

AXIS Device Manager

Table des matières

À propos d'AXIS Device Manager	3
Vue d'ensemble de la solution	4
Conditions préalables	5
MISE EN ROUTE	6
Installez le logiciel.....	6
Connecter à un serveur.....	6
Connectez-vous à plusieurs serveurs	6
Configuration initiale	7
Gérer les périphériques	8
Ajout de périphériques.....	8
Supprimer les périphériques	8
Remplacez des périphériques.....	8
Restaurer les dispositifs	8
Configuration.....	10
Créer un point de restauration.....	10
Créer des points de restauration automatique.....	10
Gérez plusieurs identifiants.....	10
Installer les certificats	11
À propos des certificats	11
Créez une autorité de certification (CA)	11
Activer HTTPS.....	12
Activer 802.1X	12
Gérez les comptes SIP.....	13
Gérer les logiciels des dispositifs.....	14
Mises à niveau d'AXIS OS	14
Recherche de panne.....	15
Contacter l'assistance.....	15
Processus d'escalade.....	15

À propos d'AXIS Device Manager

AXIS Device Manager est une application logicielle d'installation et de gestion de produits Axis. Le logiciel peut rechercher automatiquement des périphériques sur le réseau, attribuer des adresses IP, définir des mots de passe, afficher le statut de connexion, gérer les mises à niveau du firmware, les certificats et la configuration de plusieurs périphériques.

AXIS Device Manager comprend :

- AXIS Device Manager Service Control - le serveur qui gère toutes les communications avec les produits Axis.
- AXIS Device Manager Client - l'interface utilisateur frontale qui active la gestion à distance à partir d'internet ou du réseau d'entreprise.

Plusieurs clients peuvent être connectés au même serveur. Un client peut être connecté à plusieurs serveurs simultanément.

AXIS Device Manager est également très utile pour renforcer votre système et accroître la sécurité. Pour plus d'informations, voir le *AXIS Device Manager Security Guide*.

Vue d'ensemble de la solution

Conditions préalables

Systèmes d'exploitation compatibles :

Nécessaire : système d'exploitation 64 octets Microsoft .NET version 4.8

Systèmes d'exploitation pris en charge : Windows 10 Pro, Windows 11 Pro, Windows Server 2016, Windows Server 2019, Windows Server 2022

Recommandations: Packs de services OS les plus récents.

Recommandation système minimum :

- Minimum (jusqu'à 500 périphériques) : Intel core i5 ou équivalent, 4 Go de RAM, 100 Mo/s sur l'ensemble de l'infrastructure réseau
- Recommandé (entre 500 et 2000 périphériques) : Intel core i7 ou équivalent, 8 Go de RAM, 100 Mo/s sur l'ensemble de l'infrastructure réseau
- Il n'est pas recommandé d'utiliser plus de 2 000 périphériques par serveur.
- Assurez-vous que les périphériques Axis exécutent la dernière version d'AXIS OS disponible.

Remarque

Nous prenons toujours en charge les deux versions précédant la mise à jour la plus récente. Consultez les notes de mises à jour les plus récentes pour connaître les versions spécifiques prises en charge.

Périphériques pris en charge :

Produits AXIS avec AXIS OS version 4.40 ou supérieure. (Remarquez que la fonctionnalité exacte prise en charge varie en fonction du modèle de produit et du firmware)

Langues :

IU + fichiers d'aide : Anglais, Français, Allemand, Italien

IU uniquement : Arabe, Tchèque, Chinois (simplifié), Chinois (traditionnel), Néerlandais, Finlandais, Japonais, Coréen, Perse, Polonais, Portugais (Brésil), Russe, Espagnol, Suédois, Thaï, Turc et Vietnamien.

MISE EN ROUTE

Installez le logiciel

Pour installer AXIS Device Manager 5, assurez-vous que vous disposez des droits d'administrateur complets sur l'ordinateur sur lequel vous effectuez l'installation, puis procédez comme suit :

1. Allez à la page du produit sur axis.com et téléchargez l'application de bureau d'AXIS Device Manager
2. Exécutez le programme d'installation et suivez les instructions qui s'affichent à l'écran.

