MOBOTIX HUB – Guide de durcissement

Inhaltsverzeichnis

1 Droits d'auteur, marques de commerce et clause de non-responsabilité

Marques

MOBOTIX HUB est une marque déposée de MOBOTIX AG.
Microsoft et Windows sont des marques déposées de Microsoft Corporation. App Store est une marque de service d'Apple Inc. Android est une marque commerciale de Google Inc.
Toutes les autres marques commerciales mentionnées dans ce document sont des marques commerciales de leurs propriétaires respectifs.

Démenti

Ce texte n'est destiné qu'à des fins d'information générale, et son préparation a fait l'objet d'un soin particulier. Tout risque découlant de l'utilisation de ces informations incombe au destinataire, et rien dans les présentes ne doit être interprété comme constituant une quelconque garantie.
MOBOTIX AG se réserve le droit d'effectuer des adaptations sans préavis.
Tous les noms de personnes et d'organisations utilisés dans les exemples de ce texte sont fictifs. Toute ressemblance avec une organisation ou une personne réelle, vivante ou morte, est purement fortuite et involontaire.
Ce produit peut utiliser des logiciels tiers pour lesquels des conditions générales spécifiques peuvent s'appliquer. Dans ce cas, vous trouverez plus d'informations dans le fichier *3rd_party_software_terms_and_conditions.txt* situé dans le dossier d'installation de votre système MOBOTIX HUB.

2 Introduction

Ce guide décrit les mesures de sécurité et de sécurité physique ainsi que les meilleures pratiques qui peuvent vous aider à sécuriser votre logiciel de gestion vidéo (VMS) MOBOTIX HUB contre les cyberattaques. Cela inclut les considérations de sécurité pour le matériel et les logiciels des serveurs, des clients et des composants de périphérique réseau d'un système de vidéosurveillance.

Ce guide adopte des contrôles de sécurité et de confidentialité standard et les associe à chacune des recommandations. Cela fait de ce guide une ressource pour la conformité en matière de sécurité sectorielle et gouvernementale, ainsi que pour les exigences de sécurité du réseau.

2.1 Qu'est-ce que le « durcissement » ?

L'élaboration et la mise en œuvre de mesures de sécurité et de meilleures pratiques sont connues sous le nom de « renforcement ». Le durcissement est un processus continu d'identification et de compréhension des risques de sécurité et de prise de mesures appropriées pour les contrer. Le processus est dynamique car les menaces et les systèmes qu'elles ciblent évoluent constamment.

La plupart des informations de ce guide se concentrent sur les paramètres et les techniques informatiques, mais il est important de se rappeler que la sécurité physique est également un élément essentiel du renforcement. Par exemple, utilisez des barrières physiques pour les serveurs et les ordinateurs clients, et assurez-vous que les boîtiers de caméra, les serrures, les alarmes anti-sabotage et les contrôles d'accès sont sécurisés.

Voici les étapes pratiques pour renforcer un VMS :

1. Comprendre les composants à protéger
2. Renforcer les composants du système de surveillance :
    1. Renforcer les serveurs (physiques et virtuels) et les ordinateurs et périphériques clients
    2. Renforcer le réseau
    3. Durcir les caméras
3. Documenter et gérer les paramètres de sécurité de chaque système
4. Former et investir dans les personnes et les compétences, y compris dans votre chaîne d'approvisionnement

2.1.1 Public visé

Tous les membres d'une organisation doivent comprendre au moins les bases de la sécurité des réseaux et des logiciels. Les tentatives de compromettre les infrastructures informatiques critiques sont de plus en plus fréquentes, de sorte que tout le monde doit prendre au sérieux le renforcement et la sécurité.

Ce guide fournit des informations de base et avancées pour les utilisateurs finaux, les intégrateurs de systèmes, les consultants et les fabricants de composants.

- Les descriptions de base donnent un aperçu général de la sécurité
- Les descriptions avancées fournissent des conseils spécifiques à l'informatique pour le renforcement des produits MOBOTIX HUB VMS. Outre les logiciels, il décrit également les considérations de sécurité pour le matériel et les composants de périphérique du système.

2.1.2 Ressources et références

Les organisations suivantes fournissent des ressources et des informations sur les meilleures pratiques en matière de sécurité :

- Organisation internationale de normalisation (ISO),
- États-Unis (US) National Institute of Standards and Technology (NIST)

- Directives de mise en œuvre technique de la sécurité (STIG) de la Defense Information Systems Administration (DISA) des États-Unis
- Centre de sécurité Internet
- Institut SANS
- Cloud Security Alliance (CSA)
- Groupe de travail sur l'ingénierie de l'Internet (IETF)
- Normes britanniques

De plus, les fabricants d'appareils photo fournissent des conseils pour leurs périphériques matériels.

Voir Annexe 1 - Ressources sur la page 102 pour une liste de références et Annexe 2 - Acronymes sur la page 102 pour obtenir la liste des acronymes.

Ce guide s'appuie sur les normes et les spécifications nationales, internationales et sectorielles. En particulier, il s'agit de la publication spéciale 800-53 Revision 4 du National Institute of Standards and Technology du ministère du Commerce des États-Unis, Security and Privacy Controls for Federal Information Systems and Organizations (http://nvlpubs.nist.gov/nistpubs/specialpublications/nist.sp.800-53r4.pdf).

Le document du NIST est écrit pour le gouvernement fédéral américain ; Cependant, il est généralement accepté dans le secteur de la sécurité comme l'ensemble actuel des meilleures pratiques.

Ce guide fait référence à des informations supplémentaires sur les contrôles de sécurité et y fournit des liens vers celles-ci. Les directives peuvent être renvoyées à des exigences spécifiques à l'industrie et à d'autres normes et cadres internationaux de sécurité et de gestion des risques. Par exemple, le cadre de cybersécurité actuel du NIST utilise la norme SP 800-53 Rev4 comme base pour les contrôles et les directives. Un autre exemple est l'annexe H de la PS 800-53 Rev 4, qui contient une référence aux exigences de la norme ISO/IEC 15408, telles que les Critères communs.

2.1.3 Composants matériels et de dispositifs

En plus des logiciels, les composants d'une installation MOBOTIX HUB VMS incluent généralement des périphériques matériels, tels que :

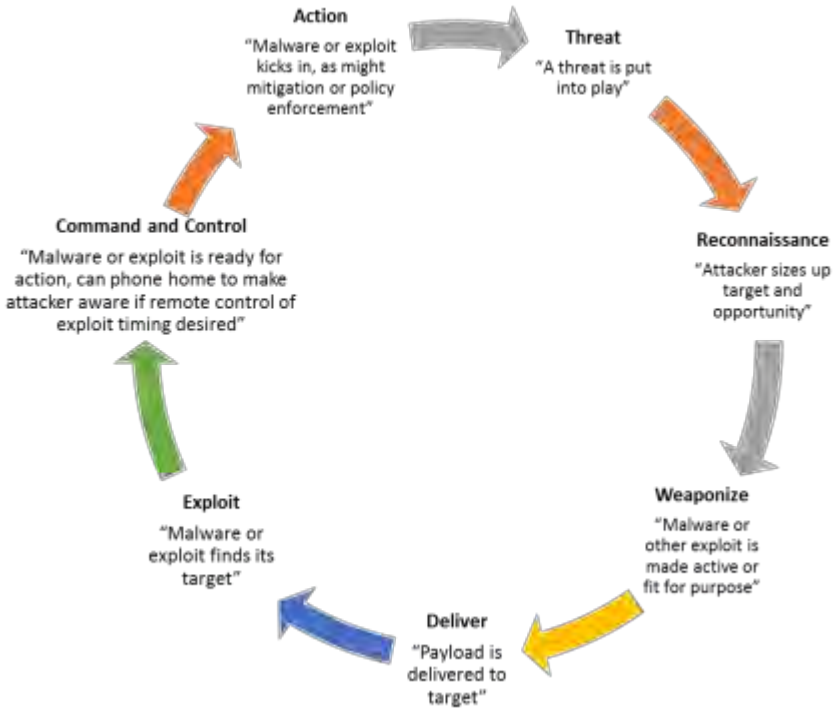
- Caméras
- Encodeurs
- Produits de mise en réseau
- Systèmes de stockage
- Serveurs et ordinateurs clients (machines physiques ou virtuelles)
- Appareils mobiles, tels que les smartphones

Il est important d'inclure des périphériques matériels dans vos efforts pour renforcer votre installation MOBOTIX HUB VMS. Par exemple, les appareils photo ont souvent des mots de passe par défaut. Certains fabricants publient ces mots de passe en ligne afin qu'ils soient faciles à trouver pour les clients. Malheureusement, cela signifie que les mots de passe sont également disponibles pour les attaquants.
Ce document fournit des recommandations pour les périphériques matériels.

2.2 Cybermenaces et cyber-risques

Il existe de nombreuses sources de menaces pour un VMS, notamment des attaques ou des défaillances commerciales, technologiques, de processus et humaines. Les menaces se manifestent tout au long d'un cycle de

vie. Le cycle de vie des menaces, parfois appelé « cyberdestruction » ou « chaîne de cybermenaces », a été développé pour décrire les étapes des cybermenaces avancées.
Chaque étape du cycle de vie d'une menace prend du temps. La durée de chaque étape est propre à la menace, ou à la combinaison de menaces, à ses acteurs et à ses cibles.



Le cycle de vie des menaces est important pour l'évaluation des risques, car il montre où vous pouvez atténuer les menaces. L'objectif est de réduire le nombre de vulnérabilités et d'y remédier le plus tôt possible. Par exemple, décourager un attaquant qui sonde un système à la recherche de vulnérabilités peut éliminer une menace.
Le renforcement met en place des actions qui atténuent les menaces pour chaque phase du cycle de vie des menaces. Par exemple, pendant la phase de reconnaissance, un attaquant recherche des ports ouverts et détermine l'état des services liés au réseau et au VMS. Pour atténuer ce problème, les conseils de renforcement consistent à fermer les ports système inutiles dans les machines virtuelles MOBOTIX HUB et les configurations Windows.
Le processus d'évaluation des risques et des menaces comprend les étapes suivantes :

- Identifier les risques liés à l'information et à la sécurité
- Évaluer et hiérarchiser les risques
- Mettre en œuvre des politiques, des procédures et des solutions techniques pour atténuer ces risques

Le processus global d'évaluation des risques et des menaces, ainsi que la mise en œuvre des contrôles de sécurité, sont appelés cadre de gestion des risques. Ce document fait référence aux contrôles de sécurité et de confidentialité du NIST et à d'autres publications sur les cadres de gestion des risques.

2.2.1 Cadre de gestion des cyberrisques

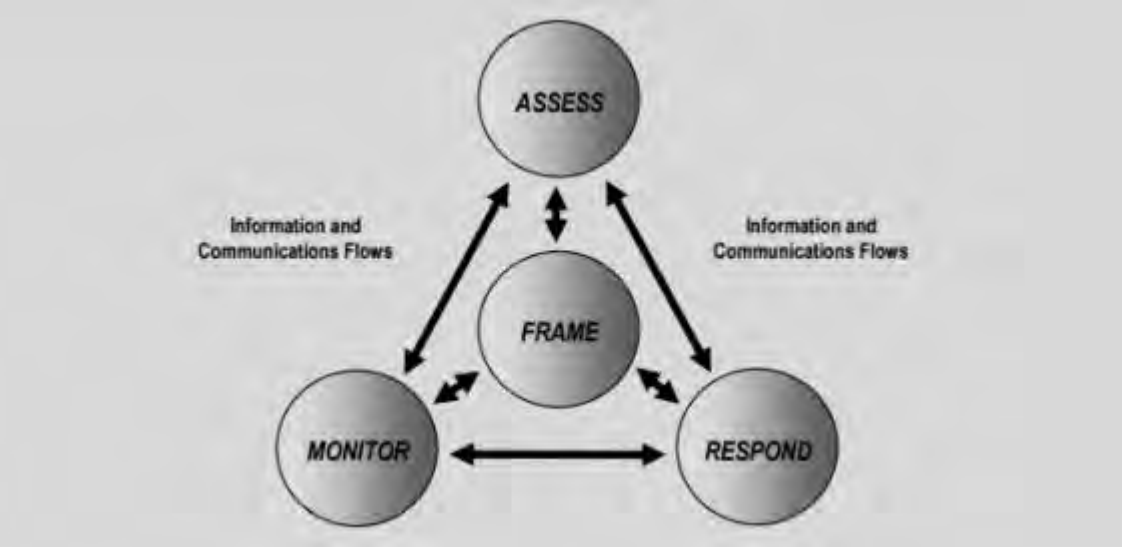
Les contrôles de sécurité et de confidentialité de la SP 800-53 révision 4 (http://nvlpubs.nist.gov/nistpubs/specialpublications/nist.sp.800-53r4.pdf) font partie d'un cadre global de gestion des risques du NIST. Le document NIST SP800-39 (http://csrc.nist.gov/publications/nistpubs/800-39/sp800-39-final.pdf) est un guide pour l'application d'un cadre de gestion des risques. SP800-36 est un document

fondamental pour le cadre de cybersécurité du NIST, qui est décrit dans le cadre de cybersécurité (http://www.nist.gov/cyberframework/).

Les chiffres ci-dessous montrent :

- Un aperçu du processus de gestion des risques. Il s'agit d'une approche globale de haut niveau.
- La gestion des risques au niveau de l'entreprise, en tenant compte des considérations stratégiques et tactiques.
- Le cycle de vie d'un cadre de gestion des risques et les documents NIST qui fournissent des détails pour chacune des étapes du cycle de vie.

Les contrôles de sécurité et de confidentialité représentent des actions et des recommandations spécifiques à mettre en œuvre dans le cadre d'un processus de gestion des risques. Il est important que le processus inclue l'évaluation de l'organisation, les exigences particulières d'un déploiement donné et l'agrégation de ces activités dans un plan de sécurité. La PS 800-18 révision 1 (http://csrc.nist.gov/publications/nistpubs/800-18-Rev1/sp800-18-Rev1-final.pdf) fournit des références pour les plans de sécurité détaillés.



Vue d'ensemble de la gestion des risques (PS 800-39, page 8 (http://csrc.nist.gov/publications/nistpubs/800-39/sp800-39-final.pdf))

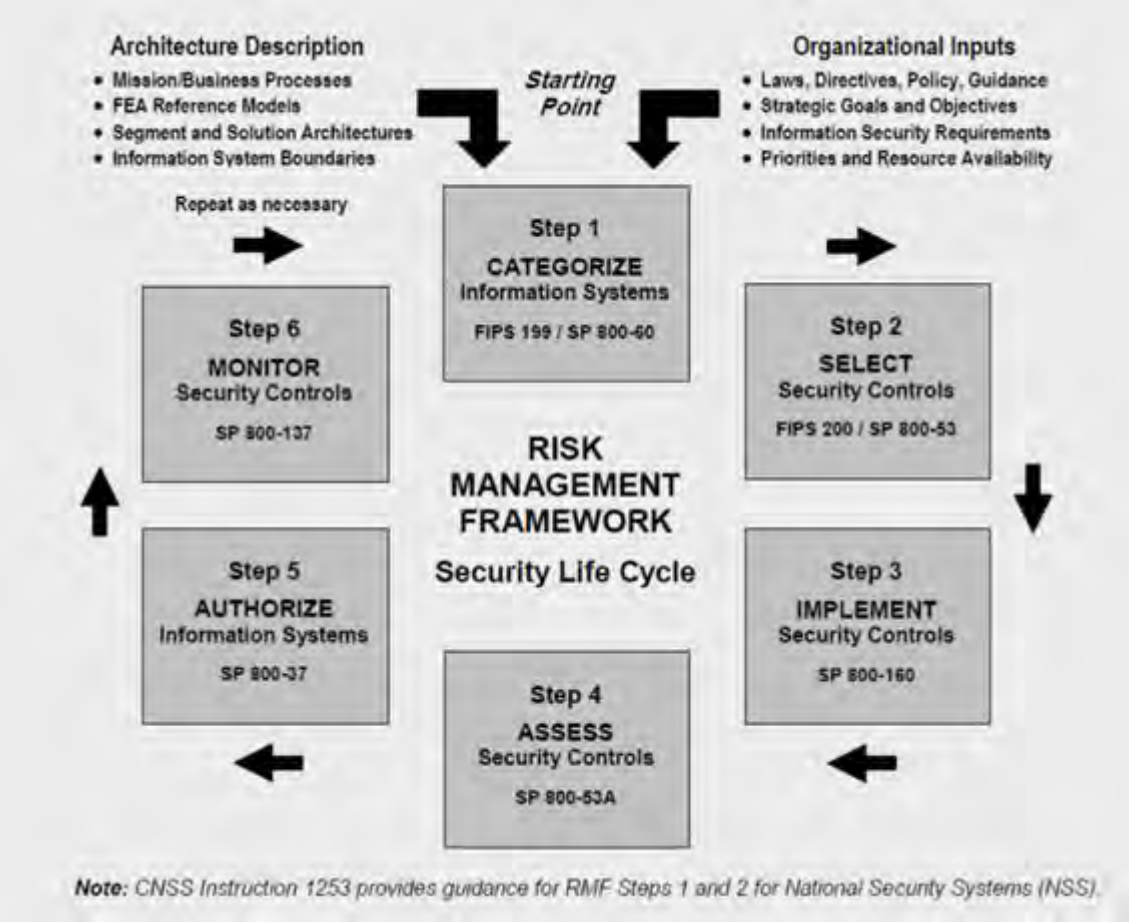
Le processus est interactif, et les réponses et leurs résultats sont itératifs. Les menaces, les risques, les réponses et les résultats de sécurité sont dynamiques et adaptables, tout comme un plan de sécurité.

Ce diagramme montre comment un cadre de gestion des risques prend en compte les systèmes informatiques, les processus opérationnels et l'organisation dans son ensemble afin de trouver un équilibre pour le plan de sécurité.

Équilibre entre la sécurité et les objectifs commerciaux (SP 800-39, page 9 (http://csrc.nist.gov/publications/nistpubs/800-39/sp800-39-final.pdf))

Lors du renforcement d'un système, vous équilibrez l'impact sur la productivité et la convivialité de l'entreprise pour des raisons de sécurité, et vice versa, dans le contexte des services que vous fournissez. Les conseils en matière de sécurité ne sont pas isolés des autres activités commerciales et informatiques.

Par exemple, lorsqu'un utilisateur saisit son mot de passe de manière incorrecte lors de trois tentatives consécutives, le mot de passe est bloqué et il ne peut pas accéder au système. Le système est protégé contre les attaques par force brute, mais l'utilisateur malchanceux ne peut pas utiliser l'appareil pour faire son travail. Une politique de mot de passe forte qui exige des mots de passe de 30 caractères et un changement de mot de passe tous les 30 jours est une bonne pratique, mais elle est également difficile à utiliser.



Exemple de cadre de gestion des risques (PS 800-53 Rev 5 page 8 (https://csrc.nist.gov/publications/detail/sp/800-53/rev-5/final))

Pour documenter son cadre de gestion des risques, le NIST a produit plusieurs publications spéciales. Il comprend les composants suivants :

1. Catégorisation (identification du niveau de risque)
2. Sélection des contrôles de sécurité et de confidentialité
3. Implémentation
4. Évaluation de l'efficacité des contrôles de sécurité
5. Création d'un profil de sécurité système amélioré et de ce qu'on appelle une autorisation d'exploitation (ATO)
6. Suivi et évaluation par itérations

Le cadre de gestion des risques permet d'établir un plan de sécurité et des directives dans un contexte de sécurité.

2.3 Composants du système de durcissement

Pour renforcer les composants du système, vous devez modifier les configurations afin de réduire le risque d'une attaque réussie. Les attaquants cherchent un moyen d'entrer et recherchent des vulnérabilités dans les parties exposées du système. Les systèmes de surveillance peuvent impliquer des centaines, voire des milliers de composants. L'échec de la sécurisation d'un composant peut compromettre le système.

La nécessité de conserver les informations de configuration est parfois négligée. MOBOTIX HUB VMS fournit des fonctionnalités pour la gestion des configurations, mais les organisations doivent avoir une politique et un processus en place, et s'engager à faire le travail.

Le renforcement nécessite que vous gardiez vos connaissances en matière de sécurité à jour :

- Soyez conscient des problèmes qui affectent les logiciels et le matériel, y compris les systèmes d'exploitation, les appareils mobiles, les appareils photo, les périphériques de stockage et les périphériques réseau. Établissez un point de contact pour tous les composants du système. Idéalement, utilisez des procédures de signalement pour suivre les bogues et les vulnérabilités de tous les composants.
- Tenez-vous au courant des vulnérabilités et expositions courantes (CVE) (décrites dans la section Vulnérabilités et expositions courantes (https://cve.mitre.org/)) pour tous les composants du système. Il peut s'agir de systèmes d'exploitation, d'appareils dotés de mots de passe de maintenance codés en dur, etc. Corrigez les vulnérabilités de chaque composant et alertez les fabricants en cas de vulnérabilité.
- Tenir à jour la configuration et la documentation du système. Utilisez des procédures de contrôle des modifications pour le travail que vous effectuez et suivez les meilleures pratiques pour la gestion de la configuration, comme décrit dans la SP 800-128 (https://csrc.nist.gov/publications/detail/sp/800-128/final).

Les sections suivantes fournissent des recommandations de base et avancées en matière de renforcement et de sécurité pour chaque composant du système. Les sections contiennent également des exemples de la façon dont ceux-ci se rapportent à des contrôles de sécurité spécifiques décrits dans la publication spéciale NIST 800-53 révision 4, intitulée *Contrôles de sécurité et de confidentialité pour les systèmes d'information et les organisations fédéraux*.
En plus du document du NIST, les sources suivantes sont référencées :

- Centre de sécurité Internet
- SP 800-53
- Norme ISO 27001
- ISO/IEC 15408 (également connue sous le nom de Critères communs, ISO/IEC 15408-1:2022 (https://www.iso.org/standard/72891.html)).

Annexe 1 - Ressources sur la page 102 dans ce document fournit des recommandations des fabricants d'appareils photo. Il s'agit d'un effort relativement nouveau de la part des fabricants, de sorte que les ressources disponibles sont limitées. Pour la plupart, les recommandations peuvent être généralisées à tous les fabricants d'appareils photo.

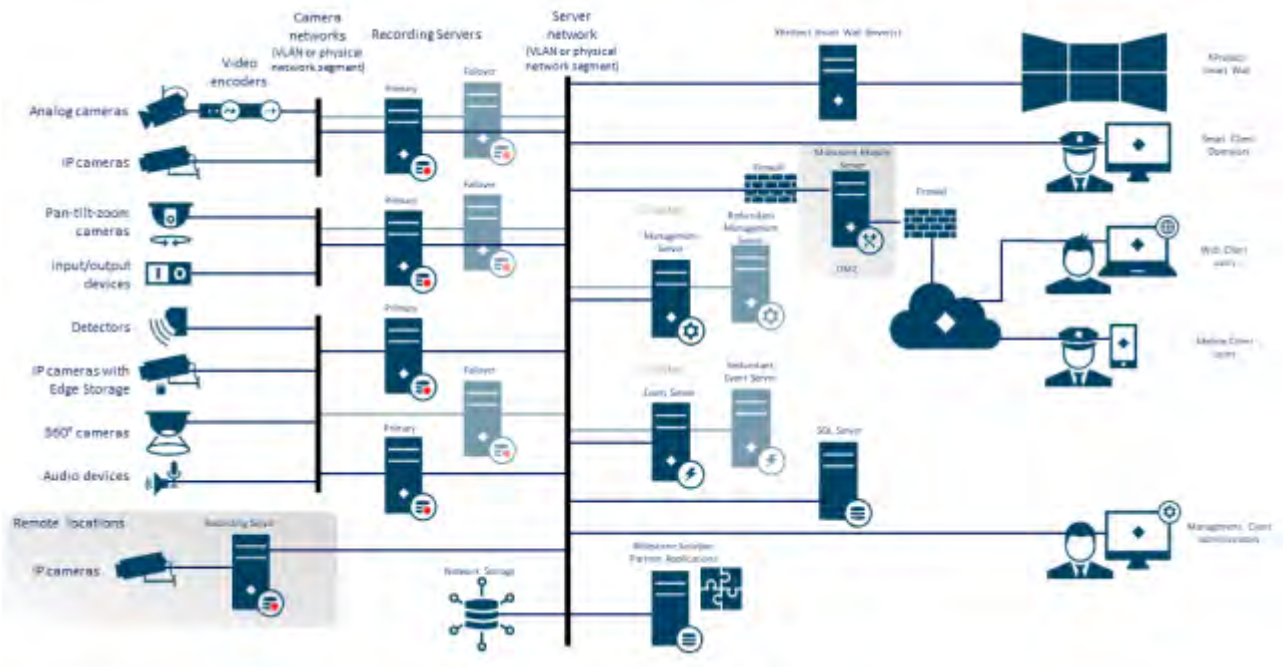
3 Configuration générale

3.1 Aperçu

Pour vous aider à sécuriser votre système de surveillance, MOBOTIX recommande ce qui suit :

- Limitez l'accès aux serveurs. Gardez les serveurs dans des pièces verrouillées et rendez difficile l'accès des intrus aux câbles réseau et d'alimentation.
  (PE2 et PE3 dans les annexes D et F de NIST SP 800-53 Rev5 (https://csrc.nist.gov/publications/detail/sp/800-53/rev-5/final) (PE Physical and Environment Protection).)
- Concevez une infrastructure réseau qui utilise autant que possible la segmentation du réseau physique ou du VLAN.
  (SC3 dans les annexes D et F du NIST SP 800-53 Rev5 (https://csrc.nist.gov/publications/detail/sp/800-53 /rev-5/final) (SC System and Communication Protection).)
  - Séparez le réseau de caméras du réseau de serveurs en ayant deux interfaces réseau dans chaque serveur d'enregistrement : une pour le réseau de caméras et une pour le réseau de serveurs.
  - Placez le serveur mobile dans une « zone démilitarisée » (DMZ) avec une interface réseau pour l'accès public et une pour la communication privée avec d'autres serveurs.
    (SC7 dans les annexes D et N IST SP 800-53 Rev5 (https://csrc.nist.gov/publications/detail/sp/800-53 /rev-5/final).)
  - De nombreuses précautions peuvent être prises en ce qui concerne la mise en place générale. En plus des pare-feu, il s'agit notamment de techniques permettant de segmenter le réseau et de contrôler l'accès aux serveurs, aux clients et aux applications.
    (AC3, AC4, AC6, CA3, CM3, CM6, CM7, IR4, SA9, SC7, SC28, SI3, SI 8 dans les annexes D et F dans NIST SP 800-53 Rev5 (https://csrc.nist.gov/publications/detail/sp/800-53/rev-5/final) (Contrôles d'accès AC), (Gestion de la configuration CM) (Réponse aux incidents IR) (Acquisition de systèmes et de services SA) (Systèmes SI et intégrité de l'information).)
- Configurez le VMS avec des rôles qui contrôlent l'accès au système et désignez les tâches et les responsabilités.
  (AC2, AC3, AC6, AC16, AC25, AU6, AU9, CM5, CM11, IA5, PL8, PS5, PS7, SC2, SI7, dans les annexes D et F du NIST SP 800-53 Rev5 (https://csrc.nist.gov/publications/detail/sp/800-53/rev-5/final) (AU Audit and Accountability) (IA Identification and Authentication) (PL Planning).)

La figure montre un exemple de configuration générale.



3.1.1 Protection de la vie privée dès la conception

Les produits MOBOTIX sont conçus pour assurer une communication sécurisée de bout en bout. Les produits MOBOTIX sont conçus pour protéger la vie privée et sécuriser les données. La protection des données est toujours importante, mais surtout si vous avez l'intention de vous conformer au règlement général sur la protection des données (RGPD) dans l'UE.

Selon le RGPD, le responsable du traitement des données personnelles, lorsqu'il traite de telles données, a l'obligation de mettre en œuvre des mesures techniques ou organisationnelles conçues pour mettre en œuvre les principes de protection des données énoncés dans le RGPD. Le RGPD fait référence à la protection de la vie privée dès la conception.

Dans le contexte d'une caméra de surveillance, un exemple pertinent de protection de la vie privée dès la conception serait une fonctionnalité qui permet numériquement à l'utilisateur de restreindre la capture d'images à un certain périmètre, empêchant ainsi la caméra de capturer des images en dehors de ce périmètre qui seraient autrement capturées.

Dans MOBOTIX HUB, le masquage de confidentialité prend en charge deux formes : les masques permanents qui ne peuvent pas être retirés et les masques relevables qui (avec les autorisations appropriées) peuvent être soulevés pour révéler l'image derrière le masque.

Le responsable du traitement a également l'obligation de mettre en œuvre des mesures techniques ou organisationnelles qui, par défaut, garantissent le traitement le moins intrusif possible des données personnelles en question. Le RGPD appelle cela la confidentialité par défaut. Dans le contexte d'une caméra, un exemple pertinent de confidentialité par défaut pourrait être l'utilisation du masquage de confidentialité pour garder privée une zone sensible dans le champ de vision de la caméra.

Que devez-vous faire pour garantir la confidentialité dès la conception ?

- Tenez compte de la résolution des différents points de la scène de la caméra et documentez ces paramètres

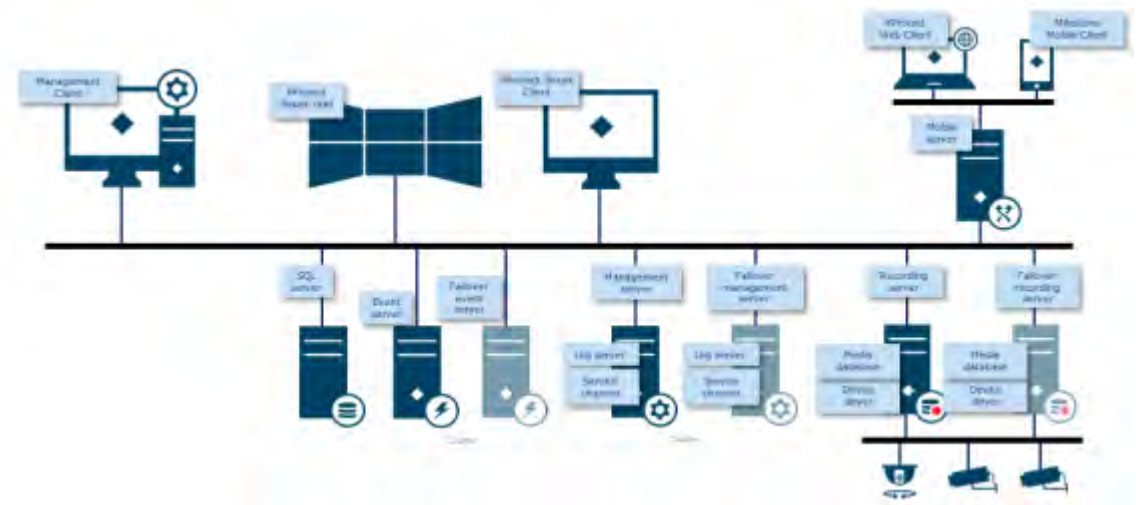
objectifs différents nécessitent des qualités d'image différentes. Lorsqu'il n'est pas nécessaire de l'identifier, la résolution de la caméra et d'autres facteurs modifiables doivent être choisis pour s'assurer qu'aucune image faciale reconnaissable n'est capturée.

- Cryptez vos enregistrements
  MOBOTIX vous recommande de sécuriser vos enregistrements en activant au moins le cryptage léger sur le stockage et les archives de vos serveurs d'enregistrement. MOBOTIX utilise l'algorithme AES-256 pour le cryptage. Lorsque vous sélectionnez le chiffrement léger, seule une partie de l'enregistrement est chiffrée. Lorsque vous sélectionnez Chiffrement fort, l'intégralité de l'enregistrement est chiffrée.
- Sécurisez le réseau
  MOBOTIX vous recommande de sélectionner des caméras qui prennent en charge HTTPS. Il est recommandé de définir les caméras sur des VLAN distincts et d'utiliser HTTPS pour que votre caméra enregistre la communication du serveur.
  Il est recommandé que les clients intelligents MOBOTIX HUB et les murs intelligents MOBOTIX HUB se trouvent sur le même VLAN que les serveurs.
  Utilisez un réseau crypté VPN ou similaire si vous utilisez Smart Client ou Smart Wall à distance.
- Activer et documenter la durée de conservation prévue
  Conformément à l'article 4, paragraphe 1, point e), du RGPD, les enregistrements ne doivent pas être conservés plus longtemps que nécessaire aux fins spécifiques pour lesquelles ils ont été réalisés. MOBOTIX vous recommande de définir la durée de conservation conformément aux lois et exigences régionales et, dans tous les cas, de fixer la durée de conservation à un maximum de 30 jours.
- Exportations sécurisées
  MOBOTIX vous recommande de n'autoriser l'accès à la fonctionnalité d'exportation qu'à un ensemble sélectionné d'utilisateurs qui ont besoin de cette autorisation.
  MOBOTIX recommande également de modifier le profil Smart Client pour n'autoriser l'exportation qu'au format MOBOTIX HUB avec le cryptage activé. Les exportations AVI et JPEG ne devraient pas être autorisées, car elles ne peuvent pas être sécurisées. Ainsi, l'exportation de tout matériel de preuve est protégée par un mot de passe, cryptée et signée numériquement, ce qui garantit que le matériel médico-légal est authentique, non altéré et consulté uniquement par le destinataire autorisé.
- Activer le masquage de l'intimité – permanent ou relevable
  Utilisez le masquage de confidentialité pour éliminer la surveillance des zones non pertinentes pour votre cible.
  MOBOTIX vous recommande de régler un masque flou relevable pour les zones sensibles et les endroits où l'identification d'une personne n'est pas autorisée. Créez ensuite un second rôle qui peut autoriser la levée du masque.
- Restreindre les droits d'accès avec des rôles
  Appliquer le principe du moindre privilège (PoLP).
  MOBOTIX vous recommande de n'autoriser l'accès aux fonctionnalités qu'à un ensemble sélectionné d'utilisateurs qui ont besoin de cette autorisation. Par défaut, seul l'administrateur système peut accéder au système et effectuer des tâches. Tous les nouveaux rôles et utilisateurs créés n'ont accès à aucune fonction tant qu'ils ne sont pas délibérément configurés par un administrateur.
  Configurez des autorisations pour toutes les fonctionnalités, y compris l'affichage de vidéos et d'enregistrements en direct, l'écoute d'audio, l'accès aux métadonnées, le contrôle des caméras PTZ, l'accès et la configuration de Smart Wall, le retrait des masques de confidentialité, l'utilisation des exportations, l'enregistrement d'instantanés, etc.

