

Bosch IP video products



Table des matières

1	Objet du document et public visé	5
2	Concept et instructions de sécurité	6
3	Installation sécurisée	7
3.1	Serveurs et stockeurs	7
3.2	Caméras et périphériques	7
4	Configuration sécurisée	8
4.1	Attribution d'adresses IP	8
4.1.1	Gestion de DHCP	10
4.2	Comptes utilisateur et mots de passe	10
4.2.1	Attribution de mots de passe	11
4.2.2	Attribution de mots de passe à l'aide de la page Web du périphérique	12
4.2.3	Attribution de mots de passe à l'aide de Configuration Manager	14
4.2.4	Attribution de mots de passe pour une installation autonome VRM	14
4.2.5	Attribution de mots de passe à l'aide de BVMS (sur DIVAR IP ou autonome)	16
4.3	Renforcement de la sécurité d'accès aux périphériques	17
4.3.1	Utilisation du port réseau général et transmission vidéo	17
4.3.2	Version TLS minimum	18
4.3.3	Utilisation des ports HTTP, HTTPS et des ports vidéo	18
4.3.4	Logiciel vidéo et sélection de port	19
4.3.5	Tunnelisation SSH	19
4.3.6	Accès Telnet	20
4.3.7	RTSP : Real Time Streaming Protocol	20
4.3.8	UPnP : Universal Plug and Play	21
4.3.9	Multidiffusion	22
4.3.10	Filtrage IPv4	22
4.3.11	SNMP	23
4.3.12	Base temporelle sécurisée	25
4.3.13	Services basés sur le cloud	25
4.4	Renforcement des caméras IP	26
4.4.1	Niveaux de renforcement	26
4.4.2	Aperçu du renforcement	26
4.4.3	Description des fonctions et recommandations de renforcement	28
4.4.4	Défense en profondeur	32
4.5	Renforcement du stockage	32
4.5.1	Définition d'un mot de passe CHAP sur les périphériques iSCSI	33
4.6	Renforcement des serveurs	33
4.6.1	Paramètres recommandés pour le matériel serveur	33
4.6.2	Paramètres de sécurité recommandés pour le système d'exploitation Windows	34
4.6.3	Mises à jour Windows	34
4.6.4	Installation d'un logiciel antivirus	34
4.6.5	Paramètres recommandés pour le système d'exploitation Windows	34
4.6.6	Activation du contrôle de compte d'utilisateur sur le serveur	35
4.6.7	Désactiver la lecture automatique	35
4.6.8	Périphériques externes	35
4.6.9	Configuration de l'attribution des droits utilisateur	36
4.6.10	Écran de veille	37
4.6.11	Activation des paramètres de stratégie de mot de passe	37
4.6.12	Désactivation des services Windows non essentiels	37

4.6.13	Comptes utilisateur du système d'exploitation Windows	38
4.6.14	Activation du pare-feu sur le serveur	39
4.7	Renforcement des clients Windows	39
4.7.1	Postes de travail Windows	39
4.7.2	Paramètres recommandés pour le matériel des postes de travail Windows	39
4.7.3	Paramètres de sécurité recommandés pour le système d'exploitation Windows	39
4.7.4	Paramètres recommandés pour le système d'exploitation Windows	39
4.7.5	Activation du contrôle de compte d'utilisateur sur le serveur	40
4.7.6	Désactiver la lecture automatique	41
4.7.7	Périphériques externes	41
4.7.8	Configuration de l'attribution des droits utilisateur	41
4.7.9	Écran de veille	42
4.7.10	Activation des paramètres de stratégie de mot de passe	42
4.7.11	Désactivation des services Windows non essentiels	43
4.7.12	Comptes utilisateur du système d'exploitation Windows	43
4.7.13	Activation du pare-feu sur le poste de travail	44
4.8	Protection de l'accès réseau	44
4.8.1	VLAN : Réseau LAN virtuel	45
4.8.2	VPN : Réseau privé virtuel	45
4.8.3	Désactivation des ports de commutateur inutilisés	46
4.8.4	Réseaux protégés par le service 802.1x	46
5	Fonctionnement sécurisé	47
5.1	Séparation réseau	47
5.2	Stockage sécurisé des clés dans un coffre matériel	47
5.3	Certificats de périphériques uniques	47
5.4	Consultation des fichiers journaux	48
5.5	Système SIEM	49
5.6	Infrastructure de clés publiques (PKI)	49
5.7	AD FS	49
5.8	Fonctionnement sécurisé des caméras IP	49
5.8.1	Création de certificats de confiance	49
5.8.2	Authentification vidéo	50
6	Gestion de la mise à jour de sécurité	53
7	Surveillance de sécurité	54
8	Mise au rebut et mise hors service sécurisées	55
9	Informations supplémentaires	56
	Glossaire	57

1 **Objet du document et public visé**

La technologie évolue à une vitesse élevée, parfois même effrénée. L'évolution rapide de l'intelligence artificielle (IA) et de l'Internet des objets (IoT), ainsi que leur utilisation de masse (AIoT), modifie le profil de risque des produits et des services. Les attaques malveillantes et intentionnelles deviennent plus faciles pour davantage de personnes et plus accessibles en raison d'une meilleure connectivité. Bosch s'est fixé pour objectif de fournir des produits et des services sécurisés et fiables aux clients.

Ce guide est destiné à aider les intégrateurs à renforcer les produits vidéo IP Bosch pour une meilleure adhésion aux politiques 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

Ce guide se concentrera principalement sur l'utilisation de Configuration Manager pour effectuer les configurations décrites. Dans la plupart des cas, toutes les configurations peuvent être effectuées avec BVMS Configuration Client, Configuration Manager, ainsi que l'interface web intégrée d'un dispositif vidéo.

2 Concept et instructions de sécurité

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 Installation sécurisée

3.1 Serveurs et stockeurs

Tous les composants du serveur (BVMS Management Server et Video Recording Manager, par exemple) et les stockeurs doivent être installés dans une zone sécurisée. L'accès à la zone sécurisée doit être assurée par un système de contrôle d'accès et doit être surveillée. Le groupe d'utilisateurs qui a accès à la salle du serveur central doit être limité à un petit nombre de personnes.

Bien que les serveurs et les stockeurs soient installés dans une zone sécurisée, ils doivent être protégés contre les accès non autorisés.

Se reporter à

- *Renforcement des serveurs, page 33*
- *Renforcement du stockage, page 32*

3.2 Caméras et périphériques

Pour l'installation de caméras et de dispositifs, vous devez choisir un emplacement d'installation et un sens de montage sûrs. Idéalement, il s'agit d'un emplacement où le dispositif ne peut pas subir d'interférence, intentionnelle ou accidentelle.

4 Configuration sécurisée

4.1 Attribution d'adresses IP

L'ensemble des périphériques vidéo IP Bosch sont actuellement fournis dans un état configuré par défaut en usine et prêts à accepter une DHCP adresse IP.

Si aucun serveur DHCP n'est disponible dans le réseau actif sur lequel un périphérique est déployé, le périphérique applique automatiquement, s'il exécute un firmware version 6.32 ou supérieure, une adresse locale de liaison 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 peuvent être utilisés pour exécuter l'affectation d'adresses IP à des périphériques vidéo IP Bosch, notamment :

- Bosch Configuration Manager
- BVMS Configuration Client
- BVMS Configuration Wizard

Tous les outils logiciels offrent une option permettant d'affecter une seule adresse IPv4 statique, ainsi qu'une plage d'adresses IPv4 à plusieurs périphériques en même temps. Il peut s'agir d'un masque de sous-réseau et d'adresses de passerelle par défaut.

Toutes les adresses et valeurs des masques de sous-réseau IPv4 doivent être saisies en « notation décimale à séparation par points ».

Remarque!



L'une des premières étapes possibles, pour limiter les risques de cyberattaques internes sur un réseau, par des dispositifs réseau connectés en local et non autorisés, consiste à limiter les adresses IP inutilisées disponibles. Pour ce faire, il est nécessaire d'utiliser IPAM (**IP Address Management**), en conjonction avec la définition de la plage de sous-adresses IP qui sera utilisée.

La définition d'un sous-réseau consiste à effacer des bits de la partie hôte d'une adresse IP afin de scinder un réseau de grande taille en plusieurs réseaux de plus petite taille. Plus vous effacez des bits, plus vous créez de réseaux, mais chaque réseau prend en charge moins d'adresses hôtes.

Suffixe	Hôtes	CIDR	Effacé	Binary
.255	1	/32	0	.11111111
.254	2	/31	1	.11111110
.252	4	/30	2	.11111100
.248	8	/29	3	.11111000
.240	16	/28	4	.11110000
.224	32	/27	5	.11100000
.192	64	/26	6	.11000000
.128	128	/25	7	.10000000

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 :

	Default (Par défaut)	Mis en sous-réseau
Portée 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 plus	65.192	168

4.1.1**Gestion de DHCP**

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

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

Remarque!

Avant même de recourir à la gestion des adresses IP pour suivre l'utilisation de ces adresses IP, il est recommandé, comme bonne pratique, de limiter l'accès au réseau via la sécurité des ports sur les commutateurs d'extrémité ; par exemple, seule une adresse MAC spécifique a accès via un port spécifique.

4.2**Comptes utilisateur et mots de passe**

L'ensemble des caméras vidéo IP et encodeurs Bosch sont fournis avec trois comptes utilisateur intégrés :

- **temps réel**

Ce compte utilisateur standard ne permet d'accéder qu'à un flux vidéo en temps réel.

- **utilisateur**
Ce compte utilisateur plus avancé permet d'accéder à des vidéos en temps direct ou enregistrées, ainsi qu'aux commandes des caméras telles que les commandes PTZ. Ce compte ne permet pas d'accéder aux paramètres de configuration.
- **service**
Ce compte administrateur permet d'accéder à tous les menus et paramètres de configuration des périphériques.

Un mot de passe doit être attribué pour chacun des comptes utilisateur.

L'affectation de mot de passe constitue une étape essentielle pour la protection d'un périphérique réseau. Il est vivement recommandé d'attribuer des mots de passe à tous les périphériques vidéo réseau installés.

**Remarque!**

À compter de la version 6.30 du firmware, la gestion des utilisateurs a été améliorée pour une plus grande flexibilité de manière à autoriser d'autres utilisateurs et noms d'utilisateur avec leurs propres mots de passe. Les anciens niveaux de compte représentent désormais les niveaux de groupes d'utilisateurs.

À compter de la version 6.32 du firmware, une stratégie de mot de passe plus stricte a été introduite (pour plus de détails, voir *Attribution de mots de passe à l'aide de la page Web du périphérique, page 12*).

4.2.1

Attribution de 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!**

Comme indiqué précédemment, la protection par mot de passe est indispensable pour sécuriser les données contre d'éventuelles cyberattaques. Ce conseil vaut pour tous les dispositifs réseau de l'ensemble de votre infrastructure de sécurité. La plupart des organisations appliquent déjà des stratégies de mot de passe fort, mais si vous utilisez une nouvelle installation à laquelle aucune stratégie n'est appliquée, voici certaines des meilleures pratiques recommandées pour la mise en œuvre d'une protection par mot de passe :

- Les mots de passe doivent comporter de 8 à 12 caractères.
- Les mots de passe doivent contenir à la fois des majuscules et des minuscules.
- 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.

4.2.2**Attribution de mots de passe à l'aide de la page Web du 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 : avant la version 6.30 du firmware, le sous-menu **Gestion des utilisateurs** s'intitulait **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.

Password

Password 'service'	<input type="password" value="....."/>	Strong
Confirm password	<input type="password"/>	
Password 'user'	<input type="password" value="....."/>	Medium
Confirm password	<input type="password"/>	
Password 'live'	<input type="password" value="....."/>	Weak
Confirm password	<input type="password"/>	



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.

User Management

 Please make sure that all users are password protected.

