Visitor Management V5.5

Avec Mobile Access

fr Manuel d'utilisation

Table des matières

1 Sécurité

Utiliser le dernier logiciel

Avant d'utiliser l'appareil pour la première fois, assurez-vous d'installer la dernière version applicable de votre logiciel. Pour une fonctionnalité, une compatibilité, des performances et une sécurité cohérentes, mettez régulièrement à jour le logiciel tout au long de la durée de vie de l'appareil. Suivez les instructions de la documentation produit relative aux mises à jour logicielles.

Les liens suivants fournissent plus de précisions :

– Informations générales : https://www.boschsecurity.com/xc/en/support/product-security/
– Avis de sécurité (liste des vulnérabilités identifiées et des solutions proposées) : https://www.boschsecurity.com/xc/en/support/product-security/security-advisories.html

Bosch n'assume aucune responsabilité en cas de dommages provoqués par l'utilisation de ses produits avec des composants logiciels obsolètes.

2 Introduction

2.1 À propos de Bosch Visitor Management

Visitor Management, ci-après appelé VisMgmt est un outil logiciel basé sur un navigateur, qui fonctionne en tandem avec les systèmes de contrôle d'accès Bosch. Il permet de gérer les visites de sites à accès contrôlé, notamment la programmation des visites, les données professionnelles des visiteurs, les documents et contrats associés, et l'attribution d'identifiants temporaires.
L'interface utilisateur est personnalisable et tout utilisateur peut changer de langue instantanément sans se déconnecter.
Principaux utilisateurs et cas d'utilisation :

Type d'utilisateur	Cas d'utilisation
Réceptionniste	Enregistrement des nouvelles visites et nouveaux visiteurs Approbation et refus de visites Création d'une liste noire de visiteurs Attribution et annulation d'attribution de cartes visiteur Gestion des documents associés Suivi du nombre de visiteurs sur le site
Visiteur	Auto-enregistrement et pré-enregistrement Création et gestion d'un profil visiteur Signature de documents
Hôte	Gestion des plannings et de listes de visites et de visiteurs Pré-enregistrement de visites
Administrateur	Définition des paramètres globaux Personnalisation du comportement de l'outil et de son interface utilisateur Plus : Tous les cas d'utilisation des réceptionnistes

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.

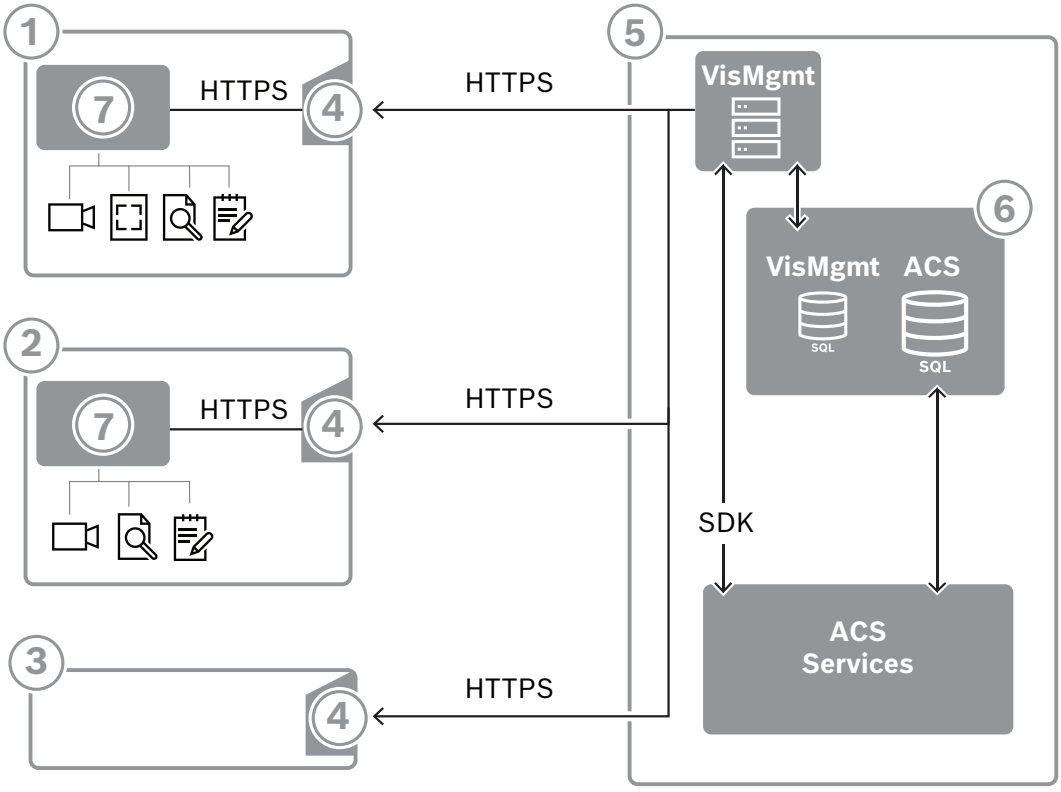
2.3 Public visé

- Visitor Management - Installateurs et administrateurs
- Principaux types d'utilisateurs de Visitor Management

2.4 Comment utiliser cette documentation

- Utilisez la fonctionnalité de **recherche** dans votre visionneur d'aide pour rechercher le contenu pertinent.
- Les sections **Présentation du système, Installation** et **Configuration** s'adressent principalement aux administrateurs système.
- Les sections **Fonctionnement** s'adressent principalement aux utilisateurs du système.

3 Présentation et topologie du système



Étiquette	Description
1	Le poste de travail **Réceptionniste**. Ce poste de travail peut comporter du matériel périphérique en option, tel qu'un lecteur d'inscription, une caméra Web ainsi que des scanners pour les signatures et les documents.
2	Le poste de travail **Visiteur** (kiosque), avec un navigateur pris en charge en mode kiosque. Ce poste de travail peut comporter du matériel périphérique en option, comme une caméra Web et des scanners pour les signatures et les documents.
3	Le poste de travail **Hôte**, c'est-à-dire le poste de travail du collaborateur qui reçoit le visiteur.
4	Navigateur pris en charge par le site Internet VisMgmt
5	Serveur ACS (BIS ou AMS)
6	L'instance de base de données du serveur ACS (Peut se trouver sur un ordinateur distinct).
7	Le **module complémentaire Bosch Peripheral Devices**, qui gère la communication entre le navigateur et le matériel périphérique.

Pour respecter la topologie de système recommandée, le serveur VisMgmt doit se trouver sur le même ordinateur que celui du système de contrôle d'accès principal, et sa base de données sur la même instance de base de données.

Le module complémentaire Bosch Peripheral Devices est installé uniquement sur les postes de travail nécessitant un accès aux périphériques.
Le poste de travail hôte ne nécessite généralement qu'un accès via navigateur au serveur VisMgmt.

4 Installation et désinstallation

4.1 Configuration logicielle et matérielle requise

Installez le serveur VisMgmt sur le même ordinateur que le système de contrôle d'accès principal : les mêmes exigences logicielles et matérielles s'appliquent.
Si le système de contrôle d'accès principal n'est pas encore installé, assurez-vous de l'installer d'abord, avant d'installer Visitor Management.
Lors de la première installation ou des mises à jour, l'ordre d'installation doit être le suivant :

1. Système de contrôle d'accès principal - Access Management System.
2. Credential Management et/ou Visitor Management.
3. Mobile Access.

Configuration serveur requise

Systèmes d'exploitation	– Windows 11 Professional and Enterprise 23H2 ; – 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)
Résolution minimale du moniteur	Full HD 1 920 x 1 080
Navigateurs pris en charge	Google Chrome, Mozilla Firefox, Microsoft Edge (basé sur Chromium) Utilisez la version la plus récente du navigateur pour votre système d'exploitation Windows .

Configuration requise pour le module complémentaire Bosch Peripheral Devices
Le **module complémentaire Bosch Peripheral Devices** est le programme qui gère la communication électronique entre le navigateur et les périphériques tels que le lecteur d'inscription, la caméra Web, le scanner de signatures et le scanner de documents.
L'ordinateur client est l'ordinateur physiquement connecté au matériel périphérique. Il exécute également le navigateur qui se connecte au serveur VisMgmt.
Bien que les périphériques ne soient pas indispensables pour l'installation, ils sont vivement recommandés, car ils augmentent considérablement l'efficacité du processus d'enregistrement des visiteurs.

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.

4.1.1 Le système de contrôle d'accès principal

Sans Mobile Access

Si Mobile Access n'est pas requis, VisMgmt version 5.5 fonctionne avec les systèmes de contrôle d'accès Bosch suivants :

– Access Management System (AMS) versions 5.5 et ultérieures

Avec Mobile Access

Si Mobile Access est sélectionné comme licence supplémentaire, VisMgmt version 5.5 fonctionne avec les systèmes de contrôle d'accès Bosch suivants :

– Access Management System (AMS) versions 5.5 (comprend une extension Mobile Access) et versions ultérieures.

