AXIS Device Manager Extend

用户手册

目录

关于

AXIS Device Manager Extend 解决方案为系统管理员提供了一个用于在其组织网络上发现、配置和操作 Axis 设备的界面。

AXIS Device Manager Extend 桌面应用

桌面应用是一个软件实用程序，可用作按需或始终可用的用户界面，来管理系统。它可以与本地安装的边缘主机一起在专用计算机上运行，也可以与远程连接的笔记本电脑上的边缘主机分开运行。客户端向用户呈现系统的总体状态和随时可用的管理操作。

边缘主机

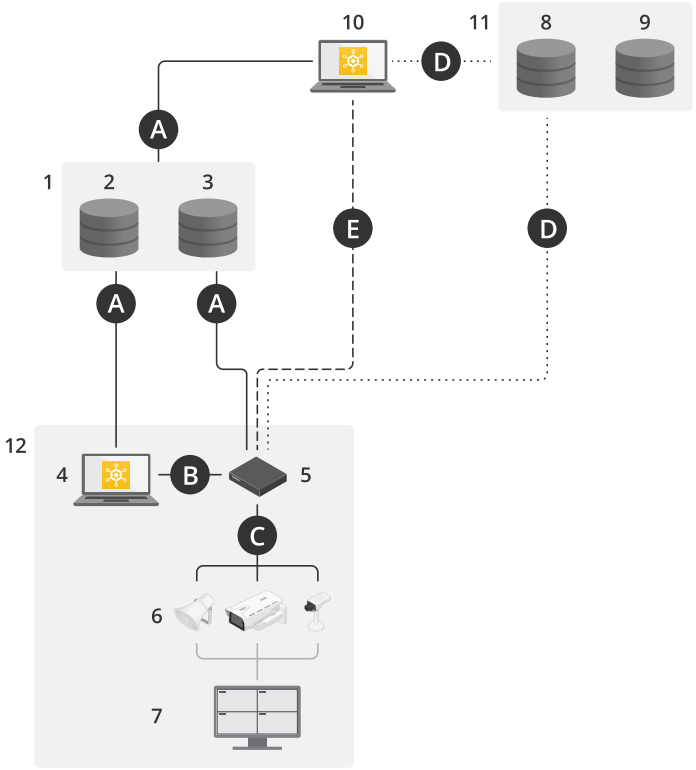
AXIS Device Manager Extend 中的边缘主机组件是一种始终可用的、预置管理服务，负责维护本地设备，如摄像机。AXIS Device Manager Extend 边缘主机还可作为指向 Axis 远程管理服务的链接，其中，相同的 API 功能支持 Axis 服务平台对站点远程管理。

关于企业

企业是您的安讯士系统安装的虚拟表示，位于您的云服务的中心。企业在规范访问并尽可能确保安全性的层次结构中托管公司的设备和用户帐户。同时，它允许为小型企业和大型企业提供灵活的用户和设备管理。

- 创建新企业时，您将成为其拥有者。企业将您的系统连接到安讯士云服务的用户。
- 您可以邀请用户加入企业。参见。
- 您可以为用户分配不同的角色。
- 企业包含一个默认文件夹，您可以在其中开始构建适合您需求的企业结构。您可将企业构建到文件夹和子文件夹中。通常，文件夹表示企业内系统的物理场所或位置。
- 管理企业内系统的许可证。
- 要创建企业，您需要一个My Axis账户。

