Contrôle de la sécurité avec AXIS Device Manager

Version 1.0

Table des matières

1. Introduction

La cybersécurité pèse de tout son poids dans les secteurs de la surveillance et de la sécurité. Une cybersécurité efficace nécessite le déploiement d'une défense en profondeur, capable de protéger correctement votre réseau IP à tous les niveaux : des produits utilisés aux partenaires avec lesquels vous collaborez, en passant par les règles qu'ils se fixent (et que vous vous fixez).

1.1 Trois couches de protection en cybersécurité

En matière de cybersécurité, nous proposons trois couches de protection :

1. La gestion de la sécurité : passe par la mise en place des contrôles de sécurité nécessaires pour limiter les menaces auxquelles vous êtes confronté. Elle se divise en deux parties : les contrôles de sécurité et une gestion rentable. Les contrôles de sécurité sont les garde-fous ou les contremesures utilisés pour éviter, détecter, neutraliser ou minimiser les risques de sécurité touchant les propriétés physiques, les informations, les systèmes informatiques ou les autres biens.

2. La gestion des vulnérabilités : comprend tout ce que Axis entreprend pour appliquer les meilleures pratiques de la cybersécurité dans la conception, le développement et le test de ses produits afin de réduire au maximum le risque de failles qui pourraient être exploitées. Dès que des vulnérabilités sont mises à jour, nous les gérons ; nous corrigeons rapidement les vulnérabilités critiques et émettons des avertissements de sécurité.

3. L'apprentissage et la collaboration : concernent Axis, vous et les partenaires impliqués dans votre réseau IP. Il s'agit d'obtenir et de partager une vision à la fois claire et commune des menaces qui se présentent à vous, de leur impact potentiel, et de définir comment protéger votre réseau.

1.2 Objectif du présent document

Le présent guide de l'application décrit comment AXIS Device Manager vient renforcer votre système et en améliorer sa sécurité. Il se concentre sur certains aspects clés et donne des recommandations.

1.3 À propos d'AXIS Device Manager

AXIS Device Manager est un outil à installer sur site, qui offre une solution à la fois simple, rentable et sécurisée pour gérer toutes les tâches majeures d'installation, de sécurité et de gestion des périphériques de maintenance (voir le tableau ci-dessous). Il est parfaitement adapté à la gestion de quelques milliers de périphériques Axis répartis sur un seul site voire plusieurs milliers de périphériques répartis sur plusieurs sites. AXIS Device Manager permet de déployer efficacement les contrôles de cybersécurité capables de protéger vos périphériques réseau et de les aligner sur une infrastructure de sécurité.

Fonctions de gestion des périphériques, AXIS Device Manager

Installation	Maintenance
> Attribution d'une adresse IP > Export de la liste des périphériques et suivi des biens* > Gestion des utilisateurs et des mots de passe* > Gestion de l'ACAP > Mise à niveau des firmwares* > Gestion des certificats HTTPS* > Distribution des certificats IEEE 802.1x* > Labélisation des périphériques	> Statut de l'appareil > Collecter les données du périphérique > Configuration des périphériques et copie des configurations vers plusieurs périphériques > Connexion à plusieurs serveurs/systèmes > Points de restauration > Rétablissement des valeurs par défaut > Remplacement de périphérique > Gestion et renouvellement des certificats* > Renforcement de la cybersécurité*

