AXIS Device Manager

Manuel d'utilisation

Introduction

La cybersécurité pèse de tout son poids dans les secteurs de la surveillance et de la sécurité. Une cybersécurité efficace exige de garantir une profondeur de défense suffisante pour protéger correctement votre réseau IP à tous les niveaux, depuis les produits et les partenaires que vous choisissez jusqu'aux exigences que vous et eux fixent.

Ce guide explique comment utiliser AXIS Device Manager pour renforcer votre système et améliorer la sécurité. Il se concentre sur certains aspects clés et donne des recommandations.

Gestion du cycle de vie des dispositifs

Chez Axis, nous comprenons l'importance d'une base solide en matière de sécurité, tout au long du cycle de vie du dispositif. Notre engagement en faveur de la cybersécurité garantit que nos produits et solutions offrent une protection robuste contre les menaces potentielles.

Mise en œuvre

Axis fournit des dispositifs conçus pour être sécurisés dès leur conception, avec des fonctionnalités de sécurité intégrées comme des mécanismes de démarrage sécurisé, un système d'exploitation signé et un stockage chiffré. En outre, AXIS Device Manager aide les installateurs et les administrateurs système à configurer et à déployer les dispositifs en toute sécurité, garantissant ainsi une configuration correcte dès le départ.

Service actif

Pendant la phase de fonctionnement, Axis propose régulièrement des mises à jour logicielles et des correctifs de sécurité pour protéger les dispositifs contre les vulnérabilités. AXIS Device Manager permet également le contrôle et la maintenance à distance, ce qui active la résolution rapide des problèmes et réduit au minimum les temps d'arrêt. Par ailleurs, nos guides de renforcement fournissent des recommandations de configuration des périphériques, afin de répondre à des exigences de sécurité spécifiques.

Mise hors exploitation

Lorsque le moment est venu de mettre les dispositifs hors service ou de les remplacer, AXIS Device Manager facilite une mise hors service sécurisée en effaçant les données sensibles et en rétablissant les paramètres d'usine. Ainsi, aucune information confidentielle ne reste sur le périphérique, ce qui protège les données de l'utilisateur et empêche tout accès non autorisé.

AXIS Device Manager

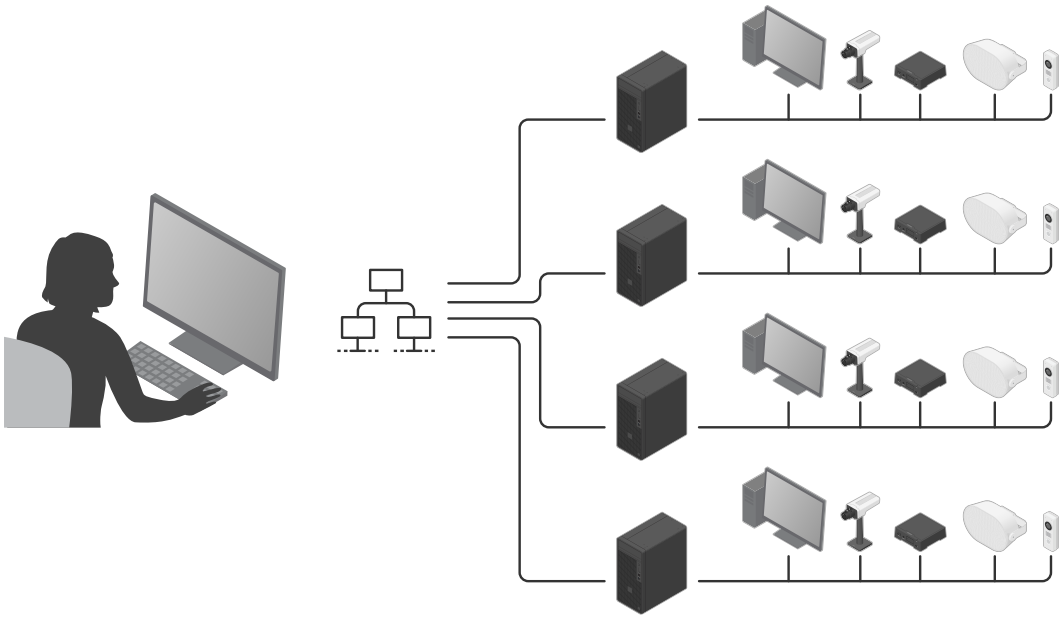
AXIS Device Manager est un outil local qui offre une solution à la fois simple, rentable et cybersécurisée pour gérer toutes les tâches majeures d'installation, de sécurité et de maintenance (voir le tableau ci-dessous). L'outil est adapté à la gestion de quelques milliers de dispositifs Axis sur un site unique, ou de plusieurs milliers de dispositifs répartis sur plusieurs sites. AXIS Device Manager permet de déployer efficacement des contrôles de cybersécurité afin de protéger vos dispositifs réseau et de les aligner sur une infrastructure de sécurité.