Effectuez et vérifiez l'installation du système de contrôle d'accès principal, selon son propre guide d'installation, avant de procéder à l'installation de VisMgmt.

4.1.2 Une instance de base de données pour héberger la base de données du système de gestion des visiteurs

L'installation du système de contrôle d'accès principal crée une instance de base de données que vous pouvez utiliser pour héberger la base de données VisMgmt, `dbVisitorManagement`.

Le nom par défaut de cette instance varie en fonction de l'ACS

– Pour AMS, le nom est `ACE`
– Pour BIS ACE, le nom est `BIS_ACE`

4.1.3 Un utilisateur dédié pour l'accès à la base de données locale

L'utilisateur `VMUser` accède à la base de données du système de gestion des visiteurs au nom de l'application VisMgmt.

Le programme d'installation du serveur VisMgmt crée un utilisateur Windows `VMUser` sur le serveur VisMgmt.

4.1.4 Un utilisateur dédié pour l'accès à la base de données distante

Si VisMgmt doit utiliser une base de données sur un serveur de base de données distant, créez et configurez l'utilisateur `VMUser` dans Windows et sur SQL Server comme décrit ci-dessous.

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

1. Sur le serveur de base de données distant, créez un utilisateur Windows avec les paramètres suivants :

– **Nom d'utilisateur** (sensible à la casse) : `VMUser`
– **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 VisMgmt.
– **Membre du groupe** : `Administrators`
– **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 VMUser en tant que nom de connexion pour l'accès à distance à SQL Server)

1. Ouvrez SQL Management Studio
2. Connectez-vous à l'instance SQL distante
3. Accédez à **Sécurité** > **Connexion**
4. Ajoutez l'utilisateur VMUser avec le rôle serveur sysadmin

Plus tard, lorsque vous exécuterez le programme d'installation de VisMgmt sur le serveur VisMgmt, vous sélectionnerez l'option pour l'ordinateur **serveur de base de données distant** et entrerez le mot de passe que vous avez défini ci-dessus pour VMUser.

4.1.5 Un utilisateur dédié dans le système de contrôle d'accès principal

1. Dans le système de contrôle d'accès principal, créez un utilisateur bénéficiant d'une **utilisation illimitée** de l'**API**.
   Pour des instructions détaillées, reportez-vous au chapitre **Attribuer des profils d'utilisateur (opérateur)** dans le manuel de l'opérateur du système de contrôle d'accès principal.
2. Si vous utilisez BIS ACE, connectez-vous une fois au client BIS Classic ou BIS Smart avec cet utilisateur afin de définir le mot de passe.
3. Notez soigneusement le nom d'utilisateur et le mot de passe, car les assistants d'installation VisMgmt en auront besoin.

4.2 Installation du serveur

Ne démarrez pas le programme d'installation tant que les conditions logicielles requises ne sont pas respectées.
En cas d'utilisation d'AMS, de Visitor Management, de Credential Management Mobile Access dans un environnement de réseau d'entreprise, il est recommandé d'utiliser des certificats émis par une autorité de certification. Les certificats doivent être organisés avant l'installation de n'importe quel système back-end. Reportez-vous à la section *Utilisation de certificats personnalisés* dans le manuel d'installation AMS.

4.2.1 Exécution du programme d'installation du serveur

1. Sur le serveur VisMgmt prévu, en tant qu'administrateur, exécutez BoschVisitorManagementServer.exe.
2. Cliquez sur **Suivant** pour accepter le package d'installation par défaut.
3. Si vous êtes d'accord avec les termes du contrat de licence utilisateur final (EULA), acceptez-le et cliquez sur **Suivant**.
4. Sélectionnez le dossier de destination de l'installation. Il est recommandé d'utiliser le dossier par défaut.

– Dans l'écran **Configuration SQL Server**

5. Indiquez si vous souhaitez créer la base de données sur l'instance locale de SQL Server, c'est-à-dire sur l'instance de base de données sur le serveur VisMgmt, ou sur un ordinateur serveur de base de données distant.
   – **Remarque :** si vous choisissez un serveur de base de données distant, le programme d'installation demande le mot de passe de VMUser, l'utilisateur administrateur que vous avez configuré sur le serveur de base de données distant (voir la section Configuration logicielle requise).

6. Vérifiez et, si nécessaire, modifiez les valeurs des paramètres suivants :

Serveur SQL	Nom de l'ordinateur du serveur de base de données
Instance SQL	Nom de l'instance de la base de données ACS principale. C'est ici que la base de données des visiteurs est créée. Pour AMS, le nom est `ACE` Pour BIS ACE, le nom est `BIS_ACE`
Nom d'utilisateur SQL	Nom d'un utilisateur administrateur de l'instance, généralement `sa`
Mot de passe SQL	Mot de passe de cet utilisateur administrateur.

7. Cliquez sur **Tester la connexion** pour tester si l'instance de base de données est accessible à l'aide des valeurs de paramètre que vous avez entrées. Si le test échoue, vérifiez à nouveau les paramètres.
8. Cliquez sur **Suivant** pour continuer.

– Dans l'écran **Configuration de l'accès ACS** (où ACS fait référence au système de contrôle d'accès principal, AMS ou ACE)

9. Entrez les valeurs des paramètres suivants :

Nom d'hôte ACS	Nom de l'ordinateur sur lequel le serveur ACS s'exécute
Nom d'utilisateur ACS	Nom de l'utilisateur dédié de l'ACS, avec une utilisation illimitée de l'API. Voir la section Configuration logicielle requise.
Mot de passe ACS	Mot de passe de cet utilisateur ACS dédié.

10. Cliquez sur **Suivant** pour continuer.

– Dans l'écran **Configuration du serveur d'identité**

11. Entrez l'URI du serveur d'identité ACS correspondant :
    – AMS : `HTTPS://`<NomServeurACS>`:44333`
    – BIS : `HTTPS://`<NomServeurACS>`/BisIdServer`
12. Cliquez sur **Tester la connexion** pour tester si le serveur d'identité est accessible.
13. Cliquez sur **Suivant** dans l'écran récapitulatif, puis cliquez sur **Installer** pour lancer l'installation du serveur VisMgmt.
14. Après l'installation, redémarrez l'ordinateur.

4.2.2 Fichier JSON des paramètres de l'application

Un certain nombre de paramètres de configuration du serveur VisMgmt sont stockés dans le fichier `.JSON` suivant :

`<installation drive>:\Program Files (x86)\Bosch Sicherheitssysteme\Bosch Visitor Management\appsettings.json`

Il n'est généralement pas nécessaire de modifier les valeurs par défaut, mais il peut être préconisé de régler les paramètres suivants dans la section **Paramètres** du fichier. Si vous réglez les paramètres, faites d'abord une copie de sauvegarde du fichier. La sauvegarde vous aidera à annuler rapidement les modifications si vos modifications provoquent un dysfonctionnement.

Enregistrez vos modifications et redémarrez le service Windows VisMgmt pour appliquer les paramètres modifiés. Le nom du service est `Bosch Visitor Management`.

Nom du paramètre	Valeur par défaut	Description
PageSizeNumberOfVisit	20	Nombre maximal d'enregistrements de visite apparaissant à l'écran en même temps. Lorsque l'utilisateur fait défiler les pages, chaque nouvelle page affiche ce nombre d'enregistrements, qui provient de la base de données.
MaximumUploadFileSizeBytes	31457289	Nombre maximal d'octets qu'un fichier téléchargé peut contenir.
StartoverTimeoutAskSeconds	300	L'application attend ce nombre de secondes si l'utilisateur fait une pause lors de la saisie des informations de connexion, puis elle affiche un message invitant l'utilisateur à reprendre la saisie.
StartoverTimeoutResetSeconds	60	Une fois l'invite affichée, l'application attend ce nombre de secondes avant de réinitialiser l'écran de connexion.

4.3 Configuration de l'ordinateur client VisMgmt

Le module complémentaire Bosch Peripheral Devices peut être installé sur l'ordinateur serveur, mais il est généralement installé sur un ordinateur client du même réseau. Si tel est le cas, copiez le certificat HTTPS à partir du serveur ACS et installez-le également sur l'ordinateur client. Pour obtenir des instructions, consultez *Certificats pour une communication sécurisée, page 16* ci-dessous.
Le module complémentaire Bosch Peripheral Devices est le logiciel de connexion des dispositifs tels que les lecteurs d'inscription et les scanners. Si de tels dispositifs ne sont pas nécessaires, par exemple pour l'utilisateur hôte, l'accès au navigateur est suffisant pour se connecter et exécuter l'application VisMgmt.

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

Se reporter à

– *Certificats pour une communication sécurisée, page 16*

4.3.1 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, en tant qu'administrateur, exécutez `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.

4.3.2 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`

Remarque : Après un roulement de certificat, redémarrez le service back-end Mobile Access ou le service Bosch Credential Management et le service Visitor Management.

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	/	/	/	/

4.3.2.1 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.

4.3.2.2 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**.

