

Access Management System V3.0.1



- ▶ Associe des fonctions de contrôle d'accès, des performances et une disponibilité de pointe à un fonctionnement intuitif.
- ▶ Hautement évolutif : de 1000 à 200,000 utilisateurs, et de 32 à 10,000 portes.
- ▶ Facile à utiliser : interface graphique intuitive pour les cartes et la visionneuse d'alarmes, et gestion des visiteurs basée sur le Web.
- ▶ Facile à configurer : licences prédéfinies, installation et configuration simples.
- ▶ Gestion complète de la sécurité : s'intègre aux systèmes de détection d'intrusion et vidéo.

Access Management System (AMS) est un système de contrôle d'accès destiné à une application autonome ou à l'intégration avec d'autres systèmes, par exemple Bosch Video Management System (BVMS) ou des centrales intrusion Bosch B series et G series.

- En tant que système autonome, il dispose d'une visionneuse de plan et d'alarme simple à utiliser pour une évaluation rapide de tous les dispositifs et entrées dans le site.
- En tant que système intégré, il permet à l'opérateur d'un système de gestion vidéo d'effectuer des tâches liées aux portes comme la vérification d'identité par vidéo, l'octroi ou le refus d'accès ou la désactivation des portes.
- Les zones d'intrusion peuvent être armées directement à partir de la Map View et les utilisateurs de la centrale intrusion peuvent être gérés de manière centralisée.

AMS associe la solidité, les performances et les fonctions de produits de contrôle d'accès de pointe, avec une IU moderne qui le rend rapide à installer et à configurer.

Le portefeuille existant des dispositifs de contrôle d'accès Bosch peut être facilement analysé et intégré.

La confidentialité des données et la sécurité informatique sont à la pointe de la technologie afin de se conformer aux dernières réglementations en matière de protection des données en vigueur.

Présentation du système

Access Management Server

Le serveur est le composant principal pour le traitement de toutes les données. Il coordonne les activités de tous les composants matériels et logiciels décrits ci-dessous.

Master Access Controller (MAC)

Le contrôleur MAC est une couche de sécurité supplémentaire pour accroître la disponibilité du système. Il possède sa propre base de données pour échanger des informations entre les contrôleurs AMC, même si le serveur principal ou le réseau est défaillant.

Contrôleur d'accès modulaire (AMC)

Le contrôleur d'accès modulaire AMC est un contrôleur de site robuste et fiable permettant de connecter jusqu'à 8 portes avec des lecteurs et gâches de porte. Grâce à sa mémoire intégrée volumineuse, le contrôleur AMC peut prendre des

décisions autonomes et stocker des centaines de milliers d'événements d'accès, quelles que soient les interruptions du réseau.

Base de données de gestion des accès

Le serveur SQL contient toutes les données permanentes (titulaire de carte, cartes, autorisations, calendriers, etc.), ainsi que tous les événements d'accès. La dernière version fournit un chiffrement pour protéger les informations personnelles contre une utilisation abusive ou le vol.

Gestionnaire de dialogue de gestion des accès

Le Gestionnaire de dialogue est l'interface utilisateur principale pour la configuration du système, ainsi que pour la collecte et la maintenance des informations relatives aux accès. Ses dialogues personnels sont notamment utilisés pour inscrire de nouveaux détenteurs de carte et conserver leurs autorisations d'accès et leurs identifiants.

Application Map View de gestion des accès

Map View est une application simple à utiliser à la fois pour visualiser la situation globale de sécurité des locaux et pour zoomer en détail. Elle affiche les alarmes de violation d'accès, de sabotage et de dysfonctionnement et permet l'envoi de commandes directement à partir des cartes elles-mêmes.

Gestion de visiteurs

Vue Réceptionniste : interface utilisateur basée sur un navigateur où les réceptionnistes peuvent enregistrer et surveiller efficacement les visiteurs et les visites.

Vue Hôte : interface utilisateur basée sur un navigateur où les employés peuvent pré-enregistrer leurs visites.

Vue Visiteur : interface utilisateur basée sur un navigateur en **mode kiosque**, où les visiteurs peuvent conserver leurs propres profils stockés, numériser leurs papiers d'identité et signer numériquement les documents requis, réduisant ainsi considérablement les temps d'attente et l'encombrement à la réception.

