HIRSCH

MICROSESAME - GUIDE DE L'EXPLOITANT

Référence du document : GU-15001-FR

Date de publication : 05/03/2026

Table des matières

Liste des illustrations

Liste des tableaux

Préface

1. Contexte d'utilisation de ce manuel

Un partenaire HIRSCH a installé MICROSESAME et formé l'exploitant aux opérations de base.

Pour l'opération préliminaire d'installation, voir le Guide de démarrage rapide de MICRO-SESAME (GD-10001-FR).

Les tâches de configuration, qui ne relèvent pas de l'exploitation au quotidien, sont détaillées dans l'aide en ligne.

Ce guide décrit les tâches d'exploitation.

2. Réserve de propriété

Les informations contenues dans ce document peuvent être modifiées sans avertissement.

Les informations citées dans ce document à titre d'exemple, ne peuvent en aucun cas engager la responsabilité de la société HIRSCH Secure SAS (nommée HIRSCH dans les documents techniques). Les sociétés, noms et données utilisés dans les exemples sont fictifs, sauf notification contraire.

Toutes les marques citées sont des marques déposées de leurs propriétaires respectifs.

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

Merci d'envoyez vos commentaires, corrections et suggestions concernant ce document à *documentation@hirschsecure.fr*, en précisant son numéro de référence, sa date et le numéro des pages concernées.

3. Glossaire

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

API	Acronyme anglais de "Application Programming Interface" (interface de programmation d'application). Ensemble normalisé d'éléments informatiques intégrés à MICROSESAME qui permettent de mettre à disposition des services et ainsi de faire communiquer MICROSESAME avec d'autres logiciels.
API REST	Interface de programmation d'application utilisée en environnement client-serveur, qui respecte un ensemble de spécifications de format et de principes de conception, tout en restant suffisamment souple, sûre et rapide.
Base de données	Ensemble de données structurées stocké dans un système électronique, conçu pour pouvoir en gérer et récupérer facilement le contenu.

Client léger	Ordinateur sur lequel l'exploitation de la solution MICROSESAME est effectuée sans aucune installation préalable, au travers de son application WEBSESAME, affichée à l'aide d'un simple navigateur.
Client lourd	Ordinateur sur lequel la version cliente de MICROSESAME est installée.
DSSI	Le Directeur de la Sécurité des Systèmes Informatiques d'un site est en charge de la sécurité du réseau informatique de son entreprise : accès à Internet, firewall, gestion des adresses IP, des protocoles, de la sécurité des ports, de la protection contre les virus, etc.
Firewall	Voir *Pare-feu*.
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.
Migration	La migration d'un serveur consiste à faire évoluer la version principale de MICROSESAME, et elle se décompose en deux étapes : - La mise à jour des programmes de MICROSESAME vers une version supérieure. - La migration de la base de données déjà installée, pour prendre en compte les évolutions et les corrections apportées par la mise à jour.
Pare-feu	Fréquemment désigné sous son nom anglais "Firewall", il s'agit d'un outil de sécurisation de l'ordinateur sur le réseau (privé ou internet). Souvent présenté sous forme d'application logicielle, le pare-feu a pour but de n'ouvrir que les ports nécessaires aux différentes applications installées et de bloquer toute émission ou réception de données par ceux-ci sans autorisation de la part de l'utilisateur.
Port	Point d'entrée à un service (service web, service DNS, service mail...) sur un équipement (PC, serveur...) connecté

	à un réseau. Les ports constituent des accès entrants ou sortants et ils permettent aux différents logiciels et/ou systèmes d'exploitation de communiquer entre eux.
Port réseau	Point d'entrée à un service (service web, service DNS, service mail...) sur un équipement (PC, serveur...) connecté à un réseau. Les ports constituent des accès entrants ou sortants et ils permettent aux différents logiciels et/ou systèmes d'exploitation de communiquer entre eux.
Port TCP	Point d'entrée TCP (Transmission Control Protocol). TCP est le principal protocole réseau utilisé par les connexions Internet. C'est un protocole de transport au même titre que l'UDP, sauf qu'il travaille en mode connecté. Les données transmises sont donc vérifiées.
Port UDP	Point d'entrée UDP (User Datagram Protocol). Le protocole UDP est l'un des deux principaux protocoles utilisé sur les réseaux TCP/IP (avec TCP), que le réseau soit Ethernet ou sans fil. Contrairement au TCP, il ne permet pas à l'émetteur de vérifier si les données sont effectivement reçues en recevant un accusé de réception.
Poste client	Ordinateur hébergeant la version cliente du logiciel *MICROSESAME* (on parle parfois de "client lourd"), qui envoie des requêtes au poste serveur MICROSESAME.
Poste serveur	Ordinateur hébergeant la version serveur du logiciel *MICROSESAME* et sur lequel est également souvent installé la base de données SQL.
Protocole de communication	Ensemble de règles et conventions permettant la communication et l'interopérabilité entre différents systèmes informatiques. Le protocole définit la structure du message envoyé au destinataire. Les protocoles suivants sont utilisables entre la TILLYS et un centre de télésurveillance : • CESA 200: chaque événement transmis est constitué d'un code numérique de 01 à 96. • ID-Contact: chaque événement est constitué de deux codes numériques, un code de type ou de catégorie de 001 à DDD et un deuxième code de type d'événement pour un type donné de 001 à 999. Celui-ci permet également de transmettre le numéro de l'utilisateur mettant en/hors service un groupe.
Restauration	Cette opération consiste à restaurer/ré-installer une base de données à partir d'une sauvegarde réalisée au préalable.
SSL	Acronyme anglais de Secure Socket Layer. La technologie SSL basée sur le protocole HTTPS, est désormais remplacé par *TLS*, plus sécurisé et plus fiable.

TILLYS	Automate *IP* programmable multifonction développé par HIRSCH 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*.
TSE	Acronyme anglais de Terminal Server Edition. TSE est un composant de MICROSOFT Windows qui permet à un utilisateur d'accéder à des applications ou a des données stockées sur un ordinateur distant au moyen d'une connexion réseau.
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 HIRSCH est la *TILLYS*, qui se décline en version V2, NG et CUBE.
VLAN	Acronyme anglais de Virtual Local Area Network. Un VLAN est un réseau local virtuel regroupant un ensemble de machines de façon logique et non physique. Grâce aux réseaux virtuels (VLAN) il est possible de s'affranchir des limitations de l'architecture physique (contraintes géographiques, contraintes d'adressage, ...), en définissant une segmentation logique (logicielle) basée sur un regroupement de machines grâce à des critères spécifiques (adresses MAC, numéros de port, protocoles, etc.).
VPN	Acronyme anglais de Virtual Private Network Le VPN, ou réseau virtuel privé, est un tunnel sécurisé à l'intérieur d'un réseau (comme Internet par exemple). Au sein d'un VPN, les données sont chiffrées entre les interlocuteurs, garantissant la confidentialité et l'intégrité de leurs échanges.
Web server	Un des deux services Windows devant être installé et démarré pour le bon fonctionnement de MICROSESAME. Son rôle est de donner accès à WEBSESAME et de gérer toute les communications entre le serveur et les postes clients.
WEBSESAME	Application web du logiciel MICROSESAME. Elle permet l'exploitation d'une grande partie des fonctions de MICROSESAME à l'aide d'un simple navigateur internet (Edge, Chrome, Firefox, Safari...). On la désigne parfois sous le nom de *client léger*.

Chapitre 1. Contexte d'intervention

1.1. Le menu principal de MICROSESAME

Le menu principal de MICROSESAME permet l'accès à l'ensemble des applications qui forment MICROSESAME.

1.1.1. Lancer le menu principal

Le lancement de MICROSESAME se fait en double-cliquant sur l'icône du raccourci "Menu Principal" disposé sur le bureau.

Dès le lancement de l'application MICROSESAME, vous devez vous authentifier en saisissant vos informations de connexion opérateur.

Au bout de trois saisies erronées, le système enregistre un événement "Tentative de connexion infructueuse".

Login et mot de passe par défaut. Lors d'une **nouvelle installation** de MICROSESAME, le login et le mot de passe sont :

- Login : "admin"
- Mot de passe : correspond au mot de passe saisi lors de l'installation

Lors d'une **migration** de MICROSESAME, le login et le mot de passe sont :

- Login administrateur : "admin"
- Mot de passe administrateur : correspond au mot de passe saisi auparavant par l'administrateur

- Login opérateur exploitant : correspond au "nom prénom"* saisi dans la fiche opérateur (anciennement fiche Agent).
- Mot de passe opérateur exploitant : correspond au mot de passe saisi auparavant de cet opérateur (anciennement Agent).

Dans le cas où l'opérateur n'a pas saisi son prénom dans la fiche opérateur, le login correspondra simplement au "nom" de cet opérateur.

Si plusieurs profils opérateurs sont disponibles pour l'utilisateur, une liste permet de sélectionner le profil opérateur souhaité pour ouvrir la session :

Sélectionner un profil opérateur de la liste et appuyer sur "Connexion".

1.1.2. Présentation du menu principal

- **Partie supérieure** (fond noir) :
  - Zone d'affichage des logos (personnalisable). Dans l'image ci-dessus, le logo "MICROSESAME" est affiché. Cette image correspond à l'affichage par défaut.
  - **?** permet d'accéder à l'aide MICROSESAME.

- L'identification de l'opérateur est constamment visible (Dans l'image, "ADMINISTRATEUR"), afin de reconnaître rapidement la session en cours.

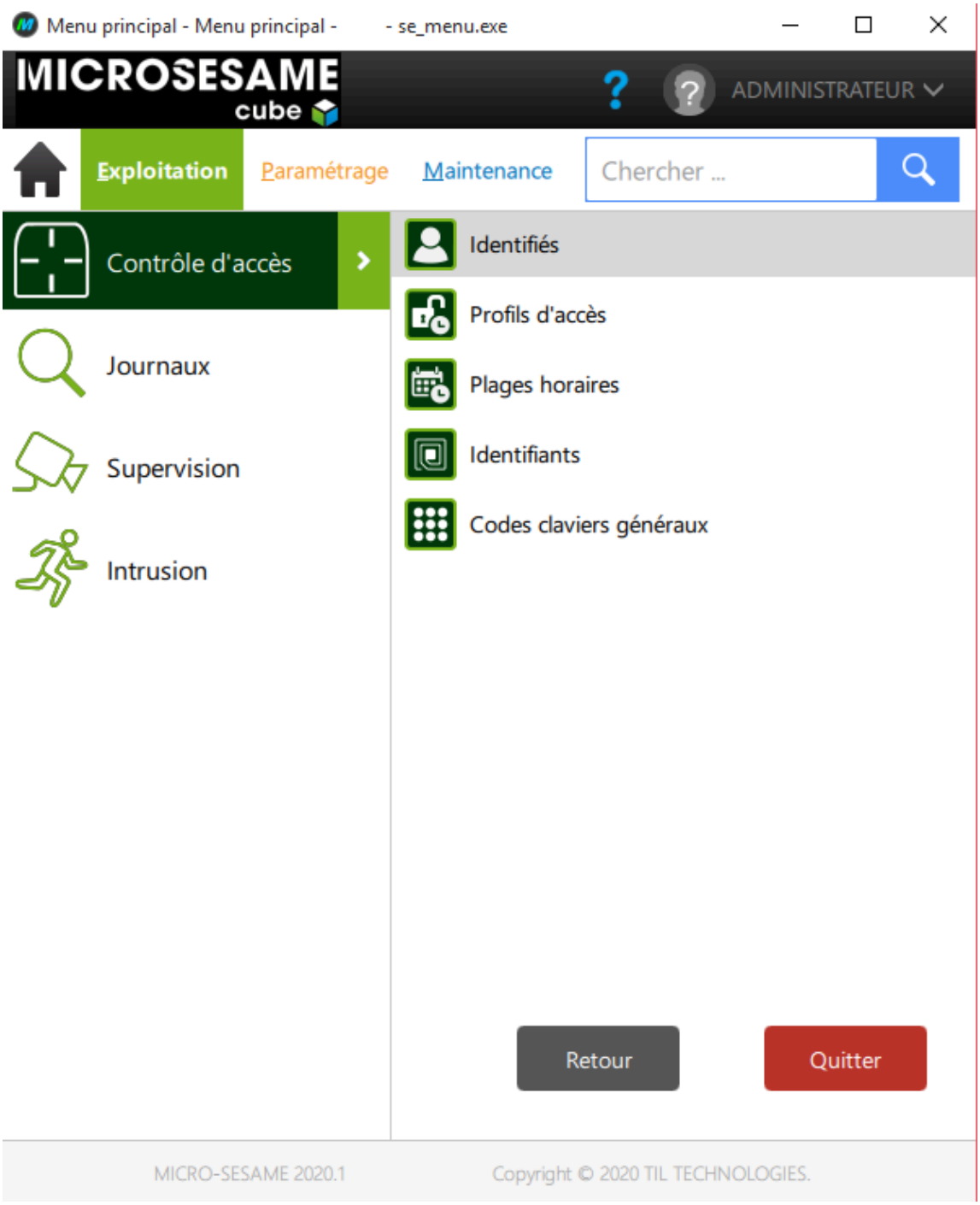
  Cliquer sur l'opérateur pour :
  - consulter et modifier les informations de l'opérateur.
  - changer le mot de passe. Lors du changement du mot de passe, la saisie est limitée à 16 caractères (Lettres, chiffres, caractères spéciaux).
  - se déconnecter ou changer d'opérateur.
- Une icône "i" permet d'accéder à la présente aide en ligne de MICROSESAME.

- **Partie centrale** (onglets contenant les applications) :
  Cette zone permet l'accès aux différentes applications qui composent MICROSESAME.
  L'icône **Accueil** permet d'afficher les applications sélectionnées comme **Favoris**.
  Pour sélectionner une application et l'ajouter aux Favoris, cliquer sur l'étoile au survol des applications.
  3 groupes d'applications sont disponibles : Applications d'exploitation (vert), applications de paramétrage (orange) et applications de maintenance (bleu).
  Pour retrouver une application, naviguer dans les différents onglets pour afficher la liste d'applications ou utiliser la barre de recherche avec le mot clé souhaité.

  Lors de la recherche, une même application peut s'afficher deux fois : 1 résultat correspondant au paramétrage de l'application, 1 résultat correspondant à l'exploitation de l'application.

  Chaque onglet contient un menu avec la liste d'applications :



L'accès à l'onglet **Maintenance** nécessite des droits **Administrateur** pour l'opérateur avec la session en cours.

- **Partie inférieure** (bandeau gris):
  La partie de gauche affiche la version du logiciel MICROSESAME. Cliquer sur cette partie pour accéder à la fenêtre "A Propos" (Voir le chapitre "A Propos" pour plus de détails).

La partie de droite permet d'accéder au site web de HIRSCH . Cliquer sur cette partie, un navigateur s'ouvre pour charger le site web de HIRSCH .

Raccourcis clavier permettant de naviguer dans les onglets du Menu principal de MICROSESAME :

- ALT + h : Accueil
- ALT + e : Exploitation
- ALT + p : Paramétrage
- ALT + m : Maintenance
- CTRL + f : se positionner dans le champ de recherche

1.2. Profils opérateurs

1.2.1. Généralités

MICROSESAME propose une gestion native et très fine des profils opérateurs : chaque profil peut être paramétré selon les besoins métier et attribué à un ou plusieurs opérateurs puis à des sites, ou tags de sites.

Les profils opérateurs permettent de définir les droits d'utilisation du logiciel MICROSESAME pour les différents types d'opérateurs.

Un opérateur est un identifié qui a besoin de se connecter au système de contrôle d'accès MICROSESAME.

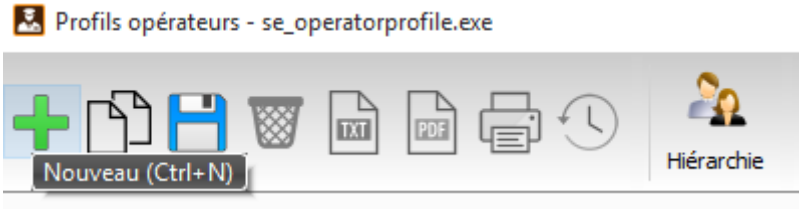
Un identifié dans le système MICROSESAME peut être déclaré en tant qu'opérateur depuis sa fiche identifié dans WS.

1.2.2. Créer un profil opérateur

Pour créer un profil opérateur, deux possibilités existent :

- **Dupliquer** un profil opérateur existant pour l'éditer :

- **Créer** un profil opérateur nouveau, à paramétrer :



Le **Nom** du profil opérateur aide à le retrouver lors des recherches dans la liste de profils opérateurs et à facilement sélectionner son profil au moment de la connexion.

Une description du profil peut être ajoutée dans le champ **Commentaire**.

Une fois le profil opérateur créé, vous pouvez lui *assigner des droits* puis attribuer ce profil à des identifiés permanents dans WS.

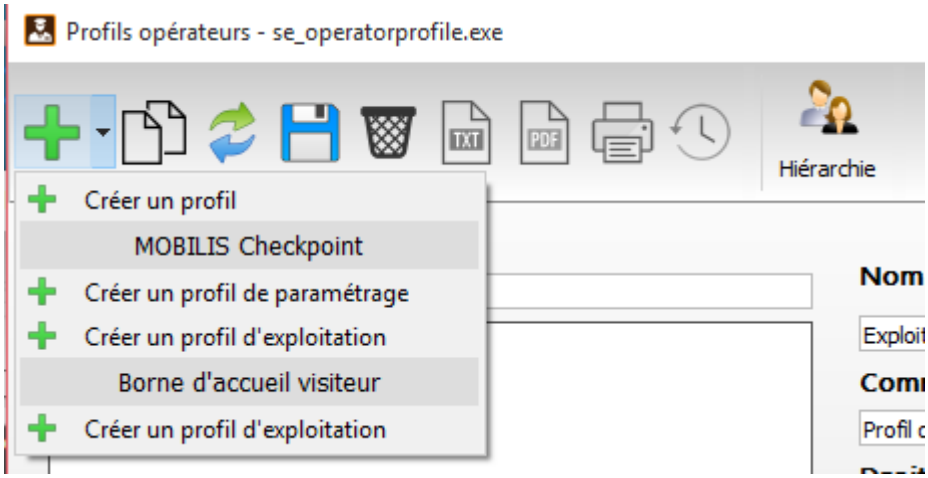
1.2.3. Créer un profil type

La création des profils opérateurs peut être accélérée avec les profils type.

Un profil opérateur type peut être modifié pendant ou après sa création.

Deux types de profils opérateurs prédéfinis sont proposés dans le cadre du paramétrage des terminaux MOBILIS : le profil de paramétrage et le profil d'exploitation.

1. Dans le menu principal de MICROSESAME, accédez à la fenêtre des profils opérateurs (Paramétrage > Système > Profils opérateurs).
2. Cliquez sur la flèche à droite de l'icône "+" (Créer un profil) pour déplier le menu.



3. Sélectionnez l'option "Créer un profil de paramétrage" ou "Créer un profil d'exploitation" pour créer les profils avec les droits opérateurs adaptés.
4. Enregistrez le profil.

1.2.4. Gérer les droits du profil opérateur

Un profil opérateur ne peut pas attribuer/modifier/supprimer un droit opérateur qu'il ne possède pas lui-même.

1. À partir du menu principal de MS, accédez à l'écran de paramétrage des **Profils opérateurs**.
2. Sélectionnez le profil opérateur que vous souhaitez paramétrer.
3. Dans la section **Droits**, cliquez sur l'onglet correspondant à la catégorie de droits opérateur que vous souhaitez définir pour ce profil.
4. Cochez les **droits opérateurs** nécessaires et enregistrez les modifications effectuées afin qu'elle soient prises en compte.

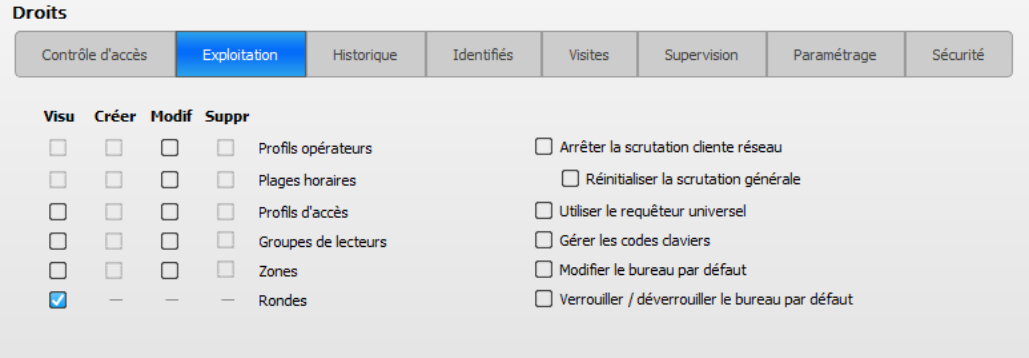
Pour certaines fonctionnalités, les droits associés à un profil opérateur peuvent être configurés selon quatre actions :

- **Visu** : consultation des données uniquement (pas de modification)

- **Créer** : création d'éléments de paramétrage
- **Modif** : modification d'éléments de paramétrage
- **Suppr** : suppression d'éléments de paramétrage

Vous pouvez attribuer un ou plusieurs de ces droits selon les besoins du site.

Par exemple, un profil opérateur peut uniquement avoir le droit de visualiser les informations, ou bien combiner les droits de visualisation et de suppression, sans être autorisé à la création ni à la modification.



1.2.5. Droits attribuables à un profil opérateur

1.2.5.1. Droits liés au contrôle d'accès

Pour attribuer un droit à l'opérateur, cochez la case correspondante.

Droit	Description
Alarme liste noire	L'opérateur peut recevoir des alarmes pour les identifiés en liste noire détectés sur passage de badge.
Observer surveillance des zones	L'opérateur peut accéder à la Surveillance des zones (surveillance des différentes zones du système de contrôle d'accès).
Forçage absence/présence d'un identifié dans une zone	L'opérateur peut ajouter ou supprimer des identifiés dans une zone.
Contrôle visuel des accès	L'opérateur a accès au PCVA
Interface Vidéo : consulter la vidéo enregistrée	L'opérateur peut consulter des vidéos générés sur l'enregistreur vidéo. L'opérateur peut accéder à l'Historique et à l'Animateur de synoptiques.
Interface Vidéo : affichage de la vidéo en temps réel	L'opérateur a accès à la vidéo en provenance de caméras en temps réel. L'opérateur peut accéder à l'Historique et à l'Animateur de synoptiques.

Droit	Description
Déclarer des passages de badges	L'opérateur à le droit de déclarer des passages de badges. Ce droit est utile aux applications tierces déclarant des passages de badges auprès de l'API REST (application de gestion de visiteurs, application checkpoint...).

1.2.5.2. Droits liés à l'exploitation

Quatre catégories d'action possibles sont disponibles pour ces droits. Pour plus d'informations, consultez la section *Gérer les droits du profil opérateur*.

Droit	Description
Utiliser les rapports	Accès à cette fonctionnalité dans WEBSESAME.
Gérer les codes claviers	L'opérateur peut accéder à la *Gestion avancée des codes claviers* (modification d'un code clavier déjà existant).

1.2.5.3. Droits liés à l'historique

Pour attribuer un droit à l'opérateur, cochez la case correspondante.

Droit	Description
Contrôle d'accès	L'opérateur peut consulter les options liées au contrôle d'accès dans Menu principal > Accès > Identifiés.
Événements techniques, Objets et propriétés de supervision	• L'opérateur peut consulter les événements techniques et les variables dans Menu principal > Journaux > Historiques. • L'opérateur peut visualiser la liste des tickets de suivi de main courante, consulter un ticket, e modifier et ajouter des notes.
Événements système	L'opérateur peut consulter les événements système dans Menu principal > Journaux > Historiques.
Audit des modifications	L'opérateur peut consulter l'audit des modifications Menu principal > Journaux > Historique.
Visites	L'opérateur peut consulter l'historique des visites **dans WEBSESAME** . Pour que l'option Visites apparaisse dans les menus **de WEBSESAME**, il faut impérativement que l'opérateur dispose également d'au moins une option

Droit	Description
	validée dans l'onglet du droit **Visites** , dans MICROSESAME (se reporter au paragraphe ***Droits liés aux visites - Option Accueil des visiteurs***) .

1.2.5.4. Droits liés aux identifiés

Quatre catégories d'action possibles sont disponibles pour ces droits. Pour plus d'informations, consultez la section *Gérer les droits du profil opérateur*.

Droit	Description
Identifiés	L'opérateur a accès aux options des identifiés dans Menu principal > Accès > Identifiés.
Validité d'un identifié	L'opérateur a accès à la validité des identifiés dans Menu principal > Accès > Identifiés.
Propriété visitable d'un permanent	L'opérateur a accès aux options d'accueil de visiteurs dans Menu principal > Accès > Identifiés.
Accès	L'opérateur peut consulter les options liées aux droits d'accès des identifiés dans Menu principal > Accès > Identifiés (Attributs, gestion spécifique, statut escorte...)
Code classe identifié	L'opérateur a accès aux options liées au code classe des identifiés dans Menu principal > Accès > Identifiés
Informations identifié	L'opérateur a accès aux données des identifiés.
Photo de profil identifié	L'opérateur peut visualiser la photo de l'identifié (présente dans la fiche identifié)
Identifiants	L'opérateur a accès aux données identifiants des identifiés dans Menu principal > Accès > Identifiants.
Code clavier personnalisé	L'opérateur peut consulter les options code clavier des identifiés dans Menu principal > Accès > Identifiés.
Habilitations	L'opérateur peut consulter les options liées aux habilitations appliquées aux identifiés dans Menu principal > Accès > Identifiés
Niveaux du mode crise	L'opérateur peut consulter les options liées au mode crise pour les identifiés
Opérateurs	L'opérateur peut consulter les données opérateur dans Menu principal > Accès > Identifiés.

Droit	Description
Contrôle temps de repos	L'opérateur peut consulter les options de temps de repos pour les identifiés dans Menu principal > Accès > Identifiés.
Entités	L'opérateur peut consulter les données concernant les entités dans Menu principal > Paramétrage > Contrôle d'accès > Entités.
Statut	L'opérateur peut attribuer des status aux utilisateurs (Normal, VIP, Indésirable) et consulter les status déjà attribués. Les status sont consultables et attribuables depuis Menu principal > Accès > Identifiés.
Intrusion	L'opérateur à accès aux fonctions d'intrusion.
Encoder des badges	L'opérateur peut encoder des identifiants pour les identifiés.
Encoder / enrôler biométrie	L'opérateur a accès aux options d'encodage/ d'enrôlement de la biométrie.
Organiser les listes dynamiques	L'opérateur peut organiser les listes dynamiques proposées par le système.
Dérogation horaire	L'opérateur peut visualiser/créer/modifier/ supprimer les dérogations horaires des identifiés permanents.

Si aucun de ces droits n'est attribué à un opérateur, mais qu'en revanche ce dernier possède des droits concernant la **gestion des rendez-vous**, il est alors considéré comme **utilisateur simple** dans le système. Dans ce cas, il lui sera possible :

1. De définir ou de visualiser des rendez-vous sur un nombre très limité d'identifiés (5 maximum)
2. Mais il ne pourra visualiser aucune des informations liées à ces identifiés, hormis les noms, prénoms et sociétés ou services.

1.2.5.5. Droits liés aux visites

Ces droits s'appliquent uniquement aux applications de gestion des rendez-vous / visites (client lourd et WEBSESAME).

Pour attribuer un droit à l'opérateur, cochez la case correspondante.

Droit	Description
Accueil des visiteurs	Permet l'accès à l'application **Réception visiteurs**. Des droits liés à l'accueil de visiteurs peuvent être paramétrés spécifiquement:

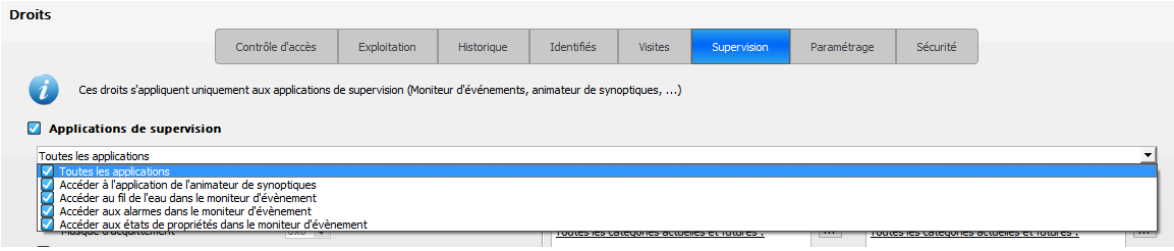
Droit	Description
	• Attribuer des accès : Permet de donner des autorisations d'accès aux visiteurs (Application web, menu Gestion de visiteurs). • Accéder à l'historique : Permet d'activer l'historique pour les visiteurs (Application web, menu Gestion de visiteurs). • Faire entrer des visiteurs sans rendez-vous : Permet la gestion de visiteurs sans rendez-vous planifié (Application web, menu Gestion de visiteurs).  Décocher l'option "Faire entrer des visiteurs sans rendez-vous" si l'objectif est d'assurer la validation de tous les rendez-vous sur site. • Visualiser statut : Permet à l'opérateur de consulter le champ Statut (informations des visiteurs que l'opérateur traite). • Modifier statut : Permet à l'opérateur d'éditer le champ Statut des visiteurs. • Consulter des rendez-vous validés du lendemain et des jours suivants : Permet de consulter les rendez-vous pour tous types d'identifiés pour les prochains jours. • Voir le statut escorte depuis la réception visiteurs • Modifier le statut escorte depuis la réception visiteurs  Une de ces options doit impérativement être validée, afin qu'un opérateur puisse accéder à l'historique des visites **dans WEBSESAME**. Il faut de plus que l'opérateur dispose du droit sur l'historique des visites, dans MICROSESAME (se reporter au paragraphe ***Droits liés à l'historique - Option Visites***).
Gestion des rendez-vous	Permet d'accéder à l'application **Gestion des rendez-vous**. Des droits liés à la gestion des rendez-vous peuvent être paramétrés spécifiquement: • Attribuer des accès : Permet de donner des autorisations d'accès aux visiteurs. • Prendre des rendez-vous pour tout le monde: Permet la gestion de visiteurs pour toute la hiérarchie du site.

Droit	Description
	• Consulter, modifier et supprimer les rendez-vous de tout le monde : permet de visualiser/éditer des rendez-vous pour toute la hiérarchie du site (Application web, menu Gestion de rendez-vous) • Valider les rendez-vous - Niveau 1 / Validation simple : Cette option permet à l'opérateur d'accéder à la validation de rendez-vous de premier niveau (1 seule étape de validation du rendez-vous par 1 opérateur seulement). La liste "Critères assignés à l'opérateur" permet d'indiquer les critères déclenchant le processus de validation pour l'opérateur. L'option "Tous" affichera à l'opérateur tous les rendez-vous associés à un ou plusieurs critères de la liste pour validation. • Valider les rendez-vous - Niveau 2 uniquement : Ce droit permet de déclencher la validation de deuxième niveau pour l'opérateur (Deuxième étape de validation requise aux opérateurs ayant ce droit attribué pour la validation d'un rendez-vous). • Création/modification de visiteurs : L'opérateur a le droit d'ajouter ou éditer un visiteur existant dans l'application de gestion des rendez-vous. • Visualiser/modifier statut : L'opérateur a le droit de consulter ou d'éditer le champ statut des visiteurs. • Voir le statut escorte depuis la gestion des rendez-vous • Modifier le statut escorte depuis la gestion des rendez-vous Si l'opérateur est défini en tant qu'**utilisateur simple**, il ne lui sera possible de gérer des rendez-vous que pour un nombre très limité d'identifiés (5 maximum). Un opérateur est dit utilisateur simple lorsque : 1. Il possède les droits liés à la gestion des rendez-vous 2. Il ne possède pas de droit sur la visualisation des identifiés (voir le paragraphe **Droits liés aux identifiés**).

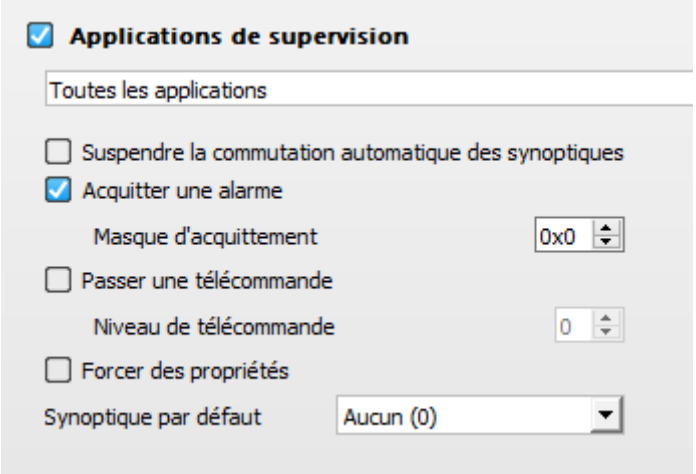
1.2.5.6. Droits liés à la supervision

Ces droits s'appliquent aux applications de supervision : Moniteur d'événements, animateur de synoptiques, ...

Applications de supervision permet à l'opérateur l'accès à toutes les applications de supervision. Pour obtenir l'accès à certaines applications seulement, déplier la liste et sélectionner les application(s) souhaitée(s).



Cocher les options pour les attribuer :



- **Suspendre la commutation automatique des synoptiques:** Ce droit a un impact sur l'animateur de synoptiques. L'opérateur peut empêcher provisoirement l'affichage automatique d'un synoptique en cas d'alarme (notamment dans le cas où trop d'alarmes se déclenchent).
- **Acquitter une alarme:** Ce droit a un impact sur l'animateur de synoptiques et sur le moniteur d'évènements. Cette option permet à l'opérateur acquitter des alarmes. L'opérateur peut acquitter les alarmes en cours en une seule opération.

  Ce droit permet aussi à l'opérateur d'ajouter un commentaire d'acquittement et de consulter le ticket de suivi associé à l'alarme lorsque celui-ci est encore ouvert.

- **Masque d'acquittement:** Ce droit a un impact sur l'animateur de synoptiques et sur le moniteur d'évènements. Cette option est disponible si **Acquitter une alarme** est sélectionnée. Ce droit permet de définir les alarmes que l'opérateur pourra acquitter en fonction du masque qui leur sera attribués (valeur max: 0x3F).

  Pour plus d'informations sur le paramétrage des masques d'acquittement, se référer à la section suivante:
  Partie 5: Supervision
  Chapitre 5: Moniteur d'évènement
  Section 1.2.3: Acquitter une alarme par plusieurs intervenants

- **Passer une télécommande:** Ce droit a un impact sur l'animateur de synoptiques et sur le moniteur d'évènements. Cette option permet à l'opérateur de passer des télécommandes lors que l'état des propriétés le permet.

- **Niveau de télécommande:** Ce droit a un impact sur l'animateur de synoptiques et sur le moniteur d'évènements. Cette option est disponible si **Passer une télécommande** est sélectionnée. "**Niveau de télécommande**" permet de définir les télécommandes que l'opérateur peut passer, avec le filtrage des télécommandes par niveau. La valeur minimale est de 0.
- **Forcer des propriétés:** Ce droit active l'option "Forcer la propriété". L'opérateur peut forcer la valeur des propriétés. Ce droit a un impact sur l'affichage des propriétés sur le moniteur d'évènements (onglet "Propriétés").
- **Synoptique par défaut** permet d'attribuer l'affichage par défaut d'un synoptique de la liste lors que l'opérateur lance l'animateur de synoptiques.

Le paramétrage des **catégories** permet de restreindre les droits d'un opérateur en fonction des catégories de propriétés, d'alarmes, de télécommandes ou de synoptiques qui lui auront été attribués.

Pour plus d'informations sur le paramétrage des propriétés, se référer à la section **Catégories opérateurs** de ce chapitre.

1.2.5.7. Droits liés à MOBILIS

La fenêtre **Profils opérateurs** de MICROSESAME a un onglet **MOBILIS** dédié : Cet onglet permet de paramétrer les droits opérateurs nécessaires à l'exploitation du terminal MOBILIS 2 avec l'application Checkpoint.

- **Exploiter** :
  Ce droit permet à l'opérateur l'utilisation du contrôle d'accès et du contrôle d'identité. Les opérateurs peuvent s'authentifier et utiliser l'application en mode en ligne ou en mode hors connexion (Pour le mode hors connexion, les données doivent avoir été synchronisées au préalable par un opérateur ayant ce droit).
- **Paramétrer** :
  Ce droit permet de paramétrer les informations qui seront utilisées avec l'application Checkpoint.
  Le droit de paramétrage permet la configuration de lecteurs, profils d'accès....
- **Gérer le mode hors connexion** :
  Ce droit permet la synchronisation de données seulement.
  La synchronisation de données permettra l'utilisation de ces données en mode hors connexion. Les données synchronisables sont soumises aux restrictions de droits opérateurs, qui doivent être paramétrés en fonction des besoins.
  L'utilisation des données synchronisées se fait par un opérateur d'exploitation.
  L'opérateur de synchronisation est spécifique à la synchronisation des données seulement et permet de synchorniesr les opérateurs possédant le droit "Exploiter".

Au survol de chaque droit, une description détaillée est disponible.

Enregistrer les modifications avant de quitter la fenêtre des Profils opérateurs.

1.2.5.8. Droits liés au paramétrage

Pour attribuer un droit à l'opérateur, cochez la case correspondante.

Droit	Description
Paramétrage général	L'opérateur peut visualiser/modifier le paramétrage général de *MICROSESAME* (options du contrôle d'accès, matériels, voies, synoptiques, sites, entités, zones horaires, passerelles, ...) dans Menu principal > Paramétrage. Autres droits associés par défaut : Microcode, Plages horaires et Jours Fériés, Mise à l'heure, Codes claviers.
Utiliser les opérations de maintenance	Le droit d'effectuer des opérations de maintenance est strictement réservé à l'opérateur Administrateur (Menu principal > Maintenance).
Modification/Visualisation des applets	Les options modification et visualisation des applets sont liées mais peuvent être cochées séparément.
Filtrage des sites lecteurs/entités identifiés/classification des accès	Il est possible de sélectionner des sites lecteurs, entités identifiés ou classifications des accès auxquels l'opérateur ayant ce droit auront accès.

1.2.5.9. Droits liés à la sécurité

Pour attribuer un droit à l'opérateur, cochez la case correspondante.

1.3. Classification des accès

1.3.1. Introduction

Sur les installations de contrôle d'accès comportant de nombreux lecteurs, groupes de lecteurs, profils d'accès, serrures, ..., il peut être intéressant de limiter la vision (mais aussi les droits) des opérateurs afin de leur faciliter l'exploitation et l'attribution des droits d'accès.

La classification des accès est un filtre permettant de limiter le choix d'un opérateur parmi des catégories définies préalablement.

L'organisation pourra se faire en groupant les éléments d'accès (par exemple par type d'accès, par droits d'attribution ou par zone géographique (bâtiment, établissement ...).

Cette notion de classification reste souple de manière à ce qu'elle puisse s'appliquer de manière simple aux besoins de chaque client.

Elle peut être mise en œuvre à tout moment, sans remettre en cause le paramétrage déjà réalisé.

L'opération de classification des accès se réalise en trois temps :

1. Déclaration des classifications qui seront utilisées.
2. Affectation des classifications déclarées aux différents types d'accès (lecteurs, groupes de lecteurs, étages ascenseurs, serrures, profils d'accès, ...).

3. Attribution des classifications visibles pour chaque opérateur MICROSESAME en mesure d'attribuer des accès.

L'exemple décrit dans ce chapitre est basé sur le filtrage de droits pour 4 opérateurs responsables de l'attribution des accès avec des niveaux hiérarchiques différents:

- Accueil: Distribution des droits sur les lecteurs concernant la circulation dans les locaux,
- RH: Distribution des droits standards aux salariés + droits accueil,
- Sécurité: Distribution des droits spéciaux sur les lecteurs donnant accès à des locaux techniques ou à circulation restreinte + droit accueil,
- Direction: Distribution des droits donnant accès aux services administratifs et à la direction générale + droits accueil

D'autres possibilités de filtrage sont réalisables en fonction des besoins du client utilisateur.

Important

La classification des accès n'a pas d'influence sur :

- la vision des événements dans le moniteur d'événements,
- la recherche dans les historiques,
- l'import des accès (lecteurs, groupes de lecteurs, profils) depuis la passerelle.

1.3.2. Exploiter la classification des accès

L'opérateur se connecte à MICROSESAME avec le profil opérateur gérant la classification des accès (crée dans l'étape 3 de la section précédente).

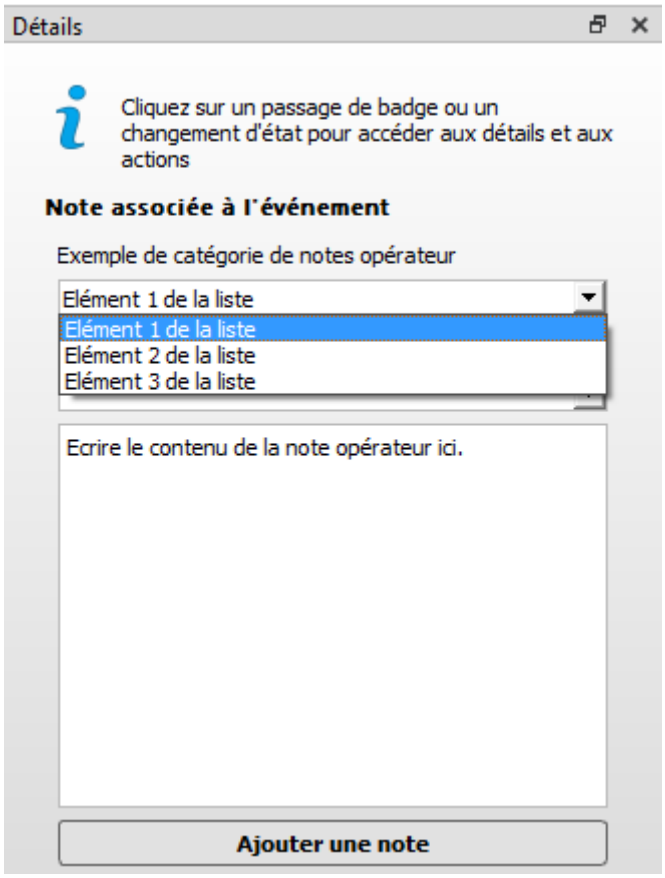
Lors que l'opérateur attribue des accès aux identifiés, les accès contenus dans les classes concernées par le profil opérateur seront disponibles.

1.4. Notes opérateur

1.4.1. Créer des notes

Lorsque les notes opérateurs ont été paramétrées et enregistrées dans MICROSESAME, elles seront accessibles depuis le **Moniteur d'évènements**.

Dans la zone **Détails**, les catégories de notes opérateur libres sont visibles. Cliquer sur la liste pour consulter les différents éléments de chaque catégorie.

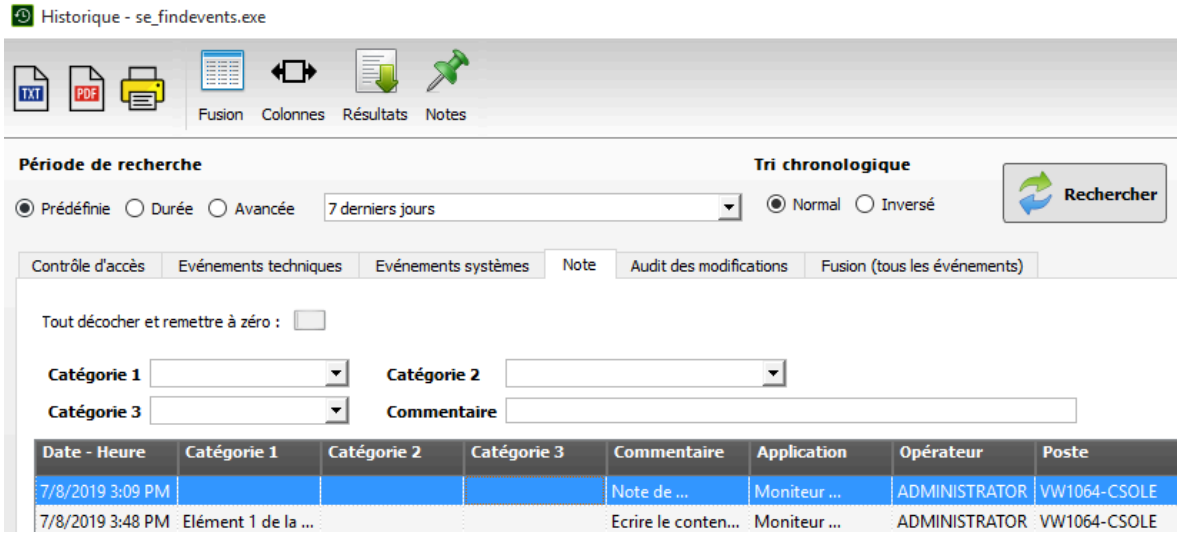


Le champ de texte permet d'écrire le contenu de la note à l'opérateur.

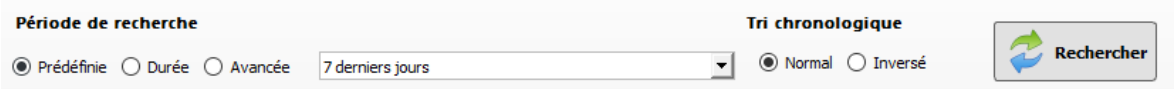
Pour enregistrer la note, cliquer sur "Ajouter une note".

1.4.2. Visualiser les notes

Dans la fenêtre de l'Historique (se_findevents), un onglet dédié **Notes** est disponible : Lors que des notes ont été enregistrées par l'opérateur, elles sont disponibles ici.

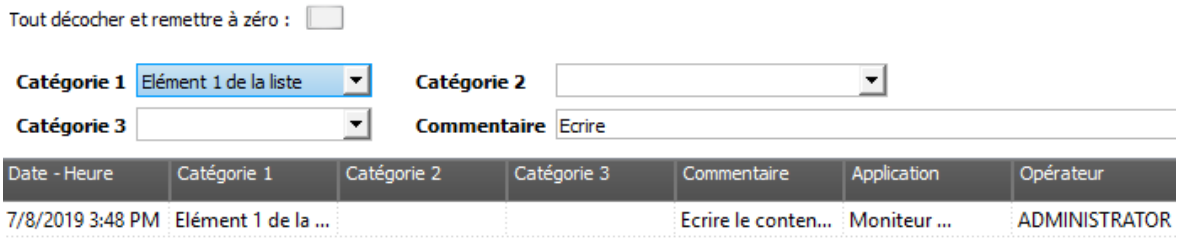


La fenêtre de l'Historique permet d'effectuer des recherches avec les filtres proposés :



Lorsque plusieurs catégories de notes ont été paramétrées, il est possible de filtrer par catégorie.

