AXIS Device Manager

Manual do Usuário

Introdução

A importância da segurança cibernética continua a aumentar nos setores de vigilância e segurança. Uma segurança cibernética eficaz requer a garantia de uma defesa suficientemente aprofundada para proteger adequadamente a sua rede IP em todos os níveis, desde os produtos e parceiros que você escolhe até os requisitos que você e eles definem.

Este guia descreve como usar o AXIS Device Manager para aumentar o nível de proteção do sistema e a segurança. Ele foca nos principais aspectos e descreve recomendações.

Gerenciamento do ciclo de vida do dispositivo

Na Axis, nós entendemos a importância de ter uma base sólida de segurança durante todo o ciclo de vida do dispositivo. Nosso compromisso com a segurança cibernética garante que nossos produtos e soluções ofereçam uma proteção robusta contra possíveis ameaças.

Implementação

A Axis fornece dispositivos seguros por design, que contam com recursos de segurança integrados, como mecanismos de inicialização segura, sistema operacional assinado e armazenamento criptografado. Além disso, o AXIS Device Manager ajuda os instaladores e administradores de sistemas a configurar e implantar dispositivos com segurança, garantindo uma configuração segura desde o início.

Serviço ativo

Durante a fase operacional, a Axis oferece atualizações regulares do software do dispositivo e patches de segurança para proteger contra vulnerabilidades. O AXIS Device Manager também permite o monitoramento e a manutenção remotos, viabilizando a resolução rápida de problemas e reduzindo períodos de inatividade. Além disso, nossos guias para aumento do nível de proteção fornecem recomendações para a configuração dos dispositivos, a fim de atender a requisitos de segurança específicos.

Desativação

Quando chega a hora de desativar ou substituir dispositivos, o AXIS Device Manager facilita a desativação segura, limpando dados confidenciais e redefinindo os dispositivos para as configurações de fábrica. Isso garante que nenhuma informação confidencial permaneça no dispositivo, protegendo os dados dos usuários e impedindo o acesso não autorizado.

AXIS Device Manager

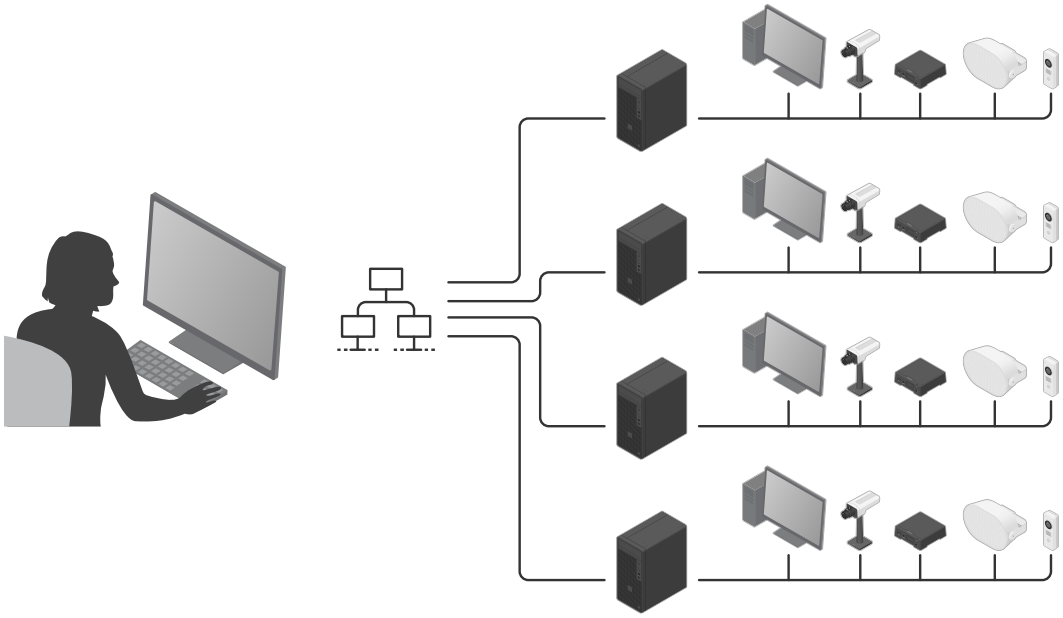
O AXIS Device Manager é uma ferramenta local que oferece uma forma fácil, econômica e segura do ponto de vista cibernético para gerenciar suas principais tarefas de instalação, segurança e manutenção (consulte a tabela abaixo). A ferramenta é indicada para o gerenciamento de milhares de dispositivos Axis em um único local ou de vários milhares de dispositivos espalhados por vários locais. O AXIS Device Manager permite a implantação eficiente de controles de segurança cibernética para proteger seus dispositivos em rede e alinhá-los a uma infraestrutura de segurança.

Funções de gerenciamento de dispositivos, AXIS Device Manager

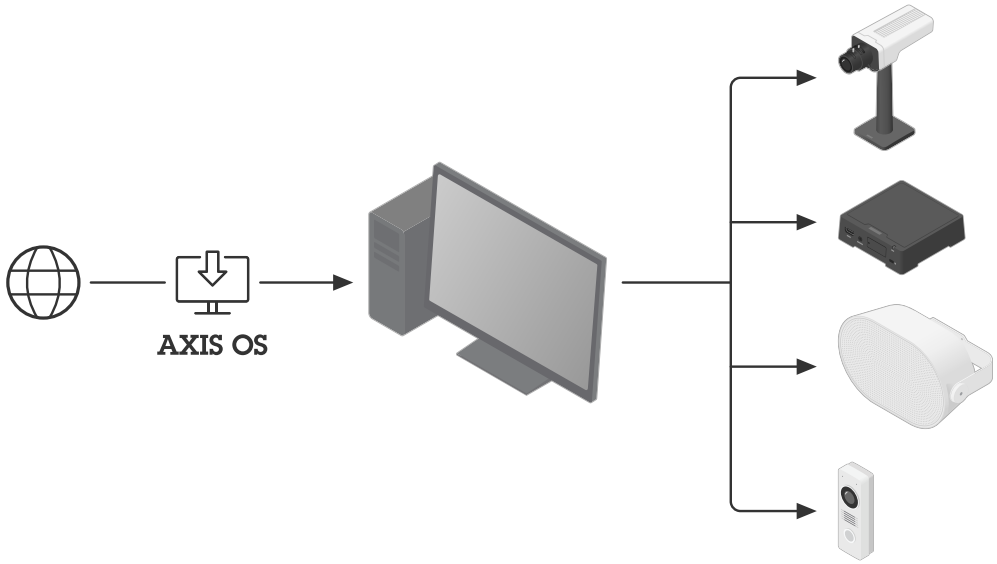
Instalação	Manutenção
Atribuir um endereço IP	Status de dispositivos
Exportação de lista de dispositivos e acompanhamento de ativos*	Coletar dados de dispositivos
Gerencimento de usuário e senha*	Configurar dispositivos e copiar configurações para vários dispositivos
Gerenciamento ACAP	Conectar-se a vários servidores/sistemas
Atualizar o AXIS OS, com base em LTS ou Ativo*	Restaurar pontos

