Credential Management V5.2

Y compris, Mobile Access

fr Manuel d'utilisation

Table des matières

1 Sécurité

Utiliser les derniers logiciels

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.

2 Introduction

2.1 À propos de Credential et de Visitor Management

Credential Management, ci-après appelé CredMgmt, est un outil logiciel basé sur un navigateur, qui fonctionne en tandem avec un système de contrôle d'accès Bosch ou ACS. Doté d'une interface utilisateur simple et intuitive, il permet même aux opérateurs relativement inexpérimentés de gérer les identifiants d'accès des employés et du personnel externe. Les informations d'identification elles-mêmes peuvent être soit des cartes physiques, soit des cartes virtuelles envoyées aux appareils mobiles des employés.

Credential Management

Dans CredMgmt, les opérateurs ACS peuvent gérer à la fois les informations d'identification et les enregistrements des employés auxquels appartiennent les informations d'identification.

Entité	Ajouter	Modifier	Supprimer	Affecter/ Désaffecter
Informations d'identification physiques				Oui
Identifiants « mobiles » virtuels (si Mobile Access est installé)	Oui		Oui	Oui
Autorisations				Oui
Enregistrements des titulaires de carte	Oui	Oui	Oui	

Visitor Management

Dans VisMgmt, les opérateurs ACS gèrent les informations d'identification, les enregistrements de visiteurs et les enregistrements de visites.

Entité	Ajouter	Modifier	Supprimer	Affecter/ Désaffecter
Informations d'identification physiques				Oui
Identifiants « mobiles » virtuels (si Mobile Access est installé)	Oui			Oui
Enregistrements des visiteurs	Oui	Oui	Oui	
Enregistrements des visites	Oui	Oui	Oui	

2.2 À propos de Mobile Access

Mobile Access permet de contrôler l'accès des personnes à l'aide d'informations d'identification virtuelles stockées sur un appareil mobile tel que le smartphone d'une personne. Les informations d'identification virtuelles sont conservées dans le système de contrôle d'accès principal ou ACS.

- Les opérateurs de l'ACS génèrent, attribuent et envoient ces informations d'identification virtuelles aux personnes via une application Web de coopération.
- Les détenteurs d'identifiants mobiles utilisent des lecteurs de contrôle d'accès via Bluetooth à partir d'une application Mobile Access sur leurs appareils mobiles.

- Les installateurs de systèmes Mobile Access configurent les lecteurs de contrôle d'accès via Bluetooth à partir d'une application de configuration spéciale sur leurs appareils mobiles.
- Le système ne stocke aucune donnée personnelle sur les appareils mobiles.

3 Présentation de Credential Management

Les exemples suivants illustrent les topologies possibles des installations de Credential Management, avec et sans Mobile Access. Chaque boîte représente un ordinateur distinct.

Clé	Signification
ACS	Principal système de contrôle d'accès : AMS ou BIS-ACE
CM/VM	Back-end pour l'application Web : Credential Management ou Visitor Management
DB	Base de données ACS principale
Collaborateur	Back-end de Mobile Access
S	Application d'installation « Setup Access » pour les appareils mobiles des installateurs et configurateurs système
M	Application d'accès « Mobile Access » pour les appareils mobiles des détenteurs de badge normaux.

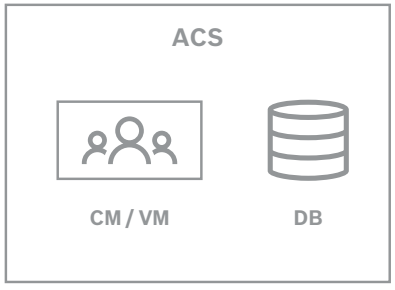
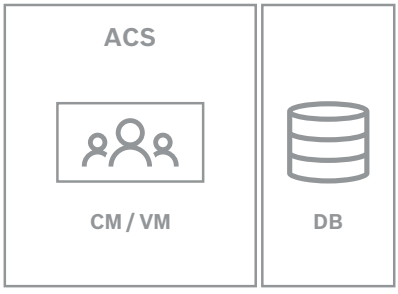
Credential Management, base de données locale	Credential Management, base de données distante
	

Tableau 3.1: Topologies de Credential Management

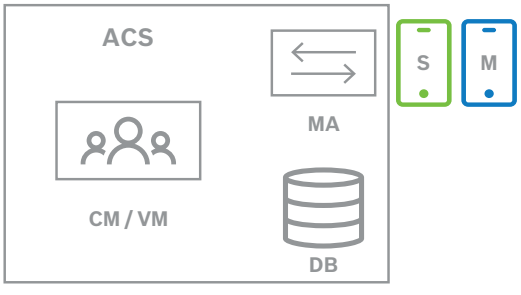
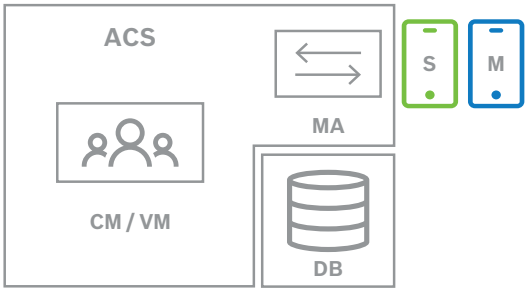
Mobile Access, colocalisé, base de données locale	Mobile Access, colocalisé, base de données distante
	

Tableau 3.2: Topologies colocalisées Mobile Access

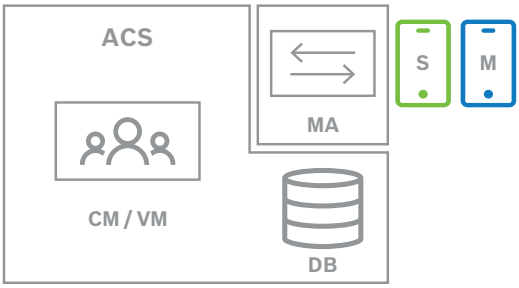
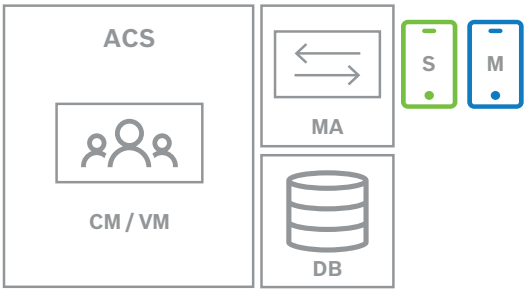
Mobile Access, distribué, base de données locale	Mobile Access, distribué, base de données distante
	

Tableau 3.3: Topologies distribuées Mobile Access

Versions compatibles des logiciels associés

Le tableau suivant répertorie les versions des outils logiciels auxiliaires compatibles avec cette version du système.

Éléments inclus	Version	Emplacement
Access Management System (AMS)	5.2 (comprend l'extension Mobile Access)	Magasin de téléchargement / Catalogue produit
Building Integration System (BIS)	5.0.1 (comprend l'extension Mobile Access)	Magasin de téléchargement / Catalogue produit
Visitor Management (VisMgmt)	5.2 (comprend l'extension Mobile Access)	Magasin de téléchargement / Catalogue produit

Remarque!

Divisions

Credential Management, Visitor Management et Mobile Access ne prennent pas en charge la fonctionnalité « Divisions » des systèmes de contrôle d'accès Bosch, où une personne (ACS) gère le contrôle d'accès de plusieurs locataires indépendants.

4 Informations de planification

5 Installation et désinstallation

5.1 Logiciels prérequis

Vous installez le serveur CredMgmt sur le même ordinateur que ACS (le principal contrôle d'accès système). Les mêmes exigences logicielles et matérielles s'appliquent.
Les programmes de configuration de CredMgmt et Mobile Access ont leur propre support d'installation, distinct de l'ACS. Ils peuvent être téléchargés depuis les catalogues de produits en ligne Bosch.

Remarque!
Nécessité d'un certificat racine stable
Avant de procéder aux installations ci-dessous, assurez-vous que l'installation de l'ACS est complète et sous licence, conformément à son propre guide d'installation. Cela inclut une décision finale sur le certificat racine du serveur ACS (qu'il soit autosigné ou basé sur une autorité de certification) et sa mise en œuvre stable. Les modifications post-hoc du certificat racine du serveur ACS nécessiteraient une reconfiguration des certificats sur tous les ordinateurs et lecteurs d'accès mobiles participant à son système de contrôle d'accès.

Configuration serveur requise
Le serveur est l'ordinateur qui exécute l'ACS et l'application CredMgmt.

Systèmes d'exploitation	Windows Server 2019 (Version 1809) (64bit, Standard, Datacenter); Windows Server 2022 (64 bits, Standard, Datacenter)
Systèmes de gestion de bases de données	MS SQL Server 2019 and later Utilisez toujours la même instance de base de données que celle de l'ACS (le principal système de contrôle d'accès)
Navigateurs pris en charge	Google Chrome, Mozilla Firefox, Microsoft Edge (Chromium based) Utilisez la version la plus récente du navigateur pour votre système d'exploitation Windows.
Résolution minimale du moniteur (pour utiliser l'interface utilisateur de l'application)	Full HD 1920x1080

Exigences des clients

Exigence	Description
Résolution minimale du moniteur	Full HD 1920x1080
Navigateurs pris en charge	Google Chrome, Mozilla Firefox, Microsoft Edge (Chromium based) Utilisez la version la plus récente du navigateur pour votre système d'exploitation Windows.

5.2 Prérequis matériels

Lecteurs d'inscription

CredMgmt nécessite au moins un lecteur d'inscription pour inscrire les cartes physiques. Les lecteurs d'inscription sont généralement installés sur les postes de travail clients. Le poste de travail client communique avec le matériel périphérique via un programme appelé `BoschPeripheralDeviceAddon.exe`. L'installation de ce programme est décrite ci-dessous. Les lecteurs d'inscription et les formats de carte suivants sont pris en charge.

	Code Bosch MIFARE DESFire EV1	MIFARE DESFire EV1 CSN	MIFARE Classic CSN	Prox HID 26 bits	iCLASS 26 bits	iCLASS 35 bits	iCLASS 37 bits	iCLASS 48 bits	EM 26 bits
LECTUS enroll ARD-EDMCV002-USB	X								
OMNIKEY 5427 CK		X	X	X	X	X	X	X	X

5.2.1 Configuration du module complémentaire pour périphériques

Le module complémentaire Peripheral Devices est requis uniquement sur les ordinateurs clients qui se connectent aux lecteurs d'inscription, aux scanners ou à d'autres périphériques. Répétez la procédure ci-dessous sur chaque ordinateur client qui présente cette exigence.

1. Sur l'ordinateur client souhaité, exécutez en tant qu'administrateur `BoschPeripheralDeviceAddon.exe` à partir du support d'installation.
   - Les composants principaux sont répertoriés, à savoir le logiciel client et le logiciel des périphériques habituels. Nous vous recommandons d'installer tous les composants répertoriés, même si vous ne disposez pas actuellement du matériel disponible.
2. Cliquez sur **Suivant** pour accepter les packages d'installation par défaut.
3. Dans l'écran **Configuration client**

- **Dossierd'installation :** Acceptez la valeur par défaut (recommandé) ou modifiez-la si nécessaire.
- **Port COM :**
  - Si vous utilisez un lecteur d'inscription LECTUS, entrez le numéro du port COM, par exemple `COM3`, auquel le lecteur d'inscription est connecté. Vérifiez cette valeur dans le Gestionnaire de périphériques Windows.
  - Si vous utilisez un lecteur HID OMNIKEY, laissez ce champ vide.
  - La caméra, le Signopad et le scanner de documents sont « plug-and-play » et ne nécessitent aucun port COM. Cliquez sur **Autoriser** lorsque le navigateur demande l'autorisation de se connecter.
- **Adresse du serveur** et **Port :**

- Entrez le nom de tous les ordinateurs serveurs, par défaut au moins l'ordinateur serveur ACS principal, et les numéros de port pour tous les services en arrière plan qui doivent contrôler les périphériques.
  Dans chaque cas, cliquez sur **Tester la connexion** et attendez la confirmation.
  Cliquez sur **Ajouter** pour ajouter d'autres serveurs.
  Cliquez sur **Supprimer** pour supprimer des serveurs.
- Les ports par défaut pour les services principaux habituels sont :
  `5806` pour CredMgmt
  `5706` pour VisMgmt

4. Cliquez sur **Suivant** pour obtenir un récapitulatif des composants à installer.
5. Cliquez sur **Installer** pour démarrer l'installation.
6. Cliquez sur **Terminer** pour finir l'installation.
7. Après l'installation, redémarrez l'ordinateur.