Fonctions de gestion des périphériques, AXIS Device Manager

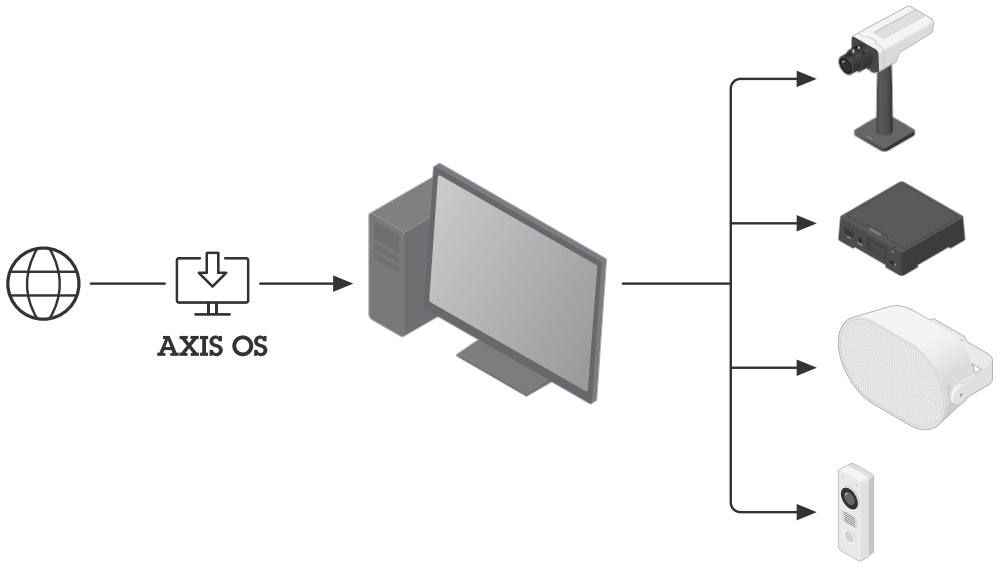
Installation	Maintenance
Attribution d'une adresse IP	Statut des appareils
Export de la liste des périphériques et suivi des biens*	Collecte des données des appareils
Gestion des utilisateurs et des mots de passe*	Configuration des appareils et copie des configurations sur plusieurs appareils
Gestion ACAP	Connexion à plusieurs serveurs/systèmes
Mise à niveau d'AXIS OS, basée sur LTS ou Active*.	Points de restauration
Gestion des certificats HTTPS*	Rétablissement des paramètres par défaut

Gérer les certificats IEEE 802.1*/**	Remplacer un ou plusieurs dispositif(s)
Étiquetage des appareils	Renouvellement et gestion des certificats*
	Renforcement de la cybersécurité*

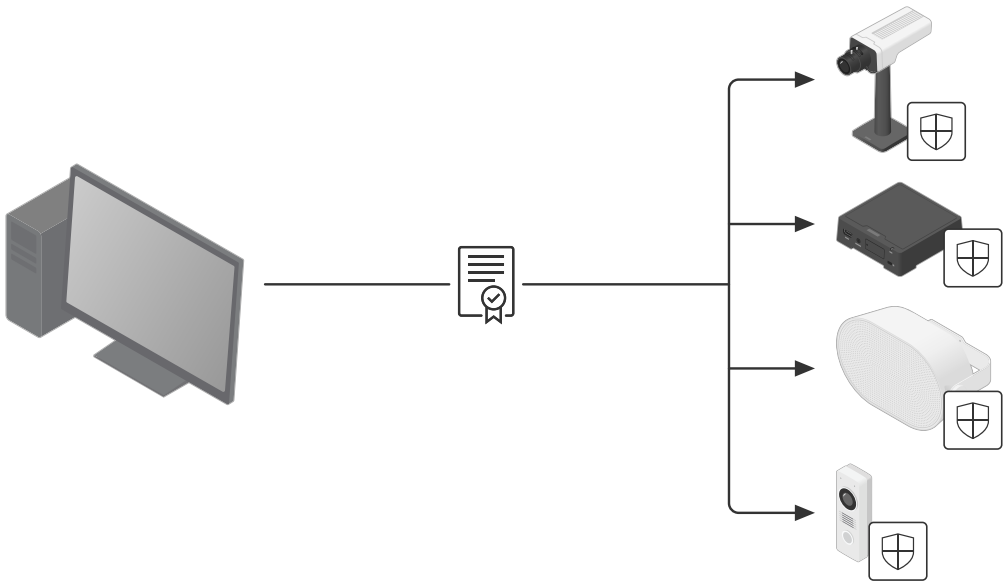
* Indique la fonction de contrôle de la cybersécurité.
** Active Directory Certificate Services (Services de certificats Active Directory) n'est pas pris en charge actuellement. Validé pour FreeRADIUS fonctionnant sous Linux.



Gestion multisite.



AXIS OS upgrade (Mise à niveau d'AXIS OS).



