Controle de segurança com o AXIS Device Manager

Versão 1.0

Sumário

1. Introdução 3

1.1 Três camadas de proteção de segurança cibernética 3

1.2 Objetivo deste documento 3

1.3 Sobre o AXIS Device Manager 3

2. Inventário de dispositivos 4

3. Política de contas e senhas 5

4. Atualizações de firmware 6

5. Fortalecimento adicional 7

6. Serviço de autoridade de certificação 7

7. Gerenciamento do ciclo de vida de certificados 9

8. Conclusão 10

1. Introdução

A importância da segurança cibernética continua a aumentar nos setores de vigilância e segurança. A segurança cibernética efetiva exige garantir a abrangência da defesa para proteger adequadamente sua rede IP em todos os níveis – dos produtos que você escolhe e os parceiros com que você trabalha até os requisitos que eles – e você – estabelecem.

1.1 Três camadas de proteção de segurança cibernética

Fornecemos três camadas de proteção de segurança cibernética:

1. Gerenciamento de segurança: requer a aplicação dos controles de segurança de que você precisa para minimizar as ameaças à segurança. Ele pode ser dividido em duas partes: controles de segurança e gerenciamento com custo eficiente. Controles de segurança são salvaguardas ou contramedidas empregadas para evitar, detectar, combater ou minimizar riscos à segurança de instalações físicas, informações, sistemas de computador ou outros ativos.

2. Gerenciamento de vulnerabilidades: engloba tudo que a Axis faz pra aplicar melhores práticas de segurança cibernética no design, desenvolvimento e teste de nossos produtos para minimizar o risco de falhas que poderiam ser exploradas. Quando as vulnerabilidades são descobertas, podemos gerenciá-las. Corrigimos vulnerabilidades críticas prontamente e emitimos comunicados de segurança.

3. Aprendizado e colaboração: é sobre a Axis, você e os parceiros envolvidos em sua rede IP conquistando e compartilhando uma compreensão clara e comum das ameaças enfrentadas por você, seu impacto potencial e como proteger sua rede.

1.2 Objetivo deste documento

Este guia de aplicação descreve como o AXIS Device Manager pode ser usado para fortalecer seu sistema e aumentar a segurança. Ele foca nos principais aspectos e descreve recomendações.

1.3 Sobre o AXIS Device Manager

O AXIS Device Manager é uma ferramenta local que oferece uma forma fácil, eficiente em termos de custo e segura para gerenciar suas principais tarefas de gerenciamento de instalações, segurança e manutenção de dispositivos (veja a tabela abaixo). Ele é capaz de gerenciar até alguns milhares de dispositivos Axis em um único site — ou vários milhares em múltiplos sites. O AXIS Device Manager permite a você implantar com eficiência controles de segurança cibernética para proteger seus dispositivos de rede e alinhá-los a uma infraestrutura de segurança.

Funções de gerenciamento de dispositivos, AXIS Device Manager

Instalação	Manutenção
> Atribuição de endereço IP > Exportação de lista de dispositivos e acompanhamento de ativos* > Gerenciamento de usuários e senhas* > Gerenciamento ACAP > Atualização de firmware* > Gerenciamento de certificados HTTPS* > Distribuição de certificados IEEE 802.1x* > Marcação de dispositivos	> Status do dispositivo > Coleta de dados do dispositivo > Configuração de dispositivos e cópia de configurações para múltiplos dispositivos > Conexão a múltiplos servidores/sistemas > Pontos de restauração > Restauração das configurações padrão de fábrica > Substituição de dispositivos > Renovação e gerenciamento de certificados* > Fortalecimento da segurança cibernética*