5.3 Installer Credential Management

Introduction

CredMgmt fonctionne comme une application Web en tandem avec un système de contrôle d'accès Bosch (ACS). Les sections suivantes décrivent l'installation du composant principal qui pilote cette application Web.

- Vous pouvez l'installer pour utiliser une base de données locale ou distante.

5.3.1 Prérequis pour CredMgmt

Utilisateur dédié pour une base de données distante (uniquement si vous utilisez une base de données distante)

L'utilisateur `CMUser` accède à la base de données d'ACS au nom de l'application CredMgmt. Si CredMgmt doit utiliser une base de données sur un serveur de base de données distant, utilisez la procédure ci-dessous.

IMPORTANT : n'exécutez pas le programme d'installation de CredMgmt avant de terminer cette procédure.

1. Sur le serveur de base de données distant, créez un utilisateur Windows de domaine dans le même domaine qu'ACS . Utilisez les paramètres suivants :

- **Nom d'utilisateur** (le nom d'utilisateur lui-même est sensible à la casse) : <ACS-Domain>\`CMUser`
- **Mot de passe** : définissez le mot de passe en fonction des politiques de sécurité qui s'appliquent à tous vos ordinateurs. Notez-le soigneusement, car il sera nécessaire pour l'installation de CredMgmt.
- **L'utilisateur doit changer de mot de passe à la prochaine connexion** : `NO`
- **L'utilisateur ne peut pas changer de mot de passe** : `YES`
- **Le mot de passe n'expire jamais** : `YES`
- **Connexion en tant que service** : `YES`
- **Le compte est désactivé** : `NO`

Ajoutez ensuite `CMUser` comme identifiant de connexion à distance au serveur SQL comme suit :

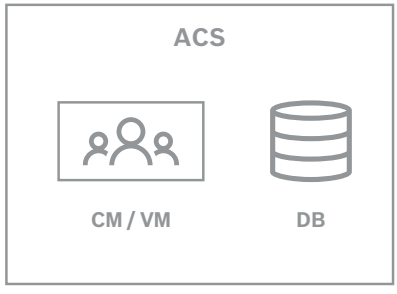
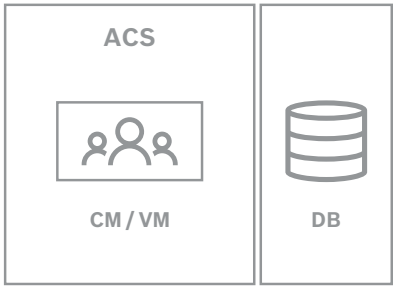
1. Ouvrez SQL Management Studio
2. Connectez-vous à l'instance SQL distante
3. Accédez à **Sécurité** > **Connexion**

4. Dans le volet **Sélectionner une page**, sélectionnez **Général**
5. Sélectionnez l'utilisateur `CMUser`
6. Dans le volet **Sélectionner une page**, sélectionnez **Rôles de serveur**
7. Cochez les cases `public` et `dbcreator`

Utilisateur dédié pour la base de données locale (uniquement si vous utilisez une base de données locale)
L'utilisateur `CMUser` accède à la base de données d'ACS au nom de l'application CredMgmt. Il n'est PAS nécessaire de créer cet utilisateur si CredMgmt doit utiliser une base de données locale, car le programme de configuration de CredMgmt crée un utilisateur Windows `CMUser` sur le serveur ACS automatiquement.

Un utilisateur dédié dans ACS
1. Dans ACS, créez un utilisateur doté de la fonctionnalité d'**utilisation API illimitée**.
– Chemin d'accès à la boîte de dialogue dans AMS : **Configuration** > **Opérateurs et postes de travail** > **Droits de l'utilisateur** > onglet : **Compte utilisateur** > **Contrôle des droits d'accès à l'API.**
Sélectionnez `Unlimited access` dans la liste.
– Chemin d'accès à la boîte de dialogue dans BIS : onglet **Configuration Parcourir** > **Administration** > **Opérateurs** > Select operator > : **Droits d'accès à l'API ACE.**
Sélectionner `Unlimited access`.
– Pour des instructions détaillées, reportez-vous au chapitre **Attribuer des profils d'utilisateur (opérateur)** dans le manuel d'ACS
2. Notez soigneusement le nom d'utilisateur et le mot de passe, car l'assistant d'installation de l'application en aura besoin.

5.3.2 Procédure d'installation

CredMgmt avec base de données locale	CredMgmt avec base de données distante
	

Procédure
1. Sur le serveur ACS exécutez `BoschCredentialManagementServer.exe` en tant qu'administrateur.
– Le programme d'installation s'ouvre
2. Sur l'écran **Composants principaux**, sélectionnez `Bosch Credential Management` et cliquez sur **Suivant**
3. Lisez attentivement et cliquez sur **Accepter** si vous acceptez le contrat de licence utilisateur final (CLUF). L'installation ne peut continuer que si vous le faites.

4. Parcourez et sélectionnez un dossier de destination pour l'installation, ou acceptez la valeur par défaut (recommandé), puis cliquez sur **Suivant**
5. Sur l'écran **SQL Server**, sélectionnez l'une des deux alternatives proposées pour l'emplacement de la base de données. Les configurations sont légèrement différentes. Choisissez une alternative pour l'étape suivante :

– ALTERNATIVE 1 **Base de données locale** :
  – Le programme d'installation trouve la base de données locale et la présélectionne.
  – Entrez le mot de passe SQL pour un utilisateur admin (la valeur par défaut est `sa`)
  – Cliquez sur **Tester la connexion**
  – Cliquez sur **Suivant**.
– ALTERNATIVE 2 **Base de données distante**
  – Entrez le nom du serveur SQL qui se trouve sur le réseau
  – Entrez le nom de l'instance SQL
  – Entrez le mot de passe SQL pour un utilisateur admin (la valeur par défaut est `sa`)
  – Cliquez sur **Tester la connexion**
  – Vérifiez le nom d'utilisateur et entrez le mot de passe de l'utilisateur administrateur Windows et SQL que vous avez créé pour l'utilisation de la base de données distante (voir Prérequis ci-dessus)
  – Cliquez sur **Suivant**.

6. Dans l'écran **Configuration de l'accès ACS** :

– Entrez le nom d'hôte du serveur ACS.
– Entrez le nom d'un utilisateur ACS avec une utilisation illimitée de l'API (voir Prérequis ci-dessus).
– Entrez le mot de passe ACS pour cet utilisateur ACS et confirmez-le.

7. Cliquez sur **Suivant**.
8. Dans l'écran **Configuration du serveur d'identité**

– Le serveur d'identité par défaut (présélectionné) est le serveur ACS principal avec le port `44333` `https://`<NameOfACSserver>`:44333`
– Cliquez sur **Tester la connexion**
– Si le test échoue, vérifiez à nouveau la disponibilité du serveur d'identité.
– Cliquez sur **Next (Suivant)**.

9. Sur l'écran **Composants principaux**, confirmez que CredMgmt est sélectionné et cliquez sur **Installer**
10. Une fois l'installation terminée, démarrez CredMgmt avec l'URL suivante :

`https://` <NameOfACSserver>`:5806`

5.4 Installer Mobile Access

Introduction

Le service back-end Mobile Access fournit une fonctionnalité d'accès mobile pour Credential Management et Visitor Management.

REMARQUE : Si vous utilisez CredMgmt et VisMgmt, vous devez installer Mobile Access une seule fois.

– Vous pouvez l'installer sur le même serveur qu'ACS (installation colocalisée) ou sur un serveur distinct (installation distribuée).
– Vous pouvez l'installer pour utiliser une base de données locale ou distante.

Accessibilité du service back-end de Mobile Access

Le service back-end de Mobile Access doit être accessible en permanence pour les appareils mobiles.

Pour des raisons de sécurité, il est très peu probable que les appareils mobiles disposent d'un accès réseau à un serveur ACS. Par conséquent, l'installation distribuée est recommandée. Cela vous permet d'exécuter le service back-end de Mobile Access sur un serveur « cloud » plus largement disponible.

5.4.1 Vue d'ensemble de l'installation, de la configuration et de l'utilisation

Mobile Access nécessite plusieurs composants qui fonctionnent de concert. Nous présentons ici les étapes générales et décrivons les prérequis et procédures respectives dans les sections suivantes de ce chapitre :

Configuration du serveur ACS

1. Un serveur ACS est installé, sous licence et opérationnel, avec un certificat racine permanent et des lecteurs d'accès compatibles. Les opérateurs y sont définis avec des autorisations leur permettant de gérer Mobile Access.

Configuration de Mobile Access

1. Un administrateur système installe l'une des applications Web ou les deux qui utilisent Mobile Access, soit Credential Management ou Visitor Management sur ACS.
2. Un administrateur système installe le back-end de Mobile Access.
3. Un administrateur système active Mobile Access dans les applications Web installées.

Configuration des lecteurs

1. Un administrateur système crée un installateur (personne autorisée à configurer les lecteurs Mobile Access) dans l'application CredMgmt.
2. Le programme d'installation télécharge l'application d'installation (« Setup Access ») sur son appareil mobile à partir de la boutique d'applications publique habituelle de l'appareil.
3. Un administrateur système envoie une invitation à l'installateur désigné.
4. L'installateur accepte l'invitation dans l'application d'installation. Cette invitation autorise l'installateur à configurer les lecteurs d'accès pour Mobile Access.
5. L'installateur configure les lecteurs à l'aide de l'application d'installation.

Utilisation de Mobile Access

1. Les détenteurs de données d'identification qui sont éligible à l'utilisation de Mobile Access téléchargent l'application correspondant (« Mobile Access ») de la boutique d'applications publique habituelle sur leurs appareils mobiles.
2. Les opérateurs de CredMgmt et/ou VisMgmt envoient des informations d'identification mobiles par code QR ou par e-mail aux détenteurs de badge admissibles.
3. Les détenteurs de données d'identification lisent le code QR ou l'e-mail dans l'application correspondante (« Mobile Access »). Cela permet à leur appareil mobile de fonctionner comme un identifiant physique lorsque l'application est en cours d'exécution.

5.4.2 Prérequis matériels pour Mobile Access

Mobile Access nécessite des lecteurs d'accès avec un module BLE. Les lecteurs Bosch suivants sont compatibles :

ARD-SELECT -BOM, -WOM, -BOKM, -WOKM

– B et W signifient la couleur, noir ou blanc

– O signifie OSDP
– K signifie la présence d'un clavier
– M signifie la compatibilité avec Mobile Access

5.4.3 Configuration prérequis pour Mobile Access

Utilisateur dédié pour une base de données distante (si vous utilisez une base de données distante)

Si Mobile Access doit utiliser une base de données sur un serveur de base de données distant, créez et configurez un utilisateur administrateur nommé `MAUser` sur ce serveur distant, à la fois sous Windows et sur SQL Server. Lors de la configuration décrite ci-dessous, sélectionnez l'option correspondant au serveur de base de données distant et entrez le mot de passe que vous avez défini pour `MAUser`.

