在同一个共存区域中时，您需要在设备界面中定义相邻雷达的数量。这有助于提高雷达的性能并避免干扰。

1. 转到雷达 > 设置 > 共存。
2. 选择相邻雷达的数量。

有关多个雷达的安装示例，请参见 *区域安装示例 7*。

在同一个共存区域中安装 4-6 个雷达

注

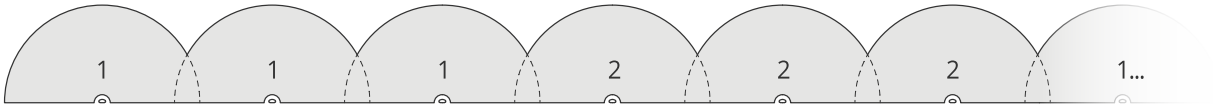
在同一共存区域中安装多达六个雷达的选项可从固件版本 11.3 获得。

当您在同一个共存区域中安装 4 到 6 个雷达时，请首先设置相邻雷达的数量，然后将每个雷达添加到一个组中。从远端的雷达（例如，左侧末端的摄像机）开始。将雷达添加到三组中，然后添加在同一个组中离彼此近的雷达。

该组内的雷达将彼此同步以优化性能并避免彼此之间的干扰。

区域监控配置文件

1. 转到雷达 > 设置 > 共存。
2. 将相邻雷达的数量设置为 3–5。
3. 为您的雷达选择一个组。



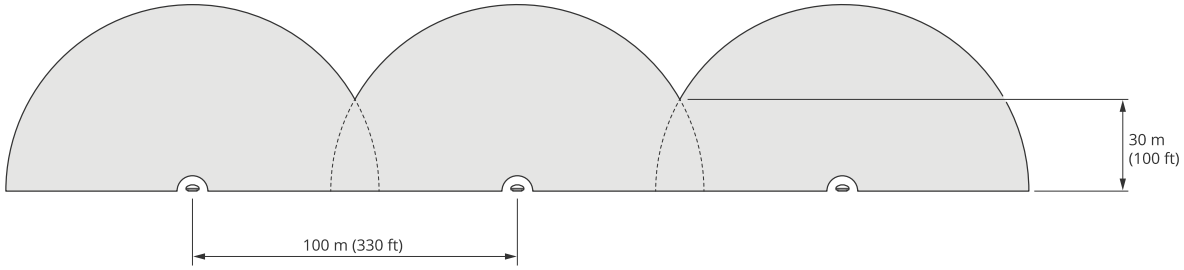
这是一个示例，说明如何对在同一个共存区域中并行安装的多个雷达进行分组。

有关多个雷达安装的更多示例，请参见 *区域安装示例 7*。

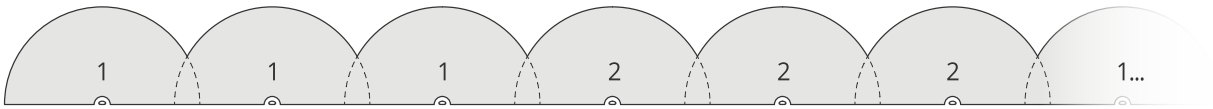
区域安装示例

使用多个雷达创建虚拟围栏

要沿或绕建筑物创建虚拟围栏，您可以并排放置多个雷达。我们建议雷达之间保持 100 米 (330 英尺) 的间距。

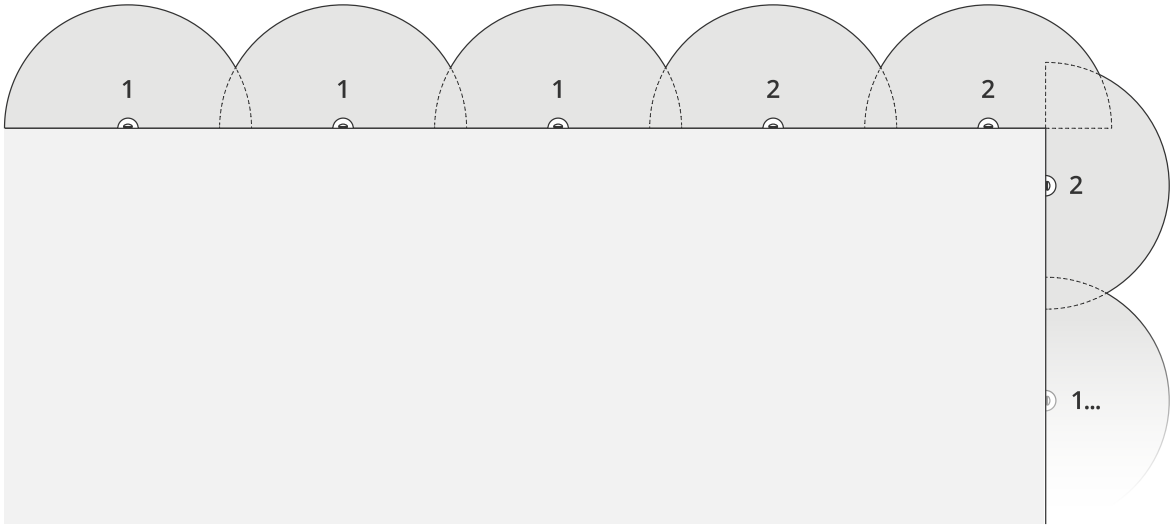


为避免在同一个共存区域中安装两个以上的雷达时产生干扰，请在设备界面中设置相邻雷达的数量。此外，当您安装超过三个雷达时，请将每个雷达添加到一个组中。



您也可将虚拟围栏调整至覆盖各角落，如本示例所示。

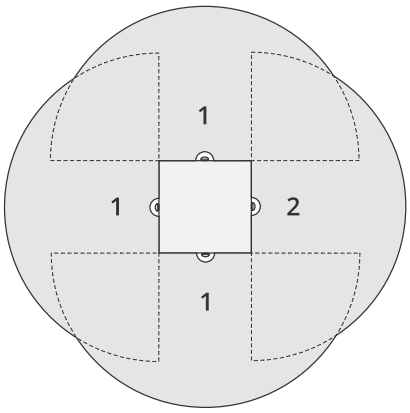
区域监控配置文件



有关相邻雷达和组的更多信息，请参见 *安装多个雷达 6*。

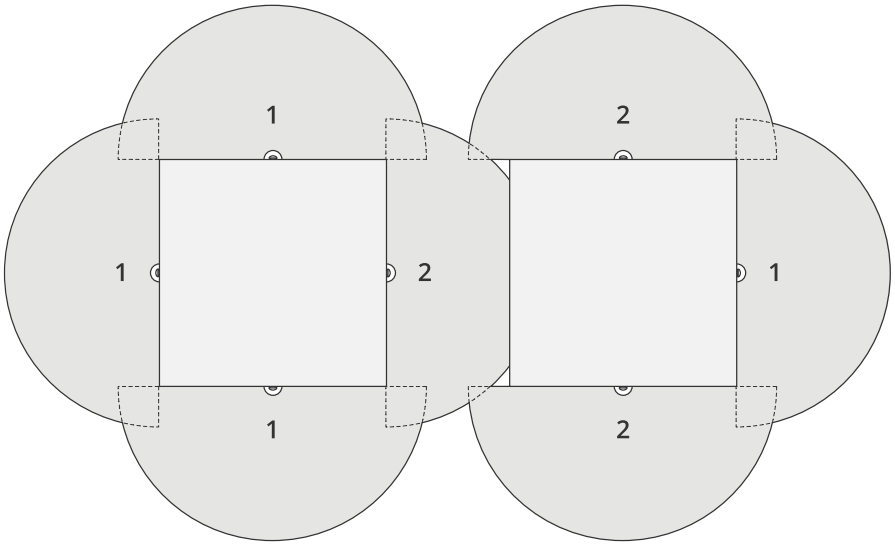
覆盖建筑物周围区域

要覆盖建筑物周围区域，请将雷达放在建筑物朝向外面的墙上。如果要将三个以上的雷达放在同一个共存区域中，请在设备界面中设置相邻雷达的数量，然后将每个雷达添加到一个组中，如本示例所示。