Gerenciamento de certificados HTTPS*	Restaurar configurações padrão de fábrica
Gerenciar certificados IEEE 802.1*/**	Substituir dispositivos
Marcação de dispositivos	Renovação e gerenciamento de certificados*
	Fortalecimento da segurança cibernética*

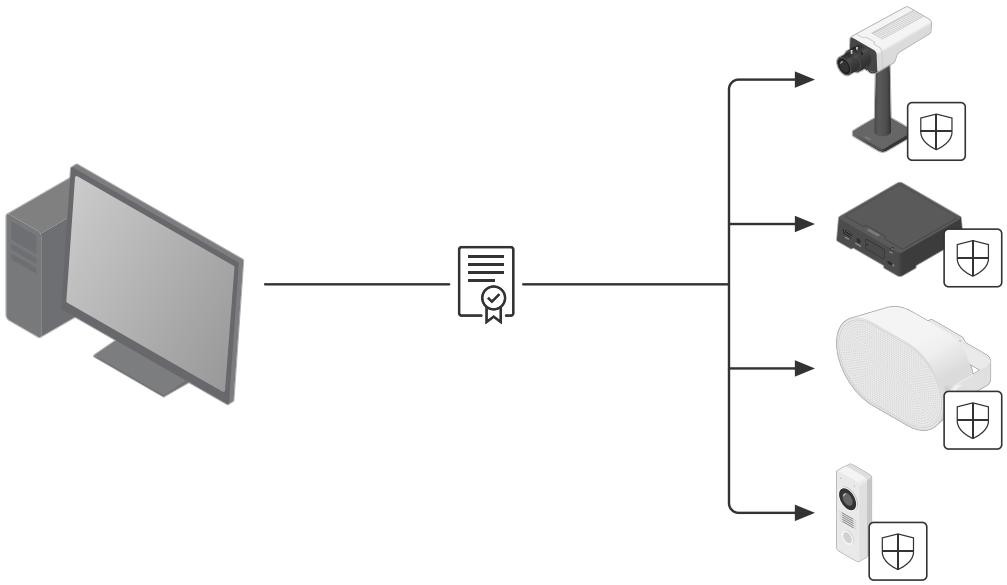
* Indica função de controle de segurança cibernética.
** Os serviços de certificado do Active Directory não são compatíveis no momento. Validado para FreeRADIUS em execução no Linux.



Gerenciamento de vários locais.



Atualização do AXIS OS.



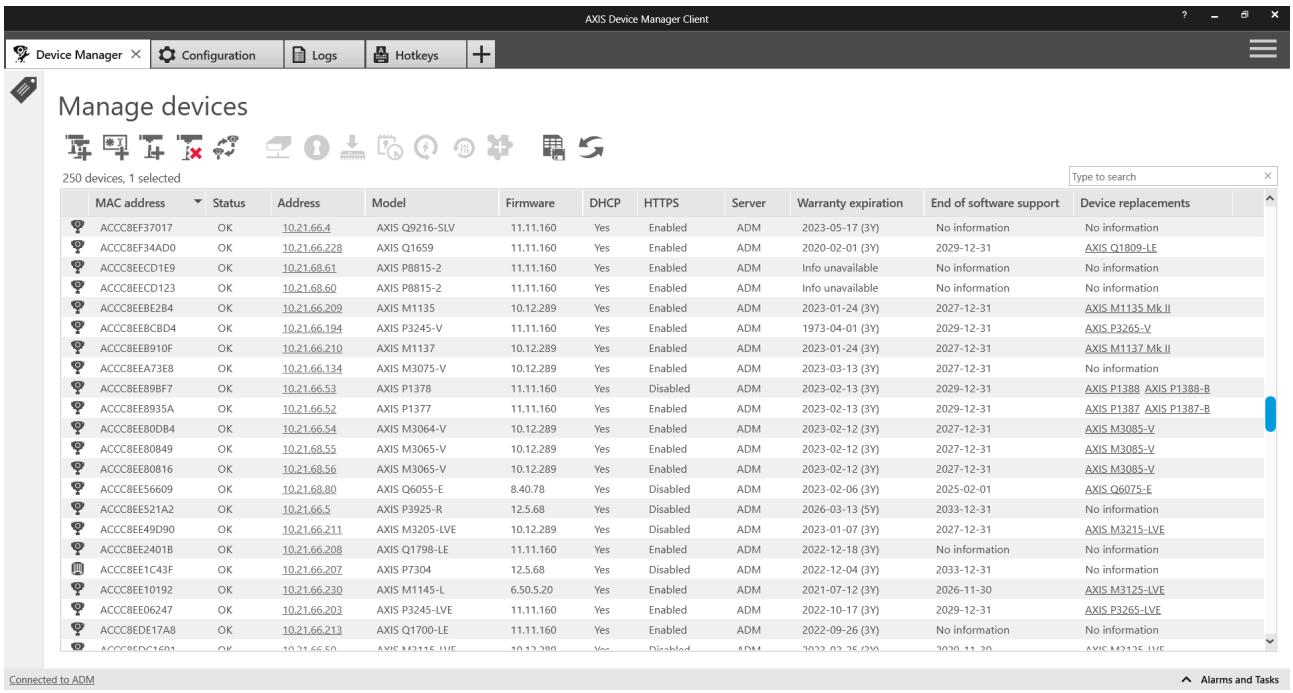
Gerenciamento de certificados.

