Guide de renforcement de la sécurité d'AXIS OS

Portail AXIS OS | *Guide AXIS OS Forensics* | *Guide du scanner de vulnérabilités AXIS OS* | *Avis de sécurité* | *Notes de mise à jour AXIS OS* | *Base de connaissances AXIS OS* | *Liste de lecture YouTube AXIS OS*

Introduction

Le guide de renforcement de la sécurité d'AXIS OS fournit des conseils pratiques pour renforcer la sécurité des dispositifs Axis fonctionnant sous AXIS OS. Il décrit les paramètres de configuration, les fonctionnalités et les pratiques opérationnelles recommandés qui contribuent à réduire la surface d'attaque, à protéger les données et à garantir un fonctionnement fiable tout au long du cycle de vie du dispositif. Le guide est destiné aux administrateurs système, aux intégrateurs et aux professionnels de la sécurité qui souhaitent déployer et entretenir les produits Axis de manière sécurisée et résiliente, conformément aux meilleures pratiques du secteur.

Configuration de l'interface Web
Le guide fait référence à la configuration des paramètres des périphériques dans l'interface Web du périphérique Axis. Le chemin d'accès à la configuration est différent selon la version d'AXIS OS installée sur le périphérique :

Version d'AXIS OS	Chemin de configuration de l'interface Web
< 7.10	Configuration > Options système > Sécurité > IEEE 802.1X
7.10	Paramètres > Sécurité > Système
≥ 10.9	Système > Sécurité

Portée

Ce guide s'applique à tous les produits basés sur AXIS OS exécutant AXIS OS (cycle LTS ou actif), ainsi qu'aux produits existants exécutant les logiciels de dispositif 4.xx et 5.xx.

Les produits basés sur AXIS OS sont destinés à être utilisés dans des systèmes de sécurité professionnels ou d'intelligence économique et sont conçus pour être intégrés à d'autres produits, tels que des systèmes de gestion vidéo (VMS) et des applications de gestion des dispositifs.

Le produit peut être utilisé dans des environnements non professionnels par des personnes ayant des compétences techniques, mais il n'est pas conçu ni destiné à être utilisé à domicile par des consommateurs individuels.

Le produit suit une approche sécurisée par défaut, mais pour atteindre des niveaux de sécurité plus élevés, il est important de suivre ce guide de renforcement de la sécurité. Pour certains systèmes intégrés, des guides de conception de systèmes sécurisés sont disponibles à l'adresse suivante : *help.axis.com*.

Niveaux de protection CIS

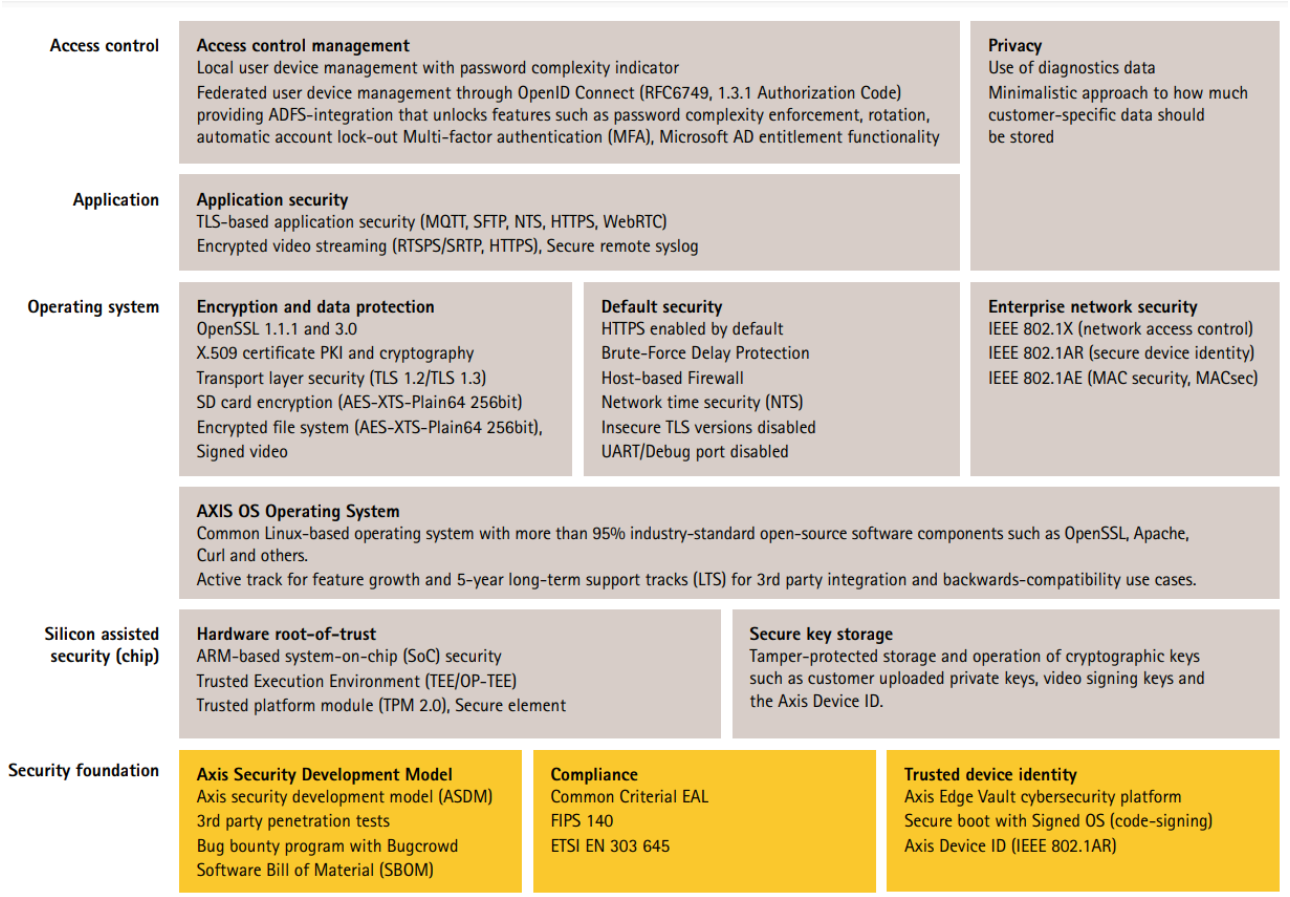
Nous appliquons les méthodes décrites dans les contrôle de sécurité du Center for Internet Safety (CIS) version 8 pour structurer nos recommandations en matière de cybersécurité. Les contrôles CIS, anciennement connus sous le nom de SANS Top 20 Critical Security Controls, fournissent 18 catégories de contrôles de sécurité critiques (CSC) centrés sur la gestion des catégories de risques de cybersécurité les plus courantes au niveau d'une organisation.

Ce guide fait référence aux contrôles de sécurité critiques en ajoutant le numéro CSC (**n° CSC**) pour chaque sujet de renforcement. Pour plus d'informations sur les catégories CSC, consultez la section *18 CIS Critical Security Controls* à l'adresse cisecurity.org.

Protection par défaut

Les périphériques Axis sont protégés par défaut. Il existe plusieurs contrôles de sécurité que vous n'avez pas besoin de configurer. Ces contrôles offrent un niveau de base de protection des périphériques et servent de base pour un renforcement plus étendu.

Le diagramme de l'architecture de sécurité d'AXIS OS présente les capacités de cybersécurité d'AXIS OS à travers différentes couches. Il donne un aperçu complet de la base de sécurité, de la sécurité assistée par silicium, du système d'exploitation AXIS OS et de la couche d'application et de contrôle d'accès.



Faites un clic droit et ouvrez l'image dans un nouvel onglet pour une meilleure expérience visuelle.

Authentification

Désactivé par défaut

CSC n°4 : Configuration sécurisée des ressources et logiciels d'entreprise

Le périphérique Axis ne fonctionne pas tant que le mot de passe administrateur n'a pas été défini.

Une fois le mot de passe administrateur configuré, l'accès aux fonctions d'administrateur et/ou aux flux de données vidéo n'est possible qu'au moyen de l'authentification des identifiants nom d'utilisateur et mot de passe valides. Il est déconseillé d'utiliser des fonctionnalités permettant un accès non automatique, notamment le visionnage anonyme et la multidiffusion permanente.

Pour savoir comment configurer l'accès aux périphériques, consultez la section relative à *l'accès aux périphérique* dans AXIS OS Knowledge base.

Authentification Digest

CSC n° 3 : Protection des pertes de données

Les clients accédant au périphérique s'authentifiera avec un mot de passe qui doit être crypté lors de son envoi sur le réseau. Nous vous recommandons d'activer HTTPS comme décrit ici. Si cela n'est pas possible, nous vous recommandons d'utiliser uniquement l'authentification Digest au lieu de l'authentification de base ou à la fois l'authentification de base et l'authentification Digest. Cela réduit le risque que des renifleurs réseau s'emparent du mot de passe.

Version d'AXIS OS	Chemin de configuration de l'interface Web
< 7.10	Configuration > Options système > Avancé > Configuration ordinaire > Réseau > Politique d'authentification HTTP réseau
7.10	Paramètres > Système > Configuration ordinaire > Réseau > Politique d'authentification HTTP réseau
≥ 10.9	Système > Configuration ordinaire > Réseau > Politique d'authentification HTTP réseau

Protection contre les attaques par relecture ONVIF

CSC n° 3 : Protection des pertes de données

La protection contre les attaques par relecture est une fonction de sécurité standard activée par défaut sur les périphériques Axis. Son objectif est de sécuriser suffisamment l'authentification des utilisateurs basée sur ONVIF en ajoutant un en-tête de sécurité supplémentaire, qui inclut le Nom d'utilisateur, un horodatage valide, la circonstance et le Digest de mot de passe. Le Digest de mot de passe est calculé à partir du mot de passe (qui est déjà stocké dans le système), la circonstance et l'horodatage. Le Digest de mot de passe a pour objectif de valider l'utilisateur et d'empêcher les attaques de relecture, ce qui explique pourquoi les Digests sont mis en cache. Nous vous recommandons de conserver ce paramètre activé.

Version d'AXIS OS	Chemin de configuration de l'interface Web
< 7.10	Configuration > Options système > Avancé > Configuration ordinaire > Système > Activer la protection contre les attaques par relecture
7.10	Paramètres >Système > Configuration ordinaire > Service Web > Protection contre les attaques par relecture
≥ 10.9	Système > Configuration ordinaire > Service Web > Protection contre les attaques par relecture

Empêcher les attaques par force brute

CSC n°4 : Configuration sécurisée des ressources et logiciels d'entreprise
CSC n°13 : Surveillance et défense réseau

Les périphériques Axis disposent d'un mécanisme de prévention permettant d'identifier et de bloquer les attaques par force brute en provenance du réseau, par exemple la découverte de mot de passe. Cette fonction, appelée protection contre les attaques par force brute, est disponible dans AXIS OS 7.30 et ultérieur.

La protection contre les retards dus aux attaques par force brute est activée par défaut à partir de la version 11.5 d'AXIS OS. Pour des exemples de configuration détaillés et des recommandations, voir *Protection contre les retards dus aux attaques par force brute* dans la base de connaissances d'AXIS OS.

Version d'AXIS OS	Chemin de configuration de l'interface Web
< 7.10	N/A
7.10	Paramètres > Système > Configuration ordinaire > Système > Prévention des attaques par déni de service (DoS)
≥ 10.9	Système > Sécurité > Prévenir les attaques par force brute

Journal d'audit

CSC n°1 : Inventaire et contrôle des ressources d'entreprise
CSC n°8 : Gestion des journaux d'audit

Les journaux d'audit sont utilisés à des fins liées à la cybersécurité, tels que la gestion des incidents, et contribuent à mettre en place une surveillance à long terme des événements et actions pertinents. Nous recommandons d'utiliser un serveur syslog distant ou une autre application de surveillance réseau afin que le dispositif Axis puisse envoyer ses journaux vers un environnement de journalisation centralisé. Cela simplifie le stockage des messages journaux et leur durée de conservation.