User name	Group	Type	
service	service	Password	 
user	user	Password	 
live	live	Password	 

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.

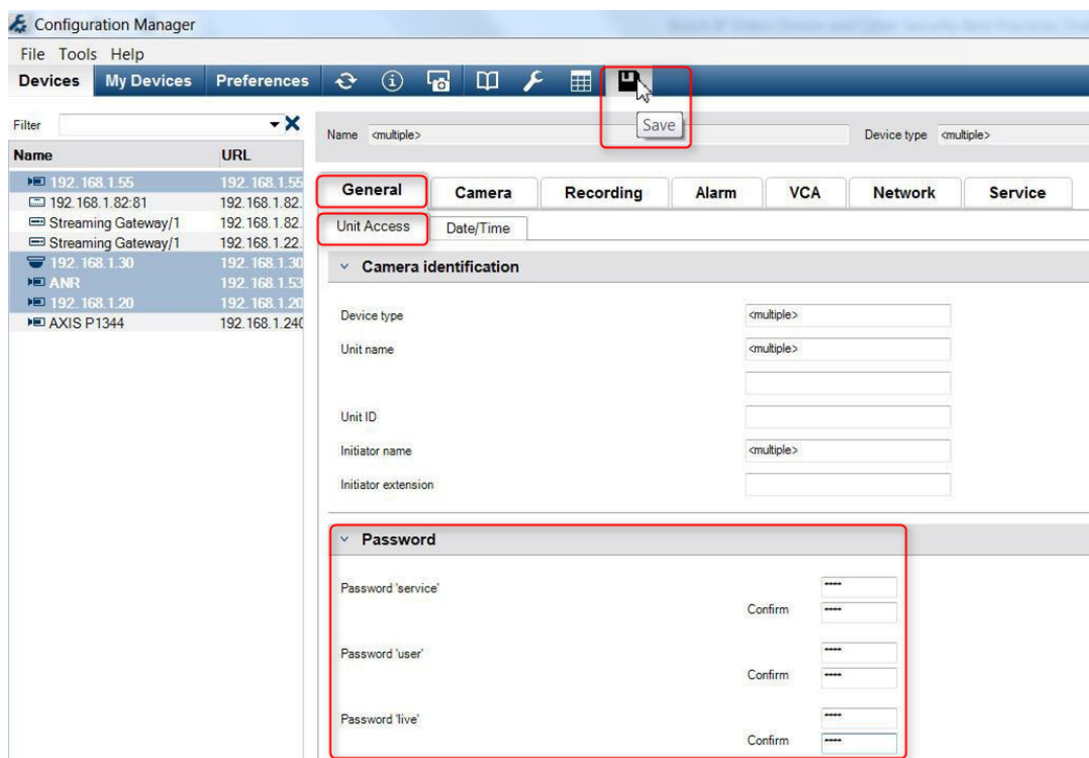
4.2.3

Attribution de mots de passe à l'aide de Configuration Manager

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 installations plus grandes qui sont gérés par BVMS, 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. Cela permet une gestion aisée et garantit un niveau de sécurité standard sur l'ensemble du système vidéo du réseau.

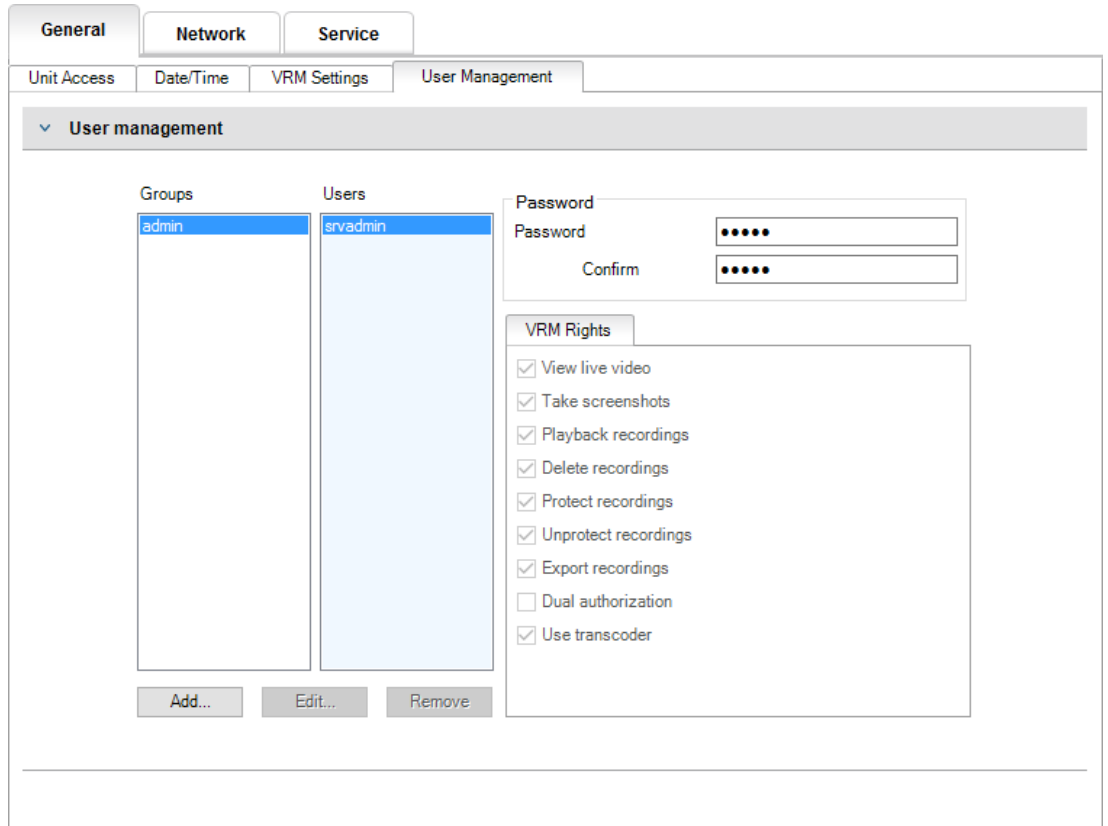
4.2.4

Attribution de mots de passe pour une installation autonome VRM

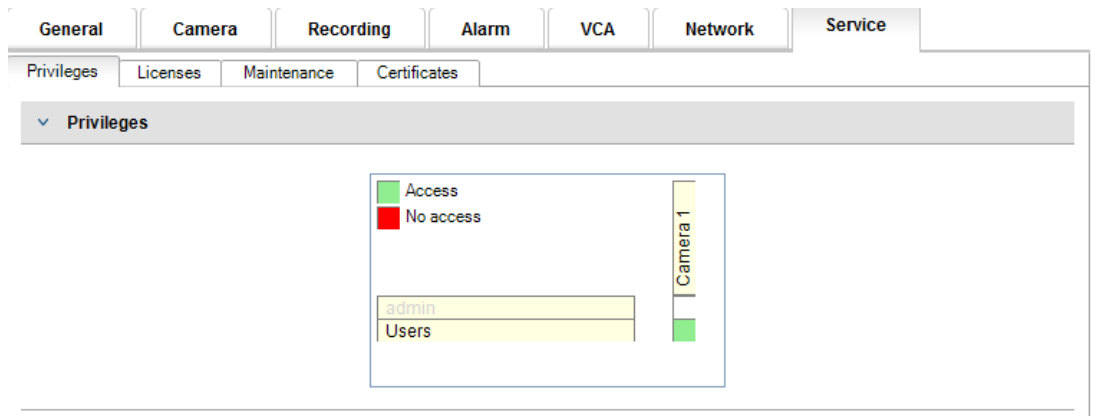
Video Recording Manager permet une gestion des utilisateurs qui améliore la flexibilité et la sécurité.

Par défaut, aucun mot de passe n'est affecté aux comptes d'utilisateur. L'affectation de mot de passe constitue une étape essentielle pour 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.



4.2.5 Attribution de mots de passe à l'aide de BVMS (sur DIVAR IP ou autonome)

Protection du périphérique par un mot de passe

Les caméras et encodeurs, gérés par BVMS, peuvent être protégés contre les accès non autorisés à l'aide d'un mot de passe.

Les mots de passe des comptes utilisateur intégrés des encodeurs/caméras peuvent être configurés avec BVMS Configuration Client.

Pour définir un mot de passe de comptes d'utilisateur intégrés dans BVMS

Configuration Client :

1. Dans l'arborescence des périphériques, sélectionnez l'encodeur souhaité.
2. Cliquez avec le bouton droit de la souris sur l'encodeur et cliquez sur **Modifier le mot de passe...**
3. Saisissez un mot de passe pour les trois comptes utilisateur intégrés live, user et service.

Protection à l'aide d'un mot de passe par défaut

BVMS Les versions 5.0 et supérieures offrent la possibilité d'appliquer des mots de passe globaux à tous les périphériques d'un système vidéo de 2 000 caméras IP au plus. Il est possible d'accéder à cette fonction via BVMS Configuration Wizard lors de l'utilisation des systèmes d'enregistrement DIVAR IP 3000 ou DIVAR IP 7000, ou via BVMS Configuration Client sur n'importe quel système.

Pour accéder au menu des mots de passe globaux dans BVMS 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**, saisissez un mot de passe et sélectionnez **Appliquer la protection par mot de passe lors de l'activation**

Une fois les modifications système enregistrées et activées, le mot de passe saisi sera appliqué aux comptes live, user et service de tous les périphériques, y compris au compte administrateur de Video Recording Manager.



Remarque!

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

Par exemple, si un mot de passe est défini pour service mais pas pour live et user, un mot de passe global ne sera configuré que pour les comptes live et user.

Configuration BVMS et paramètres VRM

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

Pour modifier le mot de passe du compte **srvadmin** dans BVMS Configuration Client :

1. Dans l'arborescence des dispositifs, sélectionnez le dispositif VRM.
2. Cliquez avec le bouton droit de la souris sur le périphérique VRM et cliquez sur **Modifier mot de passe VRM.**

La boîte de dialogue **Modifier le mot de passe...** s'affiche.

3. Entrez ensuite un mot de passe pour le compte **srvadmin** et cliquez sur **OK.**

Communication chiffrée avec les caméras

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

Après activation de la connexion sécurisée dans la boîte de dialogue **Modifier l'encodeur**, BVMS Server, Operator Client and Video Recording Manager utilise une connexion HTTPS sécurisée pour se connecter à une caméra ou un encodeur.

La chaîne de connexion utilisée en interne par BVMS, 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 (RCP+) demeure inchangée.

Si vous sélectionnez la communication HTTPS, la communication utilisera HTTPS (TLS) pour chiffrer l'ensemble des communications de commande et la charge utile vidéo via le moteur de chiffrement sur le périphérique. Lors de l'utilisation de TLS, l'ensemble des communications de commande HTTPS et la charge utile vidéo sont chiffrées à l'aide d'une clé de chiffrement AES jusqu'à 256 bits.

Pour activer la communication chiffrée dans BVMS Configuration Client :

1. Dans l'arborescence des périphériques, sélectionnez l'encodeur/la caméra souhaités.
2. Cliquez avec le bouton droit de la souris sur l'encodeur/la caméra et cliquez sur **Modifier l'encodeur**.
3. Dans la boîte de dialogue **Modifier l'encodeur**, activez **Connexion sécurisée**.
4. Enregistrez et activez la configuration.

Après activation de la connexion sécurisée à l'encodeur, il est possible de chiffrer d'autres protocoles (voir *Utilisation du port réseau général et transmission vidéo*, page 17).



Remarque!

BVMS prend uniquement en charge le port HTTPS 443 par défaut. L'utilisation de ports différents n'est pas prise en charge.