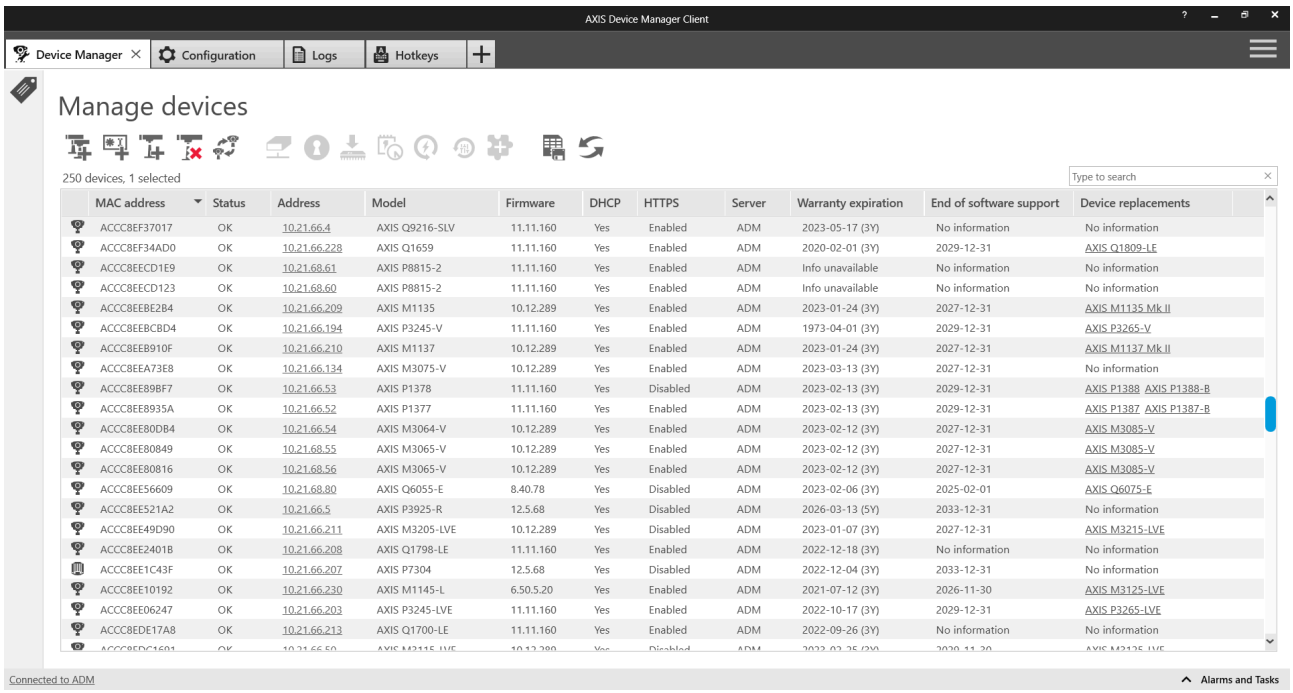
Gestion des certificats

Inventaire des périphériques

Un aspect fondamental de la sécurité d'un réseau d'entreprise consiste à maintenir un inventaire exhaustif des dispositifs résidant sur le réseau. Lors de l'élaboration ou de la révision d'une politique de sécurité globale, il est important de disposer d'une connaissance précise et d'une documentation claire pour chaque dispositif — et pas seulement pour les actifs critiques. La raison en est simple : tout dispositif ignoré peut constituer un point d'entrée pour des personnes malveillantes. Vous ne pouvez pas protéger les dispositifs que vous ignorez ou dont vous n'avez pas pleinement connaissance.

L'inventaire des dispositifs est une étape essentielle de la sécurité d'un réseau d'entreprise. AXIS Device Manager peut vous aider à cet égard car 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 une liste complète de vos dispositifs, qui peuvent être triés par numéro total, type, numéros de modèle, etc.
- Vous renseigne sur l'état de chaque dispositif du réseau.
- Vous aide à planifier en amont, en indiquant la date prévue pour la fin de la prise en charge du logiciel du dispositif et en répertoriant le ou les produit(s) plus récent(s) qui peuvent être utilisés en remplacement.



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

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

AXIS Device Manager fournit un moyen automatisé d'accéder à un inventaire en temps réel des dispositifs réseau Axis. Il vous permet d'identifier, de répertorier et de trier vos périphériques automatiquement. Tout aussi important, il vous permet d'utiliser des balises pour regrouper et trier les dispositifs en fonction de vos propres critères, ce qui facilite l'obtention d'un aperçu et d'une documentation sur tous les dispositifs Axis de votre réseau.

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 d'une politique contribue, à terme, à réduire les risques d'usages abusifs accidentels ou délibérés. Faire respecter l'utilisation de mots de passe robustes est une tâche essentielle, mais il faut aussi réduire le risque de compromission des mots de passe. Les mots de passe des dispositifs se propagent souvent au sein d'une société, et lorsque c'est le cas, vous perdez le contrôle sur les personnes qui y ont accès. AXIS Device Manager vous aide à gérer facilement plusieurs comptes et mots de passe pour les dispositifs Axis.

Raisons pour lesquelles il est vivement conseillé d'avoir plusieurs comptes utilisateur au niveau des dispositifs :

- Vous contrôlez les niveaux de privilège pour divers types d'utilisateur (machines et personnes).
- Vous réduisez le risque de compromission du mot de passe racine (principal).
- Vous pouvez réinitialiser les informations d'identification pour un type d'utilisateur unique sans répercussion sur les autres.