Interface BVMS de la gestion des accès

L'intégration transparente avec BVMS (version 10.1 ou supérieure) permet désormais la vérification vidéo des identités des détenteurs de cartes à partir du client opérateur BVMS : une personne demandant l'accès avec une carte valide peut être vérifiée manuellement via un flux de caméra en direct et la photo du titulaire de la base de données. Les événements de caméra peuvent déclencher des actions de porte. Les événements de porte peuvent déclencher des actions de caméra.

Interface Intrusion de la gestion des accès

Gestion de jusqu'à 25 centrales intrusion 25 B et G Series. Affiche les états de partition (par exemple, armé, prêt pour armement), les états des détecteurs et les événements d'intrusion dans Map View. Permet l'envoi de commandes (par exemple armer, désarmer) aux centrales.

SDK de la gestion des accès

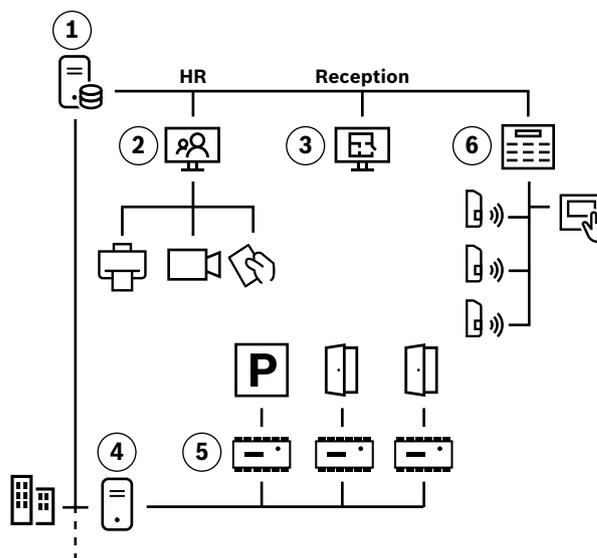
Ce SDK facilite l'intégration de systèmes tiers à AMS, par exemple un système de gestion des identités ou des visiteurs. Un avantage particulier est sa capacité à réutiliser des intégrations tierces écrites initialement pour BIS Access Engine.

Access Importer/Exporter

Cet outil facilite l'importation et l'exportation de données à partir de systèmes externes pour une migration de données unique, notamment à partir de systèmes Access PE, ou un transfert régulier de données depuis Active Directory à l'aide du protocole LDAP.

Architectures type

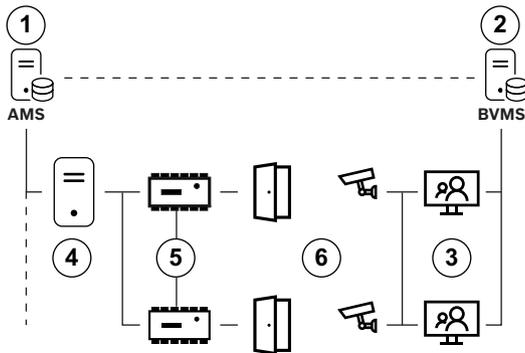
Les schémas suivants illustrent les configurations AMS avec des panneaux de détection d'intrusion intégrés et avec BVMS.



Topologie de détection d'intrus

- (1) Serveur AMS
- (2) Poste de commande de client pour les inscriptions
- (3) Poste de commande client pour le contrôle d'accès, la gestion des visiteurs, la gestion des alarmes et l'armement/le désarmement centralisé des zones d'intrusion

- (4) Serveurs MAC en option (une licence MAC est toujours incluse, sur le serveur AMS)
- (5) AMC pour le contrôle du stationnement et des portes
- (6) Centrale de détection d'intrusion avec détecteurs et clavier à écran tactile



Intégration BVMS

- (1) Serveur AMS
- (2) Serveur de gestion BVMS ou DIVAR IP all-in-one
- (3) Poste de commande de client BVMS pour l'accès et la gestion vidéo
- (4) Serveurs MAC en option (une licence MAC est toujours incluse, sur le serveur AMS)
- (5) AMC
- (6) Entrées avec caméras

