AXIS D8204-E PoE++ Switch

Manuel d'utilisation

Table des matières

À propos de ce manuel 3
Abréviations 3
Vue d'ensemble de la solution 4
Démarrage 5
Accéder au produit depuis un navigateur 5
Connaître la page Web de votre produit 5
Connaître l'aide intégrée de votre produit 6
Exemples de configuration 7
Configurer les VLAN d'accès 7
Réserver une adresse IP en fonction de l'adresse MAC 8
Créer des liaisons redondantes entre les commutateurs pour la redondance de réseau 8
Utilisez VAPIX pour allumer ou éteindre le PoE sur un port 9
Configurer MACsec 9
CAK statique 9
CAK dynamique 10
Branchement d'un module SFP de 1 Gbit/s 12
Maintenance de votre système 13
Redémarrer le produit 13
Réinitialiser les paramètres à leurs valeurs par défaut 13
Mettre à niveau le logiciel du périphérique 14
Revenir à l'image alternative du logiciel 14
Caractéristiques techniques 15
Gamme de produits 15
Recherche de panne 16
Cybersécurité 17
Gestion des vulnérabilités 17
Notifications de sécurité 17
Cycle de vie du produit en sécurité 17

À propos de ce manuel

Remarque

Le produit est destiné à être utilisé par des administrateurs réseau responsables de l'exploitation et de la maintenance des équipements réseau. Des connaissances de base sur les fonctions générales du commutateur, la sécurité, le protocole IP (Internet Protocol) et le protocole SNMP (Simple Network Management Protocol) sont supposées.

Ce manuel d'utilisateur vous fournit des informations sur la manière dont vous pouvez:

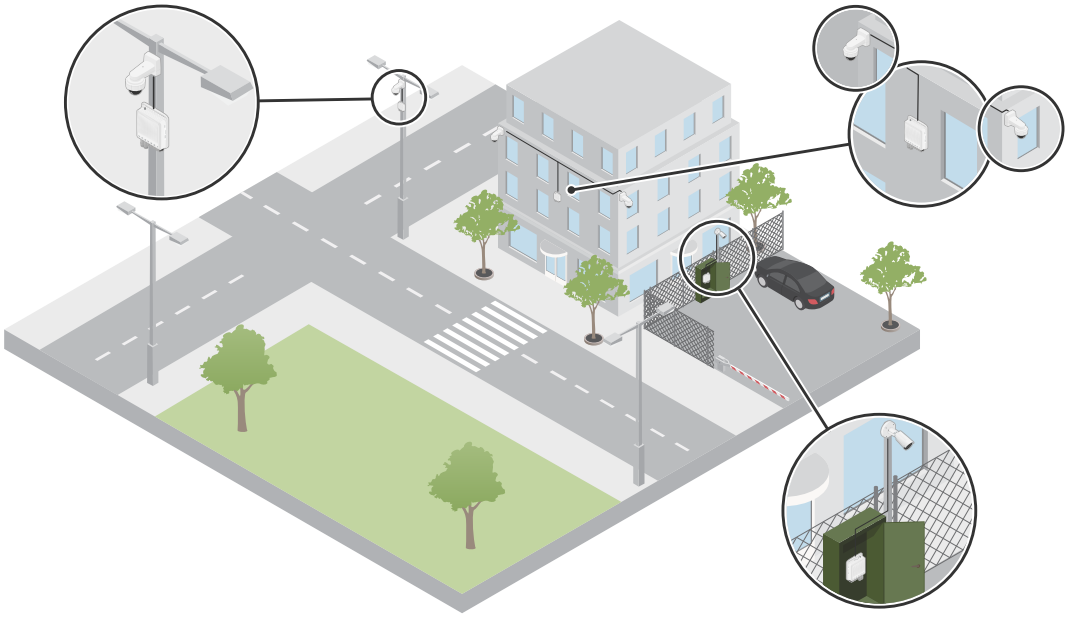
- accéder au produit
- effectuer des exemples de configurations
- réaliser la maintenance du produit

Les fonctionnalités du produit et leurs paramètres sont détaillés dans l'aide contextuelle intégrée du produit.

Abréviations

Abréviation	Description
MACsec	Sécurité du protocole MAC (Media Access Control)
802.1X	Contrôle d'accès réseau
802.1AE	Identique à MACsec
CAK	Clé de l'Association pour la connectivité
CKN	Nom de la clé de connectivité
DHCP	Dynamic Host Configuration Protocol (Protocole de configuration d'hôte dynamique)
OpenSSL	Bibliothèque de logiciels libres
PoE	Alimentation par Ethernet
RAYON	Remote Authentication Dial-in User Service
SFP	Interface fibre, Small Form-factor Plug (Émetteur-récepteur de petit facteur de forme)
SFP+	Prise améliorée à format compact
SNMP	Simple Network Management Protocol (Protocole simple de gestion de réseau)
SSL	Secure Sockets Layer
TLS	Transport Layer Security (sécurité de couche transport)
Réseau local virtuel (VLAN)	Réseau local virtuel

Vue d'ensemble de la solution



Les dispositifs AXIS edge sont installés sur les lieux et sont connectés aux commutateurs Axis par Ethernet. Les commutateurs sont reliés par une fibre .