Pour en savoir plus, consultez *Audit Log (Journal d'audit)* dans la base de connaissances AXIS OS.

Version d'AXIS OS	**Chemin de configuration de l'interface Web**
< 7.10	N/A
7.10	N/A
≥ 12.5	Système > Journaux

Stockage local

CSC n°4 : Configuration sécurisée des ressources et logiciels d'entreprise

CSC n° 3 : Protection des pertes de données

À partir de la version 12.0 d'AXIS OS, l'option de montage noexec a été ajoutée en tant qu'option de défaut pour les partages de réseau montés. Ceci désactivera toute exécution directe de fichiers binaires à partir du partage réseau monté. Cette option a déjà été ajoutée aux cartes SD dans les versions antérieures d'AXIS OS.

En outre, les périphériques Axis équipés de la version 10.10 d'AXIS OS et ultérieures prennent en charge l'exportation cryptée des enregistrements en périphérie. Nous vous recommandons d'utiliser cette fonction pour éviter que des personnes non autorisées puissent lire du matériel vidéo exporté.

Version d'AXIS OS	Chemin de configuration de l'interface Web
< 7.10	N/A
7.10	N/A
≥ 10.9	Enregistrements

Sécurité réseau

Protocoles réseau

CSC n°4 : Configuration sécurisée des ressources et logiciels d'entreprise

Seul un nombre minimal de protocoles et services réseau sont activés par défaut dans les dispositifs Axis, comme énuméré ci-dessous.

Protocole	Port	Transport	Remarques
HTTP	80	TCP	Trafic HTTP général tel que l'accès à l'interface Web, l'interface API VAPIX et ONVIF ou la communication bord à bord.*
HTTPS	443	TCP	Trafic HTTPS général tel que l'accès à l'interface Web, l'interface API VAPIX et ONVIF ou la communication bord à bord.*
RTSP	554	TCP	Utilisé par le périphérique Axis pour le flux vidéo/audio.
RTP	Plage de ports éphémère**	UDP	Utilisé par le périphérique Axis pour le flux vidéo/audio.
UPnP	49152	TCP	Utilisé par des applications tierces pour détecter le périphérique Axis via le protocole de détection UPnP. **REMARQUE :** Désactivé par défaut depuis AXIS OS 12.0.
Bonjour	5353	UDP	Utilisé par des applications tierces pour détecter le périphérique Axis via le protocole de détection mDNS (Bonjour).
SSDP	1900	UDP	Utilisé par des applications tierces pour détecter le périphérique Axis via SSDP (UPnP). **REMARQUE :** Désactivé par défaut depuis AXIS OS 12.0.
WS-Discovery***	3702	UDP	Utilisé par des applications tierces pour détecter le périphérique Axis via le protocole WS-Discovery (ONVIF).

* Pour plus d'informations sur la technologie Edge-to-Edge, consultez le livre blanc *Technologie Edge-to-Edge*.

**Attribué automatiquement dans une plage prédéfinie de numéros de port conformément à la norme RFC 6056. Pour plus d'informations, consultez l'article Wikipédia *Port éphémère*.

*** Le protocole WebService Discovery (WS-Discovery) est désactivé par défaut dans AXIS OS 12.1 et les versions ultérieures.

Nous vous recommandons de désactiver les protocoles et services réseau inutilisés partout où c'est possible. Pour obtenir une liste complète des services utilisés par défaut ou qui peuvent être activés en fonction de la configuration, veuillez consulter *Ports réseau couramment utilisés* dans la base de connaissances AXIS OS.

Par exemple, vous devez activer manuellement l'E/S audio et la fonctionnalité de microphone dans les produits de vidéosurveillance Axis tels que les caméras réseau, alors que dans les interphones et les haut-parleurs réseau Axis, l'E/S audio et la fonctionnalité de microphone sont des fonctionnalités essentielles activées par défaut.

HTTPS activé

CSC n° 3 : Protection des pertes de données

À partir de la version 7.20 d'AXIS OS, HTTPS est activé par défaut avec un certificat auto-signé qui permet de définir le mot de passe du périphérique de manière sécurisée. Dans la version 10.10 d'AXIS OS et ultérieures, le certificat auto-signé a été remplacé par le certificat d'ID sécurisé IEEE 802.1AR.

AXIS OS dispose des en-têtes HTTP(S) de sécurité les plus courants, activés par défaut pour améliorer le niveau de base de la cybersécurité dans l'état d'usine par défaut. Dans la version 9.80 d'AXIS OS et ultérieures, vous pouvez utiliser l'API VAPIX d'en tête HTTP personnalisée pour configurer des en-têtes HTTP(S) supplémentaires.

Pour plus d'informations sur l'API VAPIX d'en tête HTTP, consultez la *bibliothèque VAPIX*.

Pour en savoir plus sur les en-têtes HTTP(S) par défaut, consultez *Default HTTP(S) headers (En-têtes HTTP(S) par défaut)* dans la base de connaissances d'AXIS OS.

Version d'AXIS OS	Chemin de configuration de l'interface Web
< 7.10	Configuration > Options système > Sécurité > HTTPS
7.10	Paramètres > Système > Sécurité > HTTP et HTTPS
≥ 10.9	Système > Réseau > HTTP et HTTPS

Contrôle d'accès réseau IEEE 802.1X

CSC n°6 : Gestion du contrôle d'accès
CSC n°13 : Surveillance et défense réseau

Les périphériques Axis prennent en charge le contrôle d'accès réseau basé sur les ports IEEE 802.1X via la méthode EAP-TLS. Pour une protection optimale, nous vous recommandons d'utiliser les certificats client signés par une autorité de certification de confiance (CA) lorsque vous authentifiez votre périphérique Axis.

Version d'AXIS OS	Chemin de configuration de l'interface Web
< 7.10	Configuration > Options système > Sécurité > IEEE 802.1X
7.10	Paramètres > Sécurité > Système > IEEE 802.1X
≥ 10.9	Système > Sécurité > IEEE 802.1X

Dans la version 12.6 d'AXIS OS, nous avons ajouté l'authentification 802.1x aux enregistreurs S3008 et S3008 MK II. Si vous connectez des périphériques avec un identifiant de périphérique Axis, mais sans prise en charge MACsec, allez à **System > Network ports** (Système > Ports réseau), et sous **Security** (Sécurité), pour le(s) port(s), sélectionnez « Authentication required » (Authentification requise). Cela garantit que seuls les périphériques disposant d'un identifiant de périphérique Axis sont autorisés à se connecter.

IEEE 802.1AE MACsec

CSC n° 3 : Protection des pertes de données
CSC n°6 : Gestion du contrôle d'accès

Les périphériques AXIS prennent en charge IEEE 802.1AE MACsec qui est un protocole réseau bien défini qui sécurise cryptographiquement les liaisons Ethernet point à point sur la couche réseau 2. Il garantit la confidentialité et l'intégrité des transmissions de données entre deux hôtes. Comme MACsec agit au niveau de la couche basse 2 de la pile réseau, il ajoute une couche de sécurité supplémentaire aux protocoles réseau qui n'offrent pas les capacités de cryptage natif (ARP, NTP, DHCP, LLDP, CDP...) ainsi qu'à ceux qui en disposent déjà (HTTPS, TLS).

La norme IEEE 802.1AE MACsec décrit deux modes de fonctionnement : une clé pré-partagée (PSK) configurable manuellement / un mode CAK statique et une session maître automatique / un mode CAK dynamique utilisant les sessions IEEE 802.1X EAP-TLS. Le périphérique Axis prend en charge les deux modes.

Dans la version 12.6 d'AXIS OS, nous avons ajouté la prise en charge de 802.1AE MACsec aux enregistreurs S3008 et S3008 MK II. Si vous connectez des périphériques avec un identifiant de périphérique Axis et la prise en charge MACsec, allez à **System > Network ports** (Système > Ports réseau), et sous **Security** (Sécurité), pour le (s) port(s), sélectionnez « MACsec secured required » (Sécurisation MACsec requise). Cela applique à la fois l'authentification 802.1x et le cryptage MACsec.

Pour plus d'informations sur la norme 802.1AE MACsec et la manière de la configurer sur les périphériques AXIS OS, voir *IEEE 802.1AE* dans la base de connaissances d'AXIS OS.

Identité des périphériques sécurisés IEEE 802.1AR

CSC n°1 : Inventaire et contrôle des ressources d'entreprise
CSC n°13 : Surveillance et défense réseau

Les périphériques Axis équipés d'Axis Edge Vault prennent en charge la norme réseau IEEE 802.1AR, ce qui permet d'embarquer automatiquement et en toute sécurité les périphériques Axis dans le réseau grâce à l'identifiant de périphérique Axis, un certificat unique installé dans le périphérique au cours de la production. Pour un exemple d'intégration sécurisée de périphérique, consultez le *guide d'intégration sécurisée des périphériques Axis sur les réseaux Aruba*.

Pour plus d'informations, consultez le livre blanc *Axis Edge Vault*. Pour télécharger la chaîne de certificats de l'identifiant de périphérique Axis, utilisée pour valider l'identité des périphériques Axis, consultez la section concernant le *référentiel d'infrastructure de clé publique* sur axis.com.

Interface UART/de débogage

CSC n°4 : Configuration sécurisée des ressources et logiciels d'entreprise

Chaque périphérique Axis est équipé d'une interface physique UART (Universal Asynchronous Receiver Transmitter), parfois appelée « port de débogage » ou « console série ». L'interface elle-même n'est physiquement accessible qu'après un démontage approfondi du périphérique Axis. L'interface UART/de débogage est utilisée uniquement à des fins de développement et de débogage du produit dans le cadre de projets d'ingénierie de R&D internes au sein d'Axis.

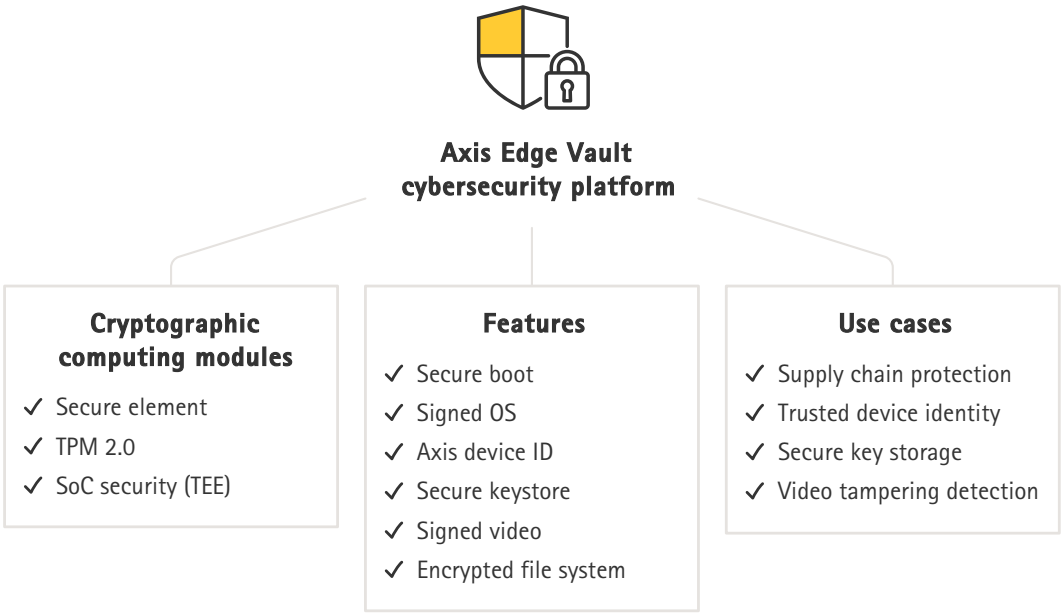
L'interface UART/de débogage est activée par défaut sur les périphériques Axis dotés de la version 10.10 d'AXIS OS et antérieures, mais elle nécessite un accès authentifié et n'expose aucune information sensible tout en étant non authentifiée. À partir de la version 10.11 d'AXIS OS, l'interface UART/de débogage est désactivée par défaut. Le seul moyen d'activer l'interface est de la déverrouiller via un certificat personnalisé unique fourni par Axis.