**Indique la fonction de contrôle de la cybersécurité*

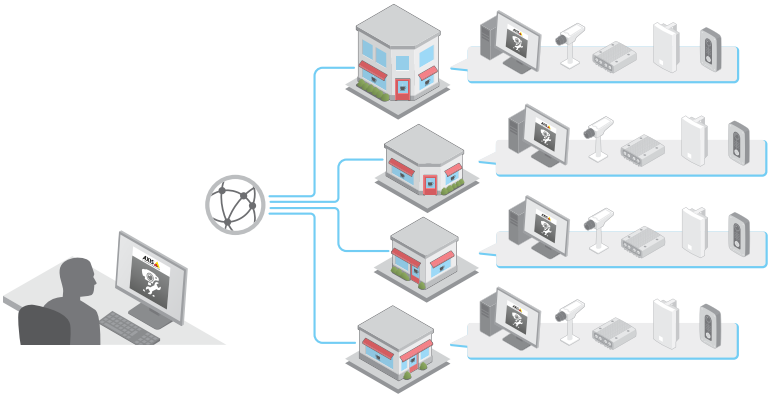


Figure 1. Gestion de plusieurs sites

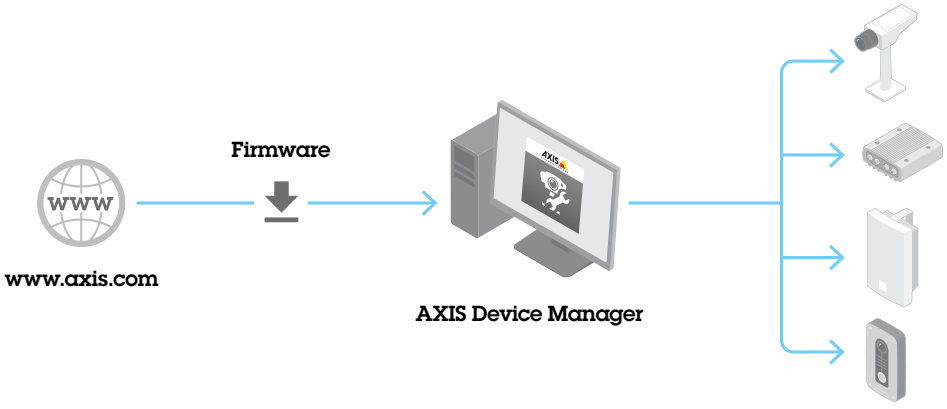


Figure 2. Mise à niveau des firmwares

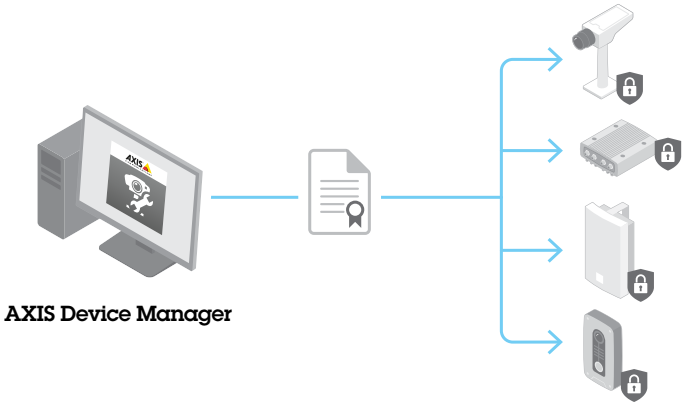


Figure 3. Gestion des certificats

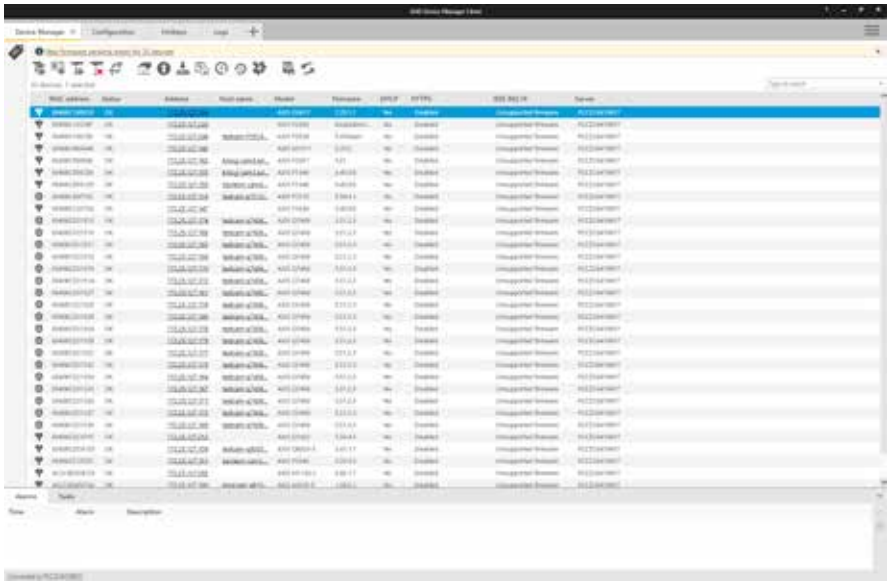
2. Inventaire des périphériques

Un des aspects fondamentaux dans la sécurité d'un réseau d'entreprise consiste à maintenir à jour un inventaire exhaustif des différents périphériques. Lorsque l'on créée ou fait évoluer une politique de sécurité générale, il est primordial de connaître chaque périphérique et de disposer d'une documentation claire pour chaque périphérique et pas seulement pour les biens critiques. La raison en est simple : chaque périphérique ignoré peut constituer un point d'entrée pour les personnes malveillantes. Vous ne pouvez pas protéger les périphériques que vous avez ignorés ou dont vous n'avez pas complètement connaissance.

L'inventaire des périphériques est une étape essentielle dans la sécurisation d'un réseau d'entreprise. AXIS Device Manager vous aide puisqu'il :

> Vous permet d'accéder facilement à un inventaire exhaustif et actualisé de vos périphériques réseau à des fins d'audits et en cas de réponse à des incidents.
> Fournit la liste complète de vos périphériques, les trie selon : le nombre total, le type, la référence du modèle, etc.
> Donne l'état de chaque périphérique du réseau.

Recommandations
AXIS Device Manager fournit un moyen automatisé d'accéder à un inventaire en temps réel des périphériques réseau Axis. Il vous permet d'identifier, de répertorier et de trier vos périphériques automatiquement. Tout aussi important, il vous laisse utiliser des labels pour que vous puissiez regrouper et trier les périphériques selon vos propres critères. Ainsi, vous obtenez plus facilement une vue d'ensemble de tous les périphériques Axis présents sur votre réseau.



AXIS Device Manager offre un aperçu clair sur votre inventaire des périphériques.

3. Politique en matière de comptes et de mots de passe

La protection des ressources réseau passe par le contrôle des authentifications et des privilèges. La mise en œuvre de politiques contribue à réduire les risques d'usages abusifs accidentels ou délibérés sur le long terme. Une part essentielle consiste à limiter les risques de mots de passe compromis. Utiliser des mots de passe forts est primordial. Ceci étant dit, les mots de passe des périphériques peuvent se répandre au sein d'une société. Dans un tel cas de figure, vous ne savez plus quelles personnes ont le droit d'y accéder ou pas. AXIS Device Manager vous aide à gérer facilement plusieurs comptes et mots de passe pour les périphériques Axis.