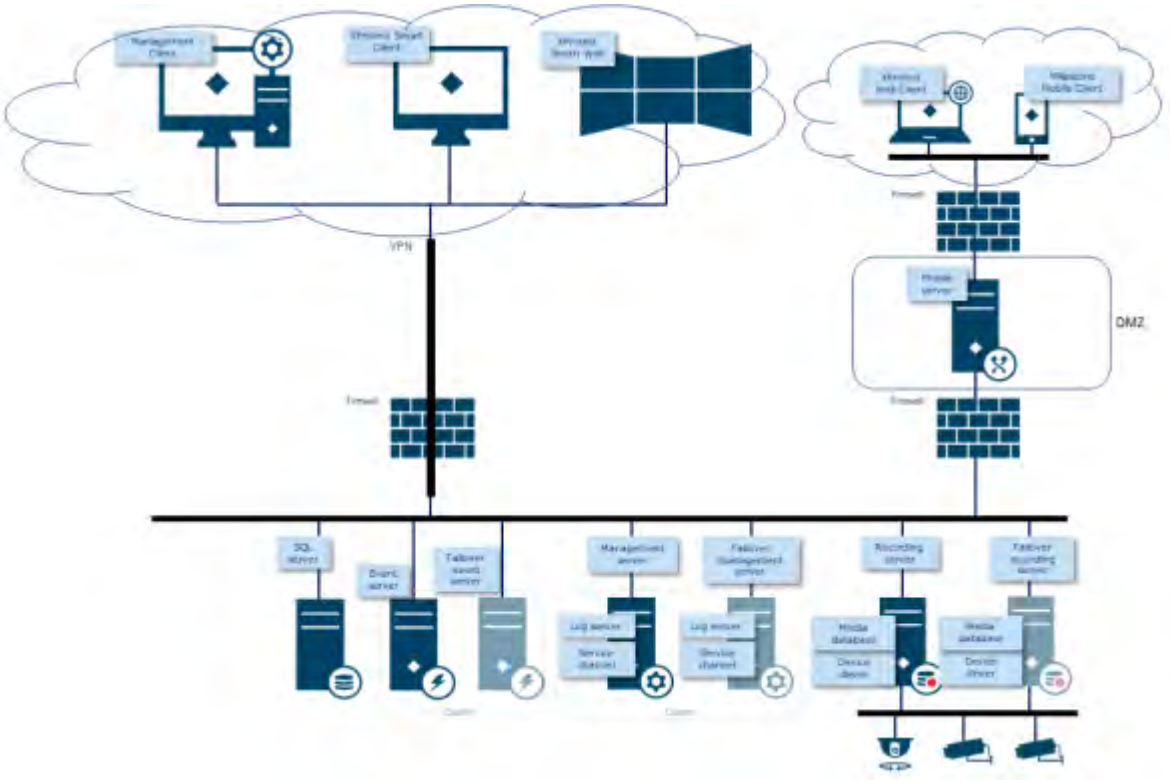
N'accordez l'accès qu'aux caméras auxquelles l'opérateur spécifique doit accéder et limitez l'accès à la vidéo, à l'audio et aux métadonnées enregistrés pour les opérateurs, soit complètement, soit n'accordez l'accès qu'à la vidéo, à l'audio ou aux métadonnées enregistrées au cours des dernières heures ou moins. Évaluer et examiner régulièrement les rôles et les responsabilités des exploitants, des enquêteurs, des administrateurs du système et des autres personnes ayant accès au système. Le principe du moindre privilège s'applique-t-il toujours ?

- Activer et utiliser la vérification en deux étapes
  MOBOTIX vous recommande de spécifier une étape de connexion supplémentaire pour les utilisateurs de MOBOTIX HUB Mobile ou de MOBOTIX HUB Web Client en activant la vérification en deux étapes.
- Restreindre les autorisations d'administrateur
  MOBOTIX vous recommande de limiter le nombre d'utilisateurs disposant d'un rôle d'administrateur. Si vous devez créer plusieurs rôles d'administrateur, vous pouvez restreindre leur accès en créant des rôles d'administrateur qui ne peuvent gérer que certaines parties du système, telles que certains périphériques ou fonctions.
  MOBOTIX recommande également que l'administrateur VMS ne dispose pas de tous les droits d'administrateur sur le stockage contenant la vidéo enregistrée, et que l'administrateur du stockage n'ait pas accès au VMS ou à l'administration de sauvegarde.

Pour des raisons de sécurité, segmentez le réseau de sorte qu'il y ait un réseau client/de gestion et des réseaux de caméras derrière les serveurs d'enregistrement :



Pour plus de sécurité, placez le serveur mobile dans une « zone démilitarisée » (DMZ) avec une interface réseau pour l'accès public et une pour la communication privée avec d'autres serveurs, et utilisez des réseaux cryptés VPN pour les connexions externes ou pour augmenter la sécurité des réseaux internes moins sécurisés :


VPN
DMZ

4 Serveurs, postes de travail, clients et applications

Cette section fournit des conseils de renforcement basés sur Microsoft Windows et les services utilisés par MOBOTIX HUB VMS. Cela comprend :

- Le produit MOBOTIX HUB VMS, par exemple MOBOTIX HUB® Corporate ou MOBOTIX HUB® Enterprise fonctionnant sur des serveurs Windows
- Le pack de périphériques installé sur les serveurs d'enregistrement
- Le matériel serveur ou les plates-formes virtuelles, ainsi que les systèmes d'exploitation et les services
- Les ordinateurs clients pour MOBOTIX HUB® Smart Client et MOBOTIX HUB® Web Client
- Appareils mobiles, leurs systèmes d'exploitation et leurs applications

4.1 Étapes de base

4.1.1 Etablir des objectifs de surveillance et de sécurité

Avant de mettre en œuvre le VMS, MOBOTIX vous recommande d'établir des objectifs de surveillance. Définissez les objectifs et les attentes liés à la capture et à l'utilisation des données vidéo et des métadonnées associées. Tous les intervenants doivent comprendre les objectifs de la surveillance.

Les spécificités des objectifs de surveillance peuvent être trouvées dans d'autres documents, par exemple BS EN 62676-1-1 : Systèmes de *vidéosurveillance pour une utilisation dans des applications de sécurité. Configuration requise. Généralités.*

Lorsque des objectifs de surveillance sont en place, vous pouvez les établir. Les objectifs de sécurité appuient les objectifs de surveillance en abordant les éléments à protéger dans le SSN. Une compréhension commune des objectifs de sécurité facilite la sécurisation du VMS et le maintien de l'intégrité des données.
Une fois les objectifs de surveillance et de sécurité en place, vous pouvez aborder plus facilement les aspects opérationnels de la sécurisation du VMS, tels que :

- Empêcher la compromission des données
- Réagir aux menaces et aux incidents lorsqu'ils se produisent, y compris les rôles et les responsabilités.

Pour en savoir plus

Les contrôles suivants fournissent des indications supplémentaires :

- Plan de sécurité du système NIST SP 800-53 PL-2
- Processus d'acquisition du NIST SP 800-53 SA-4

4.1.2 Établir une politique de sécurité officielle et un plan d'intervention

Conformément à la norme NIST SP 800-100 Information Security Handbook : A Guide for Managers (https://csrc.nist.gov/publications/detail/sp/800-100/final), MOBOTIX vous recommande d'établir une politique de sécurité formelle et un plan d'intervention qui décrivent comment votre organisation aborde les problèmes de sécurité, en termes de procédures pratiques et de directives. Par exemple, une politique de sécurité peut inclure :

- Une politique de mot de passe définie par le service informatique interne
- Contrôle d'accès avec badges d'identification
- Restrictions pour les smartphones de se connecter au réseau

Adoptez les politiques et les plans informatiques existants s'ils respectent les meilleures pratiques de sécurité.

Pour en savoir plus

Les contrôles suivants fournissent des indications supplémentaires :

- NIST SP 800-53 IR-1 Politique et procédures d'intervention en cas d'incident
- Plan de programme de sécurité de l'information NIST SP 800-53 PM-1

4.1.3 Utiliser des utilisateurs Windows avec Active Directory

Il existe deux types d'utilisateurs dans MOBOTIX HUB VMS :

- Utilisateur de base : un compte d'utilisateur VMS dédié authentifié par une combinaison de nom d'utilisateur et de mot de passe à l'aide d'une politique de mot de passe. Les utilisateurs de base se connectent au VMS à l'aide d'un protocole SSL (Secure Socket Layer) avec la session de protocole de sécurité TLS (https://datatracker.ietf.org/wg/tls/charter/ Transport Layer) actuelle pour la connexion, le cryptage du contenu du trafic, le nom d'utilisateur et le mot de passe.
- Utilisateur Windows : le compte utilisateur est spécifique à une machine ou à un domaine, et il est authentifié sur la base de la connexion Windows. Les utilisateurs Windows qui se connectent au VMS peuvent utiliser Microsoft Windows Challenge/Response (NTML) pour la connexion, Kerberos (voir

l'authentification Kerberos (expliquée) à la page 39) ou d'autres options SSP de Microsoft (https://msdn.microsoft.com/en-us /library/windows/desktop/aa380502(v=vs.85).aspx).

Dans la mesure du possible, MOBOTIX vous recommande d'utiliser des utilisateurs Windows en combinaison avec Active Directory (AD) pour autoriser l'accès au VMS. Cela vous permet d'appliquer :

- Une politique de mot de passe qui oblige les utilisateurs à changer régulièrement leur mot de passe
- Protection contre la force brute, de sorte que le compte Windows AD soit bloqué après un certain nombre de tentatives d'authentification infructueuses, toujours conformément à la politique de mot de passe de l'organisation
- Authentification multifacteur dans le VMS, en particulier pour les administrateurs
- Autorisations basées sur les rôles, afin que vous puissiez appliquer des contrôles d'accès à l'ensemble de votre domaine

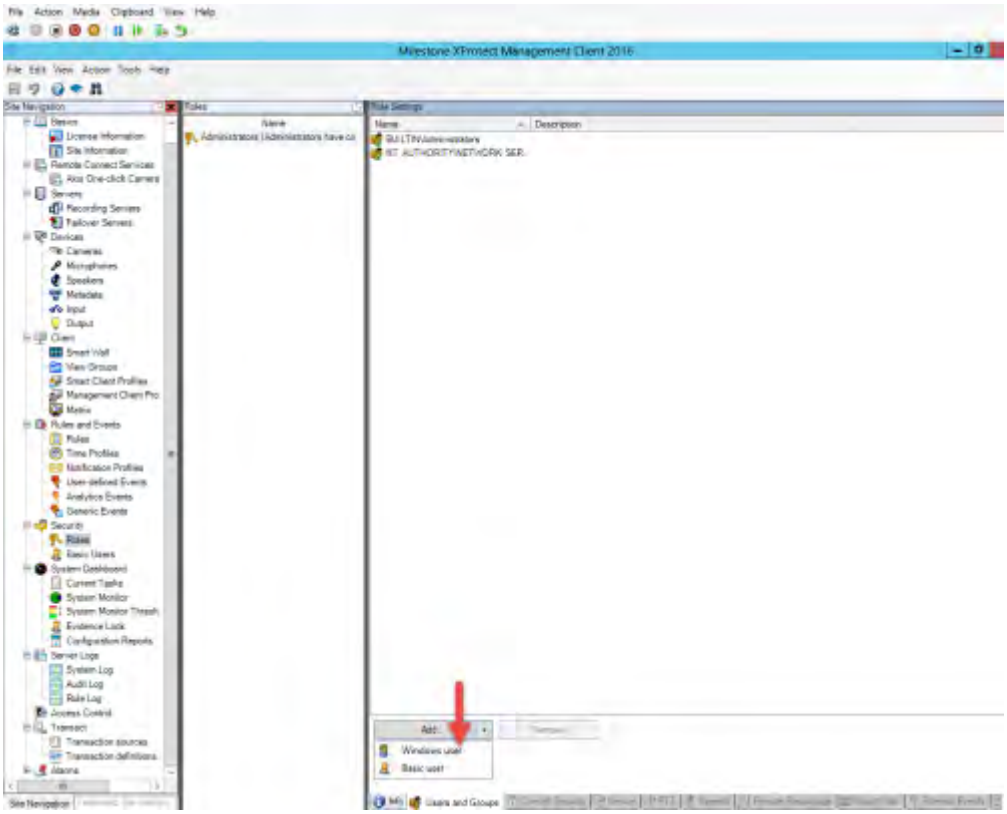
Si votre organisation n'utilise pas AD, vous pouvez ajouter des utilisateurs Windows à des groupes de travail sur le serveur d'administration. Les groupes de travail vous offrent certains des mêmes avantages que les utilisateurs Windows avec AD. Vous pouvez appliquer une politique de mot de passe, qui permet de vous protéger contre les attaques par force brute, mais MOBOTIX vous recommande d'utiliser un domaine Windows, car cela vous donne un contrôle centralisé sur les comptes d'utilisateurs.

Les utilisateurs Windows ont l'avantage d'être authentifiés via l'annuaire en tant que source unique faisant autorité et service d'entreprise pour le réseau et non ad hoc pour leur machine locale. Cela vous permet d'utiliser des contrôles d'accès basés sur les rôles pour attribuer des autorisations aux utilisateurs et aux groupes de manière cohérente sur le domaine et les ordinateurs du réseau.

Si vous utilisez des utilisateurs Windows locaux, l'utilisateur doit créer un nom d'utilisateur et un mot de passe locaux sur chaque ordinateur, ce qui est problématique du point de vue de la sécurité et de la convivialité.

Pour ajouter des utilisateurs ou des groupes Windows à des rôles dans Management Client, procédez comme suit :

1. Ouvrez Management Client.
2. Développez le nœud Sécurité.



3. Sélectionnez le rôle auquel vous souhaitez ajouter les utilisateurs Windows.
4. Sous l'onglet Utilisateurs et groupes, cliquez sur Ajouter, puis sélectionnez Utilisateur Windows. Une fenêtre contextuelle apparaît.
5. Si le nom de domaine n'apparaît pas dans le champ À partir de cet emplacement, cliquez sur Emplacements.
6. Spécifiez l'utilisateur Windows, puis cliquez sur OK.

Pour vérifier que l'utilisateur Windows est un utilisateur AD, le nom de domaine doit apparaître sous la forme d'un préfixe, par exemple « Domaine\John ».

Pour en savoir plus

Les contrôles suivants fournissent des indications supplémentaires :

- NIST SP 800-53 CM-6 Paramètres de configuration
- Documentation du système d'information NIST SP 800-53 SA-5
- Fiabilité NIST SP 800-53 SA-13

4.1.4 Communication sécurisée (expliqué)

Le protocole HTTPS (Hypertext Transfer Protocol Secure) est une extension du protocole HTTP (Hypertext Transfer Protocol) pour la communication sécurisée sur un réseau informatique. En HTTPS, le protocole de communication est chiffré à l'aide de TLS (Transport Layer Security) ou de son prédécesseur, SSL (Secure Sockets Layer).
Dans les machines virtuelles mobotix hub, la communication sécurisée est obtenue à l'aide de SSL/TLS avec chiffrement asymétrique (RSA).
SSL/TLS utilise une paire de clés, l'une privée et l'autre publique, pour authentifier, sécuriser et gérer les connexions sécurisées.

Une autorité de certification (CA) peut émettre des certificats pour des services Web sur des serveurs à l'aide d'un certificat CA. Ce certificat contient deux clés, une clé privée et une clé publique. La clé publique est installée sur les clients d'un service web (service clients) par l'installation d'un certificat public. La clé privée est utilisée pour signer les certificats de serveur qui doivent être installés sur le serveur. Chaque fois qu'un client de service appelle le service Web, celui-ci envoie le certificat du serveur, y compris la clé publique, au client. Le client de service peut valider le certificat du serveur à l'aide du certificat d'autorité de certification publique déjà installé. Le client et le serveur peuvent désormais utiliser le certificat du serveur public et privé pour échanger une clé secrète et établir ainsi une connexion SSL/TLS sécurisée.

Pour plus d'informations sur TLS : https://en.wikipedia.org/wiki/Transport_Layer_Security

Les certificats ont une date d'expiration. MOBOTIX HUB VMS ne vous avertit pas lorsqu'un certificat est sur le point d'expirer. Si un certificat expire :- Les clients ne feront plus confiance au serveur d'enregistrement avec le certificat expiré et ne pourront donc pas communiquer avec lui
- Les serveurs d'enregistrement ne feront plus confiance au serveur de gestion avec le certificat expiré et ne pourront donc pas communiquer avec lui
- Les appareils mobiles ne feront plus confiance au serveur mobile avec le certificat expiré et ne pourront donc pas communiquer avec lui
Pour renouveler les certificats, suivez les étapes de ce guide comme vous l'avez fait lors de la création des certificats.

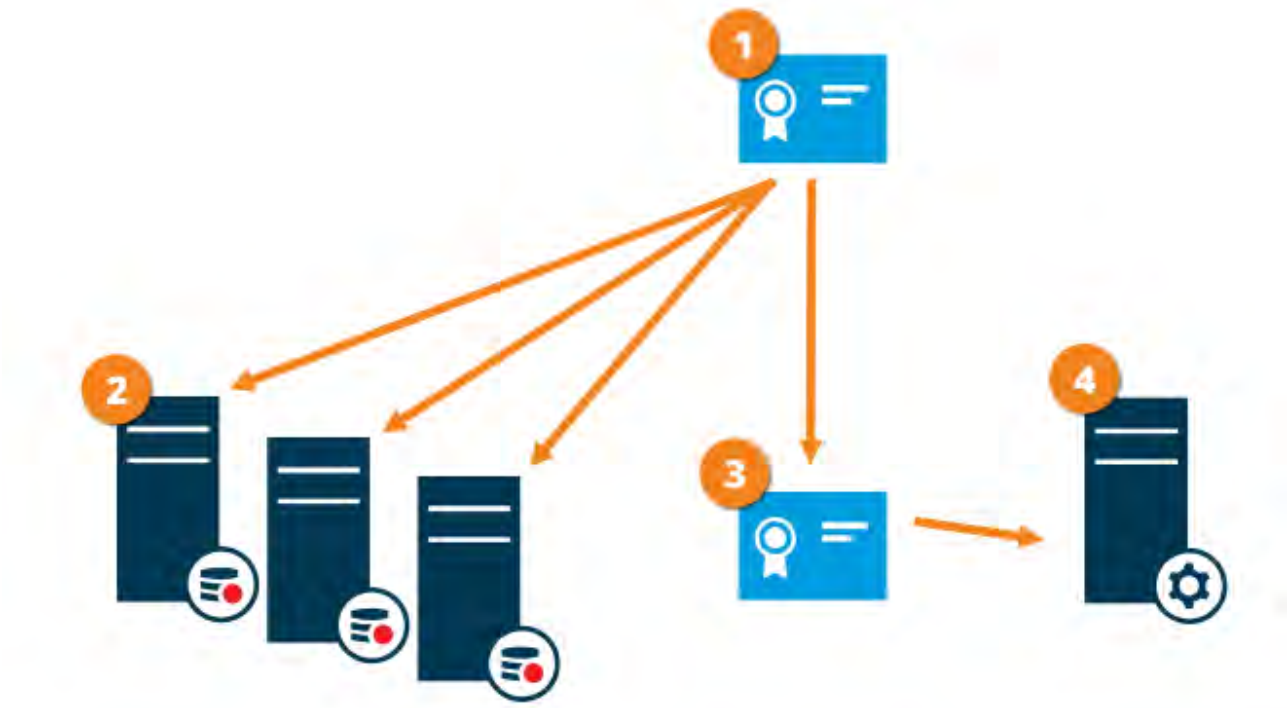
Pour plus d'informations, consultez le guide des certificats sur la sécurisation de vos installations VMS MOBOTIX Hub .

4.1.5 Chiffrement du serveur de gestion (expliqué)

Vous pouvez chiffrer la connexion bidirectionnelle entre le serveur de gestion et le serveur d'enregistrement. Lorsque vous activez le chiffrement sur le serveur d'administration, il s'applique aux connexions de tous les serveurs d'enregistrement qui se connectent au serveur d'administration. Si vous activez le chiffrement sur le serveur de gestion, vous devez également l'activer sur tous les serveurs d'enregistrement. Avant d'activer le chiffrement, vous devez installer des certificats de sécurité sur le serveur de gestion et sur tous les serveurs d'enregistrement.

Distribution de certificats pour les serveurs de gestion

Le graphique illustre le concept de base de la signature, de l'approbation et de la distribution des certificats dans les machines virtuelles MOBOTIX HUB pour sécuriser la communication avec le serveur de gestion.



❶ Un certificat d'autorité de certification agit en tant que tiers de confiance, approuvé à la fois par le sujet/propriétaire (serveur de gestion) et par la partie qui vérifie le certificat (serveurs d'enregistrement)
❷ Le certificat de l'autorité de certification doit être approuvé sur tous les serveurs d'enregistrement. De cette façon, les serveurs d'enregistrement peuvent vérifier la validité des certificats émis par l'autorité de certification
❸ Le certificat CA est utilisé pour établir une connexion sécurisée entre le serveur de gestion et les serveurs d'enregistrement
❹ Le certificat de l'autorité de certification doit être installé sur l'ordinateur sur lequel le serveur de gestion s'exécute

Conditions requises pour le certificat de serveur de gestion privé :

- Attribué au serveur de gestion afin que le nom d'hôte du serveur de gestion soit inclus dans le certificat, soit en tant qu'objet (propriétaire), soit dans la liste des noms DNS auxquels le certificat est émis.
- Approuvé sur le serveur de gestion lui-même, en approuvant le certificat de l'autorité de certification utilisé pour émettre le certificat du serveur de gestion
- Approuvé sur tous les serveurs d'enregistrement connectés au serveur de gestion, en approuvant le certificat de l'autorité de certification utilisé pour émettre le certificat du serveur de gestion

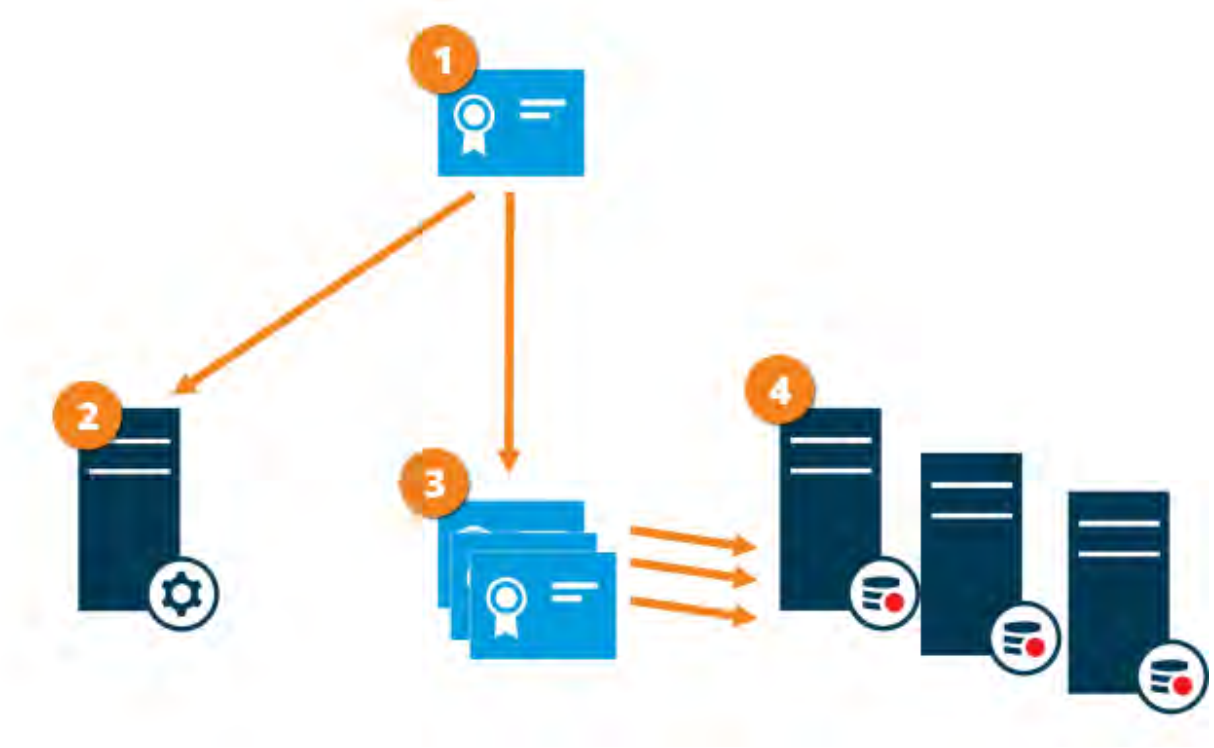
4.1.6 Chiffrement du serveur de gestion au serveur d'enregistrement (expliqué)

Vous pouvez chiffrer la connexion bidirectionnelle entre le serveur de gestion et le serveur d'enregistrement. Lorsque vous activez le chiffrement sur le serveur d'administration, il s'applique aux connexions de tous les serveurs d'enregistrement qui se connectent au serveur d'administration. Le chiffrement de cette communication

doit suivre le paramètre de chiffrement sur le serveur de gestion. Par conséquent, si le chiffrement du serveur de gestion est activé, il doit également être activé sur les serveurs d'enregistrement, et vice-versa. Avant d'activer le chiffrement, vous devez installer des certificats de sécurité sur le serveur d'administration et sur tous les serveurs d'enregistrement, y compris les serveurs d'enregistrement de basculement.

Distribution des certificats

Le graphique illustre le concept de base de la signature, de l'approbation et de la distribution des certificats dans les machines virtuelles MOBOTIX HUB pour sécuriser la communication à partir du serveur de gestion.



❶ Un certificat d'autorité de certification agit en tant que tiers de confiance, approuvé à la fois par le sujet/propriétaire (serveur d'enregistrement) et par la partie qui vérifie le certificat (serveur de gestion)
❷ Le certificat de l'autorité de certification doit être approuvé sur le serveur de gestion. De cette façon, le serveur de gestion peut vérifier la validité des certificats émis par l'autorité de certification
❸ Le certificat CA est utilisé pour établir une connexion sécurisée entre les serveurs d'enregistrement et le serveur de gestion
❹ Le certificat de l'autorité de certification doit être installé sur les ordinateurs sur lesquels les serveurs d'enregistrement s'exécutent
Conditions requises pour le certificat de serveur d'enregistrement privé :

- Attribué au serveur d'enregistrement afin que le nom d'hôte du serveur d'enregistrement soit inclus dans le certificat, soit en tant qu'objet (propriétaire), soit dans la liste des noms DNS auxquels le certificat est émis.
- Approuvé sur le serveur de gestion, en approuvant le certificat d'autorité de certification utilisé pour émettre le certificat du serveur d'enregistrement

4.1.7 Chiffrement entre le serveur de gestion et le serveur collecteur de données (explication)

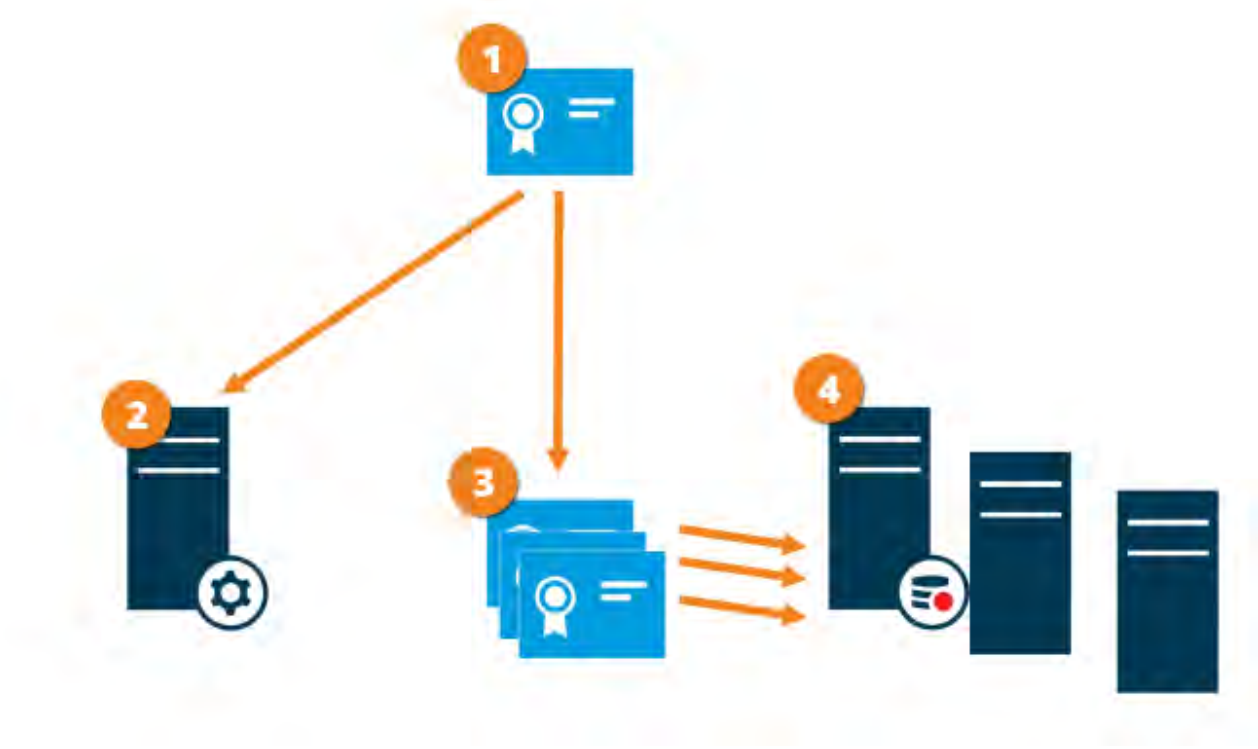
Vous pouvez chiffrer la connexion bidirectionnelle entre le serveur de gestion et le collecteur de données associé lorsque vous disposez d'un serveur distant du type suivant :

- Serveur d'enregistrement
- Serveur d'événements
- Serveur de journaux
- Serveur LPR
- Serveur mobile

Lorsque vous activez le chiffrement sur le serveur d'administration, il s'applique aux connexions de tous les serveurs du collecteur de données qui se connectent au serveur d'administration. Le chiffrement de cette communication doit suivre le paramètre de chiffrement sur le serveur de gestion. Par conséquent, si le chiffrement du serveur de gestion est activé, il doit également être activé sur les serveurs du collecteur de données affiliés à chaque serveur distant, et vice-versa. Avant d'activer le chiffrement, vous devez installer des certificats de sécurité sur le serveur de gestion et sur tous les serveurs de collecte de données affiliés aux serveurs distants.

Distribution des certificats

Le graphique illustre le concept de base de la signature, de l'approbation et de la distribution des certificats dans les machines virtuelles MOBOTIX HUB pour sécuriser la communication à partir du serveur de gestion.