Utilisation des privilèges dans AXIS Device Manager

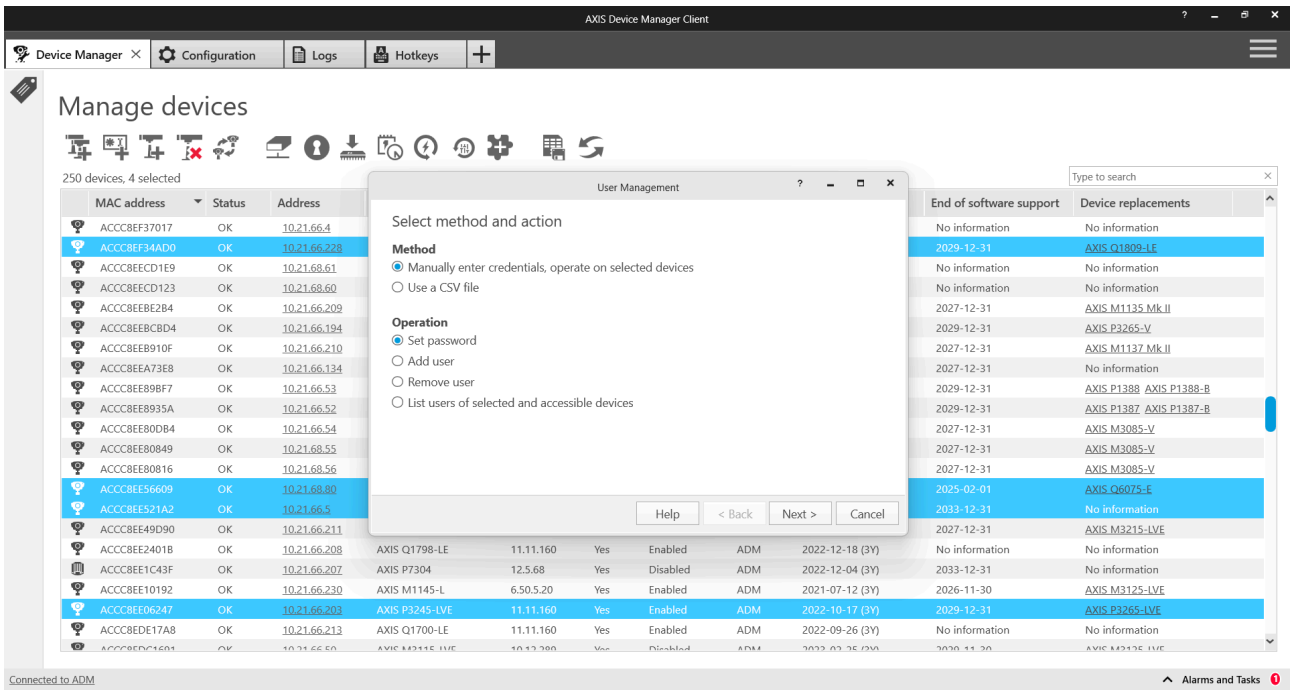
Les dispositifs Axis prennent en charge plusieurs comptes, chaque compte disposant de l'un des trois niveaux de privilèges suivants :

- **Viewers (Visionneurs)** : Ces utilisateurs ont accès à la vidéo et à la commande PTZ.
- **Operators (Opérateurs)** : Les utilisateurs bénéficiant de droits en tant qu'opérateurs peuvent optimiser les paramètres de la caméra et les profils de flux de données vidéo.
- **Administrateurs** : Les administrateurs peuvent administrer les comptes, modifier les paramètres réseau et contrôler le nombre de services au niveau du dispositif.

Chaque rôle qui accède à la caméra doit être associé à son propre compte. Par exemple, vous pouvez configurer le rôle « Personnel de la salle de contrôle » avec le niveau de privilèges « opérateur », alors que le rôle « Personnel de patrouille » n'a besoin que du niveau de privilèges « observateur ».

Mesures recommandées

- Avant d'ajouter des caméras au serveur VMS – 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 de privilèges Opérateur ou Administrateur (vérifiez auprès du fabricant).
- Ajoutez les dispositifs au serveur VMS à l'aide du compte et du mot de passe que vous avez créés.
- Retour à AXIS Device Manager – sélectionnez à 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 peut être divulgué qu'à un nombre limité de personnes (celles qui utilisent AXIS Device Manager).
- Lorsqu'une personne doit utiliser un navigateur Web pour accéder à un dispositif afin d'exécuter des tâches de maintenance ou de dépannage, ne lui communiquez **pas** le mot de passe racine. Au lieu de cela, utilisez AXIS Device Manager afin de créer un nouveau compte (temporaire) pour le(s) dispositif(s) sélectionné(s), avec privilèges en tant qu'opérateur ou administrateur. Une fois le travail terminé, 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. Nous recommandons d'utiliser des utilisateurs de domaine si la personne chargée de la maintenance du système utilisera des clients distants.



