

AXIS Device Manager

目录

| | |
|------------------------------|----|
| 关于 AXIS Device Manager | 3 |
| 开始使用 | 4 |
| 安装软件 | 4 |
| 连接至服务器 | 4 |
| 连接到多台服务器 | 4 |
| 配置服务器 | 4 |
| 初始配置 | 5 |
| 管理设备 | 6 |
| 添加设备 | 6 |
| 删除设备 | 6 |
| 替换设备 | 6 |
| 还原设备 | 6 |
| 安装应用 | 7 |
| 配置 | 8 |
| 管理恢复点 | 8 |
| 创建恢复点 | 8 |
| 创建自动恢复点 | 8 |
| 管理多个凭据 | 8 |
| 安装证书 | 9 |
| 证书简介 | 9 |
| 创建证书颁发机构 (CA) | 9 |
| 启用 HTTPS | 9 |
| 运行802.1X | 10 |
| 配置 SIP 设置 | 10 |
| 管理 SIP 帐户 | 11 |
| 添加 SIP 帐户 | 11 |
| 删除 SIP 帐户 | 12 |
| 在设备上启用元数据 | 13 |
| 管理设备软件 | 14 |
| AXIS OS 升级 | 14 |
| 故障排查 | 15 |
| 软件物料清单 | 15 |
| 联系支持人员 | 15 |
| 升级流程 | 15 |

关于 AXIS Device Manager

AXIS Device Manager 是一款用于安讯士产品的安装和管理软件应用程序。该软件可以自动在局域网中搜索设备、分配 IP 地址、设置密码、显示连接状态、管理固件升级、证书以及多个设备的配置。

AXIS Device Manager 包括：

- AXIS Device Manager 服务控制 – 处理与安讯士产品通信的服务器
- AXIS Device Manager 客户端 – 使用户能够通过互联网或企业网络进行远程管理的前端用户界面

多个客户端可连接相同服务器。一个客户端可同时连接多台服务器。

AXIS Device Manager 对于加固系统、提升安全性也非常有用。更多信息，请参见 *AXIS Device Manager 安全指南*。

开始使用

安装软件

要安装 AXIS Device Manager 5，请保障您在安装的计算机上拥有完全管理员权限，然后按照以下步骤操作：

1. 访问 *axis.com* 上的产品页面并下载 *AXIS Device Manager* 桌面应用程序
2. 运行安装程序并按照屏幕上的说明进行操作。

注意

安装 Microsoft .NET 4.8 框架（包含在安装文件中，如果尚未安装）。这将需要几分钟。在安装 AXIS Device Manager 之前，还可以通过 Windows 更新安装 Microsoft .NET 4.8 框架。

连接至服务器

首次启动 AXIS Device Manager 时，系统会提示您连接到服务器。服务器可以运行在本地计算机上，也可以运行在远程服务器上。

以本地 Windows 用户身份登录：

1. 选择 **This computer（此计算机）**。
2. 选中 **Log on as current user（以当前用户身份登录）**，以使用您当前的凭据进行登录。

以服务器或域上的其他用户身份登录：

- 选择 **Other user（其他用户）**。
- 在 **Other user（其他用户）** 下，输入该帐户的凭据。
- 选中 **Remember me（记住我）**，下次运行客户端时可跳过此步骤。
- 单击 **Log on（登录）**。

注意

要清除所有服务器的保存凭据，请转到登录屏幕并选择 **Delete saved passwords（删除保存的密码）**。

登录到远程服务器：

1. 选择**远程服务器**。
2. 从下拉列表中选择服务器，或在字段中输入 IP 或 DNS 地址。
3. 输入您的凭据。
4. 单击 **Log on（登录）**。

注意

如果计算机未加入 Windows 域，则无法使用此选项登录到远程服务器。

连接到多台服务器

您可以使用 AXIS Device Manager 连接到多台服务器。成功登录服务器后，您可以在主菜单中切换服务器。

1. 打开主菜单 >Servers（服务器）>New Connection（新连接）
2. 选择连接到您的计算机或远程服务器，如上所述。

配置服务器

AXIS Device Manager 服务器安装在您的计算机上后，服务控制支持您启动和关闭服务器，以及修改服务器设置。

要配置服务器：

1. 双击图标以打开 **AXIS Device Manager Service Control (AXIS Device Manager 服务控制)**
2. 勾选 **Modify settings (修改设置)** 复选框
3. 命名服务器。服务器名称用于标识服务器，并在客户端连接到多个服务器时显示在 AXIS Device Manager 客户端中。默认名称是安装该软件的计算机的名称。
4. 输入 HTTP 端口。默认 HTTP 端口号：55762
5. 输入 TCP 端口。默认 TCP 端口号：55764