4.3

Renforcement de la sécurité d'accès aux périphériques

L'ensemble des périphériques vidéo IP Bosch sont conçus avec des pages Web multifonctions intégrées. Les pages Web spécifiques au périphérique prennent en charge les fonctions de lecture et d'enregistrement vidéo, ainsi que certains paramètres de configuration spécifiques qui peuvent ne pas être accessibles via un système de gestion vidéo. Les comptes utilisateur intégrés permettent d'accéder aux différentes sections des pages Web dédiées. Même s'il est impossible de désactiver complètement l'accès à la page Web via la page Web elle-même - Configuration Manager pouvant être utilisé pour cela, il existe plusieurs méthodes pour occulter la présence du périphérique, restreindre l'accès et gérer l'utilisation des ports vidéo.

4.3.1

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 les périphériques vidéo IP Bosch - 1756, 1757 et 1758 et communiquer avec eux. Lors de l'utilisation de BVMS, ou d'un autre système de gestion vidéo tiers disposant de périphériques vidéo Bosch intégrés via Bosch VideoSDK, les ports répertoriés doivent être accessibles sur le réseau afin que les périphériques vidéo IP puissent fonctionner correctement.

La vidéo peut être diffusée depuis les périphériques de différentes façons : UDP (Dynamic), HTTP (80) ou HTTPS (443).

L'utilisation des ports HTTP et HTTPS peut être modifiée (voir *Utilisation des ports HTTP, HTTPS et des ports vidéo, page 18*). Avant d'effectuer des modifications de port, il est nécessaire de configurer la forme de communication souhaitée avec un périphérique. Le menu Communication est accessible via 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.

4.3.2

Version TLS minimum

Certains clients plus anciens peuvent avoir besoin d'utiliser des versions TLS plus anciennes et moins sécurisées. Cependant, si possible, définissez une version minimale de TLS afin d'éviter que les clients forcent le périphérique à utiliser un mode d'accès moins sécurisé. Sélectionnez la version TLS la plus élevée possible comme version minimale.



Remarque!

Lors de la définition du niveau de sécurité minimum pour l'accès aux périphériques depuis un logiciel client, assurez-vous que l'ensemble des ports et protocoles permettant un niveau d'accès inférieur sont arrêtés ou désactivés dans les périphériques.

4.3.3

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. Des communications chiffrées peuvent être mises en œuvre en désactivant le port RCP+ ainsi que le port HTTP, ce qui force toutes les communications à utiliser le chiffrement. Si l'utilisation des ports HTTP est désactivée, HTTPS reste actif et toutes les tentatives pour le désactiver échouent.

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.

4.3.4

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 configurés sur le port HTTP 10000, par exemple, et que BVMS Operator Client est configuré pour la « tunnelisation TCP », toutes les transmissions vidéo sur le réseau s'effectuent 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!

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 présente des avantages. Changer de port dans le cadre de l'un de ces protocoles peut permettre d'éviter de fournir des informations aux outils réseau tels que NMAP (Network Mapper, scanner de sécurité gratuit). Les applications telles que NMAP sont généralement utilisées comme outils de reconnaissance pour identifier les faiblesses d'un périphérique sur un réseau. Cette technique, associée à l'implémentation d'un mot de passe fort, renforce la sécurité globale du système.

4.3.5

Tunnelisation SSH

Pour un accès distant aux périphérique avec BVMS Operator Client via des réseaux publics, BVMS offre une tunnelisation Secure Shell (SSH) pour garantir une communication sécurisée (chiffrée).

La tunnelisation SSH construit un tunnel chiffré établi par une protocole SSH/une connexion socket. Ce tunnel chiffré peut fournir transport au trafic chiffré et non chiffré. La mise en œuvre de Bosch SSH utilise également le protocole Omni-Path, qui est un protocole de communication à faible latence hautement performant développé par Intel.

Pour plus d'informations sur la configuration du service SSH dans BVMS, reportez-vous à la documentation BVMS.

Pour plus d'informations sur la configuration des systèmes DIVAR IP pour un accès distant sécurisé avec BVMS Operator Client, consultez la documentation DIVAR IP.

4.3.6

Accès Telnet

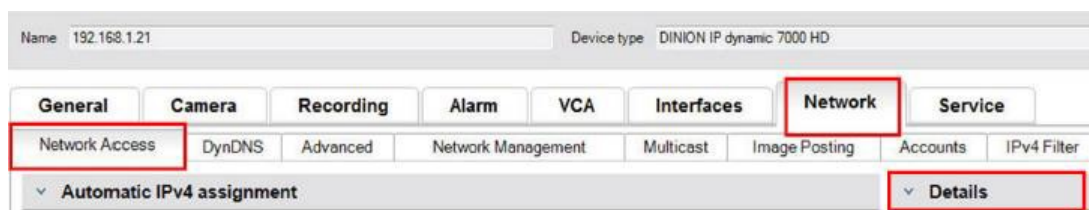
Telnet est un protocole de couche d'application qui permet la communication avec des périphériques via une session de terminal virtuelle à des fins de maintenance et de dépannage. L'ensemble des périphériques vidéo IP Bosch sont pris en charge par Telnet et, par défaut, la prise en charge Telnet est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



Remarque!

Le nombre de cyberattaques utilisant le protocole Telnet a augmenté depuis 2011. Dans l'environnement actuel, les meilleures pratiques consistent à désactiver la prise en charge Telnet sur tous les périphériques tant qu'il 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!

Depuis la version 6.20 du firmware, Telnet est également pris en charge par les « prises Web », qui utilisent des connexions HTTPS sécurisées. Les prises Web n'utilisent pas un port Telnet standard, elles offrent un moyen sécurisé d'accéder à l'interface de ligne de commande du périphérique IP, le cas échéant.

4.3.7

RTSP : Real Time Streaming Protocol

Real Time Streaming Protocol (RTSP) est le principal composant vidéo utilisé par le protocole ONVIF pour offrir une diffusion de la vidéo et une commande des périphériques aux systèmes de gestion vidéo conformes aux normes ONVIF. RTSP est également utilisé par diverses applications vidéo tierces pour des fonctions de diffusion de base et, dans certains cas, il peut être utilisé pour le dépannage des périphériques et du réseau. L'ensemble des périphériques vidéo IP Bosch sont en mesure de fournir 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.

- Sélectionnez l'onglet **Réseau**, puis sélectionnez **Avancé**.



- Localisez la partie **RTSP** sur la page.
- 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!

De récents rapports signalent des cyberattaques utilisant un assaut par débordement du tampon de pile RTSP. Ces attaques ont été écrites pour cibler des périphériques de fournisseurs spécifiques. Les meilleures pratiques consistent à désactiver le service s'il n'est pas utilisé par un système de gestion vidéo conforme aux normes ONVIF ou pour une diffusion de base de données en temps réel.

Il est également possible de tunneliser la communication RTSP, lorsque le client le permet, à l'aide d'une connexion HTTPS ; il s'agit à ce jour du seul moyen de transmettre des données RTSP chiffrées.



Remarque!

Pour plus de détails sur RTSP, reportez-vous à la note d'application relative à *l'utilisation de RTSP avec des périphériques Bosch VIP* dans le catalogue de produits en ligne Bosch Security Systems, en suivant le lien suivant :

https://resources-boschsecurity-cdn.azureedge.net/public/documents/RTSP_VIP_Application_note_enUS_9007200806939915.pdf

4.3.8

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.

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



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



Remarque!

UPnP ne doit pas être utilisé dans les installations de grande taille en raison du grand nombre de notifications d'enregistrement et d'un risque potentiel d'accès ou d'attaques indésirables.

4.3.9

Multidiffusion

L'ensemble des dispositifs vidéo IP de Bosch peuvent fournir des vidéos de type « Multicast on Demand » (Multicast à la demande) ou « Multicast Streaming » (Diffusion multicast). Lorsque les transmissions vidéo unicast sont basées sur la destination, le multicast est basé sur la source, ce qui peut présenter des problèmes de sécurité au niveau du réseau, notamment : contrôle de l'accès de groupe, confiance dans un centre de groupe et confiance dans le routeur. Bien que la configuration du routeur dépasse la portée de ce guide, il existe une solution de sécurité pouvant être implémentée à partir du dispositif vidéo IP lui-même. La durée de vie TTL (Time-To-Live) définit la portée de diffusion du trafic multicast au sein d'un réseau, chaque saut décrémentant la valeur TTL d'une unité. Lorsque vous configurez un dispositif vidéo IP pour une utilisation en multicast, vous pouvez modifier le paquet TTL du dispositif.

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

The screenshot shows the configuration interface for Multicast. The 'Network' tab is selected, and the 'Multicast' sub-tab is active. The page is divided into sections for Multicast Stream 1, Multicast Stream 2, and Multicast TTL. The Packet TTL is set to 64.

Stream	Enable	Multicast Address	Port	Streaming
Multicast Stream 1	<input type="checkbox"/>	0.0.0.0	60010	<input type="checkbox"/>
Multicast Stream 2	<input checked="" type="checkbox"/>	226.3.209.201	60020	<input type="checkbox"/>

Multicast TTL

Packet TTL: 64



Remarque!

En matière de données de vidéosurveillance, il est préférable de définir vos paramètres TTL sur 15, limités au même site. Ou mieux encore, si vous connaissez le nombre maximal exact de sauts, utilisez les valeurs TTL suivantes.

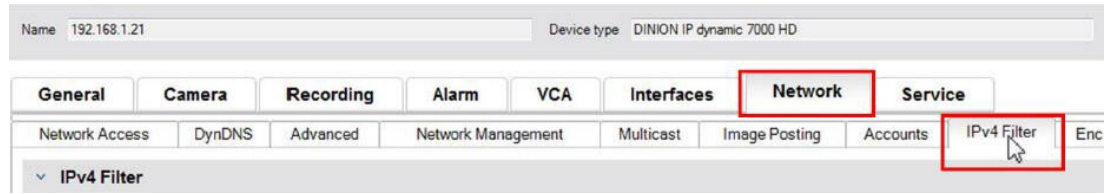
4.3.10

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**.

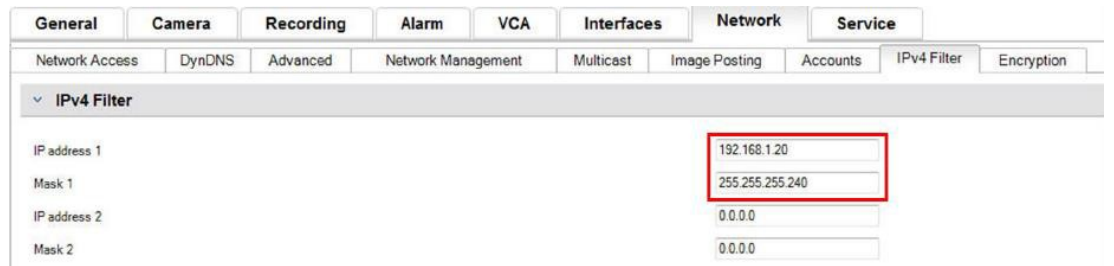


Remarque!

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!

En fonction de la configuration de votre système, l'utilisation de l'option **Filtre IPv4** peut réduire la visibilité non souhaitée des dispositifs sur un réseau. Si vous activez cette fonction, assurez-vous de bien documenter les paramètres pour référence ultérieure.

Notez que les dispositifs seront toujours accessibles via IPv6. Le filtrage IPv4 n'a donc de sens que pour les réseaux IPv4.

4.3.11

SNMP

Simple Network Management Protocol (SNMP) est un protocole commun pour la surveillance de l'état d'un système. Un système de surveillance de ce type dispose généralement d'un serveur central qui recueille toutes les données des composants et périphériques compatibles du système.

SNMP offre deux méthodes pour obtenir l'état de votre système :

- Le serveur de gestion du réseau peut interroger l'état d'un périphérique à l'aide de requêtes SNMP.
- Les périphériques peuvent activement informer le serveur réseau de l'état de leur système en cas d'erreur ou de conditions d'alarme par l'envoi de traps SNMP au serveur SNMP. Ces traps doivent être configurés à l'intérieur 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!