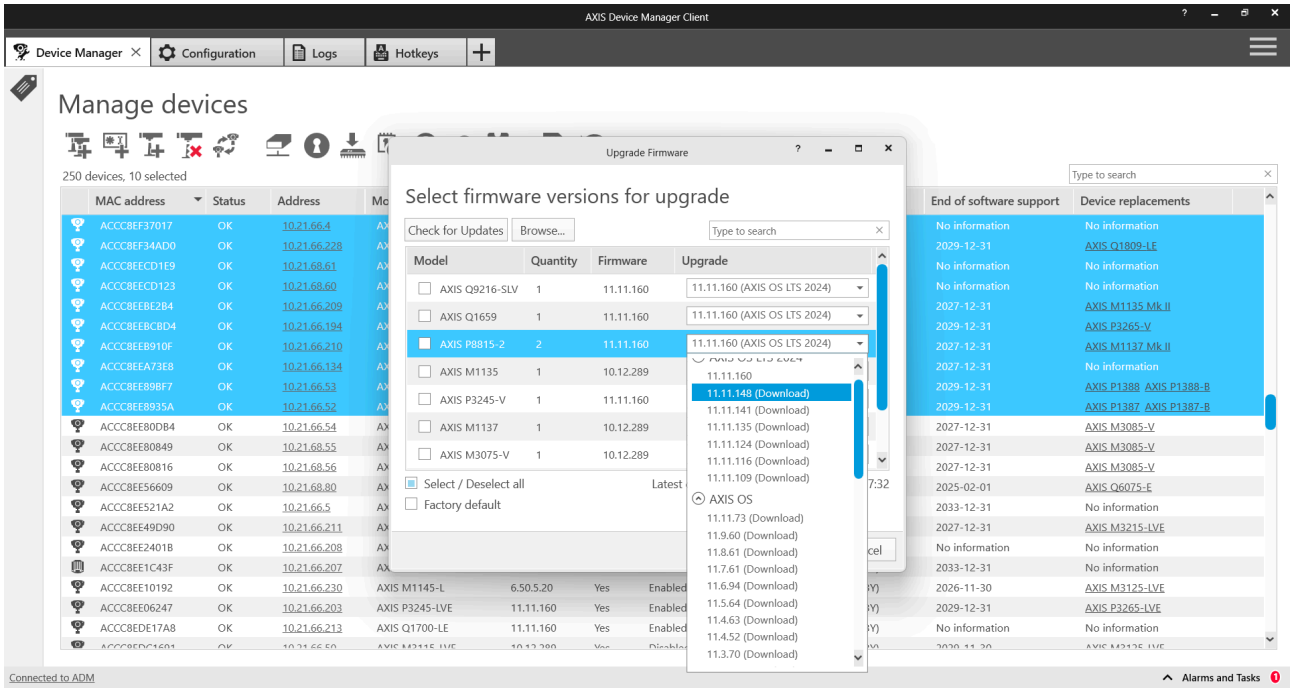
Modification des mots de passe et des rôles utilisateur dans AXIS Device Manager.

Mises à niveau d'AXIS OS

Les versions d'AXIS OS actualisées incluent des correctifs pour les vulnérabilités connues. Il est indispensable de toujours utiliser les logiciels les plus récents car des personnes malveillantes peuvent essayer d'exploiter les vulnérabilités connues. Tout aussi important, le déploiement rapide d'une nouvelle version d'AXIS OS renforce les capacités opérationnelles et élimine les goulets d'étranglement liés au déploiement manuel de nouvelles mises à niveau de versions. AXIS Device Manager se connecte à www.axis.com et télécharge les dernières versions d'AXIS OS ou de service applicables. 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 nouvelles versions d'AXIS OS sont disponibles et vous permet de les déployer rapidement sur les dispositifs Axis.

Raisons pour lesquelles il est vivement recommandé d'exécuter les versions d'AXIS OS les plus récentes :

- Votre réseau et vos dispositifs sont protégés grâce aux derniers correctifs appliqués contre les vulnérabilités connues, en particulier les plus critiques.
- Vos dispositifs sont mis à jour avec les dernières améliorations de performance, ainsi que des correctifs d'erreurs et autres failles.
- Vous bénéficiez d'un accès immédiat aux fonctionnalités et améliorations les plus récentes.



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

Sécurisation complémentaire

L'application d'une bonne politique en matière d'utilisateurs et de mots de passe, ainsi que l'utilisation de versions d'AXIS OS actualisées, permettent d'atténuer les risques habituels liés aux dispositifs. Le *Guide de renforcement AXIS* décrit des mesures supplémentaires visant à réduire les risques au sein des sociétés de grande taille et critiques. Il s'agit notamment de désactiver les services susceptibles de ne pas être utilisés et d'activer les services qui peuvent aider à détecter et à surveiller les signes d'une attaque ou d'une violation. 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.

Comment renforcer les dispositifs selon le Guide de renforcement Axis :

- Lisez le *Guide de renforcement AXIS* et téléchargez le fichier type à la fin du document.
- Modifiez le fichier de configuration en sélectionnant des éléments pertinents.
- Sélectionnez les dispositifs dans l'inventaire d'AXIS Device Manager.
- Cliquez avec le bouton droit et sélectionnez « Configure Devices > Configure… » (Configurer les dispositifs > Configurer...).
- Cliquez sur Fichier de configuration et sélectionnez le fichier téléchargé.
- Réglez les paramètres au besoin.

Service d'autorité de certification (CA)

Une autorité de certification (CA) est un service qui délivre des certificats numériques à des 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) délivre des certificats pour des services réseaux privés/internes. Dans un système de gestion vidéo, il s'agit principalement du cryptage réseau HTTPS et du contrôle d'accès réseau IEEE 802.1x. AXIS Device Manager inclut un service CA pour dispositifs Axis et peut fonctionner comme CA racine privée ou comme CA intermédiaire privée, dans le cadre d'une infrastructure à clé publique (PKI) d'entreprise.

