



## **Configuration et utilisation de la borne offline OSS**

## **Configuration et utilisation de la borne offline OSS**

## Table des matières

<b>1. Avertissement .....</b>	<b>6</b>
1.1. Réserve de propriété .....	6
<b>2. Configuration de la borne OSS .....</b>	<b>7</b>
2.1. Introduction .....	7
2.2. Configuration du mode de fonctionnement .....	9
2.2.1. Mode encodage .....	9
2.2.2. Mode mis à jour .....	10
2.2.3. Mode encodage+mise à jour .....	10
2.3. Connexion à l'interface web de la borne .....	12
2.3.1. Prérequis de connexion .....	12
2.3.2. Utilisateurs .....	12
2.3.3. Première connexion .....	14
2.4. Résumé des caractéristiques de la borne .....	15
2.5. Mise à l'heure manuelle de la borne .....	15
2.6. Mise à jour de la borne offline .....	16
2.7. Gestion des certificats .....	16
2.8. Paramétrage réseau .....	20
2.9. Sécurité .....	21
2.10. Configuration du contrôle d'accès offline .....	21

## Liste des illustrations

2.1. Borne Offline .....	8
--------------------------	---

## Liste des tableaux

2.1. Informations relatives à la borne offline .....	15
2.2. Types de certificats .....	17
2.3. Ajouter un certificat signé .....	18
2.4. Compatibilité TLS pour UTL .....	19
2.5. Système configuration .....	20
2.6. Apps configuration .....	20
2.7. Connexion à MICROSESAME .....	21
2.8. Offline parameters .....	22
2.9. Offline parameters .....	22
2.10. Encoding parameters .....	22

# Chapitre 1. Avertissement

## 1.1. Réserve de propriété

Les informations présentes dans ce document sont susceptibles d'être modifiées sans avertissement.

Les informations citées dans ce document à titre d'exemples, ne peuvent en aucun cas engager la responsabilité de TIL TECHNOLOGIES. Les sociétés, noms et données utilisés dans les exemples sont fictifs, sauf notification contraire.

Toutes les marques citées sont des marques déposées par leur propriétaire respectif.

Aucune partie de ce document ne peut être ni altérée, ni reproduite ou transmise sous quelque forme et quelque moyen que ce soit sans l'autorisation expresse de TIL TECHNOLOGIES.

Envoyez vos commentaires, corrections et suggestions concernant ce guide à [documentation@til-technologies.fr](mailto:documentation@til-technologies.fr)

## Chapitre 2. Configuration de la borne OSS

### 2.1. Introduction

**La borne offline OSS est un module électronique proposant plusieurs modes de fonctionnement :**

- **Mode encodage** : ce mode permet de préparer les badges sous le format attendu par le protocole OSS ( création de l'application, création des fichier, encodage de l'identifiant offline ... etc)
- **Mode mise à jour** : ce mode permet aux identifiés de mettre à jour les droits d'accès de leur badge OSS pour un temps défini, d'y inscrire la blacklist et de récupérer les alarmes/historiques
- **Mode encodage + mise à jour** : Pour les badges non encodés OSS, ce mode permet de préparer les badges sous le format attendu par le protocole OSS puis de mettre à jour automatiquement les droits offline associés à l'identifié. Pour un badge déjà encodé OSS, la borne passe directement à la mise à jour des accès et des données du badge.

**Figure 2.1. Borne Offline**

La borne offline fonctionne uniquement en mode paysage.

La borne est munie d'un serveur web permettant de configurer l'équipement ainsi que les fonctionnalités de contrôle d'accès offline. L'utilisateur connecté peut aussi effectuer des opérations de maintenance.

**Les pages du serveur web sont réparties entre 3 parties:**

- Maintenance
- Configuration
- System information

## 2.2. Configuration du mode de fonctionnement

### 2.2.1. Mode encodage

Le mode encodage permet de préparer les badges sous le format attendu par le protocole OSS ( création de l'application, création des fichiers, encodage de l'identifiant offline ... etc).

Ce dernier doit être réalisé avant la distribution des badges aux différents identifiés, il devra être suivi d'une étape de mise à jour des droits d'accès sur une borne en mode "mise à jour" ou sur un lecteur actualisateur par le détenteur du badge.