Inventário de dispositivos

Um aspecto fundamental para a garantia da segurança de uma rede corporativa é manter um inventário completo dos dispositivos que fazem parte da rede. Ao criar ou revisar uma política de segurança geral, é importante conhecer e manter uma documentação clara de cada dispositivo, não apenas de ativos críticos. Isso é necessário porque um único dispositivo negligenciado pode representar uma porta de acesso para criminosos. E você não conseguirá proteger dispositivos que não reconhece ou que nem sabe que existem.

Um inventário de dispositivos representa uma etapa essencial para a segurança em uma rede corporativa. O AXIS Device Manager pode ajudá-lo nesse sentido, pois ele:

- Permite que você acesse facilmente um inventário completo e atualizado dos seus dispositivos na rede ao trabalhar com auditorias e com equipes de resposta a incidentes.
- Fornece uma lista completa de seus dispositivos, que podem ser classificados por número total, tipo, números de modelos etc.
- Fornece o status de todos os dispositivos em sua rede.
- Ajuda a planejar com antecedência, mostrando quando o suporte ao software do dispositivo está programado para terminar, bem como listando quais produtos mais novos podem ser usados como substitutos.



MAC address	Status	Address	Model	Firmware	DHCP	HTTPS	Server	Warranty expiration	End of software support	Device replacements
ACCC8EF37017	OK	10.21.66.4	AXIS Q9216-SLV	11.11.160	Yes	Enabled	ADM	2023-05-17 (3Y)	No information	No information
ACCC8EF34AD0	OK	10.21.66.228	AXIS Q1659	11.11.160	Yes	Enabled	ADM	2020-02-01 (3Y)	2029-12-31	AXIS Q1809-LE
ACCC8EECD1E9	OK	10.21.68.61	AXIS P8815-2	11.11.160	Yes	Enabled	ADM	Info unavailable	No information	No information
ACCC8EECD123	OK	10.21.68.60	AXIS P8815-2	11.11.160	Yes	Enabled	ADM	Info unavailable	No information	No information
ACCC8EEBE2B4	OK	10.21.66.209	AXIS M1135	10.12.289	Yes	Enabled	ADM	2023-01-24 (3Y)	2027-12-31	AXIS M1135 Mk II
ACCC8EEBCBD4	OK	10.21.66.194	AXIS P3245-V	11.11.160	Yes	Enabled	ADM	1973-04-01 (3Y)	2029-12-31	AXIS P3265-V
ACCC8EEB910F	OK	10.21.66.210	AXIS M1137	10.12.289	Yes	Enabled	ADM	2023-01-24 (3Y)	2027-12-31	AXIS M1137 Mk II
ACCC8EEA73E8	OK	10.21.66.134	AXIS M3075-V	10.12.289	Yes	Enabled	ADM	2023-03-13 (3Y)	2027-12-31	No information
ACCC8EE89BF7	OK	10.21.66.53	AXIS P1378	11.11.160	Yes	Disabled	ADM	2023-02-13 (3Y)	2029-12-31	AXIS P1388 AXIS P1388-B
ACCC8EE8935A	OK	10.21.66.52	AXIS P1377	11.11.160	Yes	Enabled	ADM	2023-02-13 (3Y)	2029-12-31	AXIS P1387 AXIS P1387-B
ACCC8EE80DB4	OK	10.21.66.54	AXIS M3064-V	10.12.289	Yes	Enabled	ADM	2023-02-12 (3Y)	2027-12-31	AXIS M3085-V
ACCC8EE80849	OK	10.21.68.55	AXIS M3065-V	10.12.289	Yes	Enabled	ADM	2023-02-12 (3Y)	2027-12-31	AXIS M3085-V
ACCC8EE80816	OK	10.21.68.56	AXIS M3065-V	10.12.289	Yes	Enabled	ADM	2023-02-12 (3Y)	2027-12-31	AXIS M3085-V
ACCC8EE56609	OK	10.21.68.80	AXIS Q6055-E	8.40.78	Yes	Disabled	ADM	2023-02-06 (3Y)	2025-02-01	AXIS Q6075-E
ACCC8EE521A2	OK	10.21.66.5	AXIS P3925-R	12.5.68	Yes	Disabled	ADM	2026-03-13 (5Y)	2033-12-31	No information
ACCC8EE49D90	OK	10.21.66.211	AXIS M3205-LVE	10.12.289	Yes	Disabled	ADM	2023-01-07 (3Y)	2027-12-31	AXIS M3215-LVE
ACCC8EE2401B	OK	10.21.66.208	AXIS Q1798-LE	11.11.160	Yes	Enabled	ADM	2022-12-18 (3Y)	No information	No information
ACCC8EE1C43F	OK	10.21.66.207	AXIS P7304	12.5.68	Yes	Disabled	ADM	2022-12-04 (3Y)	2033-12-31	No information
ACCC8EE10192	OK	10.21.66.230	AXIS M1145-L	6.50.5.20	Yes	Enabled	ADM	2021-07-12 (3Y)	2026-11-30	AXIS M3125-LVE
ACCC8EE06247	OK	10.21.66.203	AXIS P3245-LVE	11.11.160	Yes	Enabled	ADM	2022-10-17 (3Y)	2029-12-31	AXIS P3265-LVE
ACCC8EDE17A8	OK	10.21.66.213	AXIS Q1700-LE	11.11.160	Yes	Enabled	ADM	2022-09-26 (3Y)	No information	No information

O AXIS Device Manager oferece uma visão clara do seu inventário de dispositivos.