❶ Un certificat d'autorité de certification agit en tant que tiers de confiance, approuvé à la fois par le sujet/propriétaire (serveur collecteur de données) et par la partie qui vérifie le certificat (serveur de gestion)
❷ Le certificat de l'autorité de certification doit être approuvé sur le serveur de gestion. De cette façon, le serveur de gestion peut vérifier la validité des certificats émis par l'autorité de certification

3 Le certificat CA est utilisé pour établir une connexion sécurisée entre les serveurs collecteurs de données et le serveur de gestion

4 Le certificat de l'autorité de certification doit être installé sur les ordinateurs sur lesquels les serveurs collecteurs de données s'exécutent

Conditions requises pour le certificat de serveur de collecteur de données privées :

- Attribué au serveur collecteur de données afin que le nom d'hôte du serveur collecteur de données soit inclus dans le certificat, soit en tant qu'objet (propriétaire), soit dans la liste des noms DNS auxquels le certificat est émis
- Approuvé sur le serveur de gestion, en approuvant le certificat de l'autorité de certification utilisé pour émettre le certificat du serveur de collecte de données

4.1.8 Chiffrement des clients et des serveurs qui récupèrent les données du serveur d'enregistrement (expliqué)

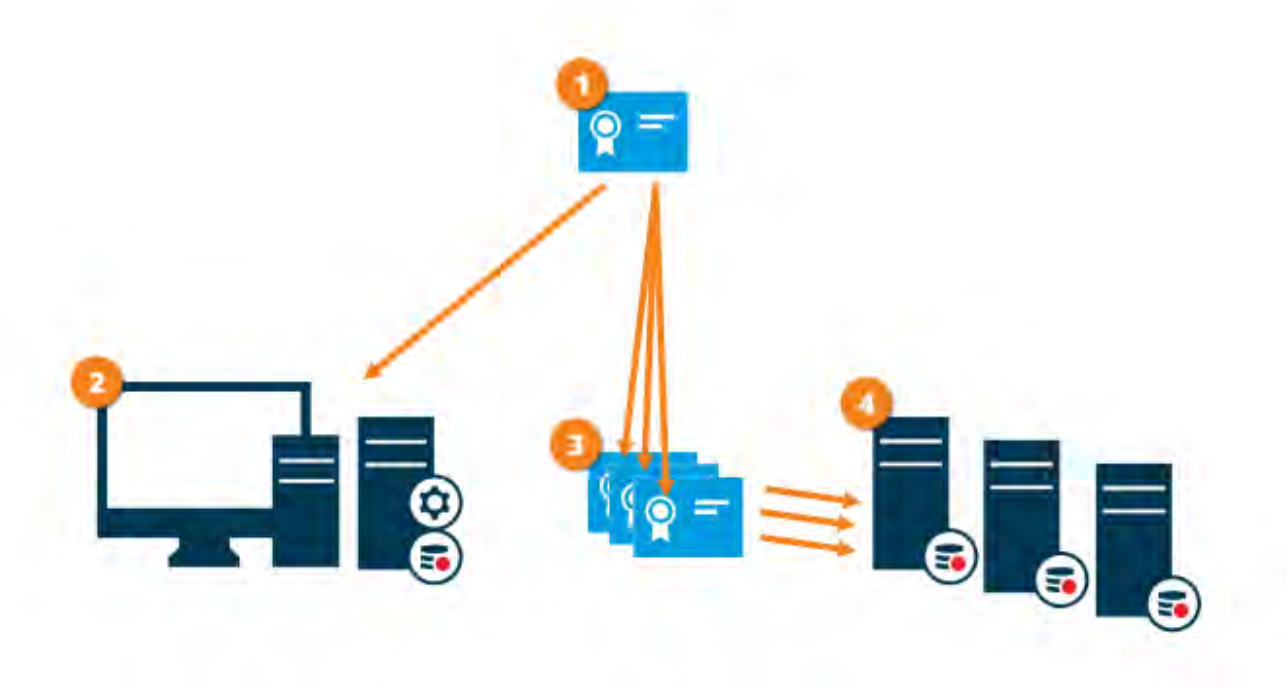
Lorsque vous activez le chiffrement sur un serveur d'enregistrement, la communication avec tous les clients, serveurs et intégrations qui récupèrent les flux de données du serveur d'enregistrement est chiffrée. Dans le présent document, on entend par « clients » :

- Client intelligent MOBOTIX HUB
- Client de gestion
- Serveur de gestion (pour le Moniteur système et pour les images et les clips vidéo AVI dans les notifications par e-mail)
- Serveur mobile MOBOTIX HUB
- Serveur d'événements MOBOTIX HUB
- MOHUB MOBOTIX LPR
- Pont de réseau ouvert MOBOTIX
- Serveur DLNA MOBOTIX HUB
- Sites qui récupèrent des flux de données à partir du serveur d'enregistrement via MOBOTIX Interconnect
- Certaines intégrations tierces du SDK MIP

Pour les solutions créées avec MIP SDK 2018 R3 ou version antérieure qui accède aux serveurs d'enregistrement : si les intégrations sont effectuées à l'aide des bibliothèques MIP SDK, elles doivent être reconstruites avec MIP SDK 2019 R1 ; si les intégrations communiquent directement avec les API du serveur d'enregistrement sans utiliser les bibliothèques MIP SDK, les intégrateurs doivent eux-mêmes ajouter la prise en charge HTTPS.

Distribution des certificats

Le graphique illustre le concept de base de la signature, de l'approbation et de la distribution des certificats dans les machines virtuelles MOBOTIX HUB pour sécuriser la communication avec le serveur d'enregistrement.



❶ Un certificat d'autorité de certification agit en tant que tiers de confiance, approuvé à la fois par le sujet/propriétaire (serveur d'enregistrement) et par la partie qui vérifie le certificat (tous les clients)
❷ Le certificat de l'autorité de certification doit être approuvé sur tous les clients. De cette façon, les clients peuvent vérifier la validité des certificats émis par l'autorité de certification
❸ Le certificat CA est utilisé pour établir une connexion sécurisée entre les serveurs d'enregistrement et tous les clients et services
❹ Le certificat de l'autorité de certification doit être installé sur les ordinateurs sur lesquels les serveurs d'enregistrement s'exécutent
Conditions requises pour le certificat de serveur d'enregistrement privé :

- Attribué au serveur d'enregistrement afin que le nom d'hôte du serveur d'enregistrement soit inclus dans le certificat, soit en tant qu'objet (propriétaire), soit dans la liste des noms DNS auxquels le certificat est émis.
- Approuvé sur tous les ordinateurs exécutant des services qui récupèrent des flux de données à partir des serveurs d'enregistrement, en approuvant le certificat d'autorité de certification utilisé pour émettre le certificat de serveur d'enregistrement
- Le compte de service qui exécute le serveur d'enregistrement doit avoir accès à la clé privée du certificat sur le serveur d'enregistrement.

Si vous activez le chiffrement sur les serveurs d'enregistrement et que votre système applique des serveurs d'enregistrement de basculement, MOBOTIX vous recommande de préparer également les serveurs d'enregistrement de basculement pour le chiffrement.

4.1.9 Chiffrement de la communication avec le serveur d'événements

Vous pouvez chiffrer la connexion bidirectionnelle entre le serveur d'événements et les composants qui communiquent avec le serveur d'événements, y compris le serveur LPR. Lorsque vous activez le chiffrement sur le serveur d'événements, il s'applique aux connexions de tous les composants qui se connectent au serveur

d'événements. Avant d'activer le chiffrement, vous devez installer des certificats de sécurité sur le serveur d'événements et tous les composants de connexion.

Lorsque la communication du serveur d'événements est chiffrée, cela s'applique à toutes les communications avec ce serveur d'événements. C'est-à-dire qu'un seul mode est pris en charge à la fois, http ou https, mais pas en même temps.

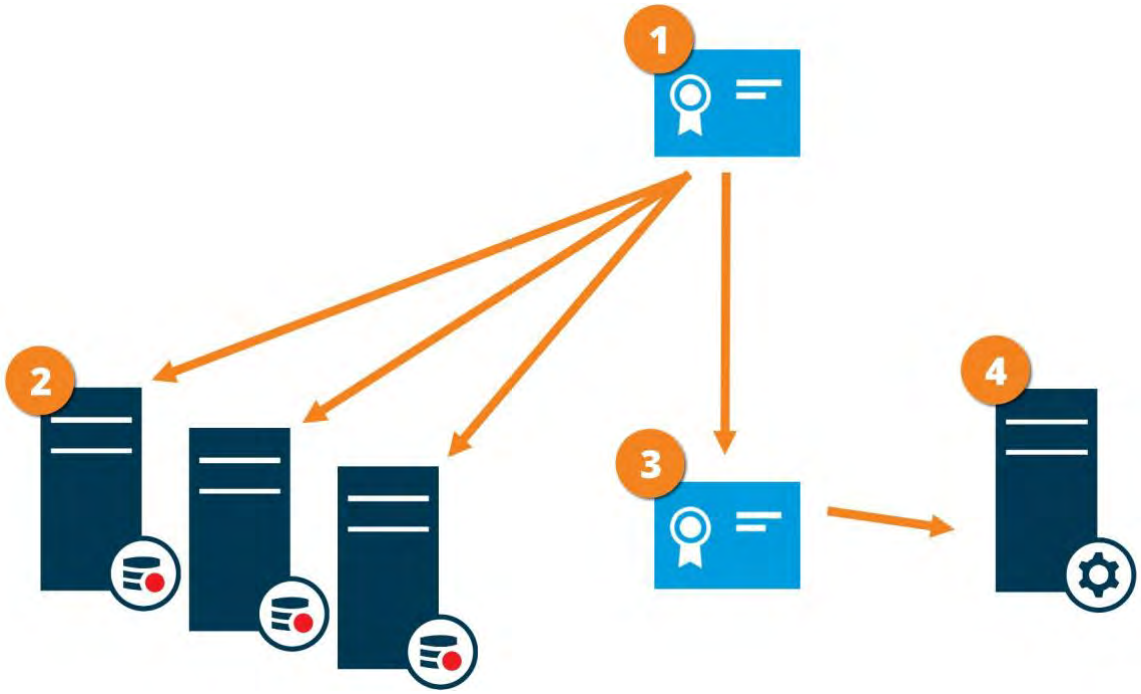
Le chiffrement s'applique à tous les services hébergés dans le serveur d'événements, y compris Transact, Maps, GisMap et Intercommunication.

Avant d'activer le chiffrement dans Event Server, tous les clients (Smart Client et Management Client) et le plug-in MOBOTIX HUB PR doivent être mis à jour vers au moins la version 2022 R1.

HTTPS n'est pris en charge que si chaque composant est mis à jour vers au moins la version 2022 R1.

Distribution des certificats

Le graphique illustre le concept de base de la signature, de l'approbation et de la distribution des certificats dans les machines virtuelles MOBOTIX HUB pour sécuriser la communication avec le serveur d'événements



❶ Un certificat d'autorité de certification agit en tant que tiers de confiance, approuvé à la fois par le sujet/propriétaire (serveur d'événements) et par la partie qui vérifie le certificat

❷ Le certificat de l'autorité de certification doit être approuvé sur tous les clients. De cette façon, les clients peuvent vérifier la validité des certificats émis par l'AC

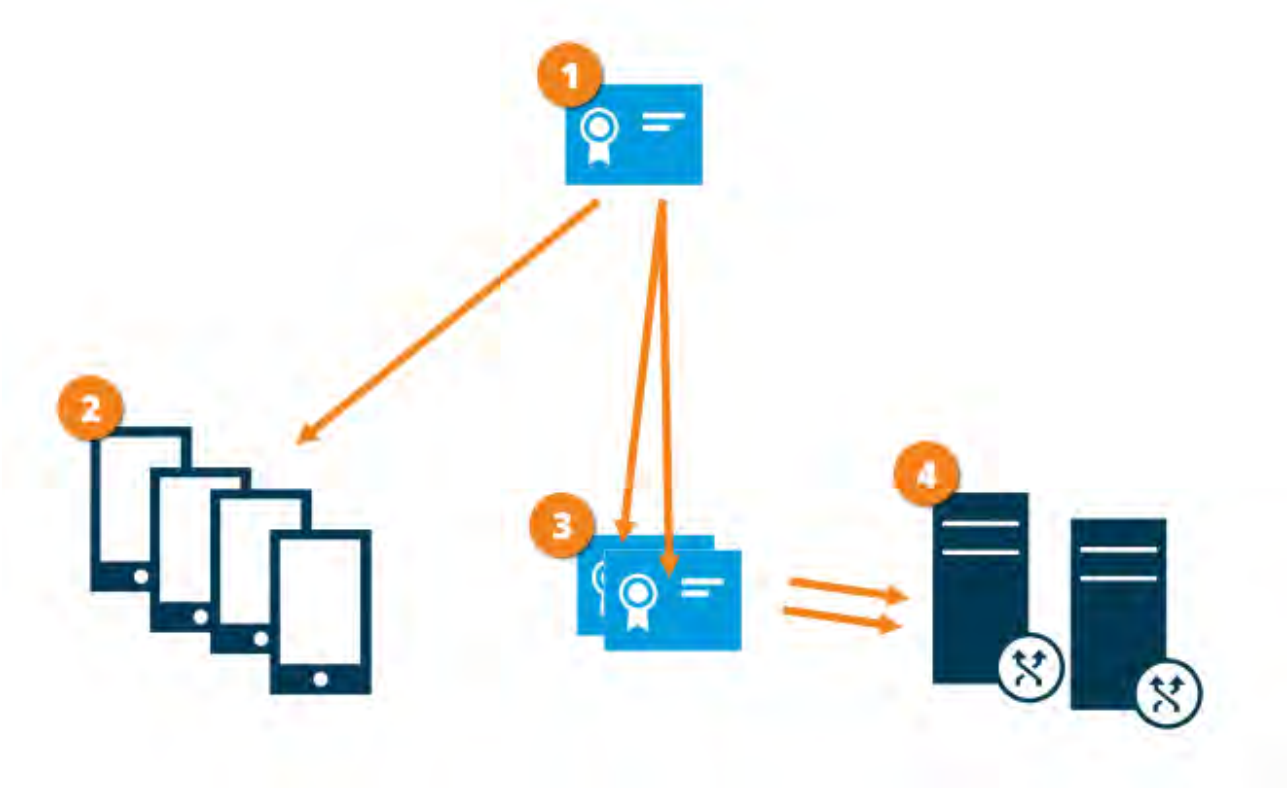
❸ Le certificat de l'autorité de certification est utilisé pour établir une connexion sécurisée entre le serveur d'événements et les clients❹ . Le certificat de l'autorité de certification doit être installé sur l'ordinateur sur lequel le serveur d'événements s'exécute.

4.1.10 Cryptage des données du serveur mobile (expliqué)

Dans les machines virtuelles Mobotix Hub, le chiffrement est activé ou désactivé par serveur mobile. Lorsque vous activez le chiffrement sur un serveur mobile, vous avez la possibilité d'utiliser une communication chiffrée avec tous les clients, services et intégrations qui récupèrent les flux de données.

Distribution de certificats pour les serveurs mobiles

Le graphique illustre le concept de base de la signature, de l'approbation et de la distribution des certificats dans les machines virtuelles MOBOTIX HUB pour sécuriser la communication avec le serveur mobile.



❶ Un certificat d'autorité de certification agit en tant que tiers de confiance, approuvé à la fois par le sujet/propriétaire (serveur mobile) et par la partie qui vérifie le certificat (tous les clients)
❷ Le certificat de l'autorité de certification doit être approuvé sur tous les clients. De cette façon, les clients peuvent vérifier la validité des certificats émis par l'autorité de certification
❸ Le certificat CA est utilisé pour établir une connexion sécurisée entre le serveur mobile et les clients et services
❹ Le certificat CA doit être installé sur l'ordinateur sur lequel le serveur mobile s'exécute

Conditions requises pour le certificat CA :

- Le nom d'hôte du serveur mobile doit être inclus dans le certificat, soit en tant que sujet/propriétaire, soit dans la liste des noms DNS auxquels le certificat est délivré
- Le certificat doit être approuvé sur tous les appareils qui exécutent des services qui récupèrent des flux de données à partir du serveur mobile
- Le compte de service qui exécute le serveur mobile doit avoir accès à la clé privée du certificat de l'autorité de certification

Exigences de chiffrement des serveurs mobiles pour les clients

Si vous n'activez pas le cryptage et que vous utilisez une connexion HTTP, la fonction Push-to-Talk du client Web MOBOTIX HUB ne sera pas disponible.

4.1.11 Authentification Kerberos (expliquée)

Kerberos est un protocole d'authentification réseau basé sur des tickets. Il est conçu pour fournir une authentification forte pour les applications client/serveur ou serveur/serveur.
Utilisez l'authentification Kerberos comme alternative à l'ancien protocole d'authentification Microsoft NT LAN (NTLM).
L'authentification Kerberos nécessite une authentification mutuelle, dans laquelle le client s'authentifie auprès du service et le service s'authentifie auprès du client. De cette façon, vous pouvez vous authentifier de manière plus sécurisée à partir des clients MOBOTIX HUB vers les serveurs MOBOTIX HUB sans exposer votre mot de passe.
Pour rendre l'authentification mutuelle possible dans vos machines virtuelles Mobotix Hub, vous devez enregistrer les noms de principal de service (SPN) dans l'annuaire actif. Un SPN est un alias qui identifie de manière unique une entité telle qu'un service de serveur MOBOTIX HUB. Chaque service qui utilise l'authentification mutuelle doit avoir un SPN enregistré afin que les clients puissent identifier le service sur le réseau. Sans SPN correctement enregistrés, l'authentification mutuelle n'est pas possible.
Le tableau ci-dessous répertorie les différents services MOBOTIX avec les numéros de port correspondants que vous devez enregistrer :

Service	Numéro de port
Serveur de gestion - IIS	80 - Configurable
Serveur de gestion - Interne	8080
Serveur d'enregistrement - Collecteur de données	7609
Serveur de basculement	8990
Serveur d'événements	22331
Serveur LPR	22334

Le nombre de services que vous devez enregistrer dans l'Active Directory dépend de votre installation actuelle. Data Collector est installé automatiquement lors de l'installation du serveur de gestion, du serveur d'enregistrement, du serveur d'événements, du serveur LPR ou du serveur de basculement.

Vous devez enregistrer deux SPN pour l'utilisateur qui exécute le service : l'un avec le nom d'hôte et l'autre avec le nom de domaine complet.
Si vous exécutez le service sous un compte de service d'utilisateur réseau, vous devez inscrire les deux SPN pour chaque ordinateur exécutant ce service.
Voici le schéma de nommage SPN MOBOTIX :

```
VideoOS/[Nom d'hôte DNS] :[Port]
VideoOS/[Nom de domaine complet] :[Port]
```

Voici un exemple de SPN pour le service de serveur d'enregistrement s'exécutant sur un ordinateur avec les détails suivants :

`d'hôte : Record-Server1`
`Domaine : Surveillance.com`
SPN à enregistrer :
`VideoOS/Record-Server1:7609`
`VideoOS/Record-Server1.Surveillance.com :7609`

4.1.12 Utiliser la mise à jour Windows

MOBOTIX vous recommande d'utiliser Windows Update pour protéger votre VMS contre les vulnérabilités du système d'exploitation en vous assurant que les dernières mises à jour sont installées. MOBOTIX HUB VMS est basé sur Windows, les mises à jour de sécurité de Windows Update sont donc importantes.
Les mises à jour peuvent nécessiter une connexion à Internet, c'est pourquoi MOBOTIX recommande que cette connexion ne soit ouverte qu'en cas de besoin et qu'elle soit surveillée pour détecter les modèles de trafic inhabituels.
Les mises à jour Windows nécessitent souvent un redémarrage. Cela peut poser un problème si une haute disponibilité est requise, car le serveur ne peut pas recevoir de données des périphériques pendant le redémarrage.
Il existe plusieurs façons d'éviter cela ou d'en minimiser l'impact. Par exemple, vous pouvez télécharger des mises à jour sur le serveur, puis les appliquer à un moment où un redémarrage perturbera le moins possible la surveillance.
Si la haute disponibilité est un problème, MOBOTIX vous recommande d'exécuter le serveur de gestion et les serveurs d'événements dans des clusters comprenant un ou plusieurs serveurs de basculement. Le serveur de basculement prend le relais pendant que le serveur d'enregistrement redémarre et la surveillance n'est pas interrompue. N'incluez pas les serveurs d'enregistrement dans le cluster. Pour les serveurs d'enregistrement, utilisez un serveur d'enregistrement de basculement.

Avant d'implémenter les mises à jour Windows dans l'ensemble de l'organisation, MOBOTIX vous recommande de vérifier les mises à jour dans un environnement de test. Voir NIST 800-53 CM-8 Inventaire *des composants du système d'information et bac à sable et SC-44 Chambres de détonation*.

Pour en savoir plus

Les contrôles suivants fournissent des indications supplémentaires :

- Correction des défauts NIST SP 800-53 SI-2

4.1.13 Maintenir le logiciel et le micrologiciel de l'appareil à jour

MOBOTIX vous recommande d'utiliser la dernière version de MOBOTIX HUB VMS et du firmware pour les périphériques matériels, par exemple les caméras. Cela garantira que votre système inclut les derniers correctifs de sécurité.
Pour le matériel, les composants réseau et les systèmes d'exploitation, consultez la base de données CVE ainsi que toutes les mises à jour publiées par les fabricants.
Avant de mettre à niveau le micrologiciel de l'appareil, vérifiez que MOBOTIX HUB VMS le prend en charge. Assurez-vous également que le pack de périphériques installé sur les serveurs d'enregistrement prend en charge le micrologiciel de l'appareil.
Faites-le dans un environnement de test pour la configuration, l'intégration et les tests avant de le mettre dans l'environnement de production.
Pour vérifier que le VMS prend en charge un appareil, procédez comme suit :

1. Ouvrez ce lien (https://www.mobotix.com/mobotix_custom_table/hub_compatibility).
2. Sélectionnez le fabricant de votre appareil, puis cliquez sur Filtrer. La version du microprogramme prise en charge par le pack de périphériques est répertoriée dans la colonne Microprogramme testé.

Pour en savoir plus

Les contrôles suivants fournissent des indications supplémentaires :

- Correction des défauts NIST SP 800-53 SI-2

4.1.14 Utiliser un antivirus sur tous les serveurs et ordinateurs

MOBOTIX vous recommande de déployer un logiciel antivirus sur tous les serveurs et ordinateurs qui se connectent au VMS. Les logiciels malveillants qui pénètrent dans votre système peuvent verrouiller, chiffrer ou compromettre les données sur les serveurs et autres appareils du réseau.

Si des appareils mobiles se connectent au VMS, il faut s'assurer que les derniers systèmes d'exploitation et correctifs (mais pas directement antivirus) sont installés.

Lorsque vous effectuez une analyse antivirus, n'analysez pas les répertoires et sous-répertoires du serveur d'enregistrement qui contiennent des bases de données d'enregistrement. De plus, ne recherchez pas de virus dans les répertoires de stockage d'archives. La recherche de virus dans ces répertoires peut avoir un impact sur les performances du système.

Pour plus d'informations sur les ports, répertoires et sous-répertoires à exclure de l'analyse antivirus, reportez-vous à la section *À propos de* l'analyse antivirus dans le *manuel de l'administrateur MOBOTIX HUB* VMS.

Pour en savoir plus

Les contrôles suivants fournissent des indications supplémentaires :

- Architecture de sécurité de l'information NIST SP 800-53 PL-8
- NIST SP 800-53 SI-2 Correction des défauts
- Protection contre les codes malveillants NIST SP 800-53 SI-3
- NIST SP 800-53 SI Surveillance des systèmes d'information

4.1.15 Surveillez les journaux dans le VMS pour détecter les signes d'activité suspecte

MOBOTIX HUB VMS fournit des fonctionnalités de génération et d'affichage de journaux qui fournissent des informations sur les modèles d'utilisation, les performances du système et d'autres problèmes. MOBOTIX vous recommande de surveiller les journaux pour détecter tout signe d'activités suspectes.

Il existe des outils qui exploitent les journaux à des fins opérationnelles et de sécurité. De nombreuses entreprises utilisent des serveurs syslog pour consolider les journaux. Vous pouvez utiliser syslog pour noter les activités au niveau Windows, mais MOBOTIX HUB VMS ne prend pas en charge syslog.

MOBOTIX vous recommande d'utiliser le journal d'audit dans les machines virtuelles MOBOTIX HUB et d'activer la journalisation de l'accès des utilisateurs dans Management Client. Par défaut, le journal d'audit note uniquement les connexions des utilisateurs. Toutefois, vous pouvez activer la journalisation de l'accès utilisateur afin que le journal d'audit note toutes les activités des utilisateurs dans tous les composants clients des produits MOBOTIX HUB VMS. Cela inclut les heures des activités et les adresses IP sources.

Les composants clients sont MOBOTIX HUB Smart Client, Web Client, le composant MOBOTIX HUB Management Client et les intégrations effectuées à l'aide du SDK MIP. Des exemples d'activités sont les exportations, l'activation de sorties, l'affichage de caméras en direct ou en lecture, etc.

Le journal d'audit ne note pas les tentatives de connexion infructueuses ou le moment où l'utilisateur se déconnecte.

La journalisation de toutes les activités des utilisateurs dans tous les clients augmente la charge sur le système et peut affecter les performances.

Vous pouvez ajuster la charge en spécifiant les critères suivants qui contrôlent le moment où le système génère une entrée de journal :

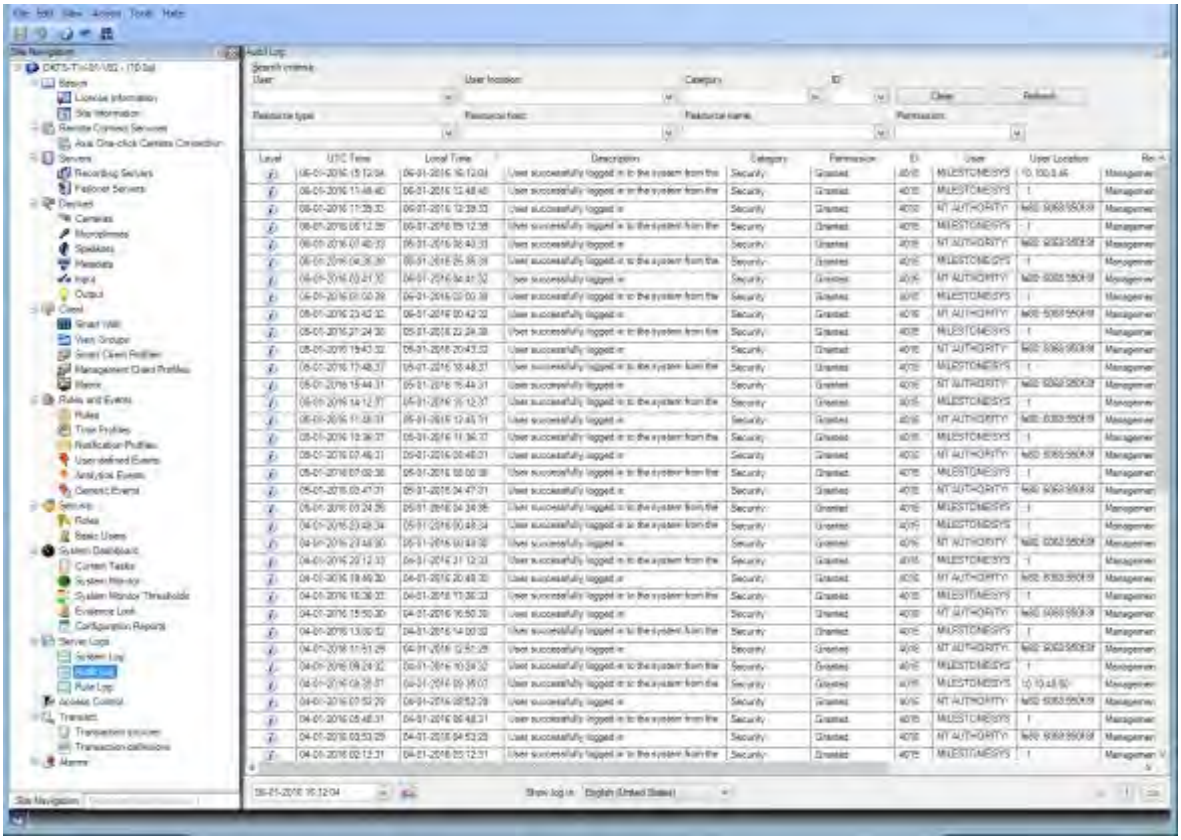
- Nombre de secondes qui composent une séquence. Le VMS génère une entrée de journal lorsqu'un utilisateur lit une vidéo dans la séquence.
- Nombre d'images qu'un utilisateur doit afficher lors de la lecture d'une vidéo avant que le VMS ne génère une entrée de journal.

Pour activer et configurer la journalisation étendue de l'accès utilisateur, procédez comme suit :

1. Dans Management Client, cliquez sur Outils, puis sélectionnez Options.
2. Sous l'onglet Journaux du serveur, sous Paramètres du journal, sélectionnez Journal d'audit.
3. Sous Paramètres, cochez la case Activer la journalisation de l'accès utilisateur.
4. Facultatif : Pour spécifier les limitations des informations notées et réduire l'impact sur les performances, effectuez des sélections dans les champs Durée de journalisation de la séquence de lecture et Enregistrements vus avant la journalisation.

Pour afficher le journal d'audit dans MOBOTIX HUB VMS, procédez comme suit :

1. Ouvrez Management Client.
2. Développez le nœud Journaux du serveur.
3. Cliquez sur Journal d'audit.



Pour en savoir plus

Les contrôles suivants fournissent des indications supplémentaires :

- NIST SP 800-53 AU-3 Contenu des dossiers d'audit
- Analyse des vulnérabilités NIST SP 800-53 RA-5
- NIST SP 800-53 AU-6 Examen, analyse et rapports d'audit

4.2 Étapes avancées

4.2.1 Adopter des normes pour la mise en œuvre de réseaux et de VMS sécurisés

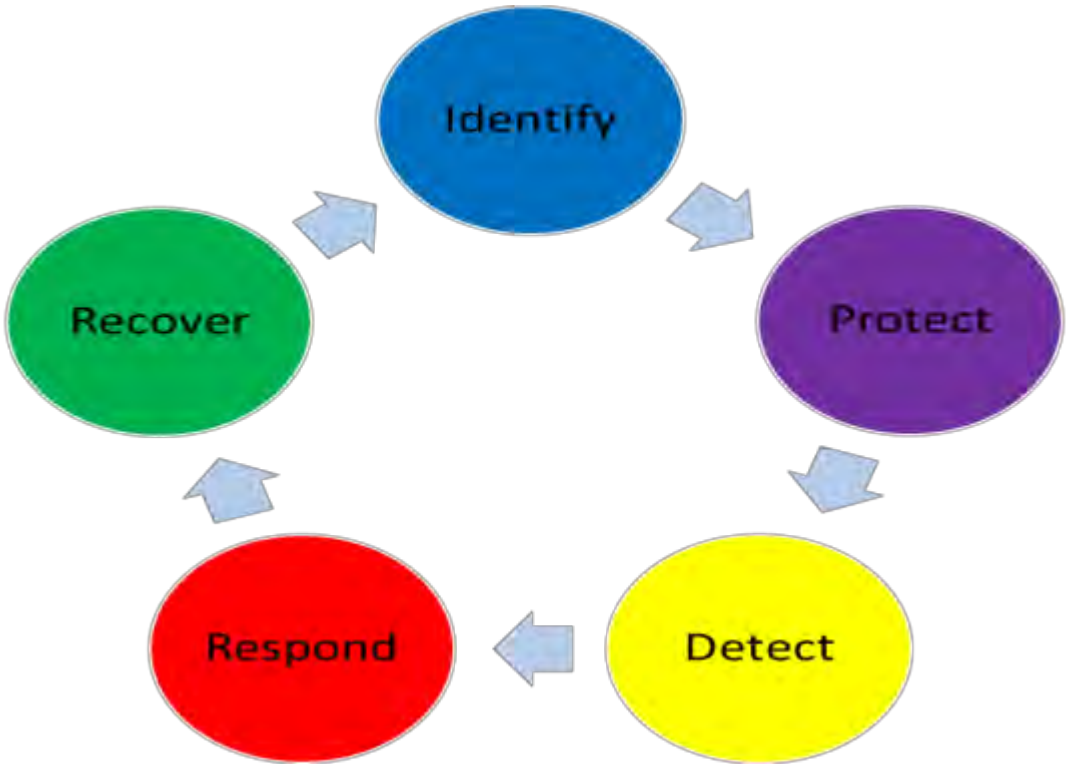
MOBOTIX vous recommande d'adopter des normes pour la mise en réseau sécurisée et les implémentations de MOBOTIX HUB VMS. L'utilisation de normes est un élément fondamental de l'ingénierie d'Internet et des réseaux,

ainsi que la base de l'interopérabilité et de la conformité des systèmes. Cela s'applique également à l'utilisation de solutions cryptographiques, où la cryptographie basée sur des normes est l'approche la plus couramment acceptée.

4.2.2 Etablir un plan d'intervention en cas d'incident

MOBOTIX vous recommande de commencer par un ensemble de politiques et de procédures et d'établir un plan de réponse aux incidents. Désignez du personnel pour surveiller l'état du système et répondre aux événements suspects. Par exemple, des activités qui se déroulent à des moments inhabituels. Établissez un point de contact (POC) de sécurité avec chacun de vos fournisseurs, y compris MOBOTIX.

L'image suivante est adaptée du cadre de cybersécurité du NIST (http://www.nist.gov/cyberframework/). Il montre le cycle de vie qui doit être pris en compte lors de la création d'un plan. Les documents à l'appui du cadre fournissent des détails sur le cycle de vie et les contrôles de sécurité des plans d'intervention en cas d'incident.



