AXIS OS Hardening Guide

AXIS OS Portal | *Notes de version d'AXIS OS* | *AXIS OS Knowledge base* | *Avis de sécurité d'AXIS OS*

AXIS OS Hardening Guide

Présentation

Présentation

Axis Communications s'efforce d'appliquer les bonnes pratiques de cybersécurité dans la conception, le développement et le test de nos dispositifs. L'objectif est de réduire le risque d'un défaut qui pourrait être exploité par des pirates informatiques lors d'une attaque. Toutefois, l'ensemble de la chaîne logistique du fournisseur et de l'organisation de l'utilisateur final doivent être impliqués dans la sécurisation d'un réseau, de ses périphériques et des services pris en charge. Un environnement sécurisé dépend de ses utilisateurs, process et technologies. L'objectif de ce guide est de vous aider à sécuriser votre réseau, vos périphériques et vos services.

Les menaces les plus évidentes pour un périphérique Axis sont la destruction physique, le vandalisme et le sabotage. Pour protéger un produit contre ces menaces, il est important de choisir un modèle ou un boîtier anti-vandalisme, de le monter dans les règles de l'art et de protéger les câbles.

Les périphériques Axis sont des points de terminaison en réseau comme les ordinateurs et les téléphones mobiles. Nombre d'entre eux sont dotés d'une interface Web qui peut présenter des vulnérabilités aux systèmes connectés. Dans ce guide, nous expliquons comment vous pouvez réduire ces risques.

Le présent guide fournit des conseils techniques à tous ceux qui sont chargés du déploiement des solutions Axis. Il comprend une configuration de base recommandée ainsi qu'un guide de renforcement qui prend en compte l'évolution des menaces. Vous devrez peut-être consulter le manuel d'utilisation du produit pour apprendre à configurer des paramètres spécifiques. Notez que les périphériques Axis ont reçu une mise à jour de l'interface Web dans AXIS OS 7.10 et 10.9, qui a modifié le chemin d'accès à la configuration.

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 du système d'exploitation AXIS 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

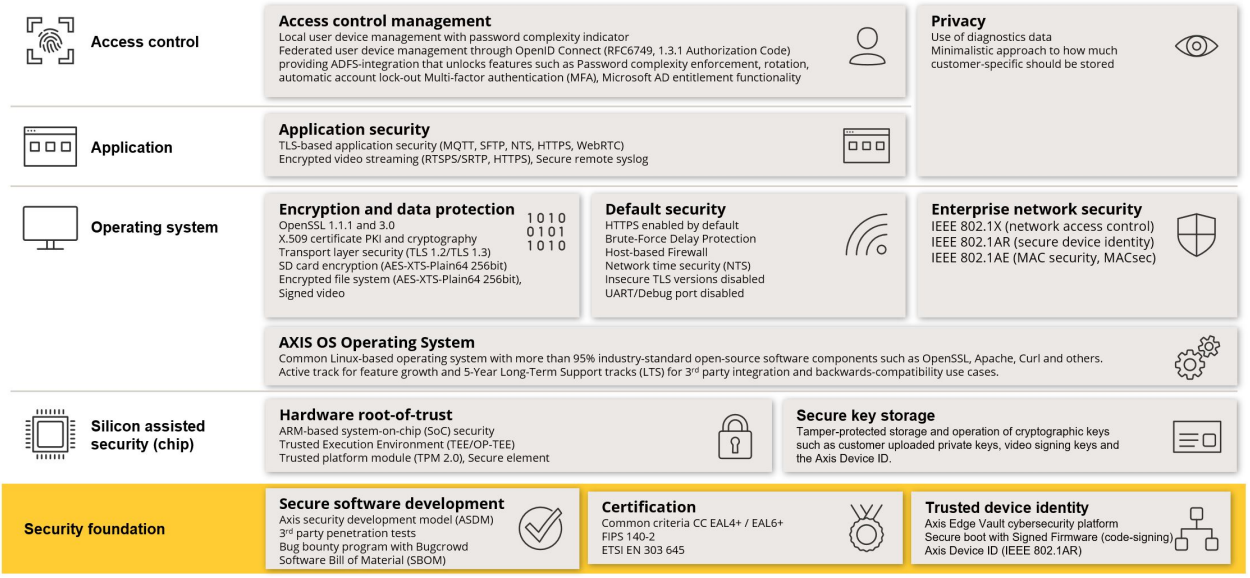
Portée

Ce guide s'applique à tous les produits basés sur AXIS OS exécutant AXIS OS (suivi LTS ou actif) ainsi qu'aux produits existants des versions 4.xx et 5.xx.

Présentation

Architecture de sécurité d'AXIS OS

Le diagramme de l'architecture de sécurité d'AXIS OS décrit les capacités de cybersécurité d'AXIS OS à travers différentes couches, offrant une vue complète 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.

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.

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

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.

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.

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

Accès avec accréditation

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.

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 sur les périphériques Axis. Ceux-ci sont répertoriés dans ce tableau.