Démarrage

Accéder au produit depuis un navigateur

Remarque

- Installez, connectez et mettez le dispositif sous tension comme indiqué dans le guide d'installation.
- Une fois que vous aurez suivi les étapes décrites dans cette section, vous accéderez à la page Web du produit et vous pourrez configurer et gérer le produit.

1. Utilisez AXIS IP Utility ou AXIS Device Manager pour trouver le périphérique sur le réseau. Pour plus d'informations sur la découverte des périphériques, allez à *axis.com/support*..
2. Saisissez le nom d'utilisateur et le mot de passe indiqués sur l'étiquette du produit.
   Le nom d'utilisateur par défaut est root (racine).
3. Suivez les étapes de l'assistant de configuration pour :

– Modifier le mot de passe (recommandé pour des raisons de sécurité)

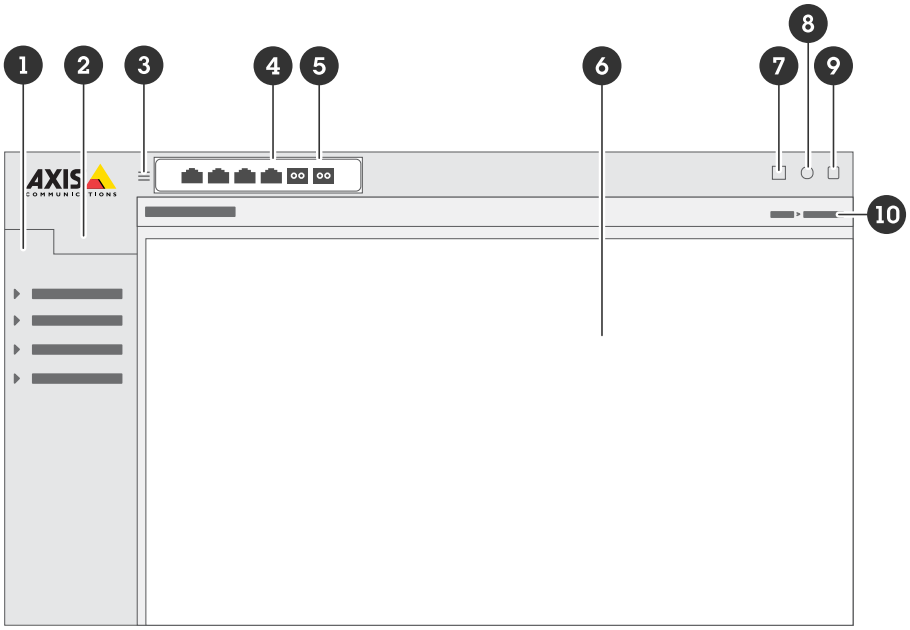
– Définir l'adresse IP via DHCP ou manuellement

– Définir les informations de date et d'heure

– Définissez les informations système

4. Cliquez sur **Save (Enregistrer)**.
5. Reconnectez-vous avec le nouveau mot de passe.

Connaître la page Web de votre produit



1 Fonctionnalités de base
2 Fonctionnalités avancées
3 Bouton de basculement - pour masquer ou démasquer le menu
4 LED de statut des ports RJ45
5 LED de statut des ports SFP
6 Zone de contenu pour fonctionnalités de base/avancées
7 Bouton « Sauvegarder » - Sauvegarder vos paramètres dans le fichier de configuration de démarrage.
8 Bouton Aide : accès à l'aide contextuelle intégrée
9 Bouton Se déconnecter
10 Chemin d'accès au menu

Connaître l'aide intégrée de votre produit

Votre produit dispose d'une aide contextuelle intégrée. L'aide fournit des informations plus détaillées sur les fonctions de base et avancées du produit ainsi que leurs paramètres. Pour accéder au contenu de l'aide pour une vue donnée, cliquez sur

