AXIS Device Manager

用户手册

引言

网络安全在监控和安全领域中越来越重要。有效的网络安全需要确保足够的防御深度，以便在各个层面妥善保护您的 IP 网络——从您选择的产品和合作伙伴，到您和他们设定的要求。

本指南介绍了如何使用 AXIS Device Manager 来强化您的系统并提高安全性。它集中讨论了一些重要方面并提出建议。

设备生命周期管理

在安讯士，我们深知在设备的整个生命周期中建立强大的安全基础的重要性。我们对网络安全的承诺确保我们的产品和解决方案能够提供强大的防护，抵御潜在威胁。

实施

安讯士提供安全设计设备，并内置安全功能，例如安全启动机制、签名操作系统和加密存储。此外，AXIS Device Manager 可帮助安装人员和系统管理员安全地配置和部署设备，确保从一开始就实现架构安全。

主动服务

在运行阶段，安讯士会定期提供设备软件更新和安全补丁，以防御漏洞。AXIS Device Manager 还支持远程监控和维护，从而能快速解决问题并最大程度地减少停机时间。此外，我们的强化配置指南提供了实用建议，帮助您配置设备以满足特定安全要求。

停运

当需要退役或更换设备时，AXIS Device Manager 可以通过擦除敏感数据并将设备恢复到出厂设置来促进安全退役。这可确保设备上不会残留任何机密信息，从而保护用户数据并防止未经授权的访问。

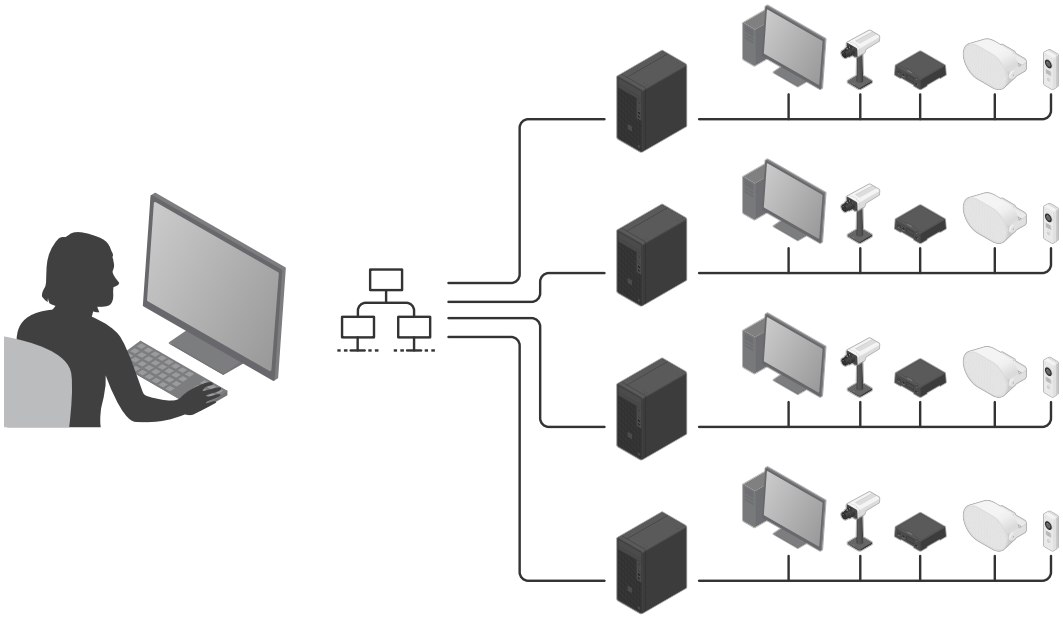
AXIS Device Manager

AXIS Device Manager 是一款本地工具，它提供了一种简单、经济高效且网络安全的方式来管理所有主要的安装、安全和维护任务（请参阅下表）。该工具适用于管理单个场所中多达数千台安讯士设备，或分布在多个场所中的数千台设备。AXIS Device Manager 使您能够高效地部署网络安全控制措施，以保护您的网络设备，并使其与安全基础设施保持一致。