Fonctions

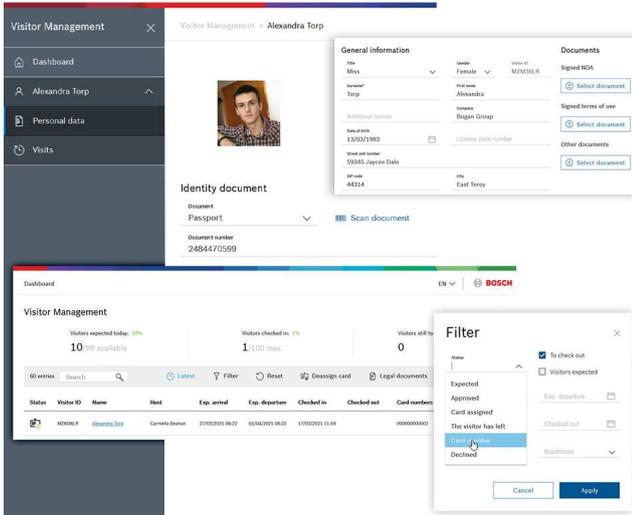
- Enregistrement des nouveaux titulaires de badge :
 - Utilisez des boîtes de dialogue d'inscription entièrement personnalisables pour rationaliser le processus d'inscription des titulaires de badge.
 - Capturez les caractéristiques conventionnelles et biométriques, y compris les photos et les signatures.
 - Concevez et produisez des références physiques.
 - Tirez parti des boîtes de dialogue pour l'importation en masse des données du personnel stockées.
- Attribution des autorisations d'accès :
 - Collectez les autorisations d'accès dans des profils réutilisables et attribuez-les à des types de personnel prédéfinis ou personnalisés.
- Fonctions des portes :

- Utilisez un ensemble complet de modèles de porte, y compris des ascenseurs et des places de parking, pour accélérer la phase de configuration de votre projet.
- Mode bureau : déverrouillez les portes pour un accès libre pendant les heures de bureau ou de magasin.
- Lutte contre le vol et les menaces de sécurité en procédant à une vérification aléatoire des titulaires de carte.
- Vérifiez l'identité du titulaire de carte avec des contrôles biométriques aux entrées et avec une vérification d'ID par vidéo supplémentaire alimentée par BVMS.
- Désarmez une zone d'intrusion et accordez l'accès d'un simple glissement de carte.
- Utilisez la technologie SimonsVoss SmartIntego pour améliorer votre système avec des portes en ligne à distance programmables par carte, telles que celles couramment utilisées dans les hôtels, les établissements de santé, les bureaux et les établissements d'enseignement.

- Création de rapports :
 - Tirez parti d'un grand nombre de modèles de rapports prédéfinis.
- Gestion de visiteurs
 - Pré-enregistrez les rendez-vous dans le système, pour raccourcir le temps de traitement.
 - Permettez aux visiteurs de créer leurs propres profils en mode kiosque, pour éviter les files d'attente à la réception.
 - Utilisez un tableau de bord pour surveiller les visites prévues de la journée, le nombre de visiteurs sur les lieux, les informations d'identification utilisées et les informations d'identification qui doivent encore être collectées.
 - Définissez des dates d'expiration sur les profils des visiteurs et leurs pièces jointes afin de respecter les réglementations nationales en matière de confidentialité des données, telles que le RGPD européen.

Welcome

Please enter your visitor ID.



- Tours de garde et patrouilles :
 - Définissez jusqu'à 200 tours de garde et surveillez jusqu'à 8 patrouilles simultanément.
- Surveillez les parkings et les points de rassemblement :
 - Affichez des résumés personnalisables des employés et des véhicules sur site.
 - Surveillez le nombre de places de parking disponibles.
- Divisions :
 - Fournissez un contrôle d'accès unifié à une installation partagée par un certain nombre de parties indépendantes.
 - Les opérateurs individuels peuvent être limités à la seule gestion des personnes, des appareils et des entrées des divisions qui leur sont affectées.
- Surveillance, commande et contrôle des alarmes :
 - Map View prend en charge jusqu'à 1000 cartes, qui peuvent être imbriquées pour fournir à la fois des aperçus et des détails rapprochés.
 - Utilisez Map View pour contrôler simultanément un grand nombre d'entrées.
 - Utilisez Map View pour contrôler les alarmes entrantes et les alertes en temps réel. AMS ne met pas en mémoire tampon les alarmes d'intrusion qui se produisent lorsque le réseau ou le système lui-même est en panne.