**Dans ce mode, deux types de fonctionnements sont possibles :**

- *UID copy* : l'identifiant qui sera utilisé pour le contrôle d'accès offline OSS sera la valeur de l'UID du badge.
- *CSV file* : l'identifiant qui sera utilisé pour le contrôle d'accès offline sera celui indiqué dans un fichier de format "\*.csv" qui sera à importer depuis l'interface web avant passage des badges sur la borne.

**Pour paramétrer la borne en mode encodage:**

1. Alimenter la borne
2. Ouvrir depuis le menu de paramétrage la section **Offline settings**
3. Activer la coche *Encoding mode*
4. sélectionner le type de fonctionnement voulu *UID copy* ou *CSV file*
5. Sortir du menu



Dans le cas où le type *UID copy* a été sélectionné, la borne est prête à encoder les badges afin de les mettre au format OSS.

**Dans le cas où le type *CSV file* a été sélectionné, il est nécessaire dans un premier temps, d'importer à partir du serveur web de la borne un fichier de type CSV (extension .csv) respectant le format suivant :**

- délimiteur ";"
- 1ère colonne : en entête "uid", cette colonne doit contenir pour chaque ligne l'uid du badge
- 2ème colonne : en entête "credentialID", cette colonne doit contenir pour chaque ligne l'identifiant utilisé pour l'Offline OSS

**Exemple :**

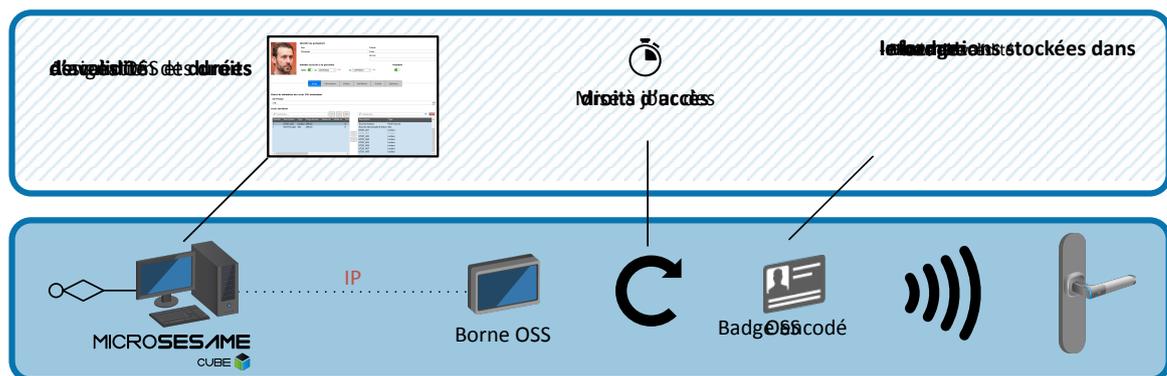
```
uid;credentialID
0444467afd5180;BB112233445566778899
7FED887AB4C56E;A589C56247252D5632D1
```

## 2.2.2. Mode mis à jour

Le mode "Mise à jour" permet de mettre à jour pour un temps défini les droits d'accès des badges étant déjà encodé dans le format OSS, d'écrire la blacklist ou encore récupérer les historiques/ alarmes présents dans les badges.

### Pour configurer la borne en mode Mise à jour :

1. Alimenter la borne
2. Ouvrir depuis le menu de paramétrage la section **Offline settings**
3. Désactiver la coche *Encoding mode*
4. Sortir du menu



## 2.2.3. Mode encodage+mise à jour

**En fonction du type de badge présenté devant le lecteur de la borne, ce mode procède de deux manières distinctes pour traiter les données OSS dans le badge :**

- **Le badge n'est pas encodé OSS :** La borne encode automatiquement le badge pour qu'il puisse fonctionner sur les équipements OSS présents sur le site. Une fois le badge préparé, la borne met automatiquement à jour les droits d'accès offline associés à l'identifié.
- **Le badge est déjà encodé OSS :** La borne détecte que le badge est déjà encodé OSS, le terminal passe directement à la mise à jour des droits offline associés à l'identifié.