Axis Edge Vault

Axis Edge Vault offre une plate-forme de cybersécurité matérielle qui protège les périphériques Axis. Elle repose sur des bases solides constituées de modules de calcul cryptographique (élément sécurisé et TPM) et d'une sécurité SoC (TEE et démarrage sécurisé), associés au savoir-faire en matière de sécurité des dispositifs périphériques. Axis Edge Vault repose sur une racine de confiance solide établie par un démarrage sécurisé et un

système d'exploitation signé. Ces fonctionnalités activent une chaîne ininterrompue de logiciels validés cryptographiquement pour la chaîne de confiance dont dépendent toutes les fonctions sécurisées.

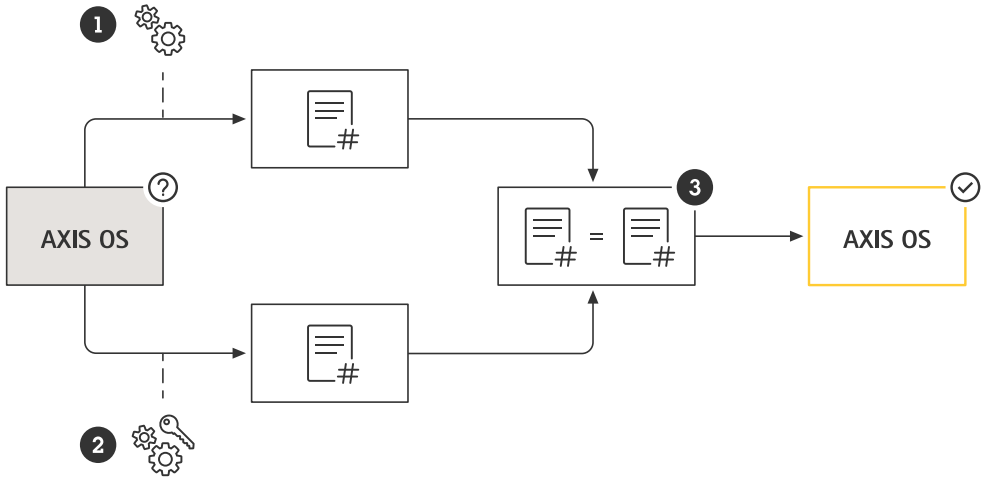
Les périphériques avec Axis Edge Vault minimisent l'exposition aux risques de cybersécurité en empêchant les écoutes électroniques et l'extraction malveillante des informations sensibles. Axis Edge Vault garantit également que le périphérique Axis est une unité fiable et de confiance au sein du réseau.



Système d'exploitation signé

CSC n°2 : Inventaire et contrôle des ressources logicielles

AXIS OS est signé à partir de la version 9.20.1. Lorsque vous effectuez une mise à niveau de la version, le périphérique vérifie l'intégrité des fichiers de mise à jour à l'aide d'une vérification de signature cryptographique et rejette tout fichier ayant été saboté. Cela permet d'éviter que des personnes malveillantes dupent les utilisateurs pour qu'ils installent des fichiers compromis.



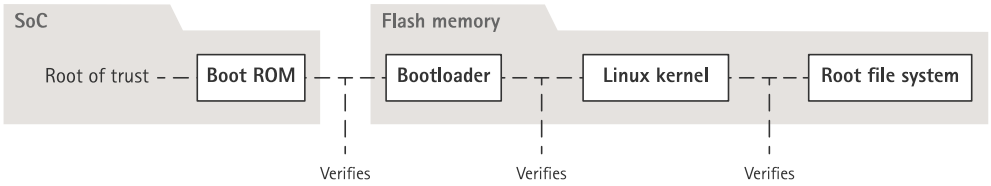
1) Le périphérique calcule la valeur de hachage de l'AXIS OS. 2) Le périphérique utilise la clé publique pour déchiffrer la signature, obtenant ainsi la valeur de hachage. 3) Si les résultats correspondent, la signature de l'OS est vérifiée.

Pour plus d'informations, consultez le livre blanc *Axis Edge Vault*.

Démarrage sécurisé

CSC n°2 : Inventaire et contrôle des ressources logicielles

La plupart des périphériques Axis ont une séquence de démarrage sécurisée pour garantir l'intégrité du périphérique. Le démarrage sécurisé vous permet d'éviter le déploiement de périphériques Axis qui ont été sabotés.

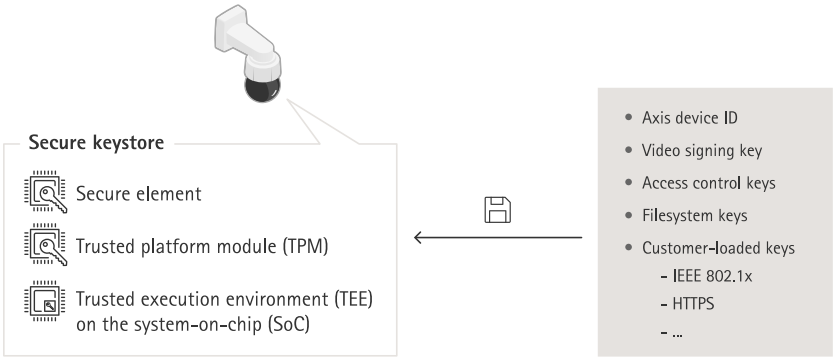


Pour plus d'informations, consultez le livre blanc *Axis Edge Vault*.

Fichier de clés sécurisé

CSC n°6 : Gestion du contrôle d'accès

Le fichier de clés sécurisé fournit un stockage matériel des informations cryptographiques protégé contre le sabotage. Il protège l'identifiant de périphérique Axis ainsi que les informations cryptographiques téléchargées par le client, tout en empêchant tout accès non autorisé et toute extraction malveillante en cas de faille de sécurité. Selon les exigences de sécurité en vigueur, un périphérique Axis peut être doté d'un ou de plusieurs modules de ce type, tels qu'un module Trusted Platform Module (TPM 2.0) ou un élément sécurisé, et/ou un environnement TEE de confiance intégré sur un processeur (SoC).



Pour plus d'informations, consultez le livre blanc *Axis Edge Vault*.

Système de fichiers crypté

CSC n° 3 : Protection des pertes de données

Une personne malveillante pourrait essayer d'extraire des informations du système de fichiers en démontant la mémoire flash et en y accédant via un périphérique de lecteur flash. Cependant, le périphérique Axis peut protéger le système de fichiers contre l'exfiltration de données malveillantes et le sabotage de configuration si quelqu'un accède physiquement à celui-ci ou essaie de le voler. Lorsque le périphérique Axis est mis hors tension, les informations du système de fichiers sont cryptées sur le système de fichiers avec AES-XTS-Plain64 256 bits. Au cours du processus de démarrage sécurisé, le système de fichiers en lecture-écriture est décrypté et peut être monté et utilisé par le périphérique Axis.

Pour plus d'informations, consultez le livre blanc *Axis Edge Vault*.

Facture des matériels du logiciel (SBOM)

CSC n°1 : Inventaire et contrôle des ressources d'entreprise

La facture des matériels du logiciel (SBOM) pour la gestion des vulnérabilités et l'amélioration de la transparence de la chaîne d'approvisionnement est un outil essentiel pour renforcer la confiance dans les produits Axis. La SBOM est fournie avec chaque version du logiciel du dispositif publiée sur axis.com.

Mise hors exploitation

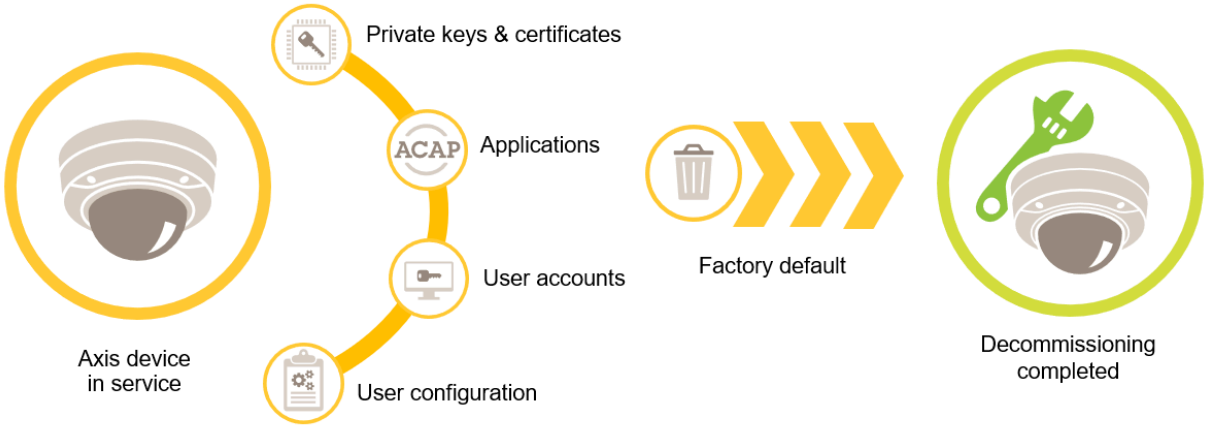
CSC n° 3 : Protection des pertes de données

Les périphériques Axis utilisent à la fois une mémoire volatile et une mémoire non volatile. La mémoire volatile est effacée chaque fois que vous débranchez le périphérique de sa source d'alimentation, tandis que les informations stockées dans la mémoire non volatile sont conservées et disponibles à nouveau au démarrage. Nous évitons la pratique courante de simplement supprimer les pointeurs de données pour rendre les données stockées invisibles au système de fichiers, raison pour laquelle une réinitialisation aux paramètres d'usine est nécessaire. Pour la mémoire flash NAND, la fonction UBI « Supprimer le volume » est utilisée. La fonction équivalente est utilisée pour la mémoire flash eMMC, qui indique que les blocs de stockage ne sont plus utilisés. Le contrôleur de stockage supprime ensuite ces blocs en conséquence.

Lors du démantèlement d'un périphérique Axis, nous vous recommandons de réinitialiser le périphérique aux paramètres d'usine par défaut, ce qui effacera toutes les données stockées dans la mémoire non volatile du périphérique.

Notez que l'émission d'une commande de Remise en paramètres d'usine n'effacera pas immédiatement les données. Le périphérique redémarrera et l'effacement des données se produira pendant le démarrage du système. Il ne suffit donc pas d'émettre la commande « Remise en paramètres d'usine », il faut également laisser le périphérique redémarrer et terminer son amorçage avant de l'éteindre pour garantir que l'effacement des données est terminé.

Cette procédure d'effacement des données clients suit la technique d'assainissement « Clear » décrite dans le document NIST SP-800-88 Révision 1.



Version d'AXIS OS	Chemin de configuration de l'interface Web
< 7.10	Configuration > Options du système > Maintenance > Par défaut.
7.10	Paramètres > Système > Maintenance > Par défaut
≥ 10.9	Maintenance > Par défaut

Ce tableau contient plus d'informations sur les données stockées dans la mémoire non volatile.