解决方案概述

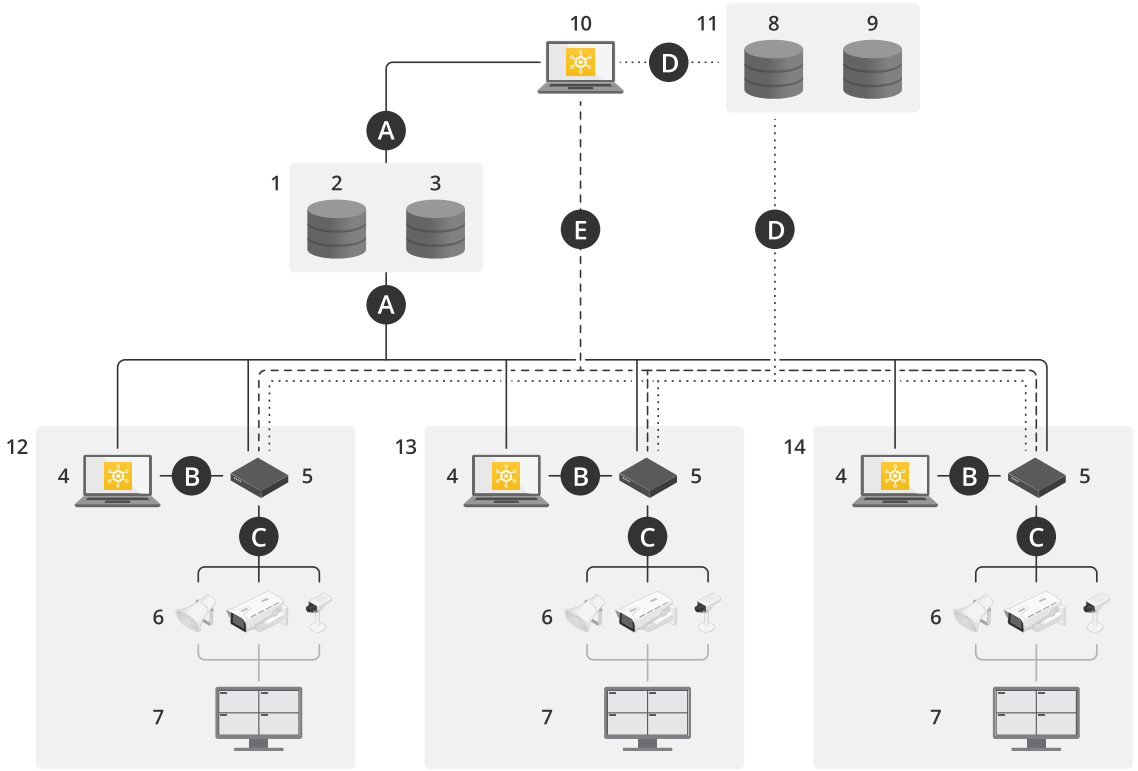


AXIS Device Manager Extend，本地和远程访问

1 Axis
2 IAM (My Axis)
3 企业数据
4 本地客户端
5 边缘主机
6 设备
7 VMS
8 TURN
9 信号传递
10 远程客户端
11 远程访问 WebRTC 服务器
12 场所1

连接	URL和IP	端口	协议	备注
A	prod.adm.connect.axis.com（52.224.128.152或40.127.155.231）	443	HTTPS	必需
B	HTTP 发现（从客户端到边缘主机） 数据传输（客户端和边缘主机之间） 组播发现（从客户端到边缘主机） 组播发现（从边缘主机到客户端）	37080 37443 6801 6801	HTTP HTTPS UDP UDP	需要，用于配置场所。配置之后可选。
C	数据传输（边缘主机与设备之间）	80/自定义端口，443	HTTP，HTTPS	必需