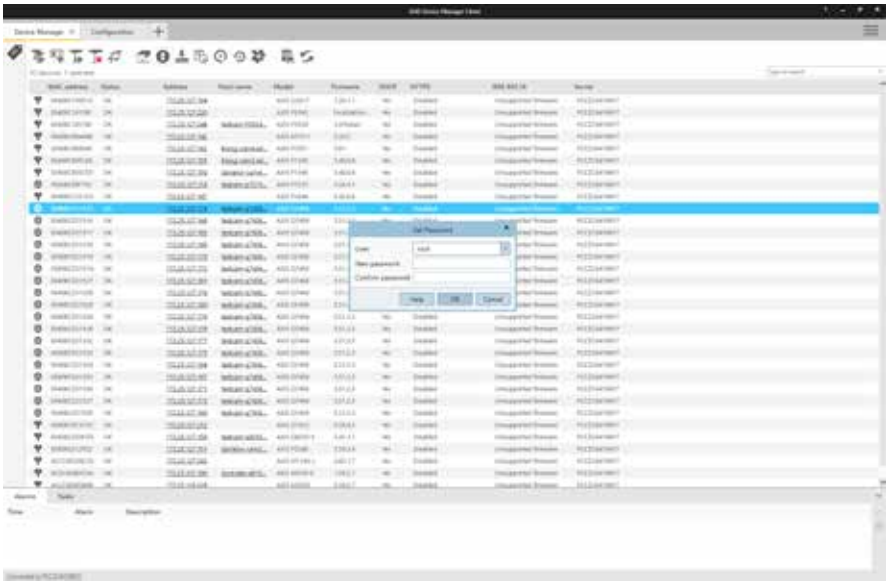
Raisons pour lesquelles il est vivement conseillé d'avoir plusieurs comptes utilisateur au niveau des périphériques :
> Vous contrôlez les niveaux de privilège pour divers types d'utilisateur (machines et personnes)
> Vous réduisez le risque de compromettre le mot de passe root (maître)
> Vous pouvez réinitialiser les informations d'identification pour un seul type d'utilisateur sans répercussion sur les autres

Utilisation des privilèges dans AXIS Device Manager
Dans AXIS Device Manager, les périphériques Axis peuvent prendre en charge plusieurs comptes et comprennent trois niveaux de privilège différents : observateur, opérateur et administrateur. Voici comment gérer les privilèges pour les caméras réseau Axis.

Les utilisateurs avec les privilèges Observateur peuvent accéder à la vidéo et contrôler les fonctions panoramique/inclinaison/zoom (PTZ). Les utilisateurs ayant des droits Opérateur peuvent optimiser les paramètres de la caméra et les profils de flux de données vidéo. Les administrateurs peuvent administrer les comptes, modifier les paramètres réseau et contrôler le nombre de services au niveau du périphérique. Chaque rôle qui accède à la caméra doit être associé à son propre compte.

Étapes recommandées

> Avant d'ajouter des caméras au serveur VMS, il est conseillé d'ajouter les caméras à AXIS Device Manager.
> Dans AXIS Device Manager, sélectionnez toutes les caméras et créez un compte utilisateur appelé « vms » ou quelque chose d'identique, et définissez un mot de passe fort. Les privilèges doivent être alignés avec les exigences du serveur VMS, il peut s'agir des privilèges Opérateur ou Administrateur (vérifiez auprès du fabricant).
> Ajoutez les périphériques au VMS à l'aide du compte « vms » et du mot de passe définis
> Revenez à AXIS Device Manager et sélectionnez de nouveau toutes les caméras et réinitialisez (changez) le mot de passe du compte « root » avec un nouveau mot de passe fort. Ce mot de passe du compte « root » ne doit pas être divulgué (seules les personnes qui utilisent AXIS Device Manager doivent le connaître).
> Lorsqu'une personne de la société doit utiliser un navigateur Web pour accéder au périphérique pour exécuter des tâches de maintenance ou de dépannage, ne lui communiquez pas le mot de passe root. Utilisez AXIS Device Manager pour créer un compte (temporaire) pour le(s) périphérique(s) sélectionné(s) avec les privilèges Opérateur ou Administrateur. Une fois les tâches terminées, utilisez AXIS Device Manager pour supprimer le compte temporaire.
> AXIS Device Manager prend en charge les administrateurs locaux ainsi que les groupes et les utilisateurs d'un domaine. Utilisez un administrateur local si le client AXIS Device Manager accède uniquement depuis la machine qui héberge le serveur AXIS Device Manager. Il est conseillé d'utiliser des utilisateurs de domaine si la personne chargée de maintenir le système utilise des clients à distance.



