

## BIS - Access Engine (ACE) version 5.0



Le contrôle d'accès est devenu l'une des plus importantes technologies actuelles destinées à améliorer la sécurité des personnes, des immeubles et des biens. Le module BIS Access Engine et les produits de contrôle sophistiqués proposés offrent une large gamme de fonctionnalités de contrôle d'accès.

Associez le progiciel de base Access Engine à des fonctionnalités disponibles en option et bénéficiez d'un système de contrôle d'accès personnalisé adapté exactement à vos besoins. Puis utilisez le logiciel Building Integration System pour intégrer le module Access Engine avec votre équipement de sécurité vidéo et de détection d'intrusion.

### Présentation du système

Associé au matériel d'accès Bosch, le logiciel Access Engine (ACE) constitue un système de contrôle d'accès complet au sein du Building Integration System (BIS). Il intègre toutes les fonctionnalités essentielles des systèmes de contrôle d'accès autonomes, ainsi qu'une large gamme d'améliorations disponibles en option.

Tout comme les autres modules BIS, le module ACE exploite toutes les fonctionnalités du système BIS, telles que les plans d'emplacement interactifs et les plans d'action, pour une gestion des alarmes puissante et totalement intégrée. Les messages d'alarme et les événements de contrôle d'accès

- ▶ Système de contrôle d'accès distribué avec gestion graphique des alarmes
- ▶ Intégration et interaction transparentes avec les systèmes vidéo, de détection incendie, de détection d'intrusion et PA/VA via la plate-forme BIS commune
- ▶ Haute résilience grâce à une architecture système à 4 niveaux et à un déploiement redondant de composants critiques
- ▶ Intégration de produits tiers via SDK et des protocoles ouverts et sécurisés
- ▶ Processus d'inscription efficace avec la solution Mobile Access entièrement intégrée de Bosch

peuvent être affichés avec des informations de localisation graphique et des instructions de flux de travail.

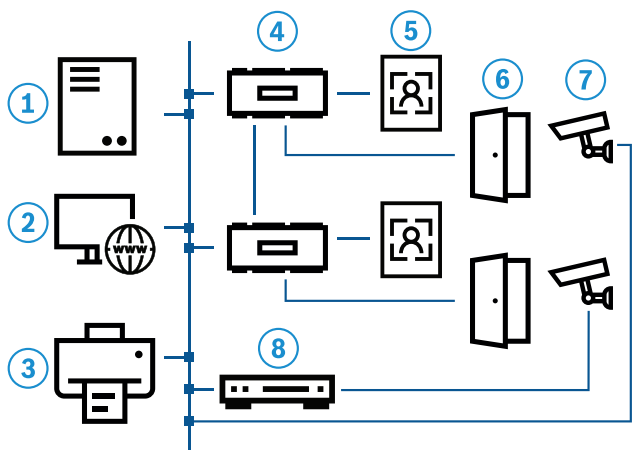
Le module ACE utilise les interfaces utilisateur BIS standard et leur souplesse de personnalisation. Il propose en outre des interfaces de configuration d'accès spécifiques pour les détenteurs de cartes, le matériel d'accès et les règles d'accès.

Le principal atout de la gamme Building Integration System réside dans l'intégration d'un large éventail de systèmes de sécurité dans les mêmes locaux. En associant le module ACE aux autres modules BIS (Automation et Vidéo, par exemple), vous pouvez concevoir des solutions de sécurité intelligentes sur mesure pour répondre aux besoins exacts de votre offre.

Access Engine s'exécute sur un poste de travail unique dans un système client-serveur, ou dans un environnement distribué doté d'un serveur central et de serveurs locaux ou régionaux.

Dans l'environnement multi-serveur distribué, tous les appareils, détenteurs de carte et autorisations peuvent être gérés depuis le serveur de niveau supérieur.

Pour garantir une sécurité et une intégrité des données optimales, BIS ACE peut gérer des contrôleurs RS485 haute sécurité avec le protocole OSDP v2 pour une communication chiffrée authentifiée et la supervision du lecteur.



