AXIS Device Manager

用户手册

目录

关于 AXIS 设备管理器

AXIS Device Manager 是用于安讯士产品的安装和管理软件。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。

解决方案概述

前提条件

兼容的操作系统：

运行要求：64 位操作系统 Microsoft .NET 版本 4.8

支持的操作系统：Windows 10 Pro、Windows 11 Pro、Windows Server 2016、Windows Server 2019、Windows Server 2022

建议：最新的操作系统服务包。

最低系统建议：

- 最低配置（最多 500 台设备）：英特尔酷睿 i5 或同等处理器，4GB 内存，网络基础设施中速率为 100 Mbits/s
- 推荐配置（500 到 2,000 台设备）：英特尔酷睿 i7 或同等处理器，8GB 内存，网络基础设施中速率为 1000 Mbits/s
- 不建议每台服务器连接超过 2,000 个设备。
- 确保安讯士设备运行最新的 AXIS OS。

注意

我们始终支持最新版本之前的两个版本。查看最新的发行说明，了解支持哪些具体版本。

支持的设备：

运行 AXIS OS 版本 4.40 或更高版本的安讯士产品。（请注意，具体支持的功能会因特定产品型号和固件而有所不同）

语言：

用户界面 + 帮助文件：英语、法语、德语、意大利语

仅用户界面：阿拉伯语、捷克语、中文（简体）、中文（繁体）、荷兰语、芬兰语、日语、韩语、波斯语、波兰语、葡萄牙语（巴西）、俄语、西班牙语、瑞典语、泰语、土耳其语和越南语。

开始使用

安装软件

要安装 AXIS Device Manager 5，请确保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. 选择连接到本地计算机或远程服务器，如上所述。

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：。

- 为您的系统提供网络安全强化。请参见

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。

移除设备

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。必须至少有一个还原点可用于该设备，参见 。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还原点。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还原点：

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）。

配置

创建还原点

要创建手动还原点：

- 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，以便识别还原点。
- 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（**还原点设置**）。
- 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。

管理 SIP 帐户

管理设备软件

AXIS OS 更新

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）。

AXIS OS 手动升级

1. 选择您要升级到新版本 AXIS OS 的设备，右键单击并选择 **Upgrade AXIS OS（升级 AXIS OS）**。
2. 在 **Upgrade firmware（升级固件）**对话框中：要更新可供下载的固件版本列表请单击 **Check for Updates（检查更新）**按钮。
3. 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。
4. 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。
5. 选择要升级的设备和 AXIS OS 版本，然后单击 **OK（确定）**开始升级列表中的选定设备。

注意

默认情况下，将同时为所有选定设备进行 AXIS OS 更新。可以在 **Configuration（配置）>Connected Services（连接服务）>Firmware upgrade（固件升级）**设置中更改更新顺序。

自动更新

AXIS Device Manager 5 默认设置为不检查任何 AXIS OS 更新，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 更新。

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

AXIS OS 升级顺序

可以同时在所有设备上进行 AXIS OS 更新，也可以逐一进行。

- 要同时更新所有设备，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

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 *Axis 在线帮助台*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： • 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）： `http://root:pass@192.168.0.90/axis-cgi/debug/debug.tgz?cmd=pcapdump&duration=60` • 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**。

其他信息	
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

2025-03 (M1.9)