Guide sur la sécurité des données et des vidéos IP Bosch

BOSCH

fr

Table des matières

1 Introduction

Même si chaque organisation met aujourd'hui en œuvre des procédures et stratégies de cybersécurité, les normes peuvent varier d'une organisation à l'autre en fonction de nombreux facteurs tels que la taille, la région et le secteur.
En février 2014, le National Institute of Standards and Technology (NIST) a introduit un cadre de cybersécurité. Ce cadre repose sur le décret 13636 et il a été élaboré à partir de normes, consignes et meilleures pratiques existantes. Il est spécifiquement conçu pour réduire les risques informatiques des infrastructures critiques ainsi que des dispositifs et données reliées à leur réseau. Ce cadre est conçu pour aider les organisations à comprendre les risques de cybersécurité aussi bien externes qu'internes et il peut être appliqué à toutes les tailles d'organisations classées du Niveau 1 (Partiel) au Niveau 4 (Adaptatif).

Ce document d'information est destiné à aider les intégrateurs à renforcer la sécurité des produits vidéo IP Bosch afin qu'ils adhèrent aux stratégies et procédures de sécurité réseau de leurs clients.
Ce guide couvrira les sujets suivants :
- Informations critiques relatives aux fonctionnalités et principes fondamentaux des périphériques vidéo IP Bosch
- Fonctionnalités spécifiques qui peuvent être modifiées ou désactivées
- Fonctionnalités spécifiques qui peuvent être activées et utilisées
- Meilleures pratiques en termes de systèmes et de sécurité vidéo

Le présent guide sera axé essentiellement sur l'utilisation de Bosch Configuration Manager pour la réalisation des configurations décrites. Dans la plupart des cas, toutes les configurations peuvent être réalisées en utilisant Bosch Video Management System Configuration Client, Bosch Configuration Manager, ainsi que l'interface Web intégrée d'un périphérique vidéo.

2 Périphériques vidéo IP Bosch

Les produits vidéo IP sont devenus monnaie courante dans l'environnement réseau d'aujourd'hui. Et comme pour n'importe quel périphérique IP installé en réseau, les administrateurs informatiques et les gestionnaires de sécurité ont le droit de connaître l'ampleur réelle de fonctions et capacités d'un périphérique.

Lorsqu'il s'agit de périphériques vidéo IP Bosch, votre première ligne de protection est constituée par les périphériques eux-mêmes. Les encodeurs et caméras Bosch sont fabriqués dans un environnement contrôlé et sécurisé qui est continuellement audité. Il n'est possible d'écrire sur les périphériques qu'au moyen d'un téléchargement de firmware valide, lequel est spécifique à la gamme et au jeu de puces du matériel.

La plupart des périphériques vidéo IP Bosch sont fournis avec une puce de sécurité intégrée qui offre des fonctionnalités similaires aux cartes à puce intelligente de cryptage, baptisée Trusted Platform Module ou TPM dans sa forme abrégée. Cette puce fait office de coffre-fort pour les données critiques, en protégeant les certificats, les clés, les licences, etc. contre tout accès non autorisé, même lorsque la caméra est physiquement ouverte aux accès.

Les périphériques vidéo IP Bosch ont été soumis à plus de trente mille (30 000) tests de vulnérabilité et de pénétration effectués par des fournisseurs de sécurité indépendants. Jusqu'à présent, aucune cyberattaque n'a pu aboutir sur un périphérique correctement sécurisé.

3 Attribution d'adresses IP

Tous les périphériques vidéo IP Bosch sont livrés en sortie d'usine avec un état par défaut prêt à accepter une adresse IP DHCP.
Si aucun serveur DHCP n'est disponible au sein du réseau actif sur lequel est déployé un périphérique, ce dernier, s'il exécute un firmware 6.32 ou supérieur, applique automatiquement une adresse link-local située en dehors de la plage 169.254.1.0 à 169.254.254.255 ou 169.254.0.0/16.
Avec un firmware antérieur, il s'attribue lui-même l'adresse IP par défaut 192.168.0.1.
Plusieurs outils permettent d'attribuer des adresses IP aux périphériques vidéo IP Bosch, notamment :

- IP Helper
- Bosch Configuration Manager
- Bosch Video Management System Configuration Client
- Bosch Video Management System Configuration Wizard

Tous les outils logiciels comportent une option permettant d'attribuer une adresse IPv4 statique unique, ainsi qu'une plage d'adresses IPv4 à plusieurs périphériques simultanément. Cela inclut l'adressage de masque de sous-réseau et de passerelle par défaut.
L'ensemble des adresses IPv4et des valeurs de masque de sous-réseau doivent être entrées en « notation décimale à point ».

Remarque!
Conseil de sécurité des données n°1
L'une des premières actions visant à limiter les possibilités de cyberattaques internes sur un réseau, exécutées par des périphériques réseau non autorisés reliés en local, consiste à restreindre les adresses IP inutilisées disponibles. Cela peut s'effectuer à l'aide de l'outil IPAM (ou gestion d'**adress**e IP **)**, conjointement avec la mise en sous-réseau de la plage d'adresse IP qui sera utilisée.

La mise en sous-réseau est une opération qui consiste à emprunter des bits de la partie hôte d'une adresse IP afin de scinder un grand réseau en plusieurs réseaux plus petits. Plus vous empruntez de bits, plus vous pouvez créer des réseaux, mais chacun d'eux prendra en charge moins d'adresses hôte.

Suffixe	Hôtes	CIDR	Emprunté	Binaire
.255	1	/32	0	.11111111
.254	2	/31	1	.1111111**0**
.252	4	/30	2	.111111**00**
.248	8	/29	3	.11111**000**
.240	16	/28	4	.1111**0000**
.224	32	/27	5	.111**00000**
.192	64	/26	6	.11**000000**
.128	128	/25	7	.1**0000000**

Depuis 1993, l'Internet Engineering Task Force (IETF) a introduit un nouveau concept d'attribution de blocs d'adresses IPv4 plus souple que celui utilisé dans l'ancienne architecture d'adressage « réseau avec classes ». La nouvelle méthode est appelée « Classless Inter-Domain Routing » (CIDR) et elle est aussi utilisée avec les adresses IPv6.

Les réseaux IPv4 avec classes sont conçus en tant que Classes A, B et C, avec 8, 16 et 24 bits de nombre réseau respectivement, et en tant que Classe D utilisée pour l'adressage multidiffusion.

Exemple :
Pour donner un exemple facile à comprendre, nous allons utiliser un scénario d'adresse de Classe C. Le masque de sous-réseau par défaut d'une adresse de Classe C est 255.255.255.0. Techniquement, aucune mise en sous-réseau n'est effectuée pour ce masque, de sorte que l'intégralité du dernier octet est disponible pour un adressage hôte valide. Comme nous empruntons des bits de l'adresse hôte, nous avons les options de masque possibles suivantes dans le dernier octet :
.128, .192, .224, .240, .248 et .252.

Si le masque de sous-réseau 255.255.255.240 (4 bits) est utilisé, nous créons 16 réseaux plus petits qui prennent en charge 14 adresses hôtes par sous-réseau.
- ID de sous-réseau 0 :
  plage d'adresses hôte 192.168.1.1 à 192.168.1.14. Adresse de diffusion 192.168.1.15
- ID de sous-réseau 16 :
  plage d'adresses hôte 192.168.1.17 à 192.168.1.30. Adresse de diffusion 192.168.1.31
- ID de sous-réseau : 32, 64, 96, etc.

Pour les réseaux de plus grande taille, la Classe réseau B suivante plus grande peut être nécessaire, ou un bloc CIDR approprié est défini.

Exemple :
Avant de déployer votre réseau de sécurité vidéo, vous effectuez un simple calcul du nombre de périphériques IP nécessaires sur le réseau, afin de prévoir de la place en vue d'une croissance future :
- 20 postes de travail vidéo
- 1 serveur central
- 1 serveur VRM
- 15 applications de stockage vidéo iSCSI
- 305 caméras IP

Total = 342 adresses IP nécessaires

Si l'on tient compte du nombre calculé de 342 adresses IP, nous avons besoin au minimum d'un schéma d'adressage IP de Classe B pour accueillir autant d'adresses IP. L'utilisation du masque de sous-réseau 255.255.0.0 de Classe B par défaut permet d'utiliser
65 534 adresses IP disponibles au sein du réseau.

Il est possible également de planifier le réseau en utilisant un bloc CIDR avec 23 bits utilisés comme préfixe, ce qui fournit un espace d'adresse de 512 adresses respectivement 510 hôtes.

Vous pouvez diminuer ce risque en scindant un grand réseau en plus petits éléments, par une simple mise en sous-réseau ou l'indication d'un bloc CIDR.

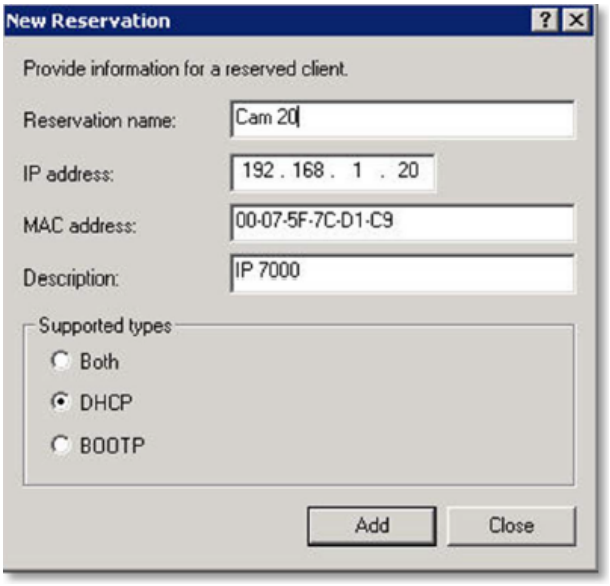
Exemple :

	Par défaut	**En sous-réseau**
Plage d'adresses IP	172.16.0.0 – 172.16.255.255	172.16.8.0 – 172.16.9.255
Masque de sous-réseau	255.255.0.0	255.255.254.0
Notation CIDR	172.16.0.0/16	172.16.8.0/23
Nombre de sous-réseaux	1	128
Nombre d'hôtes	65.534	510
Adresses en excès	65.192	168

3.1 Gestion de DHCP

IPAM peut utiliser DHCP en tant qu'outil puissant pour le contrôle et l'utilisation des adresses IP dans votre environnement. DHCP peut être configuré pour l'utilisation d'une portée spécifique d'adresses IP. Il peut aussi être configuré pour exclure une plage d'adresses.

Si DHCP est utilisé, il est préférable, lors du déploiement de périphériques vidéo, de configurer des réservations d'adresses qui n'expirent pas en fonction de l'adresse MAC de chaque périphérique.



Remarque!
Conseil de sécurité des données n°2
Même avant d'utiliser la gestion d'adresse IP pour suivre l'utilisation des adresses IP, une meilleure pratique de gestion réseau consiste à limiter l'accès au réseau via une sécurité de port sur les commutateurs latéraux ; par exemple, seule une adresse spécifique MAC peut accéder via un port spécifique.

4 Comptes utilisateur et mots de passe

Tous les périphériques vidéo IP Bosch sont fournis avec trois comptes utilisateur intégrés :

- **temps réel (live)**
  Ce compte utilisateur standard autorise uniquement l'accès à la diffusion vidéo en temps réel.
- **utilisateur (user)**
  Ce compte utilisateur plus évolué autorise l'accès aux vidéos en temps réel et enregistrées, ainsi qu'aux commande des caméras comme le contrôle PTZ.
  Ce compte n'autorise pas l'accès aux paramètres de configuration.
- **maintenance (service)**
  Ce compte administrateur permet d'accéder aux menus et paramètres de configuration de tous les périphériques.

Par défaut, aucun mot de passe n'est affecté à aucun des comptes utilisateur. L'attribution de mot de passe est une étape critique dans la protection d'un périphérique réseau. Il est vivement recommandé d'attribuer des mots de passe à tous les périphériques vidéo réseau installés.

Remarque!
Dans la version 6.30 du firmware, la gestion des utilisateurs a été améliorée pour plus de souplesse en matière d'autorisation d'autres utilisateurs et noms d'utilisateur disposant de leurs propres mots de passe. Les anciens niveaux de compte représentent désormais les niveaux de groupe utilisateur.
Dans la version 6.32 du firmware, une stratégie de mot de passe plus stricte est introduite (pour plus de détails, voir *Page Web de périphérique, Page 11*).

4.1 Application des mots de passe

L'attribution de mots de passe peut s'effectuer de différentes manières, en fonction de la taille du système de sécurité vidéo et des logiciels utilisés. Dans les installations plus petites composées de seulement quelques caméras, les mots de passe peuvent être définis à partir de la page Web d'un périphérique ou à l'aide de Bosch Configuration Manager qui est pratique car il prend en charge plusieurs configurations de périphérique simultanément et un assistant de configuration.

Remarque!
Conseil de sécurité des données n°3
Comme indiqué plus haut, la protection par mot de passe est essentielle lorsqu'il s'agit de sécuriser les données contre de possibles cyberattaques. Cela s'applique à tous les périphériques réseau de toute votre infrastructure de sécurité. La plupart des organisations disposent déjà de stratégies de mot de passe puissant, mais si vous effectuez une nouvelle installation sans aucune stratégie existante, voici quelques meilleures pratiques pour la mise en place d'une protection par mot de passe :
- Les mots de passe doivent être d'une longueur de 8 à 12 caractères.
- Les mots de passe doivent contenir à la fois des lettres en minuscules et en majuscules.
- Les mots de passe doivent contenir au moins un caractère spécial.
- Les mots de passe doivent contenir au moins un chiffre.

Exemple :
Utilisation de la phrase secrète « to be or not to be » et règles de base pour une génération de mot de passe correcte.

– 2be0rnOt!t0Be

Remarque!
Certaines restrictions s'appliquent à l'utilisation des caractères spéciaux tels que : ‘@’, '&', '<', '>', ‘:’ dans les mots de passe en raison de leur sens dédié dans XML et d'autres langage de marquage. Même si l'interface Web accepte ces caractères, d'autres logiciels de gestion et de configuration pourraient les refuser.