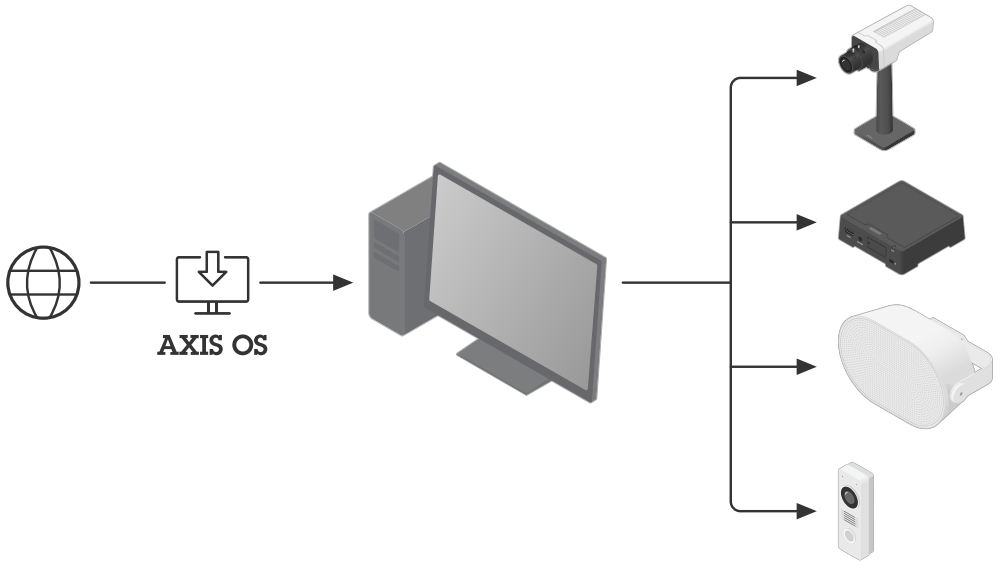
设备管理功能，AXIS 设备管理器

安装	**维护**
分配 IP 地址	设备状态
导出设备列表并保持跟进资产*	收集设备数据
用户和密码管理*	配置设备并将配置复制到多台设备
ACAP 管理	连接至多个服务器/系统
升级 AXIS OS，基于 LTS 或 Active*	复位点
HTTPS 证书管理*	恢复出厂默认设置
管理 IEEE 802.1 证书*/**	替换设备
设备标记	证书续订和管理*
	网络安全强化*

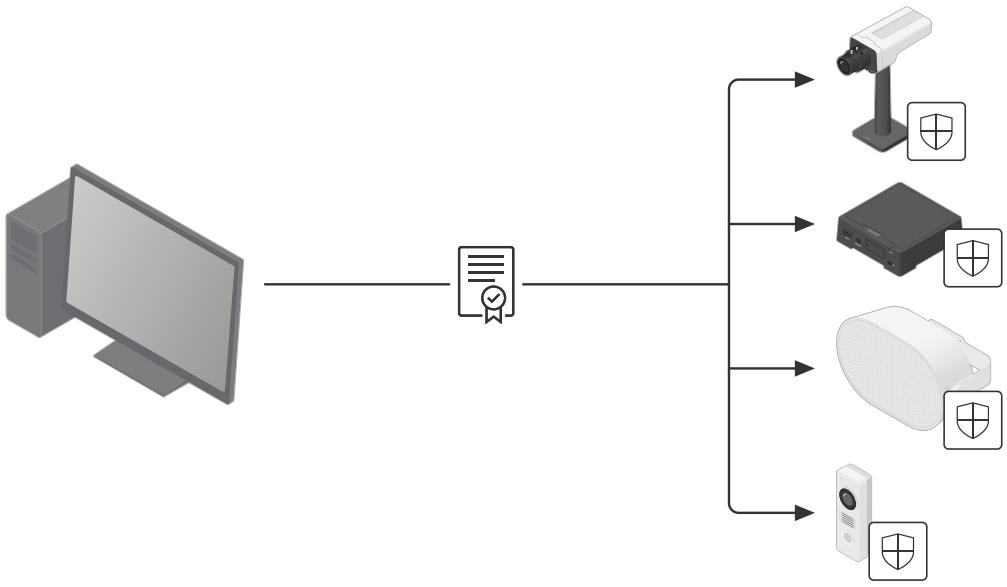
*指网络安全控制功能。
**目前不支持 Active Directory 证书服务。已针对在 Linux 上运行的 FreeRADIUS 验证。