Les versions SNMPv1 et SNMPv2c sont toutes deux menacées du fait de leur manque de fonctionnalités de sécurité. Elles utilisent uniquement des chaînes de communauté en guise de mots de passe, et ces chaînes sont transmises en texte clair.

SNMPv1 ou SNMPv2c ne doit donc être utilisé que lorsqu'il est certain que le réseau est physiquement protégé contre les accès non autorisés.

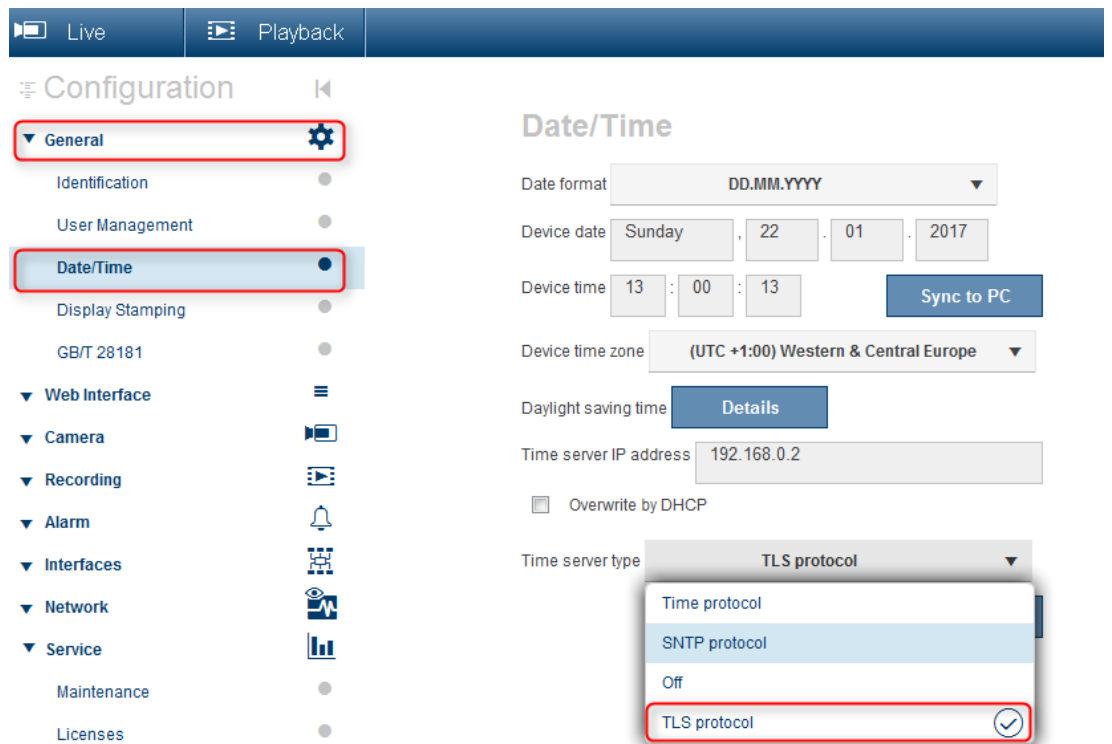
Les caméras Bosch ne prennent actuellement en charge que SNMPv1. Assurez-vous d'avoir désactivé SNMP si vous ne l'utilisez pas.



4.3.12 Base temporelle sécurisée

En plus du protocole de synchronisation et du protocole SNTP, qui sont deux protocoles non sécurisés, un 3eme mode pour le client Timeserver a été introduit avec FW 6.20, qui utilise le protocole TLS. Cette méthode est 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!

Assurez-vous que l'adresse IP saisie pour le serveur de temps possède une base de temps stable et optimale.

4.3.13 Services basés sur le cloud

L'ensemble des périphériques vidéo IP Bosch peuvent communiquer avec des Bosch services cloud tels que Remote Portal. Selon la région dans laquelle les dispositifs vidéo IP sont déployés, ces derniers peuvent utiliser des services tels que Remote Device Management ou Cloud VMS pour transmettre des alarmes et d'autres données à un centre de télésurveillance. Pour plus d'informations, reportez-vous à Bosch Building Technologies – Base de connaissances :

<https://community.boschsecurity.com>.

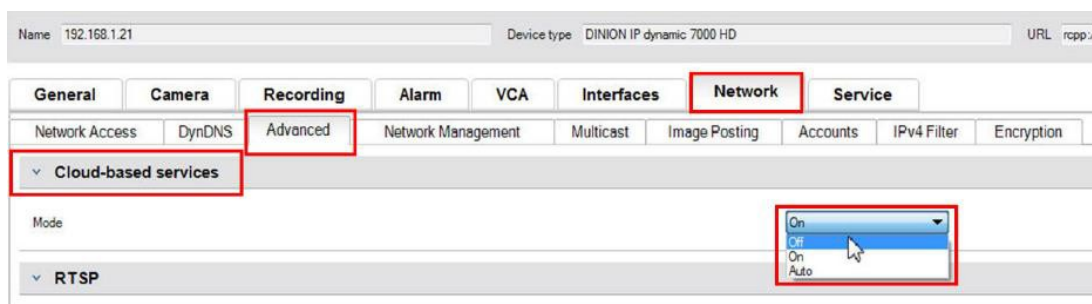
Les services Cloud proposent trois modes de fonctionnement :

- **On (activé) :**
Le périphérique vidéo interrogera en permanence le serveur cloud.

- **Auto** (valeur par défaut) :
Les dispositifs vidéo essaieront d'interroger le serveur cloud plusieurs fois, et s'ils échouent, ils cesseront leurs tentatives.
- **Off (désactivé)** :
Aucune interrogation n'est effectuée.

Les services dans le cloud" peuvent être facilement désactivés à l'aide de Configuration Manager.

1. Dans Configuration Manager, sélectionnez le périphérique de votre choix.
2. Sélectionnez l'onglet **Réseau**, puis l'onglet **Avancé**.
3. Localisez la section **Services en nuage** de la page et sélectionnez **Off (désactivé)** dans la liste.



Remarque!

Si vous utilisez les services cloud de Bosch, conservez la configuration par défaut. Dans tous les autres cas, définissez le mode des services cloud sur **Off (désactivé)**.

4.4 Renforcement des caméras IP

Les caméras IP Bosch sont livrées avec une configuration par défaut qui permet une intégration facile dans différents environnements.

En fonction de l'environnement cible et du niveau de sécurité prévu, il peut être nécessaire de modifier certains paramètres de la caméra afin d'augmenter la cybersécurité et la sécurité des données.

Cependant, l'environnement opérationnel peut être limité à l'utilisation d'un certain protocole ou d'une fonction moins sécurisée (SNMPv1, par exemple).

4.4.1 Niveaux de renforcement

Deux niveaux de renforcement sont définis : *élevé* et *strict*.

Le niveau de renforcement *strict* dispose du mode de configuration de périphérique le plus sécurisé, mais il peut limiter l'usage du périphérique car certaines fonctions, telles que la détection automatique d'un périphérique, sont désactivées. Pour chaque fonction, il convient d'évaluer si le paramètre *élevé* ou *strict* peut être appliqué.

4.4.2 Aperçu du renforcement

Réseau - Services de réseau	Default (Par défaut)	Élevé	Strict
HTTP	Activé	Désactivé	Désactivé
HTTPS	Activé	Activé	Activé
RTSP	Activé	Facultatif	Désactivé

Réseau - Services de réseau	Default (Par défaut)	Élevé	Strict
RCP	Activé	Désactivé	Désactivé
SNMPv1	Désactivé	Désactivé	Désactivé
SNMPv3	Désactivé	Activé	Activé
iSCSI	Activé	Facultatif	Désactivé
UPnP	Désactivé	Désactivé	Désactivé
Serveur NTP	Désactivé	Désactivé	Désactivé
Discovery	Activé	Activé	Désactivé
ONVIF Discovery	Activé	Activé	Désactivé
GBT/28181	Désactivé	Désactivé	Désactivé
Mécanisme de réinitialisation du mot de passe	Activé	Désactivé	Désactivé
Réponse Ping	Activé	Activé	Désactivé
RTSPS	Activé	Activé	Activé
HTTP	Activé	Désactivé	Désactivé

Réseau - Accès réseau	Default (Par défaut)	Élevé	Strict
Version TLS minimum	1.0	1.2	1.2
HSTS	Désactivé	Activé	Activé

Réseau - Avancé	Default (Par défaut)	Élevé	Strict
802.1x	Désactivé	Facultatif	Activé
Syslog	Désactivé	TCP	TLS

Réseau - Gestion du réseau	Default (Par défaut)	Élevé	Strict
Mode SNMPv3	Désactivé	SHA1 / AES	SHA1 / AES

Réseau - Filtre IPv4	Default (Par défaut)	Élevé	Strict
Filtre IPv4	Désactivé	Activé	Activé

Généralités - Date/Heure	Default (Par défaut)	Élevé	Strict
Date/Heure (client NTP)	Désactivé	Date SNTP / TLS	Date TLS

Connectivité - Services cloud	Default (Par défaut)	Élevé	Strict
Remote Portal	Désactivé	Activé	Activé

Administration - Journalisation	Default (Par défaut)	Élevé	Strict
Scellage logiciel	Désactivé	Activé	Activé

4.4.3

Description des fonctions et recommandations de renforcement

HTTP

HTTP est activé par défaut, mais non chiffré. Les identifiants ou paramètres sont ainsi transférés sous forme non chiffrée s'ils sont utilisés.

Recommandation : le HTTP brut doit être désactivé au profit du HTTPS chiffré, en particulier si le réseau n'est pas fiable.

HTTPS

HTTPS est chiffré et doit être le choix par défaut pour accéder à l'interface Web ou pour accéder à l'API RCP Web. L'utilisation de PKI et de certificats propres est recommandée.

Recommandation : HTTPS est le protocole sécurisé par défaut qui est utilisé pour la configuration et il doit demeurer activé.

RTSP

RTSP est utilisé pour le flux vidéo, mais il est normalement non chiffré. Si le logiciel qui reçoit le flux vidéo est capable d'utiliser RTSPS, il est recommandé de désactiver le RTSP brut. Lorsque vous utilisez d'autres composants Bosch (par exemple, des décodeurs/BVMS/VRM/DIVAR IP), il est possible d'activer un chiffrement propriétaire Bosch pour RTSP, ce qui permet de sécuriser la transmission.

Recommandation : approche basée sur le risque si la vidéo peut être transmise non chiffrée ou via un chiffrement Bosch. Dans la mesure du possible, utilisez RTSPS chiffré.

RCP

Le protocole RCP+ (Remote Control Protocol) propriétaire de Bosch est le protocole de configuration pour les caméras IP Bosch. Le RCP brut n'est pas chiffré ; les paramètres sont donc transférés sous forme non chiffrée. Tous les outils Bosch utilisent désormais la communication RCP sur HTTPS depuis quelques temps, mais elle peut être nécessaire pour des outils d'intégration ou des outils de scripts tiers qui reposent encore sur ce protocole.

Recommandation : Désactivez RCP s'il n'est pas utilisé par des outils tiers ou des systèmes existants.

SNMPv1

SNMP est le protocole de surveillance réseau commun utilisé pour interroger les informations d'état d'un périphérique ou l'envoi de traps à un récepteur distant, mais non chiffré.

Recommandation : A maintenir désactivé si non requis pour la surveillance d'état ou d'autres raisons de compatibilité. Utilisez SNMPv3 si possible.

SNMPv3

SNMPv3 est le successeur de SNMPv1 et il peut être aussi utilisé non chiffré.

Recommandation : recommandé si une surveillance SNMP doit être mise en oeuvre.

iSCSI

Désactive le serveur iSCSI interne qui est utilisé pour effectuer des enregistrements internes sur la caméra accessible via iSCSI. iSCSI est un protocole non chiffré.

