# Guide de configuration et de mise en place d'un système Offline OSS

FR 1.19

2023 - 06 - 15

# TABLE DES MATIÈRES

# Chapitre 1. Présentation et prérequis pour un système offline OSS

## 1.1. Fonctionnement général

L'OSS est un standard dans le domaine du contrôle d'accès "offline" (lecteurs autonome) permettant de s'interfacer avec de nombreux équipements mécatroniques provenant de divers constructeurs ( ASSA ABLOY, DEISTER, Uhlmann & Zacher, DORMA KABA, Zugang GmBH...etc)

***Un système offline est composé au minimum :***

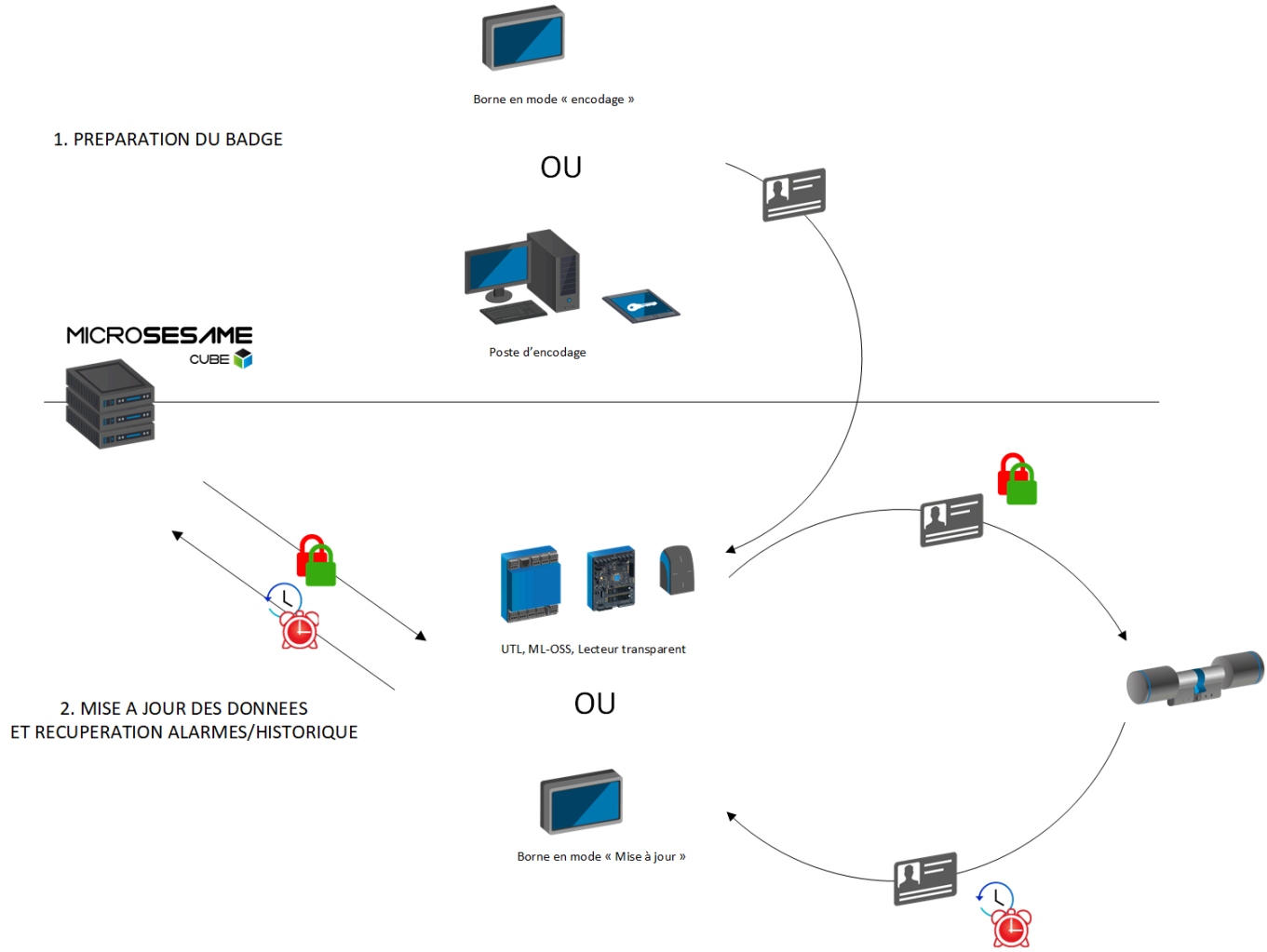
- d'un logiciel de gestion des droits accès
- d'un ou plusieurs lecteurs autonome ( i.e. Les lecteurs prennent eux même la décision d'ouverture/fermeture sans nécessité d'être câblé à d'autres modules)
- d'un équipement (matériel ou logiciel ) de mise à jour des droits de badge
- d'un ou plusieurs badges

Les droits d'accès au(x) lecteur(s) autonome sont distribués depuis le logiciel de gestion de droits d'accès, puis sont téléchargés dans l'équipement de mise à jour des droits du badge. Lorsque le badge est présenté sur l'équipement de mise à jour, les droits d'accès aux serrures autonome sont inscrits dans ce dernier pour une durée limitée. Enfin lorsque le badge est présenté sur la serrure, cette dernière prend la décision d'ouverture en fonction des droits inscrits dans le badge, puis, inscrit l'historique et les alarmes dans le badge qui seront récupérés au prochain passage du badge sur l'équipement de mise à jour des droits.