O AXIS Device Manager oferece um meio automatizado de acessar o inventário de dispositivos em rede Axis em tempo real. Ele permite a você identificar, listar e classificar automaticamente seus dispositivos. Igualmente importante, ele permite o uso de etiquetas para agrupar e classificar dispositivos com base em seus próprios critérios, facilitando na hora de documentar e obter uma visão geral de todos os dispositivos Axis em sua rede.

Política de contas e senhas

A autenticação e o controle de privilégios são parte importante da proteção dos recursos de rede. A implementação de políticas ajuda a reduzir os riscos de mau uso acidental ou proposital ao longo do tempo. A imposição do uso de senhas robustas é uma tarefa fundamental, mas também é importante reduzir o risco de comprometimento das senhas. As senhas dos dispositivos muitas vezes são compartilhadas dentro de uma organização e, quando isso acontece, perde-se o controle de quem tem acesso a elas. O AXIS Device Manager ajuda a gerenciar facilmente contas e senhas de vários dispositivos Axis.

Por que você deve ter mais de uma conta de usuário nos dispositivos:

- Você pode controlar níveis de privilégios para diferentes tipos de usuários (máquinas e humanos).
- Os riscos de comprometimento da senha de root (mestre) são menores.
- Você pode redefinir as credenciais de um tipo de usuário sem afetar os outros.

Trabalhando com privilégios no AXIS Device Manager

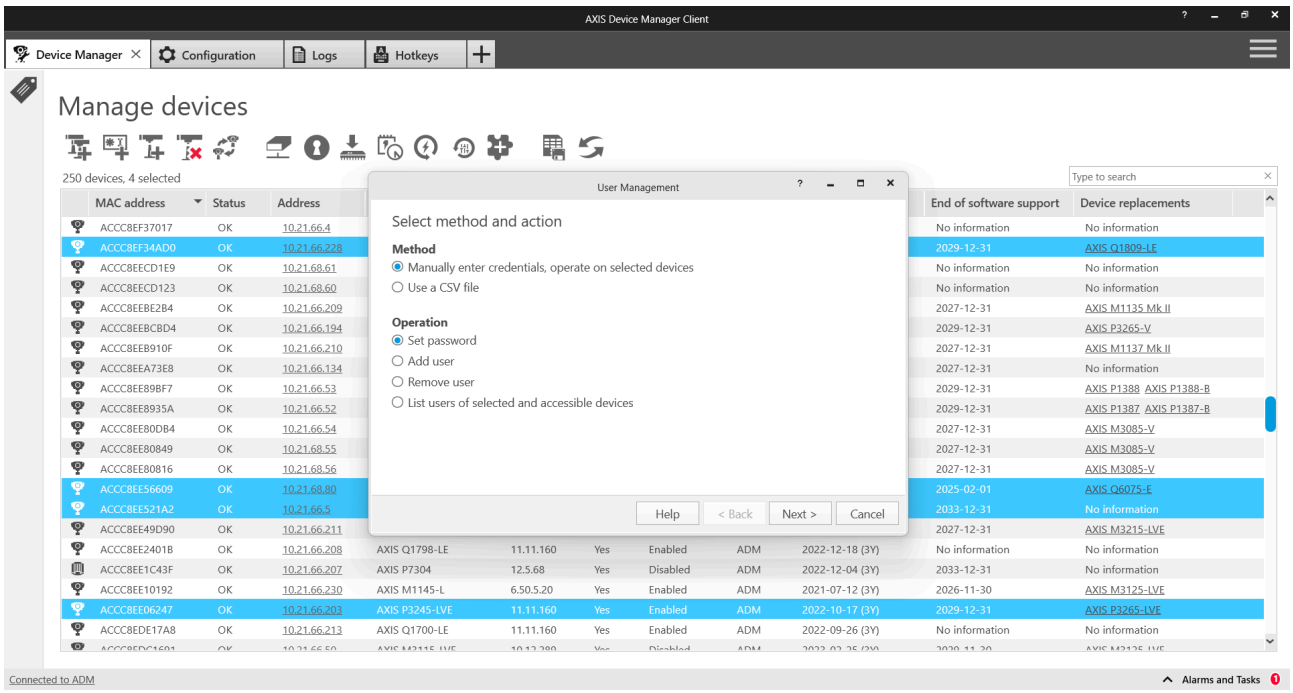
Os dispositivos Axis suportam várias contas, sendo que cada conta tem um de três níveis de privilégio diferentes:

- **Viewers (Visualizadores)**: Esses usuários têm acesso a vídeo e controle PTZ.
- **Operators (Operadores)**: Usuários com direitos de operador podem otimizar as configurações da câmera e os perfis de stream de vídeo.
- **Administrators (Administradores)**: Administradores podem administrar contas, modificar configurações de rede e controlar vários serviços nos dispositivos.

Cada função com acesso à câmera deve ter sua própria conta. Por exemplo, a função "Control room personnel" (Equipe da sala de controle) pode ser configurada com o nível de privilégio "operator" (operador), enquanto a função "Patrolling staff" (Equipe de patrulhamento) pode precisar apenas do nível de privilégio "viewer" (visualizador).

Etapas recomendadas

- Antes de adicionar câmeras ao VMS, adicione-as ao AXIS Device Manager.
- No AXIS Device Manager, selecione todas as câmeras e crie uma nova conta de usuário chamada "vms" ou semelhante e defina uma senha forte. Os privilégios devem estar alinhados aos requisitos do VMS, podendo ser tanto de operador quanto de administrador (consulte o fabricante).
- Adicione os dispositivos ao VMS usando a conta e a senha que você criou.
- Volte para o AXIS Device Manager, selecione todas as câmeras novamente e redefina (altere) a senha da conta "root" usando uma nova senha forte. A senha da conta "root" deve ser conhecida apenas por um número limitado de pessoas (aqueles que usam o AXIS Device Manager).
- Quando alguém precisa usar um navegador da Web para acessar um dispositivo para realizar tarefas de manutenção ou solução de problemas, **não** forneça a senha de root. Em vez disso, use o AXIS Device Manager para criar uma nova conta (temporária) para os dispositivos selecionados, com privilégios de administrador ou operador. Após o trabalho ser concluído, use o AXIS Device Manager para excluir a conta temporária.
- O AXIS Device Manager oferece suporte a administradores locais, bem como a usuários e grupos do domínio. Você poderá usar um administrador local se o cliente do AXIS Device Manager for acessado somente pela mesma máquina que hospeda o servidor do AXIS Device Manager. Recomendamos o uso de usuários de domínio se a pessoa que estiver mantendo o sistema usar clientes remotos.



