TIL TECHNOLOGIES

Une société du groupe vitaprotech

OSS STANDARD OFFLINE

Configuration et utilisation de la borne offline OSS

Référence du document : GU-15008-FR

Date de publication : 15/04/2025

Configuration et utilisation de la borne offline OSS

Table des matières

Liste des illustrations

Liste des tableaux

Préface

1. Matériel nécessaire

- Un réseau de contrôle d'accès et de surveillance intrusion basé sur des *TILLYS* **TILLYS24-CUBE**.
- Un ou plusieurs bornes offline OSS (ou un ou plusieurs lecteurs encodeurs de table).
- Un ou plusieurs lecteurs autonomes.
- Un ou plusieurs lecteurs transparents qui seront utilisés comme lecteurs actualisateurs.
- Des badges de type DESFIRE.

2. Version logicielle et licences

- MICROSESAME à partir de la version logicielle 2021.4.X.
- En cas d'utilisation de ML-OSS, firmware de la TILLYS CUBE à partir de la version 5.6.0.
- Disposer dans les licences MICROSESAME de l'élément LIC-LOCKS avec une valeur de serrures mécatronique supérieure ou égale au nombre des serrures qui seront utilisées.

3. Contexte d'utilisation de ce manuel

Les pastilles de couleur orange ● en haut de chaque page signalent que ce document est un guide utilisateur.

Le partenaire ou installateur TIL TECHNOLOGIES configure MICROSESAME, la borne offline OSS et les TILLYS CUBE et il teste leur fonctionnement.

Le client exploite les fonctions de la borne offline OSS.

4. Voir aussi

- *Vidéo Mécatronique online, offline OSS et clés électroniques*.
- *Fiche technique du module MLP2-OSS-CUBE*
- *Notice technique de la configuration MLP-UPDATER OSS OFFLINE*
- *Fiche produit : actualisateur de droits offline MLP2 OSS CUBE*
- *Fiche produit : borne de mise à jour des droits offline*

5. 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.

Envoyez vos commentaires, corrections et suggestions concernant ce guide à *documentation@til-technologies.fr*

6. Glossaire

Les termes techniques utilisés dans ce guide sont expliqués ci-après.

Badge	Un badge permet d'identifier une personne sur un système de contrôle d'accès. Il comporte un identifiant (sécurisé ou pas) qui est détecté et traité par une tête de lecture physique. Cette opération peut nécessiter un contact direct (comme avec une carte à puce ou une bande magnétique) ou l'approche à distance (pour un badge NFC sans contact). Les badges les plus couramment utilisés sont de technologie MIFARE DESFIRE de type EV1, EV2 ou EV3.
Borne offline	Type de lecteur autonome placé à l'intérieur d'une zone sécurisée et servant à recharger les droits d'accès de courte durée, utilisés par un badge pour accéder à des serrures *offline*. Une borne offline est souvent constituée d'un terminal TACTILLYS sur lequel le firmware OSS a été chargé.
Contrôle d'accès	Le contrôle d'accès désigne différentes solutions techniques qui permettent de sécuriser et gérer les accès physiques à un bâtiment ou un site. Des droits d'accès sont associés à un identifié, afin qu'il puisse franchir un obstacle de type porte, barrière, portail, tourniquet, etc... sans contraintes.
Encodeur de table	Lecteur spécialisé dans l'encodage de badges de contrôle d'accès sans contact.
GTB	Acronyme de Gestion Technique des Bâtiments. Système de pilotage, de contrôle, de supervision et d'optimisation des divers services comme l'éclairage, le chauffage ou la ventilation, présents dans les bâtiments tertiaires et industriels (immotique).
IP	Acronyme anglais d'Internet Protocol.

	Le protocole Internet permet aux équipements qui l'utilisent de communiquer entre eux par paquets, de type *TCP* ou *UDP*. Le protocole IP est transporté par des réseaux locaux filaires utilisant le protocole de connexion Ethernet. Les cartes ou interfaces réseau équipées de connecteurs de type *RJ45* y ont accès physiquement et y sont identifiées logiquement via leur adresse IP.
Lecteur	Équipement utilisé pour la détection d'un identifiant sur un système de contrôle d'accès. L'identifiant peut prendre différentes formes : badge, code clavier, empreinte biométrique, plaque minéralogique... Selon sa technologie, un lecteur peut être utilisé pour : ● Assurer la simple détection du support de l'identifiant, par exemple un lecteur de type "transparent" qui se limite à détecter la présence d'un badge. ● Assurer en plus la lecture d'un identifiant standard, par exemple un lecteur "simple" qui ne sait lire que le numéro de série d'un badge (identifiant *CSN*). ● Assurer en plus la fonction de déchiffrement d'un identifiant sécurisé encodé dans un badge, par exemple un lecteur sécurisé dans lequel on enregistre la clé des badges.
Lecteur actualisateur	Lecteur transparent SSCPv2 ou SSCPv1 câblé sur un module MLP2-OSS-CUBE qui a été configuré via MLP-UPDATER. Ce lecteur, relié par IP à MICROSESAME, permet de gérer, en plus du contrôle d'accès, le rechargement des droits utilisateur d'un badge pour autoriser son accès à une liste de lecteurs OSS offline, qui sont situés à l'intérieur de ce premier contrôle d'accès au bâtiment. De plus, ce type de lecteur lit sur le badge les historiques des lecteurs autonomes franchis, qu'il transmet à MICROSESAME, et il copie sur le badge la liste noire des accès interdits au niveau de MICROSESAME.
Lecteur autonome	Type de lecteur qui n'est connecté ni à une alimentation électrique externe ni à un réseau de surveillance. Il est nécessaire de changer sa batterie régulièrement. Au passage d'un badge autorisé, il autorise ou non l'accès selon les droits du badge, il met à jour sa liste noire de badges interdits par MICROSESAME et il copie sur le badge son historique de passage.
Lecteur transparent	Lecteur de badge en protocole *SSCP*, *DeBus* ou *OSDP*, utilisé uniquement pour détecter la présence d'un badge, sans lecture de son identifiant. La récupération de l'identifiant (sécurisé

	ou pas) est assurée par un module de type MLDx ou MLPx. Un lecteur transparent se comporte en quelque sorte comme une simple antenne et ne comporte aucune clé de chiffrement servant à la lecture de l'identifiant sécurisé d'un badge (au contraire de certains lecteurs sécurisés). Il peut toutefois recevoir une clé de chiffrement (gestion par protocoles *SSCPv2*, *DeBus Secure* ou *OSDP Secure*) qui permet de chiffrer les communications avec le module.
Mécatronique	Dans le contexte TIL TECHNOLOGIES, ce qualificatif désigne des serrures intégrant des éléments mécaniques et électroniques.
MICROSESAME	Logiciel de supervision unifiée qui permet de centraliser toutes les informations électroniques du bâtiment : contrôle d'accès, détection intrusion, gestion technique, vidéo, interphonie... Le pilotage des différentes fonctions à travers une interface graphique commune rend leur exploitation beaucoup plus simple et les interventions plus efficaces. Les interactions entre les différents systèmes pouvant être complètement automatisées (actions sur évènements), la rapidité des traitements est également garantie.
MLP2-OSS CUBE	Module logique pour 2 lecteurs par bus, qui peut être configuré comme MLP-UPDATER pour gérer le contrôle d'accès, l'intrusion et la gestion technique de bâtiment des portes mais aussi la mise à jour de badges OSS.
Module déporté	Équipement raccordé sur un bus de la *TILLYS* qui assure une fonction spécifique (gestion de lecteurs, gestion de détecteurs intrusion, gestion de capteurs de mesures physiques ...). Chez TIL, il existe plusieurs gammes de modules déportés qui ne sont pas compatibles entre elles : ancienne gamme V2 (modules MD en RS485) et gammes NG ou CUBE (modules ML en RS485). Les claviers (utilisés pour le contrôle d'accès, comme pour l'intrusion) sont également considérés comme des modules déportés. Les modules déportés possèdent tous une roue codeuse qui leur attribue une adresse sur les bus RS485 de la TILLYS. Le module MDT2 (transmetteur téléphonique) est le seul de la gamme qui ne se raccorde pas en RS485, mais se connecte sur un bus série qui n'équipe que les TILLYS V2. Ce module peut toutefois être exploité sur une TILLYS NG ou CUBE, en utilisant une carte fille NG-CF-RS.
Offline	Caractéristique d'une serrure électronique qui fonctionne de manière autonome, sans être directement connectée à un réseau ou à un système centralisé. Une serrure de ce type ne stocke qu'une liste de badges interdits d'accès et une liste de badges