Protocole	Port	Transport	Commentaires
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	UDP	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
Bonjour	5353	UDP	Utilisé par des applications tierces pour détecter le périphérique Axis via le protocole de détection mDNS (Bonjour)

Protection par défaut

Protocole	Port	Transport	Commentaires
SSDP	1900	UDP	Utilisé par des applications tierces pour détecter le périphérique Axis via SSDP (UPnP)
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 bord à bord, consultez le livre blanc Technologie bord à bord.*

***Attribution automatique dans une plage prédéfinie de numéros de port conformément à la norme RFC 6056. Pour plus d'informations, consultez l'article Wikipedia sur les ports éphémères.*

Nous vous recommandons de désactiver, si possible, les protocoles et services réseau inutilisés. Pour obtenir une liste complète des services utilisés par défaut ou qui peuvent être activés en fonction de la configuration, voir *Ports couramment utilisés* dans AXIS OS Knowledge base.

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 et donc activées par défaut.

Interface UART/de débogage

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

Chaque périphérique Axis est fourni avec une interface UART physique (Universal Asynchronous Receiver Transmitter), parfois appelée « port de débogage » ou « console série ». L'interface elle-même n'est accessible que physiquement en raison d'un vaste démantèlement 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.

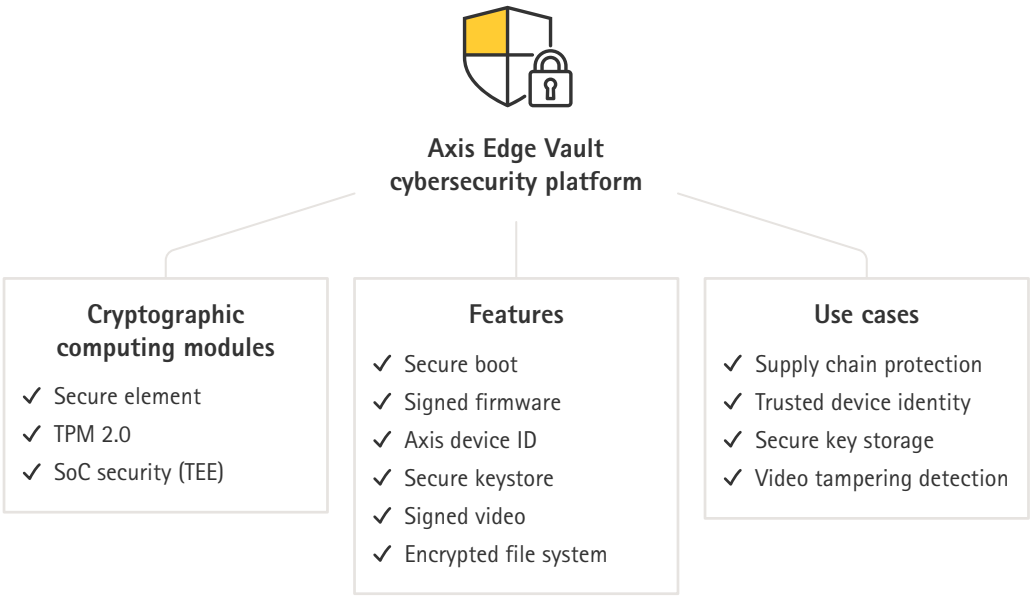
L'interface UART/de débogage est activée par défaut sur les périphériques Axis dotés d'AXIS OS 10.10 et versions antérieures, mais elle nécessite un accès authentifié et n'expose aucune information sensible tout en étant non authentifiée. À compter de la version 10.11 d'AXIS OS, l'interface UART/de débogage 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 s'appuie sur de solides modules de calcul cryptographique (élément sécurisé et TPM) et de sécurité SoC (TEE et amorçage sécurisé), associés à une expertise en sécurité des périphériques edge. Axis Edge Vault repose sur une racine de confiance solide établie par un démarrage sécurisé et un firmware signé. Ainsi, tous les logiciels sont validés de manière cryptographique et ces fonctionnalités forment une chaîne de confiance dont dépendent toutes les opérations sécurisées.

Les périphériques Axis avec Axis Edge Vault minimisent l'exposition des clients 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 du client.