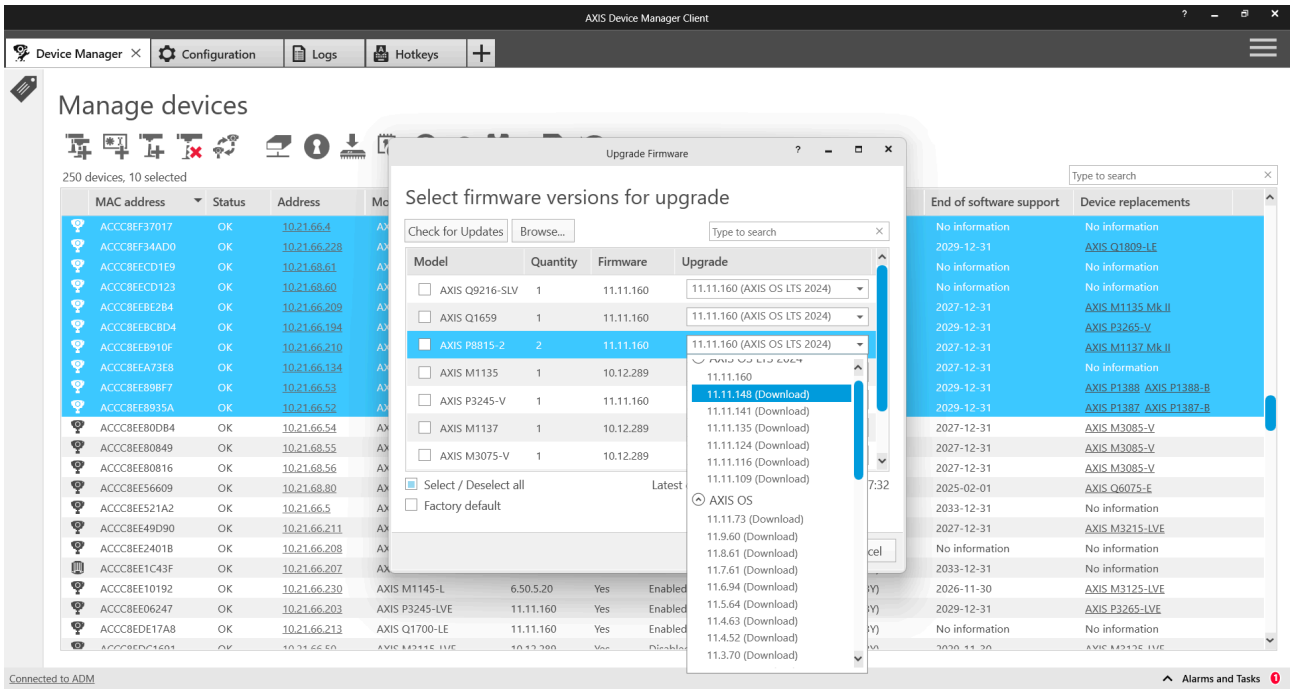
Alterando funções de usuários e senhas no AXIS Device Manager.

Atualizações do AXIS OS

As versões atualizadas do AXIS OS incluem patches para vulnerabilidades conhecidas. É indispensável usar sempre o software mais recente, pois os criminosos podem tentar explorar vulnerabilidades conhecidas. Igualmente importante, a rápida implantação de uma nova versão do AXIS OS fortalece os recursos operacionais e remove os gargalos relacionados à implementação manual de atualizações de novas versões. O AXIS Device Manager se conecta ao site www.axis.com e baixa as versões mais recentes do AXIS OS ou de serviços aplicáveis. Se preferir não baixar diretamente da Internet para sua rede, você poderá salvar as atualizações em uma unidade USB e então carregá-las em seu cliente do AXIS Device Manager. Ele também mostra se há novas versões do AXIS OS disponíveis e permite implantá-las rapidamente em seus dispositivos Axis.

Por que você sempre deve executar as versões mais recentes do AXIS OS:

- Sua rede e seus dispositivos são protegidos com os patches mais recentes contra vulnerabilidades conhecidas, especialmente as mais críticas.
- Seus dispositivos são atualizados para incorporar as melhorias de desempenho mais recentes, bem como correções de bugs ou falhas conhecidas.
- Você obtém acesso imediato aos recursos e aprimoramentos de funcionalidades mais recentes.



A tarefa de atualizar o AXIS OS usando o AXIS Device Manager é simplificada graças a notificações na tela e caixas de diálogo intuitivas.

Fortalecimento adicional

O emprego de uma boa política de usuários e senhas e a execução de versões atualizadas do AXIS OS reduzirão os riscos comuns para os dispositivos. O *AXIS Hardening Guide* descreve medidas adicionais para reduzir os riscos em organizações críticas e de grande porte. Isso inclui a desativação de serviços que não estejam em uso e a ativação de serviços que possam ajudar a detectar e monitorar indicações de ataques ou violações. O AXIS Device Manager simplifica o processo de implantação de algumas dessas políticas. A Axis fornece um modelo de configuração das opções básicas recomendadas.

Como aumentar o nível de proteção dos dispositivos de acordo com o Axis Hardening Guide:

- Leia o *AXIS Hardening Guide* e baixe o arquivo de modelo ao final do documento.
- Edite o arquivo de configuração para selecionar os itens relevantes.
- Selecione os dispositivos no inventário do AXIS Device Manager.
- Clique com o botão direito do mouse e selecione "Configure Devices > Configure..." (Configurar dispositivos > Configurar...).
- Clique em "Arquivo de configuração" e selecione o arquivo baixado.
- Ajuste as configurações conforme necessário.