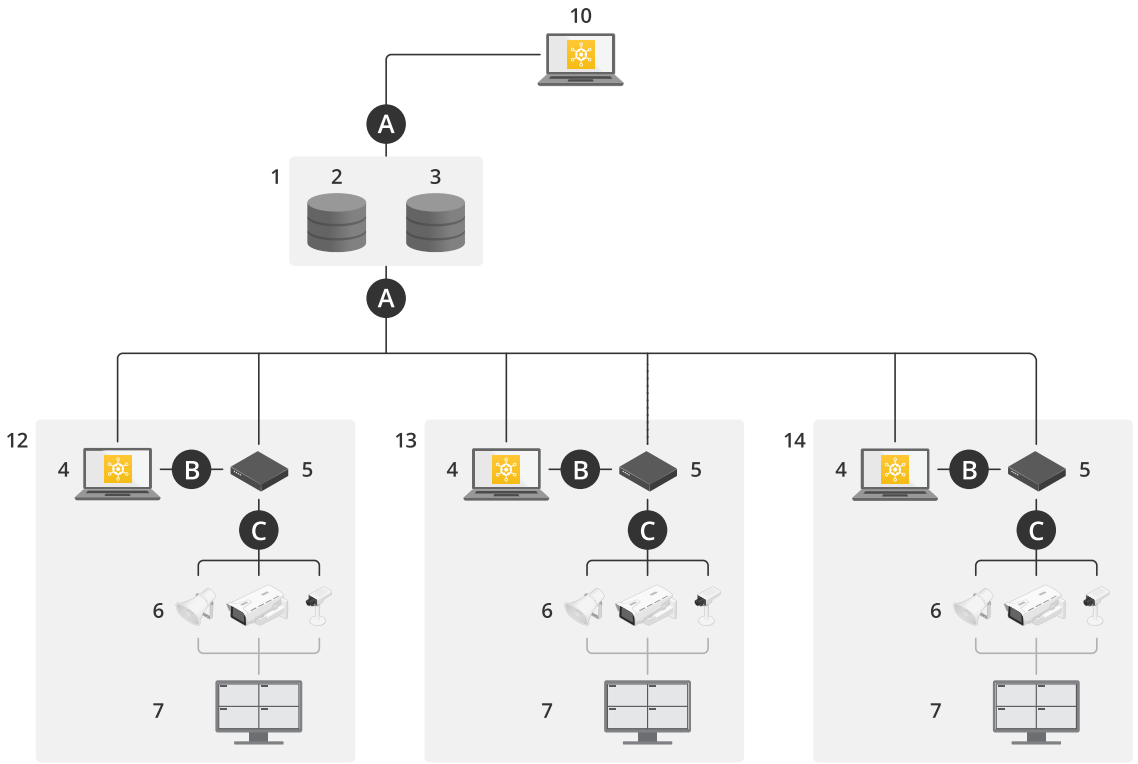
	单播发现 组播发现 HTTP发现	 1900 1900, 5353 80,443	SSDP，Bonjour	
D	signaling.prod.webrtc.connect.axis.com *.turn.prod.webrtc.connect.axis.com	443 443, 5349	HTTPS HTTPS、DTLS（UDP和TCP）	基于 WebRTC 标准 可选，默认设置为关闭
E	点对点 (P2P)	49152–65535	DTLS（UDP和TCP）	



AXIS Device Manager Extend，使用本地和远程访问的多场所设置

1 Axis
2 IAM (My Axis)
3 企业数据
4 本地客户端
5 边缘主机
6 设备
7 VMS
8 TURN
9 信号传递
10 远程客户端
11 远程访问 WebRTC 服务器
12 场所1
13 场所2
14 场所3

连接	URL和IP	端口	协议	备注
A	prod.adm.connect.axis.com（52.224.128.152或40.127.155.231）	443	HTTPS	必需
B	HTTP 发现（从客户端到边缘主机） 数据传输（客户端和边缘主机之间） 组播发现（从客户端到边缘主机） 组播发现（从边缘主机到客户端）	37080 37443 6801 6801	HTTP HTTPS UDP UDP	需要，用于配置场所。配置之后可选。
C	数据传输（边缘主机与设备之间） 单播发现 组播发现 HTTP发现	80/自定义端口，443 1900 1900, 5353 80,443	HTTP，HTTPS SSDP，Bonjour	必需
D	signaling.prod.webrtc.connect.axis.com *.turn.prod.webrtc.connect.axis.com	443 443, 5349	HTTPS HTTPS、DTLS（UDP和TCP）	基于 WebRTC 标准 可选，默认设置为关闭
E	点对点 (P2P)	49152–65535	DTLS（UDP和TCP）	



AXIS Device Manager Extend，使用 VPN 连接的本地和远程访问

1 Axis
2 IAM (My Axis)
3 企业数据
4 本地客户端
5 边缘主机
6 设备
7 VMS
8 TURN
9 信号传递
10 远程客户端
11 远程访问 WebRTC 服务器
12 场所1
13 场所2
14 场所3

连接	URL和IP	端口	协议	备注
A	prod.adm.connect.axis.com（52.224.128.152或40.127.155.231）	443	HTTPS	必需
B	HTTP 发现（从客户端到边缘主机） 数据传输（客户端和边缘主机之间） 组播发现（从客户端到边缘主机） 组播发现（从边缘主机到客户端）	37080 37443 6801 6801	HTTP HTTPS UDP UDP	需要，用于配置场所。配置之后可选。
C	数据传输（边缘主机与设备之间） 单播发现 组播发现 HTTP发现	80/自定义端口，443 1900 1900, 5353 80,443	HTTP，HTTPS SSDP，Bonjour	必需
D	signaling.prod.webrtc.connect.axis.com *.turn.prod.webrtc.connect.axis.com	443 443, 5349	HTTPS HTTPS、DTLS（UDP和TCP）	基于 WebRTC 标准 可选，默认设置为关闭
E	点对点 (P2P)	49152–65535	DTLS（UDP和TCP）	