**Indica função de controle de segurança cibernética*

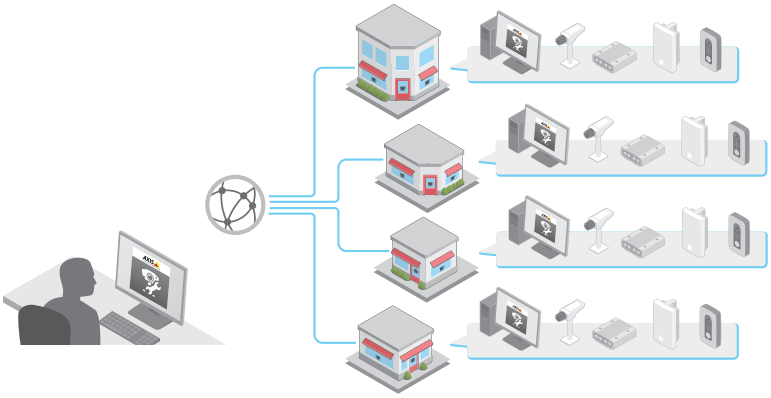


Figura 1 – Gerenciamento de múltiplos sites

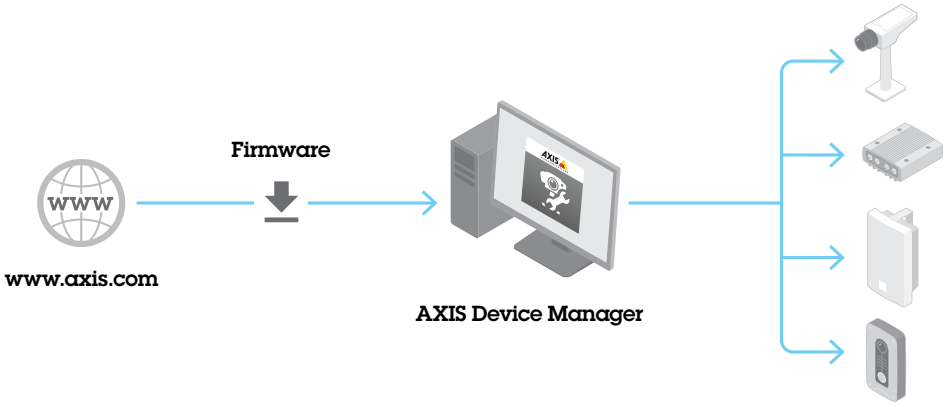


Figura 2 – Atualização de firmware

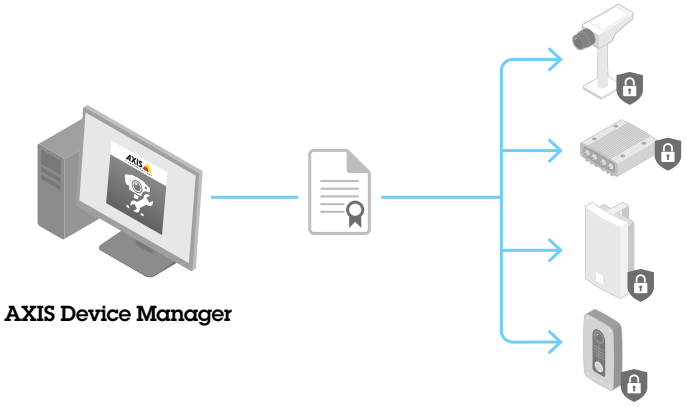


Figura 3 – Gerenciamento de certificados

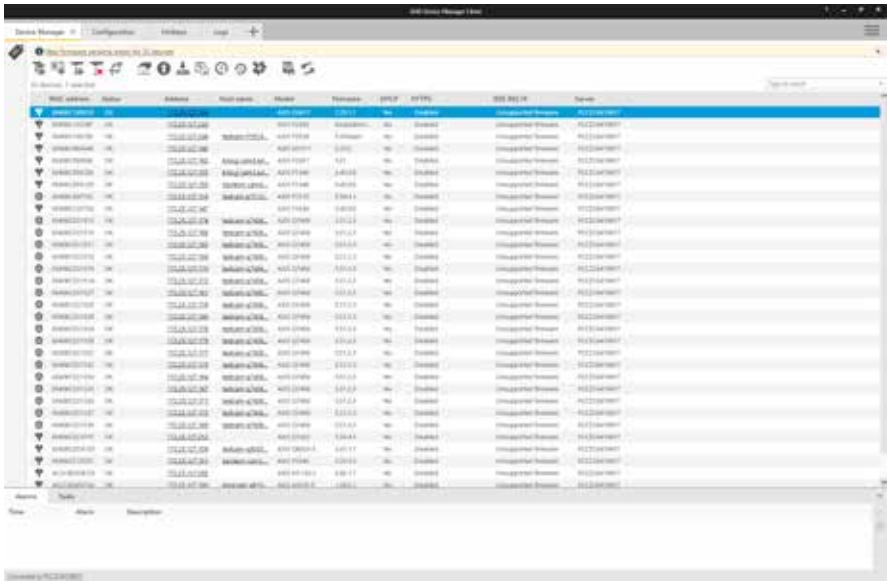
2. Inventário de dispositivos

Um aspecto fundamental para a garantia da segurança de uma rede corporativa é manter um inventário completo dos dispositivos conectados a ela. Ao criar ou revisar uma política de segurança geral, é importante conhecer e manter uma documentação clara de cada dispositivo, e não apenas de ativos críticos. Isso é necessário porque um único dispositivo deixado de lado pode representar uma porta de acesso para agressores. Você não pode proteger dispositivos que ignorou ou não conhece completamente.

O inventário de dispositivos representa uma etapa essencial para a segurança de uma rede corporativa. O AXIS Device Manager é útil porquê:

> Permite a você acessar facilmente um inventário atualizado e completo dos seus dispositivos de rede quando você trabalha com auditorias e respondedores de incidentes
> Fornece uma lista completa dos seus dispositivos, classificada por: número total, tipo, números de modelo, etc.
> Fornece o status de cada dispositivo em sua rede

Recomendações