Les paramètres d'encodage OSS sont définis par l'intégrateur sur le serveur web de la borne, pour plus d'informations se référer à la section [Section 2.10, « Configuration du contrôle d'accès offline »](#).



Sur une installation, ce mode permet de gérer tous les types de badges grâce à une seule et même borne sans rajouter d'étape intermédiaires lors de la remise d'un badge à un nouvel identifié.

### Dans ce mode, deux type de fonctionnements sont possible :

- *UID copy* : l'identifiant qui sera utilisé pour le contrôle d'accès offline OSS sera la valeur de l'UID du badge.
- *CSV file* : l'identifiant qui sera utilisé pour le contrôle d'accès offline sera celui indiqué dans un fichier de format "\*.csv" qui sera à importer depuis l'interface web avant passage des badges sur la borne.

### Pour paramétrer la borne en mode encodage+mise à jour:

1. Alimenter la borne
2. Ouvrir depuis le menu de paramétrage la section **Offline settings**
3. Activer la coche *Encoding mode*
4. Cocher *Update badge after encoding*
5. sélectionner le type de fonctionnement souhaité *UID copy* ou *CSV file*
6. Sortir du menu



Dans le cas où le type *UID copy* a été sélectionné, la borne est prête à encoder les badges afin de les mettre au format OSS.

### Dans le cas où le type *CSV file* a été sélectionné, il est nécessaire dans un premier temps, d'importer à partir du serveur web de la borne un fichier de type CSV (extension .csv) respectant le format suivant :

- délimiteur ";"
- 1ère colonne : en entête "uid", cette colonne doit contenir pour chaque ligne l'uid du badge
- 2ème colonne : en entête "credentialID", cette colonne doit contenir pour chaque ligne l'identifiant utilisé pour l'Offline OSS



Le chargement du fichier CSV de correspondance identifiants/UID se charge directement sur le serveur web de la borne.

### Suivre la procédure suivante pour ajouter un fichier CSV :

1. Se rendre sur le server web de la borne et s'authentifier

2. Suivre **Configuration > Access control**
3. Dans la partie *Encoding parameters* localiser *CredentialID CSV File Upload*
4. Cliquer sur **parcourir**, sélectionner le fichier CSV puis cliquer sur **upload**

**Exemple :**

```
uid;credentialID
0444467afd5180;BB112233445566778899
7FED887AB4C56E;A589C56247252D5632D1
```

## 2.3. Connexion à l'interface web de la borne

### 2.3.1. Prérequis de connexion

La connexion au serveur web de la borne nécessite de vérifier les prérequis ci-dessous :

Prérequis	Détails
Compatibilité IP	Un PC avec la configuration suivante est nécessaire :  Une adresse IP et masque de sous réseau compatible avec l'adresse IP d'usine de la borne (172.16.5.240) : <ul style="list-style-type: none"> <li>● adresse IP commençant par 172.16.x.x (exemple : 172.16.5.240)</li> <li>● masque de sous réseau en 255.255.0.0</li> </ul>
Compatibilité navigateur	Un navigateur à jour sur le PC (Internet Explorer en version 9 ou supérieur, Firefox).

### 2.3.2. Utilisateurs

Afin de répondre aux différents besoins et responsabilités des acteurs de la sécurité de l'installation, la borne gère 3 niveaux de connexion. Par ordre croissant de responsabilités ces 3 niveaux sont les suivants :

Niveau de login	Gestion certificats	Modif. Config. réseau	Modif. Config. générale	Visu. Config. site	Visu. Config. de base	Modif. de son propre mot de passe	Login et mot de passe par défaut
<b>Utilisateur</b>	NON	NON	NON	NON	<b>OUI</b>	<b>OUI</b>	Login : user  Password : user

Niveau de login	Gestion certificats	Modif. Config. réseau	Modif. Config. générale	Visu. Config. site	Visu. Config. de base	Modif. de son propre mot de passe	Login et mot de passe par défaut
Installateur	NON	NON	OUI	OUI	OUI	OUI	Login : service Password : service
Administrateur	OUI	OUI	OUI	OUI	OUI	OUI	Login : admin Password : admin

 L'information de connexion avec un niveau Administrateur est systématiquement tracé dans les logs de la TILLYS et le cas échéant, transmise au serveur MICROSESAME.