	toujours autorisés (liste blanche). Les informations et l'historique d'accès sont stockés sur chaque badge, sur lequel les droits d'accès doivent être rechargés fréquemment en utilisant une *borne offline*.
Online	Caractéristique d'une serrure électronique qui est contrôlée et surveillée à distance via une liaison filaire, au travers d'un hub radio. Les autorisations et l'historique d'accès ne sont pas stockées localement sur ce type de serrure électronique, mais au niveau de la plate-forme centrale.
OSS	Acronyme anglais d'Open Security Standard. Norme dans le domaine du contrôle d'accès permettant le fonctionnement de lecteurs de divers constructeurs (ASSA ABLOY, DEISTER, Uhlmann & Zacher, DORMA KABA, Zugang GmBH...etc) de fonctionner avec des réseaux de sûreté sans y être physiquement connectés. Ces lecteurs fonctionnent sur batterie et leurs données sont mises à jour régulièrement.
Sécurité	La sécurité électronique inclut la cybersécurité, le contrôle d'accès, la sûreté, la GTB, la surveillance sécurité, la supervision, l'intrusion et la télésurveillance. Elle est plus spécifique que la notion générale de sécurité des biens et des personnes, dont elle fait partie.
SSCP	Acronyme anglais de Smart and Secure Communication Protocol. Protocole de sécurisation des communications, utiliser chez TIL pour assurer les échanges en RS 485 avec des lecteurs compatibles. Les lecteurs EVOLUTION fabriqués par la société française STID communiquent à l'aide de ce protocole. Deux versions de ce protocole existent. La version V1, pour laquelle les lecteurs ne sont pas prévus pour recevoir des clés de chiffrement, est moins sécurisée que la version V2 qui autorise le stockage de clés de chiffrement dans les lecteurs, afin de chiffrer les communications entre modules et lecteurs. Les deux versions n'étant pas compatibles, les modules MLP1-2 et les lecteurs EVOLUTION doivent être choisis en fonction de l'une ou l'autre de ces versions. Depuis plusieurs années maintenant, TIL ne propose plus dans ses solutions que des modules MLP2 et des lecteurs EVOLUTION SCCPV2, pour garantir une sécurisation de type ANSSI.
TACTILLYS	Clavier tactile TIL TECHNOLOGIES dédié à la gestion de l'intrusion, équipé d'un écran couleur 7 pouces. Raccordé sur un bus

	RS 485 de la TILLYS, il permet à un opérateur intrusion de s'authentifier, afin d'accéder à certaines actions paramétrées dans la fonction intrusion. Il peut être équipé d'un lecteur de badge qui se substitue au code à saisir, ou au contraire qui renforce l'authentification nécessaire d'un opérateur intrusion (passage d'un badge + saisie d'un code).
TILLYS	Automate *IP* programmable multifonction développé par TIL TECHNOLOGIES qui dispose des fonctionnalités de contrôle d'accès, de détection intrusion et de *GTB*. Grâce à 3 bus RS 485 (A, B et C), chaque TILLYS permet le raccordement de 8, 16 ou 24 lecteurs pour le contrôle d'accès. Elle constitue également une véritable centrale d'alarme. Voir aussi *UTL*.
UTL	Acronyme d'Unité de Traitement Local. Terme générique qui désigne un automate *IP* programmable et multifonction, utilisé dans le domaine du contrôle d'accès, de l'intrusion et de la GTB. C'est grâce à cet automate que vont être gérés par exemple, les accès des identifiés, les informations provenant des lecteurs ou des systèmes anti-intrusion, etc. L'UTL de TIL TECHNOLOGIES est la *TILLYS*, qui se décline en version V2, NG et CUBE.

Chapitre 1. Présentation et prérequis d'un système offline OSS

1.1. Principes de fonctionnement de la norme OSS

L'*OSS* est une norme dans le domaine du *contrôle d'accès* "*offline*" (*lecteurs autonome*), permettant à *MICROSESAME* 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, comme *MICROSESAME*.
- d'un ou plusieurs *lecteurs autonomes*, qui prennent la décision d'ouverture/fermeture sur la base des droits d'accès contenus dans le badge et non pas en communiquant par IP avec le réseau de surveillance.
- d'un ou plusieurs lecteurs transparents, configurés comme *lecteurs actualisateurs* sur le chemin d'entrée des identifiés dans le bâtiment, pour mettre à jour les droits OSS sur leur badge.
- d'un ou plusieurs badges au format reconnu par les lecteurs du système offline.

Les droits d'accès au(x) lecteur(s) autonome(s) sont distribués depuis le logiciel de gestion de droits d'accès, puis sont téléchargés dans le lecteur actualisateur des droits du badge. Lorsque le badge est passé sur cet équipement de mise à jour, les droits d'accès aux serrures autonome sont inscrits dans ce dernier pour une durée limitée.

Lorsque le badge est ensuite présenté sur la serrure autonome, cette dernière prend la décision d'ouverture en fonction des droits inscrits dans le badge, puis elle inscrit l'historique et les alarmes dans le badge qui seront déchargés sur le lecteur actualisateur au prochain passage du badge sur cet équipement.

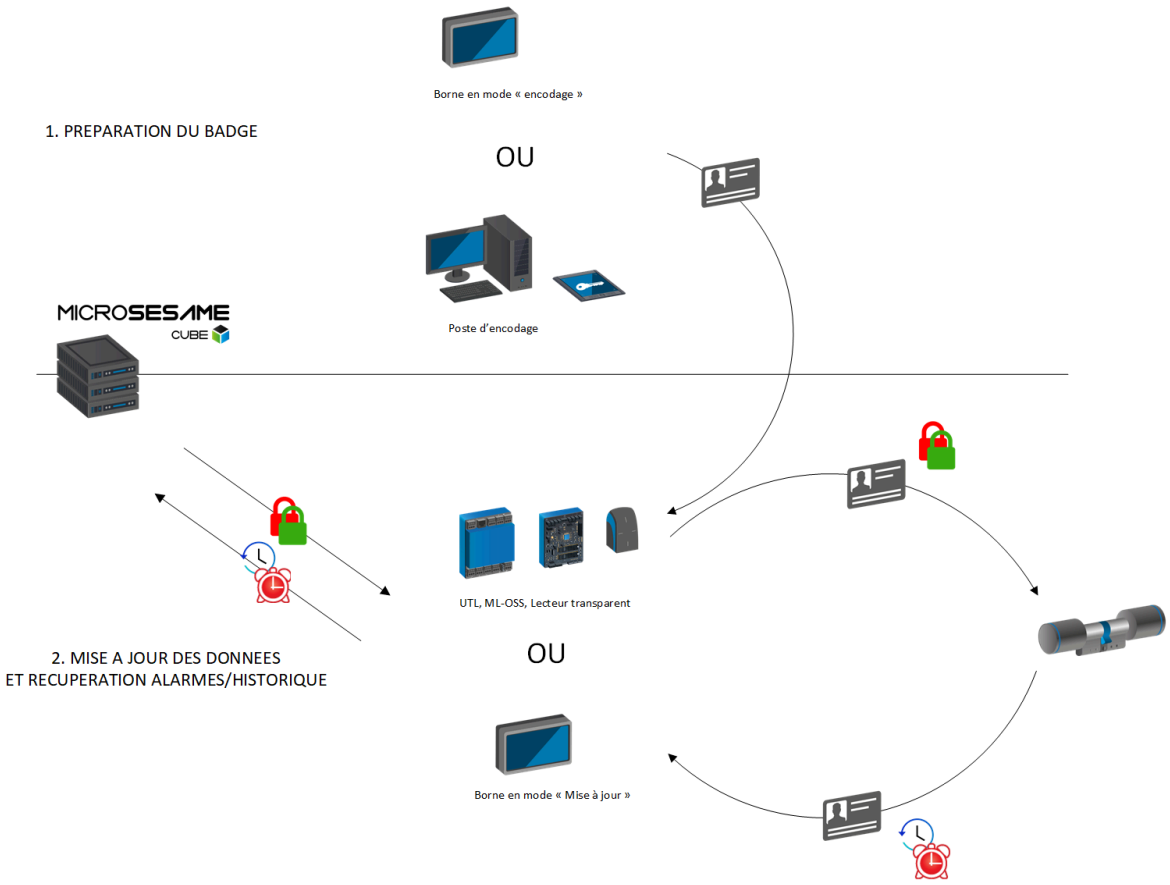
Le système offline OSS avec les produits TIL TECHNOLOGIES fonctionne en suivant les étapes ci-dessous :

Le système offline OSS est activé en 2 étapes :

1. Préparation du badge pour le rendre compatible avec le format OSS offline :
   - Pour un format de badge standard, par encodage sur une *borne offline*, configurée en mode "encodage".

- Pour un format de badge avancé (comme un badge non vierge avec CMK personnalisée), sur un *encodeur de table* comme Omnikey, par encodage via l'application "encodage JS" de MICROSESAME.

2. Configuration des droits avec MICROSESAME, puis mise à jour des données offline dans le badge et récupération des historiques et des alarmes :
   - Soit par une *borne offline*, configurée en mode "mise à jour".
   - Soit par un *lecteur transparent*, configuré comme lecteur actualisateur et branché physiquement sur un *module déporté* MLP2-OSS-CUBE, en utilisant le contrôle d'accès online classique de MICROSESAME via *l'UTL*.



1.2. Prérequis et vérifications avant utilisation du système offline OSS

Avant d'utiliser le système offline OSS avec les produits de TIL TECHNOLOGIES, il est nécessaire de respecter les prérequis suivants :

- Voir *Section 1, « Matériel nécessaire »*.
- Voir *Section 2, « Version logicielle et licences »*.

La mise en place d'un système OSS offline nécessite la configuration des différents produits qui le composent avant sa mise en exploitation. La modification de la valeur de certains de ces éléments

après une première utilisation peut s'avérer assez complexe (nécessité de formatage du badge, reconfiguration des serrures, etc.).