Pour en savoir plus

Les contrôles suivants fournissent des indications supplémentaires :

- NIST SP 800-53 IR 1-13 Réponse aux incidents

4.2.3 Protéger les composants VMS sensibles

MOBOTIX vous recommande d'utiliser le contrôle d'accès physique et d'utiliser le VMS pour surveiller et protéger ses composants VMS sensibles. La restriction physique et le contrôle d'accès physique basé sur les rôles sont des contre-mesures qui assurent la sécurité des serveurs et des postes de travail.

Les administrateurs et les utilisateurs ne doivent avoir accès qu'aux informations dont ils ont besoin pour s'acquitter de leurs responsabilités. Si tous les utilisateurs internes ont le même niveau d'accès aux données critiques, il est plus facile pour les attaquants d'accéder au réseau.

Pour en savoir plus

Les contrôles suivants fournissent des indications supplémentaires :

- NIST SP 800-53 PE-1 Politique et procédures de protection physique et environnementale
- NIST SP 800-53 PE-2 Autorisations d'accès physique
- NIST SP 800-53 PE-3 Contrôle d'accès physique
- NIST SP 800-53 AC-4 Moindre privilège

4.2.4 Suivez les meilleures pratiques de sécurité du système d'exploitation Microsoft

MOBOTIX vous recommande de suivre les meilleures pratiques de sécurité pour les systèmes d'exploitation Microsoft afin d'atténuer les risques liés au système d'exploitation et de maintenir la sécurité. Cela vous aidera à assurer la sécurité des serveurs et des ordinateurs clients Microsoft.

Pour plus d'informations, consultez *le Guide des mises à jour de sécurité Microsoft* (https://msrc.microsoft.com/update-guide).

4.2.5 Utiliser des outils pour automatiser ou mettre en œuvre la politique de sécurité

MOBOTIX vous recommande de trouver un ou plusieurs outils pour vous aider à automatiser et à mettre en œuvre la politique de sécurité. L'automatisation réduit le risque d'erreur humaine et facilite la gestion de la politique. Par exemple, vous pouvez automatiser l'installation de correctifs de sécurité et de mises à jour sur les serveurs et les ordinateurs clients.

L'une des façons de mettre en œuvre cette recommandation consiste à combiner le gestionnaire de configuration de sécurité Microsoft (SCCM) avec le protocole SCAP (Security Content Automation Protocol). (Voir par exemple, *Geek de tous les corps de métier : Automatisez les paramètres de sécurité de base* (https://technet.microsoft.com/en-us/magazine/ff721825.aspx) et *le programme de validation du protocole d'automatisation du contenu de sécurité (SCAP)* (https://csrc.nist.gov/projects/scap-validation-program).) Cela vous donne un cadre pour créer, distribuer et valider les paramètres de sécurité sur les ordinateurs de votre réseau.

Pour en savoir plus

Les contrôles suivants fournissent des indications supplémentaires :

- NIST SP 800-53 CM-1 Politique et procédures de gestion de la configuration
- Configuration de base NIST SP 800-53 CM-2
- NIST SP 800-53 CM-3 Contrôle des changements de configuration

4.2.6 Suivre les meilleures pratiques de sécurité réseau établies

MOBOTIX vous recommande de suivre les meilleures pratiques informatiques et des fournisseurs pour vous assurer que les appareils de votre réseau sont configurés en toute sécurité. Demandez à vos fournisseurs de vous fournir ces informations. Il est important d'ouvrir et de maintenir un dialogue sur la sécurité, et une discussion sur les meilleures pratiques est un bon point de départ.

Il est important de refuser l'accès au VMS en n'utilisant pas de paramètres réseau vulnérables. Pour plus d'informations, consultez *les normes SP 800-128* (https://csrc.nist.gov/publications/detail/sp/800-128/final), *SP 800-41-rev1* (https://csrc.nist.gov/publications/detail/sp/800-41/rev-1/final) (spécifique aux pare-feu) et *Normes et références ICS-CERT* (https://www.cisa.gov/ics) (liste générale).

Pour en savoir plus

Les contrôles suivants fournissent des indications supplémentaires :

- Paramètres de configuration du NIST 800-53 CM-6
- Outils d'entretien NIST 800-53 MA-3

5 Appareils et réseau

Cette section fournit des conseils pour le renforcement des périphériques et des composants réseau liés aux machines virtuelles Mobotix Hub. Cela inclut des éléments clés du système tels que les caméras, le stockage et le réseau.

Les systèmes de surveillance incluent souvent des caméras à la périphérie du réseau. Les caméras et leurs connexions réseau, si elles ne sont pas protégées, représentent un risque important de compromission, ce qui peut donner aux intrus un accès supplémentaire au système.

5.1 Étapes de base – Appareils

5.1.1 Utilisez des mots de passe forts au lieu des mots de passe par défaut

MOBOTIX vous recommande de modifier les mots de passe par défaut sur les appareils, par exemple sur un appareil photo. N'utilisez pas de mots de passe par défaut, car ils sont souvent publiés sur Internet et sont facilement accessibles.

Utilisez plutôt des mots de passe forts pour les appareils. Les mots de passe forts comprennent huit caractères alphanumériques ou plus, utilisent des majuscules et des minuscules et des caractères spéciaux.

Pour en savoir plus

Les contrôles suivants fournissent des indications supplémentaires :

- Gestion de l'authentificateur NIST 800-53 IA-4
- Retour d'information sur l'authentificateur NIST 800-53 IA-8
- Gestion des erreurs NIST 800-53 SI-11

5.1.2 Arrêter les services et protocoles inutilisés

Pour éviter tout accès non autorisé ou toute divulgation d'informations, MOBOTIX vous recommande d'arrêter les services et protocoles inutilisés sur les appareils. Par exemple, Telnet, SSH, FTP, UPnP, Ipv6 et Bonjour.

Il est également important d'utiliser une authentification forte sur tous les services qui accèdent au VMS, au réseau ou aux appareils. Par exemple, utilisez des clés SSH au lieu de noms d'utilisateur et de mots de passe, et utilisez des certificats d'une autorité de certification pour HTTPS. Pour plus d'informations, consultez les guides de durcissement et d'autres conseils du fabricant de l'appareil.

Pour en savoir plus

Les contrôles suivants fournissent des indications supplémentaires :

- Accès à distance NIST SP 800-53 AC-17 (désactivation des protocoles inutilisés)
- NIST SP 800-53 CM-6 Paramètres de configuration

- NIST SP 800-53 CM-7 Fonctionnalité minimale
- NIST SP 800-53 IA-2 Identification et authentification
- NIST SP 800-53 SA-9 Services d'information externes

5.1.3 Créez des comptes d'utilisateur dédiés sur chaque appareil

Toutes les caméras ont un compte utilisateur par défaut avec un nom d'utilisateur et un mot de passe que le VMS utilise pour accéder à l'appareil. À des fins d'audit, MOBOTIX vous recommande de modifier le nom d'utilisateur et le mot de passe par défaut.

Créez un compte utilisateur spécifiquement destiné au VMS et utilisez ce compte utilisateur et ce mot de passe lorsque vous ajoutez la caméra au VMS. Lorsqu'un serveur d'enregistrement se connecte à la caméra, il utilise le nom d'utilisateur et le mot de passe que vous avez créés. Si l'appareil photo dispose d'un journal, ce journal indique que le serveur d'enregistrement s'est connecté à l'appareil photo.

À l'aide d'un nom d'utilisateur et d'un mot de passe dédiés, les journaux de l'appareil peuvent vous aider à déterminer si un serveur d'enregistrement ou une personne a accédé à l'appareil photo. Ceci est pertinent lors de l'enquête sur les problèmes de sécurité potentiels affectant les appareils.

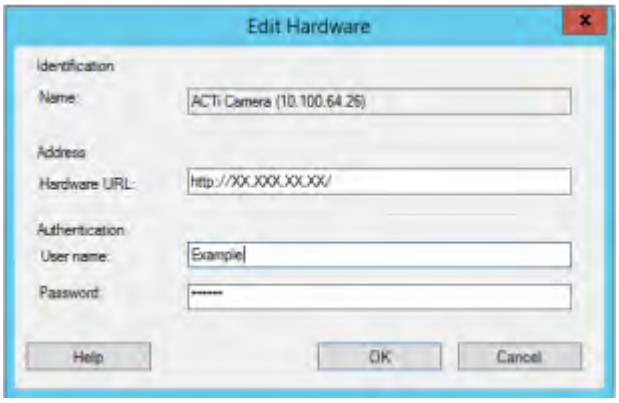
Vous pouvez modifier le nom d'utilisateur et le mot de passe d'un périphérique avant ou après l'avoir ajouté dans Management Client.

Pour modifier le nom d'utilisateur et le mot de passe avant d'ajouter l'appareil, procédez comme suit :

1. Accédez à l'interface Web de l'appareil et modifiez le nom d'utilisateur et le mot de passe par défaut.
2. Dans Management Client, ajoutez le périphérique, puis spécifiez le nom d'utilisateur et le mot de passe.

Pour modifier le nom d'utilisateur et les mots de passe des appareils déjà ajoutés, procédez comme suit :

1. Dans Management Client, dans le volet de navigation du site, développez le nœud Serveurs et sélectionnez Serveurs d'enregistrement.
2. Dans le volet Serveur d'enregistrement, développez le serveur d'enregistrement qui contient le périphérique, puis cliquez avec le bouton droit sur le périphérique et sélectionnez Modifier le matériel.



3. Sous Authentification, entrez le nouveau nom d'utilisateur et le nouveau mot de passe.

Pour en savoir plus

Les contrôles suivants fournissent des indications supplémentaires :

- NIST SP 800-53 AC-2 Gestion de compte
- NIST SP 800-53 AC-4 Moindre privilège

5.1.4 Recherche d'appareils

La recherche de périphériques (par exemple, l'analyse express ou **l'analyse de plage d'adresses** lors de l'ajout de matériel) s'effectue à l'aide de diffusions qui peuvent contenir des noms d'utilisateur et des mots de passe en texte brut.

À moins qu'il ne s'agisse d'une configuration initiale, cette fonctionnalité ne doit pas être utilisée pour ajouter des périphériques au système. Utilisez plutôt l' **option Manuel** et sélectionnez manuellement le pilote.

Sur les systèmes sensibles, la fonctionnalité de **découverte automatique des périphériques** doit être désactivée sur MOBOTIX HUB Professional VMS (située dans **Paramètres** > **Connexion des périphériques matériels**), car elle enverra périodiquement des diffusions pouvant contenir des noms d'utilisateur et des mots de passe.

5.2 Étapes de base – Réseau

5.2.1 Utilisez une connexion réseau sécurisée et fiable

Les communications réseau doivent être sécurisées, que vous soyez ou non sur un réseau fermé. Par défaut, les communications sécurisées doivent être utilisées lors de l'accès au VMS. Par exemple:

- Tunnels VPN ou HTTPS par défaut
- Dernière version de Transport Layer Security (https://datatracker.ietf.org/wg/tls/charter/) (TLS, actuellement 1.2) avec des certificats valides qui répondent aux meilleures pratiques du secteur, telles que l'infrastructure à clé publique (X.509) (https://datatracker.ietf.org/wg/ipsec/documents/) et le CA/Browser Forum (https://cabforum.org/).

Sinon, les informations d'identification peuvent être compromises et des intrus peuvent les utiliser pour accéder au VMS.

Configurez le réseau pour permettre aux ordinateurs clients d'établir des sessions HTTPS sécurisées ou des tunnels VPN entre les périphériques clients et les serveurs VMS.

Pour en savoir plus

Les contrôles suivants fournissent des indications supplémentaires :

- NIST SP 800-53 SI-2 Correction des défauts
- NIST SP 800-53 CM-6 Paramètres de configuration
- NIST SP 800-53 SC-23 Authenticité de la session

5.2.2 Utilisez des pare-feu pour limiter l'accès IP aux serveurs et aux ordinateurs

MOBOTIX vous recommande d'utiliser des connexions sécurisées et d'effectuer les étapes supplémentaires suivantes :

- Utiliser l'authentification sécurisée de l'appareil
- Utiliser TLS

- Utiliser la liste blanche des appareils pour authentifier les appareils
- Utilisez des pare-feu pour limiter la communication réseau entre les serveurs et les ordinateurs et programmes clients.

Tous les composants MOBOTIX HUB et les ports dont ils ont besoin sont répertoriés dans les différentes sections ci-dessous. Pour vous assurer, par exemple, que le pare-feu ne bloque que le trafic indésirable, vous devez spécifier les ports utilisés par les machines virtuelles Mobotix Hub. Vous ne devez activer que ces ports. Les listes incluent également les ports utilisés pour les processus locaux.
Ils sont disposés en deux groupes :

- Composants de serveur (services) : offrent leur service sur les ports, c'est pourquoi ils doivent écouter les demandes des clients sur ces ports. Par conséquent, ces ports doivent être ouverts dans le pare-feu Windows pour les connexions entrantes.
- Composants clients (clients) : lancez des connexions aux ports sur les composants serveur. Par conséquent, ces ports doivent être ouverts pour les connexions sortantes. Les connexions sortantes sont généralement ouvertes par défaut dans le pare-feu Windows.

Si rien d'autre n'est mentionné, les ports pour les composants du serveur doivent être ouverts pour les connexions entrantes et les ports pour les composants du client doivent être ouverts pour les connexions sortantes.
Gardez à l'esprit que les composants du serveur peuvent également agir en tant que clients pour d'autres composants du serveur.
Les numéros de port sont les numéros par défaut, mais ils peuvent être modifiés. Contactez l'assistance MOBOTIX si vous devez modifier des ports qui ne sont pas configurables via le client de gestion.

Composants serveur (connexions entrantes)

Chacune des sections suivantes répertorie les ports qui doivent être ouverts pour un service particulier. Afin de déterminer quels ports doivent être ouverts sur un ordinateur particulier, vous devez prendre en compte tous les services exécutés sur cet ordinateur.

Limitez l'accès à distance au serveur de gestion en ajoutant des règles de pare-feu pour autoriser uniquement les serveurs d'enregistrement à se connecter au port TCP 9993.

Service du serveur de gestion et processus associés

Numéro de port	Protocole	Processus	Liaisons depuis...	But
80	HTTP	L'IIS	Tous les serveurs, le MOBOTIX HUB Smart Client et le Client de gestion	L'objectif du port 80 et du port 443 est le même. Toutefois, le port utilisé par le VMS dépend du fait que vous ayez utilisé des certificats pour sécuriser la communication. • Lorsque vous n'avez pas sécurisé la communication avec des certificats, le VMS utilise le port 80. • Lorsque vous avez sécurisé la communication à l'aide de certificats, le VMS utilise le port 443, à l'exception de la communication entre le serveur d'événements et le serveur de gestion. La communication entre le serveur d'événements et le serveur d' administration utilise Windows Secured Framework (WCF) et l'authentification Windows sur le port 80.
443	HTTPS	L'IIS		
6473	TCP	Service de serveur de gestion	Icône de la barre d'état du Gestionnaire du Gestionnaire de serveur de gestion, connexion locale uniquement.	Affichage de l'état et gestion du service.
8080	TCP	Serveur de gestion	Connexion locale uniquement.	Communication entre les processus internes sur le serveur.
9000	HTTP	Serveur de gestion	Services de serveur d'enregistrement	Service Web pour la communication interne entre serveurs.

Numéro de port	Protocole	Processus	Liaisons depuis...	But
12345	TCP	Service de serveur de gestion	Client intelligent MOBOTIX HUB	Communication entre le système et les destinataires de Matrix. Vous pouvez modifier le numéro de port dans le client de gestion.
12974	TCP	Service de serveur de gestion	Windows SNMP Service	Communication avec l'agent d'extension SNMP. N'utilisez pas le port à d'autres fins, même si votre système n'applique pas SNMP. Dans les systèmes MOBOTIX HUB 2014 ou antérieurs, le numéro de port était 6475. Dans les systèmes MOBOTIX HUB 2019 R2 et antérieurs, le numéro de port était le 7475.

Service SQL Server

Numéro de port	Protocole	Processus	Liaisons depuis...	But
1433	TCP	Serveur SQL	Service de serveur de gestion	Stockage et récupération des configurations.
1433	TCP	Serveur SQL	Service de serveur d'événements	Stockage et récupération d'événements.
1433	TCP	Serveur SQL	Service de serveur de journaux	Stockage et récupération des entrées de journal.

Service de collecte de données

Numéro de port	Protocole	Processus	Liaisons depuis...	But
7609	HTTP	L'IIS	Sur l'ordinateur du serveur d'administration : services de collecte de données sur tous les autres serveurs. Sur d'autres ordinateurs : service Data Collector sur le Serveur de gestion.	Moniteur système.

Service de serveur d'événements

Numéro de port	Protocole	Processus	Liaisons depuis...	But
1234	TCP/UDP	Service de serveur d'événements	Tout serveur envoyant des événements génériques à votre système MOBOTIX HUB.	Écouter des événements génériques provenant de systèmes ou de périphériques externes. Uniquement si la source de données appropriée est activée.
1235	TCP	Service de serveur d'événements	Tout serveur envoyant des événements génériques à votre système MOBOTIX HUB.	Écouter des événements génériques provenant de systèmes ou de périphériques externes. Uniquement si la source de données appropriée est activée.
9090	TCP	Service de serveur d'événements	Tout système ou appareil qui envoie des événements d'analyse à votre système MOBOTIX HUB.	Écouter les événements d'analyse provenant de systèmes ou d'appareils externes. Pertinent uniquement si la fonctionnalité Événements Analytics est activée.
22331	TCP	Service de serveur d'événements	MOBOTIX HUB Smart Client et le client de gestion	Configuration, événements, alarmes et données cartographiques.
22333	TCP	Service de serveur d'événements	MIP Plug-ins et applications.	Messagerie MIP.

Service de serveur d'enregistrement

Numéro de port	Protocole	Processus	Liaisons depuis...	But
25	SMTP	Service de serveur d'enregistrement	Caméras, encodeurs et périphériques d'E/S.	Écoute des messages d'événement provenant des appareils. Le port est désactivé par défaut. (Obsolète) L'activation de cette option ouvrira un port pour les connexions non chiffrées et n'est pas recommandée.

Numéro de port	Protocole	Processus	Liaisons depuis...	But
5210	TCP	Service de serveur d'enregistrement	Serveurs d'enregistrement de basculement.	Fusion de bases de données après l'exécution d'un serveur d'enregistrement de basculement.
5432	TCP	Service de serveur d'enregistrement	Caméras, encodeurs et périphériques d'E/S.	Écoute des messages d'événement provenant des appareils. Le port est désactivé par défaut.
7563	TCP	Service de serveur d'enregistrement	MOBOTIX HUB Smart Client, Client de gestion	Récupération de flux vidéo et audio, commandes PTZ.
8966	TCP	Service de serveur d'enregistrement	Icône de la barre d'état du Gestionnaire du serveur d'enregistrement, connexion locale uniquement.	Affichage de l'état et gestion du service.
9001	HTTP	Service de serveur d'enregistrement	Serveur de gestion	Service Web pour la communication interne entre serveurs. Si plusieurs instances du serveur d'enregistrement sont utilisées, chaque instance a besoin de son propre port. Les ports supplémentaires seront 9002, 9003, etc.
11000	TCP	Service de serveur d'enregistrement	Serveurs d'enregistrement de basculement	Interrogation de l'état des serveurs d'enregistrement.
12975	TCP	Service de serveur d'enregistrement	Service SNMP Windows	Communication avec l'agent d'extension SNMP. N'utilisez pas le port à d'autres fins, même si votre système n'applique pas SNMP. Dans les systèmes MOBOTIX HUB 2014 ou antérieurs, le numéro de port était 6474. Dans les systèmes MOBOTIX HUB 2019 R2 et antérieurs, le numéro de port était le 7474.
65101	UDP	Service de serveur d'enregistrement	Connexion locale uniquement	Écoute des notifications d'événements des pilotes.

En plus des connexions entrantes au service de serveur d'enregistrement énumérées ci-dessus, le service de serveur d'enregistrement établit des connexions sortantes vers des caméras, des NVR et des sites interconnectés distants (MOBOTIX Interconnect ICP).

Service de serveur de basculement et service de serveur d'enregistrement de basculement

Numéro de port	Protocole	Processus	Liaisons depuis...	But
25	SMTP	Service de serveur d'enregistrement de basculement	Caméras, encodeurs et périphériques d'E/S.	Écoute des messages d'événement provenant des appareils. Le port est désactivé par défaut. (Obsolète) L'activation de cette option ouvrira un port pour les connexions non chiffrées et n'est pas recommandée.
5210	TCP	Service de serveur d'enregistrement de basculement	Serveurs d'enregistrement de basculement	Fusion de bases de données après l'exécution d'un serveur d'enregistrement de basculement.
5432	TCP	Service de serveur d'enregistrement de basculement	Caméras, encodeurs et périphériques d'E/S.	Écoute des messages d'événement provenant des appareils. Le port est désactivé par défaut.
7474	TCP	Service de serveur d'enregistrement de basculement	Service SNMP Windows	Communication avec l'agent d'extension SNMP. N'utilisez pas le port à d'autres fins, même si votre système n'applique pas SNMP.
7563	TCP	Service de serveur d'enregistrement de basculement	Client intelligent MOBOTIX HUB	Récupération de flux vidéo et audio, commandes PTZ.
8844	UDP	Service de serveur d'enregistrement de basculement	Connexion locale uniquement.	Communication entre les serveurs.
8966	TCP	Service de serveur d'enregistrement de basculement	Icône de la barre d'état du gestionnaire du serveur d'enregistrement de basculement, connexion locale uniquement.	Affichage de l'état et gestion du service.
8967	TCP	Service de serveur de basculement	Icône de la barre d'état du Gestionnaire de serveur de	Affichage de l'état et gestion du service.

Numéro de port	Protocole	Processus	Liaisons depuis...	But
			basculement, connexion locale uniquement.	
8990	TCP	Service de serveur de basculement	Service de serveur de gestion	Surveillance de l'état du service Serveur de basculement.
9001	HTTP	Service de serveur de basculement	Serveur de gestion	Service Web pour la communication interne entre serveurs.

En plus des connexions entrantes au service Serveur de basculement/Serveur d'enregistrement de basculement répertorié ci-dessus, le service Serveur de basculement/Serveur d'enregistrement de basculement établit des connexions sortantes vers les enregistreurs standard, les caméras et pour le Push vidéo.

Service de serveur de journaux

Numéro de port	Protocole	Processus	Liaisons depuis...	But
22337	HTTP	Service de serveur de journaux	Tous les composants MOBOTIX HUB, à l'exception du client de gestion et du serveur d'enregistrement.	Écrivez dans le serveur de journaux, lisez-le et configurez-le.

Service de serveur mobile

Numéro de port	Protocole	Processus	Liaisons depuis...	But
8000	TCP	Service de serveur mobile	Icône de la barre d'état du Gestionnaire de serveur mobile, connexion locale uniquement.	Application SysTray.
8081	HTTP	Service de serveur mobile	Clients mobiles, clients Web et client de gestion.	Envoi de flux de données ; vidéo et audio.
8082	HTTPS	Service de serveur mobile	Clients mobiles et clients Web.	Envoi de flux de données ; vidéo et audio.
40001 - 40099	HTTP	Service de serveur mobile	Service de serveur d'enregistrement	Push vidéo sur le serveur mobile. Cette plage de ports est désactivée par défaut.

Service de serveur LPR

Numéro de port	Protocole	Processus	Liaisons depuis...	But
22334	TCP	Service de serveur LPR	Serveur d'événements	Récupération des plaques d'immatriculation reconnues et de l'état du serveur. Pour se connecter, le plug-in LPR doit être installé sur le serveur d'événements.
22334	TCP	Service de serveur LPR	Icône de la barre d'état du Gestionnaire de serveur LPR, connexion locale uniquement.	Application SysTray

Service de pont MOBOTIX Open Network

Numéro de port	Protocole	Processus	Liaisons depuis...	But
580	TCP	Service de pont de réseau ouvert MOBOTIX	Clients ONVIF	Authentification et demandes de configuration du flux vidéo.
554	RTSP	RTSP Service	Clients ONVIF	Diffusion en continu de la vidéo demandée vers les clients ONVIF.

MOBOTIX HUB DLNA Service de serveur

Numéro de port	Protocole	Processus	Liaisons depuis...	But
9100	HTTP	Service de serveur DLNA	Dispositif DLNA	Découverte de l'appareil et configuration des canaux DLNA. Demandes de flux vidéo.
9200	HTTP	Service de serveur DLNA	Dispositif DLNA	Diffusion en continu de la vidéo demandée vers des appareils DLNA.

MOBOTIX HUB Service d'enregistrement d'écran

Numéro de port	Protocole	Processus	Liaisons depuis...	But
52111	TCP	MOBOTIX HUB Enregistreur d'écran	Service de serveur d'enregistrement	Fournit une vidéo à partir d'un moniteur. Il apparaît et agit de la même manière qu'une caméra sur le serveur d'enregistrement. Vous pouvez modifier le numéro de port dans le client de gestion.

Service de gestion des incidents MOBOTIX HUB

Numéro de port	Protocole	Processus	Liaisons depuis...	But
80	HTTP	L'IIS	MOBOTIX HUB Smart Client et le client de gestion	L'objectif du port 80 et du port 443 est le même. Toutefois, le port utilisé par le VMS dépend du fait que vous ayez utilisé des certificats pour sécuriser la communication. • Lorsque vous n'avez pas sécurisé la communication avec des certificats, le VMS utilise le port 80. • Lorsque vous avez sécurisé la communication avec des certificats, le VMS utilise le port 443
443	HTTPS			

Composants serveur (connexions sortantes)

Service de serveur de gestion

Numéro de port	Protocole	Connexions à...	But
443	HTTPS	Serveur de licences qui héberge le service de gestion des licences.	Activation des licences.

Service de serveur d'enregistrement

Numéro de port	Protocole	Connexions à...	But
80	HTTP	Caméras, NVR, encodeurs Sites interconnectés	Authentification, configuration, flux de données, vidéo et audio. Connectez-vous
443	HTTPS	Caméras, NVR, encodeurs	Authentification, configuration, flux de données, vidéo et audio.
554	RTSP	Caméras, NVR, encodeurs	Flux de données, vidéo et audio.
7563	TCP	Sites interconnectés	Flux de données et événements.
11000	TCP	Serveurs d'enregistrement de basculement	Interrogation de l'état des serveurs d'enregistrement.
40001 – 40099	HTTP	Service de serveur mobile	Push vidéo sur le serveur mobile. Cette plage de ports est désactivée par défaut.

Service de serveur de basculement et service de serveur d'enregistrement de basculement

Numéro de port	Protocole	Connexions à...	But
11000	TCP	Serveurs d'enregistrement de basculement	Interrogation de l'état des serveurs d'enregistrement.

Service de serveur de journaux

Numéro de port	Protocole	Connexions à...	But
443	HTTPS	Serveur de journaux	Transfert des messages vers le serveur de journaux.

Passerelle API

Numéro de port	Protocole	Connexions à...	But
80	HTTP	Serveur de gestion	RESTful API

Numéro de port	Protocole	Connexions à...	But
443	HTTPS	Serveur de gestion	RESTful API

Caméras, encodeurs et périphériques d'E/S (connexions entrantes)

Numéro de port	Protocole	Liaisons depuis...	But
80	TCP	Serveurs d'enregistrement et serveurs d'enregistrement de basculement	Authentification, configuration et flux de données ; vidéo et audio.
443	HTTPS	Serveurs d'enregistrement et serveurs d'enregistrement de basculement	Authentification, configuration et flux de données ; vidéo et audio.
554	RTSP	Serveurs d'enregistrement et serveurs d'enregistrement de basculement	Flux de données ; vidéo et audio.

Caméras, encodeurs et périphériques d'E/S (connexions sortantes)

Numéro de port	Protocole	Connexions à...	But
25	SMTP	Serveurs d'enregistrement et serveurs d'enregistrement de basculement	Envoi de notifications d'événements (obsolète).
5432	TCP	Serveurs d'enregistrement et serveurs d'enregistrement de basculement	Envoi de notifications d'événements. Le port est désactivé par défaut.
22337	HTTP	Serveur de journaux	Transfert des messages vers le serveur de journaux.

Seuls quelques modèles de caméras sont capables d'établir des connexions sortantes.

Composants clients (connexions sortantes)

Client intelligent MOBOTIX HUB, Client de gestion MOBOTIX HUB, Serveur mobile MOBOTIX HUB

Numéro de port	Protocole	Connexions à...	But
80	HTTP	Service de serveur de gestion	Authentification
443	HTTPS	Service de serveur de gestion	Authentification des utilisateurs de base.
7563	TCP	Service de serveur d'enregistrement	Récupération de flux vidéo et audio, commandes PTZ.
22331	TCP	Service de serveur d'événements	Alarmes.

Client Web MOBOTIX HUB, client mobile MOBOTIX HUB

Numéro de port	Protocole	Connexions à...	But
8081	HTTP	MOBOTIX HUB Serveur mobile	Récupération de flux vidéo et audio.
8082	HTTPS	MOBOTIX HUB Serveur mobile	Récupération de flux vidéo et audio.

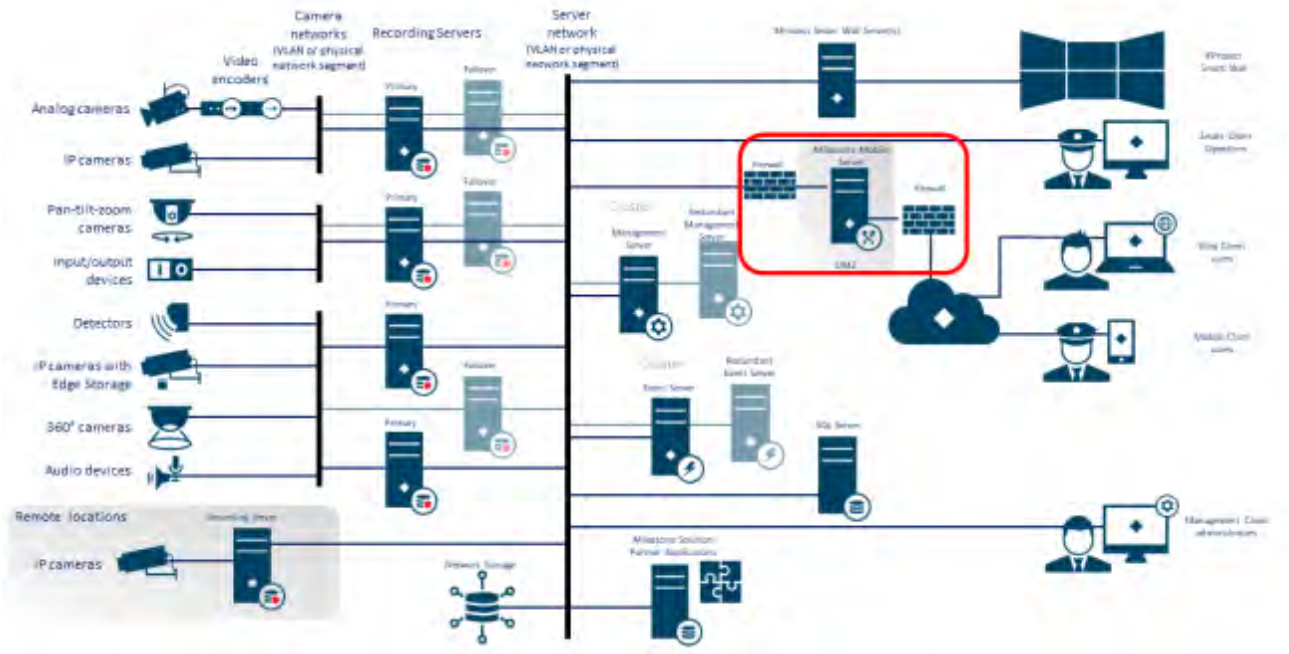
Pour en savoir plus

Les contrôles suivants fournissent des indications supplémentaires :

- NIST SP 800-53 Interconnexions de systèmes CA-3
- NIST SP 800-53 CM-6 Paramètres de configuration
- NIST SP 800-53 SC-7 Protection des limites

5.2.3 Utiliser un pare-feu entre le VMS et Internet

Le VMS ne doit pas se connecter directement à Internet. Si vous exposez des parties du VMS à Internet, MOBOTIX vous recommande d'utiliser un pare-feu correctement configuré entre le VMS et Internet.
Si possible, n'exposez que le composant du serveur MOBOTIX Mobile à Internet et localisez-le dans une zone démilitarisée (DMZ) avec des pare-feu des deux côtés. Ceci est illustré dans la figure suivante.



Pour en savoir plus

Les contrôles suivants fournissent des indications supplémentaires :

- NIST SP 800-53 Interconnexions de systèmes CA-3

5.2.4 Connectez le sous-réseau de la caméra au sous-réseau du serveur d'enregistrement uniquement

MOBOTIX vous recommande de connecter le sous-réseau de la caméra uniquement au sous-réseau du serveur d'enregistrement. Les caméras et autres appareils ne doivent communiquer qu'avec les serveurs d'enregistrement.
Pour plus d'informations, consultez Serveur d'enregistrement sur la page 62.