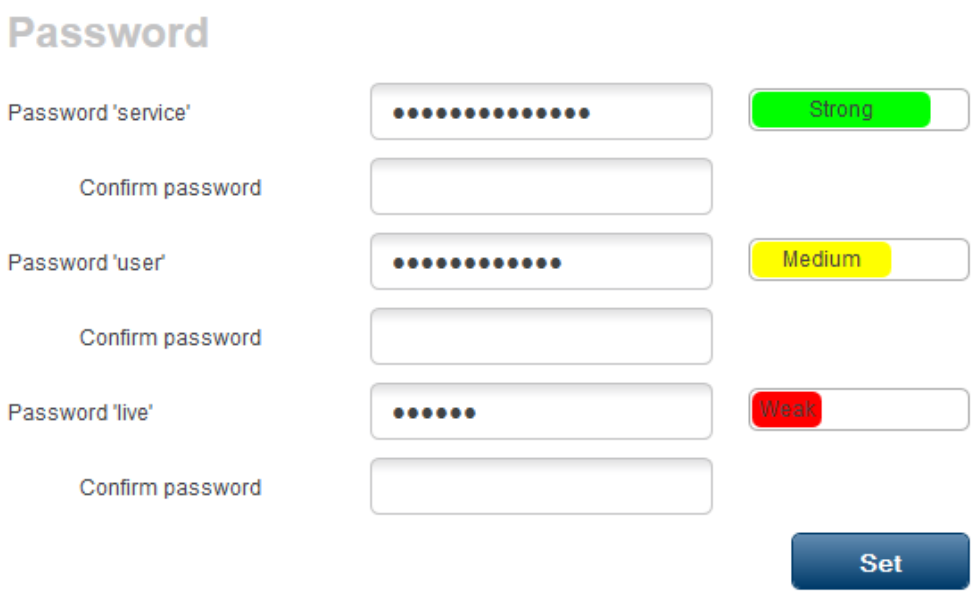
4.2 Page Web de périphérique

1. Depuis la page Web du périphérique, accédez à la page **Configuration** .
2. Sélectionnez le menu **Généralités** et le sous-menu **Gestion des utilisateurs** (Remarque : Dans les versions antérieures à la version 6.30 du firmware, le sous-menu **Gestion des utilisateurs** était appelé **Mot de passe**).

Lors du premier accès à la page Web d'une caméra, l'utilisateur est invité à attribuer des mots de passe afin de garantir une protection minimum.
Cette invite s'affiche à chaque rechargement des pages Web de la caméra jusqu'à ce que tous les mots de passe soient définis. Un clic sur **OK** permet d'accéder au menu **Gestion des utilisateurs** automatiquement.

Dans la version 6.30 du firmware, il était possible d'activer une case à cocher **Ne pas afficher...**. Cette option a été retirée dans la version 6.32 du firmware afin d'éviter des fuites de sécurité.

1. Sélectionnez le menu **Gestion des utilisateurs** , puis entrez et confirmez le mot de passe de votre choix pour chacun des trois comptes.
   Remarque :
   – Les mots de passe doivent tout d'abord être attribués au niveau d'accès le plus élevé (**Mot de passe 'service'**).
   – Depuis la version 6.20 du firmware, un nouvel indicateur appelé « mesure de puissance du mot de passe » (password strength meter) fournit des indices sur la puissance potentielle des mots de passe. Il s'agit d'un outil d'assistance qui ne garantit pas qu'un mot de passe répond réellement aux exigences de sécurité d'une installation.
2. Cliquez sur **Définir** pour appliquer et enregistrer les modifications.



La fonction **Gestion des utilisateurs** introduite dans la version 6.30 du firmware offre plus de souplesse en matière de création libre d'utilisateurs nommés disposant de leurs propres mots de passe. Les anciens niveaux de compte représentent désormais les niveaux de groupe utilisateur.

Les anciens utilisateurs continuent d'exister et utilisent les mots de passe qui leur ont été attribués dans un firmware plus ancien, ils ne peuvent pas être supprimés et leur niveau de groupe utilisateur ne peut pas être modifié.

Les mots de passe peuvent être attribués ou modifiés en cliquant sur ou .
Un message d'avertissement s'affiche dès lors que certains utilisateurs n'ont pas de protection par mot de passe.

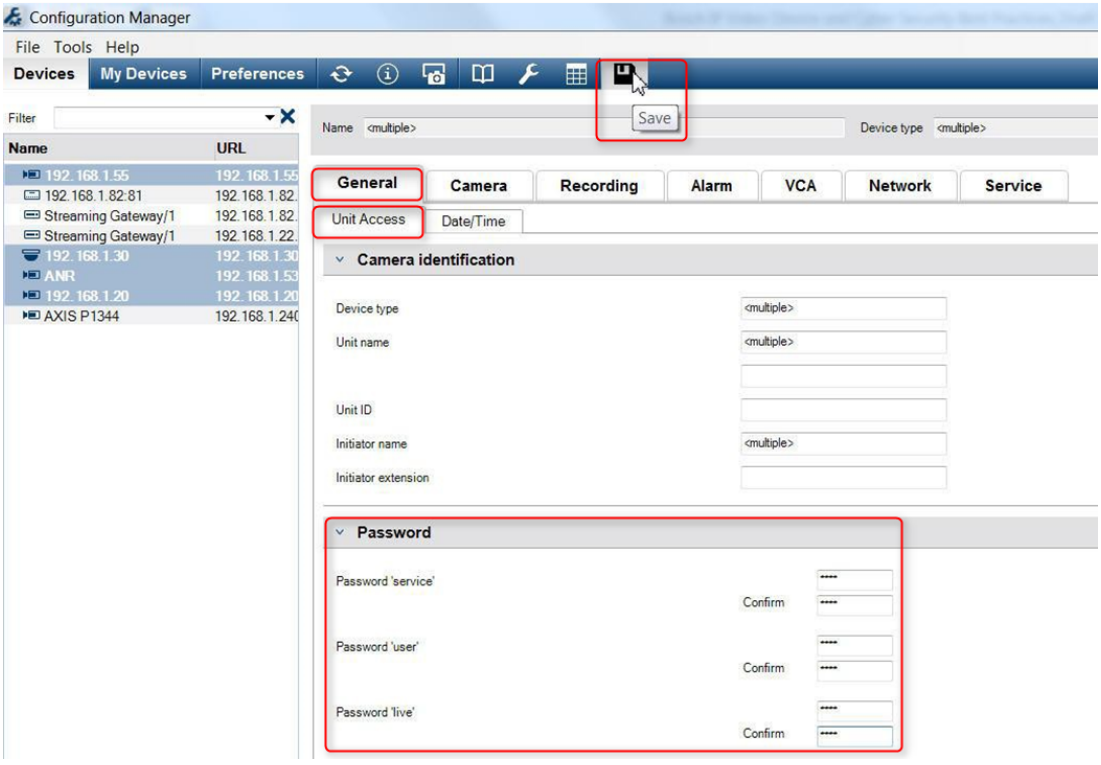
1. Pour ajouter un utilisateur, cliquez sur **Ajouter**.
   Une fenêtre contextuelle s'affiche.
2. Entrez les nouveaux identifiants et attribuez le groupe utilisateur.
3. Cliquez sur **Définir** pour enregistrer les modifications.

Remarque!
Dans la version 6.32 du firmware, une stratégie de mot de passe plus stricte a aussi été introduite.
Les mots de passe doivent désormais avoir une longueur minimum de 8 caractères.

4.3 Gestionnaire de configuration

Avec le Configuration Manager de Bosch, il est facile d'appliquer des mots de passe à des périphériques individuels ou à plusieurs périphériques simultanément.

1. Dans le Configuration Manager, sélectionnez un ou plusieurs périphériques.
2. Sélectionnez l'onglet **Généralités** , puis sélectionnez **Accès à l'appareil**.
3. Dans le menu **Mot de passe** , entrez et confirmez le mot de passe de votre choix pour chacun des trois comptes (**Mot de passe 'service'**, **Mot de passe 'user'** et **Mot de passe 'live'**).
4. Cliquez sur pour appliquer et enregistrer les modifications.



Dans les plus grandes installations qui sont gérées par Bosch Video Management System, ou Video Recording Manager installé sur un dispositif d'enregistrement, des mots de passe globaux peuvent être appliqués à tous les périphériques vidéo IP qui sont ajoutés au système. La gestion est ainsi plus facile avec la garantie d'un niveau de sécurité standard au sein de l'intégralité du système vidéo réseau.

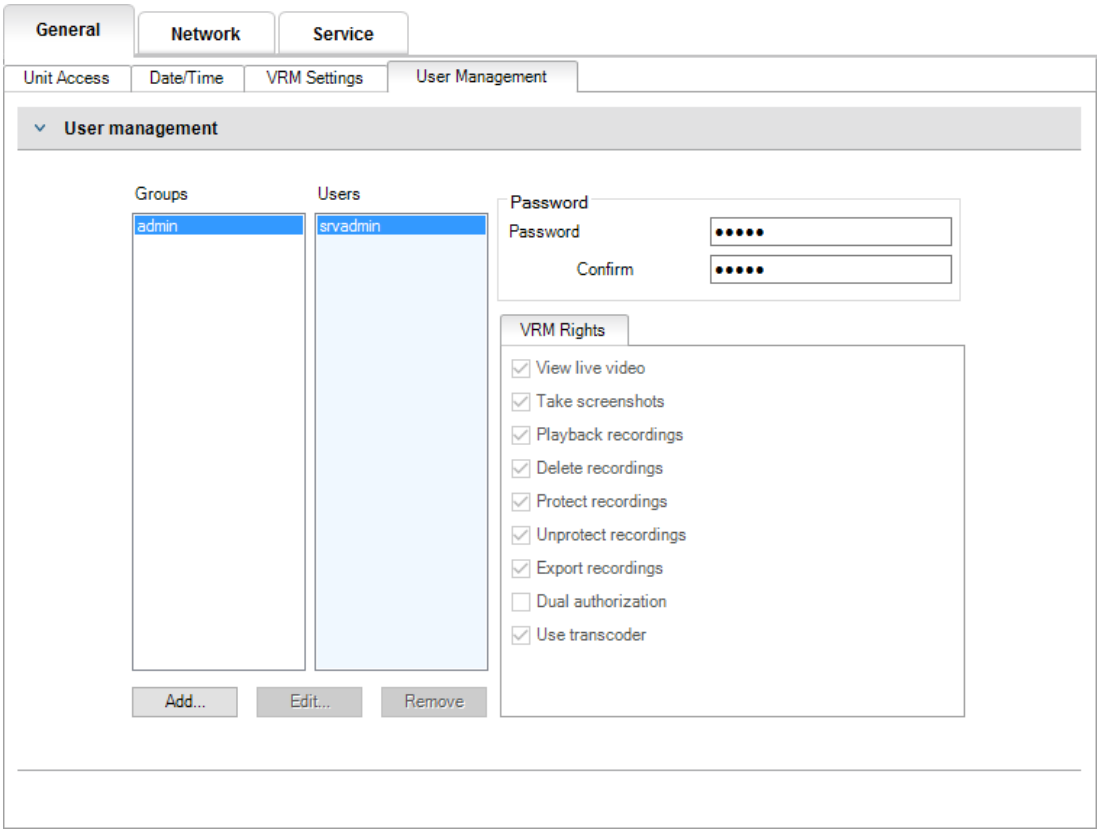
4.4 DIVAR IP 2000 / DIVAR IP 5000

Les dispositifs d'enregistrement DIVAR IP sont dotés d'un Configuration Wizard d'utilisation simple. L'attribution d'un mot de passe administrateur au niveau du système est obligatoire lors de la configuration du système. Ce mot de passe est attribué au compte service de toutes les caméras vidéo IP ajoutées au système. La possibilité d'ajouter un mot de passe de compte

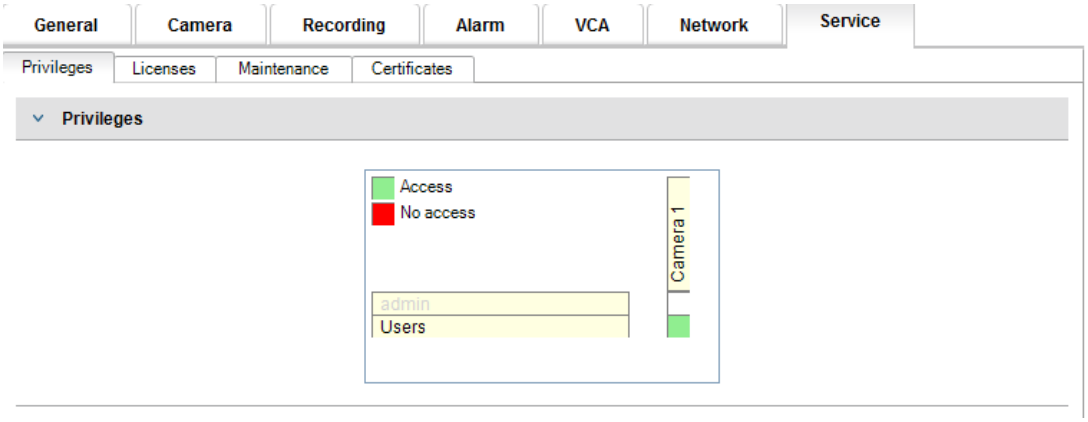
userest également offerte par l'Configuration Wizard, mais sa mise en œuvre n'est pas obligatoire. L'indicateur de puissance de mot de passe utilise un algorithme similaire à celui mis en œuvre lors de l'utilisation des pages Web de caméra.

4.5 Installation autonome de VRM

Bosch Video Recording Manager offre une fonction de gestion des utilisateurs pour améliorer la flexibilité et la sécurité.
Par défaut, aucun mot de passe n'est affecté à aucun des comptes utilisateur. L'attribution de mot de passe est une étape critique dans la protection d'un périphérique réseau. Il est vivement recommandé d'attribuer des mots de passe à tous les périphériques vidéo réseau installés.
Ceci est valable pour les utilisateurs de Video Recording Manager.



De plus, il est possible d'accorder aux membres d'un groupe d'utilisateurs l'accès à certaines caméras et des privilèges. Par conséquent, une gestion détaillée des droits peut être basée sur les utilisateurs.

