AXIS A8207–VE Network Video Door Station

用户手册

目录

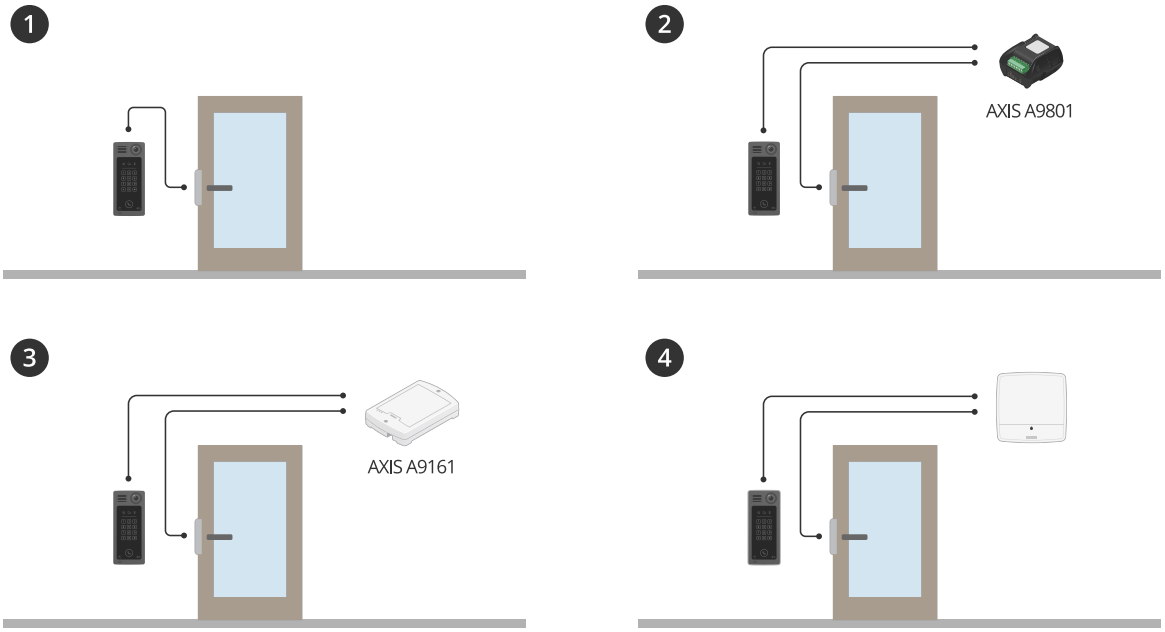
解决方案概述 4
产品概述 5
安装 7
开始 8
在网络上查找设备 8
打开设备的网页界面 8
为 root 用户设置一个新密码 8
安全密码 8
验证没有人篡改过固件 9
网页界面概览 9
配置设备 10
更改root用户密码 10
设置直连 SIP (P2P) 10
通过服务器设置 SIP (PBX) 10
创建一位联系人 11
配置呼叫按钮 12
设置为阅读器 – 网络连接 12
设置为阅读器 – 有线连接 12
使用 DTMF 为来访者开门 13
将实时视频传输至一个监视器 14
设备界面 15
状态 15
通信 16
视频 20
阅读器 28
音频 29
录制内容 30
应用 31
系统 32
维护 49
了解更多 50
IP 语音 (VoIP) 50
设置事件规则 51
应用 52
日常使用 53
使用键盘 53
故障排查 54
重置为出厂默认设置 54
检查当前固件版本 54
升级固件 54
技术问题、线索和解决方案 54
性能考虑 55
规格 57
前面板指示灯和控制 57
LED 指示灯 57
SD 卡插槽 57

目录

按钮 57
连接器 58
安全信息 62
危险等级 62
其他消息等级 62

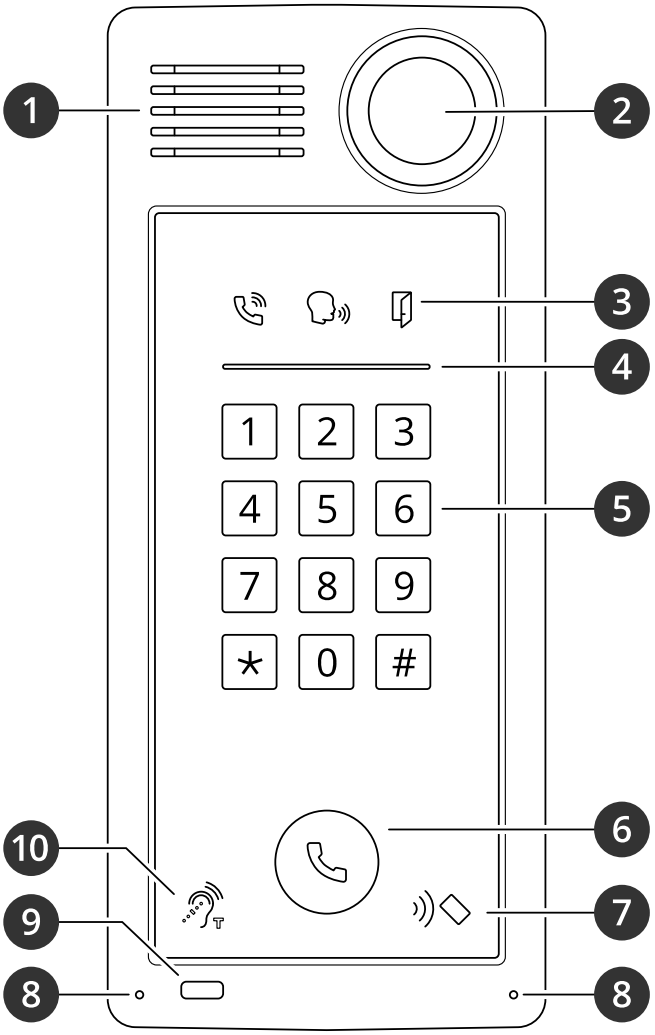
解决方案概述

解决方案概述



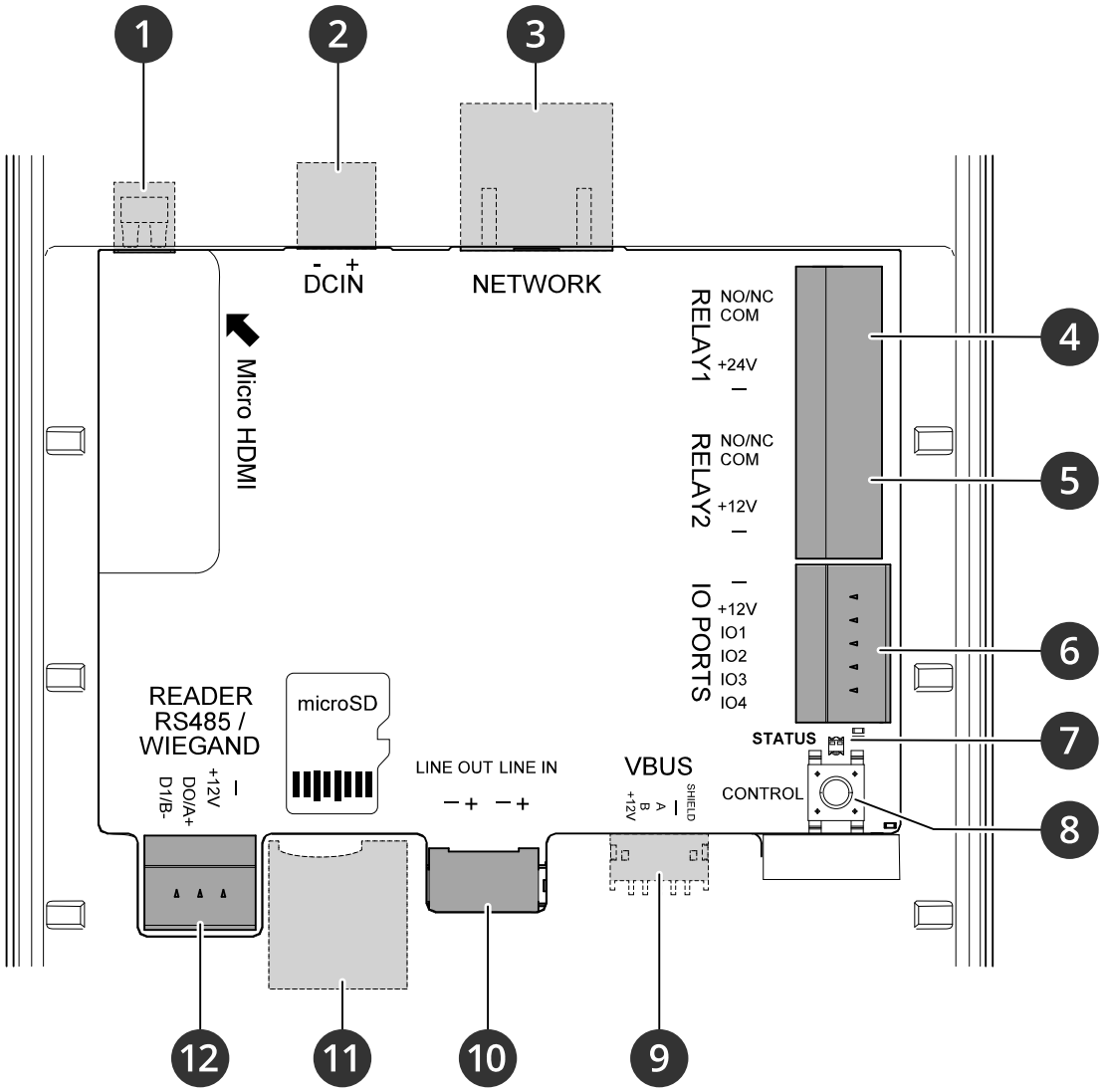
1 门站
2 门站与 AXIS A9801 配合使用
3 门站与 AXIS A9161 配合使用
4 门站与某个访问控制系统配合使用，例如 AXIS A1001 或 AXIS A1601