Remarque

S'il n'est pas déjà installé, le cadre Microsoft .NET 4.8 sera installé (inclus dans le fichier d'installation). Cela prendra quelques minutes. Le cadre Microsoft .NET 4.8 peut également être installé via Windows Update avant l'installation d'AXIS Device Manager.

Connecter à un serveur

Lorsque vous démarrez AXIS Device Manager pour la première fois, vous serez invité(e) à vous connecter à un serveur. Le serveur peut être exécuté sur la machine locale ou sur un serveur distant.

Pour vous connecter en tant qu'utilisateur local de Windows :

1. Sélectionnez **This computer (Cet ordinateur)**.
2. Cochez **Log on as current user (Se connecter en tant qu'utilisateur actuel)** pour vous connecter à l'aide de vos identifiants actuels.

Pour vous connecter en tant qu'autre utilisateur sur le serveur ou le domaine :

- Sélectionnez **Other user (Autre utilisateur)**.
- Sous **Other user (Autre utilisateur)**, saisissez les identifiants de ce compte.
- Cochez **Remember me (Se souvenir de moi)** pour sauter cette étape lors de la prochaine exécution du client.
- Cliquez sur **Log on (Connexion)**.

Remarque

Pour effacer les identifiants sauvegardés pour tous les serveurs, allez à l'écran de connexion et sélectionnez **Delete saved passwords (Supprimer les mots de passe sauvegardés)**.

Pour vous connecter à un serveur distant :

1. Sélectionnez **Serveur distant**.
2. Sélectionnez un serveur dans la liste déroulante ou saisissez l'adresse IP ou DNS dans le champ.
3. Saisissez vos identifiants
4. Cliquez sur **Log on (Connexion)**.

Remarque

Cette option ne permet pas de se connecter à un serveur distant à partir d'un ordinateur n'appartenant pas à un domaine Windows.

Connectez-vous à plusieurs serveurs

Vous pouvez vous connecter à plusieurs serveurs avec AXIS Device Manager. Une fois que vous vous êtes connecté à un serveur, vous pouvez passer d'un serveur à l'autre dans le menu principal.

1. Allez au menu principal > Servers (Serveurs) > New connection (Nouvelle connexion)
2. Choisissez de vous connecter à votre ordinateur ou à un serveur distant comme décrit ci-dessus.

Configuration initiale

Pour commencer, vous devez procéder comme suit :

- Ajoutez des périphériques et créez des comptes utilisateurs, consultez :
- Renforcez la cybersécurité de votre système. Cf.

Gérer les périphériques

Ajout de périphériques

AXIS Device Manager recherche automatiquement les périphériques connectés au réseau, et tente de se connecter à tous les périphériques. La liste des dispositifs trouvés indique l'adresse du dispositif (adresse IP ou nom d'hôte), son numéro de série, son modèle et son statut. Le numéro de série est imprimé sur l'étiquette du produit.

Pour ajouter des périphériques à partir de la liste :

1. Sélectionnez les périphériques à ajouter et cliquez sur **Next (Suivant)**.
2. Sélectionnez **Use host name when possible (Utiliser le nom d'hôte si possible)**. Si un périphérique est ajouté en utilisant son nom d'hôte, celui-ci sera utilisé pour toutes les communications avec ce périphérique. Si un nom d'hôte n'est pas disponible, l'adresse IP sera utilisée.
3. Paramétrez un mot de passe pour les périphériques sans mot de passe. Si un mot de passe n'est pas nécessaire, sélectionnez **Skip (Passer)**.
4. Cliquez sur **Next (Suivant)**.

La page "Prêt à ajouter des périphériques" affiche les dispositifs à ajouter.

5. Cliquez sur **Finish (Terminer)** pour ajouter les périphériques.

Supprimer les périphériques

Pour supprimer des périphériques dans la liste :

1. Allez à **Device management (Gestion des périphériques)**.
2. Sélectionnez les périphériques.
3. Faites un clic droit et sélectionnez **Remove (Supprimer)**.
4. Cliquez sur **Yes (Oui)**.