**N° Description (système à serveur unique)**

|   |   |
|---|---|
| 1 | Serveur BIS central avec logiciels Access Engine et Vidéo Engine  |
| 2 | Plusieurs postes de travail pour la gestion des alarmes ou l'inscription  |
| 3 | Appareils d'inscription comme une imprimante de cartes, un scanner de signature, un lecteur d'inscription, un appareil photo pour les photos d'identité |
| 4 | Contrôleurs d'accès   |
| 5 | Lecteurs d'accès  |
| 6 | Gâches  |
| 7 | Caméra IP   |
| 8 | Enregistreur numérique, par ex. DIVAR pour l'enregistrement d'alarme  |

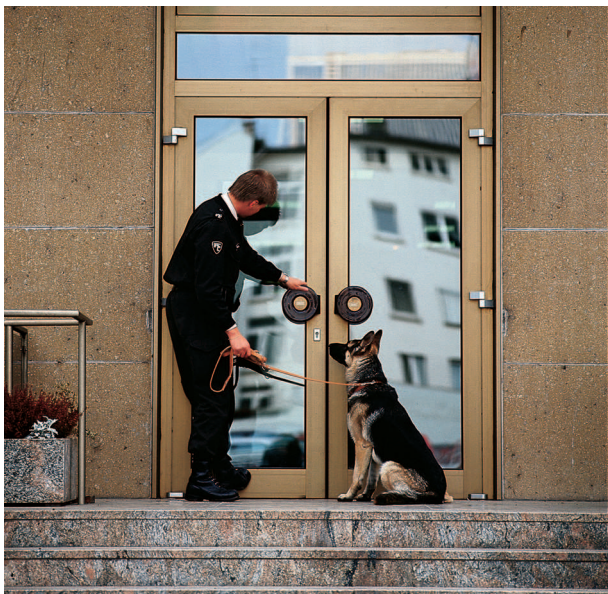
**Fonctions**

Le progiciel de base Access Engine, associé aux contrôleurs d'accès AMC, offre les fonctionnalités suivantes :

- Une large gamme de modèles intuitifs de portes permettant une configuration matérielle rapide et facile (par ex., porte standard, tourniquet, ascenseur avec lecteurs Heure & présence (TA), etc.).
- La boîte de dialogue de configuration du modèle de porte génère un plan de câblage pour l'installateur du matériel.
- Processus d'intégration souple, y compris l'inscription par carte et par biométrie.
- Boîtes de dialogue personnalisables pour ne collecter que les informations personnelles nécessaires.

- Plages horaires pour un contrôle d'accès basé sur les horaires, y compris les jours spéciaux, les jours fériés récurrents, etc.
- Plages horaires pour activation/désactivation automatique des comptes du détenteur de carte (codes PIN, etc.).
- Modèles horaires pour activation/désactivation automatique des paramètres système, par exemple définition d'une porte de bureau comme devant être déverrouillée de 9 h à 17 h
- Code PIN supplémentaire pour armement/désarmement de l'alarme intrusion.
- Blocage/débloccage temporaire des détenteurs de carte, soit manuellement, soit contrôlé par temporisation.
- Liste noire des cartes.
- Anti-Passback.
- La répartition équilibrée des zones d'accès (incluant la vérification des séquences d'accès) offre un moyen de limiter le nombre de personnes présentes dans une zone donnée, d'armer ou de désarmer automatiquement des alarmes si zone vide (ou non vide) et de générer des listes d'échantillons.
- Le principe d'autorisation d'un nombre N de personnes permet l'accès à une porte uniquement lorsqu'un nombre défini (N) de détenteurs de carte autorisés présentent leurs badges à un lecteur configuré en conséquence. Le paramètre peut être défini pour chaque lecteur, de 2 à N (illimité) personnes.
- La fonctionnalité de contrôle des sas gère deux portes jumelées avec deux paires de lecteurs. Elle est recommandée pour des niveaux de sécurité élevée, par exemple pour les entrées des salles serveur ou des services de recherche.
- Guard Tour : système de suivi de patrouille de pointe utilisant les lecteurs de contrôle d'accès existants, la vérification des séquences d'accès et des horaires d'accès. Toute violation de la séquence ou des horaires déclenche une alarme, qui est ensuite contrôlée par les fonctions sophistiquées

de gestion des alarmes du système BIS. Les rapports Guard Tour peuvent être générés depuis le journal des événements du système BIS.