Il est donc fortement recommandé, avant toute utilisation des produits, d'effectuer les vérifications suivantes :

Questions	Détail des vérifications
Quel est l'état actuel du badge ?	Le badge est-il vierge ou a-t-il déjà été encodé par d'autres applications ?
	Quelle est la taille du badge ?
	Sur un badge déjà encodé pour d'autres applications, quelle est la place restante ?
Définir les valeurs des éléments ci-contre en fonction de la place disponible dans le badge. 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 *Section 3.3, « Ajout et configuration d'une borne OSS offline »*).	Quel est le nombre maximum de serrures autonome qui seront installées sur le site ?
	Quel est le nombre maximum d'historique/alarmes qui pourront être inscrits dans le badge ?
	Quel est le nombre maximum de numéros de badge qui pourront être inscrits dans la liste noire (blacklist) ?
	Quel est le nombre maximum de plages horaires qui seront utilisées pour les accès offline et quelle est leur définition ? Voir *Section 3.9, "Plages horaires OSS"*.
Quel sera l'ID des serrures autonomes ?	Définir l'ID qui sera associé à chaque serrure. 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 MICROSESAME 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 *Section 3.10, « Application de la configuration OSS »*). Import d'une configuration
	Définir les groupes d'appartenance.
Quelles seront les valeurs des autres éléments devant être paramétrés ?	Clé de lecture/écriture utilisée pour l'application offline (32 caractères hexadécimaux).
	Numéro de l'application qui sera créé dans le badge (6 caractères hexadécimaux).

Questions	Détail des vérifications
	Numéro code site (sur 3 caractères XXX).

Chapitre 2. Configuration du protocole OSS offline dans la TILLYS

Ce chapitre explique comment configurer dans la TILLYS le fonctionnement de l'OSS pour des serrures mécatroniques Offline.

Pour des informations complètes sur les installations OSS offline, voir *Configuration et utilisation de la borne OSS offline*.

1. À partir du menu Burger de l'interface d'administration de la TILLYS, suivre **Access control > Offline configuration**.
2. Cliquer sur l'interrupteur **Enable Offline Access Control** pour le faire passer en bleu et cliquer sur Submit.
3. Renseigner les champs de la section **Badge configuration** selon le tableau ci-après et cliquer sur Submit.

Tableau 2.1. Configuration des badges offline

Paramètre	Détails
AID	Renseigner l'identifiant de l'application offline dans les badges.
Site ID	Renseigner le code site tel que renseigné dans MICROSESAME.

4. Dans la section **Badge key configuration**, le champ **R/W Key**, renseigner la clé de lecture/écriture des données offline utilisées dans les badges, puis cliquer sur Submit.

Chapitre 3. Configuration de MICROSESAME pour l'utilisation d'OSS offline

3.1. Activation de la ligne 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 gérés par le serveur MICROSESAME.

L'activation de la ligne OSS offline permet de rendre visible ses paramètres :

- Définir une plage horaire OSS
- Attribuer les accès OSS dans la fiche d'un identifié

1. Depuis le menu principal de MICROSESAME, suivre **Paramétrage > Matériel > Architecture matérielle [ARC]**.
2. Dans la table **Architecture matérielle** située dans la partie gauche de la fenêtre, cliquer sur **OSS offline**.
3. Dans la section Paramètres généraux, cocher la case **Activation de la ligne OSS offline**.
4. Sélectionner la **technologie associée aux bornes OSS**.
5. Cliquer sur l'icône Enregistrer et continuer en *Section 3.2, « Configuration de la ligne OSS : identifiants et durée de validité »*.

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. En effet, la modification de ce paramétrage sur un site en exploitation nécessite un nouvel encodage des badges, pour pouvoir continuer à utiliser les lecteurs autonomes.

3.2. Configuration de la ligne OSS : identifiants et durée de validité

L'identifiant est généré lors de l'encodage des badges OSS par le script MICROSESAME.

1. Depuis le menu principal de MICROSESAME, suivre **Paramétrage > Matériel > Architecture matérielle [ARC]**.
2. Dans la catégorie OSS offline, cliquer sur la ligne du site à paramétrer.

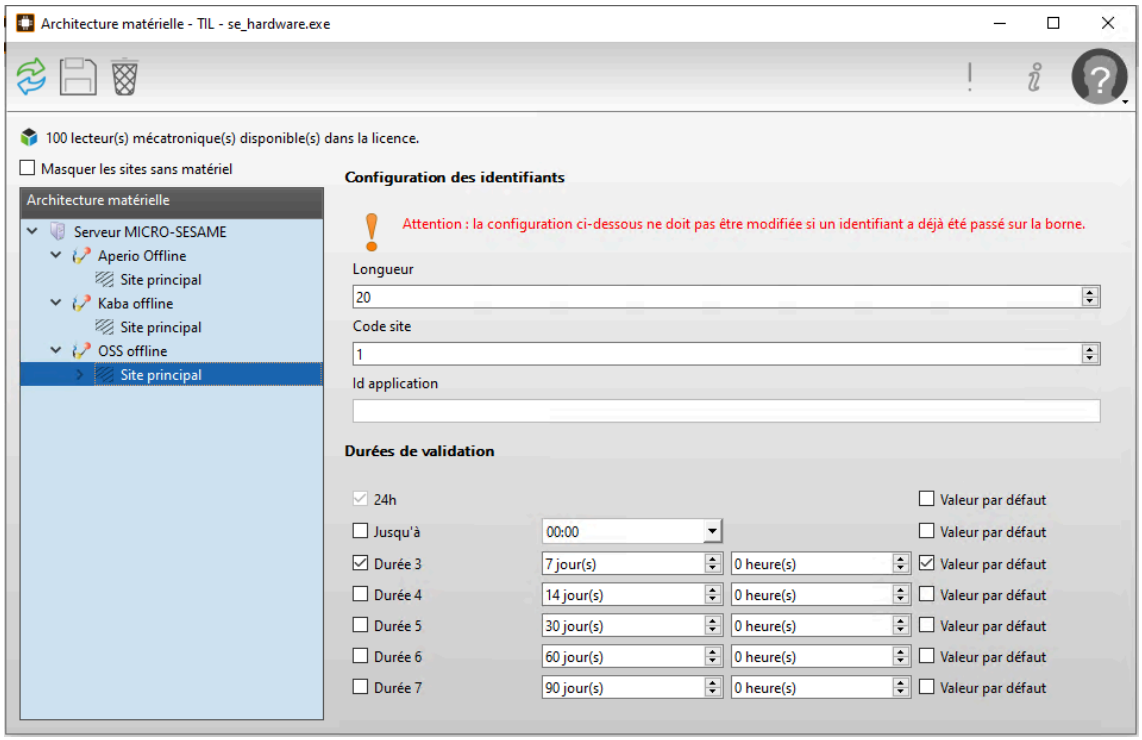


Figure 3.1. Paramétrage d'un site en OSS

3. La longueur de l'identifiant n'est pas modifiable et est fournie à titre indicatif.
4. Renseigner le code site choisi lors de l'encodage des badges OSS.
5. Paramétrer les durées de validité désirées et cocher la case associée, pour qu'elles puissent être distribuées lors de l'assignation d'un accès OSS dans la fiche de l'identifié.

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

6. Cliquer sur l'icône Enregistrer.

Si la case **Jusqu'à** est activée sur une certaine heure, le fonctionnel sera le 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.

Si l'encodage des badges est effectué avec un script personnalisé, respecter le format suivant :

- DECIMAL
- 20 caractères
- Remplissage à gauche (si l'identifiant fait moins de 20 caractères, il sera complété par des 0 en début d'identifiant).

3.3. Ajout et configuration d'une borne OSS offline

Les bornes OSS offline proposent deux modes de fonctionnement :

- 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 ...).
- Borne en mode "mise à jour" : permet de mettre à jour les droits d'accès OSS pour une période définie, d'écrire la liste noire et de récupérer les alarmes/historiques d'un badge.

Pour configurer le mode de fonctionnement d'une borne OSS, utiliser son serveur web.

1. À partir du menu principal de MICROSESAME, suivre **Paramétrage > Matériel > Architecture matérielle**.
2. Dans la table **Architecture matérielle** située dans la partie gauche de la fenêtre, localiser la catégorie **OSS offline**.
3. Dans la catégorie **OSS offline**, effectuer un clic-droit sur la ligne correspondant au **site d'appartenance**.
4. Dans le menu contextuel, sélectionner **Ajouter une borne**.
5. Une nouvelle borne apparaît dans la table, cliquer sur la ligne correspondante.
6. Cocher la case **Activé** pour activer la borne.
7. Sélectionner le mode d'adressage IP (**IP fixe** ou **DHCP**).
8. Renseigner l'information de connexion associée (**Adresse IP** ou **Nom d'hôte**)
9. Modifier si besoin le port de communication proposé (par défaut 20300).

Pour pouvoir renommer une borne, faire un double clic sur son nom dans la partie gauche de l'écran.

Si le port de communication par défaut est modifié, la même modification doit être effectuée au niveau de la TILLYS. Pour connaître la procédure de connexion de la TILLYS à son serveur web, consulter son aide en ligne.