O AXIS Device Manager oferece um meio automatizado de obter acesso ao inventário em tempo real de dispositivos de rede Axis. Ele permite a você identificar, listar e classificar automaticamente seus dispositivos. Tão importante quanto, ele permite que você use marcas para agrupar e classificar dispositivos com base em seus próprios critérios. Isso facilita obter uma visão geral e documentar todos os dispositivos Axis em sua rede.



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

3. 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 má utilização acidental ou proposital ao longo de um período maior. Uma parte fundamental é a redução do risco de comprometimento de senhas. Senhas fortes são importantes. No entanto, senhas de dispositivos podem se espalhar por uma organização. Quando isso ocorre, você acaba perdendo o controle sobre quem pode acessá-los. O AXIS Device Manager ajuda você a gerenciar facilmente múltiplas contas e senhas para os dispositivos Axis.

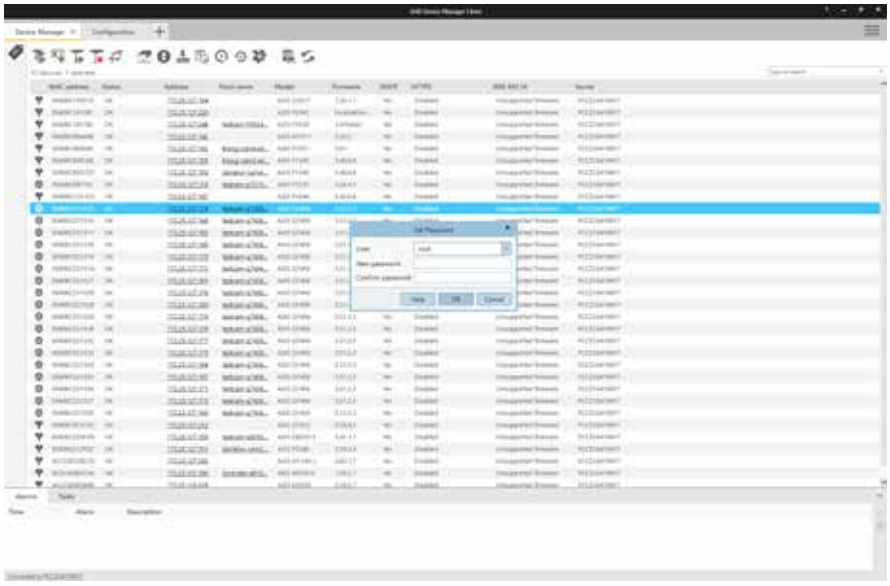
Por que você deve ter mais de uma conta de usuário nos dispositivos
> Você pode controlar níveis de privilégios para diferentes tipos de usuários (máquinas e humanos)
> Os riscos de comprometimento da senha de root (mestre) são menores
> Você pode redefinir as credenciais para um tipo de usuário sem afetar os outros

Trabalhando com privilégios no AXIS Device Manager
No AXIS Device Manager, os dispositivos Axis oferecem suporte a várias contas e podem pertencer a três níveis de privilégios diferentes: visualizador, operador e administrador. Vejamos como os privilégios podem ser gerenciados para as câmeras de rede Axis.