您还可覆盖多个建筑物的周边区域。

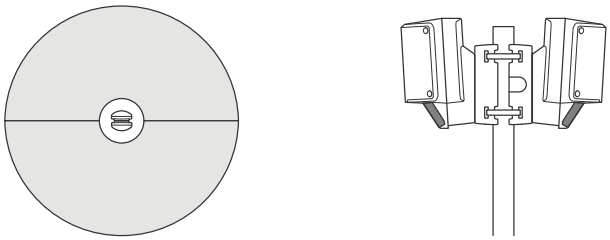
区域监控配置文件



有关相邻雷达和组的更多信息，请参见 *安装多个雷达 6*。

覆盖开放区域

要覆盖一个较大的开放区域，请使用两个立杆托架将两个雷达背靠背放置。

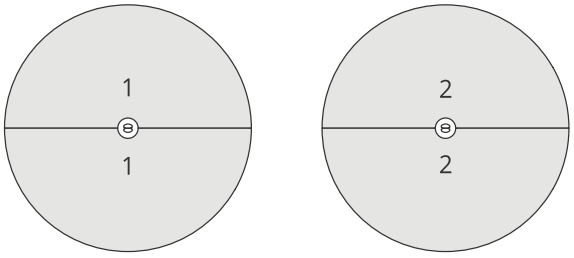


您可以使用一个雷达的 PoE 输出来为第二个雷达供电，但无法以这种方式连接第三个雷达。

注

当雷达由 60 W 中跨供电时，雷达上的 PoE 输出将启用。

如果您需要在同一个共存区域中进行多个背到背安装，请在设备界面中设置相邻雷达的数量，并将每个雷达添加到一个组中，以避免干扰。这是如何在背到背安装中对雷达进行分组的一个示例。



区域监控配置文件

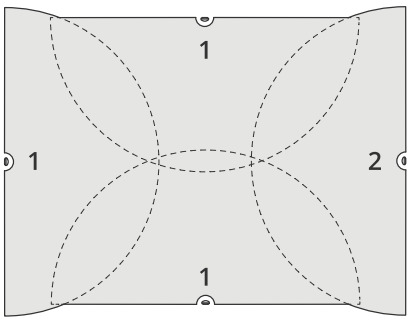
有关相邻雷达和组的更多信息，请参见 *安装多个雷达 6*。

安装彼此相对的多个雷达

通常，不建议安装三个以上的雷达，因为这会增加雷达之间发生干扰的风险。但是，在某些特定区域，可能有此必要。例如，如果要覆盖足球场，则不能将雷达放在场地的中间。

如果安装的雷达超过三个，则从一个雷达到另一个雷达的下限距离需要 40 米（130 英尺）。在设备界面中设置相邻雷达的数量，并将每个雷达添加到一个组中也是很重要的。这将有助于提高雷达的性能。

这是一个如何对覆盖一个字段的四个 radars 进行分组的示例。



有关相邻雷达和组的更多信息，请参见 *安装多个雷达 6*。

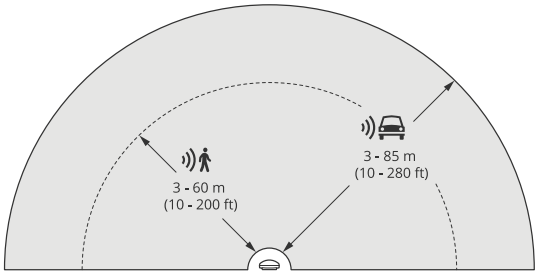
区域侦测范围

侦测范围是指能够跟踪物体并触发警报的距离。它是从接近侦测限制（可进行侦测的设备接近）到较远侦测限制（可进行侦测的距离）算起的。

但区域监控配置文件针对人机侦测进行了优化，它还允许您以 +/– 2 km/h (1.24 mph) 的速度准确度及高达 55 km/h (34 mph) 的速度跟踪车辆和其他物体。

以理想安装高度安装时，侦测范围包括：

- 当侦测人时，3–60 m (10–200 ft)
- 当侦测车辆时，3–85 m (10–280 ft)



区域监控配置文件

注

- 如果您将雷达安装在其他不同高度，请在校准雷达时在产品网页中输入实际的安装高度。
- 侦测范围受场景的影响。
- 侦测范围受邻近雷达的影响。
- 侦测范围受物体类型的影响。

在以下情况下会测量侦测范围：

- 范围将沿地面测量。
- 目标为身高170 cm (5 ft 7 in) 的人。
- 人在雷达前方行走。
- 当人进入侦测区域时将测量这些值。
- 雷达灵敏度设置为中。

安装高度	垂直转动 0°	垂直转动 10°	垂直转动 20°
2.5 米 （8.2 英尺）	3.0–60 米 （9.8–197 英尺）	不推荐	不推荐
3.5 米 （11 英尺）	3.0–60 米 （9.8–197 英尺）	不推荐	不推荐
4.5 米 （15 英尺）	4.0–60 米 （13–197 英尺）	不推荐	不推荐
5.5 米 （18 英尺）	7.5–60 米 （25–197 英尺）	不推荐	不推荐
6.5 米 （21 英尺）	7.5–60 米 （25–197 英尺）	5.5–60 米 （18–197 英尺）	不推荐
8 米 （26 英尺）	不推荐	9–60 米 （30–197 英尺）	7.5–30 米 （25–98 英尺）
10 米 （33 英尺）	不推荐	15–60 米 （49–197 英尺）	9–35 米 （30–115 英尺）
12 米 （39 英尺）	不推荐	23–60 米 （75–197 英尺）	13–38 米 （43–125 英尺）
14 米 （36 英尺）	不推荐	27–60 米 （89–197 英尺）	17–35 米 （56–115 英尺）
16 米 （52 英尺）	不推荐	不推荐	25–50 米 （82–164 英尺）

区域监控使用案例

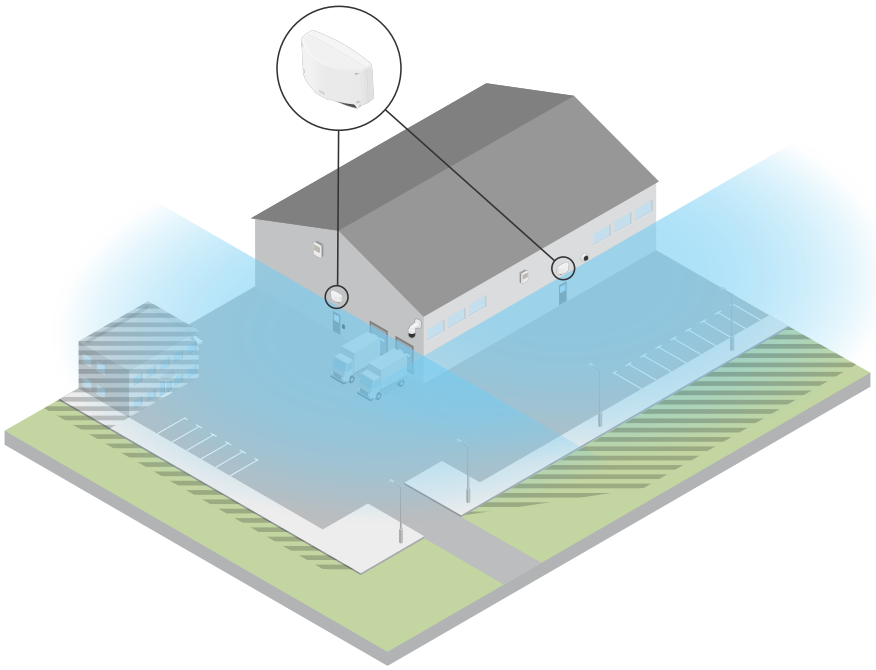
游泳池区域覆盖范围

公共游泳池在营业时间之后曾有一系列入侵。由于业务的私密特性，业主无法安装视频监控。他们已选择安装雷达并在区域监控配置文件进行设置。雷达安装在建筑上，涵盖整个游泳池及其周围的大部分区域。当侦测到在 20:00 关闭到 06:00 开放期间有人时，将触发来自扬声器的警告。

覆盖建筑物周围场地

区域监控配置文件

化学工厂通过使用雷达来覆盖敏感建筑物周围的区域，向系统中添加另一个安全层。安全系统已包括摄像机、热成像摄像机和门禁控制器。雷达可触发导致摄像机跟踪入侵者、放大和录制活动的事件。与热成像摄像机关联的闪烁信标被触发到刷新，因此入侵者知道该区域受到保护。而门禁控制器可限制访问。雷达帮助防护系统在入侵者到达敏感建筑之前进入操作的时间。



覆盖一个较大的开放区域

小型购物中心外的停车场在下班后已增加车辆休息时间。他们一次有一个安全保护措施，但感觉他们需要在夜间提供安全保护，而不会增加聘用更多员工成本。他们决定在区域监控配置文件中安装两个安全雷达，以使其覆盖整个停车区域。雷达配置为提醒当值安保人员有可疑行为，以便他们能够调查场景。它们还可以安装由雷达触发的触角扬声器，以播放可能会阻止盗窃的警报。

道路监控配置文件

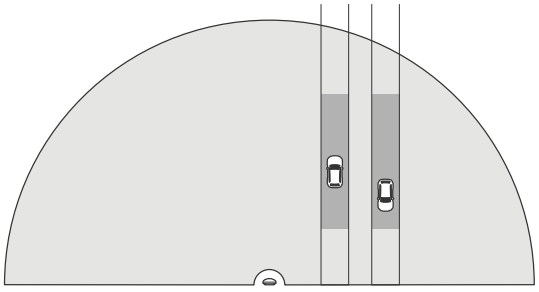
道路监控配置文件

道路监控配置文件 适用于在市内区域、封闭区域和子城市道路上跟踪高达 105 km/h（65 英里小时）的车辆。此模式不应用于侦测人或其他类型的物体。要跟踪车辆以外的物体，请在*区域监控配置文件 6*中使用雷达。