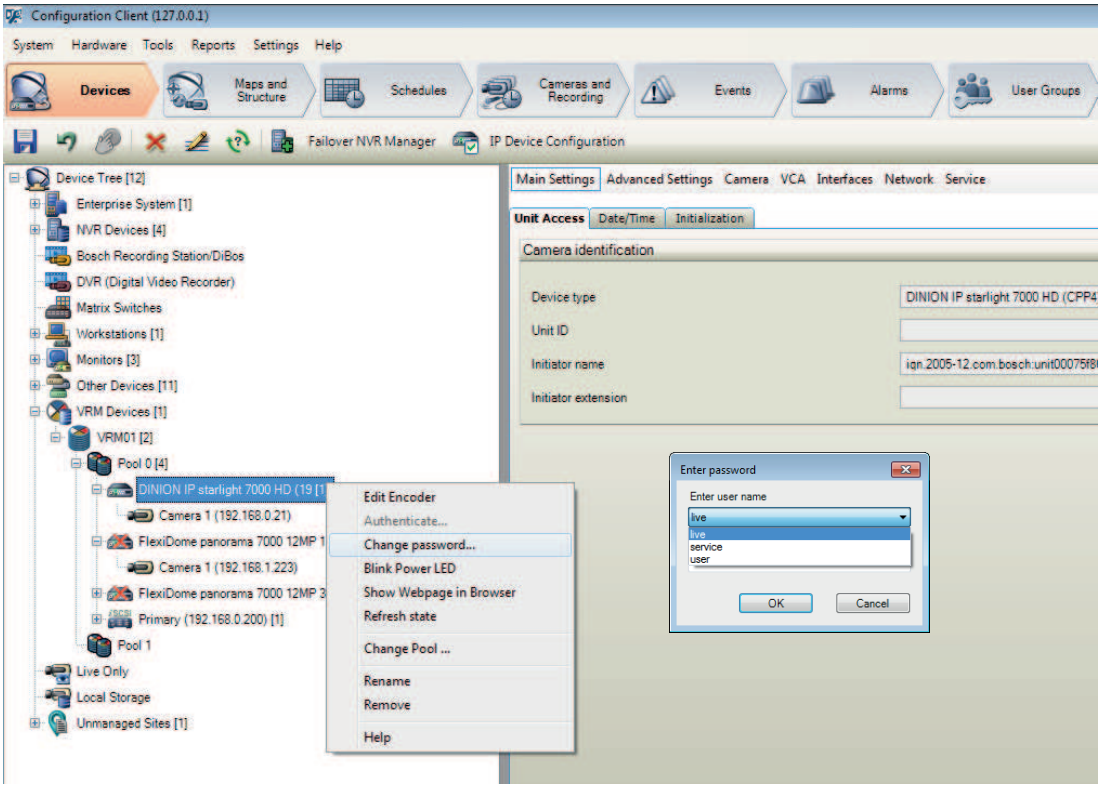


4.6 Bosch Video Management System

4.6.1 Protection par mot de passe des périphériques Bosch VMS / DIVAR IP 3000 / DIVAR IP 7000 :

Les caméras et les encodeurs, gérés par Bosch Video Management System, peuvent être protégés contre les accès non autorisés grâce à une protection par mot de passe.
Les mots de passe des comptes utilisateur intégrés des encodeurs / caméras peuvent être configurés avec Bosch Video Management System Configuration Client.
Pour définir un mot de passe pour les comptes utilisateur intégrés dans Bosch Video Management System Configuration Client :

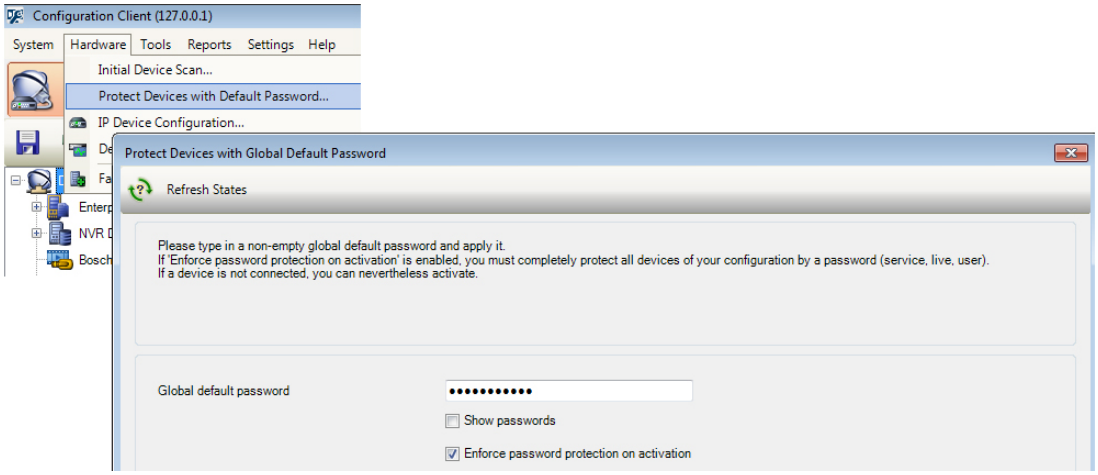
1. Dans l'arborescence des périphériques, sélectionnez l'encodeur de votre choix.
2. Faites un clic droit sur l'encodeur et cliquez sur **Modifier le mot de passe....**
3. Entrez un mot de passe pour les trois comptes utilisateur intégrés live, user et service.



4.6.2 Bosch VMS / DIVAR IP 3000 / DIVAR IP 7000 : protection par mot de passe par défaut

Les versions 5.0 et supérieures de Bosch Video Management System offrent la possibilité d'implémenter des mots de passe globaux sur tous les périphériques d'un système vidéo comportant jusqu'à 2 000 caméras IP. Cette fonctionnalité est accessible via l' Configuration Wizard de Bosch Video Management System lors de l'utilisation des dispositifs d'enregistrement DIVAR IP 3000 ou DIVAR IP 7000, ou via Bosch Video Management System Configuration Client sur un autre système.
Pour accéder au menu des mots de passe globaux dans Bosch Video Management System Configuration Client :

1. Dans le menu **Matériel** , cliquez sur **Protéger les périphériques avec un mot de passe par défaut...**.
2. Dans le champ **Mot de passe par défaut global** , entrez un mot de passe et sélectionnez **Appliquer la protection par mot de passe à l'activation**.



Après enregistrement et activation des modifications système, le mot de passe entré sera appliqué aux comptes live, user et service de tous les périphériques, y compris le compte administrateur de Video Recording Manager.

Remarque!

Si des mots de passe sont déjà définis pour les comptes sur les périphériques, ils ne seront pas remplacés.

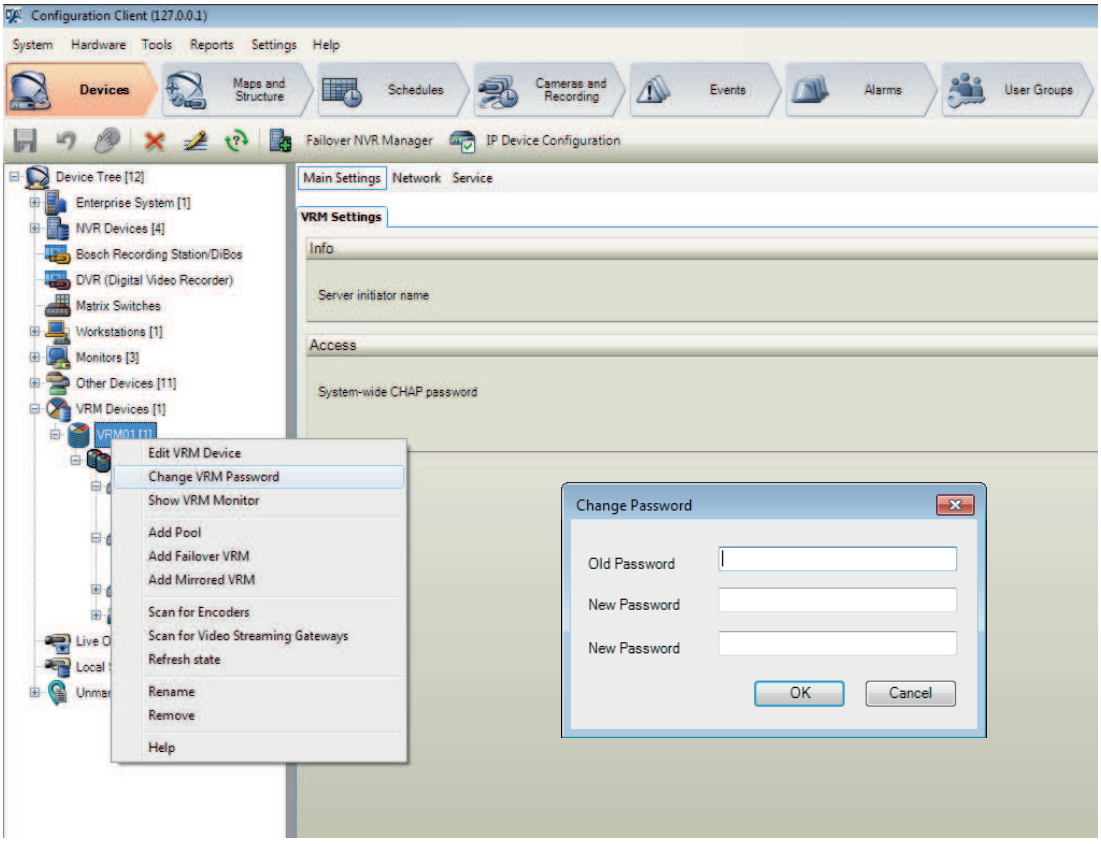
Par exemple, si un mot de passe est défini pour le compte service mais pas pour les comptes live et user, des mots de passe globaux seront uniquement configurés pour les comptes live et user.

4.6.3 Configuration de Bosch VMS et paramètres VRM

Par défaut, Bosch Video Management System utilise le compte d'administration intégré **srvadmin** pour se connecter à Video Recording Manager avec une protection par mot de passe. Pour éviter un accès non autorisé à Video Recording Manager, le compte admin **srvadmin** sera protégé avec un mot de passe complexe.

Pour modifier le mot de passe du compte **srvadmin** dans Bosch Video Management System Configuration Client :

1. Dans l'arborescence des périphériques, sélectionnez le périphérique VRM.
2. Faites un clic droit sur le périphérique VRM et cliquez sur **Modifier mot de passe VRM.** La boîte de dialogue **Modifier le mot de passe...** s'affiche.
3. Entez un nouveau mot de passe pour le compte **srvadmin** et cliquez sur **OK**.



4.6.4 Bosch VMS / DIVAR IP 3000 / DIVAR IP 7000 : communication chiffrée avec les caméras

Depuis la version 7.0 de Bosch Video Management System, il est possible de chiffrer les données vidéo et la communication en temps réel entre la caméra et Bosch Video Management System Operator Client, Configuration Client, Management Server et Video Recording Manager.

Après activation de la connexion sécurisée dans la boîte de dialogue **Modifier l'encodeur**, le serveur Bosch Video Management System Operator Client et Video Recording Manager utilisent une connexion HTTPS sécurisée pour la connexion à une caméra ou un encodeur.

La chaîne de connexion utilisée en interne par Bosch Video Management System, rcpp://a.b.c.d (connexion RCP+ brute sur le port 1756) sera remplacée par https://a.b.c.d (connexion HTTPS sur le port 443).

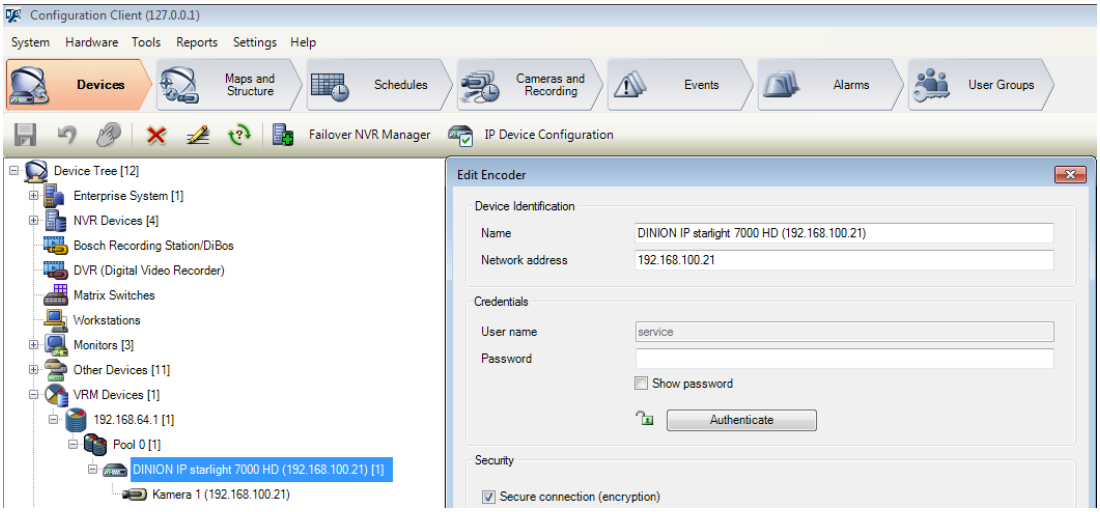
Pour les périphériques existants qui ne prennent pas en charge HTTPS, la chaîne de connexion demeure inchangée (RCP+).

Si la communication HTTPS est sélectionnée, elle utilise HTTPS (TLS) pour chiffrer toues les communications de contrôle et les contenus vidéo via le moteur de chiffrement sur le périphérique. Si TLS est utilisé, toutes les communications de contrôle et le contenu vidéo HTTPS sont chiffrés à l'aide d'une clé de chiffrement AES d'une longueur de 256 bits.

Pour activer la communication chiffrée dans Bosch Video Management System Configuration Client :

1. Dans l'arborescence des périphériques, sélectionnez l'encodeur/la caméra de votre choix.
2. Faites un clic droit sur l'encodeur/la caméra et cliquez sur **Modifier l'encodeur**.
3. Dans la boîte de dialogue **Modifier l'encodeur**, activez **Sécuriser la connexion (chiffrement).**

4. Enregistrement et activation de la configuration



Après activation de la connexion sécurisée à l'encodeur, il est possible de désactiver d'autres protocoles (voir *Utilisation du port réseau général et transmission vidéo, Page 19*).

Remarque!
Bosch VMS prend uniquement en charge le port HTTPS 443 par défaut. L'utilisation de ports différents n'est pas possible.

5 Renforcement de la sécurité d'accès aux périphériques

Tous les périphériques vidéo IP Bosch sont fournis avec des pages Web multifonction intégrées. Les pages Web spécifiques aux périphériques prennent en charge les fonctions vidéo en temps réel et lecture, ainsi que des paramètres de configuration spécifiques qui ne sont peut-être pas accessibles via un système de gestion vidéo. Les comptes utilisateur intégrés peuvent accéder aux différentes sections des pages Web dédiées. Bien que l'accès à la page Web ne puisse pas être complètement désactivé via la page Web elle-même (Configuration Manager peut être utilisé pour cela), plusieurs méthodes permettent de dissimuler la présence du périphérique, de restreindre l'accès et de gérer l'utilisation des ports vidéo.

5.1 Utilisation du port réseau général et transmission vidéo

Tous les périphériques vidéo IP Bosch utilisent Remote Control Protocol Plus (RCP+) pour la détection, le contrôle et les communications. RCP+ est un protocole Bosch propriétaire qui utilise des ports statiques spécifiques pour détecter et communiquer avec des périphériques vidéo IP Bosch : 1756, 1757 et 1758. Lors de l'utilisation de Bosch Video Management System, ou d'un autre système de gestion vidéo de fournisseur tiers doté de périphériques vidéo IP Bosch intégrés via le VideoSDK Bosch, les ports listés doivent être accessibles sur le réseau pour que les périphériques vidéo IP fonctionnent correctement.

La vidéo peut être diffusée depuis les périphériques de différentes manières : UDP (Dynamique), HTTP (80) ou HTTPS (443).
L'utilisation du port HTTP et HTTPS peut être modifiée (voir *Utilisation des ports HTTP, HTTPS et des ports vidéo, Page 20*). Avant d'apporter des modifications de port, il est nécessaire de configurer le mode de communication avec un périphérique. Le menu Communication est accessible avec Configuration Manager.

1. Dans Configuration Manager, sélectionnez le périphérique de votre choix.
2. Sélectionnez l'onglet **Généralités** , puis sélectionnez **Accès à l'appareil**.
3. Localisez la partie **Accès au périphérique** sur la page.