Pour en savoir plus

Les contrôles suivants fournissent des indications supplémentaires :

- NIST 800-53 SC-7 Protection des limites

5.3 Étapes avancées – Appareils

5.3.1 Utiliser le protocole Simple Network Management Protocol pour surveiller les événements

MOBOTIX vous recommande d'utiliser le protocole SNMP (Simple Network Management Protocol) pour surveiller les événements sur les appareils du réseau. Vous pouvez utiliser SNMP en complément de syslog. SNMP fonctionne en temps réel avec de nombreux types d'événements qui peuvent déclencher des alertes, par exemple si un périphérique est redémarré.

Pour que cela fonctionne, les appareils doivent prendre en charge la journalisation via SNMP.

Il existe plusieurs versions de protocoles SNMP disponibles. Les versions 2c et 3 sont les plus récentes. La mise en œuvre implique une série de normes. Vous trouverez un bon aperçu sur le site de référence SNMP (http://www.snmp.com/protocol/snmp_rfcs.shtml).

Pour en savoir plus

Les contrôles suivants fournissent des indications supplémentaires :

- NIST SP 800-53 SI-4 Surveillance des événements

5.4 Étapes avancées – Réseau

5.4.1 Utilisez des protocoles sans fil sécurisés

Si vous utilisez des réseaux sans fil, MOBOTIX vous recommande d'utiliser un protocole sans fil sécurisé pour empêcher tout accès non autorisé aux appareils et aux ordinateurs. Par exemple, utilisez des configurations standardisées. Les directives du NIST sur les réseaux locaux sans fil fournissent des détails spécifiques sur la gestion et la configuration du réseau. Pour plus d'informations, reportez-vous à *la SP 800-48 révision 1, Guide de sécurisation des réseaux sans fil IEEE 802.11* hérités (https://csrc.nist.gov/publications/detail/sp/800-48/rev-1/archive/2008-07-25).

De plus, MOBOTIX vous recommande de ne pas utiliser de caméras sans fil dans des endroits critiques. Les caméras sans fil sont faciles à brouiller, ce qui peut entraîner une perte de vidéo.

Pour en savoir plus

Les contrôles suivants fournissent des indications supplémentaires :

- NIST SP 800-53 AC-18 Accès sans fil
- NIST SP 800-53 SC-40 Protection de liaison sans fil

5.4.2 Utiliser le contrôle d'accès basé sur les ports

Utilisez le contrôle d'accès basé sur le port pour empêcher tout accès non autorisé au réseau de la caméra. Si un périphérique non autorisé se connecte à un port de commutateur ou de routeur, le port doit être bloqué. Des informations sur la configuration des commutateurs et des routeurs sont disponibles auprès des fabricants. Pour plus d'informations sur la gestion de la configuration des systèmes d'information, reportez-vous à la norme SP 800-128, Guide de gestion de la configuration des systèmes d'information https://csrc.nist.gov/publications/detail/sp/800-128/final axée sur la sécurité.

Pour en savoir plus

Les contrôles suivants fournissent des indications supplémentaires :

- NIST 800-53 CM-1 Politique et procédures de gestion de la configuration
- Configuration de base NIST 800-53 CM-2
- NIST 800-53 AC-4 Moindre privilège
- Paramètres de configuration du NIST 800-53 CM-6
- NIST 800-53 CM-7 Fonctionnalité minimale

5.4.3 Exécuter le VMS sur un réseau dédié

Dans la mesure du possible, MOBOTIX vous recommande de séparer le réseau sur lequel le VMS est exécuté des réseaux à d'autres fins. Par exemple, un réseau partagé tel que le réseau d'imprimantes doit être isolé du réseau VMS. En outre, les déploiements de MOBOTIX HUB VMS doivent suivre un ensemble général de bonnes pratiques pour les interconnexions système.

Pour en savoir plus

Les contrôles suivants fournissent des indications supplémentaires :

- NIST SP 800-53 Interconnexions de systèmes CA-3

6 Serveurs MOBOTIX

6.1 Étapes de base – Serveurs MOBOTIX

6.1.1 Utilisez des contrôles d'accès physiques et surveillez la salle des serveurs

MOBOTIX vous recommande de placer le matériel avec les serveurs installés dans une salle de serveurs désignée et d'utiliser des contrôles d'accès physiques. En outre, vous devez tenir des journaux d'accès pour documenter qui a eu un accès physique aux serveurs. La surveillance de la salle des serveurs est également une précaution préventive.
MOBOTIX prend en charge l'intégration des systèmes de contrôle d'accès et de leurs informations. Par exemple, vous pouvez consulter les journaux d'accès dans MOBOTIX HUB Smart Client.

Pour en savoir plus

Les contrôles suivants fournissent des indications supplémentaires :

- NIST 800-53 PE-3 Contrôle d'accès physique

6.1.2 Utilisez des canaux de communication cryptés

MOBOTIX vous recommande d'utiliser un VPN pour les canaux de communication pour les installations où les serveurs sont répartis sur des réseaux non fiables. Il s'agit d'empêcher les attaquants d'intercepter les communications entre les serveurs. Même pour les réseaux de confiance, MOBOTIX vous recommande d'utiliser HTTPS pour la configuration des caméras et autres composants du système.

Pour en savoir plus

Les contrôles suivants fournissent des indications supplémentaires :

- NIST 800-53 AC-4 Application de la circulation de l'information
- Accès à distance NIST 800-53 AC-17

6.2 Étapes avancées – Serveurs MOBOTIX

6.2.1 Exécuter des services avec des comptes de service

MOBOTIX vous recommande de créer des comptes de service pour les services liés aux machines virtuelles MOBOTIX HUB, au lieu d'utiliser un compte d'utilisateur standard. Configurez les comptes de service en tant qu'utilisateurs du domaine et donnez-leur uniquement les autorisations requises pour exécuter les services appropriés. Voir 4.1.11 Authentification Kerberos (expliquée). Par exemple, le compte de service ne doit pas être en mesure de se connecter au bureau Windows.

Pour en savoir plus

Les contrôles suivants fournissent des indications supplémentaires :

- NIST 800-53 AC-5 Séparation des tâches
- NIST 800-53 AC-6 Principe de moindre privilège

6.2.2 Exécuter des composants sur des serveurs virtuels ou physiques dédiés

MOBOTIX vous recommande d'exécuter les composants des MOBOTIX HUB VMS uniquement sur des serveurs virtuels ou physiques dédiés, sans qu'aucun autre logiciel ou service ne soit installé.

Pour en savoir plus

Les contrôles suivants fournissent des indications supplémentaires :

- Plan de gestion de la configuration NIST 800-53 CM-9

6.2.3 Restreindre l'utilisation des supports amovibles sur les ordinateurs et les serveurs

MOBOTIX vous recommande de limiter l'utilisation de supports amovibles, par exemple des clés USB, des cartes SD et des smartphones sur les ordinateurs et les serveurs où des composants de MOBOTIX HUB VMS sont installés. Cela permet d'empêcher les logiciels malveillants de pénétrer dans le réseau. Par exemple, n'autorisez que les utilisateurs autorisés à connecter des supports amovibles lorsque vous devez transférer des preuves vidéo.

Pour en savoir plus

Les contrôles suivants fournissent des indications supplémentaires :

- NIST 800-53 MP-7 Utilisation des supports

6.2.4 Utilisez des comptes d'administrateur individuels pour un meilleur audit

Contrairement aux comptes d'administrateur partagés, MOBOTIX recommande d'utiliser des comptes individuels pour les administrateurs. Cela vous permet de savoir qui fait quoi dans MOBOTIX HUB VMS. Cela permet d'empêcher les logiciels malveillants de pénétrer dans le réseau. Vous pouvez ensuite utiliser un répertoire faisant autorité, tel qu'Active Directory, pour gérer les comptes d'administrateur.
Vous attribuez des comptes d'administrateur à des rôles dans Management Client sous **Rôles**.

Pour en savoir plus

Les contrôles suivants fournissent des indications supplémentaires :

- NIST 800-53 AC-5 Séparation des tâches
- Plan de gestion de la configuration NIST 800-53 CM-9

6.2.5 Utiliser des sous-réseaux ou des VLAN pour limiter l'accès au serveur

MOBOTIX vous recommande de regrouper logiquement les différents types d'hôtes et d'utilisateurs dans des sous-réseaux distincts. Cela peut présenter des avantages dans la gestion des privilèges de ces hôtes et utilisateurs en

tant que membres d'un groupe avec une fonction ou un rôle donné. Concevez le réseau de manière à ce qu'il existe un sous-réseau ou un VLAN pour chaque fonction. Par exemple, un sous-réseau ou un VLAN pour les opérateurs de surveillance et un autre pour les administrateurs. Cela vous permet de définir des règles de pare-feu par groupe plutôt que pour des hôtes individuels.

Pour en savoir plus

Les contrôles suivants fournissent des indications supplémentaires :

- NIST SP 800-53 AC-2 Gestion de compte
- NIST SP 800-53 CSC 11 : Configurations sécurisées pour les périphériques réseau tels que les pare-feu, les routeurs et les commutateurs
- NIST SP 800-53 SC-7 Protection des limites

6.2.6 Activer uniquement les ports utilisés par Event Server

MOBOTIX vous recommande d'activer uniquement les ports utilisés par Event Server et de bloquer tous les autres ports, y compris les ports Windows par défaut.
Les ports de serveur d'événements utilisés dans les machines virtuelles Mobotix Hub sont les suivants : 22331, 22333, 9090, 1234 et 1235.

Les ports utilisés dépendent du déploiement. En cas de doute, contactez l'assistance MOBOTIX.

Pour en savoir plus

Les contrôles suivants fournissent des indications supplémentaires :

- NIST SP 800-53 CSC 11 : Configurations sécurisées pour les périphériques réseau tels que les pare-feu, les routeurs et les commutateurs

6.3 Serveur SQL

6.3.1 Connexion au serveur SQL et à la base de données

N'importe quelle chaîne de connexion SQL peut être spécifiée, y compris celle où l'authentification SQL est utilisée (nom d'utilisateur/mot de passe). Cela peut être utile lors des tests, car il ne nécessite pas d'accès à un AD. Toutefois, nous ne recommandons pas l'utilisation de l'authentification par nom d'utilisateur/mot de passe pour les configurations de production, car le nom d'utilisateur et le mot de passe sont conservés non chiffrés sur l'ordinateur. Pour les configurations de production, nous vous recommandons d'utiliser la sécurité intégrée.

La communication entre les machines virtuelles MOBOTIX MOBOTIX HUB et SQL Server et la base de données peut être altérée par un attaquant, car le certificat n'est pas validé.
Pour atténuer ce problème, vous devez d'abord configurer des certificats de serveur vérifiables. Une fois les certificats configurés, vous devez modifier ConnestionString dans le registre Windows en supprimant trustServerCertificate=true, comme suit :
Clé de registre : Computer\HKEY_LOCAL_MACHINE\SOFTWARE\VideoOS\Server\Common\ConnectionString

- Courant
  chaîne de connexion : Source de données=localhost ; initial catalog='Surveillance' ; Sécurité intégrée = SSPI ; encrypt=true ; trustServerCertificate=vrai
- Durci

chaîne de connexion : Source de données=localhost ; initial catalog='Surveillance' ; Sécurité intégrée = SSPI ; encrypt=true

Cela signifie que le chiffrement ne se produit que s'il existe un certificat de serveur vérifiable, sinon la tentative de connexion échoue.

Ce problème est décrit en détail dans l'article Utilisation du chiffrement sans validation.

6.3.2 Exécuter SQL Server et la base de données sur un serveur distinct

MOBOTIX vous recommande de rendre le serveur SQL et la base de données redondants. Cela réduit le risque de temps d'arrêt réel ou perçu.

Pour prendre en charge le clustering de basculement Windows Server (WSFC), MOBOTIX vous recommande d'exécuter le serveur SQL et la base de données sur un serveur distinct, et non sur le serveur de gestion.

SQL Server doit s'exécuter dans le programme d'installation WSFC, et les serveurs de gestion et d'événements doivent s'exécuter dans un système d'installation de cluster Microsoft (ou une technologie similaire). Pour plus d'informations sur WSFC, consultez *Clustering de basculement Windows Server (WSFC) avec SQL Server* (https://msdn.microsoft.com/en-us/library/hh270278.aspx).

Pour en savoir plus

Les contrôles suivants fournissent des indications supplémentaires :

- NIST 800-53 SC-7 Protection des limites
- Plan de gestion de la configuration NIST 800-53 CM-9

6.4 Serveur de gestion

6.4.1 Ajuster le délai d'expiration du jeton

MOBOTIX HUB VMS utilise des jetons de session lorsqu'il se connecte au serveur de gestion à l'aide des protocoles SSL (utilisateurs de base) ou NTLM (utilisateurs Windows). Un jeton est récupéré du serveur de gestion et utilisé sur les serveurs secondaires, par exemple le serveur d'enregistrement et parfois aussi le serveur d'événements. Cela permet d'éviter que la recherche NTLM et AD ne soit effectuée sur chaque composant du serveur.

Par défaut, un jeton est valide pendant 240 minutes. Vous pouvez l'ajuster à des intervalles de 1 minute. Cette valeur peut également être ajustée au fil du temps. Des intervalles courts augmentent la sécurité, cependant, le système génère une communication supplémentaire lorsqu'il renouvelle le jeton.

Le meilleur intervalle à utiliser dépend du déploiement. Cette communication augmente la charge du système et peut avoir un impact sur les performances.

Pour en savoir plus

Les contrôles suivants fournissent des indications supplémentaires :

- NIST SP 800-53 IA-5 Gestion de l'authentificateur

6.4.2 Activer uniquement les ports utilisés par le serveur d'administration

MOBOTIX vous recommande d'activer uniquement les ports utilisés par le serveur de gestion et de bloquer tous les autres ports, y compris les ports Windows par défaut. Ces instructions sont cohérentes pour les composants serveur des machines virtuelles MOBOTIX HUB.
Les ports du serveur de gestion utilisés dans les machines virtuelles Mobotix Hub sont les suivants : 80, 443, 1433, 7475, 8080, 8990, 9993, 12345.

Les ports utilisés dépendent du déploiement. En cas de doute, contactez l'assistance MOBOTIX.

Pour en savoir plus

Les contrôles suivants fournissent des indications supplémentaires :

- NIST SP 800-53 AC-2 Gestion de compte
- NIST SP 800-53 SC-7 Protection des limites

6.4.3 Désactiver les protocoles non sécurisés

Lorsqu'un utilisateur de base se connecte au serveur de gestion via IIS, le client de gestion utilise n'importe quel protocole disponible. MOBOTIX vous recommande de toujours mettre en œuvre la dernière version de TLS (Transport Layer Security, actuellement 1.2) (https://datatracker.ietf.org/wg/tls/charter/) et de désactiver toutes les suites de chiffrement incorrectes et les versions obsolètes des protocoles SSL/TLS. Effectuez des actions pour bloquer les protocoles non sécurisés au niveau du système d'exploitation. Cela empêche le client de gestion d'utiliser des protocoles qui ne sont pas sécurisés. Le système d'exploitation détermine le protocole à utiliser.

Les protocoles utilisés dépendent du déploiement. En cas de doute, contactez l'assistance MOBOTIX.

Pour en savoir plus

Les contrôles suivants fournissent des indications supplémentaires :

- Accès à distance NIST 800-53 AC-17 (désactivation des protocoles inutilisés)
- Paramètres de configuration du NIST 800-53 CM-6
- NIST 800-53 CM-7 Fonctionnalité minimale

6.4.4 Désactiver le canal de communication à distance hérité

La communication entre les serveurs d'enregistrement et le serveur de gestion est devenue plus sécurisée avec la solution mise en place en 2019 R2. Si vous effectuez une mise à niveau à partir d'une version précédente de MOBOTIX HUB VMS, le serveur de gestion démarre toujours la technologie 3rd party héritée pour pouvoir communiquer avec les serveurs d'enregistrement sur les versions plus anciennes.
Lorsque tous les serveurs d'enregistrement de votre système sont mis à niveau vers la version 2019 R2 ou ultérieure, vous pouvez configurer le serveur de gestion pour qu'il ne démarre pas le canal de communication à distance hérité, pour rendre votre système moins vulnérable, MOBOTIX vous recommande de définir **UseRemoting** sur **False** dans le fichier de configuration du serveur de gestion.

Pour en savoir plus

Les contrôles suivants fournissent des indications supplémentaires :

- Accès à distance NIST 800-53 AC-17 (désactivation des protocoles inutilisés)
- Paramètres de configuration du NIST 800-53 CM-6

6.4.5 Gérer les informations d'en-tête IIS

Désactiver les informations d'en-tête IIS

Pour des raisons de sécurité, MOBOTIX vous recommande de désactiver les en-têtes HTTP X-Powered-By et X-AspNet-Version.
L'en-tête HTTP X-Powered-By révèle la version d'IIS utilisée sur le serveur. Désactivez cet en-tête en procédant comme suit :

1. Ouvrez le Gestionnaire IIS.
2. Sélectionnez le site Web par défaut.
3. Sélectionnez En-têtes de réponse HTTP.
4. Sélectionnez l'en-tête HTTP X-Powered-By et sélectionnez Supprimer.

L'en-tête HTTP X-AspNet-Version révèle la version de ASP.NET utilisée par le pool d'applications Management Server. Désactivez cet en-tête en procédant comme suit :

1. Ouvrez le fichier web.config situé dans %windir %\Microsoft.NET\Framework\v4.0.30319\CONFIG.
2. Après la balise <system.web>, ajoutez ceci : <httpRuntime enableVersionHeader="false » />
3. Enregistrez le fichier.

La variable d'en-tête SERVER ne doit pas être supprimée, car elle entraînerait l'interruption de fonctionnalités du Serveur de gestion.

Définition des options X-Frame

Pour des raisons de sécurité, MOBOTIX vous recommande de définir les options X-Frame sur **refuser**.
Lorsque vous définissez l'en-tête HTTP X-Frame-Options sur deny, cela désactive le chargement de la page dans un cadre, quel que soit le site qui tente d'y accéder.
Modifiez cet en-tête en procédant comme suit :

1. Ouvrez le Gestionnaire IIS.
2. Sélectionnez le site Web par défaut > Installation.
3. Sélectionnez En-têtes de réponse HTTP.
4. Faites un clic droit et sélectionnez Ajouter... dans le menu
5. Dans le champ Nom, écrivez X-Frame-Options, et dans le champ Valeur, écrivez deny.

6.4.6 Désactiver les verbes IIS HTTP TRACE / TRACK

Pour des raisons de sécurité, MOBOTIX vous recommande de désactiver le verbe HTTP TRACE dans votre installation IIS. Désactivez le verbe HTTP TRACE en procédant comme suit :

1. Ouvrez le gestionnaire IIS.
2. Sélectionnez le site Web par défaut.
3. Double-cliquez sur Filtrage des demandes.

Si **le filtrage des requêtes** n'est pas disponible, installez-le en suivant les instructions ici : https://docs.microsoft.com/en-us/iis/configuration/system.webserver/security/requestfiltering/

4. Sélectionnez l'onglet Verbes HTTP.
5. Sélectionnez Refuser le verbe dans le menu Actions.
6. Tapez TRACE et cliquez sur OK.

7. Sélectionnez Refuser le verbe dans le menu Actions.
8. Tapez TRACK et cliquez sur OK.
9. Sélectionnez Refuser le verbe dans le menu Options.
10. Tapez OPTIONS et cliquez sur OK.

6.4.7 Désactiver la page par défaut IIS

Pour des raisons de sécurité, MOBOTIX vous recommande de désactiver la page par défaut IIS. Ce faisant, vous supprimez les informations qui pourraient être utilisées pour découvrir les technologies utilisées dans votre installation et vous vous alignez sur les meilleures pratiques IIS telles que définies par Microsoft. Désactivez la page par défaut en procédant comme suit :

1. Ouvrez le gestionnaire IIS.
2. Sélectionnez le site Web par défaut.
3. Double-cliquez sur Document par défaut.
4. Sélectionnez Désactiver dans le menu Actions.

6.5 Fournisseur d'identité

6.5.1 Désactiver les informations d'en-tête IIS sur le fournisseur d'identité

Pour des raisons de sécurité, MOBOTIX AG vous recommande de désactiver l'en-tête du serveur sur l'application Fournisseur d'identité .

L'en-tête du serveur décrit le logiciel utilisé par le serveur d'origine qui traite une requête. Désactivez cet en-tête en procédant comme suit.

Ceci ne s'applique qu'à IIS 10 et versions ultérieures.

1. Ouvrez le Gestionnaire IIS.
2. Sous le site Web par défaut, sélectionnez **IDP**.
3. Ouvrez l' **éditeur de configuration**.
4. Sélectionnez la section **system.webServer/security/requestFiltering**.
5. Définissez **removeServerHeader** sur **True**.

6.6 Serveur d'enregistrement

6.6.1 Propriétés des paramètres de stockage et d'enregistrement

Les fonctionnalités disponibles dépendent du système que vous utilisez. Voir https://www.mobotix.com/en/vms/mobotix-hub/levels pour plus d'informations.

Dans la boîte de dialogue **Paramètres de stockage et d'enregistrement**, spécifiez les éléments suivants :

Nom	Description
Nom	Renommez le stockage si nécessaire. Les noms doivent être uniques.

Nom	Description
Chemin	Spécifiez le chemin d'accès au répertoire dans lequel vous enregistrez les enregistrements dans ce stockage. Il n'est pas nécessaire que le stockage se trouve sur l'ordinateur du serveur d'enregistrement. Si le répertoire n'existe pas, vous pouvez le créer. Les lecteurs réseau doivent être spécifiés à l'aide du format UNC (Universal Naming Convention), par exemple : \\server\volume\directory\.
Temps de rétention	Spécifiez la durée pendant laquelle les enregistrements doivent rester dans l'archive avant d'être supprimés ou déplacés vers l'archive suivante (en fonction des paramètres d'archivage). La durée de conservation doit toujours être supérieure à celle de l'archive précédente ou de la base de données d'enregistrement par défaut. En effet, le nombre de jours de rétention spécifié pour une archive inclut toutes les périodes de conservation indiquées précédemment dans le processus.
Taille maximale	Sélectionnez le nombre maximal de gigaoctets de données d'enregistrement à enregistrer dans la base de données d'enregistrement. Les données d'enregistrement dépassant le nombre de gigaoctets spécifié sont automatiquement déplacées vers la première archive de la liste (le cas échéant) ou supprimées. Lorsque moins de 5 Go d'espace libre sont disponibles, le système archive toujours automatiquement (ou supprime si aucune archive suivante n'est définie) les données les plus anciennes d'une base de données. Si moins de 1 Go d'espace libre est disponible, les données sont supprimées. Une base de données nécessite toujours 250 Mo d'espace libre. Si vous atteignez cette limite (si les données ne sont pas supprimées assez rapidement), aucune autre donnée n'est écrite dans la base de données jusqu'à ce que vous ayez libéré suffisamment d'espace. La taille maximale réelle de votre base de données correspond à la quantité de gigaoctets que vous spécifiez, moins 5 Go.
Signature	Permet une signature numérique pour les enregistrements. Cela signifie, par exemple, que le système confirme que la vidéo exportée n'a pas été modifiée ou altérée lors de la lecture. Le système utilise l'algorithme SHA-2 pour la signature numérique.
Chiffrement	Sélectionnez le niveau de cryptage des enregistrements : • Aucun • Léger (moins d'utilisation du processeur) • Fort (plus d'utilisation du processeur) Le système utilise l'algorithme AES-256 pour le cryptage. Si vous sélectionnez **Lumière**, une partie de l'enregistrement est cryptée. Si vous sélectionnez Fort, l'ensemble de l'enregistrement est crypté. Si vous choisissez d'activer le chiffrement, vous devez également spécifier un mot de passe ci-dessous.
Mot de passe	Entrez un mot de passe pour les utilisateurs autorisés à afficher les données chiffrées. MOBOTIX vous recommande d'utiliser des mots de passe forts. Les mots de passe forts ne contiennent pas de mots qui peuvent être trouvés dans un dictionnaire ou qui font partie du nom de l'utilisateur. Il s'agit d'au moins huit caractères alphanumériques, de majuscules et de minuscules et de caractères spéciaux.

6.6.2 Utiliser des cartes d'interface réseau distinctes

MOBOTIX vous recommande d'utiliser plusieurs cartes d'interface réseau (NIC) pour séparer la communication entre les serveurs d'enregistrement et les appareils de la communication entre les serveurs d'enregistrement et les programmes clients. Les programmes clients n'ont pas besoin de communiquer directement avec les appareils.

Pour en savoir plus

Les contrôles suivants fournissent des indications supplémentaires :

- NIST SP 800-53 SC-7 Protection des limites

6.6.3 Renforcer le stockage en réseau (NAS) pour stocker les données multimédias enregistrées

Le serveur d'enregistrement peut utiliser le stockage en réseau (NAS) pour stocker les données multimédias enregistrées.
Si vous choisissez d'utiliser un NAS, il peut être renforcé à l'aide des améliorations de sécurité SMB 3.0, comme décrit dans ce document sur les améliorations de sécurité SMB.

6.7 Composant de serveur MOBOTIX Mobile

6.7.1 N'activez que les ports utilisés par le serveur MOBOTIX Mobile

MOBOTIX vous recommande d'activer uniquement les ports utilisés par le serveur MOBOTIX HUB Mobile et de bloquer tous les autres ports, y compris les ports Windows par défaut.
Par défaut, le serveur mobile utilise les ports 8081 et 8082.

Les ports utilisés dépendent du déploiement. En cas de doute, contactez l'assistance MOBOTIX.

Pour en savoir plus

Les contrôles suivants fournissent des indications supplémentaires :

- NIST SP 800-53 AC-2 Gestion de compte
- NIST SP 800-53 SC-7 Protection des limites

6.7.2 Utiliser une « zone démilitarisée » (DMZ) pour fournir un accès externe

MOBOTIX vous recommande d'installer le serveur MOBOTIX HUB Mobile dans une DMZ et sur un ordinateur doté de deux interfaces réseau :

- Un pour la communication interne
- Un pour l'accès public à Internet

Cela permet aux utilisateurs du client mobile de se connecter au serveur MOBOTIX Mobile avec une adresse IP publique, sans compromettre la sécurité ou la disponibilité du réseau VMS.

Pour en savoir plus

Les contrôles suivants fournissent des indications supplémentaires :

- NIST SP 800-53 SC-7 Protection des limites

6.7.3 Désactiver les protocoles non sécurisés

MOBOTIX vous recommande de n'utiliser que les protocoles nécessaires et uniquement les versions les plus récentes. Par exemple, implémentez la dernière version de TLS (Transport Layer Security, actuellement 1.2) et désactivez toutes les autres suites de chiffrement et les versions obsolètes des protocoles SSL/TLS. Cela nécessite la configuration de Windows et d'autres composants du système, ainsi que l'utilisation correcte des certificats et des clés numériques.

La même recommandation est donnée pour le serveur de gestion. Pour plus d'informations, consultez Désactiver les protocoles non sécurisés sur la page 60.

Pour en savoir plus

Les contrôles suivants fournissent des indications supplémentaires :

- Accès à distance NIST 800-53 AC-17 (désactivation des protocoles inutilisés)
- Paramètres de configuration du NIST 800-53 CM-6
- NIST 800-53 CM-7 Fonctionnalité minimale

6.7.4 Configurer les utilisateurs pour la vérification en deux étapes par e-mail

Les fonctionnalités disponibles dépendent du système que vous utilisez. Voir https://www.mobotix.com/en/vms/mobotix-hub/levels pour plus d'informations.

Pour imposer une étape de connexion supplémentaire aux utilisateurs du client MOBOTIX HUB Mobile ou du client Web MOBOTIX HUB, configurez la vérification en deux étapes sur le serveur MOBOTIX HUB Mobile. En plus du nom d'utilisateur et du mot de passe standard, l'utilisateur doit saisir un code de vérification reçu par e-mail.

La vérification en deux étapes augmente le niveau de protection de votre système de surveillance.

Exigences

- Vous avez installé un serveur SMTP.
- Vous avez ajouté des utilisateurs et des groupes à votre système MOBOTIX HUB dans le client de gestion sur le nœud Rôles du volet de navigation du site. Sur le rôle approprié, sélectionnez l'onglet Utilisateurs et groupes.
- Si vous avez mis à niveau votre système à partir d'une version précédente de MOBOTIX HUB, vous devez redémarrer le serveur mobile pour activer la fonction de vérification en deux étapes.

Dans le client de gestion ou l'application de gestion, procédez comme suit :

1. Entrez des informations sur votre serveur SMTP.
2. Spécifiez les paramètres du code de vérification qui sera envoyé aux utilisateurs clients.
3. Attribuez une méthode de connexion aux utilisateurs et aux groupes de domaines.

Cette rubrique décrit chacune de ces étapes.

Entrez des informations sur votre serveur SMTP

Le fournisseur utilise les informations relatives au serveur SMTP :

1. Dans le volet de navigation, sélectionnez Serveurs mobiles, puis le serveur mobile approprié.
2. Sous l'onglet Vérification en deux étapes, cochez la case Activer la vérification en deux étapes.

3. Sous Paramètres du fournisseur, sous l'onglet E-mail, entrez des informations sur votre serveur SMTP et spécifiez l'e-mail que le système enverra aux utilisateurs clients lorsqu'ils se connecteront et seront configurés pour une connexion secondaire. Pour plus de détails sur chaque paramètre, voir l'onglet Vérification en deux étapes sur la page 66.

Spécifiez le code de vérification qui sera envoyé aux utilisateurs

Pour spécifier la complexité du code de vérification :

1. Dans l'onglet Vérification en deux étapes, dans la section Paramètres du code de vérification, spécifiez la période pendant laquelle les utilisateurs du client MOBOTIX Mobile ou du client Web MOBOTIX HUB n'ont pas à revérifier leur connexion en cas, par exemple, d'un réseau déconnecté. La période par défaut est de 3 minutes.
2. Spécifiez la période pendant laquelle l'utilisateur peut utiliser le code de vérification reçu. Passé ce délai, le code n'est pas valide et l'utilisateur doit demander un nouveau code. La période par défaut est de 5 minutes.
3. Spécifiez le nombre maximal de tentatives de saisie de code, avant que l'utilisateur ne soit bloqué. Le nombre par défaut est 3.
4. Spécifiez le nombre de caractères du code. La longueur par défaut est de 6.
5. Spécifiez la complexité du code que vous souhaitez que le système compose.

Attribuer une méthode de connexion aux utilisateurs et aux groupes Active Directory

Dans l' onglet **Vérification en deux étapes**, dans la section **Paramètres utilisateur**, la liste des utilisateurs et des groupes ajoutés à votre système MOBOTIX HUB s'affiche.

1. Dans la colonne Méthode de connexion, choisissez entre aucune connexion, aucune vérification en deux étapes ou méthode de livraison des codes.
2. Dans le champ Détails, ajoutez les détails de la livraison, tels que les adresses e-mail de chaque utilisateur. La prochaine fois que l'utilisateur se connectera au client Web MOBOTIX HUB ou au client mobile MOBOTIX HUB, il lui sera demandé de se connecter secondairement.
3. Si un groupe est configuré dans Active Directory, le serveur mobile utilise les détails, tels que les adresses e-mail, d'Active Directory.
4. Les groupes Windows ne prennent pas en charge la vérification en deux étapes.
5. Enregistrez votre configuration.

Vous avez terminé les étapes de configuration de vos utilisateurs pour la vérification en deux étapes par e-mail.

Onglet de vérification en deux étapes

Les fonctionnalités disponibles dépendent du système que vous utilisez. Voir https://www.mobotix.com/en/vms/mobotix-hub/levels pour plus d'informations.

Utilisez l' onglet **Vérification en deux étapes** pour activer et spécifier une étape de connexion supplémentaire sur les utilisateurs de :

- L'application mobile MOBOTIX HUB sur leurs appareils mobiles iOS ou Android
- MOBOTIX HUB Web Client

Le premier type de vérification est un mot de passe. Le deuxième type est un code de vérification, que vous pouvez configurer pour qu'il soit envoyé à l'utilisateur par e-mail.

Pour plus d'informations, consultez Configurer les utilisateurs pour la vérification en deux étapes par e-mail sur la page 65.

Les tableaux suivants décrivent les paramètres de cet onglet.

Paramètres du fournisseur > E-mail

Nom	Description
Serveur SMTP	Entrez l'adresse IP ou le nom d'hôte du serveur SMTP (Simple Mail Transfer Protocol) pour les e-mails de vérification en deux étapes.
Port du serveur SMTP	Spécifiez le port du serveur SMTP pour l'envoi d'e-mails. Le numéro de port par défaut est 25 sans SSL et 465 avec SSL.
Utiliser SSL	Cochez cette case si votre serveur SMTP prend en charge le cryptage SSL.
Nom d'utilisateur	Spécifiez le nom d'utilisateur pour la connexion au serveur SMTP.
Mot de passe	Spécifiez le mot de passe pour la connexion au serveur SMTP.
Utiliser l'authentification par mot de passe sécurisé (SPA)	Cochez cette case si votre serveur SMTP prend en charge SPA.
Adresse e-mail de l'expéditeur	Spécifiez l'adresse e-mail pour l'envoi des codes de vérification.
Objet de l'e-mail	Spécifiez le titre de l'objet de l'e-mail. Exemple : Votre code de vérification en deux étapes.
Texte de l'e-mail	Entrez le message que vous souhaitez envoyer. Exemple : Votre code est {0}. Si vous oubliez d'inclure la variable {0}, le code est ajouté à la fin du texte par défaut.