IMPORTANT : n'exécutez pas le programme d'installation de Mobile Access avant de terminer cette procédure.

Procédure

1. Sur le serveur de base de données distant, créez un utilisateur Windows de domaine dans le même domaine qu'ACS . Utilisez les paramètres suivants :

– **Nom d'utilisateur** (le nom d'utilisateur lui-même est sensible à la casse) : <ACS-Domain>\`MAUser`
– **Mot de passe** : définissez le mot de passe en fonction des politiques de sécurité qui s'appliquent à tous vos ordinateurs. Notez-le soigneusement, car il sera nécessaire pour l'installation de Mobile Access.
– **L'utilisateur doit changer de mot de passe à la prochaine connexion** : `NO`
– **L'utilisateur ne peut pas changer de mot de passe** : `YES`
– **Le mot de passe n'expire jamais** : `YES`
– **Connexion en tant que service** : `YES`
– **Le compte est désactivé** : `NO`

Ajoutez ensuite `MAUser` comme identifiant de connexion à distance au serveur SQL comme suit :

1. Ouvrez SQL Management Studio
2. Connectez-vous à l'instance SQL distante
3. Accédez à **Sécurité** > **Connexion**
4. Dans le volet **Sélectionner une page**, sélectionnez **Général**
5. Sélectionnez l'utilisateur `MAUser`
6. Dans le volet **Sélectionner une page**, sélectionnez **Rôles de serveur**
7. Cochez les cases `public` et `dbcreator`

Utilisateur dédié pour la base de données locale (si vous utilisez une base de données locale)

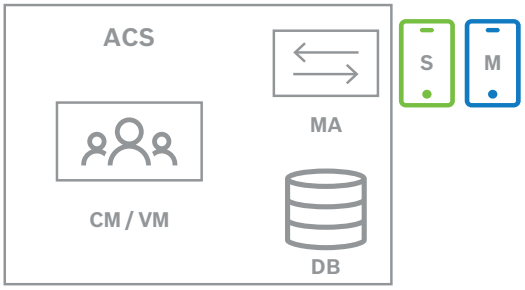
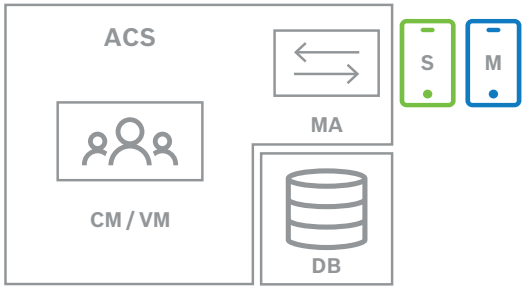
L'utilisateur `MAUser` accède à la base de données d'ACS au nom de l'application Mobile Access.

Il n'est PAS nécessaire de créer cet utilisateur si vous utilisez une base de données locale. Le programme d'installation de Mobile Access un utilisateur Windows `MAUser` automatiquement sur le serveur ACS.

5.4.4 Procédure pour une installation colocalisée

L'installation colocalisée signifie que le service back-end de Mobile Access s'exécute sur le même serveur qu'ACS.

L'installation distribuée signifie que le service back-end de Mobile Access s'exécute sur un serveur différent, par exemple un « serveur cloud ».
Pour l'option distribuée, consultez la section suivante **Procédure pour une installation distribuée**.

Colocalisé avec une base de données locale	Colocalisé avec une base de données distante
	

Clé	Signification
ACS	Principal système de contrôle d'accès : AMS ou BIS-ACE
CM/VM	Back-end pour l'application Web : Credential Management ou Visitor Management
DB	Base de données ACS principale
Collaborateur	Back-end de Mobile Access
S	Application d'installation « Setup Access » pour les appareils mobiles des installateurs et configurateurs système
M	Application d'accès « Mobile Access » pour les appareils mobiles des détenteurs de badge normaux.

Procédure

1. Sur le serveur ACS, qui est aussi le serveur Mobile Access pour les installations colocalisées, exécutez `BoschMobileAccessBackend.exe` en tant qu'administrateur
– Le programme d'installation s'ouvre
2. Dans l'écran **Emplacement**, sélectionnez le type de configuration : **Colocalisé**
3. Sur l'écran **Composants**, vérifiez que `Bosch Mobile Access` est sélectionné, puis cliquez sur **Suivant**
4. Sur l'écran **CLUF**, lisez attentivement et cliquez sur **Accepter** si vous acceptez le contrat de licence utilisateur final (CLUF). L'installation ne peut continuer que si vous le faites.
5. Sur l'écran **Répertoire d'installation** :
– Parcourez et sélectionnez un dossier de destination pour l'installation, ou acceptez la valeur par défaut (recommandé).
– Saisissez le nom de votre entreprise tel qu'il doit être affiché dans l'application mobile et dans les modèles d'e-mail HTML
– Cliquez sur **Next (Suivant)**.
6. Sur l'écran **Certificat**
– Entrez le nom d'hôte sur lequel le service back-end Mobile Access doit s'exécuter

- Si vous le souhaitez, ou si le réseau ne fournit pas de résolution de nom d'hôte, entrez l'adresse IP de cet hôte
- Cliquez sur **Suivant**.

7. Sur l'écran **SQL Server**, sélectionnez l'une des deux alternatives proposées pour l'emplacement de la base de données. Les configurations sont légèrement différentes. Choisissez une alternative pour l'étape suivante :

- ALTERNATIVE 1 **Base de données locale** :
  - Le programme d'installation trouve la base de données locale et la présélectionne.
  - Entrez le mot de passe SQL pour un utilisateur admin (la valeur par défaut est `sa`)
  - Cliquez sur **Tester la connexion**
  - Cliquez sur **Suivant**.
- ALTERNATIVE 2 **Base de données distante**
  - Entrez le nom du serveur SQL qui se trouve sur le réseau
  - Entrez le nom de l'instance SQL
  - Entrez le mot de passe SQL pour un utilisateur admin (la valeur par défaut est `sa`)
  - Cliquez sur **Tester la connexion**
  - Vérifiez le nom d'utilisateur et entrez le mot de passe de l'utilisateur administrateur Windows et SQL que vous avez créé pour l'utilisation de la base de données distante (voir Prérequis ci-dessus)
  - Cliquez sur **Suivant**.

8. Dans l'écran **Configuration du serveur d'identité**

- Le serveur d'identité par défaut (présélectionné) est le serveur ACS principal avec le port `44333` `https://`<NameOfACSserver>`:44333`
- Cliquez sur **Tester la connexion**
- Si le test échoue, vérifiez à nouveau la disponibilité du serveur d'identité.
- Cliquez sur **Next (Suivant)**.

9. Sur l'écran **Composants principaux**, confirmez que **BoschMobile Access** est sélectionné et cliquez sur **Installer**

- L'assistant d'installation se termine.

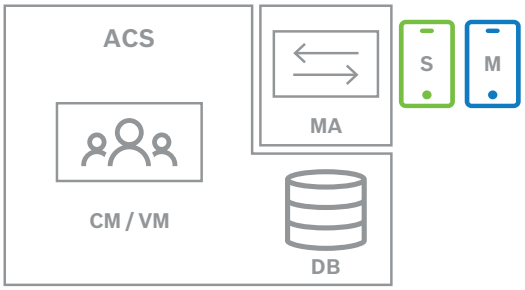
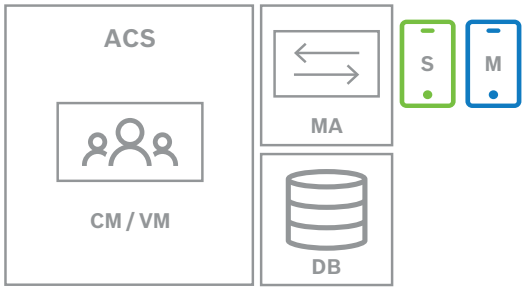
10. Cliquez sur **Suivant**.
11. Sur l'écran **Composants principaux**, vérifiez que l'installation s'est terminée avec succès, puis cliquez sur **Terminer**
12. Dans l'application Windows `Services`, vérifiez que le service `Bosch Mobile Access` est en cours d'exécution.

5.4.5 Procédure pour une installation distribuée

L'installation colocalisée signifie que le service back-end de Mobile Access s'exécute sur le même serveur qu'ACS.

L'installation distribuée signifie que le service back-end de Mobile Access s'exécute sur un serveur différent, par exemple un « serveur cloud ».

Pour l'option colocalisée, consultez la section précédente **Procédure pour une installation colocalisée**.

Distribué avec une base de données locale	Distribué avec une base de données distante
	

Clé	Signification
ACS	Principal système de contrôle d'accès : AMS ou BIS-ACE
CM/VM	Back-end pour l'application Web : Credential Management ou Visitor Management
DB	Base de données ACS principale
Collaborateur	Back-end de Mobile Access
S	Application d'installation « Setup Access » pour les appareils mobiles des installateurs et configurateurs système
M	Application d'accès « Mobile Access » pour les appareils mobiles des détenteurs de badge normaux.

Procédure

1. Sur le serveur de back-end Mobile Access, exécutez `BoschMobileAccessBackend.exe` en tant qu'administrateur
– Le programme d'installation s'ouvre
2. Dans l'écran **Emplacement**, sélectionnez le type de configuration : **Distribué**
3. Sur l'écran **Hôte**, sélectionnez **Mobile Access Back-end** et cliquez sur **Suivant**
– Remarque : L'option **ACS** sera utilisée plus tard dans cette procédure, lorsque nous installerons Mobile Access sur le serveur ACS.
4. Sur l'écran **Composants**, vérifiez que **BoschMobile Access** est sélectionné, puis cliquez sur **Suivant**
5. Sur l'écran **CLUF**, lisez attentivement et cliquez sur **Accepter** si vous acceptez le contrat de licence utilisateur final (CLUF). L'installation ne peut continuer que si vous le faites.
6. Sur l'écran **Répertoire d'installation** :
– Parcourez et sélectionnez un dossier de destination pour l'installation, ou acceptez la valeur par défaut (recommandé).
– Saisissez le nom de votre entreprise tel qu'il doit être affiché dans l'application mobile et dans les modèles d'e-mail HTML
– Cliquez sur **Suivant**.
7. Sur l'écran **SQL Server**, sélectionnez l'une des deux alternatives proposées pour l'emplacement de la base de données. Les configurations sont légèrement différentes. Choisissez une alternative pour l'étape suivante :
– ALTERNATIVE 1 **Base de données locale** :
  – Le programme d'installation trouve la base de données locale et la présélectionne.

  - Entrez le mot de passe SQL pour un utilisateur admin (la valeur par défaut est `sa`)
  - Cliquez sur **Tester la connexion**
  - Cliquez sur **Suivant**.
- ALTERNATIVE 2 **Base de données distante**
  - Entrez le nom du serveur SQL qui se trouve sur le réseau
  - Entrez le nom de l'instance SQL
  - Entrez le mot de passe SQL pour un utilisateur admin (la valeur par défaut est `sa`)
  - Cliquez sur **Tester la connexion**
  - Vérifiez le nom d'utilisateur et entrez le mot de passe de l'utilisateur administrateur Windows et SQL que vous avez créé pour l'utilisation de la base de données distante (voir Prérequis ci-dessus)
  - Cliquez sur **Suivant**.