Serviço de autoridade de certificação

Uma autoridade de certificação (CA) é um serviço que emite certificados digitais para servidores, clientes ou usuários. Uma CA pode ser pública ou privada. CAs reconhecidamente confiáveis, como Comodo e Symantec (antiga Verisign), são normalmente usadas para serviços públicos como sites e email.

Uma CA privada (em geral, um serviço de Active Directory/certificados) emite certificados para serviços de rede internos/privados. Em um sistema de gerenciamento de vídeo, isso se aplica principalmente à criptografia de rede HTTPS e ao controle de acesso à rede IEEE 802.1x. O AXIS Device Manager inclui um serviço de CA para dispositivos Axis e pode operar como uma CA raiz privada ou como uma CA intermediária privada, como parte de uma Infraestrutura de chaves públicas (PKI) empresarial.

Os certificados assinados pela CA são usados tanto para certificados IEEE 802.1x (cliente) quanto HTTPS (servidor).

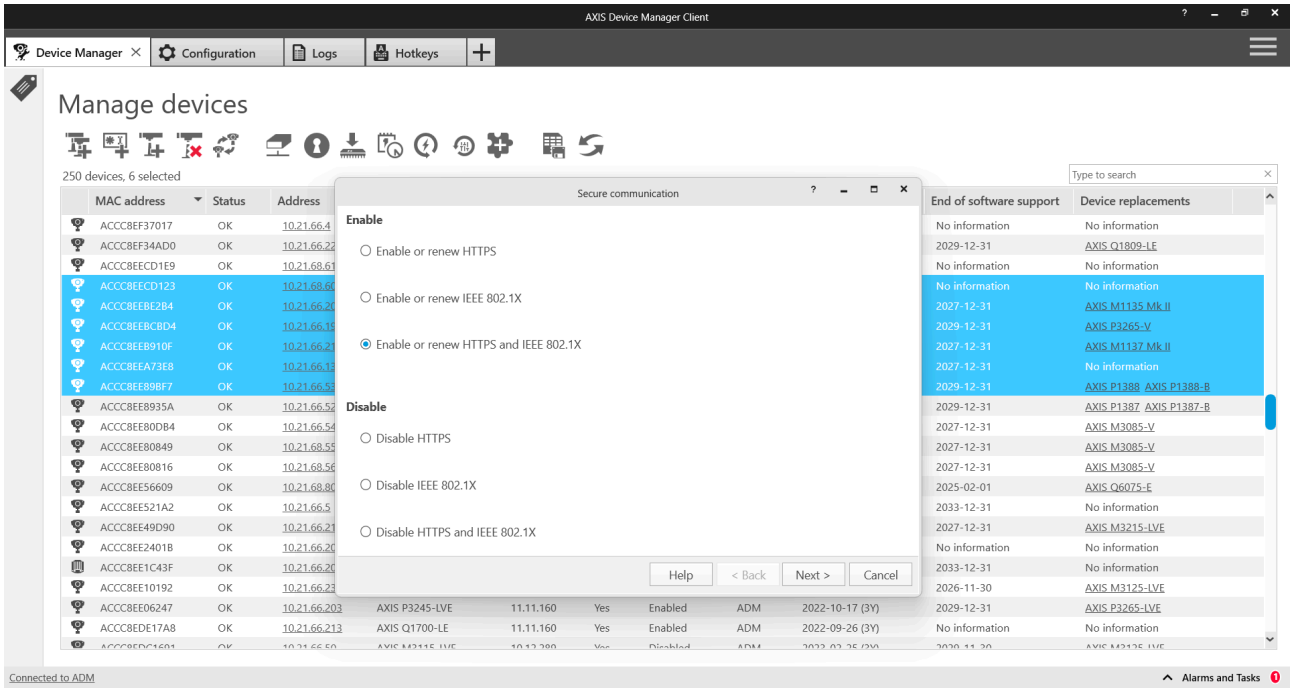
HTTPS

HTTPS é a versão segura do HTTP na qual as comunicações entre um cliente e um servidor são criptografadas. Certificados autoassinados são suficientes para estabelecer uma conexão criptografada. Não há diferenças no nível de criptografia entre certificados autoassinados e certificados assinados por CA. A diferença é que os certificados autoassinados não protegem contra ataques de falsificação (spoofing) à rede, na qual um computador invasor tenta se passar por um servidor legítimo. Os certificados assinados por CA adicionam um ponto de confiança para que os clientes façam a autenticação que garante que eles estejam acessando um dispositivo confiável. Observe que o cliente de vídeo (VMS) deve oferecer suporte à solicitação de vídeo via HTTPS (RTP via RTSP via HTTPS) para criptografar vídeo.

IEEE 802.1X

Geralmente conhecido como 802.1X, esse padrão impede que dispositivos de rede não autorizados acessem a rede local. Um dispositivo deve poder se autenticar antes que seja permitido acessar a rede (e seus recursos). Vários métodos de autenticação podem ser usados: endereço MAC (filtragem de MAC), usuário/senha ou certificado de cliente. O proprietário do sistema decide qual método será usado. A escolha apropriada depende de ameaças, riscos e custos.

Operar uma infraestrutura 802.1X é um investimento. Fazer isso requer switches gerenciados e servidores adicionais, tipicamente um RADIUS (Remote Authentication Dial-In User Service). O uso de certificados de clientes requer uma CA (privada ou pública) que possa emitir certificados de clientes. Na maioria dos casos, a infraestrutura necessita de uma equipe para mantê-la e monitorá-la.



Configuração do certificado no AXIS Device Manager.