Remplacez des périphériques

Pour remplacer un périphérique dans AXIS Device Manager, connectez un nouveau périphérique et réutilisez la configuration du périphérique actuel. Si l'opération réussit, le dispositif remplacé sera supprimé. Un périphérique doit comporter au moins un point de restauration. Reportez-vous à . Aucun point de restauration ne sera programmé sur le nouveau dispositif.

1. Allez à **Device management (Gestion des périphériques)**.
2. Allez à la barre d'outils et cliquez sur l'icône de remplacement du périphérique.
3. Sélectionnez un périphérique à remplacer et cliquez sur **OK**.
4. Sélectionnez le périphérique par lequel vous souhaitez le remplacer et cliquez sur **OK**.
5. Cliquez sur **Suivant** pour récupérer la configuration d'un périphérique à partir du dernier point de restauration.
6. Allez à **Parameters (Paramètres) > Additional Settings (Réglages supplémentaires)** et sélectionnez les paramètres et réglages à appliquer.
7. Cliquez sur **Next (Suivant)**.
8. Cliquez sur **Terminer** pour appliquer vos paramètres.

Restaurer les dispositifs

Il est possible de restaurer un ou plusieurs dispositifs à partir de points de restauration précédemment créés. Pour être restauré, un périphérique doit comporter au moins un point de restauration. Par défaut, des points de restauration automatique sont créés et supprimés chaque nuit pour tous les périphériques du serveur.

sélectionné. Un nombre défini des derniers points de restauration automatique est conservé à des fins de restauration.

Restaurer les dispositifs à partir d'un point de restauration :

1. Allez à l'espace de travail **Device management (Gestion des périphériques)**.
2. Sélectionnez le ou les dispositifs à restaurer.
3. Cliquez avec le bouton droit de la souris et sélectionnez **Backup/Restore (Sauvegarder/Restaurer) > Restore to a Previous Time (Restaurer à une date antérieure)** dans le menu déroulant.
4. Sélectionnez un point de restauration dans la liste des points de restauration les plus récents, et cliquez sur **Suivant**.
5. Vérifiez les paramètres de chaque périphérique et cliquez sur **Terminer**.

Configuration

Créer un point de restauration

Pour créer un point de restauration manuelle :

- Allez à l'espace de travail **Device management (Gestion des périphériques)**.
- Sélectionnez le ou les dispositifs à restaurer.
- Cliquez-droit et sélectionnez **Sauvegarder/Restaurer > Créer des points de restauration**.
- Tapez une description qui identifie le point de restauration.
- Cliquez sur **OK**.

Remarque

il est impossible de supprimer automatiquement des points de restauration créés manuellement.

Créer des points de restauration automatique

Si vous avez plus d'un serveur, sélectionnez le serveur à configurer, dans la liste de serveurs.

- Allez à **Options > Paramètres du point de restauration**.
- Sélectionnez **Créer automatiquement des points de restauration** afin d'activer la création automatique de points de restauration.
- Entrez le nombre de points de restauration automatique à enregistrer, et cliquez sur **OK**.

Gérez plusieurs identifiants

Cette fonctionnalité fournit à AXIS Device Manager les identifiants pour un compte administrateur des périphériques.

Tapez manuellement les identifiants des périphériques

Si vous choisissez de saisir manuellement les identifiants des périphériques, les identifiants seront mis à jour dans AXIS Device Manager pour les périphériques sélectionnés.

- Sélectionnez un ou plusieurs périphériques.
- Cliquez avec le bouton droit de la souris et sélectionnez **Advanced (Avancés) -> Enter Device Credentials (Saisir les identifiants des périphériques)** dans le menu déroulant.

Remarque

Les identifiants dont on ne peut vérifier qu'ils fonctionnent pour le périphérique ne seront pas mis à jour. Le même mot de passe et le même nom d'utilisateur doivent être utilisés pour tous les périphériques participant à une telle opération.