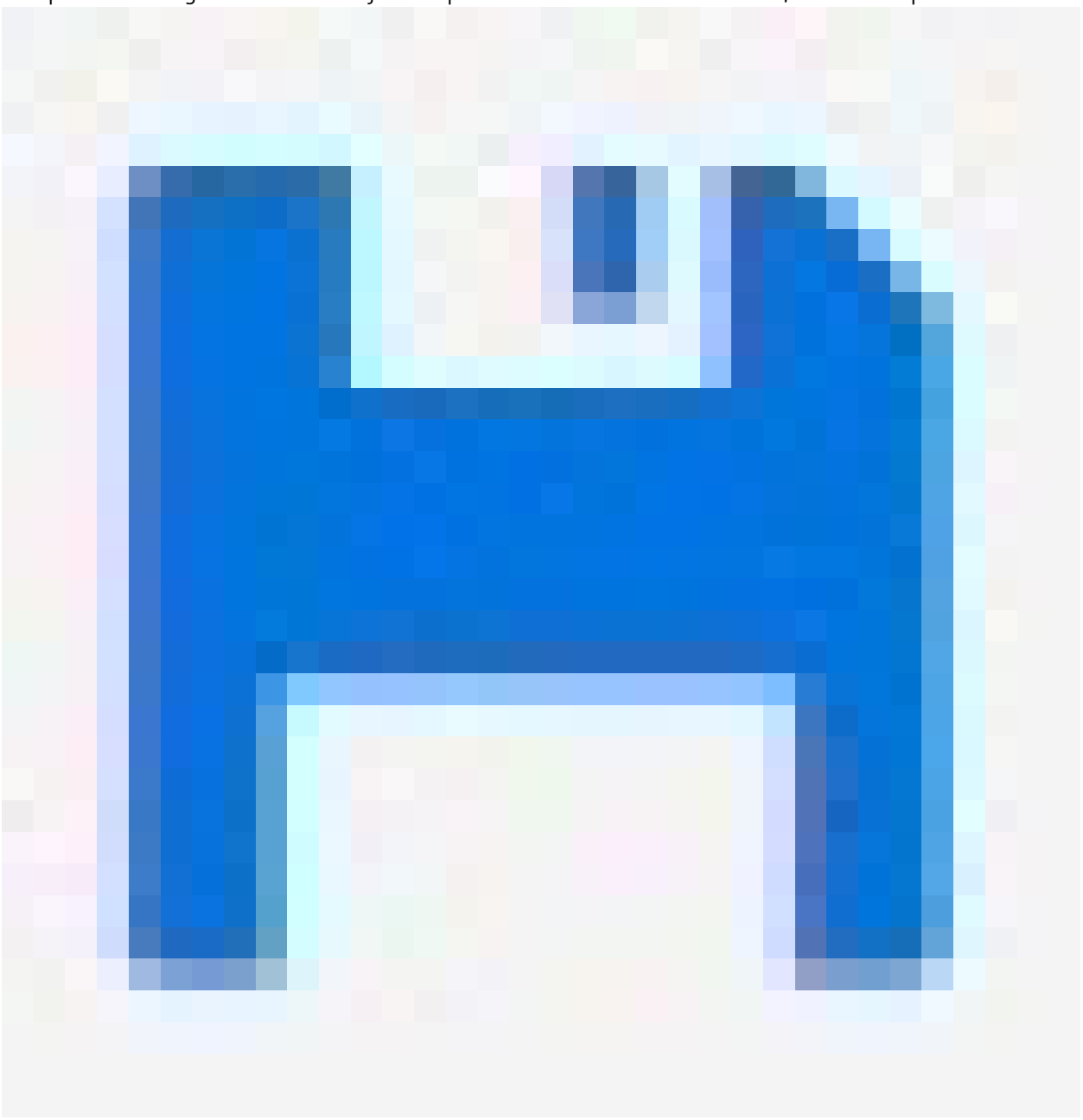


. Le contenu de l'aide peut également comporter des termes et des acronymes cliquables, expliqués plus en détail dans le glossaire intégré.

Exemples de configuration

Remarque

Lorsque vous configurez ou mettez à jour les paramètres de votre commutateur, veillez à cliquer sur



pour sauvegarder les mises à jour dans le fichier de configuration de démarrage.

Le fichier de configuration de démarrage est conservé lorsque vous redémarrez ou réinitialisez le commutateur, mais pas après avoir réinitialisé le commutateur aux paramètres des valeurs par défaut.

Configurer les VLAN d'accès

Des VLAN sont généralement utilisés sur de grands réseaux pour créer plusieurs domaines de diffusion, mais ils peuvent également être utilisés pour séparer le trafic réseau. Par exemple, le trafic vidéo peut faire partie d'un VLAN et un autre trafic réseau peut faire partie d'un autre.

1. Allez à **Advanced (Avancé)** > **VLANs (Réseaux locaux virtuels (VLAN))** > **Configuration**.
2. Sous **Global VLAN Configuration (Configuration globale des réseaux locaux virtuels (VLAN)**, dans le champ **Allowed Access VLANs (Réseaux locaux virtuels (VLAN) à accès autorisé)**, saisissez les identifiants des réseaux locaux virtuels (VLAN) à créer. Par exemple, si vous saisissez : 1, 10-13, 200,

300, les identifiants de réseaux locaux virtuels (VLAN) suivants seront créés : 1, 10, 11, 12, 13, 200 et 300.

3. Pour attribuer un port donné à un identifiant de réseau local virtuel (VLAN) créé sous **Port VLAN Configuration (Configuration de réseau local virtuel (VLAN)**, saisissez l'identifiant dans le champ **Port VLAN (Réseau local virtuel (VLAN) du port)**.
4. Cliquez sur **Save (Enregistrer)**.