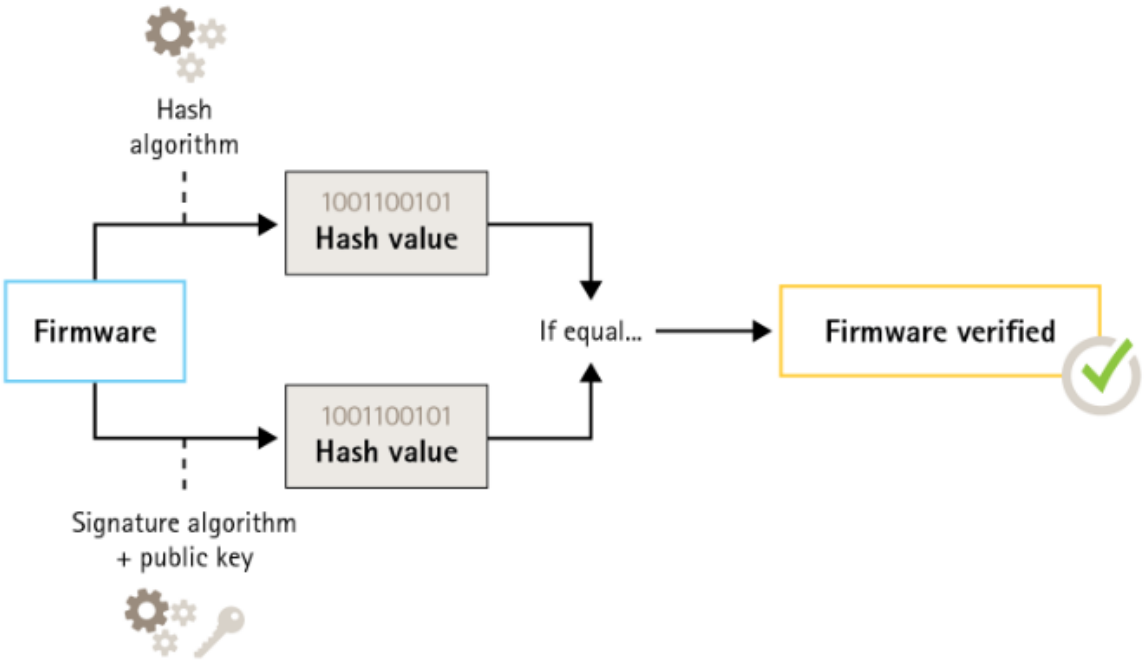
Protection par défaut



Firmware signé

CSC n° 2 : Inventaire et contrôle des ressources logicielles

AXIS OS est signé à partir de la version 9.20.1. Chaque fois que vous mettez à niveau la version d'AXIS OS sur le périphérique, ce dernier vérifie l'intégrité des fichiers de mise à jour via la vérification de la signature cryptographique et rejette tout fichier falsifié. Cela permet d'éviter que des personnes malveillantes leurrent les utilisateurs pour qu'ils installent des fichiers compromis.



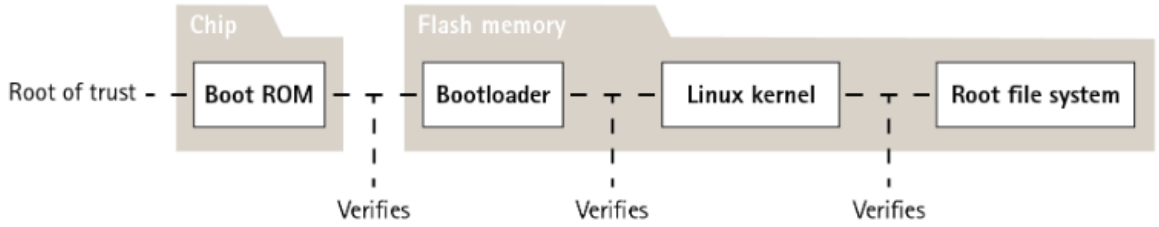
Protection par défaut

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.

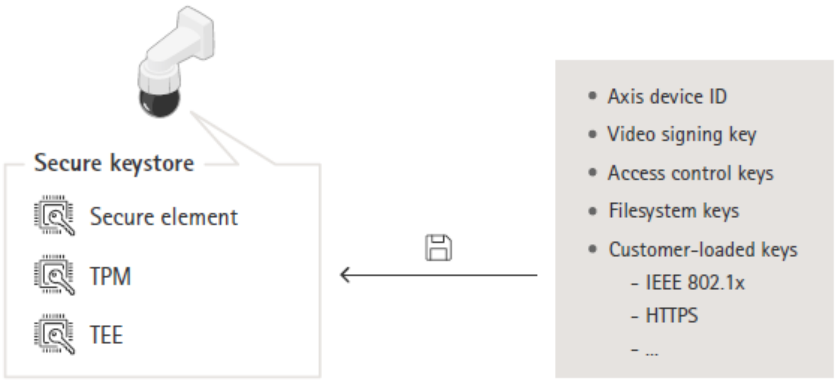


Pour plus d'informations, consultez le livre blanc *Axis Edge Vault*.

Keystore sécurisé

CSC n° 6 : Gestion du contrôle d'accès

Le keystore sécurisé fournit un espace de stockage matériel infalsifiable des informations cryptographiques. 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 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-Plain64256 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*.

HTTPS activé

CSC n 3 : Protection des données

À compter 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. À compter 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

En-têtes HTTP(S) par défaut

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. À compter de la version 9.80 d'AXIS OS, 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 la section concernant les *en-têtes HTTP(S) par défauts* dans Axis OS Knowledge base.

Authentification Digest

CSC n 3 : Protection des 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 donc d'utiliser l'authentification Digest uniquement au lieu d'une authentification de type Base ou à la fois de type Base et 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 > Politique d'authentification HTTP réseau
≥ 7.10	Paramètres > Système > Configuration ordinaire > Politique d>authentification HTTP réseau
≥ 10.9	Système > Configuration ordinaire > Politique d>authentification HTTP réseau

Protection contre les attaques par relecture ONVIF

CSC n 3 : Protection des 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 attaques par force brute est activée par défaut à partir d'AXIS OS 11.5. Pour des exemples de configuration et des recommandations détaillés, consultez la section concernant la *protection contre les attaques par force brute* dans AXIS OS Knowledge base.