Informations et données	Effacées après paramètres d'usine par défaut
Nom d'utilisateur et mot de passe VAPIX et ONVIF	Oui
Certificats et clés privées	Oui
Certificat auto-signé	Oui
Informations stockées TPM et Axis Edge Vault	Oui
Paramètres WLAN et utilisateurs/mots de passe	Oui
Certificats personnalisés*	Non
Clé de cryptage de la carte SD	Oui
Données de carte SD**	Non
Paramètres de partage réseau et utilisateurs/mots de passe	Oui
Données de partage réseau**	Non
Configuration utilisateur***	Oui
Applications téléchargées (ACAP)****	Oui
Données de production et statistiques de durée de vie*****	Non
Images et incrustations chargées	Oui
Données d'horloge RTC	Oui

* Le processus d'OS signé utilise des certificats personnalisés qui permettent aux utilisateurs de télécharger (entre autres) AXIS OS.
** Les enregistrements et les images stockés sur un stockage edge (carte SD, partage de réseau) doivent être supprimés séparément par l'utilisateur. L'effacement des données client sur la SD carte SD est effectué conformément à la norme NIST SP-800-88 Revision 1 Cryptographic Erase (CE) et pour les données sur les disques durs (série S30-Recorder), il s'agit de la norme NIST SP-800-88 Revision 1 Clear. Pour plus d'informations, consultez dans la base de connaissances d'AXIS OS.
*** Toutes les configurations faites par l'utilisateur, de la création de comptes aux configurations du réseau, d'O3C, d'événements, d'images, de PTZ et du système.
**** Le périphérique conserve toutes les applications préinstallées mais supprime toutes les configurations faites par l'utilisateur.
***** Les données de production (étalonnage, certificats de production 802.1AR) et les statistiques de durée de vie comprennent des informations non sensibles et non liées à l'utilisateur.

Renforcement de base

Le renforcement de base est le niveau de protection minimal recommandé pour les périphériques Axis. Les rubriques de renforcement de base sont « configurables en périphérie ». Cela signifie qu'elles peuvent être directement configurées sur le périphérique Axis sans dépendances supplémentaires des infrastructures réseau, de la vidéo ou de systèmes de gestion des preuves (VMS, EMS), d'équipements ou d'applications.

Paramètres d'usine

CSC n°4 : Configuration sécurisée des ressources et logiciels d'entreprise

Avant de configurer votre périphérique, assurez-vous qu'il est dans l'état d'usine par défaut. Il est également important de réinitialiser le périphérique aux paramètres d'usine par défaut lorsque vous devez l'effacer de données utilisateur ou le démanteler. Pour en savoir plus, consultez *Mise hors exploitation, on page 12*.

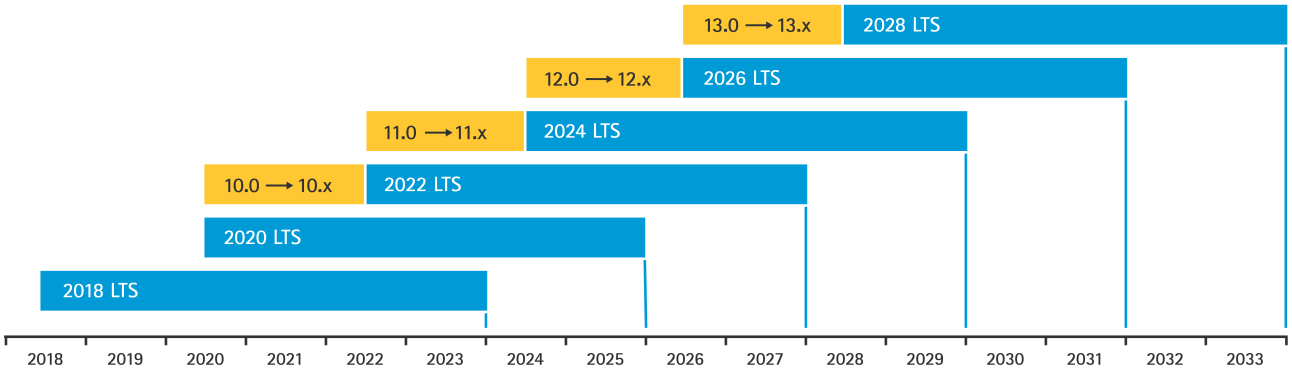
Version d'AXIS OS	Chemin de configuration de l'interface Web
< 7.10	Configuration > Options du système > Maintenance > Par défaut.
7.10	Paramètres > Système > Maintenance > Par défaut
≥ 10.9	Entretien > Remise en paramètres d'usine

Mise à niveau vers la dernière version d'AXIS OS

CSC n°2 : Inventaire et contrôle des ressources logicielles

Les correctifs de logiciels sont un élément essentiel de la cybersécurité. Les pirates essaient souvent d'exploiter les vulnérabilités communément connues et peuvent réussir si ils accèdent au réseau à un service non corrigé. Assurez-vous d'utiliser toujours la version d'AXIS OS la plus récente, car elle peut inclure des correctifs de sécurité pour les vulnérabilités connues. Les notes de version d'une version spécifique peuvent mentionner de façon explicite un correctif de sécurité critique, mais pas tous les correctifs généraux.

Axis gère deux types de pistes AXIS OS : les pistes actives et la piste de support à long terme (LTS). Bien que les deux incluent les derniers correctifs de vulnérabilité critiques, les cycles LTS n'incluent pas de nouvelles fonctionnalités, car l'objectif est de minimiser le risque de problèmes de compatibilité. Pour plus d'informations, consultez la section concernant le *cycle de vie d'AXIS OS* dans AXIS OS Information.



Axis fournit des prévisions sur les versions à venir avec notamment des informations sur les nouvelles fonctionnalités importantes, les résolutions de bogues et les correctifs de sécurité. Pour en savoir plus, consultez la section sur les *versions à venir* dans AXIS OS Information. Consultez la section relative au *logiciel du périphérique* sur axis.com afin de télécharger AXIS OS pour votre périphérique.

Version d'AXIS OS	Chemin de configuration de l'interface Web
< 7.10	Configuration > Options système > Maintenance > Mettre le serveur à niveau
7.10	Paramètres > Système > Maintenance > Mise à niveau du firmware
≥ 10.9	Entretien > Mise à niveau d'AXIS OS

Créer des comptes dédiés

CSC n°4 : Configuration sécurisée des ressources et logiciels d'entreprise
CSC n° 5 : Gestion des comptes

Les périphériques Axis peuvent avoir deux types de comptes : un compte administrateur et un compte utilisateur client. Le compte administrateur est le compte principal pour la gestion de votre périphérique, et il est essentiel de le réserver aux seules tâches administratives. Lors de la configuration de votre périphérique, vous devrez créer un nom d'utilisateur et un mot de passe pour le compte administrateur.

En plus du compte de l'administrateur, créez un compte utilisateur client avec des privilèges limités pour le fonctionnement quotidien. Vous pouvez ainsi gérer votre périphérique en toute sécurité, en réduisant le risque de compromettre le mot de passe de l'administrateur du périphérique. Vous devez utiliser le compte utilisateur client pour les tâches qui ne requièrent pas de privilèges d'administration complets.

Lorsque vous créez des mots de passe pour l'un ou l'autre compte, nous vous recommandons d'appliquer des directives telles que les recommandations du NIST ou du BSI en matière de mots de passe, qui exigent que les nouveaux mots de passe soient suffisamment longs et complexes. Les périphériques Axis peuvent prendre en charge des mots de passe jusqu'à 64 caractères. Les mots de passe d'une longueur inférieure à 8 caractères sont considérés comme faibles. Pour plus d'informations, consultez *Identity and access management (Gestion des identités et des accès)* dans la base de connaissances d'AXIS OS.

Les périphériques Axis fonctionnant sous AXIS OS 11.6 ou supérieur prennent en charge OAuth 2.0, qui permet une gestion centralisée des identités et des accès (IAM) et des identités fédérées pour s'authentifier sur le périphérique. Il n'est donc plus nécessaire de procéder à une gestion locale des utilisateurs des périphériques. Pour en savoir plus, consultez *OAuth 2.0, on page 27*.

Version d'AXIS OS	Chemin de configuration de l'interface Web
< 7.10	Configuration > Configuration de base > Utilisateurs
7.10	Paramètres > Système > Utilisateurs
≥ 10.9	Système > Utilisateurs
≥ 11.6	Système > Comptes

Configurer les paramètres de réseau, de date et d'heure

CSC n°4 : CSC n°8 : Gestion des journaux d'audit
CSC n°12 : Gestion de l'infrastructure réseau

Il est important de configurer correctement les paramètres du réseau, de la date et de l'heure du périphérique afin de garantir le bon fonctionnement et la sécurité de votre périphérique Axis. Ces paramètres affectent divers aspects du comportement du périphérique, notamment la communication réseau, la connexion et la validation des certificats.

La configuration IP du périphérique dépend de la configuration du réseau, telle que IPv4/IPv6, l'adresse réseau statique ou dynamique (DHCP), le masque de sous-réseau et le routeur par défaut. Révisez la topologie de votre réseau chaque fois que vous ajoutez de nouveaux composants. Nous vous recommandons d'utiliser une

configuration d'adresse IP statique afin de garantir l'accessibilité du réseau et de minimiser les dépendances vis-à-vis des serveurs réseau susceptibles d'être vulnérables aux attaques, tels que les serveurs DHCP.

Version d'AXIS OS	Chemin de configuration de l'interface Web
< 7.10	Configuration > Configuration de base > TCP/IP
7.10	Paramètres > Système > TCP/IP
≥ 10.9	Système > Réseau

La précision de l'horloge est essentielle pour maintenir les journaux du système, valider les certificats numériques et activer des services tels que HTTPS, IEEE et 802.1x. Nous vous recommandons de synchroniser l'horloge de votre périphérique avec des serveurs NTP (Network Time Protocol) ou NTS (Network Time Security). Network Time Security (NTS), une variante cryptée et sécurisée de Network Time Protocol (NTP), a été ajoutée à AXIS OS 11.1. Nous vous recommandons de configurer plusieurs serveurs NTP pour une plus grande précision et pour tenir compte des défaillances potentielles. Si vous ne pouvez pas héberger de serveurs de synchronisation locale, envisagez d'utiliser des serveurs NTP ou NTP publics. Pour plus d'informations sur les NTP/NTS sur les périphériques Axis, voir la section concernant *NTP et NTS* dans AXIS OS Knowledge base.

Version d'AXIS OS	Chemin de configuration de l'interface Web
< 7.10	Configuration > Configuration de base > Date et heure
7.10	Paramètres > Système > Date et heure
≥ 10.9	Système > Date et heure
≥ 11.6	Système > Heure et emplacement

Cryptage du stockage périphérique

CSC n° 3 : Protection des pertes de données

Carte SD
Si le périphérique Axis prend en charge et utilise des cartes SD (Secure Digital) pour stocker des enregistrements vidéo, nous vous recommandons d'appliquer un cryptage. Cela permettra d'éviter que des personnes non autorisées puissent lire la vidéo stockée à partir d'une carte SD retirée.

Pour en savoir plus sur le cryptage d'une carte SD sur les périphériques Axis, voir la section concernant la *prise en charge d'une carte SD* sur AXIS OS Knowledge base.

Version d'AXIS OS	Chemin de configuration de l'interface Web
< 7.10	Configuration > Options système > Stockage
7.10	Paramètres > Système > Stockage
≥ 10.9	Système > Stockage

Partage de réseau (NAS)
Si vous utilisez un espace de stockage réseau (NAS) comme dispositif d'enregistrement, nous vous recommandons de le conserver dans une zone verrouillée avec accès limité et d'activer le cryptage sur disque dur. Les périphériques Axis utilisent le protocole SMB comme protocole réseau pour la connexion à un espace de stockage réseau NAS pour stocker les enregistrements vidéo. Bien que les versions antérieures de SMB (1.0 et 2.0) ne fournissent aucune sécurité ou cryptage, les versions suivantes (2.1 et ultérieures) le font, raison pour laquelle nous vous recommandons d'utiliser des versions ultérieures pendant la production.

Pour en savoir plus sur la configuration SMB appropriée lorsque vous connectez un périphérique Axis à un partage réseau, voir la section relative au *partage réseau* dans AXIS OS Knowledge base.

Version d'AXIS OS	Chemin de configuration de l'interface Web
< 7.10	Configuration > Options système > Stockage
7.10	Paramètres > Système > Stockage
≥ 10.9	Système > Stockage

Applications (ACAP)

CSC n°4 : Configuration sécurisée des ressources et logiciels d'entreprise

Vous pouvez charger des applications sur le périphérique Axis pour étendre sa fonctionnalité. Nombre d'entre elles sont dotées de leur propre interface utilisateur pour interagir avec une fonction. Les applications peuvent utiliser les fonctionnalités de sécurité fournies par AXIS OS.