4. Dans la liste **Protocole**, sélectionnez le protocole de votre choix :

– RCP+
– HTTP (par défaut)
– HTTPS

Si les communications HTTPS sont sélectionnées, la communication entre Configuration Manager et les périphériques vidéo utilise HTTPS (TLS) pour chiffrer le contenu avec une clé de chiffrement AES d'une longueur de 256 bits. Il s'agit d'une fonction de base gratuite. Si TLS est utilisé, toutes les communications de contrôle HTTPS et le contenu vidéo sont chiffrés à l'aide du moteur de chiffrement sur le périphérique.

Remarque!
Le chiffrement est spécifiquement pour la « voie de transmission ». Une fois la vidéo reçue par un décodeur logiciel ou matériel, le flux est déchiffré de manière permanente.

Remarque!

Conseil de sécurité des données n°4

Lors de la définition du niveau de sécurité minimum pour l'accès aux périphériques depuis un logiciel client, assurez-vous que tous les ports et protocoles autorisant un niveau d'accès inférieur sont désactivés sur les périphériques.

5.1.1 Utilisation des ports HTTP, HTTPS et des ports vidéo

L'utilisation des ports HTTP et HTTPS sur tous les périphériques peut être modifiée ou désactivée. Une communication chiffrée peut être appliquée par la désactivation des ports RCP+ et du port HTTP, en forçant toutes les communications à utiliser le chiffrement. Si l'utilisation du port HTTP est désactivée, HTTPS demeure actif et toute tentative pour le désactiver échoue.

1. Dans Configuration Manager, sélectionnez le périphérique de votre choix.
2. Sélectionnez l'onglet **Réseau**, puis sélectionnez **Accès réseau**.
3. Localisez la partie **Détails** sur la page.

4. Dans la partie **Détails** , modifiez les ports de navigateur HTTP et HTTPS et le port RCP+ à l'aide du menu déroulant :
   - Modification du port de navigateur HTTP : 80 ou ports 10000 à 10100
   - Modification du port de navigateur HTTPS : 443 ou ports 10443 à 10543
   - Port RCP+ 1756 : **Activé** ou **Désactivé**

Remarque!

Dans la version 6.1x du firmware, si le port HTTP est désactivé et qu'une tentative est effectuée pour accéder à la page Web du périphérique, la demande est dirigée vers le port HTTPS qui est actuellement défini.

La fonction de redirection est omise à partir de la version 6.20 du firmware. Si le port HTTP est désactivé et que le port HTTPS a été modifié pour utiliser un port autre que 443, l'accès aux pages Web n'est possible qu'en accédant à l'adresse IP des périphériques et au port attribué.

Exemple :

https://192.168.1.21:10443. Toute tentative de connexion à l'adresse par défaut échoue.

5.1.2 Logiciel vidéo et sélection de port

Le réglage de ces paramètres a aussi une incidence sur le port qui est utilisé pour la transmission vidéo lors de l'utilisation d'un logiciel de gestion vidéo dans votre réseau LAN. Si tous les périphériques vidéo IP sont définis sur le port HTTP 10000, par exemple, et que Bosch Video Management System Operator Client est configuré pour la « tunnelisation TCP », toutes les transmissions vidéo sur le réseau sont effectuées via le port HTTP 10000.

Remarque!

Les modifications apportées aux paramètres de port sur les périphériques doivent correspondre aux paramètres sur le système de gestion et ses composants ainsi que sur les clients.

Remarque!
Conseil de sécurité des données n°5
En fonction du scénario de déploiement et des objectifs de sécurité de l'installation, les meilleures pratiques peuvent varier. La désactivation et la redirection de l'utilisation des ports HTTP ou HTTPS présentent ses avantages. La modification du port dans un protocole peut permettre d'éviter de fournir des informations à des outils réseau tels que NMAP (Network Mapper, scanner de sécurité gratuit). Les applications telles que NMAP sont généralement utilisées en tant qu'outils de reconnaissance pour identifier les faiblesses d'un périphérique sur un réseau. Cette technique associée à l'implémentation de mots de passe puissants permettent de renforcer la sécurité globale du système.

5.1.3 Accès Telnet

Telnet est un protocole de couche d'application qui assure la communication avec les périphériques via une session de terminal virtuelle à des fins de maintenance et de dépannage. Tous les périphériques vidéo IP Bosch sont compatibles Telnet, et par défaut la prise en charge Telnet est activée dans les versions du firmware jusqu'à la version 6.1x. À partir de la version 6.20 du firmware, le port Telnet est désactivé par défaut.

Remarque!
Conseil de sécurité des données n°6
Les cyberattaques via le protocole Telnet se sont accrues depuis 2011. Dans l'environnement d'aujourd'hui, les meilleures pratiques indiquent que vous devez désactiver la prise en charge Telnet sur tous les périphériques tant qu'elle n'est pas nécessaire pour la maintenance ou le dépannage.

1. Dans Configuration Manager, sélectionnez le périphérique de votre choix.
2. Sélectionnez l'onglet **Réseau**, puis sélectionnez **Accès réseau**.
3. Localisez la partie **Détails** sur la page.

4. Dans la partie **Détails**, vous pouvez l' **Prise en charge Telnet Activer** ou la **Désactiver** à l'aide du menu déroulant.

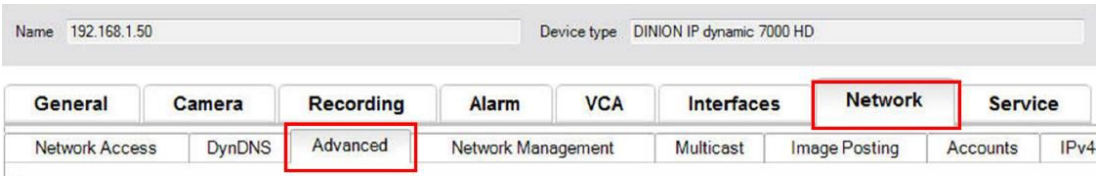
Remarque!
Conseil de sécurité des données n°7
Depuis la version 6.20 du firmware, Telnet est également pris en charge via des « sockets web », qui utilisent des connexions HTTPS sécurisées. Les sockets web n'utilisent pas le port Telnet standard et constituent un moyen sécurisé pour l'accès à l'interface de ligne de commande du périphérique IP, si nécessaire.

5.1.4 RTSP : Real Time Streaming Protocol

Real Time Streaming Protocol (RTSP) est le principal composant vidéo utilisé par le protocole ONVIF pour le contrôle de la diffusion vidéo et du périphérique sur les systèmes de gestion vidéo conformes à ONVIF. RTSP est aussi utilisé par différentes applications vidéo tierces pour

les fonctions de diffusion de base, et dans certains cas, il peut être utilisé pour le dépannage des périphériques et du réseau. Tous les périphériques vidéo IP Bosch sont capables de produire des flux à l'aide du protocole RTSP.
Les services RTSP peuvent être facilement modifiés à l'aide de Configuration Manager.

1. Dans Configuration Manager, sélectionnez le périphérique de votre choix.
2. Sélectionnez l'onglet **Réseau**, puis sélectionnez **Avancé**.



3. Localisez la partie **RTSP** sur la page.
4. Dans le menu déroulant **Port RTSP** , désactivez ou modifiez le service RSTP :
   - Port par défaut RTSP : 554
   - Modification du port RTSP : 10554 à 10664

Remarque!
Conseil de sécurité des données n°8
De récents rapports signalent des cyberattaques comportant une attaque avec dépassement de pile RTSP. Ces attaques ont ciblé les périphériques de fournisseurs spécifiques cibles. Les meilleures pratiques consisteraient à désactiver le service s'il n'est pas utilisé par un système de gestion vidéo conforme à ONVIF ou pour une diffusion en temps réel de base.
Si le client de réception l'autorise, la communication RTSP peut aussi être tunnelisée à l'aide d'une connexion HTTPS, ce qui est de loin la seule façon de transmettre des données RTSP chiffrées.

Remarque!
Pour plus de détails sur RTSP, consultez la note de service technique « RTSP usage with Bosch VIP Devices » dans le catalogue produit en ligne de Bosch Security Systems sous le lien suivant :

http://resource.boschsecurity.com/documents/RTSP_VIP_Configuration_Note_enUS_9007200806939915.pdf

5.1.5 UPnP : Universal Plug and Play

Les périphériques vidéo IP Bosch sont capables de communiquer avec des périphériques réseau via **UPnP**. Cette fonction est essentiellement utilisée sur des plus petits systèmes avec seulement quelques caméras qui apparaissent automatiquement dans le répertoire réseau du PC et peuvent ainsi être facilement détectées. Mais cela s'applique également à tout périphériques du réseau.
UPnP peut être désactivé à l'aide de Configuration Manager.

1. Dans Configuration Manager, sélectionnez le périphérique de votre choix.
2. Sélectionnez l'onglet **Réseau**, puis sélectionnez **Gestion du réseau**.

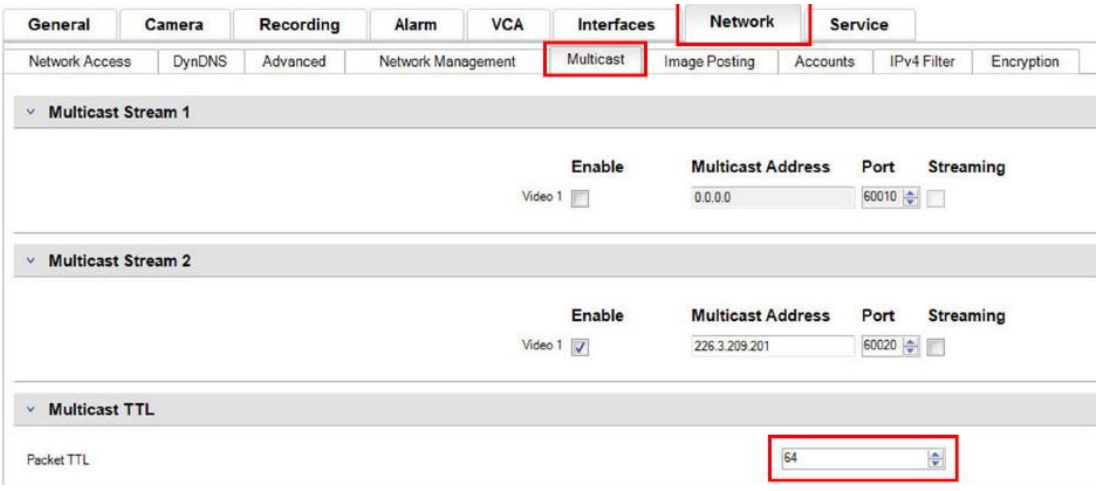
3. Localisez la partie **UPnP** sur la page.
4. Dans le menu déroulant **UPnP**, sélectionnez **Désactivé** pour désactiver **UPnP**.

Remarque!
Conseil de sécurité des données n°9
UPnPne doit pas être utilisé dans les grandes installations en raison du grand nombre de notifications d'inscription et du risque potentiel d'un accès ou d'une attaque indésirables.

5.1.6 Multidiffusion

Tous les périphériques vidéo IP Bosch sont capables de produire des vidéos « Multidiffusion à la demande » ou « Diffusion multidiffusion ». Les transmissions vidéo unicast étant basées sur la destination et les transmissions multicast étant basées sur la source, cela peut présenter des problèmes de sécurité au niveau réseau : contrôle d'accès de groupe, confiance de centre de groupe et confiance de routeur. Alors que la configuration de routeur dépasse la portée du présent guide, une solution de sécurité peut être mise en œuvre depuis le périphérique vidéo IP lui-même.
La portée TTL (time-to-live) définit où et à quelle distance le trafic multicast est autorisé à se répandre au sein d'un réseau, chaque segment diminuant la portée TTL de un. Lors de la configuration des périphériques vidéo IP pour une utilisation multicast, il est possible de modifier la portée TTL de paquet du périphérique.

1. Dans Configuration Manager, sélectionnez le périphérique de votre choix.
2. Sélectionnez l'onglet **Réseau**, puis sélectionnez **Multicast**.
3. Localisez la partie **Multicast TTL** sur la page.
4. Réglez les paramètres **Paquet TTL** à l'aide des valeurs TTL et des limites de portée suivantes :
   - Valeur TTL 0 = Portée limitée à l'hôte local
   - Valeur TTL 1 = Portée limitée au même sous-réseau
   - Valeur TTL 15 = Portée limitée au même site
   - Valeur TTL 64 (par défaut) = Portée limitée à la même région
   - Valeur TTL 127 = Portée mondiale
   - Valeur TTL 191 = Portée mondiale avec bande passante limitée
   - Valeur TTL 255 = Données non limitées

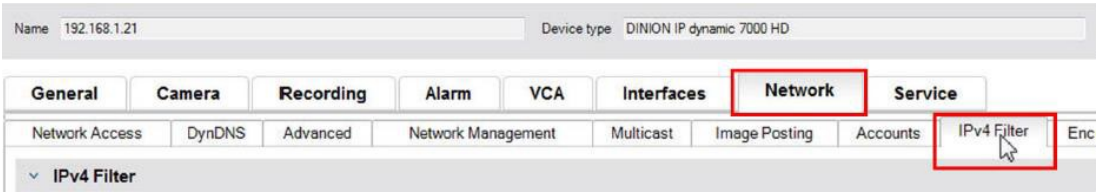


Remarque!
Conseil de sécurité des données n°10
Lorsqu'il s'agit de traiter des données de surveillance vidéo, une meilleure pratique consiste à définir vos paramètres TTL sur 15, dont la portée est limitée au même site. Ou mieux, si vous connaissez le nombre maximum exact de segments, utilisez-le comme valeur TTL.

5.1.7 Filtrage IPv4

Vous pouvez limiter l'accès à un périphérique vidéo IP Bosch via une fonction appelée filtrage IPv4. Le filtrage IPv4 utilise les fondamentaux de la « mise en sous-réseau » afin de définir jusqu'à deux plages d'adresses IP autorisées. Une fois ces plages définies, l'accès depuis une adresse IP en dehors de ces plages est refusé.

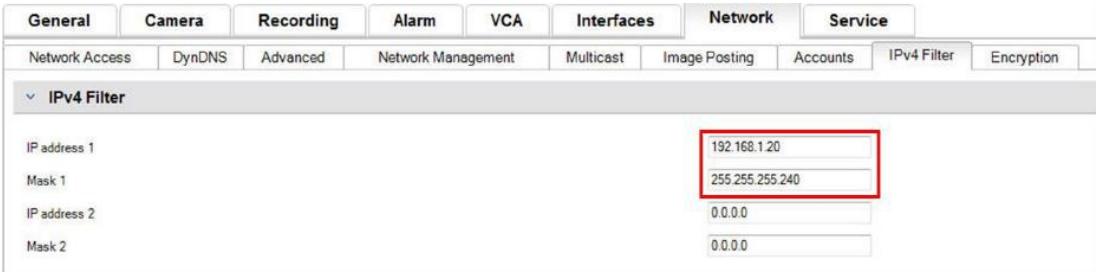
1. Dans Configuration Manager, sélectionnez le périphérique de votre choix.
2. Sélectionnez l'onglet **Réseau**, puis sélectionnez **Filtre IPv4**.