Recommandation : Désactivez le serveur iSCSI s'il n'est pas utilisé sur la caméra.

UPnP

Permet de rendre la caméra détectable via le protocole UPnP.

Recommandation : Désactivez UPnP s'il n'est pas nécessaire.

Serveur NTP

Activez un serveur NTP sur la caméra pour autoriser d'autres périphériques ou caméras à synchroniser l'heure. Dans la mesure du possible, un périphérique dédié doit fournir l'heure au réseau de caméras en permettant la séparation des services. Si aucun autre périphérique n'est disponible, l'heure peut être fournie par une caméra.

Recommandation : le serveur NTP doit être désactivé s'il n'est pas nécessaire.

Discovery

Utilisation d'un mécanisme propriétaire Bosch pour rendre les caméras détectables par un logiciel Bosch tel que Configuration Manager.

Recommandation : Lors de l'utilisation d'adresses IP dynamiques, cette fonction doit être maintenue activée. Lorsque vous travaillez dans un environnement avec des adresses IP fixes, cette fonction peut être désactivée.

ONVIF Discovery

Prise en charge de la détection de périphériques de caméra via le protocole ONVIF Discovery

Recommandation : Lors de l'utilisation d'adresses IP dynamiques et d'outils conformes ONVIF, cette fonction doit demeurer activée. Lorsque vous travaillez dans un environnement fixe avec des adresses IP fixes, cette fonction peut être désactivée.

GBT/28181

GBT/28181 est une norme chinoise en matière d'interopérabilité entre différents périphériques.

Recommandation : à maintenir désactivée si elle n'est pas nécessaire.

Mécanisme de réinitialisation du mot de passe

Les caméras IP peuvent être installées dans des emplacements très distants, ce qui complique les travaux de maintenance ou la réinitialisation aux paramètres d'usine dans le cas où l'accès à la caméra a été verrouillé. Bosch offre la possibilité de réinitialiser le mot de passe d'une caméra via un mécanisme de réponse à une question, sur la base d'un mécanisme sécurisé de sécurité à clé publique/privée.

Recommandation : si cette fonctionnalité n'est pas nécessaire, il est recommandé de la désactiver.

Réponse Ping

Configure si la caméra répond aux requêtes ping sur le réseau. Peut être utile lors du débogage. Dans un réseau hautement sécurisé, il est possible de désactiver cette fonction afin d'éviter l'énumération des périphériques via un balayage ping, même si un grand nombre d'autres dispositifs peuvent être utilisés par un pirate informatique.

Recommandation : approche basée sur le risque ; peut être désactivée pour les réseaux de haute sécurité.

RTSPS

RTSPS est la version chiffrée de RTSP et elle est utilisée pour le flux vidéo. Si le logiciel de réception la prend en charge, RTSPS doit toujours être choisi de préférence au RTSP brut. Comme de nombreux clients RTSP ne prennent pas en charge la variante sécurisée, RTSP est toujours activé pour la sécurité de niveau 1.

Recommandation : Utilisez RTSPS si possible.

Version TLS minimum

Les caméras IP n'autorisent pas les connexions SSLv3 non sécurisées ou les connexions plus anciennes. Les versions 1.0 et 1.1 de TLS sont dépréciées par IETF et de possibles problèmes de sécurité sont connus (CEM, FIN DE COURSE).

Les caméras CPP4, CPP6, CPP7 et CPP7.3 prennent en charge la version sécurisée de TLS 1.2, laquelle doit être définie comme version requise minimum.

Les caméras CPP13 et CPP14 n'autorisent pas les versions antérieures à la version 1.2 de TLS. Elles prennent également en charge la spécification TLS1.3 la plus récente.

Recommandation : définissez la version TLS minimum sur 1.2.

HSTS

HTTP Strict Transport Security (HSTS) est une stratégie définie par un site Web afin de protéger contre les attaques de type intermédiaire (« man in the middle ») et les attaques rétrogrades de protocole. Elle permet au site Web d'indiquer au navigateur d'autoriser uniquement les connexions HTTPS au sein de cette connexion et de ne pas autoriser les connexions HTTP non chiffrées.

Recommandation : Activez HSTS sur la caméra.

802.1x

802.1x est une norme pour le contrôle d'accès réseau (NAC). Elle permet aux périphériques de s'authentifier sur le réseau, en n'autorisant l'accès au réseau qu'aux périphériques authentifiés. Les caméras IP Bosch prennent en charge 802.1x avec mot de passe ou

authentification basée sur certificat, l'authentification basée sur un certificat étant la méthode privilégiée. Pour pouvoir utiliser 802.1x, le commutateur réseau doit prendre en charge cette norme et un serveur d'authentification est nécessaire.

Recommandation : Si l'infrastructure réseau le permet, utilisez l'authentification réseau avec 802.1x.

Syslog

Comme la caméra ne fournit qu'un espace réduit pour les messages journaux, ceux-ci doivent être envoyés à un emplacement central et analysés afin de détecter les attaques ou les configurations incorrectes.

Recommandation : utilisez TCP Syslog afin d'éviter de perdre des messages en raison de la perte de paquet. Utilisez Syslog avec TLS pour chiffrer et authentifier des messages.

Mode SNMPv3

SNMPv3 est le successeur de SNMPv1 et il permet une authentification sécurisée et le transfert d'informations.

Recommandation : Lors de l'utilisation de SNMPv3, utilisez SHA1 comme protocole d'authentification et AES comme protocole de confidentialité (si pris en charge).

Filtre IP

Dans le filtre IP, il est possible de définir plusieurs adresses IP (hôtes uniques ou sous-réseaux de réseau), lesquelles sont autorisées à accéder à la caméra. Il est recommandé de définir les ordinateurs ou les réseaux accédant à la caméra ici.

Recommandation : il est recommandé d'utiliser le filtre IP pour définir les hôtes ou réseaux autorisés.

Date/Heure

Pour disposer d'un horodatage correct dans les journaux et les données vidéo, il est recommandé de synchroniser l'heure avec un serveur de synchronisation central. Il est possible d'utiliser une date SNTP ou TLS pour cela. L'avantage de SNTP est qu'il s'agit d'une synchronisation temporelle plus précise. L'avantage de la date TLS est qu'il est possible de vérifier que le certificat est correct, ce qui en fait la solution la plus sécurisée.

Recommandation : utilisez un moyen sécurisé de synchroniser l'heure, avec une date SNTP ou une date TLS.

Services basés sur le cloud

Bosch propose ses propres services dans le cloud pour la gestion des caméras dans le cloud Bosch (Remote Portal). Les services cloud ne se connectent pas automatiquement à Remote Portal et ils sont désactivés par défaut. Chaque caméra doit préalablement se connecter au Remote Portal si elle doit être utilisée. Toutes les précautions ont été prises pour sécuriser la connexion entre le Remote Portal et la caméra. Si nécessaire, le Remote Portal peut être utilisé dans n'importe quel environnement.

Recommandation : l'utilisation de Remote Portal dépend de la solution cloud utilisée.

Scellage logiciel

Une fois la configuration de la caméra IP terminée, les paramètres du périphérique ne doivent pas être modifiés. Il est possible d'activer un scellage de logiciel pour avertir les utilisateurs en cas de modification apportée à la configuration du périphérique.

Recommandation : activez le scellage de logiciel s'il n'y a pas de modifications de configuration en attente.

4.4.4

Défense en profondeur

La défense en profondeur fait référence à une approche de sécurité à plusieurs couches, où aucune mesure individuelle n'est responsable de la sécurité d'un produit ; un pirate informatique doit donc violer plusieurs couches pour pouvoir exploiter un produit. À chaque version du produit, il est évalué si de nouvelles fonctionnalités sont nécessaires pour atténuer les nouvelles attaques ou améliorer la sécurité globale du produit.

Voici une vue d'ensemble des principales fonctions de sécurité de la caméra IP.

- **Signature du firmware**

Chaque fichier de mise à jour du firmware est chiffré et signé par un certificat Bosch.

Seules les mises à jour publiées par Bosch peuvent être installées sur les caméras, ce qui permet d'éviter l'installation d'un firmware malveillant.

- **Démarrage sécurisé**

Les caméras des plateformes CPP13, CPP14 ou plus récentes, sont dotées d'un mécanisme de démarrage sécurisé. Ce mécanisme de démarrage sécurisé vérifie l'intégrité de l'ensemble du système, en commençant par le chargeur de démarrage et en continuant avec le firmware proprement dit sur les caméras. Chaque étape du processus de démarrage vérifie l'étape suivante, en commençant par une racine de confiance qui ne peut pas être modifiée. Cela permet d'éviter qu'un pirate informatique ne modifie le chargeur de démarrage ou le firmware sur le périphérique.

- **Pare-feu de connexion**

Pour assurer une protection contre l'attaque de mot de passe par force brute tout en permettant en même temps aux administrateurs de se connecter et de se protéger des attaques par déni de service (DoS), un pare-feu de connexion contrôle les tentatives de connexion sur la base d'une analyse comportementale et bloque ou autorise de manière dynamique l'accès basé sur les adresses IP.

- **Authentification de la caméra**

Afin d'identifier et d'authentifier de manière unique une caméra, un certificat de périphérique Bosch est créé sur chaque caméra durant la production. Ce certificat permet de vérifier si vous communiquez avec un véritable périphérique Bosch. En outre, il est possible de charger ou de créer des certificats personnalisés sur la caméra pour assurer l'intégration à un environnement PKI afin de protéger contre les attaques de type intermédiaire (« man in the middle »).

4.5

Renforcement du stockage

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 tout accès non autorisé aux données vidéo enregistrées, il est nécessaire de protéger les unités iSCSI contre tout accès non autorisé :

- 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, puis entrez le mot de passe configuré dans la configuration VRM. Le mot de passe CHAP est valide pour VRM et est automatiquement envoyé à tous les périphériques. Si un mot de passe CHAP est utilisé dans un environnement BVMS VRM, tous les systèmes de stockage doivent être configurés pour l'utilisation du même mot de passe.
- Supprimez tous les noms d'utilisateur et mots de passe par défaut de la cible iSCSI.

- Utilisez un mot de passe fort pour les comptes administrateur de la cible iSCSI.
- Désactivez les accès administratifs via Telnet aux cibles iSCSI. Utilisez plutôt l'accès SSH.
- Protégez l'accès de la console à la cible iSCSI via des mots de passe forts
- Désactivez les cartes d'interface réseau inutilisées.
- Surveillez l'état système des stockages iSCSI à l'aide d'outils tiers pour identifier les anomalies.

4.5.1

Définition d'un mot de passe CHAP sur les périphériques iSCSI

Lorsque vous définissez un mot de passe CHAP global dans Configuration Client de BVMS, ce mot de passe est automatiquement transféré sur tous les encodeurs, décodeurs et périphériques VSG.

Pour certains périphériques iSCSI, cette fonction n'est pas prise en charge. Vous devez définir manuellement le mot de passe CHAP sur ces périphériques.



Remarque!

Vous devez définir le mot de passe CHAP global sur les périphériques iSCSI avant de les ajouter à BVMS.

Les périphériques iSCSI ne peuvent pas être ajoutés à une configuration BVMS où le mot de passe CHAP global est déjà activé.