Usuários com privilégios de visualizador podem acessar vídeo e controlar PTZ. Aqueles com direitos de operador podem otimizar as configurações da câmera e os perfis de stream de vídeo. Administradores podem administrar contas, modificar configurações de rede e controlar vários serviços no dispositivo. Cada função com acesso à câmera deve ter sua própria conta.

Etapas recomendadas a serem seguidas

> Antes de adicionar câmeras ao VMS, recomenda-se adicioná-las 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. Ele pode ser tanto um operador quanto um administrador (consulte o fabricante).
> Adicione os dispositivos ao VMS com a conta "vms" e a senha que você definiu.
> Volte para o AXIS Device Manager, selecione todas as câmeras novamente e redefina (altere) a senha da conta "root" por 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 dentro da organização 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. Use o AXIS Device Manager para criar uma nova conta (temporária) para os dispositivos selecionados com privilégios de administrador ou operador. Quando a tarefa estiver concluída, use o AXIS Device Manager para remover 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. Recomenda-se utilizar usuários de domínio se a pessoa que administra o sistema pretende usar clientes remotos.



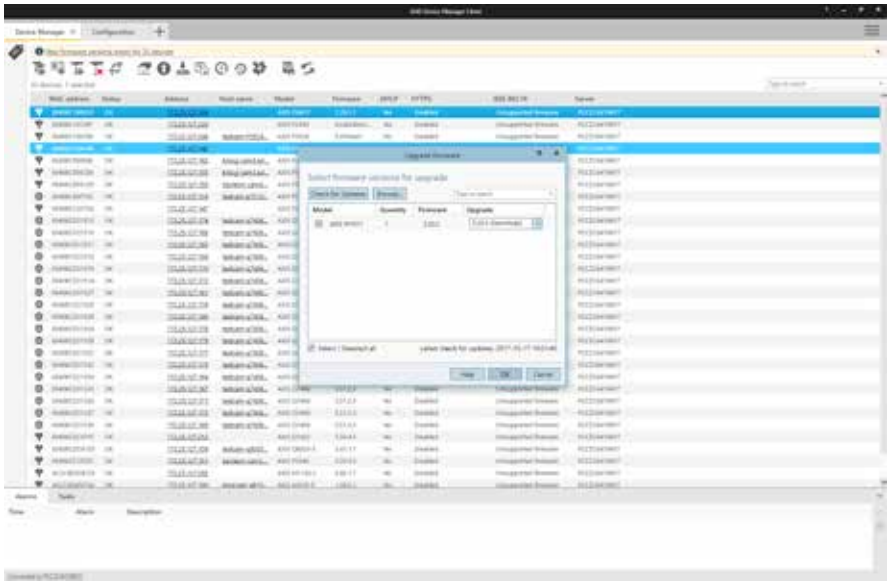
Alterando funções de usuários e senhas no AXIS Device Manager.

4. Atualizações de firmware

As versões de firmware mais recentes incluem patches para vulnerabilidades conhecidas. É indispensável usar sempre o software mais recente porque os agressores podem tentar explorar quaisquer vulnerabilidades conhecidas. Da mesma forma, a implantação rápida do novo firmware potencializa os recursos operacionais e remove gargalos relacionados à distribuição manual de novas atualizações de versão. O AXIS Device Manager conecta-se a www.axis.com e baixa o firmware ou as versões de serviço mais recentes disponíveis. 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 novo firmware disponível e permite a você implantá-lo rapidamente em seus dispositivos Axis.

Por que você sempre deve executar as versões mais recentes do firmware

> 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 resolver quaisquer bugs ou falhas conhecidos.
> Você obtém acesso imediato aos recursos e aprimoramentos de funcionalidades mais recentes



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

5. Fortalecimento adicional

Uma boa política de usuários/senhas e a execução de dispositivos com versões de firmware atualizadas ajudarão a minimizar riscos comuns para os dispositivos. O Guia de Fortalecimento Axis descreve medidas adicionais para reduzir riscos em organizações grandes e críticas. Isso inclui desativar serviços que podem não estar sendo usados e ativar serviços que podem 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 para as opções básicas recomendadas, saiba mais em: www.axis.com/products/axis-device-manager/support-and-documentation.

