

AXIS Device Manager Extend

Table des matières

À propos de.....	3
À propos des organisations	4
Vue d'ensemble de la solution	5
Conditions préalables	10
MISE EN ROUTE	12
Enregistrer un compte MyAxis	12
Installez le client et activez votre compte	12
Créer une organisation.....	12
Installation de l'hôte edge.....	12
Demander l'hôte edge.....	12
Gérer les périphériques.....	14
Ajouter des périphériques détectés à l'hôte edge	14
Ajouter des périphériques à partir des adresses IP.....	14
Ajouter des dispositifs à partir de la plage IP	14
Ajouter des périphériques à partir d'un fichier.....	14
Supprimer les périphériques	15
Se connecter aux périphériques	15
Configuration.....	16
Activation de l'accès distant.....	16
Supprimer un site.....	16
Ajouter des utilisateurs à l'organisation	16
À propos des rôles d'utilisateur	16
Attribuer un rôle d'utilisateur	17
Supprimer des utilisateurs.....	17
Gestion d'AXIS OS.....	18
Gérer les versions d'AXIS OS en fonction des modèles.....	18
Gérez AXIS OS sur un hôte edge.....	18
Consulter les mises à niveau d'AXIS OS en cours et terminées	18
Politiques.....	19
Créer et appliquer une politique de sécurité	19
Créer et appliquer une politique d'application	19
Modifier une politique	20
Supprimer une politique.....	20
Gérer les licences.....	21
Licence de votre produit.....	21
Recherche de panne.....	22
Comment configurer les paramètres du pare-feu	22

À propos de

La solution AXIS Device Manager Extend propose aux administrateurs système une interface pour la découverte, la configuration et l'exploitation des périphériques Axis sur les réseaux de leur organisation.

L'application de bureau AXIS Device Manager Extend

L'application de bureau est un utilitaire logiciel qui peut être utilisé comme une interface utilisateur à la demande ou toujours disponible pour gérer le système. Elle peut être exécutée sur une machine dédiée avec un hôte edge installé localement, ou à part de l'hôte edge sur un ordinateur portable connecté à distance. Le client présente à l'utilisateur le statut général du système et les actions de gestion pouvant être exécutées.

Hôte edge

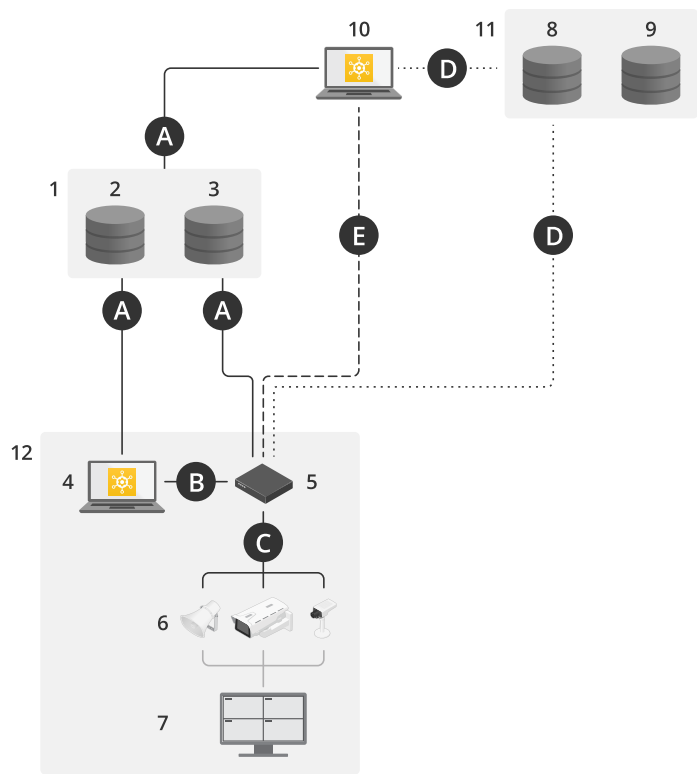
Le composant hôte edge dans AXIS Device Manager Extend est un service de gestion sur site toujours disponible, chargé de mettre à jour les périphériques locaux, tels que les caméras. L'hôte edge AXIS Device Manager Extend assure également la liaison vers le service de gestion à distance Axis, où la même fonctionnalité de l'API prend en charge l'administration distante des sites via la plateforme de service Axis.