Pour définir manuellement un mot de passe CHAP sur un périphérique iSCSI (par exemple DIVAR IP), basé sur une version récente du système d'exploitation Microsoft Windows

Server :

1. Ouvrez le **Gestionnaire de serveur** et accédez à **Fichier et Services de stockage (File and Storage Services) > iSCSI**.
2. Dans la liste **CIBLES iSCSI (iSCSI TARGETS)**, cliquez avec le bouton droit de la souris sur la cible iSCSI de votre choix et cliquez sur **Propriétés (Properties)**.
La boîte de dialogue **Propriétés (Properties)** s'affiche.
3. Dans la boîte de dialogue **Propriétés (Properties)**, cliquez sur **Sécurité (Security)**, puis sélectionnez la case **Activer CHAP (Enable CHAP)**.
4. Saisissez ce qui suit :
 - **Nom d'utilisateur (User name)** : user
 - **Mot de passe (Password)** : entrez le mot de passe CHAP global tel que fourni dans BVMS Configuration Client (sous le menu **Matériel (Hardware) > Protection des stockages iSCSI avec un mot de passe CHAP (Protect iSCSI storages with CHAP password)...**).
5. Cliquez sur **OK**.
Le mot de passe CHAP est affecté à la cible iSCSI.

4.6

Renforcement des serveurs

4.6.1

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.

4.6.2 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.

4.6.3 Mises à jour Windows

Les correctifs et mises à jour logiciels Windows doivent être installés et doivent être maintenus à jour. Les mises à jour Windows incluent souvent des correctifs pour des vulnérabilités de sécurité récemment détectées, telle que la vulnérabilité SSL Heartbleed, qui a affecté des millions d'ordinateurs du monde entier. Il est nécessaire d'installer les correctifs pour ces problèmes importants.

4.6.4 Installation d'un logiciel antivirus

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

4.6.5 Paramètres recommandés pour le système d'exploitation Windows

Il est recommandé de définir des paramètres de groupe, notamment les paramètres de stratégie de groupe locale suivants sur un système d'exploitation Windows Server. Pour modifier les stratégies LCP (stratégies d'ordinateur locales), 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**.

4.6.6

Activation du contrôle de compte d'utilisateur sur le serveur

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

Contrôle de compte utilisateur : mode d'homologation admin. pour le compte Administrateur intégré	Activé
Contrôle de compte utilisateur : permet aux applications UIAccess d'afficher l'invite d'élévation sans utiliser le bureau sécurisé	Désactivé
Contrôle de compte utilisateur :comportement de l'invite d'élévation pour les administrateurs en mode d'approbation Administrateur	Demande de permission
Contrôle de compte utilisateur :comportement de l'invite d'élévation pour les utilisateurs standard	Invite pour les identifiants sur le bureau sécurisé
Contrôle de compte utilisateur : détection d'installations d'application et invite d'élévation	Activé
Contrôle du compte utilisateur : élévation de niveaux d'exécutables seulement signés et validés	Désactivé
Contrôle de compte utilisateur : exécution de tous les administrateurs en mode d'approbation Administrateur	Activé
Contrôle de compte utilisateur : bascule sur le bureau sécurisé lorsque de l'invite d'élévation	Activé
Contrôle de compte utilisateur : virtualisation des défaillances d'écriture et de fichier dans le fichier pour chaque emplacement utilisateur	Activé

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

Enumération des comptes administrateurs en élévation	Désactivé
--	-----------

4.6.7

Désactiver la lecture automatique

Stratégies ordinateur locales -> Configuration ordinateur -> Modèles d'administration -> Composants Windows -> Stratégies d'exécution automatique

Désactiver l'exécution automatique	Activé sur tous les lecteurs
Comportement par défaut pour AutoRun	Activé, ne pas exécuter de commandes AutoRun
Désactiver l'exécution automatique pour les périphériques sans volume	Activé

4.6.8

Périphériques externes

Stratégies ordinateur locales -> 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 médias 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

4.6.9

Configuration de l'attribution des droits utilisateur

Stratégies ordinateur locales -> 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
Modifier l'heure système	Administrateurs
Changer de fuseau horaire	Administrateurs, service local
Créer un fichier d'échange	Administrateurs
Créer un objet-jeton	Personne
Créer des objets partagés permanents	Personne
Interdire l'accès à cet ordinateur à partir du réseau	Ouverture de session anonyme, groupe Invité
Interdire l'ouverture de session en tant que tâche	Ouverture de session anonyme, groupe Invité
Interdire l'ouverture de session en tant que service	Personne
Interdire l'ouverture d'une session locale	Ouverture de session anonyme, groupe 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
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
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

4.6.10

Écran de veille

- Activer l'écran de veille protégé par mot de passe et définir un délai :
Stratégies ordinateur locales -> 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

4.6.11

Activation des paramètres de stratégie de mot de passe

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

Stratégies ordinateur locales -> Paramètres Windows -> Paramètre de sécurité -> Stratégies de compte -> 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
Stocker le mot de passe à l'aide d'un chiffrement réversible pour tous les utilisateurs du domaine	Désactivé

4.6.12

Désactivation des services Windows non essentiels

- La désactivation des services Windows non essentiels permet d'augmenter la sécurité et de minimiser les points d'attaque.

Service de la passerelle de la couche Application	Désactivé
---	-----------

Gestion des 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 des connexions automatiques d'accès à distance	Désactivé
Gestionnaire des connexions d'accès à distance	Désactivé
Routage et accès à distance	Désactivé
Détection matériel noyau	Désactivé
Application d'assistance de la Console d'administration spéciale	Désactivé
Découverte SSDP	Désactivé

4.6.13

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

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

Durée de verrouillage de comptes	Durée de verrouillage de comptes
Seuil de verrouillage de comptes de 15 minutes 10 échecs de tentatives de connexion	Seuil de verrouillage de comptes de 15 minutes 10 échecs de tentatives de connexion
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.

4.6.14 Activation du pare-feu sur le serveur

- ▶ Activez la communication des ports standard de BVMS en fonction des ports de BVMS.



Remarque!

Reportez-vous à la documentation BVMS pour en savoir plus sur les paramètres et l'utilisation des ports pertinents. Vérifiez une nouvelle fois les paramètres relatifs aux mises à niveau de firmware ou de logiciel.

4.7 Renforcement des clients Windows

4.7.1 Postes de travail Windows

Les systèmes d'exploitation du bureau Windows, utilisés pour des applications clientes BVMS telles que BVMS Operator Client ou Configuration Client, sont installés à l'extérieur de la zone sécurisée. Les postes de travail doivent être renforcés pour protéger les données vidéo, les documents et les autres applications contre les accès non autorisés.

Les paramètres suivants doivent être appliqués ou vérifiés.

4.7.2 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.

4.7.3 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.

4.7.4 Paramètres recommandés pour le système d'exploitation Windows

Il est recommandé de définir des paramètres de groupe, notamment les paramètres de stratégie de groupe locale suivants sur un système d'exploitation WindowsServer. Pour modifier les stratégies LCP (stratégies d'ordinateur locales), 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**.

4.7.5

Activation du contrôle de compte d'utilisateur sur le serveur

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

Contrôle de compte utilisateur : mode d'homologation admin. pour le compte Administrateur intégré	Activé
Contrôle de compte utilisateur : permet aux applications UIAccess d'afficher l'invite d'élévation sans utiliser le bureau sécurisé	Désactivé
Contrôle de compte utilisateur :comportement de l'invite d'élévation pour les administrateurs en mode d'approbation Administrateur	Demande de permission
Contrôle de compte utilisateur :comportement de l'invite d'élévation pour les utilisateurs standard	Invite pour les identifiants sur le bureau sécurisé
Contrôle de compte utilisateur : détection d'installations d'application et invite d'élévation	Activé
Contrôle du compte utilisateur : élévation de niveaux d'exécutables seulement signés et validés	Désactivé
Contrôle de compte utilisateur : exécution de tous les administrateurs en mode d'approbation Administrateur	Activé
Contrôle de compte utilisateur : bascule sur le bureau sécurisé lorsque de l'invite d'élévation	Activé
Contrôle de compte utilisateur : virtualisation des défaillances d'écriture et de fichier dans le fichier pour chaque emplacement utilisateur	Activé

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

Enumération des comptes administrateurs en élévation	Désactivé
--	-----------

4.7.6

Désactiver la lecture automatique

Stratégies ordinateur locales -> Configuration ordinateur -> Modèles d'administration -> Composants Windows -> Stratégies d'exécution automatique

Désactiver l'exécution automatique	Activé sur tous les lecteurs
Comportement par défaut pour AutoRun	Activé, ne pas exécuter de commandes AutoRun
Désactiver l'exécution automatique pour les périphériques sans volume	Activé

4.7.7

Périphériques externes

Stratégies ordinateur locales -> 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 médias 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

4.7.8

Configuration de l'attribution des droits utilisateur

Stratégies ordinateur locales -> 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
Modifier l'heure système	Administrateurs
Changer de fuseau horaire	Administrateurs, service local
Créer un fichier d'échange	Administrateurs

Créer un objet-jeton	Personne
Créer des objets partagés permanents	Personne
Interdire l'accès à cet ordinateur à partir du réseau	Ouverture de session anonyme, groupe Invité
Interdire l'ouverture de session en tant que tâche	Ouverture de session anonyme, groupe Invité
Interdire l'ouverture de session en tant que service	Personne
Interdire l'ouverture d'une session locale	Ouverture de session anonyme, groupe 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
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
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

4.7.9

Écran de veille

- Activer l'écran de veille protégé par mot de passe et définir un délai :
Stratégies ordinateur locales -> 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

4.7.10

Activation des paramètres de stratégie de mot de passe

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

Stratégies ordinateur locales -> Paramètres Windows -> Paramètre de sécurité -> Stratégies de compte -> 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
Stocker le mot de passe à l'aide d'un chiffrement réversible pour tous les utilisateurs du domaine	Désactivé

4.7.11

Désactivation des services Windows non essentiels

- La désactivation des services Windows non essentiels permet d'augmenter la sécurité et de minimiser les points d'attaque.

Service de la passerelle de la couche Application	Désactivé
Gestion des 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 des connexions automatiques d'accès à distance	Désactivé
Gestionnaire des connexions d'accès à distance	Désactivé
Routage et accès à distance	Désactivé
Détection matériel noyau	Désactivé
Application d'assistance de la Console d'administration spéciale	Désactivé
Découverte SSDP	Désactivé

4.7.12

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

Stratégies ordinateur locales -> Configuration ordinateur -> Paramètres Windows ->

Paramètres de sécurité -> Stratégies de compte -> Stratégie de verrouillage de compte

Durée de verrouillage de comptes	Durée de verrouillage de comptes
Seuil de verrouillage de comptes de 15 minutes 10 échecs de tentatives de connexion	Seuil de verrouillage de comptes de 15 minutes 10 échecs de tentatives de connexion
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.

4.7.13

Activation du pare-feu sur le poste de travail

- ▶ Activez la communication des ports standard de BVMS en fonction des ports de BVMS.



Remarque!

Reportez-vous à la documentation BVMS pour en savoir plus sur les paramètres et l'utilisation des ports pertinents. Vérifiez une nouvelle fois les paramètres relatifs aux mises à niveau de firmware ou de logiciel.

4.8

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.

4.8.1

VLAN : Réseau LAN virtuel

Un réseau LAN virtuel est créé en subdivisant un réseau LAN en plusieurs segments. La segmentation du réseau s'effectue par le biais d'un commutateur réseau ou d'un routeur. Un réseau VLAN présente l'avantage que ses besoins en ressources peuvent être résolus sans le câblage de connexions réseau de périphérique.

La qualité des services, appliquée à des segments spécifiques comme la vidéosurveillance, peut non seulement améliorer la sécurité, mais également les performances.

Les réseaux VLANs sont mis en œuvre sur une couche de liaison aux données (couche OSI 2) et ils offrent un accès analogique au sous-réseau IP (voir *Attribution d'adresses IP, page 8*) similaire à la couche réseau (couche OSI 3).

4.8.2

VPN : Réseau privé virtuel

Un réseau privé virtuel est un réseau séparé (privé) qui s'étend souvent au sein de réseaux publics ou Internet. Divers protocoles sont disponibles pour créer un VPN, généralement un tunnel qui véhicule le trafic protégé. Les réseaux privés virtuels peuvent être conçus comme des tunnels point à point, des connexions directes ou multi-points. Les réseaux VPN peuvent être déployés avec des communications chiffrées ou simplement reposer sur une communication sécurisée au sein du VPN lui-même.