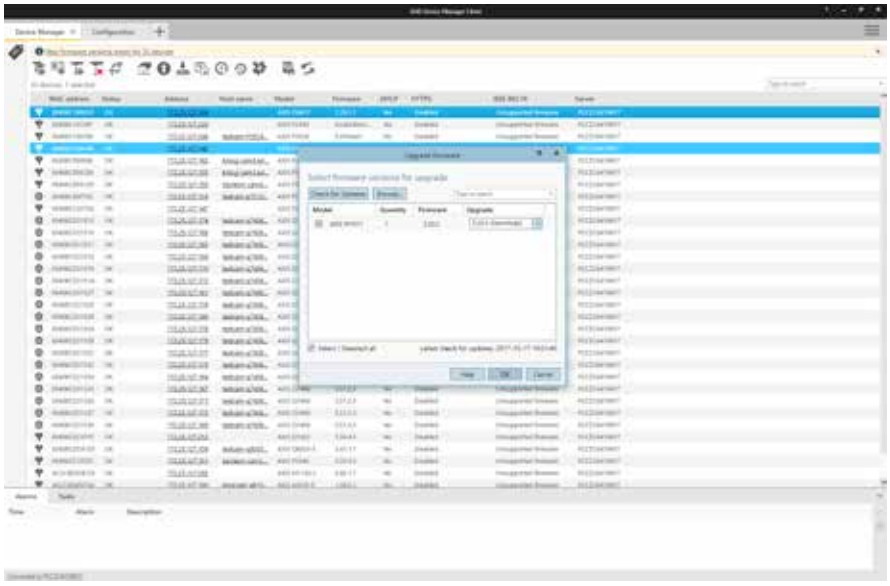
Modification des mots de passe et des rôles utilisateur dans AXIS Device Manager.

4. Mises à niveau des firmwares

Les dernières versions de firmware incluent les correctifs pour les vulnérabilités connues. Il est indispensable d'utiliser toujours les derniers logiciels car les personnes malveillantes peuvent essayer d'exploiter toute vulnérabilité connue. Deuxième point important : le déploiement rapide des nouveaux firmwares stimule les capacités de fonctionnement et supprime les goulots d'étranglement associés au déploiement manuel des nouvelles mises à niveau de version. AXIS Device Manager se connecte à www.axis.com et télécharge les derniers firmwares ou les dernières versions de service disponibles. Si vous préférez ne pas les télécharger directement depuis Internet vers votre réseau, enregistrez les mises à niveau sur une clé USB, puis chargez-les sur votre client AXIS Device Manager. Il indique également si de nouveaux firmwares sont disponibles et vous permet de les déployer rapidement sur les périphériques Axis.

Raisons pour lesquelles il est vivement recommandé d'exécuter les dernières versions des firmwares :

> Les derniers correctifs sont appliqués à votre réseau et vos périphériques, les protégeant des vulnérabilités connues, dont les vulnérabilités critiques.
> Vos périphériques sont mis à jour et bénéficient des dernières améliorations de performance ainsi que corrections relatives aux failles et bogues connus
> Vous avez immédiatement accès aux dernières améliorations apportées aux caractéristiques et aux fonctions



Les notifications à l'écran et les boîtes de dialogues intuitives simplifient la mise à niveau des firmwares avec AXIS Device Manager.

5. Sécurisation complémentaire

Une politique d'identification/authentification adaptée, couplée à des versions de firmware à jour, permet d'atténuer les risques communs au niveau des périphériques. Le guide intitulé « Axis Hardening Guide » (en anglais) présente des mesures supplémentaires visant à réduire les risques au sein des sociétés grandes et sensibles. Ceci passe par la désactivation des services qui ne peuvent pas être utilisés et l'activation des services qui contribuent à détecter et à surveiller les éléments annonciateurs d'une attaque ou une faille de sécurité.

AXIS Device Manager simplifie le processus de déploiement de certaines de ces politiques. Axis fournit un modèle de configuration pour les réglages de base recommandés. Plus d'informations ici : www.axis.com/products/axis-device-manager/support-and-documentation.