- Fonctionnalité de surveillance aléatoire : les détenteurs de carte accédant au site ou le quittant peuvent être arrêtés de manière aléatoire et dirigés vers le personnel de sécurité pour une inspection plus approfondie. Les cartes appartenant aux personnes dites « VIP » peuvent être exclues de cette surveillance aléatoire.
- Visitor Management : les cartes des visiteurs peuvent faire l'objet d'un suivi et être gérées séparément selon leurs périodes de validité et la nécessité probable d'une escorte.
- Interface d'armement/désarmement d'un système de détection d'intrusion (avec gestion des autorisations et affectation des cartes).
- Importation et exportation sur le Web de données de détenteurs de cartes stockées sur des systèmes tiers ou sur un serveur d'annuaire, tel que Microsoft Active Directory ou Apache Directory.
- Toutes les informations personnelles (notamment les photos et les signatures) sont stockées dans une base de données SQL sécurisée.
- Gestion du niveau de menace pour préconfigurer jusqu'à 15 scénarios, y compris les situations de verrouillage et d'évacuation.
- Interface d'ascenseur pour contrôler jusqu'à 64 étages via un lecteur de carte interne à l'ascenseur et pour affecter des autorisations par étage aux détenteurs de carte.
- Interface avec les systèmes de gestion de destination pouvant autoriser jusqu'à 255 étages avec portes avant et arrière dans un système d'ascenseur.
- Interface d'importation des données du personnel depuis un système RH ou d'exportation de ces données du module ACE vers ce système.

- Personnalisation améliorée des cartes permettant d'importer les images des détenteurs de carte et de créer des badges avec une mise en page propre à votre entreprise et imprimables sur des imprimantes de carte standard.
- Fonction de déverrouillage des portes à distance (par ex. par un simple clic sur une icône du plan d'emplacement interactif du système BIS).
- Création de zones logiques (salles individuelles, groupes de salles, étages entiers ou parkings) auxquelles des points de contrôle d'accès spécifiques peuvent être assignés.
- Gestion souple des alarmes pour une grande variété de conditions d'alarme (par exemple : accès refusé, détection de sabotage, liste noire de badges, alarme de contrainte, etc.) qui peuvent être associées à des fonctions BIS telles que les plans d'emplacement interactifs et les plans d'action.
- Utilisation des entrées et sorties contrôlées et numériques de la gamme des contrôleurs Bosch pour des fonctions de contrôle et de surveillance supplémentaires, incluant la détection d'intrusion et de sabotage.
- La communication entre les contrôleurs d'accès locaux et les lecteurs est sécurisée par OSDP V2 (OSDP Secure Channel).
- La communication entre le système de contrôle d'accès principal et les contrôleurs d'accès locaux est sécurisée par DTLS (avec chiffrement AES-256).



- Enregistrement centralisé de tous les événements d'accès et de toutes les alarmes pour conformité réglementaire et recherche contextuelle.
  - Piste de vérification des modifications apportées aux enregistrements à long terme et aux autorisations (création, modification et suppression d'enregistrements).
  - Génération de rapports intégrée avec capacité de filtrage.
- Prise en charge simultanée de huit formats de cartes Wiegand différents, au maximum.
- Modification en masse des autorisations et autres données.