4.3.2.3 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

4.3.3 Fichier JSON des paramètres de l'application

Un certain nombre de paramètres de configuration de l'ordinateur client VisMgmt sont stockés dans le fichier `.JSON` suivant :
<lecteur d'installation>:`\Program Files (x86)\Bosch Sicherheitssysteme\Bosch Visitor Management\appsettings.json`
Il n'est généralement pas nécessaire de modifier les valeurs par défaut, mais il peut être préconisé de régler les paramètres suivants dans la section **AppSettings** du fichier.
Enregistrez vos modifications et redémarrez le Service Windows VisMgmt pour appliquer les paramètres modifiés. Le nom du service est `Bosch Ace Visitor Management Client`

Nom du paramètre	Exemple	Description
`CorseOrigins`	`"https://my-vm-server:5706"`	Adresse et numéro de port du serveur de gestion des visiteurs.
`CardReaderPort`	`"com3"`	Le numéro de port COM auquel un lecteur d'inscription LECTUS est connecté. Pour les lecteurs HID OMNIKEY, ce paramètre peut être vide.

4.4 Vérification de l'installation du serveur

À partir d'un ordinateur du même réseau, à l'aide de l'un des navigateurs pris en charge, ouvrez l'URL suivante :
`https://`<Ordinateur serveur VisMgmt>`:5706/main`
Si le serveur est en cours d'exécution, il affiche la page de connexion de l'application.

4.5 Installer Mobile Access

Introduction
Le service back-end Mobile Access fournit une fonctionnalité d'accès mobile pour Credential Management et Visitor Management.
Assurez-vous d'utiliser la dernière version du système de contrôle d'accès principal et la dernière version du serveur back-end Mobile Access.

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.

4.5.1 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.

4.5.2 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

4.5.3 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`

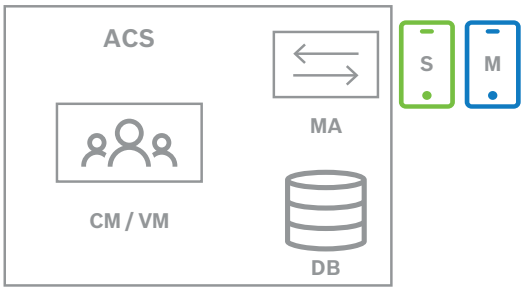
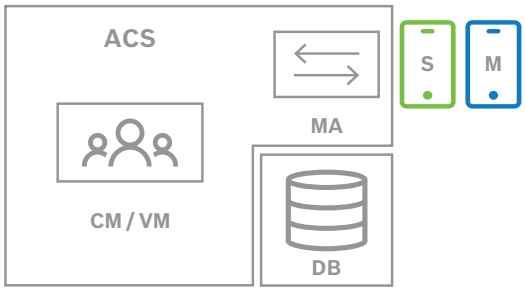
Ajoutez ensuite `MAUser` comme identifiant de connexion à distance au serveur SQL comme suit :

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.

4.5.4 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 **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 **Suivant**.

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

– L'assistant d'installation se termine.

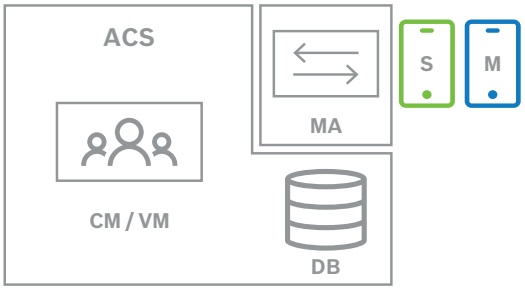
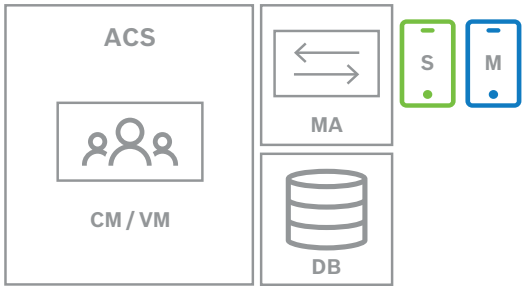
10. Cliquez sur **Suivant**.
11. Sur l'écran **Composants principaux**, vérifiez que l'installation s'est terminée avec succès, puis cliquez sur **Terminer**
12. Dans l'application Windows `Services`, vérifiez que le service `Bosch Mobile Access` est en cours d'exécution.

4.5.5 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**.
Sur un serveur back-end Mobile Access distribué, la condition préalable suivante est requise avant de lancer l'installation de Mobile Access ou de mettre à jour le système. Elle n'est pas nécessaire dans un environnement colocalisé :

– Installez **le pack d'hébergement ASP.NET Core 8.0 Runtime (v8.0.2)** sur le serveur back-end Mobile Access distribué avant d'exécuter l'installateur de Mobile Access.
– Utilisez le lien suivant pour télécharger le pack d'hébergement requis : https://dotnet.microsoft.com/en-us/download/dotnet/thank-you/runtime-aspnetcore-8.0.2-windows-hosting-bundle-installer.

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
Assurez-vous que vous avez la dernière version du système de contrôle d'accès principal.

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 **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.

4.6 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

4.7 Matériel périphérique

Les périphériques USB suivants ont été testés et approuvés pour une utilisation avec VisMgmt et CredMgmt au moment de la rédaction. Pour une liste continuellement mise à jour des appareils compatibles, consultez la fiche technique du système de contrôle d'accès principal.

Lecteur d'inscription de carte	LECTUS enroll ARD-EDMCV002-USB, HID OMNIKEY 5427 CK
Scanner pour les documents d'identité	ARH Combo, ARH Osmond
Lecteur de signatures	signotec LITE, signotec Omega

Suivez les instructions du fabricant pour connecter ces appareils à vos ordinateurs clients.

Lecteurs d'enrôlement
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

4.7.1 Enregistrement du matériel périphérique auprès de l'ordinateur client

Pour enregistrer le matériel périphérique auprès de l'ordinateur client VisMgmt, exécutez le programme d'installation des périphériques Bosch, `BoschPeripheralDeviceAddon.exe`, sur le client. Pour obtenir des instructions, voir *Configuration du module complémentaire pour périphériques, page 15*.

Se reporter à

– *Configuration du module complémentaire pour périphériques, page 15*

4.8 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, redémarrez le serveur.
4. Lancez 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.

4.9 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.

Remarque : Après avoir désinstallé le serveur back-end Mobile Access, les traces suivantes de la configuration doivent être supprimées manuellement :

- **MAUser** - cet utilisateur reste après la désinstallation. Un administrateur doit le supprimer manuellement.
- **Certificats** - utilisez *Gérer les certificats d'ordinateur* pour supprimer manuellement tous les certificats installés en raison de l'installation de Mobile Access.
- **Configuration du serveur d'ID pour Mobile Access** - le fichier *appsettings.Extension.MobileAccessBackend* reste une fois le serveur back-end désinstallé. Supprimez-le manuellement.

5 Configuration

5.1 Création d'utilisateurs du système de gestion des visiteurs dans l'ACS

Introduction

Chaque Administrateur, Réceptionniste ou Hôte de VisMgmt doit être titulaire d'une carte avec une définition d'opérateur distincte dans l'ACS, c'est-à-dire le système de contrôle d'accès principal.

Ces définitions d'opérateurs contiennent des droits VisMgmt 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 le système de gestion des visiteurs. Vous ne pouvez pas affecter plusieurs titulaires de carte au même opérateur.

Remarque!

Sécurité informatique et comptes utilisateur

Conformément aux bonnes pratiques en matière de sécurité informatique, nous recommandons que chaque utilisateur Réceptionniste, Hôte et Administrateur travaille sous son propre compte Windows.

Création de profils d'utilisateur pour le système de gestion des visiteurs

1. Connectez-vous au système de contrôle d'accès principal avec des privilèges d'administrateur.
2. Créez un ou plusieurs profils d'utilisateur (opérateurs) pour utilisateurs VisMgmt.
   Chemin d'accès de la boîte de dialogue :
– **Configuration > Opérateurs et postes de travail** > **Profils d'utilisateur**
– Navigateur de configuration > **Administration** > **Profils d'utilisateur ACE**
3. Attribuez l'un des droits d'utilisateur suivants à ces profils.
– Administrateur : `Visitor Management > Administrator`
– Hôte : `Visitor Management > Host`
– Réceptionniste : `Visitor Management > Receptionist`

Lorsque vous avez créé les profils d'utilisateur dont vous avez besoin pour les différents rôles VisMgmt (Administrateur, Réceptionniste, Hôte), vous pouvez attribuer chaque profil à plusieurs opérateurs.

Attribuer des profils d'utilisateur aux opérateurs ACS et aux titulaires de carte

Chemin d'accès de la boîte de dialogue :

– **Configuration** > **Opérateurs et postes de travail** > **Droits de l'utilisateur**
– Navigateur de configuration > **Administration** > **Opérateurs**

1. Ajouter un nouveau type d'opérateur (cliquez sur  ou sur  , selon l'ACS) et donnez-lui un nom qui se rapporte clairement à l'un des rôles VisMgmt (Administrateur, Hôte ou Réceptionniste).
2. Dans l'onglet **Paramètres généraux de l'opérateur**, sélectionnez `Operator ACE` dans la liste d'autorisations.