Les périphériques Axis sont préchargés avec plusieurs applications développées par Axis conformément au *modèle ASDM (Security Development Model) d'Axis*. Pour plus d'informations sur les applications Axis, consultez la section concernant les *analyses* sur axis.com.

Pour les applications tierces, nous vous recommandons de contacter le fournisseur pour obtenir éléments probants concernant la sécurité de l'application en termes de fonctionnement et de tests et si elle a été développée selon les modèles de développement de sécurité les plus courants. Les vulnérabilités trouvées dans les applications tierces doivent être directement signalées au fournisseur tiers.

Nous vous recommandons de n'utiliser que les applications de confiance et de supprimer les applications inutilisées des périphériques Axis.

Version d'AXIS OS	Chemin de configuration de l'interface Web
< 7.10	Configuration > Applications
7.10	Paramètres > Applications
≥ 10.9	Applications

À partir de la version 12.0 d'AXIS OS (septembre 2024), la signature ACAP est requise et activée par défaut, avec la possibilité de la désactiver. À partir de la version 13.0 d'AXIS OS (septembre 2026), la signature ACAP sera obligatoire et ne pourra pas être désactivée. Les ACAP sont signés dans le portail ACAP à l'aide de SHA-512 et d'une clé privée RSA 4096 bits stockée de manière sécurisée dans un HSM Thales Luna Network 7 dans le centre de données Axis à Lund, en Suède. Les périphériques réseaux Axis sont préchargés avec la clé publique RSA 4096 bit afin de valider la signature ACAP avant l'installation d'ACAP. La clé publique est stockée sur le périphérique réseau Axis dans le système de fichiers Linux.

Désactiver les services/fonctions inutilisés

CSC n°4 : Configuration sécurisée des ressources et logiciels d'entreprise

Même si les services et fonctions inutilisés ne sont pas une menace immédiate pour la sécurité, il est pratique de les désactiver afin de minimiser les risques inutiles. Poursuivez la lecture afin d'en apprendre davantage sur les services et les fonctions que vous pouvez désactiver lorsqu'ils ne sont pas utilisés.

Accès à l'interface web

CSC n°4 : Configuration sécurisée des ressources et logiciels d'entreprise

CSC n° 5 : Gestion des comptes

Les dispositifs Axis disposent d'un serveur web qui permet aux utilisateurs d'accéder au dispositif via un navigateur standard. L'interface web est conçue pour la configuration, la maintenance et le dépannage, et non pour le fonctionnement quotidien, par exemple comme client pour visionner des vidéos.

Les seuls clients qui doivent être autorisés à interagir avec les périphériques Axis au cours des opérations quotidiennes sont les systèmes de gestion vidéo (VMS) ou les outils d'administration et de gestion des périphériques tels que AXIS Device Manager. Les utilisateurs du système ne doivent jamais être autorisés à accéder directement aux périphériques Axis.

Depuis la version 9.50 d'AXIS OS, il est possible de désactiver l'interface web d'un dispositif Axis. Dès qu'un périphérique Axis est déployé sur un système (ou que vous l'ajoutez à AXIS Device Manager), nous vous recommandons de supprimer l'option pour que le personnel de l'organisation accède au périphérique via un navigateur Web. Cela crée en effet un niveau de sécurité supplémentaire si le mot de passe du compte périphérique est partagé au sein de l'organisation. L'option la plus sûre consiste à configurer exclusivement l'accès aux périphériques Axis à l'aide d'applications dédiées qui offrent une architecture de gestion des accès aux identités (IAM) avancée, un meilleur suivi et des protections pour éviter les fuites de compte.

Version d'AXIS OS	Chemin de configuration de l'interface Web
< 7.10	N/A
7.10	Paramètres > Système > Configuration ordinaire > Système > Interface Web désactivée
≥ 10.9	Système > Configuration ordinaire > Système > Interface Web désactivée

Ports réseau physiques non inutilisés

À partir de la version 11.2 d'AXIS OS, les périphériques avec plusieurs ports réseau, tels qu'AXIS S3008, sont dotés d'une fonction de désactivation de PoE et du trafic réseau sur leur ports réseau. Si les ports réseau non inutilisés sont laissés sans surveillance et qu'ils sont actifs, cela représente un risque sérieux pour la sécurité.

Version d'AXIS OS	Chemin de configuration de l'interface Web
< 7.10	N/A
7.10	N/A
≥ 11.2	Système > Power over Ethernet

Protocoles de découverte de réseau

Les protocoles de détection, tels que Bonjour, UPnP, ZeroConf, WS-Discovery et LLDP/CDP, sont des services d'assistance qui facilitent la recherche du périphérique Axis et de ses services sur le réseau. Une fois le périphérique déployé et ajouté à VMS, nous vous recommandons de désactiver le protocole de détection pour empêcher le périphérique Axis d'annoncer sa présence sur le réseau.

Version d'AXIS OS	Chemin de configuration de l'interface Web
< 7.10	Configuration > Options système > Avancé > Configuration ordinaire > Réseau > Réseau Bonjour activé, réseau UPnP activé, réseau ZeroConf activé, réseau UPnP NATTraversal activé*
	N/A
7.10	Paramètres > Système > Configuration ordinaire > Réseau > Réseau Bonjour activé, réseau UPnP activé, réseau ZeroConf activé, réseau UPnP NATTraversal activé*

Version d'AXIS OS	Chemin de configuration de l'interface Web
	Paramètres > Système > Configuration ordinaire > Service Web > Mode de détection
≥ 10.9	Paramètres > Configuration ordinaire > Réseau > Réseau Bonjour activé, réseau UPnP activé, réseau ZeroConf activé
	Système > Configuration ordinaire > Service Web > Mode de détection > Activer le mode détectable WS-Discovery
≥ 11.11	Système > Réseau > Protocoles de détection réseau > LLDP et CDP**

*La fonctionnalité a été supprimée d'Axis OS 10.12 et n'est pas disponible dans les versions ultérieures.

**La désactivation de LLDP et CDP a pu avoir une incidence sur la négociation de puissance PoE.

Divulgation d'informations

Par défaut, les dispositifs Axis annoncent les versions de base de leurs logiciels Apache, OpenSSL et AXIS OS actuels, soit lors des connexions HTTP(S) avec des clients sur le réseau, soit via l'API Basic Device Info VAPIX (*https://developer.axis.com/vapix/network-video/basic-device-information/*).

Ces informations sont indispensables aux scanners de sécurité réseau ou aux systèmes de surveillance réseau tels que Rapid7, Tenable Nessus et autres, pour scanner des dispositifs Axis à la recherche de vulnérabilités non corrigées. Sans ces informations, ces applications pourraient ne pas fonctionner correctement sur les dispositifs Axis. En règle générale, Axis recommande d'activer et de maintenir la fonctionnalité de divulgation des informations, car elle contribue à la mise à jour des logiciels, à la connaissance de la situation, à la surveillance et au fonctionnement sécurisé des dispositifs Axis.

Cependant, certaines approches de cybersécurité exigent que la divulgation d'informations soit réduite au minimum ou complètement désactivée. Afin de respecter cette exigence, des paramètres de configuration ont été mis en place pour désactiver la divulgation d'informations. Cependant, nous vous recommandons simplement de désactiver cette fonctionnalité si vous utilisez votre dispositif conformément à nos recommandations et que vous le tenez à jour à tout moment.

Versions d'Apache/OpenSSL

La possibilité de désactiver les en-têtes du serveur HTTP(S) pour réduire l'exposition des informations lors des connexions HTTP(S) est disponible à partir de la version 10.6 d'AXIS OS.

Version d'AXIS OS	Chemin de configuration de l'interface Web
< 7.10	N/A
7.10	Paramètres > Système > Configuration ordinaire > Système > Commentaires d'en-tête de serveur HTTP

Version d'AXIS OS	Chemin de configuration de l'interface Web

≥ 11.11	*https://IP_OR_HOSTNAME/config/web-ui/swagger-ui/?url=/config/discover/apis/basic-device-info/v2/openapi.json#/basic-device-info.v2beta/patch_basic_device_info_v2beta_allowAnonymous*
	
	{
	« données » : faux
	}

Audio

Dans les produits de vidéosurveillance Axis, tels que les caméras réseau, l'E/S audio et la fonctionnalité de microphone sont désactivés par défaut. Si vous avez besoin de fonctionnalités audio, vous devez les activer avant de les utiliser. Dans les produits Axis où l'E/S audio et la fonctionnalité de microphone sont des fonctions essentielles, comme dans les interphones et les haut-parleurs réseau Axis, les fonctionnalités audio sont activées par défaut.

Nous vous recommandons de désactiver les fonctionnalités audio si vous ne les utilisez pas.

Version d'AXIS OS	Chemin de configuration de l'interface Web
< 7.10	Configuration > Options système > Avance > Configuration ordinaire > Audio > Audio A* > Activé
7.10	Paramètres > Audio > Autoriser l'audio
≥ 10.9	Audio > Paramètres du périphérique

Emplacement(s) pour carte SD

Les périphériques Axis prennent généralement en charge au moins une carte SD pour le stockage edge des enregistrements vidéo. Nous vous recommandons de désactiver complètement l'emplacement pour carte SD si vous n'utilisez pas de cartes SD. L'option de désactivation de l'emplacement pour carte SD est disponible à compter de la version 9.80 d'AXIS OS.

Pour plus d'informations, consultez la section concernant *la désactivation de la carte SD* dans AXIS OS Knowledge base.

Version d'AXIS OS	Chemin de configuration de l'interface Web
< 7.10	N/A
7.10	Paramètres > Système > Configuration ordinaire > Stockage > Disque SD activé
≥ 10.9	Système > Configuration ordinaire > Stockage > Disque SD activé

Accès SSH

Le protocole SSH est un protocole de communication sécurisé utilisé à des fins de dépannage et de débogage uniquement. Il est pris en charge par les périphériques Axis à partir de la version 5.50 d'AXIS OS. Nous vous recommandons de désactiver l'accès SSH.

Pour plus d'informations sur les options de débogage à l'aide de SSH, consultez la section concernant *l'accès SSH* dans AXIS OS Knowledge base.

Version d'AXIS OS	Chemin de configuration de l'interface Web
< 7.10	Configuration > Options système > Configuration ordinaire > Réseau > SSH activé
7.10	Paramètres > Système > Configuration ordinaire > Réseau > SSH activé
≥ 10.9	Système > Configuration ordinaire > Réseau > SSH activé

USB

À partir du système d'exploitation AXIS OS 12.1, l'AXIS D1110 offre la possibilité de désactiver le port USB. Si les ports USB non inutilisés sont laissés sans surveillance et qu'ils sont actifs, cela représente un risque sérieux pour la sécurité.

Version d'AXIS OS	Chemin de configuration de l'interface Web
< 7.10	N/A
7.10	N/A
≥ 12.1	Système > > Accessories > Configuration USB

Capacités Wi-Fi

Certains périphériques Axis offrent des fonctionnalités Wi-Fi grâce à un point d'accès intégré via une clé Wi-Fi USB. Le Wi-Fi n'est activé qu'en appuyant sur le bouton physique de configuration WLAN lorsqu'aucune connexion réseau RJ45 physique n'est présente. Ceci est vrai que le périphérique soit dans ses valeurs par défaut ou qu'il soit en fonctionnement. Avec l'AXIS M1075, l'utilisateur peut se connecter au point d'accès à l'aide du SSID et du mot de passe SSID unique au périphérique, indiqués sur l'étiquette du produit. Dans certains nouveaux produits Axis, seul le SSID est requis (aucun mot de passe), ce qui améliore l'expérience d'installation sans compromettre la cybersécurité.