Utilisez un fichier CSV pour différents identifiants

En utilisant un fichier CSV, vous pouvez utiliser des mots de passe et des noms d'utilisateur distincts pour chaque périphérique. L'adresse MAC, l'adresse IP ou l'adresse de l'hôte est utilisée pour associer les lignes du fichier CSV aux périphériques correspondants dans la base de données d'Axis Device Manager.

Lors de l'utilisation d'un fichier CSV, l'interface utilisateur vous demande de spécifier comment interpréter les colonnes du fichier CSV.

Remarque

Comment spécifier à quel périphérique appartient une ligne du fichier CSV.

Une colonne du fichier CSV doit contenir soit des adresses MAC, soit des adresses IP, soit des adresses d'hôtes. Il faut donc spécifier si une colonne du fichier CSV doit être interprétée comme une adresse MAC, une adresse IP ou une adresse d'hôtes. C'est nécessaire pour spécifier à quel périphérique appartiennent les données d'une ligne du fichier CSV. En outre, une colonne peut être spécifiée pour être interprétée comme nom de serveur. Il est ainsi possible de distinguer les lignes du fichier CSV qui concernent des périphériques situés sur des serveurs Axis Device Manager différents, mais ayant la même adresse IP ou la même adresse

d'hôte. Si une telle distinction n'est pas nécessaire, il n'est pas utile de disposer d'une colonne à interpréter comme nom de serveur. Dans une configuration où un serveur utilise la même adresse IP ou adresse d'hôte pour plusieurs périphériques, mais utilise des ports pour les distinguer les uns des autres, une colonne peut être spécifiée pour être interprétée comme Port. Si aucune distinction sur le port n'est nécessaire, il n'y a généralement aucune raison d'interpréter une colonne comme Port. Une option pour fournir le port à une colonne dédiée est d'indiquer le port avec l'adresse IP ou l'adresse de l'hôte. L'adresse IP ou l'adresse de l'hôte doit ensuite être suivie de deux points et du numéro de port.

Installer les certificats

À propos des certificats

AXIS Device Manager propose les paramètres pour gérer les certificats serveur/client. Les certificats client sont utilisés pour IEEE 802.1X et les certificats serveur sont utilisés pour HTTPS. Pour changer quoi que ce soit, sélectionnez les périphériques appropriés dans la gestion des périphériques, puis sélectionnez Activer/mettre à jour dans le menu contextuel.

Créez une autorité de certification (CA)

Une autorité de certification vous autorise à activer HTTPS et IEEE 802.1X sur des périphériques sans aucun certificat serveur/client en place. L'autorité de certification indique aux périphériques de créer des certificats à l'aide de leurs propres clés privées, de les signer et de les installer

Pour créer une autorité de certification :

- Allez à l'onglet **Configuration**.
- Allez à **Security (Sécurité) > Certificates (Certificats)**
- Sous **Certificate authority (Autorité de certification)**, cliquez sur **Generate... (Générer...)**
- Tapez une phrase de passe et confirmez-la.
- Cliquez sur **OK**.

L'autorité de certification sera maintenant générée et prête à l'emploi.

Remarque

Votre certificat racine auto-signé et votre clé privée qui est protégée par une phrase de passe de votre choix. Un certificat généré par AXIS Device Manager a une durée de vie de 3 ans. Si vous souhaitez que AXIS Device Manager renouvelle automatiquement les certificats serveur/client, vous devez cocher la case intitulée **Remember passphrase (Se souvenir de la phrase de passe)**. Si une autorité de certification n'est pas configurée, vous devrez créer des certificats serveur/client en dehors de AXIS Device Manager. Vous perdrez alors les avantages de la gestion automatique des certificats.

Importer : en utilisant la fonction Importer, vous pouvez importer une CA existante composée d'un certificat public et d'une clé privée. Il vous faudra indiquer une phrase secrète.

Enregistrer dans un fichier : enregistrer le certificat public de l'autorité de certification aux formats .cer ou .crt. Le fichier ne contient pas de clé privée et ne doit donc pas être crypté.