多场所管理。



AXIS OS 升级。



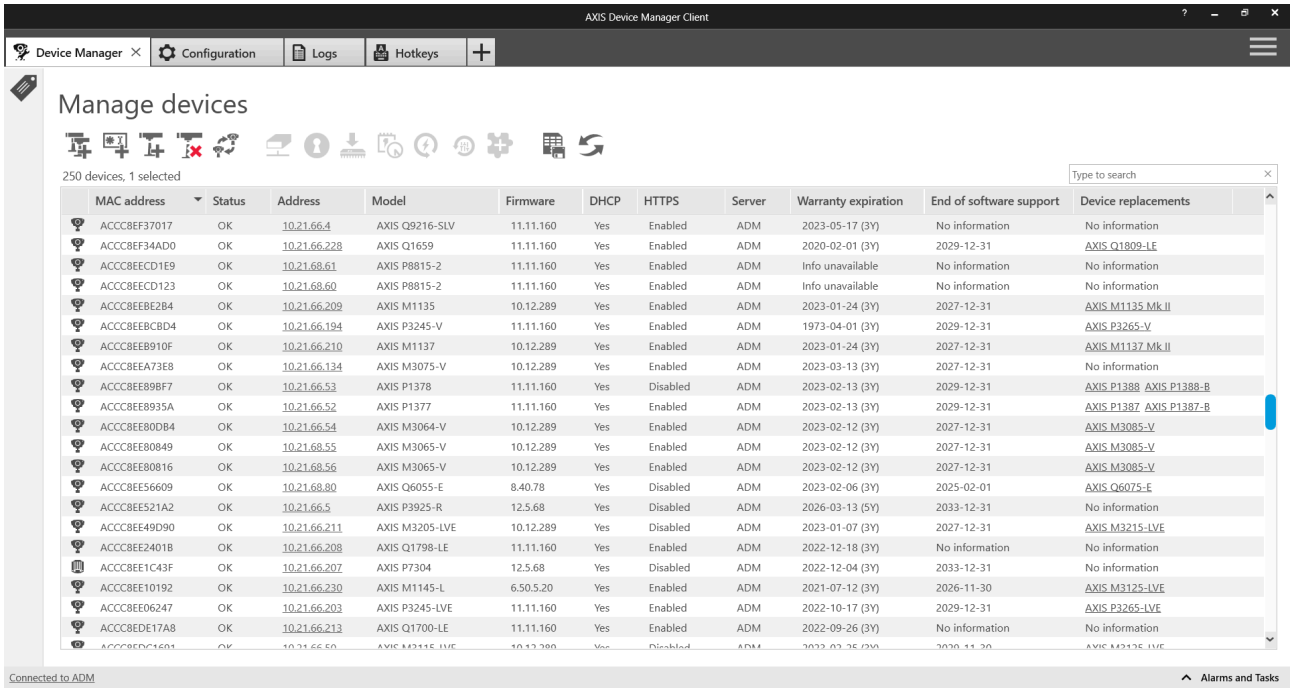
证书管理。

设备清单

确保企业网络安全的一个基本方面是维护网络上所有设备的完整清单。在创建或审查整体安全策略时，了解并清晰地记录每台设备（而不仅仅是关键资产）至关重要。这是因为任何被忽视的设备都可能成为攻击者入侵的途径。您无法保护您忽视或不完全了解的设备。

设备清单是保护企业网络安全的重要步骤。AXIS Device Manager 可以为您提供以下帮助：

- 在进行审计和事件响应时，让您能轻松访问最新、完整的网络设备清单。
- 提供完整的设备列表，可按总数、类型、型号等排序。
- 提供网络上每台设备的状态。
- 通过显示设备软件支持计划结束的时间以及列出可用作替代品的较新产品，帮助您提前规划。



AXIS 设备管理器可针对您的设备清单提供一个清晰视图。

AXIS Device Manager 提供自动化方式，以访问安讯士网络设备的实时清单。它可让您自动识别、列出您的设备并进行分类。同样重要的是，它允许您使用标签根据自己的标准对设备进行分组和排序，从而轻松概览和记录网络上的所有安讯士设备。

帐号和密码政策

身份验证和权限控制是保护网络资源的一个重要部分。实施策略有助于降低意外或故意滥用的风险。强制使用强密码是一项关键任务，但降低密码泄露的风险也同样重要。设备密码往往会在组织内传播，一旦发生泄露，您将无法控制谁有权访问它们。AXIS Device Manager 可帮助您轻松管理安讯士设备的多个帐户和密码。