Version d'AXIS OS	Chemin de configuration de l'interface Web
< 7.10	Sans objet
≥ 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

Démantèlement

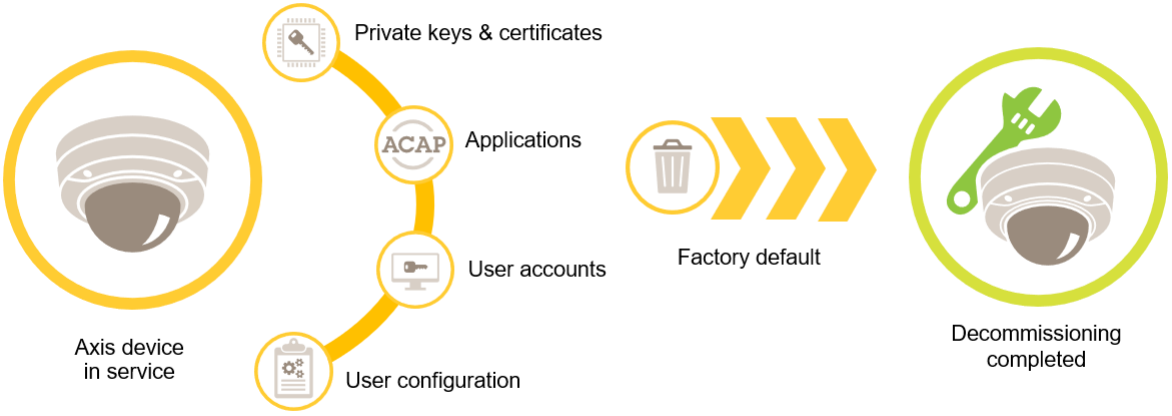
CSC n 3 : Protection des données

Les périphériques Axis utilisent à la fois une mémoire volatile et non volatile, et si cette mémoire volatile est effacée dès que vous débranchez le périphérique de sa source d'alimentation, les informations stockées dans la mémoire non volatile sont conservées et à nouveau disponibles 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. La fonction UBI de suppression de volume est utilisée pour la mémoire Flash de type NAND ; la fonction équivalente est utilisée pour la mémoire Flash eMMC qui signale 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'efface pas immédiatement les données. En effet, le périphérique redémarre et l'effacement des données a lieu pendant le démarrage du système. Ainsi, il ne suffit pas de simplement émettre la commande de remise en paramètres d'usine, le périphérique doit également être autorisé à redémarrer et terminer son processus de démarrage avant d'être mis hors tension pour garantir que l'effacement des données est bien effectué.

Protection par défaut



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
≥ 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

Protection par défaut

** Le processus de firmware signé utilise des certificats personnalisés qui permettent aux utilisateurs de charger (entre autres) AXIS OS.*
*** Les enregistrements et images stockés sur le stockage edge (carte SD, partage réseau) doivent être supprimés par l'utilisateur séparément. Pour plus d'informations, voir Formatage des cartes SD Axis* dans AXIS OS Knowledge base.
**** Toutes les configurations créées par l'utilisateur, de la création de comptes aux configurations réseau, O3C, événement, image, PTZ et système.*
***** Le périphérique conserve les applications préinstallées mais supprime toutes les configurations que l'utilisateur y a créé*
****** Les données de production (calibrage, certificats de production 802.1AR) et statistiques de durée de vie incluent des données non sensibles et des informations non liées aux utilisateur.*

Renforcement de base

Le renforcement de base est le niveau de protection minimal recommandé pour les périphériques Axis. Les sujets relatifs au renforcement de base sont « configurables en périphérie ». Cela signifie qu'ils peuvent être directement configurés 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 par défaut

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 *Démantèlement à la page 10*.

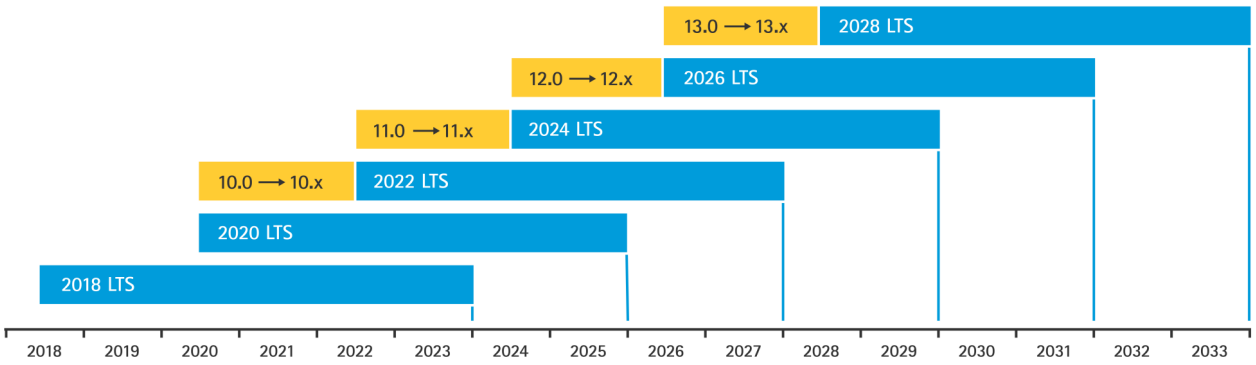
Version d'AXIS OS	Chemin de configuration de l'interface Web
< 7.10	Configuration > Options du système > Maintenance > Par défaut.
≥ 7.10	Paramètres > Système > Maintenance
≥ 10.9	Maintenance > Par défaut