Gerenciamento do ciclo de vida de certificados

O gerenciamento do ciclo de vida dos certificados é um meio de lidar de forma econômica com todos os processos e tarefas relacionados à emissão, instalação, inspeção, correção e renovação de certificados ao longo do tempo. O AXIS Device Manager possibilita o gerenciamento eficiente dos certificados, permitindo que os administradores:

- Emitam certificados assinados por CA quando nenhuma outra CA está disponível
- Gerenciem facilmente certificados IEEE 802.1X
- Gerenciem facilmente certificados HTTPS
- Monitorem datas de expiração de certificados
- Renovem facilmente certificados antes da expiração

Recomendações para CAs intermediárias e raiz privadas

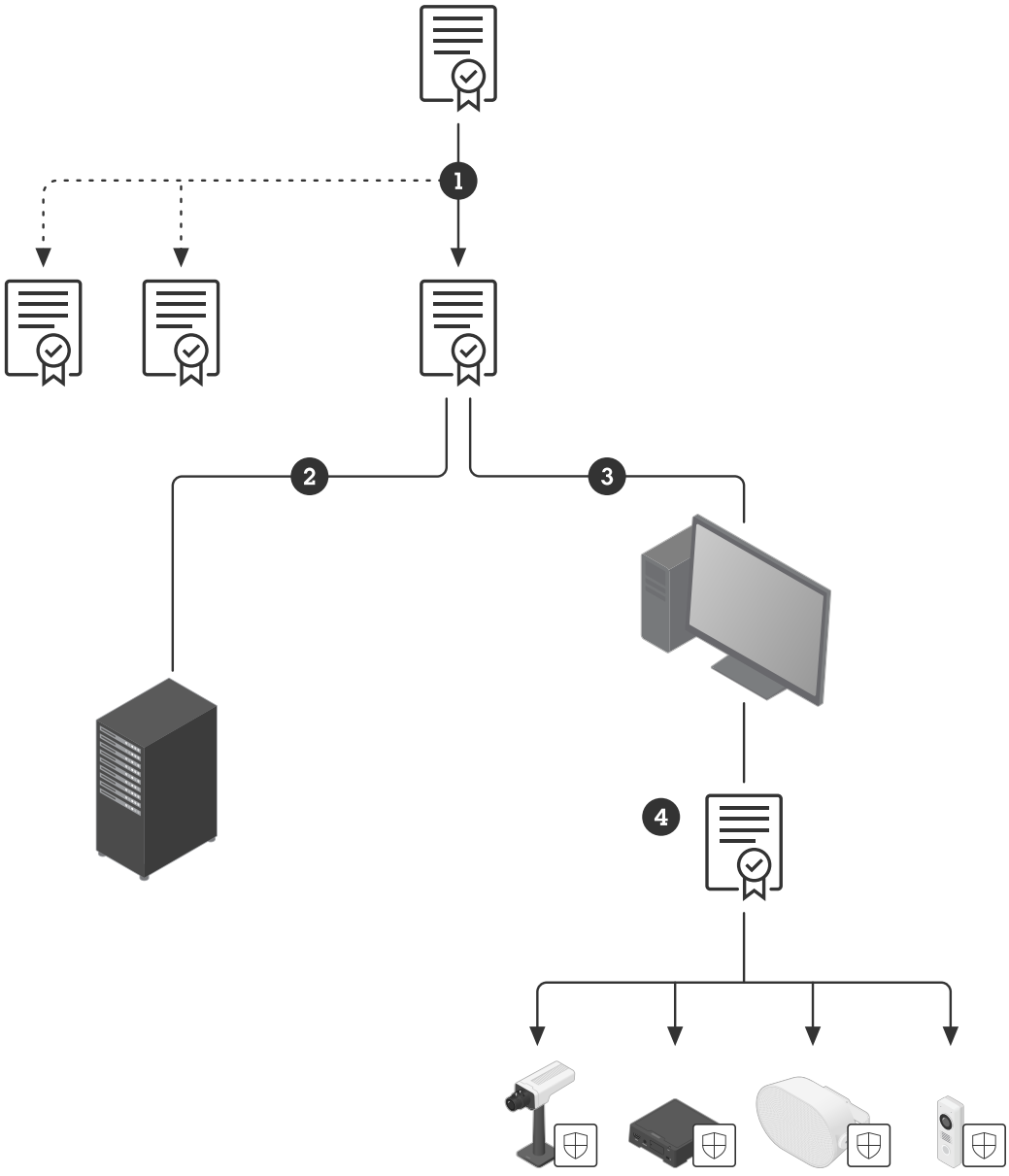
Não é recomendado expor os dispositivos Axis como servidores públicos voltados para o público em geral. Por isso, usar uma CA pública para recursos privados não é uma opção eficaz.

Para HTTPS, o servidor VMS é o único cliente que precisa validar que está acessando uma câmera confiável. Os clientes operadores jamais acessarão as câmeras diretamente, pois os vídeos ao vivo e gravados são fornecidos pelo servidor VMS. Nessa situação, há valor limitado em incorporar certificados de servidores de câmera a uma PKI empresarial existente.