道路安装示例

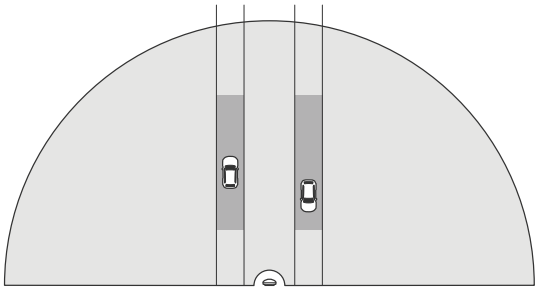
侧面安装

要监视沿道路的车辆，您可以将雷达安装在道路的一侧。雷达将提供 10 米（32 英尺）的横向覆盖距离。



中心安装

此安装选项需要稳定的位置。雷达可安装在道路中间的立杆上或在道路上方的桥架上。这样，雷达将在雷达的两边提供 10 米（32 英尺）的横向覆盖距离。安装中心时，雷达覆盖范围更广的横向距离。



注

我们建议道路监控配置文件 的雷达安装在高度为3 m (10 ft) 和 8 m (26 ft) 之间。

道路侦测范围

侦测范围是指能够跟踪物体并触发警报的距离。它是从接近侦测限制（可进行侦测的设备接近）到较远侦测限制 （可进行侦测的距离）算起的。

当监控高达 105 km/h（65 英里小时）的车辆时，此配置文件已针对侦测车辆进行优化，并将产生 +/– 2 km/h (1.24 mph) 的速度准确性。

在采用理想安装高度安装雷达时的侦测范围：

- 25–70 米（82–229 英尺），适用于以 60 km/h (37 mph) 速度移动的车辆。

- 30–60 米（98–196 英尺），适用于以 105 km/h (65 mph) 速度移动的车辆。

注

如果同一个共存区域中的雷达上限数量超过 2 个，则预计范围将下降约 10%（近）和 20%（远）。

公路监控使用案例

在低速区域中调节车辆

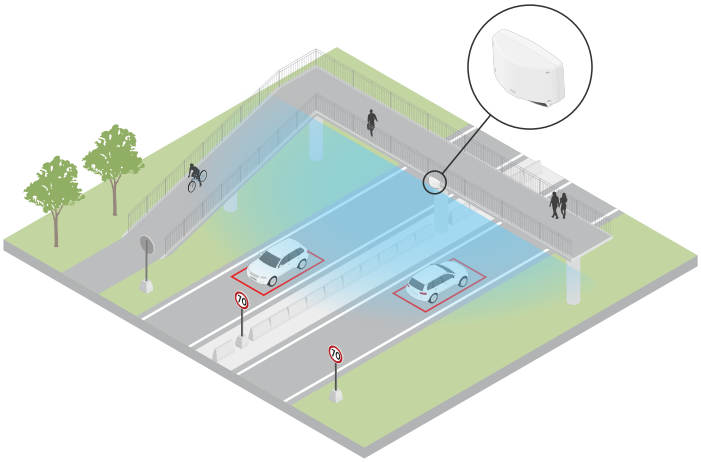
两个仓库之间的工业复合体安装了雷达，能够帮助实施 60 km/h（37 英里小时）的速度限制。在道路监控配置文件 中，雷达可侦测到其侦测区域中的车辆超出该速度。然后，它触发向驱动程序和管理者发送电子邮件通知的事件。该提醒有助于提高对速度限制的遵守。

闭合道路上不需要的车辆

已关闭了通往旧码头的小路，但是，路上驾驶车辆报告导致在道路监控配置文件安装了安全雷达。雷达沿着道路安装，覆盖整个道路宽度。每当车辆进入场景时，它都会触发闪烁的信标，以警告驱动程序离开道路。它还向安全小组发送消息，以便他们能够在需要时派送设备。

加快对道路的关注

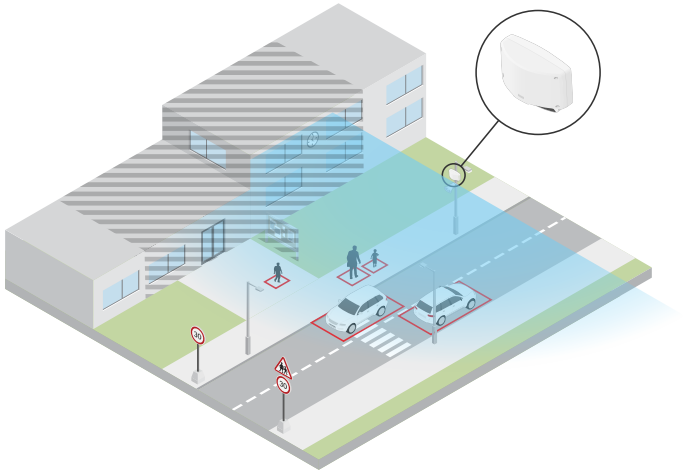
穿过小型城镇的道路有一些加速事件。为了强制实施 70 km/h (43 mph)的速度限制，交通控制已在一个基于道路的桥上的道路监控配置文件安装了安全雷达。这就让他们能够侦测车辆正在行使的速度，并在其有沿路布点时进行对交通进行控制。



人和车辆安全

学校员工已确定要解决的两个安全问题。他们的问题是有不希望来访的人在学校日进入场所，以及在学校外违反 20 km/h (12 mph) 低速区域的车辆。雷达安装在靠近人行道的一根立杆上。选择*区域监控配置文件 6*因为它让雷达能够跟踪低于 55 km/h (34 mph) 速度的人和车辆。这可帮助员工跟踪在学校上课时间内进出校园的人员，同时还能够在过往车辆行使速度太快时触发扬声器，提醒行人。

道路监控配置文件



开始

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 设备管理器。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，请转到设置 > Safari > 高级 > 实验功能，禁用 NSURLSession Websocket。*

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 *创建管理员账户 16*。

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 *安全密码 16*。
3. 重新输入密码。
4. 单击添加用户。

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*重置为出厂默认设置 67*。

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。

网页界面概览

该视频为您提供设备网页界面的概览。

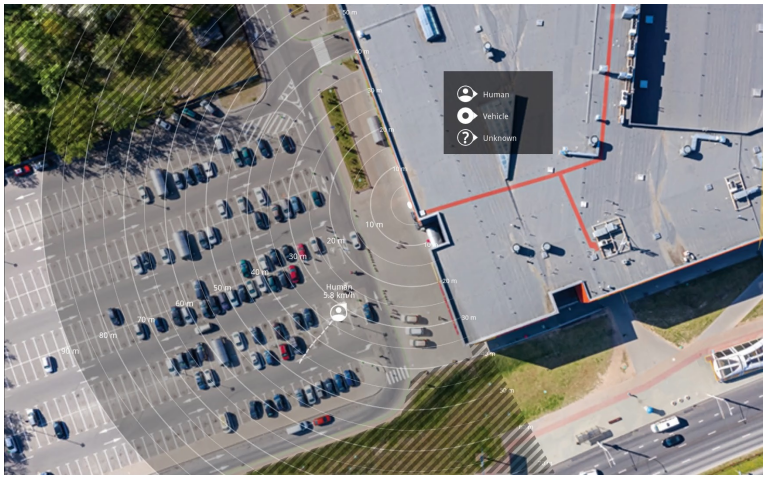
Axis 设备网页界面

配置设备

校准雷达

一旦安装完毕，雷达即可使用。默认实时视图将显示雷达覆盖范围和侦测到的移动，您可以立即添加侦测区域和规则。

如果雷达安装在地面以上 3.5 米（11 英尺）处，则无需再执行其他操作。如果安装在其他高度，您需要校准雷达来达到安装高度要求。



为了能够更加轻松地查看物体移动位置，您可以上载一份显示雷达覆盖区域的参考图（例如，一份平面图或航拍照片）。

图像要求：

- 支持的文件格式为 jpeg 和 png。
- 方向并不重要，因为在校准期间雷达覆盖范围形状会移动，以使其适应图像。

上传参考地图

上传参考地图并对其进行校准，使实际雷达覆盖范围符合地图的位置、方向和比例。

1. 转到雷达 > 地图校准。
2. 上传您的参考地图，然后按照设置助手操作。

设置侦测区域

要确定运动的侦测位置，您可以添加多个区域。不同区域可用于触发不同的操作。

有两种区域：

- 场景（以前称为包含区域）是移动物体将在其中触发规则的区域。默认场景与雷达覆盖的整个区域相匹配。
- 排除区域是将忽略移动物体的区域。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。