Mise à niveau vers la dernière version d'AXIS OS

CSC n° 2 : Inventaire et contrôle des ressources logicielles

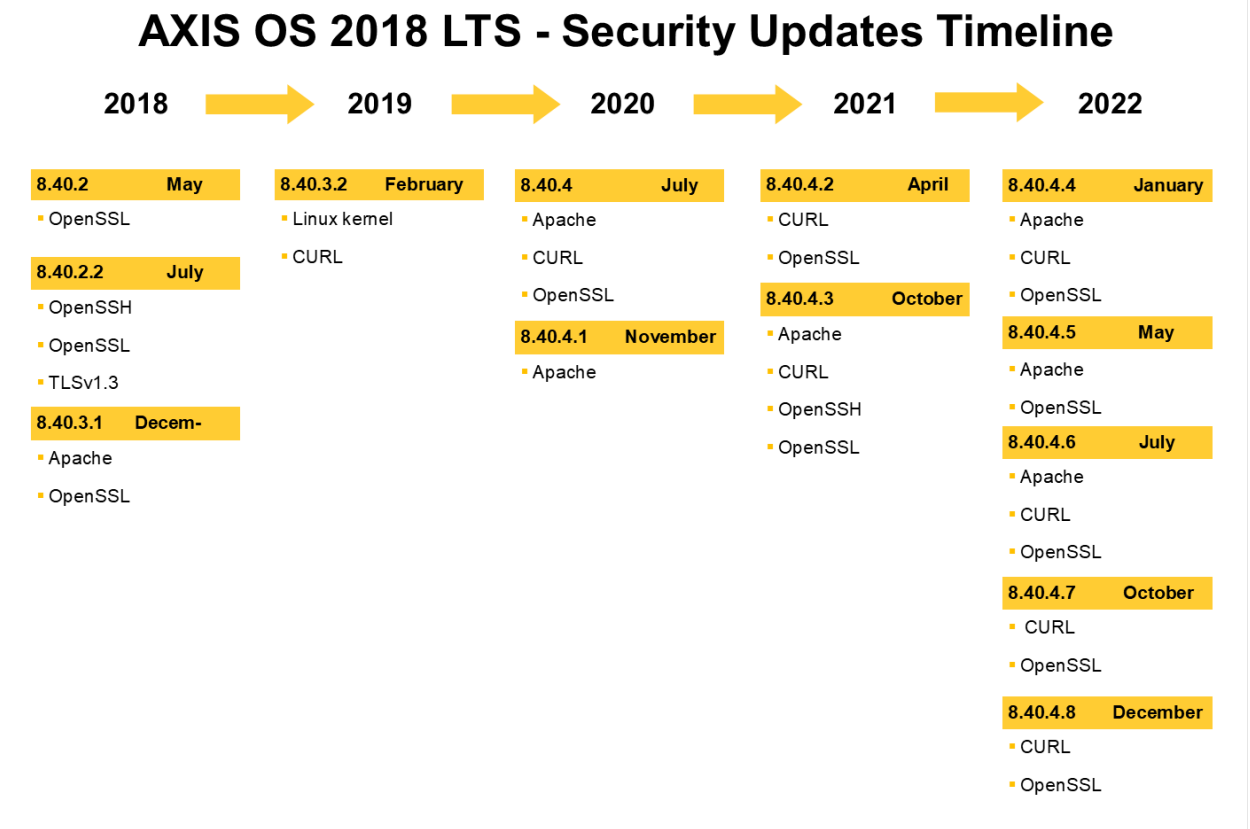
Les correctifs de logiciels sont un élément essentiel de la cybersécurité. Les pirates essaient souvent d'exploiter les vulnérabilités communément connues et peuvent réussir si ils accèdent au réseau à un service non corrigé. Assurez-vous d'utiliser toujours l'AXIS OS le plus récent, car il peut inclure 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 maintient deux types de suivis d'AXIS OS : le suivi actif et le suivi à long terme (LTS). Bien que les deux types incluent les derniers correctifs de vulnérabilité critiques, les suivis 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 *firmware* sur axis.com afin de télécharger AXIS OS pour votre périphérique.

Ce graphique illustre l'importance de tenir les périphériques Axis à jour.



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	Maintenance > Mise à niveau du firmware

Définir un mot de passe racine pour le périphérique

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

Le compte racine du périphérique est le compte principal d'administration des périphériques. Pour pouvoir utiliser le compte racine, vous devez définir un mot de passe pour périphérique. Assurez-vous d'utiliser un mot de passe fort et de limiter l'utilisation du compte racine aux tâches administratives uniquement. Il est déconseillé d'utiliser le compte racine dans la production quotidienne.

Lorsque vous utilisez des périphériques Axis, l'utilisation du même mot de passe simplifie la gestion, mais augmente votre vulnérabilité aux violations et aux fuites de données. L'utilisation de mots de passe uniques pour chaque périphérique Axis offre une haute sécurité, mais rend la gestion des périphériques plus complexe. Nous vous recommandons de modifier régulièrement le mot de passe de vos périphériques.

Nous vous recommandons de mettre en œuvre des directives qui exigent que les nouveaux mots de passe soient suffisamment longs et complexes, par exemple *les recommandations de mots de passe NIST*. 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.

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

Créer des comptes dédiés

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

Le compte racine par défaut a tous les privilèges et doit être réservé aux tâches d'administrations. Nous vous recommandons de créer un compte utilisateur client avec des droits d'accès limités pour le fonctionnement quotidien. Cela réduit le risque de compromettre le mot de passe de l'administrateur du périphérique.