Comment renforcer la sécurité des périphériques selon le guide « Axis Hardening Guide » :

> Téléchargez le fichier de configuration du modèle de sécurisation complémentaire depuis www.axis.com/products/axis-device-manager/support-and-documentation
> Modifiez le fichier de configuration en choisissant des éléments pertinents
> Sélectionnez les périphériques
> Faites un clic droit et sélectionnez Configurer les dispositifs | Configurer...
> Cliquez sur Fichier de configuration et sélectionnez le fichier téléchargé
> Réglez les paramètres selon vos besoins

6. Service d'autorité de certification (CA)

L'autorité de certification (CA) est un service qui émet des certificats numériques aux serveurs, clients ou utilisateurs. Une CA peut être publique ou privée. Les CA reconnues publiquement, telles que Comodo et Symantec (anciennement Verisign), sont généralement utilisées pour les services publics comme les sites Web publics et les e-mails.

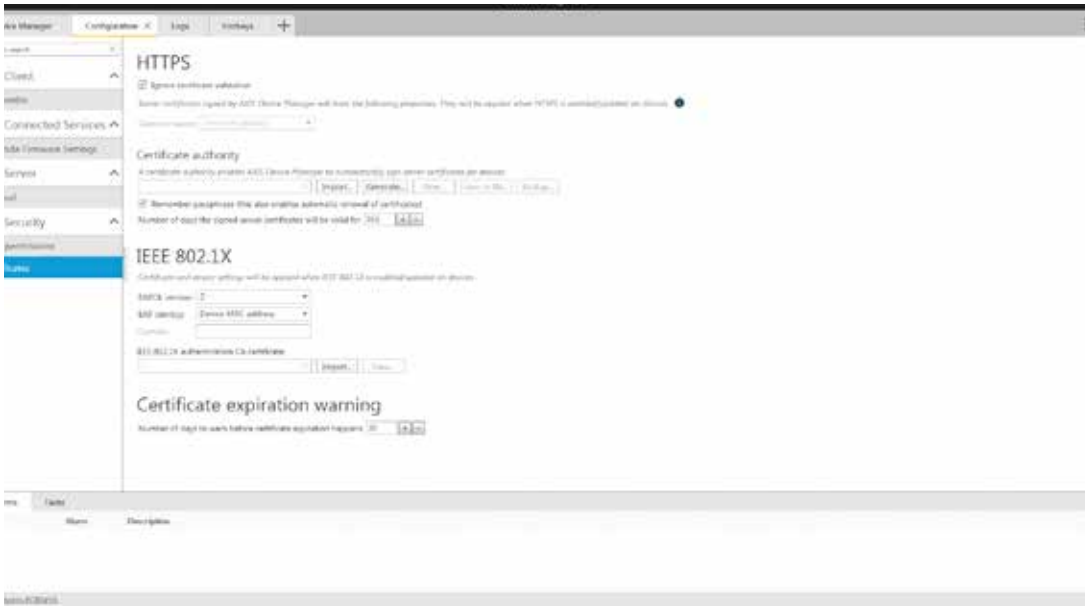
Une CA privée (généralement un service de certification/Active Directory) émet des certificats pour des services réseaux privés/internes. Dans un système de gestion de la vidéo, cela concerne principalement le protocole HTTPS (Hypertext Transfer Protocol Secure) (cryptage réseau) et la norme IEEE 802.1x (contrôle d'accès au réseau). AXIS Device Manager inclut un service de CA pour les périphériques Axis et peut fonctionner comme une CA racine privée ou comme une CA intermédiaire privée, dans le cadre d'une IGC (infrastructure de gestion de clés) d'entreprise.

Les certificats signés CA sont utilisés à la fois pour les certificats IEEE 802.1x (client) et HTTPS (serveur).