À propos des organisations

L'organisation, qui est une représentation virtuelle de vos installations système Axis, est au cœur de vos services cloud. Une organisation héberge tous les périphériques et comptes utilisateur d'une entreprise dans une hiérarchisation qui régule l'accès et garantit une sécurité maximale. Cela permet en même temps une gestion flexible des utilisateurs et des périphériques, pour les petites et grandes entreprises.

- Lorsque vous créez une organisation, vous en devenez propriétaire. Cette organisation connecte votre système aux utilisateurs du service cloud Axis.
- Vous pouvez inviter des utilisateurs à rejoindre l'organisation. Cf. .
- Vous pouvez attribuer différents rôles aux utilisateurs.
- L'organisation contient un dossier par défaut où vous pouvez commencer à mettre en place une structure qui répond à vos besoins. Vous pouvez structurer l'organisation en dossiers et sous-dossiers. Généralement, un dossier représente un site ou un emplacement physique d'un système au sein d'une organisation.
- Gérez vos licences pour votre système au sein de votre organisation.
- Pour créer une organisation, vous avez besoin de votre compte My Axis.

Vue d'ensemble de la solution

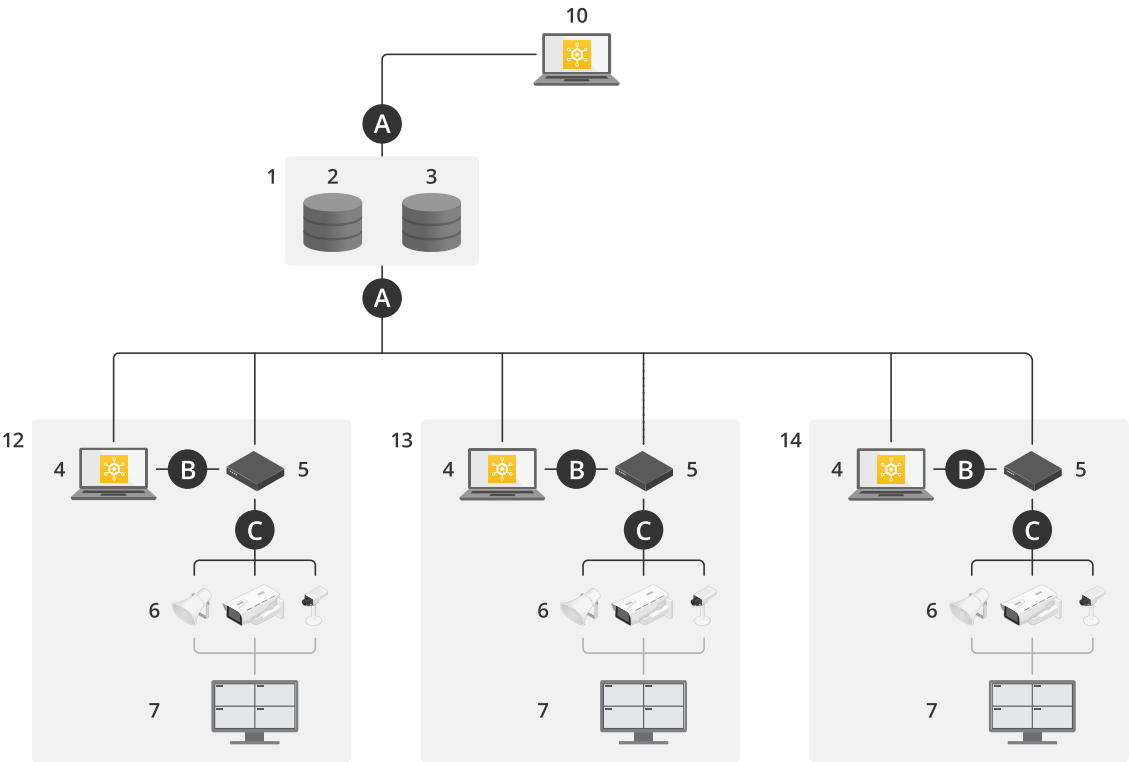


AXIS Device Manager Extend avec accès local et distant

- 1 Axis
- 2 IAM (My Axis)
- 3 Données de la société
- 4 Client local
- 5 Hôte edge
- 6 Périphériques
- 7 VMS
- 8 TURN
- 9 Signalisation
- 10 Client distant
- 11 Serveurs WebRTC à accès distant
- 12 Site 1