为什么您应在设备中设置多个用户帐户：

- 您可以控制不同用户类型（机器和人员）的权限级别。
- 您可以降低泄露根（主）密码的风险。
- 您可以重置某一用户类型的凭据，而不会影响其他用户。

使用 AXIS 设备管理器中的权限进行操作

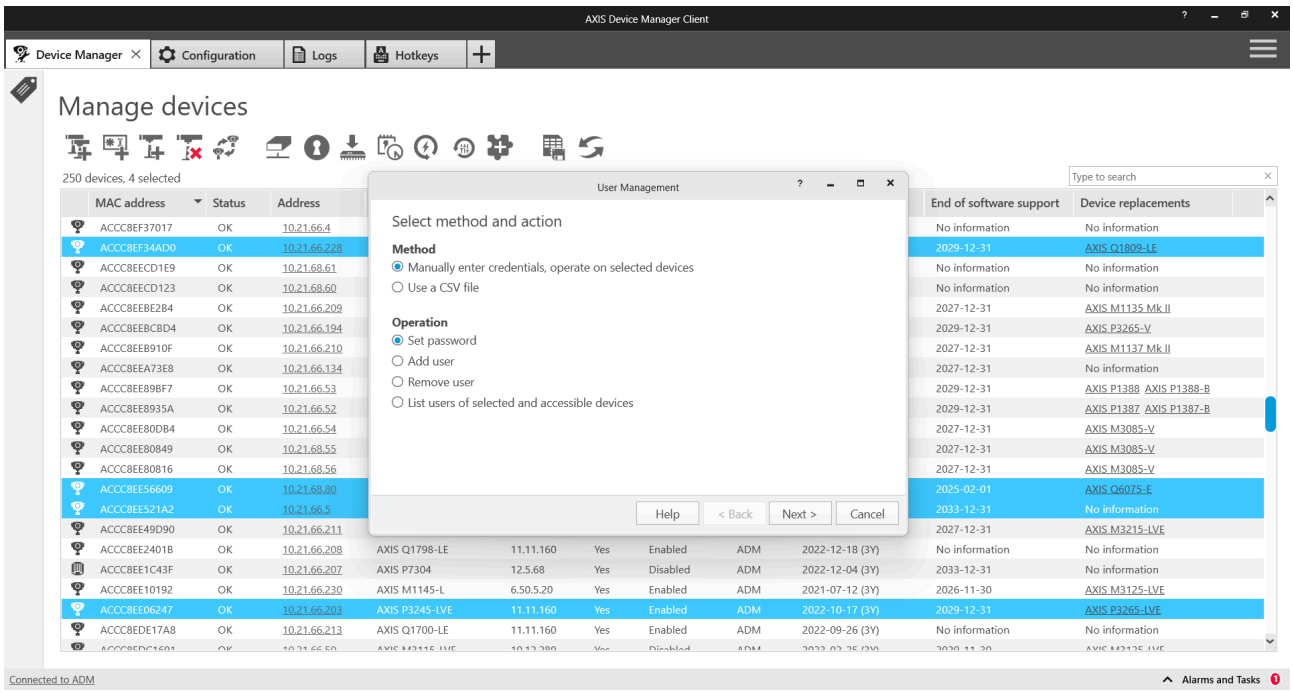
安讯士设备支持多个帐户，每个帐户具有三种不同权限级别之一：

- **浏览者**：这些用户可以访问视频和 PTZ 控制。
- **操作员**：拥有操作员权限的用户可以优化摄像机设置和视频流配置文件。
- **管理员**：管理员可以管理帐户、修改网络设置并控制设备中的多项服务。

每个可访问摄像机的角色都应拥有各自的帐号。例如，您可以将“控制室人员”角色的权限级别配置为“操作员”，而“巡逻人员”角色可能只需要“查看者”权限级别。

建议步骤

- 在将摄像机添加到 VMS 之前，请先将摄像机添加到 AXIS Device Manager。
- 在 AXIS Device Manager 中，选择所有摄像机，并创建一个名为“vms”或类似名称的新用户帐户，并设置一个强密码。权限需要符合 VMS 的要求——这可能是操作员或管理员（请咨询制造商）。
- 使用您创建的帐户和密码将设备添加到 VMS。
- 返回 AXIS Device Manager，再次选择所有摄像机，并使用新的强密码重置（更改）“root”帐户密码。“root”帐户密码应该只有少数人（使用 AXIS Device Manager 的用户）知晓。
- 当有人需要使用网络浏览器访问设备进行维护或故障排查任务时，**不要**为其提供 root 密码。相反，使用 AXIS Device Manager 为选定的设备创建一个新的（临时）帐户，并赋予其管理员或操作员权限。工作完成后，使用 AXIS Device Manager 删除临时帐户。
- AXIS 设备管理器支持本地管理员以及域用户和域组。如果仅能从托管 AXIS 设备管理器服务器的相同机器才能访问 AXIS 设备管理器客户端，那么您可以使用本地管理员权限。如果系统维护人员将使用远程客户端，我们建议使用域用户。