添加场景

场景（以前称为包含区域）是移动对象将在其中触发规则的区域。如果要为场景的不同部分创建不同的规则，请添加场景。

添加场景：

1. 转到雷达 > 场景。
2. 单击添加场景。
3. 键入场景的名称。
4. 如果您希望物体在区域中移动或物体跨越一条或两条线时触发，请选择此选项。

物体在区域内移动时触发：

1. 选择在区域中移动。
2. 单击下一步。
3. 选择场景中应包含的区域类型。

   使用鼠标来移动和重塑区域，使该区域覆盖雷达图像或参考地图中所需的部件。
4. 单击下一步。
5. 添加侦测设置。

   5.1 在忽略短暂停留的物体下添加触发前的秒数。

   5.2 在对象类型触发下选择要触发的对象类型。

   5.3 在速度限制下添加速度限制的范围。
6. 单击下一步。
7. 在触发持续时间下限下设置警报的下限持续时间。
8. 单击保存。

对象越界时触发：

1. 选择越线。
2. 单击下一步。
3. 在场景中定位线。

   使用鼠标移动线条和修改线条形状。
4. 要更改侦测方向，请启用更改方向。
5. 单击下一步。
6. 添加侦测设置。

   6.1 在忽略短暂停留的物体下添加触发前的秒数。

   6.2 在对象类型触发下选择要触发的对象类型。

   6.3 在速度限制下添加速度限制的范围。
7. 单击下一步。
8. 在触发持续时间下限下设置警报的下限持续时间。

默认值设为 2 秒。如果希望在物体每次越线时触发场景，请将持续时间降低为 0 秒。

9. 单击保存。

物体跨越两条线时触发：

1. 选择越线。
2. 单击下一步。
3. 要使物体跨越两条线以触发警报，请打开 要求跨越两条线 。
4. 在场景中定位线。

   使用鼠标移动线条和修改线条形状。
5. 要更改侦测方向，请启用更改方向。
6. 单击下一步。
7. 添加侦测设置。

   7.1 在跨越之间的上限时间下设置跨越首条线与第二条线的时间限制。

   7.2 在对象类型触发下选择要触发的对象类型。

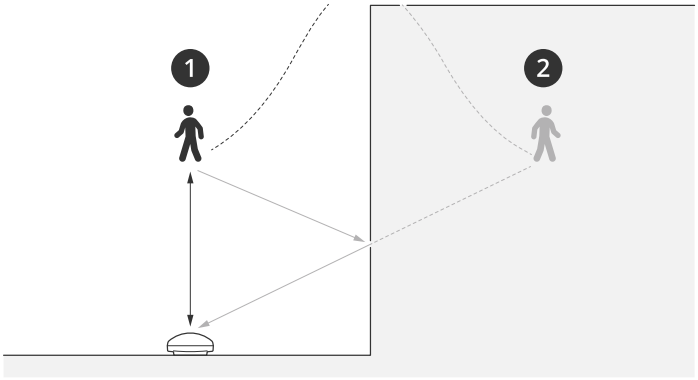
   7.3 在速度限制下添加速度限制的范围。
8. 单击下一步。
9. 在触发持续时间下限下设置警报的下限持续时间。

   默认值设为 2 秒。如果希望在物体每次跨越两条线时触发场景，请将持续时间降低为 0 秒。
10. 单击保存。

添加排除区域

排除区域是将忽略移动物体的区域。添加排除区域以忽略有可能导致误报的移动物体的区域。

示例:
金属顶部、围栏、车辆甚至砖墙墙壁等雷达反射材料的物体可能会干扰雷达的性能。它们可能会创建可导致难以与实际侦测分离出来的明显侦测的反射或迭影轨迹。



1 实际侦测
2 反射侦测

添加排除区域：

1. 转到雷达 > 排除区域。
2. 单击添加排除区域。

   使用鼠标来移动和重塑区域，使该区域覆盖雷达图像或参考地图中所需的部件。

注

从固件版本 11.4 开始，不再有排除区域数量的限制。

大幅度减少假警报

如果发现自己收到太多假警报，则可过滤某些类型的移动或物体、更改范围，或调整侦测灵敏度。查看哪些设置更适用于您的环境。

- 调整雷达的侦测灵敏度：

  转到雷达 > 设置 > 侦测，并选择较低的侦测灵敏度。这会减少假警报的风险，但也可能导致雷达无法捕捉到某些移动。

  灵敏度设置会影响大多数区域。

  - 低：当区域中存在大量金属物体或大型车辆时，请使用此灵敏度。这将花费更长的时间来跟踪和对物体进行分类。这可能会减少侦测范围，尤其是对于快速移动的物体。
  - 中：这是默认设置。
  - 高：在雷达前面有一个无金属物体的开阔场地时，请使用这种灵敏度。这将增加人的侦测范围。

- 修改方案并排除区域：

  如果场景包括硬表面（如金属壁），则可能会存在导致对单个实体物体进行多次侦测的反射。您可以修改场景的形状，或添加忽略场景特定部分的排除区域。有关详细信息，请参见*添加场景 19*和*添加排除区域 20*。

- 在物体跨越两条线（而非一条线）时触发：

  如果越线场景中包括摆动的物体或走动的动物，则存在物体越线并触发假警报的风险。在这种情况下，您可以将场景配置为仅在物体跨越两条线时触发。有关详细信息，请参见*添加场景 19*。

- 移动过滤：

  - 转到雷达 > 设置 > 侦测，然后选择忽略摆动的物体。该设置可尽量降低因覆盖区域内树木、灌木丛和旗杆引起的假警报的发生。
  - 转到雷达 > 设置 > 侦测，然后选择忽略摆动的小型物体。该设置可在区域监控配置文件中使用，可尽量降低因覆盖范围内小型物体（如猫和兔子）引起的假警报的发生。

- 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。
  - 在触发前秒数下选择一个较高的值。这是从雷达开始跟踪某个物体到其触发警报之间的延迟时间。当雷达首次侦测到物体时计时器开始计时（并非从物体进入场景中的指定区域时开始）。

- 按物体类型过滤：

  - 转到雷达 > 场景。

- 选择一个场景，然后单击 ⋮ 修改其设置。
- 要避免触发特定的物体类型，取消选择不会触发该场景事件的物体类型。

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 *码流传输和存储 59*。

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. 转到雷达 > 流。
2. 在直播视图中单击 ⚙ 。
3. 选择视频格式 H.264。
4. 转到雷达 > 流 > 常规并增加压缩。

注

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（在网络存储下）。
3. 键入主机服务器的 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 *设置网络存储 22*

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

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，然后添加一个规则。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

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。

如果有人打开护罩，将触发警报

本示例解释了如果有人打开护罩，将如何触发警报。

添加接受者：

1. 转到系统 > 事件 > 接受者并单击添加接受者。
2. 键入接受者的名称。
3. 选择电子邮件。
4. 键入电子邮件地址以发送邮件。
5. 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是情况填写其余信息。
6. 要发送测试电子邮件，单击测试。
7. 单击保存。

创建一个规则：

8. 转到系统 > 事件 > 规则，然后添加一个规则。
9. 为规则键入一个名称。
10. 在条件列表中，选择外壳打开。
11. 在操作列表中，选择发送电子邮件通知。
12. 从列表中选择接受人。
13. 键入电子邮件的主题和消息。

14. 单击保存。

当侦测到运动时录制摄像机视频

本示例解释了如何设置雷达和摄像机，以便在雷达侦测到移动并在其后停止一分钟之前，摄像机开始录制到 SD 卡上。

连接设备：

1. 将电缆从雷达上的 I/O 输出连接到摄像机上的 I/O 输入。

配置雷达的 I/O 端口：

2. 转到系统 > 附件 > I/O 端口，并将 I/O 端口配置为输出，然后选择正常状态。

在雷达中创建规则：

3. 转到系统 > 事件，然后添加一个规则。
4. 为规则键入一个名称。
5. 从条件列表中，在雷达运动下选择场景。

   要设置场景，请参见*添加场景 19*。
6. 从操作列表中，选择当规则处于活动状态时切换 i/o，然后选择连接到摄像机的端口。
7. 单击保存。

配置摄像机的 i/o 端口：

8. 转到系统 > 附件 > I/O 端口，并将 I/O 端口配置为输入，然后选择正常状态。

在摄像机中创建规则：

9. 转到系统 > 事件，然后添加一个规则。
10. 为规则键入一个名称。
11. 从条件列表中，选择数字输入已激活，然后选择应触发规则的端口。
12. 从操作列表中，选择"录制视频"。
13. 从存储选项列表中选择 SD 卡。
14. 选择现有流配置文件或创建新的流配置文件。
15. 将预缓冲设置为 5 秒。
16. 将后缓冲设置为1 分钟。
17. 单击保存。