产品概述



1 扬声器
2 摄像机
3 呼叫指示器图标 57
4 阅读器指示条 57
5 键盘
6 呼叫按钮 57
7 阅读器图标
8 麦克风
9 PIR 传感器
10 电感线圈图标

产品概述



1 *HDMI 连接器 58（微型 HDMI）*
2 *电源连接器 60*
3 *网络连接器 58 (PoE+)*
4 *继电器连接器 58*
5 *继电器连接器 58*
6 *I/O 连接器 59*
7 *LED 状态指示灯*
8 *控制按钮 58*
9 *2N VBUS（未使用）*
10 *音频连接器 58*
11 *SD 卡插槽 57 (microSD/microSDHC/microSDXC)*
12 *阅读器连接器 59*

安装

要观看此视频，请转到本文档的网页版本。

help.axis.com/?&piaId=44899&section=solution-overview

A8207-VE 阅读器的安装视频。

要观看此视频，请转到本文档的网页版本。

help.axis.com/?&piaId=44899&section=solution-overview

A8207-VE 继电器安装视频。

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。*

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

打开设备的网页界面

1. 打开一个浏览器，键入 Axis 设备的 IP 地址或主机名。

   如果您不知道 IP 地址，请使用 AXIS IP Utility 或 AXIS Device Manager 在网络上查找设备。

2. 键入用户名和密码。如果您是首次访问设备，则必须设置 root 用户密码。请参见 *为 root 用户设置一个新密码 8*。

为 root 用户设置一个新密码

默认管理员用户名为 `root`。无默认根帐户密码。您首次登录设备时设置密码。

1. 键入密码。请按照安全密码的相关说明操作。请参见 *安全密码 8*。
2. 重新键入密码以确认拼写。
3. 单击添加用户。

重要

如果丢失了根帐户密码，请转到 *重置为出厂默认设置 54*并按照说明进行操作。

安全密码

重要

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

设备密码是对数据和服务的主要保护。Axis 设备不会强加密码策略，因为它们可能会在不同类型的安装中使用。

为保护您的数据，我们强烈建议您：

- 使用至少包含 8 个字符的密码，而且密码建议由密码生成器生成。
- 不要泄露密码。
- 定期更改密码，至少一年一次。

验证没有人篡改过固件

要确保设备具有其原始的 Axis 固件，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 54*。

   重置后，安全启动可保证设备的状态。
2. 配置并安装设备。

网页界面概览

该视频为您提供设备网页界面的概览。



Axis 设备网页界面

配置设备

本部分介绍了安装程序在硬件安装完成后启动和运行产品所需的全部重要配置。

更改root用户密码

1. 登录到设备界面，并转到系统 > 用户。
2. 对于根用户，请单击 ⋮ > 更新用户。
3. 输入新密码并保存。

设置直连 SIP (P2P)

VoIP（IP 语音）是一组支持通过 IP 网络进行语音和多媒体通信的技术。有关详细信息，请参见 *IP 语音 (VoIP) 50*。

在该产品中，VoIP 通过 SIP 协议启用。如需了解更多关于 SIP 的信息，请参见 *会话初始化协议 (SIP) 50*

SIP 有两种类型的设置。其中一种是点对点。如果是同一 IP 网络内少数用户代理之间的通信且无需 PBX 服务器可提供的额外功能，则使用点对点。如需了解关于如何安装的信息，请参见 *点对点 SIP (P2PSIP) 50*。

1. 转到通信 > SIP > SIP 设置，然后选择启用 SIP。
2. 要允许设备接收呼入，选择允许呼入。

注意

当您允许呼入时，设备会接受来网络中不同设备的呼叫。如果可从公共网络或互联网访问该设备，我们建议您不要允许呼入。

3. 单击呼叫处理。
4. 在呼叫超时中，设置在无应答时呼叫在结束前持续的秒数。
5. 如果您已允许呼入，请在呼入超时中设置呼入超时前的秒数。
6. 单击端口。
7. 输入 SIP 端口号和 TLS 端口号。

注

- SIP 端口 – 对于 SIP 会话。通过此端口的信令流量为非加密。默认端口号为 5060。
- TLS 端口 – 对于 SIPS 和 TLS 保护的 SIP 会话。通过此端口的信令流量使用传输层安全协议 (TLS) 进行加密。默认端口号为 5061。
- RTP 起始端口 – 输入 SIP 呼叫中用于首个 RTP 媒体流的端口。媒体传输的默认开始端口为 4000。有些防火墙可能会阻止某些端口号上的 RTP 通信。端口号必须在 1024 到 65535 之间。

8. 单击NAT 穿越。
9. 选择要启用 NAT 穿越功能的协议。

注

当设备从 NAT 路由器或防火墙后方连接到网络时，使用 NAT 穿越。有关详细信息，请参见 。

10. 单击保存。

通过服务器设置 SIP (PBX)

VoIP（IP 语音）是一组支持通过 IP 网络进行语音和多媒体通信的技术。有关详细信息，请参见 *IP 语音 (VoIP) 50*。

在该设备中，VoIP 通过 SIP 协议启用。如需了解更多关于 SIP 的信息，请参见 *会话初始化协议 (SIP) 50*

SIP 有两种类型的设置。其中一种是 PBX 服务器。当应在 IP 网络内外的无数用户代理之间进行通信时，使用 PBX 服务器。可以在设置中添加其他功能，具体取决于 PBX 供应商。有关详细信息，请参见 *专用分支交换机 (PBX) 51*。

1. 请求您的 PBX 供应商提供以下信息：
   - 用户 ID
   - 域
   - 密码
   - 身份验证 ID
   - 呼叫者 ID
   - 注册服务器
   - RTP 开始端口
2. 转到通信 > SIP > SIP 账户，然后单击 + 账户。
3. 输入账户名称。
4. 选择已注册。
5. 选择一种传输模式。
6. 添加 PBX 供应商提供的账户信息。
7. 单击保存。
8. 使用与点对点相同的方法创建 SIP 设置，请参见 *设置直连 SIP (P2P) 10*。使用 PBX 供应商的 RTP 启动端口。

创建一位联系人

本示例说明了如何在联系人列表中创建一位新的联系人。在您开始之前，请在通信 > SIP 中启用 SIP。

要创建一位新联系人：

1. 转到通信 > 联系人列表。
2. 单击 + 添加联系人。
3. 输入联系人的姓名。
4. 输入联系人的 SIP 地址。

注

有关 SIP 地址的信息，请参见 *会话初始化协议 (SIP) 50*。

5. 选择用于发出呼叫的 SIP 帐号。

注

可用性选项在系统 > 事件 > 时间表中定义。

6. 选择联系人的可用性。如果在联系人不可用时有呼叫，呼叫将被取消，除非有备用联系人。

注

备用联系人是一个在原始联系人未作出回应或不可用时可将电话转接的对象。

7. 在备用联系人中，选择无。
8. 单击保存。

配置呼叫按钮

在默认情况下，将呼叫按钮配置为进行 VMS（视频管理系统）呼叫。如果您想保留此配置，您仅需将 Axis 对讲机添加至 VMS。

本示例说明了如何设置系统以在来访者按下呼叫按钮时呼叫联系人列表中的联系人。

1. 转到通信 > 呼叫 > 呼叫按钮。
2. 关闭在视频管理系统 (VMS) 中发起呼叫。
3. 在接受者下，选择一个联系人。

要禁用呼叫按钮，关闭启用呼叫按钮。

设置为阅读器 – 网络连接

要将门站用作一个阅读器，必须将其连接至一个门控制器。该门控制器存储凭证并保持追踪允许进门的人员。在此示例中，我们通过网络连接设备。我们还修改允许的卡类型。

重要

网络连接仅对 Axis 门禁控制器有用。要连接至某个非 Axis 门禁控制器，你需要用电线物理连接这些设备。请参见 *设置为阅读器 – 有线连接 12*。

在您开始之前

使用针对阅读器的 Wiegand 协议配置该门禁控制器的硬件。有关说明的信息，请参见门禁控制器用户手册。

将门站设置为一个读卡器

1. 转到读卡器 > 读卡器协议 。
2. 选择 VAPIX 阅读器协议类型。
3. 选择用于与门禁控制器通信的协议。

注

如果您使用的是 HTTPS ，我们建议打开验证证书。

4. 输入门禁控制器的 IP 地址。
5. 输入门禁控制器的凭证。
6. 单击连接。
7. 选择适当门的入口阅读器。
8. 单击保存。

设置为阅读器 – 有线连接

要将门站用作一个阅读器，则你必须将其连接至一个门控制器。该门控制器存储凭证并保持追踪允许进门的人员。在此示例中，我们通过电线连接设备，我们使用 Wiegand 协议，激活蜂鸣器并使用一个适用于 LED 的 I/O 端口。我们还修改允许的卡类型。