Veuillez consulter le manuel d'utilisation pour la configuration de votre périphérique Axis et ses capacités Wi-Fi. Ce qui suit explique le fonctionnement des capacités intégrées du point d'accès dans certains produits Axis prenant en charge le Wi-Fi :

- Le point d'accès intégré ne peut être activé qu'en appuyant sur le bouton physique de configuration WLAN, à condition qu'aucun SSID/mot de passe Wi-Fi ne soit configuré et qu'aucune connexion réseau RJ45 physique ne soit présente. Ceci est vrai que le périphérique soit dans ses valeurs par défaut ou qu'il soit en fonctionnement.
- Le point d'accès intégré est désactivé dès que la caméra se connecte à un point d'accès configuré par l'utilisateur. Sinon, elle est automatiquement désactivée 15 minutes après que l'utilisateur a appuyé sur le bouton physique de configuration WLAN pendant l'installation.

Si le périphérique utilise une clé Wi-Fi connectée, il est recommandé de configurer correctement les fonctionnalités Wi-Fi, en utilisant un SSID + mot de passe lors de la configuration initiale du périphérique, afin d'assurer une sécurité optimale.

Bluetooth

Certains dispositifs Axis sont équipés d'une fonctionnalité Bluetooth intégrée, que vous pouvez utiliser pour une expérience utilisateur fluide lors de la configuration initiale du dispositif après la remise en paramètres d'usine, par exemple pour régler l'image et les objectifs.

Veuillez consulter le manuel d'utilisation de votre dispositif pour connaître ses paramètres de configuration et ses capacités Bluetooth. Les descriptions ci-dessous expliquent les fonctionnalités Bluetooth générales des produits Axis :

- Le Bluetooth est automatiquement activé selon les valeurs par défaut, à condition qu'aucun utilisateur n'ait été configuré, et ce pendant une durée maximale de 2 heures après le démarrage initial. Le Bluetooth est automatiquement désactivé lorsqu'un utilisateur est configuré ou deux heures après le démarrage initial, qu'une connexion réseau RJ45 physique soit présente ou non.
- Une fois que le Bluetooth a été désactivé, l'utilisateur ne peut pas l'activer manuellement. La fonctionnalité Bluetooth ne peut être rétablie qu'en réinitialisant le dispositif à ses valeurs par défaut.
- La connexion Bluetooth entre votre dispositif et la caméra Axis utilise un tunnel HTTPS qui emploie le dernier cryptage TLS 1.2/1.3. Aucune autre fonctionnalité de sécurité Bluetooth intégrée n'est requise ou utilisée.

Limiter l'accès au réseau

CSC n°1 : Inventaire et contrôle des ressources d'entreprise
CSC n°4 : Configuration sécurisée des ressources et logiciels d'entreprise
CSC n°13 : Surveillance et défense réseau

AXIS OS 11.9 a vu le lancement d'un pare-feu basé sur l'hôte, une fonctionnalité de sécurité qui vous permet de créer des règles réglementant le trafic entrant par adresse IP et/ou numéros de port TCP/UDP. Cela permet d'éviter tout accès non autorisé au périphérique ou à ses services.

Si vous définissez la politique par défaut sur « Drop » (Rejeter), veillez à ajouter tous les clients autorisés (clients VMS et administratifs) et/ou les ports à votre liste.

Version d'AXIS OS	**Chemin de configuration de l'interface Web**
≥ 11.9	System (Système) > Security (Sécurité) > Firewall (Pare-feu)

Filtrage d'adresses IP

Les périphériques équipés de la version 11.8 d'AXIS OS et antérieures utilisent le filtrage des adresses IP pour empêcher l'accès des clients non autorisés. Nous vous recommandons soit de configurer votre dispositif pour autoriser les adresses IP des hôtes réseau autorisés, soit de refuser celles des hôtes non autorisés.

Si vous choisissez d'autoriser les adresses IP, assurez-vous d'ajouter tous les clients autorisés, y compris les serveurs VMS et les clients d'administration à votre liste.

Version d'AXIS OS	Chemin de configuration de l'interface Web
< 7.10	Configuration > Options système > Sécurité > Filtrage d'adresses IP
7.10	Configuration > Système > TCP/IP >Filtrage d'adresses IP
10.9 — 11.8	Configuration > Sécurité > Filtrage d'adresses IP

Remarque

Vous pouvez activer des journaux plus détaillés des tentatives d'accès au réseau pour vous aider à identifier les tentatives d'accès indésirables provenant d'autres hôtes du réseau. Pour ce faire, veuillez aller à **System (Système)** > **Plain config (Configuration ordinaire)** > **Network (Réseau)** et au journal de filtrage du réseau.

HTTPS

CSC n° 3 : Protection des pertes de données

HTTP et HTTPS sont activés par défaut dans les périphériques Axis à partir de la version 7.20 d'AXIS OS. Alors que l'accès HTTP n'est pas sécurisé en l'absence de tout cryptage, HTTPS crypte le trafic entre le client et le périphérique Axis. Nous vous recommandons d'utiliser HTTPS pour toutes les tâches d'administration sur le périphérique Axis.

Pour les instructions de configuration, consultez les sections *HTTPS uniquement, on page 23* et *Cryptogrammes HTTPS, on page 23*.

HTTPS uniquement

Nous vous recommandons de configurer votre périphérique Axis pour la seule utilisation du protocole HTTPS (sans accès HTTP possible). Cela activera automatiquement le protocole HSTS (HTTP Strict Transport Security) et améliorera encore davantage la sécurité du périphérique.

À partir de la version 7.20 d'AXIS OS, les périphériques Axis sont fournis avec un certificat auto-signé, valable jusqu'au 19 janvier 2038. Bien qu'un certificat auto-signé ne soit pas considéré comme fiable par défaut, il est suffisant pour garantir un accès sécurisé au périphérique Axis lors de la configuration initiale et lorsqu'aucune infrastructure à clé publique (PKI) n'est disponible. Si disponible, le certificat auto-signé doit être supprimé et remplacé par des certificats client signés correctement et émis par une autorité KPI. À partir de la version 10.10 d'AXIS OS, le certificat auto-signé a été remplacé par le certificat d'ID sécurisé IEEE 802.1AR.

Version d'AXIS OS	Chemin de configuration de l'interface Web
< 7.10	Configuration > Options système > Sécurité > HTTPS
7.10	Paramètres > Système > Sécurité > HTTP et HTTPS
≥ 10.9	Système > Réseau > HTTP et HTTPS

Cryptogrammes HTTPS

Les périphériques Axis prennent en charge et utilisent les suites cryptographiques TLS 1.2 et TLS 1.3 pour crypter en toute sécurité les connexions HTTPS. La version TLS et la suite de cryptogramme spécifiques utilisées dépendent du client qui se connecte au périphérique Axis et elle est négociée en conséquence. Au cours des mises à jour régulières d'AXIS OS, la liste des cryptogrammes disponibles du périphérique Axis peut être mise à jour sans que la configuration réelle du cryptogramme ne soit modifiée. Une modification des configurations de cryptogramme doit être initiée par l'utilisateur, soit en réinitialisant les valeurs par défaut des périphériques Axis, soit en procédant à une configuration manuelle. À partir de la version 10.8 d'AXIS OS et ultérieures, la liste des cryptogrammes est automatiquement mise à jour lorsque l'utilisateur exécute une mise à jour d'AXIS OS.

TLS 1.2 et antérieur

Avec TLS 1.2 ou une version antérieure, vous pouvez spécifier les cryptogrammes HTTPS à utiliser par le périphérique Axis lors de son redémarrage. Il n'y a pas de restriction concernant les cryptogrammes que vous pouvez choisir, mais il est recommandé de sélectionner l'un ou l'ensemble des cryptogrammes forts suivants :

```
ECDHE-ECDSA-AES128-GCM-SHA256:ECDHE-RSA-AES128-GCM-SHA256:ECDHE-ECDSA-
AES256-GCM-SHA384:ECDHE-RSA-AES256-GCM-SHA384:ECDHE-ECDSA-CHACHA20-
POLY1305:ECDHE-RSA-CHACHA20-POLY1305
```

Version d'AXIS OS	Chemin de configuration de l'interface Web
< 7.10	Configuration > Options système > Avancé > Configuration ordinaire > HTTPS > Cryptogrammes
7.10	Paramètres > Système > Configuration ordinaire > HTTPS > Cryptogrammes
≥ 10.9	Système > Configuration ordinaire > HTTPS > Cryptogrammes

TLS 1.3

Par défaut, seules les suites cryptographiques puissantes répondant aux spécifications TLS 1.3 sont disponibles :

```
TLS_AES_128_GCM_SHA256:TLS_CHACHA20_POLY1305_SHA256:TLS_AES_256_GCM_
SHA384
```

Ces suites ne peuvent pas être configurées par l'utilisateur.

Renforcement étendu

Les instructions relatives à un renforcement étendu s'appuient sur les rubriques de renforcement décrites dans *Protection par défaut, on page 4* et dans *Renforcement de base, on page 14*. Mais même si vous pouvez appliquer les instructions de renforcement par défaut et de base directement sur votre périphérique Axis, ce renforcement étendu nécessite une participation active de l'ensemble de la chaîne logistique des fournisseurs, de l'organisation de l'utilisateur final et de l'infrastructure IT sous-jacente et /ou réseau.

Limiter l'exposition à internet et aux réseaux

CSC n°12 : Gestion de l'infrastructure réseau

Nous vous recommandons d'éviter d'exposer un périphérique Axis en tant que serveur web public ou d'autoriser de quelque manière que ce soit des clients inconnus à accéder au périphérique en réseau. Pour les petites sociétés et les particuliers qui n'utilisent pas de logiciel de gestion vidéo (VMS) ou qui ont besoin d'accéder à la vidéo à partir de lieux distants, AXIS Camera Station Edge est une bonne option.

Disponible gratuitement sur Windows, iOS et Android, AXIS Camera Station Edge offre un moyen simple d'accéder à la vidéo en toute sécurité sans exposer son périphérique à internet. Pour en savoir plus, consultez *axis.com/products/axis-camera-station-edge*.

Remarque

Si votre société utilise un VMS, consultez votre fournisseur de VMS pour connaître les meilleures pratiques en matière d'accès vidéo distant.

L'isolation des périphériques réseau ainsi que de l'infrastructure et des applications connexes réduit le risque d'exposition du réseau.

Nous vous recommandons d'isoler les périphériques Axis, les infrastructures et les applications connexes sur un réseau local séparé de votre réseau de production et d'entreprise.

Pour appliquer un renforcement de base, protégez le réseau local et son infrastructure (routeur, commutateurs) contre tout accès non autorisé en utilisant plusieurs mécanismes de sécurité réseau. Il peut s'agir d'une segmentation VLAN, de capacités de routage limitées, d'un VPN pour l'accès site à site ou WAN, d'un pare-feu de couche réseau 2/3 et de listes de contrôle d'accès (ACL).

Pour étendre le renforcement de base, appliquez des techniques avancées d'inspection des réseaux, telles que l'inspection approfondie des paquets et la détection des intrusions. La protection contre les menaces au sein du réseau s'en trouve renforcée. Notez qu'un renforcement étendu du réseau nécessite généralement des logiciels et/ou du matériel spécialisés.

Analyse de détection des vulnérabilités

CSC n°1 : Inventaire et contrôle des ressources d'entreprise
CSC n°12 : Gestion de l'infrastructure réseau

Vous pouvez utiliser des scanners de sécurité réseau pour exécuter des évaluations de vulnérabilité de vos périphériques réseau. L'objectif d'une évaluation des vulnérabilité est de permettre un examen systématique des vulnérabilités de sécurité et des erreurs de sécurité potentielles.

Nous vous recommandons d'exécuter des analyses régulières des vulnérabilités de vos périphériques Axis et de leur infrastructure associée. Avant de commencer le scan, assurez-vous que vos dispositifs Axis ont été mis à jour vers la dernière version d'AXIS OS disponible, sur le cycle LTS ou le cycle actif.

Nous vous recommandons également de passer en revue le rapport d'analyse et de filtrer les faux positifs connus pour les périphériques Axis, que vous pouvez trouver dans le manuel *AXIS OS Vulnerability Scanner Guide*. Soumettez le rapport ainsi que toute autre remarque supplémentaire sous la forme d'un ticket à l'*assistance Axis* sur axis.com.