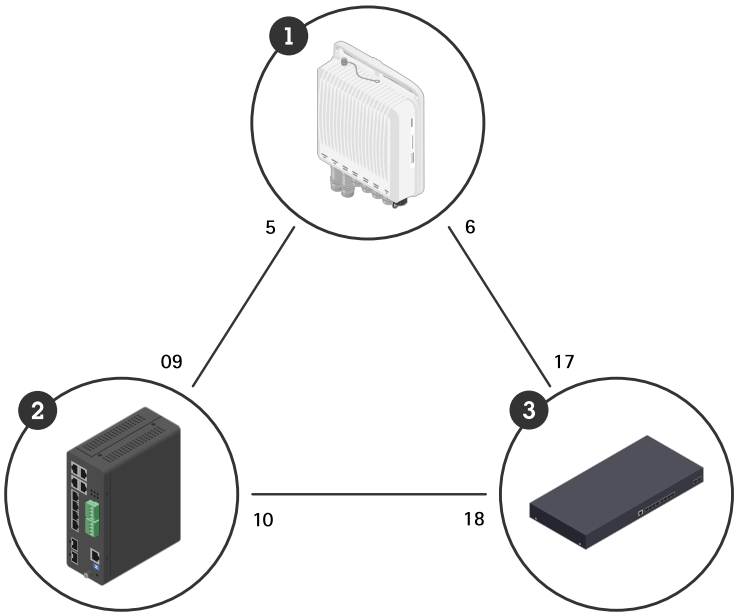
Réserver une adresse IP en fonction de l'adresse MAC

1. Allez à **Advanced (Avancé)** > **DHCP** > **Server (Serveur)** > **Configuration** > **Pool**.
2. Cliquez sur **Add New Pool (Ajouter nouveau pool)**.
3. Saisissez un nom pour le pool et cliquez sur **Save (Sauvegarder)**. Aucun espace n'est autorisé dans le nom.
4. Pour accéder aux paramètres du pool, cliquez sur le nom ajouté.
5. Dans le menu déroulant **Type**, sélectionnez **Host (Hôte)**.
6. Saisissez les autres paramètres requis, notamment Adresse **IP**, **Subnet Mask (Masque de sous-réseau)** et **Default Router (Routeur par défaut)**.
7. Dans le menu déroulant **Client Identifier (Identifiant client)**, sélectionnez **MAC**.
8. Dans le champ **Hardware Address (Adresse du matériel)**, saisissez l'adresse MAC du périphérique.
9. Cliquez sur **Save (Enregistrer)**.

Créer des liaisons redondantes entre les commutateurs pour la redondance de réseau

Si la redondance de réseau est requise, vous pouvez créer des liaisons redondantes entre les commutateurs avec une configuration d'arbre maximal.

Exemple:
Dans cet exemple, les commutateurs AXIS D8204-E (1), AXIS D8208-R (2), et AXIS T8516 (3) sont reliés par une liaison redondante, sans réseaux locaux virtuels (VLAN) supplémentaire. En cas d'échec de l'une des liaisons montantes entre les commutateurs, la liaison redondante est activée et procure la connectivité réseau.



Nom de dispositif	Nom du modèle	Ports CIST
Commutateur - 01	AXIS D8204-E	5, 6
Commutateur - 02	AXIS D8208-R	9, 10
Commutateur - 03	AXIS T8516	17, 18

Pour créer une liaison redondante sur la page Web de chaque commutateur :

1. Allez à **Advanced (Avancé)** > **Spanning Tree** > **Configuration** > **Bridge Settings (Paramètres de pont)**.
2. Sous **Basic Settings (Paramètres de base)** dans le menu déroulant **Protocol Version (Version de protocole)**, sélectionnez **RSTP**, et cliquez sur **Save (Sauvegarder)**.
3. Allez à **Advanced (Avancé)** > **Spanning Tree** > **Configuration** > **CIST Port (Port CIST)**.
4. Sous **CIST Normal Port Configuration (Configuration normale de port CIST)**, assurez-vous que **STP Enabled (STP activé)** est sélectionné pour les ports du commutateur comme suit :

- Commutateur - 01 : ports 5 et 6
- Commutateur - 02 : ports 9 et 10
- Commutateur - 03 : ports 17 et 18

5. Cliquez sur **Save (Enregistrer)**.

Remarque

Si vous souhaitez vous assurer qu'un port donné est utilisé comme liaison de communication principale, saisissez **Path Cost (Coût de trajet)** pour ce port sous **CIST Normal Port Configuration (Configuration normale de port CIST)**. S'il n'est pas spécifié, le commutateur sélectionne automatiquement le port. Par exemple, si vous souhaitez utiliser le port 17 comme liaison de communication principale, saisissez la valeur **Path Cost (Coût de trajet)** 10 pour le port 6 et la valeur **Path Cost (Coût de trajet)** 50 pour le port 18.

Utilisez VAPIX pour allumer ou éteindre le PoE sur un port

Vous pouvez utiliser les commandes suivantes dans VAPIX pour allumer ou éteindre le PoE pour un port spécifique :

- Allumer le PoE :
  `http://[IP address of the switch]/axis-cgi/nvr/poe/setportmode.cgi?port=[number of the port on the switch]&enabled=yes&schemaversion=1`
- Éteindre le PoE :
  `http://[IP address of the switch]/axis-cgi/nvr/poe/setportmode.cgi?port=[number of the port on the switch]&enabled=no&schemaversion=1`

Configurer MACsec

La configuration MACsec établit une connexion sécurisée entre deux dispositifs compatibles MACsec, afin de garantir que les communications entre vos dispositifs soient confidentielles, soumises à l'authentification et protégées contre les attaques par rejeu.