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

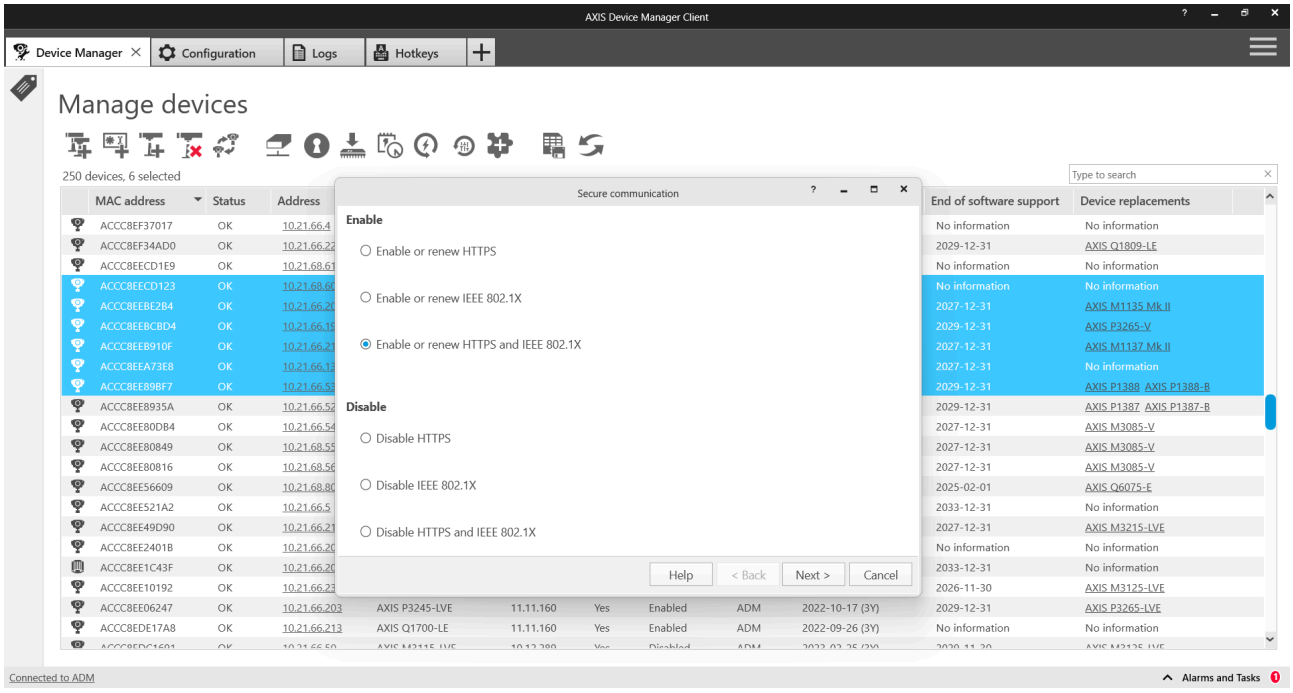
HTTPS

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 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 l'usurpation d'identité sur le réseau, dans le cadre de laquelle un ordinateur malveillant tente de se faire passer pour un serveur légitime. Les certificats signés par une autorité de certification (CA) ajoutent un point de confiance permettant aux clients de vérifier qu'ils accèdent bien à un dispositif de confiance. 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.

IEEE 802.1X

Connue simplement sous l'appellation 802.1X, cette norme empêche les périphériques réseau non autorisés d'accéder au réseau local. Un périphérique doit s'authentifier pour pouvoir accéder au réseau (et à ses ressources). Différentes méthodes d'authentification peuvent être utilisées : adresse MAC (filtrage MAC), utilisateur/mot de passe ou certificat client. Le responsable du système choisit la méthode à utiliser ; ce choix dépend des menaces, des risques et des coûts.

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.

Gestion du cycle de vie des certificats

La gestion du cycle de vie des certificats est un moyen de gérer de manière rentable tous les processus et toutes les tâches liés à l'émission, à l'installation, à l'inspection, à la remédiation et au renouvellement des certificats au fil du temps. AXIS Device Manager permet de gérer efficacement les certificats en faisant en sorte que les administrateurs puissent :

- Émettre des certificats signés par une autorité de certification lorsqu'aucune autre autorité de certification n'est disponible
- Gérer facilement les certificats IEEE 802.1X
- Gérer facilement les certificats HTTPS
- Contrôler les dates d'expiration des certificats
- Renouveler facilement les certificats avant expiration

Recommandations pour les autorités de certification racine et intermédiaires privées