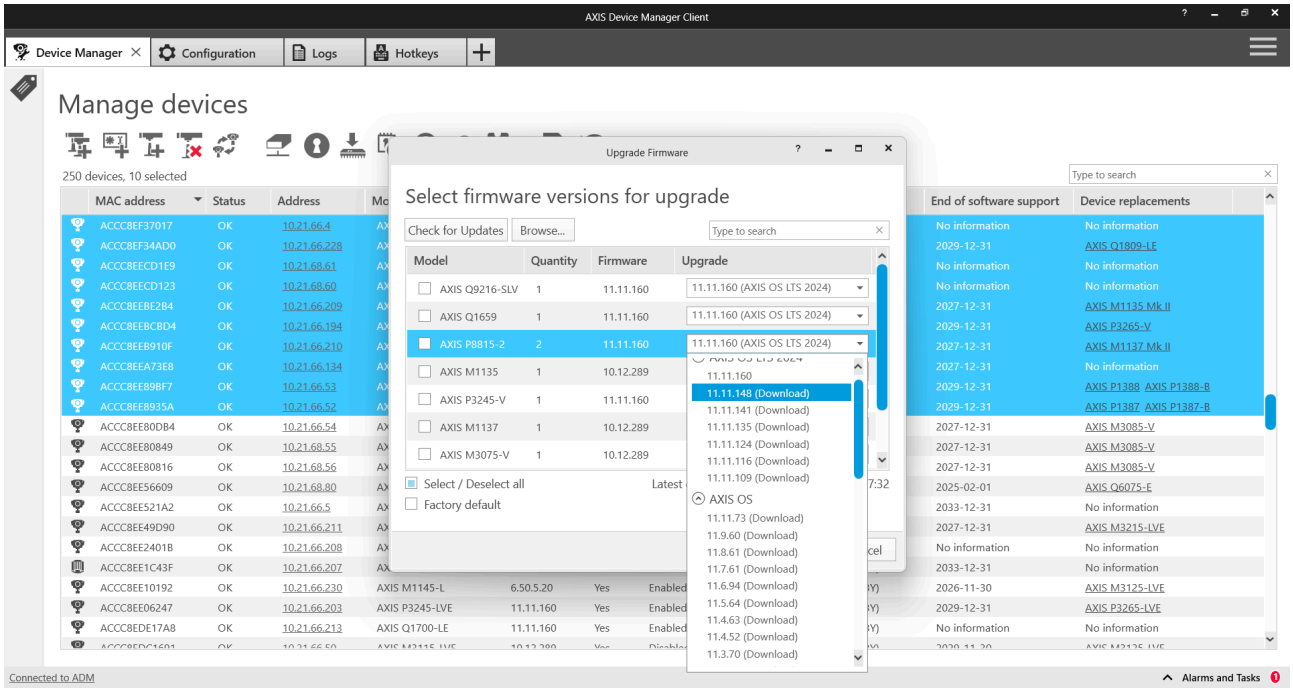
更改 AXIS 设备管理器中的用户角色和密码。

AXIS OS 升级

更新的 AXIS OS 版本包含已知漏洞的补丁。始终使用最新软件至关重要，因为攻击者可能会尝试利用已知漏洞。同样重要的是，快速部署新的 AXIS OS 版本可以提升运营能力，并消除与手动部署新版本升级相关的阻碍。AXIS Device Manager 连接到 www.axis.com 并下载最新的适用 AXIS OS 或服务版本。如果您不想从互联网上直接将其下载至您的网络，则您可以将升级版本保存至一个 USB 记忆棒中，随后将其上传至您的 AXIS 设备管理器客户端。它还会显示是否有新的 AXIS OS 版本可用，并允许您在安讯士设备上快速部署它们。

为什么您应该始终运行最新的 AXIS OS 版本：

- 您的网络和设备通过最新的补丁得到保护，以防范已知漏洞，尤其是关键漏洞。
- 您的设备更新了最新的性能改进，并修复了错误和缺陷。
- 您能够立即获得最新的功能和功能增强。



借助屏幕通知和直观的对话框，使用 AXIS Device Manager 升级 AXIS OS 变得非常简单。

附加强化

采用完善的用户和密码策略，并运行最新的 AXIS OS 版本，可以有效降低设备的常见风险。*安讯士强化配置指南*介绍了在大型关键组织中降低风险的其他措施。这包括禁用可能不使用的服务，以及启用有助于监测和监控攻击或违规迹象的服务。AXIS Device Manager 简化了部分策略的部署流程。安讯士提供了用于基本推荐设置的配置模板。

如何根据安讯士强化配置指南强化设备：

- 阅读*安讯士强化配置指南*，并在文档末尾下载模板文件。
- 编辑配置文件以选择相关项目。
- 在 AXIS Device Manager 清单中选择设备。
- 右键单击并选择“Configure Devices Configure…（配置设备…）”
- 单击“Configuration File（配置文件）”并选择下载的文件。
- 根据需要调整设置。

证书授权服务

证书颁发机构 (CA) 是一种为服务器、客户端或用户颁发数字证书的服务。一个 CA 可以是公有的，也可以是私有的。公开可信的 CA（例如 Comodo 和 Symantec（原名 Verisign））通常可用于公共服务，例如公共网站和电子邮件。

私有 CA（通常是活动目录/证书服务）为内部/私有网络服务颁发证书。在视频管理系统中，这主要用于 HTTPS 网络加密和 IEEE 802.1x 网络访问控制。AXIS Device Manager 为安讯士设备提供 CA 服务，可以作为私有根 CA 或私有中间 CA 运行；作为企业公钥基础设施 (PKI) 的一部分。