Como fortalecer dispositivos de acordo com o Guia de Fortalecimento Axis

> Baixe o arquivo de configuração do modelo de fortalecimento de www.axis.com/products/axis-device-manager/support-and-documentation
> Edite a configuração para escolher itens relevantes
> Selecione os dispositivos
> Clique com o botão direito e selecione "Configurar dispositivos | Configurar..."
> Clique em "Arquivo de configuração" e selecione o arquivo baixado
> Ajuste as configurações conforme necessário

6. Serviço de autoridade de certificação

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.

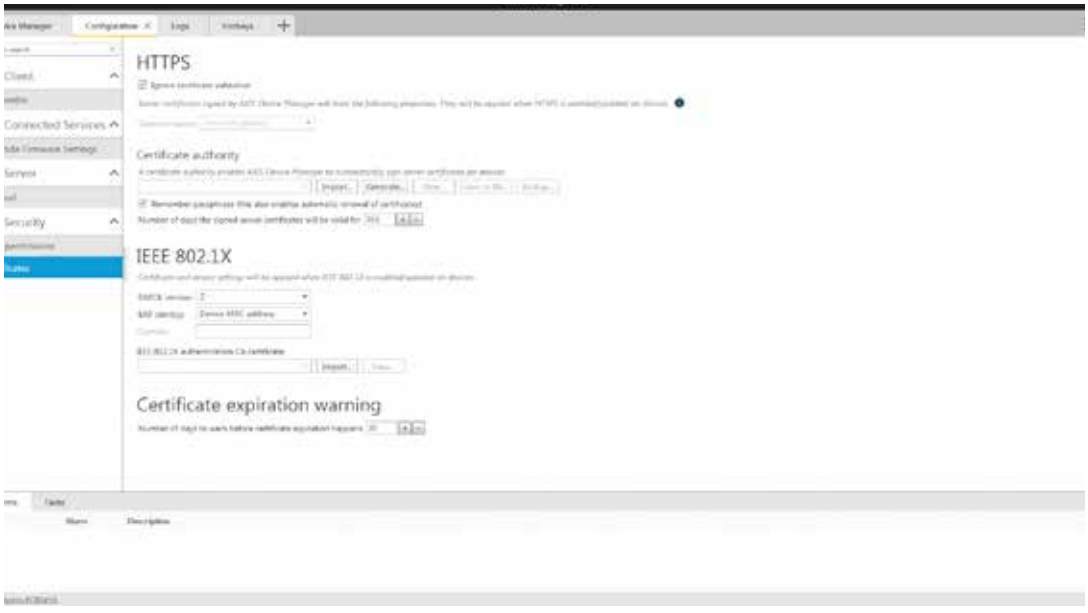
Uma CA privada (em geral, serviço de diretório ativo/certificados) emite certificados para serviços de rede internos/privados. Em um sistema de gerenciamento de vídeo, isso ocorre principalmente para Hyper Text Transfer Protocol Secure (HTTPS) (criptografia de rede) e IEEE 802.1x (controle de acesso à rede). O AXIS Device Manager inclui um serviço de CA para dispositivos Axis e pode atuar como CA raiz privada ou CA intermediária privada; parte de uma infraestrutura de chave pública (PKI) corporativa.

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 oferecem proteção contra spoofing de rede, onde um computador agressor tenta personificar um servidor legítimo. Os certificados assinados por CA adicionam um ponto de confiança para a autenticação dos clientes, que é acessar 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
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). Há diferentes métodos de autenticação que podem ser usados, como: endereço MAC (filtragem de MAC), usuário/senha ou certificado de cliente. O dono 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 mão de obra para mantê-la e monitorá-la.



Configuração do certificado no AXIS Device Manager.

7. Gerenciamento do ciclo de vida de certificados

O gerenciamento do ciclo de vida de certificados é uma forma de lidar de maneira eficiente em termos de custos com todos os processos e tarefas relacionados à emissão, inspeção, correção e renovação de certificados ao longo de períodos prolongados. O AXIS Device Manager permite que você gerencie certificados de forma eficiente permitindo que os administradores:

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

Recomendações de CA raiz e intermediária privadas
Não é recomendado expor os dispositivos Axis como servidores públicos voltados para o público em geral. É por isso que usar uma CA pública para recursos privados não é eficiente em termos de custos.