Remarque!
Pour pouvoir configurer cette fonction, vous devez posséder quelques connaissances de base sur la mise en sous-réseau ou avoir accès à un calculateur de sous-réseau. la saisie de valeurs incorrectes pour ce paramètre peut limiter l'accès au périphérique lui-même et une réinitialisation des paramètres par défaut peut être nécessaire pour récupérer l'accès.

3. Pour ajouter une règle de filtre, créez deux entrées :
   - Entrez une adresse IP de base s'inscrivant dans la règle de sous-réseau que vous créez.
     L'adresse IP de base indique le sous-réseau que vous autorisez et qui doit faire partie de la plage souhaitée.
   - Entrez un masque de sous-réseau qui définit les adresses IP avec lesquelles le périphérique vidéo IP accepte de communiquer.

Dans l'exemple suivant, l'**Adresse IP 1** 192.168.1.20 et le **Masque 1** 255.255.255.240 sont saisis. Ce paramètre limite l'accès depuis les périphériques qui entrent dans la plage d'adresses IP définie : 192.168.1.16 à 192.168.1.31.



Lors de l'utilisation de la fonction **Filtre IPv4**, les périphériques peuvent être détectés par RCP +, mais l'accès aux paramètres de configuration et aux vidéos n'est pas possible depuis des clients qui n'entrent pas dans la plage d'adresses IP autorisée. Cela inclut l'accès du navigateur Web.
Il n'est pas nécessaire que le périphérique vidéo IP lui-même se trouve dans la plage d'adresses autorisée.

Remarque!

Conseil de sécurité des données n°11

En fonction de la configuration de votre système, l'utilisation de l'option **Filtre IPv4** permet de réduire la visibilité non souhaitée des périphériques sur un réseau. Si cette fonction est activée, notez les paramètres à des fins de référence future.

Notez que le périphérique est encore accessible via IPv6, de sorte que le filtrage IPv4 n'a de réelle utilité que dans les réseaux IPv4.

5.1.8 SNMP

Simple Network Management Protocol (SNMP) est un protocole commun qui permet de surveiller l'état d'un système. Un tel système de surveillance dispose généralement d'un serveur de gestion central qui collecte l'ensemble des données des composants et périphériques compatibles du système.

SNMP fournit deux méthodes pour obtenir l'état de santé du système :

- Le serveur de gestion réseau peut interroger l'état de santé d'un périphérique via des demandes SNMP.
- Les périphériques peuvent informer de manière active le serveur de gestion réseau sur l'état de santé du système en cas d'erreur ou de conditions d'alarme par l'envoi d'alertes SNMP au serveur SNMP. De telles alertes doivent être configurées au sein du périphérique.

SNMP autorise également la configuration de certaines variables au sein des périphériques et composants.

Ces informations (messages pris en charge par un périphérique et alertes qu'il peut envoyer) sont dérivées de Management Information Base, également appelé fichier MIB, qui est fourni avec un produit pour une intégration facile à un système de surveillance réseau.

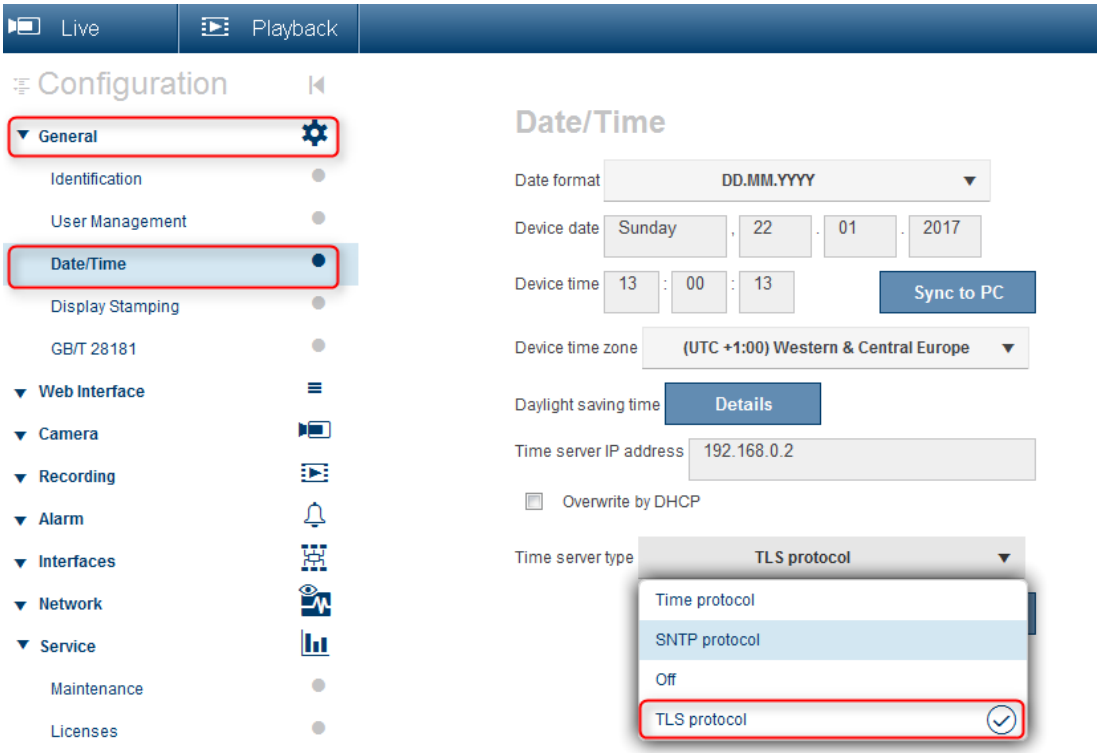
Il existe trois versions différentes du protocole SNMP :

- SNMP version 1
  SNMP version 1 (SNMPv1) est l'implémentation initiale du protocole SNMP. Il est largement utilisé et est devenu de facto le protocole standard pour la gestion et la surveillance réseau.
  Cependant, SNMPv1 est désormais menacé car il manque de fonctions de sécurité. Il utilise uniquement des '*chaînes de communauté*' comme sortes de mots de passe, qui sont transmises en texte clair.
  Par conséquent, SNMPv1 ne doit être utilisé que lorsqu'il est absolument sûr que le réseau est physiquement protégé contre tout accès non autorisé.
- SNMP version 2
  SNMP version 2 (SNMPv2) incluait des améliorations en termes de sécurité et de confidentialité, entre autres, avec l'introduction de la demande en masse pour l'extraction de grandes quantités de données en une seule demande. Toutefois, son approche de la sécurité était considérée trop complexe, ce qui a freiné son développement.
  Il a alors été rapidement remplacé par la version SNMPv2c, semblable à SNMPv2 mais sans son modèle de sécurité controversé, revenant ainsi à la méthode basée sur la communauté de SNMPv1, avec des lacunes similaires en termes de sécurité.
- SNMP version 3
  SNMP version 3 (SNMPv3) ajoute essentiellement des améliorations en termes de sécurité et de configuration à distance. Ces améliorations concernent la confidentialité grâce au chiffrement des paquets, à l'intégrité des messages et l'authentification.
  SNMP est un protocole qui convient également au déploiement à grande échelle.

Remarque!
Conseil de sécurité des données n°12
SNMPv1 et SNMPv2c sont désormais menacés car ils ne comportent pas suffisamment de fonctions de sécurité. Ils utilisent uniquement des ‘chaînes de communauté’ comme sortes de mot de passe, qui sont transmises en texte clair.
Par conséquent, SNMPv1 ou SNMPv2c ne doivent être utilisés que lorsqu'il est absolument sûr que le réseau est physiquement protégé contre tout accès non autorisé.
Les caméras Bosch à ce jour ne prennent en charge que le protocole SNMPv1. Assurez-vous que SNMP est désactivé si vous ne l'utilisez pas.

5.2 Base temporelle sécurisée

Outre le protocole horaire et SNTP, qui sont tous deux des protocoles non sécurisés, un 3e mode pour le serveur de temps est introduit avec FW 6.20, qui utilise le protocole TLS. Cette méthode est aussi couramment appelée *TLS-Date*.
Dans ce mode, tout serveur HTTPS arbitraire peut être utilisé comme serveur de temps. La valeur temporelle est dérivée comme effet secondaire du processus d'établissement de liaison HTTPS. La transmission est sécurisée par TLS. Un certificat racine en option pour le serveur HTTPS peut être chargé dans le magasin de certificats de la caméra afin d'authentifier le serveur.



Remarque!
Conseil de sécurité des données n°13
Assurez-vous que l'adresse IP de serveur de temps entrée a elle-même une base temporelle stable et non menacée.

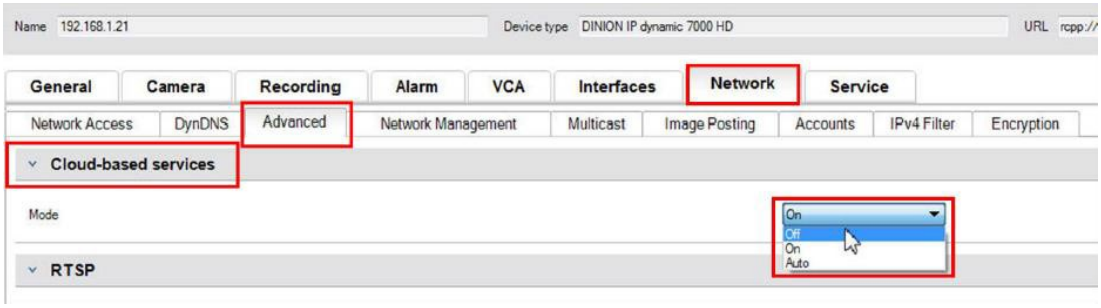
5.3 Services basés sur le cloud

L'ensemble des périphériques vidéo IP Bosch peuvent communiquer avec les **Services en nuage** Bosch. En fonction de la région de déploiement, cela permet aux périphériques vidéo IP de transférer les alarmes et autres données à un centre de télésurveillance.
Il existe trois modes de fonctionnement pour les **Services en nuage** :

- **Actif** :
  Le périphérique vidéo interroge constamment le serveur de cloud.
- **Auto** (par défaut) :
  Les périphériques vidéo essaient d'interroger le serveur de cloud quelques fois, et en cas d'échec, ils n'essaient plus d'atteindre le serveur de cloud.
- **Inactif** :
  Aucune interrogation n'est effectuée.

Les **Services en nuage** peuvent facilement être désactivés à l'aide de Configuration Manager.

1. Dans Configuration Manager, sélectionnez le périphérique de votre choix.
2. Sélectionnez l'onglet **Réseau**, puis sélectionnez **Avancé**.
3. Localisez la partie **Services en nuage** sur la page.
4. Sélectionnez **Inactif** dans le menu déroulant.



Remarque!
Conseil de sécurité des données n°14
Si vous utilisez les **Services en nuage** de Bosch, conservez la configuration par défaut.
Dans tous les autres cas, définissez les **Services en nuage** sur le mode **Inactif.**

6 Renforcement de la sécurité du stockage

Les unités de stockage iSCSI doivent être installées dans une zone sécurisée. L'accès à la zone sécurisée doit être garanti à l'aide d'un système de contrôle d'accès et il doit être surveillé. Le groupe d'utilisateurs, qui a accès à la salle du serveur central, doit être limité à un petit groupe de personnes.

Comme les caméras ou encodeurs IP Bosch peuvent établir une session iSCSI directement sur une unité iSCSI et écrire des données vidéo sur une unité iSCSI, les unités iSCSI doivent être connectées au même réseau LAN ou WAN comme les périphériques Bosch.

Pour éviter un accès non autorisé aux données vidéo enregistrées, les unités iSCSI doivent être protégées contre les accès non autorisés :

- Par défaut, les unités iSCSI accordent à tous les initiateurs iSCSI l'accès aux unités logiques iSCSI. Pour garantir que seuls les composants de la solution de gestion vidéo Bosch (caméras, encodeurs, postes de travail et serveurs) sont autorisés à accéder à l'unité logique iSCSI, le mappage d'unité logique peut être désactivé.
  Pour autoriser les périphériques à accéder aux cibles iSCSId'un Bosch Video Management System, le nom IQN (iSCSI Qualified Names) de tous les composants du Bosch Video Management System doit être configuré sur toutes les cibles iSCSI. Cela demande des efforts lors de l'installation, mais limite le risque de perte, de fuite ou de manipulation des données vidéo.
- Utilisez l'authentification par mot de passe via CHAP pour garantir que seuls les périphériques connus sont autorisés à accéder à la cible iSCSI. Définissez un mot de passe CHAP sur la cible iSCSI et entrez le mot de passe configuré dans la configuration VRM. Le mot de passe CHAP est valide pour VRM et envoyé automatiquement à tous les périphériques. Si le mot de passe CHAP est utilisé dans un environnement Bosch Video Management System VRM, tous les systèmes de stockage doivent être configurés pour l'utilisation du même mot de passe.
- Retirez tous les noms d'utilisateur et mots de passe par défaut de la cible iSCSI.
- Utilisez un mot de passe puissant pour les comptes utilisateur d'administration de la cible iSCSI.
- Désactivez l'accès administratif via telnet aux cibles iSCSI ; utilisez l'accès SSH à la place.
- Protégez l'accès de la console à la cible iSCSI avec un mot de passe puissant.
- Désactivez les cartes d'interface réseau inutilisées.
- Surveillez l'état système des stockages iSCSI à l'aide d'outils tiers afin d'identifier les anomalies.

7 Renforcement de la sécurité des serveurs

7.1 Serveurs Windows

Tous les composants de serveurs, comme Bosch VMS Management Server et le serveur Video Recording Manager, doivent être placés dans une zone sécurisée. L'accès à la zone sécurisée doit être garanti à l'aide d'un système de contrôle d'accès et il doit être surveillé. Le groupe d'utilisateurs, qui a accès à la salle du serveur central, doit être limité à un petit groupe de personnes.
Bien que le matériel serveur soit installé dans une zone sécurisé, il doit être protégé contre les accès non autorisés.

7.1.1 Paramètres recommandés pour le matériel serveur

- Le BIOS du serveur offre la possibilité de définir des mots de passe de niveau inférieur. Ces mots de passe permettent d'éviter que des personnes non autorisées puissent amorcer l'ordinateur, à partir de périphériques amovibles, et modifier les paramètres BIOS ou UEFI (Unified Extensible Firmware Interface).
- Afin d'éviter le transfert de données vers le serveur, les ports USB et le lecteur CD / DVD doivent être désactivés.
  En outre, les ports NIC inutilisés doivent être désactivés et les ports de gestion tels que l'interface HP ILO (HP Integrated Lights-Out) ou les ports de console doivent être désactivés ou protégés par mot de passe.