Sauvegarder : une sauvegarde d'une CA est recommandée en cas de panne matérielle. Si cette option est sélectionnée, une sauvegarde du certificat et de la clé publique de la CA utilisés par Axis Device Manager sera réalisée. Les données sauvegardées seront protégées par la phrase secrète utilisée pour générer la CA.

Avertissement d'expiration de certificat Une notification système sera créée si un certificat a expiré ou est sur le point d'expirer. Cela s'applique à tous les certificats installés sur des périphériques connectés, sauf pour les CA installées en dehors de AXIS Device Manager. L'avertissement apparaît comme une alarme système, dans la colonne statut du gestionnaire de périphériques, sous forme d'icônes dans la boîte de dialogue « Afficher les certificats installés », et dans l'espace de travail Configuration.

Précisez à quel moment vous souhaitez que AXIS Device Manager vous notifie quand les certificats approchent de leur date d'expiration. Par défaut, le serveur et les certificats clients générés par AXIS Device Manager seront automatiquement renouvelés sept jours avant que l'avertissement d'expiration n'apparaisse. Pour recevoir une notification du moment auquel la CA doit expirer, la case « Se souvenir de la phrase secrète » doit être cochée.

Activer HTTPS

Pour activer HTTPS, un certificat de serveur doit être présent sur chaque périphérique. AXIS Device Manager peut utiliser une autorité de certification (CA) pour signer et installer des certificats de serveur pour les périphériques.

Vous pouvez aussi le faire manuellement :

1. Allez à l'onglet **Device manager (Gestionnaire de périphériques)**
2. Cliquez avec le bouton droit sur les périphériques et choisissez **Install server certificates (Installer les certificats de serveur)** pour chaque périphérique dans le menu contextuel.

Il ne peut y avoir qu'un seul certificat de serveur présent sur chaque périphérique avant d'activer HTTPS. Les certificats excédentaires peuvent être supprimés à partir du menu contextuel.

3. Après avoir installé les certificats, vous pouvez activer HTTPS dans le menu contextuel.

Remarque

Une connexion peut être réalisée à l'aide de HTTP si une connexion sécurisée (HTTPS) n'est pas disponible. Cela afin de pouvoir configurer les périphériques qui ne sont pas encore sécurisés.

Ignorer la validation du certificat

AXIS Device Manager ne se connectera pas à un périphérique si son certificat n'est pas validé. Le certificat serveur doit être signé par la CA active dans AXIS Device Manager ou validé via le magasin de certificats Windows. En sélectionnant Ignorer la validation du certificat, AXIS Device Manager ne validera pas si le certificat envoyé par le périphérique est fiable ou non.

Pour qu'AXIS Device Manager ignore la validation du certificat.

- Allez à l'onglet **Configuration**.
- Sous **HTTPS**, activez **Ignore certificate validation (Ignorer la validation du certificat)**.

Activer 802.1X

Pour activer IEEE 802.1X, un certificat client doit être présent sur chaque périphérique. AXIS Device Manager peut utiliser une autorité de certification (CA) pour signer et installer des certificats clients serveur pour les périphériques.

Vous pouvez également procéder manuellement dans Gestion des périphériques avec un clic droit sur les périphériques et en choisissant d'installer des certificats clients pour chaque périphérique dans le menu contextuel. Il ne peut y avoir qu'un seul certificat client présent sur chaque périphérique avant d'activer IEEE 802.1X. Les certificats excédentaires peuvent être supprimés à partir du menu contextuel. Après avoir installé les certificats, vous pouvez activer IEEE 802.1X dans le menu contextuel.

Vous avez également besoin d'un certificat CA d'authentification IEEE 802.1X pour utiliser le protocole IEEE 802.1X.

Version EAPOL : sélectionnez la version du protocole EAP (Extensible Authentication Protocol) que vous souhaitez utiliser.

Identité EAP : saisir l'adresse MAC du périphérique, le nom d'hôte du périphérique ou le texte personnalisé.

Personnalisé : saisir n'importe quel texte qui servira d'identité EAP.