Conne- xion	URL et IP	Port	Protocole	Commentaire
A	prod.adm.connect.axis.com (52.224.128.152 ou 40.127.155.231)	443	HTTPS	Requis
B	Détection HTTP (du client aux hôtes edge)	37080	HTTP	Obligatoire pour provisionner le site. Facultatif après provisionnement.
	Transfert de données (entre le client et les hôtes edge)	37443	HTTPS	
	Détection multicast (du client aux hôtes edge)	6801	UDP	
	Détection multicast (des hôtes edge au client)	6801	UDP	

Conne- xion	URL et IP	Port	Protocole	Commentaire
A	prod.adm.connect.axis.com (52.224.128.152 ou 40.127.155.231)	443	HTTPS	Requis
B	Détection HTTP (du client aux hôtes edge) Transfert de données (entre le client et les hôtes edge) Détection multicast (du client aux hôtes edge) Détection multicast (des hôtes edge au client)	37080 37443 6801 6801	HTTP HTTPS UDP UDP	Obligatoire pour provisionner le site. Facultatif après provisionnement.
C	Transfert de données (entre hôte local et dispositifs) Détection unicast Détection multicast Détection HTTP	80 / port personnalisé, 443 1900 1900, 5353 80,443	HTTP, HTTPS SSDP, Bonjour	Requis
D	signaling.prod.webrtc.connect.axis.com *.turn.prod.webrtc.connect.axis.com	443 443, 5349	HTTPS HTTPS, DTLS (UDP et TCP)	Basé sur la norme WebRTC En option et désactivé par défaut
-	Poste-à-poste (P2P)	49152-65535	DTLS (UDP et TCP)	



AXIS Device Manager Extend avec accès local et accès distant à l'aide d'une connexion VPN

- 1 Axis
- 2 IAM (My Axis)
- 3 Données de la société
- 4 Client local
- 5 Hôte edge
- 6 Périphériques
- 7 VMS
- 8 TURN
- 9 Signalisation
- 10 Client distant
- 11 Serveurs WebRTC à accès distant
- 12 Site 1
- 13 Site 2
- 14 Site 3

Conne- xion	URL et IP	Port	Protocole	Commentaire
A	prod.adm.connect.axis.com (52.224.128.152 ou 40.127.155.231)	443	HTTPS	Requis
B	Détection HTTP (du client aux hôtes edge) Transfert de données (entre le client et les hôtes edge) Détection multicast (du client aux hôtes edge) Détection multicast (des hôtes edge au client)	37080 37443 6801 6801	HTTP HTTPS UDP UDP	Obligatoire pour provisionner le site. Facultatif après provisionnement.

C	Transfert de données (entre hôte local et dispositifs) Détection unicast Détection multicast Détection HTTP	80 / port personnalisé, 443 1900 1900, 5353 80,443	HTTP, HTTPS SSDP, Bonjour	Requis
D	signaling.prod.webrtc.connect.axis.com *.turn.prod.webrtc.connect.axis.com	443 443, 5349	HTTPS HTTPS, DTLS (UDP et TCP)	Basé sur la norme WebRTC En option et désactivé par défaut
-	Poste-à-poste (P2P)	49152-65535	DTLS (UDP et TCP)	

- Un DNS public tel que Google DNS : 8.8.8.8 / 8.8.4.4 ou Cloudflare DNS : 1.1.1.1 est une exigence supplémentaire
- Les connexions A et C sont nécessaires pour prendre en charge toutes les fonctionnalités du système AXIS Device Manager Extend.
- L'application est en cours de développement, nous vous conseillons donc d'autoriser l'accès du pare-feu aux connexions réseau sortantes pour l'application de bureau AXIS Device Manager Extend et tous les hôtes edge.

Conditions préalables

Systèmes d'exploitation compatibles :

- Windows 10 Pro et Enterprise
- Windows 11 Pro et Enterprise
- Windows Server 2016, 2019 et 2022 (système x64)
- Privilège d'administrateur système requis pour l'installation et les modifications de configuration.

Recommandation système minimum :

- Processeur : Intel Core i5
- RAM : 4 Go
- Réseau : 100 Mbps

Connectivité Internet

Remarque

L'application AXIS Device Manager Extend nécessite la mise à disposition d'une connexion Internet, avec des certificats l'identifiant comme appartenant à l'organisation créée et associée au compte My Axis utilisé dans l'installation. Cependant, pour accéder à certaines fonctions telles que les informations sur la garantie et la prise en charge multisite, vous aurez besoin d'une connexion Internet. De plus, le client et/ou l'hôte edge se mettent à jour automatiquement uniquement en mode en ligne.