3. Dans l'onglet **Paramètres de l'opérateur ACE**, utilisez les boutons fléchés pour attribuer le **profil d'utilisateur ACE** que vous avez créé ci-dessus.
   Annulez l'attribution du profil par défaut `UP-Administrator`, sauf dans le cas peu probable où le titulaire de la carte nécessite des droits d'administrateur général dans l'ACS.
4. Toujours dans l'onglet **Paramètres de l'opérateur ACE**, utilisez le volet **Affecter une personne** pour rechercher dans le système le titulaire de carte auquel attribuer le rôle VisMgmt.
5. Cliquez sur **Affecter une personne** pour terminer l'attribution au titulaire de carte sélectionné.

– Vous devez définir un opérateur distinct pour chaque titulaire de carte utilisant le système de gestion des visiteurs. Vous ne pouvez pas affecter plusieurs titulaires de carte au même opérateur.

5.2 Création d'autorisations et de profils de visiteurs dans l'ACS

Introduction

Le réceptionniste ou l'administrateur du système VisMgmt sélectionne un **type de visiteur** pour chaque nouveau visiteur. Ce type de visiteur est basé sur un **type de personne** prédéfini appelé **Visiteur** dans le système de contrôle d'accès principal (ACS), ou sur un sous-type de **visiteur** que les administrateurs de l'ACS ont créé.
Ces administrateurs doivent également configurer le type de personne **Visiteur** et ses sous-types dans l'ACS avec des profils d'accès. Les profils d'accès permettent à ces types de personnes d'actionner les portes physiques sur le site.

5.3 Configuration de l'ordinateur du réceptionniste

L'ordinateur du réceptionniste exécute le **module complémentaire Bosch Peripheral Devices**, qui lui permet de se connecter physiquement à des périphériques pour la lecture de cartes, la numérisation de documents d'identité et la numérisation de signatures.
Connectez tous les périphériques requis avant d'installer le logiciel client.
Assurez-vous que l'ordinateur et ses périphériques sont correctement protégés contre tout accès non autorisé.

5.4 Configuration d'un ordinateur kiosque pour les visiteurs

Introduction

Les visiteurs enregistrent généralement leurs visites et créent leurs propres profils sur un ordinateur librement accessible dans la zone d'accueil du site à accès contrôlé. Pour des raisons de sécurité, le navigateur Web de l'ordinateur s'exécute en mode kiosque, qui ne permet d'accéder qu'à VisMgmt, et non à plusieurs onglets, paramètres de navigateur ou système d'exploitation de l'ordinateur. Tous les navigateurs pris en charge disposent d'un mode kiosque, mais sa configuration exacte dépend du navigateur.
L'ordinateur kiosque exécute le module complémentaire **Bosch Peripheral Devices**, qui lui permet de se connecter physiquement à des périphériques pour numériser des documents d'identité et des signatures.

– L'URL du mode kiosque est `https://`<Mon_serveur_VisMgmt>`:5706`

Configuration des navigateurs pour le mode kiosque

Les liens suivants décrivent la configuration du mode kiosque pour les navigateurs pris en charge par VisMgmt

	Instructions pour la configuration du mode kiosque
Chrome	https://support.google.com/chrome/a/answer/9273974
Firefox	https://support.mozilla.org/en-US/kb/firefox-enterprise-kiosk-mode
Edge	https://docs.microsoft.com/en-us/deployedge/microsoft-edge-configure-kiosk-mode

Remarque!
Pour des raisons de sécurité, désactivez toujours l'option de navigateur permettant d'enregistrer automatiquement les mots de passe.

5.5 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 VisMgmt, suivi du signe deux-points et du numéro de port (par défaut `5706`)
   `https://`<Mon_serveur_VisMgmt>`:5706/main`
   L'écran **Connexion** apparaît.
2. Connectez-vous à VisMgmt en tant qu'utilisateur **Administrateur**.
3. Cliquez sur  pour ouvrir le menu **Paramètres**.

5.6 Configuration à l'aide du menu Paramètres

Le menu **Paramètres** contient des sous-sections qui vous permettent d'effectuer les étapes de configuration suivantes :

Paramètres généraux	– **Période de conservation (jours)** : ce paramètre régit le traitement des enregistrements de visite. – 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. – **Mode de stockage des documents** : indiquez si les documents doivent être stockés sous forme de fichiers papier ou numériques. – **Nombre maximal de visiteurs** autorisé sur le site en même temps. La valeur par défaut est `100`. Attribuez la valeur `0` pour désactiver complètement les compteurs de visiteurs sur le tableau de bord. – **Délai d'expiration du document (jours)** : entrez la durée pendant laquelle les documents téléchargés, tels que les accords de non-divulgation (NDA) et les conditions d'utilisation, doivent rester

valides. Le délai s'applique aussi bien aux fichiers papier qu'aux fichiers numériques.
Passé ce délai, les documents sont marqués comme expirés dans le profil du visiteur (icône d'horloge avec un point rouge).
La valeur par défaut est `365`

- **Période d'avertissement de l'expiration des documents (jours)** : entrez la durée de la période d'avertissement avant la date d'expiration.
  Durant cette période d'avertissement, les documents sont marqués dans le profil du visiteur (icône d'horloge avec un point orange).
  Avant l'activation de la période d'avertissement, l'icône de l'horloge comporte un point vert.
- **Logo :** Sélectionnez ou désactivez les cases à cocher qui déterminent si les fenêtres de dialogue affichent un logo personnalisé ou le logo par défaut, et si le **supergraphique** Bosch s'affiche.
  - Pour les critères des fichiers de logo personnalisés, voir : *Personnaliser le logo de l'entreprise, page 38*
- 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. Si le serveur de messagerie externe nécessite un certificat SSL/TSL supplémentaire, importez-le sur l'ordinateur exécutant le serveur back-end Mobile Access. Après l'importation, il est nécessaire de redémarrer `VisitorManagerServer`.
- **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.
Réceptionniste	– Cet écran de paramètres comporte 2 cases à cocher pour chacun des champs de données figurant dans les boîtes de dialogue d'enregistrement des visiteurs du réceptionniste. – Désactivez ou sélectionnez la première case à cocher pour déterminer si le champ de données est **visible** dans toutes les boîtes de dialogue d'enregistrement. – Désactivez ou sélectionnez la seconde case à cocher (marquée d'un astérisque) pour déterminer si le champ de données est **obligatoire**. – Personnalisez les textes d'en-tête par défaut dans les boîtes de dialogue de collecte de données. Pour plus de détails, reportez-vous à *Personnalisation de l'interface utilisateur, page 37* ci-dessous.
	Option spéciale : Permettre l'enregistrement/le départ sans carte Si les visiteurs sont accompagnés ou si seuls les espaces publics leur sont autorisés, il peut être inutile de les doter de cartes individuelles. Pour de tels cas, il existe une option permettant aux visiteurs de s'enregistrer et de quitter les lieux sans utiliser de carte. Pour des raisons de sécurité, cette option est désactivée par défaut. Pour l'activer, sélectionnez la case à cocher : – **Remarque :** si cette option est activée, tout **visiteur** qui s'auto-enregistre sur l'ordinateur kiosque approuve et enregistre sa propre visite en même temps. – Reportez-vous au chapitre **Fonctionnement** *Enregistrement et départ sans carte, page 55* de ce document pour plus de détails sur la façon dont l'utilisateur **Réceptionniste** gère les visiteurs sans carte.
Hôte	Les paramètres des utilisateurs **Hôte** et **Visiteur** restent en lecture seule jusqu'à ce que vous ayez modifié et enregistré les paramètres applicables à **Réceptionniste**. Les champs que vous avez définis comme non visibles dans les paramètres de l'utilisateur **Réceptionniste** sont automatiquement définis comme non visibles pour les utilisateurs **Hôte** et **Visiteur**. La procédure de configuration est ensuite identique.
Visiteur	

Se reporter à

- *Attribuer des informations d'identification physiques, page 51*
- *Personnalisation de l'interface utilisateur, page 37*

5.6.1 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. Lorsque vous téléchargez un modèle pour le modifier, il est copié dans le dossier de téléchargements 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.
- `VisitorInvite.html` Invitation destinée aux personnes visitant votre site, avec la possibilité d'ajouter un fichier iCalendar à l'e-mail.
- `InformHostAboutCheckin.html` E-mail destiné à informer l'hôte qu'un visiteur est arrivé.

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

Espace réservé	Description
{{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

Invitation visiteur

E-mail envoyé à un visiteur lorsqu'une visite est créée ou modifiée pour lui.