Le système offline OSS avec les produits TIL TECHNOLOGIES fonctionne en suivant les étapes ci-dessous :

***Le système offline OSS avec les produits TIL TECHNOLOGIES fonctionne en suivant les étapes ci-dessous :***

1. Préparation du badge pour le rendre compatible au format OSS offline :
   - Soit encodé directement par une borne configurée en mode "encodage"
   - Soit par l'application "encodage JS" de MICRO-SESAME pour un format de badge avancé (exemple : badge non vierge avec CMK personnalisée .. etc)
2. Configuration des droits avec MICRO-SESAME, puis mise à jour des données offline dans le badge et récupération des historiques alarmes :
   - Soit par une borne offline configurée en mode "mise à jour"
   - Soit par le contrôle d'accès online classique via l'UTL associé à un ML-OSS et un lecteur transparent




## 1.2. Prérequis

***Pour pouvoir utiliser le système OSS Offline avec les produits de TIL TECHNOLOGIES il est nécessaire de respecter les prérequis suivants :***

- Utiliser des badges de type DESFIRE
- Utiliser une version MICRO-SESAME 2021.4.X ou supérieure
- Avoir dans les licences MICRO-SESAME l'élément **LIC-LOCKS** comportant une valeur de serrures mécatronique égale ou supérieure au nombre de serrures qui seront utilisé.
- Dans le cas où le ML-OSS est utilisé, avoir une UTL dont la version est supérieure ou égale à la version 5.6.0

Avant exploitation, la mise en place d'un système OSS offline nécessite la configuration des différents produits qui le compose. La modification de la valeur de certains de ces éléments après une première utilisation peut s'avérer complexe (nécessité de formatage du badge, re-configuration des serrures ... etc) .

C'est pour cela qu'il est fortement recommandé avant toute configuration et mise en place des produits de réaliser en amont les actions suivantes :

| Etapes | Détails |
|---|---|
| Se renseigner sur l'état actuel du badge | badge vierge ou déjà encodé par d'autres applications ? |
| | taille du badge |
| | vérifier la place restante dans le cas d'un badge déjà encodé pour d'autres applications |
| Définir les valeurs des éléments suivants en fonction de la place disponible dans le badge<br><br>*Il est possible de voir la valeur de la taille qui sera occupé par l'application offline en fonction de ses éléments depuis le serveur web de paramétrage d'une borne offline (voir chapitre "XXX")* | nombre maximum de serrures autonome qui seront installé sur le site |
| | nombre maximum d'historique/alarmes qui pourront être inscrit dans le badge |
| | nombre maximum de numéros de badge qui pourront être inscrits dans la blacklist |
| | nombre maximum et définition des plages horaires qui seront utilisées pour les accès offline<br>(voir le chapitre "XXXX" pour plus de renseignements sur les limitations des plages horaires) |
| Définir pour chaque serrure :<br><br>*Il est conseillé d'établir un fichier comportant les différentes informations afin d'avoir un suivi rigoureux sur l'installation. Ce fichier pourra être ensuite importé dans le logiciel MICRO-SESAME afin d'effectuer un paramétrage automatique en fonction des informations qui auront été indiqué dans le fichier (pour plus de renseignements sur le format du fichier attendu, voir le chapitre "importer une configuration")* | l'id qui sera associé |
| | les groupes d'appartenance |
| Définir une valeur pour les éléments qui devront être paramétrés | clé lecture/écriture utilisée pour l'application offline (32 caractères hexadécimal) |
| | Numéro de l'application qui sera créé dans le badge (6 caractères hexadécimal) |
| | Numéro code site ( valeur max : XXX ) |

# Chapitre 2. Configuration MICRO-SESAME

## 2.1. Activer et configurer la ligne OSS

Il est nécessaire d'activer la ligne OSS offline afin de rendre visible les paramètres liés à cette fonctionnalités dans les applications d'exploitation :

- Définition d'une plage horaire OSS
- Assigner les accès OSS dans la fiche d'un identifié
- ...

*Depuis le menu principal, suivre **Paramétrage > matériel > Architecture matériel**.*

***Suivre la procédure suivante pour activer la ligne OSS :***

1. Dans la table Architecture matériel située dans la partie gauche de la fenêtre, localiser la catégorie **OSS offline**
2. Cliquer sur le ligne correspondant à l'OSS offline pour afficher le paramétrage général
3. Cocher la case **Activation de la ligne OSS offline**
4. Sélectionner la **technologie associée aux bornes OSS**.

*La technologie associée aux bornes OSS concerne la lecture des identifiants OSS encodés dans l'application dédiée. Cette technologie est commune à toutes les bornes de tous les sites gérées par le serveur MICRO-SESAME.*

*Une fois la ligne OSS activée, il est nécessaire de configurer les identifiants et les durées de validité des accès.*

*Ces paramètres sont définis pour chaque site **avant** la mise en exploitation des bornes OSS.*

*La modification de ce paramétrage sur un site en exploitation nécessite de ré-encoder les badges afin de pouvoir continuer à utiliser les lecteurs autonomes.*

***Suivre la procédure suivante pour configurer les identifiants et les durées de validité distribuables par site :***

1. Dans la catégorie OSS offline, cliquer sur la ligne correspondant au site à paramétrer.
2. Renseigner le code site choisi pour l'installation lors d l'encodage des badges OSS.
3. Paramétrer les durées de validité et cocher la case associée pour qu'elles puissent être distribuées lors de l'assignation d'un accès OSS dans la fiche identifiée.