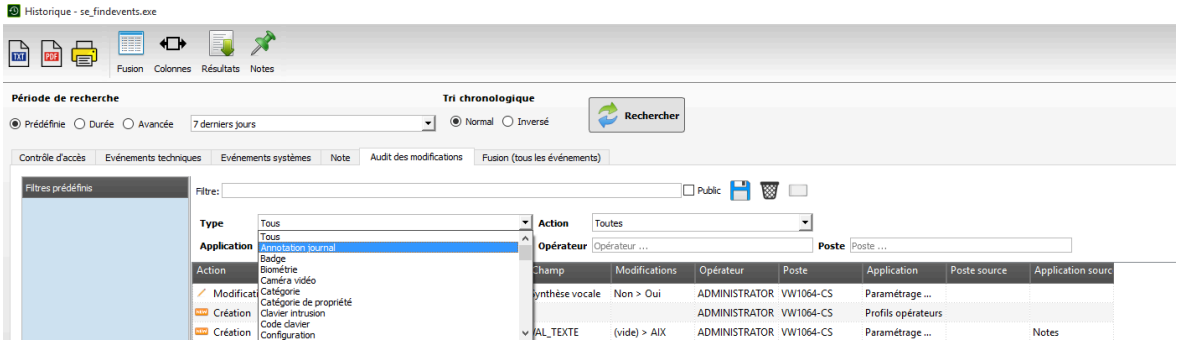
Le champ Commentaire permet d'effectuer une recherche sur les notes écrites par l'opérateur.



1.5. Audit des modifications

Les différents évènements du système de contrôle d'accès sont enregistrés et disponibles dans l'**Historique** de MICROSESAME (se_findevents). Les modifications réalisées par l'opérateur font partie de ces évènements. L'onglet **Audit des modifications** contient les opérations réalisées par l'opérateur.

La recherche d'un évènement précis se réalise à l'aide des filtres dans la partie supérieure :



Une recherche avec des filtres spécifiques peut être enregistrée. Cette recherche sera visible dans la colonne "Filtres prédéfinis".

Une recherche en mode "public" sera visible par tous les opérateurs accédant à l'onglet de l'audit des modifications.

Pour paramétrer la durée de conservation des données de l'Historique, voir *Purge automatique*

1.6. Les raccourcis clavier dans MICRO-SESAME

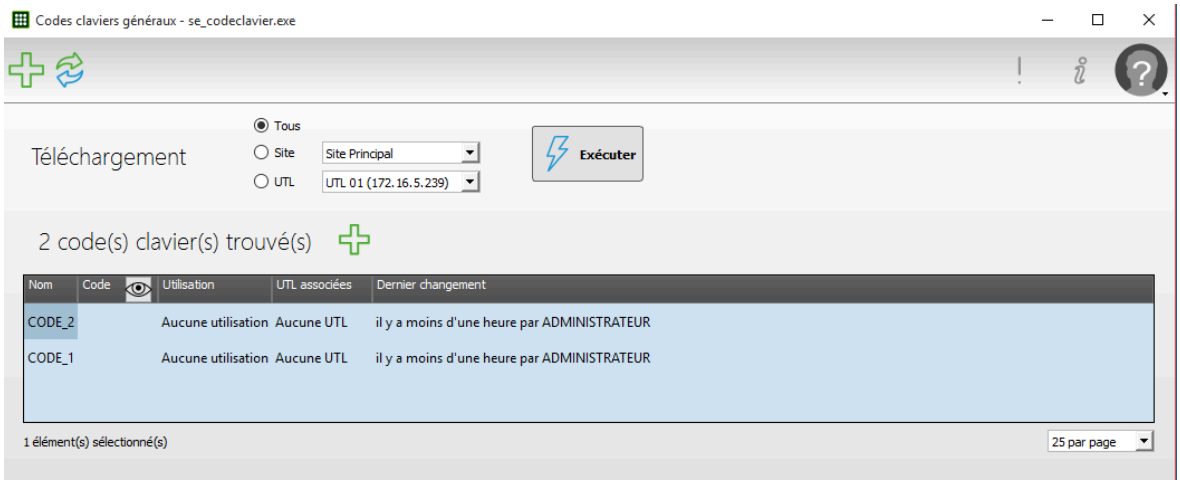
Raccourci	Fonction
ALT+H	Aller à l'Accueil - Dans le menu principal de MICROSESAME, ALT+H permet de revenir à l'accueil (Applications ajoutées aux Favoris).
ALT+E	Aller à l'Exploitation - Dans le menu principal de MICROSESAME, ALT+E permet d'accéder à l'onglet Exploitation.
ALT+P	Aller au Paramétrage - Dans le menu principal de MICROSESAME, ALT+P permet d'accéder au Paramétrage.
ALT+M	Aller à la Maintenance - Dans le menu principal de MICROSESAME, ALT+M permet d'accéder à la Maintenance.
CTRL + N	Nouveau
CTRL + I	Importer
CTRL+ F	Rechercher
CTRL + D	Dans MICROSESAME, CTRL + D permet de dupliquer. Dans l'application Réception de visiteurs, CTRL + D sert à effacer les filtres.
F5	Recharger
CTRL + S	Enregistrer
CTRL + DEL	Supprimer
CTRL + P	Imprimer
CTRL + SHIFT + H	Afficher l'historique
CTRL + E	Exporter
CTRL + Q	Accueil pour la réception de visiteurs
F7	Afficher tous les résultats de la recherche (dans l'Historique).
F12	Ajuster à l'écran (synoptiques)
CTRL + O	Ouvrir (synoptiques)
CTRL +Z	Annuler (défaire - synoptiques)
CTRL + Y	Rétablir (refaire - synoptiques)

1.7. Code clavier généraux

1.7.1. L'application des codes clavier généraux

Cette application permet de déclarer des codes claviers. Ces codes clavier générés peuvent être utilisés pour, par exemple, déclencher du microcode permettant d'ouvrir une porte d'entrée d'un immeuble.

Les codes claviers généraux sont accessibles depuis le menu principal de MICROSESAME : Exploitation > Contrôle d'accès > Codes clavier généraux. Pour accéder et utiliser cette application, un profil exploitant est nécessaire. Les droits de paramétrage ne sont pas obligatoires.



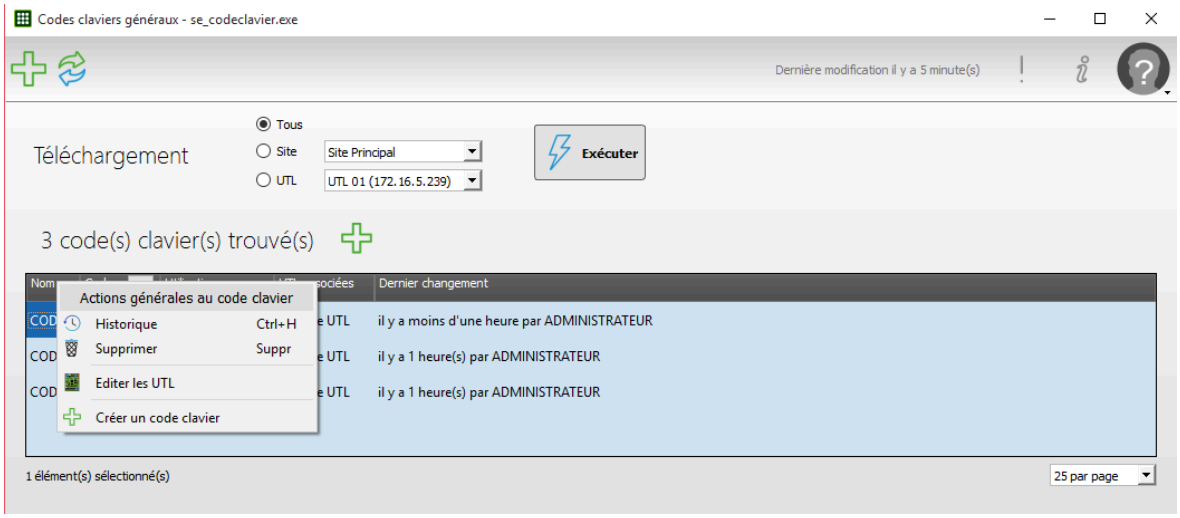
1.7.2. Créer un code clavier

1. Cliquer sur "+"
2. Une ligne est générée dans le tableau des codes clavier. La colonne code est affichée en mode édition.
3. Indiquer le code clavier à déclarer. Le code peut être vérifié avec l'icône dans l'en-tête de cette colonne.
4. Associer le code à une UTL dans la colonne "UTL associées".
5. Télécharger les données : Les codes clavier générés peuvent être associés à une UTL/site.Sélectionner les options de téléchargement et cliquer "Exécuter". Cette étape est obligatoire.

1.7.3. Modifier un code clavier existant

Un code clavier déclaré au préalable peut être modifié.

Dans la fenêtre des codes claviers généraux, sélectionner le code clavier à éditer et cliquer droit pour afficher le menu contextuel avec les actions disponibles.


Codes claviers généraux - se_codeclavier.exe
Dernière modification il y a 5 minute(s)
Téléchargement
Tous
Site
Site Principal
UTL
UTL 01 (172.16.5.239)
Exécuter
3 code(s) clavier(s) trouvé(s)
Dernier changement
Actions générales au code clavier
Historique Ctrl+H
Supprimer Suppr
Editer les UTL
Créer un code clavier
il y a moins d'une heure par ADMINISTRATEUR
il y a 1 heure(s) par ADMINISTRATEUR
il y a 1 heure(s) par ADMINISTRATEUR
1 élément(s) sélectionné(s)
25 par page

Chapitre 2. Supervision

2.1. Rondes

2.1.1. Exploitation : Gestion des rondes

L'application des rondes (se_rondes.exe) permet aux rondiers de gérer l'exploitation des rondes de surveillance.

Pour que les rondes soient opérationnelles, elles doivent avoir été configurés au préalable (Voir Paramétrage des rondes pour plus de détails) et mises à disposition pour utilisation (Activation des rondes lors du paramétrage).

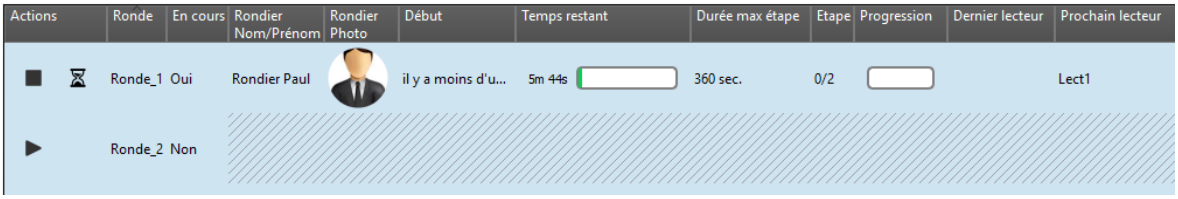
2.1.1.1. Gestion des rondes : Onglet Rondes

L'onglet **Rondes** permet l'exploitation des rondes existantes.

1) Après avoir sélectionné une ronde de la liste, dans la colonne **Actions**, cliquer pour **Démarrer la ronde**.

2) Une fenêtre contenant l'équipe de rondiers s'affiche. Choisir la personne en charge d'effectuer la ronde sur le terrain pour continuer.

3) Le tableau avec les différentes données de la ronde est mis à jour en temps réel :



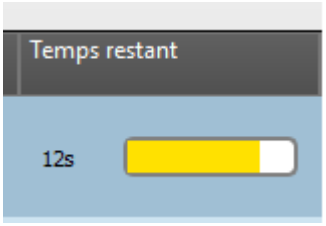
La colonne **En cours** indique si la ronde a été démarrée ou pas.

La colonne **Rondier** indique la personne qui réalise la ronde de surveillance sur le terrain. Si la fiche identifié de cette personne a une photo de profil, elle est affiché dans la colonne **Rondier Photo**.

La colonne **Début** indique le délai passé depuis le démarrage de la ronde.

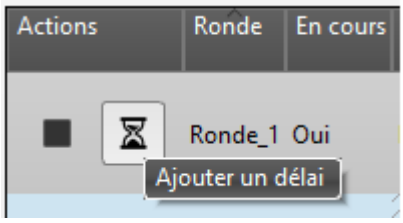
La colonne **Temps restant** indique le temps que le rondier a pour présenter le badge dans le lecteur indiqué dans le parcours de la ronde.

Un code couleur affiche la progression (verte, jaune, orange, rouge) selon la quantité de temps restant.



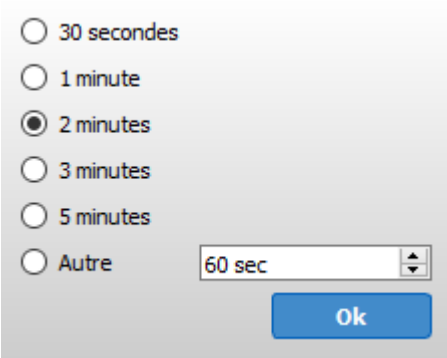
Un délai supplémentaire peut être ajouté avec l'icône **Ajouter un délai** de la colonne Actions.

Un délai supplémentaire peut indépendamment être ajouté lors qu'une étape est en cours ou une fois que le délai de temps a été dépassé.



L'option **Autre** permet de choisir une valeur personnalisée.

Les valeurs personnalisés sont indiquées en secondes.



La colonne **Durée max étape** indique le temps total pour chaque étape de la ronde (temps initial de l'étape plus temps supplémentaire).

La colonne **Étape** indique le nombre total d'étapes de la ronde et l'étape actuel ou le rondier se trouve ("étape 1/2").

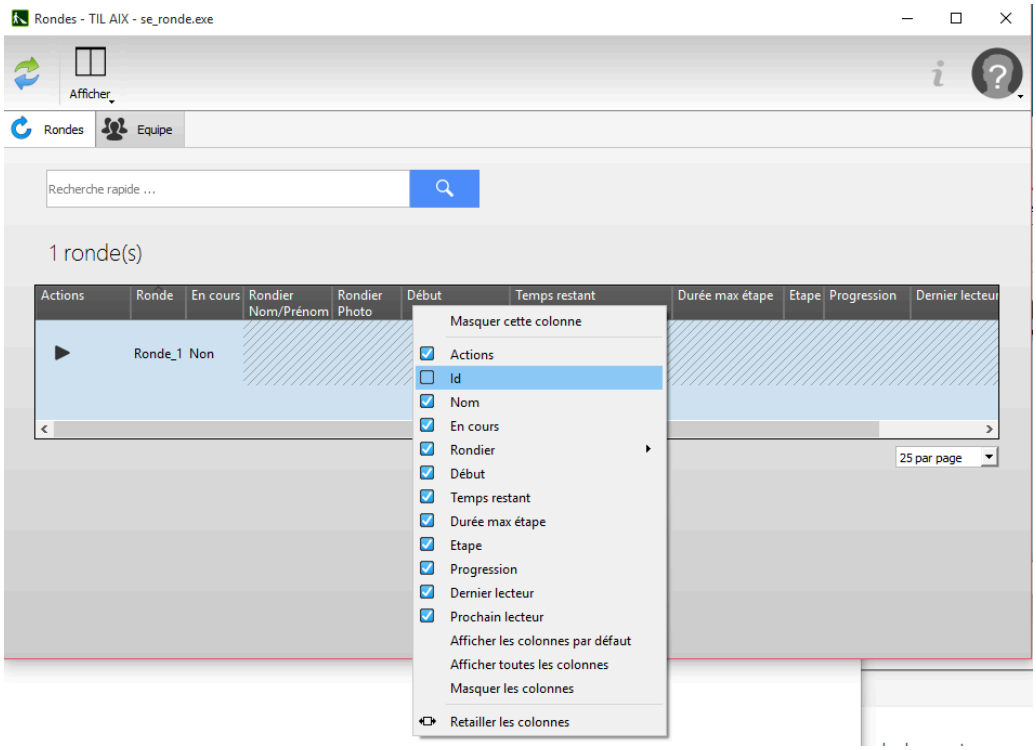
La colonne **Progression** utilise un code couleur pour montrer l'état de progression globale de la ronde.

La colonne **Dernier lecteur** indique le dernier lecteur où l'identifiant du rondier a été détecté.

La colonne **Prochain lecteur** indique le point ou l'identifiant du rondier doit être présenté.

Pour personnaliser les colonnes affichés dans l'onglet Rondes, faire clique droit sur l'en-tête pour afficher la liste de colonnes.

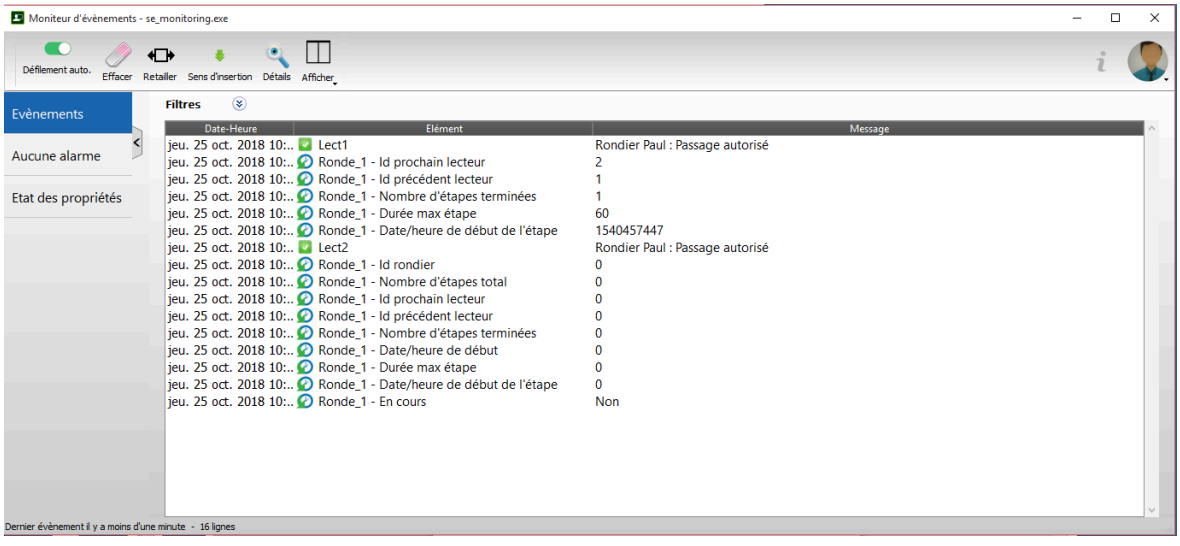
Cocher ou décocher les options souhaitées.



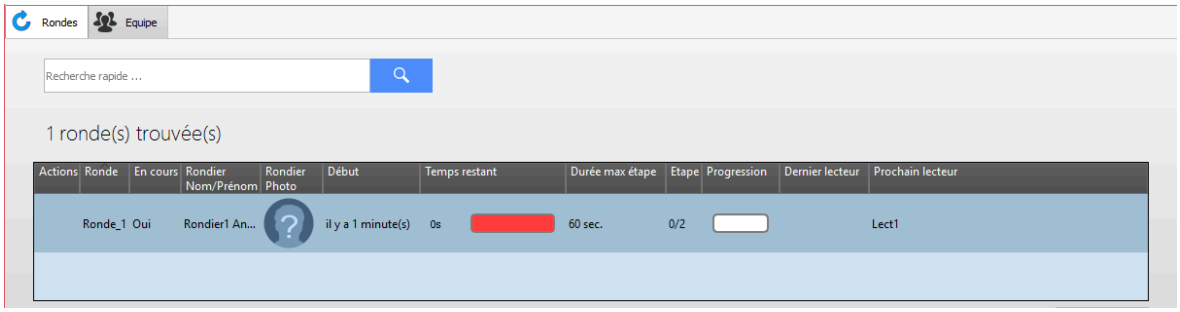
4) Une ronde en cours d'exécution peut être interrompue. Dans la colonne Actions, **Annuler la ronde** permet d'arrêter la ronde en cours d'exécution.

5) Si un badge appartenant au rondier en charge de la ronde est passé sur le lecteur spécifié dans le parcours dans les temps indiqués, la ronde passe à l'étape suivante.

Toute trace liée aux rondes est remontée dans le moniteur d'évènements. La colonne **Élément** contient une description de l'action réalisée :



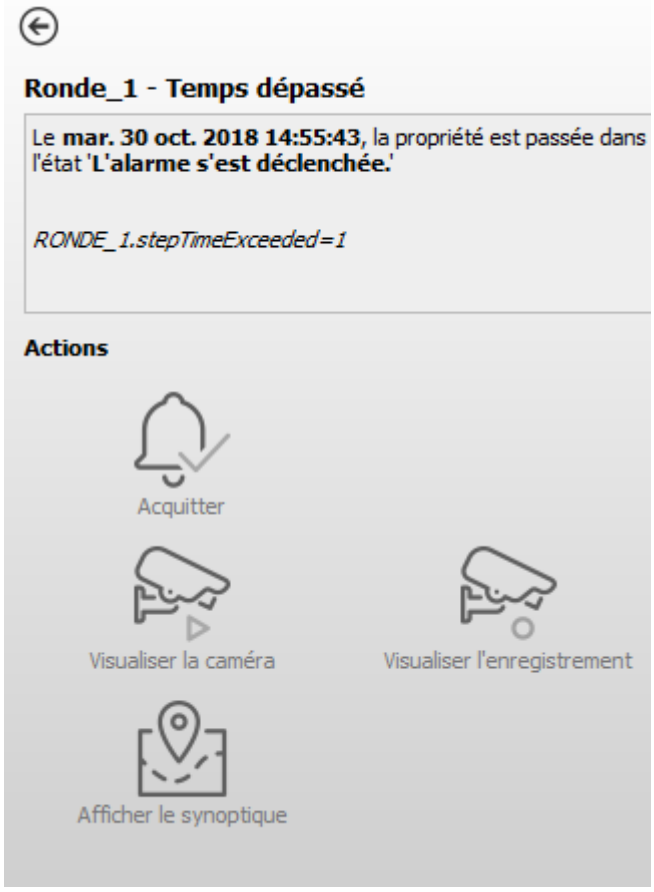
6) En cas de dépassement du délai établi, l'automate déclenche une **alarme** :



Dans le moniteur d'évènements, l'onglet **Fil de l'eau** affiche ces informations :

jeu. 25 oct. 2018 14:.. Ronde_1 - Temps dépassé Oui
jeu. 25 oct. 2018 14:.. Ronde_1 - Temps dépassé L'alarme s'est déclenchée.

La zone **Détails** permet d'accéder directement aux **Actions** liées à cette alarme (selon la configuration mise en place) :



Dans le moniteur d'évènements, l'onglet **Alarmes** contient les détails de l'alarme déclenchée.

L'acquittement de l'alarme est réalisée manuellement depuis la fenêtre du moniteur d'évènements.

L'acquittement d'une alarme correspond à la prise de connaissance de l'alarme déclenchée. L'acquittement d'une alarme n'entraine pas la désactivation de l'alarme.

7) Suite au déclenchement d'alarme, il est possible d'ajouter un temps supplémentaire (pour permettre au rondier plus de tempos pour présenter son badge au lecteur) ou arrêter la ronde (pour vérifier l'état du rondier sur le terrain).

8) Une fois que la ronde est réalisée correctement, la ronde est finalisée automatiquement, aucune action est à réaliser. La ronde peut être redémarrée à nouveau.

2.1.1.2. Gestion des rondiers : Onglet Équipe

L'onglet **Équipe** permet de définir l'équipe d'identifiés a charge des rondes de surveillance.

Après avoir paramétré les identifiés selon le fonctionnement souhaité (Voir Paramétrage de l'identifié rondier), l'identifié peut être ajouté à l'équipe de rondiers.

Cliquer sur + ou - pour accéder à la fenêtre d'ajout/suppression de rondiers.

Une seule personne peut être a charge d'une ronde.

A chaque démarrage d'une ronde, la liste de rondiers s'affiche et il est nécessaire de sélectionner le rondier a charge de la ronde sur le terrain.

2.1.2. FAQ Rondes

2.1.2.1. Problèmes liés au fonctionnements des rondes

Le rondier souhaité n'est pas affiché dans l'onglet Équipe :

Le rondier doit s'afficher dans l'onglet Équipe. S'il n'est pas affiché, vérifier le paramétrage de l'identifié dans la fiche identifié du rondier concerné (se_identifie.exe).

La ronde souhaitée ne s'affiche pas dans l'onglet Rondes:

Toutes les rondes crées doivent s'afficher dans l'onglet Rondes.

Si une ronde ne s'affiche pas dans la liste de rondes, vérifier la configuration de la ronde (depuis se_config.exe). Elle doit contenir au moins deux lecteurs différents et deux étapes pour une ronde. Modifier la ronde, enregistrer les changements, compiler pour vérifier les éventuels erreurs et appliquer les changements pour transmettre la configuration aux automates. Dans l'application d'exploitation des rondes (se_ronde.exe), rafraîchir la fenêtre pour mettre à jour cette liste.

Les derniers changements ne s'affichent pas :

En cas de modification de la configuration, enregistrer les changements, compiler pour vérifier que la configuration ne contienne pas d'erreurs et **appliquer les changements** (Bouton "Appliquer les changements") pour transmettre la mise à jour en temps réel.

La ronde en cours est interrompue :

Vérifier qu'aucun changement n'est pas réalisé dans l'application de paramétrage des rondes pendant qu'une ronde est en cours d'exécution dans l'application se_ronde.exe.

Si une ronde est en cours, et qu'on réalise des modifications dans le paramétrage en même temps (Clic sur le bouton "Appliquer les changements") , la ronde en cours sera terminée.

L'identifiant du rondier ne marche pas :

Si l'identifiant du rondier ne permet pas de passer à l'étape suivante de la ronde en cours, vérifier le paramétrage de l'identifiant dans la fiche identifié.

Dans se_identifie, aller à l'onglet Identifiant pour vérifier que l'identifiant est correctement attribué au rondier concerné.

Si plusieurs technologies d'identifiant sont utilisées pour les lecteurs concernés par la ronde, vérifier que l'identifiant et la technologie soient associées correctement.

Si l'identifiant est associé au rondier mais qu'il n'est pas associé à la technologie correcte, le passage du badge par le lecteur en question ne permettra pas l'avancement de la ronde.

2.2. Les zones

Une zone est un lieu (bureau, étage, bâtiment,...) qui nécessite une gestion particulière de type :

- Comptage/ décomptage de présence (variable numérique automatiquement incrémentée et décrémentée en fonction des entrées et des sorties).
- Anti-Retour (logique ou temporisé)
- Plan d'opération interne
- Autres types de zones

La zone permet aussi :

- De contrôler l'éjection automatique d'un badge (temporisation)

- D'activer les mécanismes de classe (suivi d'une population spécifique)
- De verrouiller l'accès à d'autres zones (groupe de lecteurs dépendants))

Une zone répond à des règles précises :

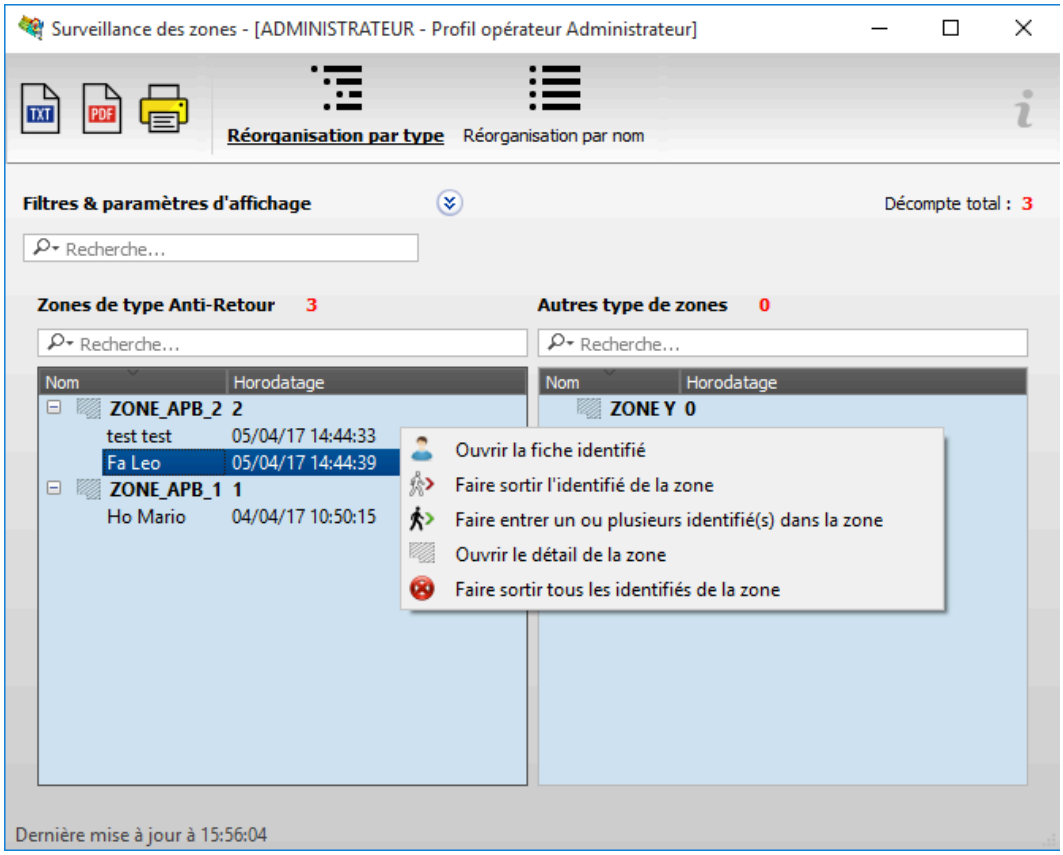
- Elle doit posséder un groupe de lecteurs en entrée
- Elle doit posséder un groupe de lecteurs en sortie
- Son étanchéité physique garantit son bon fonctionnement. On entend par "étanchéité", l'impossibilité d'entrer ou de quitter la zone sans être contrôlé.
- Le nombre de zones est limité à 128 (limites système)
- La création et/ou la gestion d'une zone est soumise à droits opérateur.

Dans le cadre d'un système de contrôle d'accès gérant une ou plusieurs zones, les éléments suivants doivent être pris en considération pour chacun des sites :

- Le nom et l'adresse du site (identification et géolocalisation),
- La nature du site et s'il est partagé avec d'autres entreprises,
- Les services à proximité du site et les risques naturels de la zone
- Le nombre de personnes actuel et potentiel du site.

2.3. Surveillance des zones

Il est possible, via une fenêtre dédiée, de surveiller le nombre d'identifiés présents, les alarmes, ainsi que d'autres informations relative au contrôle d'accès des différentes zones créées. Pour cela, accéder à la surveillance des zones: *Menu MICROSESAME> Supervision > Surveillances des zones*



Cette fenêtre permet donc de visualiser et d'effectuer des actions sur la population occupant les différentes zones :

- Les boutons "Réorganisation par type" et "Réorganisation par nom" permettent de permuter l'affichage, soit les résultats sont affichées par Type de zone (Anti-retour, POI ...etc), soit par nom de zone.
- La section "Filtres & paramètres d'affichage" peut être cachée ou affichée. L'utilisation de filtres et paramètres d'affichage permet d'obtenir des résultats précis en manipulant les fonctions suivantes :
  1. La fréquence de rafraîchissement.
  2. L'option "Masquer les zones POI", permettant de ne pas afficher les zones de type POI.

     Filtre actif par défaut

  3. Le bouton d'Information(s) supplémentaire(s) à afficher, permettant d'ajouter des colonnes additionnelles aux informations de la zone (6 colonnes maximum peuvent être affichées). Les colonnes par défaut sont "Nom" et "Horodatage".
  4. La case "Liste noire" : permettant d'effectuer un filtre sur la zone, seuls les identifiés présents dans la zone et ayant été typés "liste noire" apparaîtront dans les résultats
- Chaque ligne d'une liste correspond à une personne présente dans la zone sélectionnée. Par défaut on retrouve le nom de la personne, la date et l'heure de son dernier passage sur un lecteur d'entrée dans la zone

- Lors d'un clic droit sur un identifié ou sur une zone, il est possible :
  1. d'ouvrir la fiche identifié ou les détails de la zone
  2. de forcer la sortie d'un identifié ou de tous les identifiés de la zone
  3. de faire entrer un ou plusieurs identifiés dans la zone manuellement

2.4. Accéder à la surveillance des zones depuis WEBSESAME

L'accès au service WEBSESAME se fait grâce à l'adresse suivante: `https://nom_du_serveur:443/`

Le port à renseigner dans l'URL d'accès à WEBSESAME est susceptible de changer en fonction de la configuration du poste serveur.

Depuis l'onglet Zones de **WEBSESAME** l'opérateur peut effectuer des recherches par **type de zone** ainsi qu'en tapant directement le **libellé** de la zone concernée. Il peut activer la fonction **Rafraichir les données automatiquement** pour visualiser en temps réel le nombre d'identifiés présents dans une zone. En sélectionnant une zone, l'opérateur accède à la liste des identifiés présent à un temps donné et peut prendre connaissance de leur fiche.

Chapitre 3. Moniteur d'évènements

3.1. Présentation du moniteur d'évènements

L'outil **Moniteur d'évènements** centralise la surveillance d'évènements dans tout le système MICROSESAME de type Gestion Technique ou Contrôle d'accès, permet l'acquittement des alarmes et télécommandes en cours, la commande de l'état des propriétés.

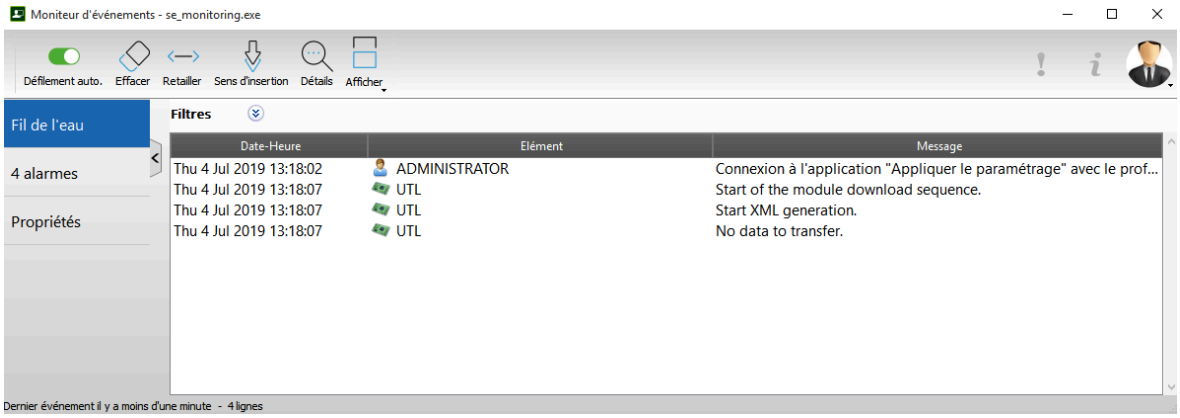
Tous les évènements générés sont historisés dans le système : Les évènements des historiques ne peuvent pas être supprimés par un opérateur. Les évènements sont archivés dans l'historique pendant une période définie, paramétrable (Paramétrage système pour la durée de rétention - Pour savoir plus, voir le *traceur de logs*).

- Sur passage de badge, il est possible d'*accéder rapidement aux informations principales de l'identifié*, *ouvrir la fiche complète de l'identifié* et le *débloquer en cas d'anti-retour*.
- Sur alarme, il est possible d'*acquitter une alarme* (si l'alarme est de type acquittable), *visualiser la caméra liée à l'alarme, visualiser les enregistrements liés à l'alarme ou visualiser les synoptiques liés à l'alarme*.
- Sur changement de propriété, l'application permet des opérations tels que *connaître l'état*, *forcer l'état*, l'*envoi d'une télécommande* et la *consultation des courbes*.

3.2. Fil de l'eau

L'onglet **Fil de l'eau** remonte les différents types d'évènements. Les événements apparaissent de manière chronologique. Le sens d'insertion est personnalisable par l'opérateur.

Parmi les événements, on trouve ceux du domaine du contrôle d'accès, la gestion technique du bâtiment et du système.



3.2.1. Visualiser en temps réel les évènements

Par défaut, les événements apparaissent de manière chronologique, avec l'évènement le plus récent en bas de la liste.

Le sens d'insertion est personnalisable par l'opérateur : **Sens d'insertion** dans la barre d'outils permet d'inverser ce paramètre.

Il est possible de retailler les colonnes avec le bouton **Retailler**.

3.2.2. Afficher les détails d'un évènement

Lors de la sélection d'un évènement affiché dans le fil de l'eau, la zone **Détails** permet de consulter des informations supplémentaires sur l'évènement.

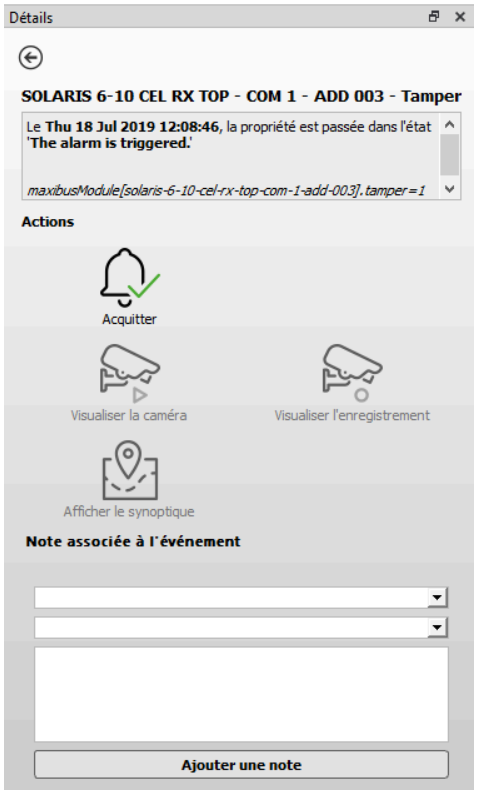
Cette zone est détachable (Maintenir le clic gauche sur la zone et déplacer dans l'emplacement souhaité).

Si la zone n'est pas affichée, cliquer sur l'icône **Détails** de la barre d'outils pour l'afficher.

Lors de la sélection d'un évènement, la liste d'actions disponibles est visible dans la zone **Actions** :

Les actions disponibles sont affichées en noir. Les actions qui ne sont pas disponibles pour l'évènement sont affichées en gris.

Plus ou moins d'actions peuvent être disponibles en fonction de la configuration mise en place.



3.2.3. Filtrer les évènements

Sur la zone **Filtres**, cliquer sur la flèche pour déplier la zone. Sélectionner une ou plusieurs options permet de filtrer l'affichage :

- d'évènements générés par le passage de badges.

- d'évènements liés au type de propriétés (La case "Autres" permet l'affichage des propriétés qui ne sont pas liées ni aux alarmes ni aux télécommandes. Par exemple, les propriétés d'état).
- d'évènements système.

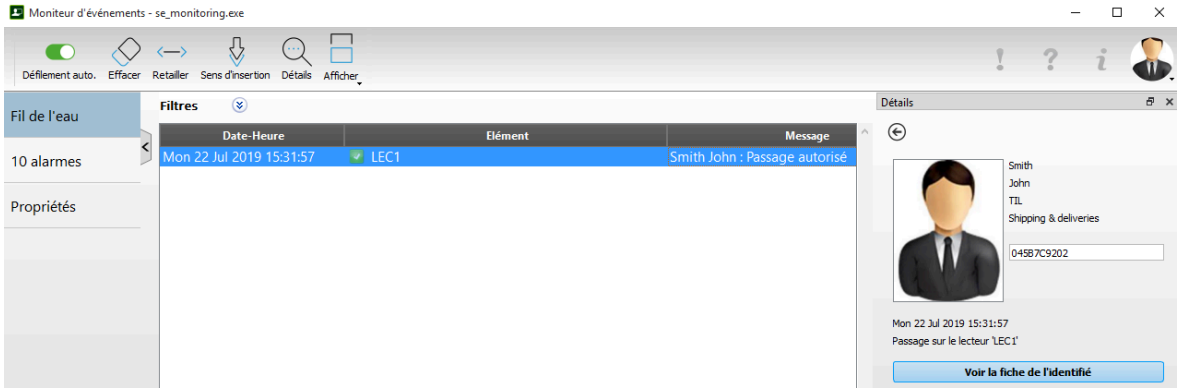
Décocher un maximum de filtres permet d'obtenir un résultats plus précis.

La liste dépliant permet de filtrer par site (si plusieurs sites existent).

3.2.4. Voir la fiche de l'identifié suite à un passage de badge

Sur passage de badge, il est possible d'*accéder rapidement aux informations principales de l'identifié*, ouvrir la fiche complète de l'identifié et le *débloquer en cas d'anti-retour*.

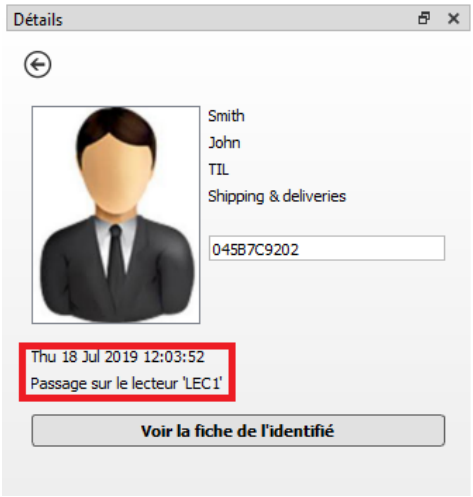
Pour ouvrir la fiche complète de l'identifié, sélectionner l'évènement dans le fil de l'eau, accéder à la zone **Détails** et cliquer sur le bouton **Voir la fiche de l'identifié**.



3.2.5. Afficher automatiquement le dernier passage d'un identifié

Un évènement généré suite à un passage de badge affiche automatiquement le dernier passage de l'identifié.

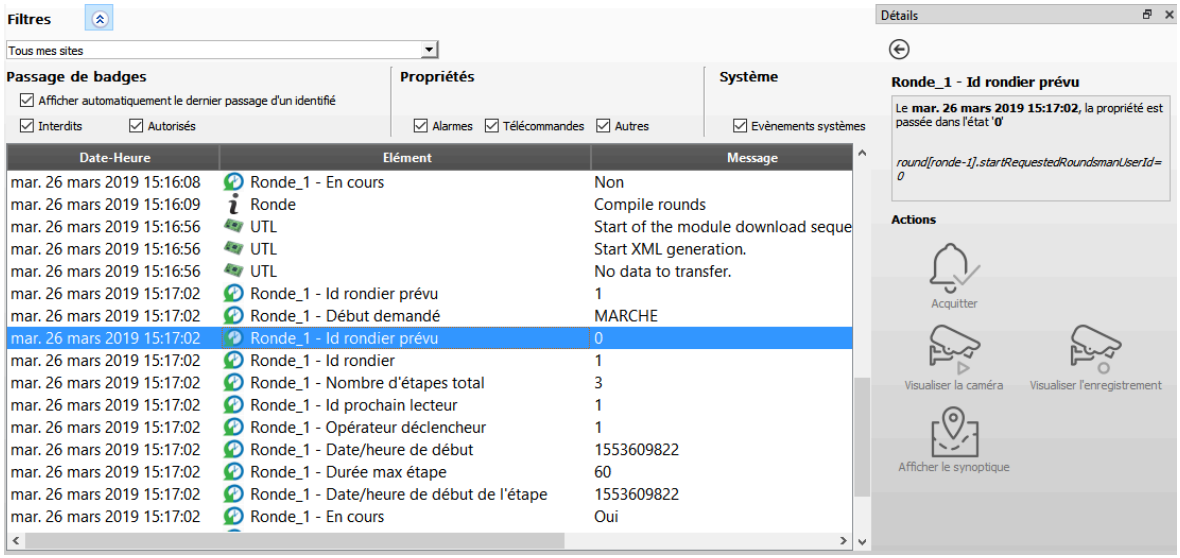
Pour accéder à cette information, sélectionner l'évènement depuis le fil de l'eau. Dans la zone Détails, cette information est visible comme dans l'exemple :



3.2.6. Visualiser la vidéo d'un passage de badge

Si un enregistrement vidéo est déclenché pour chaque passage de badge sur lecteur (selon la configuration du site), et lors que l'évènement de passage de badge est généré dans le moniteur d'évènements, l'enregistrement vidéo lié peut être consulté depuis le fil de l'eau.

Sélectionner l'évènement dans le fil de l'eau pour consulter les détails. La zone Actions contient des options comme **Visualiser l'enregistrement** :

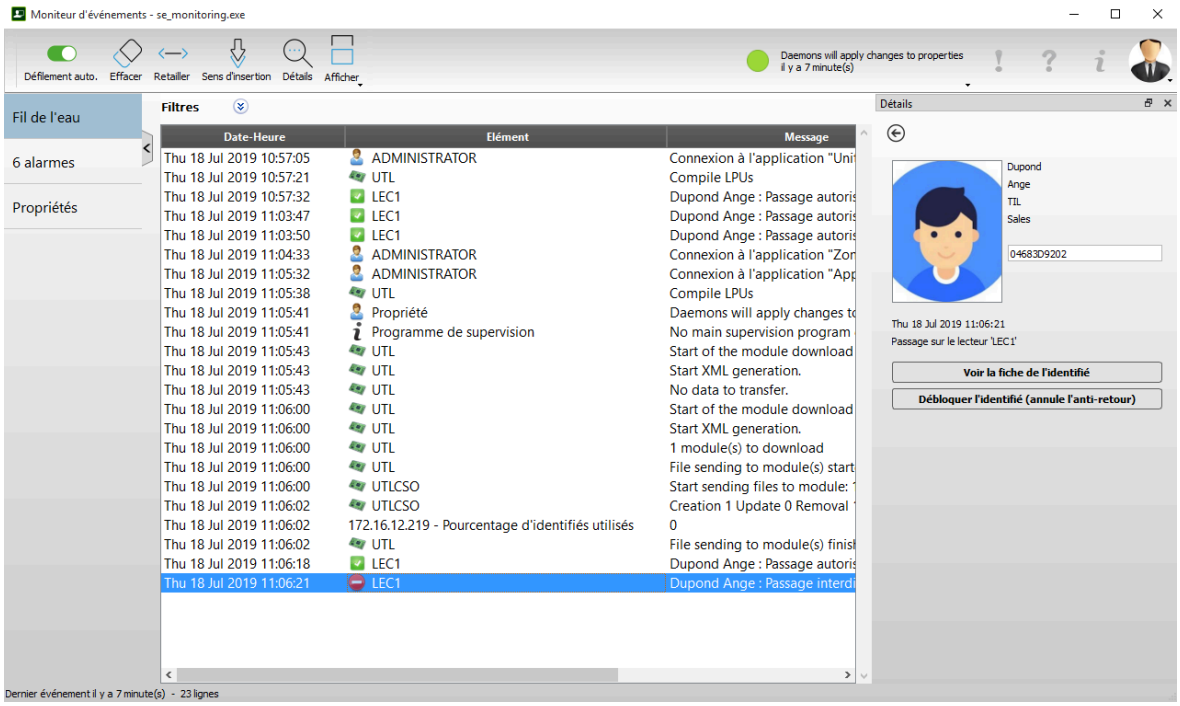


Pour plus de détails sur le paramétrage vidéo, voir *ce chapitre*.

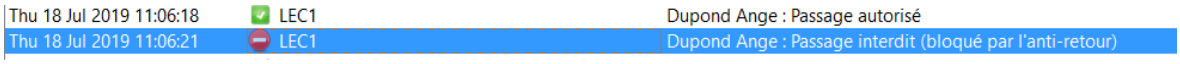
3.2.7. Débloquer un identifié : Annuler l'anti-retour pour l'identifié

Lors de la sélection d'un évènement affiché dans le fil de l'eau, la zone **Détails** permet de consulter des informations supplémentaires sur l'évènement.

Si l'anti-retour est paramétré sur site et est actif sur l'identifié ayant présenté son badge, dans le cas de blocage de cet identifié, celui-ci peut être débloqué depuis le "fil de l'eau" du moniteur d'évènements :



Dans le fil de l'eau, sélectionner l'évènement **Passage interdit (bloqué par l'anti-retour)**.