Espace réservé	Description
{{VisitorID}}	code d'identification du visiteur, tel que généré par l'application VisMgmt
{{Title}}	Titre du visiteur (M., Mme, Dr., etc.)
{{FirstName}}	prénom du visiteur
{{LastName}}	nom du visiteur
{{CompanyName}}	entreprise du visiteur
{{HostFirstName}}	prénom de l'hôte
{{HostLastName}}	Nom de l'hôte
{{ExpArrivalDate}}	date de visite prévue

Visiteur arrivé

E-mail envoyé à l'hôte lorsque la réceptionniste approuve la visite

Espace réservé	Description
{{VisitorID}}	code d'identification du visiteur, tel que généré par l'application VisMgmt
{{Title}}	Titre du visiteur (M., Mme, Dr., etc.)
{{FirstName}}	prénom du visiteur
{{LastName}}	nom du visiteur
{{CompanyName}}	entreprise du visiteur
{{HostFirstName}}	prénom de l'hôte
{{HostLastName}}	Nom de l'hôte
{{ExpArrivalDate}}	date de visite prévue
{{ArrivalDate}}	date réelle de la visite

passe de visite

Document pouvant être imprimé et remis à un visiteur. Peut contenir une carte du bâtiment ou une liste de contrôle, par exemple.

Espace réservé	Description
{{VisitorID}}	code d'identification du visiteur, tel que généré par l'application VisMgmt
{{Title}}	Titre du visiteur (M., Mme, Dr., etc.)
{{FirstName}}	prénom du visiteur
{{LastName}}	nom du visiteur
{{CompanyName}}	entreprise du visiteur
{{HostFirstName}}	prénom de l'hôte
{{HostLastName}}	Nom de l'hôte
{{ExpArrivalDate}}	date de visite prévue
{{ArrivalDate}}	date réelle de la visite

5.6.2 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.

5.6.3 Modèles de documents

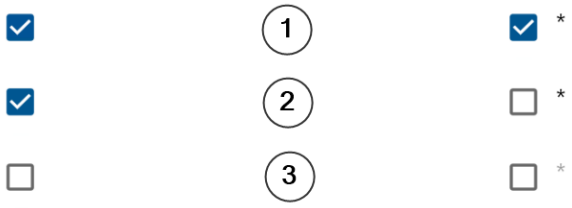
Pour les différents documents et e-mails, vous pouvez télécharger des modèles et charger des versions personnalisées de ces modèles dans la boîte de dialogue **Tableau de bord** > **Paramètres > Général**.

5.7 Personnalisation de l'interface utilisateur

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

5.7.1 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.