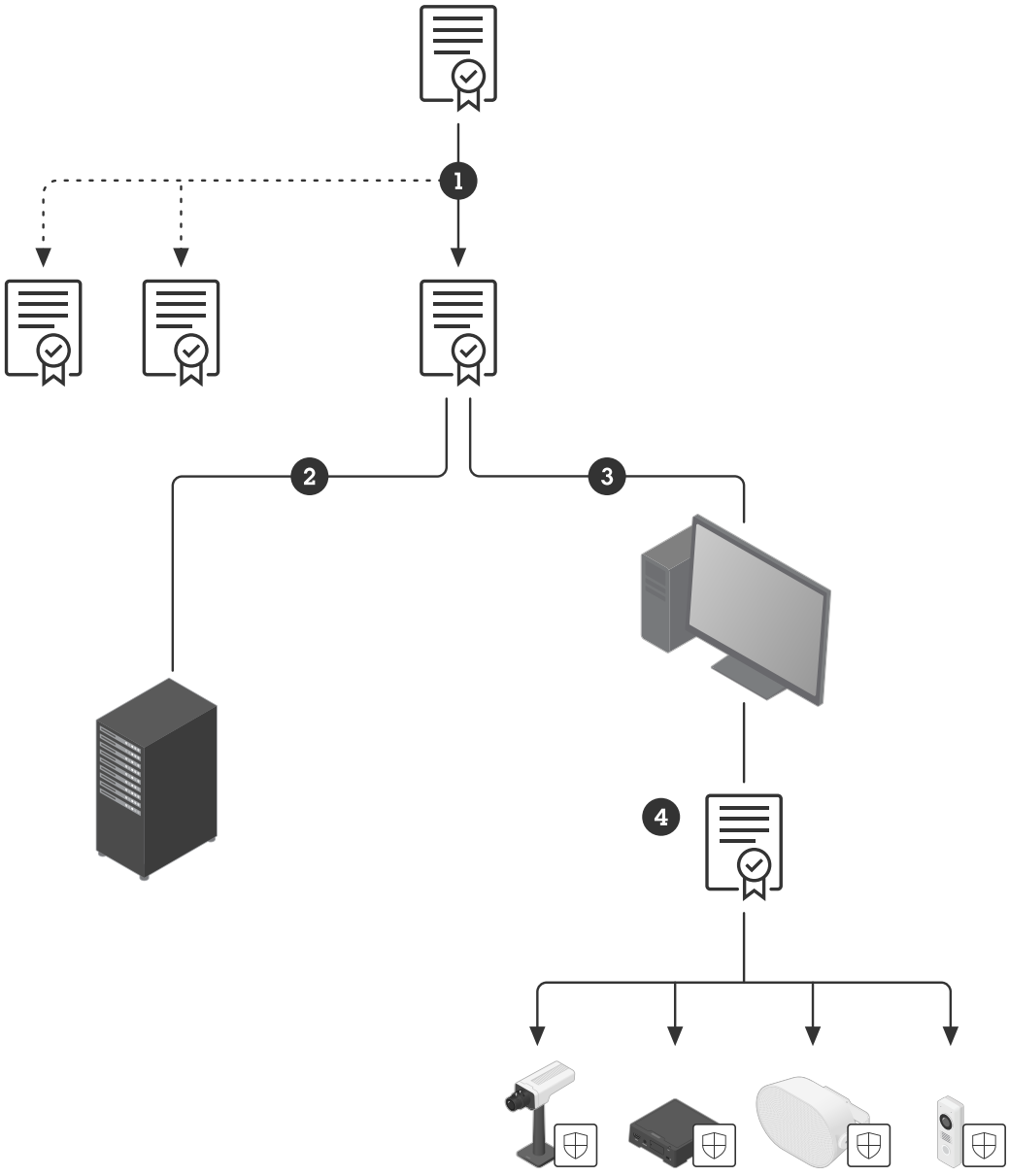
Il n'est pas conseillé d'exposer les périphériques Axis en tant que serveurs publics pour le public. Utiliser une autorité de certification publique pour des ressources privées n'est donc pas rentable.

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 cette situation, l'intégration des certificats serveur des caméras dans une infrastructure à clé publique (PKI) d'entreprise existante présente un intérêt limité.

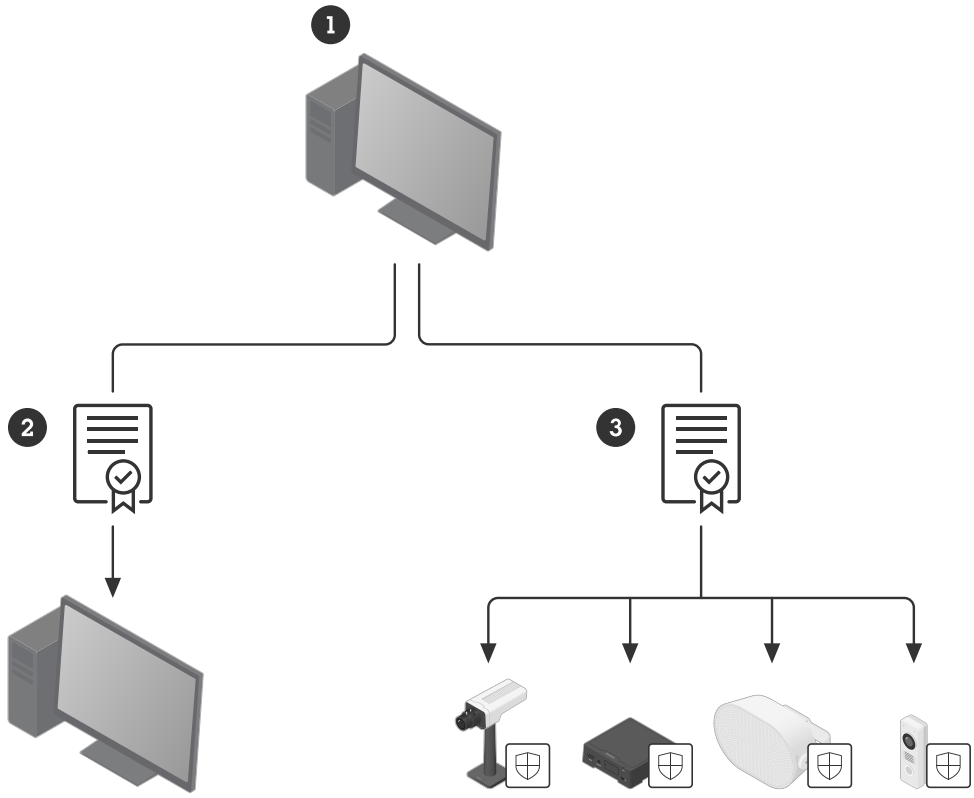
Utiliser AXIS Device Manager en tant que CA privée s'avère être la solution la plus rentable. Dès qu'un certificat CA racine est généré, installez le certificat AXIS Device Manager dans le magasin de certificats du serveur VMS. Si d'autres clients accèdent directement aux caméras (pour la maintenance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