Certificat CA d'authentification IEEE 802.1X : en plus du certificat client, un certificat CA d'authentification IEEE 802.1X doit être installé. Pour activer IEEE 802.1X, seul le certificat public est nécessaire et non la clé privée, une phrase secrète est donc inutile. Le certificat CA d'authentification IEEE 802.1X sera installé lors de l'activation ou de la mise à jour du protocole IEEE 802.1X.

Importer : sélectionner un certificat CA qui sera installé sur les périphériques et utilisés pour valider le serveur d'authentification. Le certificat de l'autorité de certification peut être créé par la CA dans AXIS Device Manager ou venir d'une source externe.

Afficher : détails du certificat CA utilisé lors du processus d'authentification IEEE 802.1X.

Nom courant : sélectionner l'identité EAP du périphérique ou l'adresse IP du périphérique. Si le champ Personnalisé est vide, le nom d'hôte est sélectionné. S'il y a un problème avec le nom d'hôte, l'adresse IP sera utilisée comme nom courant.

Gérez les comptes SIP

Gérer les logiciels des dispositifs

Mises à niveau d'AXIS OS

Les nouvelles versions d'AXIS peuvent être obtenues de deux manières :

- téléchargement avec AXIS Device Manager (via une connexion Internet)
- Importation à partir d'un fichier (sur un disque dur ou une carte mémoire, par ex.).

Remarque

Nous vous encourageons à suivre la procédure de mise à niveau recommandée par AXIS OS. Pour en savoir plus : <https://help.axis.com/axis-os#upgrade-path>

Mise à niveau manuelle d'AXIS OS

1. Sélectionnez les dispositifs que vous souhaitez mettre à niveau avec une nouvelle version d'AXIS OS, cliquez avec le bouton droit de la souris et sélectionnez **Upgrade firmware (Mettre à niveau le firmware)**.
2. Lorsque vous avez connaissance du fait que les dispositifs deviendront inaccessibles pendant la mise à niveau, cliquez sur **Yes (Oui)**.
3. Pour mettre à jour la liste des versions du firmware disponibles pour le téléchargement dans le dialogue **Upgrade firmware (Mettre à niveau le firmware)**, cliquez sur **Check for Updates (Rechercher des mises à jour)**.
4. Pour rechercher un ou plusieurs fichiers de version d'AXIS OS stockés sur un client local, cliquez sur le bouton **Browse (Parcourir)**.
5. Sélectionnez les dispositifs et les versions d'AXIS OS que vous souhaitez mettre à niveau.
6. Pour définir les paramètres d'usine des périphériques sélectionnés lors de la mise à niveau d'AXIS, cliquez sur la **Factory default checkbox (Case à cocher Remise en paramètres d'usine)**. Il s'agit d'une exigence lors de la rétrogradation pour certaines versions d'AXIS OS.
7. Cliquez sur **OK** pour commencer la mise à niveau des dispositifs sélectionnés dans la liste.

Remarque

Par défaut, les mises à niveau d'AXIS OS se font simultanément sur tous les dispositifs sélectionnés. L'ordre de mise à niveau peut être changé dans **Configuration > Connected Services (Services connectés) > Firmware upgrade settings (Paramètres de mise à niveau du firmware)**.

Mises à niveau automatiques

AXIS Device Manager 5 est configuré par défaut pour ne pas rechercher de mises à niveau du firmware, mais il peut être configuré pour vérifier automatiquement si des mises à niveau d'AXIS OS sont disponibles sur le serveur ou sur axis.com.

Pour rechercher manuellement des mises à niveau d'AXIS OS, appuyez sur le bouton **Check now (Rechercher maintenant)** dans le menu d'action.

Ordre de mise à niveau d'AXIS OS

Les mises à niveau d'AXIS OS peuvent être effectuées sur tous les dispositifs en même temps, ou sur un dispositif après l'autre.

- Pour mettre à niveau tous les dispositifs en même temps, sélectionnez l'ordre de mise à niveau **Parallel (Parallèle)**
- Pour mettre à niveau les périphériques les uns après les autres, sélectionnez **Sequential (Séquentiel)**. Cette option sera plus longue, mais les périphériques ne seront pas tous hors ligne en même temps. Vous pouvez également choisir d'arrêter une mise à niveau séquentielle en cas de problème, en cochant la case **Cancel all remaining upgrades if one device fails (Annuler toutes les mises à niveau restantes en cas d'échec d'un périphérique)**.