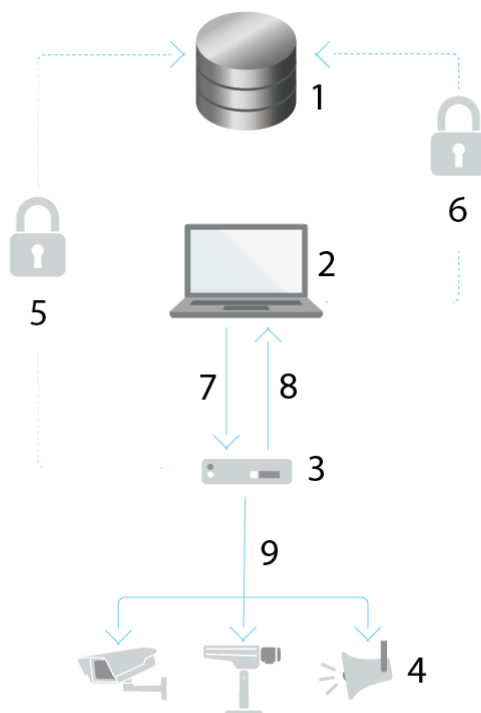
Date et heure synchronisées

Remarque

Vérifiez que tous les composants du système sont synchronisés. Dans le cas contraire, l'authentification entre l'hôte edge et le client ou le back end pourrait échouer. Il est recommandé de synchroniser toutes les machines hôtes avec un serveur de temps réseau commun afin d'éviter tout problème éventuel.

Ports réseau ouverts :

pour des connexions sécurisées depuis l'application de bureau AXIS Device Manager Extend vers l'hôte edge, la détection de l'hôte edge et Axis Remote Service.



- 1 Axis Service Platform
- 2 Application de bureau AXIS Device Manager Extend
- 3 Hôte edge
- 4 Périphériques
- 5 HTTPS (port 443)
- 6 HTTPS (port 443)
- 7 HTTPS (port 37443), détection multicast UDP (port 6801), détection HTTP (port 37080)
- 8 Détection multicast UDP (port 6801)
- 9 HTTPS et HTTP (port 443 et 80), détection multicast - SSDP (port 1900) - Bonjour (port 5353), détection unicast (port 1900), détection HTTP (port 80 et 443)

Accès au réseau sortant

L'application est en cours de développement, nous vous conseillons donc d'autoriser l'accès du pare-feu aux connexions réseau sortantes pour l'application de bureau AXIS Device Manager Extend et tous les hôtes edge.

MISE EN ROUTE

Enregistrer un compte MyAxis

1. Enregistrez un compte My Axis sur axis.com/my-axis/login.
2. Choisissez l'une des méthodes d'authentification multifactorielle (MFA) suivantes : **Authenticator App (TOTP)** ou **E-mail** et suivez les instructions à l'écran. La MFA est un système de sécurité qui ajoute un niveau de vérification supplémentaire afin de garantir l'identité de l'utilisateur.

Installez le client et activez votre compte

Allez à la page produit sur axis.com et téléchargez le client Axis Device Management.

1. Accédez à l'emplacement où vous avez téléchargé l'application et cliquez dessus pour l'installer.
2. Sélectionnez le client et cliquez sur **Install (Installer)**.
3. Connectez-vous à votre compte My Axis.
4. Confirmez votre adresse e-mail pour terminer l'activation.
5. Créez ou rejoignez une organisation existante.

Créer une organisation

Pour ajouter des dispositifs à votre système, vous devez faire partie d'une organisation. C'est ainsi que vous conservez et protégez vos dispositifs de manière sécurisée sur un ou plusieurs sites. Si vous n'êtes pas encore membre d'une organisation, un assistant de configuration apparaîtra et vous guidera tout au long du processus.

Pour créer une organisation :

1. Connectez-vous à votre compte MyAxis.
2. Suivez les instructions de l'assistant de configuration.

Pour créer des organisations supplémentaires :

- Allez au menu déroulant avec le nom de votre organisation.
- Sélectionnez **+ Create new organization (+ Créer une nouvelle organisation)**
- Suivez les instructions de l'assistant de configuration.

Installation de l'hôte edge

Allez à la page produit sur axis.com et téléchargez l'hôte edge (Axis Device Manager Server)..

1. Choisissez un serveur sur lequel vous souhaitez installer l'hôte edge. Nous vous conseillons d'installer l'hôte edge sur un serveur aussi proche que possible de vos dispositifs.
2. Exécutez le programme d'installation sur le serveur.