CAK statique

Une clé d'association de connectivité (CAK) est une clé cryptographique qui garantit la sécurité des communications entre les dispositifs. Elle doit comporter 32 caractères hexadécimaux pour une clé de 128 octets ou 64 caractères hexadécimaux pour une clé de 256 octets.

Un nom de clé de connectivité (CKN) identifie la clé permettant d'établir une connexion MACsec sécurisée entre des dispositifs et garantit que seuls les dispositifs autorisés puissent participer à la communication sécurisée. Le CKN doit comporter entre 2 et 64 caractères hexadécimaux et le nombre de caractères doit être pair. Le CKN identifie le CAK à utiliser et tant le CAK aue le CKN doivent correspondre aux deux extrémités de la liaison pour établir une communication MACsec.

Vous pouvez créer les fichiers CAK et CKN manuellement ou les générer à l'aide d'OpenSSL.

Générer des fichiers CAK et CKN avec OpenSSL

1. Ouvrez une invite de commande sur un ordinateur sur lequel OpenSSL est installé.
2. Pour générer un CAK :
   - Saisissez `openssl rand -hex 16`.
   - Appuyez sur Enter (Entrée).
3. Pour générer un CKN :
   - Saisissez `openssl rand -hex 8`.
   - Appuyez sur Enter (Entrée).
4. Sauvegardez les fichiers CAK et CKN. Vous en aurez besoin plus tard.

Configurer un dispositif AXIS OS

1. Dans l'interface web du dispositif, allez à **System (Système)** > **Security (Sécurité)** > **Network access control and encryption (Contrôle d'accès au réseau et chiffrement)**.
2. Pour **Authentication method (Méthode d'authentification)**, sélectionnez **IEEE 802.1AE MACsec (Static CAK/Pre-Shared Key) (IEEE 802.1AE MAXCsec (Clé CAK statique/pré-partagée)**.
3. Pour **Key agreement connectivity association key name (Nom de la clé d'association de connectivité de l'accord de clés)**, saisissez le CKN.
4. Pour **Key agreement connectivity association key (Clé d'association de connectivité de l'accord de clés)**, saisissez le CAK.
5. Cliquez sur **Save (Enregistrer)**.

Configurer le commutateur

1. Dans l'interface web du commutateur, allez à **Advanced (Avancé)** > **Security (Sécurité)** > **MACsec** > **Configuration** > **Policies (Politiques)**.
2. Cliquez sur **Add Policy (Ajouter une politique)**.
3. Saisissez un nom pour la politique.
4. Sélectionnez **Enable (Activer)** et saisissez les codes CAK et CKN que vous avez générés.
5. Cliquez sur **Save (Enregistrer)**.
6. Allez à **Advanced (Avancé)** > **Security (Sécurité)** > **MACsec** > **Configuration** > **Interfaces**.
   - Pour l'**Interface** connectée au dispositif, sélectionnez la nouvelle politique dans la liste déroulante.
   - Cliquez sur **Save (Enregistrer)**.

Vérifiez la connexion

1. Dans l'interface web du commutateur, allez à **System (Système)** > **Security (Sécurité)** > **MACsec** > **Status (État)** > **Status (État)**.
2. Vérifiez que **State (État)** affiche un indicateur d'état vert.

CAK dynamique

Lq CAK est générée à l'issue d'un processus d'authentification et de gestion des clés utilisant la norme IEEE 802.1X et un serveur d'authentification. Cela vous permet de générer et de gérer des clés de manière dynamique, ce qui vous évite d'avoir à effectuer une configuration manuelle des clés à long terme.

Remarque

- Assurez-vous qu'un serveur RADIUS est configuré et accessible sur le réseau.
- Installez le *Certificat CA de l'identifiant de périphérique Axis* sur le serveur RADIUS.

Configurer le dispositif connecté

1. Dans l'interface web du dispositif, allez à **System (Système)** > **Security (Sécurité)** > **Network access control and encryption (Contrôle d'accès au réseau et chiffrement)**.
2. Pour **Authentication method (Méthode d'authentification)**, sélectionnez **IEEE 802.1X EAP-TLS / IEEE 802.1AE MACsec (CAK dynamique)**.
3. Pour **Client certificate (Certificat client)**, sélectionnez le certificat d'identifiant de dispositif auquel le serveur RADIUS accorde sa confiance<. Le serveur d'authentification utilise le certificat CA pour valider l'identité du client.
4. Pour **Certificats CA**, lorsqu'aucun certificat n'est sélectionné, le dispositif effectue l'authentification quel que soit le réseau auquel il est connecté.
5. Pour **EAP Identity (Identité EAP)**, saisissez l'identité de l'utilisateur associée au certificat client. L'identité EAP doit correspondre au champ Common Name (Nom commun) (CN) du certificat client sélectionné.
6. Dans la liste **EAPOL Version (des versions d'EAPOL)**, sélectionnez la version utilisée par le commutateur réseau.
7. Activez **Use IEEE 802.1x (Utiliser IEEE 802.1X)** pour utiliser le protocole IEEE 802.1x.
8. Cliquez sur **Save (Enregistrer)**.