Dans la zone **Détails** de l'évènement, le bouton **Débloquer l'identifié (annule l'anti-retour)** permet de débloquer l'identifié. Le fil de l'eau affiche l'évènement suivant suite à cette action :

Pour plus d'information sur l'anti-retour et le paramétrage des zones, consulter *le chapitre dédié*.

3.2.8. Consulter une consigne depuis le fil de l'eau

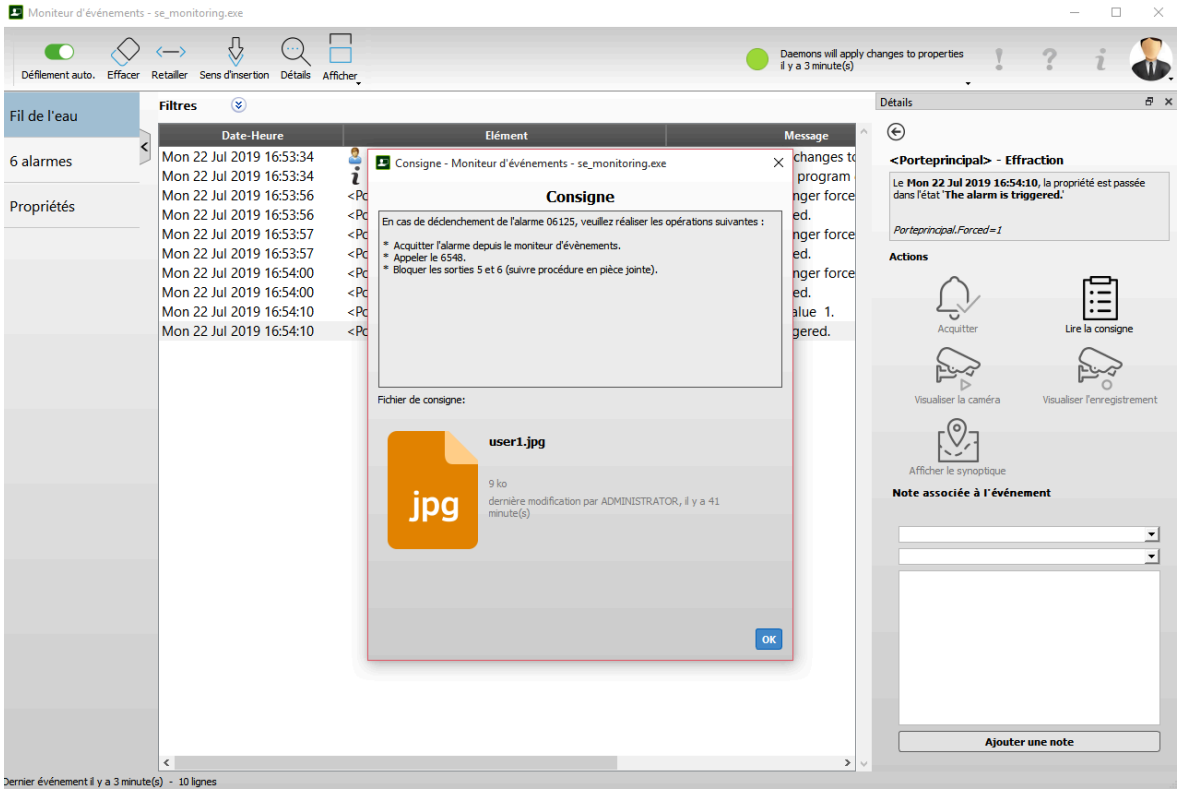
Une consigne contient une liste d'instructions et est destinée à l'opérateur chargé de la surveillance. Une consigne est affichée dans le cadre d'un déclenchement d'une alarme. Son objectif est de fournir des instructions à l'opérateur pour le traitement de l'alarme déclenchée.

Lors que les consignes sont paramétrées, elles seront affichées en tant qu'actions liée à l'alarme ("Détails" > "Consulter la consigne"). Les consignes seront visibles dans le moniteur d'évènements, depuis l'onglet "Fil de l'eau" ou l'onglet *"Alarmes"*.

Pour le paramétrage des consignes, voir la section dédiée.

Lors qu'une consigne est associée à une propriété, et la propriété déclenche une alarme, l'onglet **Fil de l'eau** affiche l'icône permettant l'accès à la consigne dans la zone "Détails".

Cliquer sur **Lire la consigne** pour consulter les informations de la consigne :



Si la consigne contient une pièce jointe (optionnel), cliquer sur cet élément afin de le consulter ou le télécharger.

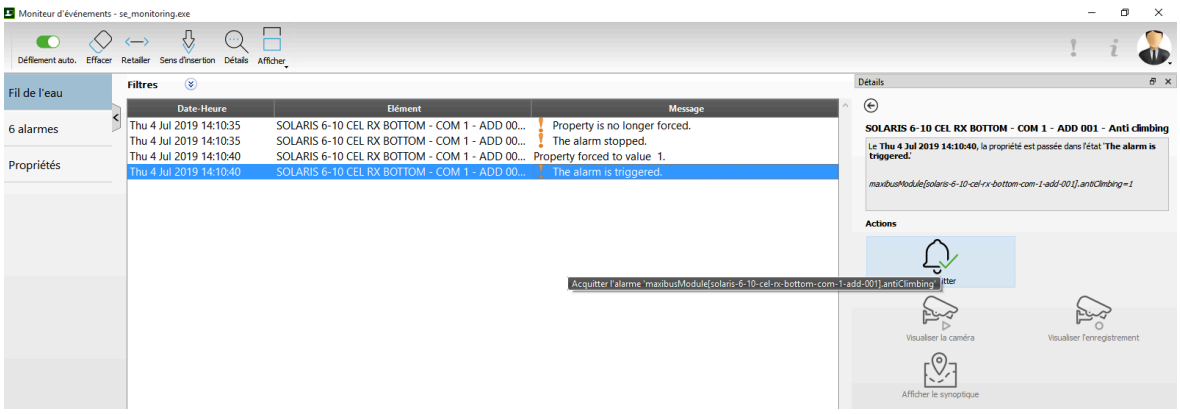
Après consultation de la consigne, cliquer sur OK pour fermer cette fenêtre.

3.2.9. Acquitter une alarme

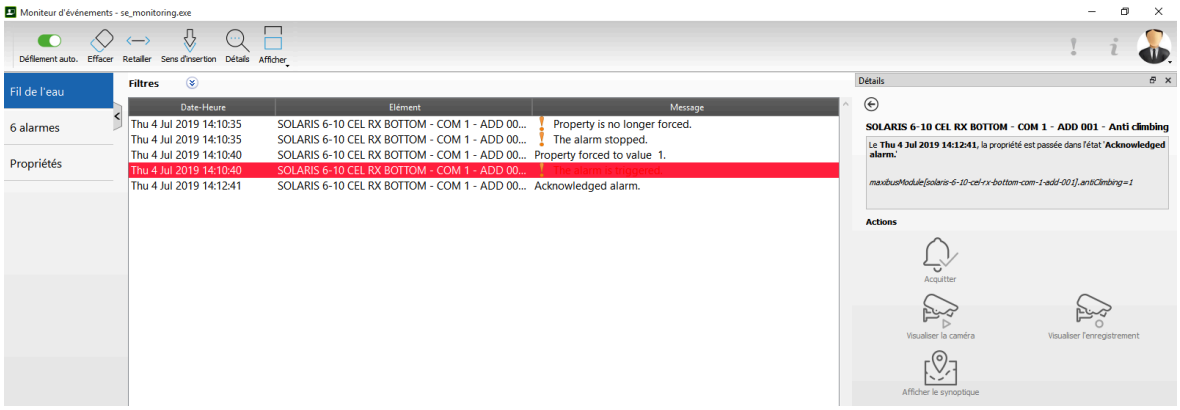
Les alarmes déclenchées depuis le fil de l'eau peuvent être acquittées depuis cette interface.

Sélectionner l'alarme déclenchée et aller dans la zone **Actions**. Les actions disponibles pour cette alarme sont affichées en couleur noir.

Sélectionner l'option **Acquitter**.



Le fil de l'eau est mis à jour avec les informations de l'**alarme acquittée** :



3.2.10. Visualiser la vidéo d'une alarme

Lorsque l'alarme déclenchée dans le fil de l'eau est liée à un groupe de caméras, il est possible de visualiser les images en direct et les images enregistrées au moment de l'alarme : Cliquer sur les boutons "Visualiser la caméra" ou "Visualiser l'enregistreur" dans la rubrique "Actions" après avoir cliqué sur l'alarme.

3.2.11. Afficher le synoptique associé à une alarme

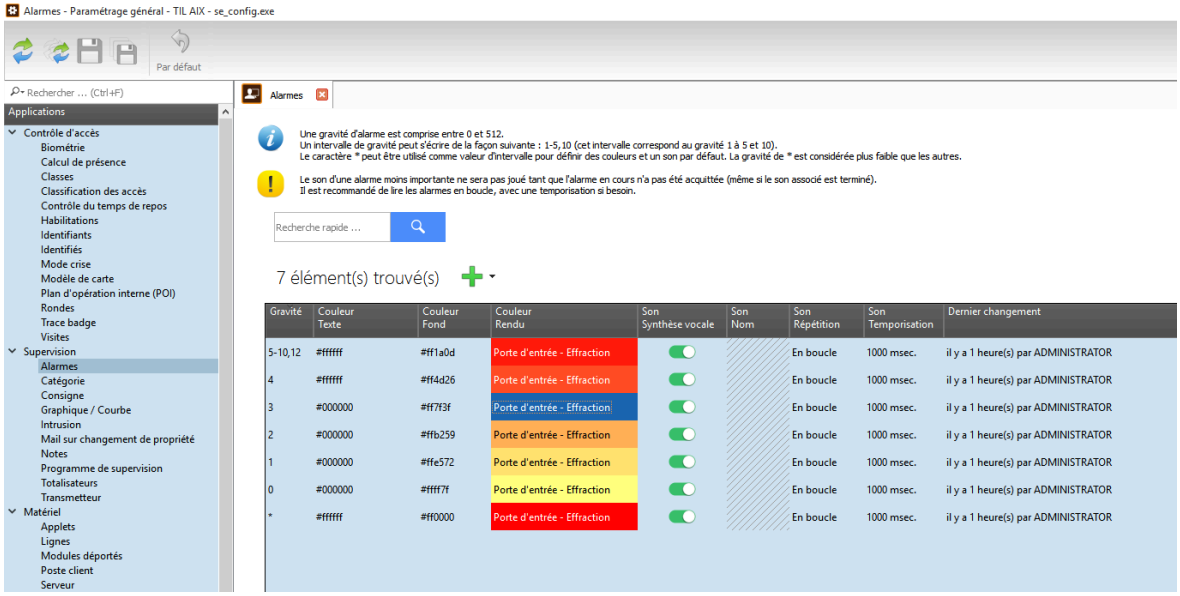
Lorsqu'une alarme apparait dans le fil de l'eau, si celle ci est liée à un synoptique, la fonctionnalité **Afficher le synoptique** est disponible dans la rubrique **Actions**.

Cette fonctionnalité lance l'application **Animateur de synoptique** pour visualiser le synoptique lié à l'alarme. Pour plus de détails, voir la documentation de l'*animateur de synoptique* et de l'*éditeur de synoptique*.

3.2.12. Distinguer les alarmes en fonction de leur gravité

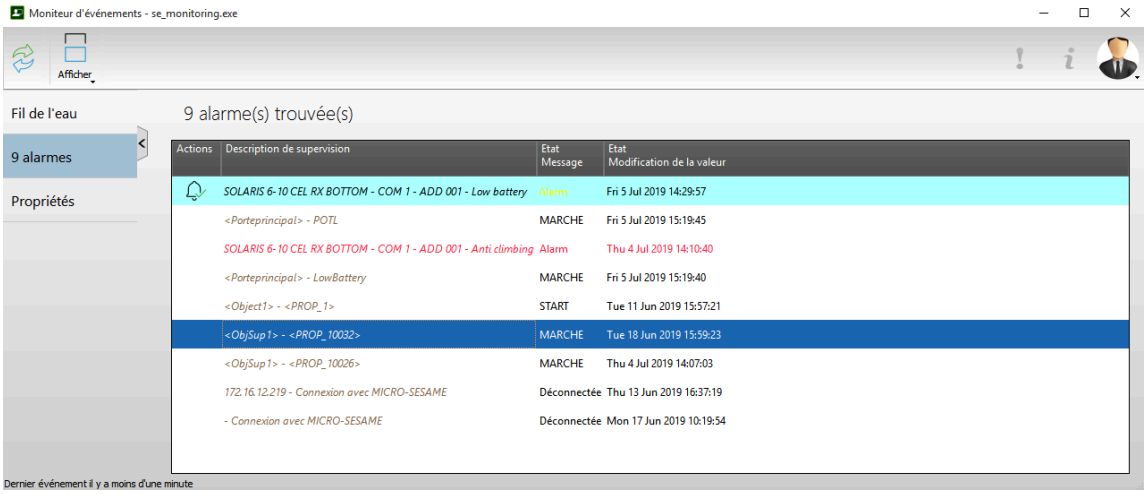
Il est possible de personnaliser les couleurs d'affichage (fonds, textes...) et l'audio des alarmes, afin de différencier leur niveau de gravité.

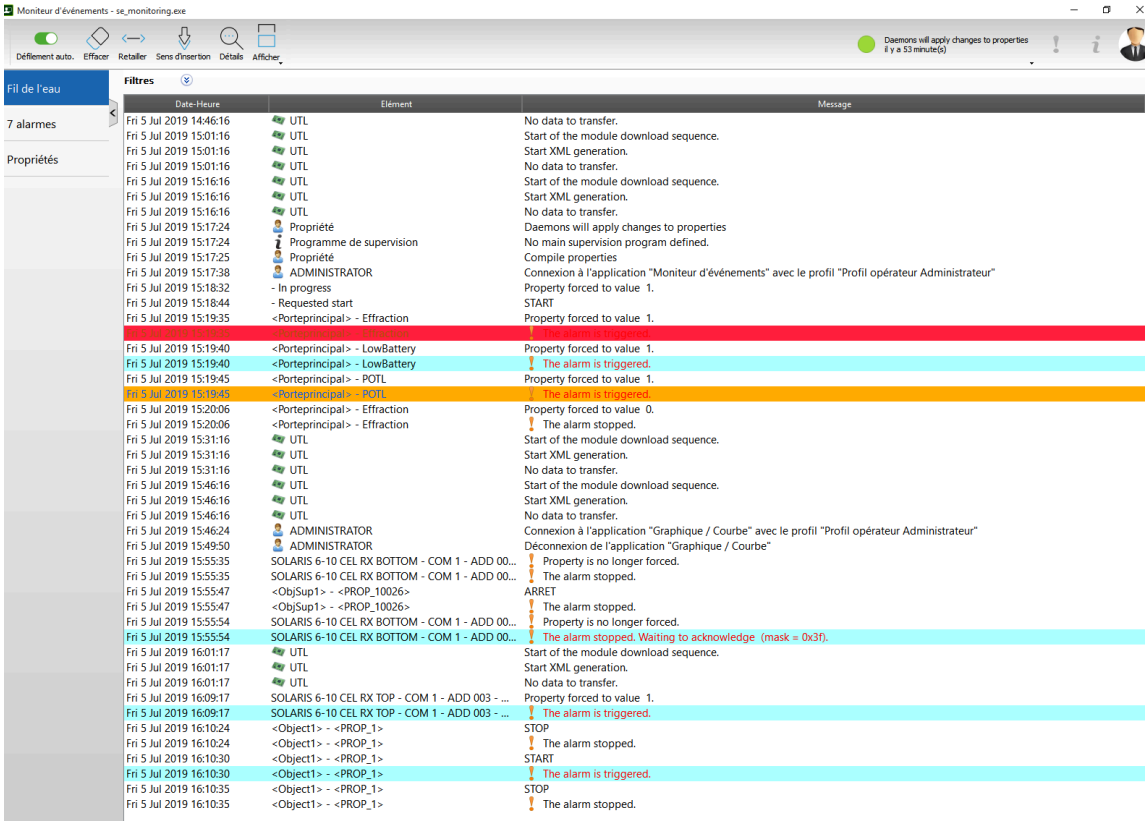
Pour accéder à l'interface de personnalisation, ouvrir l'application **paramétrage général** de MICROSESAME (se_config.exe). Dans le paramétrage général, suivre **Supervision > Alarmes**.



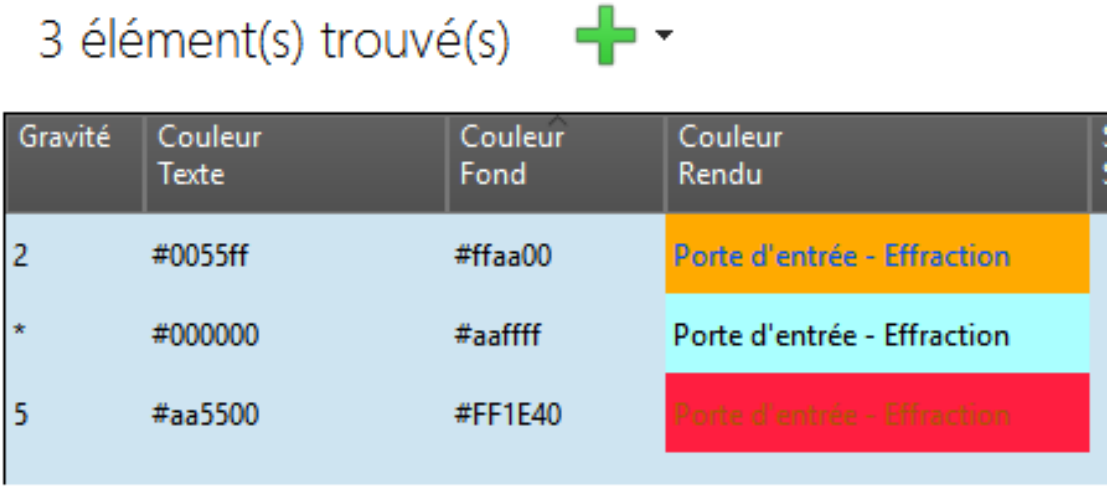
Ce tableau permet d'ajuster les paramètres suivants :

- **Gravité** : Degré d'importance des alarmes, traduits par des couleurs et/ou des audios spécifiques.





Les niveaux de gravité sont organisés de 0 (le plus important) à 512 (le degré d'importance d'alarme le moins élevé).

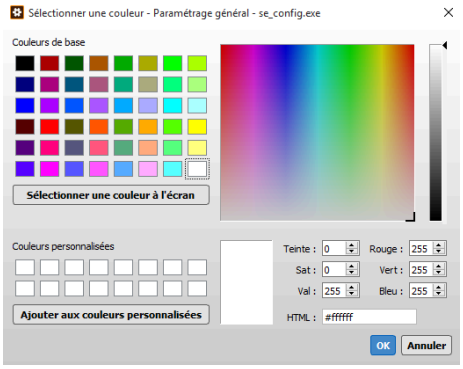


Il est possible de spécifier des couleurs et/ou des audios à des groupes de niveaux : "*1-5,10 #ff0000 Alarm01.wav*" attribuera la couleur rouge et le son "*alarm01.wav*" aux niveaux de 1 à 5, et le niveau 10.
Tous les niveaux non spécifiés adopteront la couleur et l'audio attribué à *. Une alarme non spécifiée (*) sera toujours considéré comme moins prioritaire à une alarme spécifiée.

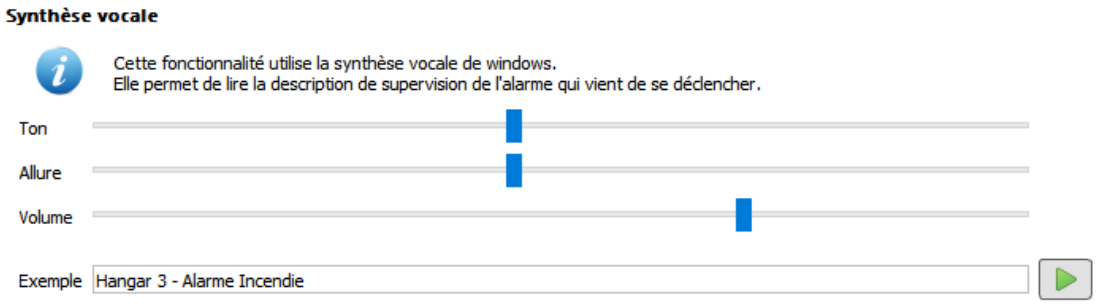
Dans le cas où une alarme se déclenche alors qu'une autre est déjà en cours, l'audio de celle dont le niveau de gravité est le plus élevé sera celui joué, et coupera l'audio de la première.

- **Couleur texte** : Couleur du texte. Peut être paramétrée en éditant le code couleur HTML, ou à l'aide de la palette de couleurs.
- **Couleur fond** : Couleur de fond. Peut être paramétrée avec le code couleur HTML, ou à l'aide de la palette de couleur.
  Sélection de la couleur avec le code HTML et enregistrement des modifications :

  Sélection de la couleur avec la palette :
  Les couleurs personnalisées peuvent être mémorisées avec le bouton **Ajouter aux couleurs personnalisées**.



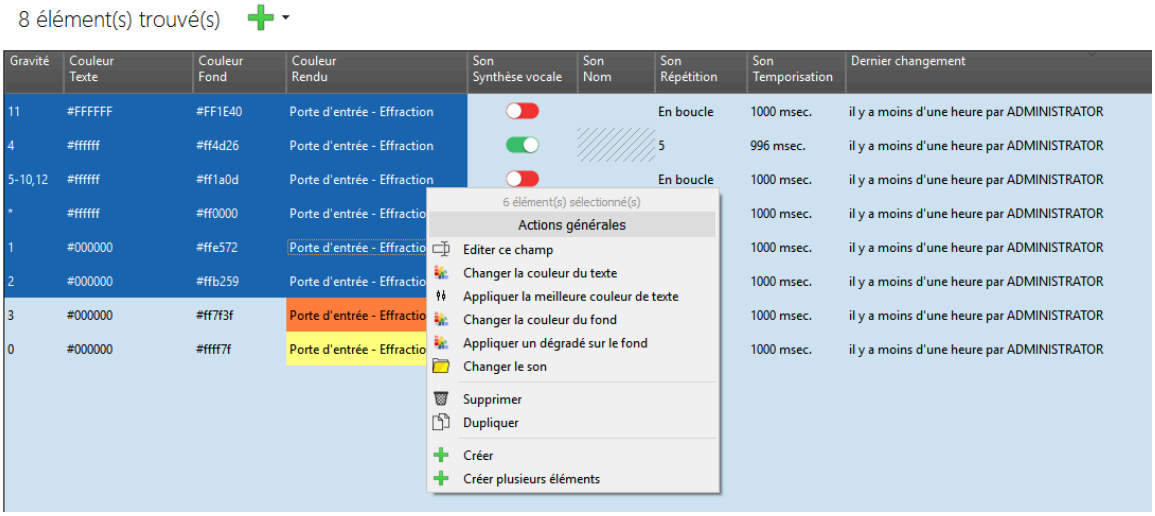
- **Couleur rendu** : Permet de voir le résultat obtenu.
- **Son synthèse vocale** : Passer en vert ce bouton pour activer la fonctionnalité. Le niveau de gravité d'alarme en cours de paramétrage utilisera la synthèse vocale de Windows pour lire l'alarme lors qu'elle est déclenchée.
  La zone **Synthèse vocale** dans la partie inférieure de cette fenêtre permet de paramétrer le ton, l'allure et le volume utilisés par la synthèse vocale.
  Le résultat qui sera obtenu avec le déclenchement de l'alarme peut être reproduit dans "Exemple".



- **Son Nom** : Si la synthèse vocale n'a pas été activée, il est possible de sélectionner un fichier audio à reproduire depuis la colonne "Son nom". Un niveau de gravité aura donc un fichier audio associé. L'alarme déclenchée avec ce niveau de gravité jouera ce fichier audio.
  L'icône du répertoire permet de choisir le fichier audio à associer au niveau de gravité.
  L'icône vert permet de jouer le son sélectionné afin de le vérifier.

- **Son Répétition** : Permet de paramétrer le type de répétition appliquée à l'audio de l'alarme (synthèse vocale ou fichier audio). Le son d'une alarme moins importante ne sera pas joué tant que l'alarme en cours n'a pas été acquittée (même si le son associé est terminé). Il est recommandé de lire les alarmes en boucle, avec une temporisation si besoin.
- **Son Temporisation** : Permet de paramétrer la cadence de répétition pour l'audio de l'alarme (synthèse vocale ou fichier audio). Ajuster la valeur avec les flèches, en msec.
- **Dernier changement** : Affiche la date et l'heure du dernier changement réalisé au paramétrage concerné.

Il est possible de sélectionner plusieurs alarmes pour les éditer à la fois. Sélectionner les éléments souhaités puis cliquer droit pour afficher les **Actions générales** disponibles :



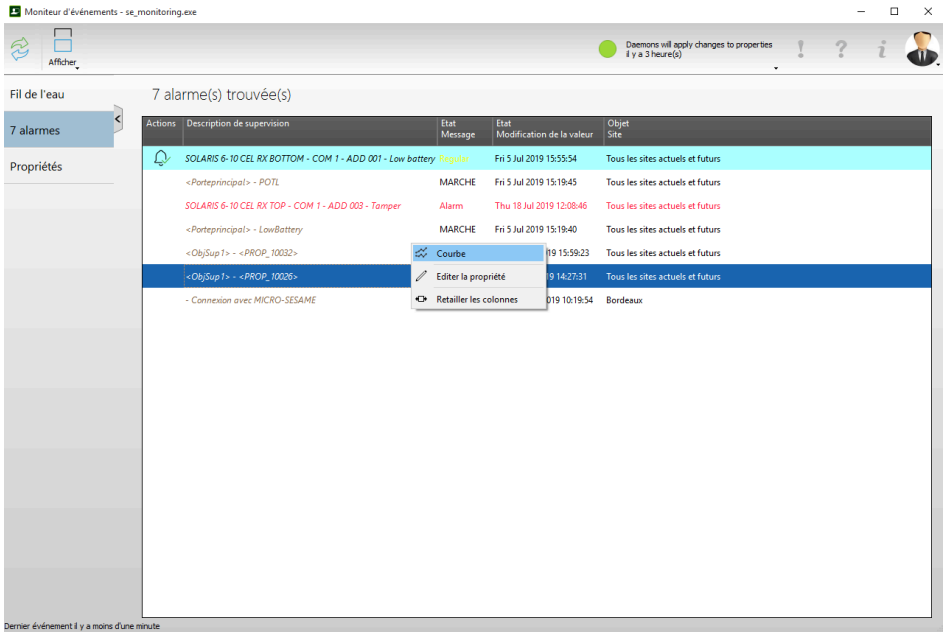
3.3. Alarmes

Cet onglet donne une vue exhaustive des alarmes en cours ou qui n'ont pas encore été acquittées.

Les alarmes sont d'abord triées par ordre de gravité.

Les alarmes sont organisées par ordre de gravité. Le code couleur permet de distinguer les niveaux de gravité et les types d'alarmes.et de distinguer les alarmes entre elles.

La majeure partie des actions disponibles dans le fil de l'eau à propos des alarmes sont aussi disponibles dans cette vue :



3.3.1. Code couleur des animations

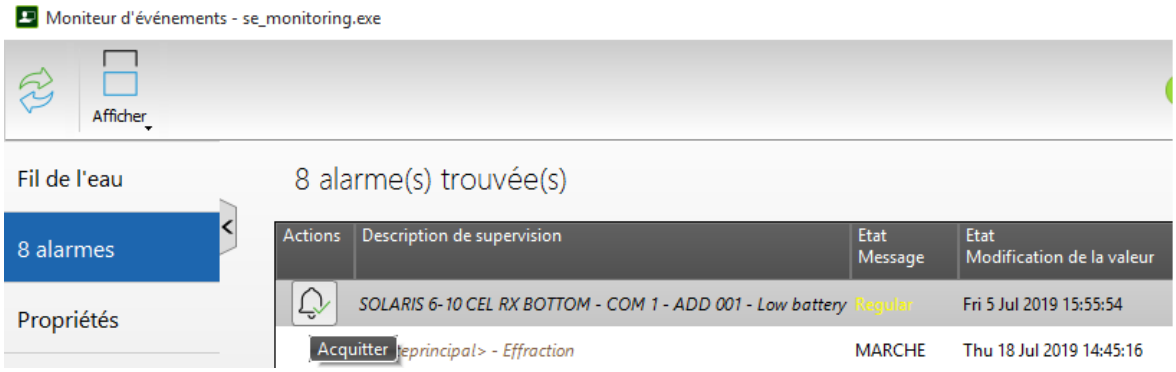
	État normal
	Alarme en cours acquittée
	Alarme en attente d'acquittement
	Propriété forcée
	Propriété forcée et en alarme non acquittée
	Propriété n'ayant pas reçu d'état
	Sans propriété
	Propriété **logique** à l'état 1 / Mono état récemment modifiée

3.3.2. Acquitter une alarme

L'onglet **Alarmes** affiche les alarmes trouvées. Uniquement les alarmes en cours ou non acquittées seront affichées dans cette zone.

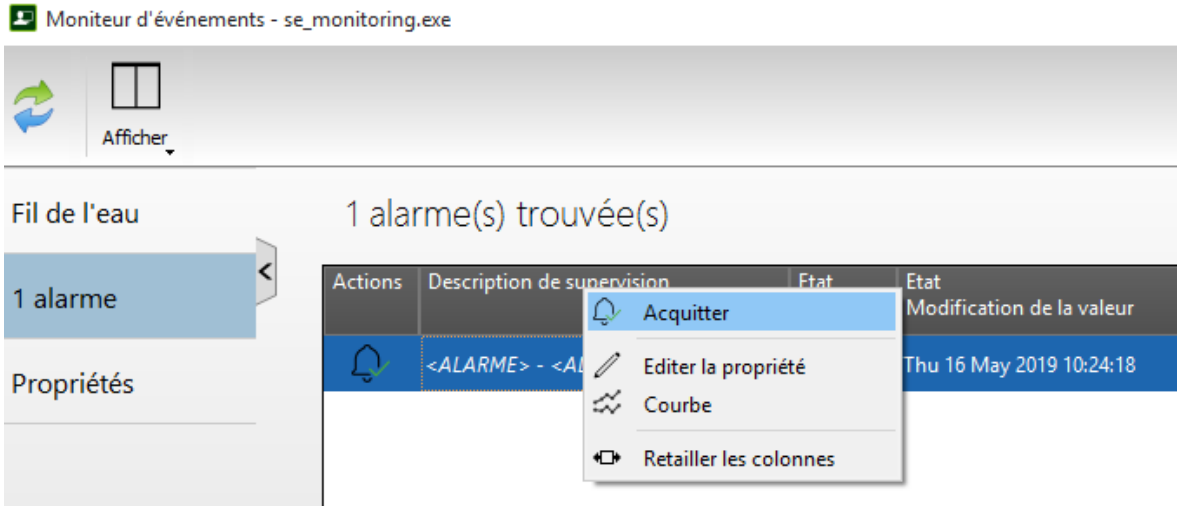
Les alarmes acquittées et qui ne sont plus en cours disparaissent.

Lors qu'une alarme est en cours, la colonne **Actions** affiche les options disponibles :

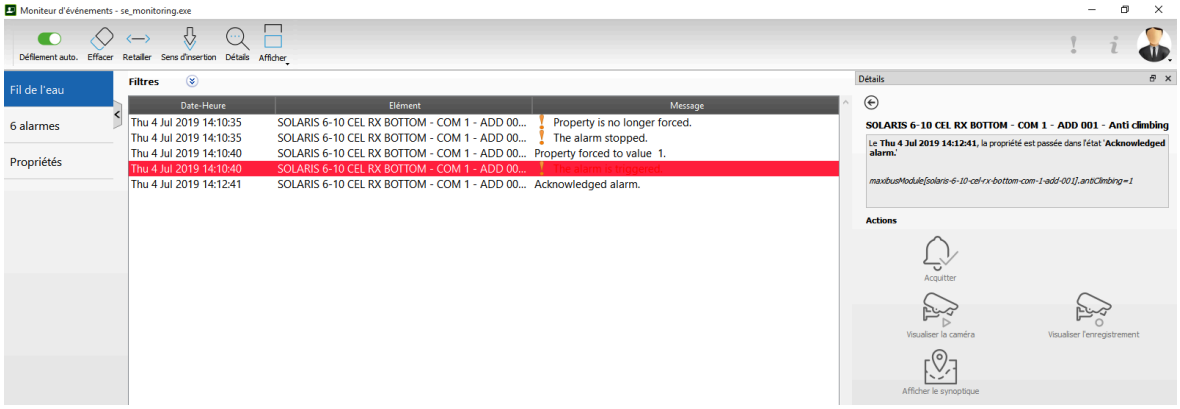


Pour une alarme acquittable, utiliser le **bouton** dans la colonne Actions ou accéder au menu disponible en cliquant droit et choisir l'option **Acquitter**.

Les alarmes acquittables peuvent avoir la synthèse vocale paramétrée (un son est joué lors que l'alarme est déclenchée). Pour plus de détails, consulter *la section dédiée.*



Lorsque l'alarme est acquittée, le couleur d'affichage de l'alarme change.



Une alarme acquittée est toujours affichée dans l'onglet Alarmes si celle-ci est toujours en cours.

3.3.3. Acquitter une alarme par plusieurs intervenants

L'acquittement d'une alarme peut être réalisé en plusieurs étapes, nécessitant l'intervention de plusieurs opérateurs.

L'acquittement par plusieurs intervenants peut être réalisé depuis des applications différentes (Moniteur d'évènements, animateur de synoptiques...).

Cas d'usage

L'installation du site et le paramétrage mise en place inclut des alarmes que, lorsqu'elles sont déclenchées, elles doivent être acquittées par deux intervenants différents : L'opérateur 1 et l'opérateur 2.

Chaque opérateur réalise un acquittement partiel.

L'opérateur 1 peut acquitter l'alarme depuis le moniteur d'évènements.
L'opérateur 2 peut acquitter l'alarme depuis l'animateur de synoptiques.

Pendant le processus, l'alarme s'affiche comme étant non acquittée (lorsqu'aucun opérateur a acquitté) ou acquittée partiellement (lorsqu'un des deux opérateurs a réalisé cette opération).

A la fin, l'alarme est affichée comme acquittée (comme une alarme nécessitant un seul intervenant pour l'acquitter) dans le moniteur d'évènements.

Pour paramétrer ce type d'acquittement pour une alarme, suivre ces indications :

- Paramétrer l'alarme et son masque d'acquittement depuis la fenêtre des *Objets et propriétés* :
  1. Dans le tableau d'édition des propriétés, cliquer droit sur l'en-tête du tableau et vérifier/activer l'option **Alarme > Masque d'acquittement**.
  2. Rechercher et sélectionner l'objet de surveillance et la propriété qui peut déclencher l'alarme.
  3. Dans la colonne **Alarme masque d'acquittement** attribuer la valeur d'acquittement.
     Une alarme déclenchée peut être :
     - acquittée entièrement par un opérateur ayant une valeur d'acquittement égale ou supérieure à la valeur définie sur la propriété
     - acquittée partiellement par des opérateurs ayant une valeur d'acquittement inférieure à la valeur définie sur la propriété
- Paramétrer les droits opérateurs des opérateurs en charge de l'acquittement depuis la fenêtre des **profils opérateurs**:
  Pour plus de détails sur les droits opérateurs, voir le chapitre dédié.
  1. Aller à l'onglet **Supervision**.
  2. Dans **Applications de supervision**, sélectionner **Toutes les applications** de supervision (sauf cas de paramétrage spécifique).
  3. Sélectionner l'option **Acquitter une alarme**.
  4. Dans le champ **Masque d'acquittement**, indiquer la valeur d'acquittement qui sera attribuée aux opérateurs ayant ce profil opérateur.

Calculer la valeur d'acquittement :

La valeur d'acquittement maximale est 0x3F.

Le profil opérateur Admin, lors qu'il a un masque d'acquittement associé, a par défaut la valeur 0x3F.

La conversion hexadécimale-binaire peut être utilisée afin de calculer correctement les valeurs d'acquittement à utiliser pour les différents profils opérateurs.

Afin d'acquitter une alarme de ce type, la valeur du masque d'acquittement des opérateurs et celle de l'alarme doivent être du même niveau ou supérieur (valeur d'acquittement égale ou supérieure à l'alarme afin de pouvoir l'acquitter).

Exemple d'acquittement par plusieurs intervenants avec des profils opérateurs ayant des valeurs d'acquittement différents:

Les opérateurs suivants sont chargés de la surveillance et de l'acquittement des alarmes.

Opérateurs	Valeur du masque d'acquittement en Hexadécimal	Valeur du masque d'acquittement en Binaire
Administrateur	0x3F	111111
Opérateur 1	0x1A	11010
Opérateur 2	0x1B	11011
Opérateur 3	0x3C	111100

Une alarme avec un masque d'acquittement d'une valeur 0x35 est déclenchée et doit être acquittée.

Alarme	Valeur du masque d'acquittement en Hexadécimal	Valeur du masque d'acquittement en Binaire
Alarme	0x35	110101

Pour qu'un opérateur ou un groupe d'opérateurs puissent acquitter totalement une alarme, il faut que les bits hauts (valeur à 1) du masque résultant correspondent à ceux du masque paramétré pour l'alarme.

Consulter la liste suivante pour avoir des exemples d'acquittements totaux ou partiels.

Cas rencontrés:

- L'administrateur peut acquitter l'alarme directement (acquittement total).

Masque de l'alarme	1	1	0	1	0	1
Masque d'acquittement	1	1	1	1	1	1

- L'opérateur 1 peut acquitter l'alarme. Cependant, il sera seulement capable de réaliser un acquittement partiel. Une intervention par un autre opérateur est nécessaire (acquittement supplémentaire) afin d'acquitter l'alarme complétement.

Masque de l'alarme	1	1	0	1	0	1
Masque d'acquittement	x	1	1	0	1	0

- L'opérateur 2 peut acquitter l'alarme. Cependant, il sera seulement capable de réaliser un acquittement partiel. Une intervention par un autre opérateur est nécessaire (acquittement supplémentaire) afin d'acquitter l'alarme complétement.

Masque de l'alarme	1	1	0	1	0	1
Masque d'acquittement	x	1	1	0	1	1

- Si les opérateurs 1 et 2 acquittent l'alarme chacun leur tour, l'alarme sera totalement acquittée (affichée dans le moniteur d'évènements comme acquittée).

Masque de l'alarme	1	1	0	1	0	1
Masque d'acquittement Résultant	1	1	0	1	0	1

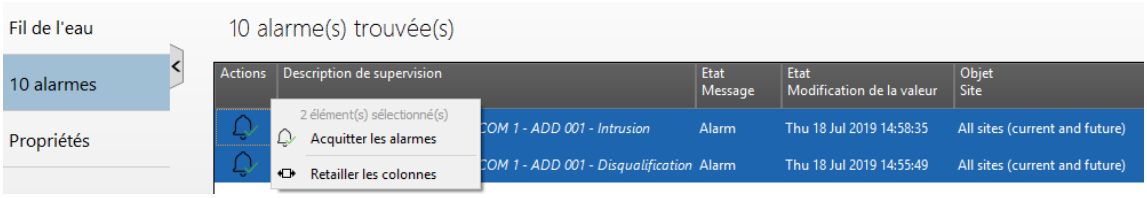
- **Attention:**Un masque ayant une valeur hexadécimale plus élevée que le masque de l'alarme ne suffit pas forcément à l'acquitter totalement.
  L'opérateur 3 peut acquitter l'alarme.Cependant, il sera seulement capable de réaliser un acquittement partiel. Une intervention par un autre opérateur est nécessaire (acquittement supplémentaire) afin d'acquitter l'alarme complétement.

Masque de l'alarme	1	1	0	1	0	1
Masque d'acquittement Résultant	1	1	1	1	0	0

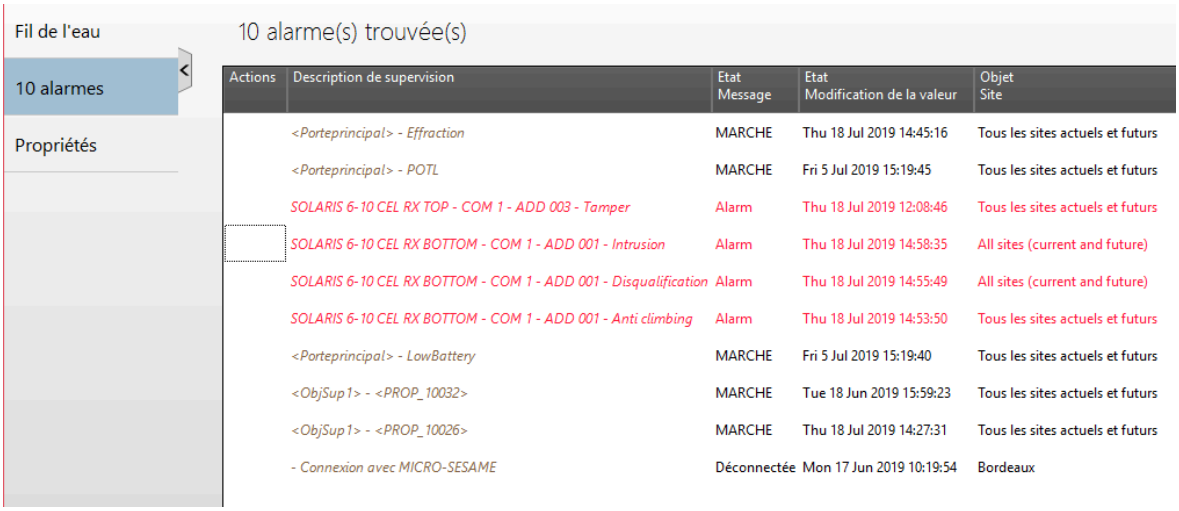
3.3.4. Acquitter un lot d'alarmes

Il est possible d'acquitter un lot d'alarmes en une seule opération :

- Dans l'onglet Alarmes, sélectionner les alarmes à acquitter.
- Cliquer droit pour afficher le menu contextuel.
- Sélectionner l'option **Acquitter les alarmes**:



- Les alarmes sont affichées en tant qu'alarmes acquittées :



3.3.5. Utiliser les tickets de main courante

La main courante est disponible à partir de la version 2021.2.

Au déclenchement d'une alarme acquittable, un ticket de suivi main courante est automatiquement ouvert pour rassembler les informations relatives à celle-ci:

- Opérateurs ayant interagi avec l'alarme.
- Commentaires d'acquittement.
- Horaires de déclenchement, d'acquittement, d'arrêt de l'alarme.
- Notes et commentaires.

Selon le paramétrage effectué, l'opérateur qui acquitte l'alarme doit effectuer une des actions suivantes:

- **Commentaire Obligatoire**: L'opérateur acquittant l'alarme doit nécessairement renseigner un commentaire afin d'acquitter l'alarme.
- **Commentaire optionnel** : L'opérateur acquittant l'alarme peut choisir de laisser un commentaire ou non.

- **Commentaire désactivé** : L'opérateur ne peut pas laisser de commentaires à l'acquittement d'une alarme.

Le paramétrage du commentaire d'acquittement se fait depuis l'onglet **Acquittement des alarmes** dans le paramétrage général.

Un ticket de suivi reste ouvert et accessible depuis le moniteur d'évènement tant que l'alarme acquittable n'a pas été totalement arrêté, c'est à dire totalement acquitté et la propriété associée de retour à son état normal. Dans le cas ou une alarme se redéclenche et le ticket associé est toujours ouvert, cet évènement sera inscrit dans le suivi du même ticket.

Pour ouvrir le ticket de suivi, effectuer un clic-droit sur l'alarme associée puis choisir **Voir le ticket main courante**. L'opérateur ayant les droits peut ainsi consulter le ticket, les évènements associés et ajouter une note si besoin.

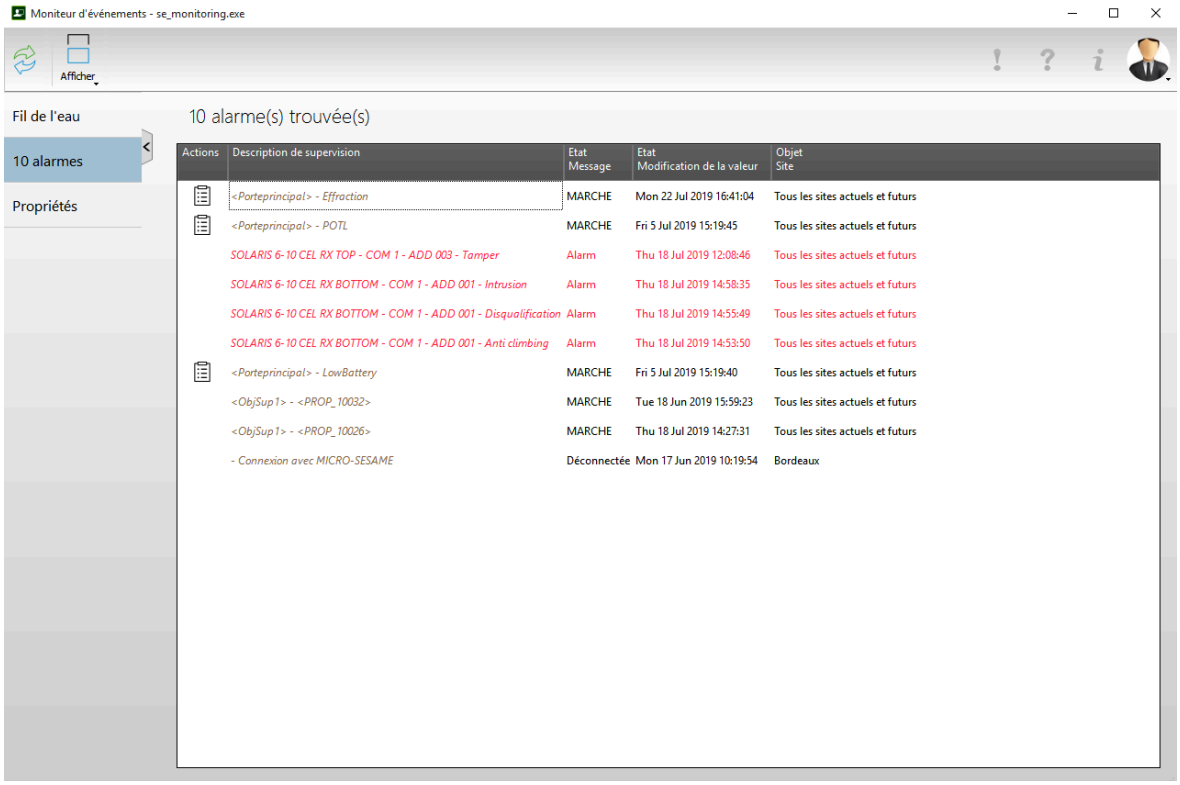
Une fois le ticket fermé, il ne sera plus disponible dans le moniteur d'évènement. Pour consulter les tickets fermés, se rendre sur WEBSESAME et suivre l'onglet **Main courante**.

