AXIS Device Manager Extend

Manuel d'utilisation

AXIS Device Manager Extend

Table des matières

AXIS Device Manager Extend

À propos

À propos

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.

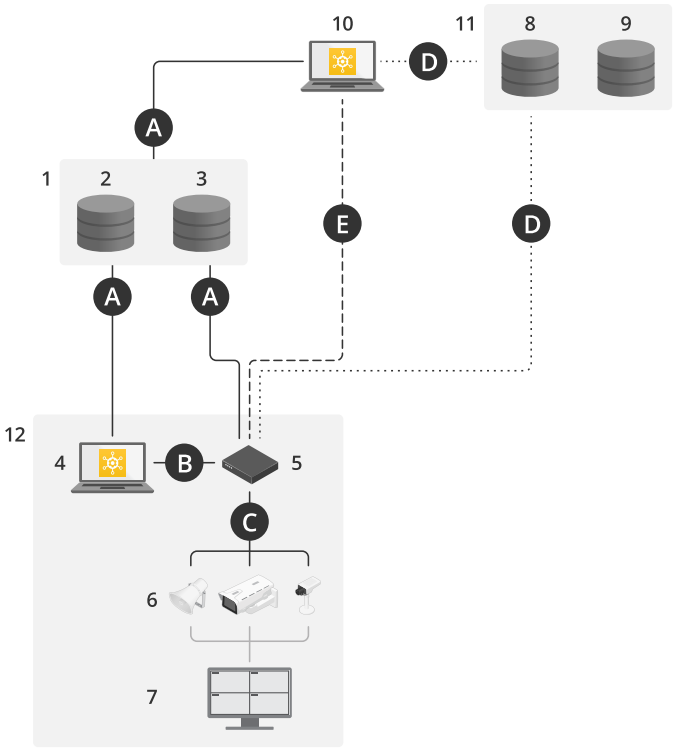
L'application de bureau AXIS Device Manager Extend

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.

Présentation de la solution



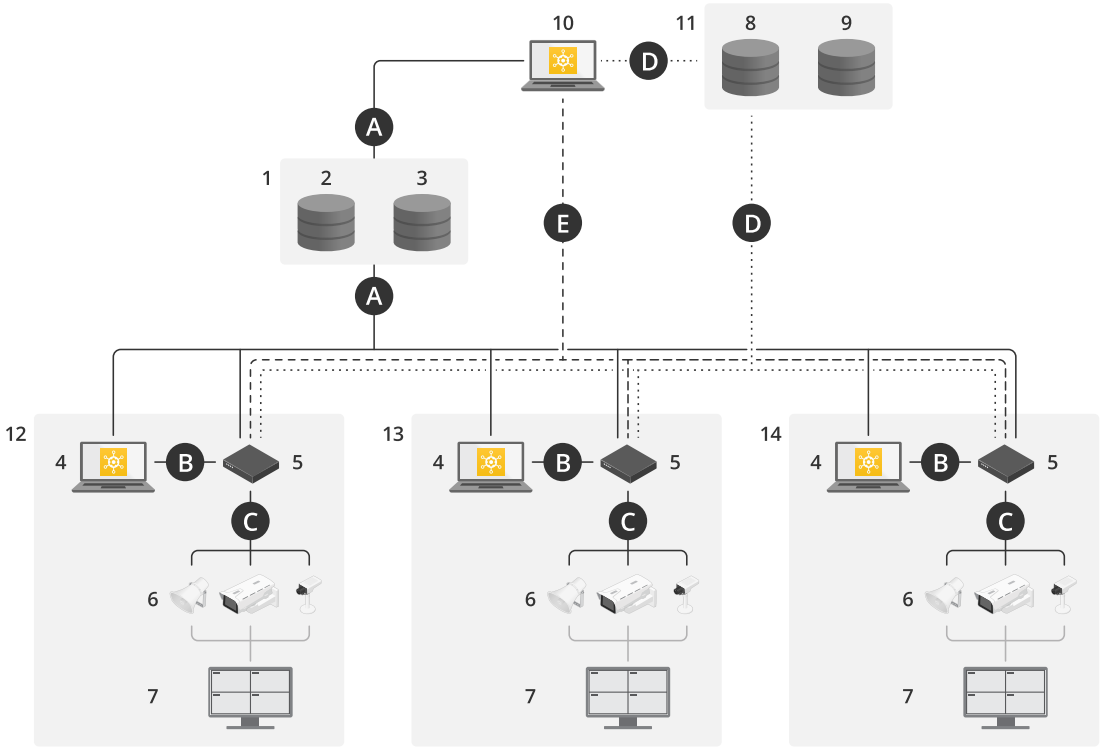
AXIS Device Manager Extend avec accès local et distant

1 *Axis*
2 *IAM (My Axis)*
3 *Données de l'organisation*
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*

Connexion	URL et IP	Port	Protocole	Commentaire
A	prod.adm.connect.axis.com (52.224.128.152 ou 40.127.155.231)	443	HTTPS	Obligatoire
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	Nécessaire pour la mise en service du site. En option après la mise en service.