Infrastructure de clé publique (PKI) fiable

CSC n° 3 : Protection des pertes de données

CSC n°12 : Gestion de l'infrastructure réseau

Nous vous recommandons de déployer des certificats serveur et client Web sur vos périphériques Axis, fiables et signés par une autorité de certification publique ou privée (CA). Un certificat signé par une autorité de certification avec une chaîne de confiance validée permet de supprimer les avertissements de certificat du navigateur lorsque vous vous connectez via HTTPS. Un certificat signé par une autorité de certification garantit également l'authentification du périphérique Axis lors du déploiement d'une solution de contrôle d'accès réseau (NAC). Cela atténue le risque d'attaque d'un ordinateur se faisant passer pour un périphérique Axis.

Vous pouvez utiliser AXIS Device Manager, qui est fourni avec un service CA intégré, pour émettre des certificats signés sur les périphériques Axis.

Journal système distant

CSC n°8 : Gestion des journaux d'audit

Vous pouvez configurer un périphérique Axis pour l'envoi de tous ses messages journaux cryptés à un serveur syslog central. Les audits sont ainsi plus faciles et empêchent la suppression des messages journaux sur le périphérique Axis, que ce soit de manière intentionnellement et/ou malveillante. Selon les politiques de l'entreprise, il peut également fournir une durée de conservation étendue des journaux des périphériques.

Pour plus d'informations sur la façon d'activer le serveur syslog distant dans les différentes versions d'AXIS OS, consultez la section concernant *Syslog* dans AXIS OS Knowledge base.

Version d'AXIS OS	Chemin de configuration de l'interface Web
< 7.10	Pour plus d'instructions, consultez la section concernant *Syslog* dans AXIS OS Portal
7.10	Paramètres > Système > TCP/IP
≥ 10.9	Système > Journaux

SNMP

CSC n° 3 : Protection des pertes de données
CSC n°8 : Gestion des journaux d'audit

Il est possible de configurer un dispositif Axis pour qu'il envoie des données de surveillance SNMP cryptées à un serveur SNMP central via SNMPv3. La surveillance réseau basée sur SNMP permet de créer des alertes et de surveiller le dispositif sur une longue période. Veuillez noter que seul le protocole SNMPv3 offre un cryptage et une confidentialité, c'est pourquoi nous recommandons fortement son utilisation plutôt que celle des protocoles SNMPv1 et SNMPv2c.

Pour en savoir plus sur *SNMP*, veuillez consulter la base de connaissances d'AXIS OS.

Version d'AXIS OS	**Chemin de configuration de l'interface Web**
< 7.10	Pour plus d'instructions, consultez *SNMP* dans la base de connaissances d'AXIS OS.
7.10	Settings(Paramètres) > System(Système) > Network (Réseau) > SNMP
≥ 10.9	Système > Réseau > SNMP

Flux vidéo sécurisé (SRTP/RTSPS)

CSC n° 3 : Protection des pertes de données

À partir de la version 7.40 d'AXIS OS, les périphériques Axis prennent en charge le flux vidéo sécurisé sur RTP, également appelé SRTP/RTSPS. SRTP/RTSPS utilise une méthode de transport sécurisée et chiffrée de bout en bout pour s'assurer que seuls les clients autorisés reçoivent le flux vidéo du périphérique Axis. Nous vous recommandons d'activer SRTP/RTSPS si votre système de gestion vidéo (VMS) le prend en charge. Si possible, utilisez SRTP au lieu du flux vidéo RTP non crypté.

Remarque

SRTP/RTSPS crypte uniquement les données de flux vidéo. Pour les tâches de configuration d'administration nous vous recommandons d'activer HTTPS uniquement pour crypter ce type de communication.

Version d'AXIS OS	Chemin de configuration de l'interface Web
< 7.10	Configuration > Options système > Avancé > Configuration ordinaire > Réseau > RTSPS
7.10	Configuration > Système > Configuration ordinaire > Réseau > RTSPS
≥ 10.9	Système > Configuration ordinaire fil > Réseau > RTSPS

Vidéo signée

CSC n° 3 : Protection des pertes de données

À partir de la version 10.11 d'AXIS OS, les dispositifs Axis équipés d'Axis Edge Vault prennent en charge la vidéo signée, ce qui leur permet d'ajouter une signature à leur flux de données vidéo afin de garantir l'intégrité de la vidéo et de permettre la vérification de son origine en remontant jusqu'au dispositif qui l'a produite.

Axis fournit l'outil *Axis Signed media verifier*, que vous pouvez utiliser pour vérifier l'authenticité des vidéos enregistrées à partir d'un dispositif Axis. Nous proposons ces trois fichiers d'exemple que vous pouvez utiliser pour découvrir l'outil.

- *Vidéo originale mais non signée*
- *Vidéo originale et signée*
- *Vidéo modifiée*

Le système de gestion vidéo (VMS) ou le système de gestion des preuves (EMS) peut également vérifier l'authenticité de la vidéo fournie par un dispositif Axis.

Pour plus d'informations, consultez le livre blanc *Axis Edge Vault*. Pour trouver les certificats racine Axis utilisés pour valider l'authenticité de la vidéo signée, consultez la section concernant *l'accès au périphérique* dans AXIS OS Knowledge base.

Version d'AXIS OS	Chemin de configuration de l'interface Web
< 7.10	N/A
7.10	N/A
≥ 10.9	Système > Configuration ordinaire > Image > Vidéo signée

OAuth 2.0

CSC n°4 : Configuration sécurisée des ressources et logiciels d'entreprise
CSC n° 5 : Gestion des comptes

Avec OAuth 2.0, vous pouvez intégrer les périphériques AXIS OS fonctionnant sous AXIS OS 11.6 ou une version ultérieure dans une infrastructure informatique dotée d'un service centralisé de gestion des identités et des accès (IAM). Vous pouvez ainsi utiliser des identités fédérées pour vous authentifier sur le périphérique Axis, éliminant ainsi la nécessité d'une gestion locale des utilisateurs du périphérique.

OAuth atténue les attaques CSRF en utilisant un jeton unique pour garantir la validité de chaque requête.

Selon les caractéristiques du fournisseur de services, vous pouvez utiliser les mécanismes de sécurité suivants pour améliorer l'authentification basée sur l'identité vers le périphérique Axis :

- Authentification multifactorielle (MFA)
- Application de la complexité des mots de passe
- Rotation du mot de passe
- Authentification limitée dans le temps
- Gestion centralisée des identités (utilisateur/compte de service)

Pour plus d'informations sur la manière d'activer et de configurer OAuth 2.0 dans les périphériques AXIS OS, consultez *OAuth 2.0 OpenID Connect* dans la base de connaissances d'AXIS OS.

Version d'AXIS OS	Chemin de configuration de l'interface Web
< 7.10	N/A
7.10	N/A
≥ 11.6	System (Système) > Accounts (Comptes) > OpenID Configuration (Configuration OpenID)

Accessoires physiques anti-sabotage

CSC n°1 : Inventaire et contrôle des ressources d'entreprise
CSC n°12 : Gestion de l'infrastructure réseau

Axis propose des commutateurs d'intrusion physique et/ou de sabotage comme accessoires en option pour améliorer la protection physique des périphériques Axis. Ces commutateurs peuvent déclencher une alarme qui permet aux périphériques Axis d'envoyer une notification ou une alarme à des clients sélectionnés.

Pour plus d'informations sur les accessoires anti-sabotage disponibles, consultez :

- *AXIS TA8501 Physical Tampering Switch*
- *AXIS Dome Intrusion Switch C*
- *Contacteur de porte AXIS A*

Renforcement de la sécurité des dispositifs existants

Cette section présente des instructions de renforcement de la sécurité pour sécuriser les configurations des paramètres présents dans les versions ou produits AXIS OS hérités. Ces paramètres ne se trouvent pas sur les cycles LTS plus récents, les derniers cycles LTS en date, ou le cycle actif.

Environnement d'édition de scripts

Nous vous recommandons de désactiver l'accès à l'environnement d'éditeur de scripts. L'éditeur de script est utilisé à des fins de dépannage et de débogage uniquement.

L'éditeur de script a été supprimé de la version 10.11 d'AXIS OS et n'est plus disponible dans les versions ultérieures.

Version d'AXIS OS	Chemin de configuration de l'interface Web
< 7.10	N/A
7.10	Paramètres > Système > Configuration ordinaire > Système > Activer l'éditeur de script (editcgi)
≥ 10.9	Système > Configuration ordinaire > Système > Activer l'éditeur de script (editcgi)

Accès FTP

FTP est un protocole de communication non sécurisé utilisé uniquement à des fins de dépannage et de débogage. L'accès FTP a été supprimé dans AXIS OS 11.1 et n'est pas disponible dans les versions ultérieures. Nous vous recommandons de désactiver l'accès FTP et d'utiliser l'accès SSH sécurisé aux fins de dépannage.

Pour plus d'informations sur SSH, consultez la section concernant *l'accès SSH* dans AXIS OS Portal. Pour plus d'informations sur les options de débogage à l'aide de FTP, consultez la section concernant *l'accès FTP* dans AXIS OS Portal.

Version d'AXIS OS	Chemin de configuration de l'interface Web
< 7.10	Configuration > Options système > Configuration ordinaire > Réseau > FTP activé
7.10	Paramètres > Système > Configuration ordinaire > Réseau > FTP activé
≥ 10.9	Système > Configuration ordinaire > Réseau > FTP activé

Accès Telnet

Telnet est un protocole de communication non sécurisé utilisé à des fins de dépannage et de débogage uniquement. Il est pris en charge par les périphériques Axis dont la version est antérieure à AXIS OS 5.50. Nous vous recommandons de désactiver l'accès Telnet.

Version d'AXIS OS	Chemin de configuration de l'interface Web
< 5.50	Pour plus d'instructions, consultez *Device access (Accès aux périphériques)* dans la base de connaissances d'AXIS OS.
< 7.10	N/A

Version d'AXIS OS	Chemin de configuration de l'interface Web
7.10	N/A
≥ 10.9	N/A

ARP/Ping

ARP/Ping était une méthode permettant de définir l'adresse IP du périphérique Axis à l'aide d'outils comme AXIS IP Utility. Cette fonctionnalité a été supprimée de la version 7.10 d'AXIS OS et n'est plus disponible dans les versions ultérieures. Nous vous recommandons de désactiver la fonction sur les périphériques Axis dotés de la version 7.10 'd'AXIS OS et antérieures.

Version d'AXIS OS	Chemin de configuration de l'interface Web
< 7.10	Configuration > Options système > Avancé > Configuration ordinaire > Réseau > ARP/Ping
7.10	N/A
≥ 10.9	N/A

Versions TLS obsolètes

Nous vous recommandons de désactiver les versions TLS anciennes, obsolètes et non sécurisées avant de mettre votre périphérique Axis en production. Les versions TLS obsolètes sont généralement désactivées par défaut, mais il est toujours possible de les activer sur les dispositifs Axis pour permettre une rétrocompatibilité avec des applications tierces qui n'ont pas encore implémenté TLS 1.2 et TLS 1.3.

Les versions TLS obsolètes ont été supprimées de la version 12.0 d'AXIS OS et ne sont pas disponibles dans les versions ultérieures.

Version d'AXIS OS	Chemin de configuration de l'interface Web
< 7.10	Configuration > Options système > Avancé > Configuration ordinaire > HTTPS > Autoriser TLSv1.0 et/ou Autoriser TLSv1.1
7.10	Paramètres > Système > Configuration ordinaire > HTTPS > Autoriser TLSv1.0 et/ou Autoriser TLSv1.1
≥ 10.9 – 11.11.X -	Système > Configuration ordinaire > HTTPS > Autoriser TLSv1.0 et/ou Autoriser TLSv1.1

Journal d'accès

CSC n°1 : Inventaire et contrôle des ressources d'entreprise
CSC n°8 : Gestion des journaux d'audit

Le journal d'accès fournit les journaux détaillés des utilisateurs accédant au périphérique Axis, ce qui facilite les vérifications et la gestion du contrôle d'accès. Nous vous recommandons d'activer cette fonction et de la combiner à un serveur syslog distant pour que le périphérique Axis puisse envoyer ses journaux à un environnement de journalisation central. Cela simplifie le stockage des messages journaux et leur durée de conservation.