重要

使用尚未使用的 I/O 端口。如果你使用了已经使用的 I/O 端口，那么针对这些端口创建的事件都将停止工作。

在您开始之前

- 将门站连接至门禁控制器，请参见 *电气接线图*。
- 使用针对阅读器的 Wiegand 协议配置该门禁控制器的硬件。有关说明的信息，请参见门禁控制器用户手册。

将门站设置为一个读卡器

1. 转到读卡器 > 读卡器协议 。
2. 选择 Wiegand 。
3. 打开 蜂鸣器。
4. 在蜂鸣器输入下，选择 I3。
5. 在用于 LED 控制的输入中，选择 1。
6. 在 LED1 输入下，选择 I1。
7. 选择不同状态所使用的颜色。
8. 在 按键格式下，选择 FourBit。
9. 单击保存。
10. 转到读卡器 > 芯片类型并激活要使用的芯片类型。

注

您可以保留默认的芯片类型集，但我们建议根据您的具体需求修改该列表。

11. 单击添加数据集 以指定不同芯片类型的数据组。
12. 单击保存。

使用 DTMF 为来访者开门

当来访者从门站进行呼叫时，接听人员可使用其 SIP 设备的双音多频 (DTMF) 信号发送装置来开门。门禁控制器可开门和锁门。

本示例说明了如何进行操作：

- 定义门站的 DTMF 信号
- 将门站设置为：
  - 请求门禁控制器开门，或
  - 使用内部继电器开门。

您可在门站网页上进行设置。

在您开始之前

- 允许从该设备进行 SIP 呼叫并设置一个 SIP 帐号。请参见 *设置直连 SIP (P2P) 10* 和 *通过服务器设置 SIP (PBX) 10*。

定义门站的 DTMF 信号

1. 转到通信 > SIP > SIP 账户并找到 SIP 账户。
2. 单击 ⋮ > 编辑。
3. 单击 DTMF。
4. 单击 + DTMF 序列。
5. 在序列字段中，输入“1”。
6. 在描述字段中，输入“解锁门”。
7. 单击保存。

设置门站，以使用内部继电器解锁门

8. 转到系统 > 事件 > 规则，然后添加一个规则。
9. 在名称字段中，输入“DTMF 解锁门”。
10. 从条件列表中，在呼叫下，选择 DTMF 和解锁门。
11. 从操作列表中，在 I/O下，选择 切换 I/O 一次。
12. 从端口列表中，选择 继电器 1。
13. 将持续时间更改为 00:00:07，这意味着门将打开 7 秒。
14. 单击保存。

将实时视频传输至一个监视器

你的设备可在无网络连接的情况下将一个实时视频流传输至一个 HDMI 监视器。通过监视器查看谁在门口。

1. 将一个外部监视器连接至 HDMI 接口。
2. 在 系统 > 视频输出中调整 HDMI 设置。

设备界面

设备界面

要达到设备界面，在 web 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。
- 更改用户：退出当前用户并登录新用户。
- 退出：退出当前用户。

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 和许可证的信息。
- 关于：查看设备信息，包括固件版本和序列号。
- 旧设备界面: 将设备接口更改为旧设备接口。

状态

设备信息

显示设备信息，包括固件版本和序列号。

升级固件：单击转到可在其中进行固件升级的维护页面。

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：单击转到可更改 NTP 设置的日期和时间页面。

安全

显示对活动设备的访问类型以及正在使用的加密协议。对设置的建议基于《AXIS OS 强化指南》。

强化指南：单击转到*《AXIS OS 强化指南》*，您可在其中了解有关如何应用网络安全理想实践的更多信息。

连接的客户端

查看详细信息：单击显示了与设备连接的客户端。

持续录制中

录像：显示每个正在进行的录制内容及其来源。有关详细信息，请参见 *录制内容 30*

显示保存录制内容的存储空间。

通信

联系人名单

联系人

单击可将联系人列表下载为 json 文件。

单击导入联系人列表（json）。

添加联系人：单击此处，将新联系人添加到联系人列表中。

名字：输入联系人的名字。

姓氏：输入联系人的姓氏。

快速拨号：输入联系人的可用快速拨号号码。此号码用于从设备呼叫联系人。

SIP 地址：输入联系人的 IP 地址或分机号。

：单击以进行测试调用。当应答时，呼叫将自动结束。

SIP 账户：选择要用于从设备呼叫联系人的 SIP 账户。

可用性：选择联系人的可用性时间表。如果在联系人不可用时尝试呼叫，呼叫将被取消，除非有备用联系人。

备用：如果适用，请从列表中选择一个备用联系人。

上下文菜单包括：

编辑联系人：编辑联系人的属性。

删除联系人：删除联系人。

设备界面

组

单击可将联系人列表下载为 json 文件。

单击导入联系人列表（json）。

添加组：单击以创建新的现有联系人组。

名称：为组输入一个名称。

快速拨号：输入组的可用快速拨号号码 此号码用于从设备呼叫组。

接受者：选择要包括在组中的联系人。呼叫将同时发送给大多数接受者。接受者数量上限为 6。

备用: 如果适用，请从列表中选择一个备用联系人。

上下文菜单包括：

编辑组：编辑组的属性。

删除组：删除组。

SIP

SIP 设置

会话初始协议 (SIP) 用于用户间的交互式通信会话。该会话可包含音频和视频。

启用 SIP: 选中此选项，可以初始化和接收 SIP 呼叫。

允许呼入：勾选此选项以允许来自其他 SIP 设备的呼入。

呼叫处理

- 呼叫超时t: 设置在无应答的情况下，一个呼叫在结束前可持续的时间上限（上限为 10 分钟）。
- 呼入持续时间: 设置一个呼入可持续的时间上限（上限为 10 分钟）。
- 在这之后结束呼叫：设置一个呼叫可持续的上限时间（上限为 60 分钟）。如果您不想限制呼叫长度，请选择无限期呼叫持续时间。

端口

端口号要在 1024 到 65535 之间。

- SIP 端口：用于 SIP 通信的网络端口。通过此端口的信令流量为非加密。默认端口号为 5060。如果需要，输入一个不同的端口号。
- TLS 端口：用于已加密 SIP 通信的网络端口。通过此端口的信令流量使用传输层安全协议 (TLS) 进行加密。默认端口号为 5061。如果需要，输入一个不同的端口号。
- RTP 开始端口：SIP 呼叫中用于第一个 RTP 媒体流的网络端口。默认开始端口号为 4000。一些防火墙会拦截某些端口号上的 RTP 通信。

NAT 穿透

当设备位于某个专用网络 (LAN)，并且您希望使它在该网络之外可用时，则使用 NAT（网络地址转换）穿透。

注

要使 NAT 穿透发挥作用，则要使用支持其的路由器。该路由器还要支持 UPnP®。

每个 NAT 穿透协议可单独使用或组合使用，具体取决于网络环境。

- ICE: ICE（交互式连接建立）协议可增加找到点设备之间进行成功通信的有效路径的机会。如果您还启用了 STUN 和 TURN，则您可提高 ICE 协议的机会。
- STUN: STUN（NAT 会话遍历实用程序）是一个客户端服务器网络协议，可让设备确定是否其位于 NAT 或防火墙的后方，如果是的话，则获取映射的公共 IP 地址和分配用于连接至远程主机的端口号。输入 STUN 服务器地址，例如一个 IP 地址。
- TURN: TURN（通过中继方式穿越 NAT）是一个可让 NAT 路由器或防火墙后方的设备通过 TCP 或 UDP 接收其他主机的呼入数据的协议。输入 TURN 服务器地址和登录信息。

音频和视频

- 音频编解码器优先级：针对 SIP 呼叫选择至少一个具有所需音频质量的音频编解码器。拖放可更改优先级。

注

选定编解码器要与呼叫接收编解码器匹配，因为进行呼叫时，接收编解码器起着决定性作用。

- 音频方向：选择允许的音频方向。
- H.264 packetization 模式：选择要使用的 packetization 模式。
  - 自动：（推荐）该设备决定要使用哪种 packetization 模式。
  - 无：未设置 packetization 模式。此模式通常被解释为模式 0。
  - 0: 非隔行模式。
  - 1: 单 NAL 单元模式。
- 视频方向：选择允许的视频方向。