5.7.2 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>
   ```

5.7.3 Personnalisation du mode kiosque

Si votre site ne dispose pas d'aucun dispositif matériel, par exemple un scanner de documents, vous pouvez personnaliser le processus d'auto-enregistrement du visiteur en mode kiosque en désactivant les cases à cocher des étapes d'enregistrement correspondantes.

5.7.4 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

5.8 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>:5701 - 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	5701	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	5701	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
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.

5.8.1 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
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

Programme	Emplacement du fichier
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
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
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
Bosch.MUM	[MUM-chemin-installation]\

5.8.2 Mobile Access API

Depuis Mobile Access 5.2 et versions ultérieures, Credential Management 5.2 et versions ultérieures, et Visitor Management 5.2 et versions ultérieures, l'API du serveur back-end de Mobile Access a été divisée en un canal avant et un canal arrière. Le canal avant doit communiquer avec les téléphones portables tandis que le canal arrière communique avec Credential Management et/ou Visitor Management.

Cela permet de définir des règles de pare-feu et des itinéraires pour réglementer le trafic réseau afin de renforcer la sécurité informatique. La division de l'API comporte deux numéros de port distincts. Le numéro de port des téléphones mobiles est 5700, tandis que Credential Management et Visitor Management utilisent le port 5701.
Credential Management et Visitor Management possèdent deux paramètres distincts, respectivement pour l'URL du canal avant et l'URL du canal arrière. L'interface utilisateur les appelle « Adresse du service administratif » (canal arrière) et « Adresse du service d'enregistrement » (canal avant).
Le port par défaut de l'adresse du service administratif (canal arrière) est 5701. Dans une règle de pare-feu spécifique au client, ce port doit être configuré uniquement pour communiquer avec la machine qui exécute le serveur back-end de la Credential Management et/ou Visitor Management, qui est le serveur AMS dans la plupart des cas.
Le port par défaut de l'adresse du service d'enregistrement (canal avant) est 5700. Dans une règle de pare-feu spécifique au client, ce port doit être configuré pour être accessible à partir des applications Mobile Access. Dans de nombreux cas, ce point d'extrémité est accessible de l'extérieur. En revanche, cette situation dépend fortement du scénario du client.
Si le client est en cours de mise à jour à partir d'une version antérieure vers la version la plus récente du système AMS, les paramètres de Credential Management et de Visitor Management doivent être modifiés. Ce paramètre est accessible pour le rôle Administrateur pour Credential Management et Visitor Management sur la page des paramètres.
Le canal arrière doit être sécurisé afin qu'il ne soit pas accessible depuis l'Internet public ou tout réseau non autorisé.

5.9 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 :

5.9.1 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.

5.9.2 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.
- Attribution et configuration correctes des profils d'utilisateur pour les opérateurs afin d'éviter que des opérateurs normaux n'affectent des autorisations de sécurité élevées sans appliquer le principe de double contrôle.

5.9.3 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.

5.10 Sauvegarde du système

VisMgmt est une application Web auxiliaire pour un système de contrôle d'accès principal. Consultez la documentation du système de contrôle d'accès principal concernant la sauvegarde des bases de données du système.

6 Fonctionnement

6.1 Aperçu des rôles d'utilisateur

Type d'utilisateur	Cas d'utilisation
Réceptionniste	Enregistrement des nouvelles visites et nouveaux visiteurs Approbation et refus de visites Création d'une liste noire de visiteurs Attribution et annulation d'attribution de cartes visiteur Gestion des documents associés Suivi du nombre de visiteurs sur le site
Visiteur	Auto-enregistrement et pré-enregistrement Création et gestion d'un profil visiteur Signature de documents
Hôte	Gestion des plannings et de listes de visites et de visiteurs Pré-enregistrement de visites
Administrateur	Définition des paramètres globaux Personnalisation du comportement de l'outil et de son interface utilisateur Plus : Tous les cas d'utilisation des réceptionnistes

6.2 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.

Aperçu et filtres rapides
La partie supérieure du tableau de bord offre un aperçu rapide des visites de la journée. Elle permet à l'utilisateur de surveiller facilement le nombre de visiteurs sur le site.

Visiteurs attendus aujourd'hui : _%	**Visiteurs enregistrés : _%**	**Visiteurs dont le départ est attendu aujourd'hui**	**Visiteurs pour lesquels l'heure de départ est dépassée**
`<current count> / <total capacity>`	`<current count> / <total capacity>`	`<current count>`	`<current count>`

Cliquez sur l'un des en-têtes pour filtrer le tableau des visites en fonction de la signification de l'en-tête. Par exemple, cliquez sur **Visiteurs enregistrés** pour afficher uniquement les visiteurs auxquels une carte a été attribuée.
La valeur de `<total capacity>` est un paramètre de configuration défini par l'administrateur système. Cf. *Configuration à l'aide du menu Paramètres, page 32*.

6.2.1 Présentation de page personnelle

Sur le tableau de bord, cliquez sur le nom d'une personne donnée. Une boîte de dialogue s'ouvre avec ses données personnelles. Les données s'affichent. La présentation de la page personnelle contient quatre sections de champs de données personnelles :
- Image ID
- Document d'identité
- Informations générales

– Documents

6.2.2 Tableau des visites

Chaque ligne du tableau représente un rendez-vous pour une visite.

- 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 visites individuelles, ou plusieurs visites à la fois, à l'aide des commandes clavier-souris suivantes :
  - Ctrl + clic pour sélectionner plusieurs lignes individuelles.
  - Maj + clic sur une ligne déjà sélectionnée pour la supprimer de la sélection.
  - Maj + clic pour sélectionner plusieurs lignes contiguës.
- Vous pouvez ajouter de nouvelles visites au tableau
- Vous pouvez gérer les visites et les détails des visiteurs en cliquant sur les boutons d'action
  - Approuver la visite
  - Refuser la visite
  - Attribuer des cartes au visiteur
  - Modifier les détails de la visite et du visiteur
- Vous pouvez exporter toutes les données vers un fichier .CSV ou .XLSX. Si vous ne souhaitez utiliser que certaines données spécifiques, utilisez le filtre. Il est impossible d'exporter les données souhaitées en les sélectionnant. Seules les lignes actuellement filtrées peuvent être exportées vers un fichier .CSV ou .XLSX.

La barre d'outils horizontale offre les fonctionnalités suivantes :

Étiquette	Fonction
1 N **entrées**	Le nombre total N de visites (chaque visite correspond à une ligne dans le tableau).
2 **Recherche**	Permet de recherche un texte quelconque parmi les visites du tableau
3	Affiche les visites les plus récemment ajoutées au tableau.
4	Ouvre une boîte de dialogue permettant de sélectionner les critères de filtre
5	Réinitialise le tableau à sa vue par défaut et rétablit tous les filtres.
6 **Annuler une carte attribuée**	Ouvre une boîte de dialogue pour annuler des cartes attribuées à l'aide d'un lecteur d'inscription connecté.

Étiquette	Fonction
	Ouvre une boîte de dialogue pour créer une nouvelle entrée de visite dans le tableau
...	Cliquez sur le symbole des points de suspension pour afficher un menu permettant d'exporter les visites 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.

6.2.3 Colonnes du tableau et actions

Colonnes

Colonne	Valeur	Description
État	 Visite prévue  Visite approuvée  Visite refusée  Carte attribuée  Carte expirée  Visite terminée (Le visiteur ne détient plus de cartes et a quitté les lieux)	Icône reflétant le statut de la visite
Nom	Nom du visiteur sous forme de lien hypertexte	Cliquez sur le lien hypertexte pour afficher les détails du visiteur et de sa visite en cours.
Arrivées att.	Date et heure	Date et heure d'arrivée prévues du visiteur
Départ att.	Date et heure	Date et heure de départ prévues du visiteur

Colonne	Valeur	Description
Arrivée	Date et heure	Date et heure à laquelle la première carte du visiteur lui a été attribuée.
Sortie	Date et heure	Date et heure à laquelle la dernière carte attribuée au visiteur a été annulée.
Numéros de carte	Numérique	Les numéros des cartes attribuées à ce visiteur.
Actions	Icônes	Voir tableau ci-dessous

Actions

Icône	Fonction
	Pour **approuver** la visite. REMARQUE : il n'est pas possible d'attribuer une carte aux visiteurs sur liste noire. Supprimez d'abord le visiteur de la liste noire, ou exemptez-le temporairement. Voir *Ajouter, supprimer ou exclure de la liste noire, page 56*
	Pour **refuser** la visite. Ce bouton est désactivé une fois que le visiteur s'est enregistré, c'est-à-dire lorsqu'il possède déjà une carte.
	Pour **attribuer** une ou plusieurs cartes au visiteur
	Pour **modifier** l'événement de visite et/ou les informations d'identification des visiteurs

6.3 Réceptionniste

6.3.1 Se connecter au rôle Réceptionniste

1. Dans votre navigateur, ouvrez `https://`<Mon_serveur_VisMgmt>`:5706/main/` pour afficher l'écran de connexion.
2. Entrez le nom d'utilisateur d'un compte disposant des droits requis pour votre rôle. Consultez votre administrateur système si vous n'avez pas de compte.
3. Entrez le mot de passe.
4. Cliquez sur **Connexion**.

6.3.2 Rechercher et filtrer des visites

Dans le tableau de bord VisMgmt, dans la barre d'outils figurant au-dessus du tableau des visites.

Recherche

Pour rechercher des noms et des hôtes, entrez du texte alphanumérique dans la zone de recherche, puis appuyez sur Entrée.

Filtrage

– Pour afficher les visites les plus proches de l'heure actuelle, cliquez sur **Dernières**

- Pour créer un filtre complexe à partir du statut de la visite, des dates d'arrivée et de départ et des numéros de carte, cliquez sur **Filtrer**.
  - Entrez les critères de filtre souhaités dans la boîte de dialogue contextuelle
  - Cliquez sur **Appliquer**
    Le système réduit le tableau des visites aux seuls rendez-vous de visite qui répondent aux critères du filtre.
- Pour supprimer tous les critères de filtre, cliquez sur **Réinitialiser**

6.3.3 Enregistrer des visites

Introduction

Le réceptionniste a deux possibilités pour enregistrer les visites :

- **A :** si le visiteur utilise le kiosque visiteur pour créer son propre identifiant de visiteur et télécharger des documents, il suffit au réceptionniste de renseigner les éventuelles informations et signatures requises manquantes, puis d'attribuer une carte au visiteur.
- **B :** si le visiteur ignore le kiosque visiteur et s'adresse directement à la réception, le réceptionniste peut enregistrer la visite intégralement, c'est-à-dire recueillir les informations nécessaires, obtenir les signatures pour les documents requis, puis attribuer une carte au visiteur.