- 另一个要求是公共DNS，如Google DNS：8.8.8.8 / 8.8.4.4或Cloudflare DNS：1.1.1.1
- 需要使用 A 和 C 连接来支持 AXIS Device Manager Extend 系统的全部功能。
- 我们正在不断开发应用，因此我们建议您允许防火墙访问AXIS Device Manager Extend桌面应用和边缘主机的传出网络连接。

前提条件

兼容的操作系统：

- Windows 10 Pro 和 Enterprise
- Windows 11 Pro 和 Enterprise
- Windows Server 2016、2019 和 2022（基于 x64 的系统）
- 安装和配置更改所需的系统管理员权限。

最低系统建议：

- CPU：Intel Core i5
- 内存：4 GB
- 网络：100 Mbps

互联网连接

注意

AXIS Device Manager Extend应用需要使用证书配置互联网连接，以将其识别为属于所创建的企业，并与安装中所用的My Axis账户相关联。但是，为了从某些功能（如保修信息和多站点支持）中受益，您需要互联网连接。此外，客户端和/或边缘主机仅在联机模式下自动更新。

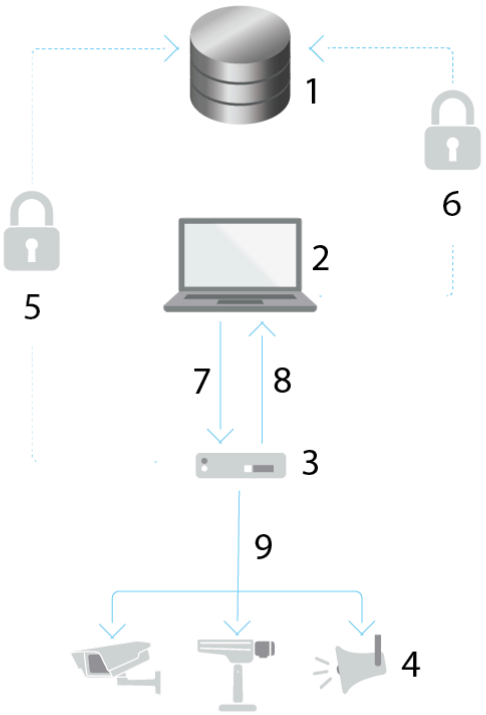
同步的时间和日期

注意

确保系统组件均已同步，否则，边缘主机与客户端或后端之间的证书身份验证可能会失败。建议将主机同步到公共网络时间服务器，以避免潜在问题。

打开网络端口：

用于从 AXIS Device Manager Extend 桌面应用到边缘主机的安全连接，边缘主机发现和 Axis 远程服务。



1 Axis 服务平台
2 AXIS Device Manager Extend 桌面应用

3 *边缘主机*
4 *设备*
5 *HTTPS（端口 443）*
6 *HTTPS（端口 443）*
7 *HTTPS（端口 37443）、UDP 组播发现（端口 6801）、HTTP 发现（端口 37080）*
8 *UDP 组播发现（端口 6801）*
9 *HTTPS 和 HTTP（端口 443 和 80）、多播发现 — SSDP（端口 1900）— Bonjour（端口 5353）、单播发现（端口 1900）、HTTP 发现（端口 80 和 443）*

出网访问

我们正在不断开发应用，因此我们建议您允许防火墙访问AXIS Device Manager Extend桌面应用和边缘主机的传出网络连接。

开始使用

注册 My Axis 账户

1. 在axis.com/my-axis/login上注册*My Axis*账户。
2. 选择其中一种多因素认证 (MFA) 方法：**身份验证器应用 (TOTP)** 或**电子邮件**，然后按照屏幕说明操作。MFA是一种安全系统，通过增加额外的验证层来确认用户身份。