Recherche de panne

Contacter l'assistance

Lorsque vous contactez l'assistance, créez d'abord un ticket et incluez un fichier de rapport système pour faciliter le dépannage de votre problème particulier :

1. Allez au menu principal.
2. Allez à **Help (Aide) > System Report... (Rapport système...)**
3. Sauvegardez le fichier de rapport dans un dossier choisi.
4. Allez à axis.com/support.
5. Créez un ticket d'assistance.
6. Joignez le fichier à votre ticket d'assistance.

Remarque

Pour créer un rapport système à partir d'un système qui ne répond pas :

1. Atteindre `C:\ProgramData\Axis Communications\`
2. Archivez le contenu du dossier dans un fichier .zip et joignez-le au ticket d'assistance.

Processus d'escalade

En cas de problème ne pouvant pas être résolu à l'aide de ce guide, faites-le remonter à l'Assistance en ligne Axis ; reportez-vous à *l'Assistance en ligne Axis*. Afin que notre équipe d'assistance puisse comprendre votre problème et le résoudre, vous devez inclure les informations suivantes :

- Une description claire de comment reproduire le problème ou des circonstances dans lesquelles il a eu lieu.
- L'heure et le nom ou l'adresse IP du périphérique concerné où le problème survient.
- AXIS Device Manager doit être généré directement après la survenue du problème. Le rapport système doit être généré depuis le client ou le serveur sur lequel le problème a été reproduit.
- Captures d'écran ou enregistrements facultatifs montrant le problème.
- Si nécessaire, incluez les fichiers de la base de données. Excluez ces éléments pour accélérer le téléchargement.

Certains problèmes nécessitent des informations supplémentaires que l'équipe d'assistance demande si nécessaire.

Remarque

Si la taille du fichier est supérieure à 100 Mo, comme dans le cas d'un fichier de suivi réseau ou de base de données, par exemple, envoyez le fichier en utilisant un service de partage de fichier sécurisé auquel vous faites confiance.

Informations supplémentaires	
Journaux de niveau de débogage	Nous activons parfois les niveaux de journalisation de débogage pour collecter plus d'informations. Vous ne pouvez le faire qu'à la demande d'un ingénieur du support Axis. Vous pouvez trouver des instructions à ce sujet dans <i>l'Assistance en ligne Axis</i> .
Trace réseau	À la demande de l'ingénieur support, générez des traces réseau lorsque vous créez le rapport système. Prenez des suivis réseau lorsque le problème survient, si reproductibles. Éléments concernés : • un suivi réseau de 60 sec pris sur la caméra (uniquement pour le firmware 5.20 ou versions ultérieures) Utilisez la commande VAPIX suivante pour modifier la connexion, l'adresse IP et la durée (en secondes) si nécessaire :

Informations supplémentaires	
	<code>http://root:pass@192.168.0.90/axis-cgi/debug/debug.tgz?cmd=pcapdump&duration=60</code> • un suivi réseau de 10 à 30 sec pris sur le serveur montrant les communications entre le serveur et la caméra.
Fichiers de la base de données	Au cas où nous devrions examiner ou réparer manuellement la base de données. Sélectionnez Include database in the report (Inclure la base de données dans le rapport) avant de générer le rapport système.
Captures d'écran	Utilisez des captures d'image en cas de problème de vidéo en direct lié à l'interface utilisateur. Par exemple, lorsque vous souhaitez afficher une chronologie des enregistrements ou lorsque le problème est difficilement descriptible.
Enregistrements de l'écran	Utilisez des enregistrements de l'écran lorsqu'il est difficile de décrire le problème avec des mots, par exemple si un grand nombre d'interactions sur l'interface utilisateur sont nécessaires pour reproduire le problème.

T10211981_fr

2025-09 (M3.2)

© 2024 – 2025 Axis Communications AB