其他

- UDP–to–TCP 转换：选择以允许暂时将传输协议从 UDP（用户数据报协议）转换成 TCP（传输控制协议）的呼叫。转换的原因是为了避免分片，如果请求在传输单元 (MTU) 上限的 200 字节内或大于 1300 字节，则可以进行切换。
- 允许通过重写：选择以发送本地 IP 地址，而不是路由器的公共 IP 地址。
- 允许触点重写：选择以发送本地 IP 地址，而不是路由器的公共 IP 地址。
- 每次向服务器登记：设置您希望设备就现有 SIP 账户向 SIP 服务器登记的频率。
- DTMF 有效负载类型：更改 DTMF 的默认有效负载类型。

SIP 账户

当前的 SIP 账户都列在SIP 账户之下。针对已注册账户，彩色圆圈可使您了解其状态。

● 该账户通过 SIP 服务器成功注册。

● 该账户存在问题。原因可能是授权失败、账户证书错误或 SIP 服务器无法找到该账户。

点对点（默认）账户是一个自动创建的账户。如果您至少创建了一个其他账户，并将该账户设置为默认，则您可以删除点对点账户。在未指定从哪个 SIP 账户呼叫的情况下，进行 VAPIX® 应用程序接口 (API) 呼叫时，始终使用默认账户。

+ 账户: 单击以创建新的 SIP 账户。

- 激活：选择能够使用该账户。
- 设为默认：选择将此账户设为默认账户。要设置一个默认账户，且仅能存在一个默认账户。
- 名称：输入说明性名称，例如，可以是名字、姓氏、职务或地点。该名称可重复。
- 用户 ID：输入分配给设备的仅有的扩展名或电话号码。
- 点对点：用于本地网络上向另一个 SIP 设备进行直接呼叫。
- 已注册：用于通过 SIP 服务器向本地网络外的 SIP 设备进行呼叫。
- 域: 如果可行，输入公开域名。它将在呼叫其他账户时将显示为 SIP 地址的一部分。
- 密码：输入与 SIP 账户关联的密码，以针对 SIP 服务器进行验证。
- 身份验证 ID: 输入用于针对 SIP 服务器进行验证的身份验证 ID。如果它与用户 ID 相同，则您无需输入身份验证 ID。
- 呼叫者 ID：从设备向呼叫接收人所显示的名称。
- 注册服务器：输入注册服务器的 IP 地址。

- 传输模式：选择针对该账户的 SIP 传输模式：UPD、TCP 或 TLS。当您选择 TLS 时，您可获得使用媒体加密的选项。
- 媒体加密（仅与 TLS 传输模式一同使用）：选择 SIP 呼叫中媒体（音频和视频）的加密类型。
- 证书（仅与 TLS 传输模式一同使用）：选择一个证书。
- 验证服务器证书（仅与 TLS 传输模式一同使用）：选中以验证该服务器证书。
- 辅助 SIP 服务器：若在主 SIP 服务器上注册失败，如果您想让设备在一台辅助 SIP 服务器上进行注册，则打开。
- 自动应答：选择自动接听呼入。
- SIP 安全：选择使用安全会话初始协议 (SIPS)。SIPS 使用 TLS 传输模式来加密通信。
- 代理
  - + 代理：单击添加代理。
  - 优先排序：如果您已添加两个或更多代理，请单击以对其进行优先排序。
  - 服务器地址：输入 SIP 代理服务器的 IP 地址。
  - 用户名：如果需要，输入 SIP 代理服务器的用户名。
  - 密码：如果需要，输入 SIP 代理服务器的密码。
- 视频
  - 视点区域：选择用于视频呼叫的视点区域。如果您选择无，则使用原始视图。
  - 分辨率：选择用于视频呼叫的分辨率。该分辨率会影响所需带宽。
  - 帧速：选择视频通话的每秒帧数。帧速率会影响所需的带宽。
  - H.264 配置文件：选择用于视频通话的配置文件。
- DTMF
  - 使用 RTP (RFC2833)：选择以允许 RTP 数据包中的双音多频 (DTMF) 信令、其他音调信号和电话事件。
  - 使用 SIP INFO (RFC2976)：选择以使 SIP 协议中包含 INFO 方法。INFO 方法会添加通常与会话有关的可选应用程序层信息。
  - + DTMF 序列：单击以添加由按键音触发的响应规则。您要在事件选项卡中激活该响应规则。
  - 序列：输入字符以触发响应规则。允许的字符：0–9、A–D、# 和 *。
  - 描述：输入要触发操作的描述。

SIP 测试呼叫

SIP 账户：选择要从中进行测试呼叫的账户。

SIP 地址：输入 SIP 地址，然后单击 测试账户发起测试呼叫，验证账户是否正常工作。

呼叫

呼叫按钮

启用呼叫按钮：打开以使用呼叫按钮。

在视频管理系统（VMS）中拨打电话：当有人按下呼叫按钮时，打开以进行 VMS呼叫。关闭，仅当有人按下呼叫按钮时，才呼叫联系人列表中的联系人。VMS 呼叫是通过设备中的事件系统从设备到 VMS 的模拟呼叫。即使 SIP 关闭，也可进行 VMS 呼叫。

备用光：在呼叫按钮周围为内置光选择一个选项。

- 自动：设备根据周围光线的情况打开和关闭内置光。
- 打开：当设备处于备用模式下时，内置灯始终处于打开状态。
- 关闭：当设备处于备用模式下时，内置灯始终处于关闭状态。

接受者：选择或创建一个或多个要呼叫的联系人，以便在某人按下呼叫按钮时进行呼叫。如果您添加多个接受者，则呼叫将同时对各收件人进行。接受者数量上限为 6。

备用：如果没有接受者回复，则从列表中添加备用联系人。

设备界面

常规

音频

注

- 所选音频剪辑仅在进行呼叫时播放。
- 如果在正在进行的呼叫过程中更改音频剪辑或增益，则直到下一个呼叫才会生效。

铃声：选择要在有人呼叫设备时播放的音频剪辑。使用滑块调整增益。

回铃音：选择要在有人从设备呼叫时播放的音频剪辑。使用滑块调整增益。

视频

单击以播放实时视频流。

单击以冻结实时视频流。

单击以对实时视频流拍摄快照。该文件将保存在计算机上的“下载”文件夹中。图像名称为 [快照_年_月_日_时_分_秒.jpg]。快照的实际大小取决于从接收快照的特定网页浏览器引擎应用的压缩，因此，快照大小可能与设备中配置的实际压缩设置不同。

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

单击以手动打开或关闭红外照明。

单击以手动打开或关闭白光。

单击以访问屏幕控制：

- 预定义控制：打开以使用可用的屏幕控制。
- 自定义控制：单击 + 添加自定义控件 以添加屏幕控制。

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

启动雨刮器。

单击并选择一个预置位置，以转到直播视图中的预置位置。或者，单击设置转到预置位置页面。

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

单击以选择一个轮巡，然后单击开始进行轮巡功能。或者，单击设置以转到轮巡功能页面。

单击以在选定的时间段内手动打开加热器。

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

单击以显示为设备配置的存储。要配置存储，您需要以管理员身份登录。

单击以访问更多设置：

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

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

单击以全屏显示实时视频流。按下 Esc 要退出全屏模式。

安装

取景模式 ：取景模式是一种预设配置，用于定义摄像机取景的方式。当您更改取景模式时，它可能会影响许多其他设置，例如，视点区域和隐私遮罩。

安装位置 ：图像的方向会根据摄像机的安装方式而变化。

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

图像

外观

设备界面

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

- Forensic：适合监控。
- 室内：适合室内环境。
- 室外：适合室外环境。
- 生动逼真：适用于演示目的。
- 交通概况：适用于车辆交通监控。

饱和度：使用滑块调整色彩浓度。例如，您可以获取一个灰度图像。



对比度：此滑块以调整明暗之间的差别。



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



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



宽动态范围

设备界面

WDR : 打开以使图像的明暗区域均可视。

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

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

白平衡

当摄像机侦测到进入光线的色温时，它可以调整图像，以便让颜色看起来更加自然。如果这还不够，您可从列表中选择合适的光源。

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

光线环境：

- 自动：自动识别和补偿光源颜色。这是在多数情况下建议使用的设置。
- 自动 – 室外 ：自动识别和补偿光源颜色。这是在多数室外场景下建议使用的设置。
- 自定义 – 室内 ：固定颜色调整，用于采用人造光源（荧光照明除外）的房间，适合约 2800 K 的正常色温。
- 自定义 – 室外 ：固定颜色调整，用于色温约 5,500 K 的晴朗天气条件。
- 固定 – 荧光 1：固定颜色调整，用于色温约 4000 K 的荧光照明。
- 固定 – 荧光 2：固定颜色调整，用于色温约 3000 K 的荧光照明。
- 固定 – 室内: 固定颜色调整，用于采用人造光源（荧光照明除外）的房间，适合约 2800 K 的正常色温。
- 固定 – 室外 1: 固定颜色调整，用于色温约 5,500 K 的晴朗天气条件。
- 固定 – 室外 2: 固定颜色调整，用于色温约 6500 K 的多云天气条件。
- 路灯 – 汞 ：固定颜色调整，用于街道照明中常用汞蒸汽灯发出的紫外线。
- 路灯 – 钠 ：固定颜色调整，用于补偿街道照明中常用钠蒸气灯的橙黄色。
- 保持当前设置：保持当前设置，不补偿光线变化。
- 手动 ：借助白色物体固定白平衡。将圆圈拖曳到您想让摄像机显示为白色的实景图像中的物体上。使用红平衡和蓝平衡滑块以手动调整白平衡。