注意

服务器端口号必须在 1024 到 65533 之间。TCP 端口号将始终为服务器端口号 + 2。例如，如果服务器端口号是 55765，那么 TCP 端口号就是 55767。

注意

对于大型安装，我们建议使用 AXIS Device Manager 服务管理。它是一个控制台应用，可通过命令提示符或批脚本使用，以启动和停止服务，备份数据库等。该控制台应用“AdmAdminConsole.exe”位于服务器安装目录中。

初始配置

开始使用设备时，您需要完成以下操作：

- 添加设备并创建用户帐户，参见：*添加设备, on page 6*。
- 为您的系统提供网络安全强化。请参见 *安装证书, on page 9*

管理设备

添加设备

AXIS Device Manager 会自动在局域网中搜索已连接的设备，并尝试登录到所有设备。已找到设备列表显示了设备地址（IP 地址或主机名称）、序列号、型号和状态。序列号 (S/N) 打印在产品标签上。

要从列表中添加设备：

1. 选择要添加的设备，然后单击 **Next (下一步)**。
2. 选择 **Use host name when possible (尽可能使用主机名)**。如果使用主机名称添加设备，主机名称将用于与设备的所有进一步通信中。如果主机名不可用，则将使用 IP 地址。
3. 为没有密码的设备设置密码。如果不应该设置密码，请选择 **Skip (跳过)**。
4. 单击 **Next (下一步)**。

“准备好添加设备”页面显示了要添加的设备。

5. 单击 **Finish (完成)** 添加设备。

删除设备

要从列表中删除设备：

1. 转到 **Device management (设备管理)**。
2. 选择设备。
3. 右键单击并选择 **Remove (删除)**。
4. 单击 **Yes (是)**。

替换设备

要在 AXIS Device Manager 中替换设备，请连接一台新设备并重复使用现有设备的配置。如果操作成功，被替换的设备将被删除。必须至少有一个恢复点可用于该设备，参见 [创建恢复点](#), on page 8。恢复点不会迁移至新设备。

1. 转到 **Device management (设备管理)**。
2. 转到工具栏并单击替换设备图标。
3. 选择要替换的设备并单击 **OK (确定)**。
4. 选择您要用它替换的设备并单击 **OK (确定)**。
5. 单击 **Next (下一步)** 从最近恢复点中检索设备配置。
6. 转到 **Parameters (参数) > Additional Settings (其他设置)**，并选择要应用的参数和设置。
7. 单击 **Next (下一步)**。
8. 单击 **Finish (完成)** 应用设置。

还原设备

可以将一个或多个设备恢复至以前创建的恢复点。每个需恢复的设备必须具有至少一个可用的恢复点。默认情况下，会为选定服务器上的所有设备每天自动创建并持续删除恢复点。为便于恢复，固定数量的最新自动恢复点会被保留。

将设备还原到以前的恢复点：

1. 转到 **Device management (设备管理)** 工作区。
2. 选择一个或多个设备恢复。

3. 右键单击并从下拉菜单中选择 **Backup/Restore (备份/还原) >Restore to a Previous Time (还原到以前的时间)**。
4. 在最近可用恢复点列表中选择 **一个恢复点**，并单击 **Next (下一步)**。
5. 检查每个设备的设置，并单击 **Finish (完成)**。

安装应用

应用是一种可以上传并安装到安讯士设备上的软件。应用可以安装在支持 AXIS Camera Application Platform 的设备上。它们为设备添加功能，例如检测、识别、追踪或计数功能。应用必须先从 www.axis.com 或应用供应商的网站下载。某些应用还要求特定的 AXIS OS 版本或设备型号。如果应用需要许可证，许可证密钥文件可以与应用同时安装，也可以稍后使用设备的设置页面安装。如果应用无法安装，请访问 www.axis.com 并检查设备型号和 AXIS OS 版本是否支持 AXIS Camera Application Platform。

要安装应用：

1. 转到 axis.com 并下载应用。
2. 转到 **Browse to Application (浏览到应用)**
3. 单击 **Browse (浏览)**，然后转到您的下载文件夹
4. 选择该应用，然后单击 **Next (下一步)**