*La Durée de validité assignée **Jusqu'à** une certaine heure répond au fonctionnel suivant :*

1. *L'identifié actualise ses droits sur une borne ou un lecteur actualisateur.*
2. *Ses droits sont valides ce jour jusqu'à l'heure paramétrée*
3. *Passé cette heure, ses droits ne sont plus valides et l'identifié doit attendre le jour suivant avant d'actualiser de nouveau ses droits.*

*Si l'identifié actualise ses droits après l'heure de fin de validité, ils seront valables pour le jour suivant.*

*Il est fortement conseillé de ne pas distribuer d'accès avec une durée de validité trop élevée pour éviter, en cas de perte / vol du badge, qu'un individu non autorisé puisse accéder au site pendant une durée étendue.*

*La longueur de l'identifiant n'est pas modifiable et est donnée à titre indicatif.*

*L'identifiant est générer lors de l'encodage des badges OSS avec le scripts fournis dans MICRO-SESAME.*

***Dans le cas ou l'encodage des badges serait effectué avec un script personnalisé, il est nécessaire de conserver le format suivant :***

- *DECIMAL*
- *20 caractères*
- *Remplissage à gauche (si l'identifiant fait moins de 20 caractères, remplir avec des 0 à gauche)*

## 2.2. Ajouter et configurer une borne OSS

Une borne OSS a deux modes de fonctionnement :

- Une borne en mode "encodage" : permet de préparer le badge dans le format attendu par le fonctionnement d'un système OSS (création de l'application, fichiers de données... etc)
- Une borne en mode "mise à jour" : permet de mettre à jour les droits d'accès OSS pour une période définie, d'écrire la blacklist et de récupérer les alarmes/historiques d'un badge.

*Le mode de fonctionnement d'une borne se configure depuis le serveur web de cette dernière.*

*Depuis le menu principal, suivre **Paramétrage > matériel > Architecture matériel**.*

***Suivre la procédure suivante pour ajouter et configurer une borne OSS :***

1. Dans la table Architecture matériel située dans la partie gauche de la fenêtre, localiser la catégorie **OSS offline**
2. Dans la catégorie **OSS offline**, effectuer un clic-droit sur la ligne correspondant au **site d'appartenance**
3. Dans le menu contextuel, sélectionner **Ajouter une borne**
4. Une nouvelle borne apparaît dans la table, cliquer sur la ligne correspondante.
5. Cocher la case **Activé** pour activer la borne
6. Sélectionner le mode d'adressage IP ( **IP fixe** ou **DHCP**)
7. Renseigner l'information de connexion associée (**Adresse IP** ou **Nom d'hôte**)
8. Modifier si besoin le port de communication proposé
9. Personnaliser le nom de la borne en double cliquant dessus.

*Double cliquer sur une borne dans la table située dans la partie gauche de la fenêtre pour renommer l'élément.*

*Si le port de communication est modifié (par défaut 20300), il est nécessaire de faire de même dans l'UTL. Pour cela, se reporter à la documentation **Aide en ligne TILLYS CUBE** pour connaître la procédure de connexion à son serveur web.*

## 2.3. Déclarer un lecteur actualisateur

Un lecteur actualisateur est un lecteur utilisé pour le contrôle d'accès online et aussi pour le contrôle d'accès offline OSS.

*Le lecteur actualisateur doit être un lecteur transparent SSCPv2 ou SSCPv1.*

Ce dernier doit être câblé sur un "MLP-OSS" et permet :

- de mettre à jour les droits d'accès offline OSS du badge pour une période définie, d'écrire la blacklist et de récupérer les historiques/alarmes
- de lire l'identifiant du badge utilisé pour le contrôle d'accès online

*Il est nécessaire d'avoir activé la ligne OSS afin de voir le paramétrage OSS dans les applications MICRO-SESAME.*

*Depuis le menu-principal, suivre **Paramétrage > matériel > lecteur**.*

*L'interface de paramétrage est aussi accessible depuis l'onglet **Contrôle d'accès** de la fiche d'une UTL ( **Paramétrage > matériel > UTL (unité de traitement logique)**).*

***Suivre la procédure suivante pour déclarer un lecteur actualisateur :***

1. Créer un nouveau lecteur ou sélectionner le lecteur à paramétrer
2. Depuis la fenêtre de configuration du lecteur ou directement dans la liste des lecteurs cliquer sur le bouton à bascule correspondant à la colonne **Actualisateur OSS**.
3. Vérifier que le lecteur est **activé** et possède une **licence**
4. Se rendre dans l'interface de configuration OSS ( **Paramétrage > matériel > Architecture matériel**)
5. Dans la catégorie **OSS offline** cliquer sur **lecteurs actualisateurs**
6. Vérifier que le lecteur paramétré soit présent dans la table et soit activé.

*Il est impossible de définir un lecteur simultanément en tant que lecteur APERIO et lecteur actualisateur.*

## 2.4. Ajouter et configurer un lecteur OSS Offline

Un lecteur autonome OSS offline correspond à une serrure, un cylindre ou une poignée encastrée dans une porte et capable d'autoriser ou refuser le passage à un identifié lors d'un passage d'un badge.

Ces lecteurs ne peuvent être téléchargés ou supervisés en direct depuis MICRO-SESAME, ils sont **autonomes** sur site et répondent à un fonctionnel particulier.

Le standard OSS permet de s'interfacer avec un grand nombre d'équipements provenant de fournisseurs divers.