曝光

设备界面

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

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

曝光区域：使用曝光区域优化场景选定部分的曝光，例如，入口门前面的区域。

注

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

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

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

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

运动自适应曝光：选择以减少低照度条件下的运动模糊。

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

注

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

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

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

曝光级别：使用滑块调整图像曝光。

除雾：打开以侦测多雾天气的影响，并自动除雾以获得清晰的图像。

注

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

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

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

选择比特率降低强度：

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

优化存储: 优化设置，以通过降低比特率来存储流，同时保持质量。优化不应用于网络客户端中显示的流。打开优化存储还会打开动态 GOP。

动态 FPS（每秒帧数）：打开以允许带宽随场景中的活动级别不同而异。更多的活动需要更多带宽。

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

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

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

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。

方向

镜像：打开以镜像图像。

音频

包含：打开以在视频流中使用音频。

源 ：选择要使用的音频源。

立体声 ：打开以包括内置音频以及来自外部麦克风的音频。

叠加

+ ：单击以添加叠加。从下拉列表中选择叠加类型：

- 文本：选择以显示集成在实时视图图像中且在各视图、录制和快照中可见的文本。您可以输入自己的文本，也可以包括预先配置的修饰符，以自动显示示例时间、日期、帧率。
  - ：单击以添加日期修饰符 %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。
- 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。

隐私遮罩

+ ：单击以创建新的隐私遮罩。遮罩数量上限取决于遮罩共同的复杂程度。每个遮罩可包含多达 10 个锚点。

隐私遮罩: 单击此处可更改各隐私遮罩的颜色，或永久删除各隐私遮罩。

遮罩 x：单击可重命名、禁用或永久删除遮罩。

阅读器

阅读器协议

阅读器协议类型: 选择要用于读卡器功能的协议。

- VAPIX 阅读器: 仅可与 Axis 门禁控制器一起使用。
  - 协议: 选择 HTTPS 或 HTTP。
  - 门禁控制器地址: 输入门禁控制器的 IP 地址。
  - 用户名: 输入门禁控制器的用户名。
  - 密码：输入门禁控制器的密码。
  - 连接：单击以连接到门禁控制器。
  - 选择读取器: 为恰当的门选择入口阅读器。
- OSDP：
  - OSDP 地址：输入 OSDP 阅读器地址。0 是单个读卡器的默认和常用地址。
- Wiegand:
  - 寻呼机: 打开以激活寻呼机输入。
  - 寻呼机输入: 选择用于寻呼机的 I/O 端口。
  - LED 控制输入：选择在设备上用于控制 LED 反馈的输入/输出端口数量。
  - LED1/LED2 输入：选择用于 LED 输入的 I/O 端口。
  - 空闲的颜色：如果没有用于控制 LED 的 I/O 端口，则您可以选择要在读卡器指示器带上显示的静态颜色。
  - 高/低状态的颜色：如果一个 I/O 端口用于 LED 控制，请分别选择显示低和高状态的颜色。
  - 空闲颜色/LED1 颜色/LED2 颜色/LED1 + LED2 颜色：如果两个 I/O 端口用于 LED 控制，请分别为空闲、LED1、LED2 和 LED1 + LED2 选择要显示的颜色。
  - 按键格式: 选择将 PIN 发送至访问控制单元时如何格式化。
  - FourBit：PIN `1234` 予以编码并发送为 0x1 0x2 0x3 0x4。这是默认和常见的行为。
  - EightBitZeroPadded：PIN `1234` 予以编码并 发送为 0x01 0x02 0x03 0x04。
  - EightBitInvertPadded：PIN `1234` 予以编码并发送为 0XE1 0XD2 0xC3 0xB4。
  - Wiegand26: PIN 以 Wiegand26 格式编码，具有 8 位功能码和一个 16 位的识别码。
  - Wiegand34: PIN 以 Wiegand34 格式编码，具有一个 16 位的设施代码和一个 16 位的识别码。
  - Wiegand37: PIN 采用 35 位识别码的 Wiegand37 格式（H10302）编码。
  - Wiegand37FacilityCode: PIN 以 Wiegand37 格式 (H10304) 编码，具有一个 16 位的设施代码和一个 19 位的识别码。
  - 设施代码：输入要发送的设施代码。此选项仅适用于某些按键格式。

输出格式

选择数据格式: 选择将卡数据发送到访问控制单元的格式。

- 原始: 按原样传输卡数据。
- Wiegand26: 以 Wiegand26 格式对卡数据进行编码，采用 8 位设施代码和一个 16 位的识别码。
- Wiegand34: 以 Wiegand34 格式对卡数据进行编码，采用一个 16 位的设施代码和一个 16 位的识别码。
- Wiegand37: 使用 35 位识别码 Wiegand37 格式（H10302）对卡数据进行编码。
- Wiegand37FacilityCode: 以 Wiegand37 格式 (H10304) 对卡数据进行编码，采用一个 16 位的设施代码和一个 19 位的识别码。
- 自定义：定义您自己的格式。

设施代码覆盖模式：选择用于覆盖设施代码的选项。

- 自动：不覆盖设施代码，并从输入数据自动侦测创建设施代码。使用卡的原始设施代码，或放弃其超出卡号的多余位。
- 可选: 使用输入数据中的设施代码，或使用配置的可选值重写。
- 覆盖: 始终以指定的设施代码覆盖。

芯片类型

芯片类型显示现用芯片类型列表及其是否使用默认数据或自定义数据。

上下文菜单包括：

- 停用：单击以从活动芯片类型列表中移除芯片类型。

使用完整卡序列号 (UID/CDN) 反转芯片类型的字节顺序：打开以对各芯片类型反转 UID/CDN 字节顺序。

激活芯片类型：从列表中选择一种芯片类型以将其激活。

PIN

激活 PIN：如果用户在使用读卡器时需要使用 PIN，请打开。PIN 设置必须与在访问控制单元中配置的设置相匹配。

长度 (1–32)：输入 PIN 中的数字位数。

超时（3–50 秒）：输入在未收到 PIN 时设备返回到空闲模式之前需要经过的秒数。

音频

设备设置

输入：打开或关闭音频输入。显示输入类型。

输入类型：选择输入类型，例如，它是内部麦克风或线路输入。

电源类型：选择用于输入的电源类型。

应用更改：单击以使用您的选择。

单独的增益控制：打开以单独调整不同输入类型的增益。

自动增益控制：打开以动态调整声音中的变化增益。

增益：使用滑块更改增益。单击麦克风图标可静音或取消静音。

输出：显示输出类型。

增益：使用滑块更改增益。单击扬声器图标可静音或取消静音。

流

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

消除回音: 打开以在双向通信期间移除回声。

音频剪辑

+ 添加剪辑: 单击以添加新的音频剪辑。您可以使用 .au、.mp3、.opus、.vorbis、.wav 文件。

▶ 单击以播放音频剪辑。

■ 单击以停止播放音频剪辑。

⋮ 上下文菜单包括：

- 重命名: 更改音频剪辑的名称。
- 创建链接: 创建一个 URL，并在使用时在设备上播放音频剪辑。指定音量和播放剪辑的次数。
- 下载： 将音频剪辑下载到您的电脑上。
- 删除： 从设备上删除音频剪辑。

录制内容

正在进行的录制内容： 显示摄像机上全部正在进行的录制内容。

● 选择以开始在摄像机上进行录制。

选择要保存到哪个存储设备。

● 选择以停止摄像机上的录制。

触发的录制将在手动停止以及摄像机关闭时结束。

连续录制将继续，直到手动停止。即使摄像机关闭，录制也会在摄像机再次启动时继续。

▶ 单击以播放录制内容。

■ 单击以停止播放录制。

⌄ 单击以显示有关录制内容的更多信息和选项。

设置导出范围: 如果只想导出部分录制内容，请输入从何时开始。

单击以删除录制内容。

导出: 单击可导出（部分）录制内容。

设备界面

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。

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： 单击安装新应用。

查找更多应用： 单击以转到 Axis 应用的概览页面。

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可对设备进行完全访问。

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： 单击以访问应用的设置。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: 单击此处，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： 单击以查看应用事件的日志。当您与支持人员联系时，日志很有用。
- 使用密钥激活许可证： 如果应用需要许可证，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。
  如果你没有许可证密钥，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。
- 自动激活许可证： 如果应用需要许可证，则需要激活它。如果您的设备有互联网接入，请使用此选项。您需要许可证密钥来激活许可证。
- 停用许可证： 停用许可证以在另一设备中使用它。如果要停用许可证，您还会将其从设备中移除。要停用许可证，需要互联网接入。
- 设置： 配置参数。
- 删除： 永久从设备中删除应用。如果不先停用许可证，则许可证将保持活动状态。