如果应用启动时需要许可证，您必须已下载许可证文件；如果未下载，请单击 **No (否)**，然后继续执行第 8 步：

5. 选择 **Yes (是)**，然后单击 **Next (下一步)**
6. 单击 **Browse (浏览)** 并选择许可证文件。
7. 单击 **Next (下一步)**。
8. 请选择您希望的安装类型：
 - **Application downgrade (应用降级)** 会安装应用的旧版本。
 - **Application overwrite (应用覆盖)** 将重新安装应用。

注意

降级或覆盖应用会重置设备上的应用设置。

可以安装

将要安装该应用的设备已列出。如果应用已安装在一些设备上，现有应用将被覆盖。覆盖会删除全部应用设置。

9. 单击 **完成**

配置

管理恢复点

恢复点是一种保存的设备配置，可用于备份和恢复设备设置。对于服务器上所有重新配置的设备，自动恢复点每晚都会创建。如果自上个恢复点创建以来设备的设置并未改变，那么将不会创建新恢复点。为了优化存储容量，最旧的恢复点会自动删除。为便于恢复，固定数量的最新自动恢复点会被保留。

创建恢复点

要创建手动恢复点：

- 转到 **Device management (设备管理)** 工作区。
- 选择一个或多个设备恢复。
- 右键单击并选择 **Backup / Restore > Create Restore Points (备份/恢复 > 创建恢复点)**。
- 输入一个描述，以便识别恢复点。
- 单击 **确定**。

注意

手动创建的恢复点不会自动删除。

创建自动恢复点

如果您拥有多台服务器，请从服务器列表中选择需配置的服务器。

- 转到 **Options (选项) > Restore point settings (恢复点设置)**。
- 选择 **Create restore points automatically (自动创建恢复点)**，支持自动创建恢复点。
- 输入需保存的自动恢复点的数量，并单击 **OK (确定)**。

管理多个凭据

此功能为 AXIS Device Manager 提供设备管理员帐户的凭据。

手动输入设备凭据

如果您选择手动输入设备凭据，则凭证将在 AXIS Device Manager 中针对所选设备进行更新。

- 选择一个或多个设备
- 右键单击并从下拉菜单中选择 **Advanced (高级) > – Enter Device Credentials (输入设备凭据)**。

注意

无法通过设备验证的凭据不会更新。此类操作中涉及的所有设备必须使用相同的用户名和密码。

使用 CSV 文件设置不同的凭据

通过使用 CSV 文件，您可以为每个设备使用单独的密码和单独的用户名。使用 MAC 地址、IP 地址或主机地址将 CSV 文件中的行映射到 AXIS Device Manager 数据库中对应的设备。

使用 CSV 文件时，用户界面会提示您指定如何解释 CSV 文件中的列。

注意

指定 CSV 文件中一行属于哪个具体设备。

CSV 文件中的一列需要包含 MAC 地址、IP 地址或主机地址，因此需要指定 CSV 文件中的哪一列应解释为 MAC 地址，以及哪一列应解释为 IP 或主机地址。这是为了指定 CSV 文件中一行的数据属于哪个设备。此外，还可以指定一列，将其解释为服务器名称。通过这种方式，可以区分 CSV 文件中针对位于不同 Axis Device Manager 服务器但具有相同 IP 地址或主机地址的设备的行。如果不需要这种区分，则无需设置要解释为服务器名称的列。如果一台服务器使用相同的 IP 地址或

主机地址为多个设备提供服务，但通过端口来区分它们，可以指定一列解释为端口。如果不需要通过端口进行区分，通常不需要设置要解释为端口的列。指定端口的另一种选择是在一个专门的列中提供端口，也就是将端口与 IP 地址或主机地址一起提供。IP 地址或主机地址后面应跟冒号和端口号。

安装证书

证书简介

AXIS Device Manager 提供用于管理服务器/客户端证书的设置。客户端证书用于 IEEE 802.1X，服务器证书用于 HTTPS。要实施任何更改，需要在 Device management (设备管理) 中选择适当的设备，然后在上下文菜单中选择 Enable/update (启用/更新)。

创建证书颁发机构 (CA)

CA 允许您在没有服务器/客户端证书的设备上启用 HTTPS 和 IEEE 802.1X。CA 指示设备使用自己的私钥创建证书，对其进行签名，然后进行安装。

要创建证书颁发机构：

- 转到 **Configuration (配置)** 选项卡。
- 转到 **Security (安全) > Certificates (证书)**
- 在 **Certificate authority (证书颁发机构)** 下，单击 **Generate... (生成...)**
- 输入密码并确认。
- 单击 **确定**。