La visualisation, l'édition et le paramétrage des tickets de suivis dépendent des droits opérateurs suivants:

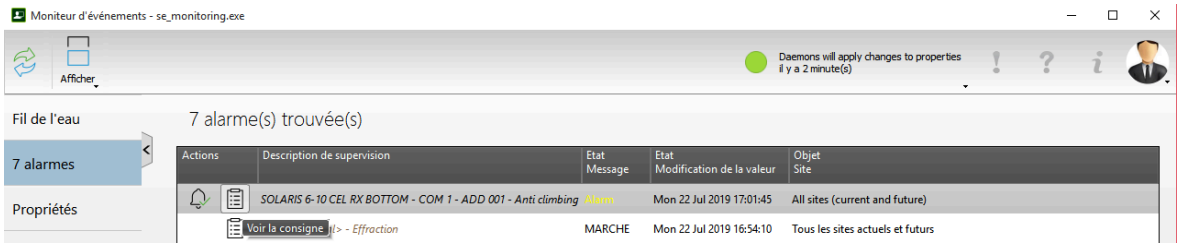
- Si l'opérateur a le droit d'**acquitter une alarme**, il peut visualiser le ticket associé et y ajouter une note.
- Si l'opérateur a le droit **Evènements techniques, Objets et propriétés de supervision** (onglet historique), il peut effectuer les actions suivantes:
  - Visualiser l'ensemble des tickets sur WEBSESAME.
  - Consulter un ticket, l'éditer, ajouter une note.
  - Modifier le sujet ou la description du ticket.

3.3.6. Consulter une consigne depuis l'onglet Alarmes

Lors qu'une consigne est associée à une propriété, et la propriété déclenche une alarme, la colonne **Actions** affiche l'icône permettant l'accès à la consigne :



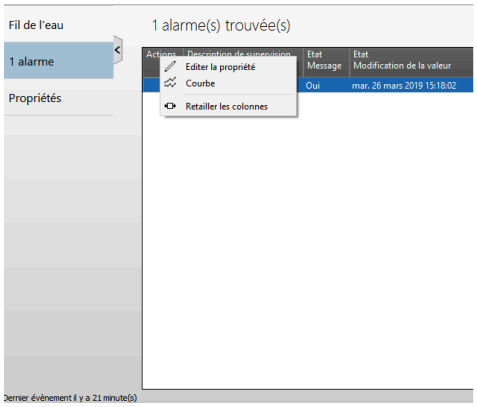
La colonne **Actions** peut signaler plusieurs actions à réaliser. Dans l'exemple ci-dessous, une alarme est à acquitter et contient une consigne pour l'opérateur (Après avoir acquitté l'alarme, la consigne est toujours disponible pour consultation dans cette colonne).



La consigne s'affiche. Lorsqu'une pièce jointe est disponible dans la consigne, cliquer sur cet élément pour l'ouvrir ou l'enregistrer :

3.3.7. Afficher la courbe d'historique d'une alarme

Faire clic droit sur l'élément concerné et sélectionner l'option **Courbe**.



La fenêtre **Graphique / courbe (se_chart.exe)** permet de visualiser les données de l'alarme en format graphique.

Une période peut être sélectionnée pour l'affichage des données.

Un export des données en format PDF est possible.

3.3.8. Accéder rapidement au paramétrage d'une propriété

Le paramétrage de la propriété liée à l'alarme se réalise depuis la fenêtre des Objets et propriétés de supervision.

Choisir l'option **Éditer la propriété** pour y accéder.

Pour plus de détails, consulter le chapitre *Objets et propriétés de supervision*.

3.4. Propriétés

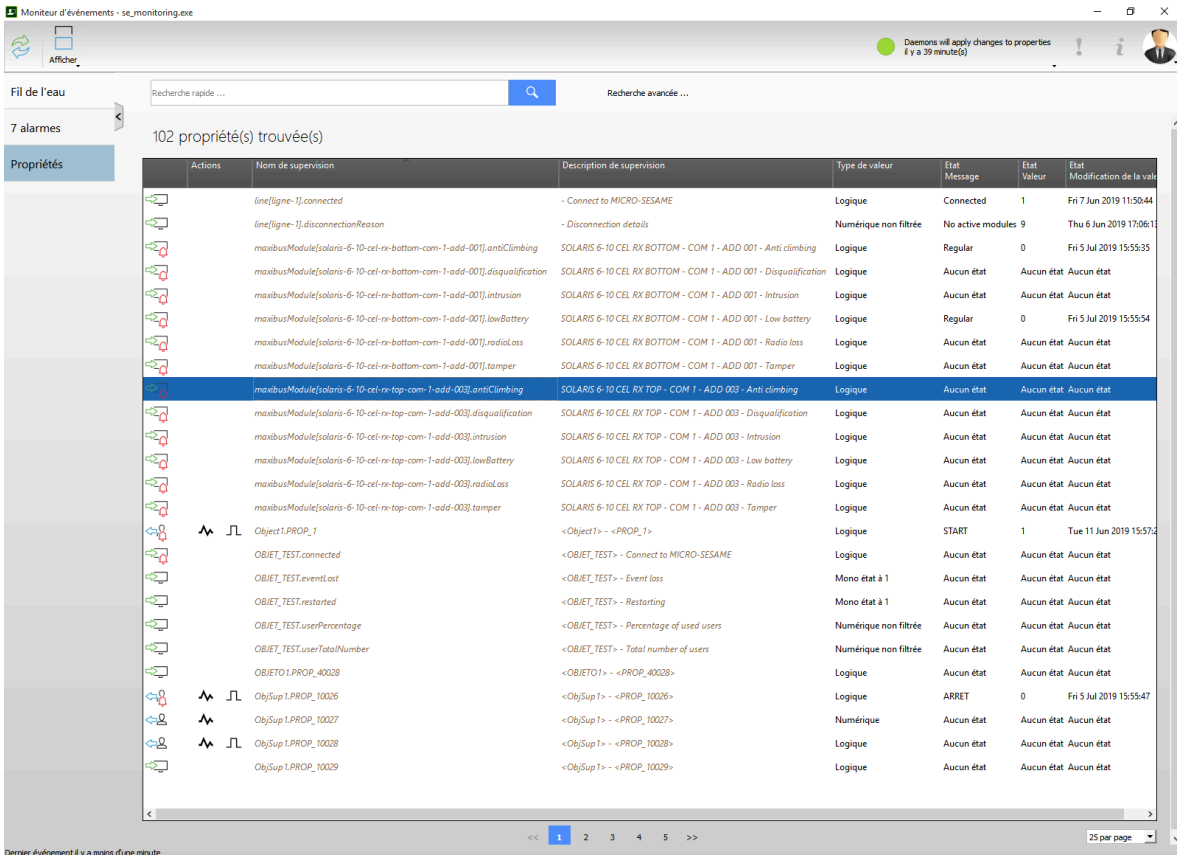
Un objet représente un élément installé sur site qui génère des informations (par exemple, une porte d'entrée/sortie équipée d'un lecteur). Les propriétés de supervision sont les différentes informations qui s'appliquent aux objets (par exemple, la propriété de porte ouverte) et qui permettent de les piloter dans MICROSESAME

L'onglet Propriétés dans le moniteur d'évènements permet de surveiller les différents types de propriétés, de surveiller son état (notification lors qu'une porte ouverte est détectée, par exemple) et de les éditer.

Cet onglet permet de rechercher des propriétés afin de connaître leur état et interagir avec.

Forcer une propriété permet d'inhiber les propriétés dans le cadre d'une maintenance, un détecteur défaillant ...

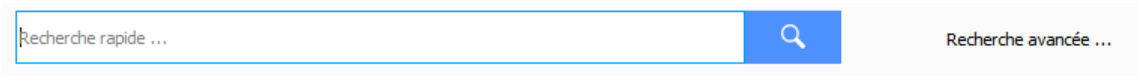
Cette vue est utile à l'exploitant mais aussi à l'intégrateur lors du paramétrage du site. Cette vue permet de diagnostiquer son installation en visualisant les états des propriétés, de télécommander les propriétés, d'ouvrir un synoptique associé à la propriété.



3.4.1. Utilisation de la recherche avancée sur les UTL

3.4.1.1. Utilisation des filtres dans une recherche avancée

1. Depuis le menu principal de MICROSESAME, suivre **Paramétrage > Matériels > Unité de traitement local [UTL]**.
2. Dans la section supérieure de la fenêtre, cliquer sur **Recherche avancée**, à droite du champ de recherche rapide.



3. Utiliser les filtres listés dans les 3 tableaux ci-après.

Tableau 3.1. Utilisation des filtres pour une recherche avancée

Filtre	Description
Filtre sélectionné	Des recherches peuvent avoir été sauvegardées après paramétrage, pour faciliter leur réutilisation. Cliquer dans le champ **Filtre sélectionné**, puis sélectionner éventuellement un filtre dans la liste déroulante.
3 champs de filtres paramétrables	Trois champs sont disponibles, dans lesquels la même liste de filtres est proposée. Par défaut, ces champs sont respectivement configurés sur les filtres *Nom*, *Activée*, *Microode (utilisateur)*, mais il est possible de paramétrer chacun d'entre eux sur n'importe quel filtre de la liste. Ces trois filtres peuvent se cumuler pour affiner la recherche.

Tableau 3.2. Affichage des filtres utilisables pour une recherche avancée

Filtre	Description
Nom	Filtrage sur tout ou partie du nom d'une UTL. Dans le premier champ, sélectionner la façon dont le nom va être utilisé et dans le deuxième champ, saisir une partie du nom d'une UTL.
Activée	Filtrage des UTLs qui sont activées dans le système ou pas. Le filtre est choisi en activant la case correspondante Oui ou Non (actif si coché).
Adresse	Filtrage sur l'adresse IP des UTLs. Dans le premier champ, sélectionner la façon dont l'adresse va être utilisée et dans le deuxième champ, saisir une partie d'une adresse IP ou une adresse IP spécifique.
Numéro de série	Filtrage sur un numéro de série d'UTL. Pour que la recherche soit possible, il faut que les numéros de série des UTLs aient été saisis dans les fiches UTL (automatiquement ou manuellement).

Filtre	Description
	Dans le premier champ, sélectionner la façon dont le numéro va être utilisé et dans le deuxième champ, saisir un numéro.
Ligne	Filtrage sur tout ou partie du nom d'une ligne de communication allouée à des UTLs. Dans le premier champ, sélectionner la façon dont le nom va être utilisé et dans le deuxième champ, saisir une partie d'un nom de ligne.
Microcode (utilisateur)	Filtrage sur tout ou partie d'un mot contenu dans du microcode saisi par un utilisateur. Dans le premier champ, sélectionner la façon dont le mot va être utilisé et dans le deuxième champ, saisir du texte. La recherche peut s'effectuer sur un mot contenu dans des fonctions (PULSE, SET ...) ou dans des commentaires.
Périmètre	Filtrage sur tout ou partie d'un nom de périmètre alloué à une UTL. Dans le premier champ, sélectionner la façon dont le nom va être utilisé et dans le deuxième champ, saisir une partie d'un nom de périmètre.
Commentaire	Filtrage sur tout ou partie d'un mot contenu dans les commentaires de la fiche UTL. Dans le premier champ, sélectionner la façon dont le mot va être utilisé et dans le deuxième champ, saisir du texte.

Tableau 3.3. Filtres liés à des fonctions de la fiche UTL

Filtre	Description
Filtres sur les lecteurs	Nombre de lecteurs, codes classes associés ...
Filtres sur les échanges	Propriétés émises ou reçues par l'UTL, sur des échanges avec le serveur ou avec d'autres UTLs.
Filtres sur les fonctions Intrusion V1 ou Intrusion CUBE	Nombre de détecteurs, de groupes, de claviers, de profils ...
Filtres sur la fonction transmission	Nombre de destinataires, de profils, de télécommandes ...
Filtres sur les utilisateurs	Nom d'un opérateur qui a créé ou modifié une UTL.
Compilation	Nombre d'erreurs, types d'avertissement, nombre de succès ...

4. Pour lancer la recherche, cliquer sur le bouton **Rechercher**.
5. Pour supprimer les filtres, cliquer sur le bouton **Effacer**.

3.4.1.2. Sauvegarde d'une recherche définie avec différents filtres

1. Paramétrer les filtres désirés dans chaque champ en utilisant les listes déroulantes.
2. Renseigner le nom du filtre final à enregistrer dans le champ **Filtre sélectionné**.
3. Cliquer sur le bouton ✚. Le filtre est enregistré et peut être rappelé à tout moment en le sélectionnant depuis la liste déroulante.

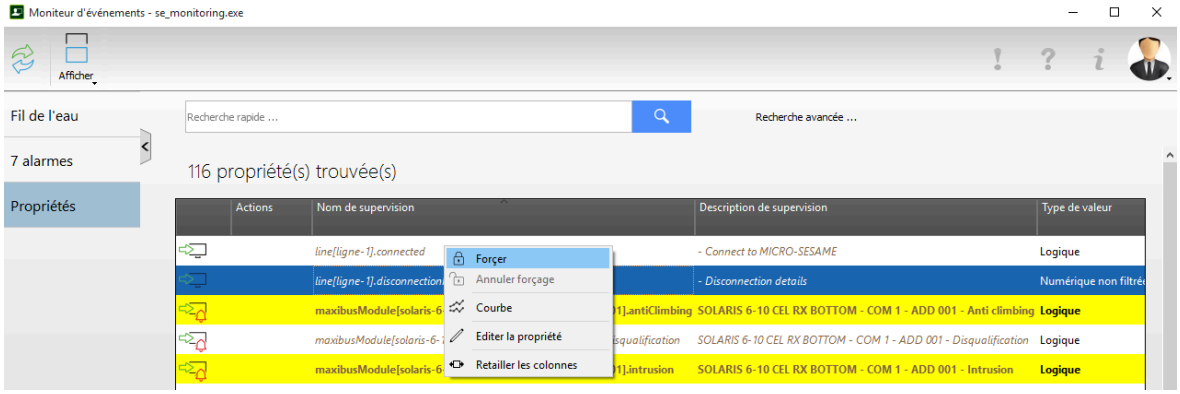
3.4.2. Connaître l'état des propriétés

La première colonne affiche l'état des **propriétés**, pouvant être :

- Un message
- Une valeur
- Une propriété forcée

3.4.3. Forcer l'état d'une propriété

Sélectionner la propriété souhaitée et cliquer droit pour afficher le menu. Sélectionner l'option **Forcer**.



Une fenêtre permet de choisir la valeur qui sera utilisée pour forcer la propriété.

Les options de forçage peuvent varier selon la nature de la propriété. Pour plus de détails sur les propriétés, consulter *Objets et propriétés de supervision*

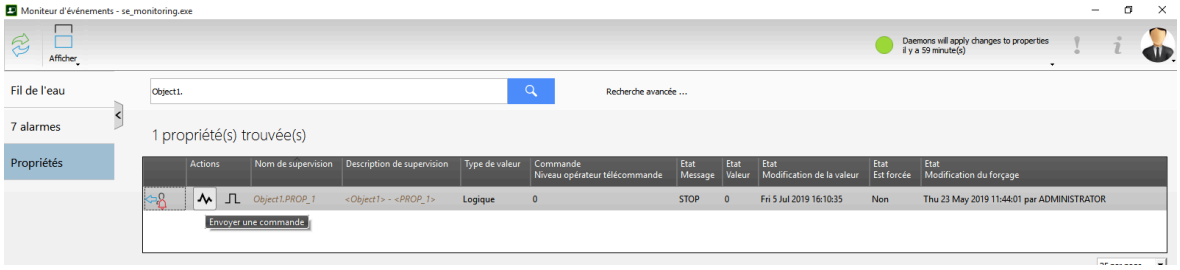
3.4.4. Envoyer une impulsion ou une commande

En fonction du type de commande, les options suivantes peuvent être proposées :

- Booléen
- Entier
- Impulsion

Pour les télécommandes, la colonne **Actions** affiche les options disponibles :

- Envoyer une télécommande
- Envoyer une impulsion



3.4.5. Comprendre les codes couleurs des propriétés

- **Fond jaune texte marron** : L'état d'une propriété a été **forcé**. Le texte est affiché en jaune ou le fond de la ligne est affiché en jaune, selon si la ligne est sélectionnée ou pas.
- **Fond blanc texte marron** : Propriété d'alarme (affichée dans l'onglet "Alarmes" en cas d'alarme en cours ou non acquittée).

3.4.6. Voir les courbes et graphes liés à une propriété

Sur la propriété souhaitée, cliquer droit et sélectionner l'option **Courbe**.

3.5. FAQ

3.5.1. Pourquoi certaines informations ne sont pas visibles dans le fil de l'eau ?

Certaines fonctionnalités peuvent être disponibles uniquement pour certains opérateurs avec des droits d'accès particuliers.

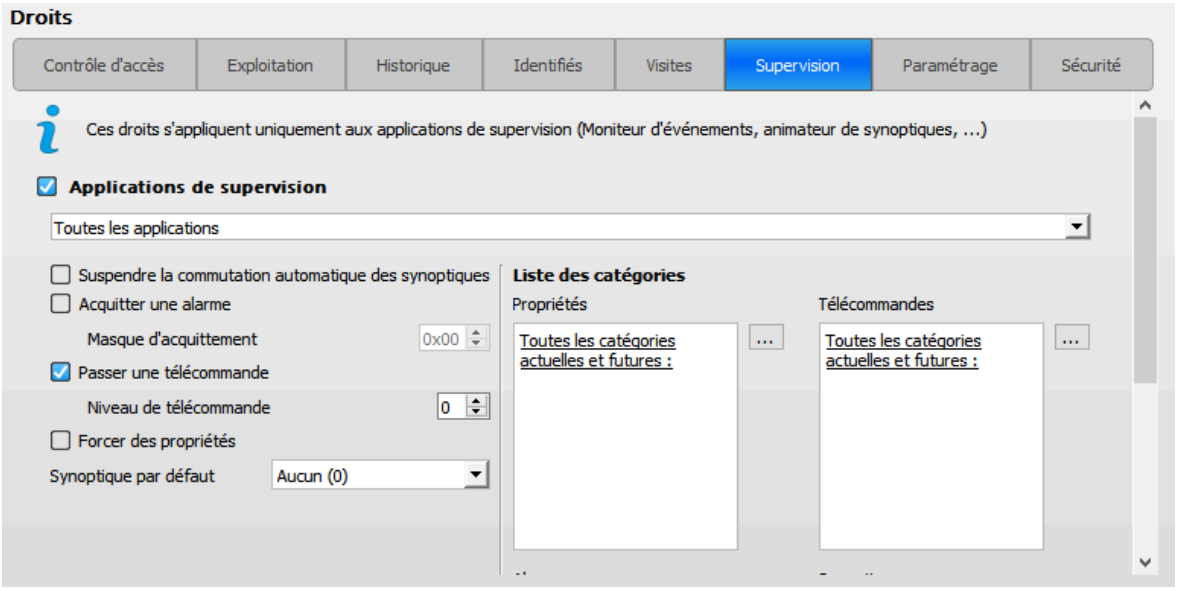
L'affichage de plus ou moins d'information dans le fil de l'eau peut être conditionné aux **droits opérateurs de l'opérateur MICROSESAM**.

Pour plus d'information, voir la section sur les droits opérateurs.

3.5.2. Pourquoi les télécommandes ne passent pas ?

Vérifier le droit opérateur "Passer une télécommande" dans le profil opérateur utilisé par l'opérateur essayant de passer la télécommande.

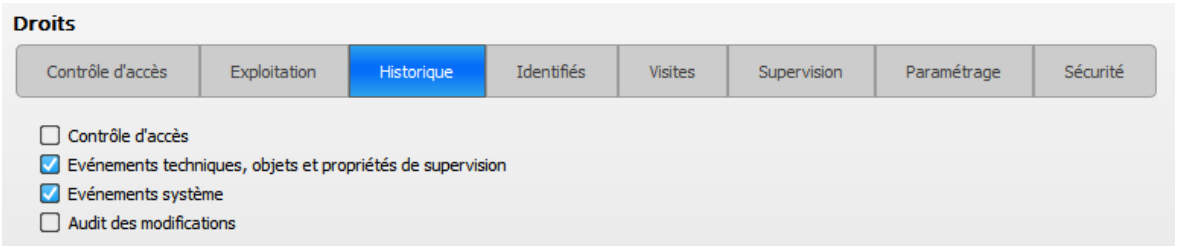
Pour vérifier ce droit, aller à la fenêtre des profils opérateurs. Dans l'onglet Supervision, vérifier l'option "Passer une télécommande" et le niveau de télécommande :



3.5.3. Pourquoi la propriété ne remonte jamais dans le fil de l'eau ?

L'opérateur a besoin d'un droit d'accès aux fonctions l'historique :

Dans la fenêtre des profils opérateurs, accéder à l'onglet Historique et cocher les options nécessaires :



3.5.4. Pourquoi ma ligne est jaune ?

Lorsque la ligne d'une propriété est affichée en jaune, l'état a été forcée.

3.5.5. Pourquoi la synthèse vocale sur les alarmes à acquitter n'est pas fonctionnelle ?

Lorsqu'un site a mis en place la synthèse vocale sur les alarmes à acquitter et que l'opérateur n'a pas cette fonction (impossibilité d'entendre les alarmes déclenchant la synthèse vocale), vérifier les droits attribués au profil opérateur utilisé par l'opérateur pour se connecter à MICROSESAME:

Vérifier dans l'onglet Supervision que le droit d'acquittement est attribué.

Pour plus d'information sur les droits opérateurs, consulter le chapitre dedié.

Pour plus d'information sur la configuration des alarmes, consulter la section ???

Chapitre 4. Contrôle visuel des accès (PVCA)

4.1. Le contrôle visuel des accès

Le **Contrôle Visuel des Accès (PCVA)** permet à l'opérateur le traitement des événements suivants :

- Passage d'un identifié autorisé sur un lecteur ou sur un groupe de lecteurs.
- Passage d'un identifié interdit sur un lecteur ou sur un groupe de lecteurs.
- Passage à 1 d'une propriété logique.

Cas d'usage :

Lorsqu'une personne présente son identifiant autorisé, la fonction PCVA est déclenchée et permet d'afficher simultanément la photo de l'identifié et l'image vidéo de l'accès, si la vidéo est disponible. Suite à cette vérification, l'ouverture de la porte peut être effectuée de manière manuelle par l'opérateur ou de manière automatique. D'autres actions peuvent être aussi paramétrées.

Pour **accéder** à cette fonctionnalité, taper PCVA dans la barre de recherche du menu principal de MICROSESAME:

- Pour accéder au **paramétrage**, sélectionner Paramétrage > Contrôle d'accès > Contrôle Visuel des accès (PCVA).
- Pour accéder à l'**exploitation**, sélectionner Exploitation > Supervision > Contrôle Visuel des accès (PCVA) ou Contrôle Visuel des accès élargi (PCVA WIDE).

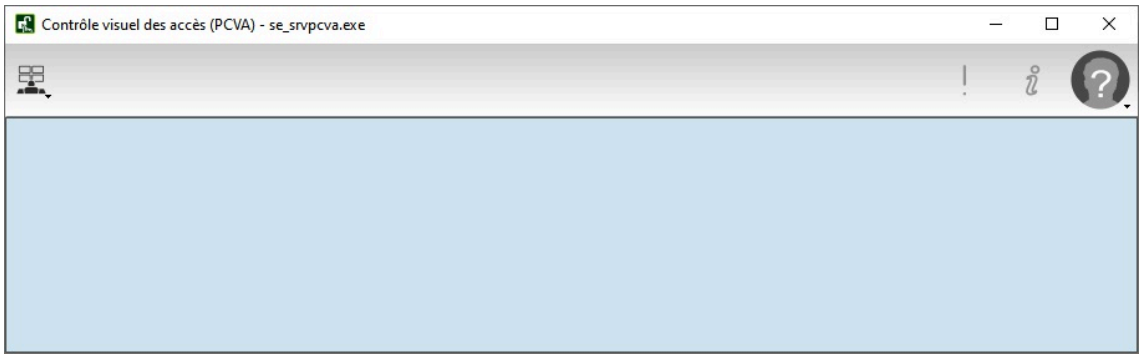
Pour garder un accès direct aux applications, il est possible de les ajouter aux **favoris** dans le menu principal de MICROSESAME. Pour cela, cliquer sur l'icône "Ajouter aux favoris".

4.2. Exploitation d'un point de contrôle visuel des accès (PCVA)

Après le paramétrage d'un PCVA, la procédure suivante décrit son exploitation dans MICROSESAME

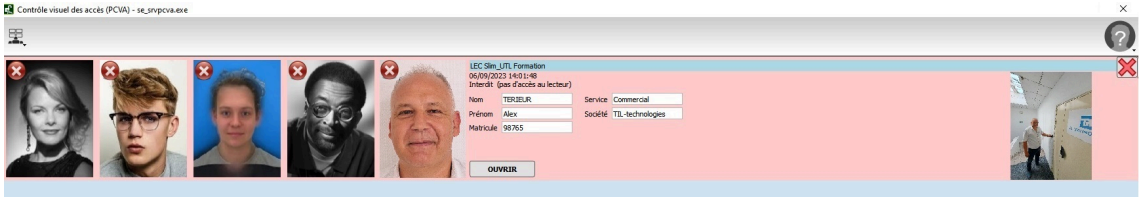
1. Se connecter au poste client avec le profil opérateur ayant les droits opérateurs nécessaires au lancement du PCVA.
2. Lancer MICROSESAME et lancer l'une des deux applications d'exploitation du PCVA :
   - **Exploitation > Supervision > Contrôle visuel des accès (PCVA)** : L'affichage des évènements est en mode "normal". Jusqu'à **5 évènements d'un même PCVA peuvent être affichés simultanément** sur la même ligne (dans la limite définie lors du paramétrage du PCVA avec le paramètre "Nombre maximum d'évènements affichés par PCVA").
   - **Exploitation > Supervision > Contrôle visuel des accès élargi (PCVA WIDE)** : L'affichage d'un évènement PCVA se fait en plan élargi (grossissement des informations à l'écran). Avec ce type d'exploitation, **un seul évènement peut être visualisé** à la fois. Ainsi, si plusieurs évènements d'un même PCVA surviennent, seul le dernier sera affiché (par remplacement de l'évènement précédent).

3. La fenêtre du PCVA se lance. Cette fenêtre s'affiche vide, lorsqu'aucun évènement PCVA n'est déclenché.

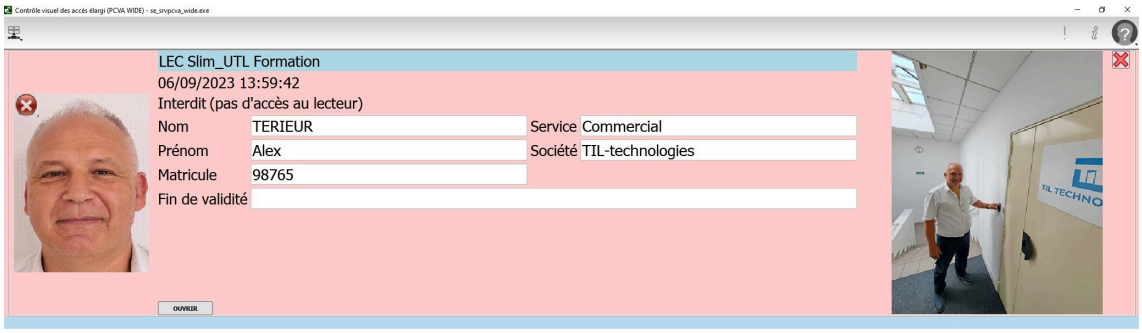


Vérifier que le nom du poste et le nom d'hôte correspondent.
Le message "Aucune information affichable, aucun paramétrage concernant le PCVA n'a été configuré" peut apparaître, si le nom du poste client n'est pas exactement le nom d'hôte de la machine qui exécute l'application d'exploitation du PCVA.

Exemple d'affichage avec le PCVA déclenché :



Exemple d'affichage avec le PCVA élargi déclenché :



Consulter les remontées dans le moniteur d'évènements pour vérifier le fonctionnement des différents éléments utilisés par le PCVA.

Chapitre 5. L'animateur de synoptique

5.1. Introduction

L'**animateur de synoptiques** est une application permettant de visualiser une représentation graphique d'une installation MICROSESAME à superviser. L'animateur de synoptiques permet l'exploitation des synoptiques déjà générés.

La représentation est composée d'un ensemble de **dessins** élémentaires (nommés **composants**) pouvant interagir avec l'environnement technique (remontées d'alarme ou télécommandes) en fonction des changements d'états des équipements représentés et surveillés par le superviseur.

Cette documentation décrit l'utilisation de l'animateur de synoptiques uniquement, pour détailler l'exploitation de synoptiques déjà crées.

Pour savoir plus sur la création ou l'import de synoptiques, consulter la documentation dédié de l'éditeur de synoptique.

5.2. Accès aux applications

Pour lancer l'**animateur de synoptiques** (se_synoptic_animator.exe) depuis l'application MICROSESAME, suivre *Supervision > Animateur de synoptique* ou chercher "synoptique" dans le menu principal.

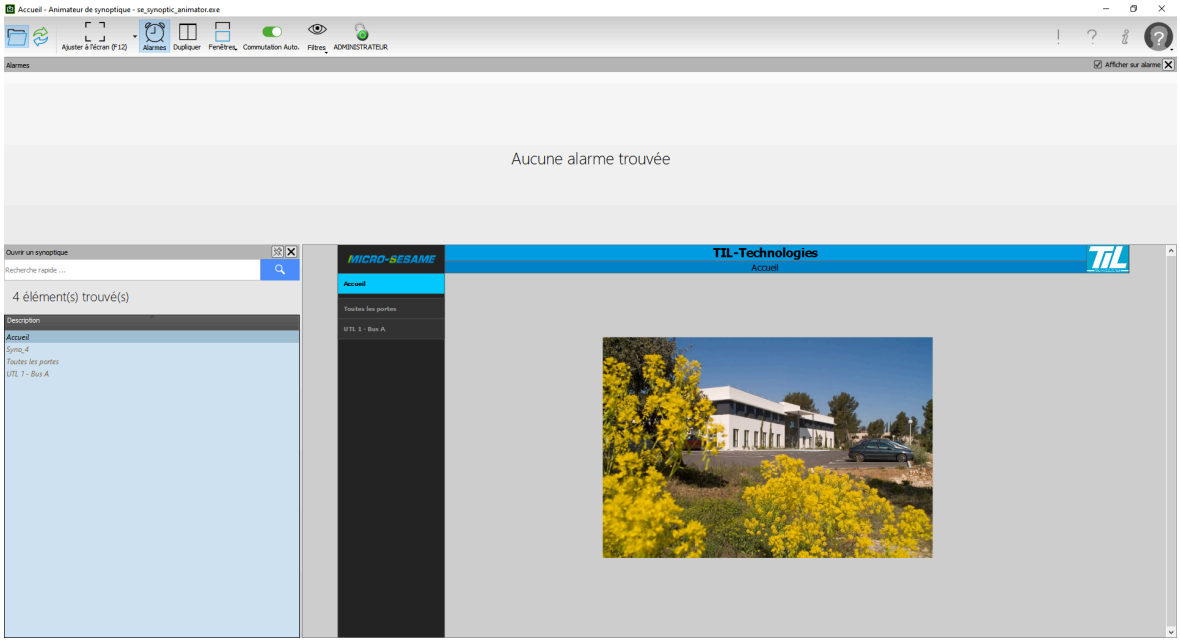
Pour lancer l'**éditeur de synoptique** (se_synoptic_editor.exe) depuis l'application MICROSESAME, suivre *Paramétrage > Supervision > Éditeur de synoptique* ou chercher "synoptique" dans le menu principal.

Pour ajouter ces applications à l'accueil du menu MICROSESAME, il est possible de les ajouter aux **Favoris** en cliquant sur l'icône étoile.

(Cliquer à nouveau sur l'icône étoile supprime ces applications des Favoris).

5.3. Présentation de l'animateur de synoptiques

Après lancement de l'application, la fenêtre s'affiche sous une apparence ressemblant à ceci :



La barre de menu est composée de différentes actions possibles :

Fonction	Description
Ouvrir	Afficher les synoptiques existants
Recharger	Actualiser le synoptique principal
Ajuster à l'écran (F12)	Afficher le synoptique sélectionné selon les options suivantes : • zoom avant/zoom arrière (+/-) • 100% • plein écran Pour un meilleur rendu du synoptique, l'affichage avec le mode "en haut à gauche" est recommandé.
Plein écran (F11)	Basculer la fenêtre de l'application au format de l'écran
Alarmes	Lister les alarmes actives/en défaut.
Dupliquer (shift + double clic)	Permettre un affichage de plusieurs synoptiques simultanément. Afficher des synoptiques dans une fenêtre secondaire.
Fenêtre	Fermer les synoptiques secondaires / Permettre l'ouverture et la fermeture des listes de synoptiques ou d'alarmes

Fonction	Description
Commutation auto	Activer/désactiver le basculement automatique vers un synoptique lié à une alarme qui se déclenche
Filtres	Permet de filtrer les composants en fonction du site ou des catégories assignées.
Connecter	Autoriser les actions possibles définies dans les synoptiques selon les droits opérateurs
Rafraichir les propriétés	Indique quel(s) automate(s) ont été rafraichi et la fréquence si un rafraichissement des propriétés a eu lieu.
Informations / A propos	Indique les informations de l'installation de MICROSESAME et les types de traces possibles
Utilisateur	Permettre l'affichage de la fiche identifié et du profil de l'opérateur connecté

5.4. Gestion des synoptiques

Les représentations graphiques réalisées par l'éditeur de synoptique ont la possibilité d'être visibles dans l'interface utilisateur selon les **droits des opérateurs**.

Voir la documentation dédiée pour savoir plus sur le fonctionnement des droits opérateurs.

5.4.1. Visualisation de synoptiques

La visualisation des synoptiques dépend des paramètres définis depuis les **catégories** et les **profils opérateurs** (voir les chapitres correspondants dans la documentation).

Un utilisateur ayant des droits restreints et une **visibilité** réduite ne pourra pas voir des synoptiques d'une catégorie différente de la sienne.

Depuis un synoptique, une commande de basculement d'un synoptique autorisé vers un synoptique restreint génère un message d'erreur.

L'utilisateur est donc averti que ses droits ne suffisent pas.

Les synoptiques sans catégories sont visibles par tout le monde.

La fonction **Filtres** située dans la barre de menu permet à l'utilisateur de se focaliser sur un **site** ou une **catégorie d'éléments** à superviser.

1. Dans la partie supérieure de la fenêtre, cliquer sur **Filtres**.

2. Dans la liste déroulante, sélectionner les sites et les catégories d'éléments à superviser.

Après validation, seules les informations associées aux sites et catégorie sélectionnés seront remontées dans l'animateur de synoptique.

L'utilisation de cette fonctionnalité **désactivera** la **commutation automatique** sur des alarmes associées à des **sites** ou **catégories** non sélectionnés dans les filtres

5.4.2. Télécommandes

Une télécommande permet de changer l'état d'une propriété d'objet suivant un clic ou une saisie de valeur.

Les télécommandes dépendent des filtres définis depuis les catégories et les profils opérateurs (voir les chapitres correspondants pour plus de détails sur les catégories et les profils opérateurs).

5.4.2.1. Télécommandes logiques

Une télécommande logique agit uniquement sur un changement d'état Tout Ou Rien (TOR).

Afin d'utiliser ces télécommandes logiques, préalablement définies dans les propriétés d'objet ("Objets et propriétés de supervision"), il suffit de cliquer sur les boutons prévus à cet effet sur le synoptique.

Cela aura pour effet de changer les propriétés adéquates de l'état '0' à '1' et inversement.

5.4.2.2. Télécommandes numériques

Une télécommande de type numérique permet de changer la valeur d'une propriété en fonction d'une valeur saisie manuellement.

La valeur renseignée sera comprise dans un intervalle particulier et paramétré dans l'éditeur de synoptique.

5.4.2.3. Télécommandes mono état

Les télécommandes avec des propriétés mono état changent selon le paramétrage appliqué à la propriété depuis la fenêtre "Objets et propriétés de supervision".

L'animateur de synoptiques affiche le changement d'état avec une animation. Pour le paramétrage de l'affichage selon le changement d'état, voir l'*Éditeur de synoptique*.

5.5. Bureau synoptique

La fonctionnalité **bureau synoptique** est disponible à partir de **MS 2021.4**. Elle permet à l'utilisateur de sauvegarder une configuration de synoptique afin de pouvoir la rétablir simplement.

Une fois une configuration synoptique mise en place (instances ouvertes, filtres appliqués, préférences paramétrées,...), l'opérateur peut choisir de sauvegarder la configuration actuelle pour pouvoir la rouvrir quand il le souhaite.

5.5.1. Éléments de configuration des bureaux synoptiques

Les bureaux synoptiques permettent de conserver les éléments de configuration suivants :

- Instances de l'application **Animateur de synoptique** ouvertes
- Filtres appliqués (Sites et catégories)
- Commutation automatique
- Affichage du dock des alarmes
- Son alarme
- Afficher sur alarme

La fonctionnalité bureau est également disponible dans l'application PCVA. La configuration d'un bureau dans l'animateur de synoptique rend donc possible l'association, **dans un même bureau**, de l'application **Animateur de synoptique** et de l'application **PCVA**.

5.5.2. Enregistrement d'un bureau synoptique

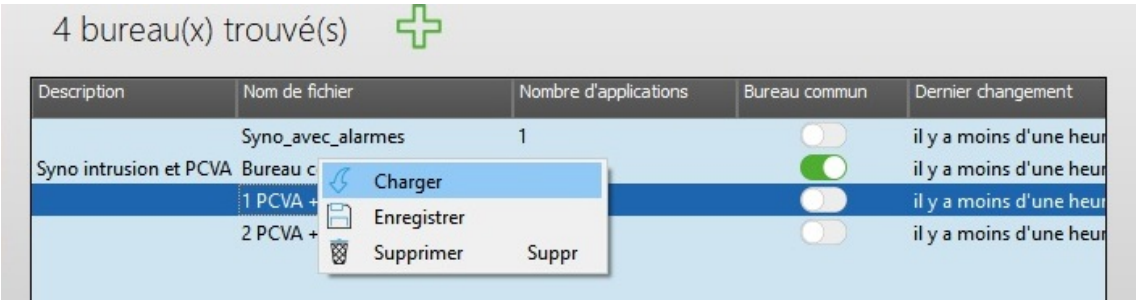
1. Ouvrir les instances et/ou applications PCVA et Animateur de synoptiques désirées, devant être enregistrées dans le même bureau.
2. Dans la fenêtre de l'application Animateur de synoptiques, cliquer sur l'icône  .
3. Cliquer sur **Gérer les bureaux** , puis dans la fenêtre qui s'ouvre, cliquer sur **Créer une nouvelle configuration (+)** .
4. Sélectionner la nouvelle ligne qui se crée dans la liste, puis double-cliquer dans les champs **Description** et **Nom de fichier** pour saisir des libellés.
5. Par défaut, le bureau créé est limité à l'opérateur responsable de son enregistrement. Positionner l'interrupteur **Bureau commun** au vert, si le bureau doit être accessible pour l'ensemble des opérateurs.
6. Cliquer sur **Modifier la configuration (disquette)** : Le bureau est désormais enregistré.

   Avant d'enregistrer, bien vérifier que la ligne sélectionnée correspond bien au bureau à créer. Si la sélection est faite sur une autre ligne, alors le bureau associé sera remplacé par celui en cours.

7. La colonne **Nombres d'applications** indique le nombre d'instances de l'application et/ou le nombre d'applications qui ont été enregistrées.

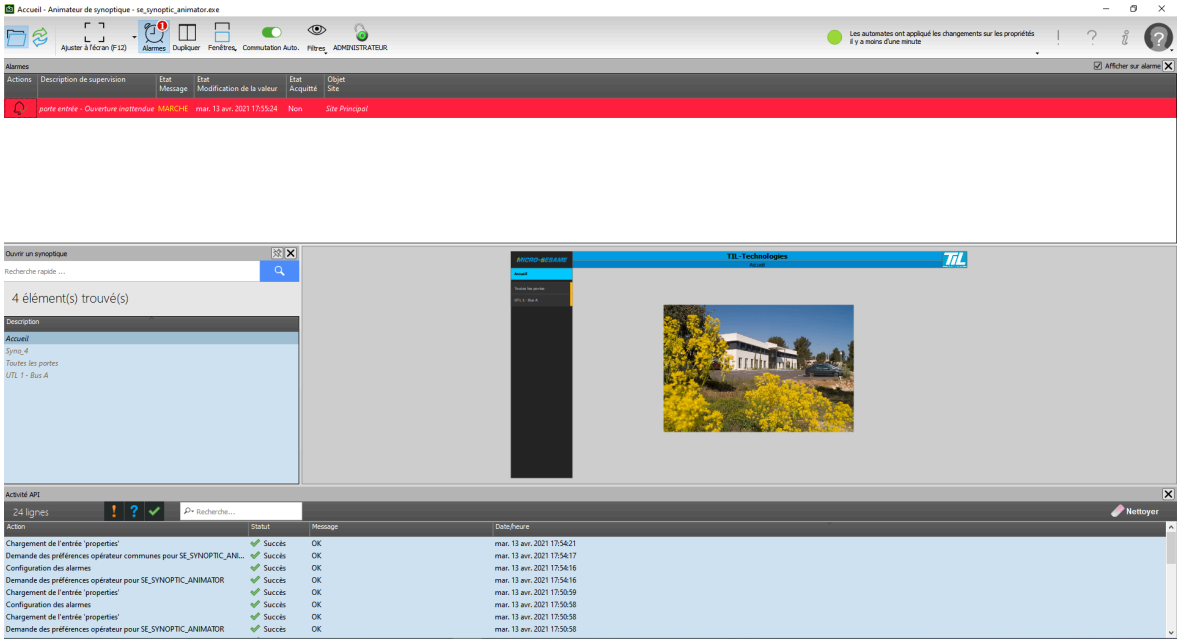
5.5.3. Choix d'un bureau synoptique

1. Pour afficher la liste des bureaux visibles par l'opérateur et ouvrir une configuration, cliquer sur l'icône associée aux bureaux synoptiques.
   Seuls les trois derniers bureaux appelés sont proposés.
2. Pour ouvrir un autre bureau, sélectionner **Gérer les bureaux**, puis faire un clic droit sur le bureau souhaité et sélectionner l'option **Charger**.



5.6. Alarmes

La gestion des alarmes est accessible depuis le moniteur d'évènements mais également depuis l'animateur de synoptiques, grâce aux représentations graphiques et au menu Alarmes.

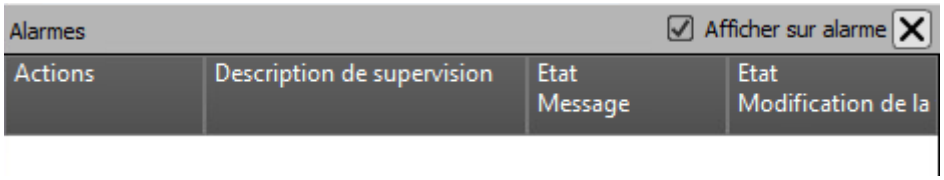


L'animateur offre, selon les droits opérateurs et l'édition des synoptiques, la possibilité d'afficher les alarmes, d'acquitter les alarmes, d'accéder aux propriétés et d'observer les courbes correspondantes.

Pour afficher le menu contextuel, effectuer un clic droit sur la propriété en alarme.

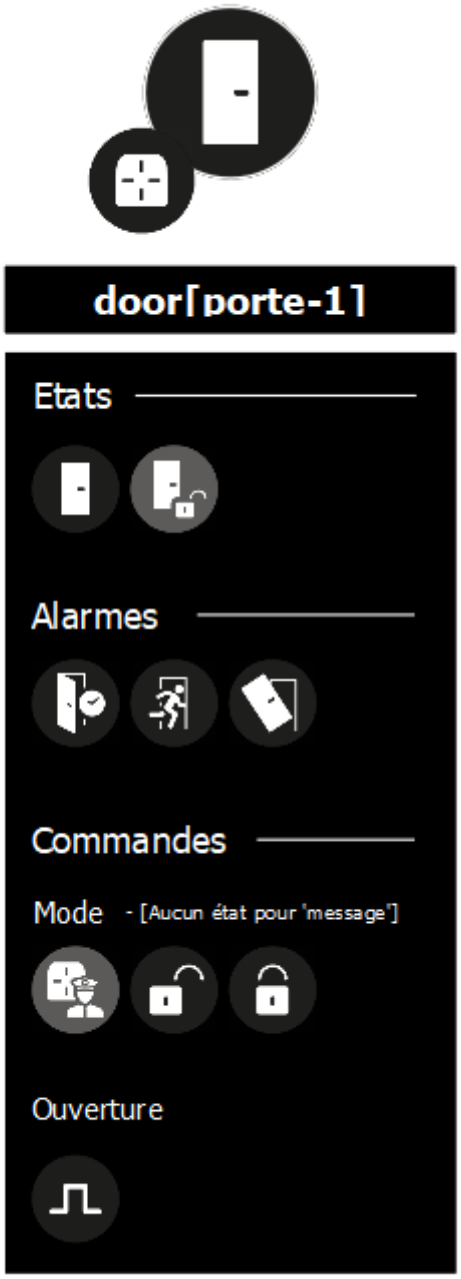
Il est possible d'ajouter des informations dans le tableau des alarmes en effectuant un clic droit dans l'entête du tableau et en sélectionnant les cases adéquates.

L'option "Afficher sur alarme" permet l'affichage de la fenêtre "Alarmes" lors du déclenchement d'une alarme. Cette option fait partie des préférences opérateur conservées entre deux lancements de l'animateur.



5.6.1. Symboles pré-configurés

Les symboles **"Door System"** permettent à l'utilisateur de visualiser les états de sa porte de façon synthétique mais aussi de passer des commandes.