系统

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：选择同步设备日期和时间的选项。

- 自动日期和时间（手动 NTS KE 服务器）：与安全 NTP 密钥建立连接至 DHCP 服务器的服务器进行同步。
  - 手动 NTS KE 服务器：输入一个或两个 NTP 服务器的 IP 地址。当您使用两台 NTP 服务器时，设备会根据两者的输入同步并调整其时间。
- 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一次日期和时间设置。

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。

配置检查

单击图像中的按钮模拟实际按键。这允许您尝试配置或排除硬件故障，而无需物理访问设备。

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，添加要用作备用静态 IP 地址，请选择此项。

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

设备界面

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。主机名称用于服务器报告和系统日志中。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

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。

HTTPS 是一种协议，可为来自用户的页面请求和 web 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。

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。端口 80 或范围 1024–65535 中的端口均被允许。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。端口 443 或 1024–65535 范围中的端口均被允许。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

设备界面

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：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，将一直启用，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。一旦注册，设备会一直连接到 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 对象的团体名称。默认值为公共。
  - 写入团体：输入可读取/写入访问支持全部的 SNMP 对象（只读对象除外）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。在设备界面中，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” 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。

连接的客户端

查看详细信息：单击显示了与设备连接的客户端。

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。

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。

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）。

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，必须在设备上安装已签名的客户端证书。

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。

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。

策略：选择是否允许访问或拒绝访问特定 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。自定义签名固件证书只能由 Axis 创建，因为 Axis 持有对其进行签名的密钥。

单击安装以安装证书。在安装固件之前，您需要安装证书。

用户

+ 添加用户：单击以添加新用户。您可以添加多达 100 个用户。

用户名：输入单独的用户名。

新密码：输入用户的密码。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：完全访问各设置。管理员也可以添加、更新和删除其他用户。
- 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：有权访问：

- 观看并拍摄视频流的快照。
- 观看和导出录音。
- 使用 PTZ 用户访问：水平转动、垂直转动和变焦。

上下文菜单包括：

更新用户：编辑用户的属性。

删除用户：删除用户。无法删除根用户。

匿名用户

允许匿名浏览者：打开以允许其他人以查看者的身份访问设备，而无需登录用户帐户。

允许匿名 PTZ 操作员：打开允许匿名用户平移、倾斜和缩放图像。

事件

规则

规则定义产品执行操作必须满足的条件。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：单击以创建规则。

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，以避免在日出期间发生小的光变化，并且日落会重复激活规则，此功能将非常有用。

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，它将一直保持活动状态，只要满足首个条件的状态，其他条件都将保持有效。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

设备界面

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。这样您就知道具有所需名称的全部文件都是正确的。
  - 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收者。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/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。这样您就知道具有所需名称的文件都是正确的。

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

注

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

手动触发器用于手动触发规则。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系统（VM）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、客户端和中介。客户端可以发送和接收消息。代理负责客户端之间路由消息。

您可在 *AXIS OS Portal* 中了解有关 MQTT 的更多信息 。

ALPN

ALPN 是一种 TLS/SSL 扩展，允许在客户端和服务器之间的连接信号交换阶段中选择应用协议。这用于在使用其他协议（如 HTTP）的同一个端口上启用 MQTT 流量。在某些情况下，可能没有为 MQTT 通信打开专用端口。这种情况下的解决方案是使用 ALPN 来协商将 MQTT 用作标准端口上的应用协议（由防火墙允许）。

MQTT 客户端

连接：打开或关闭 MQTT 客户端。

状态：显示 MQTT 客户端的当前状态。

代理

主机：输入 MQTT 服务器的主机名或 IP 地址。

协议: 选择要使用的协议。

端口：输入端口编号。

- 1883 是 TCP 的 MQTT 的默认值
- 8883 是 SSL 的 MQTT 的默认值
- 80 是 WebSocket 的 MQTT的默认值
- 443 是 WebSocket Secure 的 MQTT 的默认值

ALPN 协议：输入 MQTT 代理供应商提供的 ALPN 协议名称。这仅适用于 SSL 的 MQTT 和 WebSocket Secure 的 MQTT。

用户名：输入客户将用于访问服务器的用户名。

密码：输入用户名的密码。

客户端 ID: 输入客户端 ID。客户端连接到服务器时，客户端标识符发送给服务器。

清理会话: 控制连接和断开时间的行为。选定时，状态信息将在连接及断开连接时被丢弃。

保持活动状态间隔: 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，侦测服务器何时不再可用。

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。

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

发送消息: 打开以发送消息。

使用默认设置: 关闭以输入您自己的默认消息。

主题： 输入默认消息的主题。

有效负载: 输入默认消息的内容。

保留： 选择以保留此主题的客户端状态

QoS: 更改数据包流的 QoS 层。

MQTT 出版

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

包括主题名称： 选择以包含描述 MQTT 主题中的条件的主题。

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

包含序列号： 选择以将设备的序列号包含在 MQTT 有效负载中。

+ 添加条件: 单击以添加条件。

保留： 定义将哪些 MQTT 消息作为保留发送。

- 无： 全部消息均以不保留状态发送。

- 性能：仅将有状态消息作为保留发送。
- 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。
- 即使连接测试失败，添加共享：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、取消删除绑定与网络共享的连接。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：选择保留录像的时间、限制旧录像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：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。

单击使用工具以激活所选工具。

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：格式化 SD 卡，例如，您需要更改文件系统或快速清除数据。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。

单击使用工具以激活所选工具。

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。

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*流 25*。

帧速：有关该设置的说明，请参见*流 25*。

压缩：有关该设置的说明，请参见*流 25*。

Zipstream ⓘ：有关该设置的说明，请参见*流 25*。

优化存储 ⓘ：有关该设置的说明，请参见*流 25*。

动态 FPS ⓘ：有关该设置的说明，请参见*流 25*。

动态 GOP ⓘ：有关该设置的说明，请参见*流 25*。

镜像 ⓘ：有关该设置的说明，请参见*流 25*。

GOP 长度 ⓘ：有关该设置的说明，请参见*流 25*。

比特率控制：有关该设置的说明，请参见*流 25*。

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 27*。

保护音频 ⓘ：有关该设置的说明，请参见*流 25*。

ONVIF

ONVIF 用户

设备界面

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

+ 添加用户：单击以添加新 ONVIF 用户。

用户名：输入单独的用户名。

新密码：输入用户的密码。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：完全访问各设置。管理员也可以添加、更新和删除其他用户。
- 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。
- 媒体用户：仅允许访问视频流。

⋮ 上下文菜单包括：

更新用户：编辑用户的属性。

删除用户：删除用户。无法删除根用户。

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。

+ 添加媒体配置文件：单击以添加新 ONVIF 媒体配置文件。

profile_x：单击要编辑的配置文件。

分析元数据

元数据生成者

元数据发生器列出应用程序使用的通道以及它们从设备流式传输的元数据。

生产者：生成元数据的应用。

通道：应用使用的通道。选中以启用元数据流。取消选中以禁用流，以实现兼容性或资源管理原因。

侦测器

摄像机遮挡

当场景发生变化时，摄像机遮挡侦测器将生成警报，例如，镜头被覆盖、喷洒或严重超出对焦，以及超过触发延迟时间。只有在摄像机至少移动了 10 秒后，遮挡侦测器才会激活。在此期间，该侦测器将设置场景模型，以用作在当前图像中侦测遮挡的比较。要正确设置场景模型，请确保摄像机已对焦，照明条件良好，并且摄像机未指向缺少轮廓的场景（如，空白的墙壁）。摄像机遮挡也可用作触发操作的条件。

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

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

注

用于在静态和非拥挤场景中侦测篡改尝试。

音频侦测

这些设置可用于每个音频输入。

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

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。

视频输出

HDMI

您可通过 HDMI 电缆将外部显示器连接至设备。

单个来源

来自单个摄像机的流显示在外部监视器上。

- 来源：仅选择一个摄像机。
- 旋转图像 180°：单击以旋转图像。
- 镜像图像：单击可翻转图像。
- 动态叠加：单击可叠加。

四画面

在外部监视器上同时查看来自四个独立摄像机的流。

- 来源：从四个下拉列表中选择一个不同的摄像机。来源旁边的图像显示了来自该摄像机的视频将在屏幕上显示的位置。
- 旋转图像 180°：单击可旋转各图像。

播放列表

来自外部监视器上的多个摄像机交替的单个流。

- 旋转图像 180°：单击可旋转各来源的图像。
- ＋：单击将摄像机添加到播放列表。
- 来源：选择所需的摄像机。
- 持续时间：设置播放列表在每次旋转时从该摄像机传输多长时间（以 mm 为 ss）。
- 镜像图像：单击可翻转图像。
- 创建：单击以保存。