- Intégration BVMS et DIVAR IP :
 - Vérification vidéo aux entrées.
 - Actions de caméra (par exemple, démarrage/arrêt de l'enregistrement, panoramique/inclinaison/zoom) déclenchées par des événements d'accès (par exemple, ouverture non autorisée d'une porte).
 - Événements de porte (par exemple déverrouillage/verrouillage de porte) déclenchés par des événements de caméra (par exemple, Intelligent Video Analytics).
 - Requiert la version 10.1 ou ultérieure.
- Intégration XProtect de Milestone :
 - Utilisez AMS pour soutenir XProtect avec des événements d'accès et des alarmes, afin de les traiter sur le client XProtect.
- Intégration d'intrusion :
 - Prend en charge jusqu'à 50 centrales Bosch B Series (Bx512) et G Series (Bx512G) pour la gestion centralisée des utilisateurs et 25 pour la commande et le contrôle.
 - Un contingent complet de centrales fournit jusqu'à 12,800 détecteurs d'intrusion.
- Intégration des appareils mobiles :
 - Prend en charge HID Mobile Access (sur MIFARE CSN via NFC et Wiegand) et STid Mobile ID (sur MIFARE CSN via Wiegand et OSDP, NFC et BLE).

Remarques sur l'installation/la configuration

Les tableaux suivants illustrent la configuration matérielle et logicielle requise pour exécuter AMS.

Serveur	
Systèmes d'exploitation pris en charge.	<ul style="list-style-type: none"> • Windows Server 2016 (64 bits, Standard, Datacenter)
Les installations sur d'autres systèmes d'exploitation peuvent	<ul style="list-style-type: none"> • Windows 10 Version 1809 LTSC, Windows 10 Professional and Enterprise, Version 20H2

Serveur	
réussir, mais ne font l'objet d'aucune garantie.	<ul style="list-style-type: none"> • Assurez-vous que les dernières mises à jour logicielles sont installées. • Remarque : SQL Server 2017 Express avec services avancés est la base de données fournie par défaut avec ce système.
Configuration matérielle minimale requise	<ul style="list-style-type: none"> • Processeur Intel i5 avec au moins 4 cœurs physiques • 8 Go de RAM (32 Go recommandé) • 200 Go d'espace disque disponible (disques SSD recommandés) • Carte graphique avec <ul style="list-style-type: none"> – 256 Mo de RAM – Une résolution de 1280x1024 (Utilisez la résolution graphique recommandée pour le client si vous souhaitez exécuter le client Map View sur le serveur AMS). – Au moins 32 000 couleurs • Carte Ethernet 1 Gbit/s • Un port USB libre ou un partage réseau pour les fichiers d'installation

Client, y compris le client Map View	
Systèmes d'exploitation pris en charge.	<ul style="list-style-type: none"> • Windows 10 Version 1809 LTSC, Windows 10 Professional and Enterprise, Version 20H2
Les installations sur d'autres systèmes d'exploitation peuvent réussir, mais ne font l'objet d'aucune garantie.	<ul style="list-style-type: none"> • Assurez-vous que les dernières mises à jour logicielles sont installées.
Configuration matérielle minimale requise	<ul style="list-style-type: none"> • Intel i5 ou supérieur • 8 Go de RAM (16 Go recommandé) • 20 Go d'espace disque disponible • Carte graphique <ul style="list-style-type: none"> – 256 Mo de RAM – Pour utiliser le gestionnaire de boîte de dialogue AMS, une résolution de 1280x1024 est suffisante. – Pour AMS Map View, une résolution de 1920x1080 (Full HD) est requise. – Au moins 32 000 couleurs • DirectX® 11 • Carte Ethernet 1 Gbit/s

Client, y compris le client Map View	
	<ul style="list-style-type: none"> • Un port USB libre ou un partage réseau pour les fichiers d'installation

Client de gestion des visiteurs	
Navigateurs pris en charge.	Google Chrome, Mozilla Firefox, Microsoft Edge (Chromium based)
Résolution d'écran minimale recommandée	Full HD 1920x1080

Serveur MAC	
Systèmes d'exploitation pris en charge.	<ul style="list-style-type: none"> • Windows Server 2016 (64 bits, Standard, Datacenter) • Windows 10 Version 1809 LTSC, Windows 10 Professional and Enterprise, Version 20H2
Les installations sur d'autres systèmes d'exploitation peuvent réussir, mais ne font l'objet d'aucune garantie.	<ul style="list-style-type: none"> • Assurez-vous que les dernières mises à jour logicielles sont installées.
Configuration matérielle minimale requise	<ul style="list-style-type: none"> • Intel i5 ou supérieur • 8 Go de RAM (16 Go recommandé) • 20 Go d'espace disque disponible • Carte graphique avec <ul style="list-style-type: none"> – 256 Mo de RAM – Une résolution de 1280x1024 – Au moins 32 000 couleurs • Carte Ethernet 1 Gbit/s

La complexité des systèmes de sécurité a considérablement augmenté au cours des deux dernières années. Dans le même temps, vous comptez toujours sur votre système pour atténuer les risques de sécurité. Avec Bosch Software Assurance, vous pouvez toujours nous contacter pour obtenir de l'aide afin de garantir que votre système continue de fonctionner.