Pour plus d'informations, consultez la section concernant la *journalisation des accès aux périphériques* dans AXIS OS Knowledge base.

Version d'AXIS OS	Chemin de configuration de l'interface Web
< 7.10	Configuration > Système > Système avancé > Configuration ordinaire > Système > Journal d'accès
7.10	Paramètres > Système > Configuration ordinaire > Système > Journal d'accès
≥ 10.9	Système > Configuration ordinaire > Système > Journal d'accès

Guide de prise en main

Le guide de démarrage rapide fournit une brève vue d'ensemble des paramètres que vous devez configurer lorsque vous renforcez les périphériques Axis avec les versions AXIS OS 5.51 et ultérieures. Il couvre les sujets relatifs au renforcement présentés dans *Renforcement de base, on page 14* ; cependant, il ne couvre pas les sujets présentés dans *Renforcement étendu, on page 25* car ils nécessitent une configuration étendue et spécifique au client au cas par cas.

Nous vous recommandons d'utiliser AXIS Device Manager pour renforcer plusieurs périphériques Axis de façon rapide et économique. Si vous devez utiliser une autre application pour la configuration des périphériques ou uniquement pour renforcer quelques périphériques Axis, nous vous recommandons d'utiliser l'API VAPIX.

Erreurs de configuration courantes

Remarque

Les erreurs de configuration courantes répertoriées ci-dessous augmentent potentiellement la surface d'attaque du périphérique Axis et réduisent ses couches de défense en matière de cybersécurité, ce qui entraîne un risque plus élevé d'exploitation, d'utilisation abusive, ou de fonctionnement non sécurisé du périphérique.

Périphériques exposés à Internet
CSC n°12 : Gestion de l'infrastructure réseau

Il est déconseillé d'exposer le périphérique Axis en tant que serveur Web public ou d'accorder à des clients inconnus un accès au réseau au périphérique. Pour en savoir plus, consultez .

Mot de passe commun
CSC n°4 : Configuration sécurisée des ressources et logiciels d'entreprise
CSC n° 5 : Gestion des comptes

Nous vous recommandons fortement d'utiliser un mot de passe unique pour chaque périphérique au lieu d'un mot de passe générique pour tous les périphériques. Pour obtenir des instructions, consultez *Identity and access management (Gestion des identités et des accès)* dans la base de connaissances d'AXIS OS et *Créer des comptes dédiés, on page 15*.

Accès anonyme
CSC n°4 : Configuration sécurisée des ressources et logiciels d'entreprise
CSC n° 5 : Gestion des comptes.

Il est déconseillé d'autoriser des utilisateurs anonymes à accéder aux paramètres vidéo et de configuration sur le périphérique sans avoir à fournir les identifiants de connexion. Pour plus d'informations, consultez *Désactivé par défaut, on page 4*.

Communication sécurisée désactivée
CSC n° 3 : Protection des pertes de données

Il est déconseillé d'utiliser le périphérique en employant des méthodes de communication et d'accès non sécurisées, telles que HTTP ou l'authentification de base lorsque les mots de passe sont transférés sans cryptage. Pour en savoir plus, consultez *HTTPS activé, on page 8*. Pour des recommandations de configuration, consultez la section concernant consultez la section *Authentification Digest, on page 4*.

Version d'AXIS OS obsolète
CSC n°2 : Inventaire et contrôle des ressources logicielles

Nous vous recommandons vivement d'utiliser le périphérique Axis avec la dernière version d'AXIS OS disponible, soit sur le LTS, soit sur la piste active. Ces deux pistes fournissent les derniers correctifs de sécurité et résolutions de bogues. Pour en savoir plus, consultez *Mise à niveau vers la dernière version d'AXIS OS, on page 14*.

Renforcement de base via API VAPIX

Vous pouvez utiliser l'API VAPIX pour renforcer vos périphériques Axis en vous basant sur les rubriques couvertes dans *Renforcement de base, on page 14*. Dans ce tableau, vous pouvez trouver tous les paramètres de base d'une configuration de renforcement, indépendamment de la version AXIS OS de votre périphérique Axis.

Il est possible que certains paramètres de configuration ne soient plus disponibles dans la version AXIS OS de votre périphérique, car certaines fonctionnalités ont été supprimées au fil du temps pour renforcer la sécurité. Si vous recevez une erreur lors de l'émission de l'appel VAPIX, cela peut indiquer que la fonctionnalité n'est plus disponible dans la version d'AXIS OS.

Objectif	Appel API VAPIX
*Désactiver POE dans les ports réseau inutilisés**	`http://ip-address/axis-cgi/nvr/poe/setportmode.cgi?port=X&enabld=no`
*Désactiver le trafic réseau dans les ports réseau inutilisés***	`http://ip-address/axis-cgi/network_settings.cgi { "apiVersion": "1.17", "method": "setDeviceConfiguration", "params": { "deviceName": "eth1.1", "staticState": "down" } }`
Désactiver le protocole de détection Bonjour	`https://ip-address/axis-cgi/param.cgi?action=update&Network.Bonjour.Enabled=no`
Désactiver le protocole de détection UPnP	`https://ip-address/axis-cgi/param.cgi?action=update&Network.UPnP.Enabled=no` `https://ip-address/axis-cgi/param.cgi?action=update&Network.UPnP.NATTraversal.Enabled=no`
Désactiver le protocole de détection WebActiver	`https://ip-address/axis-cgi/param.cgi?action=update&WebService.DiscoveryMode.Discoverable=no`
Désactiver le service one-click cloud connection (O3C)	`https://ip-address/axis-cgi/param.cgi?action=update&RemoteService.Enabled=no`
Désactiver l'accès à la maintenance SSH du périphérique	`https://ip-address/axis-cgi/param.cgi?action=update&Network.SSH.Enabled=no`
Désactiver l'accès à la maintenance FTP du périphérique	`https://ip-address/axis-cgi/param.cgi?action=update&Network.FTP.Enabled=no`
Désactiver la configuration de l'adresse IP ARP-Ping	`https://ip-address/axis-cgi/param.cgi?action=update&Network.ARPPingIPAddress.Enabled=no`
Désactiver la configuration de l'adresse IP Zero-Conf	`http://ip-address/axis-cgi/param.cgi?action=update&Network.ZeroConf.Enabled=no`
Activer HTTPS seulement	`https://ip-address/axis-cgi/param.cgi?action=update&System.BoaGroupPolicy.admin=https`

Objectif	Appel API VAPIX
	`https://ip-address/axis-cgi/param.cgi?action=update&System.BoaGroupPolicy.operator=https` `https://ip-address/axis-cgi/param.cgi?action=update&System.BoaGroupPolicy.viewer=https`
Activer TLS 1.2 et TLS 1.3 uniquement	`https://ip-address/axis-cgi/param.cgi?action=update&HTTPS.AllowTLS1=no` `https://ip-address/axis-cgi/param.cgi?action=update&HTTPS.AllowTLS11=no`
Configuration de cryptogrammes TLS 1.2	`https://ip-address/axis-cgi/param.cgi?action=update&HTTPS.Ciphers=ECDHE-ECDSA-AES128-GCM-SHA256:ECDHE-RSA-AES128-GCM-SHA256:ECDHE-ECDSA-AES256-GCM-SHA384:ECDHE-RSA-AES256-GCM-SHA384:ECDHE-ECDSA-CHACHA20-POLY1305:ECDHE-RSA-CHACHA20-POLY1305`

*Activer la protection contre les attaques par force brute****	`https://ip-address/axis-cgi/param.cgi?action=update&System.PreventDoSAttack.ActivatePasswordThrottling=on`
	`https://ip-address/axis-cgi/param.cgi?action=update&System.PreventDoSAttack.DoSBlockingPeriod=10`
	`https://ip-address/axis-cgi/param.cgi?action=update&System.PreventDoSAttack.DoSPageCount=20`
	`https://ip-address/axis-cgi/param.cgi?action=update&System.PreventDoSAttack.DoSPageInterval=1`
	`https://ip-address/axis-cgi/param.cgi?action=update&System.PreventDoSAttack.DoSSiteCount=20`
	`https://ip-address/axis-cgi/param.cgi?action=update&System.PreventDoSAttack.DoSSiteInterval=1`

Désactiver l'environnement d'éditeur de scripts	`https://ip-address/axis-cgi/param.cgi?action=update&System.EditCgi=no`
Activer les journalisations d'accès utilisateur améliorées	`https://ip-address/axis-cgi/param.cgi?action=update&System.AccessLog=On`
Activer la protection contre les attaques par relecture ONVIF	`https://ip-address/axis-cgi/param.cgi?action=update&WebService.UsernameToken.ReplayAttackProtection=yes`
Désactiver l'accès à l'interface Web du périphérique	`https://ip-address/axis-cgi/param.cgi?action=update&System.WebInterfaceDisabled=yes`

Objectif	Appel API VAPIX
Désactiver l'en-tête de serveur HTTP/OpenSSL	`https://ip-address/axis-cgi/param.cgi?action=update&System.HTTPServerTokens=no`

Désactiver la consultation anonyme et l'accès PTZ	`https://ip-address/axis-cgi/param.cgi?action=update&root.Network.RTSP.ProtViewer=password`
	`https://ip-address/axis-cgi/param.cgi?action=update&root.System.BoaProtViewer=password`
	`https://ip-address/axis-cgi/param.cgi?action=update&root.PTZ.BoaProtPTZOperator=password`

Empêcher l'installation du privilège racine exigeant des applications ACAP	`http://ip-address/axis-cgi/applications/config.cgi?action=set&name=AllowRoot&value=false`
Empêcher l'installation d'applications ACAP non signées	`http://ip-address/axis-cgi/applications/config.cgi?action=set&name=AllowUnsigned&value=false`

* Remplacez « X » par le numéro de port réel dans « port=X ». Exemples : « port=1 » désactivera le port 1 et « port=2 » désactivera le port 2.
** Remplacez « 1 » par le numéro de port réel dans « eth1.1 ». Exemples : « eth1.1 » désactivera le port 1 et « eth1.2 » désactivera le port 2.
*** Après 20 tentatives de connexion échouées en l'espace d'une seconde, l'adresse IP du client est bloquée pendant 10 secondes. Chaque demande en échec suivante dans l'intervalle de 30 secondes de la page entraîne l'extension de 10 secondes de la période de blocage DoS.

Renforcement de base via AXIS Device Manager (Extend)

Vous pouvez utiliser AXIS Device Manager et AXIS Device Manager Extend pour renforcer vos périphériques Axis en vous aidant des informations présentées dans *Renforcement de base, on page 14*. Utilisez ce *fichier de configuration*, qui se compose des mêmes paramètres de configuration répertoriés dans *Renforcement de base via API VAPIX, on page 33*.

Il est possible que certains paramètres de configuration ne soient plus disponibles dans la version AXIS OS de votre périphérique, car certaines fonctionnalités ont été supprimées au fil du temps pour renforcer la sécurité. AXIS Device Manager et AXIS Device Manager Extend suppriment automatiquement ces paramètres de la configuration de renforcement.

Remarque

Une fois le fichier de configuration chargé, le périphérique Axis est configuré sur HTTPS uniquement et l'interface Web est désactivée. Vous pouvez modifier le fichier de configuration en fonction de vos besoins, par exemple en supprimant ou en ajoutant des paramètres.

Notifications de sécurité

Nous vous recommandons de vous inscrire au *service de notification de sécurité Axis* pour recevoir des informations sur les vulnérabilités récemment découvertes dans les produits, solutions et services Axis, ainsi que sur la manière de sécuriser vos périphériques Axis.

T10177717_fr

2026-03 (M62.2)