**Une fois connecté, l'administrateur peut modifier les règles de définition des mots de passe pour tous les utilisateurs :**

- Longueur des mots de passe
- Caractères spéciaux
- Majuscule
- Caractère numérique



Seul l'administrateur peut modifier les règles de définition de mots de passe.

**Suivre la procédure ci-dessous pour modifier le mot de passe du compte utilisateur:**

1. Se connecter au serveur web avec le compte utilisateur concerné.
2. Dans la partie droite du bandeau supérieur, cliquer sur l'espace correspondant au nom de l'utilisateur :
  - Administrator
  - Service
  - User

3. Renseigner l'ancien de mot de passe
4. Renseigner le nouveau mot de passe puis confirmer le en le renseignant une nouvelle fois
5. Cliquer sur submit



Chaque utilisateur est responsable de la définition de son mot de passe.

### 2.3.3. Première connexion

Une borne sortie d'usine possède des paramètres réseaux par défaut tel que son adresse IP (par défaut 172.16.5.240). Lors de la première connexion au serveur web d'une borne il est donc nécessaire de vérifier qu'aucun autre équipement sorti d'usine de ce type est raccordé sur le réseau.



Pour des raisons de facilité, lorsque la configuration IP d'une borne est encore celle par défaut, il est conseillé de connecter la borne en direct sur le PC.



Une fois connecté au serveur Web de la borne il est obligatoire de modifier l'adresse IP en veillant à ce que celle-ci soit accessible sur le réseau.

Pour ce faire, se rendre sur la page **Configuration > Network**.

Lors de la première connexion, il est obligatoire de se connecter avec le compte **Admin** (Login et mot de passe par défaut).

#### **Une fois connecté, la borne demandera automatiquement de modifier le mot de passe des utilisateurs suivants :**

- Admin
- System (root)

Cette opération est obligatoire, **aucune** configuration ne peut être effectuée avant d'avoir mis à jour les informations de connexion de ces utilisateurs.



Il est impossible de se connecter avec l'utilisateur système directement sur la borne. Il est nécessaire d'utiliser un outil tiers en connexion SSH.



**Attention:** Le remplacement du mot de passe System est une opération définitive:

- Il ne pourra plus être modifié par la suite.
- Il ne pourra pas être récupéré par le biais du support technique (SAV) Til technologies.

Une procédure similaire sera requise lors de la première connexion des utilisateurs suivants:

- Service
- User

## 2.4. Résumé des caractéristiques de la borne

C'est la page d'accueil du serveur web de la borne, elle est aussi accessible depuis l'onglet **System Information > Overview**.

**Tableau 2.1. Informations relatives à la borne offline**

Section	Paramètres	Détails
Serial Number and versions	Binaries version	Version du firmware de la borne
	OS version	Version du système d'exploitation de la borne
	Serial number	Numéro de série de la borne
Security summary	Binaries Version	Version firmware de la borne
	HTTPS	Etat d'activation connexion HTTPS sécurisée
	MICROSESAME	Mode de communication avec MICROSESAME
NEtwork	IP	Adresse IP de la borne
	MAC address	Adresse MAC de la borne
Hardware information	Power	Tension d'alimentation actuelle du module
	RAM	Capacité mémoire RAM
	Processor cores	Nombre de cœurs physiques dans le processeur
	CPU température	Température du CPU
	Hardware revision	Version de la révision du cuivre

## 2.5. Mise à l'heure manuelle de la borne

Cette page permet de régler manuellement l'heure et la date de la borne, elle est accessible depuis l'onglet **Maintenance > Date & Time**.

L'heure et la date sont mises à jour automatiquement au téléchargement depuis MICROSESAME.



Une fois l'heure et la date configurées, cliquer sur **submit** pour appliquer le paramétrage.

La mise à l'heure manuelle de la borne peut être utile pour une mise en service ou des opérations de maintenance.

## 2.6. Mise à jour de la borne offline

Cette page permet de mettre à jour la borne directement depuis le serveur web, elle accessible dans l'onglet **Maintenance > Firmware upload**.