Symbole DoorSystem	Sybole DoorSystemContextMenu
	
	État de la porte : Ouverte / Fermée

	État de pilotage d'ouverture de la porte : Relais d'ouverture est piloté ou non
	État de la commande manuelle d'ouverture : Commande actionnée ou non
	Alarme POTL : se déclenche lorsque la porte est trop longtemps ouverte (temporisation paramétrable dans le MICROCODE)
	Alarme Ouverture inattendue
	Alarme Ouverture d'urgence
	Envoi d'une impulsion sur le relais d'ouverture de la porte

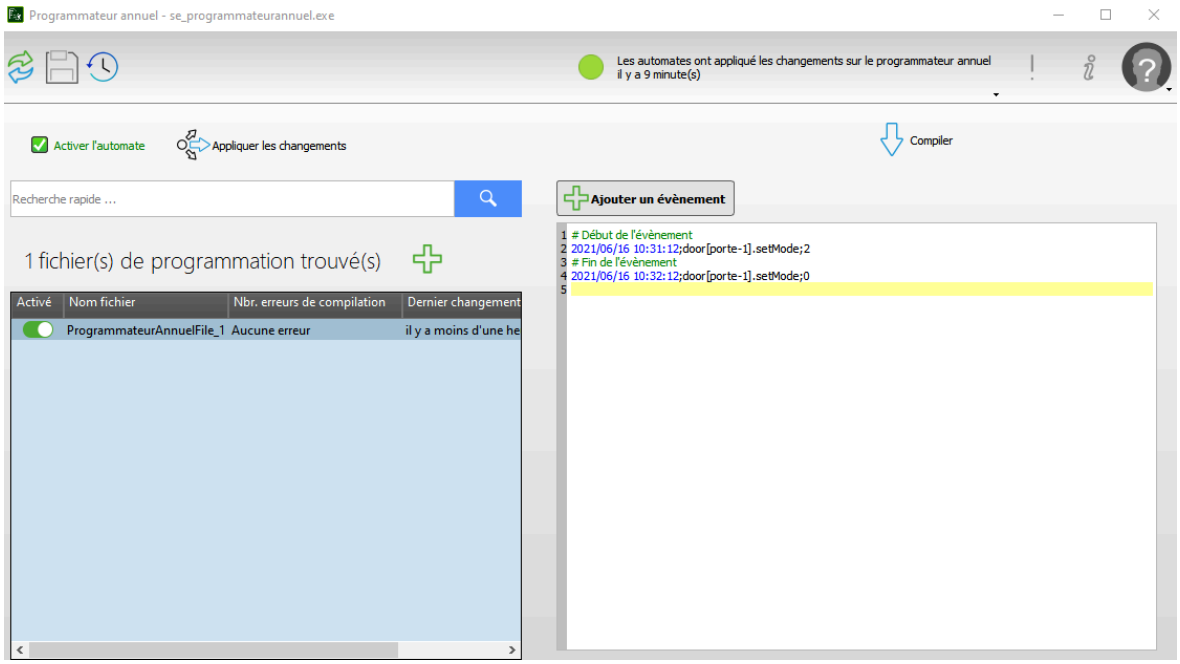
	État normal
	Alarme en cours acquittée
	Alarme en attente d'acquittement
	Propriété forcée
	Propriété forcée et en alarme non acquittée
	Propriété n'ayant pas reçu d'état
	Sans propriété
	Propriété **logique** à l'état 1 / Mono état récemment modifiée

Chapitre 6. Programmateur annuel

6.1. Présentation

Le programmateur annuel permet de paramétrer le changement de la valeur d'une propriété de type commande à une date et heure précise. L'évènement créé sera maintenu et répété annuellement.

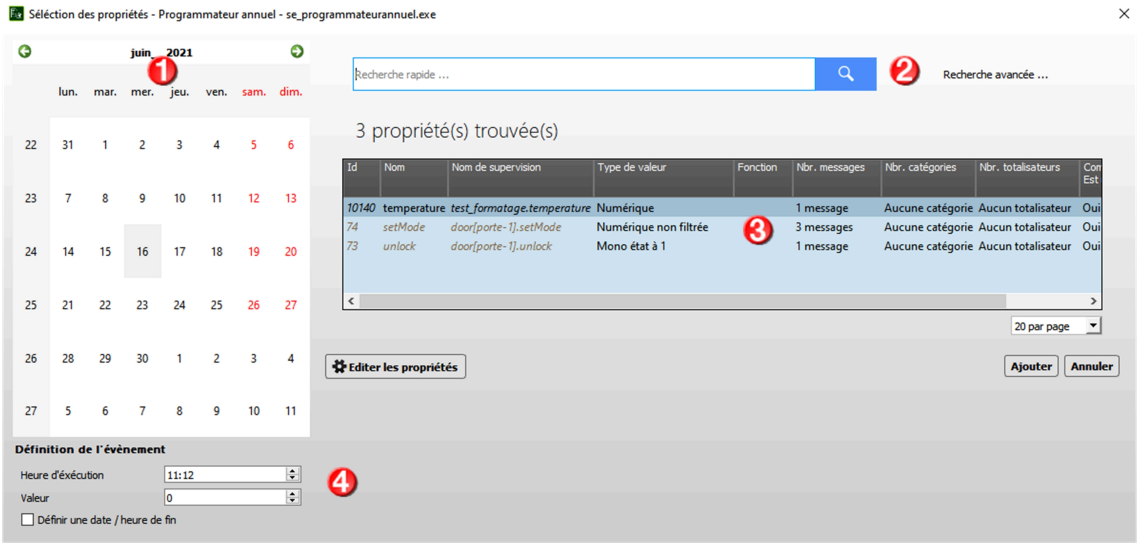
Un évènement créé sur une propriété d'état ou d'alarme n'aura aucun effet sur la valeur de celles-ci.



6.2. Paramétrage des évènements

Cliquer sur pour créer un nouveau fichier de programmation, le fichier peut être activé ou désactive avec la commande dédiée dans la partie gauche de la fenêtre.

Pour créer un évènement de changement de valeur d'une commande à une date et heure précise, Cliquer sur **Ajouter un évènement**.



1	Sélectionner la date dans le calendrier.
2	Rechercher la commande à modifer.
3	Sélectionner la commande à modifier
4	**Définir les éléments suivants:** • Heure d'éxecution • Valeur de la propriété après évènement Cliquer sur la case dédiée pour ajouter automatiquement une date de fin de l'évènement et paramétrer la valeur de la propriété.

Les évènements créés sont ajoutés sous la forme d'une ligne de commande dans la fichier de programmation. Il est cependant possible d'ajouter ou de modifier les évènements sans utiliser l'assistant de création. Le format de la ligne de commande est le suivant:

<DATE><HEURE>;<Télécommande>;<Valeur>

Arguments:

- **<DATE>**: AAAA/MM/JJ
- **<HEURE>**: HH:MM:SS
- **<Télécommande>**: Autocomplétion automatique
- **<Valeur>**: Renseigner un nombre cohérent avec le type de valeur de la télécommande (logique,numérique). Utiliser la fonction PULSE pour assigner temporairement une valeur à la télécommande.

Une ligne peut être définie comme **commentaire** en la faisant précéder du caractère #.

2022/12/23 12:00:00;NOM_PROPRIETE;1 => Passage à 1 de la propriété 'NOM_PROPRIETE' le 23/12/2022 à 12h

2022/12/* 12:00:00;NOM_PROPRIETE;1 => Passage à 1 de la propriété 'NOM_PROPRIETE' tous les jours du mois de décembre à 12h

2022/*/* 12:00:00;NOM_PROPRIETE;1 => Passage à 1 de la propriété 'NOM_PROPRIETE' tous les jours de l'année à 12h

2022/*/23 12:00:00;NOM_PROPRIETE;1 => Passage à 1 de la propriété 'NOM_PROPRIETE' tous les 23e jour du mois à 12h

Une fois le fichier de programmation configuré, effectuer les manipulations suivantes pour valider le paramétrage et activer la fonctionnalité:

1. Cliquer sur Activer l'automate.
2. Cliquer sur  .
3. Cliquer sur compiler.
4. Cliquer sur Appliquer les changements.

Chapitre 7. Main courante

7.1. Généralités

La fonctionnalité main courante permet de rassembler dans un ticket de suivi tous les évènements relatifs au déclenchement, traitement et acquittement d'une alarme quelle que soit sa nature (capteur intrusion, ouverture de porte inattendue...).

Les opérateurs autorisés pourront ajouter des notes et commentaires afin d'apporter du contexte aux actions effectuées ou aux évènements passés.

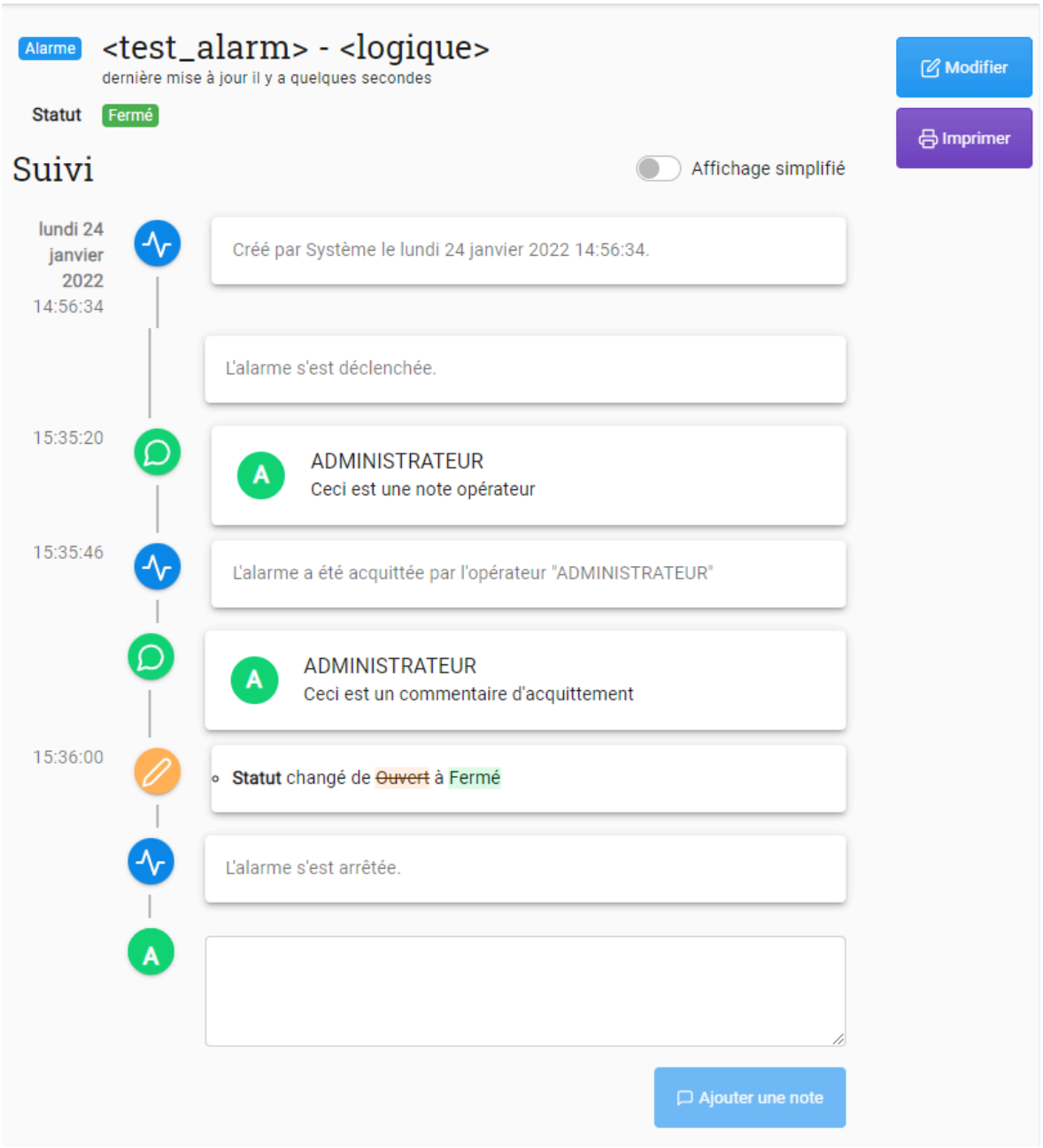
Le récapitulatif des évènements survenus pendant le traitement de l'alarme et répertoriés dans le suivi est en lecture seule uniquement. Il est impossible d'altérer l'heure, le type d'évènement ou l'identité de l'opérateur responsable de l'opération.

De manière identique, une fois qu'une note opérateur ou un commentaire d'acquittement a été ajoutée au ticket, il est impossible de la retirer ou de la modifier.

L'exploitation des tickets de main courante intervient à différents niveaux et dans différentes interfaces

- Ajout de commentaires à l'acquittement d'une alarme directement dans les applications de supervision (MICROSESAME ou WEBSESAME).
- Recherche des évènements systèmes liés à un ticket de main courante dans l'historique MICROSESAME.
- Accès et consultation d'un ticket de main courante à partir d'un évènement système lié depuis le moniteur d'évènement ou l'historique dans MICROSESAME.
- Accès et consultation de tous les tickets de main courante (ouverts et fermés) depuis un onglet dédié dans WEBSESAME

Figure 7.1. Consultation d'un ticket de main courante dans WEBSESAME



Un opérateur possédant les droits adaptés pourra rechercher et consulter les tickets de main courante:

Section	Détails
En-tête	• Nom du ticket (par défaut la description de supervision de la propriété) • Statut du ticket • Site

Suivi	• Suivi chronologique des évènements :
	  • Déclenchement
	  • Retour à l'état normal
	  • Acquittement
	  • Commentaires d'acquittement et notes opérateurs
	  Chaque évènement est répertorié avec sa date et heure d'exécution ainsi que l'opérateur responsable.

Actions	• Modifier le nom et la description du ticket • Imprimer le ticket • Ajouter une note opérateur  Les fonctionnalités disponibles dépendent de l'interface utilisée pour consulter le ticket.

7.2. Paramétrage

7.2.1. Droits opérateurs

L'exploitation des tickets de main courante nécessite de paramétrer des droits spécifiques aux opérateurs.

Exploitation	Droit associé
Dans MICROSESAME • Consulter le ticket de main courante associé à une alarme à partir des applications de supervision • Ajouter une note opérateur • Ajouter un commentaire lors de l'acquittement d'une alarme	**Acquitter une alarme**

Dans MICROSESAME
• Rechercher un évènement système lié à un ticket de main courante
• Consulter le ticket de main courante associé à une alarme à partir de l'historique
  • Ajouter une note opérateur
Dans WEBSESAME
• Visualiser l'ensemble des tickets de main courante et effectuer des recherches filtrées
• Consulter tous les tickets de main courante
  • Ajouter une note opérateur
  • Modifier le sujet ou la description du ticket
• Télécharger ou imprimer une liste filtrée des tickets de main courantes
• Imprimer un ticket de main courante
	Evènements techniques, Objets et propriétés de supervision

7.2.2. Commentaire d'acquittement

Le commentaire d'acquittement permet à l'opérateur responsable de cette opération de renseigner un commentaire directement dans l'interface de traitement des alarmes (Moniteur d'évènement ou animateur de synoptique). Ce commentaire sera intégré au ticket de main courante et lié à l'évènement d'acquittement.

L'intégrateur peut sélectionner le mode à mettre en place parmi les suivants :

- **Optionnel** : A l'acquittement d'une alarme, la fenêtre d'ajout de commentaire s'affiche automatiquement. L'opérateur peut décider de valider sans renseigner de commentaire.
- **Obligatoire** : A l'acquittement d'une alarme, la fenêtre d'ajout de commentaire s'affiche automatiquement. L'opérateur est obligé de renseigner un commentaire pour valider l'opération.
- **Désactivé** : A l'acquittement d'une alarme, la fenêtre d'ajout de commentaire est désactivée. L'alarme est directement acquittée.

7.3. Exploitation

7.3.1. Génération d'un ticket de main courante

Un ticket de main courante est automatiquement généré par le système au déclenchement d'une alarme acquittable.

L'opération de génération du ticket sera la première opération répertoriée dans le suivi chronologique.

Les alarmes mono-état sont obligatoirement acquittable et déclenchent alors obligatoirement l'ouverture d'un ticket de main courante.

7.3.2. Ajouter un commentaire d'acquittement

On considère le commentaire d'acquittement activé (optionnel ou obligatoire).

L'ajout d'un commentaire d'acquittement peut être paramétré depuis le paramétrage général, pour plus d'informations, voir *Section 7.2.2, « Commentaire d'acquittement »*.

Lors de l'acquittement d'une alarme depuis une interface de supervision,

1. Une fenêtre de saisie s'affiche automatiquement.
2. L'opérateur peut y renseigner tout commentaire associé à l'évènement puis valider.
3. Le commentaire est automatiquement ajouté au suivi du ticket de main courante.

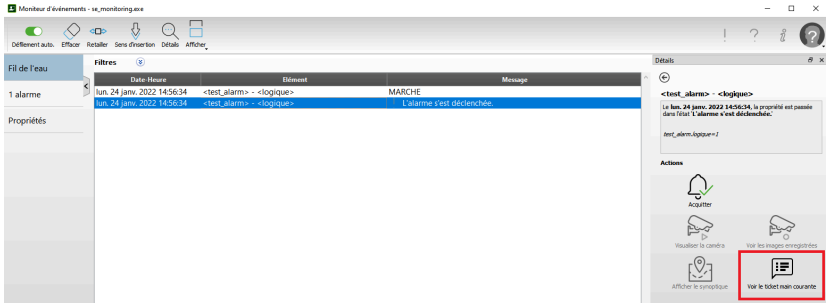
Si le mode de commentaire a été fixé sur **Optionnel**, l'opérateur peut valider sans renseigner de commentaire pour finaliser l'acquittement de l'alarme.

Une fois ajouté, un commentaire d'acquittement ne peut être modifié ou supprimé par personne.

7.3.3. Consulter un ticket de main courante

7.3.3.1. Moniteur d'évènement

Figure 7.2. L'opérateur peut consulter un ticket de main courante lié à une alarme directement dans le fil de l'eau



Au déclenchement d'une alarme :

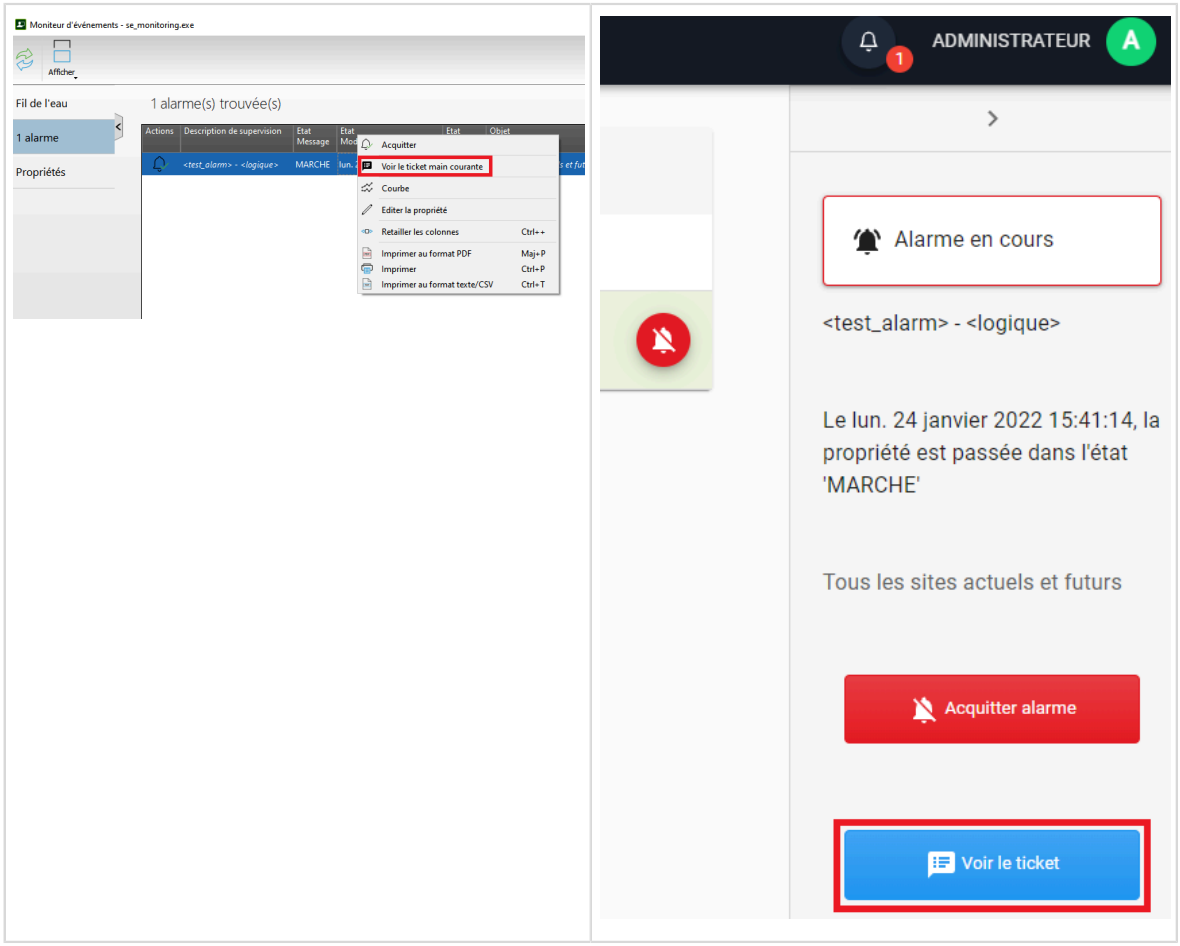
1. Cliquer sur l'onglet fil de l'eau.
2. Cliquer sur l'alarme en cours.
3. Dans la partie détails, sélectionner **Voir le ticket de main courante**.

Le ticket de main courante n'est pas accessible depuis l'onglet fil de l'eau dans WEBSESAME.

L'accès au ticket de main courante est possible tant que l'alarme n'a pas été complètement traitée, c'est à dire Acquittée et que la propriété en alarme soit de retour à son état de repos.

Une fois l'alarme traitée il est nécessaire de passer par l'application historique ou la liste des tickets dans WEBSESAME pour consulter le ticket de main courante associé.

Figure 7.3. L'opérateur peut consulter un ticket de main courante lié à une alarme dans l'onglet alarme



MICROSESAME	WEBSESAME
Au déclenchement d'une alarme : 1. Cliquer sur l'onglet alarme. 2. Cliquer sur l'alarme. 3. Dans le menu contextuel, sélectionner **Voir le ticket de main courante**.	**Au déclenchement d'une alarme :** 1. Cliquer sur l'onglet alarme. 2. Cliquer sur l'alarme en cours. 3. Dans le menu affiché dans la partie droite de la fenêtre, sélectionner **Voir le ticket de main courante**.

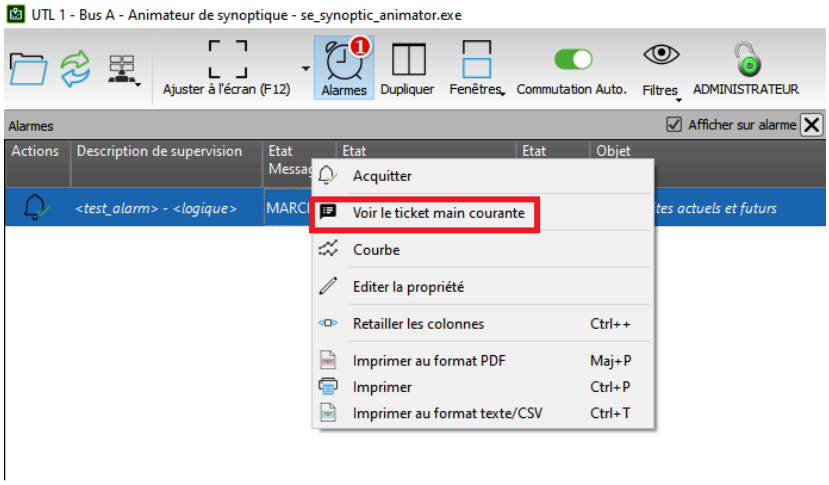
L'accès au ticket de main courante est possible tant que l'alarme n'a pas été complètement traitée, c'est à dire Acquittée et que la propriété en alarme soit de retour à son état de repos.

Une fois l'alarme traitée il est nécessaire de passer par l'application historique ou la liste des tickets dans WEBSESAME pour consulter le ticket de main courante associé.

7.3.3.2. Animateur de synoptique

L'onglet alarme de l'animateur de synoptique est identique à celui du moniteur d'évènement.

Figure 7.4. L'opérateur peut consulter un ticket de main courante lié à une alarme dans l'onglet alarme de l'animateur de synoptique



Au déclenchement d'une alarme :

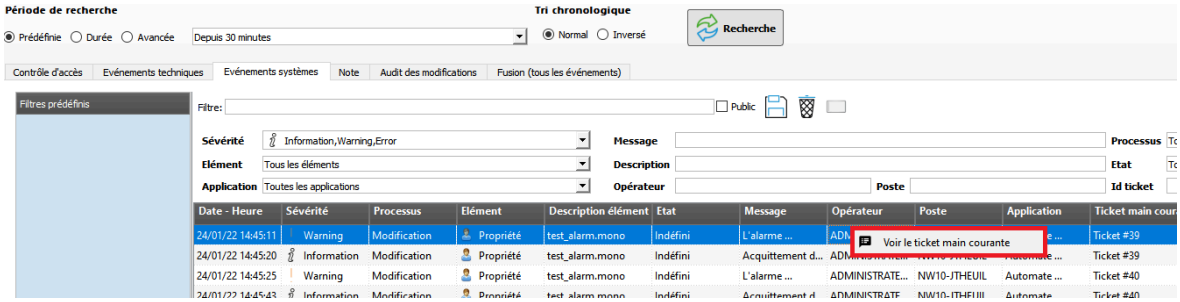
1. Cliquer sur l'onglet alarme.
2. Cliquer sur l'alarme.
3. Dans le menu contextuel, choisir **Voir le ticket de main courante**

L'accès au ticket de main courante est possible tant que l'alarme n'a pas été complètement traitée, c'est à dire Acquittée et que la propriété en alarme soit de retour à son état de repos.

Une fois l'alarme traitée il est nécessaire de passer par l'application historique ou la liste des tickets dans WEBSESAME pour consulter le ticket de main courante associé.

7.3.3.3. Application historique

Figure 7.5. L'opérateur peut consulter un ticket de main courante lié à un évènement depuis l'application historique

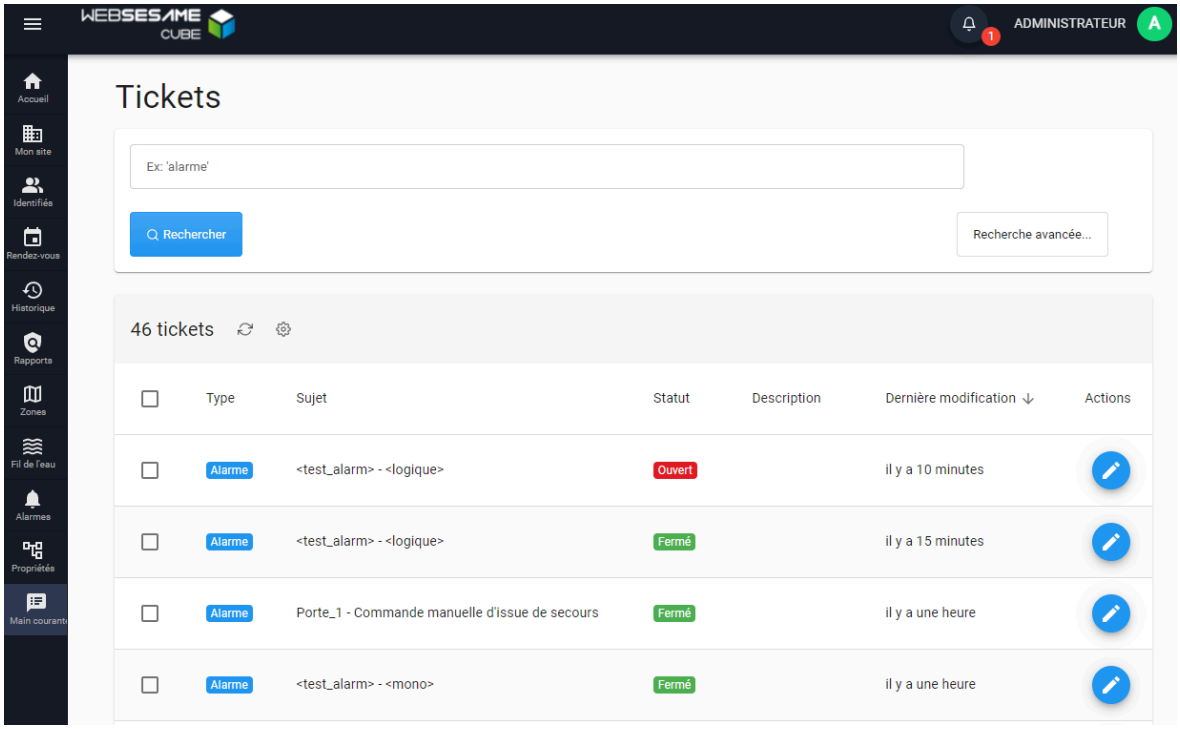


Pour retrouver un ticket associé à un évènement :

1. Se rendre dans l'onglet Évènements systèmes
2. Effectuer une recherche
3. Si l'évènement est lié à un ticket de main courante, le numéro du ticket est indiqué dans la colonne **Ticket main courante**.
4. Effectuer un clic-droit sur l'évènement souhaité
5. Sélectionner **Voir le ticket de main courante** dans le menu contextuel

7.3.3.4. Liste des tickets dans WEBSESAME

Figure 7.6. L'opérateur peut accéder à la liste de tous les tickets de main courante sur WEBSESAME



Cet onglet présente tous les tickets de main courante créés par le système (ouverts et fermés).

L'opérateur peut effectuer une recherche rapide pour retrouver un ticket grâce à son **nom** ou alors passer en mode recherche avancé et filtrer la liste des tickets grâce aux filtres suivants:

- Nom du ticket
- Description
- Id
- Statut
- Site

Pour consulter un ticket, cliquer sur la ligne associée.

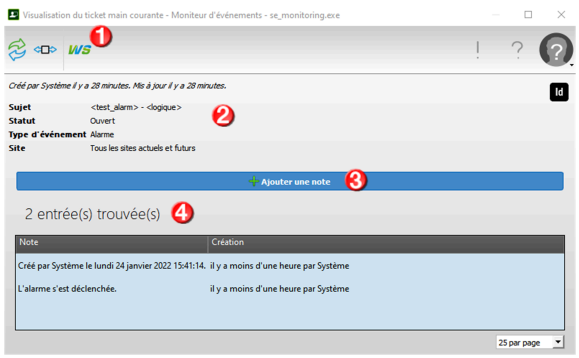
7.3.4. Suivre l'évolution d'un ticket de main courante

RAPPEL : Le récapitulatif des évènements survenus pendant le traitement de l'alarme et répertoriés dans le suivi est en lecture seule uniquement. Il est impossible d'altérer l'heure, le type d'évènement ou l'identité de l'opérateur responsable de l'opération.

Cette section est dédié à la compréhension du mécanisme de suivi implémenté avec MICROSESAME

Deux interfaces de suivi des tickets de mains courantes peuvent être utilisés par l'opérateur. L'une est accessible uniquement depuis WEBSESAME et l'autre uniquement depuis les applications de supervision MICROSESAME.

Pour plus d'informations sur les méthodes d'accès aux tickets de main courante, se référer à la section suivante :*Section 7.3.3, « Consulter un ticket de main courante »*.

MICROSESAME	WEBSESAME
	
❶ Accès à la visualisation du ticket sur WEBSESAME	❶En-tête
❷ En-tête	❷ **Actions sur le ticket:** • **Modifier** le nom et la description du ticket • **Imprimer** le ticket
❸ Ajouter une note opérateur	❸ Activer /Désactiver l'affichage simplifié
❹ Suivi chronologiques des évènements relatifs au traitement du ticket	❹ Suivi chronologiques des évènements relatifs au traitement du ticket
	❺ Ajouter une note opérateur

Certaines opérations ne sont disponibles que depuis l'interface WEBSESAME.

Tableau 7.1. Fonctionnalités de suivi

Fonctionnalité de suivi	
Statut du ticket	Le statut d'un ticket permet de visualiser d'un coup d'œil l'état de traitement d'une alarme. **Le ticket peut avoir différents états :** • Ouvert : Le traitement de l'alarme est toujours en cours • Fermé : Le traitement de l'alarme est terminé, l'alarme est acquitté et la propriété associée de retour à son état de repos  Lorsque le traitement d'une alarme est terminé, le statut de l'alarme passe automatiquement à **Fermé** et le ticket est archivé. Il n'est alors plus accessibles dans les applications de supervision.  Dans WEBSESAME, le statut de ticket peut être utilisé pour effectuer des recherches filtrées.
Evènements	**Les évènements répertoriés dans le suivi du ticket de main courante sont les suivants:** • Création du ticket par le système • Déclenchement de l'alarme • Arrêt de l'alarme • Acquittement de l'alarme • Commentaire d'acquittement • Note opérateur  Chaque évènement est rentré avec un marqueur temporel. Désactiver l'affichage simplifié pour observer le timestamp exact de l'exécution de l'évènement.
Note opérateur	Les opérateurs autorisés peuvent ajouter librement des notes opérateurs quelque soit le statut du ticket  Une fois ajouté une note opérateur ne peut être ni modifié ni supprimé par aucun opérateur.

Fonctionnalité de suivi	
Alarmes Mono-état	**Les tickets de mains courantes liés à des alarmes mono-état ont un traitement particulier :** • Le statut du ticket passe à l'état **Fermé** dés l'acquittement de l'alarme. • La remontée de l'évènement **Arrêt de l'alarme** n'est pas supportée.
Export et impression	• Dans la consultation d'un ticket sur WEBSESAME, un bouton dédié permet d'imprimer le ticket de main courante. • Dans l'onglet Main courante de WEBSESAME, les fonctionnalités d'export et d'impression sont disponibles pour générer une liste filtrées des tickets au format CSV, JSON ou pdf.

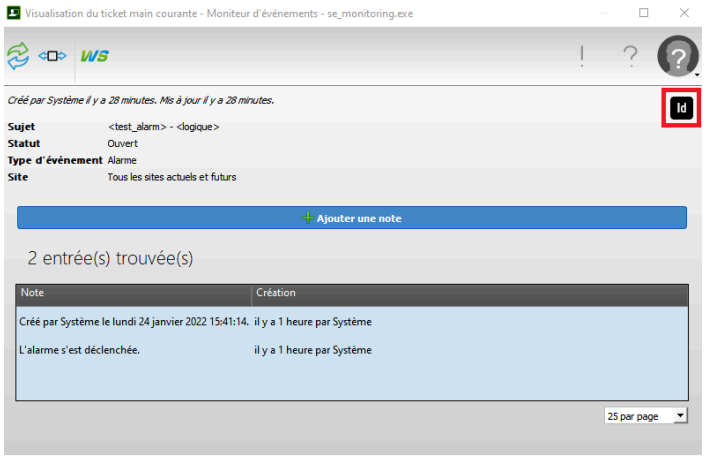
7.3.5. Retrouver les évènements systèmes liés à un ticket de main courante

Depuis le menu-principal MICROSESAME, Suivre Exploitation > Journaux > Historique :

1. Se rendre dans l'onglet **Évènements systèmes**
2. Dans le champ de filtrage **Id ticket**, renseigner l'identifiant unique lié au ticket de main courante
3. Tous les évènements systèmes liés au ticket sont affichés dans la table d'évènements

L'identifiant unique d'un ticket peut être retrouvé de plusieurs manières :

- Copier dans le presse-papier depuis un bouton dédié depuis la consultation du ticket dans MICROSEAME.



- Depuis la liste des tickets dans WEBSESAME en ajoutant la colonne ID à partir du bouton .
- Depuis la colonne Ticket main courante dans l'historique des évènements systèmes.

Chapitre 8. Contrôle d'accès

8.1. Gestion des identifiés

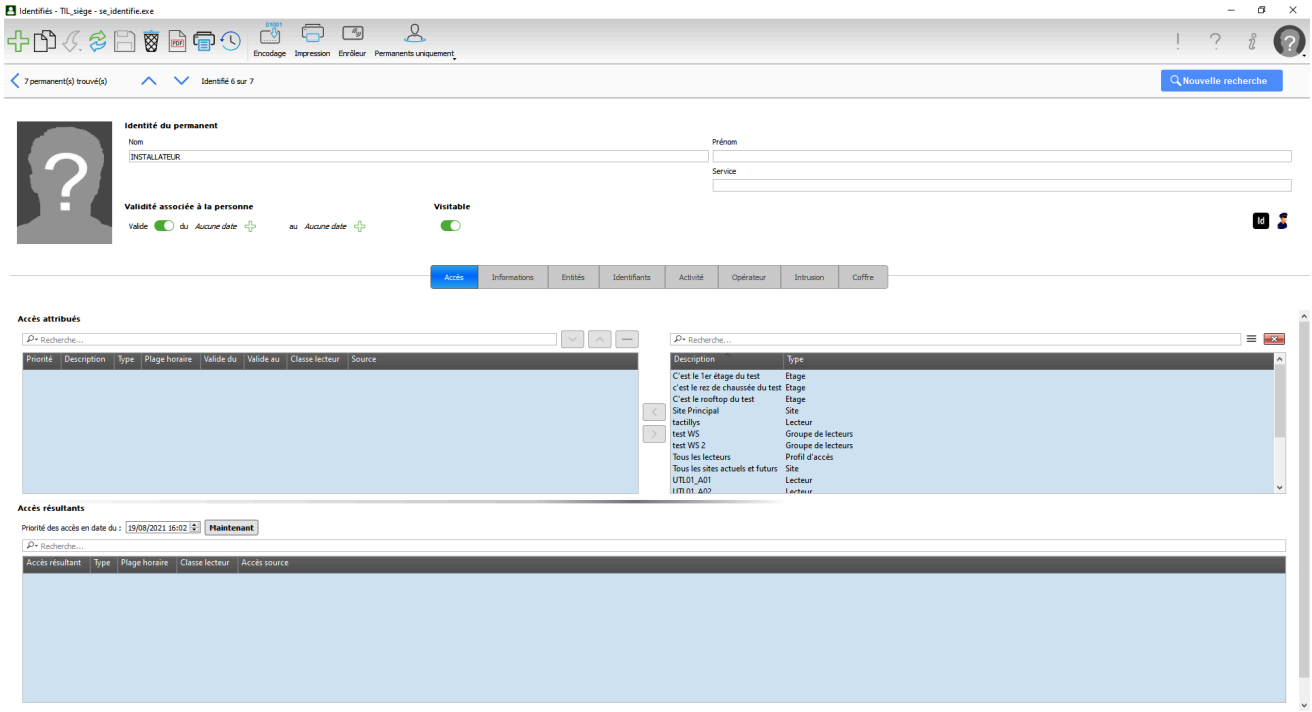
8.1.1. Généralités

Un identifié est la personne physique devant disposer d'un accès au site protégé par le système de contrôle d'accès. L'identifié est en général le porteur d'un ou plusieurs identifiants.

Dans MICROSESAME, plusieurs types d'identifiés existent :

- Les permanents sont des utilisateurs réguliers du système de contrôle d'accès.
- Les visiteurs sont des utilisateurs occasionnels du système de contrôle d'accès, avec une validité et des attributs (visites, collaborateurs externes, etc ...).

La gestion de ces derniers se fait dans la "Gestion des identifiés" : **Menu principal > Exploitation > Contrôle d'accès > Identifiés**.



8.1.2. Paramétrage de l'application de gestion des identifiés

L'interface de gestion des identifiés peut être personnalisée afin de s'adapter aux besoins du site.

Pour accéder au paramétrage de l'interface de gestion des identifiés, depuis le menu-principal, suivre **Paramétrage > Contrôle d'accès > Identifiés**.

Sélectionner le type d'identifié pour lequel le paramétrage sera effectué:

- Permanent

- Visiteur

Onglet Champs

Cet onglet permet d'ajouter ou de retirer des champs dans la fiche identifié, afin de personnaliser les informations relatives à l'identifié.

Critère	Détails
Type	• MS : Champ système pré-paramétré. • Champ libre : Champ dont le paramétrage est libre.
Nom	Libellé du champ
Visible	Lorsque cette case est cochée, le champ associé s'affiche dans la fiche identifié.
Modifiable	• Oui : Le champ peut être modifié (identifié créé localement ou importé par une passerelle). • Non : Le champ peut être modifié uniquement par une passerelle. • Seulement si créé par un opérateur : Le champ peut être modifié uniquement si l'identifié a été créé localement.
Mode	• Adresse e-mail • Liste dynamique • Liste statique courte • Liste statique longue • Texte libre
Obligatoire	Lorsque cette case est cochée, le champ associé doit être rempli pour sauvegarder l'identifié.
Doublons	• Autorisé : Plusieurs identifiés peuvent avoir la même valeur renseignée dans le champ associé. • Avertissement : Un avertissement est affiché si plusieurs identifiés ont la même valeur dans le champ associé. • Interdit : Une erreur est affichée si plusieurs identifiés ont la même valeur dans le champ associé. L'identifié ne pourra pas être sauvegardé.

Le champ **Statut Escorte** correspond à une fonctionnalité particulière et répond donc à un fonctionnel prédéfini, pour plus d'informations se référer à la section suivante : *Section 8.1.7, « Fiche identifié »*

Onglet Clé d'unicité

Cet onglet permet de créer une combinaison de champs pour lesquels les doublons seront interdits. La combinaison des champs ajoutés liés par un "et logique" définira la clé d'unicité.

Double-cliquez sur un champ pour l'ajouter à la liste.

Si les champs **NOM** , **PRENOM** ont été ajoutés à la liste, le système vérifiera les doublons sur la combinaison de ces deux valeurs.

Exemple:

- Jean Dupont - Jean Rousseau = OK
- Jean Dupont - Louis Dupont = OK
- Jean Dupont - Jean Dupont = KO

Si on ajoute le champ **SOCIETE** à la clé d'unicité précédente, la règle résultante sera la suivante :

"Il est interdit que deux identifiés portant le même nom ET prénom proviennent de la même société".

Onglet Matériel

Cet onglet permet :

- d'activer la saisie du code clavier par l'identifié via un second clavier
- de paramétrer un lecteur de documents (CNI, passeport) pour la saisie automatique des informations identifiés.

MICROSESAME supporte l'utilisation des lecteurs de documents suivants :

- GEMALTO AT9000
- RTE 670x, CR series

Il est nécessaire d'installer les pilotes spécifiques au matériel à utiliser. Les exécutables permettant d'installer ces pilotes sont livrés avec le matériel ou sont disponibles sur le site du constructeur.

Pour ces deux modèles supportés, il est conseillé d'**installer les pilotes avant de connecter le lecteur sur un port USB**.

La lecture d'informations à partir de documents d'identification remonte les informations suivantes :

- Nom
- Prénom
- Photo

Une fois le lecteur de document branché et la référence concernée sélectionnée dans la liste déroulante, la lecture d'informations peut être demandée depuis les applications suivantes :

- Gestion des identifiés
- Réception visiteurs

Onglet Durée de validité

Cet onglet permet de paramétrer la durée de validité par défaut des identifiés et des accès d'identifiés.

8.1.2.1. Activer la saisie du code clavier personnalisé par l'identifié via un second clavier

Cas d'usage : Un opérateur souhaite paramétrer MICROSESAME pour que les identifiés puissent saisir leur code personnalisé via un second clavier.

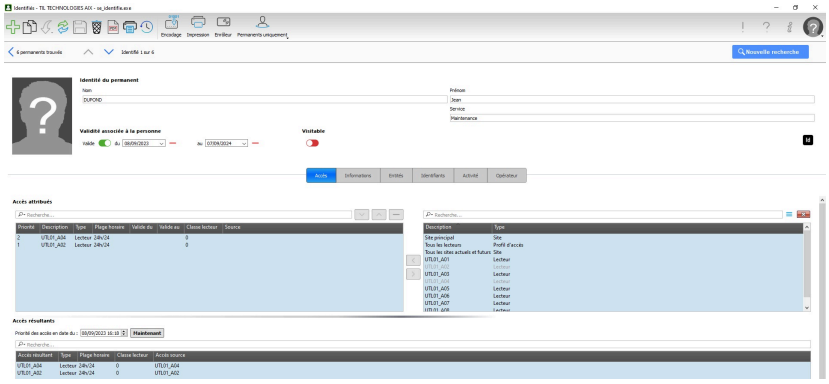
Pour activer la saisie du code clavier personnalisé par l'identifié via un second clavier

1. À partir du menu principal de MS, accédez à l'écran de paramétrage des **Identifiés** (**Paramétrage** > **Contrôle d'accès** > **Identifiés**).
2. Dans l'onglet **Champs**, paramétrez le champ **Code clavier personnalisé** comme *Visible* et *Modifiable*.
3. Dans l'onglet **Matériel**, cliquez sur le commutateur (rouge >vert) **Activer la saisie du code clavier personnalisé par l'identifié via un second clavier**.
4. Pour sauvegarder le paramétrage, cliquez sur .

Et après ?

- Exploitation dans MS dans l'écran Gestion des identifiés (onglet **Identifiants**) et dans l'écran **Réception visiteurs**.
- Exploitation dans WS dans la vue **Identifiés**

8.1.3. Créer un identifié

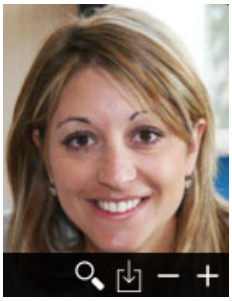


Dans le cas où le site ne dispose pas de passerelle d'alignement de la base de données du personnel, la création d'un nouvel identifié peut être réalisée par la méthode suivante :

1. Sélectionner le type d'identifié à ajouter (permanent ou visiteur).
2. Cliquer sur pour créer un nouvel identifié, renseigner son nom et prénom.
3. Dans l'onglet **Informations**, renseigner les données relatives à l'identifié puis lui assigner, si besoin, une période de validité. Les accès qui lui seront affectés seront désactivés hors de cette période.

4. Dans l'onglet **Entités**, si des *entités* ont été définies et si la saisie d'une entité est obligatoire par le paramétrage effectué dans MICROSESAME MS, sélectionnez l'entité à laquelle appartient l'identifié.
5. Pour ajouter une photo à l'identifié, cliquer sur "+" en bas à droite de l'emplacement réservé à la photo de l'identifié.
   L'ajout d'une photo peut être effectué de plusieurs manières :
   - Webcam connectée au poste, caméra IP ou enregistreur vidéo.
     Le bouton ... permet d'afficher la fenêtre de configuration de la webcam, si le pilote de cette dernière est installé.
     Le bouton permet de démarrer/arrêter la vidéo pour une webcam ou une caméra IP déjà configurée.
   - Fichier image (formats JPEG ou bitmap) déjà existant : Cliquer sur ce bouton pour importer une image au format JPEG (.jpg) ou bitmap (.bmp) déjà existante. Sélectionner un fichier compatible dans l'arborescence affichée.
   - Scanner connecté au poste : Cliquer sur ce bouton pour capturer l'image en provenance d'un scanner connecté au poste.

   Charger l'image, puis effectuer les réglages nécessaires jusqu'à l'obtention de la vue souhaitée. Lors du téléchargement d'une image, sa qualité sera testée pour assurer le rendu. Utiliser éventuellement les réglages de contraste et de luminosité pour obtenir un meilleur rendu. Le résultat est affiché en direct sur l'image.
   L'image chargée sera centrée automatiquement. La mire permet de sélectionner manuellement la partie de l'image à conserver. L'icône indique que le visage a été détecté et que la qualité de l'image est correcte (permet l'identification).
   Pour modifier une photo existante, utiliser les icônes en bas de l'image (vérification de l'image, téléchargement, suppression de l'image, changement de l'image).



6. Pour sauvegarder les modifications, cliquer sur **Enregistrer** dans la barre d'icônes principale.

L'identifié créé doit être défini comme valide par l'opérateur pour que ses accès soient fonctionnels.

Les champs présents dans la fiche identifié, ainsi que certaines fonctionnalités peuvent être personnalisées depuis le paramétrage de la gestion des identifiés. Certaines fonctionnalités ne sont pas actives par défaut.

Pour créer un identifié à partir des informations contenues dans un document d'identification (CNI, passeport) :

On considère le lecteur de document branché est configuré avec les drivers nécessaires.