*Chaque lecteur mécatronique (autonome) est soumis à l'activation d'une licence individuelle.*

*La configuration de ces lecteurs s'effectue par l'intermédiaire d'outils tiers fournis par le constructeur. Pour les lecteurs, l'élément de configuration permettant de faire le lien entre MICRO-SESAME et l'outil de configuration est le* ***Lock ID*** *(identifiant unique du lecteur).*

*Il est donc nécessaire de renseigner ce paramètre en fonction de la valeur définie dans l'outil de configuration.*

*Depuis le menu principal, suivre* ***Paramétrage > matériel > Architecture matériel****.*

***Suivre la procédure suivante pour ajouter et configurer un lecteur OSS :***

1. Dans la table Architecture matériel située dans la partie gauche de la fenêtre, localiser la catégorie **OSS offline**
2. Dans la catégorie **OSS offline**, effectuer un clic-droit sur la ligne correspondant au **site d'appartenance**
3. Dans le menu contextuel, sélectionner **Ajouter un lecteur**
4. Un nouveau lecteur apparaît dans la table, cliquer sur la ligne correspondante.
5. Renseigner le **Lock ID** conformément à la configuration effectuée dans l'outil tiers (outil constructeur de configuration des lecteurs)
6. Renseigner un commentaire (optionnel)
7. Sélectionner la classification associée dans la liste déroulante (optionnel)

*Chaque lecteur mécatronique (autonome) est soumis à l'activation d'une licence individuelle. Vérifier l'activation de la licence pour chaque lecteur créé.*

*Double cliquer sur un lecteur dans la table située dans la partie gauche de la fenêtre pour renommer l'élément.*

## 2.5. Ajouter et configurer un groupe de lecteur OSS OFFline

Les groupes de lecteurs OSS permettent d'assigner des accès par lot aux identifiés.

*Pour les groupes de lecteurs l'élément de configuration permettant de faire le lien entre MICRO-SESAME et l'outil de configuration est le **Group ID** (identifiant unique du groupe de lecteur).*

*Il est donc nécessaire de renseigner ce paramètre en fonction de la valeur définie dans l'outil de configuration.*

*Depuis le menu principal, suivre **Paramétrage > matériel > Architecture matériel**.*

***Suivre la procédure suivante pour ajouter et configurer un groupe de lecteurs OSS :***

1. Dans la table Architecture matériel située dans la partie gauche de la fenêtre, localiser la catégorie **OSS offline**
2. Dans la catégorie **OSS offline**, effectuer un clic-droit sur la ligne correspondant au **site d'appartenance**
3. Dans le menu contextuel, sélectionner **Ajouter un groupe de lecteurs**
4. Un nouveau groupe de lecteurs apparaît dans la table, cliquer sur la ligne correspondante.
5. Renseigner le **Group ID** conformément à la configuration effectuée dans l'outil tiers (outil constructeur de configuration des lecteurs)
6. Sélectionner la classification associée dans la liste déroulante (optionnel)
7. Sélectionner les lecteurs à affecter au groupe de lecteurs.

*L'affectation des lecteurs aux groupes dans MICRO-SESAME est uniquement à visée informative (visualisation de la configuration effectuée dans l'outil tiers) et n'a aucun impact lors du téléchargement des accès.*

*Cette opération est effectuée directement depuis l'outil de configuration tiers lors de la configuration des lecteurs.*

*Double cliquer sur un groupe de lecteur dans la table située dans la partie gauche de la fenêtre pour renommer l'élément.*

## 2.6. Ajouter des identifiants dans la blacklist

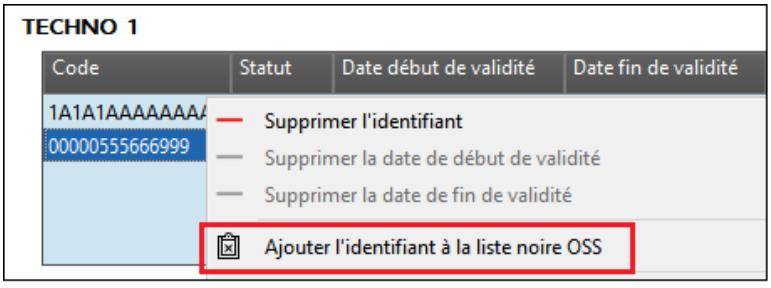
Il est possible de créer et de diffuser dans les serrures OSS une blacklist, c'est à dire une liste de badges qui seront interdits lors de leur passage sur ces dernières.

Cela permet notamment d'interdire des badges qui auraient été : volés, perdues ... etc.

Cette blacklist est descendue dans les serrures OSS par l'intermédiaire des badges utilisateurs OSS.

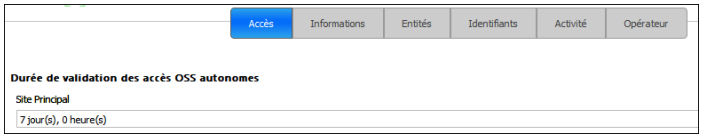
Pour descendre la blacklist dans les serrures, il est nécessaire de réaliser les opérations suivantes :

1. Déclarer l'identifiant dans la blacklist :
   a. Ouvrir l'onglet "Identifiants" de la fenêtre "gestion des identifié"
   b. Effectuer un click droit et sélectionner "ajouter l'identifiant à la liste noire OSS"




   c. Paramétrer la date de fin d'expiration

*Il est conseillé de mettre la date d'expiration au minimum à la date : <date/heure actuelle> + "durée de validition des accès OSS autonomes"*




d. Changer le statut de l'identifiant (perdu, voler ... etc) ou le supprimer de la fiche identifié dans le cas où le badge ne doit plus être utilisé par l'identifié après la date d'expiration paramétrée précédemment