Demander l'hôte edge

Pour créer une connexion sécurisée à vos périphériques à partir du client Axis Device Manager Extend, vous devez d'abord demander un hôte edge à votre société.

1. Cliquez sur un hôte edge dont le statut est défini sur **Unclaimed (Non demandé)**
 - 1.1. Cliquez sur **Add new edge host (Ajouter un nouvel hôte edge)** si aucun hôte edge n'est présent dans la liste
 - 1.2. Saisissez l'adresse IP de l'emplacement de l'hôte edge
2. Tapez le nom de l'hôte edge
3. Ajoutez une description facultative (recommandé)

4. Cliquez sur Claim edge host (Demander l'hôte edge)

Gérer les périphériques

Ajouter des périphériques détectés à l'hôte edge

1. Accédez à Edge hosts (Hôtes edge).
2. Sélectionnez un hôte edge installé dans la liste à laquelle vous voulez ajouter des périphériques.
3. Accédez à Devices > Discovered (Périphériques > Détectés).
4. Sélectionnez les périphériques que vous souhaitez ajouter ou sélectionnez tous les périphériques en cochant la case en haut de la colonne de sélection.
5. Cliquez sur Add devices to edge host (Ajouter des périphériques à l'hôte edge) .

Les périphériques sont désormais répertoriés dans l'onglet Managed (Gérés) et leur statut peut être vérifié dans Edge host overview (Aperçu de l'hôte edge).

Ajouter des périphériques à partir des adresses IP

Ajoutez des périphériques qui ne sont pas automatiquement identifiés à partir de sous-réseaux, d'adresses IP individuelles ou d'une plage IP.

Ajouter des dispositifs à partir de la plage IP

1. Accédez à un hôte edge demandé par votre organisation.
2. Accédez à Settings > Device discovery (Paramètres > Détection des périphériques).
3. Cliquez sur Add by IP (Ajouter par IP)
4. Sélectionner Manual entry (Entrée manuelle)
5. Saisissez la plage IP
6. Cliquez sur Add IP addresses (Ajouter les adresses IP)
7. Accédez à Devices > Discovered (Dispositifs > Détectés)
8. Sélectionnez les périphériques que vous souhaitez ajouter ou sélectionnez tous les périphériques en cochant la case en haut de la colonne de sélection.
9. Cliquez sur Add devices (Ajouter des appareils).

Ajouter des périphériques à partir d'un fichier

1. Accédez à un hôte edge demandé par votre organisation.
2. Accédez à Settings > Device discovery (Paramètres > Détection des périphériques).
3. Cliquez sur Add by IP (Ajouter par IP)
4. Sélectionnez Import from file (Importer depuis un fichier).
5. Sélectionner le fichier .CSV comportant les adresses IP
6. Cliquez sur Import (Importer)
7. Accédez à Devices > Discovered devices (Périphériques > Périphériques détectés)
8. Sélectionnez les périphériques que vous souhaitez ajouter ou sélectionnez tous les périphériques en cochant la case en haut de la colonne de sélection.
9. Cliquez sur Add devices (Ajouter des appareils).

Remarque

Le fichier doit avoir :

Un en-tête pour la colonne des adresses IP.

Une colonne unique.

Un maximum de 25 600 adresses IP.

Supprimer les périphériques

1. Cliquez sur **Edge host (Hôte Edge)**
2. Sélectionnez un hôte edge.
3. Accédez à **Devices (Dispositifs)**
4. Sélectionnez les périphériques que vous souhaitez supprimer ou sélectionnez tous les périphériques en cochant la case en haut de la colonne de sélection.
5. Cliquez sur l'icône **Remove devices from edge host (Supprimer les périphériques de l'hôte edge)** dans le menu **Action**.
6. Cliquez sur **Remove (Supprimer)**.

Les périphériques supprimés se trouvent sous **Devices > Discovered (Périphériques > Détectés)**.

Se connecter aux périphériques

1. Cliquez sur **Edge hosts (Hôtes Edge)**.
2. Sélectionnez un hôte edge.
3. Accédez à **Devices > Managed (Périphériques > Gérés)**.
4. Sélectionnez les périphériques auxquels vous souhaitez accéder ou sélectionnez tous les périphériques en cochant la case en haut de la colonne de sélection.
5. Cliquez sur **Log in (Se connecter)** pour vous connecter automatiquement à plusieurs périphériques.
6. Saisissez le nom d'utilisateur et le mot de passe.
7. Cliquez sur **Log in (Connexion)**

Remarque

Si le nom d'utilisateur et le mot de passe sont corrects, l'option **Status (Statut)** affiche **Reachable (Accessible)**.