Les derniers firmware pour produits TIL sont disponibles sur le site **support.til-technologies.fr** rubrique **Téléchargements**.



Le nom du firmware doit obligatoirement être de type **update\_borne.img** pour être accepté.

### Suivre la procédure ci-dessous pour mettre à jour la borne :

1. Se connecter au serveur web de la borne et se rendre dans la page **Maintenance > Firmware upload**
2. Sélectionner le fichier de mise à jour en cliquant sur le bouton d'exploration **Browse**
3. Une fois le fichier sélectionné, cliquer sur **Upload and flash firmware**
4. Attendre la fin de la mise à jour puis vérifier que la nouvelle version a correctement été installée en se rendant sur la page **System information > Overview**



En cas d'erreur lors de la mise à jour, consulter les logs pour obtenir des informations sur la résolution du problème.

## 2.7. Gestion des certificats

Cette page est accessible depuis **Configuration > Certificates**, elle permet d'effectuer les opérations suivantes:

- Générer des certificats auto-signés
- Générer des CSR (Certificate Signing Request) ou demande de signature de certificat
- Importer des certificats signés
- Importer des certificats d'autorités racines ou intermédiaires



Les certificats sont nécessaires pour la communication avec MICROSESAME via liaison TLS ou encore pour une communication HTTPS avec le serveur web de la borne. Par défaut, un certificat auto-signé est généré au démarrage du clavier.

### Tableau 2.2. Types de certificats

Types de certificats	Détails
Auto-signés	<p>Les certificats Autosignés sont générés et signés par la borne elle-même, ce type de certificats permet d'initialiser une liaison TLS mais ne garantit pas l'identité de l'interlocuteur lors d'une communication.</p> <p> Il n'est pas conseillé d'utiliser ce type de certificat sur un site en exploitation.</p>
Signés	<p><b>Les certificats signés sont générés en plusieurs étapes :</b></p> <ol style="list-style-type: none"> <li>1. L'intéressé génère un CSR (Certificate Signing Request) ou requête de signature de certificats</li> <li>2. Il transfère cette requête à une autorité de confiance qui pourra garantir l'identité de l'intéressé</li> <li>3. Cette dernière renvoie alors un certificat signé ainsi que son propre certificat (certificat d'autorité de certification)</li> </ol>
Certificat d'autorité de certification	L'import du certificat de l'autorité de certification ayant signé le certificat de l'intéressé permet de le stocker dans une banque de certificats racines acceptés.

### Suivre la procédure suivante pour Générer un certificat autosigné pour la borne :

1. Cliquer sur le bouton **generate self-signed**
2. Remplir les informations demandées
  - **Nom** : nom qui sera donné au fichier généré
  - **Country** : Sélectionner le pays

- **State** : Correspond à l'état/Région/Département
- **City** : Correspond à la ville
- **Organization** : Correspond à l'entreprise
- **Unit** : Correspond au service
- **Common name** : Correspond à l'adresse IP de la borne ou à son nom d'hôte (host name)
- **Days before expiration** : Correspond au nombre de jours de validité du certificat

Une fois les informations validées, Une ligne se crée dans le tableau se trouvant dans la partie **Self-signed certificates** de la page HTML. Dans la première colonne on retrouve le nom du fichier que l'on a configuré et dans la deuxième colonne la valeur *Not available yet*.

3. Attendre environ 30 secondes pour que le certificat puisse se générer puis rafraîchir la page. Lorsque les colonnes *Issued on* et *Expires on* sont remplies, le certificat est prêt à être utilisé, dans le cas contraire répéter cette étape.



Le certificat est maintenant prêt à être utilisé soit dans le paramétrage pour la sécurisation de la page web https (Configuration / Security) soit pour le paramétrage de la sécurisation de la communication TCP (Configuration / Network).

Une fois le certificat utilisé par une des deux fonctions, la colonne **usage** du tableau sera renseigné.

Une fois que le requête CSR ait été généré, il est nécessaire de faire signer ce fichier par un organisme d'autorité de certification. Généralement cette étape est réalisé par le RSSI du site.