À ce stade de l'installation distribuée, vous devez passer sur l'ordinateur sur lequel s'exécute le serveur ACS et y configurer Mobile Access *, afin qu'il puisse ensuite communiquer avec le back-end* Mobile Access *sur l'ordinateur local.*
Après avoir suivi les étapes indiquées, le programme d'installation vous guidera vers le serveur local pour confirmer et continuer.

1. Sur l'ordinateur du serveur ACS, exécutez `BoschMobileAccessBackend.exe` en tant qu'administrateur
- Le programme d'installation s'ouvre
2. Dans l'écran **Emplacement**, sélectionnez le type de configuration : **Distribué**
3. Sur l'écran **Hôte**, sélectionnez **ACS** et cliquez sur **Suivant**
4. Sur l'écran **Assistant d'accompagnement**, lisez le texte explicatif et cliquez sur **Suivant**
5. Sur l'écran **Certificat**
- Entrez le nom d'hôte sur lequel le service back-end Mobile Access doit s'exécuter
- Si vous le souhaitez, ou si le réseau ne fournit pas de résolution de nom d'hôte, entrez l'adresse IP de cet hôte
- Cliquez sur **Suivant**.
6. Dans l'écran **Configuration du serveur d'identité**
- Le serveur d'identité par défaut (présélectionné) est le serveur ACS principal avec le port `44333` `https://`<NameOfACSserver>`:44333`
- Cliquez sur **Tester la connexion**
- Si le test échoue, vérifiez à nouveau la disponibilité du serveur d'identité.
- Cliquez sur **Next (Suivant)**.
7. Sur l'écran **Créer un fichier**
   , nous créons un fichier de configuration dans un fichier ZIP protégé par mot de passe, et nous le rendons disponible pour le service back-end de Mobile Access.
- **Mot de passe utilisateur** : saisissez un mot de passe pour le fichier ZIP
- **Fichier de configuration** : saisissez ou recherchez un dossier dans lequel placer le fichier ZIP. Notez que ce dossier doit être accessible à l'ordinateur sur lequel s'exécute le service back-end de Mobile Access. Si ce n'est pas le cas, vous devez transférer le fichier ZIP sur cet ordinateur par d'autres moyens.
- Cliquez sur **Créer un fichier de configuration**
- Cliquez sur **Suivant**.
8. Sur l'écran **Changer de machine**
   Les étapes d'installation sur le serveur ACS sont maintenant terminées.
- Cliquez sur **Confirmer** pour terminer la procédure

À ce stade de l'installation distribuée, vous revenez au programme de configuration sur l'ordinateur back-end de Mobile Access.

1. Revenez au programme de configuration `BoschMobileAccessBackend.exe` sur l'ordinateur serveur de Bosch Mobile Access.
2. Sur la page **Changer de machine**
– cochez la case intitulée **J'ai déjà effectué les étapes requises sur la machine ACS**
– Cliquez sur **Suivant**.
3. Sur l'écran **Télécharger un fichier**
– **Télécharger le fichier de configuration :** sélectionnez le fichier de configuration que vous avez créé sur le serveur ACS
– **Vérification du mot de passe :** entrez le mot de passe que vous avez défini pour le fichier ZIP sur le serveur ACS
– Lorsque vous avez saisi le mot de passe correct, vous pouvez cliquer sur **Suivant** pour lire le fichier de configuration
4. Sur l'écran **Composants principaux**, confirmez que **BoschMobile Access** est sélectionné et cliquez sur **Installer**
– L'assistant d'installation se termine.
5. Cliquez sur **Suivant**.
6. Sur l'écran **Composants principaux**, vérifiez que l'installation s'est terminée avec succès, puis cliquez sur **Terminer**
7. Dans l'application Windows `Services`, vérifiez que le service `Bosch Mobile Access` est en cours d'exécution.

5.5 Installation d'applications Mobile Access

Introduction

Bosch fournit les applications suivantes pour Mobile Access

– Bosch Mobile Access : application de gestion des détenteurs de carte qui stocke les informations d'identification virtuelles et les transmet via Bluetooth aux lecteurs configurés pour Mobile Access. Un tel lecteur accorde ou refuse ensuite l'accès si l'une des informations d'identification stockées dans l'application est valide.
– Bosch Setup Access : application d'installation pour scanner et configurer les lecteurs via Bluetooth.

Les opérateurs autorisés pour Visitor Management et Credential Management peuvent envoyer des informations d'identification virtuelles pour les applications du titulaire de carte et de l'installateur.

Tant que l'application du titulaire de carte est en cours d'exécution et que Bluetooth est activé sur l'appareil mobile, vous pouvez l'utiliser comme s'il s'agissait d'une carte physique. Il n'est pas nécessaire de fournir des commandes depuis l'application ou même de déverrouiller l'écran.

Remarque!

IMPORTANT : N'utilisez pas simultanément les applications du titulaire de carte et de l'installateur

Assurez-vous que personne n'utilise l'application de l'installateur lorsque l'application du titulaire de carte est utilisée, et inversement.

Procédure

Les applications Mobile Access Bosch peuvent être téléchargées à partir des magasins d'applications Google et Apple et installées de la manière habituelle. Leurs noms dans les magasins d'applications sont les suivants :

– Bosch Mobile Access
– Bosch Setup Access

5.6 Certificats pour une communication sécurisée

Pour une communication sécurisée entre le navigateur sur l'ordinateur client et le serveur ACS, copiez le certificat suivant du serveur ACS sur les ordinateurs clients. Pour l'installer, utilisez un compte disposant des droits d'administrateur Windows.

Le chemin habituel vers le certificat est le suivant :

– <lecteur d'installation>:
  `\Bosch Sicherheitssysteme\Access Management System\Certificates\Bosch Security System Internal CA - BISAMS.cer`

Vue d'ensemble des transferts de certificats

Vers → **De ↓**	**ACS**	Back-end **MA** Mobile Access	**DB** Base de données	**S** Application de configuration	**M** Application d'accès Titulaire de carte	**R** Lecteur
ACS	/	Transféré par l'assistant de configuration (au moyen de l'outil de cert)	/	/	/	/
Back-end **MA** Mobile Access	Transféré par l'assistant de configuration MA	/	/	Transféré par inscription par code QR Mise à jour via notification push	Transféré par inscription par code QR Mise à jour via notification push	/
BD Base de données	/	/	/	/	/	/

S Application de configuration	/	Transféré par inscription par code QR	/	/	/	/
M Application d'accès Titulaire de carte	/	Transféré par inscription par code QR	/	/	/	/

5.6.1 Certificats pour le navigateur Firefox

Vous pouvez ignorer cette section si vous n'utilisez pas le navigateur Firefox.

Le navigateur Firefox gère les certificats racine différemment : Firefox ne consulte pas le magasin de certificats Windows pour les certificats racine approuvés. Au lieu de cela, chaque profil de navigateur gère son propre magasin de certificats racine. Pour plus de détails, reportez-vous à l'adresse suivante : https://support.mozilla.org/en-US/kb/setting-certificate-authorities-firefox
Cette page Web contient également des instructions pour forcer Firefox à utiliser le magasin de certificats Windows pour tous les utilisateurs.
Vous pouvez aussi importer les certificats par défaut comme décrit ci-dessous. Remarque :

- Vous devez importer les certificats pour chaque utilisateur et profil Firefox.
- Le certificat du serveur décrit ci-dessous est le certificat par défaut créé par l'installation. Si vous avez acheté votre propre certificat auprès d'une autorité de certification, vous pouvez l'utiliser à la place.

Importation de certificats dans le magasin de certificats Firefox
Pour accéder au serveur ACS depuis Firefox sur l'ordinateur client, vous pouvez importer le certificat par défaut suivant depuis le serveur :

- <lecteur d'installation>:
  `\Bosch Sicherheitssysteme\Access Management System\Certificates\Bosch Security System Internal CA - BISAMS.cer`

Ou, pour BIS ACE, vous pouvez également télécharger le certificat via le Web :

- `HTTP://`<Nom d'hôte>`/`<Nom d'hôte>`.cer`

Périphériques : pour accéder à un périphérique connecté, tel qu'un scanner de documents ou de signatures, à partir de Firefox sur l'ordinateur client, vous pouvez utiliser le certificat par défaut. Il se trouve sur l'ordinateur client à l'emplacement suivant :
<lecteur d'installation>`:\Program Files (x86)\Bosch Sicherheitssysteme\Bosch Peripheral Device Addon\BoschAcePeripheralDeviceAddonHardware CA.cer`

Procédure (à répéter pour chaque certificat et profil Firefox) :
Utilisez la procédure suivante sur l'ordinateur client pour installer les certificats dont vous avez besoin :

1. Recherchez le certificat que vous souhaitez installer.
2. Ouvrez le navigateur Firefox et tapez `about:preferences` dans la barre d'adresse.

- Une page d'options s'ouvre.

3. Dans le champ **Rechercher dans Options**, tapez `certificate`
– Le bouton **Afficher les certificats** apparaît sur la page.
4. Cliquez sur le bouton **Afficher les certificats**.
– La boîte de dialogue **Gestionnaire de certificats** s'ouvre avec plusieurs onglets
5. Sélectionnez l'onglet **Autorités**.
6. Cliquez sur **Importer**...
– Une boîte de dialogue de sélection de certificat s'ouvre.
7. Sélectionnez le certificat recherché à l'étape 1, puis cliquez sur **Ouvrir**.
– La boîte de dialogue **Téléchargement du certificat** s'ouvre.
8. Sélectionnez **Faire confiance à cette autorité de certification pour identifier les sites Web**, puis cliquez sur **OK**.
– La boîte de dialogue **Téléchargement du certificat** se ferme.
9. Dans la boîte de dialogue **Gestionnaire de certificats**, cliquez sur **OK**.
– La procédure d'importation du certificat est terminée.

5.6.2 Certificats pour le navigateur Chrome

Vous pouvez ignorer cette section si vous n'utilisez pas le navigateur Chrome.
Veuillez consulter les notes de mise à jour de votre serveur ACS pour connaître les modifications apportées à la gestion des certificats dans le navigateur Chrome.
Pour installer un certificat sur le navigateur Chrome sous Microsoft Windows :

1. Téléchargez le fichier de certificat.
2. Accédez à la page des paramètres de Chrome (`chrome://settings`) et cliquez sur **Avancé**.
3. Sous **Confidentialité et sécurité**, cliquez sur **Gérer les certificats**
4. Dans l'onglet **Vos certificats**, cliquez sur **Importer** pour lancer le processus d'installation du certificat :
– Un assistant d'importation de certificat apparaît.
5. Sélectionnez le fichier de certificat et terminez l'assistant.
6. Le certificat installé sera affiché sous l'onglet **Autorités de certification racines de confiance**.

5.7 Réparer les installations de Mobile Access

Introduction

Pour mettre à jour les fichiers binaires ou recréer le certificat Mobile Access, vous pouvez exécuter le programme d'installation de la version actuelle ou ultérieure de Mobile Access, sur une installation existante :

Procédure

1. Sur le serveur back-end de Mobile Access, exécutez la nouvelle version de `BoschMobileAccessBackend.exe` en tant qu'administrateur.
– Notez que pour les installations colocalisées, le serveur back-end Mobile Access est le même que le serveur d'ACS.
2. Suivez l'assistant d'installation en définissant les mêmes paramètres que lors de l'installation initiale.
– Pour recréer le certificat, sur l'écran **Certificats**, sélectionnez le bouton radio **Recréer un certificate.**

3. Une fois le programme d'installation terminé, démarrez une nouvelle session de connexion sur chaque application Web utilisant Mobile Access (CredMgmt ou VisMgmt ou les deux).