安装客户端并激活您的帐户

进入 axis.com 的产品页面，并下载 AXIS Device Management 客户端

1. 找到您下载该应用的位置，然后单击以安装。
2. 选择**客户端**，然后单击**安装**。
3. 登录到您的 My Axis 账户。
4. 确认您的电子邮件地址以完成激活。
5. 创建或加入现有企业。

创建企业

为了在系统中添加设备，您需要成为某个企业的一部分。这是您在一个或多个场所以安全方式维护和保护设备的方法。如果您还不是某个企业的成员，将弹出一个设置助手，引导您完成该过程。

创建一个企业：

1. 用您的 My Axis 账户登录。
2. 按照设置助手的说明操作

创建其他企业：

- 转到带有贵企业名称的下拉菜单。
- 选择**+ Create new organization（创建新企业）**
- 按照设置助手的说明操作。

安装边缘主机

前往 axis.com 上的产品页面并下载边缘主机（AXIS Device Management Server）。

1. 选择要在其中安装边缘主机的服务器。我们建议您将边缘主机安装在尽可能靠近设备的服务器上。
2. 在服务器上运行安装程序。

声明边缘主机

要建立从 AXIS Device Management 客户端到设备的安全连接，您必须首先为您的组织申请一个边缘主机。

1. 单击状态为**无人声明**的边缘主机
   1.1. 如果列表中没有边缘主机，请单击**添加新边缘主机**
   1.2. 键入边缘主机所在的 IP 地址
2. 键入边缘主机的名称
3. 添加可选描述（推荐）
4. 单击**声明边缘主机**

管理设备

将已发现的设备添加到您的边缘主机

1. 转到**边缘主机**。
2. 在您要添加设备的列表中选择一个已声明的边缘主机。
3. 转到**设备 > 已发现**。
4. 选择要添加的设备，或通过选中选择列顶部的复选框来选择全部设备。
5. 单击**添加设备至边缘主机** 。

设备现已在**托管**选项卡中列出，其状态可在**边缘主机概览**中查看。

通过 IP 地址添加设备

添加不能从子网、单个 IP 地址或 IP 范围自动发现的设备。

从 IP 范围添加设备

1. 转到您的企业声明的边缘主机。
2. 转到**设置 > 设备发现**。
3. 单击**按 IP 添加**
4. 选择**手动输入**
5. 键入 IP 范围
6. 单击**添加 IP 地址**
7. 转到Devices（**设备**）> Discovered（**已发现**）
8. 选择要添加的设备，或通过选中选择列顶部的复选框来选择全部设备。
9. 单击**添加设备** 。

从文件添加设备

1. 转到您的企业声明的边缘主机。
2. 转到**设置 > 设备发现**。
3. 单击**按 IP 添加**
4. 选择**从文件导入**。
5. 选择逗号分隔 (.CSV) 文件的 IP 地址
6. 单击 **导入**
7. 转到**设备 > 已发现设备**。
8. 选择要添加的设备，或通过选中选择列顶部的复选框来选择全部设备。
9. 单击**添加设备** 。

注意

该文件应具有：

IP 地址列的标头。

单个列。

最多 25600 个 IP 地址。

删除设备

1. 单击**边缘主机**
2. 选择边缘主机。
3. 转到Devices（**设备**）
4. 选择要删除的设备，或通过选中选择列顶部的复选框来选择全部设备。
5. 单击操作菜单中的**从边缘主机删除设备**图标。
6. 单击 Remove（**删除**）。

可在**设备 > 已发现**中找到已删除设备。

登录到您的设备

1. 单击**边缘主机**
2. 选择边缘主机。
3. 转到**设备 > 托管**
4. 选择要访问的设备，或通过选中选择列顶部的复选框来选择全部设备。
5. 单击**登录**可自动登录到多个设备。
6. 键入用户名和密码。
7. 单击Log in（**登录**）

注意

如果用户名和密码正确，**状态**将显示为**可访问**

配置

激活远程访问

如果防火墙设置阻止出站连接，您可能必须输入代理连接以远程访问站点。

1. 选择要激活远程访问的边缘主机。
2. 转到**设置 > 边缘主机连接**。
3. 激活**允许远程访问边缘主机**。
4. 如果需要输入代理服务器地址才能访问互联网，请在**代理服务器地址**下键入地址。