Configurer le protocole 802.1X sur le commutateur

1. Dans l'interface web du commutateur, allez à **Advanced (Avancé)** > **Security (Sécurité)** > **Radius** > **Configuration**.
2. Cliquez sur **Add new server (Ajouter un nouveau serveur)**, puis saisissez le nom d'hôte et le mot de passe.
3. Cliquez sur **Save (Enregistrer)**.
4. Allez à **Advanced (Avancé)** > **Spanning Tree** > **Configuration** > **CIST Ports (Ports CIST)**.
5. Effacez la case **STP Enabled (STP activé)** correspondant au port connecté à votre dispositif.
6. Cliquez sur **Save (Enregistrer)**.
7. Allez à **Advanced (Avancé)** > **Security (Sécurité)** > **802.1X** > **Configuration**.
8. Dans la liste **Mode**, sélectionnez **Enabled (Activé)**.
9. Pour le port concerné, définissez **Admin state (État d'administration)** sur **Port-based 802.1X (802.1X basé sur le port)** .
10. Cliquez sur **Save (Enregistrer)**.

Vérifier la connexion 802.1x

1. Dans l'interface web du dispositif, allez à **System (Système)** > **Security (Sécurité)**.
2. Vérifiez que l'indicateur d'état **802.1X authorised (802.1X autorisé)** est vert.

Configurer MACsec sur le commutateur

1. Dans l'interface web du commutateur, allez à **Advanced (Avancé)** > **Security (Sécurité)** > **MACsec** > **Configuration** > **Policies (Politiques)**.
2. Cliquez sur **Add policy (Ajouter une politique)** et saisissez un nom pour la politique.
3. Cliquez sur **Save (Enregistrer)**.
4. Allez à **Advanced (Avancé)** > **Security (Sécurité)** > **MACsec** > **Configuration** > **Interfaces**.
5. Pour l'interface connectée au dispositif, sélectionnez la politique nouvellement créée dans la liste.
6. Cliquez sur **Save (Enregistrer)**.

Vérifier la connexion MACsec

1. Allez à **System (Système)** > **Security (Sécurité)** > **MACsec** > **Status (État)** > **Status (État)**.

2. Vérifiez que **State (État)** affiche un indicateur d'état vert.

Remarque

Si l'état de la connexion reste « en attente, redémarrez le dispositif.

Branchement d'un module SFP de 1 Gbit/s

1. Allez à **Advanced (Avancé)** > **Ports** > **Configuration**.
2. Pour le port de connexion du module (5 ou 6), définissez **Configured (Configuré)** sur **1 Gops FDX (1 Gops FDX)**.

Remarque

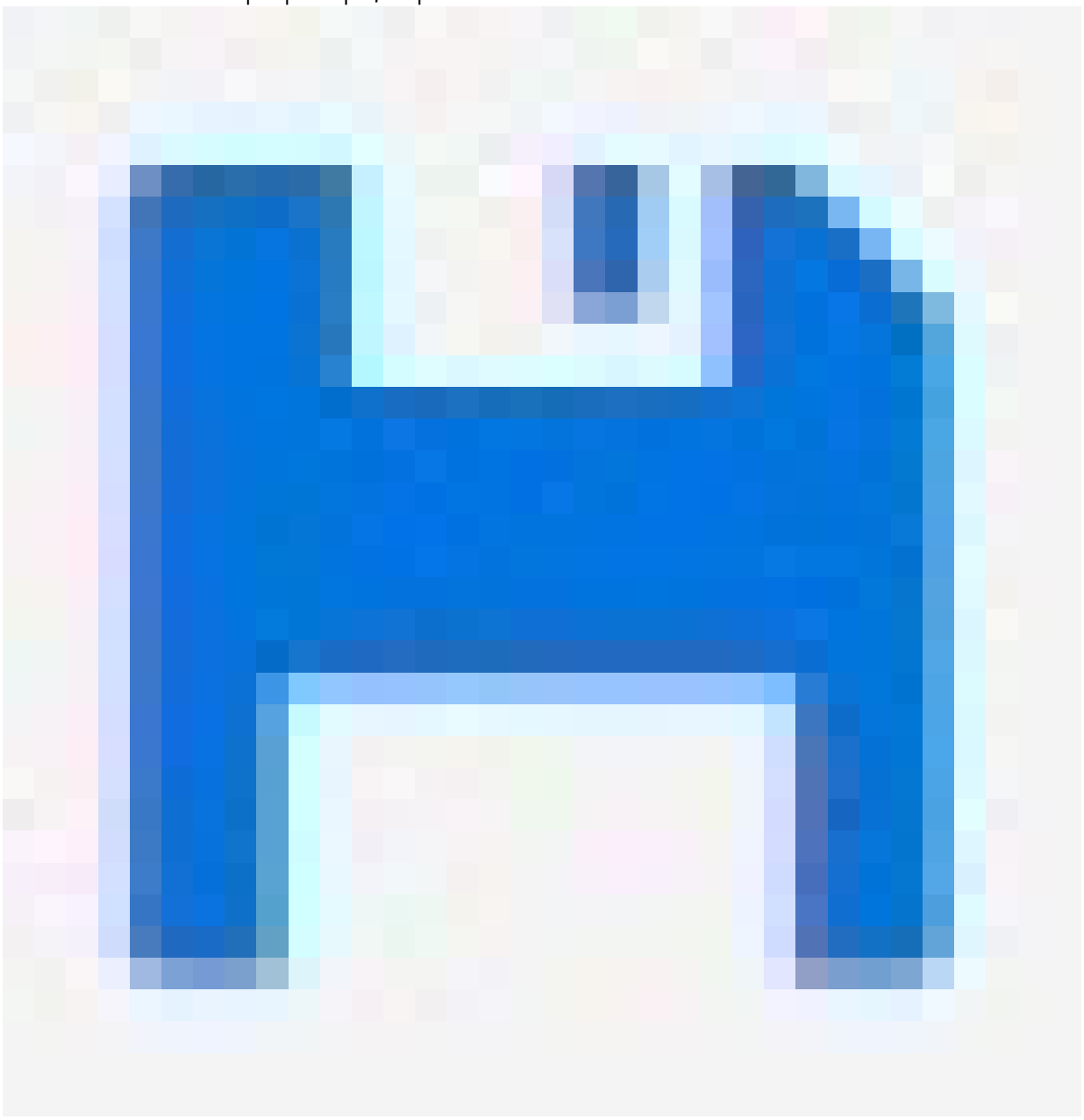
Si vous définissez le port sur **Auto**, SFP et SFP+ fonctionnent tous les deux.