Vous pouvez trouver les conditions générales de Bosch Software Assurance sur le site Web de Bosch Building Technologies : <https://www.boschsecurity.com/xc/en/solutions/management-software/bosch-software-assurance/>

Caractéristiques techniques

Les tableaux suivants spécifient les dimensions d'un système de contrôle d'accès AMS sous deux aspects :

- Selon le lot de licences respectif : **LITE, PLUS** ou **PRO**.
- Au maximum, si les licences nécessaires sont achetées.

Lot de licences LITE

LITE	Nombre sous licence	Nombre maximal
Nombre de portes (avec 1 ou 2 lecteurs) :	16	144
Nombre de cartes :	1000	200,000
Nombre de divisions :	1	400
Nombre de clients configurables :	1	2
Nombre de MAC	1	1
Nombre de contrôleurs AMC	125 maximum par MAC Jusqu'à 60 (sur le réseau) recommandés pour des performances élevées	
Nombre d'autorisations	1024 maximum par MAC	
Nombre de tours de garde	50	
SDK disponible	✓	
Intégration BVMS disponible	✓	
Intégration d'intrusion	Nombre maximal de centrales Bosch B Series (Bx512) et G Series (Bx512G) : <ul style="list-style-type: none"> pour la commande et le contrôle : 25 pour la gestion centralisée des utilisateurs : 50 	

Lot de licences PLUS

PLUS	Nombre sous licence	Nombre maximal
Nombre de portes (avec 1 ou 2 lecteurs) :	32	512
Nombre de cartes :	2000	200,000
Nombre de divisions :	1	400
Nombre de clients configurables :	1	5
Nombre de MAC	3	10
Nombre de contrôleurs AMC	125 maximum par MAC Jusqu'à 60 (sur le réseau) recommandés pour des performances élevées	
Nombre d'autorisations	1024 maximum par MAC	

PLUS	Nombre sous licence	Nombre maximal
Nombre de tours de garde	100	
SDK disponible	✓	
Intégration BVMS disponible	✓	
Intégration d'intrusion	Nombre maximal de centrales Bosch B Series (Bx512) et G Series (Bx512G) : <ul style="list-style-type: none"> pour la commande et le contrôle : 25 pour la gestion centralisée des utilisateurs : 50 	

Lot de licences PRO

PRO	Nombre sous licence	Nombre maximal
Nombre de portes (avec 1 ou 2 lecteurs) :	32	10,000
Nombre de cartes :	5000	200,000
Nombre de divisions :	1	400
Nombre de clients configurables :	1	40
Nombre de MAC	5	40
Nombre de contrôleurs AMC	125 maximum par MAC Jusqu'à 60 (sur le réseau) recommandés pour des performances élevées	
Nombre d'autorisations	1024 maximum par MAC	
Nombre de tours de garde	200	
SDK disponible	✓	
Intégration BVMS disponible	✓	
Intégration d'intrusion	Nombre maximal de centrales Bosch B Series (Bx512) et G Series (Bx512G) : <ul style="list-style-type: none"> pour la commande et le contrôle : 25 pour la gestion centralisée des utilisateurs : 50 	

Langues de l'interface utilisateur

- AR : Arabe *
- DE : Allemand
- EN : Anglais
- ES : Espagnol *

- FR : Français *
- HU : Hongrois *
- NL : Néerlandais *
- PL : Polonais
- PT : Portugais
- RU : Russe
- TR : Turc *
- ZH-CN : Chinois (simplifié) *
- ZH-TW : Chinois (traditionnel) *

(*) Cette langue n'est pas disponible pour Gestion des visiteurs dans AMS version mineure 3.0.1

Périphériques matériels pris en charge

- La gamme Bosch AMC2 de contrôleurs d'accès
Voir les fiches techniques correspondantes dans les catalogues de produits à l'adresse <https://www.boschsecurity.com>
- Cartes d'extension Bosch AMC2
Voir les fiches techniques correspondantes dans les catalogues de produits à l'adresse <https://www.boschsecurity.com>
- Composants de porte en ligne à distance
SimonsVoss SmartIntego

Pour Gestion des visiteurs

- Lecteur d'inscription de carte : LECTUS enroll 5000 MD
- Lecteur de signature : signotec LITE, signotec Omega
- Scanner pour les documents d'identité : ARH Combo, ARH Osmond