Présentation de la solution

C	Transfert de données (entre l'hôte edge et les périphériques) Détection unicast Détection multicast Détection HTTP	80 / port personnalisé, 443 1900 1900, 5353 80,443	HTTP, HTTPS SSDP, Bonjour	Obligatoire
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
E	Poste-à-poste (P2P)	49152–65535	DTLS (UDP et TCP)	

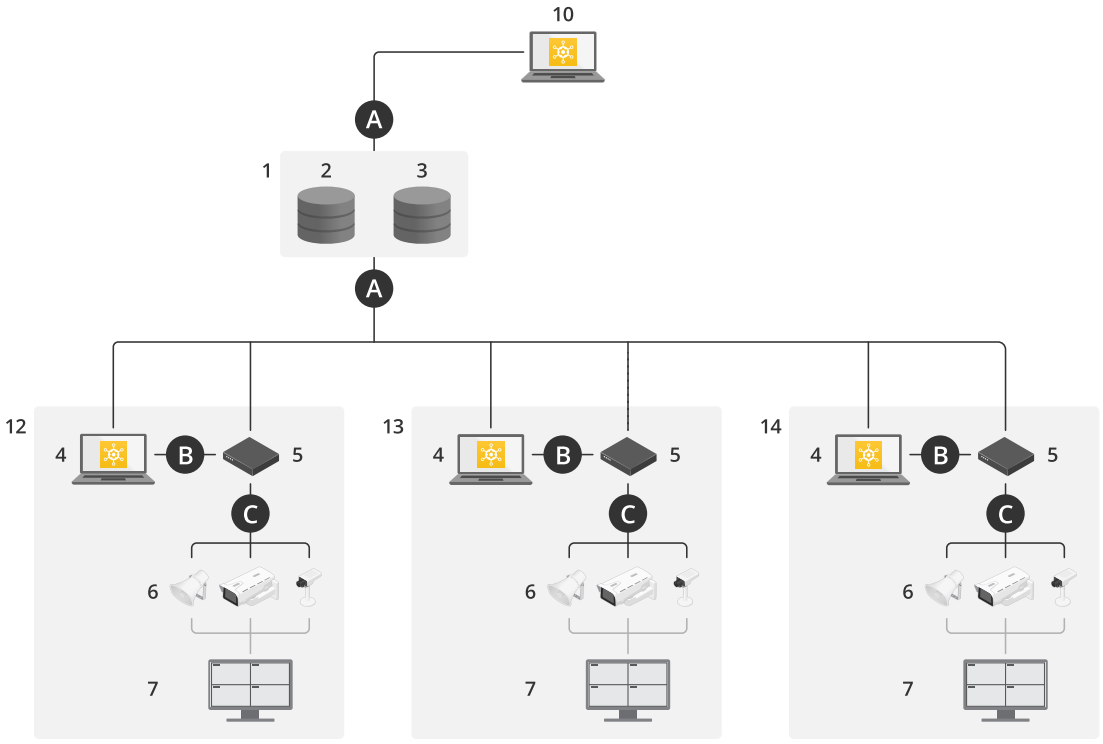


AXIS Device Manager Extend avec une configuration multisite utilisant l'accès local et distant

1 *Axis*
2 *IAM (My Axis)*
3 *Données de l'organisation*
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*

Présentation de la solution

Connexion	URL et IP	Port	Protocole	Commentaire
A	prod.adm.connect.axis.com (52.224.128.152 ou 40.127.155.231)	443	HTTPS	Obligatoire
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	Nécessaire pour la mise en service du site. En option après la mise en service.
C	Transfert de données (entre l'hôte edge et les périphériques) Détection unicast Détection multicast Détection HTTP	80 / port personnalisé, 443 1900 1900, 5353 80,443	HTTP, HTTPS SSDP, Bonjour	Obligatoire
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
E	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 l'organisation*
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

Connexion	URL et IP	Port	Protocole	Commentaire
A	prod.adm.connect.axis.com (52.224.128.152 ou 40.127.155.231)	443	HTTPS	Obligatoire
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	Nécessaire pour la mise en service du site. En option après la mise en service.
C	Transfert de données (entre l'hôte edge et les périphériques) Détection unicast Détection multicast Détection HTTP	80 / port personnalisé, 443 1900 1900, 5353 80,443	HTTP, HTTPS SSDP, Bonjour	Obligatoire
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
E	Poste-à-poste (P2P)	49152–65535	DTLS (UDP et TCP)	

- Un DNS public tel que Google DNS est une exigence supplémentaire : 8.8.8.8 / 8.8.4.4 ou Cloudflare DNS : 1.1.1.1
- 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

Conditions préalables

Systèmes d'exploitation compatibles :

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

Recommandation système minimum :

- Processeur : Intel Core i5
- Mémoire RAM : 4 Go
- Réseau : 100 Mbit/s

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 le contrôleur de site se met à jour automatiquement uniquement en mode en ligne.