Paramètres du code de vérification

Nom	Description
Délai de reconnexion (0 à 30 minutes)	Spécifiez la période pendant laquelle les utilisateurs du client MOBOTIX HUB Mobile n'ont pas à revérifier leur connexion en cas de, par exemple, un réseau déconnecté. Le point par défaut est de trois minutes. Ce paramètre ne s'applique pas au client Web MOBOTIX HUB.
Le code expire après (1 à 10 minutes)	Spécifiez la période pendant laquelle l'utilisateur peut utiliser le code de vérification reçu. Passé ce délai, le code n'est pas valide et l'utilisateur doit demander un nouveau code. La période par défaut est de cinq minutes.
Tentatives de saisie de code (1 à 10 tentatives)	Spécifiez le nombre maximal de tentatives de saisie de code avant que le code fourni ne devienne invalide. Le nombre par défaut est trois.
Longueur du code (4-6 caractères)	Spécifiez le nombre de caractères du code. La longueur par défaut est de six.
Composition du code	Spécifiez la complexité du code que vous souhaitez que le système génère. Vous pouvez choisir parmi : Majuscules latines (A-Z) Minuscules latines (a-z) Chiffres (0-9) Caractères spéciaux (!@#...)

Paramètres utilisateur

Nom	Description
Utilisateurs et groupes	Répertorie les utilisateurs et les groupes ajoutés au système MOBOTIX HUB. Si un groupe est configuré dans Active Directory, le serveur mobile utilise les détails, tels que les adresses e-mail, d'Active Directory. Les groupes Windows ne prennent pas en charge la vérification en deux étapes.
Méthode de vérification	Sélectionnez un paramètre de vérification pour chaque utilisateur ou groupe. Vous pouvez choisir parmi : Pas de connexion : l'utilisateur ne peut pas se connecter Pas de vérification en deux étapes : l'utilisateur doit saisir son nom d'utilisateur et son mot de passe E-mail : l'utilisateur doit saisir un code de vérification en plus du nom d'utilisateur et du mot de passe
Détails de l'utilisateur	Entrez l'adresse e-mail à laquelle chaque utilisateur recevra les codes.

6.7.5 Configurer la stratégie de sécurité du contenu (CSP)

Les WebSockets avec des caractères génériques doivent être supprimés des en-têtes CSP sur le serveur mobile. À l'heure actuelle, les ws://*:* et wss://*:* ne peuvent pas être supprimés du fournisseur de services de configuration décrit dans Configuration du serveur mobile en raison des limitations du navigateur Safari.
Pour renforcer la sécurité de votre serveur mobile, procédez comme suit :

1. Ouvrez le fichier VideoOS.MobileServer.Service.exe.config, qui se trouve dans le dossier d'installation du serveur mobile.
2. Modifiez la section <HttpHeaders> où la valeur de key="Content-Security-Policy » comme suit :
   - Si la prise en charge du navigateur Safari n'est pas nécessaire, supprimez ws://*:* et wss://*:* de l'en-tête.
   - Si la prise en charge du navigateur Safari est requise, remplacez ws://*:* et wss://*:* par les valeurs appropriées « ws:// [nom d'hôte] :[port] et wss://[nom d'hôte] :[port] », où le nom d'hôte et le port sont les valeurs pertinentes utilisées pour accéder au serveur mobile.
3. Redémarrez le serveur mobile.

6.8 Serveur de journaux

6.8.1 Installer le serveur de journaux sur un serveur distinct avec SQL Server

Pour les systèmes de très grande taille avec de nombreuses transactions vers et depuis la base de données SQL du serveur de journaux, MOBOTIX recommande d'installer le composant Log Server sur un serveur distinct avec son propre serveur SQL et de stocker les journaux dans une base de données SQL sur ce serveur SQL local. Si le serveur de journaux est affecté par des problèmes de performances, par exemple en raison d'une saturation ou d'autres raisons, et qu'il utilise le même serveur SQL Server que le serveur de gestion, les deux services peuvent être affectés.

Pour en savoir plus

Les contrôles suivants fournissent des indications supplémentaires :

- NIST SP 800-53 SC-7 Protection des limites
- Plan de gestion de la configuration NIST SP 800-53 CM-9

6.8.2 Limiter l'accès IP au serveur de journaux

MOBOTIX recommande que seuls les composants VMS puissent contacter le serveur de journaux.Le serveur de journaux utilise le port 22337.

Pour en savoir plus

Les contrôles suivants fournissent des indications supplémentaires :

- Paramètres de configuration du NIST 800-53 CM-6
- NIST 800-53 CM-7 Fonctionnalité minimale

7 Programmes clients

Cette section fournit des conseils sur la façon de protéger les programmes clients MOBOTIX.

Les programmes clients sont les suivants :

- Client intelligent MOBOTIX HUB
- MOBOTIX HUB Web Client
- Client de gestion MOBOTIX HUB
- Client mobile MOBOTIX

7.1 Étapes de base (tous les programmes clients)

7.1.1 Utiliser des utilisateurs Windows avec AD

Dans la mesure du possible, MOBOTIX vous recommande d'utiliser les utilisateurs Windows en combinaison avec Active Directory (AD) pour vous connecter au VMS avec les programmes clients. Cela vous permet d'appliquer une politique de mot de passe et d'appliquer les paramètres utilisateur de manière cohérente sur l'ensemble du domaine et du réseau. Il offre également une protection contre les attaques par force brute. Pour plus d'informations, consultez Utiliser des utilisateurs Windows avec Active Directory.

Pour en savoir plus

Les contrôles suivants fournissent des indications supplémentaires :

- Paramètres de configuration du NIST 800-53 CM-6
- Documentation du système d'information NIST 800-53 SA-5
- Fiabilité NIST 800-53 SA-13

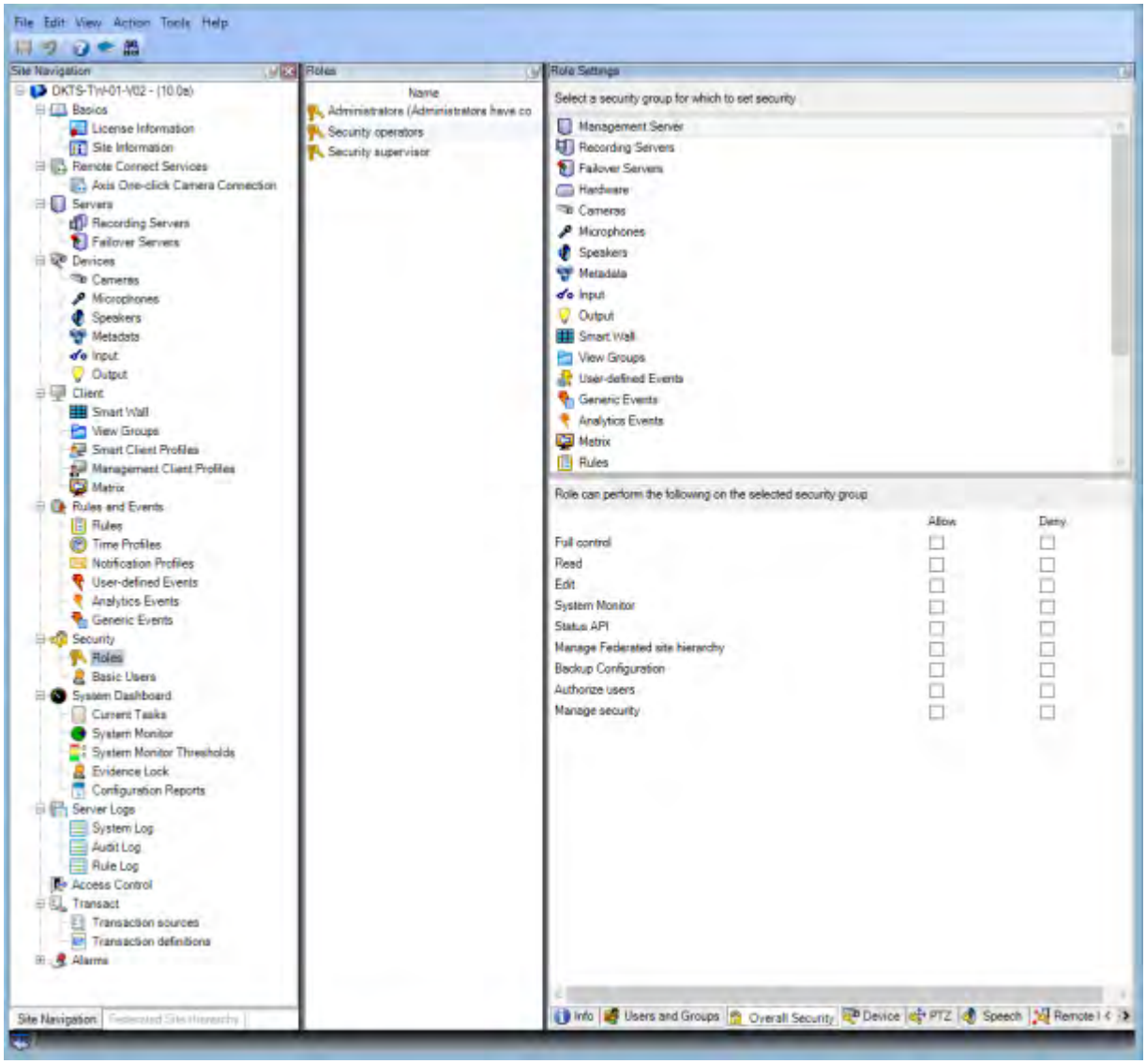
7.1.2 Restreindre les autorisations pour les utilisateurs clients

MOBOTIX recommande aux administrateurs de spécifier ce que les utilisateurs peuvent faire dans Management Client ou MOBOTIX HUB Smart Client.

Les instructions suivantes décrivent comment procéder.

Pour restreindre les autorisations des utilisateurs du client, procédez comme suit :

1. Ouvrez Management Client.
2. Développez le nœud Sécurité, sélectionnez Rôles, puis sélectionnez le rôle auquel l'utilisateur est associé.
3. Dans les onglets en bas, vous pouvez définir des autorisations et des restrictions pour le rôle.



Par défaut, tous les utilisateurs associés au rôle Administrateur disposent d'un accès illimité au système. Cela inclut les utilisateurs associés au rôle Administrateur dans AD ainsi que ceux ayant le rôle d'administrateur sur le serveur de gestion.

Pour en savoir plus

Les documents suivants fournissent des informations supplémentaires :

- NIST 800-53 AC-4 Moindre privilège
- Paramètres de configuration du NIST 800-53 CM-6
- NIST 800-53 CM-7 Fonctionnalité minimale

7.1.3 Exécutez toujours les clients sur du matériel de confiance sur des réseaux de confiance

MOBOTIX vous recommande de toujours exécuter les clients MOBOTIX HUB sur des périphériques matériels dotés des paramètres de sécurité appropriés. Des instructions spécifiques pour les appareils mobiles sont disponibles dans la SP 800-124 (https://csrc.nist.gov/publications/detail/sp/800-124/rev-1/final). Ces paramètres sont spécifiques à l'appareil.

Pour en savoir plus

Les contrôles suivants fournissent des indications supplémentaires :

- NIST SP 800-53 SC-7 Protection des limites
- NIST SP800-53 CM-6 Paramètres de configuration

7.2 Étapes avancées – MOBOTIX HUB Smart Client

7.2.1 Limitez l'accès physique à tout ordinateur exécutant MOBOTIX HUB Smart Client

MOBOTIX vous recommande de restreindre l'accès physique aux ordinateurs exécutant MOBOTIX HUB Smart Client. N'autorisez que le personnel autorisé à accéder aux ordinateurs. Par exemple, gardez la porte verrouillée et utilisez des contrôles d'accès et une surveillance.

Pour en savoir plus

Les contrôles suivants fournissent des indications supplémentaires :

- NIST SP 800-53 PE-1 Politique et procédures de protection physique et environnementale
- NIST SP 800-53 PE-2 Autorisations d'accès physique
- NIST SP 800-53 PE-3 Contrôle d'accès physique
- NIST SP 800-53 PE-6 Surveillance de l'accès physique

7.2.2 Utilisez toujours une connexion sécurisée par défaut, en particulier sur les réseaux publics

Si vous avez besoin d'accéder au VMS avec MOBOTIX HUB Smart Client via un réseau public ou non fiable, MOBOTIX vous recommande d'utiliser une connexion sécurisée via VPN. Cela permet de garantir la protection de la communication entre MOBOTIX HUB Smart Client et le serveur VMS.

Pour en savoir plus

Les contrôles suivants fournissent des indications supplémentaires :

- NIST SP 800-53 AC-2 Gestion de compte
- Accès à distance NIST SP 800-53 AC-17
- NIST SP 800-53 CM-6 Paramètres de configuration

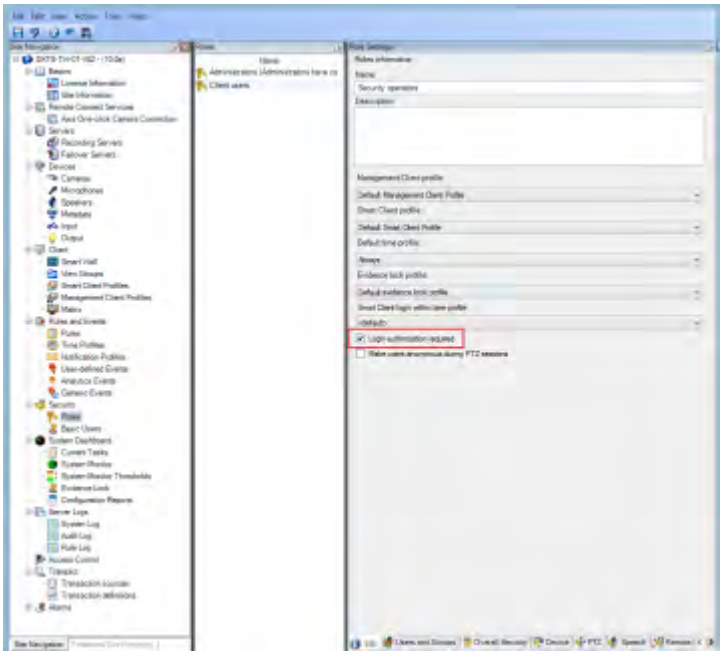
7.2.3 Activer l'autorisation de connexion

L'autorisation de connexion nécessite qu'un utilisateur se connecte sur MOBOTIX HUB Smart Client ou Management Client, et qu'un autre utilisateur ayant un statut élevé, tel qu'un superviseur, fournisse l'approbation. Vous configurez l'autorisation de connexion sur les rôles. Les utilisateurs associés au rôle sont invités à demander à un deuxième utilisateur (un superviseur) d'autoriser leur accès au système.

L'autorisation de connexion n'est actuellement pas prise en charge par le client mobile, le client Web MOBOTIX HUB et les intégrations du SDK MOBOTIX Integration Platform (MIP).

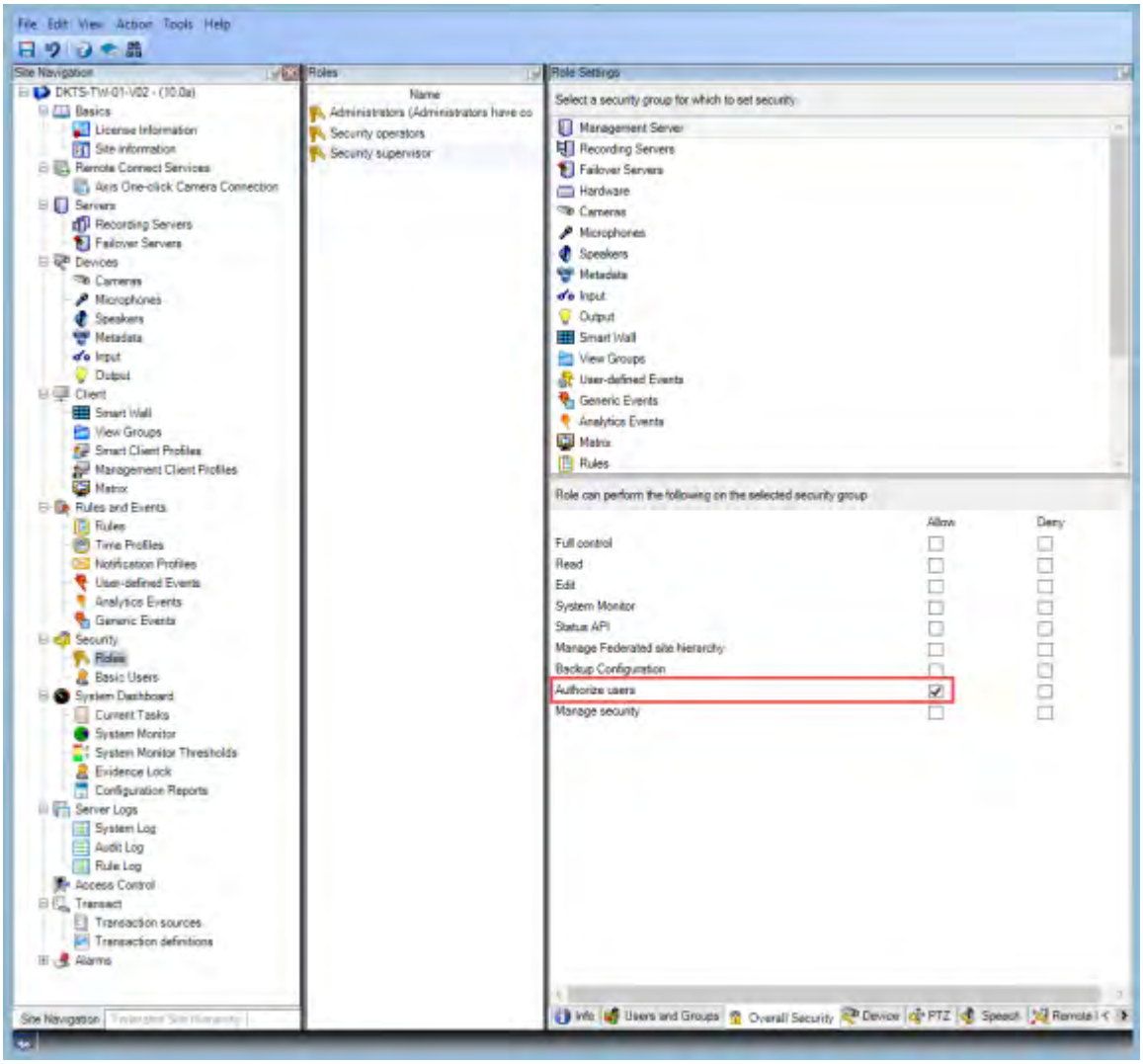
Pour activer l'autorisation de connexion pour un rôle, procédez comme suit :

1. Ouvrez Management Client.
2. Développez le nœud Sécurité, sélectionnez Rôles, puis sélectionnez le rôle approprié.
   Cochez la case **Autorisation de connexion requise**.



Pour configurer les rôles qui autorisent et accordent l'accès, procédez comme suit :

1. Pour créer un nouveau rôle, par exemple « Superviseur de sécurité », développez le nœud Sécurité, cliquez avec le bouton droit sur Rôles et créez un nouveau rôle.
2. Cliquez sur l'onglet Sécurité globale, puis sélectionnez le nœud Serveur de gestion.
   Cochez la case **Autoriser** en regard de la case **à cocher Autoriser les utilisateurs**.



Pour en savoir plus

Les contrôles suivants fournissent des indications supplémentaires :

- NIST SP 800-53 AC-2 Gestion de compte
- NIST SP 800-53 AC-6 Moindre privilège
- Accès à distance NIST SP 800-53 AC-17
- NIST SP 800-53 CM-6 Paramètres de configuration

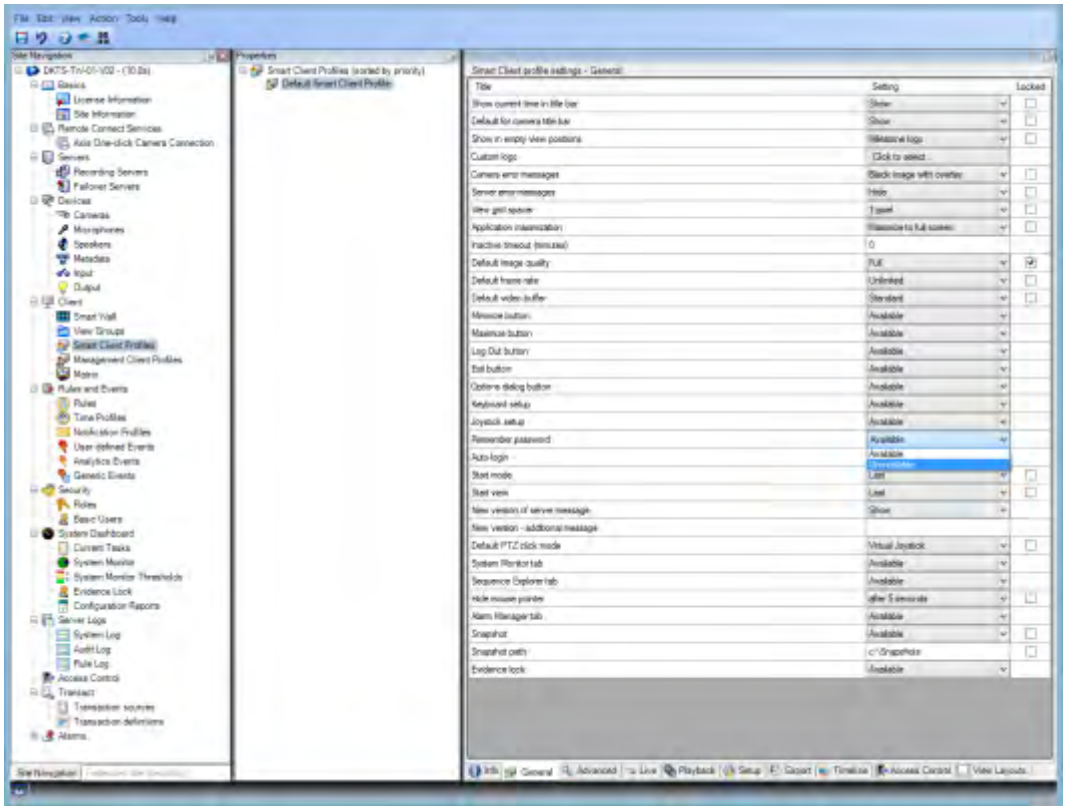
7.2.4 Ne pas stocker les mots de passe

MOBOTIX HUB Smart Client offre la possibilité aux utilisateurs de mémoriser leurs mots de passe. Pour réduire le risque d'accès non autorisé, MOBOTIX vous recommande de ne pas utiliser cette fonctionnalité.

Pour désactiver la fonction de mémorisation du mot de passe, procédez comme suit :

1. Ouvrez Management Client.
2. Développez le nœud Client, sélectionnez Profils Smart Client, puis sélectionnez le profil Smart Client approprié.
3. Dans la liste Mémoriser le mot de passe, sélectionnez Non disponible.

L'option Mémoriser **le mot de passe** n'est pas disponible la prochaine fois qu'un utilisateur disposant de ce profil se connecte à MOBOTIX HUB Smart Client.



Pour en savoir plus

Les contrôles suivants fournissent des indications supplémentaires :

- NIST SP 800-53 AC-2 Gestion de compte
- NIST SP 800-53 CM-6 Paramètres de configuration
- NIST SP 800-53 IA-1 Politique et procédures d'identification et d'authentification

7.2.5 Activer uniquement les fonctionnalités client requises

N'activez que les fonctionnalités requises et désactivez les fonctionnalités dont un opérateur de surveillance n'a pas besoin. Il s'agit de limiter les possibilités d'utilisation abusive ou d'erreurs.

Vous pouvez activer et désactiver des fonctionnalités dans MOBOTIX HUB Smart Client et dans MOBOTIX HUB Management Client.

Dans Management Client, configurez les profils Smart Client pour spécifier des ensembles d'autorisations pour les utilisateurs qui sont affectés au profil. Les profils Smart Client sont similaires aux profils Management Client, et le même utilisateur peut être affecté à chaque type de profil.

Pour configurer un profil Smart Client, procédez comme suit :

1. Ouvrez Management Client.
2. Développez le nœud Client, sélectionnez Profils Smart Client, puis sélectionnez le profil Smart Client approprié.
3. Utilisez les onglets pour spécifier les paramètres des fonctionnalités dans Smart Client. Par exemple, utilisez les paramètres de l'onglet Lecture pour contrôler les fonctionnalités utilisées pour examiner la vidéo enregistrée.

Avant d'attribuer un utilisateur à un profil Smart Client, assurez-vous que les autorisations pour le rôle de l'utilisateur sont appropriées pour le profil. Par exemple, si vous souhaitez qu'un utilisateur puisse examiner la vidéo, assurez-vous que le rôle lui permet de lire la vidéo à partir de caméras et que l'onglet Explorateur de séquences est disponible sur le profil Smart Client.

Pour en savoir plus

Les contrôles suivants fournissent des indications supplémentaires :

- NIST SP 800-53 AC-2 Gestion de compte
- NIST SP 800-53 AC-6 Moindre privilège
- NIST SP 800-53 CM-6 Paramètres de configuration

7.2.6 Utiliser des noms distincts pour les comptes d'utilisateur

MOBOTIX vous recommande de créer un compte utilisateur pour chaque utilisateur et d'utiliser une convention de nommage qui facilite l'identification personnelle de l'utilisateur, comme son nom ou ses initiales. Il s'agit d'une bonne pratique pour limiter l'accès à ce qui est nécessaire, et elle réduit également la confusion lors de l'audit.

Pour en savoir plus

Les contrôles suivants fournissent des indications supplémentaires :

- NIST 800-53 AC-4 Moindre privilège
- NIST 800-53 CM-1 Politique et procédures de gestion de la configuration
- Configuration de base NIST 800-53 CM-2
- Paramètres de configuration du NIST 800-53 CM-6
- NIST 800-53 CM-7 Fonctionnalité minimale

7.2.7 Interdire l'utilisation de supports amovibles

Pour les exportations de vidéos, établissez une chaîne de procédures spécifiques aux preuves. MOBOTIX recommande que la politique de sécurité n'autorise que les opérateurs autorisés de MOBOTIX HUB Smart Client à connecter des périphériques de stockage amovibles tels que des clés USB, des cartes SD et des smartphones à l'ordinateur sur lequel MOBOTIX HUB Smart Client est installé.
Les supports amovibles peuvent transférer des logiciels malveillants sur le réseau et soumettre la vidéo à une distribution non autorisée.
La stratégie de sécurité peut également spécifier que les utilisateurs ne peuvent exporter des preuves que vers un emplacement spécifique sur le réseau ou vers un graveur de média uniquement. Vous pouvez contrôler cela via le profil Smart Client.

Pour en savoir plus

Les contrôles suivants fournissent des indications supplémentaires :

- NIST SO 800-53 MP-7 Utilisation des supports
- Protection contre les codes malveillants NIST SP 800-53 SI-3

7.3 Étapes avancées – Client MOBOTIX Mobile

La PS 800-124 révision 1 (http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-124r1.pdf) fournit des conseils spécifiques aux appareils mobiles. Les informations qu'il contient s'appliquent à toutes les rubriques de cette section.

7.3.1 Utilisez toujours le client MOBOTIX Mobile sur des appareils sécurisés

MOBOTIX vous recommande de toujours utiliser le client MOBOTIX HUB Mobile sur des appareils sécurisés qui sont configurés et entretenus conformément à une politique de sécurité. Par exemple, assurez-vous que les appareils mobiles ne permettent pas aux utilisateurs d'installer des logiciels provenant de sources non autorisées. Un magasin d'applications d'entreprise est un exemple de moyen de limiter les applications d'appareil dans le cadre de la gestion globale des appareils mobiles.

Pour en savoir plus

Les contrôles suivants fournissent des indications supplémentaires :

- NIST SP 800-53 SC-7 Protection des limites
- NIST SP800-53 CM-6 Paramètres de configuration

7.3.2 Téléchargez le client MOBOTIX Mobile à partir de sources autorisées

MOBOTIX vous recommande de télécharger le client MOBOTIX HUB Mobile à partir de l'une des sources suivantes :

- Google Play Store
- App Store d'Apple
- Microsoft Windows Store.

Pour en savoir plus

Les contrôles suivants fournissent des indications supplémentaires :

- NIST SP 800-53 SC-7 Protection des limites
- NIST SP 800-53 CM-6 Paramètres de configuration

7.3.3 Les appareils mobiles doivent être sécurisés

Si vous souhaitez accéder au VMS avec un appareil mobile via un réseau public ou non fiable, MOBOTIX vous recommande de le faire avec une connexion sécurisée, d'utiliser une authentification appropriée et TLS (https://datatracker.ietf.org/wg/tls/charter/) (ou de vous connecter via VPN (https://datatracker.ietf.org/wg/ipsec/documents/)) et HTTPS. Cela permet de protéger les communications entre l'appareil mobile et le VMS.

MOBOTIX recommande aux appareils mobiles d'utiliser le verrouillage de l'écran. Cela permet d'empêcher tout accès non autorisé au VMS, par exemple, en cas de perte du smartphone. Pour une sécurité maximale, mettez en œuvre une politique de sécurité interdisant au client MOBOTIX HUB Mobile de se souvenir du nom d'utilisateur et du mot de passe.

Pour en savoir plus

Les contrôles suivants fournissent des indications supplémentaires :

- NIST SP 800-53 AC-2 Gestion de compte
- Accès à distance NIST SP 800-53 AC-17
- NIST SP 800-53 CM-6 Paramètres de configuration

7.4 Étapes avancées – MOBOTIX HUB Web Client

7.4.1 Exécutez toujours MOBOTIX HUB Web Client sur des ordinateurs clients de confiance

Connectez toujours en toute sécurité tous les composants du VMS. Les connexions de serveur à serveur et de client à serveur doivent utiliser l'authentification appropriée et le protocole TLS (Transport Layer Security) (https://datatracker.ietf.org/wg/tls/charter/) (ou se connecter via VPN (https://datatracker.ietf.org/wg/ipsec/documents/)) et HTTPS. Exécutez toujours MOBOTIX HUB Web Client sur des ordinateurs de confiance, par exemple, n'utilisez pas d'ordinateur client dans un espace public. MOBOTIX vous recommande d'informer les utilisateurs sur les mesures de sécurité à prendre en compte lors de l'utilisation d'applications basées sur un navigateur, telles que MOBOTIX HUB Web Client. Par exemple, assurez-vous qu'ils savent qu'ils doivent empêcher le navigateur de se souvenir de leur mot de passe.

Pour en savoir plus

Les contrôles suivants fournissent des indications supplémentaires :

- NIST SP 800-53 AC-2 Gestion de compte
- NIST SP 800-53 CM-6 Paramètres de configuration
- NIST SP 800-53 IA-2 Identification et authentification

7.4.2 Utilisez des certificats pour confirmer l'identité d'un serveur MOBOTIX Mobile

Ce document met l'accent sur l'utilisation de la dernière version de TLS. D'où la nécessité d'une utilisation correcte des certificats et de la mise en œuvre de la suite de chiffrement TLS. MOBOTIX vous recommande d'installer un certificat sur le serveur MOBOTIX HUB Mobile afin de confirmer l'identité du serveur lorsqu'un utilisateur tente de se connecter via le client Web MOBOTIX HUB.
Pour plus d'informations, consultez la *section Modifier le certificat* dans le manuel de l'*administrateur MOBOTIX HUB VMS*.

Pour en savoir plus

Les contrôles suivants fournissent des indications supplémentaires :

- NIST SP 800-53 AC-2 Gestion de compte
- NIST SP 800-53 CM-6 Paramètres de configuration
- NIST SP 800-53 IA-2 Identification et authentification

7.4.3 N'utilisez que des navigateurs pris en charge avec les dernières mises à jour de sécurité

MOBOTIX vous recommande d'installer un seul des navigateurs suivants sur les ordinateurs clients. Assurez-vous d'inclure les dernières mises à jour de sécurité.

- Apple Safari
- Google Chrome
- Bord Microsoft
- Mozilla Firefox

Pour en savoir plus

Les contrôles suivants fournissent des indications supplémentaires :

- NIST SP 800-53 CM-1 Politique et procédures de gestion de la configuration
- Configuration de base NIST SP 800-53 CM-2
- NIST SP 800-53 CM-6 Paramètres de configuration

- Architecture de sécurité de l'information NIST SP 800-53 PL-8
- Protection contre les codes malveillants NIST SP 800-53 SI-3

7.5 Étapes avancées – Client de gestion

7.5.1 Utiliser les profils du client de gestion pour limiter ce que les administrateurs peuvent afficher

MOBOTIX vous recommande d'utiliser les profils du client de gestion pour limiter ce que les administrateurs peuvent afficher dans le client de gestion.
Les profils Management Client permettent aux administrateurs système de modifier l'interface utilisateur du Client de gestion. Associez des profils client de gestion à des rôles pour limiter l'interface utilisateur afin de représenter les fonctionnalités disponibles pour chaque rôle d'administrateur.
Affichez uniquement les parties du VMS dont les administrateurs ont besoin pour effectuer leurs tâches.