Maintenance de votre système

Redémarrer le produit

Remarque

- Le trafic à travers le produit est affecté pendant le redémarrage.
- Avant de redémarrer le périphérique, cliquez sur



pour sauvegarder vos paramètres dans le fichier de configuration de démarrage.

1. Allez à **Advanced (Avancé)** > **Maintenance (Entretien)** > **Restart Device (Redémarrer le dispositif)**.
2. Cliquez sur **Yes (Oui)**. Après le redémarrage, le produit s'initialise normalement.

Réinitialiser les paramètres à leurs valeurs par défaut

Important

Toute configuration sauvegardée sera restaurée aux valeurs par défaut.

1. Allez à **Advanced (Avancé)** > **Maintenance (Entretien)** > **Factory Defaults (Valeurs par défaut)**.
2. Cliquez sur **Yes (Oui)**.

Suivez les étapes suivantes pour rétablir les valeurs par défaut si vous avez oublié le mot de passe :

1. Débranchez tous les éléments connectés au commutateur, y compris l'alimentation électrique.
2. Reliez les ports 1 et 2 à l'aide d'un câble RJ45.
3. Branchez le câble d'alimentation et mettez le commutateur sous tension.
4. Au bout de 5 minutes, débranchez le câble RJ45. Le câble d'alimentation devrait rester branché.
5. Connectez l'unité à l'ordinateur et l'adresse IP devrait revenir à l'adresse IP par défaut, à savoir 192.168.0.254.
6. Allez à **Advanced (Avancé)** > **Maintenance (Entretien)** > **Factory Defaults (Valeurs par défaut)**.
7. Cliquez sur **Yes (Oui)**.

Mettre à niveau le logiciel du périphérique

Important

La mise à niveau du logiciel prend jusqu'à 10 minutes. Ne redémarrez pas ou ne mettez pas le périphérique hors tension pendant la mise à niveau.

Remarque

Le trafic à travers le produit est affecté pendant la mise à niveau.

1. Allez à **Advanced (Avancé)** > **Maintenance (Entretien)**> **Device Software (Logiciel du dispositif)** > **Software Upgrade (Mise à niveau du logiciel)**.
2. Pour sélectionner le fichier du logiciel à partir d'un emplacement spécifié, cliquez sur **Select file... (Sélectionner fichier...)**.
3. Cliquez sur **Upgrade** [Mettre à niveau].

Après la mise à niveau du logiciel, le produit redémarre normalement.

Revenir à l'image alternative du logiciel

Vous pouvez choisir d'utiliser l'image alternative (sauvegarde) du logiciel au lieu de l'image active (principale) du logiciel sur le produit. Les tableaux d'informations sur les deux images se trouvent dans **Advanced (Avancé) > Maintenance (Maintenance)> Device Software (Logiciel du périphérique) > Software Selection (Sélection du logiciel)**.

Remarque

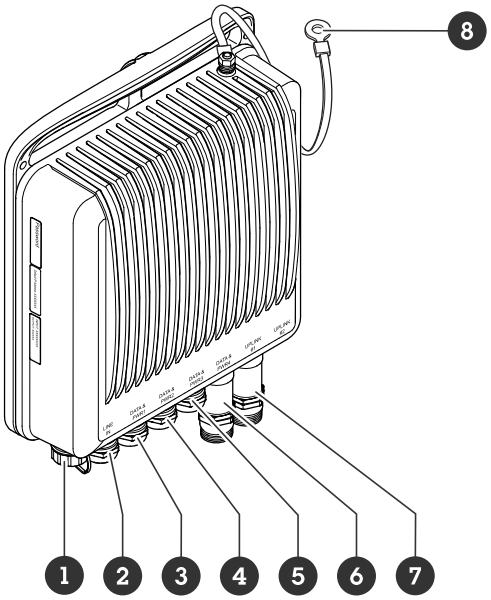
- Si l'image active est déjà définie en tant qu'image alternative, seul le tableau **Active Image (Image active)** est affiché et le bouton **Activate Alternate Image (Activer l'image alternative)** est désactivé.
- Si l'image alternative est déjà définie en tant qu'image active (manuellement ou en raison d'une image principale corrompue) et une nouvelle image du logiciel est chargée sur le produit, la nouvelle image est automatiquement définie en tant qu'image active.
- Les informations sur la version et la date du logiciel peuvent être vides sur les anciennes versions du logiciel. Cela est normal.