当侦测到运动时打开光

当入侵者进入侦测区域时，打开一种光会产生遏制的效果，同时还会提高录制入侵的视觉摄像机的图像质量。

此示例解释了如何设置雷达和照明器，以便当雷达在一分钟内侦测到运动并关闭时，照明器打开。

连接设备：

1. 通过雷达上的继电器端口将其中一个照明器电缆连接到电源。将其他电缆直接连接到电源和照明器之间。

配置雷达的继电器端口：

2. 转到系统 > 附件 > I/O 端口，然后选择开路作为继电器端口的正常状态。

在雷达中创建规则：

3. 转到系统 > 事件，然后添加一个规则。
4. 为规则键入一个名称。
5. 从条件列表中，在雷达运动下选择场景。

   要设置场景，请参见*添加场景 19*。
6. 从操作列表中，选择切换 I/O 一次，然后选择继电器端口。
7. 选择操作。
8. 设置持续时间。
9. 单击保存。

使用雷达控制 PTZ 摄像机

可以使用来自雷达的有关物体位置的信息来使 PTZ 摄像机跟踪物体。有两种方法可实现此操作：

- *使用内置雷达自动跟踪服务控制 PTZ 摄像机 25*. 内置选项适用于 PTZ 摄像机和雷达安装距离很靠近时。
- *使用 AXIS Radar Autotracking for PTZ 控制 PTZ 摄像机 26*. Windows 应用程序适用于要使用多个 PTZ 摄像机和雷达来跟踪物体时。

注

使用 NTP 服务器同步摄像机、雷达和 Windows 计算机上的时间。如果时钟不同步，则可能会出现跟踪延迟或迭影跟踪。

使用内置雷达自动跟踪服务控制 PTZ 摄像机

内置雷达自动跟踪创建了一个边缘到边缘的解决方案，其中雷达直接控制 PTZ 摄像机。其支持全部 Axis PTZ 摄像机。

本说明解释了如何将 PTZ 摄像机与雷达配对、如何校准以及如何设置物体跟踪。

注

您可以使用内置雷达自动跟踪服务将一个雷达与一台 PTZ 摄像机连接起来。对于想要使用多个雷达或 PTZ 摄像机的设置，请使用 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 26*。

将雷达与 PTZ 摄像机配对：

1. 转到系统 > 边缘到边缘 > PTZ 配对。
2. 输入 PTZ 摄像机的 IP 地址、用户名和密码。
3. 单击连接。
4. 单击配置雷达自动跟踪或转到雷达 > 自动跟踪设置雷达自动跟踪。

校准雷达和 PTZ 摄像机：

5. 转到雷达 > 自动跟踪。
6. 要设置摄像机的安装高度，转到摄像机安装高度。

7. 要水平转动 PTZ 摄像机，使其指向与雷达相同的方向，转到平移对齐。
8. 如果需要调整倾斜以补偿倾斜的地面，转到地面倾斜偏移，然后添加以度为单位的偏移量。

设置 PTZ 跟踪：

9. 转到跟踪以选择是否要跟踪人员、车辆和/或未知物体。
10. 要开始使用 PTZ 摄像机跟踪物体，打开跟踪。

    跟踪将自动聚焦一个或一组物体，以让它们保持在摄像机的画面中。
11. 如果预计有多个物体无法在摄像机视图中显示，请打开物体切换。

    使用此设置后，雷达会优先选择要跟踪的物体。
12. 要确定跟踪每个物体的秒数，请设置物体保持时间。
13. 要在雷达不再跟踪物体时让 PTZ 摄像机返回到其初始位，打开返回到初始位。
14. 要确定 PTZ 摄像机在返回到初始位前应在所跟踪物体最后已知位置停留的时间，请设置返回到初始位超时。
15. 要微调 PTZ 摄像机的变焦，请调整滑块上的变焦。

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，可以在跟踪物体时处理不同的设置：

- 使用一个雷达控制多台 PTZ 摄像机。
- 使用多个雷达控制一台 PTZ 摄像机。
- 使用多个雷达控制多台 PTZ 摄像机。
- 当安装在不同的位置覆盖同一区域时，使用一个雷达控制一台 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*。

网页界面

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

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，包括固件版本和序列号。
- 旧设备界面：将设备网页界面更改为旧版本。

状态

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 设置的日期和时间页面。

正在进行的录制

显示正在进行的录制及其指定的存储空间。

录制：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 *录制内容 33*

显示保存录制内容的存储空间。

网页界面

设备信息

显示设备信息，包括固件版本和序列号。

升级固件：升级设备上的固件。转到在其中进行固件升级的维护页面。

连接的客户端

显示连接和连接的客户端数量。

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

雷达

设置

常规

雷达传输：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。

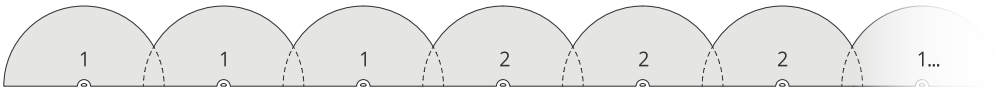
注

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。共存半径为 350 米（1148 英尺）。

- 0–1: 如果您在同一个共存区域中安装一个到两个雷达，请选择此选项。
- 2: 如果将三个雷达安装在同一个共存区域，请选择此选项。
- 3–5: 如果您在同一个共存区域中安装四个到六个雷达，请选择此选项。
  - 组：为您的雷达选择一个组（组 1 或组 2）。这还有助于避免干扰。我们建议您在每个组中添加三个雷达，并在同一个组中添加距离彼此邻近的雷达。



有关详细信息，请参见*安装多个雷达 6*。

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，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物体。
  - 忽略摆动的物体：打开以尽量减少摆动的物体（如树木、灌木丛或旗杆）发出的假警报。
  - 忽略小型物体: 打开以尽可能减少来自小型物体（如猫或兔子）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
  - 忽略摆动的物体：打开以尽量减少摆动的物体（如树木、灌木丛或旗杆）发出的假警报。

视图

信息说明：打开以显示包含雷达可侦测和跟踪的物体类型的图例。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。

物体可视化

轨迹寿命：选择所跟踪的物体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物体的图标样式。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物体移动的方向。

用图标显示信息：选择要显示在跟踪物体图标旁边的信息：

- 物体类型: 显示雷达检测到的物体类型。
- 分类概率: 显示雷达对物体分类是否正确的确定程度。
- 速度: 显示物体移动的快慢。

排除区域

排除区域是忽略移动物体的区域。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。

为排除分区选择一个区域形状预设。覆盖全部将区域设置为整个雷达覆盖区域。重置为方框会在覆盖区域的中间创建一个矩形。

要修改区域，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：如果您希望场景在物体在区域中移动时触发，请选择此选项。
- 越线：如果您希望场景在物体跨越一条或两条线时触发，请选择此项。

场景：在移动物体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，如果物体必须跨越两条线，请打开。
  - 更改方向：如果您希望场景在物体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:
  - 忽略短暂停留的物体：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。
  - 按物体类型触发：选择希望场景触发的物体类型(人、车辆、位置)。
  - 速度限制：以特定范围内的速度移动的物体触发。
  - 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：
  - 忽略短暂停留的物体：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物体。
  - 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物体。
  - 按物体类型触发：选择希望场景触发的物体类型(人、车辆、位置)。
  - 速度限制：以特定范围内的速度移动的物体触发。
  - 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。

地图校准

使用地图校准上传和校准参考地图。这将使人们更容易看到物体在雷达覆盖的区域内移动的位置。

上传地图：选择要上传的参考地图。

在地图上设置雷达位置：指定雷达在地图上的位置，在雷达正前方添加一个参考点，并键入雷达和参考点之间的距离。单击校准开始校准。

校准的结果是以适当比例显示雷达覆盖范围的参考地图。

流

常规

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。

帧速：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。

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

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。

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。

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修饰符，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`，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。
  - 大小：选择所需字体大小。
  - 外观：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。

- 场景注释  ：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，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。
  - 大小：选择所需字体大小。
  - 外观：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。
  - 外观：选择动画的颜色和背景色，如红色文本加透明背景（默认）。
  - 大小：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。
  - 叠加修饰符：选择叠加修饰符作为数据源。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。
  - 大小：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 轴
  - 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。
  - 叠加修饰符：选择叠加修饰符作为数据源。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。
  - 大小：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 轴
  - 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。