Configuration

Activation de l'accès distant

Si les paramètres du pare-feu bloquent les connexions sortantes, vous devrez peut-être utiliser une connexion proxy pour accéder au site à distance.

1. Sélectionnez l'hôte edge sur lequel activer l'accès distant.
2. Accédez à **Settings > Edge hosts connections (Paramètres > Connexions des hôtes edge)**.
3. Activez **Allow remote access to edge host (Autoriser l'accès distant à l'hôte edge)**.
4. Si vous devez saisir une adresse proxy pour accéder à Internet, saisissez une adresse sous **Proxy address (Adresse proxy)**.

Vous serez informé une fois que la connexion sera active.

Remarque

Pour prendre en charge la connexion à des hôtes edge sur d'autres réseaux, vous devrez peut-être ajouter la configuration suivante à la « liste autorisée » du pare-feu de votre réseau d'entreprise : Endpoint Port Protocol signaling.prod.webrtc.connect.axis.com 443 HTTPS *.turn.prod.webrtc.connect.axis.com 443 HTTPS webRTC (Turn et P2P) 5349, 49152 - 65535 DTLS (UDP et TCP)

Supprimer un site

Avant de supprimer un hôte edge de l'organisation, vous devez appartenir à l'hôte edge. Les périphériques se trouvent ensuite sous **Devices > Discovered (Périphériques > Détectés)**.

1. Cliquez sur **Edge hosts (Hôtes edge)**.
2. Sélectionnez l'hôte edge avec les touches fléchées ou placez-le sous le pointeur de la souris.
3. Cliquez sur **...** et sélectionnez **Remove edge host (Supprimer l'hôte edge)** dans le menu déroulant.
4. Cochez l'option **I'm aware of the risks (Je connais les risques)**.
5. Cliquez sur **Remove (Supprimer)**.

Ajouter des utilisateurs à l'organisation

1. Sélectionnez l'organisation dans laquelle vous souhaitez configurer les paramètres utilisateur.
2. Allez au panneau **My Systems**.
3. Allez à **ORGANIZATION (Société) > Users (Utilisateurs)**.
4. Cliquez sur **Invite users (Inviter des utilisateurs)**.
5. Suivez les instructions à l'écran de l'assistant de configuration.
 - Si vous avez sélectionné **Operator (Opérateur)** ou **Viewer (Observateur)**, sélectionnez les dossiers auxquels les utilisateurs auront accès. Notez que les rôles **Admin** ont accès à tous les dossiers de l'organisation.

Remarque

L'utilisateur reçoit un e-mail d'invitation qu'il peut utiliser pour se connecter à My Systems. Si l'utilisateur ne possède pas de compte My Axis, il doit utiliser cet e-mail pour s'inscrire afin d'accéder à l'organisation. Les invitations peuvent être révoquées pendant que l'acceptation est en attente.

À propos des rôles d'utilisateur

Les rôles utilisateur déterminent le nombre d'accès dont un utilisateur dispose aux systèmes de votre organisation. Les fonctionnalités disponibles varient en fonction du rôle de l'utilisateur.

Admin

Les administrateurs ont accès à l'ensemble du système. Cela comprend la gestion des utilisateurs, des périphériques, des licences, des vidéos et d'autres contenus.

Ils peuvent également embarquer des périphériques avec AXIS Camera Station Pro. Les administrateurs peuvent gérer AXIS Camera Station Pro Server Monitoring dans My Systems.

Opérateur

Les opérateurs peuvent surveiller les flux vidéo en direct, contrôler les périphériques et accéder aux enregistrements pour la lecture. Ils ont une vue d'ensemble des utilisateurs de l'organisation et de leurs rôles respectifs. Les opérateurs peuvent également gérer AXIS Camera Station Pro Server Monitoring dans My Systems.

Utilisateur

Les observateurs peuvent surveiller les flux vidéo en direct, mais ne peuvent pas contrôler les périphériques ou accéder aux enregistrements. Ils ont une vue d'ensemble des utilisateurs de l'organisation et de leurs rôles respectifs.