– L'application Web utilisera les nouveaux fichiers binaires.
– Si vous avez sélectionné **Recréer un certificat**, toutes les invitations futures que vous enverrez aux utilisateurs et installateurs de Mobile Access seront basées sur le nouveau certificat Mobile Access.

5.8 Désinstallation du logiciel

Pour désinstaller le logiciel du serveur ou du client :

1. Avec les droits d'administrateur Windows, démarrez le programme Windows **Ajouter ou supprimer des programmes**.
2. Sélectionnez le programme (serveur ou client) et cliquez sur **Désinstaller**.
3. (Pour Visitor Management uniquement) Indiquez si vous souhaitez supprimer la base de données de gestion des visiteurs ainsi que le programme.

– **Remarque** : la base de données contient les enregistrements de toutes les visites enregistrées durant l'utilisation du programme. Vous pouvez archiver la base de données ou la transférer vers un autre installation.

4. Indiquez si vous souhaitez supprimer les fichiers journaux.
5. Terminez la désinstallation de la manière habituelle.
6. (Recommandé) Redémarrez l'ordinateur pour assurer la modification complète du registre Windows.

6 Configuration

6.1 Création d'utilisateurs Credential Management dans ACS

Dans ACS (ACE ou AMS), chaque utilisateur de CredMgmt doit être un titulaire de carte avec une définition d'opérateur distincte.

Ces définitions d'opérateurs contiennent des droits CredMgmt spéciaux sous forme de **profils d'utilisateur**. Consultez l'aide en ligne de votre ACS pour obtenir des informations détaillées et des instructions concernant les **profils d'utilisateur**.
Vous devez définir un opérateur distinct pour chaque titulaire de carte utilisant CredMgmt. Vous ne pouvez pas affecter plusieurs titulaires de carte au même opérateur.

6.2 Connexion pour les tâches de configuration

Pour les tâches de configuration et d'administration, utilisez un ordinateur physiquement protégé contre tout accès non autorisé.

1. Dans votre navigateur, entrez l'adresse HTTPS du serveur CredMgmt, suivi du signe deux-points et du numéro de port (par défaut `5806`)
   `https://`<My_CredMgmt_server>`:5806`
   L'écran **Connexion** apparaît.
2. Connectez-vous à CredMgmt en tant qu'utilisateur **Administrateur**.
3. Cliquez sur  pour ouvrir le menu **Paramètres**.

6.3 Configuration à l'aide du menu Paramètres

Général	– **Période de conservation (jours)** : ce paramètre régit le traitement des enregistrements de personne. – Une fois cette période écoulée pour la première fois, l'application rend l'enregistrement anonyme. – Une fois la période écoulée pour la deuxième fois, l'application supprime l'enregistrement. La valeur par défaut est `365`. Attribuez la valeur 0 pour désactiver complètement la période de rétention. Dans ce cas, les enregistrements de visite sont conservés indéfiniment. – **Logo** : sélectionnez ou désélectionnez la case qui détermine si les boîtes de dialogue affichent un logo personnalisé ou le logo par défaut. – Pour les critères des fichiers de logo personnalisés, voir : *Personnaliser le logo de l'entreprise, page 30* – **Supergraphique :** sélectionnez ou désélectionnez la case qui détermine si les boîtes de dialogue affichent le supergraphique Bosch. – Cliquez sur **Aperçu** pour afficher la page de la boîte de dialogue telle qu'elle apparaîtrait avec ces paramètres. Pour plus de détails sur le mode Aperçu, reportez-vous à la section suivante.

	– **Langues** : Sélectionnez les langues qui doivent être disponibles dans l'interface utilisateur, ainsi que leurs préférences de formats en matière de **date** et d'**heure**. – **Serveur de messagerie** Entrez l'adresse IP, le numéro de port et les détails du compte de votre serveur de messagerie afin de permettre l'envoi d'e-mails depuis l'application. – **Modèles d'e-mails** Plusieurs modèles d'e-mails HTML, que vous personnalisez généralement selon vos propres besoins, sont proposés. Pour plus de détails, reportez-vous à la section **Modèles d'e-mails** ci-dessous. – **Mobile Access** Sélectionnez la case **Mobile Access** pour activer Mobile Access. **Connexion** : saisissez l'adresse du serveur Mobile Access (adresse du service d'enregistrement). `https://`<MyMobileAccessBackendServer>`:5700` Utilisez un (FQDN) pour <MyMobileAccessBackendServer> dans des environnements multi-domaines. **Remarque :** Pour utiliser une adresse IP au lieu d'un FQDN, vous devez saisir cette adresse IP, sous **Création de certificat**, lorsque vous exécutez l'assistant de configuration pour le service back-end de Mobile Access. **Intégration de l'installateur :** sélectionnez les informations dont vous avez besoin des installateurs, afin qu'ils puissent configurer les lecteurs d'accès mobiles à l'aide de la Bosch Setup Access. Déconnectez-vous de l'application Web et reconnectez-vous afin d'utiliser immédiatement la fonctionnalité de Mobile Access.

6.3.1 Modèles d'e-mails

Plusieurs modèles d'e-mails HTML, que vous personnalisez généralement selon les besoins de votre entreprise, sont proposés. Pour chaque modèle, vous pouvez stocker les adresses e-mail des champs Cc et Cci, et celle d'un destinataire de test, à qui vous pouvez envoyer un e-mail de test immédiatement.
Une fois téléchargés depuis le menu **Paramètres**, les modèles sont stockés dans le dossier de téléchargement par défaut de votre navigateur.

- `MobileAccess.html` Invitation destinée aux titulaires de carte leur demandant d'utiliser des informations d'identification de smartphone.
- `SetupAccess.html` Invitation destinée aux installateurs leur demandant de configurer les lecteurs pour Mobile Access.

Espaces réservés à utiliser dans les modèles d'e-mails

Les modèles d'e-mails proposent plusieurs espaces réservés permettant d'inclure des champs de base de données dans le texte. Ces espaces réservés sont décrits dans les tableaux suivants, en fonction des modèles dans lesquels ils peuvent être utilisés.

Mobile Access

E-mail envoyé à un titulaire de carte (pour l'application Mobile Access) lorsque l'accès mobile lui est accordé

Espace réservé	Description
{{Title}}	titre de la personne (M. Mme Dr. etc.)
{{FirstName}}	prénom de la personne
{{LastName}}	nom de famille de la personne
{{CompanyName}}	entreprise de la personne
{{QrcodeLink}}	Code QR correspondant au lien qui offre au titulaire de la carte un accès mobile via l'application
{{InviteLink}}	lien qui offre au titulaire de la carte un accès mobile via l'application

Setup Access

E-mail envoyé à un installateur Mobile Access (pour l'application Setup Access) lorsque l'accès mobile lui est accordé pour la configuration des lecteurs.

Espace réservé	Description
{{Title}}	titre de l'installateur (M. Mme Dr. etc.)
{{FirstName}}	prénom de l'installateur
{{LastName}}	nom de l'installateur
{{CompanyName}}	entreprise de l'installateur
{{QrcodeLink}}	QR Code correspondant au lien qui offre à l'installateur un accès mobile pour la configuration des lecteurs via l'application Setup Access
{{InviteLink}}	lien qui offre à l'installateur un accès mobile pour la configuration des lecteurs via l'application Setup Access

6.3.2 Mode aperçu

Certains ensembles d'options comportent un bouton **Aperçu** qui active le mode de prévisualisation afin de vous permettre de voir les boîtes de dialogue telles qu'elles apparaîtront avec les options définies.

En mode aperçu, les conditions suivantes s'appliquent :

– Une bannière s'affiche en haut du tableau de bord.

– Les modifications apportées au tableau de bord ou aux menus ne sont **pas** enregistrées.
– Cliquez sur **Fermer le mode aperçu** dans la bannière pour fermer ce mode
– Utilisez la liste **Changer de rôle** figurant dans la bannière pour prévisualiser l'apparence de l'interface pour les différents types d'utilisateurs.

6.3.3 Modèles de documents

Pour les différents documents et e-mails, vous pouvez télécharger des modèles et charger des versions personnalisées de ces modèles dans la boîte de dialogue **Tableau de bord** > **Paramètres > Général**.

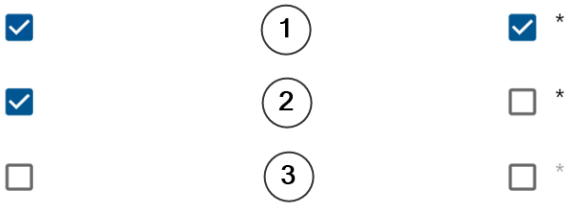
6.4 Personnalisation de l'interface utilisateur

Personnalisez l'interface utilisateur dans les boîtes de dialogue Tableau de bord > **Paramètres**.

6.4.1 Configuration des options qui seront visibles, invisibles et obligatoires

Sélectionnez les champs de données qui seront visibles dans les boîtes de dialogue, ainsi que les données qui seront obligatoires.

Exemple :



- (1) est visible et obligatoire,
- (2) est visible mais pas obligatoire
- (3) n'est pas visible.

6.4.2 Personnalisation des textes de l'interface utilisateur pour la localisation

Vous pouvez facilement personnaliser les textes de l'interface utilisateur selon la langue. Par défaut, les **textes localisables** contiennent les en-têtes standard pour les blocs de champs de données dans les boîtes de dialogue de collecte de données.

Pour personnaliser ces en-têtes en fonction des exigences locales :

1. Sélectionnez une langue d'interface utilisateur dans la liste.
2. Remplacez les textes dans la zone de texte.
   Vous pouvez utiliser des balises HTML pour un formatage simple, par exemple :
   ```
   <b>this text will appear bold </b>
   <i>italics</i>
   <u>underline</u>
   ```

6.4.3 Personnaliser le logo de l'entreprise

Les fichiers graphiques que vous téléchargez pour le logo de votre entreprise doivent répondre aux critères suivants :

Formats pris en charge	PNG, JPEG, JPG
Largeur exacte (pixels)	125
Hauteur exacte (pixels)	63

Taille max. (Mo)	1

6.5 Paramètres du pare-feu

Ajoutez des applications auxiliaires à la configuration du pare-feu des ordinateurs serveur et clients :

1. Démarrez le pare-feu Windows. Cliquez sur Démarrer > **Panneau de configuration** > **Pare-feu Windows**
2. Sélectionnez **Paramètres avancés**
3. Sélectionnez **Règles entrantes**
4. Dans le volet **Actions**, sélectionnez **Nouvelle règle...**
5. Dans la boîte de dialogue **Type de règle**, sélectionnez **Port** puis cliquez sur **Suivant >**
6. Sur la page suivante, sélectionnez **TCP et ports locaux spécifiques**
7. Autorisez la communication via les ports suivants :

– Sur le ou les ordinateurs serveurs

<nom du serveur>:`44333` - utilisé par le serveur AMS Identity **(*)**

<nom du serveur>:`5706` - utilisé par le serveur VisMgmt

<nom du serveur>:`5806` - utilisé par le serveur CredMgmt

<nom du serveur>:`5700` - utilisé par le serveur de back-end Mobile Access

– Sur les ordinateurs clients

`localhost:5707` - utilisé par le module complémentaire Bosch Peripheral Devices

(*) Nous utilisons les serveurs d'identité AMS et BIS comme décrit dans leurs manuels d'installation respectifs.