画中画 

在外部显示器上同时显示两个流。一个流填充了显示，另一个则是较小的图片。位置、图片大小 和边框都是可自定义的。

- 画中画
  - 来源：选择将作为较小图片流式传输的摄像机。
  - 旋转图像 180°：单击以旋转图像。
  - 镜像图像：单击可翻转图像。
  - 位置：选择在屏幕上应显示图片的位置。
  - 图片尺寸：拖动滑块可设置图片的大小（占屏幕的百分比）。
  - 边框：单击切换边框以打开或关闭。
  - ：拖动滑块以设置整个边框的粗细。
  - ：拖动滑块以设置上部边框的粗细。
  - ：拖动滑块以设置右侧边框的粗细。
  - ：拖动滑块以设置底部边框的粗细。
  - ：拖动滑块以设置左侧边框的粗细。
  - 边框颜色；选择边框颜色。
- 主视图
  - 来源：选择将在全显示器上进行流式传输的摄像机。
  - 旋转图像 180°：单击以旋转图像。
  - 镜像图像：单击可翻转图像。

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设备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）。

日志

报告和日志

报告

- 查看设备服务器报告：在弹出窗口中单击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：单击下载服务器报告。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景图像的快照。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：单击以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。

网络追踪

重要

网络跟踪文件可能包含敏感信息，例如证书或密码。

通过记录网络上的活动，网络追踪文件可帮助您排除问题。

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。

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：选择要使用的 syslog 消息格式。

- 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 PTZ 预设。

重要

还原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*恢复为出厂默认值。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默认值。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。

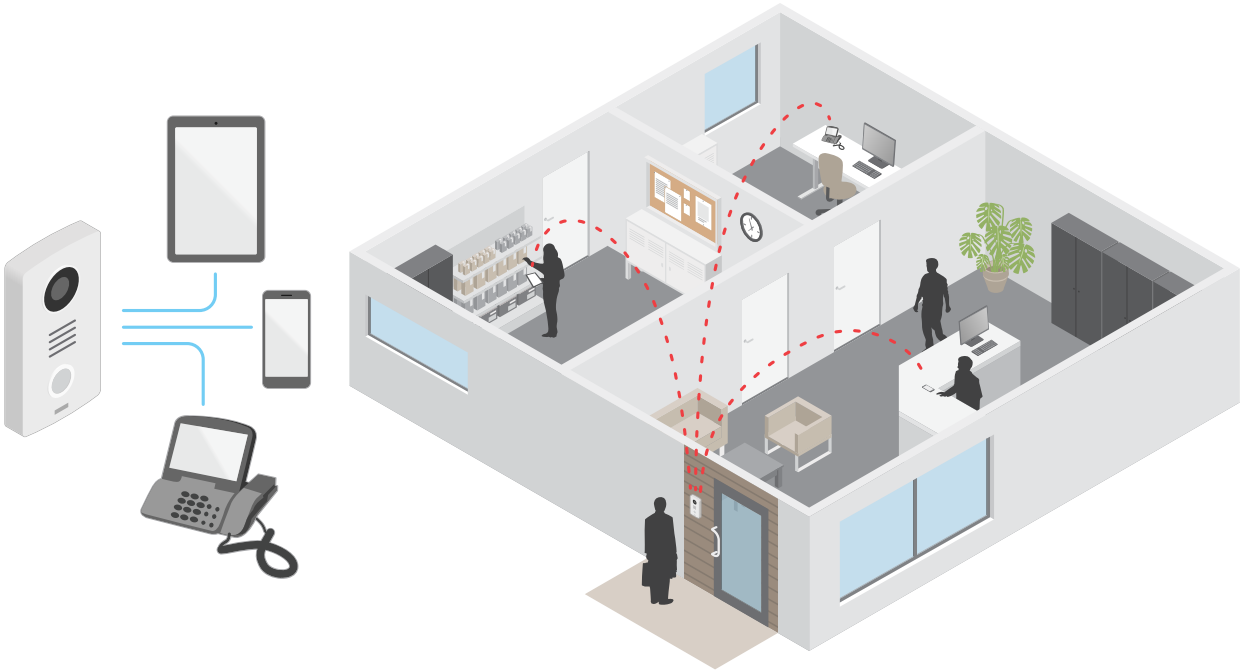
了解更多

IP 语音 (VoIP)

IP 语音 (VoIP) 是一组支持通过 IP 网络（如互联网）进行语音通信和多媒体会话的技术。在传统的电话呼叫中，模拟信号在公共交换电话网络 (PSTN) 上通过电路传输发送。在 VoIP 呼叫中，模拟信号被转化成数字信号，使其可以在本地 IP 网络或互联网间以数据包的形式发送。

在 Axis 产品中，VoIP 通过会话初始化协议 (SIP) 和双音多频 (DTMF) 信令启用。

示例



当您按下 Axis 门站上的呼叫按钮时，会向一个或多个预定的接受者发起呼叫。接受者应答时，就建立了呼叫。音频和视频通过 VoIP 技术进行传输。

会话初始化协议 (SIP)

会话初始化协议 (SIP) (SIP) 用于创建、维持和终止 VoIP 呼叫。您可以在两方或多方（称为 SIP 用户代理）之间进行呼叫。如需进行 SIP 呼叫，您可以使用（例如）SIP 电话、软件电话或已启用 SIP 的 Axis 设备。

SIP 用户代理之间的实际音频或视频通过传输协议进行交换，例如 RTP（实时传输协议）。

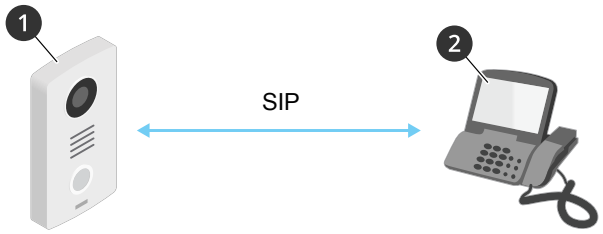
您可以使用点对点设置在本地网络上或使用 PBX 在各网络间进行呼叫。

点对点 SIP (P2PSIP)

基本的 SIP 通信类型会直接发生在两个或多个 SIP 用户代理之间。这称为点对点 SIP (P2PSIP)。如果这发生在本地网络上，则只需用户代理的 SIP 地址。在这种情况下，SIP 地址通常为 `sip:<local-ip>`。

示例

了解更多



1 用户代理 A – 门站。SIP 地址： sip:192.168.1.101
2 用户代理 B – 支持 SIP 的电话。SIP 地址： sip:192.168.1.100

您可以安装 Axis 门站来呼叫（例如）同一网络上采用点对点 SIP 设置的已启用 SIP 的电话。

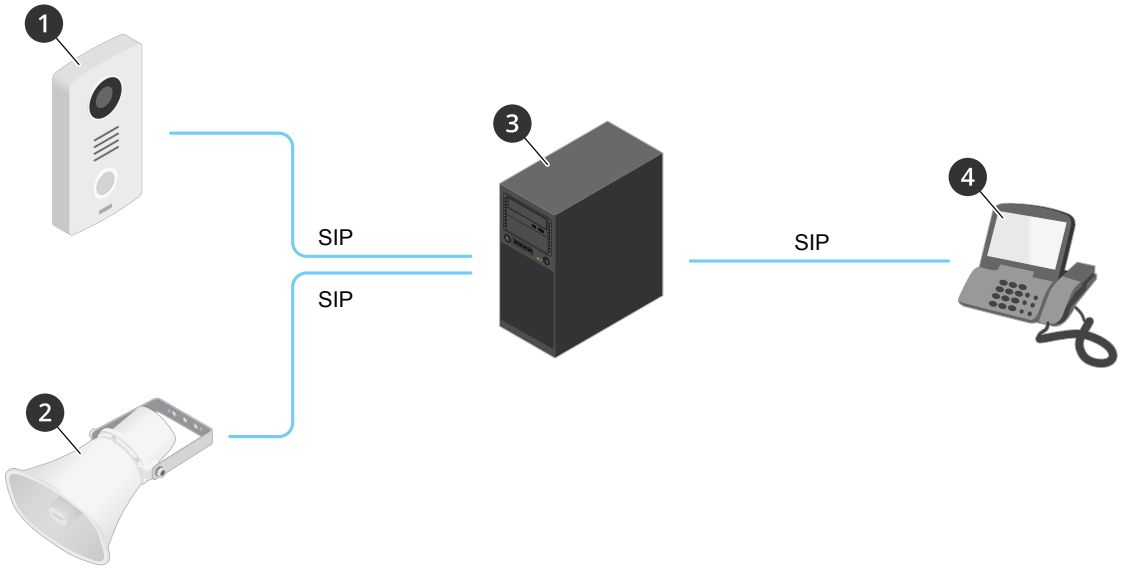
专用分支交换机 (PBX)