一旦连接处于活动状态，您将收到通知。

注意

为支持与其他网络上的边缘主机连接，您可能需要在企业网络防火墙的“allow list（允许列表）”中添加以下配置：Endpoint Port Protocol（终端端口协议）signaling.prod.webrtc.connect.axis.com 443 HTTPS *.turn.prod.webrtc.connect.axis.com 443 HTTPS webRTC（Turn和P2P）5349, 49152 – 65535 DTLS（UDP和TCP）

删除场所

在从您的企业中删除边缘主机之前，您需要以删除属于该边缘主机的设备。然后可在**设备 > 已发现**中找到。

1. 单击Edge hosts（**边缘主机**）。
2. 使用箭头键选择边缘主机或使用鼠标指针将其悬停在其上方。
3. 单击 ...，然后在下拉菜单中选择**删除边缘主机**。
4. 检查**我是否意识到风险。**
5. 单击 Remove（**删除**）。

将用户添加到您的企业

1. 选择您要配置用户设置的企业。
2. 转到My Systems（我的系统）面板。
3. 转到ORGANIZATION（**企业**）> Users（**用户**）。
4. 点击**邀请用户**。
5. 按照设置助手的屏幕说明操作。
   - 如果您已经选择了Operator（**操作员**）或Viewer（**浏览者**），请选择用户可以访问哪些文件夹。请注意，Admin（**管理员**）角色可以访问企业中的全部文件夹。

注意

用户将收到邀请电子邮件，可用于登录My Systems（我的系统）。如果用户没有My Axis账户，则他们必须使用该电子邮件进行注册，以便访问企业。在等待接受期间，邀请可以撤销。

关于用户角色

用户角色确定用户对企业中的系统具有多少访问权限。可用功能因用户角色而异。

管理员

管理员可以访问整个系统。这包括管理用户、设备、许可证、视频和其他内容。

他们还可以使用 AXIS Camera Station Pro 载入设备。管理员可以在My Systems（我的系统）中管理AXIS Camera Station Pro Server Monitoring。

操作员

操作员可以监控实时视频源、控制设备并访问录制内容以进行回放。他们大致了解企业的用户及其各自的角色。操作员还可以在My Systems（我的系统）中管理AXIS Camera Station Pro Server Monitoring。

浏览者

浏览者可以观看实时视频源，但无法控制设备或访问录制内容。他们大致了解企业的用户及其各自的角色。

提升用户角色

1. 选择您要配置用户设置的企业。
2. 转到My Systems（我的系统）面板。
3. 在ORGANIZATION（**企业**）下，转到Users（**用户**）。
4. 单击要提升级别的用户，然后单击Roles and access（**角色和权限**）。
5. 按照设置助手的屏幕说明操作。

注意

一旦选定角色，角色将立即更改。出于安全原因，邀请仅限于浏览者角色。

删除用户

1. 选择您要配置用户设置的企业。
2. 转到My Systems（我的系统）面板。
3. 在ORGANIZATION（**企业**）下，转到Users（**用户**）。
4. 将鼠标指针悬停在要删除的用户上显示新的选项菜单：...
5. 单击“...”，然后在下拉菜单中选择**删除用户**。

删除多个用户

1. 选择您想要删除的用户。
2. 单击操作菜单中的垃圾桶。
3. 单击 Remove（**删除**）。

AXIS OS 管理

使用 AXIS Device Management 客户端，您可以管理每个组织中多个设备的操作系统。

有关按型号分组的企业中每台设备都可用的AXIS OS更新列表，请转到**Home（主页）>AXIS OS inventory（AXIS OS库存）**。有关特定边缘主机上可用的AXIS OS更新列表，请选择该边缘主机，然后转到**AXIS OS inventory（AXIS OS库存）**。

根据型号管理AXIS OS版本

在企业范围内按型号管理AXIS OS：

1. 转到**主页 > AXIS OS 版本**
2. 单击推荐的AXIS OS版本链接。这将打开AXIS OS升级选项。
3. 单击**升级至**下拉菜单以查看可用内容。将预选最新的AXIS OS版本。
4. 单击**升级**。