### Tableau 2.3. Ajouter un certificat signé

Etape	Details
Génération du CSR	<p><b>Suivre la procédure suivante pour ajouter un certificat signé :</b></p> <ol style="list-style-type: none"> <li>1. Cliquer sur le bouton <b>Generate CSR</b></li> <li>2. Remplir les informations demandées : <ul style="list-style-type: none"> <li>● <b>Nom</b> : nom qui sera donné au fichier généré</li> <li>● <b>Country</b> : Sélectionner le pays</li> <li>● <b>State</b> : Correspond à l'état/Région/Département</li> <li>● <b>City</b> : Correspond à la ville</li> <li>● <b>Organization</b> : Correspond à l'entreprise</li> <li>● <b>Unit</b> : Correspond au service</li> <li>● <b>Common name</b> : Correspond à l'adresse IP de la TILLYS ou à son nom d'hôte (host name)</li> </ul> </li> </ol> <p>Une fois les informations validées, Une ligne se crée dans le tableau se trouvant dans la partie <b>Certificate Signature request (CSR)</b> de la page HTML.</p> <ol style="list-style-type: none"> <li>3. Attendre environ 30 secondes pour que le certificat puisse se générer puis rafraîchir la page. lorsque la valeur <i>Not available yet</i> a disparu,</li> </ol>

Etape	Details
	<p>cliquer sur le bouton <b>Download</b> pour télécharger le fichier CSR, indiquer l'emplacement du fichier et valider.</p>
Signature du CSR	<p>Le RSSI du site transfère la requête CSR à une autorité de certification pour qu'elle la signe.</p> <p><b>Cette dernière renvoie les éléments suivants :</b></p> <ul style="list-style-type: none"> <li>• Le certificat signé</li> <li>• Son propre certificat ou alors la <b>chaîne de certification</b> si il s'agit d'une autorité itnermédiaire.</li> </ul>
Ajout du certificat signé	<p><b>Se rendre dans la page Configuration &gt; Certificates :</b></p> <ol style="list-style-type: none"> <li>1. Dans la partie Certificate Signature Request, sélectionner le <b>CSR</b></li> <li>2. Cliquer sur <b>Parcourir</b> puis sélectionner le certificat signé correspondant</li> <li>3. Cliquer sur <b>Replace CSR</b></li> </ol> <p> Le nom du fichier du certificat signé doit obligatoirement avoir le même nom que la requête CSR</p>
Ajout du certificat de l'autorité de certification ou chaîne de certification	<p><b>Se rendre dans la page Configuration &gt; Certificates :</b></p> <ol style="list-style-type: none"> <li>1. Dans la partie CA certificates, sélectionner le <b>CSR</b></li> <li>2. Cliquer sur <b>Parcourir</b> puis sélectionner le certificat signé correspondant</li> <li>3. Cliquer sur <b>Upload</b></li> </ol> <p> Dans le cas d'une chaîne de certification il est nécessaire d'importer tous les certificats</p>

**Tableau 2.4. Compatibilité TLS pour UTL**

Types de clés	Détails
RSA	<p><b>Types de clés validés:</b></p> <ul style="list-style-type: none"> <li>• 4096 bits</li> </ul>
ECDSA	<p><b>Courbes elliptiques validées:</b></p> <ul style="list-style-type: none"> <li>• Courbe elliptique secp384r1</li> </ul>

Types de clés	Détails
	<p><b>Courbe elliptiques acceptées (en théorie):</b></p> <ul style="list-style-type: none"> <li>• secp521r1</li> <li>• brainpoolP256r1</li> <li>• brainpoolP384r1</li> <li>• brainpoolP512r1</li> </ul>

## 2.8. Paramétrage réseau

Cette page permet de configurer les paramètres réseau de la borne offline. Pour y accéder, suivre **Configuration > Network**.

**Tableau 2.5. Système configuration**

Paramètres	Détails
Hostname	Nom de la borne sur le réseau
IP address	Adresse IP de la borne
Subnet mask	<p>Masque de sous réseau</p> <p> Il est conseillé de ne pas modifier ce paramètre par défaut car un masque de sous réseau non adapté rendrait la borne inaccessible sur le réseau.</p>
Gateway	Cette option est à configurer uniquement si le module doit pouvoir communiquer avec d'autres réseaux que le réseau local.