Le scénario **A** étant un sous-ensemble du scénario **B**, seul le scénario **B** complet est décrit ici. L'utilisation du mode kiosque par un visiteur est décrite dans la section correspondante. Cf. *Présentation du mode kiosque, page 60*.

Procédure

Dans le tableau de bord VisMgmt, dans la barre d'outils figurant au-dessus du tableau des visites.

1. Cliquez sur  pour ajouter un rendez-vous de visite au tableau des visites.
2. Dans la boîte de dialogue **Données personnelles**, entrez les données que votre site exige des visiteurs. Les champs obligatoires sont marqués d'un astérisque (*).
   Vous pouvez entrer les données manuellement, mais l'utilisation d'un scanner de documents, si le poste de travail du réceptionniste en est doté, est plus rapide et précise. Voir *Matériel périphérique, page 27* pour plus de détails sur les périphériques pris en charge.

- **Informations générales**
  - Recherchez et chargez un profil visiteur complet créé lors d'une visite précédente.
    Pour rechercher des profils, cliquez sur l'icône  (recherche) située près du champ **Nom***.
    Lors de la création d'un profil visiteur, celui-ci reçoit un code alphanumérique unique qu'il doit soigneusement conserver afin d'accélérer le processus d'enregistrement lors des visites suivantes.
  - Sinon, entrez les données manuellement.
- **Photos d'identité**
  - **Téléchargez** une photo à partir du système de fichiers.
  - **Prenez** des photos du visiteur à l'aide d'une webcam connectée.
- **Pièces d'identité**
  - Cliquez sur **Numériser un document** pour lire les données à partir d'un scanner de documents (si disponible) et renseigner automatiquement les champs de données pertinents dans la boîte de dialogue.

  - Si votre système ne dispose pas d'un scanner de documents, entrez le texte manuellement.
- **Documents légaux**
  - Chargez les documents que le visiteur a signés électroniquement en mode kiosque.
  - Si votre système ne dispose pas d'un kiosque visiteur, imprimez et classez (avec la signature du visiteur) les documents PDF requis stockés dans le système de fichiers.

3. Cliquez sur **Suivant** pour ouvrir à la boîte de dialogue **Visites**.
4. Dans la boîte de dialogue **Visites**, dans le volet **Visite en cours**, entrez les données requises par votre site. Les champs obligatoires sont marqués d'un astérisque (*).

- Sélectionnez un **type de visiteur**.
  Il s'agit soit du type **Visiteur** (par défaut), soit d'une sous-classe personnalisée de **Visiteur**, définie comme un **type de personne** dans le système de contrôle d'accès principal.
- Sous **Hôte**, sélectionnez le nom du collaborateur recevant la visite.
  - Notez que vous ne pouvez sélectionner que les titulaires de carte du système de contrôle d'accès principal.
  - Une info-bulle affiche l'adresse e-mail de la personne pour faciliter l'identification.
- Si le visiteur a besoin d'être accompagné dans les locaux, dans **Accompagnateur**, sélectionnez le nom du collaborateur qui l'accompagne.
  - Notez que vous ne pouvez sélectionner que les titulaires de carte du système de contrôle d'accès principal.
  - Une info-bulle affiche l'adresse e-mail de la personne pour faciliter l'identification.
- Si le visiteur a besoin de plus de temps pour franchir une porte, sélectionnez la case à cocher **Ouverture de porte prolongée**

5. Cliquez sur **Enregistrer**.
   Notez que vous ne pourrez pas enregistrer les données tant que vous n'aurez pas renseigné tous les champs obligatoires.

Se reporter à
- *Matériel périphérique, page 27*

6.3.4 Approbation et refus de visites

Contexte : approbation des cartes physiques
Vous devez approuver une visite avant de pouvoir attribuer des cartes à un visiteur.

Contexte : approbation des informations d'identification mobiles
Vous pouvez créer et partager un identifiant mobile le jour de la visite, comme pour l'attribution d'une carte physique.
- **Remarque :** L'identifiant mobile ne fonctionnera pas tant que vous n'aurez pas approuvé la visite.

Sinon, vous pouvez créer l'identifiant mobile et le partager à l'avance. Lorsque le visiteur arrive à la réception, approuvez la visite, comme décrit ci-dessous, pour enfin activer l'identifiant.
- **Remarque :** L'identifiant mobile ne fonctionnera pas tant que vous n'aurez pas approuvé la visite.
- Si vous avez défini une heure de départ prévue pour la visite, cette heure s'appliquera.

– Si vous n'avez pas défini d'heure de départ prévue, un nombre d'heures par défaut (8) s'appliquera. Les administrateurs peuvent modifier cette valeur par défaut dans le menu **Paramètres**.

Procédures d'approbation et de refus

Les visites peuvent être approuvées ou refusées de deux manières :

– Dans le tableau des visites du tableau de bord
– Dans l'éditeur de visite

Dans le tableau des visites du tableau de bord :

– **Approuver** : dans le tableau des visites, sélectionnez une ligne du tableau et cliquez sur  . Une fenêtre contextuelle de confirmation s'affiche, puis l'icône devient grise pour indiquer que la visite est approuvée.
– **Refuser** : dans le tableau des visites, sélectionnez une ligne du tableau et cliquez sur  . Une fenêtre contextuelle de confirmation s'affiche, puis l'icône **Approuver** redevient bleue pour indiquer que la visite doit encore être approuvée.

Dans l'éditeur de visite :

1. Dans le tableau de bord, dans le tableau des visites, sélectionnez une ligne du tableau et cliquez sur  pour modifier la visite.
2. Dans la boîte de dialogue **Données personnelles**, cliquez sur **Suivant**.
3. Dans la boîte de dialogue **Visites**, cliquez sur le bouton **Approuver** ou sur le bouton **Refuser**.
4. Confirmez votre action dans la fenêtre contextuelle.

6.3.5 Attribuer des informations d'identification physiques

Introduction

Attribuez une carte visiteur à chaque visiteur que vous autorisez à entrer dans les locaux. Vous pouvez attribuer plusieurs cartes à un même visiteur si nécessaire.

– L'heure d'**arrivée** d'une visite est l'heure de l'attribution de la première carte.
– L'heure de **sortie** d'une visite est l'heure de l'annulation de la dernière carte encore attribuée au visiteur.

Le réceptionniste peut facilement attribuer et annuler l'attribution de cartes à partir du tableau de bord, si un lecteur d'inscription de carte est connecté à l'ordinateur du réceptionniste.

L'éditeur de visite permet toutefois d'attribuer des numéros de carte si aucun lecteur n'est disponible.

Remarque!
Les personnes sur liste noire ne peuvent pas obtenir de cartes
Il n'est pas possible d'attribuer de cartes aux visiteurs figurant sur la liste noire. Supprimez le visiteur de la liste noire ou créez une exemption temporaire pour le visiteur avant d'essayer de lui attribuer une carte.

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

1. Permet de disposer d'une carte visiteur physique prête à être présentée au lecteur d'inscription.
2. Dans le tableau des visites, approuvez la visite. Voir *Approbation et refus de visites, page 50*
3. Sélectionnez la ligne de la visite et cliquez sur 
4. Suivez les instructions de la fenêtre contextuelle pour l'utilisation du lecteur d'inscription.

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.

Attribuer une carte dans l'éditeur de visite

1. Dans le tableau de bord, dans le tableau des visites, sélectionnez une ligne du tableau et cliquez sur  pour modifier cette visite.
2. Dans la boîte de dialogue **Données personnelles**, cliquez sur **Suivant**.
3. Dans la boîte de dialogue **Visites**, si la visite n'a pas encore été approuvée, cliquez sur **Approuver**.
4. Si vous disposez d'un lecteur d'enrôlement connecté, cliquez sur **Lire la carte** et suivez les instructions de la fenêtre contextuelle pour l'utilisation du lecteur d'inscription.

– Sinon, cliquez sur **Afficher les cartes disponibles** pour afficher la liste des cartes visiteur encore disponibles.
Si vous disposez de cartes physiques non triées avec des numéros imprimés, vous pouvez également sélectionner n'importe quelle carte et utiliser l'outil de **recherche** pour retrouver rapidement son numéro dans la liste.
– Cliquez sur  en regard d'un numéro de carte pour attribuer cette carte au visiteur actuel.
– Répétez les dernières étapes pour attribuer d'autres cartes, si nécessaire.

5. Cliquez sur **Enregistrer** pour enregistrer la visite en cours avec les attributions de la carte.

Annuler l'attribution d'une carte dans l'éditeur de visite

1. Dans le tableau de bord, dans le tableau des visites, sélectionnez une ligne du tableau et cliquez sur  pour modifier cette visite.
2. Dans la boîte de dialogue **Données personnelles**, cliquez sur **Suivant**.
3. Dans la boîte de dialogue **Visites**, dans le volet Cartes visiteur, 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.
4. Cliquez sur **Enregistrer** pour enregistrer la visite en cours avec les attributions de la carte.
5. Lorsque vous annulez l'attribution de la dernière carte attribuée au visiteur, le système enregistre cette date et cette heure comme heure de départ du visiteur.
   Dans le tableau des visites, le statut de cet enregistrement de visite devient 

Se reporter à

- *Configuration à l'aide du menu Paramètres, page 32*
- *Enregistrer des visites, page 49*
- *Approbation et refus de visites, page 50*

6.3.6 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

Il est possible d'attribuer des identifiants mobiles à partir de l'icône du tableau de bord directement ou à partir de la présentation de la page personnelle.

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 

Dans la présentation de la page personnelle :

1. Dans le **Tableau de bord**, sélectionnez le nom de la personne et la présentation de sa page personnelle s'ouvre.

2. Sélectionnez l'onglet **Informations d'identification** > **Ajouter un accès mobile.**

Suivez les instructions ci-dessous :

1. Sélectionnez l'une des grandes icônes pour les options :
– **Code QR**
ou
– **Mail d'invitation**
2. 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, page 50*
– Les fonctions de l'appareil mobile comme une carte d'accès physique, tant que l'application est en cours d'exécution
3. 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, page 50*
– 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 pour 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, page 50*
– 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, page 50*
– 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 19*
– *Installation d'applications Mobile Access, page 18*

6.3.7 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.

6.3.8 Enregistrement et départ sans carte

Introduction

Si les visiteurs sont accompagnés ou si seuls les espaces publics leur sont autorisés, il peut être inutile de les doter de cartes individuelles. Pour de tels cas, il existe une option permettant aux visiteurs de s'enregistrer et de quitter les lieux sans utiliser de carte. Pour des raisons de sécurité, cette option est désactivée par défaut.

Condition préalable.
Votre administrateur système doit avoir activé l'option spéciale **Enregistrement/Départ sans carte** dans la boîte de dialogue **Paramètres** > **Réceptionniste > Visites**. Voir le chapitre *Configuration à l'aide du menu Paramètres, page 32* pour obtenir des instructions.

Traiter
Lorsque cette option est activée :
– Tout visiteur qui s'auto-enregistre sur l'ordinateur kiosque approuve automatiquement la visite et s'enregistre en même temps.