1. Dans le **paramétrage général**, onglet **identifiés**, se rendre dans l'onglet **Lecteur de documents**.
2. S'assurer que le lecteur sélectionné correspond à la référence utilisée.
3. **Sélectionner le type d'identifié à ajouter:**
   - Permanent
   - Visiteur
4. Cliquer sur l'icône lecteur de document dans le **bandeau de sélection**.
5. Passer la pièce d'identité dans le lecteur de document.
6. Un nouvel identifié est automatiquement créé, les éléments suivants sont directement importés dans sa fiche identifié :
   - Nom
   - Prénom
   - Photo

Seules les pièces d'identités suivantes sont supportées:

- CNI (Carte Nationale d'Identité)
- Passeport

8.1.4. Importer un identifié

Il est possible d'importer manuellement un ou plusieurs identifiés, pour cela :

1. Dans la barre d'icônes principale de la fenêtre "Identifiés", cliquer sur l'icône pour importer un ou plusieurs identifiés.
2. Dans le sous-menu, sélectionner l'option **Importer des identifiés** pour procéder à l'import d'identifiés.

L'option **Télécharger un fichier d'exemple** permet de télécharger un modèle de fichier au format CSV avec les colonnes disponibles.
La première ligne du fichier CSV à importer, correspondant à l'en-tête du fichier (nom des colonnes), est ignorée lors de l'import.

3. La fenêtre "Ouvrir un fichier .CSV d'import des identifiés" s'ouvre. Naviguer vers le fichier CSV à importer contenant les données de l'identifié.
4. Une notification "Import terminé avec succès" s'affiche pour indiquer que l'opération s'est déroulée correctement.

Limitations d'import:

- Il est possible d'importer un identifiant par technologie de badge.
- Il est possible d'importer jusqu'à 5 "Accès par profil".
- Dans le fichier d'import, il est possible d'importer un maximum de 53 colonnes.

Colonne "Code action"

Type de code	Description de l'action
S	Suppression. Afin que la suppression se réalise correctement, il faut obligatoirement les mêmes valeurs sur les champs Nom, Prénom, Matricule et Service.
A	Ajout.
M	Modification d'un identifié existant ou ajout de l'identifié si ce dernier est absent en base de données.

8.1.5. Rechercher des identifiés

MICROSESAME propose deux possibilités de recherche des identifiés : un champ de recherche rapide et une fonction de recherche avancée permettant de trouver des identifiés à partir de critères spécifiques.

8.1.5.1. Recherche rapide d'un identifié

- Se rendre dans **Menu principal > Exploitation > Contrôle d'accès > Identifiés**: le champ de recherche rapide des identifiés permanents s'affiche par défaut.
- **Si la fenêtre de gestion des identifiés est déjà ouverte sur la fiche d'un identifié** : commencer à saisir le nom d'un identifié dans le champ *Rechercher un permanent ...* situé dans la partie supérieure gauche de la fenêtre. Au fur à mesure de la saisie du nom, le système peut proposer des identifiés (autocomplétion).
- **Si un enrôleur/encodeur est connecté et paramétré sur le poste** : cliquer sur l'icône **Enrôleur** et sélectionner l'enrôleur à utiliser dans la boîte de dialogue qui s'affiche. Passer le badge sur l'encodeur : l'identifié possesseur de ce badge est affiché.

Dans tous les cas, si la recherche concerne des visiteurs : cliquer sur l'icône **Permanents uniquement** dans la barre supérieure de la fenêtre, puis sélectionner l'option **Visiteurs uniquement**.

8.1.5.2. Recherche avancée

- Se rendre dans **Menu principal > Exploitation > Contrôle d'accès > Identifiés**, puis cliquer sur le bouton **Recherche avancée** dans la fenêtre qui s'ouvre.
- **Si la fenêtre de gestion des identifiés est déjà ouverte sur la fiche d'un identifié** : cliquer sur le bouton **Recherche avancée ...** dans la partie supérieure de la fiche.

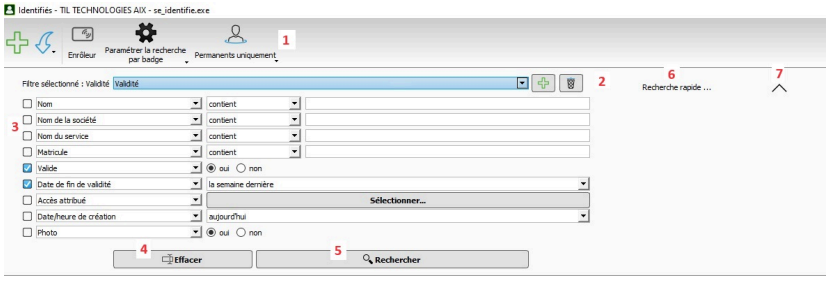


Tableau 8.1. Description de la fenêtre "Recherche avancée"

Repère	Détails
1	Icône de permutation entre identifiés permanents et identifiés visiteurs.
2	De gauche à droite : • Liste déroulante des filtres de recherche sauvegardés. • Sauvegarde d'un filtre paramétré. Lorsqu'au moins un filtre est présent dans la liste, cette icône est remplacée par le bouton . • Suppression d'un filtre sauvegardé.
3	Listes déroulantes des filtres pouvant être sélectionnés.
4	Bouton d'effacement des filtres configurés.
5	Bouton de recherche sur la base des filtres sélectionnés.
6	Bouton de retour à la recherche rapide d'un identifié.
7	Bouton permettant l'affichage ou pas des filtres (permet d'afficher plus de résultats).

Si la recherche concerne des visiteurs : cliquer sur l'icône **Permanents uniquement** dans la barre supérieure de la fenêtre, puis sélectionner l'option **Visiteurs uniquement**.

Deux méthodes de recherche sont possibles :

- **Utiliser la recherche sauvegardée** : dérouler la liste **Filtre sélectionné** située dans la partie supérieure de la fenêtre, dans laquelle chaque ligne correspond à un filtre qui a été déjà paramétré et sauvegardé.
- **Paramétrer un filtre spécifique** : utiliser les différentes listes déroulantes de filtres pour configurer un filtre spécifique.
  Les listes sont proposée par défaut, mais peuvent être modifiées à loisir, chaque liste comportant les mêmes filtres.
  Jusqu'à 9 filtres peuvent être cumulés pour affiner la recherche, en respectant la procédure décrite à la suite.

Procédure de paramétrage d'un filtre spécifique :

1. Cocher une case, puis sélectionner le critère à appliquer dans la liste déroulante associée.
2. En fonction du filtre choisi, la ligne se modifie et affiche :
   - Une liste déroulante comportant différentes possibilités de recherche (par exemple "Contient ou "Commence par") : choisir l'option désirée. Cette liste est éventuellement suivi d'un champ complémentaire : saisir le texte sur lequel la recherche va s'effectuer (par exemple tout ou partie du nom d'un identifié).
   - Des cellules de sélections (par exemple "Oui" ou "Non") : cliquer sur la cellule désirée.

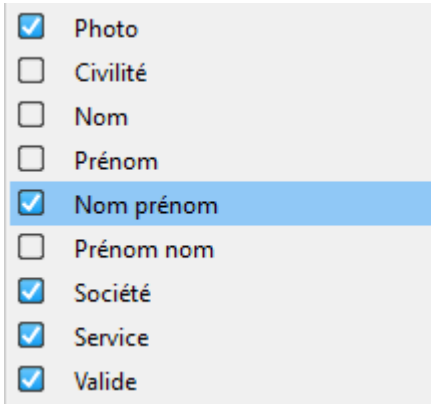
- Un bouton [Sélectionner] : cliquer dessus et effectuer les sélections désirées dans la boîte de dialogue qui s'affiche (par exemple un accès spécifique et/ou une plage horaire particulière), puis cliquer sur le bouton [OK].

3. Une fois le paramétrage effectué sur l'ensemble dles filtres voulus, cliquer sur le bouton **[Rechercher]** pour lancer la recherche.
4. **Si l'on souhaite sauvegarder ce filtre spécifique** : saisir un nom dans le champ **Filtre sélectionné**situé dans la partie supérieure de la fenêtre, puis cliquer sur le bouton **[Plus vert]** (ou le bouton **[Disquette]** si un ou plusieurs filtres sont déjà sauvegardés). Le filtre est alors incorporé à la liste déroulante.

Résultats de la recherche

Les résultats de recherche s'affichent dans un tableau :

Les colonnes peuvent être personnalisées en effectuant un clic-droit sur l'en-tête des colonnes, puis en cochant ou décochant les colonnes désirées.

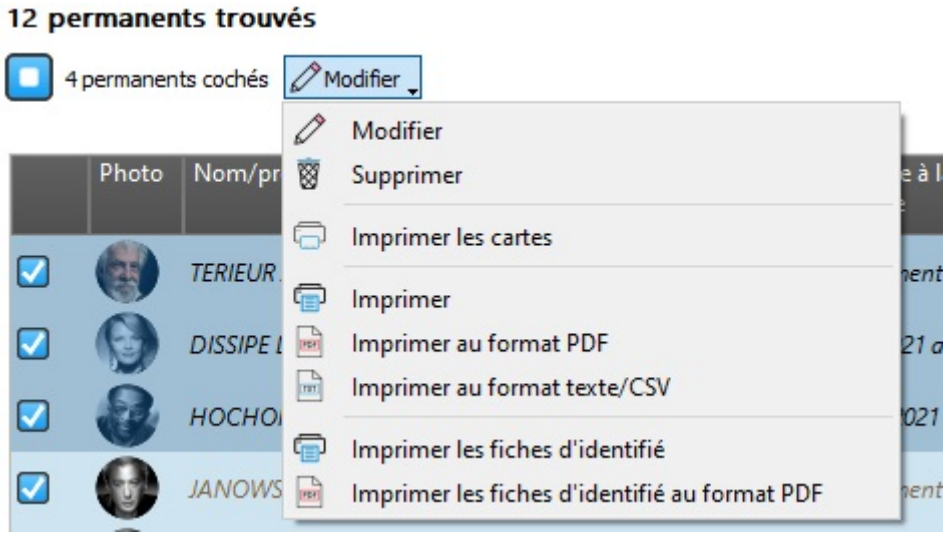


Ce menu contextuel permet aussi d'afficher toutes les colonnes simultanément ou de n'afficher que les colonnes proposées par défaut.

En fonction des droits donnés à l'opérateur, il est possible que les photos des identifiés ne s'affichent pas. La visualisation des photos des identifiés est rendue possible en activant le droit adéquat, dans le profil attribué à l'opérateur (rubrique **Identifiés** / option **Photo de profil identifié**).

Procédure pour imprimer une liste d'identifiés extraits d'une la recherche

1. Cocher les cases des identifiés désirés (s'aider éventuellement des touches [Ctrl] ou [MAJ]).
2. Cliquer sur le bouton **[Modifier]**, puis sélectionner l'option voulue dans la liste proposée, par exemple imprimer au format PDF la liste des identifiés ou l'enregistrer dans un fichier CSV.
3. Selon l'option choisie, une prévisualisation peut s'afficher à partir de laquelle l'impression pourra être lancée.



Les différentes options sont :

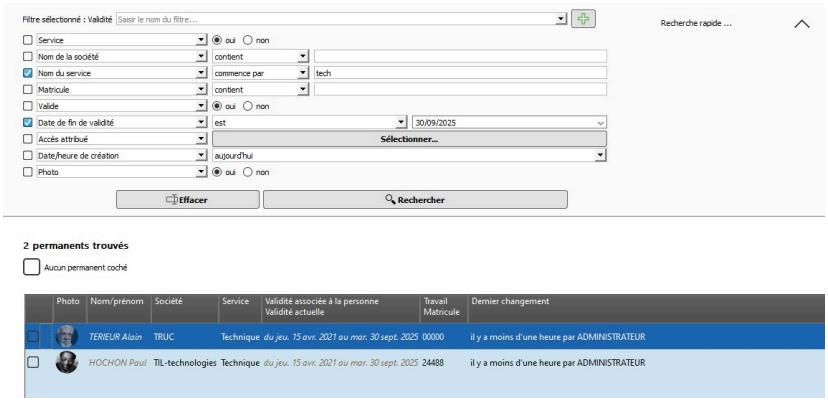
- **Modifier** : permet de modifier simultanément plusieurs identifiés (voir procédure décrite à la suite).
- **Supprimer** : supprime les identifiés sélectionnés.
- **Imprimer les cartes** : lance l'impression de badges pour les identifiés sélectionnés.
- **Imprimer**: ouvre une fenêtre d'aperçu de la liste des identifiés sélectionnés, dans laquelle il est possible de définir le format d'impression et lancer l'impression.
- **Imprimer au format PDF** : génère un fichier PDF avec la liste des identifiés sélectionnés.
- **Imprimer au format texte/CSV** : génère un fichier texte avec la liste des identifiés sélectionnés, utilisable dans un éditeur de texte, ou un fichier CSV utilisable dans Excel par exemple.
- **Imprimer les fiches identifiés** : ouvre une boîte de dialogue dans laquelle on peut définir les informations des identifiés à faire figurer. Cliquer sur le bouton [OK] ouvre une fenêtre d'aperçu avec les fiches identifié, dans laquelle il est possible de définir le format d'impression et lancer l'impression
- **Imprimer les fiches identifiés au format PDF** : génère un fichier PDF avec les fiches identifié.

8.1.5.3. Cas d'usage

On souhaite rechercher tous les identifiés du service technique pour lesquels la date de validité se termine au 30 septembre 2025.

Procédure de paramétrage du filtre :

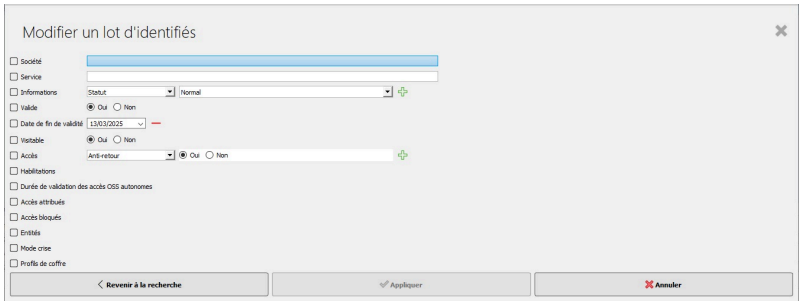
1. Cocher la case du filtre proposé par défaut **Nom du service**et dans la liste déroulante qui suit, sélectionner l'option "commence par". Taper ensuite "tech" dans le champ complémentaire.
2. Cocher la case du filtre proposé **Date de fin de validité**et dans la liste déroulante qui suit, sélectionner l'option "est". Définir la date désirée, dans le champ complémentaire, en utilisant le calendrier proposé (année, mois et date).
3. Cliquer sur le bouton **[Rechercher]** pour lancer la recherche.



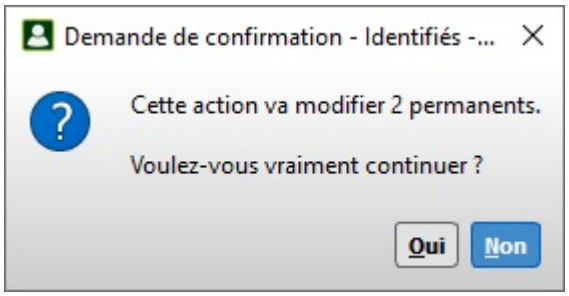
8.1.6. Modifications multiples

Pour effectuer des modifications multiples (modifier plusieurs identifiés en même temps), effectuer la procédure suivante :

1. Effectuer une recherche rapide ou une recherche avancée pour trouver les identifiés à modifier.
2. Cocher la case correspondant aux identifiés à modifier dans la liste des résultats.
3. Cliquer sur le bouton **Modifier** et dans liste qui s'affiche, sélectionner l'option **Modifier**. La fenêtre "Modifier un lot d'identifiés" s'affiche pour la configuration.



4. Paramétrer la ou les modifications à apporter à l'aide des différents champs.
   Le critère "Information" permet de sélectionner des champs supplémentaires à modifier. Cliquer sur le bouton **[Plus vert]** pour ajouter un champ supplémentaire.
5. Cliquer sur le bouton **[Appliquer]** : une boîte de dialogue s'ouvre, mentionnant le nombre d'identifiés impactés par les modifications et demandant une confirmation de l'action.



6. Confirmer en cliquant sur le bouton **[Oui]**.

8.1.7. Fiche identifié

En fonction des droits de l'opérateur, la fiche identifié peut permettre d'effectuer les actions suivantes :

- Visualiser et exploiter les informations relatives à un identifié.
- Gérer les accès, les identifiants et les entités d'appartenances de l'identifié.
- Gérer les profils de l'identifié (profils opérateur, profils intrusion, profils de coffres).

Les onglets et les informations présentes dans la fiche identifié dépendent des fonctionnalités mises en place avec MICROSESAME ainsi que du paramétrage effectué.

Cette section est une liste non-exhaustives des différentes fonctionnalités de cette interface:

Présentation	Procédure	Remarque
Désactiver un identifié	Décocher la case **Valide** pour désactiver tous les droits d'accès de l'identifié.	
Gérer les accès de l'identifié	Depuis l'onglet accès, cliquer sur et double-cliquer pour affecter ou retirer un accès.	Utiliser le simulateur d'accès résultant pour visualiser les impacts du paramétrage effectué.
Visualiser l'audit des modifications	Cliquer sur .	Il est possible d'exporter ou d'imprimer l'audit des modifications.
Dupliquer une fiche identifié	Cliquer sur .	
Exporter ou imprimer une fiche identifié	Cliquer sur ou .	
Encoder un badge	Cliquer sur pour sélectionner un format d'encodage et encoder un badge.	Il est possible d'encoder un badge avec des clés tirées d'une carte SAM directement depuis cette interface.
Imprimer un badge	Cliquer sur pour accéder à l'interface d'impression de badge personnalisé.	
Enregistrer des informations de l'identifié à l'aide d'un lecteur de document	Cliquer sur pour accéder au choix d'un lecteur optique ou d'un scanner.	Il est possible d'importer automatiquement des informations depuis un document du type carte d'identité ou passeport.

Présentation	Procédure	Remarque
Enrôler un identifiant pour un identifié	Cliquer sur pour activer la remontée d'identifiant sur passage du badge.	
Lancer la saisie du code clavier par l'identifié	Dans l'onglet Identifiants, renseigner un code clavier dans le champ correspondant.	
Envoyer à l'identifié un identifiant sous forme de QR code par mail	Dans l'onglet Identifiants, effectuer un clic-droit sur l'identifiant et sélectionner **Envoyer par mail**.	Pour plus d'informations sur l'envoi d'identifiants QR codes par mail, se référer à la section suivante ???
Ajouter une pièce jointe	Après avoir activé les pièces jointes, se rendre dans l'onglet correspondant, cliquer sur ajouter et sélectionner la pièce jointe à ajouter.	Pour activer cette fonctionnalité, se rendre dans le paramétrage des pièces jointes, cocher **Utiliser les pièces jointes** et sélectionner la taille maximum.
Mettre un identifié sur liste noire	Cocher la case **liste noire** pour pouvoir signaler un identifié.	La fonctionnalité liste noire permet de filtrer l'affichage des identifiés signalés en liste noire. Le fait qu'un identifié soit inscrit dans la liste noire n'implique pas de modification sur ses accès au site.
Définir un statut escorte ou accompagné pour un identifié	Ajouter le champ **Statut escorte** dans le paramétrage général des identifiés (permanent ou visiteur), puis sélectionner le statut souhaité dans la fiche identifié.	La mise en place d'une escorte (validation du passage de badge par un identifié escorte) nécessite un

Présentation	Procédure	Remarque
		paramétrage microcode. Pour plus d'informations se référer au guide MS_Cube_Accueil_gestion_vis ainsi qu'au chapitre dédié dans le guide microcode et programmation.

Tableau 8.2. Assigner des identifiants à l'identifié

L'interface permet d'assigner aux identifiés des identifiants réutilisables ou non, pour chaque technologie.

L'interface MICROSESAME supporte l'affectation d'identifiants pour les connecteurs suivants :

- Clés CLIQ
- Lecteurs offline
- Lecteurs online
- Armoires DEISTER
- Armoires TRAKA

Se référer à la section suivante pour plus d'informations : *Section 8.1.8.3, « Assigner des identifiants pour connecteurs spécifiques »*.

Suivre la procédure suivante pour assigner un identifiant à un identifié :

1. Se rendre dans la fiche de l'identifié à modifier
2. Se rendre dans l'onglet **Identifiants**
3. Localiser la technologie pour laquelle ajouter un identifiant
4. - Pour ajouter un nouvel identifiant : Effctuer un clic-droit dans la table et sélectionner **Créer un identifiant**, puis renseigner le code ainsi que les informations supplémentaires (références graphiques, dates de validité).
   - Pour ajouter un identifiant existant : Effectuer un clic-droit dans la table et sélectionner **Affecter un identifiant disponible**, puis sélectionner le ou les identifiants à ajouter dans la liste.
5. Enregistrer la fiche pour finaliser la procédure.

Tableau 8.3. Assigner des accès à l'identifié

L'interface permet d'affecter aux identifiés les types d'accès suivants :

- Lecteurs online classiques
- OSS offline (serrure et groupes de serrures)
- Aperio offline (serrure et groupes de serrures)
- KABA offline (serrure et groupes de serrures)
- Armoires TRAKA
- Armoires DEISTER (Keytags et groupes de keytags)
- Clés CLIQ (cylindres et groupes de cylindres)

Procédure pour affecter un accès à un identifié :

1. Se rendre dans la fiche de l'identifié à modifier.
2. Se rendre dans l'onglet**Accès**, puis dans la rubrique "Accès distribués", cliquer sur  situé à droite .
3. Double-cliquer sur un accès pour l'assigner : l'accès apparaît alors dans la colonne de gauche.
4. Pour chaque accès :
   - S'il s'agit d'un profil d'accès, valider éventuellement les **dates de validité** (par exemple : profil alloué que durant 2 mois pour un stagiaire).
     Pour définir une durée de validité particulière : cocher les case "à partir de " et "jusqu'au" et saisir les dates, puis cliquer sur le bouton OK.
   - Pour tous les autres types d'accès, valider la **plage horaire** désirée et éventuellement **les dates de validité**.
     Pour saisir une plage horaire : sélectionner la plage désirée dans la liste déroulante, puis cliquer sur le bouton OK..
     Pour définir une durée de validité particulière : cocher les case "à partir de " et "jusqu'au" et saisir les dates, puis cliquer sur le bouton OK.

   Il est possible de vérifier les lecteurs attribués (dans un groupe d'accès ou d'étages par exemple), en cliquant droit sur l'accès puis sur "Détails".
5. Cliquer sur  en haut de la fenêtre : les modifications sont enregistrées dans le système et un téléchargement dans les UTLs concernées par les accès est lancé automatiquement.

- Les accès CLIQ, DEISTER et TRAKA ne peuvent être assignés que sur la plage *24h/24*.
- Les accès Aperio offline ne peuvent être assignés que sur la plage *24h/24* ou *Toujours interdit*.
- Les accès OSS offline ne peuvent être assignés que sur les plages définies compatible OSS.
- Les accès Aperio offline, OSS Offline, CLIQ, TRAKA et DEISTER ne peuvent pas posséder de dates de validité.

Pour assigner des accès CLIQ ou TRAKA, il est nécessaire d'avoir configuré la fonctionnalité et activé l'automate associé au préalable.

Les accès aux connecteurs spécifiques ne sont pas affichés par défaut.

Effectuer un clic-droit puis afficher les accès ou groupes d'accès correspondants.

8.1.8. Fonctionnalités particulières

8.1.8.1. Paramétrage et prérequis pour l'envoi d'identifiant QR code par mail

Dans le menu principal MICROSESAME, suivre Paramétrage > Contrôle d'accès > Identifiants.

1. Se rendre dans la catégorie **Général**.
2. Définir la technologie dédiée à l'envoi d'identifiants QR codes par mails, puis l'activer.
3. Dans la colonne **Envoi par mail**, cocher la case pour activer la fonctionnalité.

Le fonctionnement de l'envoi par mail des identifiants sous forme de QR code dépend des éléments suivants :

- Visiteur créé et enregistré en base de donnée.
- Serveur mail paramétré pour MICROSESAME.
- Adresse mail renseignée pour le visiteur.
- Fonctionnalité activée dans le paramétrage des identifiants.

Pour personnaliser le **corps du mail** envoyé à l'identifié, suivre la procédure suivante:

Dans le menu principal MICROSESAME, suivre Paramétrage > Contrôle d'accès > Identifiants

1. Se rendre dans l'onglet **Personnalisation du mail**.
2. Personnaliser librement le sujet et le corps du mail envoyé à l'identifié.
3. Utiliser l'assistant de personnalisation  pour intégrer des variables :
   - Nom / Prénom identifié
   - Identifiant QR code
   - Code identifiant
   - Opérateur exécutant l'envoi du mail

Un identifiant peut être envoyé à un visiteur ou à un permanent depuis les interfaces suivantes:

- Gestion des identifiés MICROSESAME.
- Gestion des identifiés WEBSESAME.
- Application de réception des visiteurs dans MICROSESAME.

8.1.8.2. Fonctionnalité Escorte

Pour plus d'informations sur la mise en place de la fonctionnalité escorte, se référer à la section suivante de l'aide en ligne : Contrôle d'accès > Accueil de visiteurs et gestion de rendez-vous > Envoi d'identifiant QR code par mail.

8.1.8.3. Assigner des identifiants pour connecteurs spécifiques

MICROSESAME supporte nativement l'assignation d'identifiants pour les connecteurs suivants :

- Clés CLIQ
- Lecteurs OSS offline
- Armoires DEISTER
- Armoires TRAKA

Il existe cependant certaines spécificités ou restrictions selon le connecteur pour lequel ajouter un identifiant, se référer au tableau ci-dessous pour plus d'informations.

Tableau 8.4. Spécificités ou restrictions identifiants pour connecteurs spécifiques

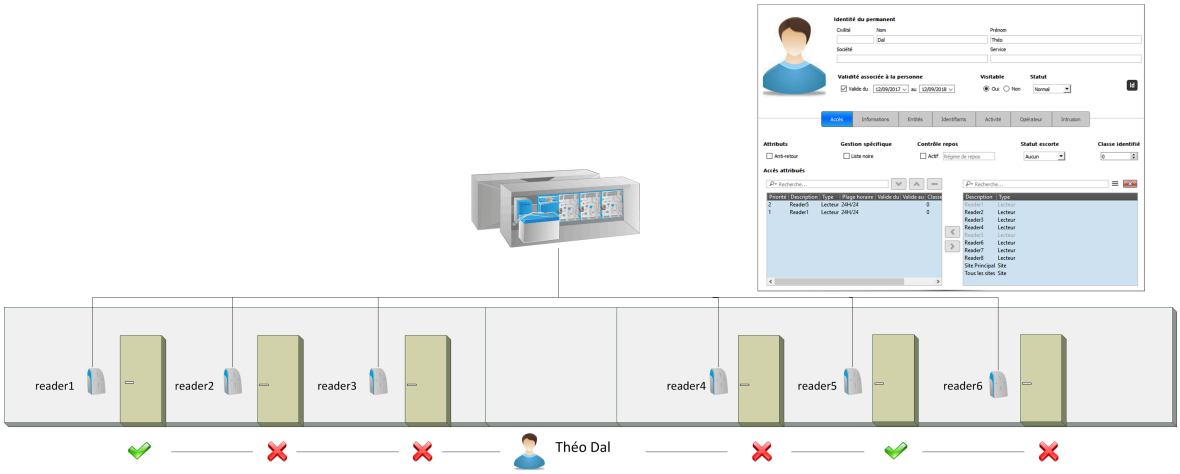
Connecteurs	Spécificités / restrictions	Remarques
CLIQ	• Identifiants importés automatiquement dans les identifiants réutilisables. • Uniquement en 24h24. • Pas de dates de validité.	Il est nécessaire d'avoir déclaré au préalable dans l'interface de paramétrage CLIQ la technologie à utiliser.
OSS Offline		Il est nécessaire d'avoir déclaré au préalable dans l'interface de paramétrage OSS la technologie à utiliser.
Armoires DEISTER		Il est nécessaire d'avoir déclaré au préalable dans l'interface de paramétrage DEISTER la technologie à utiliser.
Armoires TRAKA		Il est nécessaire d'avoir déclaré au préalable dans l'interface de paramétrage TRAKA la technologie à utiliser.

8.2. Gestion des lecteurs

8.2.1. Gestion des accès par lecteur

8.2.1.1. Description

Le lecteur est l'élément qui va lire et envoyer à l'UTL les identifiants qui lui seront présentés. Il est possible de brancher 8 lecteurs sur chaque bus de l'UTL. L'accès à un lecteur est généralement utilisé pour donner à un identifié l'accès à une salle ou un lieu spécifique.



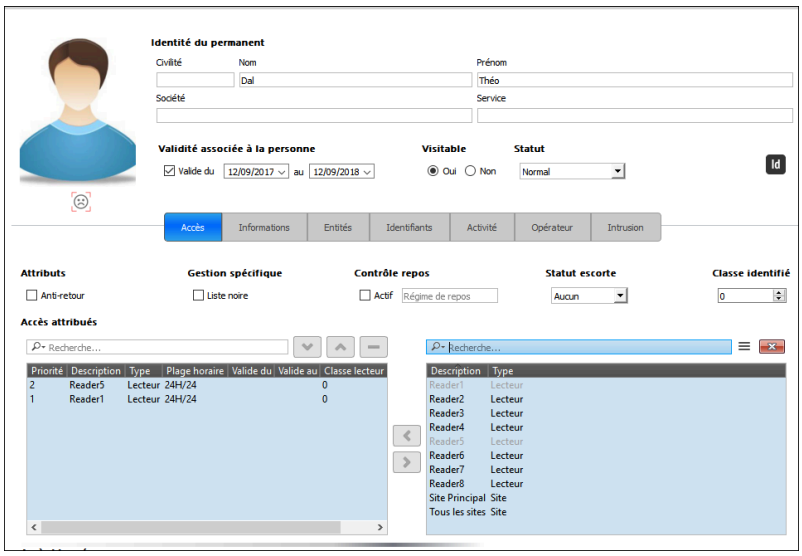
Afin de distribuer les accès méthodiquement aux identifiés, ce type d'accès est généralement intégré dans un "profil d'accès" ou un "groupe de lecteurs" (voir chapitre dédié pour plus d'informations)

8.2.1.2. Distribution des accès par lecteur

La distribution des accès se fait dans la fenêtre de gestion des identifiés : : *Menu MICROSESAME > Accès > Identifiés*.

Afin de pouvoir donner à un identifié l'accès à un lecteur spécifique, suivre les étapes suivantes :

1. Sélectionner un identifié, puis se placer dans l'onglet "accès"
2. Dans la section "Accès distribués" cliquer sur le bouton "+" pour faire apparaître les accès disponibles (items dans la liste de droite de l'image ci-dessous)



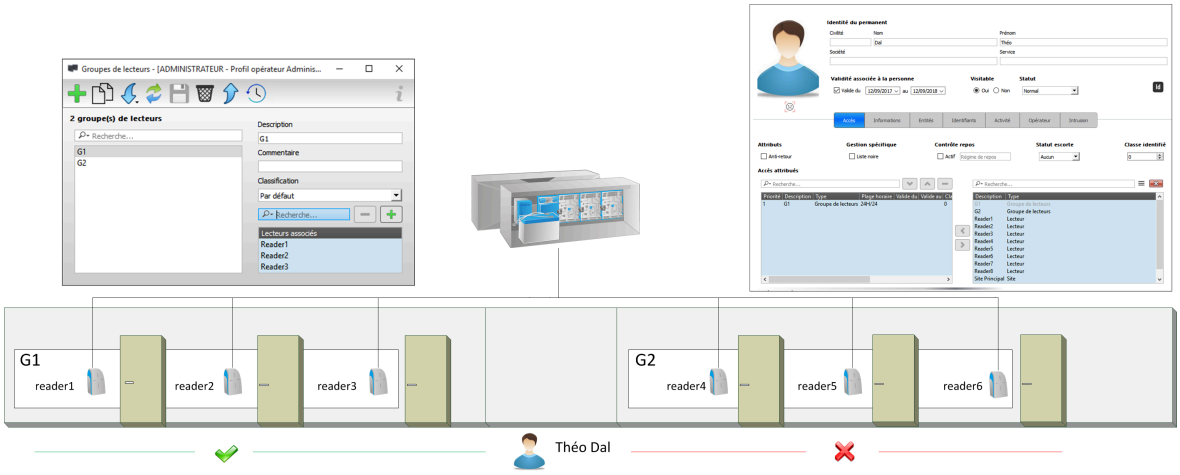
3. Sélectionner ensuite dans la liste des accès disponible les différents accès à distribuer à l'identifié puis cliquer sur le bouton "<"
4. Remplir la plage horaire sur laquelle l'identifié aura accès.
5. Remplir les dates de validités dans le cas où l'accès n'est pas permanent ou commence dans le futur
6. Dans le cas où la gestion des classes lecteurs est utilisé, compléter le numéro de la classe. Autrement laisser la valeur par défaut.
7. La priorité des accès la plus élevée est correspond au chiffre le plus élevé.
8. Confirmer en cliquant sur "OK".

1. Après chaque modification sur les accès d'un identifié, au moment de la sauvegarde, un téléchargement mise à jour des accès est automatiquement envoyé aux UTL concernées.
2. Il est possible de distribuer ou modifier des accès par lot. (voir chapitre "Gestion des accès d'un ou plusieurs identifiés")

8.2.2. Gestion des accès par groupe de lecteur

8.2.2.1. Description

Le groupe de lecteurs permet de réunir plusieurs lecteurs dans un même groupe afin de faciliter et de rendre plus méthodique la distribution des accès. Les lecteurs réunis dans un même groupe ont généralement un élément en commun : l'emplacement, un type de salle (réunion, bureau), ... Etc.



8.2.2.2. Distribution des accès groupe lecteurs

La distribution des accès se fait dans la fenêtre de gestion des identifiés : : *Menu MICROSESAME> Accès > Identifiés*.

Afin de pouvoir donner à un identifié l'accès à un groupe de lecteurs, suivre les étapes suivantes :

1. Sélectionner un identifié, puis se placer dans l'onglet "accès"
2. Dans la section "Accès distribués" cliquer sur le bouton "+" pour faire apparaître les accès disponibles
3. Sélectionner les accès concernés puis cliquer sur le bouton "<"

Les accès par groupe de lecteurs sont identifiables grâce à la valeur "Groupe de lecteurs" se trouvant dans la colonne type. Pour rechercher les accès plus aisément, il est possible de trier les accès par "Type". Pour cela, cliquer sur l'en-tête de la colonne "Type" du tableau.

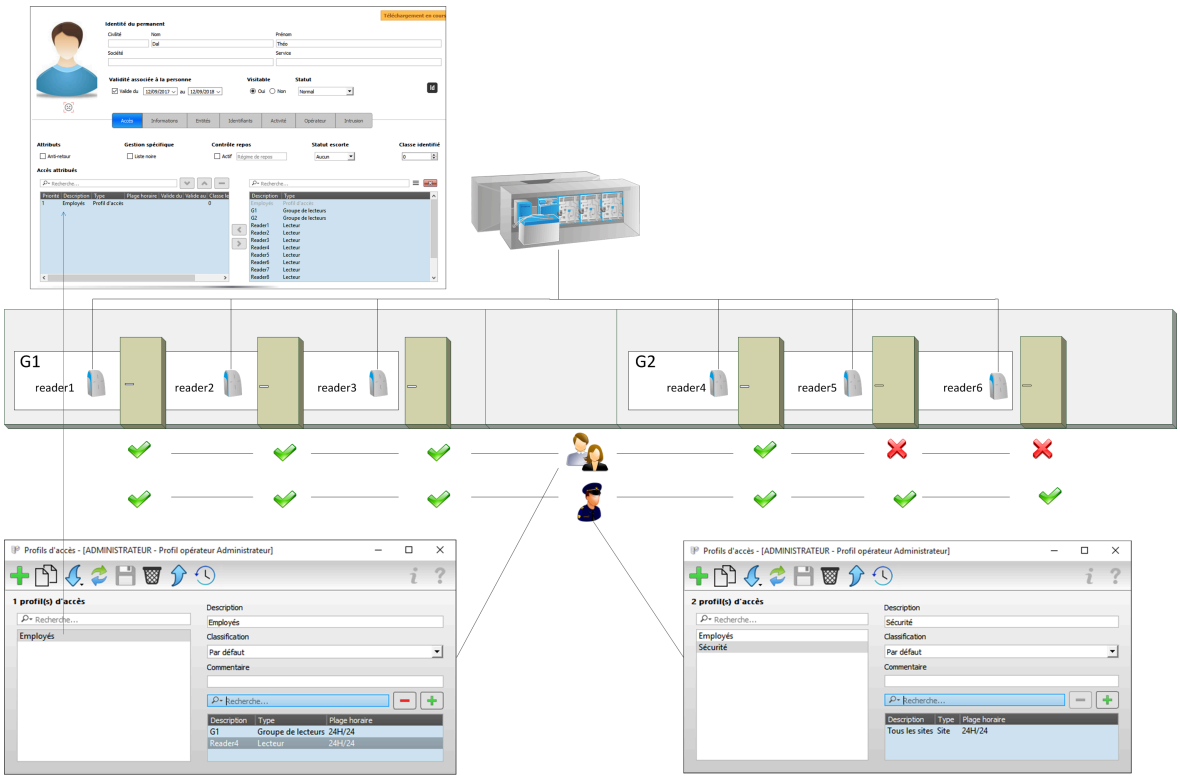
4. Sélectionner la plage horaire sur laquelle doit être appliqué l'accès
5. Paramétrer la validité si l'accès n'est pas permanent ou débute dans le futur
6. Sélectionner la classe lecteur si nécessaire, autrement laisser la valeur par défaut
7. La priorité des accès la plus élevée est correspond au chiffre le plus élevé.
8. Valider en cliquant sur le bouton "OK", puis sauvegarder

Un téléchargement mise à jour des accès est automatiquement effectué lors de la sauvegarde de l'identifié.

8.2.3. Profils d'accès

8.2.3.1. Description

Les profils d'accès permettent de redéfinir les accès pour une catégorie d'usagers de manière simple et intuitive. Le profil est composé d'une liste d'accès à des lecteurs, des groupes de lecteurs ou encore à des sites. Une plage horaire unique ou différente pour chacun de ces éléments complète le profil.



8.2.3.2. Création et paramétrage d'un profil d'accès

Afin de créer un profil d'accès:

1. Cliquer sur le bouton "+"
2. Remplir la description pour personnaliser le nom du profil
3. Cliquer sur le bouton "Ajouter des accès" pour faire apparaître la liste des accès disponible
4. Sélectionner les accès associés à ce profil puis cliquer sur le bouton "<" pour les ajouter
5. Sélectionner la plage horaire associée à l'accès ou aux accès et valider en cliquant sur "OK" .
6. Sauvegarder

Classification

La classification est une fonction qui permet de filtrer les accès à distribuer en fonction de l'opérateur connecté. C'est à dire que ce profil d'accès apparaîtra dans la liste des accès de l'opérateur connecté si et seulement si les droits de l'opérateur permet de voir la classification paramétrée dans ce champs.

Si cette fonction est utilisée, sélectionner la classification associée au profil d'accès

Pour utiliser cette fonction, les classifications doivent être préalablement paramétrées dans l'onglet **Classification** du paramétrage général de MICROSESAME. Pour plus d'informations, se référer à la documentation suivante:

MS_Cube_aide

Partie 3: **Exploitation**

Chapitre 2: **Opérateurs**

Section 4: **Classification des accès**

8.2.3.3. Création et paramétrage d'un profil d'accès

Afin de créer un profil d'accès:

1. Cliquer sur le bouton "+"
2. Remplir la description pour personnaliser le nom du profil
3. Cliquer sur le bouton "Ajouter des accès" pour faire apparaître la liste des accès disponible
4. Sélectionner les accès associés à ce profil puis cliquer sur le bouton "<" pour les ajouter
5. Sélectionner la plage horaire associée à l'accès ou aux accès et valider en cliquant sur "OK" .
6. Sauvegarder

Classification

La classification est une fonction qui permet de filtrer les accès à distribuer en fonction de l'opérateur connecté. C'est à dire que ce profil d'accès apparaîtra dans la liste des accès de l'opérateur connecté si et seulement si les droits de l'opérateur permet de voir la classification paramétrée dans ce champs.

Si cette fonction est utilisée, sélectionner la classification associée au profil d'accès

Pour utiliser cette fonction, les classifications doivent être préalablement paramétrées dans l'onglet **Classification** du paramétrage général de MICROSESAME Pour plus d'informations, se référer à la documentation suivante:

MS_Cube_aide

Partie 3: **Exploitation**

Chapitre 2: **Opérateurs**

Section 4: **Classification des accès**

8.2.3.4. Import de profils d'accès

Il est possible d'importer des listes de profils d'accès à partir d'un fichier CSV.

Le fichier d'import doit être constitué de la manière suivante:

- Une ligne d'en-tête indiquant les données importées.
- X lignes de donnée(s)

Un fichier avec l'en-tête paramétrée correctement peut être téléchargée: *bouton "Importer" > Sélectionner "Télécharger un fichier d'exemple".*

Les données pouvant être importées sont les suivantes :

- Code action ([A]jout, [M]odification ou [S]uppression)
- Description Profil d'accès
- Type (L/G/E/GE)
  avec L = Lecteur; G = Groupe de lecteur; E = Étage; GE = Groupe d'étages
- Constructeur -> Les valeurs de cette colonne peuvent être: Centralisé, APERIO autonome. Si cette colonne n'est pas présente, tous les accès sont considérés comme centralisés
- Nom lecteur/groupe/étage
- Plage horaire
- Mode Office
- Classification
- Commentaire

Les accès et les plages horaires présents dans la liste doivent être d'abord créés dans MICROSESAM

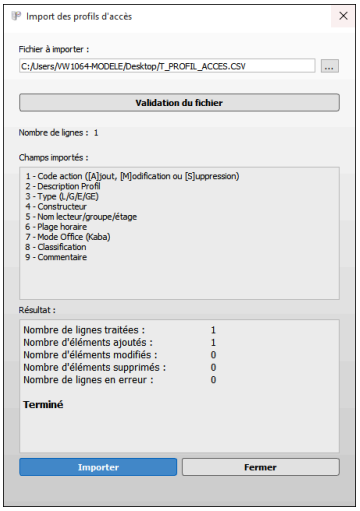
Exemple:

Figure 8.1. Données d'un fichier d'import: ajout d'un profil "Employé" avec les lecteurs "L1", "L2", "L3" en plage horaire "24H/24"

```
1  Code action;Description Profil;Type (L/G/E/GE);Nom lecteur/groupe/étage;Plage Horaire
2  A;Employé;L;L1;24H/24
3  A;Employé;L;L2;24H/24
4  A;Employé;L;L3;24H/24
```

Afin d'importer le fichier CSV:

1. Cliquer sur le bouton "Importer" puis "importer un fichier de profils" ou utiliser le raccourci "Ctrl + i"
2. Sélectionner le fichier format CSV à importer puis cliquer sur le bouton "validation du fichier"
3. Après une vérification des champs détectés dans le fichier, cliquer sur "Importer"



8.2.3.5. Export des profils d'accès

Il est possible d'exporter les profils d'accès dans un fichier .CSV:

1. Cliquer sur le bouton "Exporter" dans la barre des boutons
2. Sélectionner l'emplacement du dossier et indiquer le nom du fichier
3. Cliquer sur le bouton "exporter"

8.2.3.6. Distribution des accès par profil d'accès

La distribution des accès se fait dans la fenêtre de gestion des identifiés : : *Menu MICROSESAME > Accès > Identifiés*.

Afin de pouvoir donner à un identifié l'accès à un profil d'accès, suivre les étapes suivantes :

1. Sélectionner un identifié, puis se placer dans l'onglet "accès"
2. Dans la section "Accès distribués", cliquer sur le bouton "+" pour faire apparaître les accès disponibles
3. Sélectionner les accès concernés puis cliquer sur le bouton "<"

Les accès par profil d'accès sont identifiables grâce à la valeur "Profil d'accès" se trouvant dans la colonne type. Pour rechercher les accès plus aisément, il est possible :

a. De trier les accès par "Type" en cliquant sur l'en-tête de la colonne "Type" du tableau.
b. De filtrer les accès en tapant le type ou le nom de l'accès dans la barre de recherche se trouvant au-dessus de la liste
c. D'afficher seulement les profils d'accès en effectuant un clic droit dans le tableau et en dé-sélectionnant les autres types d'accès

4. Paramétrer la validité si l'accès n'est pas permanent ou débute dans le futur
5. Sélectionner la classe lecteur si nécessaire, autrement laisser la valeur par défaut
6. La priorité des accès la plus élevée est correspond au chiffre le plus élevé.
7. Valider en cliquant sur le bouton "OK", puis sauvegarder

Un téléchargement mise à jour des accès est automatiquement effectué lors de la sauvegarde de l'identifié.

8.2.3.7. Cas d'étude

Dans ce cas d'étude il sera décrit la création et le paramétrage de deux profils d'accès ainsi que la distribution de ces profils d'accès à deux identifiés existants.

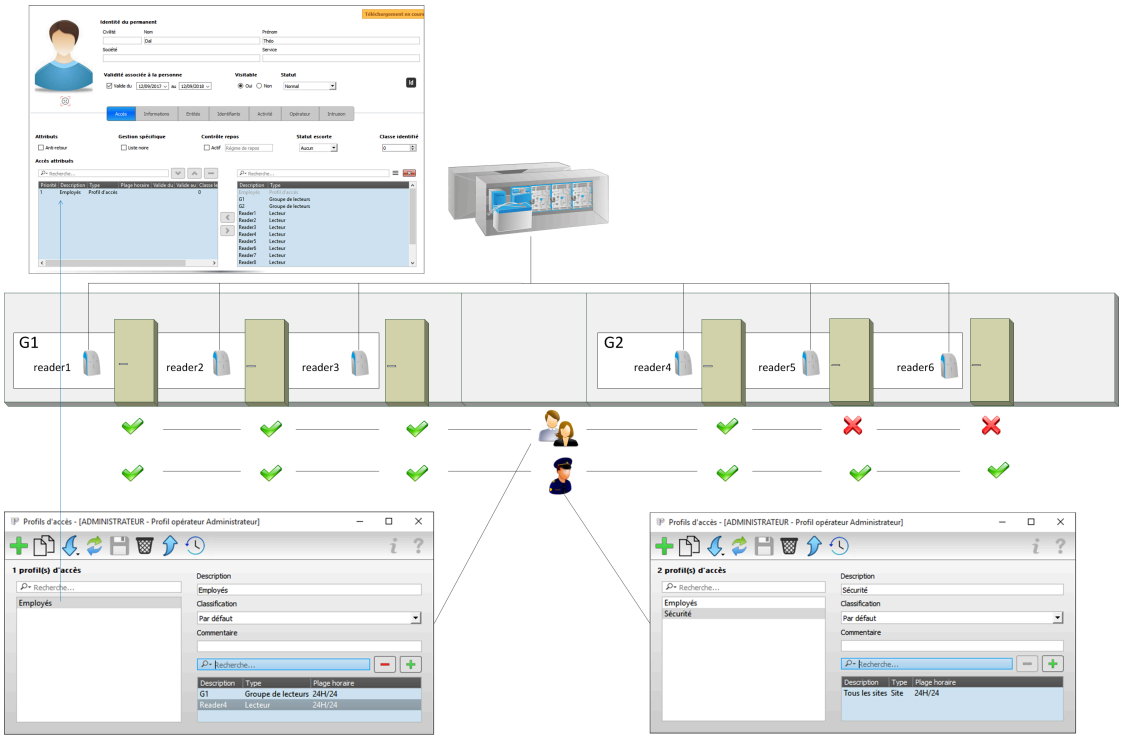
Les deux profils d'accès sont les suivants :

- Sécurité : profil disposant de l'accès à tous les lecteurs du site sur une plage horaire 24h/24.
- Employés : profil disposant de l'accès aux lecteurs se trouvant dans le groupe de lecteurs "G1" ainsi qu'au lecteur "Reader4" sur une plage horaire 24h/24.