### Mobile Access

Mobile Access comprend les fonctionnalités suivantes avec des avantages pour l'opérateur, le propriétaire du bâtiment ou l'utilisateur final :

- Intégration du smartphone comme moyen d'accès, ce qui étend la carte de contrôle d'accès classique.
- Gestion à distance des droits d'accès par l'envoi d'un jeton d'entrée virtuel (une carte virtuelle, à utiliser dans l'application) à un visiteur ou un collaborateur.

- Différentes informations d'identification mobiles, correspondant à différents sites, peuvent être stockées dans une seule application mobile.
- Identification biométrique configurable, telle que Touch ID et Face ID.

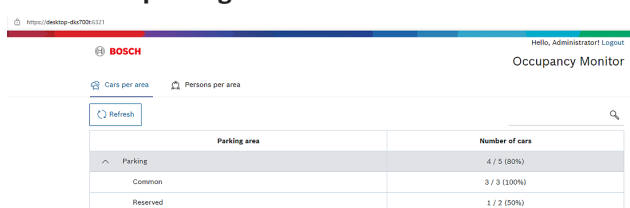
Pour plus d'informations, consultez la fiche technique de Mobile Access dans le catalogue de produits Bosch.

### Vérification vidéo

La vérification vidéo étend le niveau de sécurité de votre système de contrôle d'accès par la technologie vidéo. Lorsqu'un lecteur est en mode de vérification vidéo, le détenteur de carte ne peut pas être admis directement. Ainsi, le lecteur crée une demande d'entrée qui s'affiche sous la forme d'un message sur l'écran de l'opérateur.

Un plan d'action (voir les accessoires en option de BIS) montre à l'opérateur l'image du détenteur de carte telle qu'elle est stockée dans la base de données ACE à côté de l'image en temps réel provenant d'une caméra située à proximité de l'entrée/du lecteur qui a envoyé la demande. L'opérateur compare les deux images et décide d'ouvrir ou non la porte.

### Gestion de parkings



Cette fonctionnalité permet de définir et d'utiliser le modèle de porte « parking » intégrant le contrôle de deux barrières d'entrée et de sortie et leurs feux de signalisation, qui empêchent l'accès lorsque le parking a atteint sa capacité maximale.

L'accès aux parkings peut être régulé par un lecteur longue portée et des badges, ou par une caméra et les plaques d'immatriculation.

Chaque parking peut être divisé en zones logiques, avec un nombre maximum de voitures défini pour chacun. L'autorisation de passage par la barrière et de stationner dans une zone logique peut être assignée aux détenteurs de carte via les boîtes de dialogue standard. La répartition de charge des parkings est également possible, avec des informations de capacité affichées en temps réel sur l'écran de l'opérateur. La répartition de charge des voitures (parkings) et des personnes (zones d'accès) est gérée séparément, de telle façon qu'il est possible d'identifier l'emplacement du détenteur de carte et de sa voiture simultanément.

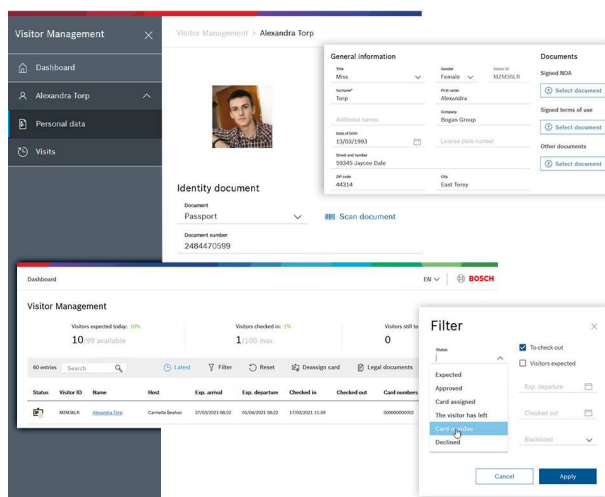
### Gestion de visiteurs

- 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.



### Intégration de centrales intrusion

Les autorisations d'utilisation des centrales intrusion Bosch B Series et G Series peuvent être affectées aux titulaires de badges de manière centralisée, leur permettant d'armer et de désarmer les zones sous contrôle d'intrusion.