Pour plus d'informations, consultez le livre blanc *Identité et gestion des accès dans les systèmes de vidéosurveillance*.

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

Limiter l'accès à l'interface Web

CSC n° : Gestion de compte

Les périphériques Axis disposent d'un serveur Web qui permet aux utilisateurs d'accéder au périphérique via un navigateur Web standard. L'interface Web est destinée à la configuration, à la maintenance et au dépannage. Elle n'est pas destinée aux opérations quotidiennes, par exemple en tant que 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. Pour en savoir plus, consultez *Désactiver l'accès à l'interface Web à la page 15*.

Désactiver l'accès à l'interface Web

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

À compter de la version 9.50 d'AXIS OS, il est possible de désactiver l'interface Web d'un périphérique 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	Sans objet
≥ 7.10	Paramètres > Système > Configuration simple > Système > Interface Web désactivée
≥ 10.9	Système > Configuration simple > Système > Interface Web désactivée

Configurer les paramètres réseau

CSC n° 12 : Gestion de l'infrastructure réseau

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. Nous vous recommandons de passer en revue votre topologie réseau dès que vous ajoutez de nouveaux types de composants.

Nous vous recommandons également d'utiliser une configuration d'adresse IP statique sur vos périphériques Axis pour garantir l'accessibilité au réseau et résoudre les problèmes de dépendance avec les serveurs réseau (comme les serveurs DHCP) qui pourraient être la cible d'attaques.

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

Configurer les paramètres de date et d'heure

CSC n° 8 : Gestion des journaux d'audit

Du point de vue de la sécurité, il est important de définir la date et l'heure correctes. Cela garantit, par exemple, que les journaux système sont correctement horodatés et que les certificats numériques peuvent être validés et utilisés au cours d'une période donnée. Sans synchronisation adéquate de l'heure, les services qui reposent sur des certificats numériques tels que HTTPS, IEEE et 802.1x peuvent ne pas fonctionner correctement.

Nous vous recommandons de synchroniser l'horloge du périphérique Axis avec les serveurs NTP (Network Time Protocol, non cryptés) ou, de préférence, les serveurs NTS (Network Time Security, crypté). Network Time Security (NTS), variante cryptée et sécurisée du protocole Network Time Protocol (NTP), a été ajouté à AXIS OS 11.1. Nous vous recommandons de configurer plusieurs serveurs de temps pour une plus grande précision de synchronisation du temps, mais également pour tenir compte d'un scénario de reprise où l'un des serveurs de temps configurés pourrait ne pas être disponible.

L'utilisation de serveurs NTP ou NTS publics peut être une alternative pour les particuliers et les petites organisations qui ne peuvent pas faciliter elles-mêmes les instances de serveur de temps local. 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 edge

CSC n 3 : Protection des 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 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

Exporter le cryptage d'enregistrement

CSC n 3 : Protection des données

À compter de la version 10.10 d'AXIS OS, les périphériques Axis prennent en charge l'exportation cryptée des enregistrements périphériques. 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	Sans objet
≥ 7.10	Sans objet
≥ 10.9	Enregistrements

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.

Renforcement de base

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

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.

Ports réseau physiques non inutilisés

À compter 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	Sans objet
≥ 7.10	Sans objet
≥ 11.2	Système > Power over Ethernet

Protocoles de détection réseau

Les protocoles de détection, tels que Bonjour, UPnP, ZeroConf et WS-Discovery, 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*
	Sans objet
≥ 7.10	Paramètres > Système > Configuration ordinaire > Avance > Réseau > Réseau Bonjour activé, réseau UPnP activé, réseau ZeroConf activé, réseau UPnP NATTraversal activé*
	Paramètres > Système > Configuration ordinaire > Service Web > Mode de détection

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

** Fonctionnalité a été supprimée d'Axis OS 10.12 et non disponible dans les versions ultérieures*

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 possible de les activer sur les périphériques Axis pour permettre une rétrocompatibilité avec les applications tierces qui n'ont pas encore implémenté TLS 1.2 et TLS 1.3.

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	Système > Configuration ordinaire > HTTPS > Autoriser TLSv1.0 *et/ou* Autoriser TLSv1.1

Environnement d'éditeur 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 d'Axis OS 10.11 et n'est plus disponible dans les versions ultérieures.

Version d'AXIS OS	Chemin de configuration de l'interface Web
< 7.10	Sans objet
≥ 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)

En-têtes de serveur HTTP(S)

Par défaut, les périphériques Axis annoncent leurs versions Apache et OpenSSL actuelles pendant lors des connexions HTTP(S) avec des clients sur le réseau. Ces informations sont utiles lorsque vous utilisez régulièrement des scanners de sécurité réseau, car elles fournissent un rapport plus détaillé des vulnérabilités exceptionnelles dans une version d'OS AXIS spécifique.

Il est possible de désactiver les en-têtes de serveur HTTP(S) pour réduire l'exposition aux informations lors des connexions HTTP(S). Cependant, nous vous recommandons uniquement de désactiver les en-têtes si vous utilisez votre périphérique conformément à nos recommandations et que vous le conservez à jour à tout moment.

L'option de désactivation des en-têtes de serveur HTTP(S) est disponible à compter de la version 10.6 d'AXIS OS.