No 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 o vídeo ao vivo e gravado é fornecido pelo servidor VMS. Nessa situação, há valor limitado para incorporar certificados de servidores de câmera em 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.

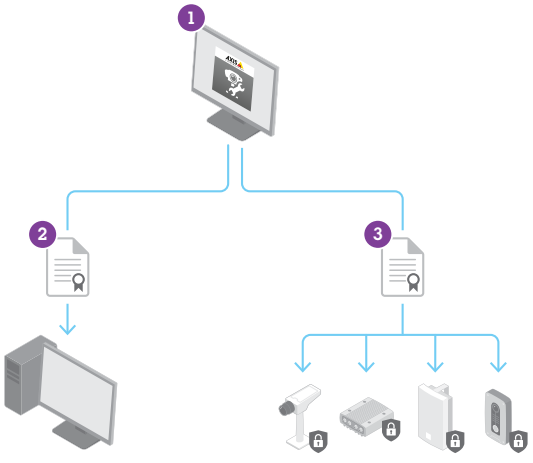


Figura 4, esquerda – O gerenciamento de certificados HTTPS envolve:
1) gerar um certificado de CA intermediária ou raiz no AXIS Device Manager, 2) exportar o certificado de CA para o VMS e 3) carregar certificados de servidor nos dispositivos.

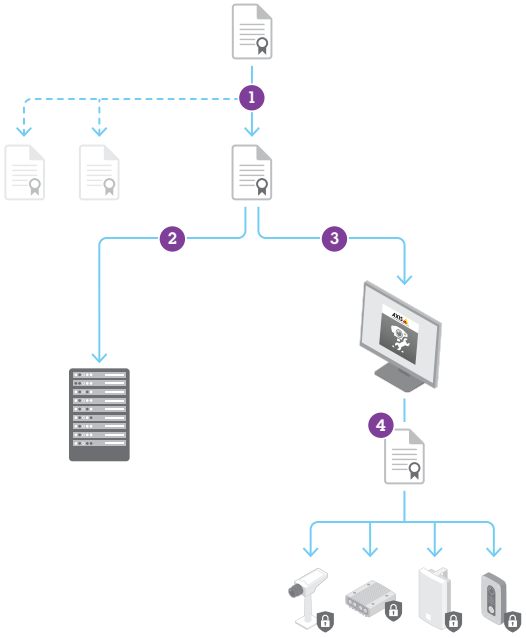


Figura 5, direita – A distribuição de certificados IEEE 802.1X envolve: 1) gerar um certificado de CA intermediária e um certificado de cliente, 2) instalar o certificado de CA no servidor RADIUS, 3) importar o certificado de CA para o AXIS Device Manager e 4) carregar os certificados de CA e cliente para os dispositivos.

8. Conclusão

Gerenciamento e controle da segurança são partes importantes da implementação de uma abordagem de segurança cibernética efetiva. Cada uma é um processo contínuo que exige a manutenção de um status claro e a execução de ações apropriadas para mitigar qualquer ameaça potencial que possa afetar sua rede IP. O AXIS Device Manager oferece a você uma ferramenta para gerenciar seus dispositivos e, ao mesmo tempo, aumentar a segurança da sua rede. Entre em contato com seu representante Axis local ou vá para www.axis.com para obter mais informações ou suporte.

Sobre a Axis Communications

A Axis oferece soluções de segurança inteligentes que contribuem para um mundo mais inteligente e mais seguro. Como líder de mercado em vídeo em rede, a Axis está movimentando o setor ao lançar continuamente produtos de rede inovadores baseados em uma plataforma aberta – proporcionando uma alta geração de valor para os clientes por meio de uma rede de parceiros global. A Axis possui relacionamentos de longo prazo com seus parceiros e fornece a eles conhecimento e produtos de rede revolucionários nos mercados existentes e em novos mercados.

A Axis possui mais de 2.700 funcionários dedicados em mais de 50 países ao redor do mundo e conta com o suporte de uma rede global formada por mais de 90.000 parceiros. Fundada em 1984, a Axis é uma empresa de TI com sede na Suécia e listada na NASDAQ Stockholm como AXIS.

Para mais informações sobre a Axis, visite nosso site www.axis.com.

AXIS COMMUNICATIONS