自动跟踪

将雷达与 PTZ 摄像机配对以使用雷达自动跟踪。要建立连接，请转至系统 > 边缘到边缘。

雷达 PTZ 自动跟踪

配置初始设置：

摄像机安装高度: 地面与 PTZ 摄像机安装高度之间的距离。

水平调整: 平移 PTZ 摄像机，使其指向与雷达相同的方向。单击 PTZ 摄像机的 IP 地址以访问 PTZ 摄像机。

保存水平转动偏移: 单击以保存平移对齐方式。

地面倾斜偏移: 使用地面倾斜偏移来微调摄像机的倾斜度。如果地面是倾斜的，或者摄像机不是水平安装，摄像机在跟踪物体时可能瞄准得太高或太低。

已完成: 单击以保存您的设置并继续配置。

配置 PTZ 自动跟踪：

跟踪： 选择是否要跟踪人员、车辆和/或未知物体。

跟踪： 打开以开始使用 PTZ 摄像机跟踪物体。跟踪将自动聚焦一个或一组物体，以让它们保持在摄像机的画面中。

物体切换： 如果雷达侦测器检测到有多个物体不适合 PTZ 摄像机的画面，PTZ 摄像机将跟踪雷达给出上限优先级的物体，并忽略其他物体。

物体保持时间: 确定 PTZ 摄像机跟踪每个物体时应持续的时间。

返回到初始位： 打开以在雷达不再跟踪物体时可以让 PTZ 摄像机返回到其初始位置。

返回到初始位超时: 确定 PTZ 摄像机在返回到初始位前应该停留在所跟踪物体新近已知位置的持续时间。

变焦： 使用滑块微调 PTZ 摄像机的变焦。

重新配置安装: 单击以清除各设置并返回到初始配置。

录制内容

正在进行的录制： 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。

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： 打开允许安装未签名的应用。

允许根权限应用： 打开以允许具有根权限的应用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

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：

- 开源许可证: 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*. 您需要牌照代码和 Axis 产品序列号才能生成牌照密钥。
- 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。
- 停用牌照：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。如果要停用牌照，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。如果不先停用牌照，则牌照将保持活动状态。

系统

时间和地点

日期和时间

时间格式取决于网页浏览器的语言设置。

注

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）：与连接到DHCP服务器的安全NTP密钥建立服务器同步。
  - 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。
- 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。
- 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。
- 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。

注

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。

公制（米、公里/小时）：选择距离按米测量，速度按公里/小时测量。

美国惯用（英尺、英里/小时）：选择距离按英尺测量，速度按英里/小时测量。

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，添加静态 IP 地址用作备用，请选择此项。

注

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：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 –。

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。

网页界面

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

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。

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。
- 一直：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。
- 否：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): 单击获取密码以获取拥有人的身份验证密钥。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 物体的团体名称。缺省值为公共。
  - 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。缺省值为写入。
  - 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

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’的账户的 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

证书

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。

过滤列表中的证书。

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。

IEEE 802.1x and IEEE 802.1AE MACsec

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）。

证书

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。默认选项是 EAP-TLS。

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。

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。

仅当您使用 EAP-TLS 作为身份验证方法时，这些设置才可用。

模式

- 动态 CAK / EAP-TLS：默认选项。安全连接后，设备会检查网络上的 MACsec。
- 静态 CAK /预共享密钥（PSK）：选择以设置连接到网络的键名称和值。

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。

IP 地址过滤器

使用过滤器: 选择以筛选允许访问设备的 IP 地址。

政策： 选择是否允许或拒绝访问特定 IP 地址。

地址: 输入允许或拒绝访问设备的 IP 编号。您也可使用 CIDR 格式。

自定义签名固件证书

要在设备上安装来自 Axis 的测试固件或其他自定义固件，您需要自定义签名的固件证书。证书验证固件是否由设备权利人和 Axis 批准。固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固件证书，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。在安装固件之前，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

添加账户： 单击以添加新账户。您可以添加多达 100 个账户。

账户： 输入仅有的账户名称。

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： 完全访问各设置。管理员也可以添加、更新和删除其他账户。
- 操作员： 有权访问不同设置，以下各项除外：
  - 全部系统设置。
  - 添加应用。
- 浏览者： 无法访问更改设置。

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。

网页界面

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。

账户：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

输入正确的值以确保您可以再次登录设备。

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。这将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

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*。

接收者

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。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

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 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。缺省值为 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

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账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 设备固件中的 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 的缺省值
- 8883 是 SSL 的 MQTT 的缺省值
- 80 是 WebSocket 的 MQTT的缺省值
- 443 是 WebSocket Secure 的 MQTT 的缺省值

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）。缺省值：60

设备主题前缀：在 MQTT 客户端选项卡上的连接消息和 LWT 消息中的主题缺省值中使用，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。

终了证明消息

终了证明（LWT）允许客户端在连接到中介时提供证明及其凭证。如果客户端在某点后仓促断开连接（可能是因为电源失效），它可以让代理向其他客户端发送消息。此终了证明消息与普通消息具有相同的形式，并通过相同的机制进行路由。

发送消息: 打开以发送消息。

使用默认设置: 关闭以输入您自己的默认消息。

主题： 输入默认消息的主题。

有效负载: 输入默认消息的内容。

保留： 选择以保留此主题的客户端状态

QoS: 更改数据包流的 QoS 层。

MQTT 出版

使用默认主题前缀: 选择以使用默认主题前缀，即在 MQTT 客户端选项卡中的设备主题前缀的定义。

包括主题名称： 选择以包含描述 MQTT 主题中的条件的主题。

包括主题命名空间： 选择以将 ONVIF 主题命名空间包含在 MQTT 主题中。

包含序列号： 选择以将设备的序列号包含在 MQTT 有效负载中。

+ 添加条件: 单击以添加条件。

保留： 定义将哪些 MQTT 消息作为保留发送。

- 无： 全部消息均以不保留状态发送。
- 性能： 仅将有状态消息作为保留发送。
- 全部: 将有状态和无状态消息发送为保留。

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

在添加 MQTT 叠加修饰符之前，请连接到 MQTT 代理。

+ 添加叠加修饰符：单击以添加新的叠加修饰。

主题筛选器：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。

修饰符：当您创建叠加时，请使用结果修饰符。

- 以 #XMP 开头的修饰符显示从主题接收到的数据。
- 以 #XMD 开头的修饰符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。
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。
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。

板载存储

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 SD 卡已满，则会在选定时间段过去之前删除旧录音。

工具

- 检查：检查 SD 卡上是否存在错误。这仅对 ext4 文件系统有效。
- 修复：修复 ext4 文件系统中的错误。要修复 VFAT 文件系统的 SD 卡，请弹出 SD 卡，然后将其插入计算机，并执行磁盘修复。
- 格式化：例如，当您需要更改文件系统或快速清除数据时，格式化 SD 卡。VFAT 和 ext4 是两个可用的文件系统选项。推荐的格式是 ext4，因为它能在卡弹出或突然断电时灵活地防止数据丢失。但需要使用第三方 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。加密会删除 SD 卡上存储的数据。使用加密后，存储在 SD 卡上的数据得到保护。
- 解密：使用此工具在不加密的情况下格式化 SD 卡。解密会删除 SD 卡上存储的数据。使用解密后，存储在 SD 卡上的数据失去保护。
- 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。

帧速：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 31*。

保护音频  ：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。

账户：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

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。

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

冲击侦测

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，然后 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 V DC 时，设备上的输入为开路。

注

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。

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

自动配对让你使用兼容的 Axis 网络扬声器，就如同它是住设备的一部分。配对后，网络扬声器充当音频输出设备，您可以播放音频片段并传输声音。

重要

要使此功能与视频管理软件 (VMS) 配合使用，您要首先将设备与扬声器配对，然后将设备添加到 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。

音频配对

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。

扬声器配对：选择配对网络扬声器。

清除字段：单击以清除各字段。

连接：单击以建立与扬声器的连接。

PTZ 配对 允许您将雷达与 PTZ 摄像机配对以使用自动跟踪。自动跟踪使 PTZ 摄像机根据雷达提供的有关物体位置的信息跟踪物体。

PTZ 配对

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 摄像机账户的密码。

清除字段: 单击以清除各字段。

连接： 单击以建立与 PTZ 摄像机的连接。

配置雷达自动跟踪: 单击以打开并配置自动跟踪。您也可以转到雷达>自动跟踪进行配置。

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。

网络跟踪

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，网络跟踪文件可帮助您排除问题。

跟踪时间： 选择以秒或分钟为单位的跟踪持续时间，并单击下载。

远程系统日志

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

+ 服务器：单击以添加新服务器。

主机：输入服务器的主机名或 IP 地址。

格式化：选择要使用的 syslog 消息格式。

- Axis
- RFC 3164
- RFC 5424

协议：选择要使用的协议和端口：

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

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

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*设置恢复为出厂缺省值。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

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

各 Axis 设备固件均经过数字签名以确保仅在设备上安装经过验证的固件。这会进一步提高 Axis 设备的总体网络安全级别门槛。有关更多信息，请参阅 *axis.com* 白皮书"签名固件、安全启动和私人密钥的安全“。

固件升级：升级到新的固件版本。新固件版本中可能包含改进的功能、补丁和新功能。建议您始终使用更新版本。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：升级到新的固件版本。
- 出厂默认设置：更新并将设置都恢复为出厂缺省值。当您选择此选项时，无法在升级后恢复到以前的固件版本。
- 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固件版本。