Version d'AXIS OS	Chemin de configuration de l'interface Web
< 7.10	Sans objet
≥ 7.10	Paramètres > Système > Configuration ordinaire > Système > Commentaires d'en-tête de serveur HTTP
≥ 10.9	Système > Configuration ordinaire > Système > Commentaires d'en-tête de serveur HTTP

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	Sans objet
≥ 7.10	Paramètres > Système > Configuration ordinaire > Stockage > Disque SD activé
≥ 10.9	Système > Configuration ordinaire > Stockage > Disque SD activé

Accès FTP

Le protocole FTP est un protocole de communication non sécurisé utilisé à des fins de dépannage et de débogage uniquement. L'accès FTP a été supprimé d'AXIS OS11.1 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 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 compter d'AXIS 5.50. 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

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 doté de versions antérieures 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 la section concernant *l'accès aux périphériques* dans AXIS Knowledge base.
< 7.10	Sans objet
≥ 7.10	Sans objet
≥ 10.9	Sans objet

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 d'Axis OS 7.10 et n'est plus disponible dans les versions ultérieures. Nous vous recommandons de désactiver la fonction sur les périphériques Axis dotés d'AXIS OS 7.10 et versions 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	Sans objet
≥ 10.9	Sans objet

Filtre d'adresse IP

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

Le filtrage d'adresses IP empêche les clients non autorisés d'accéder au périphérique Axis. Nous vous recommandons de configurer votre périphérique de manière à autoriser les adresses IP des hôtes réseau autorisés ou à rejeter les adresses IP des hôtes réseau non autorisés.

Si vous choisissez d'autoriser les adresses IP, assurez-vous d'ajouter tous les clients autorisés (serveur VMS et 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 > Filtre d'adresse IP
≥ 10.9*	Configuration > Sécurité > Filtre d'adresse IP

Dans les versions d'AXIS OS 11.9 et ultérieures, le filtre d'adresse IP a été remplacé par le nouveau pare-feu basé sur l'hôte.

Pare-feu basé sur l'hôte

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

Via le pare-feu, les utilisateurs peuvent créer des règles permettant de réguler le trafic entrant vers les périphériques par adresse IP et/ou numéro de port TCP/UDP. Par conséquent, cette politique est en mesure d'empêcher les clients non autorisés d'accéder aux périphériques Axis ou à des services spécifiques sur les périphériques.

Si vous définissez la politique par défaut sur « Deny » (Refuser), 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	Configuration > Sécurité > Pare-feu

HTTPS

CSC n 3 : Protection des données

Les protocoles HTTP et HTTPS sont activés par défaut sur les périphériques Axis à compter de la version 7.20 d'AXIS OS. Alors que l'accès HTTP n'est pas sécurisé et qu'il ne permet aucun 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 à la page 22* et *Cryptogrammes HTTPS à la 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 compter de la version 7.20 d'AXIS OS, les périphériques Axis sont signés avec un certificat auto-signé. Bien qu'un certificat auto-signé ne soit pas fiable dès la conception, il est approprié d'accéder en toute sécurité au périphérique Axis pendant la configuration initiale et lorsqu'aucune infrastructure de 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 compter 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. Après avoir réinitialisé le périphérique Axis aux paramètres d'usine par défaut, il est possible que la liste des cryptogrammes soit mise à jour automatiquement en fonction des dernières meilleures pratiques fournies par Axis.

Pour plus de référence et de transparence, utilisez les suites cryptographiques sécurisées et puissantes répertoriées dans *TLS 1.2 et antérieur à la page 23* et *TLS 1.3 à la page 23*

TLS 1.2 et antérieur

```
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:DHE-RSA-AES128-GCM-SHA256:DHE-RSA-AES256-GCM-SHA384
```

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.

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

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*
- *Interrupteur de porte AXIS A*

Renforcement étendu

Les instructions relatives à un renforcement étendu s'appuient sur les rubriques de renforcement décrites dans *Protection par défaut à la page 5* et dans *Renforcement de base à la page 13* 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

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 les petites organisations et les personnes qui ne gèrent pas un VMS ou qui ont besoin d'accéder aux vidéos à partir d'emplacements distants, nous recommandons l'utilisation d'AXIS Companion.

AXIS Companion utilise un logiciel client Windows/iOS/Android, il est gratuit et il offre un accès facile aux vidéos en toute sécurité, sans exposer le périphérique Axis à Internet. Pour obtenir plus d'informations sur AXIS Companion, consultez le site *axis.com/companion*.

Remarque

Toutes les organisations qui utilisent VMS doivent consulter le fournisseur de logiciels de gestion vidéo pour prendre connaissance des meilleures pratiques en matière d'accès vidéo à distance.

Limiter l'exposition au réseau

CSC n° 12 : Gestion de l'infrastructure réseau

Le moyen le plus courant de réduire les risques d'exposition au réseau consiste à isoler physiquement et virtuellement les périphériques réseau et les infrastructures et applications associées. Les logiciels de gestion vidéo, les enregistreurs vidéo réseau (NVR) et d'autres types d'équipements de surveillance sont des exemples d'infrastructure et d'applications de ce type.