Date et heure synchronisées

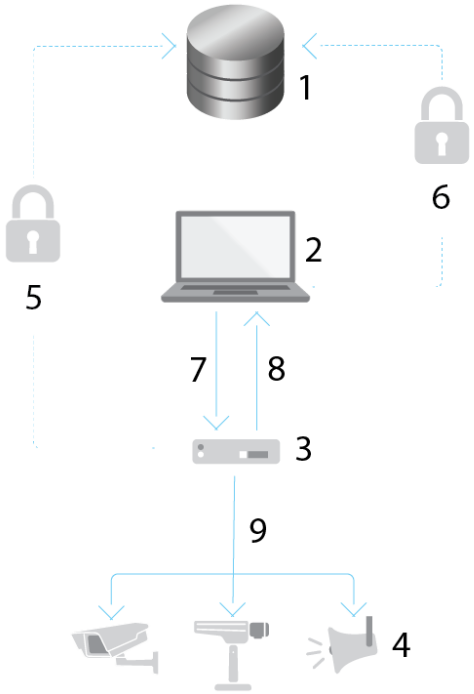
Remarque

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.

Conditions préalables



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.

Premiers pas

Enregistrer un compte MyAxis

Enregistrez un compte **My Axis** sur *axis.com/my-axis/login*

Vous pouvez sécuriser davantage votre compte MyAxis en activant l'authentification multifacteur (MFA). La MFA est un système de sécurité qui ajoute une couche supplémentaire de vérification pour garantir l'identité de l'utilisateur.

Pour activer la MFA :

1. Connectez-vous avec vos identifiants **MyAxis**.
2. Accédez à et sélectionnez **Paramètres du compte**.
3. Cliquez sur **Paramètres de sécurité**
4. Activez la **Vérification en 2 étapes**.

Vous êtes redirigé vers une page de connexion.

5. Connectez-vous avec vos identifiants **MyAxis**.

La MFA est à présent active.

Connectez-vous lorsque la MFA est active :

1. Connectez-vous en utilisant votre compte **MyAxis**.

Un e-mail vous est envoyé.

2. Ouvrez l'e-mail et cliquez sur **S'authentifier**.

Si vous n'avez pas reçu d'e-mail, vérifiez s'il se trouve dans votre dossier de courriers indésirables. S'il ne s'y trouve pas, contactez le support informatique.

Installez le client et activez votre compte

Accédez à la page du produit sur axis.com et téléchargez le programme d'installation de l'application de bureau AXIS Device Manager Extend

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.

Installer l'hôte edge

L'hôte edge et le client de bureau sont tous deux inclus dans le programme d'installation d'AXIS Device Manager Extend. Nous vous conseillons d'installer le contrôleur de site sur un serveur aussi proche que possible des périphériques.

1. Choisissez un serveur sur lequel vous souhaitez installer l'hôte edge.
2. Lancez le programme d'installation sur le serveur et sélectionnez uniquement l'installation de l'hôte edge.

Premiers pas

Demander l'hôte edge

Pour créer une connexion sécurisée vers les périphériques depuis l'application de bureau AXIS Device Manager Extend, vous devez d'abord demander un hôte edge à votre organisation.

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 (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 les périphériques)**.

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 les périphériques)**.

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

Pour regarder cette vidéo, accédez à la version Web de ce document.

help.axis.com/?&piaId=63389&section=remove-devices

Supprimer les périphériques d'un hôte edge

1. Cliquez sur **Edge host (Hôte Edge)**
2. Sélectionnez un hôte edge.
3. Accédez à **Devices (Périphériques)**
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 (Se connecter)**.

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 aux hôtes edge d'autres réseaux, vous devrez peut-être ajouter la configuration suivante à la « liste d'autorisation » du pare-feu du réseau de votre entreprise : Protocole du port du point terminal (Endpoint Port Protocol) signaling.prod.webrtc.connect.axis.com 443 HTTPS *.turn.prod.webrtc.connect.axis.com 443 HTTPS webRTC (Turn and P2P) 5349, 49152 - 65535 DTLS (UDP and TCP)

Supprimer un site

Avant de supprimer un hôte edge de l'organisation, vous devez *Supprimer les périphériques à la page 13* appartenant 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. Accédez à **Users (Utilisateurs)**.
3. Cliquez sur **Invite to organization (Inviter dans l'organisation)**.
4. Saisissez l'adresse e-mail de l'utilisateur que vous souhaitez inviter dans l'organisation.
5. Cliquez sur **Send invite (Envoyer invitation)**.