7.1.2 Paramètres de sécurité recommandés pour le système d'exploitation Windows

Les serveurs doivent faire partie d'un domaine Windows.
Avec l'intégration des serveurs à un domaine Windows, des droits utilisateurs sont affectés aux utilisateurs réseau gérés par un serveur central. Étant donné que ces comptes utilisateur implémentent souvent des règles de puissance et d'expiration des mots de passe, cette intégration peut améliorer la sécurité par rapport aux comptes locaux qui n'ont pas de telles restrictions.

7.1.3 Mises à jour Windows

Les correctifs et mises à jour logicielles Windows doivent être installés et actualisés. Les mises à jour Windows contiennent souvent des correctifs concernant des vulnérabilités de sécurité récemment découvertes, comme la vulnérabilité SSL Heartbleed qui a affecté des millions d'ordinateurs du monde entier. Il est nécessaire d'installer les correctifs créés pour des problèmes d'une telle ampleur.

7.1.4 Installation d'un logiciel antivirus

Installez un logiciel antivirus et anti-espion et tenez-le à jour.

7.1.5 Paramètres recommandés pour le système d'exploitation Windows

Les paramètres de stratégie de groupe locale suivants sont des paramètres de groupe recommandés sur un système d'exploitation de serveur Windows. Pour modifier les stratégies de groupe locales par défaut, utilisez l'éditeur de stratégie de groupe locale.
Pour ouvrir l'éditeur de stratégie de groupe locale, utilisez la ligne de commande ou Microsoft Management Console (MMC).

Pour ouvrir l'éditeur de stratégie de groupe locale depuis la ligne de commande :

- Cliquez sur **Démarrer**, saisissez **gpedit.msc** dans la zone de recherche **Démarrer**, et appuyez sur Entrée.

Pour ouvrir l'éditeur de stratégie de groupe locale en tant que composant logiciel enfichable :

1. Cliquez sur **Démarrer**, saisissez **mmc** dans la zone de recherche **Démarrer**, et appuyez sur Entrée.
2. Dans la boîte de dialogue **Ajouter ou supprimer des composants logiciels enfichables**, cliquez sur **Éditeur d'objets de stratégie de groupe**, puis cliquez sur **Ajouter**.
3. Dans la boîte de dialogue **Sélection d'un objet de stratégie de groupe**, cliquez sur **Parcourir**.
4. Cliquez sur **Cet ordinateur** afin d'éditer l'objet Stratégie de groupe locale, ou cliquez sur **Utilisateurs** pour éditer les objets Stratégie de groupe locale Administrateur, Non administrateur, ou par utilisateur.
5. Cliquez sur **Terminer**.

7.1.6 Activation du contrôle de compte d'utilisateur sur le serveur

LCP -> Configuration ordinateur -> Paramètres Windows -> Paramètres de sécurité -> Stratégies locales -> Options de sécurité

Contrôle de compte d'utilisateur : mode Approbation administrateur pour le compte Administrateur intégré	Activé
Contrôle de compte d'utilisateur : autoriser les applications UIAccess à demander l'élévation sans utiliser le bureau sécurisé	Désactivé
Contrôle de compte d'utilisateur : comportement de l'invite d'élévation pour les administrateurs en mode d'approbation Administrateur	Demande de consentement
Contrôle de compte d'utilisateur : comportement de l'invite d'élévation pour les utilisateurs standard	Demande d'informations d'identification sur le bureau sécurisé
Contrôle de compte d'utilisateur : détecter les installations d'applications et demander l'élévation	Activé
Contrôle de compte d'utilisateur : élever uniquement les exécutables signés et validés	Désactivé
Contrôle de compte d'utilisateur : exécuter les comptes d'administrateurs en mode d'approbation d'administrateur	Activé
Contrôle de compte d'utilisateur : passer au Bureau sécurisé lors d'une demande d'élévation	Activé
Contrôle de compte d'utilisateur : virtualiser les échecs d'écritures de fichiers et de Registre dans des emplacements définis par utilisateur	Activé

LCP -> Configuration ordinateur -> Modèles d'administration -> Composants Windows -> Interface utilisateur d'informations d'identification

Énumérer les comptes d'administrateur aux privilèges élevés	Désactivé

7.1.7 Désactiver la lecture automatique

LCP -> Configuration ordinateur -> Modèles d'administration -> Composants Windows -> Stratégies de lecture automatique

Désactiver le lecteur automatique	Activé sur tous les lecteurs
Comportement par défaut du programme Autorun	Activé, N'exécuter aucune commande d'exécution automatique
Désactiver la lecture automatique pour les périphériques autres que ceux du volume	Activé

7.1.8 Périphériques externes

LCP -> Configuration ordinateur -> Paramètres Windows -> Paramètres de sécurité -> Stratégies locales -> Options de sécurité

Périphériques : autoriser le retrait sans ouverture de session préalable	Désactivé
Périphériques : permettre le formatage et l'éjection des supports amovibles	Administrateurs
Périphériques : empêcher les utilisateurs d'installer des pilotes d'imprimante	Activé
Périphériques : autoriser l'accès au CD-ROM uniquement aux utilisateurs ayant ouvert une session localement	Activé
Périphériques : ne permettre l'accès aux disquettes qu'aux utilisateurs connectés localement	Activé

7.1.9 Configuration de l'attribution des droits utilisateur

LCP -> Configuration ordinateur -> Paramètres Windows -> Paramètres de sécurité -> Stratégies locales -> Attribution des droits utilisateur

Accéder au gestionnaire d'informations d'identification en tant qu'appelant approuvé	Personne
Accéder à cet ordinateur à partir du réseau	Utilisateurs authentifiés
Agir en tant que partie du système d'exploitation	Personne
Ajouter des stations de travail au domaine	Personne
Autoriser l'ouverture de session par les services Bureau à distance	Administrateurs, Utilisateurs du Bureau à distance
Sauvegarder les fichiers et les répertoires	Administrateurs
Modifier l'heure système	Administrateurs
Changer le fuseau horaire	Administrateurs, Système local
Créer un fichier d'échange	Administrateurs
Créer un objet-jeton	Personne
Créer des objets partagés permanents	Personne
Déboguer les programmes	Personne

Interdire l'accès à cet ordinateur à partir du réseau	Ouverture de session anonyme, Invité
Interdire l'ouverture de session en tant que tâche	Ouverture de session anonyme, Invité
Interdire l'ouverture de session en tant que service	Personne
Interdire l'ouverture d'une session locale	Ouverture de session anonyme, Invité
Interdire l’ouverture de session par les services Bureau à distance	Ouverture de session anonyme, Invité
Permettre à l’ordinateur et aux comptes d’utilisateurs d’être approuvés pour la délégation	Personne
Forcer l’arrêt à partir d’un système distant	Administrateurs
Générer des audits de sécurité	Service local, Service réseau
Augmenter la priorité de planification	Administrateurs
Charger et décharger les pilotes de périphériques	Administrateurs
Gérer le journal d’audit et de sécurité	Administrateurs
Modifier un nom d’objet	Personne
Modifier les valeurs de l’environnement du microprogramme	Administrateurs
Effectuer les tâches de maintenance de volume	Administrateurs
Processus unique du profil	Administrateurs
Performance système du profil	Administrateurs
Retirer l’ordinateur de la station d’accueil	Administrateurs
Restaurer les fichiers et les répertoires	Administrateurs
Arrêter le système	Administrateurs
Synchroniser les données du service d’annuaire	Personne
Prendre possession de fichiers ou d’autres objets	Administrateurs

7.1.10 Écran de veille

– Activer l'écran de veille protégé par mot de passe et définir un délai d'attente : **LCP -> Configuration utilisateur -> Modèles d'administration -> Panneau de configuration -> Personnalisation**

Activer l'écran de veille	Activé
Un mot de passe protège l’écran de veille	Activé
Dépassement du délai d’expiration de l’écran de veille	1800 secondes

7.1.11 Activation des paramètres de stratégie de mot de passe

– L'activation des paramètres de stratégie de mot de passe garantit que les mots de passe utilisateurs répondent aux exigences minimales concernant le mot de passe

LCP -> Paramètres Windows -> Paramètres de sécurité -> Stratégies de comptes -> Stratégie de mot de passe

Appliquer l'historique des mots de passe	10 mots de passe mémorisés
Antériorité maximale du mot de passe	90 jours
Antériorité minimale du mot de passe	1 jour
Longueur minimale du mot de passe	10 caractères
Le mot de passe doit respecter des exigences de complexité	Activé
Enregistrer le mot de passe en utilisant un chiffrement réversible pour tous les utilisateurs du domaine	Désactivé

7.1.12 Désactivation des services Windows non essentiels

– La désactivation des services Windows non essentiels permet de définir un niveau de sécurité supérieur et de minimiser les points d'attaque.

Service de la passerelle de la couche Application	Désactivé
Gestion d'applications	Désactivé
Explorateur d'ordinateurs	Désactivé
Client de suivi de lien distribué	Désactivé
Hôte du fournisseur de découverte de fonctions	Désactivé
Publication des ressources de découverte de fonctions	Désactivé
Accès du périphérique d'interface utilisateur	Désactivé
Partage de connexion Internet (ICS)	Désactivé
Mappage de découverte de topologie de la couche de liaison	Désactivé
Planificateur de classes multimédias	Désactivé
Fichiers hors connexion	Désactivé
Gestionnaire de connexion automatique d'accès distant	Désactivé
Gestionnaire de connexions d'accès distant	Désactivé
Routage et accès à distance	Désactivé
Détection matériel noyau	Désactivé
Application d’assistance de la Console d’administration spéciale	Désactivé
Découverte SSDP	Désactivé
Audio Windows	Désactivé
Générateur de points de terminaison du service Audio Windows	Désactivé

7.1.13 Comptes utilisateur du système d'exploitation Windows

Les comptes utilisateur du système d'exploitation Windows doivent être protégés par des mots de passe complexes.
Les serveurs sont habituellement gérés et administrés avec des comptes administrateur Windows ; assurez-vous que des mots de passe puissants sont utilisés pour ces comptes administrateur.

Les mots de passe doivent contenir des caractères appartenant aux trois catégories suivantes :

- Caractères majuscules des langues européennes (A à Z, avec signes diacritiques, grecs et cyrilliques)
- Caractères minuscules des langues européennes (a à z, eszett, avec signes diacritiques, grecs et cyrilliques)
- Chiffres de base 10 (0 à 9)
- Caractères non alphanumériques : ~!@#$%^&*_-+=`|\(){}[]:;"'<>,.?/
- Tout caractère Unicode classé en tant que caractère alphabétique mais non majuscule ou minuscule. Cela inclut les caractères Unicode des langues asiatiques.

Utilisation du verrouillage du compte Windows pour éviter que les attaques par programmes tentant de deviner les mots de passe ne réussissent.
La recommandation de base de sécurité de Windows 8.1 est 10/15/15 :

- 10 tentatives échouées
- Durée de verrouillage de 15 minutes
- Compteur réinitialisé au bout de 15 minutes

LCP -> Configuration ordinateur -> Paramètres Windows -> Paramètres de sécurité -> Stratégies de compte -> Stratégie de verrouillage du compte

Durée de verrouillage de comptes	Durée de verrouillage de comptes
Seuil de verrouillage de comptes de 15 minutes 10 échecs d'ouverture de session	Seuil de verrouillage de comptes de 15 minutes 10 échecs d'ouverture de session
Réinitialiser le compteur de verrouillages du compte après	Réinitialiser le compteur de verrouillages du compte après

- Assurez-vous que le mot de passe par défaut du serveur et du système d'exploitation Windows sont remplacés par de nouveaux mots de passe puissants.

7.1.14 Activation du pare-feu sur le serveur

- Activez la communication des ports standard de Bosch VMS en fonction des ports de Bosch VMS.

Remarque!
Conseil de sécurité des données n°15
Pour plus de détails sur le réglage et l'utilisation des ports, consultez la documentation relative à l'installation et à l'utilisation de Bosch VMS. Pensez à revérifier les paramètres de mise à niveau du firmware ou des logiciels.

8 Renforcement de la sécurité des clients

8.1 Postes de travail Windows

Les systèmes d'exploitation des postes de travail Windows, utilisés pour les applications client Bosch VMS comme Bosch VMS Operator Client ou Configuration Client, sont installés en dehors de la zone sécurisée. La sécurité des postes de travail doit être renforcée afin de protéger les données vidéo, les documents et les autres applications contre les accès non autorisés.
Les paramètres suivants doivent être appliqués ou vérifiés.

8.1.1 Paramètres recommandés pour le matériel des postes de travail Windows

- Définissez un mot de passe BIOS / UEFI afin d'éviter l'amorçage depuis d'autres systèmes d'exploitation.
- Afin d'éviter le transfert de données vers le client, les ports USB et le lecteur CD / DVD doivent être désactivés. En outre, les ports NIC inutilisés doivent être désactivés.

8.1.2 Paramètres de sécurité recommandés pour le système d'exploitation Windows

- Le poste de travail doit faire partie d'un domaine Windows.
  Avec l'intégration du poste de travail à un domaine Windows, il est possible de gérer de manière centralisée les paramètres de sécurité.
- Mises à jour Windows
  Tenez-vous informé des correctifs et mises à jour du système d'exploitation Windows.
- Installation d'un logiciel antivirus
  Installez un logiciel antivirus et anti-espion et tenez-le à jour.

8.1.3 Paramètres recommandés pour le système d'exploitation Windows

Les paramètres de stratégie de groupe locale suivants sont des paramètres de groupe recommandés sur un système d'exploitation de serveur Windows. Pour modifier les stratégies de groupe locales par défaut, utilisez l'éditeur de stratégie de groupe locale.
Pour ouvrir l'éditeur de stratégie de groupe locale, utilisez la ligne de commande ou Microsoft Management Console (MMC).

Pour ouvrir l'éditeur de stratégie de groupe locale depuis la ligne de commande :

- Cliquez sur **Démarrer**, saisissez **gpedit.msc** dans la zone de recherche **Démarrer**, et appuyez sur Entrée.

Pour ouvrir l'éditeur de stratégie de groupe locale en tant que composant logiciel enfichable :

1. Cliquez sur **Démarrer**, saisissez **mmc** dans la zone de recherche **Démarrer**, et appuyez sur Entrée.
2. Dans la boîte de dialogue **Ajouter ou supprimer des composants logiciels enfichables**, cliquez sur **Éditeur d'objets de stratégie de groupe**, puis cliquez sur **Ajouter**.
3. Dans la boîte de dialogue **Sélection d'un objet de stratégie de groupe**, cliquez sur **Parcourir**.
4. Cliquez sur **Cet ordinateur** afin d'éditer l'objet Stratégie de groupe locale, ou cliquez sur **Utilisateurs** pour éditer les objets Stratégie de groupe locale Administrateur, Non administrateur, ou par utilisateur.
5. Cliquez sur **Terminer**.