Nous vous recommandons d'isoler les périphériques Axis, les infrastructures et les applications connexes sur un réseau local non connecté à 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 ajoutant des mécanismes de sécurité réseau à plusieurs couches. Exemples de mécanismes de ce type : segmentation VLAN, capacités de routage limitées, réseau privé virtuel (VPN) pour l'accès de site à site ou accès WAN, pare-feu 2/3 couche réseau et listes de contrôle d'accès (ACL).

Pour étendre le renforcement de base, nous vous recommandons d'appliquer des techniques d'inspection réseau plus avancées, telles que l'inspection en profondeur des paquets et la détection d'intrusion. Ceci permettra de garantir une protection cohérente et complète des menaces au sein du réseau. Un renforcement du réseau étendu nécessite des logiciels et/ou des appareils matériels dédiés.

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 les analyses, assurez-vous que les périphériques Axis ont été mis à jour vers la dernière version d'AXIS OS disponible, soit sur le LTS, soit sur le suivi 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 *OS Vulnerability Scanner Guide*. Soumettez le rapport et toute autre remarque supplémentaire sous la forme d'un ticket d'assistance à *l'assistance technique d'Axis* sur axis.com.

Infrastructure de clé publique (PKI) fiable

CSC n 3 : Protection des 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 (AC) avec une chaîne de confiance validée permet de supprimer les avertissements de certificat de navigateur lorsque vous vous connectez sur HTTPS. Un certificat signé par une AC garantit également l'authenticité 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.

Contrôle d'accès réseau IEEE 802.1X

CSC n° 6 : Gestion du contrôle d'accès
CSC n° : 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

IEEE 802.1AE MACsec

CSC n 3 : Protection des 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.

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

Identité des périphériques sécurisés IEEE 802.1AR

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

Renforcement étendu

Les périphériques Axis avec Axis Edge Vault prennent en charge la norme réseau IEEE 802.1AR. Cela permet l'intégration automatique et sécurisée des périphériques Axis au sein du réseau à l'aide d'un identifiant de périphérique Axis, certificat unique installé sur le périphérique pendant 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.

Surveillance des équipements de protection individuelle (SNMP)

CSC n° 8 : Gestion des journaux d'audit

Les périphériques Axis prennent en charge les protocoles SNMP suivants.

- **SNMP v1** : pris en charge pour des raisons historiques uniquement, ne pas utiliser.
- **SNMP v2c** : peut être utilisé sur un segment de réseau protégé.
- **SNMP v3** : recommandé à des fins de surveillance.

Les périphériques Axis prennent également en charge la surveillance des caméras MIB-II et AXIS Video MIB. Pour télécharger AXIS Video MIB, consultez la section concernant *AXIS Video MIB* dans AXIS OS Knowledge base.

Pour en savoir plus sur la configuration du protocole SNMP dans AXIS OS, consultez la section concernant le *protocole SNMP (Simple Network Management Protocol)* dans AXIS OS Knowledge base.

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

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

Flux vidéo sécurisé (SRTP/RTSPS)

CSC n 3 : Protection des données

Renforcement étendu

À compter 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 cryptée et sécurisée de bout en bout pour garantir que seuls les clients autorisés reçoivent le flux vidéo du périphérique xis. 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 données

À compter de la version 10.11 d'AXIS OS, les périphériques Axis avec Axis Edge Vault prennent en charge la vidéo signée. Avec la vidéo signée, les périphériques peuvent ajouter une signature à leur flux vidéo pour s'assurer que la vidéo est intacte et pour vérifier son origine en la traçant jusqu'au périphérique Axis qui l'a produite. La vidéo signée permet au système de gestion vidéo (VMS) ou au système de gestion des preuves (EMS) permet également de vérifier l'authenticité de la vidéo fournie par un périphérique 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	Sans objet
≥ 7.10	Sans objet
≥ 10.9	Système > Configuration ordinaire > Image > Vidéo signée

Guide de démarrage rapide

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 à la page 13* ; cependant, il ne couvre pas les sujets présentés dans *Renforcement étendu à la 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

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 *Limiter l'exposition à Internet à la page 25*.

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

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 des instructions, voir *Définir un mot de passe racine pour le périphérique à la page 14* et *Créer des comptes dédiés à la page 15*.

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

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 en savoir plus, consultez *Accès avec accréditation à la page 5* .

Communication sécurisée désactivée
CSC n° 3 : Protection des 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 à la page 9* . Pour des recommandations de configuration, consultez la section concernant consultez la section *Authentification Digest à la page 9* .

Version 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 à la page 13*.

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 à la page 13*. 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.

Guide de démarrage rapide

Objet	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`
	`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`

Guide de démarrage rapide

Objet	Appel API VAPIX
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:DHE-RSA-AES128-GCM-SHA256:DHE-RSA-AES256-GCM-SHA384`

*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`
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`

Objet	Appel API VAPIX
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 » désactive le port 1 et « port=2 » désactive le port 2.*
*** Remplacez « 1 » par le numéro de port réel dans « Eth1.1 ». Exemples : « Eth1.1 » désactive le port 1 et « Eth1.2 » désactive le port 2.*
**** Après 20 échec de tentatives de connexion en 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 (extension)

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 à la page 13*. Utilisez ce *fichier de configuration*, qui se compose des mêmes paramètres de configuration répertoriés dans *Renforcement de base via API VAPIX à la page 29*.

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.

AXIS OS Hardening Guide
Ver. M46.2
Date : Mai 2024
Référence
© Axis Communications AB, 2022 - 2023