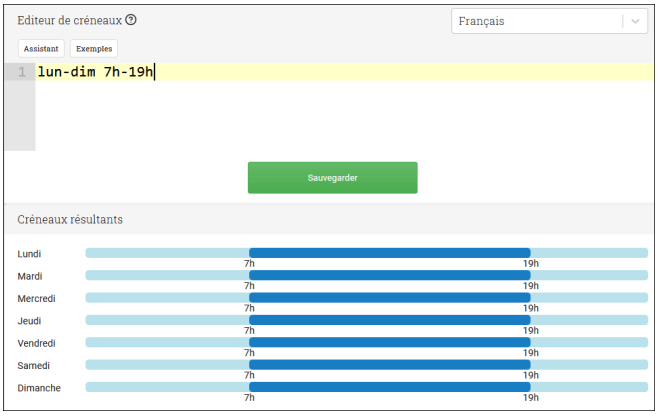
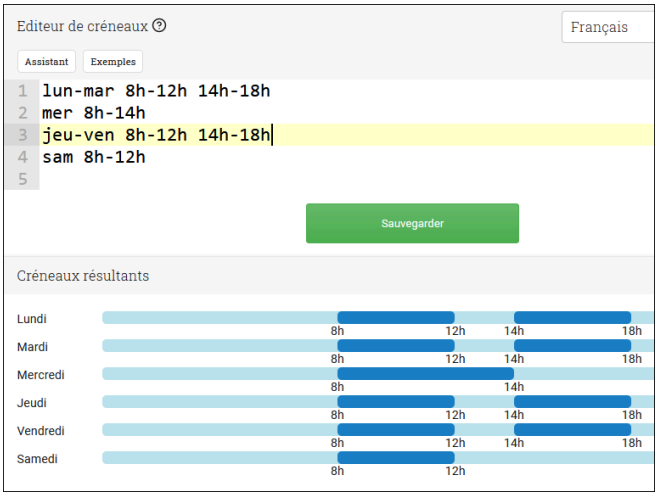
2. Passer un badge utilisateur OSS (autre que le badge en question) sur une borne ou un lecteur actualisateur
3. Passer le badge utilisateur OSS sur les serrures

## 2.7. Plages horaires OSS

### 2.7.1. Limitations sur les plages horaire OSS

***Le standard OSS Offline permet de gérer :***

- 15 plages horaires au maximum
- Chaque plages horaires peut contenir jusqu'à 4 groupes de jours
- Chaque groupe de jours peut contenir jusqu'à 4 créneaux horaires

| exemple : 1 groupe de jour, 1 créneau | exemple : 4 groupes de jours, 2 créneaux |
|---|---|
|  |  |





*La valeur de ces nominaux impacte la taille de l'application qui sera créé dans le badge lors du premier encodage*

### 2.7.2. Créer ou rendre utilisable une plage horaire pour l'offline OSS

*Pour pouvoir paramétrer des plages horaires pour le système offline OSS, il est nécessaire d'activer dans un premier temps la fonctionnalité :*

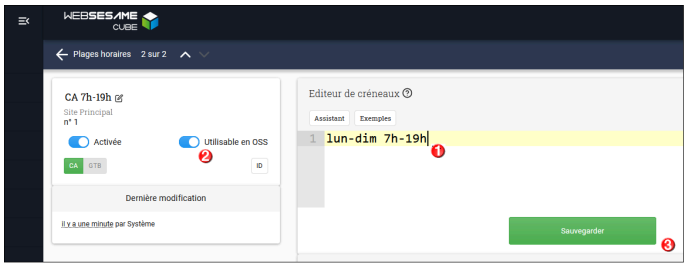
*Menu MICRO-SESAME > Paramétrage > Matériel > Architecture Matérielle, sélectionner dans la liste "Oss Offline" et cocher la case "Activation de la ligne OSS Offline".*

***Afin de créer ou modifier une plage horaire pour l'OSS :***

1. Ouvrir l'application WEB de gestion des plages horaires :

- Depuis MICRO-SESAME : Menu > Exploitation > plage horaire : Web-sesame se lance et ouvre la gestion des plages horaires
- Depuis WEB-SESAME : Plages horaires > Plages horaires

2. Cliquer sur "Créer une plage horaire", ou sélectionner une plage horaire déjà existante puis "modifier"
3. Paramétrer les groupes de jours et créneaux en respectant les limitations pour l'OSS
4. Cocher la case "utilisable en OSS"
5. Sauvegarder




## 2.8. Appliquer la configuration

Une fois la configuration OSS effectuée, il est nécessaire de télécharger les données dans la borne afin de la mettre en exploitation.

*Le téléchargement de la configuration de la borne est une opération de paramétrage initiale, elle permet de diffuser à l'équipement les éléments de fonctionnement principaux lui permettant de dialoguer avec les badges de l'installation :*

- *Technologie d'identifiants*
- *Code site*

*La modification de la configuration de la borne sur un site en exploitation est une opération sensible, nécessitant de ré-encoder les badges de tous les identifiés autorisés sur les lecteurs autonomes.*

*Depuis le menu principal, suivre **Paramétrage > matériel > Architecture matériel**.*

***Suivre la procédure suivante pour télécharger la configuration sur toutes les bornes OSS de l'installation :***

1. Dans la table Architecture matériel située dans la partie gauche de la fenêtre, localiser la catégorie **OSS offline**
2. Effectuer un clic-droit sur la ligne associée et sélectionner **Télécharger les accès et la configuration sur toutes les bornes**.

***Suivre la procédure suivante pour télécharger la configuration sur une bornes OSS spécifique :***

1. Dans la table Architecture matériel située dans la partie gauche de la fenêtre, localiser la catégorie **OSS offline**
2. Effectuer un clic-droit sur la ligne correspondant à la borne à télécharger et sélectionner **Télécharger les accès et la configuration sur cette borne**.

## 2.9. Télécharger les accès manuellement

Il est possible de télécharger les identifiants ainsi que les accès associés manuellement dans la borne afin de les mettre à disposition des identifiés.