Utilisation des ports dans le système

Serveur sortant	Port de sortie	Serveur entrant	Port d'entrée	Protocole	Commentaires
VisMgmt ou CredMgmt	*	Back-end de Mobile Access	5700	HTTPS	Commandes de l'application Web pour créer et/ou supprimer des informations d'dentification mobiles
Appareils mobiles depuis Internet	*	Back-end de Mobile Access	5700	HTTPS	Les appareils mobiles reçoivent des informations d'identification mobiles via Internet
Back-end de Mobile Access	*	Google Firebase (Internet)	*	HTTPS	Les appareils mobiles reçoivent des notifications push ; veuillez consulter la documentation de Google Firebase sur les paramètres des pare-feux https://firebase.google.com/docs/cloud-messaging/concept-options

Serveur sortant	Port de sortie	Serveur entrant	Port d'entrée	Protocole	Commentaires
Ordinateur client de l'utilisateur VisMgmt	*	Back-end de VisMgmt	5706	HTTPS	Commandes de l'ordinateur client VisMgmt vers le back-end de VisMgmt
Ordinateur client de l'utilisateur CredMgmt	*	Back-end de CredMgmt	5806	HTTPS	Commandes de l'ordinateur client CredMgmt vers le back-end de CredMgmt
Ordinateur administrateur	*	Back-end de Mobile Access	3389	Remote Desktop (RDP)	Pour des raisons de sécurité, vous ne devez autoriser l'accès administrateur à l'ordinateur back-end de Mobile Access que temporairement.

Remarque!
Notez que Mobile Access et ACS n'ont pas de connexion directe, ni entrante ni sortante.

6.5.1 Programmes et services en tant qu'exceptions de pare-feu

Vous pouvez également configurer le pare-feu en ajoutant des programmes et des services en tant qu'exceptions

1. Démarrez l'interface utilisateur du pare-feu Windows, sélectionnez **Démarrer > Paramètres > Panneau de configuration > Pare-feu Windows**.
2. Sélectionnez l'onglet **Autoriser une application ou une fonctionnalité via le pare-feu Windows**.
3. Sélectionnez **Autoriser une autre application** (si grisé, activez le bouton en sélectionnant **Modifier les paramètres**).
4. Vous pouvez ajouter les programmes suivants :

Programmes

Le chemin d'installation par défaut est `C:\Program Files (x86)\Bosch Sicherheitssysteme\`

Programme	Emplacement du fichier
acsp.exe	[Chemin-installation]\AccessEngine**AC**\BIN
ACTA-3.exe	[Chemin-installation]\AccessEngine**AC**\BIN
BioVerify.exe	[Chemin-installation]\AccessEngine**AC**\BIN
BioIdentify.exe	[Chemin-installation]\AccessEngine**AC**\BIN
Bosch.Ace.CredentialManagement.exe	[Chemin-installation]\Bosch Credential Management

Programme	Emplacement du fichier
Bosch.Access.MobileAccessBackend.exe	[Chemin-installation]\Bosch Mobile Access
Bosch.Ace.VisitorManagement.exe	[Chemin-installation]\Bosch Visitor Management
CalTa-3.exe	[Chemin-installation]\AccessEngine**AC**\BIN
CDTA-1.exe	[Chemin-installation]\AccessEngine**AC**\BIN
EMDP.exe	[Chemin-installation]\AccessEngine**AC**\BIN
KCKemas.exe	[Chemin-installation]\AccessEngine**AC**\BIN
KCS.exe	[Chemin-installation]\AccessEngine**AC**\BIN
Loggifier-2.exe	[Chemin-installation]\AccessEngine**AC**\BIN
PictureServer.exe	[Chemin-installation]\AccessEngine**AC**\BIN
ReplServer.exe	[Chemin-installation]\AccessEngine**AC**\BIN
reps.exe	[Chemin-installation]\AccessEngine**AC**\BIN
TAccExc.exe	[Chemin-installation]\AccessEngine**AC**\BIN
EMAILSP.exe	[Chemin-installation]\AccessEngine**AC**\BIN
master-3.exe	[Chemin-installation]\AccessEngine**AC**\BIN
querySrv-2.exe	[Chemin-installation]\AccessEngine**AC**\BIN
webSrv-1.exe	[Chemin-installation]\AccessEngine**AC**\BIN
LicenseGateway.exe	[Chemin-installation]\AccessEngine**AC**\BIN\net6.0
DMS.exe	[chemin-installation]\AccessEngine**MAC**\BIN
lac.exe	[chemin-installation]\AccessEngine**MAC**\BIN

Services

Le chemin d'installation par défaut est `C:\Program Files (x86)\Bosch Sicherheitssysteme\Access Management System`

Service	Emplacement du fichier
Bosch.States.Api	[chemin-d'installation]\States API
Bosch.Map.Api	[chemin-d'installation]\Map API
Bosch.MapView.Api	[chemin-d'installation]\API Map View
Bosch.Events.Api	[chemin-d'installation]\API Events
Bosch.Alarms.Api	[chemin-d'installation]\API Alarms
Bosch.Ace.IdentityServer	[chemin-d'installation]\Identity Server
Bosch.Ace.Api	[chemin-d'installation]\Access API
Bosch.DialogManager.Api	[chemin-d'installation]\API Dialog Manager

Service	Emplacement du fichier
Bosch.Intrusion.Api	[chemin-d'installation]\Intrusion API
Bosch Ace Visitor Management	[VM-chemin-installation]\
Client Bosch Ace Visitor Management	[Chemin-installation-client-VM]\
Bosch.OSS-SO	[chemin-d'installation]\OSS-SO
Bosch.OSS-SO.Configurator	[chemin-d'installation]\OSS-SO.Configurator
Bosch.Access.ProductApi.Api	[chemin-d'installation]\ProductApi

6.6 Sécurité informatique

La sécurité d'un système de contrôle d'accès d'une organisation est un élément essentiel de son infrastructure. Bosch conseille de respecter scrupuleusement les directives de sécurité informatique prescrites pour le pays d'installation.
L'organisation qui exploite le système de contrôle d'accès est responsable des éléments suivants :

6.6.1 Responsabilités matérielles

- La prévention des accès physiques non autorisés aux composants réseau, tels que les connexions RJ45.
  - Les attaquants ont besoin d'un accès physique pour mener des attaques de type « man in the middle » ou attaque de l'intercepteur.
- La prévention des accès physiques non autorisés au matériel du contrôleur AMC2.
- L'utilisation d'un réseau dédié pour le contrôle d'accès.
  - Les attaquants peuvent accéder via d'autres appareils au sein du même réseau.
- L'utilisation d'informations d'identification sécurisées telles que **DESFire** avec un code Bosch et une authentification multifacteur avec biométrie.
- L'enrôlement rapide, via l'application **Setup Access**, des lecteurs d'accès mobiles avec des modules BLE (Bluetooth Low Energy). Les lecteurs sous tension non enrôlé sont vulnérables au piratage par des tiers. Pour remédier à un tel piratage, consultez le manuel d'installation du lecteur pour obtenir des instructions sur la façon de réinitialiser les paramètres d'usine par défaut.
- La fourniture d'un mécanisme de basculement et d'une alimentation de secours pour le système de contrôle d'accès.
- Le suivi et la désactivation des identifiants prétendument perdus ou égarés.
- La mise hors service appropriée du matériel qui n'est plus utilisé, en particulier sa réinitialisation aux paramètres d'usine, et la suppression des données personnelles et des informations de sécurité.

6.6.2 Responsabilités logicielles

- La maintenance, la mise à jour et le fonctionnement corrects du pare-feu du réseau de contrôle d'accès.
- La surveillance des alarmes qui indiquent quand les composants matériels, tels que les lecteurs de cartes ou les contrôleurs AMC2, se déconnectent.
  - Ces alarmes peuvent indiquer une tentative d'échange de composants matériels.
- La surveillance des alarmes de détection de sabotage déclenchées par des contacts électriques dans le matériel de contrôle d'accès, par exemple, les contrôleurs, les lecteurs et les armoires.

- La limitation des diffusions UDP au sein du réseau dédié.
- Les mises à jour, en particulier les mises à jour de sécurité et les correctifs, du logiciel de contrôle d'accès.
- Les mises à jour, en particulier les mises à jour de sécurité et les correctifs, du firmware du matériel.
  - Notez que même le matériel récemment fourni peut nécessiter une mise à jour du firmware. Consultez le manuel du matériel pour obtenir des instructions.
  - Bosch décline toute responsabilité pour les dommages causés par des produits mis en service avec un firmware obsolète.
- L'utilisation de la communication par canal sécurisé OSDPv2.
- L'utilisation de mots de passe forts.
- L'application du *principe du moindre privilège* pour s'assurer que les utilisateurs individuels n'ont accès qu'aux ressources dont ils ont besoin pour leur objectif légitime.

6.6.3 Gestion sécurisée des informations d'identification mobiles

- Ne laissez pas les lecteurs Mobile-Access non configurés sans surveillance.
  - Un attaquant pourrait détourner le lecteur pour un autre ACS. Cela nécessiterait une coûteuse réinitialisation du système.
- Si un appareil mobile contenant des informations d'identification mobiles est perdu ou volé, traitez cet appareil comme une carte perdue : bloquez ou supprimez toutes ses informations d'identification mobiles dès que possible.
- Pour les environnements à haute sécurité, Bosch recommande une authentification à deux facteurs. Cela nécessite que le détenteur de carte déverrouille l'appareil mobile avant de l'utiliser comme information d'identification.
- Les informations d'identification mobiles ne sont pas restaurées lorsqu'un téléphone est restauré à partir d'une sauvegarde. Si un détenteur d'informations d'identification mobiles reçoit un nouvel appareil mobile, vous devez renvoyer toutes les invitations en cours.
- Un attaquant pourrait utiliser un brouilleur de communication pour bloquer la communication avec les lecteurs d'accès mobile. Les employés dont l'accès aux zones est essentiel doivent conserver des badges physiques comme solution de secours.
  - Comme solution de secours pour Mobile Access, utilisez uniquement des cartes physiques avec un codage sécurisé (tel que le code Bosch).
- Protégez le serveur Mobile Access contre tout accès physique non autorisé. Bosch recommande des mesures supplémentaires telles que, par exemple, le chiffrement de disque BitLocker.
- Protégez le serveur Mobile Access contre les attaques par déni de service (DoS). Il doit faire partie d'un environnement réseau sécurisé qui offre des protections telles qu'un limiteur de débit.
- Traitez les codes QR d'invitation de l'installateur comme des informations d'identification d'administrateur. Un téléphone d'installation volé, avec des informations d'identification d'installation actives, pourrait permettre à un attaquant de reconfigurer les lecteurs Mobile Access de manière malveillante.
  - Envoyez des invitations aux installateurs juste au moment de la configuration du lecteur et assurez-vous qu'ils suppriment ces informations d'identification dès que la configuration est terminée.
  - Utilisez la fonction « Scanner les codes QR depuis l'écran » de préférence aux invitations par e-mail. Assurez-vous que le programme d'installation prévu charge immédiatement les informations d'identification.

6.7 Confidentialité et protection des données chez Bosch

Introduction

Dans tous les processus métier et conformément aux exigences réglementaires applicables, nous veillons à ce que la confidentialité soit préservée, que les données personnelles soient protégées et que les informations commerciales soient sécurisées. Sur le plan technique et organisationnel, et notamment en matière de protection contre les accès non autorisés et les pertes, nous appliquons une norme appropriée qui reflète les pratiques correspondant à l'état de la technologie et qui tient compte des risques associés. Lors du développement de produits Bosch et de nouveaux modèles commerciaux, nous veillons à ce que les exigences règlementaires en matière de protection des données et de sécurité des informations soient prises en compte à un stade précoce.

Outre l'organisation de conformité et le service juridique, le principal interlocuteur pour les questions relatives à la bonne gestion des données est le responsable de la sécurité des données.