Avec l'autorisation appropriée, le titulaire d'un badge peut désarmer une zone et en déverrouiller la porte d'une simple lecture du badge par un lecteur.

### Contrôle d'accès pour le contrôle des maladies

- Les nouveaux lecteurs d'empreintes digitales et de reconnaissance faciale sans contact éliminent une source dangereuse de contamination. Pour une sécurité encore meilleure, le système peut éventuellement demander un badge sans contact ou un autre identifiant biométrique pour l'authentification.
- Le contrôle de la séquence d'accès permet d'appliquer un flux de foule à sens unique, réduisant le risque d'infection en éliminant les rencontres en face à face.
- La gestion du niveau de menace d'ACE permet de passer instantanément d'un schéma de flux de foule à un autre, en cas d'urgence.
- Les zones de contrôle d'accès d'ACE sont idéales pour appliquer rapidement des restrictions d'hygiène sur le nombre de personnes présentes dans un espace défini.

- Les lecteurs sans contact éliminent le besoin de boutons d'ascenseur physiques.
- L'armement et le désarmement sans contact des zones d'intrusion réduisent davantage les sources de contamination.
- L'utilisation de téléphones mobiles pour l'accès favorise l'hygiène en réduisant le nombre d'informations d'identification physiques partagées, une solution coopérative développée avec des partenaires **HID** et **STiD**.
- Les systèmes de reconnaissance des plaques d'immatriculation réduisent le besoin de cabines de contrôle avec présence physique, de claviers et de boutons, ou de devoir sortir du véhicule pour fournir des informations d'identification physiques.

### Accessoires pour le module BIS Access Engine

#### Gestion de parking étendue

Permet la gestion du parking invité, y compris la génération de tickets de parking et de notification sur les visiteurs qui dépassent leurs durées de rendez-vous programmés.

#### Interface de programmation

Kit de développement logiciel (SDK) permettant d'intégrer Access Engine à des applications tierces telles que Identity Management, Time & Attendance et des systèmes de gestion avancée des visiteurs.

#### Intégration d'armoires à clés

Intégration d'armoires à clés **Deister** et **Kemas** pour sécuriser les clés et surveiller leur utilisation. Disponible dans certains pays uniquement.

#### Intégration de verrous en ligne sans fil

Intégration de verrous en ligne **SimonsVoss SmartIntego** sans fil (barillets de serrure, poignées de porte et verrous) pour les portes qui nécessitent une sécurité de niveau intermédiaire, telles que des portes de bureaux et de salles de classe. Disponible dans certains pays uniquement.

#### Intégration de verrous hors ligne à distance

Intégration de **verrous hors ligne compatibles OSS-SO** ou de **verrous hors lignes Normbau (Pegasys)** pour des portes à distance, dont la connexion par câblage n'est pas possible en raison de la distance, des conditions de construction ou du coût. Le système de verrouillage hors ligne se compose de logiciels, de matériel et d'accessoires. Le matériel est librement disponible sur le marché libre auprès de partenaires Bosch. La licence logicielle permet un certain nombre de boîtes de dialogue dans BIS et ACE. Disponible dans certains pays uniquement.

#### Augmentation des capacités de contrôle d'accès

ACE s'adapte facilement aux besoins évolutifs de vos sites. Des licences MAC (Main Access Controller) supplémentaires vous permettent d'accroître la couverture géographique ou les performances. Il est

possible d'accueillir un plus grand nombre d'employés ou de visiteurs avec des licences de détenteur de carte supplémentaires.

Des licences permettant d'accroître le nombre d'entrées sont disponibles par incréments de 32, 128 ou 512. Une entrée, dans ce sens, équivaut à un modèle de porte ACE, facilitant ainsi les calculs de spécifications.