固件还原：恢复为先前安装的固件版本。

验证您的安装

验证雷达的安装

注

此测试可帮助您在当前条件下验证安装。场景中的变化可能会影响安装的日常性能。

但是，在安装雷达后，我们建议您先进行验证，然后再开始使用。这可帮助您识别安装或管理场景中的对象（如树和反射表面）的问题，从而提高雷达的准确性。

首先，*校准雷达 18*。

建议在以下情况下执行验证：

- 场景中有您要排除的物体，以便区域可以包含某些物体，如植物或金属表面。
- 您可将雷达与 PTZ 摄像机配对，并配置雷达自动跟踪。
- 已更改雷达安装高度。

验证雷达

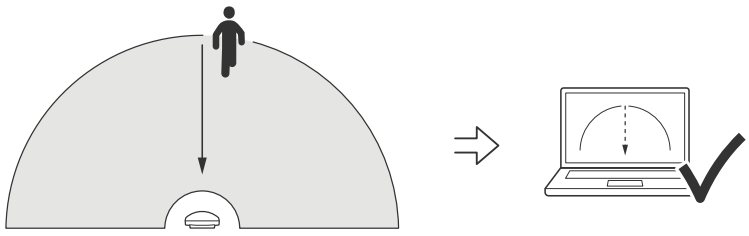
检查是否没有假侦测

1. 检查侦测区域内是否没有人员活动。
2. 等待几分钟，确保雷达未在侦测区域中侦测到静态物体。
3. 如果没有不想要的侦测，您可跳过步骤 4。
4. 如果存在不需要的侦测，请了解如何过滤掉特定类型的移动或物体，更改覆盖范围，或在*大幅度减少假警报 21*中调整侦测灵敏度。

当雷达从正面接近时，检查正确的符号和移动方向

1. 进入雷达网页界面并录制会话。要获得执行此操作的帮助，请转到 *录制并观看视频 22*。
2. 在雷达的前方开始 60 米（197 英尺），直接向雷达方向前进。
3. 在雷达的网页界面中检查会话。当您被检测到时，人员分类的符号应显示。
4. 检查雷达的网页界面是否显示了正确的移动方向。

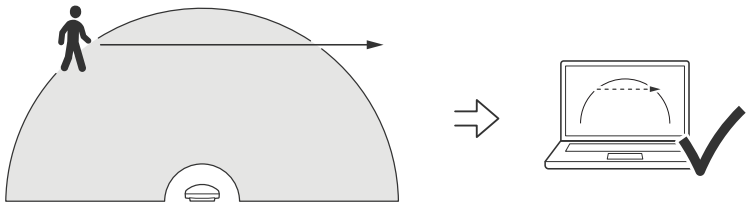
验证您的安装



当雷达从侧面接近时，检查正确的符号和移动方向

1. 进入雷达网页界面并录制会话。要获得执行此操作的帮助，请转到 *录制并观看视频 22*。
2. 从雷达开始 60 米（197 英尺），然后穿过雷达覆盖区域。
3. 检查雷达的网页界面是否显示了人员分类的符号。
4. 检查雷达的网页界面是否显示了正确的移动方向。

验证您的安装



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	注释
1. 检查区域清除时是否出现不想要的侦测		
2a. 当雷达从前面接近时，检查是否已检测到具有“人”的正确符号的物体		
2b. 当雷达从正面接近时，请检查移动方向是否正确		

3a. 当雷达从侧面接近时，检查是否已检测到具有“人”的正确符号的物体		
3b. 当雷达从侧面接近时，请检查移动方向是否正确		

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. 请确保您已配置了雷达并已按照说明操作。
2. 要进行进一步验证，请添加和校准引用映射。
3. 当侦测到适当的物体时，设置雷达场景以触发。默认情况下，触发前秒数设置为两秒，但如果需要，您可以在网页界面中更改此设置。
4. 当侦测到适当的物体时，设置雷达以记录数据。

   请参见*录制并观看视频 22*阅读有关说明。
5. 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，可以禁用。
6. 沿雷达覆盖区域的边框进行遍历，确保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。

了解更多

码流传输和存储

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

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。要购买其他牌照，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。

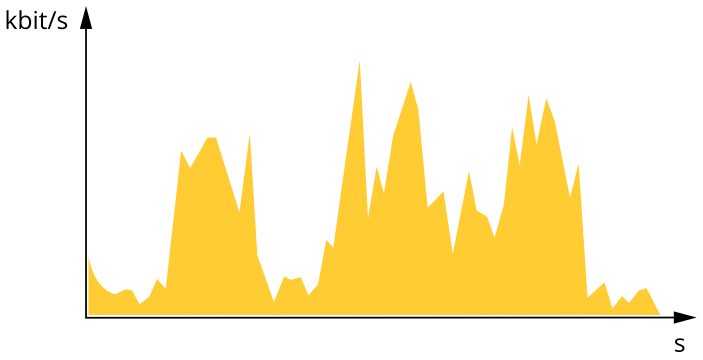
注

- 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。要购买其他牌照，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。

比特率控制

比特率控制帮助您管理视频流的带宽消耗。

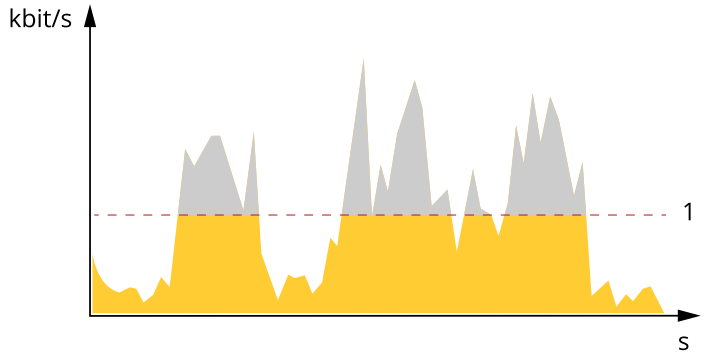
可变比特率 (VBR)
可变比特率允许带宽消耗根据场景中的活动水平而变化。活动越多，需要的带宽就越大。借助可变比特率，您可保证图像质量恒定，但您需要确保具有存储容量。



了解更多

上限比特率 (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。

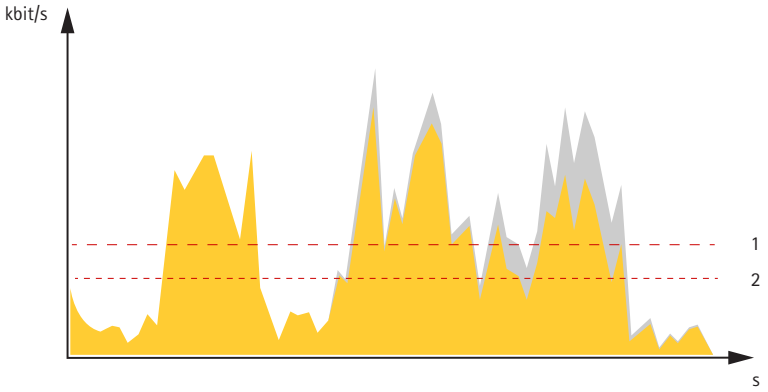


1 目标比特率

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：

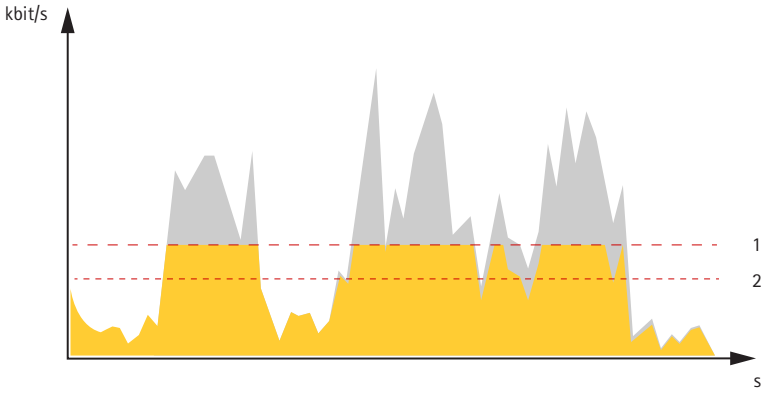
- 要计算预计存储需求，请设置目标比特率和保留时间。
- 使用目标比特率计算器，根据可用存储和所需的保留时间计算平均比特率。