Attribuer un rôle d'utilisateur

1. Sélectionnez l'organisation dans laquelle vous souhaitez configurer les paramètres utilisateur.
2. Allez au panneau My Systems.
3. Sous **ORGANIZATION (Société)**, allez à **Users (Utilisateurs)**.
4. Cliquez sur l'utilisateur que vous souhaitez élever et cliquez sur **Roles and access (Rôles et accès)**.
5. Suivez les instructions à l'écran de l'assistant de configuration.

Remarque

Le rôle change immédiatement une fois sélectionné. Pour des raisons de sécurité, les invitations sont limitées au rôle Observateur.

Supprimer des utilisateurs

1. Sélectionnez l'organisation dans laquelle vous souhaitez configurer les paramètres utilisateur.
2. Allez au panneau My Systems.
3. Sous **ORGANIZATION (Société)**, allez à **Users (Utilisateurs)**.
4. Passez la souris sur l'utilisateur à supprimer pour afficher un nouveau menu d'options : ...
5. Cliquez sur ... et sélectionnez **Remove user (Supprimer l'utilisateur)** dans le menu déroulant.

Supprimer plusieurs utilisateurs

1. Sélectionnez les utilisateurs que vous souhaitez supprimer.
2. Cliquez sur la corbeille dans le menu action.
3. Cliquez sur **Remove (Supprimer)**.

Gestion d'AXIS OS

Avec le client Axis Device Management, vous pouvez gérer le système d'exploitation de dispositifs multiples dans chaque société

Pour obtenir la liste des mises à jour d'AXIS OS disponibles pour tous les dispositifs de votre organisation, regroupés par modèle, accédez à **Home > AXIS OS versions inventory** (Accueil > Inventaire AXIS OS). Pour obtenir la liste des mises à jour d'AXIS OS disponibles sur un hôte edge spécifique, sélectionnez l'hôte edge et accédez à **AXIS OS inventory** (Inventaire AXIS OS).

Gérer les versions d'AXIS OS en fonction des modèles

Pour gérer AXIS OS par modèle au sein de votre organisation :

1. Aller à **Accueil > Versions d'OS AXIS**
2. Cliquez sur le lien de la version recommandée d'AXIS OS. Les options de mise à niveau d'AXIS OS s'affichent.
3. Cliquez sur le menu déroulant **Mettre à niveau vers** pour voir ce qui est disponible. La dernière version d'AXIS OS est présélectionnée.
4. Cliquez sur **Upgrade (Mettre à niveau)**.

Gérez AXIS OS sur un hôte edge.

Pour gérer AXIS OS sur une partie ou la totalité des dispositifs ajoutés à un hôte edge :

1. Accédez à **Edge hosts (Hôtes edge)**
2. Cliquez sur l'hôte edge auquel vous voulez accéder.
3. Accédez à **Devices (Périphériques)**
4. Sélectionnez un ou tous les périphériques que vous souhaitez gérer.
5. Cliquez sur l'icône **AXIS OS** dans le menu d'actions.
6. Vérifiez tous ou certains des modèles de la liste.
7. Pour changer la version d'AXIS OS, cliquez sur la version suggérée pour consulter les options disponibles pour chaque dispositif. La dernière version d'AXIS OS est présélectionnée.
8. Cliquez sur **Upgrade [Mettre à niveau]**.

Consulter les mises à niveau d'AXIS OS en cours et terminées

Pour afficher les mises à niveau logicielles en cours pour les dispositifs connectés à un hôte edge donné :

1. Cliquez sur **Edge hosts (Hôtes Edge)**.
2. Cliquez sur l'hôte edge auquel vous voulez accéder.
3. Allez à **Log (Journal)**

Pour voir les mises à niveau logicielles en cours :

4. Accédez à **Log > Ongoing tasks (Journal > Tâches en cours)**

Politiques

Les politiques gèrent vos périphériques automatiquement. Créez des politiques de maintenance de la cybersécurité sur l'ensemble de votre site. Vous pouvez également définir une politique d'installation et de mise à jour automatiques des applications sur vos périphériques.

Créer et appliquer une politique de sécurité

Dans cet exemple d'utilisation, nous créons et appliquons une politique de sécurité de base à un certain nombre de périphériques connectés à un hôte edge.

Créer une politique de sécurité de base :

1. Accédez à **Edge hosts (Hôtes edge)**
2. Cliquez sur l'hôte edge auquel vous voulez accéder.
3. Accédez à **Devices (Périphériques)**
4. Cliquez sur l'icône **+** en regard de **Policies (Politiques)**
5. Sélectionnez **Basic security (Sécurité de base)** et cliquez sur **Continue (Continuer)**
6. Nommez votre politique
7. Sélectionnez les paramètres adaptés à vos besoins en matière de sécurité. Pour le niveau de sécurité recommandé, conservez les paramètres par défaut.
 - Pour modifier le mot de passe root des périphériques sélectionnés, cliquez sur **Device root password (Mot de passe root du périphérique)** et saisissez le nouveau mot de passe root.
8. Cliquez sur **Créer**.