**Tableau 2.6. Apps configuration**

Paramètres	Détails
Certificate	Sélectionner le certificat à utiliser pour le téléchargement depuis MICROSESAME
TCP download port	<p>Modifier si besoin le port de communication, dédié au téléchargement de la configuration et des accès depuis MICROSESAME</p> <p>La valeur proposée par défaut est 20300.</p>



Cliquer sur **Submit** pour appliquer la configuration.

## 2.9. Sécurité

Cette page permet de paramétrer la connexion HTTPS au serveur web de la borne. Pour y accéder suivre **Configuration > Security**.

Dans la partie HTTPS, sélectionner dans la liste déroulante le certificat à utiliser pour la connexion HTTPS au serveur web de la borne.



Le certificat doit préalablement avoir été généré ou ajouté dans la partie **Configuration > Certificates**.

## 2.10. Configuration du contrôle d'accès offline

Cette page permet de configurer les paramètres relatifs a au contrôle d'accès offline. Pour y accéder suivre **Configuration > Access Control**.

Dans la partie General, l'opérateur pourra retrouver le nom de la borne offlien tel qu'il est renseigné dans la configuration MICROSESAME. Par défaut le nom de la borne est **Borne offline**.



Le nom ne peut être édité directement depuis le serveur web de la borne.

**Tableau 2.7. Connexion à MICROSESAME**

Paramètres	Détails
MICROSESAME IP address	Renseigner l'adresse IP du serveur MICROSEAME
Communication state	Après avoir renseigné l'adresse IP du serveur MICROSESAME, il est possible d'utiliser ce champ pour tester la validité de la connexion .



La configuration ci-dessous ne doit pas être modifiée après qu'un identifiant ait été passé sur la borne.

**Tableau 2.8. Offline parameters**

Paramètres	Détails
Offline application ID (HEXA format)	<p>Ce paramètre correspond à l'identifiant de l'application présente dans le badge et contenant les données offline.</p> <p> Ce paramètre peut être renseigné directement depuis cette page ou télécharger depuis MICROSESAME.</p>
Site ID	<p>Ce paramètre correspond à l'ID site encodés dans les badges OSS. Il est nécessaire que l'ID du site corresponde pour que l'identifié puisse mettre à jour ses droits sur la borne.</p> <p> Ce paramètre peut être renseigné directement depuis cette page ou télécharger depuis MICROSESAME.</p>



Les paramètres listés ci-dessous doivent être renseignés depuis le serveur web de la borne et ne peuvent être téléchargés depuis MICROSESAME.

**Tableau 2.9. Offline parameters**

Paramètres	Détails
Offline keys	<p>Ce paramètre correspond aux clés de lecture/écriture de données du badge.</p>

**Tableau 2.10. Encoding parameters**

Paramètres	Détails
Max doors	<p>Ce paramètre correspond au nombre maximum d'accès à une porte ou groupe de portes que pourra contenir un badge</p>
Max Schedule	<p>Ce paramètre correspond au nombre maximum de plage horaire que pourra contenir un badge</p> <p>Il est possible de paramétrer 15 Plages horaires au maximum</p>

Paramètres	Détails
Max Day ID	Ce paramètre correspond au nombre maximum que pourra contenir une plage horaire OSS
Max Timeperiod	Ce paramètre correspond au nombre de créneaux que peut contenir un groupe de jours
Max events	Ce paramètre correspond au nombre maximum d'évènements (historique/alarmes) que peut contenir un badge OSS
Max Blacklist	<p>Ce paramètre correspond au nombre maximum d'identifiants que peut contenir la Blacklist présente dans le badge.</p> <p>La Blacklist est une liste contenant les identifiants de badges OSS qui devront être refusé lorsque ces derniers seront présentés sur une serrure.</p> <p>Cette liste est écrite dans les badges utilisateurs lorsqu'ils sont présentés sur la borne, puis est descendue dans les serrures lors du passage du badge sur ces dernières.</p>



1. Chacun de ces paramètre impacte la taille que l'application prendra dans le badge. Une fois le badge encodé, il ne sera plus possible de modifier la taille de l'application.
2. Cliquer sur **Submit** pour appliquer la configuration