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。

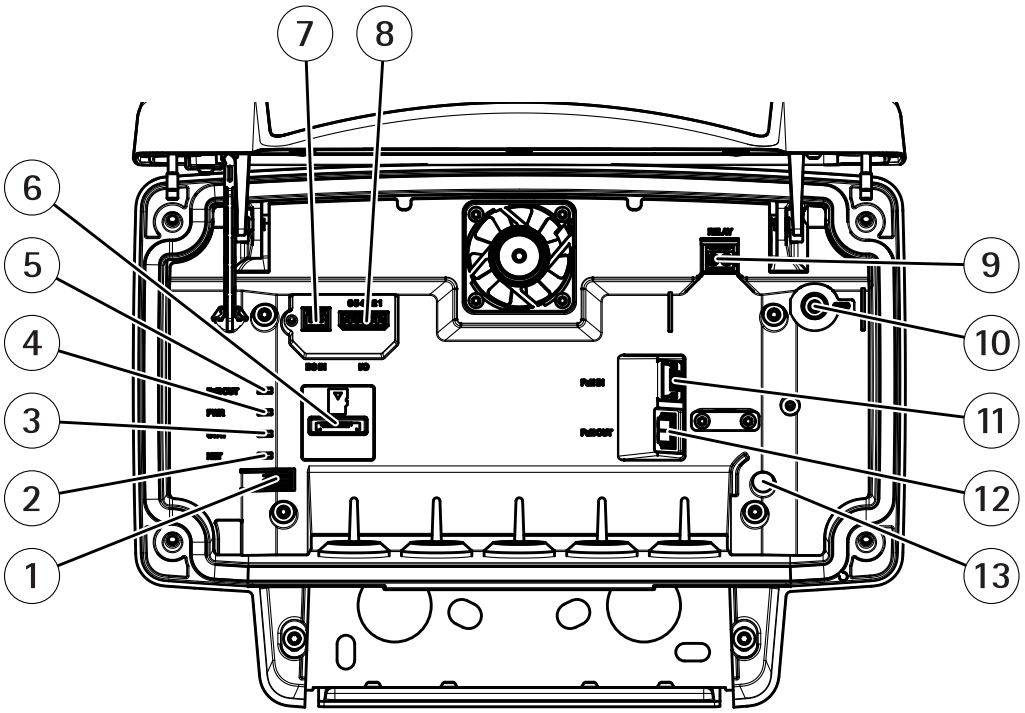
了解更多



1 目标比特率
2 实际平均比特率

规格

产品概览



1 控制按钮
2 网络指示灯
3 LED 状态指示灯
4 电源灯
5 PoE 输出 LED
6 microSD 卡插槽
7 电源连接器 (DC)
8 I/O 连接器
9 中继连接器
10 接地螺丝
11 网络连接器（PoE 输入）
12 网络连接器（PoE 输出）
13 入侵报警传感器

有关技术规格，请参见*规格 62*。

LED 指示灯

LED 状态指示灯	指示
绿色	绿色常亮表示正常工作。

规格

LED 网络指示灯	指示
绿色	常亮表示连接到 100 Mbit/s 网络。闪烁表示网络活动。
琥珀色	常亮表示连接到 10 Mbit/s 网络。闪烁表示网络活动。
不亮	无网络连接。

LED 电源指示灯	指示
绿色	工作正常。

PoE 输出 LED	指示
不亮	PoE 输出关闭
绿色	PoE 输出打开

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

有关控制按钮的位置，请参见*产品概览 62*。

控制按钮用于：

- 将产品恢复至出厂默认设置。请参见*67*。
- 连接至 AXIS Video Hosting System 服务。请参见。若要连接，请按住该按钮约 3 秒，直到状态 LED 呈绿色闪烁。

连接器

网络连接器

采用以太网供电 增强版 (PoE+) 的 RJ45 以太网连接器。

▲警示

设备损坏风险。请勿使用 PoE 和 DC 为设备供电。

网络连接器（PoE 输出）

以太网供电 IEEE 802.3at 2 型，最大 30W

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。

规格

注

PoE 输出在雷达由 60 W 中跨（PoE IEEE 802.3bt，3 型）供电时启用。

注

如果雷达通过 30 W 中跨或直流电源供电，将禁用 PoE。

注

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

注

如果已连接的 PoE 设备需要 30 W 以上，则您可在雷达和设备的 PoE 输出端口之间添加一个 60 W 的中跨。中跨将为设备供电，而安全雷达将提供以太网连接。

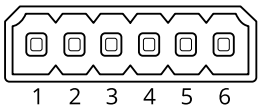
I/O 连接器

使用 I/O 连接器连接外部设备，并结合应用事件触发和报警通知等功能。除 0 V DC 参考点和电源（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。

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。

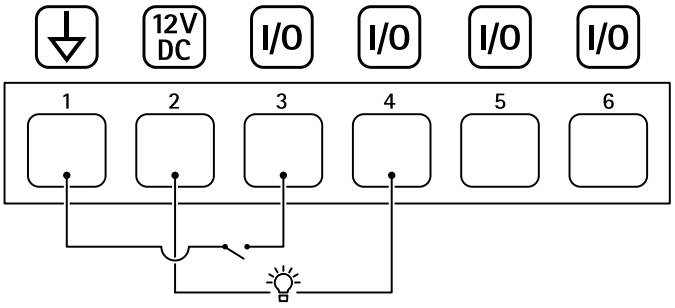
6 针接线端子



功能	针脚	备注	规格
DC 接地	1		0 V DC
DC 输出	2	可用于为辅助设备供电。 备注： 此针脚只能用作电源输出。	12 V DC 最大负载= 50 mA
可配置（输入或输出）	3–6	数字输入 – 连接至针 1 以启用，或保留浮动状态（断开连接）以停用。	0 至最大 30 V DC
		数字输出 – 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 V DC，开漏，100 mA

示例:

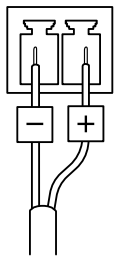
规格



1 DC 接地
2 DC 输出 12 V，最大 50 mA
3 I/O 配置为输入
4 I/O 配置为输出
5 可配置的 I/O
6 可配置的 I/O

电源连接器

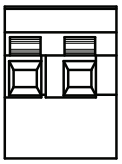
2 针接线端子，用于 DC 电源输入。使用额定输出功率限制为 ≤100 W 或额定输出电流限制为 ≤5 A 且符合安全超低电压 (SELV) 要求的限制电源 (LPS)。



⚠警示

设备损坏风险。请勿使用 PoE 和 DC 为设备供电。

中继连接器



⚠警示

使用用于中继连接器的单芯电线。

功能	规格
类型	正常开启
额定电压	24 V DC/5 A
与其他电路绝缘	2.5 kV

清洗建议

清洗建议

如果设备出现油渍或严重污垢，可以使用温和的无溶剂肥皂或清洁剂进行清洁。

注意

千万不要使用强力洗涤剂，例如汽油、笨或丙酮。

1. 使用罐装压缩空气，将已有灰尘或散落的灰尘从设备上移除。
2. 使用轻度洗涤剂和温水浸湿的软布清洁设备。
3. 使用干布小心擦拭。

注

避免在直射阳光或更高的温度下清洁，因为这可能会在水滴干时引起锈斑。

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）重置为出厂缺省值。

将产品恢复至出厂默认设置：

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*产品概览 62*。
3. 按住控制按钮 15–30 秒，直到 LED 状态指示灯呈琥珀色闪烁。
4. 松开控制按钮。当 LED 状态指示灯变绿时，此过程完成。产品已重置为出厂默认设置。如果网络上没有可用的 DHCP 服务器，则默认 IP 地址为 `192.168.0.90`。
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。

检查当前固件版本

固件是决定网络设备功能的软件。当您进行问题故障排查时，我们建议您从检查当前固件版本开始。新固件版本可能包含能修复您的某个特定问题的校正。

要检查当前固件：

1. 转到设备的网页界面 > 状态。
2. 请参见设备信息下的固件版本。

升级固件

重要

- 在升级固件时，将保存预配置和自定义设置（如果这些功能在新固件中可用），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

使用活动跟踪中的新固件升级设备时，产品将获得可用的新功能。在升级固件之前，始终阅读每个新版本提供的升级说明和版本注释。要查找更新固件和发布说明，请转到 *axis.com/support/device-software*。

1. 将固件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 > 固件升级，然后单击升级。

升级完成后，产品将自动重启。

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。

固件升级问题

固件升级失败	如果固件升级失败，该设备将重新加载以前的固件。比较常见的原因是上载了错误的固件文件。检查固件文件名是否与设备相对应，然后重试。
固件升级后出现问题	如果您在固件升级后遇到问题，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 地址>: 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。
可能是 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栏中手动键入 `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 *重置为出厂默认设置 67*。
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 Companion：免费，适用于有基本监控需求的小型系统。
- AXIS Camera Station：30 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*。

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 MQTT 的使用。请与服务器/代理提供商确认是否支持 ALPN 以及要使用的 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所需带宽量（比特率）的影响。

以下因素是重要的考虑因素：

- 由于基础设施差而导致的高网络利用率会影响带宽。

用户手册
AXIS D2110–VE Security Radar

版本 M21.3
日期： 一月 2024
零件号 T10145149