– Le système fixe la date et l'heure d'arrivée au moment de l'enregistrement.
– Le bouton bascule **Enregistrement/Départ sans carte** apparaît dans l'éditeur de visite et dans le tableau de bord pour la même visite.

Procédure : enregistrement d'un visiteur sans carte
Si un visiteur ne peut pas s'enregistrer lui-même au kiosque mais doit s'enregistrer sans carte :
1. Enregistrez la visite manuellement, tel que décrit dans le chapitre *Enregistrer des visites, page 49*
2. Dans le tableau de bord, dans le tableau des visites, cliquez sur le nom du visiteur dans le tableau ou cliquez sur  pour modifier cette visite.
3. Dans la boîte de dialogue **Données personnelles**, cliquez sur **Suivant**.
4. Dans la boîte de dialogue **Visites**, dans le volet **Cartes visiteur**, cliquez sur **Enregistrement sans carte**

Procédure : départ d'un visiteur sans carte
Si un visiteur sans carte quitte les locaux :
1. Dans le tableau de bord, dans le tableau des visites, cliquez sur le nom du visiteur dans le tableau ou cliquez sur  pour modifier cette visite.
2. Dans la boîte de dialogue **Données personnelles**, cliquez sur **Suivant**.
3. Dans la boîte de dialogue **Visites**, dans le volet **Cartes visiteur**, cliquez sur **Départ sans carte**

Se reporter à
– *Enregistrer des visites, page 49*

6.3.9 Ajouter, supprimer ou exclure de la liste noire

Les visiteurs qui ne sont pas les bienvenus sur le site peuvent figurer sur une liste noire. Tant qu'un visiteur figure sur la liste noire, il est impossible d'attribuer une carte à cette personne. Vous pouvez retirer le visiteur de la liste noire à tout moment, ou lui accorder une dérogation temporaire, afin de lui attribuer une carte.

Liste noire

1. Dans le tableau de bord, dans le tableau des visites, sélectionnez une ligne du tableau et cliquez sur  pour modifier la visite.
2. Dans la boîte de dialogue **Données personnelles**, cliquez sur **Liste noire**.
3. Dans la fenêtre contextuelle, confirmez que vous souhaitez inscrire cette personne sur liste noire.
4. Dans la fenêtre contextuelle suivante, entrez le motif de son inscription sur liste noire, puis confirmez.

– Une bannière **Liste noire** apparaît dans l'éditeur de visite,

– Deux boutons apparaissent sous la bannière : l'un pour supprimer le visiteur de la liste noire, l'autre pour lui accorder une dérogation temporaire.
– Dans le tableau des visites, le nom de chaque visiteur sur liste noire apparaît avec un triangle d'avertissement. Par exemple : 

Supprimer et exempter

1. Dans le tableau de bord, dans le tableau des visites, sélectionnez une ligne du tableau où le visiteur est signalé figurer sur liste noire, puis cliquez sur  pour modifier la visite.
2. Dans la boîte de dialogue **Données personnelles**, cliquez sur l'une des options suivantes :

– **Supprimer** pour supprimer définitivement le visiteur de la liste noire.
– **Exempter** pour maintenir le visiteur sur liste noire mais autoriser l'attribution d'une carte pour cette visite uniquement.

3. Confirmez votre action dans la fenêtre contextuelle.

6.3.10 Gérer les profils des visiteurs

Le système conserve les profils des visiteurs jusqu'à ce que les réceptionnistes, les administrateurs ou les visiteurs eux-mêmes les suppriment.
Après une période de conservation définie dans les paramètres du système (valeur par défaut 12 mois), le système supprime les enregistrements de la visite.
Lorsqu'un visiteur ou un réceptionniste crée un nouveau profil visiteur, un code alphanumérique unique est attribué à ce profil. Les visiteurs peuvent se connecter avec ce code au kiosque des visiteurs, ce qui leur permet de gérer leurs propres profils.

Remarque!
Protégez les identifiants des visiteurs
Protégez soigneusement les identifiants des visiteurs contre tout accès non autorisé, car ils donnent accès à des données personnelles.

6.3.11 Afficher des enregistrements de visite

1. Dans le tableau de bord, dans le tableau des visites, sélectionnez une ligne du tableau et cliquez sur  pour modifier cette visite.
2. Dans la boîte de dialogue **Données personnelles**, cliquez sur **Suivant**.
3. Dans la boîte de dialogue **Visite en cours**, cliquez sur **Afficher toutes les visites**
   La boîte de dialogue **Visite en cours** affiche la liste des visites précédentes.

6.4 Hôte

Les hôtes sont les collaborateurs qui reçoivent les visites. Ils peuvent enregistrer leurs propres rendez-vous et parcourir le système pour obtenir des détails sur les visiteurs et les enregistrements de leurs visites passées, actuelles et futures.

6.4.1 Se connecter au rôle Hôte

1. Dans votre navigateur, ouvrez `https://`<Mon_serveur_VisMgmt>`:5706/main/` pour afficher l'écran de connexion.
2. Entrez le nom d'utilisateur d'un compte disposant des droits requis pour votre rôle. Consultez votre administrateur système si vous n'avez pas de compte.
3. Entrez le mot de passe.
4. Cliquez sur **Connexion**.

6.4.2 Recherche et filtrage

La barre d'outils du tableau de bord Hôte contient les fonctionnalités suivantes :

Étiquette	Fonction
1 N **entrées**	Le nombre total N de visites (chaque visite correspond à une ligne dans le tableau).
2 **Recherche**	Permet de recherche un texte quelconque parmi les visites du tableau
3	Affiche les visites les plus récemment ajoutées au tableau.
4	Ouvre une boîte de dialogue permettant de sélectionner les critères de filtre
5	Réinitialise le tableau à sa vue par défaut et rétablit tous les filtres.

Étiquette	Fonction
	Ouvre une boîte de dialogue pour créer une nouvelle entrée de visite dans le tableau

Recherche
Pour rechercher des noms et des hôtes, entrez du texte alphanumérique dans la zone de recherche, puis appuyez sur Entrée.

Filtrage
- Pour afficher les visites les plus proches de l'heure actuelle, cliquez sur **Dernières**
- Pour créer un filtre complexe à partir du statut de la visite, des dates d'arrivée et de départ et des numéros de carte, cliquez sur **Filtrer**.
  - Entrez les critères de filtre souhaités dans la boîte de dialogue contextuelle
  - Cliquez sur **Appliquer**
    Le système réduit le tableau des visites aux seuls rendez-vous de visite qui répondent aux critères du filtre.
- Pour supprimer tous les critères de filtre, cliquez sur **Réinitialiser**

6.4.3 Enregistrer des visites

Pour enregistrer un rendez-vous de visite d'un nouveau visiteur :
Dans le tableau de bord VisMgmt, dans la barre d'outils figurant au-dessus du tableau des visites.

1. Cliquez sur  pour ajouter une ligne au tableau des visites.
2. Dans la boîte de dialogue **Données personnelles**, dans la section **Informations générales**, entrez les données personnelles que votre site exige des visiteurs.
3. Dans la section **Détails de la visite**, entrez les détails requis, généralement les heures d'arrivée et de départ prévues, ainsi que le motif de la visite.
4. Cliquez sur **Enregistrer** pour enregistrer le rendez-vous visiteur.
   La visite apparaît dans le tableau de bord sous la forme d'une ligne dans le tableau des visites.

6.4.4 Copier des rendez-vous visiteur

Pour programmer un autre rendez-vous avec le même visiteur
1. Dans le tableau de bord VisMgmt, recherchez un rendez-vous existant avec le même visiteur dans le tableau des visites.
2. Cliquez sur l'icône  la plus petite à la fin de la ligne.
3. Dans la boîte de dialogue **Données personnelles**, dans la section **Détails de la visite**, entrez les détails requis, généralement les heures d'arrivée et de départ prévues, ainsi que le motif de la visite.

4. Cliquez sur **Enregistrer** pour enregistrer le rendez-vous visiteur.
   La visite apparaît dans le tableau de bord sous la forme d'une ligne dans le tableau des visites.

6.5 Visiteur

Les visiteurs peuvent utiliser le système en mode kiosque sur les lieux pour créer leurs propres profils de visiteurs et signer les documents requis avant de se rendre à la réception pour récupérer leurs cartes de visiteur.

6.5.1 Présentation du mode kiosque

Les visiteurs enregistrent généralement leurs visites et créent leurs propres profils sur un ordinateur librement accessible dans la zone d'accueil du site à accès contrôlé. Pour des raisons de sécurité, le navigateur Web de l'ordinateur s'exécute en mode kiosque, qui ne permet d'accéder qu'à VisMgmt, et non à plusieurs onglets, paramètres de navigateur ou système d'exploitation de l'ordinateur. Tous les navigateurs pris en charge disposent d'un mode kiosque, mais sa configuration exacte dépend du navigateur.
L'ordinateur kiosque exécute le module complémentaire **Bosch Peripheral Devices**, qui lui permet de se connecter physiquement à des périphériques pour numériser des documents d'identité et des signatures.

- L'URL du mode kiosque est `https://`<Mon_serveur_VisMgmt>`:5706`
- En revanche, l'URL de connexion en tant qu'Administrateur, Réceptionniste ou Hôte est `https://`<Mon_serveur_VisMgmt>`:5706/main/`

6.5.2 Création d'un profil visiteur : auto-enregistrement

Nouveaux visiteurs

Notez que la procédure exacte dépend des périphériques, tels que les scanners de documents et de signatures et les appareils photo, qui sont disponibles pour l'ordinateur kiosque.

1. Dans l'écran d'accueil de l'ordinateur kiosque, cliquez sur **Continuer sans identifiants visiteur**.
2. Dans l'écran suivant, cliquez sur **Auto-enregistrement**.
3. Dans l'écran suivant, sélectionnez **Numériser un document**.
4. Suivez les instructions à l'écran concernant les exigences spécifiques au site, telles que :

- la numérisation des documents d'identité,
- la signature de tout autre document légal requis,
- la capture de photographie.

5. Le système affiche les informations recueillies pour que vous puissiez les corriger et les compléter.
6. Le système vous demande si vous avez besoin d'autorisations d'accès spéciales et communique cette information à la réception, si nécessaire.
7. À la fin du processus d'enregistrement, l'écran affiche un identifiant de visiteur unique. Présentez cet identifiant à l'accueil pour recevoir votre carte de visiteur.

Remarque!
Votre identifiant de visiteur unique
Notez soigneusement votre identifiant de visiteur et protégez-le contre toute utilisation non autorisée. Il permet d'accéder à votre profil visiteur. Vous pouvez l'utiliser pour vous connecter à l'ordinateur kiosque et ainsi accélérer votre prochain enregistrement.

Visiteurs récurrents

1. Connectez-vous au kiosque avec votre identifiant de visiteur unique.
2. Le système affiche les informations recueillies pour que vous puissiez les corriger et les compléter, si nécessaire.
3. Présentez-vous à l'accueil pour récupérer votre carte visiteur.

6.6 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.

6.6.1 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.

6.7 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.

6.7.1 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 gamme 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 typiques 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).

hôte

Dans le contexte de la gestion des visiteurs, l'hôte est la personne qui reçoit le visiteur.

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.

Mode kiosque

Mode d'utilisation du navigateur très restreint qui autorise généralement l'accès à une seule application Web, et non aux paramètres du navigateur, à plusieurs onglets ou au système d'exploitation de l'ordinateur.

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
Pays-Bas
www.boschsecurity.fr

Des solutions pour les bâtiments au service d’une vie meilleure

202405131940