现在将生成 CA 并可供使用。

注意

您的自签名根证书和私钥将受到您选择的密码的保护。AXIS Device Manager 生成的证书有效期为 3 年。如果您希望 AXIS Device Manager 自动更新服务器/客户端证书，则必须勾选 **Remember passphrase (记住密码)** 选框。如果未设置 Ca，则必须在 AXIS Device Manager 之外创建服务器/客户端证书。但这样您会失去自动证书管理的优势。

Import (导入) – 使用导入功能，您可以导入一个现有的 CA，包括公钥证书和私钥。您必须提供密码。

Save to file (保存到文件) – 以 .cer 或 .crt 格式保存 CA 的公钥证书。该文件不包含私钥，因此不会被加密。

Backup (备份) – 建议备份 CA，以防发生硬件故障。如果选中，将备份 Axis Device Manager 使用的 CA 的证书和私钥。备份数据将受到用于生成 CA 的密码保护。

Certificate expiration warning (证书到期警告) – 如果证书已到期或即将到期，将创建系统通知。它适用于安装在连接设备上的所有证书，但不适用于在 AXIS Device Manager 之外安装的 CA。警告将作为系统提醒出现在 Device management (设备管理) 的状态列中，在 View installed certificates (查看已安装的证书) 对话框中显示为图标，并会在 Configuration (配置) 工作区中显示。

指定您希望 AXIS Device Manager 在证书到期前多长时间通知您。默认情况下，AXIS Device Manager 生成的服务器和客户端证书将在到期警告出现前七天自动更新。要接收 CA 到期通知，需要选中 Remember passphrase (记住密码)。

启用 HTTPS

要启用 HTTPS，每个设备上都必须有服务器证书。AXIS Device Manager 可以使用证书颁发机构 (CA) 为设备签名并安装服务器证书。

您也可以手动执行此操作：

1. 转到 **Device manager (设备管理器)** 选项卡

2. 右键单击设备并在上下文菜单中选择 **Install server certificates for each device (为每个设备安装服务器证书)**。

在启用 HTTPS 之前，每个设备上只能有一个服务器证书。多余的证书可以从上下文菜单中删除。

3. 安装证书后，您可以在上下文菜单中启用 HTTPS。

注意

如果没有安全连接 (HTTPS)，则可以使用 HTTP 建立连接。这样做是为了能够配置尚未通过验证的设备。

忽略证书验证

如果设备的证书未通过验证，AXIS Device Manager 将不会连接到该设备。服务器证书需要由 AXIS Device Manager 中的活动 CA 签名，或者通过 Windows 证书存储进行验证。如果选择 **Ignore certificate validation (忽略证书验证)**，AXIS Device Manager 将不会验证设备发送的证书是否受信任。

要使 AXIS Device Manager 忽略证书验证。

- 转到 **Configuration (配置)** 选项卡。
- 在 HTTPS 下，启用 **Ignore certificate validation (忽略证书验证)**。

运行 802.1X

要启用 IEEE 802.1X，每个设备上都必须有客户端证书。AXIS Device Manager 可以使用证书颁发机构 (CA) 为设备签名并安装客户端证书。

您也可以在 Device management (设备管理) 中手动执行此操作，方法是右键单击设备并在上下文菜单中选择 **Install client certificates for each device (为每个设备安装客户端证书)**。在启用 IEEE 802.1X 之前，每个设备上只能有一个客户端证书。多余的证书可以从上下文菜单中删除。安装证书后，您可以在上下文菜单中启用 IEEE 802.1X。

您还需要 IEEE 802.1X 身份验证 CA 证书才能使用 IEEE 802.1X 协议。

EAPOL Version (EAPOL 版本) – 选择要使用的可扩展身份验证协议 (EAP) 版本。

EAP identity (EAP 身份) – 输入设备的 MAC 地址、设备主机名或自定义文本。

Custom (自定义) – 输入任何可用作 EAP 身份的文本。

IEEE 802.1X authentication CA certificate (IEEE 802.1X 身份验证 CA 证书) – 除了客户端证书之外，还必须安装 IEEE 802.1X 身份验证 CA 证书。启用 IEEE 802.1X 时，只需要公钥证书，而不需要私钥，因此无需任何密码。启用或更新 IEEE 802.1X 时，将安装 IEEE 802.1X 身份验证 CA 证书。