*Contrairement au **téléchargement de la configuration**, le téléchargement des accès est une opération courante d'exploitation.*

*Une fois les accès téléchargés sur la borne, ceux-ci seront mis à jours dans les badges des identifiés lors du prochain passage sur la borne.*

*Depuis le menu principal, suivre **Paramétrage > matériel > Architecture matériel**.*

***Suivre la procédure suivante pour télécharger les accès sur toutes les bornes OSS de l'installation :***

1. Dans la table Architecture matériel située dans la partie gauche de la fenêtre, localiser la catégorie **OSS offline**
2. Effectuer un clic-droit sur la ligne associée et sélectionner **Télécharger les accès sur toutes les bornes**.

***Suivre la procédure suivante pour télécharger les accès sur une bornes OSS spécifique :***

1. Dans la table Architecture matériel située dans la partie gauche de la fenêtre, localiser la catégorie **OSS offline**
2. Effectuer un clic-droit sur la ligne correspondant à la borne à télécharger et sélectionner **Télécharger les accès sur cette borne**.

*Le téléchargement des accès et identifiants s'effectue automatiquement lors d'un ajout/modification/suppression depuis la gestion des identifiés et ou des identifiants.*

# Chapitre 3. Configuration de la borne OSS

## 3.1. 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 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 drectement à la mise à jour des accès et des données du badge.

***Figure 3.1. 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

## 3.2. Configuration du mode de fonctionnement

### 3.2.1. Mode encodage

Le mode encodage permet de préparer les badges sous le format attendu par le protocole OSS ( création de l'application, création des fichier, 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 détenant du badge.

***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:***

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 :**

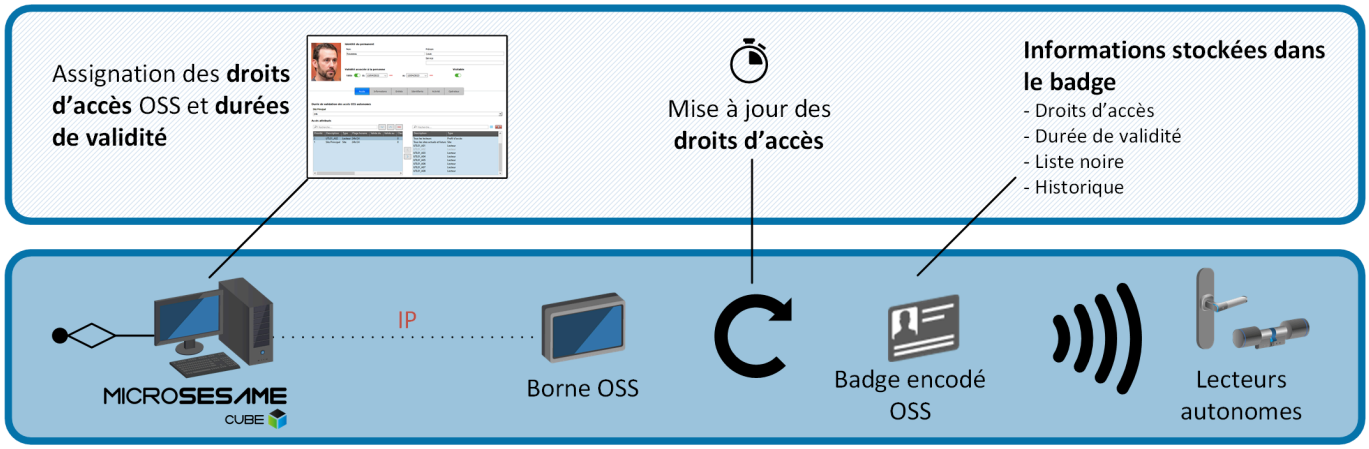
```
uid;credentialID
0444467afd5180;BB112233445566778899
7FED887AB4C56E;A589C56247252D5632D1
```