Exemple : votre site dispose de 2 entrées principales avec un lecteur d'entrée et un lecteur de sortie pour chacune, 26 portes de bureau avec lecteur d'entrée et 1 contrôle de sas pour la salle serveurs. Le nombre total de modèles de portes (et d'entrées) est de 29, quel que soit le nombre de lecteurs concernés. Un total de 32 entrées est déjà couvert par les licences fournies avec le progiciel de base ACE.

### Remarques sur l'installation/la configuration

#### Access Engine en chiffres

Les valeurs maximales suivantes s'appliquent au système de référence décrit ci-dessous.

|  |   |
|--|---|
| Nombre maximal de cartes actives par système   | 400,000   |
| Nombre maximum de lecteurs par serveur   | 10,000  |
| Nombre maximum de contrôleurs MAC (Master Access Controller) par serveur                           | 40  |
| Nombre maximum d'autorisations d'accès par MAC   | 1,000   |
| Nombre maximal d'AMC par MAC   | 125<br>Pour les systèmes hautes performances : 60 |
| Nombre maximum d'autorisations d'accès par ACE   | 40,000  |
| Nombre max de divisions par ACE  | 400   |
| Nombre max de tours de garde par ACE   | 200   |
| Nombre max de tours de garde simultanés  | 8   |
| Nombre maximal de centrales intrusion B/G pour la synchronisation des titulaires de carte avec ACE | 500   |

#### Systèmes de référence pour serveur et client

|            | Système serveur (sans client en cours d'exécution) | Système client                                      |
|------------|--|---|
| Processeur | Intel Xeon E-2144G @ 3,6 GHz (4 cœurs, 8 logiques) | Intel Core i7-8700 @ 3,2 GHz (6 cœurs, 12 logiques) |

|                                    | Système serveur (sans client en cours d'exécution)   | Système client                               |
|------------------------------------|--|--|
| RAM                                | 32 Go (2 667 MHz)  | 8 Go (2 667 MHz)                             |
| GPU                                | Cartes graphiques intégrées du processeur  | Intel UHD Graphics 630 (4 Go de mémoire GPU) |
| Disque système                     | NVMe<br>Vitesse d'écriture : 1440 Mo/s<br>Vitesse de lecture : 2250 Mo/s<br>Temps de réponse moyen : 10 ms | Disque SSD                                   |
| Disque sur lequel AMS est installé | SSD<br>Vitesse d'écriture : 1000 Mo/s<br>Vitesse de lecture : 1100 Mo/s<br>Temps de réponse moyen : 10 ms  |  |
| Système d'exploitation             | Microsoft Server 2019 Standard Edition   | Microsoft 10 Pro Edition                     |

### Versions de navigateur pour les programmes complémentaires basés sur le Web

| Navigateur Web  | Version          |
|-----------------|------------------|
| Google Chrome   | 112 ou ultérieur |
| Microsoft Edge  | 111 ou ultérieur |
| Mozilla Firefox | 102 ou ultérieur |

### Caractéristiques techniques

Voir les spécifications de la version respective du package BIS de base.

### Informations de commande

#### BIS-FACE-BPA50 Licence de base

Licence de base pour BIS Access Engine  
Numéro de commande **BIS-FACE-BPA50** | **F.01U.415.273**

#### BIS-XACE-32DR50 Licence pour 32 portes

Licence pour 32 portes  
Numéro de commande **BIS-XACE-32DR50** | **F.01U.415.287**

#### BIS-XACE-128D50 Licence pour 128 portes

Licence pour 128 portes (ACE)  
Numéro de commande **BIS-XACE-128D50** | **F.01U.415.288**

#### BIS-XACE-512D50 Licence pour 512 portes

Licence pour 512 portes  
Numéro de commande **BIS-XACE-512D50** | **F.01U.415.289**

#### BIS-FACE-OFFL50 Licence pour module de base hors ligne

Licence pour module de base hors ligne (ACE)  
Numéro de commande **BIS-FACE-OFFL50** | **F.01U.415.275**

#### BIS-XACE-25OF50 Licence pour 25 portes hors ligne

Licence pour 25 portes hors ligne  
Numéro de commande **BIS-XACE-25OF50** | **F.01U.415.286**