Les réseaux VPN peuvent être utilisés pour connecter des sites distants via des connexions de réseau WAN, tout en protégeant la confidentialité et en augmentant la sécurité au sein d'un réseau LAN. Comme un réseau VPN fait office de réseau distinct, tous les périphériques ajoutés au VPN fonctionnent en toute transparence comme s'ils étaient sur un réseau classique. Un réseau VPN ajoute non seulement une couche de protection supplémentaire pour un système de surveillance, mais il offre également l'avantage supplémentaire de segmenter le trafic des entreprises et du trafic vidéo des réseaux de production.



Remarque!

Le cas échéant, les réseaux VLAN ou VPN augmentent le niveau de sécurité du système de surveillance intégré à une infrastructure informatique existante.

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.

4.8.3 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.

4.8.4 Réseaux protégés par le service 802.1x

Tous les Boschpériphériques vidéo IP peuvent être configurés en tant que clients 802.1x. Ils peuvent ainsi s'authentifier auprès d'un serveur RADIUS et prendre part à un réseau sécurisé. Avant de placer les périphériques vidéo sur le réseau sécurisé, vous devez vous connecter directement au périphérique vidéo depuis l'ordinateur portable d'un technicien pour saisir des références valides comme indiqué dans les étapes ci-dessous.

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.

Protocole EAP (Extensible Authentication Protocol) - Transport Layer Security

Le protocole EAP (Extensible Authentication Protocol) permet la prise en charge de plusieurs méthodes d'authentification. Le protocole Transport Layer Security (TLS) garantit l'authentification mutuelle, la négociation de suite de chiffrement protégée contre l'intégrité et l'échange de clés entre deux points de terminaison. Le système EAP-TLS comprend la prise en charge de l'authentification mutuelle basée sur un certificat et la dérivation de clés.

Autrement dit, le système EAP-TLS encapsule le processus dans lequel le serveur et le client envoient tous deux un certificat.

Remarque!



Reportez-vous au livre blanc technique spécifique *Network Authentication - 802.1x - Secure the Edge of the Network*, disponibles dans le catalogue produit en ligne Bosch Security Systems sous :

http://resource.boschsecurity.com/documents/WP_802.1x_Special_enUS_22335867275.pdf.

5 Fonctionnement sécurisé

5.1 Séparation réseau

Dans la mesure du possible, le périphérique doit être utilisé sur un réseau distinct (par exemple, avec des VLAN), avec des restrictions d'accès pour limiter le trafic de diffusion et protéger le périphérique contre les attaques réseau.

5.2 Stockage sécurisé des clés dans un coffre matériel

Les clés privées des certificats sont mieux protégées lorsqu'elles sont stockées de manière sécurisée dans un composant matériel ou un coffre matériel. Ces puces assurent une protection contre les accès non autorisés aux clés privées, même lorsque le périphérique est physiquement ouvert pour permettre un accès.

Sur les caméras Bosch, ces clés sont stockées dans un crypto-coprocasseur ou un élément sécurisé (SE) distincts. L'un et l'autre assurent un stockage sécurisé des données ainsi que des fonctions de chiffrement qui n'exposent jamais les clés privées à un emplacement ou à une mémoire où elles peuvent être récupérées.

Sur les postes de travail et les serveurs, une puce TPM (Trusted Platform Module) est généralement disponible. Les bibliothèques et fonctions de chiffrement doivent être configurées de manière à utiliser le stockage TPM dans la mesure du possible.

5.3 Certificats de périphériques uniques

Bien qu'un certificat par défaut signé soit généralement disponible avec chaque périphérique compatible TLS ou HTTPS, ce certificat ne doit pas être considéré comme suffisant pour l'authentification, car il ne protège pas contre une attaque de type intermédiaire (« man in the middle »).

Si des périphériques sont déployés dans un environnement où des étapes supplémentaires sont requises pour valider l'identité de chaque périphérique vidéo IP, de nouveaux certificats et clés privées peuvent être créés et chargés sur les périphériques vidéo eux-mêmes. Il est possible d'obtenir de nouveaux certificats auprès d'une autorité de certification (CA) ou de les créer à l'aide d'un kit d'outils OpenSSL.

Si des périphériques sont utilisés sur des réseaux publics, il est recommandé d'obtenir un certificat auprès d'une autorité de certificat public ou de posséder des certificats signés par cette autorité, laquelle est également capable de vérifier l'origine et la validité, c'est-à-dire le niveau de confiance, du certificat de périphérique.

Depuis des années, toutes les caméras Bosch sont dotées d'un certificat de périphérique et d'un clé privé uniques et préinstallés, dérivés du certificat racine de Bosch et installés dans un environnement de production sécurisé, ce qui certifie que la caméra est un dispositif Bosch de « fabrication d'origine ». Ce certificat est utilisé automatiquement pour les connexions HTTPS et il peut être utilisé pour identifier et authentifier un périphérique par une vérification de la chaîne de certificate avec le certificat racine de Bosch.



Remarque!

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.

La variante la plus sécurisée d'un déploiement de certificat consiste à générer une demande de signature de certificat (CSR) sur le périphérique et de demander un certificat depuis une autorité de certification interne ou externe.

Dans le cas d'une demande de signature de certificat, le périphérique maintient la clé privée en interne et n'expose que le reste du certificat pour signature par l'autorité de certification. La clé privée est stockée de manière sécurisée dans l'élément sécurisé (SE) de la caméra, ou par exemple dans le module TPM (Trusted Platform Module) du périphérique.

Par conséquent, chaque fois qu'un périphérique offre une possibilité de demande CSR, il doit s'agir de la méthode privilégiée pour créer un certificat.

Les certificats peuvent être chargés sur un périphérique, soit via la page Web du périphérique d'un périphérique vidéo, soit à l'aide de Configuration Manager.

Chargement des certificats via la page Web du périphérique

Les certificats peuvent être chargés à l'aide de la page Web d'un périphérique vidéo.

Sur la page Web du périphérique, depuis la fenêtre **Certificats**, il est possible d'ajouter et de supprimer de nouveaux certificats, et de définir leur utilisation.

Chargement des certificats à l'aide de Configuration Manager

Dans Configuration Manager, il est facile de charger simultanément des certificats sur un ou plusieurs périphériques.

Pour charger des certificats :

1. Dans Configuration Manager, sélectionnez un ou plusieurs périphériques.
2. Cliquez avec le bouton droit de la souris sur **Chargement du fichier**, puis cliquez sur **Certificat SSL....**

Une fenêtre de l'Explorateur Windows s'ouvre pour vous permettre de localiser le certificat à charger.

Pour les systèmes plus petits, Configuration Manager propose une fonction d'aide, appelée **MicroCA**, qui permet de créer ou d'utiliser une AC racine et dériver des certificats depuis cette dernière, ou de l'utiliser pour la signature des demandes de signature de certificate des périphériques, et également pour plusieurs périphériques en même temps. Pour plus d'informations, consultez le manuel d'utilisateur de Configuration Manager.

Se reporter à

– *Création de certificats de confiance, page 49*

5.4 Consultation des fichiers journaux

La surveillance des fichiers journaux constitue un élément important de l'analyse de sécurité ou de l'activité de maintenance. Une consultation régulière des fichiers journaux peut révéler des problèmes de configuration ou des violations de sécurité, telles que les fausses connexions.

Pour analyser les fichiers journaux et les stocker sur le long terme, il est conseillé d'envoyer les fichiers journaux du périphérique sur un serveur syslog ou un système SIEM. Par exemple, une caméra se réserve un espace fixe pour la journalisation interne, mais elle remplace les anciens journaux lorsque cet espace est saturé.

5.5 Système SIEM

Le système SIEM (Security Information and Event Management) est utilisé pour la collecte et l'analyse d'informations provenant de différents périphériques et systèmes. Les périphériques peuvent être intégrés à un système SIEM par l'envoi des journaux via le protocole syslog. L'analyse de ces journaux peut faciliter la maintenance et détecter les erreurs de configuration ou les attaques sur le périphérique (par exemple, les fausses connexions).

5.6 Infrastructure de clés publiques (PKI)

L'infrastructure de clés publiques (PKI) fait référence aux systèmes nécessaires à la génération et à la gestion de certificats numériques. Pour HTTPS, l'authentification réseau avec 802.1x, l'authentification des utilisateurs avec des certificats et autres fonctions de chiffrement, vous pouvez installer des certificats personnalisés sur le périphérique.

5.7 AD FS

AD FS (Active Directory Federation Services) est un service proposé par Microsoft, qui permet l'authentification auprès d'un domaine Active Directory local (à l'aide d'un serveur AD FS) ou auprès d'Azure Cloud. Outre l'authentification utilisateur locale à l'aide de mots de passe ou d'une authentification basée sur un certificat, l'intégration de périphériques à un Active Directory est possible avec AD FS pour authentifier et gérer de façon centralisée l'accès des utilisateurs.

5.8 Fonctionnement sécurisé des caméras IP

5.8.1 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** .

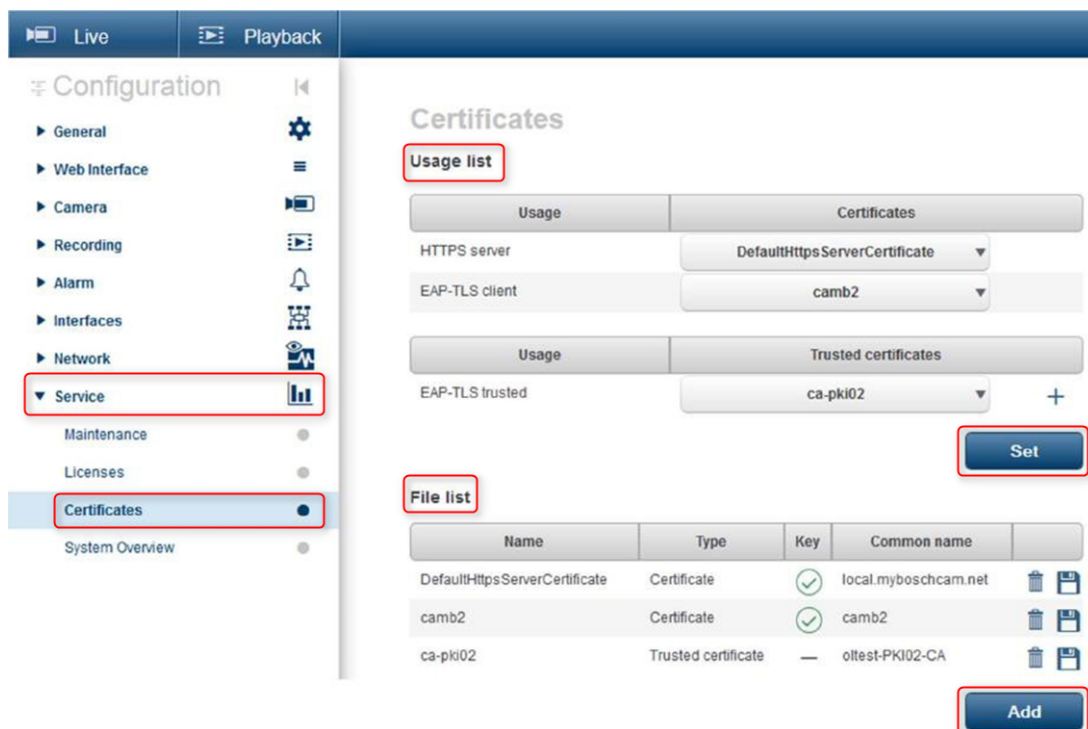


Figure 5.1: Exemple : Certificats EAP/TLS stockés sur une caméra Bosch (FW6.11)

Les certificats sont acceptés au format *.pem, *.cer ou *.crt et doivent être encodés en base64. Ils peuvent être chargés dans un seul fichier combiné, ou séparés en parties de certificat et de clés, puis chargés dans cet ordre en tant que fichiers séparés à recombinaison automatique.