当您在本地 IP 网络外进行 SIP 呼叫时，专用分支交换机 (PBX) 可用作一个中央集线器。PBX 的主要元件是 SIP 服务器，也称为 SIP 代理服务器或注册服务器。PBX 的工作方式与传统交换机相同，会显示客户的当前状态，且可允许（例如）呼叫转移、语音邮件和重定向。

PBX SIP 服务器可安装为一个本地实体或异地实体。它可以托管在内联网上或由第三方提供商进行托管。当您在网络之间进行 SIP 呼叫时，呼叫会通过一组 PBX 进行传输，PBX 会查询要到达的 SIP 地址的位置。

每个 SIP 用户代理都需注册 PBX，随后才能拨打正确的电话分机联系其他人。在这种情况下，SIP 地址通常为 `sip:<user>@<domain>` 或 `sip:<user>@<registrar-ip>`。SIP 地址独立于其 IP 地址，PBX 使设备在 PBX 上注册期间可访问。

示例



1 sip:mydoor@company.com
2 sip:myspeaker@company.com
3 PBX sip.company.com
4 sip:office@company.com

当您按下 Axis 门站上的呼叫按钮时，呼叫通过一个或多个 PBX 传输到本地 IP 网络或互联网上的 SIP 地址。

了解更多

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，设备可以在侦测到移动后开始录制或发送电子邮件，或在设备录制时显示叠加文本。

若要了解更多信息，请查看我们的指南*事件规则入门*。

应用

借助应用，您可以更充分地利用您的 Axis 设备。AXIS Camera Application Platform (ACAP) 是一个开放平台，使第三方能够为 Axis 设备开发分析和其他应用。应用可以预装在设备上，可以免费下载，或收取许可费。

要查找 Axis 应用的用户手册，请转到 *help.axis.com*。

日常使用

使用键盘

我想要...	操作
呼叫可让我进入大楼的人员。	按下  。
呼叫大楼内的某个人员。	输入该人员的快速拨号号码并按下  。
使用我的卡和 PIN 开门。	刷卡并输入 PIN。
使用我的 PIN 开门。	输入 PIN 并按下 #。
使用我的卡开门。	刷卡。

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*产品概述 5*。
3. 按住控制按钮 15–30 秒，直到 LED 状态指示灯呈橙色闪烁。
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. 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

使用活动追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/firmware*。

1. 将固件文件下载到您的计算机，该文件可从 *axis.com/support/firmware* 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。

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 root 用户的密码丢失，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 54*。
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。

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*。

性能考虑

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

以下因素是重要的考虑因素：

- 图像分辨率较高或压缩级别较低都会导致图像含更多数据，从而影响带宽。
- 大量 Motion JPEG 或单播 H.264 用户访问会影响带宽。

故障排查

- 使用不同客户端同时查看不同流（分辨率、压缩）会同时影响帧速和带宽。
  尽量使用相同流来保持高帧速。流配置文件可用于确保流是相同的。
- 同时访问 Motion JPEG 和 H.264 视频流会同时影响帧速和带宽。
- 大量使用事件设置会影响产品的 CPU 负载，从而影响帧速。
- 使用 HTTPS 可能降低帧速，尤其是传输 Motion JPEG 流时。
- 由于基础设施差而导致的高网络利用率会影响带宽。
- 在性能不佳的客户端计算机上进行查看会降低帧速，影响用户体验。
- 同时运行多个 AXIS Camera Application Platform (ACAP) 应用程序可能会影响帧速和整体性能。

规格

前面板指示灯和控制

当您将产品连接至电源时，指示灯图标和指示条亮起几秒钟。

呼叫指示器图标

图标	指示
	呼出发起时蓝色稳定。 呼入发起时闪烁蓝色。
	正在呼叫时橙色稳定。
	门打开时绿色稳定。

阅读器指示条

该条带表示阅读器反馈信息。

呼叫按钮

你可以使用呼叫按钮周围的内置照明，以照亮访客的脸部。

LED 指示灯

LED 状态指示灯	指示
绿色	绿色常亮表示正常工作。

SD 卡插槽

注意

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

本设备支持 microSD/microSDHC/microSDXC 卡。

有关 SD 卡的建议，请参见 *axis.com*。

 microSD、microSDHC 和 microSDXC 徽标是 SD–3C LLC 的商标。microSD、microSDHC、microSDXC 是 SD–3C, LLC 在美国和/或其他国家/地区的商标或注册商标。

按钮

控制按钮

控制按钮用于：

- 将产品恢复至出厂默认设置。请参见*重置为出厂默认设置 54*。

连接器

HDMI 连接器

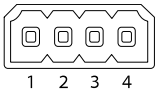
使用微型 HDMI™ 连接器连接一个显示器或公众可视监视器。

网络连接器

采用以太网供电 增强版 (PoE+) 的 RJ45 以太网连接器。

音频连接器

用于音频输入和输出的 4 针脚接线盒。

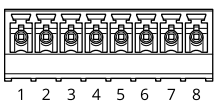


功能	针脚	备注
线路输入	1	线路输入（单声道）
接地	2	音频接地
线路输出	3	线路输出
接地	4	音频接地

继电器连接器

用于可通过以下方式使用的固态继电器的 8 针脚接线盒：

- 作为开启和关闭辅助电路的一个标准继电器。
- 直接控制一个锁。
- 通过一个安全继电器控制一个锁。在门的安全侧上使用一个安全继电器可避免线路发热。



功能	针脚	备注	规格
NO/NC	1	正常开启/正常闭合 用于连接继电器设备。 这两个继电器针脚与其余电路电位隔离。	最大电流 = 1 A 最大电压 30 V DC

COM	2	常见	
24 V DC	3	可用于为辅助设备供电。 注释：此针脚只能用作电源输出。	通过 IEEE 802.3af/802.3at 1 类 3 级 POE 供电时的输出电压 24 V DC 最大电流 50 mA[1] 通过 PoE+ IEEE 802.3at 2 类 4 级或直流电源输入供电时的最大电流为 350 mA[2]
DC 接地	4		0 V DC
NO/NC	5	正常开启/正常闭合 用于连接继电器设备。 这两个继电器针脚与其余电路电位隔离。	最大电流 = 1 A 最大电压 30 V DC
COM	6	常见	
12 V DC	7	可用于为辅助设备供电。 注释：此针脚只能用作电源输出。	输出电压 12 V DC 通过 IEEE 802.3af/802.3at 1 类 3 级 PoE 供电时的最大电流为 100 mA[3] 通过 PoE+ IEEE 802.3at 2 类 4 级或直流电源输入供电时的最大电流为 700 mA[4]
DC 接地	8		0 V DC

1. 。
2. 。
3. 。
4. 。

阅读器连接器

用于连接外部阅读器的 4 针脚接线盒。

功能	针脚	备注	规格
DC 接地	1		0 V DC
12 V DC	2	可用于为辅助设备供电。 注释：此针脚只能用作电源输出。	输出电压 12 V DC
D0/A+	3	Wiegand：DATA0 输出 RS485：A+	
D1/B–	4	Wiegand：DATA1 输出 RS485：B–	

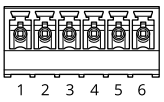
I/O 连接器

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

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

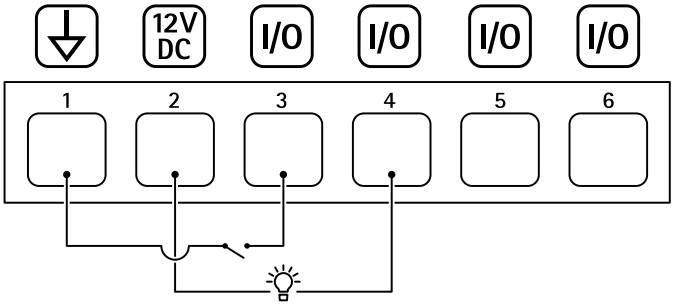
数字输出 – 用于连接继电器和 LED 等外部设备。已连接的设备可由 VAPIX® 应用程序编程接口、通过事件或从设备网页接口进行激活。

规格



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



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

用于 DC 电源输入的 2 针脚接线盒。使用一个额定输出功率限制在 ≤ 100 W 或额定输出电流限制在 ≤ 5 A 的安全超低电压 (SELV) 兼容式限功率电源 (LPS)。



规格

功能	针脚	备注	规格
DC 接地	1		0 V DC
DC 输入	2	在未使用以太网供电时，可用于给控制器供电。 注释：此针脚只能用作电源输入。	8–28 V DC，最大 22 W 输出最大负载 9 W

安全信息

危险等级

⚠危险

表示如果不避免则会导致死亡或严重伤害的危险情况。

⚠警告

表示如果不避免则可能导致死亡或严重伤害的危险情况。

⚠警示

表示如果不避免则可能导致轻微或中度伤害的危险情况。

注意

表示如果不避免则可能导致财产损失的情况。

其他消息等级

重要

表示产品正常工作所必需的重要信息。

注

表示有助于充分利用产品的有用信息。

用户手册
AXIS A8207–VE Network Video Door Station
© Axis Communications AB, 2019 – 2023
版本 M11.3
日期： 六月 2023
零件号 T10121755