#### BIS-XACE-25OS50 Licence pour 25 portes hors ligne OSS-SO

Licence pour 25 portes hors ligne OSS-SO  
Numéro de commande **BIS-XACE-25OS50** | **F.01U.415.309**

#### BIS-XACE-25ON50 Licence 25 portes distantes sans fil

Licence pour 25 portes en ligne sans fil  
Numéro de commande **BIS-XACE-25ON50** | **F.01U.415.294**

#### BIS-XACE-100C50 Licence pour 100 badges

Licence pour 100 badges (ACE)  
Numéro de commande **BIS-XACE-100C50** | **F.01U.415.290**

#### BIS-XACE-1KC50 Licence pour 1000 badges

Licence pour 1 000 badges  
Numéro de commande **BIS-XACE-1KC50** | **F.01U.415.291**

#### BIS-XACE-10KC50 Licence pour 10000 badges

Licence pour 10 000 badges (ACE)  
Numéro de commande **BIS-XACE-10KC50** | **F.01U.415.292**

#### BIS-XACE-50KC50 Licence pour 50000 badges

Licence pour 50 000 badges  
Numéro de commande **BIS-XACE-50KC50** | **F.01U.415.293**

#### BIS-FACE-MOB50 Licence Mobile Access

Licence Mobile Credentials  
Numéro de commande **BIS-FACE-MOB50** | **F.01U.416.876**

#### BIS-XACE-50MO50 Licence 50 Mobile Credentials

Licence 50 Mobile Credentials  
Numéro de commande **BIS-XACE-50MO50** | **F.01U.416.872**

#### BIS-XACE-100M50 Licence 100 Mobile Credentials

Licence 100 Mobile Credentials  
Numéro de commande **BIS-XACE-100M50** | **F.01U.416.873**

#### BIS-XACE-1KMO50 Licence 1000 Mobile Credentials

Licence 1000 Mobile Credentials  
Numéro de commande **BIS-XACE-1KMO50** | **F.01U.416.874**

#### BIS-XACE-5KMO50 Licence 5000 Mobile Credentials

Licence 5000 Mobile Access  
Numéro de commande **BIS-XACE-5KMO50** | **F.01U.416.875**

#### BIS-XACE-1MAC50 Licence pour 1 MAC

Licence pour 1 MAC  
Numéro de commande **BIS-XACE-1MAC50** | **F.01U.415.284**

**BIS-XACE-10MC50 Licence pour 10 MAC**

Licence pour 10 MAC (ACE)

Numéro de commande **BIS-XACE-10MC50** |**F.01U.415.285****BIS-XACE-1KEY50 Licence pour 1 armoire à clés**

Licence pour 1 armoire à clés

Numéro de commande **BIS-XACE-1KEY50** |**F.01U.415.295****BIS-FACE-PRK50 Licence pour gestion parking**

Licence pour gestion parking (ACE)

Numéro de commande **BIS-FACE-PRK50** | **F.01U.415.277****BIS-FACE-VISWEB50 Licence pour gestion des visiteurs**

Licence pour Visitor Management (ACE)

Numéro de commande **BIS-FACE-VISWEB50** |**F.01U.415.276****BIS-FACE-API50 Licence pour API**

Licence BIS Access Engine pour API

Numéro de commande **BIS-FACE-API50** | **F.01U.415.274****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  
[www.boschsecurity.com/xc/en/contact/](http://www.boschsecurity.com/xc/en/contact/)  
[www.boschsecurity.com](http://www.boschsecurity.com)

**Germany:**

Bosch Sicherheitssysteme GmbH  
Robert-Bosch-Ring 5  
85630 Grasbrunn  
Tel.: +49 (0)89 6290 0  
Fax: +49 (0)89 6290 1020  
[de.securitysystems@bosch.com](mailto:de.securitysystems@bosch.com)  
[www.boschsecurity.com](http://www.boschsecurity.com)