Ci-dessous les identifiés qui seront paramétrés :

- Théo Dal : identifié qui sera associé au profil "Sécurité"
- Lynda Gus: identifié qui sera associée au profil "Employés"

La création des lecteurs et des groupes de lecteurs ne seront pas décrit dans ce cas d'étude, pour plus d'informations voir les chapitres dédiés dans ce guide.



Création des profils d'accès

Ouvrir la fenêtre de gestion des profils d'accès : *Menu MICROSESAME > Accès > Profils d'accès*.

Créer le profil "Sécurité : *Bouton "+" > Entrer "Sécurité" dans le champ "Description" > Ouvrir la liste des accès disponible > Donner accès à "Tous les sites" sur la plage horaire "24h/24" (équivalent à passe-partout) > Sauvegarder le paramétrage*.

Créer le profil "Employés" : *Bouton "+" > Entrer "Employés" dans le champ "Description" > Ouvrir la liste des accès disponibles > Donner accès au groupe de lecteur "G1" et au lecteur "Reader4" sur la plage horaire "24h/24" > Sauvegarder le paramétrage*.

Distribution des profils d'accès aux identifiés

C'est dans la fenêtre de gestion des identifiés que va être distribué les accès aux identifiés concernés: *Menu MICROSESAME > Accès > Identifiés*.

Distribution du profil d'accès "Sécurité"

Sélectionner l'identifié concerné, dans ce cas d'étude "Théo Dal". Dans la liste des "accès attribués" de l'onglet "Accès", ajouter l'accès au profil d'accès "Sécurité" : *cliquer sur le bouton "+" de la section "Accès attribué > Sélectionner le profil d'accès "Sécurité" > Cliquer sur le bouton "<" puis valider en cliquant sur "OK"*. En donnant l'accès à ce profil, l'identifié aura donc accès à tous les lecteurs existants

Distribution du profil d'accès "Employés"

Sélectionner l'identifié concerné, dans ce cas d'étude "Lynda Gus". Dans la liste des "accès attribués" de l'onglet "Accès", ajouter l'accès au profil d'accès "Employés" : *cliquer sur le bouton "+" de la section "Accès attribué > Sélectionner le profil d'accès "Employés" > Cliquer sur le bouton "<" puis valider en cliquant sur "OK".* En donnant l'accès à ce profil, l'identifié aura donc accès à tous les lecteurs du groupe 1 et au lecteur se nommant "Reader4"

Téléchargement de l'UTL

Afin que tout le paramétrage effectué soit pris en compte dans l'UTL, il est nécessaire d'effectuer un téléchargement complet :

- Ouvrir la fenêtre de téléchargement : *Menu MICROSESAME> Paramétrage > Section "Mise à jour" > "Télécharger"*
- Dans l'onglet Télécharger", sélectionner le module concerné et "Toutes les données"
- Cliquer sur "Télécharger"

Dans le cas où le paramétrage a déjà été téléchargé et que seulement les accès ont été modifiés, il n'est pas nécessaire d'effectuer un téléchargement de l'UTL. La sauvegarde dans la fenêtre de gestion des identifiés effectue automatiquement une mise à jour des accès dans les UTL concernées.

8.2.3.8. Distribution des accès par lot

Ouvrir la recherche avancée, rechercher et sélectionner/cocher les identifiés concernés puis :

- Si les identifiés ont été sélectionnés : *Clic droit > Modifier*; si les identifiés ont été cochés : *Déplier le menu en cliquer sur le bouton "Modifier" au dessus du tableau > "Modifier".*
- Cocher la case "Accès distribués"
- Choisir si les accès actuels doivent être gardé ou supprimés
- Sélectionner les accès à distribuer à l'identifié puis cliquer sur le bouton "<" permettant d'ajouter l'accès sélectionné
- Sélectionner la plage horaire
- Remplir les dates de validités dans le cas où l'accès n'est pas permanent ou commence dans le futur
- Dans le cas où la gestion des classes lecteurs est utilisé, compléter le numéro de la classe. Autrement laisser la valeur par défaut
- Cliquer sur "OK" et "Appliquer"

8.2.3.9. Accès résultants : Simulation des accès

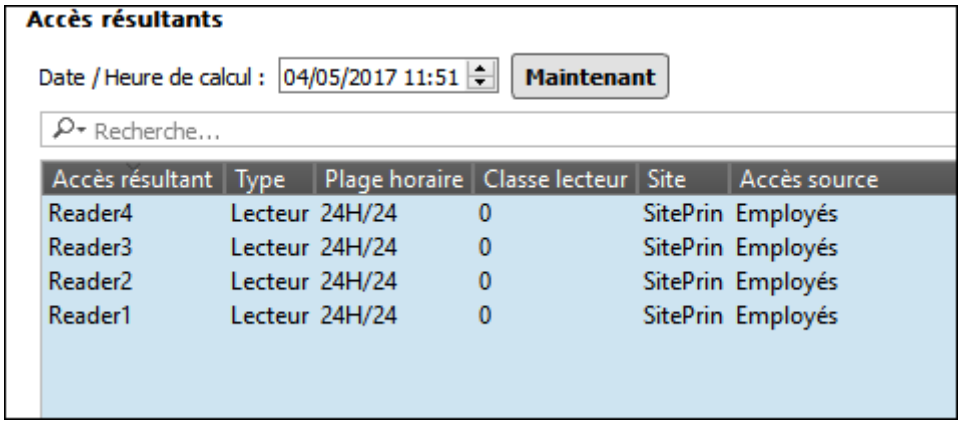
Pour chaque identifié, il est possible de visualiser tous les lecteurs auxquels l'identifié à accès à une date et heure précise. Pour cela :

- Ouvrir la fiche de l'identifié concerné
- Se placer dans l'onglet "Accès"
- Dans la section "accès résultants" inscrire la date et heure à laquelle vous voulez calculer les accès

Il apparaît dans la liste tous les lecteurs auxquels l'identifié à accès, l'accès source (Nom du profil si l'accès au lecteur vient d'un profil, Nom du groupe si l'accès au lecteur vient

d'un groupe), la classe lecteur ainsi que la plage horaire de l'accès. Les accès résultants permettent d'identifier des possibles conflits de priorités sur les accès d'un même lecteur.

Figure 8.2. Exemple d'accès résultants dont l'accès source est un profil d'accès se nommant "Employés"

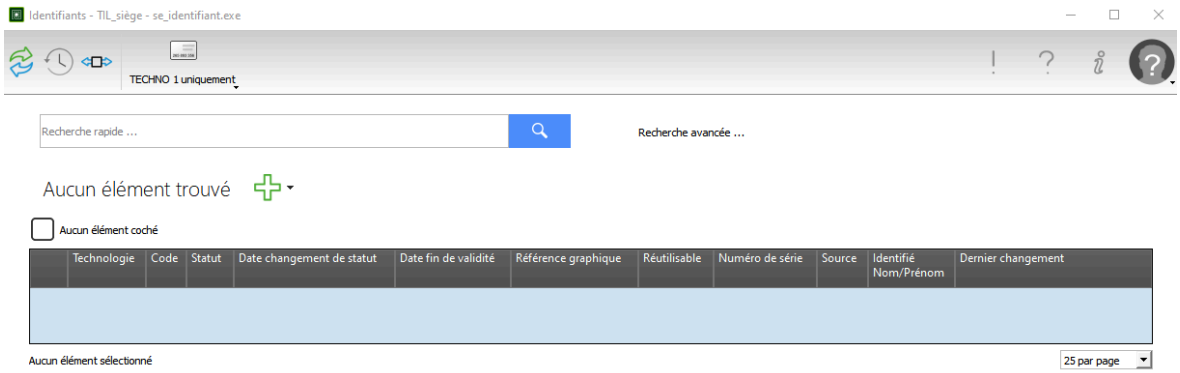


8.3. Gestion des identifiants

8.3.1. Gérer les identifiants

8.3.1.1. Généralités

Depuis le menu-principal, suivre **Exploitation > Contrôle d'accès > Identifiants**



Un identifiant correspond à un élément qui permet l'accès de l'identifié.

Un identifiant est défini par les éléments suivants:

- Un code identifiant.
- Une technologie (lecteur de plaques minéralogiques, lecteur de badges, capteur biométrique...).
- S'il est réutilisable ou non (possibilité de réaffecter l'identifiant à un autre identifié après utilisation, utile pour les visiteurs)

MICROSESAMEpeut gérer jusqu'à 4 technologies d'identifiants différentes, selon le paramétrage réalisé. Le paramétrage des identifiants est accessible via Menu principal > Paramétrage > Identifiants.

L'application permet de rechercher les identifiants présents dans le système, deux mode de recherches sont proposés:

Pour utiliser la recherche avancée, paramétrer les filtres en utilisant la liste déroulante et les champs dédiés, puis cliquer sur **Rechercher** pour lancer la recherche.

Le filtre créé peut en suite être sauvegardé pour être réutilisé:

1. Paramétrer les filtres en utilisant les listes déroulantes.
2. Renseigner le nom du filtre à enregistrer dans le champ dédié.
3. Cliquer sur .
4. Il est maintenant possible de retrouver ce filtre dans la liste déroulante.

8.3.1.2. Créer un identifiant

L'application permet de créer des identifiants afin de les stocker dans le système et de pouvoir les affecter depuis l'interface de gestion des identifiés.

Deux modes de création sont proposés:

- Création manuelle.
- Importation d'identifiants par un fichier .imp .

Tableau 8.5. Création manuelle d'un identifiant

Pour créer un nouvel identifiant associé à la **Techno 1**, cliquer sur l'icône . Pour créer un nouvel identifiant associé à une autre technologie, cliquer sur la liste déroulante et sélectionner la technologie souhaitée dans la partie **Ajouter manuellement**.	L'identifiant créé est ajouté automatiquement dans le tableau de paramétrage.
Renseigner les informations concernant l'identifiant: • **Code**: code identifiant . • **Statut**: Choisir le statut de l'identifiant (sélectionner **Valide**pour que l'identifiant soit opérationnel immédiatement).	La dernière modification concernant les statut de l'identifiant est affichée dans la colonne **Date changement de statut**. Effectuer un clic-droit sur l'entête du tableau pour afficher d'autres paramètres.

• **Date de fin de validité**: Date à partir de laquelle l'identifiant sera automatiquement dévalidé. (optionnel) • **Référence graphique**: Repère visuel présent sur le badge. • **Réutilisable**:Permet d'attribuer l'identifiant de nouveau après utilisation. • **Numéro de série**	

Tableau 8.6. Importer des identifiants

Pour impo  es identifiants depuis un fichier .im uer sur la liste déroulante de l'icône . **Dans la partie Importer depuis un fichier .imp** , Sélectionner la technologie à associer aux identifiants. L'assistant d'import des identifiants se lance automatiquement.	Par défaut, la condition d'unicité des identifiants par technologie est liée au code identifiant i.e. si l'on importe un identifiant dont le code est identique à un déjà présent dans la base de données, MICROSESAME mettra à jour la référence graphique et/ou le numéro de série de celui-ci selon les données présentes dans le fichier d'import. Pour fixer la règle d'unicité sur le numéro de série, cocher la case *Utiliser le numéro de série comme règle d'unicité*. i.e. si l'on importe un identifiant dont le numéro de série est identique à un déjà présent dans la base de données, MICROSESAME mettra à jour la référence graphique et/ou le code identifiant de celui-ci selon les données présentes dans le fichier d'import.
Rechercher et sélectionner l'emplacement du fichier .imp à importer. Une fois le fichier sélectionné, les données qu'il contient sont affichées dans le tableau.	**Syntaxe d'un fichier .imp:** • Une ligne correspond à une donnée à importer. • Chaque donnée est renseignée de la façon suivante: <Référence graphique><TAB><CodeIdentifiant><TAB • La référence et le code identifiant sont séparés par une tabulation

	• La référence graphique peut contenir des espaces. • Le code identifiant ne peut pas contenir d'espace.
Indiquer si les identifiants à importer sont définis comme réutilisables ou non. Sélectionner ensuite les identifiants à importer dans le système puis cliquer sur **Importer**	Les identifiants sont importés automatiquement dans le système. Rafraichir, si besoin, la fenêtre d'exploitation des identifiants pour la mettre à jour.

Exemple de fichier .imp:

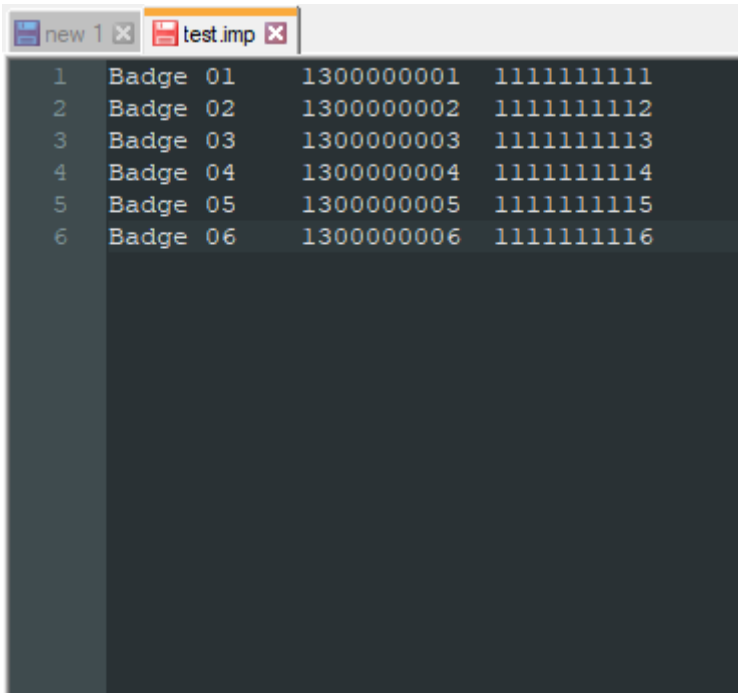


Tableau 8.7. Enrôler des identifiants

Pour enrôler des iden s depuis un lecteur / enrôleur, r sur la liste déroulante de l'icône . Vérifier que l'icône de l'enrôleur soit verte pour indiquer la connexion.	Pour paramétrer les ports de l'enrôleur, effectuer un clic-droit sur l'icône et cliquer sur **Paramétrer**.
Passer le ou les badges sur le lecteur / enrôleur pour faire remonter le code identifiant dans la technologie paramétrée.	**Dans le cas de l'utilisation de l'enrôleur PCSC JS:** • Veiller à ce que l'application Encodage JS soit fermée.

	• Si une carte SAM est utilisée, veiller à ce que le lecteur soit branché au poste de travail pendant toute la durée de la procédure enrôlement. • Si un fichier PKE est utilisé, Renseigner les informations de connexion à la configuration en question.  Il n'est nécessaire de renseigner les informations qu'une fois par jour.
Indiquer si les identifiants à importer sont définis comme réutilisables ou non.	 Rafraichir, si besoin, la fenêtre d'exploitation des identifiants pour la mettre à jour.

8.3.1.3. Exporter et imprimer une liste d'identifiants

L'application permet d'exporter une liste d'identifiants sélectionnés sous différents formats:

- PDF
- CSV
- TXT

Pour exporter une liste d'identifiants:

1. Sélectionner les identifiants concernés.
2. Effectuer un clic-droit sur la zone de sélection.
3. Sélectionner le format d'export:
   - Export PDF
   - Export CSV/TXT.
   - Assistant d'impression.
4. Valider l'emplacement d'export du fichier ou sélectionner l'imprimante à utiliser dans le cas d'une impression directe.

8.3.1.4. Imprimer les cartes

Pour lancer l'impression des cartes (badges) suivre la procédure suivante:

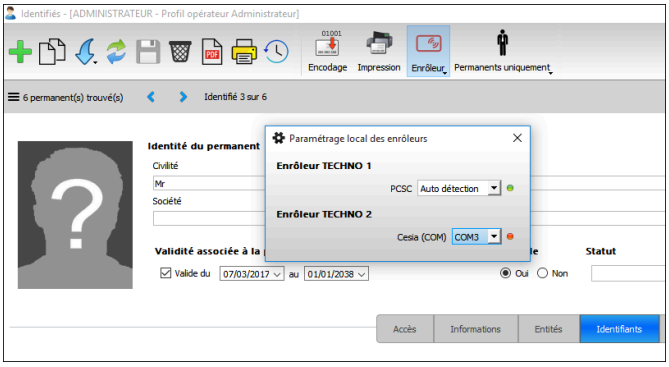
1. Sélectionner les identifiants concernés.
2. Effectuer un clic-droit sur la zone de sélection.
3. Choisir **Imprimer les cartes**.

Pour plus d'informations sur l'interface d'impression des cartes, consulter la section dédiée dans ce guide.

8.3.2. Enrôler les identifiants

8.3.2.1. Tester la communication avec l'enrôleur

1. Lancer la fenêtre de gestion des identifiés : *Menu MICROSESAME> Accès > Identifiés*
2. Cliquer sur l'icône "Enrôleur" :
   - Si l'icône devient rouge : MICROSESAMEne détecte aucun périphérique sur ce port COM/USB ou n'arrive pas à communiquer avec.



Solution : Effectuer un clic-droit sur l'icône **Enrôleur** puis paramétrer le port COM utilisé par le périphérique dans la fenêtre qui apparaît.

Le port COM peut être retrouvé via le gestionnaire de périphérique de Windows: *clic droit sur le "poste de travail" > propriété > Gestionnaire de périphériques > Ports (COM et LPT)*

- Si l'icône est verte : MICROSESAME détecte bien un périphérique sur ce port COM/ USB et est en attente d'un passage de badge sur ce dernier

8.3.2.2. Paramétrage des enrôleurs utilisés via TSE

Lors de l'utilisation d'une connexion TSE, il est nécessaire d'appliquer certaines paramétrages aux enrôleurs.

Selon le type d'enrôleur qui sera utilisé avec la "Connexion Bureau à distance", appliquer le paramètre de périphérique suivant :

Enrôleur	Périphérique
PROXILIS	• Choisir le périphérique "Ports" dans les paramètres de "Connexion Bureau à distance" (Suivre "Connexion Bureau à distance", "Afficher les options", "Ressources locales", "Ressources et périphériques locaux", "Autres". Cocher l'option "Ports"). • Choisir un port COM directement dans l'interface de gestion des identifiés dans MICROSESAME. Depuis la fenêtre de gestion des identifiés, cliquer droit sur l'icône de la barre d'outils et choisir "Paramétrer" pour lancer la fenêtre "Paramétrage local des enrôleurs".
PCSC (HID Omnikey)	Choisir le périphérique "Cartes à puce" dans les paramètres de "Connexion Bureau à distance" : Suivre "Connexion Bureau à distance", "Afficher les options", "Ressources locales", "Ressources et périphériques locaux", "Autres". Cocher l'option "Cartes à puce".
Cesia (USB)	• Choisir le périphérique "Ports" dans les paramètres de "Connexion Bureau à distance". Suivre "Connexion Bureau à distance", "Afficher les options", "Ressources locales", "Ressources et périphériques locaux", "Autres". Cocher l'option "Ports".

Enrôleur	Périphérique
	• Dans l'interface de paramétrage des identifiants de MICROSESAME paramétrer l'enrôleur Cesia. Suivre "Menu principal", "Paramétrage", "Identifiants". • Dans l'interface de gestion des identifiés de MICROSESAME, indiquer le port COM. Depuis la fenêtre de gestion des identifiés, cliquer droit sur l'icône de l'enrôleur dans la barre d'outils et choisir "Paramétrer" pour lancer la fenêtre "Paramétrage local des enrôleurs".

8.3.2.3. Enrôler un identifiant avec un lecteur de contrôle d'accès branché à l'UTL

L'enrôlement d'un identifiant à partir d'un lecteur de contrôle d'accès raccordé à l'UTL est disponible à partir de MICROSESAME Cube 2021.2

Généralités

Cette fonctionnalité permet de configurer un lecteur installé sur site afin de fonctionner comme un lecteur/enrôleur. Il pourra ainsi contrôler l'accès des identifiés et remonter un identifiant dans les interfaces suivantes:

MICROSESAM	WEBSESAME

• Gestion des identifiés :
  • Permanents
  • Visiteurs
• Gestion des identifiants
• Réception visiteur
	• Gestion des identifiés :
	  • Permanents
	  • visiteurs

Les droits opérateurs nécessaires pour le paramétrage et l'exploitation de cette fonctionnalité sont les suivants:

Intégrateur	Exploitant
• Droit de modification du paramétrage général (configuration lecteur/enrôleur) • Droit de visualisation du fil de l'eau (enrôlement de l'identifiant)	• Droit de visualisation du fil de l'eau (enrôlement de l'identifiant)

Configurer le lecteur/enrôleur

La configuration de cette fonctionnalité nécessite les droits opérateurs intégrateurs décrits dans la section précédente.

Il est impératif que le lecteur/enrôleur respecte les points de sécurité suivants:

- Le lecteur n'est pas un lecteur d'entrée du site.
- Le lecteur n'est pas installé sur un accès à une zone sensible.
- Le lecteur est installé à distance visible du poste d'enrôlement des identifiants.

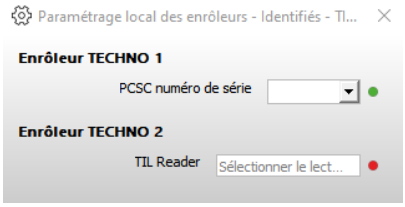
Activation de l'enrôleur

1. Depuis le menu-principal, suivre **Paramétrage > Contrôle d'accès > Identifiants**.
2. Dans la partie **Enrôleurs**, sélectionner **TIL Reader** pour la technologie souhaitée.

Assigner la technologie ainsi paramétrée au lecteur à configurer en tant qu'enrôleur.

Paramétrage du lecteur

1. Depuis le menu-principal, suivre **Exploitation > Contrôle d'accès > Identifiés**.
2. Cliquer sur l'icône enrôleur.
3. L'enrôleur TIL reader apparait dans la technologie correspondante.
4. Sélectionner le lecteur à configurer dans la liste déroulante.



La pastille associée au champ indique l'état de connexion de l'enrôleur:

- Rouge: non connecté.
- Vert: Connecté.

Enrôler un identifiant depuis MICROSESAME

Se rendre dans une des application suivantes afin d'enrôler un identifiant:

Application	Procédure
Gestion des identifiés	**Depuis le menu-principal, suivre Exploitation > Contrôle d'accès > Identifiés.** 1. Créer un nouvel identifié ou se rendre dans la fiche de l'identifié concerné (visiteur ou permanent).

Application	Procédure
	2. Cliquer sur l'icône enrôleur pour l'activer L'icône passe au vert si la connexion à l'enrôleur a correctement été paramétrée. 3. Passer un badge devant le lecteur / enrôleur. 4. L'identifiant remonté est affecté à l'identifié, sauvegarder la configuration.
Gestion des identifiants	**Depuis le menu-principal, suivre Exploitation > Contrôle d'accès > Identifiants.** 1. Cliquer sur la flèche à droite de l'icône  pour ouvrir la liste déroulante. 2. Sélectionner **Enrôler**. La validité de la connexion est indiquée par l'apparition d'une icône enrôleur et du texte suivant: "Présentez un ou plusieurs badges à l'enrôleur". 3. Passer un badge devant le lecteur / enrôleur. 4. L'identifiant remonté dans la technologie associée, sauvegarder la configuration.
Réception visiteur	**Depuis le menu-principal, suivre Exploitation > Visiteurs > Réception visiteurs.** 1. Ajouter un visiteur. 2. Sélectionner la technologie d'enrôlement associer au lecteur enrôleur **TIL Reader**. L'icône passe au vert si la connexion est réussie. 3. Passer un badge devant le lecteur / enrôleur.

Application	Procédure
	4. L'identifiant remonté dans la fenêtre de paramétrage du visiteur, cliquer sur enregistrer pour sauvegarder la configuration. Il est nécessaire d'activer la technologie associée à l'enrôleur **TIL Reader** dans le paramétrage des visites pour qu'elle puisse être utilisée dans l'application réception visiteurs.

Enrôler un identifiant depuis WEBSESAME

Accéder à WEBSESAME grâce à l'URL suivante: **https://Adresse-serveur:443**

Pour enrôler un identifiant à un permanent ou un visiteur existant, suivre la procédure suivante:	**Pour créer un permanent ou un visiteur et enrôler directement un identifiant, suivre la procédure suivante:**
1. Dans l'onglet Identifiés, cliquer sur **Permanents** ou **Visiteurs**. 2. Sélectionner l'identifié concerné. 3. Cliquer sur Modifier. 4. Faire défiler la page jusqu'à la section **Identifiants**.	1. Dans l'onglet Identifiés, cliquer sur **Créer un permanent** ou **Créer un visiteur**. 2. Renseigner les informations relatives à l'identifié puis faire défiler la page jusqu'à la section **Identifiants**.

La fenêtre **Lecteurs d'enrôlement** offre des informations sur la configuration du lecteur/enrôleur:

- Chargement: La connexion est en cours d'initialisation.
- Erreur: Une erreur est survenue.
- A configurer: Aucun lecteur n'a été configuré pour le lecteur / Enrôleur.
- Actif: Le lecteur est configuré et la connexion est fonctionnelle.

Si l'opérateur en a les droits il peut sélectionner le lecteur à configurer en tant que Lecteur / Enrôleur directement depuis WEBSESAME.

Une fois que le paramétrage a été effectuée le lecteur d'enrôlement passe en mode actif:

Passer un badge devant le lecteur / enrôleur pour faire remonter l'identifiant dans la fiche du permanent ou du visiteur.

8.3.3. Recherche par badge

La recherche par badge permet de retrouver des identifiés grâce à leurs identifiants.

La recherche par badge nécessite qu'un enrôleur soit configuré, branché au poste et que la technologie associée soit activée.

Depuis le menu-principal, suivre Exploitation > Contrôle d'accès > Identifiés:

1. Cliquer sur paramétrer la recherche par badge.
2. **Sélectionner le mode de recherche:**
   - Rechercher un badge à la fois
   - Rechercher un lot de badge
3. Cliquer sur l'icône enrôleur.

   L'icône passe au vert si la connexion est réussie.

4. Sélectionner **Permanents uniquement** ou **Visiteurs uniquement** en fonction de vos critères de recherche.
5. Passer le ou les badges sur l'enrôleur, si l'identifiant a été affecté, l'identifié associé remontera automatiquement dans la liste de recherche.

Dans le cadre d'une recherche par badge unique (et non par lot), sélectionner l'option **Ouvrir automatiquement la fiche identifié** pour que la fiche de l'identifié s'affiche lors du passage de son badge sur l'enrôleur.

8.3.4. Identifiants mobiles

8.3.4.1. Identifiants mobile STID

Introduction

Les identifiants mobiles STid sont des badges dématérialisés utilisables depuis un smartphone.Le passage de badge peut alors s'effectuer en activant le bluetooth ou le NFC de son smartphone

L'utilisation de badges dématérialisés sur les lecteurs STID nécessite l'accès à l'API stidmobile-ID et l'utilisation de crédits spéciaux. Pour l'ouverture du compte et la commande de crédits, se rapprocher du service des ventes de TIL-technologies.

Cette section est dédiée au paramétrage et l'utilisation des passerelles d'import des identifiants mobiles STID.

Deux types d'identifiants mobile sont disponibles à la création:

- STidMobile ID+ (1 crédit)
- Identifiant mobile sécurisé (5 crédits)

Prérequis

Avant de paramétrer les passerelles d'import sur MICROSESAME le client doit disposer des éléments suivants:

- Le poste serveur hébergeant MICROSESAME doit impérativement disposer d'une connexion internet vers l'extérieur. (Au minimum vers l'adresse suivante https://secure.stidmobile-ID.com avec le port correspondant ouvert)
- Un accès au portail https://secure.stidmobile-ID.com et les informations de connexions associées:
  - Token API correspondant (mode Token)
  - ID et secret client (mode (oAuth2)
- Un site configuré sur le portail Stid, accessible en suivant **Gérer mes sites clients > Sites**
- Dans le cas des identifiants mobiles sécurisés, un fichier de configuration de lecteurs **.pse**
- L'application Stid Mobile ID installée sur un smartphone compatible
- Un **lecteur Evolution Blue** configuré avec **SeCard**
- Des crédits

Pour plus d'information sur le paramétrage des lecteurs evolution Blue avec **SeCard** et la génération d'un fichier **.pse**, se référer à la documentation **constructeur** ou à la documentation suivante: **Lecteur_evolution_Blue**.

Créer un badge virtuel

La création d'un badge virtuel pour un identifié s'effectue depuis l'interface WEBSESAME

Le nombre d'identifiant mobile par utilisateur est limité à un.

Lancer WEBSESAME

- Depuis l'onglet **Identifié**, sélectionner la fiche du permanent ou du visiteur concerné
- Cliquer sur **Modifier**
- Dans la partie **Identifiants**, cliquer sur **Créer un identifiant mobile STid**

L'identifiant mobile STid est envoyé directement par mail à l'identifié concerné, il est donc nécessaire de renseigner l'adresse mail correspondante dans la fiche identifié. Dans le cas où le champ d'adresse mail est vide, WEBSESAME renverra le message d'erreur suivant.

Si la demande a été effectuée avec succès, l'état de l'identifiant mobile indiquera **En attente de génération de code**. L'utilisateur reçoit ensuite par mail permettant de télécharger le badge virtuel sur le smartphone (IOS ou Android).

Avant de cliquer sur le lien de téléchargement du badge, il est nécessaire d'installer l'application **STid mobile id** sur le smartphone.

Le portefeuille de badge virtuels se présente de la façon suivante, Dés l'installation de l'application, vous disposez d'un STid Mobile ID, gratuit et non sécurisé:

	• Coûte 1 crédit. • L'identifiant est transféré à MICROSESAMEà l'activation du badge virtuel grâce au lien reçu par mail. • L'identifiant est utilisable sur site 1 heure après activation du badge par l'identifié. De même, compter 1 heure avant modification de l'état **En attente de génération de code** à **Activé** dans la fiche identifié.
	• Coûte 5 crédits. • L'identifiant est généré aléatoirement par MICROSESAME il est téléchargé immédiatement dans la TILLYS et est donc utilisable dés l'activation de l'identifiant par l'identifié. • Compter 1 heure avant modification de l'état **En attente de génération de code** à **Activé** dans la fiche identifié.

La suppression de l'identifiant mobile affecté à un identifié depuis MICROSESAME ou WEBSESAME permet de révoquer automatiquement le badge sur le portail **https://secure.stidmobile-ID.com**.

Cette opération est pratiquement instantanée et permet de récupérer les crédits consommés par le badge.

Rappel:

- La révocation d'un badge STid Mobile ID+ (1 crédit) ne permet pas de récupérer le crédit dépensé, cependant l'identifiant sera bien libéré sur la plateforme tierce.
- La révocation d'un badge d'un badge d'accès virtuel sécurisé (5 crédits) permet de récupérer les crédits dépensés ainsi que de libérer l'identifiant sur la plateforme tierce.

8.3.5. Identifiants biométriques HID

8.3.5.1. Introduction

Les identifiants mobiles HID sont des badges dématérialisés utilisables depuis un smartphone.Le passage de badge peut alors s'effectuer en activant le bluetooth ou le NFC de son smartphone

L'utilisation de badges dématérialisés sur les lecteurs HID nécessite l'accès à l'API **https://cert.portal.origo.hidglobal.com/**. Pour l'ouverture du compte, se rapprocher du service des ventes de TIL-technologies.

Cette section est dédiée au paramétrage et l'utilisation des passerelles d'import des identifiants mobiles HID.

8.3.5.2. Prérequis

Avant de paramétrer les passerelles d'import sur MICROSESAME, le client doit disposer des éléments suivants:

- Le poste serveur hébergeant MICROSESAME doit impérativement disposer d'une connexion internet vers l'extérieur
- Le token API pour l'accès au portail https://cert.portal.origo.hidglobal.com/
- L'application **HID Reader Manager** installée sur un smartphone compatible
- L'application **HID Mobile Access** installée sur un smartphone compatible
- Un Lecteur HID compatible Bluetooth configuré

Pour plus d'information sur le paramétrage des lecteurs HID avec l'application **HID reader manager**, se référer à la documentation **constructeur** ou à la documentation suivante: **notice de l'application reader manager HID**

8.3.5.3. Créer un badge virtuel

La création d'un badge virtuel pour un identifié s'effectue depuis l'interface WEBSESAME

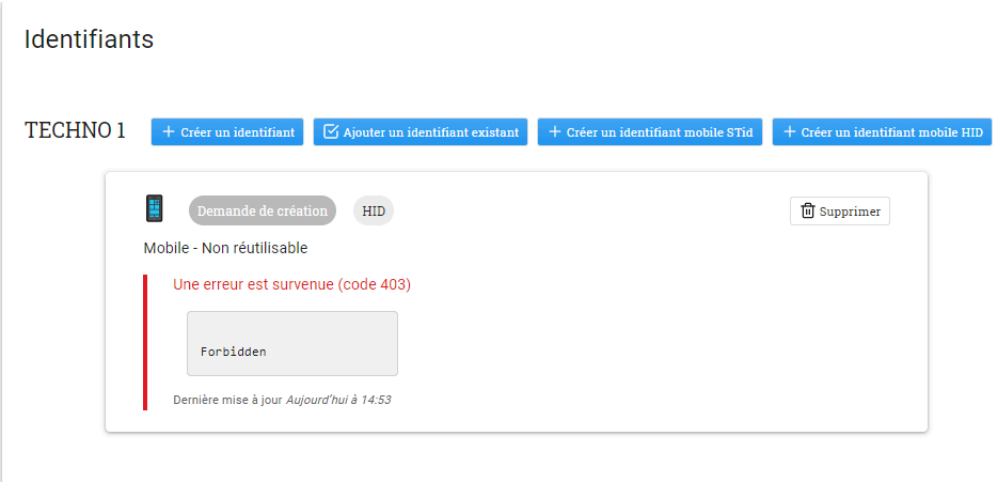
Le nombre d'identifiant mobile par utilisateur est limité à un.

Lancer WEBSESAME

- Depuis l'onglet **Identifié**, sélectionner la fiche du permanent ou du visiteur concerné
- Cliquer sur **Modifier**
- Dans la partie **Identifiants**, cliquer sur **Créer un identifiant mobile HID**

L'identifiant mobile HID est envoyé directement par mail à l'identifié concerné, il est donc nécessaire de renseigner l'adresse mail correspondante

dans la fiche identifié. Dans le cas où le champ d'adresse mail est vide, WEBSESAME renverra le message d'erreur suivant.



Si la demande a été effectuée avec succès, l'état de l'identifiant mobile indiquera **En attente de génération de code**. L'utilisateur reçoit ensuite par mail permettant de télécharger le badge virtuel sur le smartphone (IOS ou Android).

Avant de cliquer sur le lien de téléchargement du badge, il est nécessaire d'installer l'application **HID mobile access** sur le smartphone.

Supprimer l'identifiant mobile d'un identifié depuis MICROSESAME ou l'interface WEBSESAME permet uniquement de bloquer l'accès de l'identifié.

Pour **révoquer** l'identifiant mobile, se rendre sur le portail **https://cert.portal.origo.hidglobal.com/**

8.3.6. Identifiants biométriques STID

8.3.6.1. Introduction

Cette fonction est accessible à partir de la version **2020.3** de MICROSESAME

Les identifiants biométriques STid permettent de s'identifier sur un lecteur biométrique STid. Le passage de badge est alors complété par une séquence de lecture d'empreinte digitale pour autoriser ou refuser l'accès.

L'utilisation des identifiants biométriques sur les lecteurs STID nécessite une licence **PRIME**. Pour toute commande, se rapprocher du service des ventes de TIL-technologies.

Cette section est dédiée au paramétrage et l'utilisation de la passerelle d'enrôlement/ encodage d'identifiants biométriques depuis MICROSESAME

8.3.6.2. Prérequis

Avant de paramétrer les passerelles d'import sur MICROSESAME, le client doit disposer des éléments suivants:

- Un lecteur encodeur STid
- Un lecteur enrôleur d'empreinte
- Le badge Desfire EV1 à encoder
- Un lecteur evolution biométrique STid
- Logiciel **SECard**
- Une licence **PRIME** activée dans MICROSESAM
- Le logiciel **KSM NG**

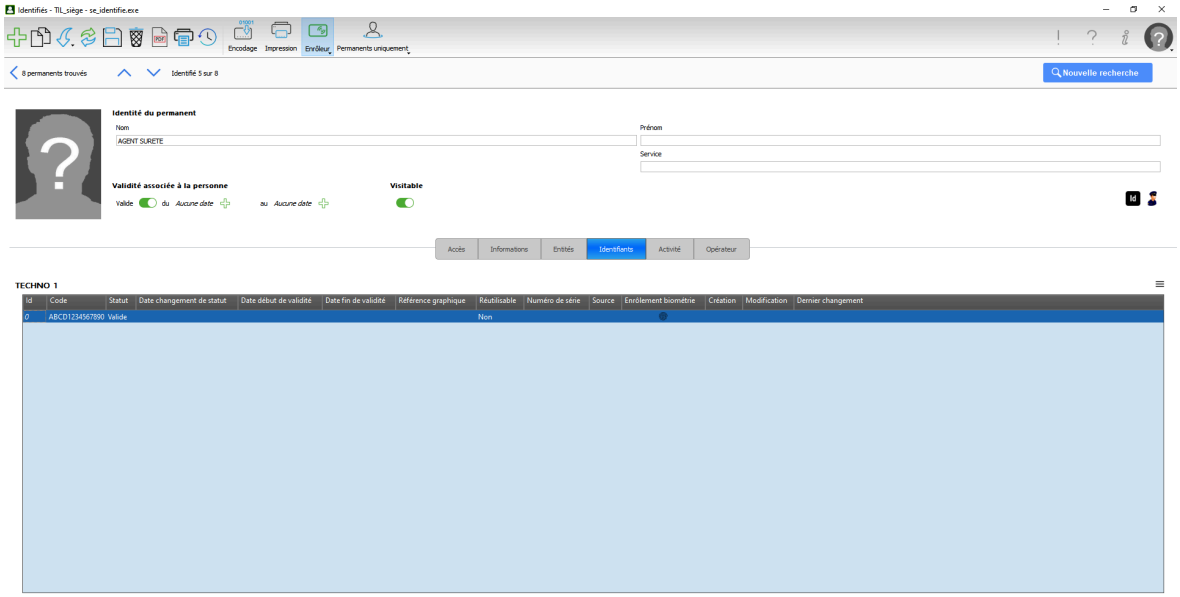
La configuration des **clés de lecture** et de l'**encodage de badge** dans **SECard** est à effectuer au préalable.

Les logiciels SECard et KSM CUBE sont livrés par HIRSCH à la commande d'un Kit de programmation de lecteurs Evolution et d'encodage de badge.

8.3.6.3. Encoder un badge biométrique et l'attribuer à un identifié

Depuis le menu-principal suivre Exploitation > Contrôle d'accès > identifiés:

1. Mettre l'application **se_identifie.exe** en plein écran
2. Sélectionner la fiche de l'identifié concerné
3. Dans l'onglet **identifiants**, effectuer un clic-droit sur l'entête des colonnes de la fenêtre inférieure.
4. Sélectionner **Enrôlement biométrie** pour afficher la colonne dans la fenêtre.
5. Brancher l'enrôleur d'empreinte
6. Brancher l'encodeur STid
7. Poser le badge DESfire EV1 sur l'encodeur



Suivre la procédure suivante:

1. Dans la fenêtre inférieure, Effectuer un clic-droit, puis sélectionner **Créer un identifiant**
2. L'opérateur définit un identifiant sécurisé dans la colonne **Code**

   La Taille de l'identifiant doit correspondre à la taille définie dans le paramétrage du logiciel SECard.

3. Cliquer sur l'icône empreinte dans la colonne **Enrôlement Biométrie**
4. La fenêtre d'acquisition des données biométriques se lance automatiquement, attendre que l'enrôleur d'empreinte s'allume.
5. L'identifié appose son doigt sur l'enrôleur pour acquisition.

   Le nombre d'empreintes requis peut être paramétré dans le logiciel SECard (Index, majeur, pouce....)

6. L'acquisition d'empreinte terminée, attendre une dizaine de seconde

Le badge contient désormais un identiant ainsi que les données biométriques de l'identifié concerné.

8.4. 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, ...) .

8.4.1. Généralités

L'OSS est un standard permettant de s'interfacer avec de nombreux équipements mécatroniques provenant de divers constructeurs :

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

Tableau 8.8. 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 • Assignation 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 (ex: 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 8.9. 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. MICROSESAMEintègre une fonctionnalité **lecteur actualisateur** permettant de remplacer les bornes de chargement par des lecteurs de contrôle d'accès classiques, capables de gérer 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: ???
Badge encodé OSS	L'implémentation de l'OSS nécessite l'utilisation de badges encodés spécifiquement pour l'utilisation de lecteurs autonomes avec ce standard. **Données relatives à l'exploitation OSS encodées dans le badge :** • Identifiants • Droits d'accès OSS • Durée de validité des droits • Liste noire • Historique (passages autorisés, interdits, ...) • Évènements lecteurs (pile faible, ...)
Lecteurs autonomes	Les lecteurs autonomes ne nécessitent aucun câblage et sont encastrées dans la porte (cylindre, béquille ou serrure mécatronique).

Équipements	Détails
	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 8.3. Schéma fonctionnel OSS

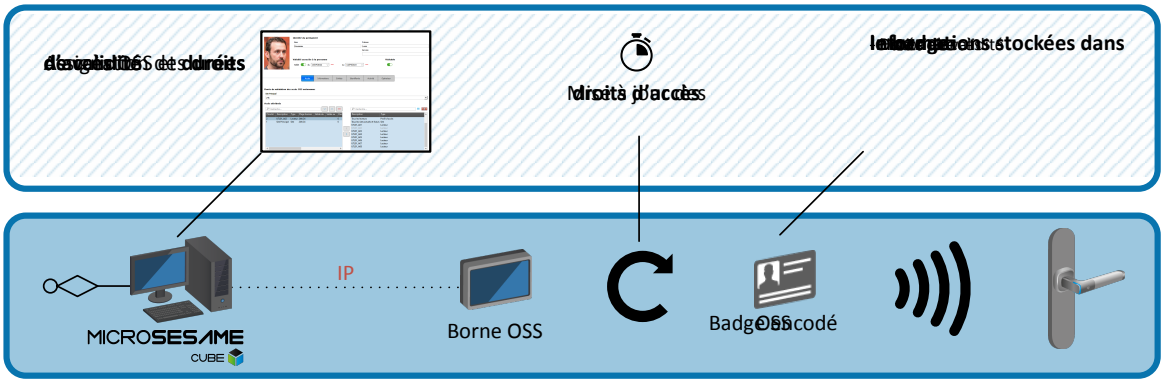
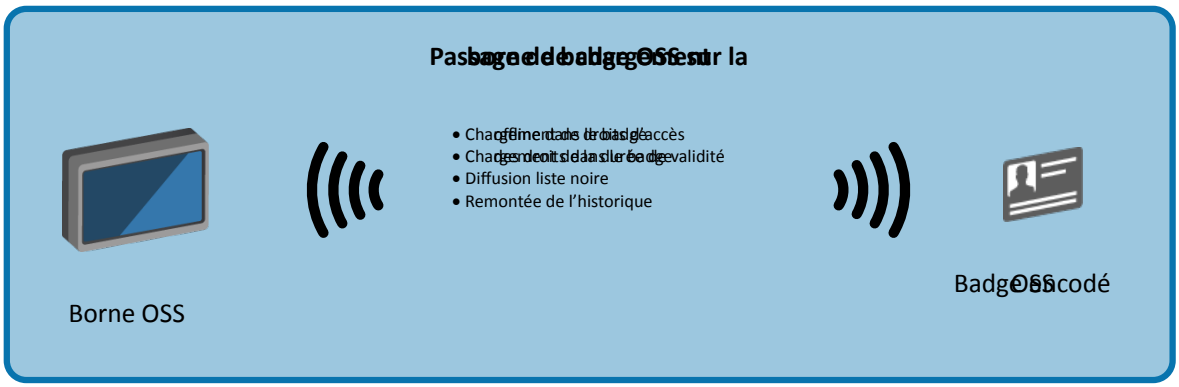


Figure 8.4. Mise à jour des droits OSS sur la borne de chargement



8.4.2. Lecteur actualisateur

L'installation d'une borne de chargement de droits OSS impose aux identifiés l'obligation de passer leur badge sur la borne régulièrement, afin de **mettre à jour leur droits d'accès** sur les lecteurs autonomes ainsi que de remonter l'historique à MICROSESAME.

Dans le cas où cette architecture ne convienne pas à l'exploitation sur site, TIL-technologies propose l'installation d'un lecteur actualisateur :

- Lecteur de contrôle d'accès classique installé sur site
- 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 OSS**
- Un même lecteur actualisateur peut traiter distinctement les passages de badges classiques, badges avec donnée sécurisée et passages de badges OSS
- S'inscrit dans l'exploitation classique du contrôle d'accès sur site et permet de s'affranchir de la contrainte imposée par la borne de chargement offline.

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, se référer à la documentation du MLP2-UPDATER.

8.4.3. Paramétrage OSS offline

8.4.3.1. Ajouter des identifiants dans la liste noire

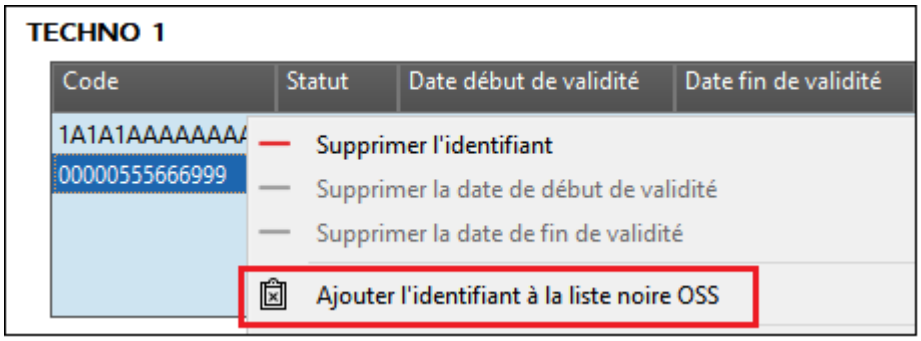
Il est possible de créer et de diffuser dans les serrures OSS une liste noire, c'est à dire une liste de badges qui seront interdits lors de leur passage sur ces dernières.

Cela permet notamment d'interdire des badges qui auraient été volés, perdus ...

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

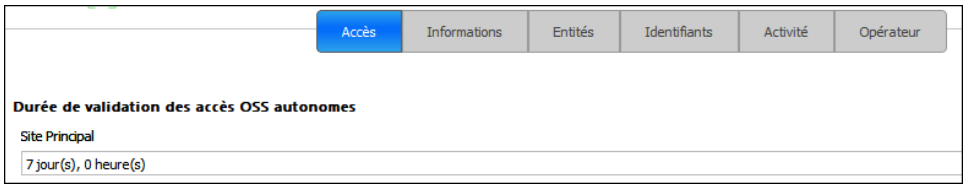
Pour descendre la liste noire dans les serrures, il est nécessaire de réaliser les opérations suivantes :

1. Déclarer un identifiant dans la liste noire :
   a. Depuis le menu principal, suivre ***Exploitation > Identifiés*** , puis cliquer sur l'onglet **Identifiants** de la fenêtre.
   b. Dans le tableau de la technologie correspondante, cliquer- droit sur l'identifiant voulu et sélectionner **Ajouter l'identifiant à la liste noire OSS**.



   c. Paramétrer la date de fin d'expiration. Il est conseillé de définir la date d'expiration au minimum à la date et à l'heure actuelles.