Étant donné que le firmware version 6.20 est pris en charge, les clés privées protégées par mot de passe PKCS#8 (cryptées en AES) doivent être téléchargées au format *.pem et codées en base64.

5.8.2

Authentification vidéo

Une fois les périphériques d'un système correctement protégés et authentifiés, il est très utile de garder un œil sur les données vidéo qui leur sont transmises. 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.

Avant la commercialisation du firmware 5.9, le filigrane vidéo était effectué via un simple algorithme de somme de contrôle sur le flux vidéo. Le filigrane vidéo de base n'utilise ni certificats, ni chiffrement. Une somme de contrôle est une mesure de référence de la « stabilité des données » permettant de valider 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).

Display Stamping

Camera name stamping

Logo

Logo position

Time stamping

Display milliseconds

Alarm mode stamping

Alarm message (max. 31 characters)

Transparent background

Video authentication

Signature interval [s]

Off

Watermarking

MD5

SHA-1

SHA-256



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.

6 Gestion de la mise à jour de sécurité

Avant d'utiliser le dispositif pour la première fois, assurez-vous d'avoir installé la dernière version applicable du logiciel. Afin de garantir la cohérence de la fonctionnalité, de la compatibilité, des performances et de la sécurité du dispositif, mettez régulièrement à jour son logiciel tout au long de sa durée de vie. Suivez les instructions contenues dans la documentation produit concernant les mises à jour logicielles.

Pour plus d'informations, cliquez sur les liens suivants :

- Informations générales : <https://www.boschsecurity.com/xc/en/support/product-security/>
- Conseils de sécurité, avec une liste des vulnérabilités et des solutions possibles : <https://www.boschsecurity.com/xc/en/support/product-security/security-advisories.html>

Bosch n'assume aucune responsabilité pour tout dommage causé par le fait que les produits livrés ont été mis en service avec du firmware obsolète.

Vous trouverez les dernières versions de firmware et de logiciels dans la boutique de téléchargement Bosch Security and Safety Systems :

<https://downloadstore.boschsecurity.com/>

Pour les périphériques connectés au Remote Portal, les utilisateurs peuvent recevoir une notification par e-mail concernant les mises à jour de firmware disponibles via le service Alerte à distance.

Des packages de téléchargement plus complets sont distribués via le catalogue de produits Bosch Security and Safety Systems :

<https://www.boschsecurity.com>

7 Surveillance de sécurité

Comme les exigences changent constamment, la sécurité n'est jamais garantie à 100 %. Par conséquent, Bosch a mis en place un processus structuré de gestion des incidents et des vulnérabilités afin de gérer de manière professionnelle les vulnérabilités et incidents de sécurité potentiels d'un produit.

La gestion systématique et professionnelle des vulnérabilités de sécurité signalées ainsi que la transparence à l'égard de nos clients sont très importantes pour nous. Pour cette raison, nous étudions tous les rapports de vulnérabilités. Nous nous faisons une évaluation des vulnérabilités de sécurité du produit conformément au système CVSS (Common Vulnerability Scoring System). CVSS est une norme industrielle libre et ouverte qui permet d'évaluer la gravité des vulnérabilités de sécurité d'un système informatique. Les scores sont calculés à l'aide d'une formule qui dépend de plusieurs mesures approximatives de la simplicité d'exploitation et de l'impact d'une exploitation. Les scores vont de 0 à 10, 10 représentant le niveau de gravité le plus élevé.

En cas de vulnérabilité confirmée, nous informons les clients que nous avons identifié une vulnérabilité de sécurité dans le produit ou la solution et proposons sa résolution en publiant des conseils de sécurité. Tous les conseils de sécurité contiennent :

- Une description de la vulnérabilité cours avec une référence CVE (Common Vulnerabilities and Exposures) et un score CVSS.
- L'identité des produits et versions logicielles/matériels concernés connus.
- Des informations sur les facteurs d'atténuation et les solutions de contournement.
- La chronologie et l'emplacement des correctifs disponibles ou d'autres mesures correctives.

Une liste des conseils de sécurité publiés est disponible sur notre site Web <https://www.boschsecurity.com/xc/en/support/product-security/security-advisories.html>.

Chaque fois que vous pensez avoir identifié une vulnérabilité ou tout autre problème de sécurité lié à un produit ou un service Bosch, contactez l'équipe PsIRT (Product Security Incident Response Team) : <https://psirt.bosch.com>.

8 Mise au rebut et mise hors service sécurisées

À un certain moment du cycle de vie d'un produit ou d'un système, il peut être nécessaire de remplacer le dispositif ou un de ses composants, ou de les mettre hors service. Étant donné que le périphérique ou le composant peut contenir des données sensibles, telles que les références de connexion ou les certificats, assurez-vous de les supprimer complètement et de manière sécurisée.

Vous pouvez configurer la plupart des périphériques sur les paramètres par défaut.

Pour la plupart des encodeurs et des caméras IP, vous pouvez utiliser pour cela le bouton de réinitialisation. Pour ceux qui n'ont pas de bouton de réinitialisation, utilisez la fonction d'usine par défaut via l'interface Web avant de les retirer du réseau.

L'ensemble des utilisateurs et leurs mots de passe respectifs seront supprimés et les paramètres seront réinitialisés aux paramètres par défaut. L'ensemble des certificats et des clés respectives stockées dans TPM ou l'élément sécurisé seront également être supprimés.

D'autres périphériques peuvent avoir des options différentes pour une configuration sur les paramètres d'usine par défaut. Reportez-vous aux instructions de la documentation utilisateur respective pour connaître les procédures de mise au rebut appropriées.

Des certificats et des identifiants peuvent également être stockés pour les serveurs et les postes de travail. Utilisez les outils et méthodes appropriés pour vérifier que vos données pertinentes sont correctement supprimées lors d'une mise hors service ou avant une mise au rebut.

Il est également recommandé de configurer les périphériques sur les paramètres d'usine par défaut dans le cas où ils doivent être déplacés vers une autre installation susceptible d'utiliser d'autres identifiants ou certificats.



Remarque!

Reportez-vous aux instructions de la documentation utilisateur respective pour connaître les procédures de mise au rebut appropriées.

9 Informations supplémentaires

Pour plus d'informations et de détails sur les logiciels, le téléchargement et la documentation, visitez le site :

<http://www.boschsecurity.com>

Glossaire

802.1x

La norme IEEE 802.1x offre un modèle général de contrôle d'accès et d'authentification pour les réseaux IEEE 802. L'authentification est assurée par un programme à cet effet (Authenticator), qui contrôle les informations d'authentification transmises à l'aide d'un serveur d'authentification (voir serveur RADIUS) et autorise ou refuse l'accès aux services disponibles (LAN, VLAN ou WLAN).

Adresse IPv4

Nombre de 4 octets permettant d'identifier un périphérique sur Internet. Une adresse IP est généralement composée de nombres décimaux (octets) séparés par des points, par exemple « 209.130.2.193 ».

authentification

Processus d'authentification d'un flux vidéo. Vous pouvez lancer un processus d'authentification. Si des données non authentifiées sont détectées, un message s'affiche.

DHCP

Dynamic Host Configuration Protocol (protocole de configuration dynamique de l'hôte) : permet l'affectation dynamique par un serveur approprié d'une adresse IP ou d'autres paramètres de configuration aux ordinateurs d'un réseau (Internet ou LAN).

Groupe d'utilisateurs

Groupe servant à définir des attributs communs à plusieurs utilisateurs, tels que des autorisations, des droits d'accès et un niveau de priorité en matière de balayage horizontal/vertical et de zoom. Lorsqu'un utilisateur devient membre d'un groupe, il hérite automatiquement de tous les attributs du groupe.

HTTP

Hypertext Transfer Protocol : protocole de transmission de données sur un réseau

HTTPS

Hypertext Transfer Protocol Secure : chiffre et authentifie la communication entre un serveur Web et un navigateur

LAN

Réseau local. Il s'agit d'un réseau reliant des périphériques d'une zone géographique limitée.

Masque réseau

Masque définissant les deux parties d'une adresse IP, l'une correspondant à l'adresse réseau et l'autre comportant l'adresse hôte. Il est généralement composé de nombres décimaux séparés par des points, par exemple « 255.255.255.192 ».

Multicast

Sur un réseau, communication entre un émetteur unique et plusieurs récepteurs par distribution d'un flux de données unique (sur le réseau lui-même) vers plusieurs récepteurs d'un groupe défini. Pour pouvoir utiliser le multicast, vous devez disposer d'un réseau compatible qui utilise les protocoles UDP et IGMP.

ONVIF

Open Network Video Interface Forum. Norme internationale pour les produits vidéo en réseau. Les dispositifs conformes à la norme ONVIF sont capables d'échanger en temps réel des informations vidéo, audio, des métadonnées et des informations de commande, et permettent de les détecter et de les raccorder automatiquement à des applications réseau, telles que des systèmes de gestion vidéo.

périphérique

Composant matériel tel qu'une caméra, un encodeur/décodeur, une unité NVR, DiBos, une matrice analogique, une passerelle ATM/POS.

RCP+

Remote Control Protocol : protocole Bosch propriétaire utilisant des ports statiques spécifiques pour détecter et communiquer avec les périphériques vidéo IP Bosch.

renforcement

Processus d'accroissement de la sécurité d'un système en utilisant uniquement un logiciel dédié requis pour le fonctionnement des systèmes, en appliquant des paramètres de protection spécifiques et en retirant les logiciels non obligatoires.

Réseau étendu

Liaison longue distance utilisée pour l'extension ou la connexion de réseaux locaux distants

RTSP

Real Time Streaming Protocol. Protocole réseau permettant de gérer la transmission continue de données ou de logiciels audiovisuels sur les réseaux IP.

Serveur RADIUS

Le service RADIUS (Remote Authentication Dial-in User Service) est un protocole client-serveur dédié à l'authentification, l'autorisation et la facturation des utilisateurs à accès commuté d'un réseau informatique. RADIUS est la norme de fait pour l'authentification centralisée des connexions commutées via modem, RNIS, VPN, LAN sans fil (voir 802.1x) et DSL.

SNMP

Simple Network Management Protocol : protocole de gestion permettant l'administration et la surveillance des composants d'un réseau

SSL

Secure Sockets Layer, protocole de chiffrement obsolète pour la transmission de données sur les réseaux IP (voir TLS).

TCP

Transmission Control Protocol (protocole de contrôle de transmission). Protocole de communication orienté connexion servant à envoyer des données via un réseau IP. Propose une transmission de données fiable et commandée.

Telnet

Protocole de connexion permettant aux utilisateurs d'accéder à un ordinateur distant (hôte) sur Internet.

TLS

Transport Layer Security. Les normes TLS 1.0 et 1.1 sont les améliorations normalisées de SSL 3.0 (voir SSL). Les périphériques modernes utilisent TLS 1.2 ou 1.3

TTL

Time-To-Live (durée de vie) : cycle de vie d'un paquet de données dans les transferts de stations

UDP

User Datagram Protocol. Protocole en mode non connecté servant à échanger des données sur un réseau IP. Le protocole UDP est plus efficace que le protocole TCP pour la transmission vidéo, car il nécessite moins de ressources.

VPN

Un réseau privé virtuel (VPN) met en œuvre un réseau privé dans un réseau public, par exemple Internet. Le trafic réseau au sein du réseau VPN est chiffré et ainsi protégé contre l'espionnage.

Bosch Sicherheitssysteme GmbH

Robert-Bosch-Ring 5

85630 Grasbrunn

Germany

www.boschsecurity.com

© Bosch Sicherheitssysteme GmbH, 2023

Building solutions for a better life.

202302091959