Appliquer la politique :

1. Sélectionnez les périphériques auxquels vous souhaitez appliquer la politique.
2. Cliquez sur l'icône **Policy options (Options de politique)** dans le menu Action.
3. Sélectionnez la politique de sécurité et cliquez sur **Save (Sauvegarder)**.

Créer et appliquer une politique d'application

Dans cet exemple d'utilisation, nous créons et appliquons une politique d'application à un certain nombre de périphériques connectés à un hôte edge.

1. Accédez à **Edge hosts (Hôtes edge)**
2. Cliquez sur l'hôte edge auquel vous voulez accéder.
3. Accédez à **Devices (Périphériques)**
4. Cliquez sur l'icône **+** en regard de **Policies (Politiques)**
5. Sélectionnez **Apps (Applications)** et cliquez sur **Continue (Continuer)**
6. Nommez votre politique
7. Sélectionnez les applications que vous souhaitez installer et mettre à jour sur vos périphériques.
8. Sélectionnez la fenêtre de mise à jour dans le menu déroulant.
9. Cliquez sur **Créer**.

Appliquer la politique :

1. Sélectionnez les périphériques auxquels vous souhaitez appliquer la politique.
2. Cliquez sur l'icône **Policy options (Options de politique)** dans le menu Action.
3. Sélectionnez la politique d'application à appliquer.
4. Cliquez sur **Save (Enregistrer)**.

Remarque

Les apps sélectionnées sont automatiquement réinstallées, si elles ont été supprimées.

Modifier une politique

Pour modifier une politique existante :

1. Accédez à **Edge hosts (Hôtes edge)**
2. Cliquez sur l'hôte edge auquel vous voulez accéder.
3. Accédez à **Devices (Périphériques)**
4. Cliquez sur ... en regard de la politique que vous voulez modifier et sélectionnez **Edit policy (Modifier la politique)** dans le menu déroulant.
5. Modifiez les paramètres de la politique en fonction de vos besoins.
6. Cliquez sur **Save (Enregistrer)**

Supprimer une politique

Pour supprimer une politique existante :

- Accédez à **Edge hosts (Hôtes edge)**
- Cliquez sur l'hôte edge auquel vous voulez accéder.
- Accédez à **Devices (Périphériques)**
- Cliquez sur ... en regard de la politique que vous voulez modifier et sélectionnez **Delete policy (Supprimer la politique)** dans le menu déroulant.
- Cliquez sur **Supprimer**

Remarque

Les périphériques auxquels cette politique est appliquée conserveront les paramètres de la politique, mais les paramètres ne sont plus persistants.

Gérer les licences

Licence de votre produit

Pour obtenir une licence pour votre produit, allez à *My Systems > Licences* (Mes systèmes > Licences). Pour en savoir plus sur les licences pour les produits et services Axis, voir le *manuel d'utilisation de My Systems*.

Recherche de panne

Comment configurer les paramètres du pare-feu

Le client Axis Device Management nécessite l'accès au domaine axis.com et à tout sous-domaine.

Pour que l'hôte edge puisse communiquer avec le service Axis, ajoutez les adresses IP et les ports suivants à la liste d'autorisations du pare-feu de la société :

- 40.127.155.231 (UE), port 443
- 52.224.128.152 and 40.127.155.231 (États-Unis), port 443
- IP d'un serveur DNS public, port 53

Sinon, le domaine prod.adm.connect.axis.com (qui est un enregistrement DNS A pointant vers les adresses IP ci-dessus) peut être utilisé dans les paramètres du pare-feu.

L'hôte edge utilise le nom de domaine prod.adm.connect.axis.com pour toutes les demandes sortantes.

Pour que cela fonctionne, le réseau devra utiliser un serveur DNS public et autoriser le trafic vers l'adresse IP du serveur DNS (et le port 53 par défaut).

Remarque

Pour plus d'informations sur la configuration des ports, consultez le livre blanc d'AXIS Device Manager Extend : *Configurations système types*.

T10153497_fr

2025-10 (M22.2)

© 2020 – 2025 Axis Communications AB