8.1.4 Activation du contrôle de compte d'utilisateur sur le serveur

LCP -> Configuration ordinateur -> Paramètres Windows -> Paramètres de sécurité -> Stratégies locales -> Options de sécurité

Contrôle de compte d'utilisateur : mode Approbation administrateur pour le compte Administrateur intégré	Activé
Contrôle de compte d'utilisateur : autoriser les applications UIAccess à demander l'élévation sans utiliser le bureau sécurisé	Désactivé
Contrôle de compte d'utilisateur : comportement de l'invite d'élévation pour les administrateurs en mode d'approbation Administrateur	Demande de consentement
Contrôle de compte d'utilisateur : comportement de l'invite d'élévation pour les utilisateurs standard	Demande d'informations d'identification sur le bureau sécurisé
Contrôle de compte d'utilisateur : détecter les installations d'applications et demander l'élévation	Activé
Contrôle de compte d'utilisateur : élever uniquement les exécutables signés et validés	Désactivé
Contrôle de compte d'utilisateur : exécuter les comptes d'administrateurs en mode d'approbation d'administrateur	Activé
Contrôle de compte d'utilisateur : passer au Bureau sécurisé lors d'une demande d'élévation	Activé
Contrôle de compte d'utilisateur : virtualiser les échecs d'écritures de fichiers et de Registre dans des emplacements définis par utilisateur	Activé

LCP -> Configuration ordinateur -> Modèles d'administration -> Composants Windows -> Interface utilisateur d'informations d'identification

Énumérer les comptes d'administrateur aux privilèges élevés	Désactivé

8.1.5 Désactiver la lecture automatique

LCP -> Configuration ordinateur -> Modèles d'administration -> Composants Windows -> Stratégies de lecture automatique

Désactiver le lecteur automatique	Activé sur tous les lecteurs
Comportement par défaut du programme Autorun	Activé, N'exécuter aucune commande d'exécution automatique
Désactiver la lecture automatique pour les périphériques autres que ceux du volume	Activé

8.1.6 Périphériques externes

LCP -> Configuration ordinateur -> Paramètres Windows -> Paramètres de sécurité -> Stratégies locales -> Options de sécurité

Périphériques : autoriser le retrait sans ouverture de session préalable	Désactivé
Périphériques : permettre le formatage et l'éjection des supports amovibles	Administrateurs
Périphériques : empêcher les utilisateurs d'installer des pilotes d'imprimante	Activé
Périphériques : autoriser l'accès au CD-ROM uniquement aux utilisateurs ayant ouvert une session localement	Activé
Périphériques : ne permettre l'accès aux disquettes qu'aux utilisateurs connectés localement	Activé

8.1.7 Configuration de l'attribution des droits utilisateur

LCP -> Configuration ordinateur -> Paramètres Windows -> Paramètres de sécurité -> Stratégies locales -> Attribution des droits utilisateur

Accéder au gestionnaire d’informations d’identification en tant qu’appelant approuvé	Personne
Accéder à cet ordinateur à partir du réseau	Utilisateurs authentifiés
Agir en tant que partie du système d’exploitation	Personne
Ajouter des stations de travail au domaine	Personne
Autoriser l’ouverture de session par les services Bureau à distance	Administrateurs, Utilisateurs du Bureau à distance
Sauvegarder les fichiers et les répertoires	Administrateurs
Modifier l’heure système	Administrateurs
Changer le fuseau horaire	Administrateurs, Système local
Créer un fichier d'échange	Administrateurs
Créer un objet-jeton	Personne
Créer des objets partagés permanents	Personne
Déboguer les programmes	Personne
Interdire l'accès à cet ordinateur à partir du réseau	Ouverture de session anonyme, Invité
Interdire l'ouverture de session en tant que tâche	Ouverture de session anonyme, Invité
Interdire l'ouverture de session en tant que service	Personne
Interdire l'ouverture d'une session locale	Ouverture de session anonyme, Invité

Interdire l’ouverture de session par les services Bureau à distance	Ouverture de session anonyme, Invité
Permettre à l’ordinateur et aux comptes d’utilisateurs d’être approuvés pour la délégation	Personne
Forcer l’arrêt à partir d’un système distant	Administrateurs
Générer des audits de sécurité	Service local, Service réseau
Augmenter la priorité de planification	Administrateurs
Charger et décharger les pilotes de périphériques	Administrateurs
Gérer le journal d’audit et de sécurité	Administrateurs
Modifier un nom d’objet	Personne
Modifier les valeurs de l’environnement du microprogramme	Administrateurs
Effectuer les tâches de maintenance de volume	Administrateurs
Processus unique du profil	Administrateurs
Performance système du profil	Administrateurs
Retirer l’ordinateur de la station d’accueil	Administrateurs
Restaurer les fichiers et les répertoires	Administrateurs
Arrêter le système	Administrateurs
Synchroniser les données du service d’annuaire	Personne
Prendre possession de fichiers ou d’autres objets	Administrateurs

8.1.8 Écran de veille

– Activer l'écran de veille protégé par mot de passe et définir un délai d'attente :
LCP -> Configuration utilisateur -> Modèles d'administration -> Panneau de configuration -> Personnalisation

Activer l'écran de veille	Activé
Un mot de passe protège l’écran de veille	Activé
Dépassement du délai d’expiration de l’écran de veille	1800 secondes

8.1.9 Activation des paramètres de stratégie de mot de passe

– L'activation des paramètres de stratégie de mot de passe garantit que les mots de passe utilisateurs répondent aux exigences minimales concernant le mot de passe

LCP -> Paramètres Windows -> Paramètres de sécurité -> Stratégies de comptes -> Stratégie de mot de passe

Appliquer l'historique des mots de passe	10 mots de passe mémorisés
Antériorité maximale du mot de passe	90 jours
Antériorité minimale du mot de passe	1 jour
Longueur minimale du mot de passe	10 caractères

Le mot de passe doit respecter des exigences de complexité	Activé
Enregistrer le mot de passe en utilisant un chiffrement réversible pour tous les utilisateurs du domaine	Désactivé

8.1.10 Désactivation des services Windows non essentiels

– La désactivation des services Windows non essentiels permet de définir un niveau de sécurité supérieur et de minimiser les points d'attaque.

Service de la passerelle de la couche Application	Désactivé
Gestion d'applications	Désactivé
Explorateur d'ordinateurs	Désactivé
Client de suivi de lien distribué	Désactivé
Hôte du fournisseur de découverte de fonctions	Désactivé
Publication des ressources de découverte de fonctions	Désactivé
Accès du périphérique d'interface utilisateur	Désactivé
Partage de connexion Internet (ICS)	Désactivé
Mappage de découverte de topologie de la couche de liaison	Désactivé
Planificateur de classes multimédias	Désactivé
Fichiers hors connexion	Désactivé
Gestionnaire de connexion automatique d'accès distant	Désactivé
Gestionnaire de connexions d'accès distant	Désactivé
Routage et accès à distance	Désactivé
Détection matériel noyau	Désactivé
Application d’assistance de la Console d’administration spéciale	Désactivé
Découverte SSDP	Désactivé
Audio Windows	Désactivé
Générateur de points de terminaison du service Audio Windows	Désactivé

8.1.11 Comptes utilisateur du système d'exploitation Windows

Les comptes utilisateur du système d'exploitation Windows doivent être protégés par des mots de passe complexes.
Les serveurs sont habituellement gérés et administrés avec des comptes administrateur Windows ; assurez-vous que des mots de passe puissants sont utilisés pour ces comptes administrateur.

Les mots de passe doivent contenir des caractères appartenant aux trois catégories suivantes :

– Caractères majuscules des langues européennes (A à Z, avec signes diacritiques, grecs et cyrilliques)
– Caractères minuscules des langues européennes (a à z, eszett, avec signes diacritiques, grecs et cyrilliques)
– Chiffres de base 10 (0 à 9)
– Caractères non alphanumériques : ~!@#$%^&*_-+=`|\(){}[]:;"'<>,.?/
– Tout caractère Unicode classé en tant que caractère alphabétique mais non majuscule ou minuscule. Cela inclut les caractères Unicode des langues asiatiques.

Utilisation du verrouillage du compte Windows pour éviter que les attaques par programmes tentant de deviner les mots de passe ne réussissent.
La recommandation de base de sécurité de Windows 8.1 est 10/15/15 :
– 10 tentatives échouées
– Durée de verrouillage de 15 minutes
– Compteur réinitialisé au bout de 15 minutes

LCP -> Configuration ordinateur -> Paramètres Windows -> Paramètres de sécurité -> Stratégies de compte -> Stratégie de verrouillage du compte

Durée de verrouillage de comptes	Durée de verrouillage de comptes
Seuil de verrouillage de comptes de 15 minutes 10 échecs d'ouverture de session	Seuil de verrouillage de comptes de 15 minutes 10 échecs d'ouverture de session
Réinitialiser le compteur de verrouillages du compte après	Réinitialiser le compteur de verrouillages du compte après

– Assurez-vous que le mot de passe par défaut du serveur et du système d'exploitation Windows sont remplacés par de nouveaux mots de passe puissants.
– Désactivez les comptes utilisateur du système d'exploitation Windows inutilisés.
– Désactivez l'accès Bureau à distance au poste de travail client.
– Lancez le poste de travail avec des droits non administratifs afin d'éviter qu'un utilisateur standard modifie les paramètres système.

8.1.12 Activation du pare-feu sur le poste de travail

▸ Activez la communication des ports standard de Bosch VMS en fonction des ports de Bosch VMS.

Remarque!
Conseil de sécurité des données n°16
Pour plus de détails sur le réglage et l'utilisation des ports, consultez la documentation relative à l'installation et à l'utilisation de Bosch VMS. Pensez à revérifier les paramètres de mise à niveau du firmware ou des logiciels.

9 Protection de l'accès réseau

Actuellement, de nombreux systèmes de surveillance vidéo IP de moyenne à grande taille sont déployés dans l'infrastructure réseau existante du client comme s'il s'agissait simplement d'une « autre application informatique ».
Bien que présentant des avantages en termes de coût et de maintenance, ce type de déploiement expose également le système de sécurité à des menaces indésirables, y compris en interne. Des mesures appropriées doivent être prises afin d'éviter des situations comme une fuite de vidéo d'événement sur Internet ou les réseaux sociaux. De tels événements ne sont pas simplement des violations de la vie privée, ils peuvent aussi porter préjudice à la société.

Deux technologies majeures permettent de créer un réseau dans le réseau. Le choix de l'une de ces technologies par les architectes infrastructure informatique dépend énormément de l'infrastructure réseau existante, de l'équipement réseau déployé, des fonctionnalités demandées et de la topologie du réseau.

9.1 VLAN : Réseau LAN virtuel

Il est possible de créer un réseau LAN virtuel en subdivisant un réseau LAN en plusieurs segments. La segmentation réseau peut s'effectuer à l'aide d'un commutateur réseau ou d'une configuration de routeur. L'avantage d'un réseau VLAN est que les besoins en ressources peuvent être résolus sans recâblage des connexions réseau de périphérique.
La qualité des programmes de service, appliqués à des segments spécifiques comme la vidéosurveillance, peut contribuer à améliorer non seulement la sécurité mais également les performances.

Les réseaux VLAN sont mis en œuvre sur une couche de liaison de données (OSI couche 2) et présentent des similitudes avec la mise en sous-réseau IP (voir *Attribution d'adresses IP, Page 7*) qui est similaire sur la couche réseau (OSI couche 3).

9.2 VPN : Réseau privé virtuel

Un réseau privé virtuel est un réseau (privé) distinct qui s'étend souvent aux réseaux publics ou à Internet. Différents protocoles sont disponibles pour créer un réseau VPN, généralement un tunnel qui achemine le trafic protégé. Les réseaux privés virtuels peuvent être conçus en tant que tunnels de point à point, connexions de point à point ou connexions multipoints. Les réseaux VPN peuvent être déployés avec des communications chiffrées, ou simplement reposer sur une communication sécurisée au sein du réseau VPN lui-même.

Les réseaux VPN peuvent être utilisés pour la connexion à des sites distants via des connexions de réseau WAN, tout en protégeant également la vie privée et en augmentant la sécurité au sein d'un réseau local (LAN). Dans la mesure où un réseau VPN fait office de réseau distinct, tous les périphériques qui lui sont ajoutés fonctionnent de façon transparente comme s'ils se trouvaient sur un réseau classique. Un réseau VPN ajoute non seulement une couche de protection supplémentaire à un système de surveillance mais il présente également un avantage supplémentaire : il permet de segmenter les réseaux de production entre le trafic commercial et le trafic vidéo.

Remarque!
Conseil de sécurité des données n°17
Le cas échéant, l'association des réseaux VLAN ou VPN au sein d'une infrastructure informatique existante permet d'accroître le niveau de sécurité du système de surveillance.

Outre la protection du système de surveillance contre les accès non autorisés dans une infrastructure informatique partagée, il convient de s'intéresser aux personnes autorisées à se connecter au réseau dans son ensemble.

9.3 Désactivation des ports de commutateur inutilisés

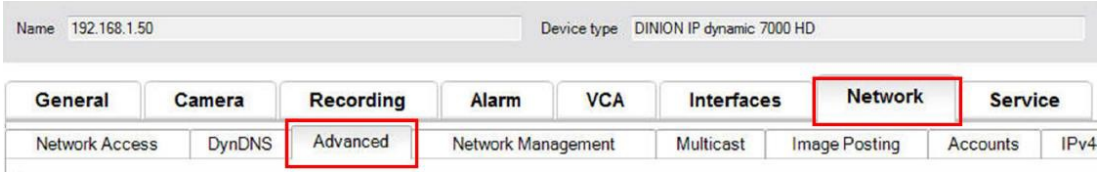
La désactivation des ports de commutateur inutilisés garantit que les périphériques inutilisés n'ont pas accès au réseau. Cela réduit le risque qu'une personne essaie d'accéder à un sous-réseau de sécurité en connectant son périphérique sur un commutateur ou un socket réseau inutilisé. L'option permettant de désactiver des ports spécifiques est une option courante sur les commutateurs gérés, qu'ils s'agisse de commutateurs à faible coût ou d'entreprise.

9.4 Réseaux protégés par le service 802.1x

Tous les périphériques vidéo IP Bosch peuvent être configurés en tant que clients 802.1x. Ils peuvent ainsi s'authentifier auprès d'un serveur RADIUS et rejoindre un réseau sécurisé. Avant de placer des périphériques vidéo sur le réseau sécurité, vous devez vous connecter directement au périphérique depuis l'ordinateur portable d'un technicien pour entrer des données d'identification valides comme indiqué dans les étapes ci-après.

Les services 802.1x peuvent être facilement configurés avec Configuration Manager.

1. Dans Configuration Manager, sélectionnez le périphérique de votre choix.
2. Sélectionnez l'onglet **Réseau**, puis sélectionnez **Avancé**.



3. Localisez la partie **802.1x** sur la page.
4. Dans le menu déroulant **802.1x** , sélectionnez **Actif.**
5. Entrez une **Identité** et un **Mot de passe valides.**
6. Enregistrez les modifications.
7. Déconnectez et placez les périphériques au sein du réseau sécurisé.

Remarque!
Le service 802.1x lui-même ne permet pas une communication sécurisée entre le demandeur et le serveur d'authentification.
Par conséquent, le nom d'utilisateur et le mot de passe pourraient être « capturés » depuis le réseau. Le service 802.1x peut utiliser EAP-TLS pour garantir une communication sécurisée.