CA 签发的证书可用于 IEEE 802.1x（客户端）和 HTTPS（服务器）证书。

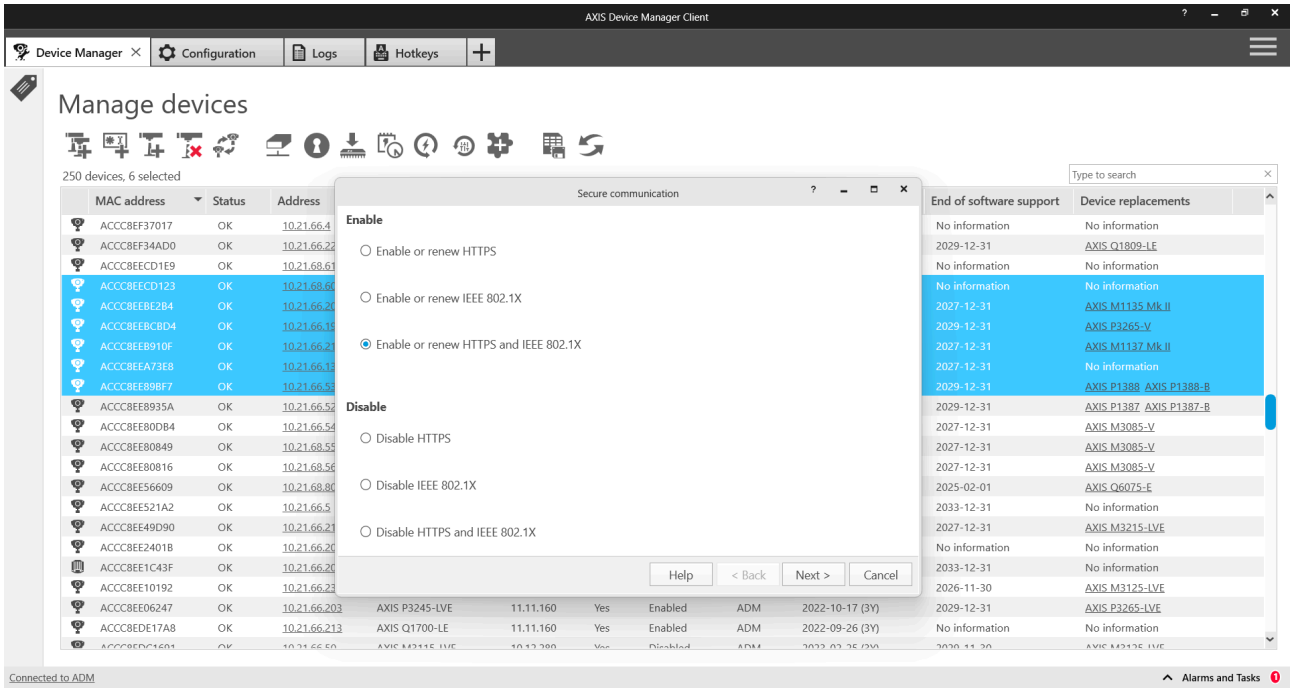
HTTPS

HTTPS 是 HTTP 的安全版，可通过此协议给客户端和服务器之间的通信加密。自签名证书足以实现加密连接。自签名证书和 CA 签名证书的加密级别没有区别。区别在于自签名证书无法防御网络欺骗，即攻击计算机试图冒充合法服务器的行为。CA 签名证书为客户端添加了一个信任点，用于验证其是否正在访问受信任的设备。请注意，视频客户端 (VMS) 需要通过 HTTPS (RTP over RTSP over HTTPS) 支持请求播放的视频以加密视频。

IEEE 802.1X

该标准通常简称为 802.1X，可防止未经授权的网络设备访问本地网络。一台设备在被允许访问网络（及其资源）之前需要对自身进行身份验证。可以使用多种身份验证方法：MAC 地址（MAC 过滤）、用户/密码或客户端证书。系统所有者决定使用哪种方法；根据威胁、风险和成本做出适当的选择。

运行一个 802.1X 基础设施就是一种投资。它需要管理型交换机和附属服务器，通常是一个 RADIUS（远程用户拨号认证服务）。使用客户端证书需要一个可颁发客户端证书的 CA（私有或公有）。大多数情况下，基础设施需要专人维护和监控。



AXIS 设备管理器中的证书配置。

证书生命周期管理

证书生命周期管理是一种经济高效地处理与证书颁发、安装、检查、修复和续期相关的所有流程和任务的方法。AXIS Device Manager 使您能够高效管理证书，管理员可以执行以下操作：

- 在没有其他证书颁发机构时颁发由 CA 签名的证书
- 轻松管理 IEEE 802.1X 证书
- 轻松管理 HTTPS 证书
- 监控证书有效期
- 轻松更新有效证书