Import (导入) – 选择将安装在设备上，并将用于验证身份验证服务器的 CA 证书。CA 证书可以由 AXIS Device Manager 中的 CA 创建，也可以来自外部来源。

View (查看) – IEEE 802.1X 身份验证过程中使用的 CA 证书的详细信息。

Common name (通用名称) – 选择设备 EAP 身份或设备 IP 地址。如果自定义字段留空，则将选择主机名。如果主机名存在问题，则将使用 IP 地址作为通用名称。

配置 SIP 设置

要配置所选设备的 SIP 和端口设置，请使用设置助手。设置助手允许您保留设备中已有的值，或输入一个将应用于大多数选定设备的值。您还可以从 CSV 文件加载值，为选定的设备应用设备特定值。

在 CSV 文件中，每个设备占用一行，每个待设置参数占用一列。设置助手允许您指定要获取的值。

要使用 CSV 文件为多个设备配置设备特定设置：

1. 转到 **Device management (设备管理)** 工作区。
2. 选择要配置的设备。

3. 右键单击并选择**配置设备 > 高级 > SIP 配置 > 设置**。
4. 若要使用 CSV 文件，请核实您已允许使用 CSV 文件。否则，请转至步骤 5。
 - 4.1. 单击**浏览**并选择您要使用的 CSV 文件。
 - 4.2. 单击**下一步**
 - 4.3. 在下拉菜单中选择如何命名 CSV 文件的列。
 - 4.4. 针对 CSV 文件中的一列选择 MAC 地址、IPv4 地址或主机地址，并将其与行中的设备相关联。
5. 单击 **Next (下一步)**。
6. 选择以下不同 SIP 和端口设置：
 - **启用 SIP** – 在所选设备上启用 SIP。
 - **允许传入 SIP 呼叫** – 允许向您的设备传入 SIP 呼叫。
 - **SIP 端口** – 分配用于 SIP 呼叫的端口号。
 - **TLS 端口** – 分配用于 TLS 加密的端口号。
 - **RTP 起始端口** – 分配用于音频流量的 RTP 端口号。
7. 单击 **Next (下一步)**。
8. 选择以下不同音频和呼叫设置：
 - **音频方向** – 在**仅发送**、**仅接收**或**发送与接收**之间选择。
 - **DTMF 有效载荷类型** – 选择用于传输 DTMF 数字、音调和信号的 DTMF 有效载荷类型。
 - **呼叫超时** – 选择等待几秒后呼叫超时。
 - **呼入超时** – 选择等待几秒后呼入超时。
 - **几秒后呼叫结束** – 选择等待几秒后呼入自动结束。您还可以选择允许无限呼叫时长。
9. 单击 **Next (下一步)**。
10. 选择以下不同网络地址转换 (NAT) 穿透参数：
 - **ICE 启用** – 在所选设备上启用交互式连接建立 (ICE)。
 - **TURN 启用 (TURN)** – 启用基于网络地址转换 (TURN) 使用中继穿透。
 - **TURN 服务器地址** – 输入 TURN 服务器的地址。
 - **TURN 用户名** – 输入 TURN 用户名。
 - **TURN 密码** – 输入 TURN 密码。
 - **启用 STUN** – 启用用于网络地址转换 (STUN) 的会话穿透实用程序
 - **STUN 服务器地址** – 输入 STUN 服务器的地址。
11. 单击 **Next (下一步)**。
12. 查看所列设备的配置。
13. 如果一切正常，单击**完成**。

管理 SIP 帐户

在 AXIS Device Manager 中，您可以配置 SIP 设置并添加或删除 SIP 帐户。

添加 SIP 帐户

要添加 SIP 帐户，您应在 CSV 文件中指定它们。您可以在设置助手中创建模板。

要生成一个模板：

1. 转到 **Device management (设备管理)** 工作区。

2. 选择要配置的设备。
3. 右键单击并选择**配置设备 > 高级 > SIP 配置 > 添加 SIP 账户**。
4. 单击**生成模板**
5. 选择一个位置来保存 CSV 文件。
6. 将账户添加到文件中。对于要向设备添加的账户，每个账户单独占用一行。您可向设备添加多个账户。