### 3.2.2. 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




### 3.2.3. 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 3.10.*

*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 filea 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
```

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

### 3.3.1. 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 :<br>Une adresse IP et masque de sous réseau compatible avec l'adresse IP d'usine de la borne (172.16.5.240) :<br>• adresse IP commençant par 172.16.x.x (exemple : 172.16.5.240)<br>• masque de sous réseau en 255.255.0.0 |
| Compatibilité navigateur | Un navigateur à jour sur le PC (Internet Explorer en version 9 ou supérieur, Firefox). |

### 3.3.2. 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 |
|---|---|---|---|---|---|---|---|
| **Utilisateur** | NON | NON | NON | NON | **OUI** | **OUI** | Login : user<br>Password : user |
| **Installateur** | NON | NON | **OUI** | **OUI** | **OUI** | **OUI** | Login : service<br>Password : service |

| 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 |
|---|---|---|---|---|---|---|---|
| **Administrateur** | **OUI** | **OUI** | **OUI** | **OUI** | **OUI** | **OUI** | Login : admin<br>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 MICRO-SESAME.*

***Une fois connecté, l'administateur 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'administateur 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 utlisateur concerné.
2. Dans la partie droite du bandeau supérieur, cliquer sur l'espace correspondant au nom de l'utlilisateur :
   - 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.*

### 3.3.3. 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

## 3.4. 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 3.1. 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 |
| | MICRO-SESAME | Mode de communication avec MICRO-SESAME |
| 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 |

## 3.5. 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 sont mises à jour automatiquement au téléchargement depuis MICRO-SESAME.

*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.

## 3.6. 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 sélectionner, 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.*

## 3.7. 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 MICRO-SESAME 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 3.2. Types de certificats***

| Types de certificats | Détails |
|---|---|
| Auto-signés | 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.<br><br>*Il n'est pas conseillé d'utiliser ce type de certificat sur un site en exploitation.* |
| Signés | ***Les certificats signés sont générés en plusieurs étapes :***<br>1. L'intéressé génère un CSR (Certificate Signing Request) ou requête de signature de certificats<br>2. Il transfère cette requête à une autorité de confiance qui pourra garantir l'identité de l'intéressé<br>3. Cette dernière renvoie alors un certificat signé ainsi que son propre certificat (certificat d'autorité de certification) |
| 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 autotsigné 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 près 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 3.3. Ajouter un certificat signé*

| Etape | Details |
|---|---|
| Génération du CSR | ***Suivre la procédure suivante pour ajoutrer un certificat signé :***<br><br>1. Cliquer sur le bouton **Generate CSR**<br>2. Remplir les informations demandées :<br>• **Nom** : nom qui sera donné au fichier généré<br>• **Country** : Sélectionner le pays<br>• **State** : Correspond à l'état/Région/Département<br>• **City** : Correspond à la ville<br>• **Organization** : Correspond à l'entreprise<br>• **Unit** : Correspond au service<br>• **Common name** : Correspond à l'adresse IP de la TILLYS ou à son nom d'hôte (host name)<br><br>Une fois les informations validées, Une ligne se crée dans le tableau se trouvant dans la partie **Certifcate Signature request (CSR)** de la page HTML.<br>3. Attendre environ 30 secondes pour que le certificat puisse se générer puis rafraîchir la page. lorsque la valeur *Not available yet* a disparu, cliquer sur le bouton **Download** pour télécharger le fichier CSR, indiquer l'emplacement du fichier et valider. |
| Signature du CSR | Le RSSI du site transfère la requête CSR à une autorité de certification pour qu'elle la signe.<br><br>***Cette dernière renvoie les éléments suivants :***<br><br>• Le certificat signé<br>• Son propre certificat ou alors la **chaîne de certification** si il s'agît d'une autorité itnermédiaire. |
| Ajout du certificat signé | ***Se rendre dans la page Configuration > Certificates :***<br><br>1. Dans la partie Certificate Signature Request, sélectionner le **CSR**<br>2. Cliquer sur **Parcourir** puis sélectionner le certificat signé correspondant<br>3. Cliquer sur **Replace CSR**<br><br>*Le nom du fichier du certificat signé doit obligatoirement avoir le même nom que la requête CSR* |
| Ajout du certificat de l'autorité de certification ou chaine de certification | ***Se rendre dans la page Configuration > Certificates :***<br><br>1. Dans la partie CA certificates, sélectionner le **CSR**<br>2. Cliquer sur **Parcourir** puis sélectionner le certificat signé correspondant<br>3. Cliquer sur **Upload**<br><br>*Dans le cas d'une chaine de certifcation il est nécessaire d'importer tous les certifcats* |

*Tableau 3.4. Compatibilité TLS pour UTL*

| Types de clés | Détails |
|---|---|
| RSA | ***Types de clés validés:***<br>• 4096 bits |
| ECDSA | ***Courbes elliptiques validées:***<br>• Courbe elliptique secp384r1<br>***Courbe elliptiques acceptées (en théorie):***<br>• secp521r1<br>• brainpoolP256r1<br>• branipoolP384r1<br>• brainpoolP512r1 |

## 3.8. Paramétrage réseau

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

*Tableau 3.5. Système configuration*

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

*Tableau 3.6. Apps configuration*

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

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

## 3.9. 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**.*

## 3.10. 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 MICRO-SESAME. 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 3.7. Connection with MICRO-SESAME***

| Paramètres | Détails |
|---|---|
| MICRO-SESAME IP address | Renseigner l'adresse IP du serveur MICRO-SEAME |
| Communication state | Après avoir renseigné l'adresse IP du serveur MICRO-SESAME, 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 3.8. Offline parameters***

| Paramètres | Détails |
|---|---|
| Offline application ID (HEXA format) | Ce paramètre correspond à l'identifiant de l"application présente dans le badge et contenant les données offline.<br><br>*Ce paramètre peut être renseigné directement depuis cette page ou télécharger depuis MICRO-SESAME.* |
| Site ID | 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.<br><br>*Ce paramètre peut être renseigné directement depuis cette page ou télécharger depuis MICRO-SESAME.* |