管理边缘主机上的AXIS OS。

管理添加到边缘主机的部分或全部设备上的AXIS OS：

1. 转到**边缘主机**
2. 单击要访问的边缘主机。
3. 转到**设备**
4. 选择全部或只选择要管理的设备。
5. 单击操作菜单中的**AXIS OS**图标。
6. 检查列表中的全部或部分型号。
7. 如果您想要更改AXIS OS版本，请单击建议的版本以查看每个设备的可用内容。将预选最新的AXIS OS版本。
8. 单击**升级**。

查看正在进行和已经完成的AXIS OS升级

查看连接到特定边缘主机的设备的正在进行的软件升级：

1. 单击**边缘主机**
2. 单击要访问的边缘主机。
3. 转到**Log（日志）**

查看正在进行的软件升级：

4. 转到**Log（日志）> Ongoing tasks（正在进行的任务）**

政策

策略会自动管理您的设备。创建策略以维护您场所内的网络安全。您还可以设置一个策略，在您的设备上自动安装和更新应用。

创建和应用安全策略

在此使用示例中，我们创建基本安全策略，并将其应用于连接到边缘主机的选择数量的设备。

创建基本安全策略：

1. 转到**边缘主机**
2. 单击要访问的边缘主机。
3. 转到**设备**
4. 单击**策略**旁边的 + 图标
5. 选择**基本安全性**，然后单击**继续**
6. 为您的策略命名
7. 选择适合您的安全需求的设置。要获得推荐的安全级别，请保留默认设置。
   - 要更改选定设备的根密码，请单击**设备根密码**，然后键入新的根密码。
8. 单击 Create（**创建**）。

应用策略：

1. 选择要应用策略的设备。
2. 单击操作菜单中的**策略选项**图标。
3. 选择安全策略，然后单击**保存**。

创建和应用应用策略

在此使用示例中，我们创建应用策略，并将其应用于连接到边缘主机的选择数量的设备。

1. 转到**边缘主机**
2. 单击要访问的边缘主机。
3. 转到**设备**
4. 单击**策略**旁边的 + 图标
5. 选择**应用**，然后单击**继续**
6. 为您的策略命名
7. 选择你想要安装并在你的设备上更新的应用。
8. 在下拉菜单中选择更新窗口。
9. 单击 Create（**创建**）。

应用策略：

1. 选择要应用策略的设备。
2. 单击操作菜单中的**策略选项**图标。
3. 选择要应用的应用策略。
4. 单击 Save（**保存**）。

注意

如果删除，所选应用将自动重新安装。

编辑策略

要编辑一个现有策略：

1. 转到**边缘主机**
2. 单击要访问的边缘主机。
3. 转到**设备**
4. 单击要编辑的策略旁边的...，然后从下拉菜单中选择**编辑策略**。
5. 编辑策略设置以满足您的需求。
6. 单击**保存**

删除策略

要删除现有策略：

- 转到**边缘主机**
- 单击要访问的边缘主机。
- 转到**设备**
- 单击要编辑的策略旁边的...，然后从下拉菜单中选择**删除策略**。
- 单击**删除**

注意

应用了该策略的不同设备都将保留策略设置，但是设置将不再持续。

管理许可证

许可您的产品

若要许可您的产品，请转到*My Systems（我的系统）> Licenses（许可证）*。若要了解有关安讯士产品和服务许可证的更多信息，请参见*My Systems user manual（我的系统用户手册）*。

故障排查

如何配置防火墙设置

AXIS Device Management 客户端需要访问 axis.com 域及其子域。

为了使边缘主机能够与安讯士服务通信，请将以下 IP 地址和端口添加到组织防火墙的允许列表中：

- 40.127.155.231 (EU)，端口 443
- 52.224.128.152 和 40.127.155.231 (US)，端口 443
- 公共域名解析服务器 IP，端口 53

或者，可以在防火墙设置中使用域 prod.adm.connect.axis.com（指向上述 IP 地址的 DNS A 记录）。

边缘主机使用 prod.adm.connect.axis.com 域名处理所有出站请求。

为此，网络需要使用公共域名解析服务器，并允许流量传至 DNS 服务器 IP 地址（和默认端口 53）。

注意

有关端口配置的更多信息，请参阅 AXIS Device Manager Extend 白皮书：*典型的系统架构*。

T10153497_zh

2025-10 (M22.2)