Pour définir l'image alternative en tant qu'image active :

1. Allez à **Advanced (Avancé) > Maintenance (Maintenance) > Device Software (Logiciel du périphérique) > Software Selection (Sélection du logiciel)**.
2. Cliquez sur **Activate Alternate Image (Activer l'image alternative)**.

Caractéristiques techniques

Gamme de produits



1 Port du connecteur d'alimentation
2 – 5. Port RJ45 PoE
6 – 7. Prise SFP
8 Câble de mise à la terre

Recherche de panne

Problèmes d'accès au périphérique

Impossible de se connecter lors de l'accès au périphérique à partir d'un navigateur

Lorsque le protocole HTTPS est activé, assurez-vous d'utiliser le protocole approprié (HTTP ou HTTPS) lorsque vous essayez de vous connecter. Il est possible que vous deviez taper manuellement `http` ou `https` dans le champ d'adresse du navigateur.

Si vous avez perdu le mot de passe pour le compte root, il est nécessaire de réinitialiser le périphérique aux paramètres des valeurs par défaut. Pour des instructions, voir *Réinitialiser les paramètres à leurs valeurs par défaut, on page 13*.

L'adresse IP a été modifiée par DHCP.

Les adresses IP obtenues auprès d'un serveur DHCP sont dynamiques et pourraient changer. Si l'adresse IP a été modifiée, utilisez AXIS IP Utility ou AXIS Device Manager pour trouver le périphérique sur le réseau. Identifiez le périphérique à partir de son numéro de modèle ou de série ou de son nom DNS (si le nom a été configuré).

Si vous avez besoin d'aide supplémentaire, allez à *axis.com/support* ou *Axis Network Switches Configuration Guide*.

Cybersécurité

La cybersécurité contribue à la réussite du cycle de vie des produits tout en minimisant les risques. Vous trouverez des informations détaillées et de la documentation sur notre approche en matière de cybersécurité à l'adresse *axis.com/about-axis/cybersécurité*. Suivez les consignes de cybersécurité ci-dessous pour recevoir les notifications de sécurité d'Axis concernant votre produit et pour configurer votre produit de manière à garantir la sécurité tout au long de son cycle de vie et lors de la mise hors service.

Sur le site *Axis Trust Center*, vous trouverez des informations sur la manière dont Axis met en œuvre la conformité en matière de sécurité, la transparence, la protection des données et la confidentialité.

Gestion des vulnérabilités

Axis est une *autorité de numérotation CVE (Common Vulnerability and Exposures) (CNA)*. Afin de réduire au minimum les risques d'exposition, nous respectons les normes du secteur lors de l'identification et de la correction des vulnérabilités de nos dispositifs, logiciels et services. Pour plus d'informations sur notre politique de gestion des vulnérabilités ou pour signaler une vulnérabilité, veuillez consulter *axis.com/vulnerability-management*.

Notifications de sécurité

Abonnez-vous aux e-mails de notification de sécurité d'Axis sur *axis.com/security-notification-service*. Nous vous enverrons des informations concernant les vulnérabilités, les avis de sécurité correspondants et d'autres questions liées à la sécurité de votre produit Axis.

Cycle de vie du produit en sécurité

Axis minimise les risques tout au long du cycle de vie de ses produits grâce à une gestion sécurisée de ce cycle. Consultez nos guides de renforcement de la sécurité sur *help.axis.com* pour configurer et faire fonctionner vos produits Axis de manière plus sécurisée, et pour obtenir des informations sur :

Première utilisation sécurisée – Les produits Axis sont configurés avec un niveau de protection élevé par défaut afin de garantir une mise en service sécurisée et des communications cryptées dès le départ.

Utilisation prévue et erreurs de configuration courantes – Nos guides fournissent des informations sur l'utilisation prévue des produits Axis, y compris les erreurs courantes de configuration et les mauvaises pratiques en matière de sécurité qu'il convient d'éviter.

Gestion des vulnérabilités et transparence de la chaîne d'approvisionnement – Une liste des composants du logiciel (SBOM) est publiée à chaque nouvelle version du logiciel sur *axis.com* afin de signaler les vulnérabilités et d'améliorer la transparence de la chaîne d'approvisionnement.

Mise hors service et effacement sécurisé des données – Pour mettre hors service un produit en toute sécurité lorsqu'il arrive en fin de vie, réinitialisez-le aux paramètres des valeurs par défaut. Cela effacera vos configurations, vos données enregistrées et vos informations sensibles.

T10231182_fr

2026-11 (M1.17)

© 2025 – 2026 Axis Communications AB