3.4. Déclaration d'un lecteur actualisateur

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

Le lecteur actualisateur doit être un lecteur transparent SSCPv2 ou SSCPv1 (voir *SSCP*), câblé sur un MLP-OSS CUBE. Il permet :

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

1. Depuis le menu principal de MICROSESAME, suivre **Paramétrage > Matériel > Lecteur [LEC]**.

   ou

   Depuis le menu principal de MICROSESAME, suivre **Paramétrage > Matériel > UTL (unité de traitement logique) [UTL]**, cliquer sur la ligne de l'UTL, puis sur l'onglet **Contrôle d'accès**.
2. Créer un nouveau lecteur ou sélectionner le lecteur à paramétrer.
3. Depuis la fenêtre de configuration du lecteur ou directement dans la liste des lecteurs, cliquer sur le commutateur dans la colonne **Actualisateur OSS**.
4. Vérifier que le lecteur est **activé** et possède une **licence** .
5. Depuis le menu principal de MICROSESAME, suivre **Paramétrage > Matériel > Architecture matériel [ARC]**).
6. Dans la catégorie **OSS offline** cliquer sur **lecteurs actualisateurs**.
7. Vérifier que le lecteur paramétré est présent dans la table et qu'il est activé.

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

3.5. Ajout et configuration d'un lecteur OSS offline

Un lecteur autonome OSS offline correspond à une serrure, un cylindre ou une poignée encastrée dans une porte permettant d'autoriser ou de refuser le passage à un identifié lorsqu'il passe un badge.

Ces lecteurs ne peuvent pas être téléchargés ou supervisés en direct depuis MICROSESAME : ils sont **autonomes** sur site et évitent de devoir câbler un lecteur.

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

Chaque lecteur *mécatronique* (également appelé *lecteur 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 MICROSESAME 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.

1. Depuis le menu principal de MICROSESAME, suivre **Paramétrage > Matériel > Architecture matérielle [ARC]**.
2. Dans la table **Architecture matérielle** située dans la partie gauche de la fenêtre, localiser la catégorie **OSS offline**.
3. Dans la catégorie **OSS offline**, faire un clic droit sur la ligne correspondant au **site d'appartenance**.
4. Dans le menu contextuel, sélectionner **Ajouter un lecteur**. Un nouveau lecteur apparaît dans la table.
5. Cliquer sur la ligne de ce lecteur.
6. Renseigner le champ **Lock ID** conformément à la configuration effectuée dans l'outil tiers (outil constructeur de configuration des lecteurs).
7. Saisir éventuellement un commentaire.
8. Sélectionner éventuellement la classification associée, depuis la liste déroulante.

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

Pour pouvoir renommer un lecteur, faire un double clic sur son nom dans la partie gauche de l'écran.

3.6. Ajout et configuration d'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 MICROSESAME 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.

1. Depuis le menu principal, suivre **Paramétrage > Matériel > Architecture matérielle**.
2. Dans la table **Architecture matérielle** située dans la partie gauche de la fenêtre, localiser la catégorie **OSS offline**.
3. Dans la catégorie **OSS offline**, effectuer un clic-droit sur la ligne correspondant au **site d'appartenance**.
4. Dans le menu contextuel, sélectionner **Ajouter un groupe de lecteurs**.
5. Un nouveau groupe de lecteurs apparaît dans la table, cliquer sur la ligne correspondante.
6. Renseigner le **Group ID** conformément à la configuration effectuée dans l'outil tiers (outil constructeur de configuration des lecteurs).

7. Sélectionner éventuellement la classification associée, depuis la liste déroulante.
8. Sélectionner les lecteurs à affecter au groupe de lecteurs.

L'affectation des lecteurs aux groupes dans MICROSESAME est uniquement à but informatif (visualisation de la configuration effectuée dans l'outil tiers) et n'a aucun impact lors du téléchargement des accès.

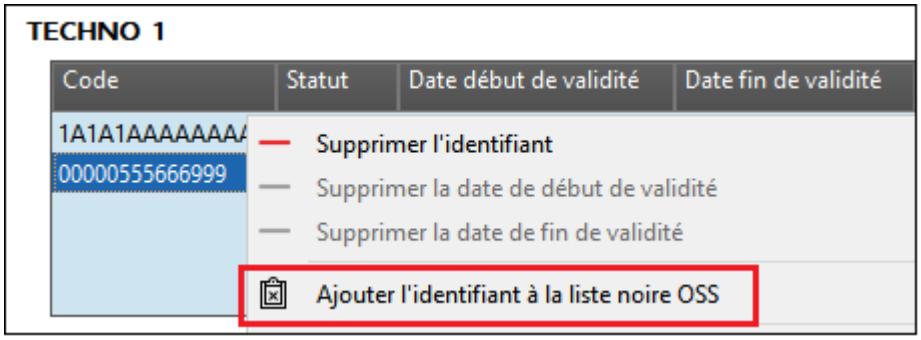
Cette opération est effectuée directement depuis l'outil de configuration tiers, lors de la configuration des lecteurs.

Double cliquer sur un groupe de lecteur dans la table située dans la partie gauche de la fenêtre pour le renommer.

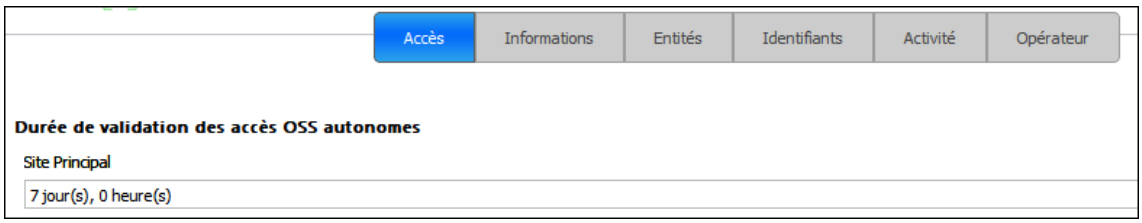
3.7. Ajout d'identifiants dans la liste noire

L'exploitant peut créer et de diffuser dans les serrures OSS une liste noire, c'est à dire une liste de badges (perdus ou volés) auxquels l'accès sera refusé. .

1. Depuis le menu principal de MICROSESAME, suivre **Exploitation > Identifiés [IDE]** , puis cliquer sur l'onglet **Identifiants**.
2. Dans le tableau de la technologie correspondante, faire un clic droit sur l'identifiant à interdire et sélectionner **Ajouter l'identifiant à la liste noire OSS**.



3. Dans l'onglet **Accès**, définir la durée **Durée de validation des accès OSS autonomes**. Il est conseillé de définir la date d'expiration au minimum à la date et à l'heure actuelles.



4. Changer le statut de l'identifiant (perdu, volé, etc ...) ou, si le badge ne doit plus jamais être utilisé par l'identifié après la date d'expiration paramétrée précédemment, le supprimer de la fiche identifié.

5. Cette liste noire est transmise aux serrures OSS par simple passage de badge utilisateur OSS, d'abord sur la borne OSS ou le lecteur actualisation, puis sur les serrures OSS (voir *Section 3.8, « Mise à jour de la liste noire sur les serrures OSS / transmission de l'historique à MICROSESAME »*).

3.8. Mise à jour de la liste noire sur les serrures OSS / transmission de l'historique à MICROSESAME

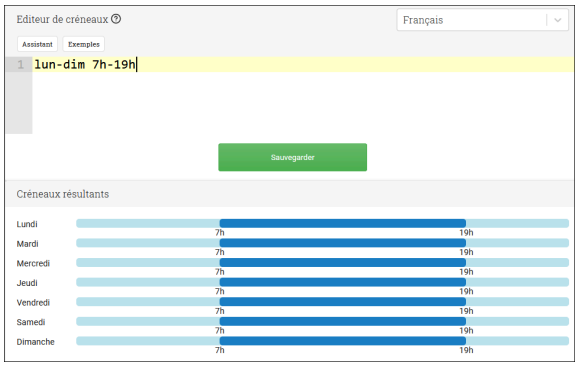
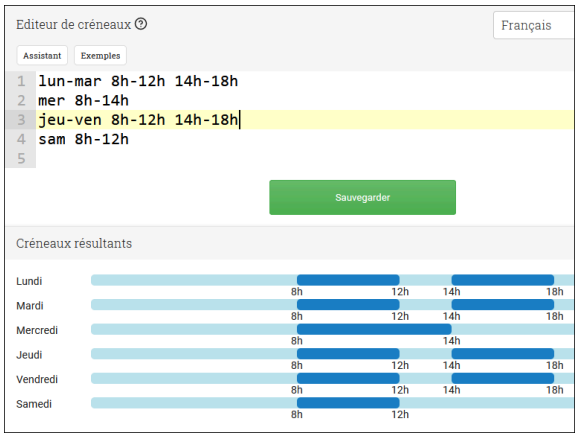
1. Déclarer un identifiant dans la liste noire (voir *Section 3.7, « Ajout d'identifiants dans la liste noire »*).
2. Passer un badge utilisateur OSS (autre que le badge en question) sur une borne OSS ou un lecteur actualisateur.
3. Passer le badge utilisateur OSS sur une serrure OSS. La liste noire est chargée sur la serrure OSS et son historique est copié en retour sur le badge.
4. Au prochain passage du badge sur la borne OSS ou sur le lecteur actualisateur, l'historique présent sur la carte est copié et envoyé à MICROSESAME.

3.9. Plages horaires OSS

3.9.1. 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 créée dans le badge, lors du premier encodage.

3.9.2. Activation de la ligne OSS offline

Avant de pouvoir paramétrer des plages horaires pour le système offline OSS, il est nécessaire d'activer la ligne OSS offline.