提供针对私有根 CA 和中间 CA 的建议

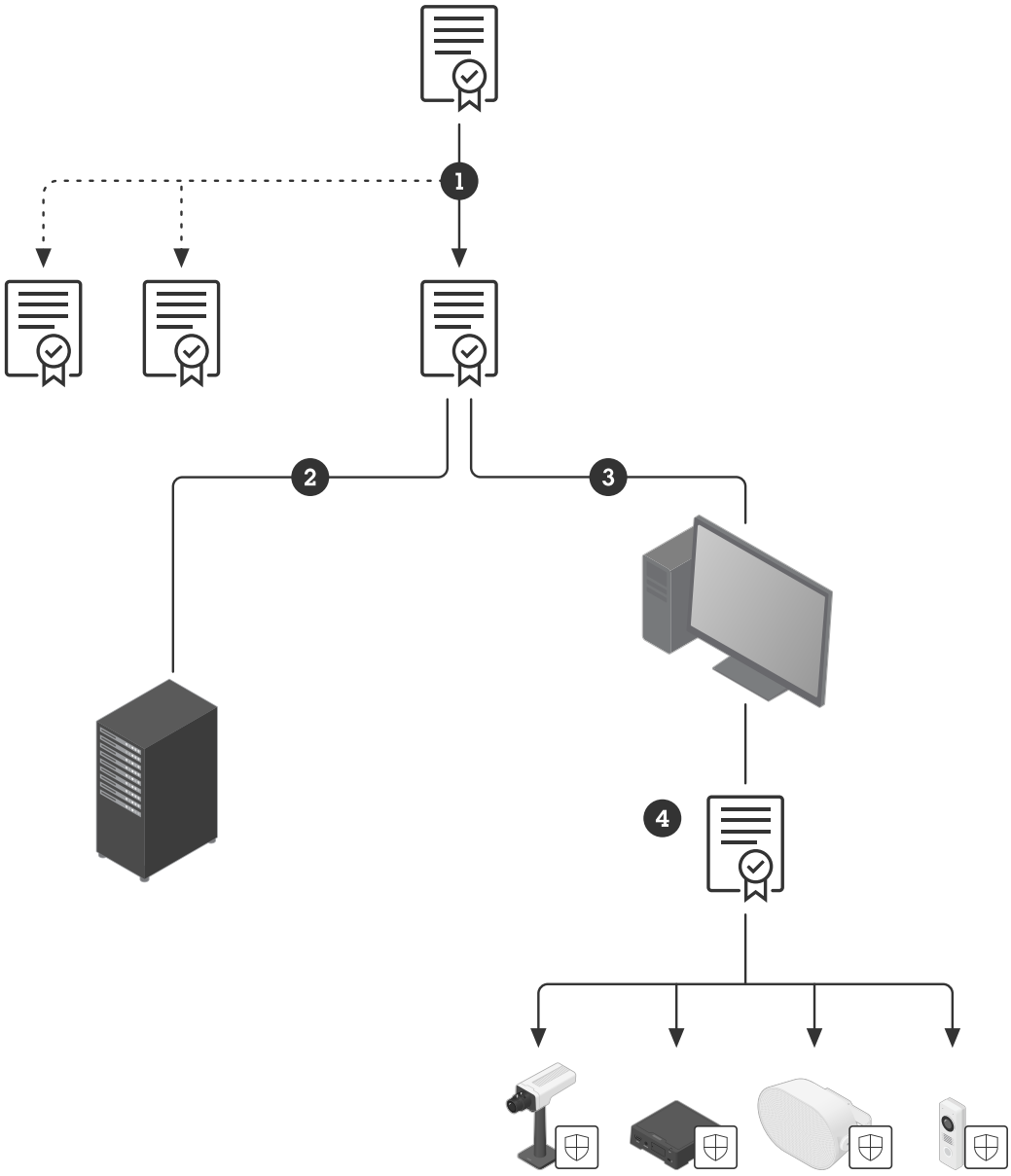
不建议将安讯士设备作为针对公众的公共服务器进行公开。这就是为什么使用公共 CA 来管理私有资源并不划算的原因。

对于 HTTPS，VMS 服务器是唯一需要验证其是否正在访问受信任摄像机的客户端。操作员客户端永远不会直接访问摄像机，因为实时和录制的视频由 VMS 服务器提供。在这种情况下，将摄像机服务器证书纳入现有企业 PKI 的价值有限。

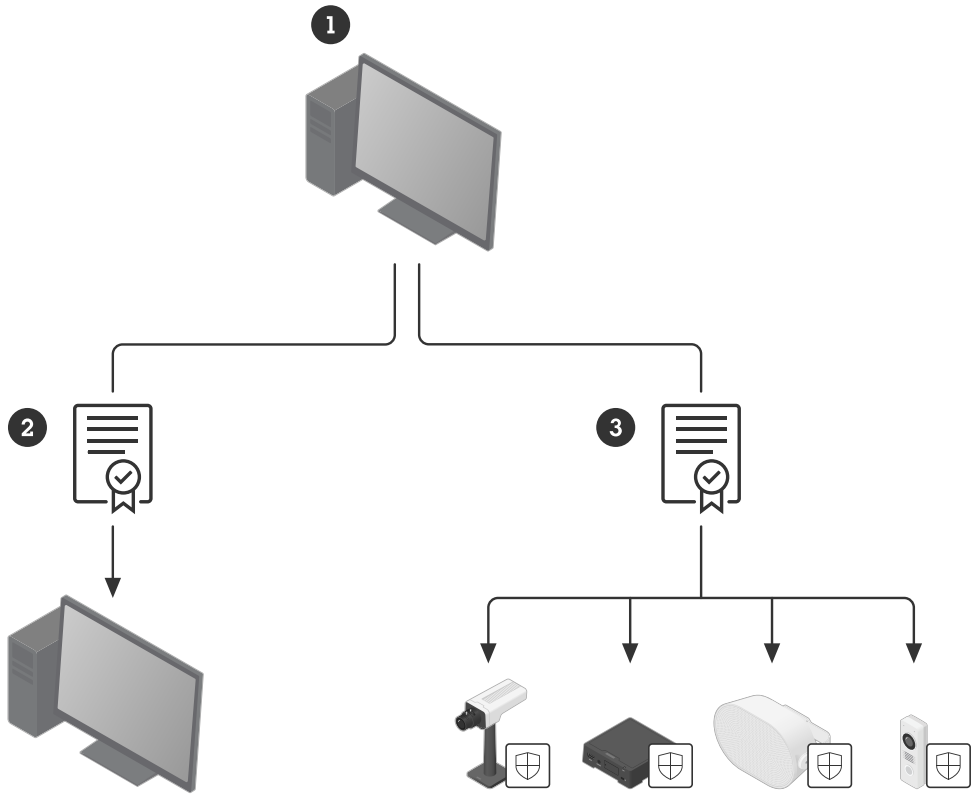
使用 AXIS Device Manager 作为私有 CA 是最经济高效的解决方案。在生成一个根 CA 证书之后，将 AXIS 设备管理器证书安装在 VMS 服务器的证书存储区中。如果有其他客户端直接访问摄像机（进行维护或故障排除），也应在这些客户端上安装 AXIS Device Manager 根 CA。