Traitement des données personnelles dans l'application Mobile Access et dans le service back-end de Mobile Access

- Catégories de données personnelles
  - Les applications Mobile Access contiennent des données personnelles. Il s'agit des informations de numéro de carte utilisées pour accéder aux lecteurs. L'accès aux données réelles de personnes réelles n'est possible que par l'utilisation supplémentaire des programmes AMS, ACE ou Visitor Management.
  - La procédure d'enregistrement de l'installateur dans le menu **Paramètres** ne nécessite pas le stockage des données personnelles. Néanmoins, certaines informations utilisateur, telles que les adresses e-mail, peuvent être stockées de manière facultative.
  - Le serveur de back-end de l'application Mobile Access stocke les données relatives aux personnes pour la gestion des informations d'identification.
- Transfert de données
  - Les informations d'identification sont transférées entre le service back-end, l'application Mobile Access et le système Visitor Management pour contrôler l'accès aux lecteurs.
- Enregistrement des données
  - L'application Mobile Access conserve des journaux techniques. Ces journaux sont stockés en local sur l'appareil mobile et peuvent être envoyés à des tiers, tels que le support technique, si nécessaire.
  - Le serveur de back-end conserve également des journaux techniques. Les données sont stockées en local sur le système serveur.
  - Par défaut, le serveur de back-end ne supprime pas automatiquement les fichiers journaux. Néanmoins, la suppression automatique peut être configurée en fonction de la capacité de stockage restante ou selon un calendrier.

Qu'avons-nous fait pour rendre la protection des données de produit conviviale ?

Les systèmes de contrôle d'accès Bosch gèrent les droits d'accès des personnes. Afin de protéger ces personnes, Bosch prend des mesures qui intègrent les exigences du RGPD directement dans le développement des produits, en suivant une approche « confidentialité intrinsèque ».

- Un chiffrement de pointe est utilisé.
- Les informations d'identification sont rendues anonymes.

- L'utilisateur de l'application n'est pas tenu de saisir des informations personnelles afin de recevoir des informations d'identification virtuelles via Code QR ou par e-mail.
- La suppression des informations d'identification est possible depuis les applications Mobile Access, depuis les systèmes de contrôle d'accès principaux et les applications auxiliaires telles que Visitor Management et Credential Management.
- Les informations d'identification peuvent être bloquées à tout moment par les opérateurs des systèmes de contrôle d'accès principaux et des applications auxiliaires.
- Les données de télémétrie sont rendues anonymes dès la conception.
- Les fichiers journaux ne sont pas transférés des appareils mobiles vers d'autres parties, telles que le support technique, sans le consentement et la coopération actifs de l'utilisateur.
- Il est possible de configurer la suppression automatique et planifiée des fichiers journaux sur le système de contrôle d'accès principal.
- Bosch n'exige aucune inscription dans l'App Store ou l'application. L'App Store ne transmet aucune donnée personnelle à Bosch.
- L'application a besoin du Bluetooth pour fonctionner, et elle demande à l'utilisateur d'activer obligatoirement le Bluetooth manuellement.

Questions supplémentaires

Pour plus d'informations sur la confidentialité des données, consultez l'avis de confidentialité des données dans l'application Mobile Access ou contactez votre équipe de projet Bosch.

7 Fonctionnement

7.1 Aperçu des rôles d'utilisateur

Les capacités des utilisateurs de Credential Management sont déterminées par leurs profils utilisateur dans ACS. Pour plus de détails, consultez la section *Création d'utilisateurs Credential Management dans ACS, page 27* ci-dessous. Il existe deux types d'utilisateurs de base :

Type d'utilisateur	Cas d'utilisation
Opérateur	Attribuer et annuler l'attribution de cartes d'accès physiques et d'informations d'dentification virtuelles pour l'accès mobile
Administrateur	Définition des paramètres globaux Personnalisation du comportement de l'outil et de son interface utilisateur plus Tous les cas d'utilisation d'Operator

Se reporter à

– *Création d'utilisateurs Credential Management dans ACS, page 27*

7.2 Utilisation du tableau de bord

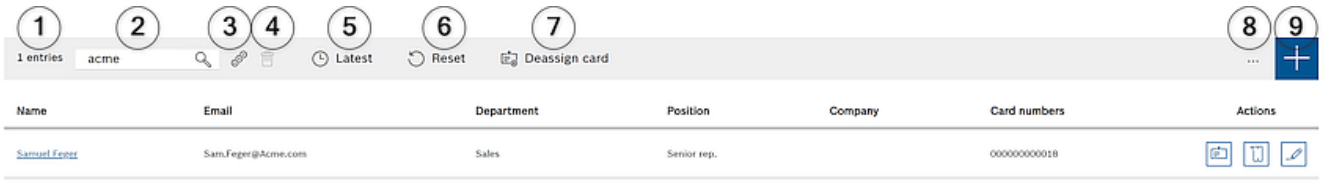
Le tableau de bord est l'écran d'accueil : une boîte de dialogue centrale qui mène à toutes les autres boîtes de dialogue.

Utilisation générale du tableau du personnel

Chaque ligne du tableau représente une personne. Il s'agit de membres du personnel interne ou externe qui ont besoin d'informations d'identification pour accéder aux locaux.

– Vous pouvez trier le tableau en fonction de n'importe quelle colonne en cliquant sur l'en-tête de la colonne.
– Vous pouvez sélectionner des personnes individuelles, ou plusieurs personnes à la fois, à l'aide des commandes clavier-souris suivantes :
  – Ctrl-clic pour une sélection multiple de lignes individuelles.
  – Ctrl-clic sur une ligne déjà sélectionnée pour la supprimer de la sélection.
  – Maj-clic pour une sélection multiple de lignes contiguës.
– Vous pouvez ajouter de nouvelles personnes au tableau
– Vous pouvez attribuer et annuler l'attribution d'informations d'identification en cliquant sur les boutons d'action
  – Attribuer une information d'identification physique
  – Attribuer des informations d'identification virtuelles (pour l'accès mobile)
  – Modifier les détails de la personne
– Vous pouvez exporter les lignes actuellement filtrées vers un fichier `.CSV` ou `.XLSX`.

Les fonctions du tableau de bord



Étiquette	Fonction
(1) N **entrées**	Le nombre total N de personnes (chaque personne correspond à une ligne dans le tableau).
(2) **Recherche**	Permet de rechercher un texte quelconque parmi les personnes du tableau
(3) 	Sélectionnez tous les éléments de la liste
(4)  **Supprimer**	Supprime les éléments sélectionnés
(5)  **Dernier**	Affiche les personnes les plus récemment ajoutées au tableau.
(6)  **Réinitialiser**	Réinitialise le tableau à sa vue par défaut et rétablit tous les filtres.
(7)  **Annuler une carte attribuée**	Ouvre une boîte de dialogue pour annuler des cartes attribuées à l'aide d'un lecteur d'inscription connecté.
(8) **. . .**	Cliquez sur le symbole des points de suspension pour afficher un menu permettant d'exporter les personnes actuellement filtrées, ainsi que les documents, vers différents formats de fichier, par exemple `.CSV` et `.XLSX` Notez que pour des raisons de sécurité des données, vous ne pouvez exporter que si votre client utilise une connexion HTTPS sécurisée avec un certificat.
(9) 	Ouvre une boîte de dialogue pour créer une nouvelle entrée dans le tableau

Les colonnes du tableau de bord

Colonne	Description
Nom	Cliquez sur le lien hypertexte pour afficher les détails de la personne.
E-mail	
Département	
Position	

Colonne	Description
Société	
Numéros de carte	Les numéros des cartes attribuées à cette personne.
Actions	Voir tableau ci-dessous

Actions à effectuer sur les enregistrements de personnel dans le tableau du tableau de bord

Icône	Actions
	**Attribuer** une ou plusieurs cartes physiques à la personne
	**Attribuer** des informations d'identification virtuelles à la personne pour l'accès mobile
	**Modifier** les détails personnels de la personne. Les modifications sont propagées à ACS. Les modifications apportées à ACS sont propagées à l'application CredMgmt.

7.3 Attribuer des informations d'identification physiques

Conditions préalables

Il est fortement recommandé d'attribuer de nouvelles informations d'identification au nouveau personnel, à l'aide d'une nouvelle carte, d'une imprimante de cartes et d'un lecteur d'inscription.

Attribuer une carte à partir du tableau de bord (nécessite un lecteur d'inscription)

1. Permet de disposer d'une carte d'accès physique prête à être présentée au lecteur d'inscription.
2. Sélectionnez la ligne de la personne et cliquez sur 
3. Suivez les instructions de la fenêtre contextuelle pour l'utilisation du lecteur d'inscription.

Attribuer une carte dans l'éditeur d'informations d'identification (nécessite un lecteur d'inscription)

1. Sur le tableau de bord, dans le tableau des personnes, sélectionnez une personne et cliquez sur  pour modifier les informations d'identification de cette personne.
2. Cliquez sur **Lire la carte** et suivez les instructions de la fenêtre contextuelle pour l'utilisation du lecteur d'inscription.

– Répétez les dernières étapes pour attribuer d'autres cartes, si nécessaire.

3. Cliquez sur **Enregistrer** pour enregistrer la personne en cours avec les attributions de la carte.

7.4 Attribuer des informations d'identification mobiles

Conditions préalables

– Mobile Access est installé et configuré sur votre système.
  – Pour obtenir des instructions, reportez-vous à la section correspondante du chapitre d'installation de ce document.
– La personne destinataire a installé l'application Mobile Access et celle-ci est en cours d'exécution sur son appareil intelligent.
  – Pour obtenir des instructions, reportez-vous à la section correspondante du chapitre d'installation de ce document.

Procédure dans le tableau de bord

1. Sélectionnez la ligne de la personne qui doit recevoir les informations d'identification mobiles
2. Sur la ligne sélectionnée, cliquez sur 
3. Sélectionnez l'une des grandes icônes pour les options :

– **Code QR**
ou
– **Mail d'invitation**

4. Si vous sélectionnez l'option **Code QR** :

– Le système affiche un code QR
– La personne scanne le code QR avec l'application Mobile Access sur son appareil mobile
– Pour que l'identifiant fonctionne, vous devez **approuver** la visite.
Pour obtenir des instructions, consultez la section Approbation et refus de visites
– Les fonctions de l'appareil mobile comme une carte d'accès physique, tant que l'application est en cours d'exécution

5. Si vous sélectionnez l'option **Mail d'invitation** :

– Par défaut, le programme sélectionne l'adresse e-mail définie pour la personne sélectionnée. Entrez une autre adresse e-mail si nécessaire
– Le système envoie un e-mail à l'adresse sélectionnée
– La personne accuse réception de l'e-mail sur son appareil mobile, qui exécute l'application Mobile Access
– La personne ouvre le lien dans l'e-mail
– Pour que l'identifiant fonctionne, vous devez **approuver** la visite.
Pour obtenir des instructions, consultez la section Approbation et refus de visites
– Les fonctions de l'appareil mobile comme une carte d'accès physique, tant que l'application est en cours d'exécution

Procédure dans les boîtes de dialogue d'édition

1. Sélectionnez la ligne de la personne qui doit recevoir les informations d'identification mobiles
2. Sur la ligne sélectionnée, cliquez sur 

– La boîte de dialogue d'édition s'ouvre

3. Dans VisMgmt, cliquez sur **Suivant** pour passer à l'écran **Détails de la visite**
4. Cliquez sur le bouton **Ajouter Mobile Access**
5. Sélectionnez l'une des grandes icônes pour les options :