Remarque

L'utilisateur reçoit un e-mail d'invitation qu'il peut utiliser pour se connecter à AXIS Device Manager Extend. Le rôle d'utilisateur par défaut est **Viewer (Observateur)**. S'il 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.

Attribuer un rôle d'utilisateur

1. Sélectionnez l'organisation dans laquelle vous souhaitez configurer les paramètres utilisateur.

2. Accédez à **Users (Utilisateurs)**.
3. Accédez à **Role (Rôle)** pour l'utilisateur à promouvoir
4. Cliquez sur le menu déroulant pour sélectionner le nouveau rôle

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. Accédez à **Users (Utilisateurs)**.
3. Passez la souris sur l'utilisateur à supprimer pour afficher un nouveau menu d'options : **...**
4. Cliquez sur **...** et sélectionnez **Remove user (Supprimer l'utilisateur)** dans le menu déroulant.

Gestion du firmware

Gestion du firmware

Avec AXIS Device Manager Extend, vous pouvez gérer le firmware de plusieurs périphériques au niveau de chaque organisation.

Pour obtenir la liste des mises à jour de firmware disponibles pour chaque périphérique de votre organisation, regroupés par modèle, accédez à **Home > Firmware inventory (Accueil > Inventaire des firmwares)**. Pour obtenir la liste des mises à jour de firmware disponibles sur un hôte edge spécifique, sélectionnez l'hôte edge et accédez à **Firmware inventory (Inventaire des firmwares)**.

Gérer le firmware à partir du modèle de périphérique

Pour gérer le firmware à partir du modèle de périphérique dans l'ensemble de l'organisation :

1. Accédez à **Home > Firmware inventory (Accueil > Inventaire des firmwares)**
2. Cochez le modèle que vous souhaitez gérer.
3. Cliquez sur le menu déroulant **Update to (Mettre à niveau vers)** pour voir ce qui est disponible. Le firmware le plus récent est présélectionné.
4. Cliquez sur **Upgrade (Mettre à niveau)**.

Gérer le firmware du périphérique sur un hôte edge.

Pour gérer le firmware de certains ou de tous les périphériques sur 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 **Firmware** dans le menu Action
6. Vérifiez tous ou certains des modèles de la liste.
7. Pour modifier le firmware sélectionné, cliquez sur le firmware suggéré pour savoir ce qui est disponible pour chaque périphérique. Le firmware le plus récent est présélectionné.
8. Cliquez sur **Upgrade (Mettre à niveau)**.

Afficher les mises à niveau de firmware en cours et terminées

Pour afficher la liste des mises à niveau de firmware terminées et en cours dans votre organisation. Depuis **Home (Accueil)** :

1. Cliquez sur **Tasks (Tâches)**.

Pour afficher les mises à niveau de firmware en cours pour les périphériques connectés à un hôte edge donné :

1. Cliquez sur **Edge hosts (Hôtes Edge)**.
2. Cliquez sur l'hôte edge auquel vous voulez accéder.
3. Accédez à **Tasks (Tâches)**

Pour voir les mises à niveau de firmware en cours :

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

Politiques

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 **Create (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 **Create (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 (Sauvegarder)**.

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 (Sauvegarder)**

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 poltique est appliquée conserveront les paramètres de la politique, mais les paramètres ne sont plus persistants.

Dépannage

Dépannage

Comment configurer les paramètres du pare-feu

Afin que l'hôte edge et le client AXIS Device Manager Extend puissent communiquer avec le service Axis, les adresses IP et/ou les noms de domaines suivants doivent être ajoutés à la liste autorisée du pare-feu de l'organisation :

-
- 40.127.155.231 (UE)
- 52.224.128.152 ou 40.127.155.231 (États-Unis)
- Adresse IP DNS publique A

L'URL est une simple entrée DNS A avec une résolution en adresse IP 52.224.128.152 ou 40.127.155.231. Ces adresses IP hébergent une passerelle d'application unique qui transmet les requêtes à l'hôte principal approprié (en fonction du chemin de la requête entrante).

Le client AXIS Device Manager Extend et l'hôte edge utilisent le nom de domaine pour toutes les requêtes.

Pour ce faire, le réseau doit utiliser un DNS public (ou par exemple mettre en cache le nom de domaine dans un DNS local). Par conséquent, outre l'adresse IP de la passerelle d'application, une adresse IP de serveur DNS public doit également être ajoutée à la liste autorisée.

Par exemple : DNS public de Google, disponible sur les adresses IP : 8.8.8.8 et 8.8.4.4.

Manuel d'utilisation
AXIS Device Manager Extend

Ver. M16.2
Date : Mars 2023
Référence T10153497