对于 802.1X，摄像机需要一个客户端证书，以向一个 RADIUS 服务器验证其身份。建议让企业 PKI/CA 管理员生成一个中间 CA 证书并将其作为一个可安装在 AXIS 设备管理器中的 PKCS#12 (P12) 证书导出。

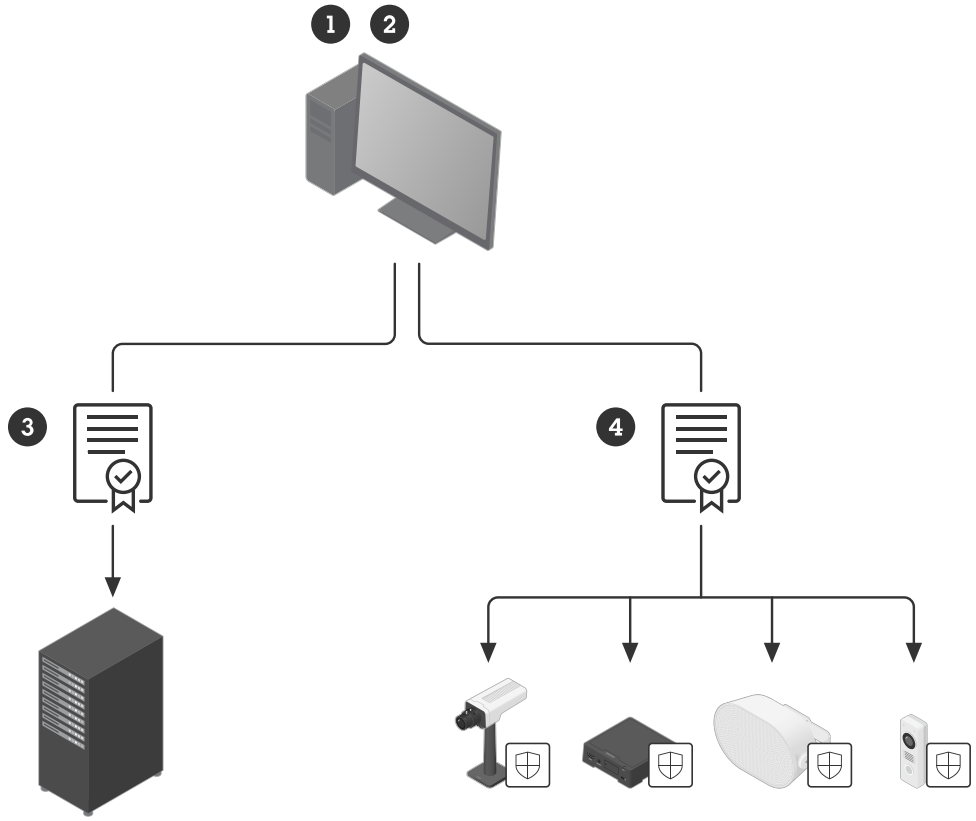
如需设置 FreeRADIUS 服务器的支持，请访问 AXIS Device Manager 的*技术论文部分*。



管理 HTTPS 证书涉及：1) 在 AXIS Device Manager 中生成中间 CA 或根 CA 证书； 2) 将 CA 证书导出到 VMS，以及 3) 将服务器证书上传到设备。



使用私有 CA。管理 IEEE 802.1X 证书包括：1) 生成中间 CA 和客户端证书；2) 在 Radius 服务器上安装 CA 证书；3) 在 AXIS Device Manager 中导入 CA 证书；4) 将 CA 和客户端证书上传到设备。



使用 AXIS Device Manager 作为 CA。要管理 IEEE 802.1X 证书，请执行以下操作：1) 在 AXIS Device Manager 中生成根 CA 证书；2) 在 AXIS Device Manager 中导入身份验证 CA 证书；3) 在 Radius 服务器上安装 CA 证书；4) 将 CA 身份验证和客户端证书上传到设备。

结束语

安全管理和安全控制是实施有效网络安全方法的重要部分。每个环节都是一个持续的过程，需要保持清晰的状态并采取适当的措施来缓解任何可能影响您 IP 网络的潜在威胁。AXIS Device Manager 为您提供一款工具，它既能管理您的设备，又能提升您的网络安全性。请联系您当地的安讯士代表或转到 *www.axis.com* 以了解更多信息或寻求支持。

T10231485_zh

2025-09 (M4.2)