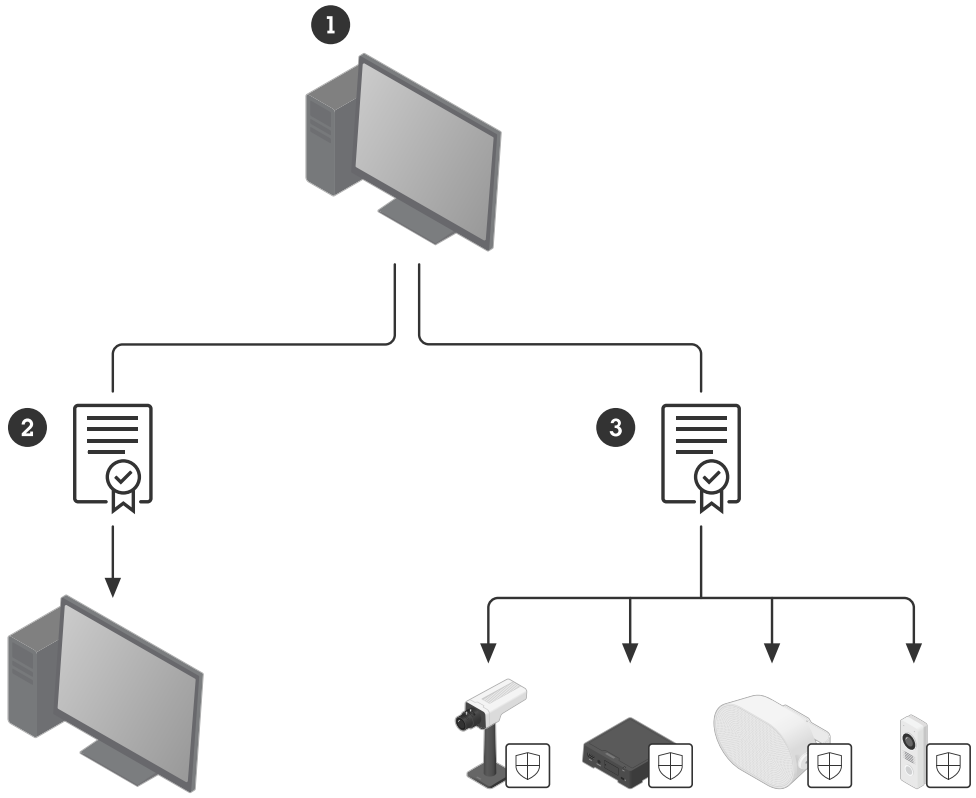
Usar o AXIS Device Manager como CA privada é a solução mais econômica. Após um certificado de CA raiz ser gerado, instale o certificado do AXIS Device Manager no armazenamento de certificados do servidor VMS. Se houver outros clientes acessando as câmeras diretamente (para manutenção ou solução de problemas), instale a CA raiz do AXIS Device Manager nesses clientes também.

No 802.1X, a câmera precisa de um certificado de cliente para se autenticar como um servidor RADIUS. Recomenda-se que o administrador da PKI/CA empresarial gere um certificado de CA intermediária e exporte-o como um certificado PKCS#12 (P12) que pode ser instalado no AXIS Device Manager.

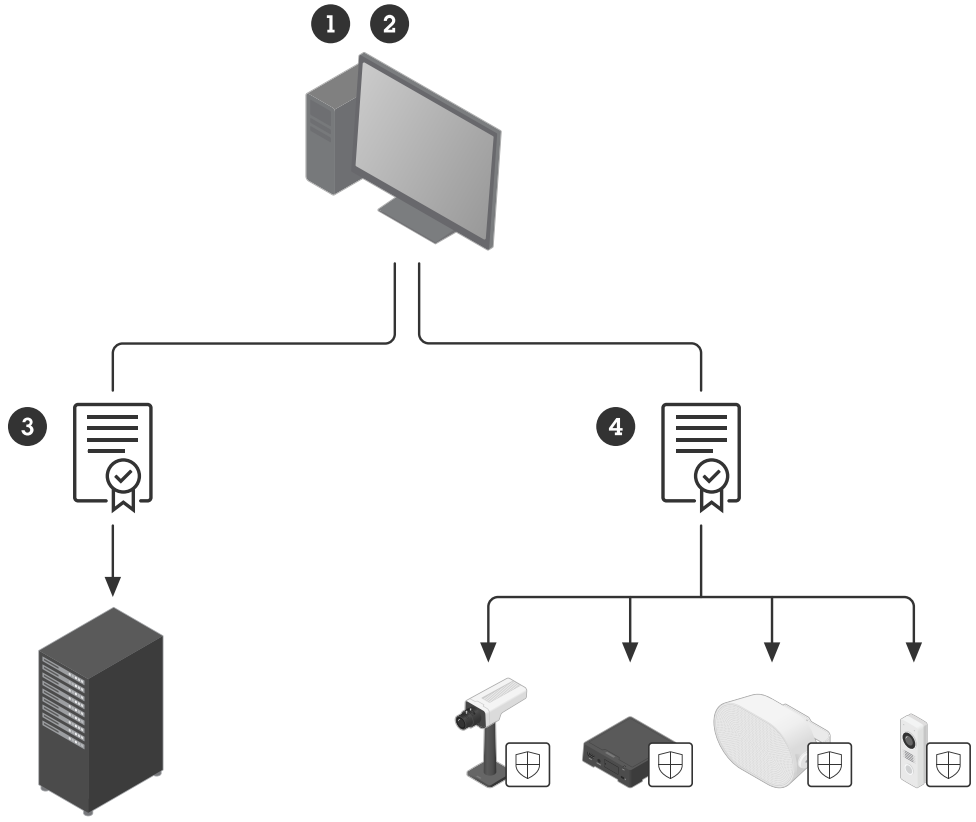
Para obter suporte na configuração de um servidor FreeRADIUS, visite a *Seção de documentos técnicos* do AXIS Device Manager.



O gerenciamento de certificados HTTPS envolve: 1) gerar um certificado de CA intermediária ou raiz no AXIS Device Manager, 2) exportar o certificado de CA para o VMS e 3) carregar certificados do servidor nos dispositivos.



Uso de uma CA privada. O gerenciamento de certificados IEEE 802.1X envolve: 1) gerar um certificado de CA intermediária e um certificado de cliente, 2) instalar o certificado de CA no servidor RADIUS, 3) importar o certificado de CA para o AXIS Device Manager e 4) carregar os certificados de CA e cliente nos dispositivos.



Uso do AXIS Device Manager como uma CA. Para gerenciar os certificados IEEE 802.1X: 1) gere o certificado de CA raiz no AXIS Device Manager, 2) importe o certificado de CA de autenticação no AXIS Device Manager; 3) instale o certificado de CA no servidor Radius; 4) carregue os certificados de CA de autenticação e de cliente nos dispositivos.

Conclusão

Gerenciamento e controle da segurança são partes importantes da implementação de uma abordagem de segurança cibernética efetiva. Eles são processos contínuos, que exigem manter um status claro e implementar as medidas adequadas para mitigar qualquer ameaça que possa afetar sua rede IP. O AXIS Device Manager oferece uma ferramenta para gerenciar seus dispositivos e aumentar a segurança em sua rede. Entre em contato com seu representante Axis local ou vá para *www.axis.com* para obter mais informações ou suporte.

T10231485_pt

2025-09 (M4.2)