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

***Tableau 3.9. Offline parameters***

| Paramètres | Détails |
|---|---|
| Offline keys | Ce paramètre correspond aux clés de lecture/écriture de données du badge. |

***Tableau 3.10. Encoding parameters***

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

| Paramètres | Détails |
|---|---|
| Max Blacklist | Ce paramètre correspond au nombre maximum d'identifiants que peut contenir la Blacklist présente dans le badge.<br>La Blacklist est une liste contenant les identifiants de badges OSS qui devront être refusé lorsque ces derniers seront présentés sur une serrure.<br>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. |

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*

# Chapitre 4. Configuration TILLYS CUBE, MLP-OSS et lecteurs actualisateurs

## 4.1. Fonctionnement

Grâce à l'association d'une "TILLYS CUBE" avec un "MLP-OSS" et un lecteur transparent (SSCPv1 ou SSCPv2), il est possible de mettre à jour les données offline OSS d'un badge tout en l'utilisant en même temps pour le contrôle d'accès online.

Lors d'un passage de badge sur le lecteur : une première étape de mise à jour des données et récupération des historiques/ alarmes OSS s'effectue si nécessaire, puis le process de lecture du contrôle d'accès online s'effectue.

## 4.2. Paramétrer le protocole bus de communication

Accessible depuis "Configuration / Bus setting" du serveur WEB de la TILLYS CUBE, cette page permet de configurer le type de module interfacé sur chaque bus.

Sélectionner le type "ML CUBE UPDATER"

*Il est possible de mettre qu'un seul module MLP-OSS par bus utilisant 1 ou 2 lecteurs.*

Sélectionner ensuite le mode de sécurité :

- **Mode standard** : ce mode accepte le branchement à chaud des modules non mis à la "clé client".

  Au branchement d'un nouveau module contenant des clés usine (clé constructeur), si la TILLYS possède une "clé client", alors elle met automatiquement le module à cette "clé client" (de manière chiffrée) afin que les produits puissent communiquer ensemble. Si aucune "clé client" n'a été transmis à la TILLYS alors le module communiquera grâce aux clé d'usine (clé constructeur).
- **Mode Secure** (renforcé) : ce mode n'accepte pas le branchement à chaud des modules non mis à la "clé client", le module doit obligatoirement être mis à la "clé client" (clé personnalisée depuis le logiciel KSM) avant son branchement sur le bus. Un module branché à chaud sans avoir été mis auparavant à la "clé client" ne communiquera pas avec la TILLYS.

  Ce mode est accessible seulement si une clé client est présente sur la TILLYS.

  Ce mode est à utiliser sur les sites hautement sensible ou voulant une sécurité maximale, il permet de contrôler de manière stricte l'ajout de nouveau modules sur le bus.

## 4.3. Configurer les paramètres offline

Accessible depuis "Configuration / Offline" du serveur WEB de la TILLYS CUBE, cette page permet de configurer les paramètres liés à l'offline

| paramètres | détails |
|---|---|
| AID | Numéro de l'application utilisé dans le badge pour le système offline<br>Ce paramètre doit être configuré au format hexadécimal |
| Site ID | Numéro à personnalisé qui sera associé au site.<br>Les accès qui seront inscrits dans le badge seront valide seulement pour les serrures offline configurées avec le même code site<br>Ce paramètre doit être en configuré au format décimal |

| paramètres | détails |
|---|---|
| R/W key | Valeur de la clé AES de lecture/écriture utilisée dans le badge pour le système offline |

## 4.4. Couleur des LED du lecteur

***Le comportement des LED du lecteur permet d'indiquer quel est le process en cours et de diagnostiquer la réussite ou l'échec de la mise à jour du process offline :***

- la LED Jaune permet d'indiquer qu'une application offline a été détectée et que le process de mise à jour et récupération des historiques/alarmes est en cours
- la LED Cyan permet d'indiquer que la procédure de mise à jour des accès offline est réussie
- la LED Mauve permet d'indiquer que la procédure de mise à jour des accès offline a échouée

# Chapitre 5. Gestion des accès OSS Offline

## 5.1. Assigner des accès offline

A partir de la version 2023 de MICRO-SESAME, l'assignation des identifiants et des accès aux serrures OSS offline s'effectue directement dans la gestion des identifiés depuis MICRO-SESAME ou WEB-SESAME.

***Tableau 5.1. Chronologie des étapes pour la gestion des accès DEISTER***

| N° | Etape | Interface | Détails |
|---|---|---|---|
| 1 | Déclaration des équipements | MICROSESAME CUBE | Déclarer les serrures, groupes de serrures et activer la ligne offline.<br><br>*Déclarer la technologie à utiliser pour les serrures OSS offline.* |
| 2 | Création des identifiés | MICROSESAME CUBE<br>WEBSESAME CUBE | La création d'identifiés susceptibles d'utiliser les équipements offline se fait directement dans la gestion des identifiés depuis MICRO-SESAME ou WEB-SESAME. |

| N° | Etape | Interface | Détails |
|---|---|---|---|
| 3 | Assignation des identifiants offline | MICROSESAME CUBE<br>WEBSESAME CUBE | L'assignation des identifiants offline se fait directement dans la gestion des identifiés depuis MICRO-SESAME ou WEB-SESAME.<br>*Ajouter les identifiants pour la technologie définie dans l'interface de paramétrage OSS.* |
| 4 | Assignation des accès OSS offline | MICROSESAME CUBE<br>WEBSESAME CUBE | L'assignation des accès aux serrures et groupes de serrures se fait directement dans la gestion des identifiés depuis MICRO-SESAME ou WEB-SESAME.<br>*Dans MICRO-SESAME il est nécessaire d'afficher les accès offline pour les assigner.*<br>*Effectuer un clic-droit puis afficher les accès ou groupes d'accès correspondant.*<br>*L'assignation des accès OSS offline supporte uniquement les plages horaires définies OSS . Ceux-ci ne peuvent avoir de dates de validité.* |

## 5.2. Mode office

Le mode office est un mode d'exploitation particulier aux serrures OSS offline. Le fonctionnel est le suivant :

***Le fonctionnel OSS office est le suivant :***

1. Le mode office est activé sur une serrure offline
2. On assigne à un identifié l'accès à cette serrure sur une plage horaire OSS déclarée dans MICRO-SESAME
3. L'identifié passe son badge sur la serrure dans l'intervalle de la plage horaire d'accès, un évènement *Accès AUTORISE* s'en suit.
4. ***La serrure reste déverrouillée jusqu'à ce qu'un des cas suivants advienne:***
   - Fin de la plage horaire associée à l'accès de l'identifié ayant badgé

- Passage de badge sur le lecteur d'un identifié possédant un accès de type office

***Suivre la procédure ci-dessous pour assigner un accès OSS office***

1. Depuis le menu principal, suivre **Exploitation > Contrôle d'accès > Identifiés**
2. Se rendre dans la fiche de l'identifié puis dans l'onglet accès
3. ***Assigner l'accès à la serrure offline concernée :***
   - Sélectionner la plage horaire OSS
   - Activer le mode *Office individual*
4. Enregistrer la fiche identifié pour télécharger automatiquement les nouveaux accès.