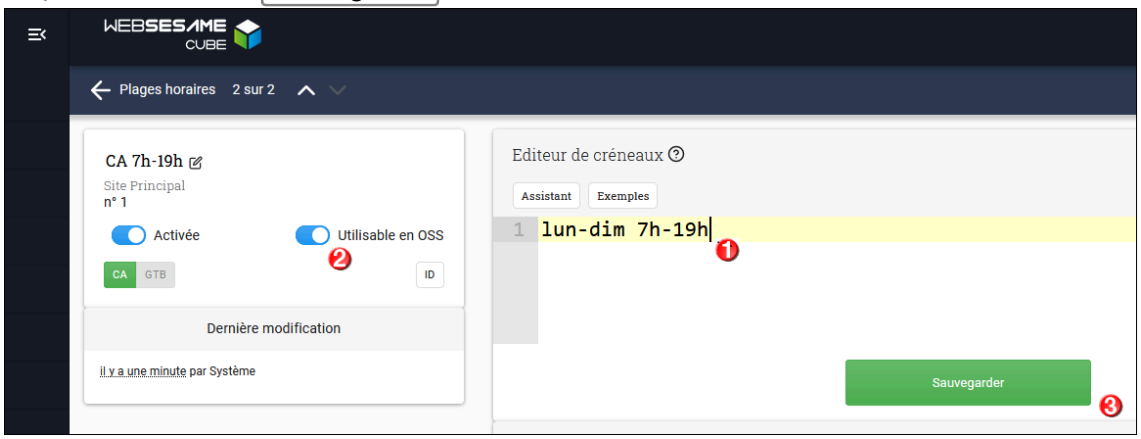
1. À partir du menu principal de MICROSESAME, suivre Paramétrage > Matériel > Architecture Matérielle [ARC].
2. Cocher la case **Activation de la ligne OSS offline**.

3.9.3. Création ou modification d'une plage horaire pour OSS offline dans MICROSESAME

1. À partir de MICROSESAME, suivre **Exploitation > Plage horaire [PLA]**
2. Cliquer sur le bouton Créer une plage horaire ou sélectionner une plage horaire déjà existante puis cliquer sur Modifier.
3. Paramétrer les groupes de jours et créneaux en respectant les limitations pour l'OSS.
4. Cocher la case **Utilisable en OSS**.
5. Cliquer sur le bouton Sauvegarder.

3.9.4. Création ou modification d'une plage horaire pour OSS offline dans WEBSESAME

1. Dans WEBSESAME, suivre **Plages horaires > Plages horaires**.
2. Cliquer sur le bouton Créer une plage horaire ou sélectionner une plage horaire déjà existante puis cliquer sur Modifier.
3. Paramétrer les groupes de jours et créneaux en respectant les limitations pour l'OSS.
4. Cocher la case **Utilisable en OSS**.
5. Cliquer sur le bouton Sauvegarder.



3.10. Application de la configuration OSS

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.

Continuer avec *Section 3.11, « Téléchargement manuel des accès sur toutes les bornes OSS »* ou *Section 3.12, « Téléchargement manuel des accès sur une borne OSS spécifique »*.

3.11. Téléchargement manuel des accès sur toutes les bornes OSS

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

Il est possible de télécharger manuellement les identifiants ainsi que les accès associés dans les bornes OSS (ou lecteurs actualisateurs). Contrairement au **téléchargement de la configuration**, le téléchargement des accès est une opération courante d'exploitation.

1. À partir du menu principal de MICROSESAME, suivre **Paramétrage > Matériel > Architecture matérielle [ARC]**.
2. Dans la table **Architecture matérielle** située dans la partie gauche de la fenêtre, localiser la catégorie **OSS offline**.
3. Faire un clic droit sur la ligne associée et sélectionner **Télécharger les accès sur toutes les bornes**.
4. Une fois les accès téléchargés sur la borne OSS, ceux-ci seront mis à jours dans tous les badges des identifiés lors de leur prochain passage sur la borne.

3.12. Téléchargement manuel des accès sur une borne OSS spécifique

1. À partir du menu principal de MICROSESAME, suivre **Paramétrage > Matériel > Architecture matérielle [ARC]**.
2. Dans la table **Architecture matérielle** située dans la partie gauche de la fenêtre, localiser la catégorie **OSS offline**.
3. Faire un clic droit sur la ligne correspondant à la borne à télécharger et sélectionner **Télécharger les accès sur cette borne**.

4. Une fois les accès téléchargés sur la borne OSS, ceux-ci seront mis à jours dans tous les badges des identifiés lors de leur prochain passage sur la borne.

Chapitre 4. Configuration de la borne offline OSS

4.1. 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 4.1. Borne offline OSS

La borne offline fonctionne uniquement en mode paysage.

La borne est équipée 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 dans 3 sous-menus :

- Maintenance
- Configuration
- System information

4.2. Configuration du mode de fonctionnement

4.2.1. 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 l'identifié porteur 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. Allumer la borne.
2. Ouvrir depuis le menu de paramétrage la section **Offline settings**.
3. Cocher la case *Encoding mode*.
4. Sélectionner le type de fonctionnement souhaité *UID copy* ou *CSV file*.
5. Fermer le menu.

Si le type *UID copy* a été sélectionné, la borne est prête à encoder des badges 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-tête "uid", cette colonne doit contenir pour chaque ligne l'uid du badge
- 2ème colonne : en-tête "credentialID", cette colonne doit contenir pour chaque ligne l'identifiant utilisé pour l'Offline OSS

Exemple :

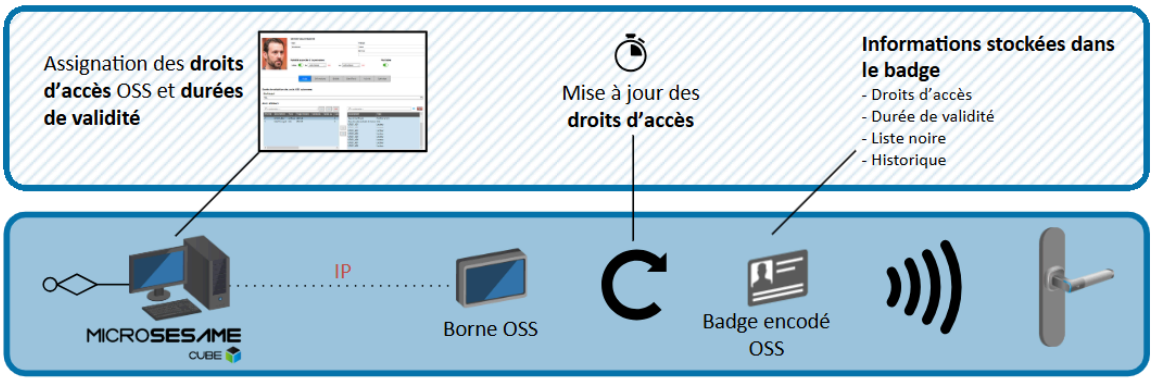
```
uid;credentialID
0444467afd5180;BB112233445566778899
7FED887AB4C56E;A589C56247252D5632D1
```

4.2.2. Mode mise 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 de récupérer les historiques/ alarmes présents dans les badges.

Pour configurer la borne en mode Mise à jour :

1. Allumer la borne.
2. Ouvrir depuis le menu de paramétrage la section **Offline settings**
3. Décocher la case *Encoding mode*
4. Fermer le menu.



4.2.3. 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 4.10, « 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 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. Allumer 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. Fermer le 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.