Pour en savoir plus

Les contrôles suivants fournissent des indications supplémentaires :

- NIST 800-53 AC-4 Moindre privilège
- NIST 800-53 CM-1 Politique et procédures de gestion de la configuration
- Configuration de base NIST 800-53 CM-2
- Paramètres de configuration du NIST 800-53 CM-6
- NIST 800-53 CM-7 Fonctionnalité minimale

7.5.2 Autoriser les administrateurs à accéder aux parties pertinentes du VMS

Si vous avez une configuration qui nécessite plusieurs administrateurs, MOBOTIX vous recommande de configurer des droits d'administrateur différents pour les administrateurs qui utilisent le client de gestion.
Pour définir les autorisations d'administrateur, procédez comme suit :

1. Dans Management Client, développez le nœud Sécurité, sélectionnez Rôles, puis sélectionnez le rôle d'administrateur approprié.
   Vous ne pouvez pas modifier le rôle d'administrateur intégré, vous devez donc créer des rôles d'administrateur supplémentaires.
2. Dans l'onglet Sécurité globale, spécifiez les actions que l'administrateur peut effectuer pour chaque groupe de sécurité.
3. Dans les autres onglets, spécifiez les paramètres de sécurité du rôle dans le VMS.
   Pour plus d'informations, consultez le manuel d'administration de MOBOTIX HUB VMS.
4. Sous l'onglet Infos, associez le rôle à un profil Client de gestion.

Vous pouvez activer ou désactiver des fonctionnalités à l'aide du profil Management Client. Avant d'attribuer un utilisateur à un profil Client de gestion, assurez-vous que les autorisations relatives au rôle de l'utilisateur sont appropriées pour le profil. Par exemple, si vous souhaitez qu'un utilisateur puisse gérer les caméras, assurez-vous que le rôle lui permet de le faire et que les caméras sont activées sur le profil du client de gestion.

Pour en savoir plus

- Les contrôles suivants fournissent des indications supplémentaires :
- NIST 800-53 AC-4 Moindre privilège
- NIST 800-53 CM-1 Politique et procédures de gestion de la configuration
- Configuration de base NIST 800-53 CM-2
- Paramètres de configuration du NIST 800-53 CM-6
- NIST 800-53 CM-7 Fonctionnalité minimale

7.5.3 Exécuter le client de gestion sur des réseaux fiables et sécurisés

Si vous accédez au Serveur de gestion avec Management Client via HTTP, la communication en texte brut peut contenir des détails système non chiffrés. MOBOTIX vous recommande d'exécuter le client de gestion uniquement sur des réseaux fiables et connus. Utilisez un VPN pour fournir un accès à distance.

Pour en savoir plus

Les contrôles suivants fournissent des indications supplémentaires :

- NIST SP 800-53 AC-2 Gestion de compte
- NIST SP 800-53 CM-6 Paramètres de configuration
- NIST SP 800-53 IA-2 Identification et authentification

8 Conformité

8.1 Conformité à la norme FIPS 140-2

Cette section traite de la norme FIPS 140-2 et de la configuration et de l'utilisation des machines virtuelles mobotix hub pour qu'elles fonctionnent en mode conforme à la norme FIPS 140-2.

Les termes « conforme à la norme FIPS 140-2 » et « mode conforme à la norme FIPS 140-2 » ne sont pas juridiquement contraignants. Les termes sont utilisés ici pour plus de clarté.

Conforme à la norme FIPS 140-2 signifie que le logiciel utilise des instances d'algorithmes et de fonctions de hachage validées par la norme FIPS 140-2 dans tous les cas où des données chiffrées ou hachées sont importées ou exportées à partir du logiciel. De plus, cela signifie que le logiciel gérera les clés de manière sécurisée, comme l'exigent les modules cryptographiques validés FIPS 140-2. Le processus de gestion des clés comprend également la génération et le stockage des clés.

Le mode conforme à la norme FIPS 140-2 fait référence aux logiciels qui contiennent à la fois des méthodes de sécurité approuvées par la norme FIPS et des méthodes non approuvées par la norme FIPS, lorsque le logiciel dispose d'au moins un « mode de fonctionnement FIPS ». Ce mode de fonctionnement ne permet d'utiliser que des méthodes de sécurité approuvées par la norme FIPS. Cela signifie que lorsque le logiciel est en « mode FIPS », une méthode non approuvée par FIPS n'est pas utilisée à la place de la méthode approuvée par FIPS.

Les sujets suivants sont abordés.

8.1.1 Qu'est-ce que FIPS ?

Les normes FIPS (Federal Information Processing Standards) sont une famille de normes élaborées par les deux organismes gouvernementaux suivants :

- Le National Institute of Standards and Technology (NIST) aux États-Unis
- Le Centre de la sécurité des télécommunications (CST) au Canada

Ces normes visent à assurer la sécurité informatique et l'interopérabilité.

Toutes les solutions logicielles déployées dans les secteurs gouvernementaux et hautement réglementés aux États-Unis et au Canada doivent être conformes à la norme FIPS 140-2.

8.1.2 Qu'est-ce que la norme FIPS 140-2 ?

La norme FIPS 140-2, intitulée « Exigences de sécurité pour les modules cryptographiques », spécifie les algorithmes de chiffrement et les algorithmes de hachage qui peuvent être utilisés, ainsi que la manière dont les clés de chiffrement doivent être générées et gérées.
Les exigences de sécurité spécifiées dans la présente norme visent à maintenir la sécurité fournie par un module cryptographique, mais la conformité à cette norme n'est pas suffisante pour garantir la sécurité d'un module particulier. L'exploitant d'un module cryptographique est responsable de s'assurer que la sécurité fournie par le module est suffisante et acceptable pour le propriétaire des informations protégées, et que tout risque résiduel est reconnu et accepté.

8.1.3 Quelles applications MOBOTIX HUB VMS peuvent fonctionner en mode conforme à la norme FIPS 140-2 ?

À partir de MOBOTIX HUB VMS 2020 R3, tous les algorithmes de chiffrement ont été remplacés par la cryptographie nouvelle génération (CNG) de Microsoft, qui adhère aux dernières technologies de sécurité disponibles et est conforme à la norme FIPS. Autrement dit, toutes les applications MOBOTIX HUB VMS 2020 R3 peuvent fonctionner en mode conforme à la norme FIPS.
Dans un souci de rétrocompatibilité, certains algorithmes et processus non conformes persistent dans les machines virtuelles Mobotix Hub, même après la version 2020 R3, mais cela n'affecte pas la capacité à faire fonctionner le système en mode conforme à la norme FIPS.

MOBOTIX HUB VMS est-il toujours conforme à la norme FIPS ?

Non. Certains algorithmes et processus non conformes persistent dans les machines virtuelles MOBOTIX HUB. Cependant, les MOBOTIX HUB VMS peuvent être configurés et exploités de manière à n'utiliser que les instances d'algorithme certifiées FIPS 140-2 et donc à fonctionner en mode conforme à la norme FIPS.

Devez-vous activer le mode FIPS 140-2 ?

Avant d'activer le mode FIPS 140–2, il est nécessaire de comprendre si vous en avez besoin ou non. Par exemple, si vous travaillez et que vous êtes connecté à un réseau et à une infrastructure du gouvernement américain ou canadien, il est obligatoire de se conformer à la norme FIPS 140-2 et de l'activer sur votre ordinateur pour la communication conformément à la norme. De plus, l'activation du mode FIPS 140-2 sur votre système d'exploitation Windows limite l'exécution de nombreux programmes et services, car seuls les algorithmes et services approuvés par FIPS seront pris en charge par la suite. Par conséquent, il est conseillé de vérifier s'il y a une nécessité ou non.

8.1.4 Comment s'assurer que les MOBOTIX HUB VMS peuvent fonctionner en mode conforme à la norme FIPS 140-2 ?

Pour utiliser MOBOTIX HUB VMS en mode FIPS 140-2, vous devez :

- Assurez-vous que les intégrations tierces peuvent fonctionner sur un système d'exploitation Windows compatible FIPS (voir Vérifier les intégrations tierces sur la page 84)
- Connectez-vous aux appareils de manière à garantir un mode de fonctionnement conforme à la norme FIPS 140-2 (voir Connecter des appareils : arrière-plan sur la page 84)

- Assurez-vous que les données de la base de données multimédia sont chiffrées à l'aide d'algorithmes conformes à la norme FIPS 140-2 (voir Base de données multimédia : considérations relatives à la compatibilité descendante sur la page 85)
- Exécutez le système d'exploitation Windows en mode de fonctionnement approuvé par la norme FIPS 140-2. Pour plus d'informations sur l'activation de FIPS, consultez le site Microsoft.

8.1.5 Considérations relatives à la mise à niveau

La mise à niveau vers MOBOTIX HUB VMS 2020 R3 pour fonctionner en mode conforme à la norme FIPS nécessite un processus de mise à niveau unique. Ce processus de mise à niveau n'est requis que par les utilisateurs existants de MOBOTIX HUB VMS qui doivent fonctionner en mode conforme à la norme FIPS.

Le processus de mise à niveau dépend de la version des machines virtuelles Mobotix Hub à partir de laquelle vous effectuez la mise à niveau.

Processus de mise à niveau recommandé pour les clients exécutant des machines virtuelles Mobotix Hub

1. Lancez l'enquête pour savoir si les intégrations tierces sont conformes à la norme FIPS 140-2 (voir Vérifier les intégrations tierces sur la page 84).
2. Préparez les connexions des appareils pour qu'elles soient conformes à la norme FIPS 140-2 (voir Connecter des appareils : contexte sur la page 84).
3. Exportez les enregistrements réalisés avec des versions de MOBOTIX HUB VMS antérieures à 2017 R2 (voir Base de données des médias : Considérations relatives à la rétrocompatibilité sur la page 85).
   Cela s'applique aux clients qui ont des enregistrements cryptés ou signés à un moment donné.
4. Désactivez FIPS sur le système d'exploitation Windows (voir Stratégie de groupe FIPS sur le système d'exploitation Windows sur la page 90).
5. Installez MOBOTIX HUB VMS2020 R3 (voir Installer MOBOTIX HUB VMS2020 R3 sur la page 90).
6. Mettez à niveau les enregistrements de la base de données de médias qui sont réalisés avec MOBOTIX HUB VMS 2019 R3 ou une version antérieure (voir Base de données de médias : Considérations relatives à la compatibilité descendante sur la page 85).
7. Mettez à jour le chiffrement des mots de passe de détection du matériel (voir Chiffrer les mots de passe de détection du matériel sur la page 90).
8. Activez FIPS sur le système d'exploitation Windows et redémarrez tous les ordinateurs sur lesquels MOBOTIX HUB VMS est installé.

N'activez pas FIPS tant que tous les ordinateurs du réseau MOBOTIX HUB VMS, y compris les postes de travail MOBOTIX HUB Smart Client, ne sont pas prêts pour FIPS.

8.1.6 Vérifier les intégrations tierces

Si une intégration n'est pas conforme à la norme FIPS 140-2, elle ne peut pas s'exécuter sur un système d'exploitation Windows avec l'indicateur de stratégie de groupe FIPS activé.
En outre, en raison des modifications apportées au SDK MIP par rapport à FIPS, les intégrations qui accèdent à la liste des fonctionnalités de la licence doivent être recompilées.
Afin de vous assurer que les intégrations fonctionneront toujours après la mise à niveau vers MOBOTIX HUB VMS 2020 R3, vous devez :

- Faites l'inventaire de toutes vos intégrations aux MOBOTIX HUB VMS
- Contactez les fournisseurs de ces intégrations et demandez-leur si elles sont conformes à la norme FIPS 140-2 et s'ils prévoient que les intégrations doivent être modifiées en raison des mises à jour du SDK MIP
- Déployez les intégrations conformes à la norme FIPS 140-2 sur les machines virtuelles Mobotix Hub après la mise à jour du VMS

8.1.7 Connecter des appareils : arrière-plan

Si vous souhaitez utiliser MOBOTIX HUB VMS en mode conforme à la norme FIPS, vous devez vous assurer que les pilotes, et donc la communication avec les appareils, sont également conformes à la norme FIPS.
Les pilotes de périphériques MOBOTIX MOBOTIX HUB VMS peuvent être conformes à la norme FIPS 140-2, car ils peuvent être configurés et fonctionner de manière à n'utiliser que des instances d'algorithme conformes à la norme FIPS 140-2. Seuls des pilotes spécifiques dans une configuration spécifique sont conformes à la norme FIPS 140-2. Dans cette configuration FIPS 140-2 spécifique, le pilote sera en mesure de communiquer avec les périphériques de manière conforme. Les appareils doivent remplir plusieurs conditions afin de pouvoir accepter cette communication. En outre, l'indicateur de stratégie de groupe FIPS doit être activé dans Windows sur le serveur sur lequel le serveur d'enregistrement est installé. Lorsque l'indicateur de stratégie de groupe FIPS est activé, les pilotes compatibles FIPS 140-2 fonctionnent en mode conforme et n'utilisent pas de primitives de chiffrement non approuvées. Les conducteurs utiliseront les algorithmes utilisés uniquement pour les canaux de communication sécurisés.

Exigences de connectivité de l'appareil

MOBOTIX HUB VMS est garanti et peut appliquer le mode de fonctionnement conforme à la norme FIPS 140-2 si les critères suivants sont remplis :

- Les périphériques utilisent uniquement les pilotes de la liste (Pilotes pris en charge sur la page 92) pour se connecter à MOBOTIX HUB VMS
  Cette liste répertorie les pilotes qui peuvent assurer et faire respecter la conformité.
- Les appareils utilisent la version 11.1 ou ultérieure du pack d'appareils
  Les pilotes des packs de périphériques de pilotes hérités ne peuvent pas garantir une connexion conforme à la norme FIPS 140-2.
- Les appareils sont connectés via HTTPS et sur le protocole SRTP (Secure Real-Time Transport Protocol) ou le protocole RTSP (Real Time Streaming Protocol) sur HTTPS pour le flux vidéo

Les modules de pilote ne peuvent pas garantir la conformité FIPS 140-2 d'une connexion via HTTP. La connexion peut être conforme, mais il n'y a aucune garantie qu'elle soit effectivement conforme.

- L'indicateur de stratégie de groupe FIPS doit être activé dans Windows sur l'ordinateur qui exécute le serveur d'enregistrement

Effets du fonctionnement en mode conforme à la norme FIPS 140-2

En mode conforme à la norme FIPS 140-2, certains pilotes ne peuvent pas être utilisés. Les pilotes répertoriés comme FIPS 140-2 peuvent ne pas être en mesure de se connecter à des périphériques qui ne répondent pas aux exigences du périphérique.

Un pilote est conforme à la norme FIPS 140-2 et la communication avec le périphérique est conforme à la norme FIPS 140-2 si le pilote compatible FIPS 140-2 :

- Fonctionne dans un environnement où la stratégie de groupe FIPS est activée
- Est connecté à un appareil qui répond aux exigences de l'appareil (voir Exigences de l'appareil sur la page 91)
- Est correctement configuré (voir Comment configurer le périphérique et le pilote pour FIPS 140-2 sur la page 92)

Si l'une des exigences du mode conforme à la norme FIPS 140-2 n'est pas remplie, il n'y a aucune garantie quant à la conformité FIPS 140-2 du pilote ou à la communication avec l'appareil. Voir Pilotes et FIPS 140-2 sur la page 91 pour plus d'informations.

Appareils fonctionnant sur MOBOTIX Open Network Bridge

Lorsqu'il s'exécute sur un ordinateur sur lequel l'indicateur de stratégie de groupe FIPS est activé dans Windows, le MOBOTIX Open Network Bridge utilise SHA265 pour chiffrer la communication. Sur un ordinateur sur lequel FIPS n'est pas activé, vous pouvez sélectionner MD5 ou SHA165 pour le chiffrement.

8.1.8 Base de données multimédia : considérations relatives à la rétrocompatibilité

Il est possible d'avoir des enregistrements dans le même stockage à partir de plusieurs versions différentes de MOBOTIX HUB VMS en même temps.

Les données signées ou chiffrées doivent être :

- Exporté à partir du stockage s'il a été enregistré avec MOBOTIX HUB VMS version 2017 R1 ou antérieure
  L'exportation des données s'effectue à l'aide du client intelligent MOBOTIX HUB.
- Mise à niveau, s'il a été enregistré avec MOBOTIX HUB VMS version 2017 R2 ou plus récente
  La mise à niveau des données s'effectue en collaboration avec l'assistance MOBOTIX, à l'aide d'un outil de conversion de médias fourni par l'assistance MOBOTIX.

L'indicateur de stratégie de groupe FIPS doit être désactivé sur le système d'exploitation Windows pour que l'outil de conversion de support puisse s'exécuter.

Le serveur d'enregistrement doit également être arrêté pendant l'exécution de l'outil de conversion multimédia, et aucun enregistrement n'est effectué pendant l'exécution de l'outil.

Mise à niveau du support en fonction de la version de MOBOTIX HUB VMS

- Données enregistrées avec MOBOTIX HUB VMS version 2017 R1 et antérieures
  Les données multimédias chiffrées qui ont été enregistrées avec MOBOTIX HUB VMS 2017 R1 et versions antérieures ne sont pas disponibles si FIPS est activé, même si l'outil de conversion multimédia a été exécuté.
  Exportez les données multimédias enregistrées avec MOBOTIX HUB VMS 2017 R1 et versions antérieures pour y accéder hors ligne.
  Voir Mise à niveau des données de la base de données multimédia : MOBOTIX HUB VMS 2017 R1 et versions antérieures sur la page 88.
- Données enregistrées avec MOBOTIX HUB VMS version 2017 R2 à 2019 R3

Les données multimédias qui ont été enregistrées avec MOBOTIX HUB VMS versions 2017 R2 à 2019 R3 ne seront pas automatiquement rechiffrées. La conversion peut prendre du temps et doit être planifiée. Pour mettre à jour les données plus anciennes afin d'utiliser des algorithmes conformes à la norme FIPS, contactez le support MOBOTIX pour obtenir l'outil de conversion multimédia.
Voir Mise à niveau de la base de données des médias : MOBOTIX HUB VMS 2017 R2 à MOBOTIX HUB VMS 2019 R3 sur la page 88.

- Données enregistrées avec MOBOTIX HUB VMS version 2020 R1 ou 2020 R2
  Les données multimédias enregistrées avec MOBOTIX HUB VMS 2020 R1 ou 2020 R2 seront automatiquement rechiffrées avec des algorithmes conformes à la norme FIPS 140-2 lorsque le serveur d'enregistrement sera démarré après une mise à niveau. Voir Mise à niveau de la base de données multimédia : MOBOTIX HUB VMS 2020 R1 ou MOBOTIX HUB VMS 2020 R2 sur la page 90.

Détails de la mise à niveau du support

Le rechiffrement des données à l'aide d'un serveur d'enregistrement doté d'algorithmes conformes à la norme FIPS est un élément central du processus de mise à niveau. Par conséquent, le processus de mise à niveau varie en fonction de la version de MOBOTIX HUB VMS utilisée pour l'enregistrement de ces données.

<table>
<tr><th colspan="5">Données enregistrées avec</th></tr>
<tr><th></th><th>2017 R1 et versions antérieures</th><th>2017 R2 - 2019 R3</th><th>2020 R1 à 2020 R2</th><th>2020 R3 et versions ultérieures</th></tr>
<tr><td>Changements</td><td>Données cryptées avec DES
Signature à l'aide de MD5
Passe:
Cookie stocké CONFIG.XML
Mot de passe _a & _b dans la table CONFIG. XML
DES crypté</td><td>Données cryptées avec AES
Signature à l'aide de SHA</td><td>Liste de mots de passe dans le CONFIG.XML de stockage
Les mots de passe de la liste de mots de passe sont cryptés DES</td><td>Les mots de passe de la liste de mots de passe sont chiffrés à l'aide d'AES
Un outil de conversion de média est disponible pour la mise à jour de la table CONFIG. XML d'avoir un mot de passe _a _b, pour utiliser une liste de mots de passe mise à jour</td></tr>
<tr><td>FIPS désactivé</td><td colspan="4">Toutes les fonctionnalités fonctionnent comme prévu</td></tr>
<tr><td>FIPS activéDonnées signées</td><td>Les données signées peuvent être lues
Vérifier l'échec de la signature lors de l'exportation</td><td colspan="3">Les données signées peuvent être lues
Vérifier la signature pendant les travaux d'exportation</td></tr>
<tr><td>FIPS activéDonnées chiffrées</td><td colspan="3">Le stockage reste hors ligne
(Le stockage peut rester hors ligne si le chiffrement a été activé pour le stockage)</td><td>Toutes les fonctionnalités fonctionnent comme prévu</td></tr>
</table>

<table>
<tr><th colspan="5">Données enregistrées avec</th></tr>
<tr><th></th><th>2017 R1 et versions antérieures</th><th>2017 R2 - 2019 R3</th><th>2020 R1 à 2020 R2</th><th>2020 R3 et versions ultérieures</th></tr>
<tr><td>L'outil de conversion multimédia ne fonctionne pas</td><td colspan="3"></td><td></td></tr>
<tr><td>FIPS activéAucun cryptage
L'outil de conversion multimédia ne fonctionne pas</td><td colspan="4">Toutes les fonctionnalités fonctionnent comme prévu</td></tr>
<tr><td>L'outil de conversion multimédia a fonctionné</td><td colspan="2">L'outil de conversion multimédia peut prendre beaucoup de temps pour s'exécuter car il met à jour la table CONFIG. XML pour toutes les tables chiffrées</td><td>L'outil de conversion multimédia fonctionne rapidement car il n'a besoin de mettre à jour que le stockage CONFIG.XML</td><td>L'outil de conversion multimédia fonctionne rapidement car aucune mise à jour n'est nécessaire</td></tr>
<tr><td>FIPS activéDonnées chiffrées
L'outil de conversion multimédia a fonctionné</td><td>Les données chiffrées ne sont pas disponibles
Connexion perdue lors de la lecture
L'archivage avec la réduction des images clés archive l'ensemble du GoP</td><td colspan="3">Les données cryptées peuvent être lues
L'archivage avec la réduction en images-clés fonctionne comme prévu</td></tr>
<tr><td>FIPS activéAucun cryptage</td><td colspan="4">Toutes les fonctionnalités fonctionnent comme prévu</td></tr>
</table>

Données enregistrées avec				
	2017 R1 et versions antérieures	**2017 R2 - 2019 R3**	**2020 R1 à 2020 R2**	**2020 R3 et versions ultérieures**
Pas de signature L'outil de conversion multimédia a fonctionné				

Mise à niveau des données de la base de données multimédia : MOBOTIX HUB VMS 2017 R1 et versions antérieures

Si vous utilisez MOBOTIX HUB VMS version 2017 R1 ou antérieure ou si vous avez signé ou chiffré des données enregistrées avec ces versions, les enregistrements sont chiffrés à l'aide d'algorithmes qui ne sont pas considérés comme sécurisés par la norme FIPS 140-2.
Il n'est pas possible d'accéder à ces enregistrements à partir d'un ordinateur sur lequel l'indicateur de stratégie de groupe FIPS est activé.
Par conséquent, il est nécessaire d'exporter la base de données multimédia vers un emplacement où elle est toujours accessible.

Mise à niveau de la base de données multimédia : MOBOTIX HUB VMS 2017 R2 vers MOBOTIX HUB VMS 2019 R3

Si vous exécutez une version de MOBOTIX HUB VMS entre MOBOTIX HUB VMS 2017 R2 et MOBOTIX HUB VMS 2019 R3 et si, à un moment donné, le chiffrement a été activé dans la base de données des médias, pour accéder à ces enregistrements, vous devez effectuer l'une des options suivantes.

Les deux options nécessitent l'utilisation de l'outil de conversion de médias. Le serveur d'enregistrement doit être arrêté pendant l'exécution de l'outil de conversion multimédia et aucun enregistrement n'est effectué pendant l'exécution de l'outil. Voir Qu'est-ce que l'outil de conversion multimédia ? sur la page 89 pour plus d'informations.

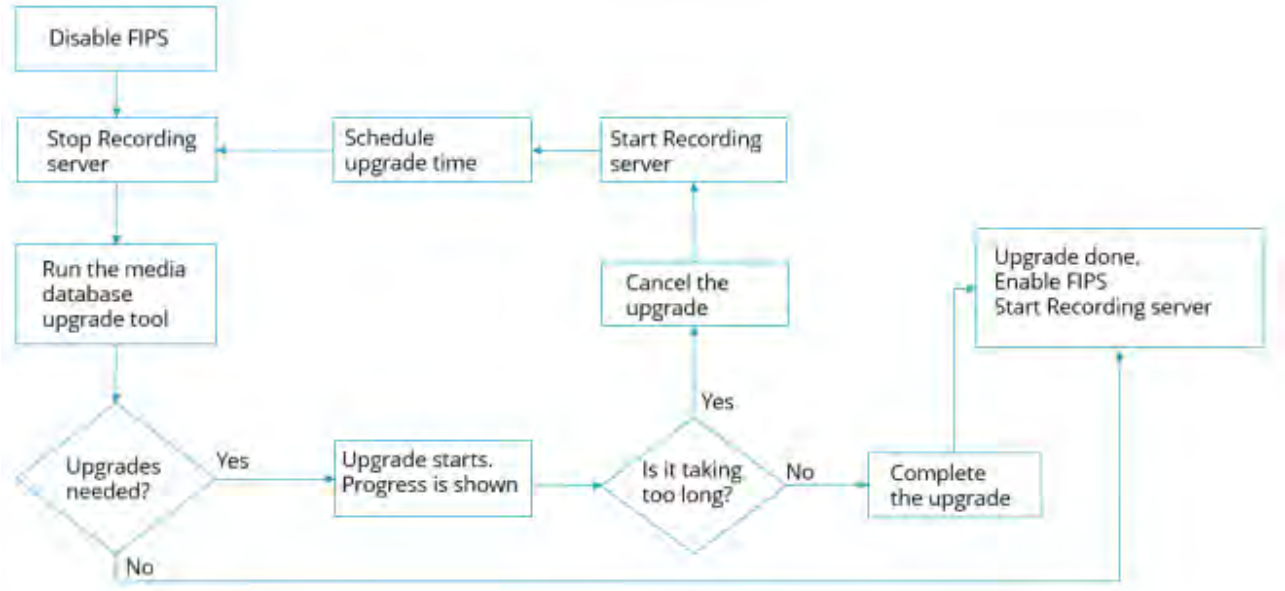
- Option 1
  Utilisez cette option pour pouvoir fonctionner immédiatement dans un environnement FIPS et si vous disposez d'une longue durée de rétention. Le temps nécessaire à l'exécution de l'outil de conversion multimédia peut être important.
  1. Mettez à niveau les machines virtuelles Mobotix Hub vers la version 2020 R3.
  2. Lorsque FIPS est désactivé sur le système d'exploitation Windows, exécutez l'outil de conversion multimédia fourni par le support MOBOTIX.
  3. Activez l'indicateur de stratégie de groupe FIPS sur le système d'exploitation Windows.
- Option 2
  Utilisez cette option si l'utilisation dans un environnement FIPS peut attendre, si vous disposez d'une courte durée de conservation et si vous exécutez l'outil de conversion multimédia avec moins de données.
  1. Mettez à niveau les machines virtuelles Mobotix Hub vers la version 2020 R3.

2. Exécutez les machines virtuelles Mobotix Hub pendant la durée de rétention sans activer FIPS sur le système d'exploitation Windows.
3. Exécutez l'outil de conversion multimédia pour vous assurer que toutes les données sont converties pour être conformes à la norme FIPS.
4. Activez l'indicateur de stratégie de groupe FIPS sur le système d'exploitation Windows.

Qu'est-ce que l'outil de conversion multimédia ?

L'outil de conversion multimédia est un script PowerShell autonome, fourni dans la source. Il ne fait partie d'aucune installation.
Il ne doit être distribué aux clients que par l'intermédiaire de l'assistance MOBOTIX.
Il peut convertir tout le stockage en masse ou être exécuté sur un stockage spécifique.
Les indicateurs de progression indiquent jusqu'où l'outil est allé.
Si la conversion prend trop de temps, vous pouvez annuler le travail et continuer sans que FIPS ne soit activé.
L'outil de conversion multimédia convertit les informations d'identification chiffrées dans les fichiers de table de médias existants au format le plus récent compatible FIPS.
L'outil de conversion multimédia ne modifie pas le cryptage des données vidéo lui-même. Si les données vidéo sont chiffrées à l'aide d'un algorithme non conforme (DES), les tables mises à jour sont chargées, mais la vidéo est inaccessible en mode conforme à la norme FIPS.
L'outil de conversion multimédia convertit et vérifie si toutes les tables utilisent des algorithmes conformes à la norme FIPS.
Les tables approuvées seront marquées pour éviter qu'elles ne soient à nouveau vérifiées par l'outil de conversion des médias.
Après avoir exécuté l'outil de conversion de support, le MOBOTIX HUB VMS 2020 R3 sera en mesure de charger des tables en mode conforme à la norme FIPS.

Flux de travail de l'outil de conversion multimédia



Mise à niveau de la base de données multimédia : MOBOTIX HUB VMS 2020 R1 ou MOBOTIX HUB VMS 2020 R2

Si vous exécutez MOBOTIX HUB VMS version 2020 R1 ou MOBOTIX HUB VMS 2020 R2, les données multimédias enregistrées avec l'une de ces versions seront automatiquement rechiffrées avec des algorithmes conformes à la norme FIPS 140-2 lors de la mise à niveau du serveur d'enregistrement.

8.1.9 Stratégie de groupe FIPS sur le système d'exploitation Windows

Le mode de fonctionnement FIPS est activé et désactivé à l'aide de l'indicateur de stratégie de groupe FIPS sur le système d'exploitation Windows. Pour plus d'informations sur l'activation et la désactivation de FIPS, consultez le site Microsoft.

Avant d'effectuer la mise à niveau, vous devez désactiver l'indicateur de stratégie de groupe FIPS sur tous les ordinateurs qui font partie des machines virtuelles MOBOTIX HUB, y compris l'ordinateur qui héberge SQL Server et tous les postes de travail MOBOTIX HUB Smart Client.

Il existe deux raisons pour lesquelles l'indicateur de stratégie de groupe FIPS doit être désactivé sur tous les ordinateurs des machines virtuelles Mobotix Hub avant la mise à niveau :

- Au cours de la mise à niveau, les données chiffrées à l'aide d'algorithmes FIPS non approuvés sont rechiffrées à l'aide d'algorithmes approuvés. Pour exécuter le déchiffrement sur le système d'exploitation Windows, l'indicateur de stratégie de groupe FIPS doit être désactivé.
- Si l'indicateur de stratégie de groupe FIPS est activé dans Windows, vous ne pourrez pas utiliser les machines virtuelles Mobotix Hub tant que tous les composants n'auront pas été mis à niveau. Par exemple, un client intelligent MOBOTIX HUB 2020 R2 ne pourra pas communiquer avec un serveur de gestion 2020 R3 si le serveur de gestion se trouve sur un ordinateur sur lequel l'indicateur de stratégie de groupe FIPS est activé.

Politique de groupe FIPS et architecture fédérée MOBOTIX

Si un site d'une architecture fédérée MOBOTIX doit fonctionner avec l'indicateur de stratégie de groupe FIPS activé dans Windows, tous les sites doivent également fonctionner avec l'indicateur de stratégie de groupe FIPS activé dans Windows.

Par conséquent, l'ensemble de l'installation de MOBOTIX Federated Architecture doit être mis à niveau vers la version 2020 R3.

8.1.10 Installer MOBOTIX HUB VMS2020 R3

Lors de la mise à niveau, le programme d'installation de MOBOTIX HUB VMS vérifie la politique de sécurité FIPS et empêche la mise à niveau de démarrer si FIPS est activé.

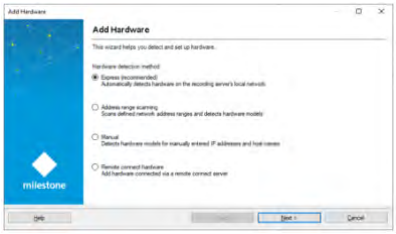
8.1.11 Chiffrer les mots de passe de détection matérielle

Les mots de passe de détection matérielle doivent être mis à jour après la mise à niveau vers MOBOTIX HUB VMS 2020 R3.

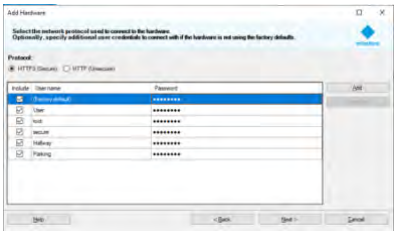
Le chiffrement des mots de passe de détection du matériel n'est pas mis à jour lors de la mise à niveau à partir d'une version antérieure des machines virtuelles Mobotix Hub. Toutefois, ces mots de passe ne peuvent pas être lus si l'indicateur de stratégie de groupe FIPS est activé dans Windows.