– **Code QR**
ou
– **Mail d'invitation**

6. Si vous sélectionnez l'option **Code QR** :

– Le système affiche un code QR
– La personne scanne le code QR avec l'application Mobile Access sur son appareil mobile
– Pour que l'identifiant fonctionne, vous devez **approuver** la visite.
Pour obtenir des instructions, consultez la section Approbation et refus de visites
– Les fonctions de l'appareil mobile comme une carte d'accès physique, tant que l'application est en cours d'exécution

7. Si vous sélectionnez l'option **Mail d'invitation** :

– Par défaut, le programme sélectionne l'adresse e-mail définie pour la personne sélectionnée. Entrez une autre adresse e-mail si nécessaire
– Le système envoie un e-mail à l'adresse sélectionnée
– La personne accuse réception de l'e-mail sur son appareil mobile, qui exécute l'application Mobile Access
– La personne ouvre le lien dans l'e-mail
– Pour que l'identifiant fonctionne, vous devez **approuver** la visite.
Pour obtenir des instructions, consultez la section Approbation et refus de visites
– Les fonctions de l'appareil mobile comme une carte d'accès physique, tant que l'application est en cours d'exécution

Se reporter à

– *Installer Mobile Access, page 15*
– *Installation d'applications Mobile Access, page 22*

7.5 Annuler l'attribution d'informations d'identification

Annuler l'attribution d'une carte à partir du tableau de bord (nécessite un lecteur d'inscription)

1. Permet de récupérer la carte physique du détenteur de carte et de faire en sorte qu'elle puisse à nouveau être présentée au lecteur d'inscription.
2. Dans la barre d'outils, cliquez sur **Annuler l'attribution de la carte**. 
3. Suivez les instructions de la fenêtre contextuelle pour l'utilisation du lecteur d'inscription.

Annuler l'attribution d'une carte dans l'éditeur d'informations de connexion

1. Dans le tableau de bord, dans le tableau principal, sélectionnez une ligne du tableau et cliquez sur  pour modifier ce détenteur de carte.

2. Dans la boîte de dialogue de modification, dans la colonne **Cartes employé**, cliquez sur  en regard de la carte dont vous souhaitez annuler l'attribution, puis confirmez votre action dans la fenêtre contextuelle.
   Répétez cette étape jusqu'à ce que vous ayez annulé l'attribution de toutes les cartes souhaitées.
3. Cliquez sur **Enregistrer** pour enregistrer la visite en cours avec les attributions de la carte.

7.6 Autoriser des installateurs de lecteurs d'accès mobiles

Introduction

Les installateurs de lecteurs d'accès mobiles utilisent Bosch Setup Access pour scanner et configurer les lecteurs via BLE.

Les opérateurs autorisés de **Credential Management** et de **Visitor Management** envoient des informations d'identification virtuelles à l'application de l'installateur, pour autoriser ce dernier. Cette section décrit cette procédure.

Conditions préalables

– Mobile Access est installé et configuré sur votre système.
  – Pour obtenir des instructions, reportez-vous à la section correspondante du chapitre d'installation de ce document.
– Assurez-vous que l'installateur qui reçoit l'autorisation a installé Bosch Setup Access et que ce dernier est en cours d'exécution sur son appareil intelligent.
  – Pour obtenir des instructions, reportez-vous à la section correspondante du chapitre d'installation de ce document.

Procédure

1. Dans le menu principal, cliquez sur  pour ouvrir la boîte de dialogue **Intégration de l'installateur**.
2. Cliquez sur **Ajouter** pour ajouter un installateur à la liste, ou sur  pour supprimer un installateur existant

– La fenêtre contextuelle **Ajouter un installateur** s'affiche.

3. Dans la fenêtre contextuelle **Ajouter un installateur**, saisissez les détails dont vous avez besoin, par exemple :

– Noms personnels, nom de l'entreprise, adresse e-mail, numéro de téléphone
– Remarque : Vous pouvez cliquer sur  pour modifier ultérieurement les détails d'un programme d'installation sélectionné

4. Cliquez sur **Suivant**.
5. Sélectionnez l'une des grandes icônes pour les options :

– **Code QR**
  ou
– **Mail d'invitation**

6. Si vous sélectionnez l'option **Code QR** :

– Le système affiche un code QR

– La personne scanne le code QR avec l'application Mobile Access sur son appareil mobile
– Le processus d'enregistrement de l'installateur est terminé
– Cela permet à l'appareil mobile de rechercher des lecteurs d'accès mobiles et de les configurer avec BLE, dès lors que l'application est en cours d'exécution

7. Si vous sélectionnez l'option **Mail d'invitation** :
– Par défaut, le programme sélectionne l'adresse e-mail définie pour la personne sélectionnée. Entrez une autre adresse e-mail si nécessaire
– Le système envoie un e-mail à l'adresse sélectionnée
– La personne accuse réception de l'e-mail sur son appareil mobile, qui exécute Bosch Setup Access
– La personne ouvre le lien dans l'e-mail
– Le processus d'enregistrement de l'installateur est terminé
– Cela permet à l'appareil mobile de rechercher des lecteurs d'accès mobiles et de les configurer avec BLE, dès lors que l'application est en cours d'exécution

Renvoyer des invitations

1. Dans la boîte de dialogue d'intégration de l'installateur, sélectionnez l'installateur souhaité
2. Cliquez sur  sur la même ligne, afin de renvoyer l'autorisation à l'installateur sélectionné par code QR ou par e-mail.
REMARQUE : Vous ne pouvez renvoyer l'autorisation que si l'installateur ne l'a pas encore activée.

7.6.1 Réinitialiser des lecteurs Mobile Access

Il peut s'avérer nécessaire de réinitialiser les lecteurs d'accès aux valeurs par défaut pour permettre leur reconfiguration.
Par exemple, si un installateur doit reconfigurer des lecteurs Mobile Access qui ont déjà été configurés pour un autre site, ces lecteurs devront alors être réinitialisés.
Consultez le manuel du lecteur LECTUS select pour une description de la procédure de réinitialisation du lecteur à l'aide de ses commutateurs DIP.

7.7 Utiliser des applications Mobile Access sur les appareils mobiles

REMARQUE : L'utilisation des applications Bosch Mobile Access est décrite en détail pour leurs utilisateurs respectifs dans des **Guides d'utilisation rapide** séparés. Ces documents sont disponibles dans le catalogue de produits en ligne Bosch.

Introduction

Bosch fournit les applications suivantes pour Mobile Access
– Bosch Mobile Access : application de gestion des détenteurs de carte qui stocke les informations d'identification virtuelles et les transmet via Bluetooth aux lecteurs configurés pour Mobile Access. Un tel lecteur accorde ou refuse ensuite l'accès si l'une des informations d'identification stockées dans l'application est valide.
– Bosch Setup Access : application d'installation pour scanner et configurer les lecteurs via Bluetooth.

Les opérateurs autorisés pour Visitor Management et Credential Management peuvent envoyer des informations d'identification virtuelles pour les applications du titulaire de carte et de l'installateur.

Remarque!
IMPORTANT : N'utilisez pas simultanément les applications du titulaire de carte et de l'installateur
Assurez-vous que personne n'utilise l'application de l'installateur lorsque l'application du titulaire de carte est utilisée, et inversement.

7.7.1 Définir des seuils RSSI dans l'application Setup Access

Introduction

Le seuil RSSI et la gamme BLE peuvent être considérés comme des concepts à peu près équivalents dans le contexte de Bosch Mobile Access.
Les appareils Mobile Access transmettent des signaux BLE aux lecteurs à proximité. Une partie importante de la configuration du lecteur est la définition d'un seuil RSSI pour chaque lecteur. Ce seuil est la puissance minimale du signal BLE, mesurée en dBm, que le lecteur (R) doit accepter comme demande d'entrée. Le lecteur doit ignorer tous les signaux BLE plus faibles.

Les valeurs RSSI peuvent varier considérablement en fonction de nombreux facteurs, notamment le type d'appareil de transmission, le niveau de la batterie, ainsi que le matériau et l'épaisseur des murs à proximité. Il n'y a pas de relation linéaire entre la valeur RSSI et la distance entre l'émetteur et le récepteur.
Pour cette raison, l'application Setup Access fournit un outil pour mesurer la valeur RSSI du lecteur à partir de la position actuelle de l'appareil mobile. La procédure ci-dessous décrit l'utilisation de cet outil.
Lorsque vous avez trouvé une valeur de seuil appropriée pour la gamme BLE, utilisez l'application Setup Access pour stocker cette valeur dans la configuration du lecteur.

Procédure

Configurez la **gamme BLE** en utilisant l'une des options suivantes, A ou B :
A : utilisation des valeurs RSSI reflétées par le lecteur

1. Positionnez-vous devant le lecteur, à l'endroit où vous supposez que l'utilisateur de l'identifiant mobile doit se trouver.
2. Appuyez sur **Vérifier et utiliser la plage actuelle**

– Un message contextuel s'affiche. Appuyez sur **OK**

3. Une valeur RSSI apparaîtra.

– Recommandé : Répétez cette étape plusieurs fois à partir de la même position, pour avoir une idée du degré de variation de la force du signal perçu.

4. Lorsque vous avez trouvé une valeur de seuil appropriée, appuyez sur **Enregistrer**.

B : réglage manuel du seuil RSSI
1. Entrez une valeur pour le seuil RSSI.
   Consulter le tableau des seuils classiques ci-dessous
2. Appuyez sur **Enregistrer**

Valeurs de seuil classiques (approximatives seulement) :

Distance attendue entre l'appareil mobile et le lecteur	**Seuil RSSI suggéré**
Proche (5 cm - 10 cm)	-30 ... -40 dBm
Moyen (0,5m - 2m)	-50 ... -60 dBm
Éloigné (> 2m)	-70 ... -90 dBm

Remarque!
Les valeurs RSSI peuvent varier considérablement en fonction de nombreux facteurs, notamment le type d'appareil de transmission, le niveau de la batterie, ainsi que le matériau et l'épaisseur des murs à proximité.

Glossaire

ACS

terme générique désignant un système de contrôle d'accès Bosch, par exemple, AMS (Access Management System) ou ACE (BIS Access Engine).

BLE

Bluetooth Low Energy est une technologie de réseau sans fil qui offre une portée de communication similaire au Bluetooth, mais avec une consommation d'énergie inférieure.

FQDN

Un nom de domaine complet est un nom de domaine réseau qui exprime son emplacement absolu dans la hiérarchie du système de noms de domaine (DNS).

GDPR

Le Règlement général sur la protection des données (RGPD) est une loi sur la confidentialité et la sécurité qui a été adoptée par l'Union européenne (UE) et est entrée en vigueur en 2018. Il impose des obligations aux organisations qui collectent des données relatives aux personnes dans l'UE.

Mobile Access

permet de contrôler l'accès des personnes à l'aide d'informations d'identification virtuelles stockées sur un appareil mobile tel que le smartphone d'une personne.

OSDP

Open Supervised Device Protocol est une norme de communication de contrôle d'accès, introduite en 2011 par la Security Industry Association (SIA). Elle offre des avantages par rapport aux protocoles plus anciens dans les domaines du chiffrement, de la biométrie, de la facilité d'utilisation et de l'interopérabilité.

RSSI

Le RSSI (Received Signal Strength Indicator) est la force du signal perçue par un appareil récepteur, mesurée en dBm. Les appareils mobiles affichent généralement le signal RSSI sous la forme d'un graphique à barres indiquant la force du signal.

Bosch Security Systems B.V.
Torenallee 49
5617 BA Eindhoven
Netherlands
www.boschsecurity.com

Building solutions for a better life.

202309221813