Si 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
```

4.3. Connexion à l'interface web de la borne

4.3.1. Prérequis de connexion

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

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) : • adresse IP commençant par 172.16.x.x (exemple : 172.16.5.240) • 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).

4.3.2. 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 Password : user
Installateur	NON	NON	**OUI**	**OUI**	**OUI**	**OUI**	Login : service 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 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'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.

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.

4.3.3. 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 n'est raccordé au 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, ouvrir 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 nécessaire lors de la première connexion des utilisateurs suivants:

- Service
- User

4.4. Résumé des caractéristiques de la borne

Ce résumé figure sur la page d'accueil du serveur web de la borne. Il est également accessible depuis l'onglet **System Information > Overview**.

Tableau 4.1. 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

4.5. 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 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.

4.6. 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.

4.7. 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 4.2. 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.

Types de certificats	Détails
	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 :** 1. L'intéressé génère un CSR (Certificate Signing Request) ou requête de signature de certificats 2. Il transfère cette requête à une autorité de confiance qui pourra garantir l'identité de l'intéressé 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 auto-signé 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.

Après que la requête CSR a été générée, 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 4.3. Ajouter un certificat signé

Etape	Details
Génération du CSR	**Pour ajouter un certificat signé :** 1. Cliquer sur le bouton **Generate CSR** 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 TILLYS ou à son nom d'hôte (host name) 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. 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. **Cette autorité de certification renvoie :** ● Le certificat signé ● Son propre certificat ou la **chaîne de certification**, s'il s'agît d'une autorité intermédiaire.
Ajout du certificat signé	**Suivre Configuration > Certificates :** 1. Dans la partie Certificate Signature Request, sélectionner le **CSR** 2. Cliquer sur **Parcourir** puis sélectionner le certificat signé correspondant 3. Cliquer sur **Replace CSR**  Le nom du fichier du certificat signé doit obligatoirement avoir le même nom que la requête CSR

Etape	Details
Ajout du certificat de l'autorité de certification ou chaine de certification	**Suivre Configuration > Certificates :** 1. Dans la partie CA certificates, sélectionner le **CSR** 2. Cliquer sur **Parcourir** puis sélectionner le certificat signé correspondant 3. Cliquer sur **Upload** Dans le cas d'une chaine de certifcation il est nécessaire d'importer tous les certifcats

Tableau 4.4. Compatibilité TLS pour UTL

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

4.8. Paramétrage réseau d'une borne OSS offline

1. Suivre **Configuration > Network**.
2. Renseigner les champs conformément aux tableaux ci-après.

Tableau 4.5. 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 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.

Paramètres	Détails
Gateway	Cette option est à configurer uniquement si le module doit pouvoir communiquer avec d'autres réseaux que le réseau local.

Tableau 4.6. Apps configuration

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

3. Pour appliquer la configuration, cliquer sur **Submit** .

4.9. Sécurité (HTTPS)

Cette page permet de paramétrer la connexion HTTPS au serveur web de la borne.

1. Suivre **Configuration > Security**.
2. Dans la partie HTTPS, sélectionner dans la liste déroulante le certificat à utiliser pour la connexion HTTPS au serveur web de la borne.

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

4.10. Configuration du contrôle d'accès offline

1. Suivre **Configuration > Access Control**.
2. Dans la partie General, chercher le nom de la borne offline tel qu'il est renseigné dans la configuration MICROSESAME. Par défaut, le nom de la borne est **Borne offline**.
   Ce nom ne peut pas être édité directement depuis le serveur web de la borne.
3. Renseigner les champs selon les tableaux ci-après.
   Cette configuration ne doit pas être modifiée après le passage d'un identifiant sur la borne.
   Chacun de ces paramètres 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.

Tableau 4.7. Connexion à MICROSESAME

Paramètres	Détails
MICROSESAME IP address	Renseigner l'adresse IP du serveur MICROSEAME

Paramètres	Détails
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 .

Tableau 4.8. 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. Ce paramètre peut être renseigné directement depuis cette page ou être téléchargé depuis MICROSESAME.
Site ID	Ce paramètre correspond à l'ID site encodé dans les badges OSS. Pour que l'identifié puisse mettre à jour ses droits sur la borne, il est nécessaire que l'ID du site sur son badge corresponde à celui déclaré sur la borne. Ce paramètre peut être renseigné directement depuis cette page ou être téléchargé depuis MICROSESAME.

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

Tableau 4.9. Offline parameters

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

Tableau 4.10. 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

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

4. Pour appliquer la configuration, cliquer sur **Submit** .

Chapitre 5. Configuration TILLYS CUBE, MLP-OSS et lecteurs actualisateurs

5.1. 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.

5.2. 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.

5.3. 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 Ce paramètre doit être configuré au format hexadécimal
Site ID	Numéro à personnalisé qui sera associé au site. Les accès qui seront inscrits dans le badge seront valide seulement pour les serrures offline configurées avec le même code site Ce paramètre doit être en configuré au format décimal
R/W key	Valeur de la clé AES de lecture/écriture utilisée dans le badge pour le système offline

5.4. 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 6. Gestion des serrures et cylindres OSS offline dans MICROSESAME

La gestion des lecteurs autonomes avec le standard OSS est disponible à partir de la version 2021.4 de MICROSESAME.

La mise en place d'une installation OSS nécessite un travail préliminaire de définition et de dimensionnement des différents éléments (accès, plages horaires, clés de sécurité, charte d'encodage...) et l'installation de matériels spécifiques (bornes de chargement des droits, lecteurs actualisateurs, lecteurs autonomes, ...) .

6.1. La norme OSS

OSS est une norme permettant d'interfacer MICROSESAME avec de nombreux équipements mécatroniques fabriqués par les divers constructeurs :

- ASSA ABLOY
- DEISTER
- DORMA KABA
- Zugang GmBH
- ...

Tableau 6.1. Éléments de l'architecture OSS centralisés dans MICROSESAME

Paramétrage	Exploitation	Supervision
• Déclaration et configuration des équipements par site (bornes, lecteurs actualisateurs, lecteurs, groupes de lecteurs) • Définition de la technologie associée et des durées de validité des accès attribuables • Encodage des badges	• Définition des plages horaires OSS • Attribution des accès et des durées de validité aux identifiés	• Visualisation de l'historique remonté depuis les bornes de chargement • Visualisation des évènements lecteurs remontés depuis la borne (exemple : pile faible)

La configuration des lecteurs offline ne peut pas être effectuée directement depuis MICROSESAME.

Les lecteurs autonomes installés sur sites nécessitent d'être configurés avec un outil fourni par le constructeur.

Exemple : APERIO avec PAP, KABA avec BCOMM