Vous devez déclencher une conversion de ces mots de passe avant d'activer FIPS. Procédez comme suit :

1. Assurez-vous que l'indicateur de stratégie de groupe FIPS est désactivé dans Windows.
2. Dans le client de gestion MOBOTIX HUB, ouvrez l'assistant d'ajout de matériel.



3. Sélectionnez la méthode de détection pour ouvrir la page de détection du matériel.



Cela déclenche le rechiffrement des mots de passe de détection du matériel avec des algorithmes conformes à la norme FIPS.

Les informations d'identification sont désormais chiffrées à l'aide d'algorithmes conformes à la norme FIPS.

8.2 Pilotes et FIPS 140-2

Cette section traite de la norme FIPS 140-2 et de la configuration et de l'utilisation des pilotes MOBOTIX pour qu'ils fonctionnent en mode conforme à la norme FIPS 140-2.

8.2.1 Exigences pour le mode conforme à la norme FIPS 140-2

Les pilotes de périphériques MOBOTIX MOBOTIX HUB VMS peuvent être conformes à la norme FIPS 140-2, car ils peuvent être configurés et fonctionner de manière à n'utiliser que des instances d'algorithme conformes à la norme FIPS 140-2. Seuls des pilotes spécifiques dans une configuration spécifique sont conformes à la norme FIPS 140-2. Dans cette configuration FIPS 140-2 spécifique, le pilote sera en mesure de communiquer avec les périphériques de manière conforme. Les appareils doivent remplir plusieurs conditions afin de pouvoir accepter cette communication. En outre, l'indicateur de stratégie de groupe FIPS doit être activé dans Windows sur le serveur sur lequel le serveur d'enregistrement est installé. Lorsque l'indicateur de stratégie de groupe FIPS est activé, les pilotes compatibles FIPS 140-2 fonctionnent en mode conforme et n'utilisent pas de primitives de chiffrement non approuvées. Les conducteurs utiliseront les algorithmes utilisés uniquement pour les canaux de communication sécurisés.

Configuration requise pour l'appareil

Pour qu'un périphérique puisse communiquer avec un pilote fonctionnant en mode conforme à la norme FIPS 140-2, il doit remplir toutes les conditions suivantes :

- L'appareil doit prendre en charge la communication HTTPS avec au moins une suite de chiffrement conforme à la norme FIPS 140-2 (pour des exemples, voir Exemple de suites de chiffrement conformes à la norme FIPS 140-2 sur la page 97)
- L'appareil doit prendre en charge RTSP sur HTTPS (Tunneling RTSP et RTP over HTTP) à l'aide de l'authentification HTTP de base (RFC2068 Section 11.1) ou de l'authentification HTTP Digest (RFC2069, RFC7616)

  ou

  L'appareil doit prendre en charge la diffusion multimédia en continu à l'aide de SRTP et RTSPS (RFC3711)

Pilotes pris en charge

À l'heure actuelle, seul un sous-ensemble de pilotes est conforme à la norme FIPS 140-2. Ces pilotes prennent en charge la communication via un canal sécurisé pour toutes les fonctionnalités disponibles.

Axe 1 canal	Axe 1 canal PTZ	Axe 2 canaux	Axe 3 canaux
Axe 4 canaux	Axe 8 canaux	Axe 11 canaux	Axe 12 canaux
Axe Audio	Bosch PTZ	Bosch 1 canal	Bosch 2 canaux
Bosch 3 canaux	Bosch 16 canaux	Bosch X20XF	Bosch X40XF
Canon 1 canal	Canon 1 canal PTZ	Canon VBM	Canon VBM 40
Canon VBS	Canon VBS No Ptz	Décodeur TVI pour barrières numériques	Hanwha Générique
ONVIF	ONVIF16	Universel	Universel 16 canaux
Universel 64 canaux	VidéoPush		

Les pilotes du tableau peuvent s'exécuter en mode conforme à la norme FIPS 140-2 lorsqu'ils sont correctement configurés. Cette liste n'est pas définitive et pourrait s'étendre à l'avenir. Certains pilotes sont conformes à la norme FIPS 140-2 et leurs capacités sont limitées. Reportez-vous aux sections spécifiques des pilotes ci-dessous pour plus d'informations sur leur configuration et les limitations.
Le mode conforme à la norme FIPS 140-2 pour les pilotes est disponible depuis Device Pack 11.1.

8.2.2 Effets de l'exécution en mode conforme à la norme FIPS 140-2

En mode conforme à la norme FIPS 140-2, certains pilotes ne peuvent pas être utilisés. Les pilotes répertoriés comme FIPS 140-2 peuvent ne pas être en mesure de se connecter à des périphériques qui ne répondent pas aux exigences du périphérique.
Un pilote est conforme à la norme FIPS 140-2 et la communication avec le périphérique est conforme à la norme FIPS 140-2 si le pilote compatible FIPS 140-2 :

- Fonctionne dans un environnement où la stratégie de groupe FIPS est activée
- Est connecté à un appareil qui répond aux exigences de l'appareil (voir Configuration requise pour l'appareil sur la page 91)
- Est correctement configuré (voir Comment configurer le périphérique et le pilote pour FIPS 140-2 sur la page 92)

Si l'une des exigences du mode conforme à la norme FIPS 140-2 n'est pas remplie, il n'y a aucune garantie quant à la conformité FIPS 140-2 du pilote ou à la communication avec l'appareil.

8.2.3 Comment configurer le périphérique et le pilote pour FIPS 140-2

La configuration du périphérique et du pilote pour le mode conforme à la norme FIPS 140-2 est spécifique au périphérique et au pilote. Certaines directives générales s'appliquent :

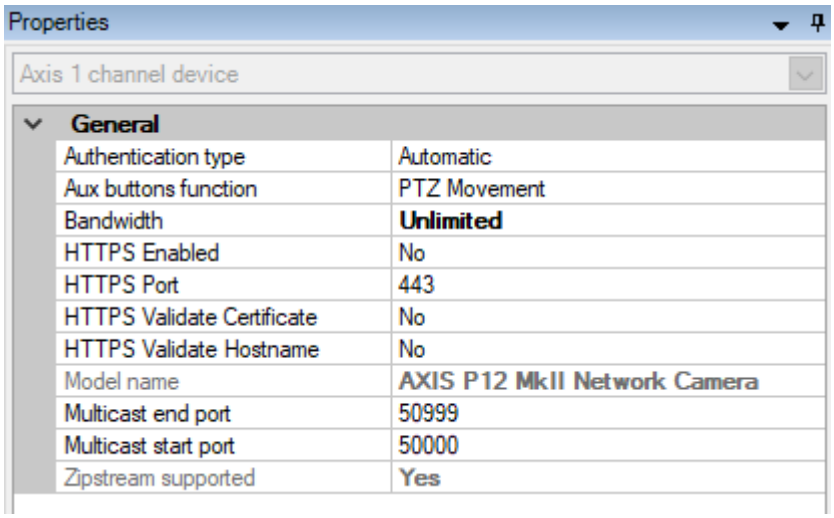
- Les canaux de communication entre le pilote et l'appareil doivent être sécurisés et chiffrés (HTTPS, RTSP sur HTTPS, SRTP).
- L'appareil doit être configuré pour fonctionner à l'aide de canaux sécurisés.
- Le pilote et le périphérique doivent être configurés pour utiliser des canaux sécurisés pour la communication dans les machines virtuelles MOBOTIX HUB.

Haut-parleurs d'axe

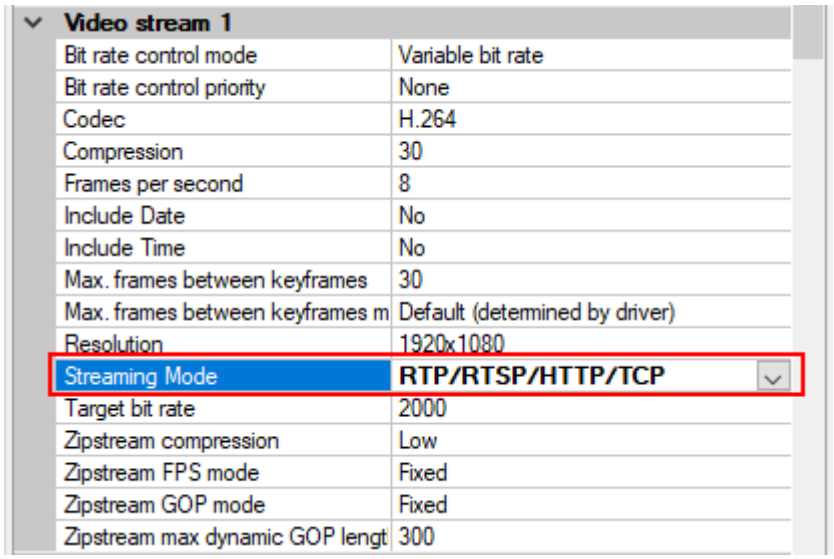
Procédez comme suit :

- Définissez HTTPS activé sur Oui.

- Définissez HTTPS Validate Certificate sur Yes.
- Définissez HTTPS Validate hostname sur Yes.

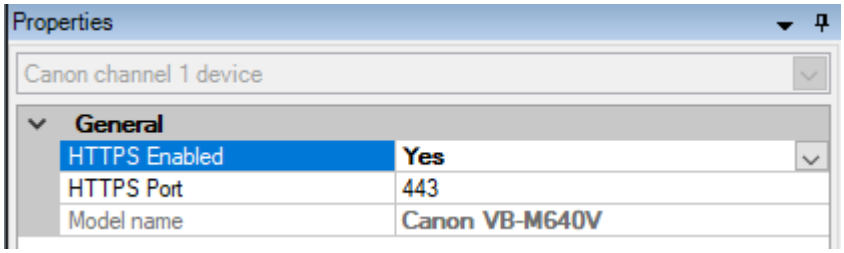


- Pour chaque canal multimédia et flux multimédia activés, définissez le mode de diffusion sur RTP/RTSP/HTTP/TCP.

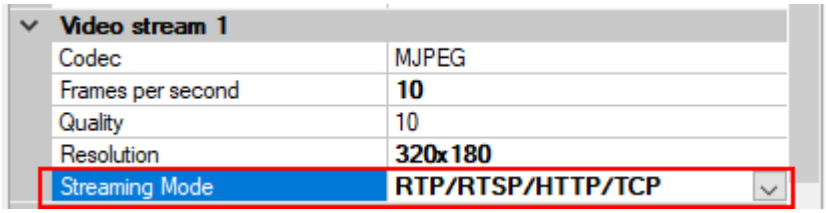


Pilotes Canon

- Définissez le HTTPS activé sur Oui.



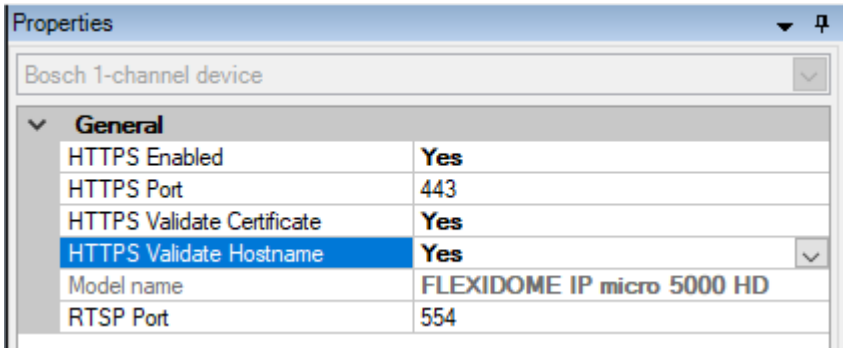
- Pour chaque canal multimédia et flux multimédia activés, définissez le mode de diffusion sur RTP/RTSP/HTTP/TCP.



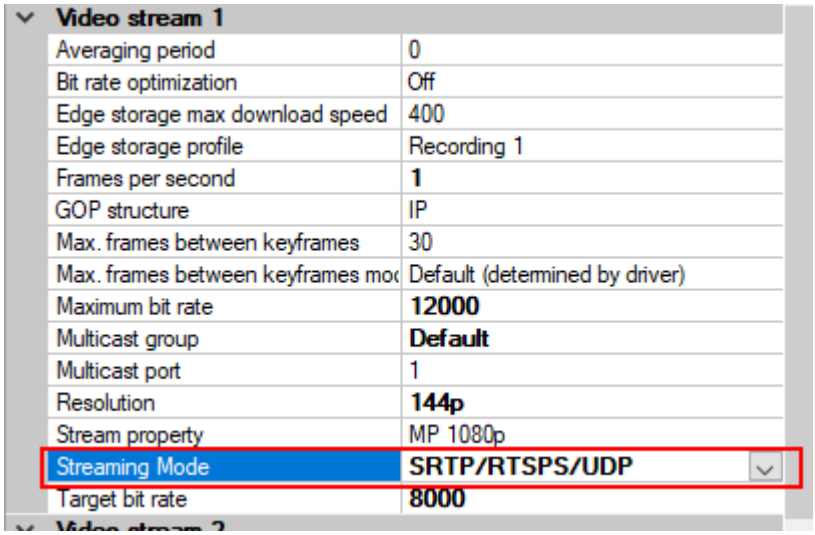
Pilotes Bosch

Procédez comme suit :

- Définissez HTTPS activé sur Oui.
- Définissez HTTPS Validate Certificate sur Yes.
- Définissez HTTPS Validate hostname sur Yes.

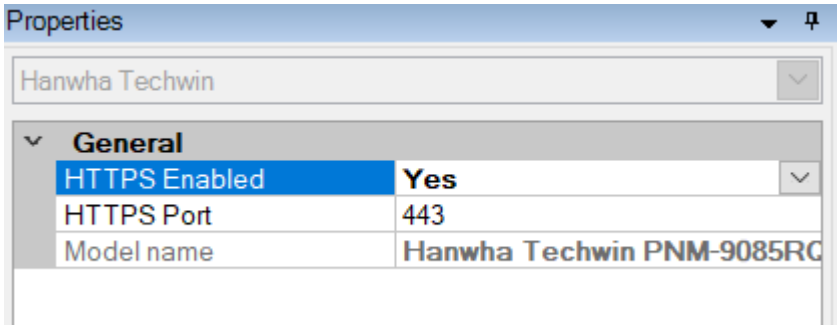


- Pour chaque canal multimédia et flux multimédia activés, définissez le mode de diffusion sur l'un des suivants :
  - RTP/RTSP/HTTP/TCP
  - SRTP/RTSPS/UDP
  - Multidiffusion SRT/RTSPS/UDP

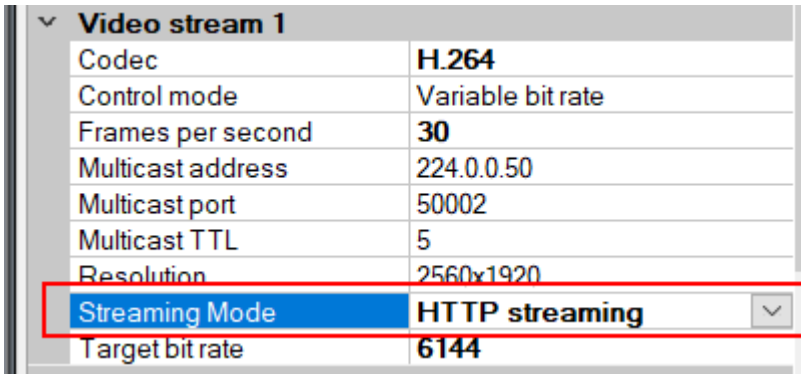


Chauffeurs Hanwha

- Définissez le HTTPS activé sur Oui.



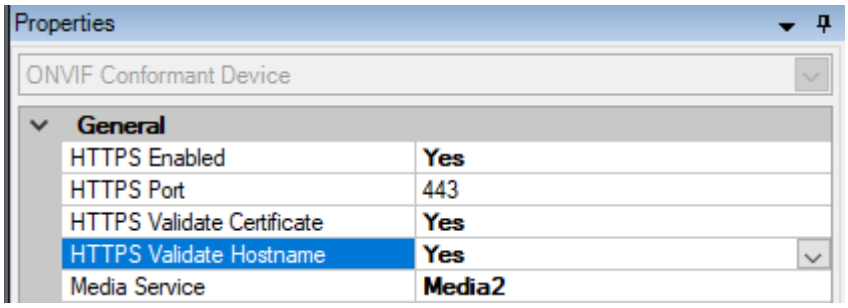
- Pour chaque canal multimédia et flux multimédia activés, définissez le mode de diffusion sur Streaming HTTP.



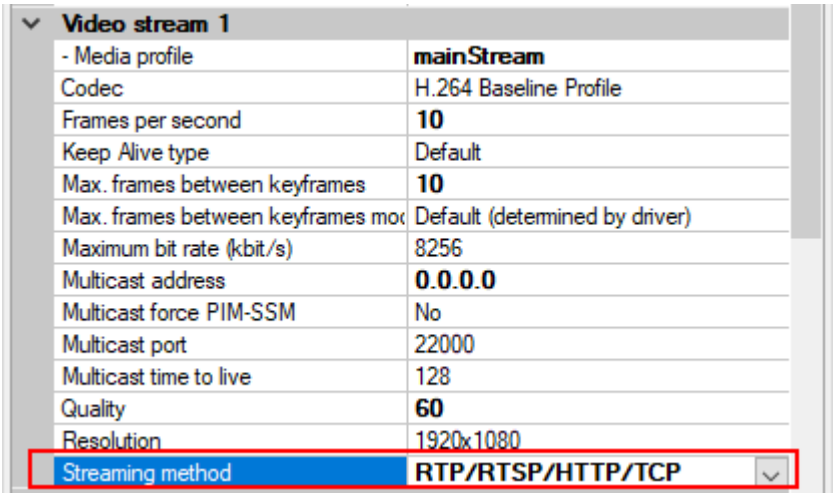
Pilotes ONVIF

Procédez comme suit :

- Définissez HTTPS activé sur Oui.
- Définissez HTTPS Validate Certificate sur Yes.
- Définissez HTTPS Validate hostname sur Yes.



- Pour chaque canal multimédia et flux multimédia activés, définissez Méthode de diffusion en continu sur RTP/RTSP/HTTP/TCP.

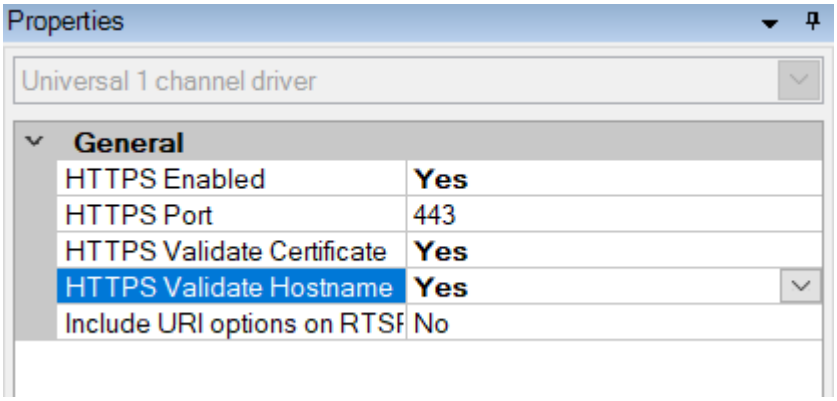


- Le canal audio arrière (sortie audio, haut-parleur du périphérique) ne doit pas être utilisé lorsque le pilote s'exécute en mode conforme à la norme FIPS 140-2.

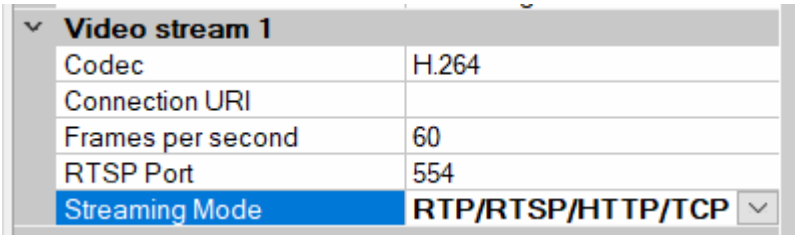
Haut-parleurs universels

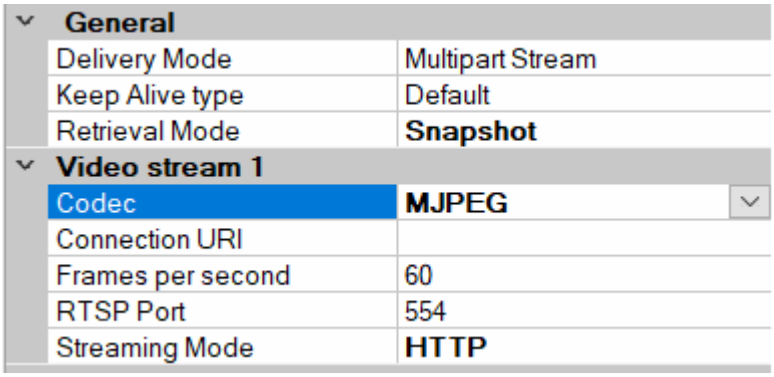
Procédez comme suit :

- Définissez HTTPS activé sur Oui.
- Définissez HTTPS Validate Certificate sur Yes.
- Définissez HTTPS Validate hostname sur Yes.



- Pour chaque canal multimédia et flux multimédia activés, définissez le mode de diffusion en continu sur RTP/RTSP/HTTP/TCP ou HTTP, selon que le mode de diffusion en continu ou de récupération d'instantanés est utilisé.





General	
Delivery Mode	Multipart Stream
Keep Alive type	Default
Retrieval Mode	**Snapshot**
Video stream 1	
Codec	**MJPEG**
Connection URI	
Frames per second	60
RTSP Port	554
Streaming Mode	**HTTP**

Pilote VideoPush

Aucune configuration spécifique n'est nécessaire. L'activation de la politique de groupe FIPS obligera le pilote à communiquer avec le serveur mobile MOBOTIX HUB d'une manière conforme à la norme FIPS 140-2.

8.2.4 Exemple de suites de chiffrement conformes à la norme FIPS 140-2

0x1302	TLS_AES_256_GCM_SHA384
0x1303	TLS_CHACHA20_POLY1305_SHA256
0x1301	TLS_AES_128_GCM_SHA256
0xC02C	TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384
0xC030	TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384
0x00A3	TLS_DHE_DSS_WITH_AES_256_GCM_SHA384
0x009F	TLS_DHE_RSA_WITH_AES_256_GCM_SHA384
0xC02B	TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256
0xC02F	TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256
0x00A2	TLS_DHE_DSS_WITH_AES_128_GCM_SHA256
0x009E	TLS_DHE_RSA_WITH_AES_128_GCM_SHA256
0xC024	TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA384
0xC028	TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384
0x006B	TLS_DHE_RSA_WITH_AES_256_CBC_SHA256
0x006A	TLS_DHE_DSS_WITH_AES_256_CBC_SHA256
0xC023	TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA256
0xC027	TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256
0x0067	TLS_DHE_RSA_WITH_AES_128_CBC_SHA256
0x0040	TLS_DHE_DSS_WITH_AES_128_CBC_SHA256
0x00AD	TLS_RSA_PSK_WITH_AES_256_GCM_SHA384
0x00AB	TLS_DHE_PSK_WITH_AES_256_GCM_SHA384
0x009D	TLS_RSA_WITH_AES_256_GCM_SHA384
0x00A9	TLS_PSK_WITH_AES_256_GCM_SHA384
0x00AC	TLS_RSA_PSK_WITH_AES_128_GCM_SHA256
0x00AA	TLS_DHE_PSK_WITH_AES_128_GCM_SHA256

0x009C	TLS_RSA_WITH_AES_128_GCM_SHA256
0x00A8	TLS_PSK_WITH_AES_128_GCM_SHA256
0x003D	TLS_RSA_WITH_AES_256_CBC_SHA256
0x003C	TLS_RSA_WITH_AES_128_CBC_SHA256
0x0035	TLS_RSA_WITH_AES_256_CBC_SHA
0x002F	TLS_RSA_WITH_AES_128_CBC_SHA

Cette liste n'est pas exhaustive. Il existe d'autres suites de chiffrement conformes à la norme FIPS 140-2. Cette liste n'est fournie qu'à titre d'exemple de suites de chiffrement conformes à la norme FIPS 140-2.

8.3 Ressources FIPS

1. Exigences de sécurité FIPS 140-2 pour les modules cryptographiques
   https://csrc.nist.gov/publications/detail/fips/140/2/final
2. Annexe A : Fonctions de sécurité approuvées pour la norme FIPS PUB 140-2
   https://csrc.nist.gov/CSRC/media/Publications/fips/140/2/final/documents/fips1402annexa.pdf
3. Instructions pour la sélection, la configuration et l'utilisation des implémentations TLS (Transport Layer Security)
   https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-52r2.pdf
4. Conseils de mise en œuvre de la norme FIPS 140-2 et du programme de validation des modules cryptographiques
   https://csrc.nist.gov/csrc/media/projects/cryptographic-module-validation-program/documents/fips140-2/fips1402ig.pdf
5. L'approche de Microsoft en matière de validation FIPS 140-2
   https://docs.microsoft.com/en-us/windows/security/threat-protection/fips-140-validation
6. Présentation TLS/SSL (Schannel SSP)
   https://docs.microsoft.com/en-us/windows-server/security/tls/tls-ssl-schannel-ssp-overview
7. Suites de chiffrement en TLS/SSL (Schannel SSP)
   https://docs.microsoft.com/en-us/windows/win32/secauthn/cipher-suites-in-schannel
8. Suites de chiffrement TLS dans Windows 10 v1903, v1909 et v2004
   https://docs.microsoft.com/en-us/windows/win32/secauthn/tls-cipher-suites-in-windows-10-v1903
9. Courbes elliptiques TLS dans Windows 10 version 1607 et ultérieure
   https://docs.microsoft.com/en-us/windows/win32/secauthn/tls-elliptic-curves-in-windows-10-1607-and-later

9 Tableau de comparaison des produits

9.1 Tableau comparatif des produits

MOBOTIX HUB VMS comprend les produits suivants :

- MOBOTIX MOHUB L1
- MOBOTIX HUB L2
- MOBOTIX HUB L3
- MOBOTIX HUB L4
- MOBOTIX HUB L5

La liste complète des fonctionnalités est disponible sur la page d'aperçu du produit sur le site Web de MOBOTIX https://www.mobotix.com/en/vms/mobotix-hub

Vous trouverez ci-dessous une liste des principales différences entre les produits :

Nom	MOBOTIX MOHUB L1	MOBOTIX HUB L2	MOBOTIX HUB L3	MOBOTIX HUB L4	MOBOTIX HUB L5
Sites par SLC	1	1	Multi-sites	Multi-sites	Multi-sites
Serveurs d'enregistrement par SLC	1	1	Illimité	Illimité	Illimité
Périphériques matériels par serveur d'enregistrement	8	48	Illimité	Illimité	Illimité
Interconnexion™ MOBOTIX	-	Site distant	Site distant	Site distant	Site central/distant
Architecture™ fédérée MOBOTIX	-	-	-	Site distant	Site central/distant
Basculement du serveur d'enregistrement	-	-	-	Veille froide et chaude	Veille froide et chaude
Services de connexion à distance	-	-	-	-	✓
Prise en charge du stockage en périphérie	-	-	✓	✓	✓
Stockage vidéo à plusieurs niveaux	Bases de données en direct + 1 archive	Bases de données en direct + 1 archive	Bases de données en direct + 1 archive	Bases de données en direct + archives illimitées	Bases de données en direct + archives illimitées
Notification SNMP	-	-	-	✓	✓
Droits d'accès des utilisateurs contrôlés dans le temps	-	-	-	-	✓
Réduire la fréquence d'images (toilettage)	-	-	-	✓	✓

Nom	MOBOTIX MOHUB L1	MOBOTIX HUB L2	MOBOTIX HUB L3	MOBOTIX HUB L4	MOBOTIX HUB L5
Cryptage des données vidéo (serveur d'enregistrement)	-	-	-	✓	✓
Signature de base de données (serveur d'enregistrement)	-	-	-	✓	✓
Niveaux de priorité PTZ	1	1	3	32000	32000
PTZ étendu (réservation d'une session PTZ et d'une patrouille à partir du client intelligent MOBOTIX HUB)	-	-	-	✓	✓
Verrouillage des preuves	-	-	-	-	✓
Fonction marque-page	-	-	Manuel uniquement	Manuel et basé sur des règles	Manuel et basé sur des règles
Multi-streaming en direct ou multidiffusion / Streaming adaptatif	-	-	-	✓	✓
Streaming direct	-	-	-	✓	✓
Sécurité globale	Droits d'utilisation du client	Droits d'utilisation du client	Droits d'utilisation du client	Droits d'utilisation du client	Droits d'utilisateur du client/ Droits d'utilisateur administrateur
MOBOTIX HUB Management Profils clients	-	-	-	-	✓
Profils de clients intelligents MOBOTIX HUB	-	-	3	3	Illimité
Mur intelligent MOBOTIX HUB	-	-	-	optionnel	✓
Moniteur système	-	-	-	✓	✓
Carte intelligente	-	-	-	✓	✓
Vérification en deux étapes	-	-	-	-	✓

Nom	MOBOTIX MOHUB L1	MOBOTIX HUB L2	MOBOTIX HUB L3	MOBOTIX HUB L4	MOBOTIX HUB L5
Prise en charge DLNA	-	✓	✓	✓	✓
Masquage de la confidentialité	-	✓	✓	✓	✓
Gestion des mots de passe de l'appareil			✓	✓	✓

10 Appendice

10.1 Annexe 1 – Ressources

Décrit la configuration minimale requise pour un système de vidéosurveillance. Voir aussi les normes connexes.

1. Axis Communications : Guide de durcissement
2. Systèmes de sécurité Bosch : Guide de sécurité des vidéos et des données IP Bosch
3. Norme britannique BS EN 62676-1-1 : Systèmes de vidéosurveillance pour utilisation dans des applications de sécurité, Partie 1-1 : Exigences système – Généralités
4. Décrit la configuration minimale requise pour un système de vidéosurveillance. Voir aussi les normes connexes.
5. Center for Internet Security : les contrôles de sécurité critiques de la CEI pour une cyberdéfense efficace
6. Cloud Security Alliance (CSA) et Cloud Controls Matrix
7. Defense Information Systems Agency (DISA) : Guides de mise en œuvre technique de la sécurité (STIGs)
8. Internet Engineering Task Force (IETF), références multiples
9. ISO/IEC 15048 Technologies de l'information - Techniques de sécurité - Critères d'évaluation de la sécurité informatique
10. ISO/IEC 31000, Gestion des risques – Principes et lignes directrices
11. ISO/IEC 31010, Management des risques – Techniques d'évaluation des risques
12. ISO 27001 : Sécurité de l'information, cybersécurité et protection de la vie privée — Systèmes de management de la sécurité de l'information — Exigences
13. ISO 27002 : Sécurité de l'information, cybersécurité et protection de la vie privée — Contrôles de la sécurité de l'information
14. Guide des mises à jour de sécurité Microsoft
15. Voir aussi Gérer les paramètres de stratégie de sécurité, entre autres
16. Institut national des normes et de la technologie : Division de la sécurité informatique Centre de ressources en sécurité informatique
17. Institut national des normes et de la technologie : Cadre de cybersécurité
18. Cadre de gestion des risques pour les systèmes d'information et les organisations : une approche du cycle de vie des systèmes pour la sécurité et la protection des renseignements personnels
19. National Institute of Standards and Technology : Gestion des risques liés à la sécurité de l'information
20. National Institute of Standards and Technology : Contrôles de sécurité et de confidentialité pour les systèmes d'information et les organisations fédérales SP 800-53 - Révision 5
21. NIST SP 800-100 Information Security Handbook : Guide pour les gestionnaires
22. NIST SP 800-124 Directives pour la gestion de la sécurité des appareils mobiles dans l'entreprise
23. Site Web de l'Institut SANS et les contrôles de sécurité critiques de SANS
24. XProtect® Corporate – Gestion avancée de la sécurité

10.2 Annexe 2 - Acronymes

AD – Annuaire actif
CSA – Cloud Security Alliance
CVE – Vulnérabilités et expositions courantes
HTTP – Protocole de transfert hypertexte
HTTPS – Protocole de transfert hypertexte sécurisé
CEI – Commission électrotechnique internationale
IETF – Groupe de travail sur l'ingénierie de l'Internet
IP – Protocole Internet
ISO – Organisation internationale de normalisation

Informatique – Technologies de l'information
Base de connaissances – Base de connaissances
NIST – Institut national des normes et de la technologie
RSTP – Protocole Rapid Spanning Tree
SMTP – Protocole de transfert de courrier simple
SSL – Secure Socket Layer
STIG – Guide d'information technique sur la sécurité
TCP – Protocole de contrôle de transmission
TLS - Sécurité de la couche de transport
UDP – Protocole de datagramme utilisateur
VMS – Logiciel de gestion vidéo
VPN – Réseau privé virtuel

MOBOTIX

BeyondHumanVision

EN_08/23

MOBOTIX AG • Kaiserstrasse • D-67722 Langmeil • Tél. : +49 6302 9816-103 • sales@mobotix.com • www.mobotix.com