9.4.1 Extensible Authentication Protocol - Transport Layer Security

Le protocole Extensible Authentication Protocol (EAP) prend en charge plusieurs méthodes d'authentification. Transport Layer Security (TLS) permet l'authentification mutuelle, la négociation de suite de chiffrement de protection d'intégrité ainsi que l'échange de clé entre deux nœuds finaux. EAP-TLS inclut la prise en charge d'un authentification mutuelle basée sur un certificat et la dérivation de clé. En d'autres termes, EAP-TLS encapsule le processus dans lequel serveur et client échangent un certificat.

Remarque!

Conseil de sécurité des données n°18

Pour plus de détails, consultez le livre blanc technique « Network Authentication - 802.1x – Secure the Edge of the Network », disponible dans le catalogue produit en ligne de Bosch Security Systems, à l'adresse :
http://resource.boschsecurity.com/documents/WP_802.1x_Special_enUS_22335867275.pdf.

10 Création de certificats de confiance

Toutes les caméras IP Bosch exécutant FW 6.10 ou ultérieur utilisent un magasin de certificats, lequel est accessible sous le menu **Administration** dans la configuration de la caméra.
Il est possible d'ajouter à ce magasin des certificats serveur, des certificats client et des certificats sécurisés spécifiques.
Pour ajouter un certificat au magasin :

1. Depuis la page Web du périphérique, accédez à la page **Configuration** .
2. Sélectionnez le menu **Administration** et le sous-menu **Certificats** .
3. Dans la section **Liste de fichiers** , cliquez sur **Ajouter**.
4. Téléchargez les certificats de votre choix.
   Une fois le téléchargement effectué, les certificats apparaissent dans la section **Liste d'utilisation** .
5. Dans la section **Liste d'utilisation** , sélectionnez le certificat de votre choix.
6. Pour activer l'utilisation des certificats, il est nécessaire de réamorcer la caméra. Pour ce faire, cliquez sur **Définir**.

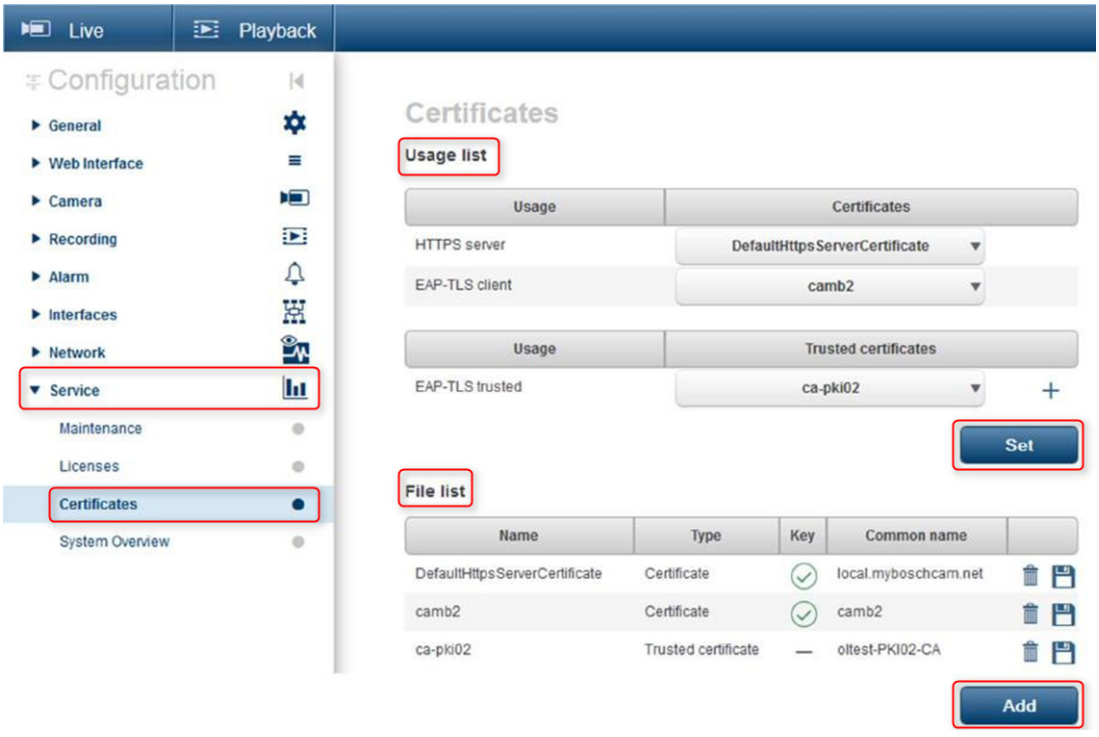


Figure 10.1: Exemple : Certificats EAP/TLS stockés sur une caméra Bosch (FW6.11)

10.1 Sécurisation dans un coffre-fort (Trusted Platform Module)

Les clés sont stockées dans une puce, également appelée « Trusted Platform Module » (ou TPM dans sa forme abrégée), comme pour une utilisation sur les cartes à puce intelligente de cryptage. Cette puce fait office de coffre-fort pour les données critiques, en protégeant les certificats, les clés, les licences, etc. contre tout accès non autorisé, même lorsque la caméra est physiquement ouverte aux accès.

Les certificats sont acceptés au format *.pem, *.cer or *.crt et ils doivent être codés en base64. Ils peuvent être téléchargés sous forme de regroupement dans un fichier, ou scindés en éléments de certificat et de clé puis téléchargés dans cet ordre sous la forme de fichiers distincts pour être automatiquement reconstruits.

Depuis le version 6.20 du firmware, les clés privés PKCS#8 protégées par mot de passe (chiffrement AES) sont prises en charge et elles doivent être téléchargées au format *.pem et codées en base64.

10.2 Certificats TLS

Tous les périphériques vidéo IP Bosch exécutant le firmware jusqu'à la version FW 6.1x sont dotés d'un certificat et d'une clé privée TLS préinstallés qui sont utilisés automatiquement pour les connexions HTTPS. Le certificat et la clé par défaut sont destinés à des fins de test uniquement, car tous les périphériques sont fournis avec le même certificat par défaut.

Depuis le version 6.20 du firmware, un certificat TLS autosigné spécifique aux périphériques est automatiquement créé lorsque nécessaire pour les connexions HTTPS, afin de permettre une authentification unique. Ce certificat autosigné peut être renouvelé manuellement par simple suppression. Le périphérique lui-même en crée un nouveau dès que cela est nécessaire.

Si les périphériques sont déployés dans un environnement où des étapes supplémentaires sont nécessaires pour valider l'identité de chaque périphérique vidéo IP individuel, il est possible de créer et de télécharger de nouveaux certificats et clés sur les périphériques vidéo eux-mêmes. De nouveaux certificats peuvent être obtenus auprès d'une autorité de certificat (CA) ou créés, par exemple, à l'aide d'un kit d'outils OpenSSL.

10.2.1 Page Web de périphérique

Les certificats peuvent être téléchargés à partir de la page Web d'un périphérique vidéo. Sur la page **Certificats** , de nouveaux certificats peuvent être créés et supprimés, et leur utilisation peut être définie.

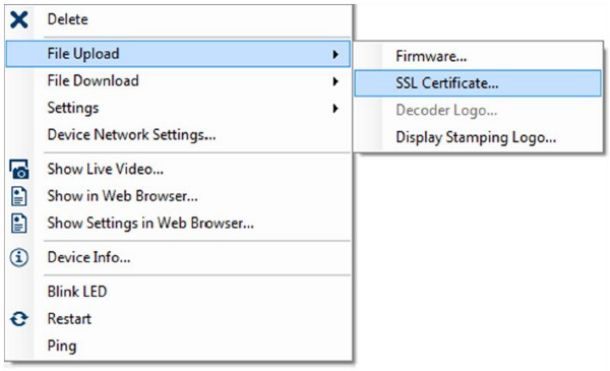
Voir également

– *Création de certificats de confiance, Page 44*

10.2.2 Gestionnaire de configuration

Dans le Configuration Manager, les certificats peuvent être facilement téléchargés sur des périphériques individuels ou sur plusieurs périphériques simultanément.
Pour télécharger des certificats :

1. Dans le Configuration Manager, sélectionnez un ou plusieurs périphériques.
2. Faites un clic droit sur **Chargement du fichier**, puis cliquez sur **Certificat SSL...**.
   Une fenêtre de l'Explorateur Windows s'ouvre pour rechercher le certificat à télécharger.



Remarque!
Les certificats peuvent être téléchargés à l'aide du Configuration Manager, mais leur utilisation doit être définie via la page Web **Certificats** .

Remarque!
Conseil de sécurité des données n°19
Les certificats doivent être utilisés pour authentifier un seul périphérique. Il est recommandé de créer un certificat spécifique par périphérique, dérivé d'un certificat racine.
Si les périphériques sont utilisés au sein de réseaux publics, il est recommandé d'obtenir les certificats auprès d'une autorité de certificat (CA) publique, ou d'avoir ses propres certificats signés par cette dernière, laquelle est également en mesure de vérifier l'origine et la validité, en d'autres termes la fiabilité, du certificat du périphérique.

11 Authentification vidéo

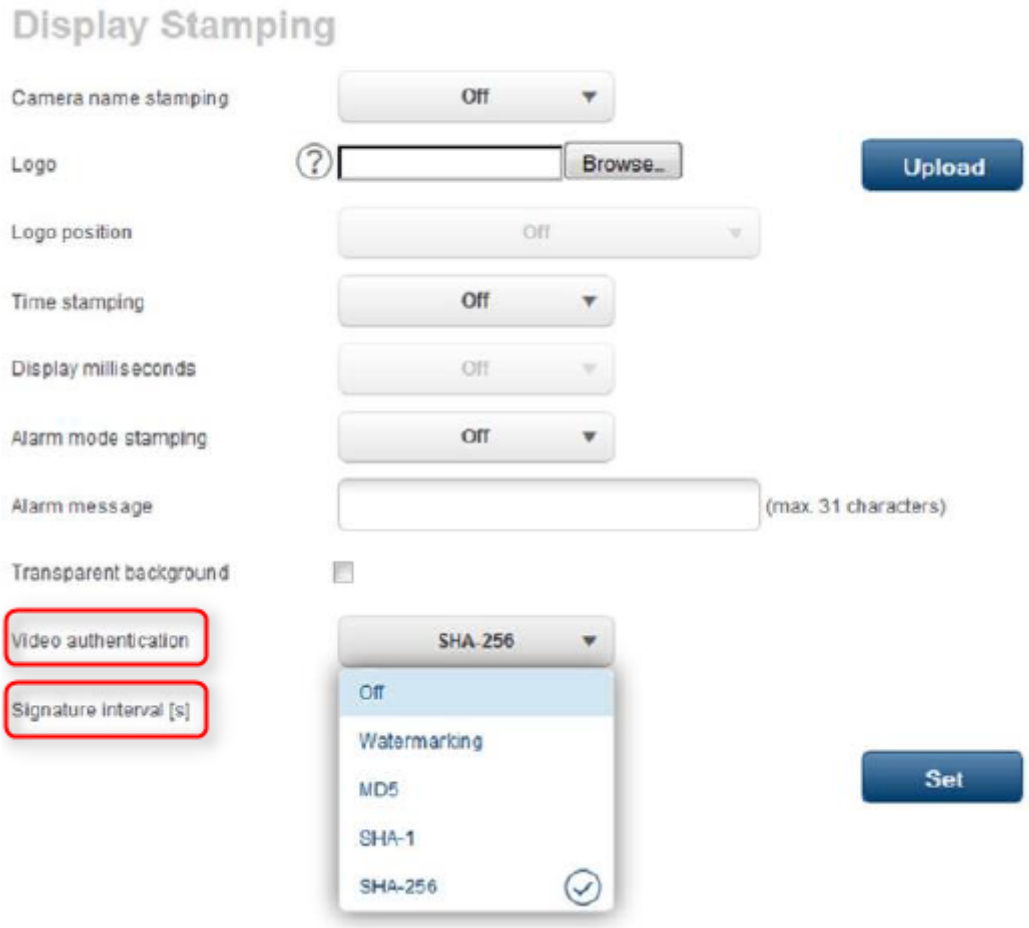
Une fois que les périphériques d'un système sont correctement protégés et authentifiés, il convient de garder un œil sur les données vidéo qu'ils fournissent. Cette méthode est appelée authentification vidéo.

L'authentification vidéo utilise seulement des méthodes de validation de l'authenticité d'une vidéo. L'authentification vidéo ne vérifie en aucun cas la transmission de vidéo, ou de données.

Dans les versions antérieures à la version 5.9 du firmware, une vérification par fonction de filigrane était effectuée via un simple algorithme de total de contrôle sur le flux vidéo. Avec ce type de vérification par filigrane, aucun certificat ni chiffrement n'est utilisé. Un total de contrôle est une mesure de base de la « fixité des données » d'un fichier et de validation de l'intégrité d'un fichier.

Pour configurer l'authentification dans le navigateur Web, par exemple :

1. Accédez au menu **Généralités** et sélectionnez **Affichage à l'écran**.
2. Dans le menu déroulant **Authentification vidéo**, sélectionnez l'option de votre choix :
   Les versions 5.9 et suivantes du firmware proposent trois options pour l'authentification vidéo en plus du filigrane classique :
   - MD5 : Synthèse de message qui produit une valeur de hachage de 128 bits.
   - SHA-1 : Conçue par la United States National Security Agency, il s'agit d'une norme FIPS (Federal Information Processing Standard) américaine publiée par la NIST des États-Unis. SHA-1 produit une valeur de hachage de 160 bits.
   - SHA-256 : L'algorithme SHA-256 génère un hachage presque unique, d'une taille fixe de 256 bits (32 octets).



Remarque!
Le hachage est une fonction à sens unique, il n'y a pas ensuite de déchiffrement possible.

Lors de l'utilisation de l'authentification vidéo, chaque paquet d'un flux vidéo est haché. Ces hachages sont imbriqués dans le flux vidéo et eux-mêmes hachés avec les données vidéo. L'intégrité du contenu vidéo est ainsi garantie.

Les hachages sont signés par périodes régulières, définies par l'intervalle de signature, à l'aide de la clé privée du certificat stockée au sein de la puce TPM du périphérique. Les enregistrements d'alarme et les modifications de bloc dans les enregistrements iSCSI sont tous fermés à l'aide d'une signature afin de garantir une authenticité vidéo continue.

Remarque!
Le calcul de la signature numérique requiert une puissance de calcul qui peut avoir une incidence sur les performances globales d'une caméra s'il a lieu trop souvent. Par conséquent, il convient de choisir un intervalle raisonnable.

Les hachages et les signatures numériques étant imbriqués dans le flux vidéo, ils sont aussi stockés dans l'enregistrement, ce qui permet également l'authentification vidéo de lectures et des exportations.

Bosch Sicherheitssysteme GmbH
Robert-Bosch-Ring 5
85630 Grasbrunn
Germany
www.boschsecurity.com