Par ailleurs, la configuration de la **borne de rechargement** des droits OSS s'effectue directement sur l'**interface web** de celle-ci.

Tableau 6.2. Équipements OSS offline

Équipements	Détails
Borne de chargement	**La borne de chargement reçoit la configuration OSS effectuée sur MICROSESAME :** ● Droits d'accès offline des identifiés ● Durées de validité des droits d'accès ● Liste noire ● ... **Lorsqu'un identifié passe son badge sur la borne :** ● Les droits d'accès sont mis à jours dans le badge ● La durée de validité des droits est mise à jour dans le badge ● La liste noire est actualisée dans le badge ● L'historique et les évènements lecteurs contenus dans le badge sont remontés à la borne puis à MICROSESAME.  MICROSESAME intègre une fonctionnalité **lecteur actualisateur** permettant de remplacer les bornes de chargement par des lecteurs de contrôle d'accès classiques, capables de jouer les 2 rôles : ● Mise à jour des droits OSS et remontées des informations relatives à l'OSS ● Contrôle d'accès sur site Pour plus d'informations, se référer à la section suivante: *Section 6.2, « Utilisation d'un lecteur actualisateur au lieu d'une borne OSS offline »*
Badge encodé OSS	L'exploitation d'OSS nécessite d'utiliser des badges encodés spécifiquement pour l'utilisation de lecteurs autonomes utilisant la norme OSS. **Données relatives à l'exploitation d'OSS encodées dans le badge :** ● Identifiants ● Droits d'accès OSS ● Durée de validité des droits ● Liste noire ● Historique (passages autorisés, interdits, ...)

Équipements	Détails
	• Évènements lecteurs (pile faible, ...)
Lecteurs autonomes	Les lecteurs autonomes ne nécessitent aucun câblage et sont installés dans la porte (cylindre, béquille ou serrure mécatronique). **Les informations suivantes sont stockées dans la serrure :** • Configuration tierce partie • Plages horaires • Liste noire (mise à jour à chaque passage de badge) La configuration du lecteur autonome et les outils associés varient selon le constructeur de l'équipement. **Exemple** : APERIO avec PAP, KABA avec BCOMM

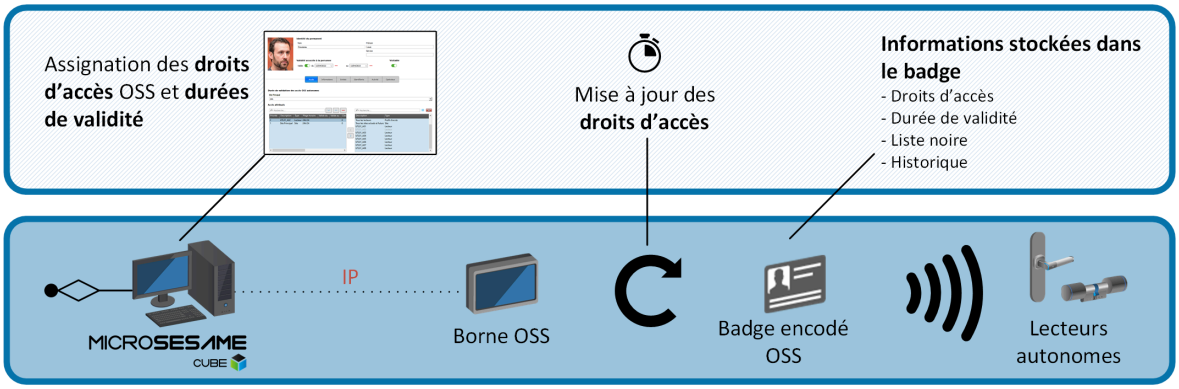


Figure 6.1. Schéma fonctionnel OSS

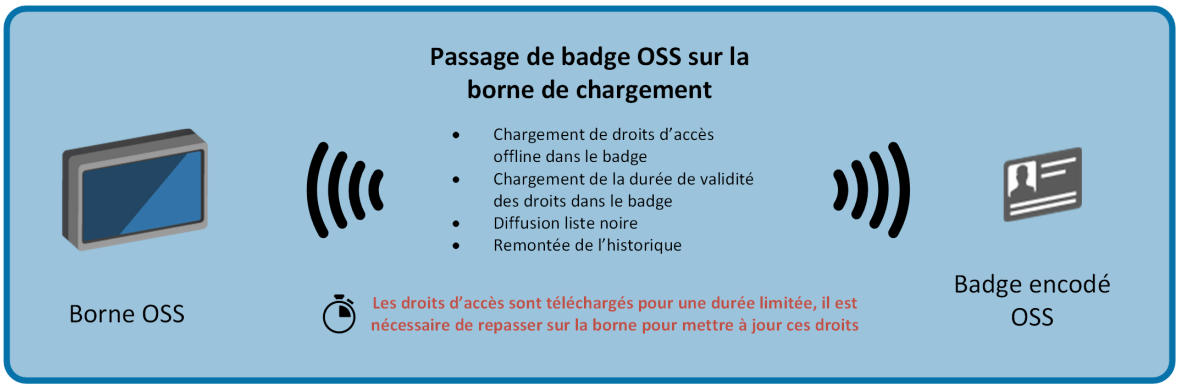


Figure 6.2. Mise à jour des droits OSS sur la borne de chargement

6.2. Utilisation d'un lecteur actualisateur au lieu d'une borne OSS offline

L'installation d'une borne de chargement de droits OSS offline impose aux identifiés de passer leur badge sur la borne régulièrement, afin de **mettre à jour leur droits d'accès** sur les lecteurs autonomes, qui remontent également l'historique de ces lecteurs à MICROSESAME.

Si, d'autre part, pour une raison quelconque, il n'a pas été choisi d'installer une borne de chargement des droits OSS offline, l'utilisation d'un lecteur actualiseur est possible.

- Utilisation d'un lecteur de contrôle d'accès classique installé sur site comme lecteur actualiseur.
- Ce lecteur permet, lors d'un passage de badge, de gérer simultanément le **contrôle d'accès** d'une porte et la **mise à jour des informations relatives à OSS**.
- Un même lecteur actualisateur peut traiter les passages de badges classiques, ceux des badges avec donnée sécurisée et les passages de badges OSS.
- L'installation d'un lecteur actualisateur nécessite le raccordement de modules spécifiques sur site et l'affectation d'un bus de la TILLYS à cette fonctionnalité. Pour plus d'informations, voir la *documentation du MLP2 UPDATER*.

6.3. Paramétrage d'OSS offline

Le paramétrage d'OSS offline, nécessite les opérations suivantes :

1. *Section 3.1, « Activation de la ligne OSS »*
2. *Section 3.2, « Configuration de la ligne OSS : identifiants et durée de validité »*
3. *Section 3.3, « Ajout et configuration d'une borne OSS offline »*
4. *Section 3.4, « Déclaration d'un lecteur actualisateur »*
5. *Section 3.5, « Ajout et configuration d'un lecteur OSS offline »*
6. *Section 3.6, « Ajout et configuration d'un groupe de lecteur OSS offline »*
7. *Section 3.7, « Ajout d'identifiants dans la liste noire »*
8. *Section 3.10, « Application de la configuration OSS »*

6.3.1. Activation de la ligne 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 gérés par le serveur MICROSESAME.

L'activation de la ligne OSS offline permet de rendre visible ses paramètres :

- Définir une plage horaire OSS
- Attribuer les accès OSS dans la fiche d'un identifié

1. Depuis le menu principal de MICROSESAME, suivre **Paramétrage > Matériel > Architecture matérielle [ARC]**.
2. Dans la table **Architecture matérielle** située dans la partie gauche de la fenêtre, cliquer sur **OSS offline**.
3. Dans la section Paramètres généraux, cocher la case **Activation de la ligne OSS offline**.
4. Sélectionner la **technologie associée aux bornes OSS**.
5. Cliquer sur l'icône Enregistrer et continuer en *Section 3.2, « Configuration de la ligne OSS : identifiants et durée de validité »*.

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. En effet, la modification de ce paramétrage sur un site en exploitation nécessite un nouvel encodage des badges, pour pouvoir continuer à utiliser les lecteurs autonomes.

6.3.2. Configuration de la ligne OSS : identifiants et durée de validité

L'identifiant est généré lors de l'encodage des badges OSS par le script MICROSESAME.

1. Depuis le menu principal de MICROSESAME, suivre **Paramétrage > Matériel > Architecture matérielle [ARC]**.
2. Dans la catégorie OSS offline, cliquer sur la ligne du site à paramétrer.

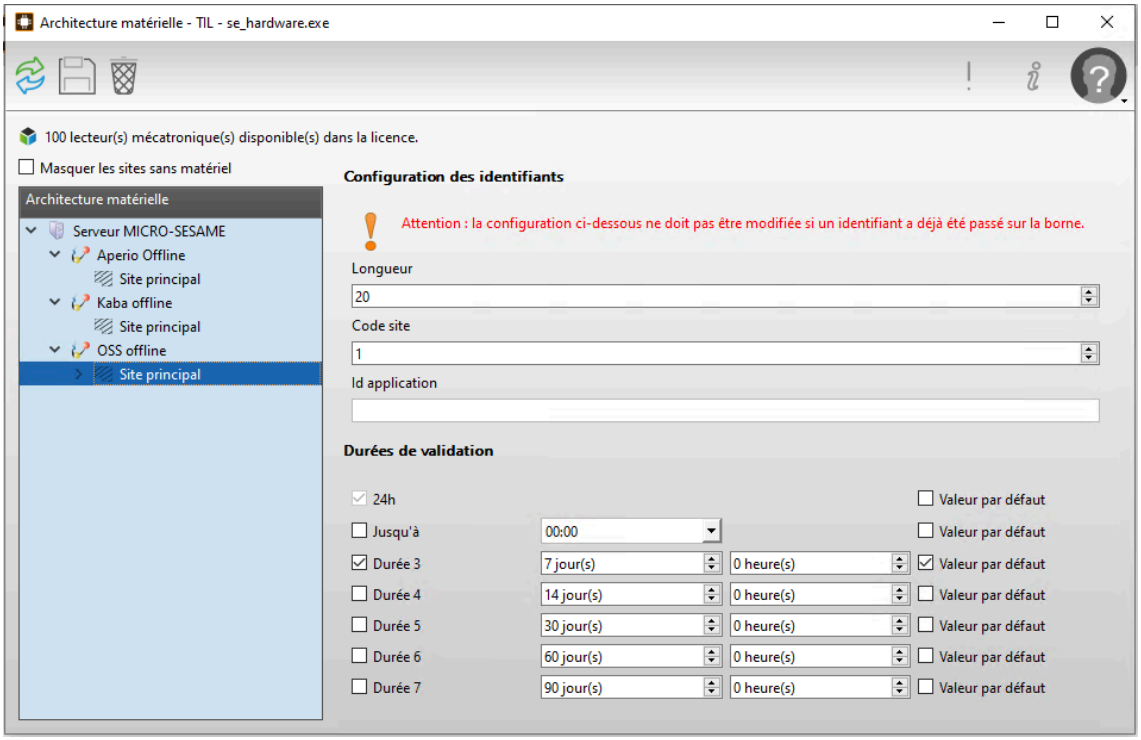


Figure 6.3. Paramétrage d'un site en OSS

3. La longueur de l'identifiant n'est pas modifiable et est fournie à titre indicatif.
4. Renseigner le code site choisi lors de l'encodage des badges OSS.
5. Paramétrer les durées de validité désirées et cocher la case associée, pour qu'elles puissent être distribuées lors de l'assignation d'un accès OSS dans la fiche de l'identifié.

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

6. Cliquer sur l'icône  Enregistrer.

Si la case **Jusqu'à** est activée sur une certaine heure, le fonctionnel sera le 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.

Si l'encodage des badges est effectué avec un script personnalisé, respecter le format suivant :

- DECIMAL
- 20 caractères
- Remplissage à gauche (si l'identifiant fait moins de 20 caractères, il sera complété par des 0 en début d'identifiant).

6.3.3. Ajout et configuration d'une borne OSS offline

Les bornes OSS offline proposent deux modes de fonctionnement :

- 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 ...).
- Borne en mode "mise à jour" : permet de mettre à jour les droits d'accès OSS pour une période définie, d'écrire la liste noire et de récupérer les alarmes/historiques d'un badge.

Pour configurer le mode de fonctionnement d'une borne OSS, utiliser son serveur web.

1. À partir du menu principal de MICROSESAME, suivre **Paramétrage > Matériel > Architecture matérielle**.
2. Dans la table **Architecture matérielle** située dans la partie gauche de la fenêtre, localiser la catégorie **OSS offline**.
3. Dans la catégorie **OSS offline**, effectuer un clic-droit sur la ligne correspondant au **site d'appartenance**.

4. Dans le menu contextuel, sélectionner **Ajouter une borne**.
5. Une nouvelle borne apparaît dans la table, cliquer sur la ligne correspondante.
6. Cocher la case **Activé** pour activer la borne.
7. Sélectionner le mode d'adressage IP (**IP fixe** ou **DHCP**).
8. Renseigner l'information de connexion associée (**Adresse IP** ou **Nom d'hôte**)
9. Modifier si besoin le port de communication proposé (par défaut 20300).

Pour pouvoir renommer une borne, faire un double clic sur son nom dans la partie gauche de l'écran.

Si le port de communication par défaut est modifié, la même modification doit être effectuée au niveau de la TILLYS. Pour connaître la procédure de connexion de la TILLYS à son serveur web, consulter son aide en ligne.

6.3.4. Déclaration d'un lecteur actualisateur

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

Le lecteur actualisateur doit être un lecteur transparent SSCPv2 ou SSCPv1 (voir *SSCP*), câblé sur un MLP-OSS CUBE. Il permet :

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

1. Depuis le menu principal de MICROSESAME, suivre **Paramétrage > Matériel > Lecteur [LEC]**.

   ou