Informations de commande

AMS-BASE-LITE30 Licence Lite

Licence de base LITE
Numéro de commande **AMS-BASE-LITE30** |
F.01U.386.724

AMS-BASE-PLUS30 Licence Plus

Licence de base PLUS
Numéro de commande **AMS-BASE-PLUS30** |
F.01U.386.725

AMS-BASE-PRO30 Licence Pro

Licence de base PRO
Numéro de commande **AMS-BASE-PRO30** |
F.01U.386.726

AMS-XDIV-1V30 Licence pour 1 division

Licence pour 1 division supplémentaire
Numéro de commande **AMS-XDIV-1V30** | **F.01U.387.838**

AMS-XCLI-1V30 Licence pour 1 client opérateur

Licence pour 1 client opérateur
Numéro de commande **AMS-XCLI-1V30** | **F.01U.386.727**

AMS-XCLI-5V30 Licence pour 5 clients opérateur

Licence pour 5 clients opérateur
Numéro de commande **AMS-XCLI-5V30** | **F.01U.386.728**

AMS-XMAC-1V30 Licence pour 1 serveur MAC

Licence pour 1 serveur MAC
Numéro de commande **AMS-XMAC-1V30** |
F.01U.386.729

AMS-XMAC-5V30 Licence pour 5 serveurs MAC

Licence pour 5 serveurs MAC
Numéro de commande **AMS-XMAC-5V30** |
F.01U.386.730

AMS-XCRD-100V30 Licence pour 100 badges

Licence pour 100 badges
Numéro de commande **AMS-XCRD-100V30** |
F.01U.386.736

AMS-XCRD-1KV30 Licence pour 1000badges

Licence pour 1 000 badges
Numéro de commande **AMS-XCRD-1KV30** |
F.01U.386.737

AMS-XCRD-10KV30 Licence pour 10.000badges

Licence pour 10 000 badges
Numéro de commande **AMS-XCRD-10KV30** |
F.01U.386.738

AMS-XCRD-50KV30 Licence pour 50.000badges

Licence pour 50 000 badges
Numéro de commande **AMS-XCRD-50KV30** |
F.01U.386.739

AMS-XDRS-32V30 Licence pour 32 portes

Licence pour 32 portes
Numéro de commande **AMS-XDRS-32V30** |
F.01U.386.731

AMS-XDRS-128V30 Licence pour 128 portes

Licence pour 128 portes
Numéro de commande **AMS-XDRS-128V30** |
F.01U.386.732

AMS-XDRS-512V30 Licence pour 512 portes

Licence pour 512 portes
Numéro de commande **AMS-XDRS-512V30** |
F.01U.386.733

AMS-XOND-25V30 Licence 25 portes distantes en ligne

Licence pour 25 portes en ligne à distance
Numéro de commande **AMS-XOND-25V30** |
F.01U.386.734

Licence AMS-XPAN-1V30 pour 1 centrale intrusion

Licence pour 1 centrale intrusion
Numéro de commande **AMS-XPAN-1V30** | **F.01U.387.836**

AMS-XPAN-10V30 Licence pour 10 centrales intrusion

Licence pour 10 centrales intrusion
Numéro de commande **AMS-XPAN-10V30** |
F.01U.386.740

AMS-FVIS-WEBV30 Licence pour gestion des visiteurs

Licence pour gestion des visiteurs
Numéro de commande **AMS-FVIS-WEBV30** |
F.01U.395.536

AMS-FUPG-TOPL30 Licence de Lite à Plus

Mise à niveau de Lite à Plus
Numéro de commande **AMS-FUPG-TOPL30** |
F.01U.386.742

AMS-FUPG-TOPR30 Licence de Plus à Pro

Mise à niveau de Plus à Pro
Numéro de commande **AMS-FUPG-TOPR30** |
F.01U.386.743

TRA-AMS-CE Formation AMS - Expert

Formation locale pour un expert AMS

Numéro de commande **TRA-AMS-CE | F.01U.367.232**

TRA-AMS-EE Formation AMS - Expert

Formation au siège pour un expert AMS

Numéro de commande **TRA-AMS-EE | F.01U.367.233**

Représenté par :

Europe, Middle East, Africa:

Bosch Security Systems B.V.
P.O. Box 80002
5600 JB Eindhoven, The Netherlands
Phone: + 31 40 2577 284
emea.securitysystems@bosch.com
emea.boschsecurity.com

Germany:

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