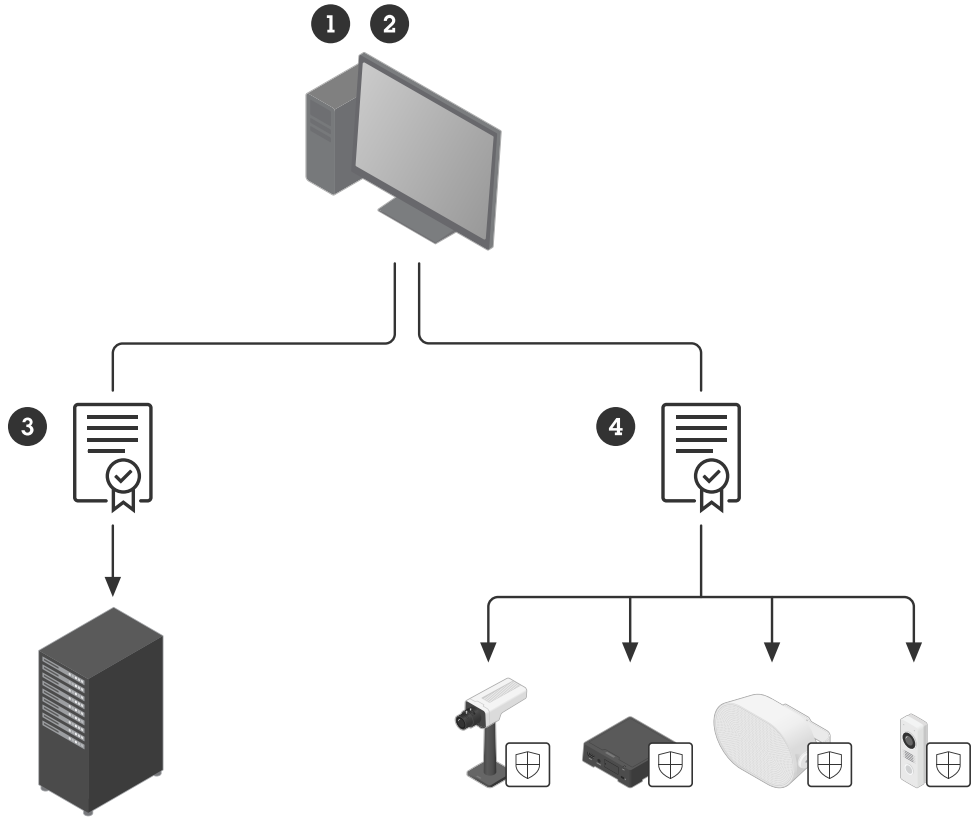
Pour obtenir de l'aide sur la configuration d'un serveur FreeRADIUS, veuillez consulter la *section Technical papers* pour AXIS Device Manager.



La gestion de certificats HTTPS implique : 1) la production d'un certificat CA intermédiaire ou racine dans AXIS Device Manager; 2) l'exportation d'un certificat CA vers le serveur VMS, et 3) le chargement des certificats du serveur sur les dispositifs.



Utilisation d'une autorité de certification privée, la gestion des certificats IEEE 802.1X implique : 1) la production d'un certificat CA intermédiaire et d'un certificat client ; 2) l'installation d'un certificat CA sur le serveur Radius, 3) l'importation d'un certificat CA dans AXIS Device Manager et 4) le chargement des certificats CA et client sur les dispositifs.



Utilisation d'AXIS Device Manager comme autorité de certification. Pour gérer les certificats IEEE 802.1X : 1) générez le certificat CA racine dans AXIS Device Manager ; 2) importez le certificat CA d'authentification dans AXIS Device Manager ; 3) installez le certificat CA sur le serveur Radius ; 4) chargez le certificat CA d'authentification et le certificat client sur les dispositifs.

Conclusion

La gestion et le contrôle de la sécurité sont primordiaux lorsque l'on souhaite mettre en œuvre une cybersécurité efficace. Chacun de ces aspects est un processus continu qui exige de maintenir une visibilité claire de l'état des dispositifs et de suivre les actions appropriées pour atténuer toute menace potentielle pouvant affecter votre réseau IP. AXIS Device Manager vous offre un outil pour gérer vos dispositifs tout en améliorant 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.

T10231485_fr

2025-09 (M4.2)