   Depuis le menu principal de MICROSESAME, suivre **Paramétrage > Matériel > UTL (unité de traitement logique) [UTL]**, cliquer sur la ligne de l'UTL, puis sur l'onglet **Contrôle d'accès**.
2. Créer un nouveau lecteur ou sélectionner le lecteur à paramétrer.
3. Depuis la fenêtre de configuration du lecteur ou directement dans la liste des lecteurs, cliquer sur le commutateur dans la colonne **Actualisateur OSS**.
4. Vérifier que le lecteur est **activé** et possède une **licence** .
5. Depuis le menu principal de MICROSESAME, suivre **Paramétrage > Matériel > Architecture matériel [ARC]**).
6. Dans la catégorie **OSS offline** cliquer sur **lecteurs actualisateurs**.
7. Vérifier que le lecteur paramétré est présent dans la table et qu'il est activé.

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

6.3.5. Ajout et configuration d'un lecteur OSS offline

Un lecteur autonome OSS offline correspond à une serrure, un cylindre ou une poignée encastrée dans une porte permettant d'autoriser ou de refuser le passage à un identifié lorsqu'il passe un badge.

Ces lecteurs ne peuvent pas être téléchargés ou supervisés en direct depuis MICROSESAME : ils sont **autonomes** sur site et évitent de devoir câbler un lecteur.

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

Chaque lecteur *mécatronique* (également appelé *lecteur 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 MICROSESAME 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.

1. Depuis le menu principal de MICROSESAME, suivre **Paramétrage > Matériel > Architecture matérielle [ARC]**.
2. Dans la table **Architecture matérielle** située dans la partie gauche de la fenêtre, localiser la catégorie **OSS offline**.
3. Dans la catégorie **OSS offline**, faire un clic droit sur la ligne correspondant au **site d'appartenance**.
4. Dans le menu contextuel, sélectionner **Ajouter un lecteur**. Un nouveau lecteur apparaît dans la table.
5. Cliquer sur la ligne de ce lecteur.
6. Renseigner le champ **Lock ID** conformément à la configuration effectuée dans l'outil tiers (outil constructeur de configuration des lecteurs).
7. Saisir éventuellement un commentaire.
8. Sélectionner éventuellement la classification associée, depuis la liste déroulante.

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

Pour pouvoir renommer un lecteur, faire un double clic sur son nom dans la partie gauche de l'écran.

6.3.6. Ajout et configuration d'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 MICROSESAME 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.

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

L'affectation des lecteurs aux groupes dans MICROSESAME est uniquement à but informatif (visualisation de la configuration effectuée dans l'outil tiers) et n'a aucun impact lors du téléchargement des accès.

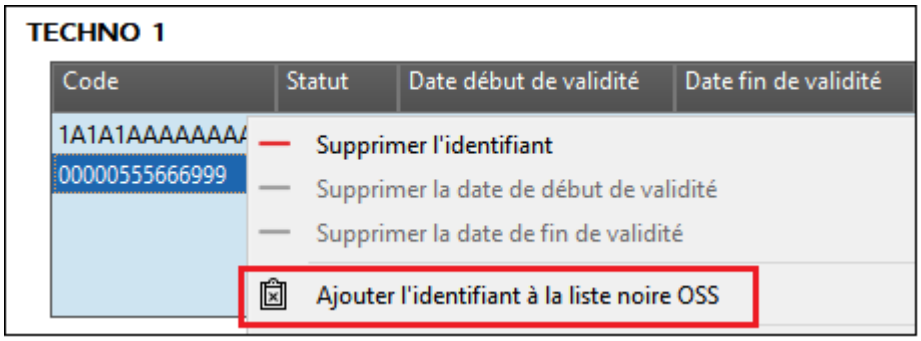
Cette opération est effectuée directement depuis l'outil de configuration tiers, lors de la configuration des lecteurs.

Double cliquer sur un groupe de lecteur dans la table située dans la partie gauche de la fenêtre pour le renommer.

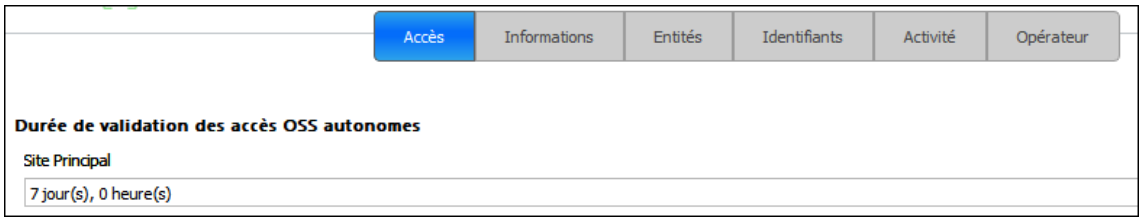
6.3.7. Ajout d'identifiants dans la liste noire

L'exploitant peut créer et de diffuser dans les serrures OSS une liste noire, c'est à dire une liste de badges (perdus ou volés) auxquels l'accès sera refusé. .

1. Depuis le menu principal de MICROSESAME, suivre **Exploitation > Identifiés [IDE]** , puis cliquer sur l'onglet **Identifiants**.
2. Dans le tableau de la technologie correspondante, faire un clic droit sur l’identifiant à interdire et sélectionner **Ajouter l'identifiant à la liste noire OSS**.



3. Dans l'onglet **Accès**, définir la durée **Durée de validation des accès OSS autonomes**. Il est conseillé de définir la date d'expiration au minimum à la date et à l'heure actuelles.



4. Changer le statut de l'identifiant (perdu, volé, etc ...) ou, si le badge ne doit plus jamais être utilisé par l'identifié après la date d'expiration paramétrée précédemment, le supprimer de la fiche identifié.
5. Cette liste noire est transmise aux serrures OSS par simple passage de badge utilisateur OSS, d'abord sur la borne OSS ou le lecteur actualisation, puis sur les serrures OSS (voir *Section 3.8, « Mise à jour de la liste noire sur les serrures OSS / transmission de l'historique à MICROSESAME »*).

6.3.8. Mise à jour de la liste noire sur les serrures OSS / transmission de l'historique à MICROSESAME

1. Déclarer un identifiant dans la liste noire (voir *Section 3.7, « Ajout d'identifiants dans la liste noire »*).
2. Passer un badge utilisateur OSS (autre que le badge en question) sur une borne OSS ou un lecteur actualisateur.
3. Passer le badge utilisateur OSS sur une serrure OSS. La liste noire est chargée sur la serrure OSS et son historique est copié en retour sur le badge.
4. Au prochain passage du badge sur la borne OSS ou sur le lecteur actualisateur, l'historique présent sur la carte est copié et envoyé à MICROSESAME.

6.3.9. Application de la configuration OSS

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.

Continuer avec *Section 3.11, « Téléchargement manuel des accès sur toutes les bornes OSS »* ou *Section 3.12, « Téléchargement manuel des accès sur une borne OSS spécifique »*.

6.3.10. Téléchargement manuel des accès sur toutes les bornes OSS

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

Il est possible de télécharger manuellement les identifiants ainsi que les accès associés dans les bornes OSS (ou lecteurs actualisateurs). Contrairement au **téléchargement de la configuration**, le téléchargement des accès est une opération courante d'exploitation.

1. À partir du menu principal de MICROSESAME, suivre **Paramétrage > Matériel > Architecture matérielle [ARC]**.
2. Dans la table **Architecture matérielle** située dans la partie gauche de la fenêtre, localiser la catégorie **OSS offline**.
3. Faire un clic droit sur la ligne associée et sélectionner **Télécharger les accès sur toutes les bornes**.
4. Une fois les accès téléchargés sur la borne OSS, ceux-ci seront mis à jours dans tous les badges des identifiés lors de leur prochain passage sur la borne.

6.3.11. Téléchargement manuel des accès sur une borne OSS spécifique

1. À partir du menu principal de MICROSESAME, suivre **Paramétrage > Matériel > Architecture matérielle [ARC]**.
2. Dans la table **Architecture matérielle** située dans la partie gauche de la fenêtre, localiser la catégorie **OSS offline**.
3. Faire un clic droit sur la ligne correspondant à la borne à télécharger et sélectionner **Télécharger les accès sur cette borne**.
4. Une fois les accès téléchargés sur la borne OSS, ceux-ci seront mis à jours dans tous les badges des identifiés lors de leur prochain passage sur la borne.

Chapitre 7. Gestion des accès OSS Offline

7.1. Attribution d'accès offline

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

Tableau 7.1. 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.  Déclarer la technologie à utiliser pour les serrures OSS offline.
2	Création des identifiés	MICROSESAME CUBE WEBSESAME CUBE	La création d'identifiés susceptibles d'utiliser les équipements offline se fait directement dans la gestion des identifiés depuis MICROSESAME ou WEBSESAME.
3	Assignation des identifiants offline	MICROSESAME CUBE WEBSESAME CUBE	L'assignation des identifiants offline se fait directement dans la gestion des identifiés depuis MICROSESAME ou WEBSESAME.  Ajouter les identifiants pour la technologie définie dans l'interface de paramétrage OSS.
4	Assignation des accès OSS offline	MICROSESAME CUBE WEBSESAME CUBE	L'assignation des accès aux serrures et groupes de serrures se fait directement dans la gestion des identifiés depuis MICROSESAME ou WEBSESAME.  Dans MICROSESAME il est nécessaire d'afficher les accès offline pour les assigner. Effectuer un clic-droit puis afficher les accès ou groupes d'accès correspondant.  L'assignation des accès OSS offline supporte uniquement les plages horaires définies OSS . Ceux-ci ne peuvent avoir de dates de validité.

7.2. 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 MICROSESAME.
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 de MICROSESAME, suivre **Exploitation > Contrôle d'accès > Identifiés [IDE]**
2. Cliquer sur la fiche de l'identifié puis dans l'onglet accès.
3. **Attribuer 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.