CSV 文件的布局如下：

| 列名 | 说明 | 必选/可选 | 注意 |
|---------|-------------------|-------|--|
| 设备标识符 | MAC 地址、IP 地址或主机地址 | 必选 | 此列指定应将账户添加至哪个设备。可以是 MAC 地址、IPv4 地址或主机地址。 |
| 有效 | 布尔值 | 必选 | |
| 设为默认 | 布尔值 | 必选 | |
| 自动应答 | 布尔值 | 必选 | |
| name | 字符串 | 必选 | |
| 用户 ID | 字符串 | 必选 | |
| 域 | 字符串 | 可选 | 若 CSV 文件中缺少此列，则大多数账户均设置为点对点账户。若此列存在，且单元格为空，账户则设置为点对点账户；若单元格不为空，则设置为注册账户。 |
| 密码 | 字符串 | 必选 | |
| 身份验证 ID | 字符串 | 必选 | |
| 呼叫者 ID | 字符串 | 必选 | |
| 注册 | 字符串 | 可选 | |
| 传输模式 | UDP 或 TCP | 必选 | 在 MVP1 中，TLS 不受支持。 |

要将账户添加到所选设备：

- 转到 **Device management (设备管理)** 工作区。
- 选择要配置的设备。
- 右键单击并选择**配置设备 > 高级 > SIP 配置 > 添加 SIP 账户**。
- 单击**浏览**。
- 选择您已添加账户的 CSV 文件。
- 单击**下一步**
- 查看所列设备的配置。
- 如果一切正常，单击**完成**。

删除 SIP 账户

要删除所选设备上除默认账户外的大多数 SIP 账户：

1. 转到 Device management (设备管理) 工作区。
2. 选择要配置的设备。
3. 右键单击并选择配置设备 > 高级 > SIP 配置 > 删除账户。
4. 在设置助手中，勾选删除所选设备上除默认账户外的大多数 SIP 账户。
5. 单击完成。

在设备上启用元数据

在此用例示例中，我们将为多台设备启用元数据。在执行此操作之前，我们建议您先在一台设备上尝试，以避免同时处理多台设备时出现问题。要在一台或多台设备上启用元数据：

1. 转到 Device management (设备管理) 工作区。
2. 选择您想要启用元数据的设备。
3. 右键单击并选择配置设备 > 高级 > 设置配置。
4. 单击确定
5. 在下拉菜单中选择设置 NTP 服务器。
6. 在 URI 下拉菜单中，保障方法为 Post。
7. 在地址字段中添加以下内容：AXIS-CGIAnytalycsMetadataconfig.cgi
8. 在内容中添加以下代码：

```
{ "apiVersion": "1.0", "context": "my context", "method": "setEnabledProducers", "params": {
  "producers": [ { "name": "objectanalytics", "videochannels": [ { "channel": 1, "enabled": true }
  ] } ] }
```

9. 检查内容-类型是否为应用程序/json
10. 单击发送。

注意

请注意，当您使用上述方法时，AXIS 设备管理器将不会返回响应。请务必检查任务面板是否现出错误。您还可以使用像 Postman 这样的专用软件来测试功能得以改进的 API。某些 VMS 可能存在限制，仅允许一次存在一个生产者，因此您可能需要通过上述 API 禁用额外的生产者。

管理设备软件

AXIS OS 升级

可以通过两种方式获取新的 AXIS OS 版本：

- 通过 AXIS Device Manager 下载（需要联网）
- 从文件导入（例如硬盘或 U 盘）。

注意

我们建议您遵循 AXIS OS 推荐的升级路径。点击此处了解更多信息：<https://help.axis.com/axis-os#upgrade-path>

AXIS OS 手动升级

1. 选择您要升级到新 AXIS OS 版本的设备，右键单击并选择 **Upgrade firmware（升级固件）**。
2. 当提示设备将在升级过程中无法访问时，请单击 **Yes（是）**。
3. 要在 **Upgrade firmware（升级固件）** 对话框中更新可供下载的固件版本列表，请单击 **Check for Updates（检查更新）**。
4. 要浏览存储在本地客户端上的一个或多个 AXIS OS 版本文件，单击 **Browse（浏览）** 按钮。
5. 选择要升级的设备和 AXIS OS 版本。
6. 要在 AXIS OS 升级期间将所选设备恢复为出厂默认设置请单击 **Factory default（恢复出厂设置）** 复选框。在某些版本的 AXIS OS 降级时，此步骤是必需的。
7. 单击 **OK（确定）** 开始升级列表中的所选设备。