Protocole HTTPS
Le protocole HTTPS est la version sécurisée du protocole HTTP sur lequel les communications entre un client et un serveur sont cryptées. Les certificats auto-signés sont suffisants pour obtenir une connexion cryptée. Il n'existe aucune différence en matière de niveau de cryptage entre les certificats auto-signés et les certificats signés CA. La différence réside dans le fait que les certificats auto-signés ne protègent pas contre la mise en file d'attente réseau où un ordinateur malveillant tente d'emprunter l'identité d'un serveur légitime. Les certificats signés CA ajoutent un niveau de confiance à l'authentification des clients qui certifie qu'ils accèdent à un périphérique approuvé. Notez que le client vidéo (VMS) doit prendre en charge la demande de vidéo sur HTTPS (RTP sur RTSP sur HTTPS) pour crypter la vidéo.

Norme IEEE 802.1x
Connue sous l'appellation 802.1X, cette norme empêche les périphériques non autorisés d'accéder au réseau local. Un périphérique doit s'authentifier pour pouvoir accéder au réseau (et à ses ressources). Il existe différentes méthodes d'authentification : par adresse MAC (filtrage MAC), par utilisateur/mot de passe ou par certificat client. Le propriétaire du système décide de la méthode à employer, le choix approprié dépendant des menaces, du risque et du coût.

Faire fonctionner une infrastructure 802.1X représente un investissement. Elle exige des switches manageables et des serveurs supplémentaires, en général, un serveur RADIUS (Remote Authentication Dial-In User Service). L'utilisation de certificats client nécessite une CA (privée ou publique) capable d'émettre des certificats client. Dans la plupart des cas, l'infrastructure a besoin de personnel pour la maintenance et la surveillance.



Configuration de la certification dans AXIS Device Manager.

7. Gestion du cycle de vie des certificats

La gestion du cycle de vie des certificats est un moyen rentable de gérer tous les processus et toutes les tâches associés à l'émission, l'installation, l'inspection, la correction et le renouvellement des certificats sur une longue période. AXIS Device Manager vous aide à gérer efficacement les certificats en permettant aux administrateurs d'effectuer les tâches suivantes :

> Émettre des certificats signés CA lorsqu'aucune autre CA n'est disponible
> Distribuer facilement les certificats IEEE 802.1X
> Déployer facilement les certificats HTTPS
> Contrôler les dates d'expiration des certificats
> Renouveler facilement les certificats avant expiration

Recommandations en matière de CA intermédiaires et racines privées
Il n'est pas conseillé d'exposer les périphériques Axis en tant que serveurs publics pour le public. C'est la raison pour laquelle utiliser une CA publique pour les ressources privées n'est pas rentable.

Pour HTTPS, le serveur VMS est le seul client qui doit valider son accès à une caméra approuvée. Les clients de l'opérateur n'ont jamais directement accès aux caméras puisque la vidéo en direct et enregistrée est fournie par le serveur VMS. Dans ce cas, il n'est pas vraiment intéressant d'intégrer les certificats du serveur de caméras à une IGC d'entreprise existante.

Utiliser AXIS Device Manager en tant que CA privée s'avère être la solution la plus rentable. Dès qu'un certificat CA racine est généré, installez le certificat AXIS Device Manager dans le magasin de certificats du serveur VMS. Si d'autres clients accèdent directement aux caméras (pour la maintenance ou le dépannage), installez également la CA racine AXIS Device Manager dans ces clients.

Pour la norme 802.1X, la caméra a besoin d'un certificat client pour s'authentifier sur un serveur RADIUS. Il est conseillé de demander à l'administrateur des CA/IGC d'entreprise de générer un certificat CA intermédiaire et de l'exporter en tant que certificat PKCS#12 (P12) qui peut être installé sur AXIS Device Manager.