注意

默认情况下，选定设备的 AXIS OS 升级将同时完成。可以在 **Configuration（配置）>Connected Services（连接服务）>Firmware upgrade（固件升级）** 设置中更改升级顺序。

自动升级

AXIS Device Manager 5 默认设置为不检查固件升级，但可以将其设置为自动检查服务器或 axis.com 上是否有可用的 AXIS OS 升级。

要手动检查 AXIS OS 升级，请按操作菜单中的 **Check now（立即检查）** 按钮。

AXIS OS 升级顺序

可以同时在全部设备上进行 AXIS OS 升级，也可以逐一进行。

- 要同时升级全部设备，请选择 **Parallel（并行）** 升级顺序
- 要逐一升级设备，请选择 **Sequential（顺序）**。此选项耗时更长，但设备不会同时离线。如果在顺序升级过程中出现问题，您还可以通过选中 **Cancel all remaining upgrades if one（如果一个设备失败，则取消所有剩余升级）** 复选框来停止顺序升级。

故障排查

软件物料清单

获取软件物料清单 (SBOM):

1. 转到 axis.com 上的 *AXIS Device Manager* 产品支持页面。
2. 单击 **SOFTWARE BILL OF MATERIALS (软件物料清单)**。

如需进一步了解 SBOM, 请转到 axis.com 上的 *AXIS OS* 门户。

联系支持人员

联系支持人员时, 请先创建工单并附上系统报告文件, 以便于他们解决您的问题:

1. 转到主菜单。
2. 转到 **Help (帮助) > System Report... (系统报告...)**
3. 将报告文件保存在选定的文件夹中。
4. 转到 axis.com/support。
5. 创建支持工单。
6. 将文件附加到您的支持工单。

注意

从无响应系统创建系统报告:

1. 转到 `C:\ProgramData\Axis Communications\`
2. 将文件夹内容存档为 .zip 文件, 并将其作为附件, 添加到支持工单中。

升级流程

当您遇到无法使用本指南解决的问题时, 请将问题上报给 Axis 在线帮助台, 请参阅 *Axis 在线帮助台*。为让我们的支持团队了解您的问题并能够解决问题, 您必须提供以下信息:

- 有关如何重现问题或在什么情况下发生问题的清晰描述。
- 出现问题的时间以及相关设备的名称或 IP 地址。
- *AXIS Device Manager* 问题发生后直接生成的系统报告。系统报告必须从重现问题的客户端或服务器生成。
- 显示问题的可选屏幕截图或屏幕录制。
- 如有必要, 请包含数据库文件。排除这些以使上传速度更快。

必要时, 对于某些问题, 支持团队要求提供其他信息。

注意

如果文件大于 100 MB (例如网络跟踪或数据库文件), 请使用您信任的安全文件共享服务发送文件。

| | |
|---------------|---|
| 其他信息 | |
| 调试级别日志 | 有时我们使用调试级别日志记录来收集更多信息。此操作仅应 Axis 支持工程师的请求完成。您可以在 <i>Axis 在线帮助台</i> 上找到说明。 |
| 网络追踪 | 如果支持工程师提出请求, 请在创建系统报告时生成网络跟踪。如果问题可重现, 则在问题发生期间进行网络跟踪。这包括: <ul style="list-style-type: none"> • 对摄像机进行的 60 秒网络跟踪 (仅适用于固件 5.20 及更高版本) 如有必要, 使用以下 VAPIX 命令更改登录名、IP 地址和持续时间 (以秒为单位): |

| | |
|-------|--|
| 其他信息 | |
| | <p><code>http://root:pass@192.168.0.90/axis-cgi/debug/debug.tgz?cmd=pcapdump&duration=60</code></p> <ul style="list-style-type: none"> 在服务器上进行的 10–30 秒网络跟踪，显示服务器与摄像机之间的通信。 |
| 数据库文件 | 在我们必须检查或手动修复数据库的情况下。在生成系统报告之前，选择在报告中包括数据库。 |
| 屏幕截图 | 如果与用户界面相关且是实时画面问题，请使用屏幕截图。例如，当您想要显示录制的时间线或难以描述问题时。 |
| 屏幕记录 | 当难以用语言描述问题时，例如，当涉及许多 UI 交互来重现问题时，请使用屏幕录制。 |

T10211981_zh

2026-03 (M5.2)

© 2024 – 2026 Axis Communications AB