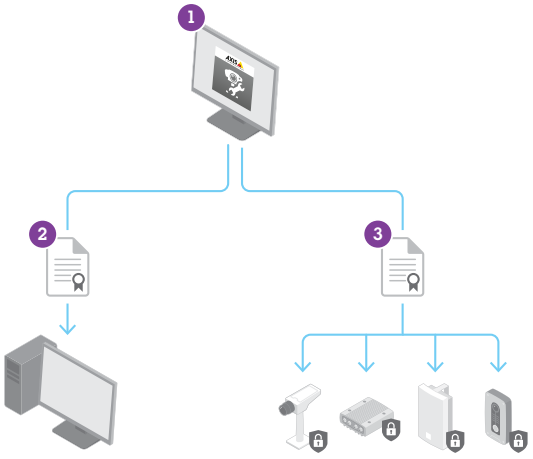


Figure 4, à gauche : la gestion des certificats HTTPS implique de :
1) générer un certificat CA intermédiaire ou racine dans AXIS Device Manager, 2) exporter le certificat CA vers le serveur VMS et 3) charger les certificats du serveur sur les périphériques.

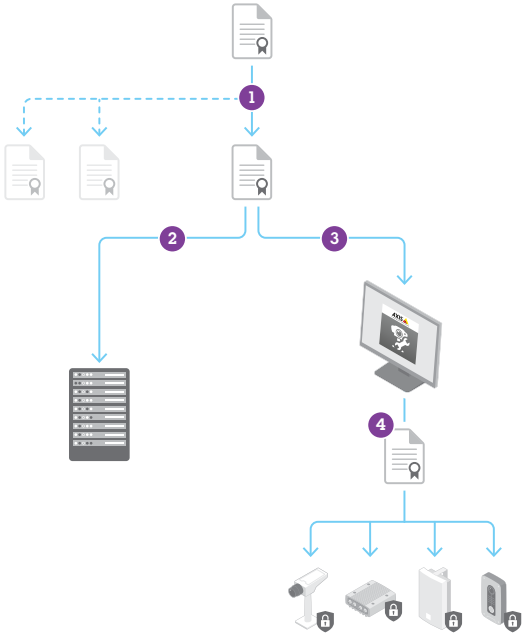


Figure 5, à droite : la distribution des certificats IEEE 802.1X implique de : 1) générer un certificat CA intermédiaire et un certificat client, 2) installer le certificat CA sur le serveur RADIUS, 3) importer le certificat CA dans AXIS Device Manager et 4) charger les certificats client et CA sur les périphériques.

8. Conclusion

La gestion et le contrôle de la sécurité sont primordiaux lorsque l'on souhaite mettre en œuvre une cybersécurité efficace. Chaque élément est un processus continu qui exige de conserver des états clairs et de suivre des actions appropriées afin d'atténuer toute menace potentielle qui aurait un impact sur votre réseau IP. AXIS Device Manager est un outil qui vous permet à la fois de gérer vos périphériques et d'améliorer la sécurité de votre réseau. Contactez votre représentant Axis local ou consultez le site www.axis.com pour plus d'informations ou pour obtenir une assistance technique.

À propos d'Axis Communications

Axis propose des solutions intelligentes qui contribuent à construire un monde plus sûr et plus clairvoyant. En tant que leader sur le marché de la vidéo sur IP, Axis reste à la pointe dans son domaine en lançant des produits réseau innovants basés sur une plate-forme ouverte et en apportant de la valeur ajoutée à ses clients grâce à son réseau mondial de partenaires. Axis entretient une relation durable avec ses partenaires et leur fournit la connaissance et des produits réseau révolutionnaires à destination des marchés nouveaux et existants.

Axis emploie plus de 2 700 employés dans plus de 50 pays à travers le monde et peut compter sur le soutien d'un réseau mondial de plus de 90 000 partenaires. Fondée en 1984, Axis est une société informatique suédoise listée au NASDAQ de Stockholm sous le titre AXIS.

Pour plus d'informations sur Axis, rendez-vous sur notre site Web www.axis.com.

AXIS COMMUNICATIONS