Dans l'onglet **Accès**, définir la durée **Durée de validation des accès OSS autonomes**.



   d. Changer le statut de l'identifiant (perdu, volé, etc ...) ou encore 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.

8.4.3.2. 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 matérielle**.*

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

1. Dans la table **Architecture matérielle** 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 matérielle** 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, d'une modification ou d'une suppression, depuis la gestion des identifiés ou des identifiants.

8.5. Accueil visiteurs et gestion des rendez-vous

8.5.1. Préparer et accueillir les visites

Sur un site équipé en contrôle d'accès, les personnes extérieures à l'entreprise doivent pouvoir être enregistrées, accompagnées, voire munies d'un identifiant, pour pouvoir circuler dans les zones qui lui sont autorisées.

MICROSESAMEintègre une gestion spécialisée, qui permet la planification et la gestion des flux de ces visiteurs, à travers deux interfaces étudiées pour optimiser les procédures d'accueil :

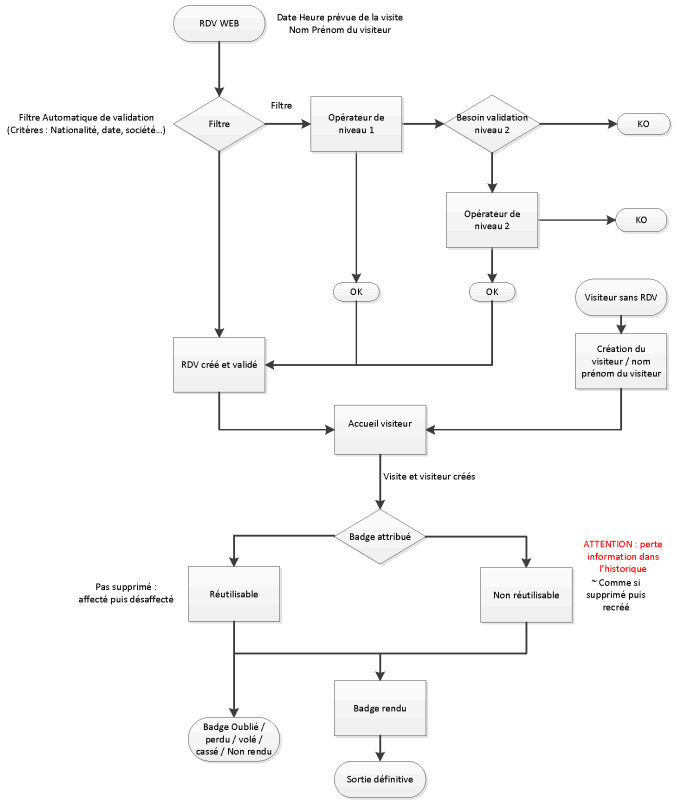
- L'application **Accueil de visiteurs** (se_visit_reception.exe), installé en poste client lourd sur chaque poste client. Disponible à l'entrée physique du bâtiment, permet les opérations les plus complètes, de l'attribution des droits au contrôle des sorties, avec scan des papiers d'identité ou encore l'impression de badges personnalisés.
- L'application **WEBSESAME** (client léger web) ouvre à n'importe quel utilisateur muni d'un navigateur web (et autorisé), la possibilité de saisir des visiteurs, planifier des rendez-vous et valider les informations nécessaires (plage horaire, profil d'accès, accompagnant...).

Ces deux interfaces permettent un traitement accéléré et une plus grande fluidité de l'accueil physique des visiteurs.

Elles allient flexibilité et sécurité pour s'adapter à toutes les organisations.

8.5.2. L'accueil de visiteurs

Le processus d'accueil de visiteurs le plus complet est le suivant :



8.5.3. Planifier et Gérer les rendez-vous

8.5.3.1. Généralités

La planification et la gestion des rendez-vous est gérée entièrement par l'interface WEBSESAME. La solution proposée permet de gérer tous les points suivants depuis une seule et même interface :

- Création de rendez-vous (date, objet, personnes concernées)
- Création de visiteurs
- Distribution d'un profil d'accès en prévision de la visite
- Fonctionnalités additionnelle nécessitant un paramétrage particulier (Notification par mail, identifiant pour accès anticipé, validation des rendez-vous...)
- Recherche des rendez-vous passés, en cours et à venir (recherche rapide ou recherche par filtre)

Certaines des fonctionnalités décrites dans cette section nécessite d'effectuer un paramétrage spécifique. Pour plus d'informations se référer à la section précédente : ??? .

L'interface WEBSESAME pour la gestion de rendez-vous ne permet pas la réception des visiteurs.

Pour enregistrer les visiteurs attendus à la suite de la création d'un rendez-vous, depuis le menu-principal MICROSESAME, suivre **Exploitation > Visiteurs > Réception visiteurs** .

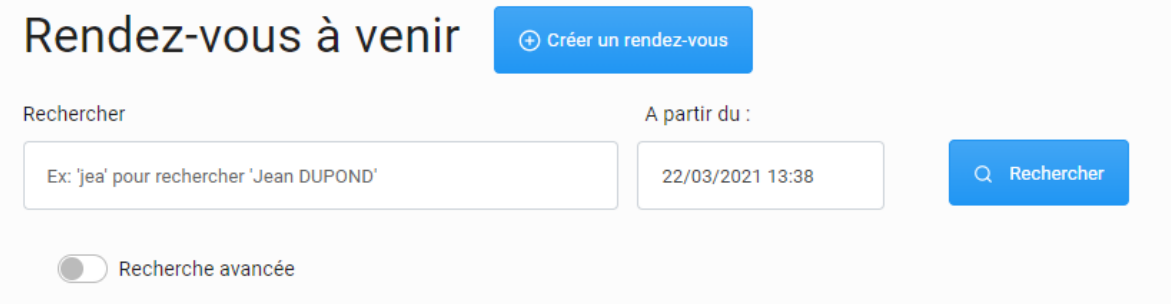
L'accès au service WEBSESAME se fait grâce à l'adresse suivante: `https://nom_du_serveur:443/`

Le port à renseigner dans l'URL d'accès à WEBSESAME est susceptible de changer en fonction de la configuration du poste serveur.

L'opérateur peut aussi accéder à WEBSESAME depuis le menu-principal: **Exploitation > Visiteurs > Rendez-vous**.

8.5.3.2. Gestion des rendez-vous

L'application de gestion des rendez-vous permet de planifier la visite d'un ou plusieurs visiteurs.



2 actions sont disponibles : créer un rendez-vous ou rechercher un rendez-vous existant.

La création et la recherche de rendez-vous sont soumises à droits opérateur.

Un opérateur défini comme **utilisateur simple**dans le système (opérateur avec droit de gestion des rendez-vous, mais sans droit de visualisation des identifiés), n'accède qu'aux actions suivantes :

- **Créer ou visualiser des rendez-vous pour cinq identifiés maximum.** Lorsque l'opérateur entrera un nom d'identifié, cinq noms d'identifiés lui seront alors proposés : celui de l'identifié saisi, ainsi que les noms des quatre identifiés suivants dans l'ordre alphabétique.
- **Visualiser un nombre très restreint d'informations concernant l'identifié** : Nom, prénom, société ou service.

Création d'un rendez-vous

Ce tableau contient les sections disponibles lors de la création d'un rendez-vous.

Enregistrer les modifications afin que le rendez-vous soit pris en compte correctement.

Les informations affichées dans cette interface peuvent contenir plus ou moins de données, en fonction du paramétrage appliqué à l'Accueil de visiteurs et à WEBSESAME.

élément	description
Visité	Indiquer le nom et le prénom de la personne visitée lors du rendez-vous qui sera programmé. Ce champ est obligatoire. Un identifié visitable peut recevoir des visiteurs, des visites peuvent être planifiées pour lui. La fonctionnalité d'auto-complétion permet, pendant l'édition, d'afficher des suggestions pour le champ à remplir, assurant une saisie rapide tout en évitant les doublons d'informations. Après avoir sélectionné la personne visitée, les données suivantes de l'utilisateur sont affichées :  L'opérateur peut alors effectuer les actions suivantes (de gauche à droite) :  • Supprimer la personne visité de la visite • Accéder à la fiche identifiée de la personne visitée • Modifier la fiche identifiée de la personne visitée
Accompagnant	Remplir ce champ si, lors du rendez-vous, un accompagnant doit être présent. Pour supprimer l'accompagnant, utiliser Retirer l'accompagnant.  La définition d'un accompagnant de la visite n'est pas lié à la fonctionnalité escorte visiteur.  Il est nécessaire d'activer les accompagnants dans le paramétrage général de MICROSESAME, onglet **visites**.

élément	description
Horaires et informations	Renseigner l'heure, la date et l'objet de la visite. Si les champs **Informations complémentaires** ou **Libellés** sont actifs, il est possible de les remplir pour fournir des informations complémentaires. Les champs avec un astérisque sont obligatoires.
Visiteurs	Depuis le champ Visiteurs, il est possible de créer un visiteur ou rechercher un visiteur existant.  Un ou plusieurs visiteurs peuvent être ajoutés au rendez-vous. Une fois présents dans la liste de visiteurs, il est possible d'éditer ou supprimer les visiteurs. Pour plus d'informations sur l'ajout d'un statut escorte au visiteur, consulter la section suivante : *???*
Accès	Cliquer ou commencer la saisie pour sélectionner un profil d'accès à attribuer au rendez-vous. Ces accès seront activés à l'enregistrement du visiteur. Il est nécessaire de paramétrer les **accès distribuable** dans le paramétrage général de MICROSESAME, onglet **visites**.

Une fois le rendez-vous créé, les informations relatives à cette visite peuvent être retrouvées dans différentes interfaces:

- Dans l'onglet Rendez-vous de **WEBSESAME**, se rendre dans la sous catégorie **A venir** pour accéder à la liste des rendez-vous passés, en cours ou planifiés. La fonctionnalité de recherche de rendez vous est expliquée en détail dans la section suivante.
- Dans l'application de réception des visiteurs de **MICROSESAME**, l'utilisateur pourra visualiser les visiteurs déclarés pour ce rendez-vous ainsi que toutes les informations relatives à la visite. Ces visiteurs possèderont le statut **En Attente**, jusqu'à leur enregistrement.

Recherche d'un rendez-vous

La sous catégorie **A venir** de l'onglet **Rendez-vous** permet de rechercher, filtrer et consulter les rendez-vous préalablement créés.

Seuls les rendez-vous à venir sont disponibles dans la table, pour consulter l'historique des visites, se rendre dans la'application MICROSESAME **Réception visiteur**.

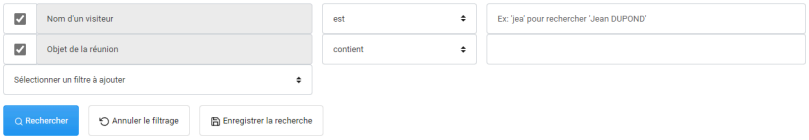
Pour rechercher rapidement un rendez-vous, suivre la procédure suivante

1. Dans le champ **recherche** , entrer le Nom ou prénom d'un des intervenants de la visite (Visité, visiteur ou accompagnant)
2. Dans le champ **A partir du**, sélectionner la date et l'heure à partir de laquelle rechercher le rendez-vous

Pour rechercher un rendez-vous grâce à un filtre prédéfini, suivre la procédure suivante:

1. Cliquer sur **filtre à ajouter** puis sélectionner un filtre dans la liste déroulante
2. Ajouter tous les filtres nécessaires à la recherche
3. Paramétrer les conditions de recherches avec les opérateurs logiques (est, commence par, contient,...)
4. Cliquer sur rechercher.

Cliquer sur Enregistrer la recherche pour ajouter le modèle de recherche paramétré dans la liste des filtres prédéfinis



8.5.4. Valider les rendez-vous

Il est nécessaire d'activer cette fonctionnalité dans le paramétrage des visites pour en bénéficier. Pour plus d'informations se référer à la section ???.

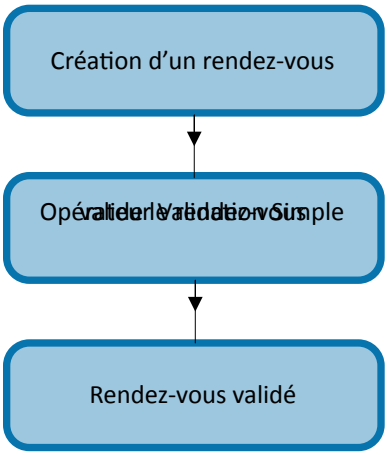
Pour utiliser la fonctionnalité, il est nécessaire d'effectuer les opérations suivantes :

- Activer la fonctionnalité dans le paramétrage des visites et configurer le mode de validation.

- Les opérateurs chargés de la validation des rendez-vous doivent posséder les droits adéquats dans leur profil opérateur.

Lorsque cette fonctionnalité est activée, il est nécessaire que le rendez-vous est été totalement validé afin de recevoir un visiteur sur site.

8.5.4.1. Validation simple d'un rendez-vous

Validation simple
Tous les rendez-vous créés depuis WEBSESAME seront soumis à l'approbation d'un opérateur possédant le droit de validation *Valider les rendez-vous : Niveau 1 / Validation simple* . Aucun des critère définis n'est pris en compte dans ce mode.


L'automate **ms_aut_visit_validation.exe** est uniquement lié à la validation par niveaux. La validation simple ne requiert pas le lancement de ce dernier

Tableau 8.10. Cas d'usage : Validation simple

Étapes	Détails
1. Création du rendez-vous	Un opérateur créé un rendez-vous sur WEBSESAME, le statut de validation passe automatiquement à nouveau L'opérateur responsable de la création de rendez-vous peut modifier son rendez-vous tant

Étapes	Détails
	que le statut de validation de celui-ci est fixé sur **Nouveau**.
2. Notification des opérateurs de validation	Les opérateurs possédant le droit *Valider les rendez-vous : Niveau 1 / Validation simple* sont notifiés du rendez-vous à valider : • Sur la page d'accueil de WEBSESAME • Par mail si l'envoi de mail au validateur a été paramétré  L'opérateur de validation doit posséder les mêmes entités que la personne visitée.
3. Décision du validateur	Le validateur visualise la liste des rendez-vous à valider dans WEBSESAME, onglet **Rendez-vous > A valider**. **L'opérateur peut consulter les informations relatives au rendez-vous puis prendre une décision quant au statut de validation :** • Nouveau • En cours • **Validé** : Le rendez-vous est validé • **Rejeté** : le rendez-vous demandé sera automatiquement supprimé  A tout moment, jusqu'à la réception du visiteur sur site, l'opérateur de validation peut rétrograder le statut de validation.
4. Réception du visiteur	Le visiteur peut être reçu sur site uniquement si le statut du rendez-vous est passé à **Demande validée**.

8.5.4.2. Validation par niveaux des rendez-vous

Validation par niveaux (avec critères)
Les rendez-vous créés depuis WEBSESAME correspondant aux critères définis dans le paramétrage des visites seront soumis à l'approbation des opérateurs autorisés à valider les rendez-vous.  Il est possible d'affiner les opérateurs de niveau 1 autorisés à valider les rendez-vous en fonction des critères définis.

Validation par niveaux (avec critères)

La création d'un critère **vide** (sans condition de validation) permettra de soumettre tous les rendez-vous à la validation.

Ce mode permet de mettre en place une validation des rendez-vous sur deux niveaux d'opérateurs, permettant ainsi d'impliquer un responsable ayant plus d'autorité dans la prise de décision.

Les opérateurs impliqués dans la prise de décision doivent posséder des droits en accord avec leur responsabilités

- **Premier niveau de validation** :*Valider les rendez-vous : Niveau 1 / Validation simple* et *Critères assignés à l'opérateur*
- **Second niveau de validation** : *Valider les rendez-vous : Niveau 2 uniquement*

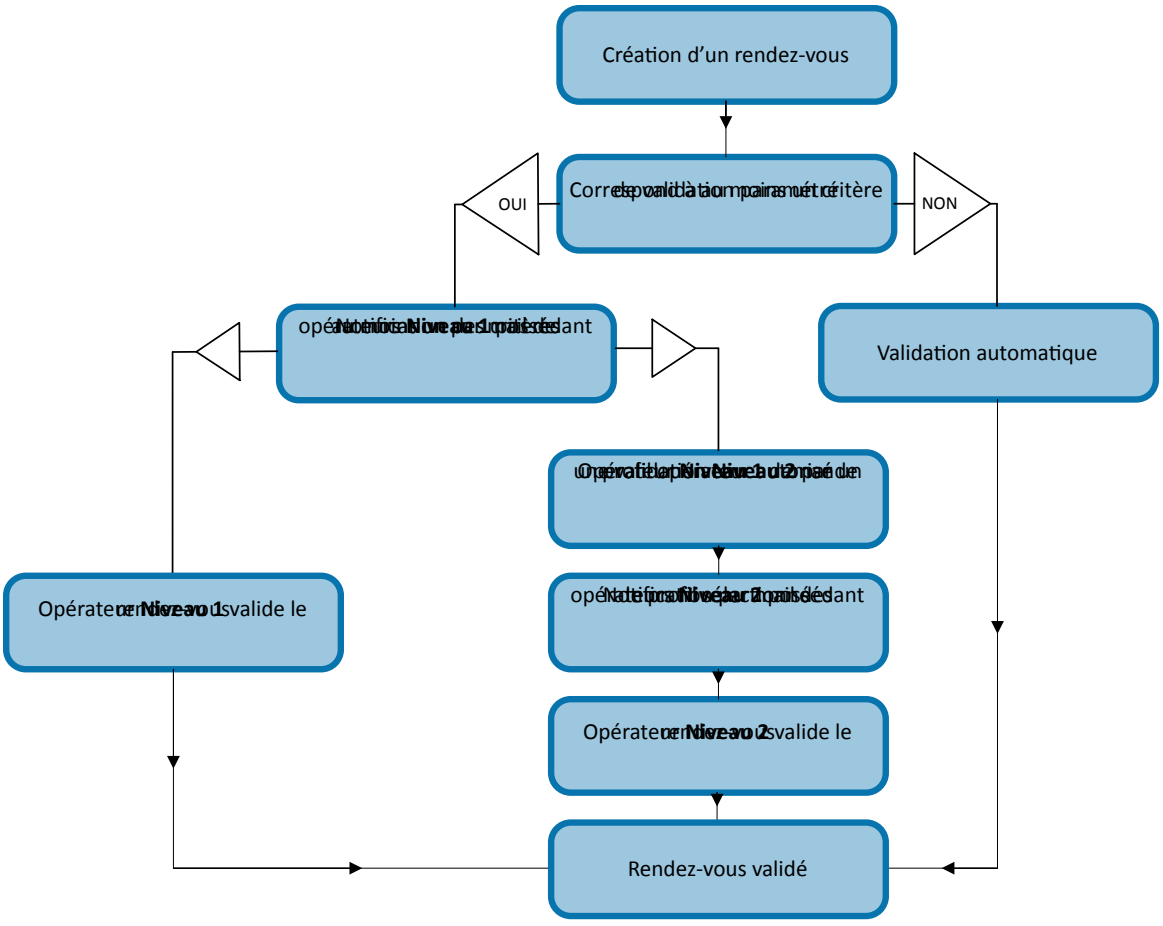


Tableau 8.11. Cas d'usage : Validation par niveaux avec critères

Étapes	Détails
1. Création du rendez-vous	**Un opérateur créé un rendez-vous sur WEBSESAME :** • Le rendez-vous ne correspond à aucun des critères paramétrés, il est validé automatiquement • Le rendez-vous correspond à un des critères paramétrés, il est envoyé à valider aux opérateurs de validation possédant ce critère dans leur profil.  L'opérateur responsable de la création de rendez-vous peut modifier son rendez-vous tant que le statut de validation de celui-ci est fixé sur **Nouveau**.
2. Notification des opérateurs de validation **Niveau 1**	Les opérateurs possédant le droit *Valider les rendez-vous : Niveau 1 / Validation simple* sont notifiés du rendez-vous à valider : • Sur la page d'accueil de WEBSESAME • Par mail si l'envoi de mail au validateur a été paramétré  L'opérateur de validation doit posséder les mêmes entités que la personne visitée.
3. Décision du validateur **Niveau 1**	Le validateur visualise la liste des rendez-vous à valider dans WEBSESAME, onglet **Rendez-vous > A valider**. **L'opérateur peut consulter les informations relatives au rendez-vous puis prendre une décision quant au statut de validation :** • Nouveau • En cours • **Validation Niveau 2** : L'opérateur de niveau 1 requiert l'approbation du'un opérateur de niveau 2, il renseigne le profil opérateur associé. • **Validé** : le rendez-vous est validé • **Rejeté** : le rendez-vous demandé sera automatiquement supprimé

Étapes	Détails
	A tout moment, jusqu'à la réception du visiteur sur site, l'opérateur de validation peut rétrograder le statut de validation.
4. Notification des opérateurs de validation **Niveau 2**	Les opérateurs possédant le profil renseigné par le validateur de niveau 1 sont notifiés du rendez-vous à valider : • Sur la page d'accueil de WEBSESAME • Par mail si l'envoi de mail au validateur a été paramétré L'opérateur de validation doit posséder les mêmes entités que la personne visitée.
5. Décision du validateur **Niveau 2**	Le validateur visualise la liste des rendez-vous à valider dans WEBSESAME, onglet **Rendez-vous > A valider**. **L'opérateur peut consulter les informations relatives au rendez-vous puis prendre une décision quant au statut de validation :** • Nouveau • En cours • **Validation Niveau 1** : L'opérateur de niveau 2 renvoie la prise de décision à l'opérateur de validation initial (ex: demande de validation par un autre profil opérateur de niveau 2). • **Validé** : le rendez-vous est validé • **Rejeté** : le rendez-vous demandé sera automatiquement supprimé A tout moment, jusqu'à la réception du visiteur sur site, l'opérateur de validation peut rétrogader le statut de validation. Une fois impliqué dans le orcessus de validation d'un rendez-vous, le validateur de niveau 2 peut intéragir avec la demande de validation meme si elle ne lui est plus assignée.

Étapes	Détails
6. Réception du visiteur	Le visiteur peut être reçu sur site uniquement si le statut du rendez-vous est passé à **Demande validée**.

8.5.5. Recevoir les visiteurs

8.5.5.1. Généralités

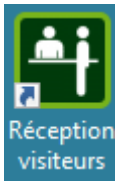
L'application de réception de visiteurs dans MICROSESAME permet de gérer entièrement l'accueil et la supervision des visiteurs (accès, validité, statut identifiant, alertes...)

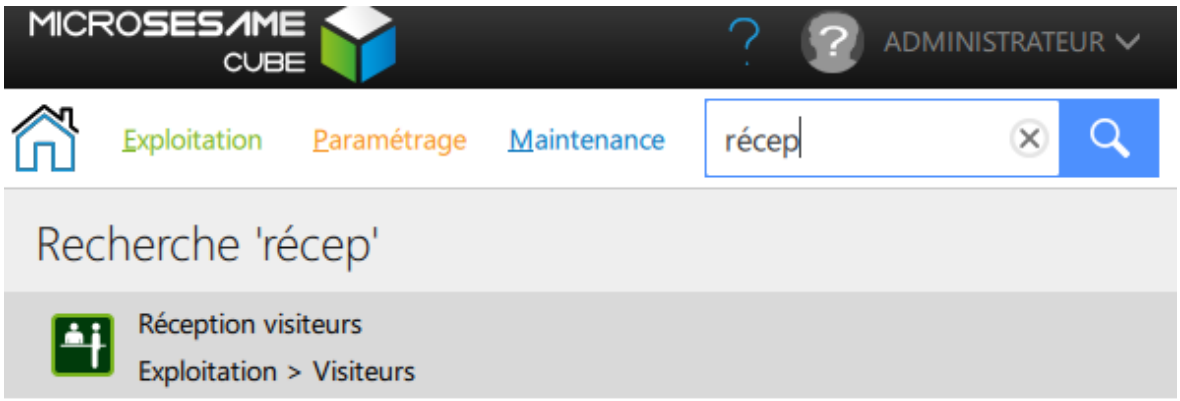
L'application de réception des visiteurs dans MICROSESAMEne permet pas de planifier des rendez-vous à l'avance.

Pour créer des rendez-vous à l'avance, depuis l'interface WEBSESAME, suivre **Rendez-vous > Créer** .

Pour accéder à l'application de l'accueil de visiteurs (se_visit_reception.exe), rechercher **Reception visiteurs** dans la barre de recherche depuis le menu principal de MICROSESAME

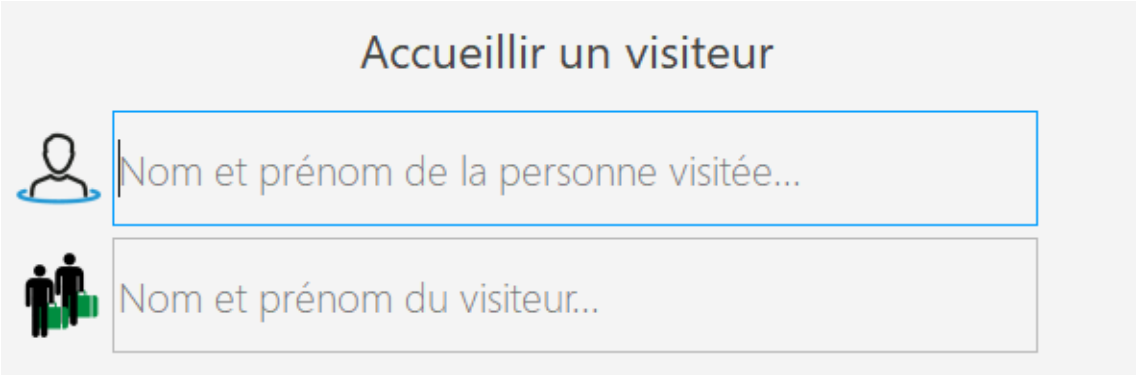
suivre Exploitation > Visiteurs ou utiliser l'icône créée sur le bureau lors de l'installation de MICROSESAME. Le login et le mot de passe d'accès à MICROSESAME sont demandés.





8.5.5.2. Enregistrer un visiteur/création d'une nouvelle visite

1. **Rechercher** le visiteur/la visite à créer. Cette vérification permet d'éviter la création de doublons. La personne visitée peut être aussi utilisée comme critère de recherche de visites/visiteurs dans l'application. Si le visiteur (ou la visite) à créer n'existe pas, cliquer sur "+" (ou CTRL+N) pour créer le nouveau visiteur.
2. Indiquer le **nom du visiteur**.



3. La fenêtre **Réception de visiteurs** (se_visit_reception.exe) s'ouvre.

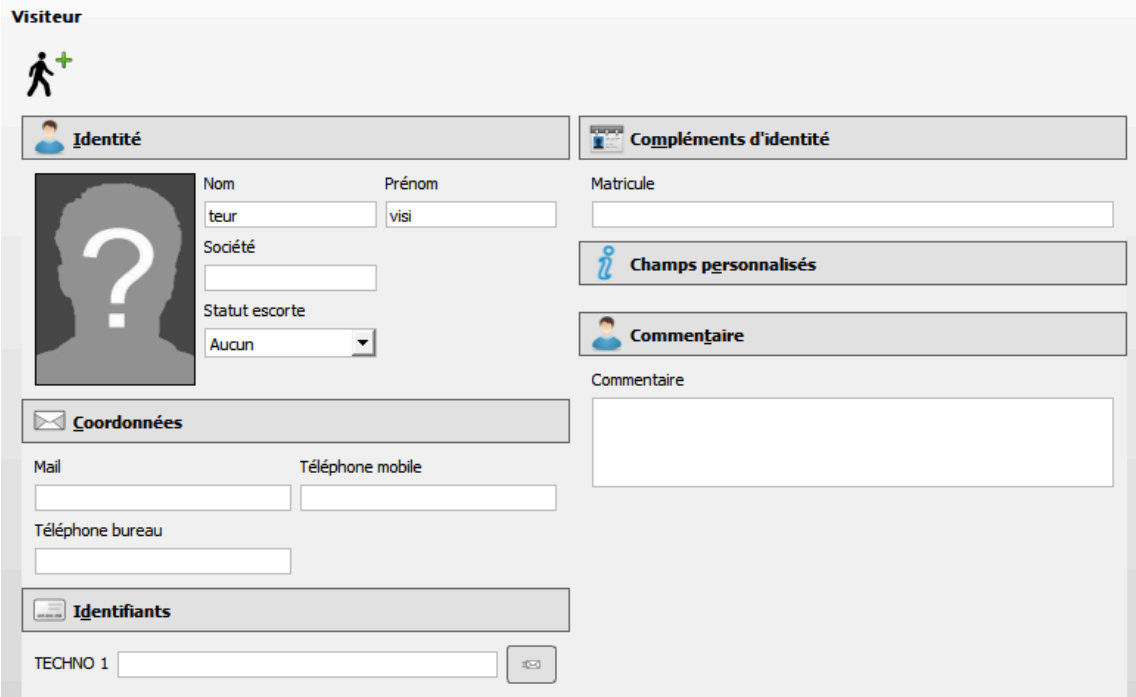
Les données affichées dans cette fenêtre peuvent varier, selon le paramétrage appliqué.

4. Renseigner la **personne visitée** (si elle n'a pas été indiquée au préalable et si l'option est disponible).
5. Renseigner l'**accompagnant** du visiteur sur site (si elle n'a pas été indiquée au préalable et si l'option est disponible).

La définition d'un accompagnant de la visite n'est pas lié à la fonctionnalité escorte visiteur.

6. Compléter les différentes **informations** du visiteur et de la visite :

Lorsque les données de nom et prénom sont remplies manuellement, le champ nom est rempli en premier.



Les informations du visiteur peuvent être rédigés en écrivant sur chacun des champs éditables, ou pré-remplies à l'aide d'un lecteur de code-barres, qui doit avoir été connecté et paramétré au préalable (sélection du port COM).
Si le visiteur a une carte avec un code-barres, lire cette carte avec le lecteur de code-barres :
Les champs "Nom", "Prénom", "Nationalité", "Pièce d'identité" et "Date de naissance" seront remplis automatiquement.
Le champ "Société" devra être renseigné manuellement dans tous les cas.

Dans le cas de la création d'un visiteur avec un lecteur de document, suivre la procédure suivante:

a. Dans le paramétrage général, onglet identifiés, paramétrer le lecteur de document souhaité pour les visiteurs.
b. L'icône **lecteur de document** apparaîtra dans l'application de réception des visiteurs.
c. Cliquer sur l'icône et vérifier son passage au vert avant d'insérer une pièce d'identité dans le lecteur pour créer un nouveau visiteur.

Pour plus d'informations sur l'ajout d'un statut escorte au visiteur, consulter la section suivante : ???

7. **Attribuer un identifiant au visiteur :**

- Saisie manuelle
- Recherche parmis les identifiants réutilisables

- Enrôlement des identifiants

Pour plus d'informations sur le paramétrage de l'onglet visiteur, se référer à la section dédiée ???
Pour plus d'inforamtions sur l'envoi de l'identifiant QR code par mail au visiteur, se référer à la section dédiée ???

8. Attribuer des **accès** au visiteur :
   Cliquer sur l'onglet "Accès" pour naviguer dans la liste d'accès. Sélectionner les accès à attribuer au visiteur.
   Lorsque l'opérateur fait entrer le(s) visiteur(s), les accès assignés seront activés.
9. Mettre à jour l'**état** du visiteur :
   Faire entrer le visiteur ou placer le visiteur en attente (Visiteur enregistré mais en attente dans l'accueil visiteur du site).

10. Dans le cas où **plusieurs visiteurs** devraient être renseignés pour un même rendez-vous, procéder à l'enregistrement du visiteur suivant.
    Il est aussi possible d'annuler l'enregistrement d'un visiteur.
    Après avoir déclaré tous les visiteurs de la visite, faire entrer tous les visiteurs de la visite en changeant l'état de chacun des visiteurs.
11. Lors de l'entrée des visiteurs, une carte ou **bordereau de visite** peut être généré pour impression.
    Sélectionner l'option "**Enr & Imp**", le modèle d'impression à appliquer et le format à générer.

Gestion des visiteurs avec l'application de l'Accueil de visiteurs (Réception de visiteurs) et/ou de gestion des rendez-vous (WEBSESAME)

Les visiteurs doivent être **gérés exclusivement** avec l'application de l'Accueil de visiteurs (Réception de visiteurs) et/ou de gestion des rendez-vous (WEBSESAME).

Les visiteurs ne doivent pas être créés avec l'application de gestion des identifiés.

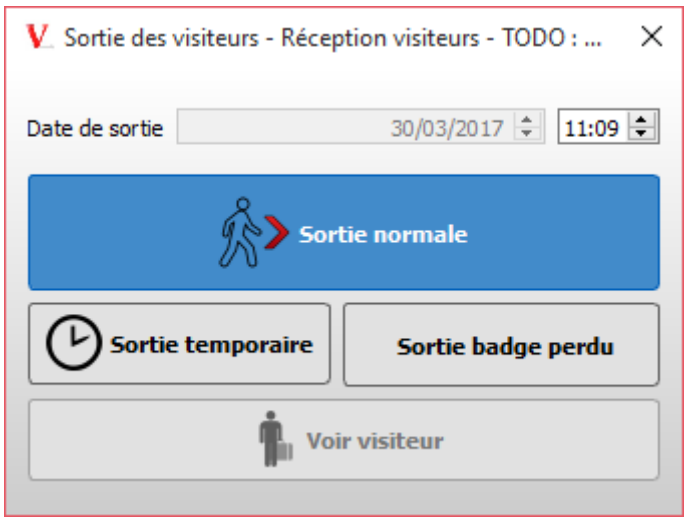
Si un visiteur est créé avec la gestion des identifiés, et que des accès sont assignés, ceux-ci seront supprimés par l'accueil visiteur.

8.5.5.3. Faire sortir un visiteur et terminer une visite

Plusieurs méthodes existent pour faire sortir un visiteur :

- Sélectionner le visiteur puis valider sa sortie avec l'icône **Sortie**.
- Dans une liste de visiteurs, cliquer droit sur les visiteurs sélectionnés puis **Faire sortir les visiteurs sélectionnés**.

Plusieurs types de sorties existent :



- Dans le cadre de la sortie d'un visiteur avec un identifiant attribué, le visiteur doit retourner l'identifiant à la zone de l'accueil visiteur. Dans ce cas, la sortie du visiteur sera enregistrée en tant que **sortie normale**

- Si l'identifiant n'est pas rendu à l'accueil (badge perdu, cassé, volé, non rendu) lors de la sortie du visiteur, l'option **sortie badge perdu** doit être utilisée.
- Si le visiteur souhaite quitter temporairement le site pour revenir plus tard, utiliser l'option **sortie temporaire**. Une fois que le visiteur a quitté temporairement le site, il doit être enregistré à nouveau à son retour. Sinon, uniquement les sorties normales et badge perdu seront disponibles pour ce visiteur.

Lors de la sortie du visiteur, un lecteur de cartes est nécessaire afin de restituer l'identifiant attribué au visiteur :

Présenter l'identifiant sur le lecteur de cartes puis utiliser une des options de sortie.

L'identifiant réutilisable deviendra à nouveau disponible. Dès sa restitution, il pourra être utilisé par un autre visiteur.

Avec l'option de sortie "sortie badge perdu", l'identifiant attribué n'est plus attribuable.

Les identifiants assignés aux visiteurs sont supprimés lorsque l'opérateur d'accueil fait sortir les visiteurs ("sortie normale", "badge perdu", "sortie temporaire"), ou lorsque l'heure de sortie est atteinte et uniquement si la case "Suppression des accès à l'heure de sortie" a été cochée lors de l'attribution des accès.

8.5.5.4. Gérer le statut du visiteur

Les visiteurs enregistrés auront des statuts différents en fonction de leur emplacement physique dans le site, la progression de sa visite, etc.

La gestion des visites est optimisée par le filtrage des visiteurs selon leur état.

La liste suivante contient les différents types de statuts qui peuvent être attribués à un visiteur.

L'icône **Accueil** permet de revenir à l'accueil, qui contient la liste de visiteurs et ses différents statuts.

- **Visiteurs attendus** : le visiteur pre-enregistré dans l'outil de gestion des rendez-vous. Le visiteur ne s'est pas encore présenté à l'accueil visiteur.
- **Visiteurs en attente** : le visiteur s'est déjà présenté à l'accueil sur site, mais le visiteur n'est pas entré sur site.

- **Visiteurs entrés** : le visiteur est enregistré et entré sur site. Il est possible d'enregistrer le visiteur simplement, ou d'enregistrer le visiteur ET d'imprimer une carte de visite.
- **Visiteurs sortis** : Après la visite, il est nécessaire de déclarer la sortie du visiteur. Plusieurs types de sorties sont possibles :
  - Sortie normale : Clôture de la visite en cours. Le visiteur disparaît de la liste des visiteurs enregistrés. L'identifiant visiteur est à nouveau disponible (en cas d'identifiant réutilisable).
  - Sortie temporaire : Une fois que le visiteur a quitté temporairement le site, il doit être enregistré à nouveau à son retour.
  - Sortie badge perdu : Le visiteur termine la visite sur site, mais son identifiant n'est pas rendu (carte perdue, non-rendu, cassée, volée). La visite en cours est clôturée. Le visiteur disparaît de la liste des visiteurs enregistrés. L'identifiant attribué n'est plus attribuable.
- **Visite dépassée** : Lorsque l'heure prévue de fin de visite est dépassée, et si le visiteur n'a pas quitté le site, une alarme s'affiche et une icône signale le dépassement

8.5.5.5. Personnaliser et générer des documents

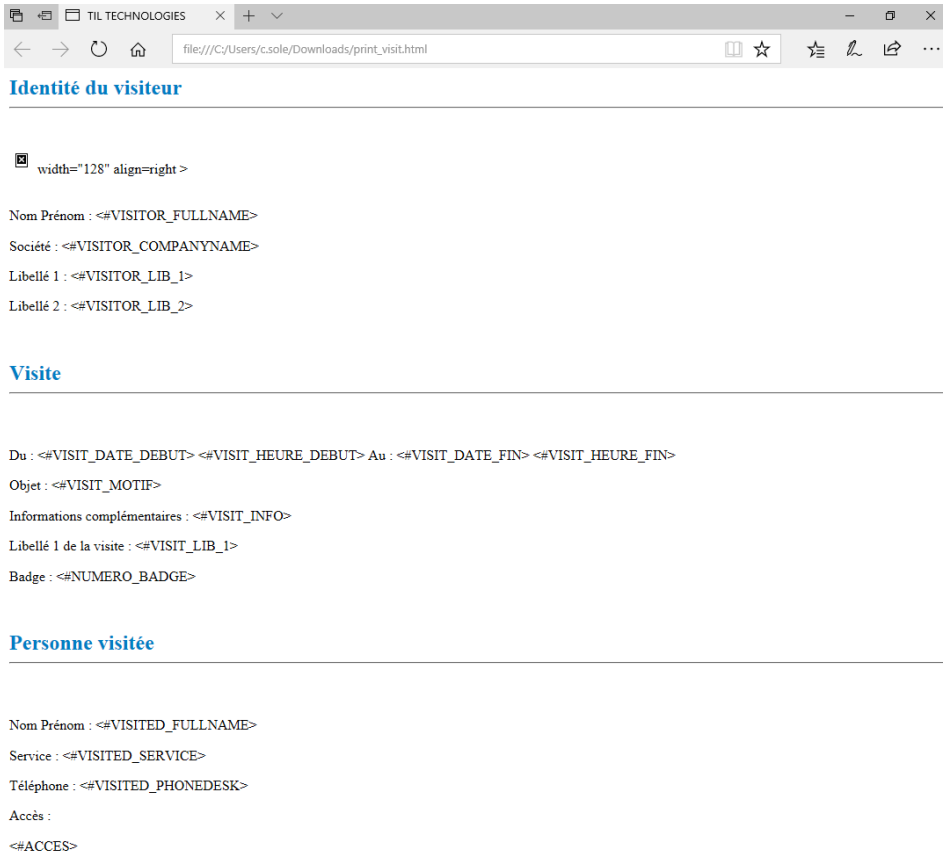
Plusieurs types de documents peuvent être émis dans le cadre de la gestion des visites :

- une **carte de visite** (Impression d'un badge éphémère, impression d'un badge visiteur, impression d'un badge visiteur réutilisable).
- un **bordereau de visite** (Création d'un bordereau à imprimer ou d'un bordereau à fournir en format PDF).
- une **liste de visiteurs** sur site peut être générée.

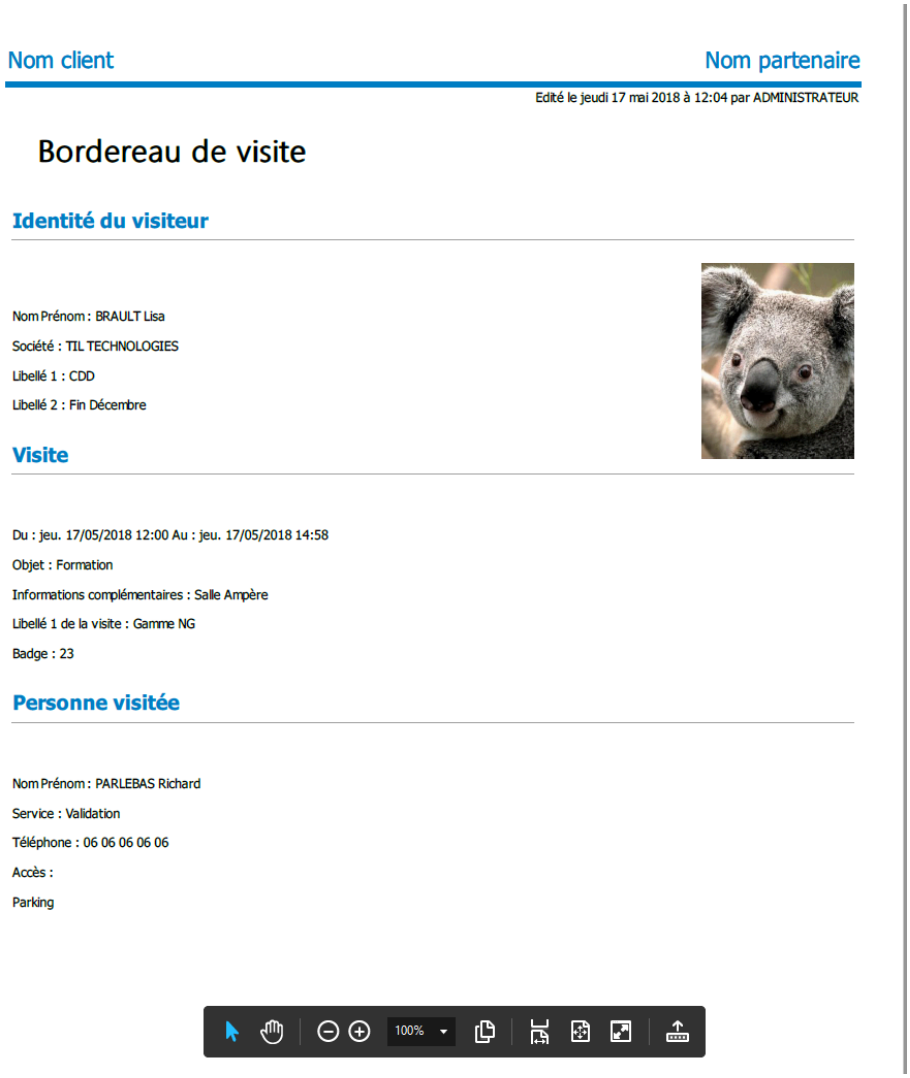
Pour **personnaliser des cartes de visite imprimables**, utiliser le fichier **visit.dfc** qui est créé dans le répertoire VISIT du répertoire de travail de MICROSESAME(Par exemple, C:\MICROSESAME/CONFIG). Ce fichier visit.dfc contient un modèle de carte prédéterminé. Des modèles personnalisés peuvent être crées avec l'Éditeur de fond de cartes (Consulter la documentation dédiée pour plus de détails). Plusieurs modèles de cartes peuvent être stockés dans ce répertoire.

Pour **personnaliser les bordereaux de visite imprimables**, utiliser le fichier **print_visit.htm** qui est créé dans le répertoire VISIT du répertoire de travail de MICROSESAME(Par exemple, C:\MICROSESAME/CONFIG/VISIT/print_visit.html)).

Ce fichier print_visit.html contient un modèle qui peut être personnalisé :



Il est possible de créer différents modèles et les stocker dans ce répertoire. Ci-dessous un exemple de bordereau de visite personnalisé :



Nom client Nom partenaire

Edité le jeudi 17 mai 2018 à 12:04 par ADMINISTRATEUR

Bordereau de visite

Identité du visiteur

Nom Prénom : BRAULT Lisa
Société : TIL TECHNOLOGIES
Libellé 1 : CDD
Libellé 2 : Fin Décembre

Visite

Du : jeu. 17/05/2018 12:00 Au : jeu. 17/05/2018 14:58
Objet : Formation
Informations complémentaires : Salle Ampère
Libellé 1 de la visite : Gamme NG
Badge : 23

Personne visitée

Nom Prénom : PARLEBAS Richard
Service : Validation
Téléphone : 06 06 06 06 06
Accès :
Parking

100%

Les bordereaux de visite personnalisés peuvent contenir les champs suivants :

- Nom du visiteur (VISITOR_FULLNAME)
- Nom de la société (VISITOR_COMPANYNAME)
- Libellés personnalisables 1 à 16 pour le visiteur (VISITOR_LIB_1 à VISITOR_LIB_16)
- Photo du visiteur (VISITOR_PHOTO)
- Nom de la personne visitée (VISITED_FULLNAME)
- Téléphone de la personne visitée (VISITED_PHONEDESK)
- Service de la personne visitée (VISITED_SERVICE)

- Date de début de la visite (VISIT_DATE_DEBUT)
- Date de fin de la visite (VISIT_DATE_FIN)
- Heure de début de la visite (VISIT_HEURE_DEBUT)
- Heure de fin de la visite (VISIT_HEURE_FIN)
- Motif de la visite (VISIT_MOTIF)
- Information de la visite (VISIT_INFO)
- Libellés personnalisables 1 à 10 pour la visite (VISIT_LIB_1 à VISIT_LIB_10)
- Numéro d'identifiant du visiteur (NUMERO_BADGE)
- Les accès du visiteur (ACCES)

Pour créer des **listes de visiteurs**, sélectionner les filtres nécessaires avec les options **Filtre rapide** et **Filtres** depuis la fenêtre de l'Accueil des visiteurs.

Les résultats de la recherche, affichés à droite, seront exportés dans une liste.

Ces listes de visiteurs peuvent être exportées en différents formats : txt, csv, pdf.

Afin de pouvoir imprimer les documents générés, vérifier les paramètres liés au mode d'impression :

1. Cliquer sur **Afficher les paramètres**.
2. Dans la fenêtre Paramètres, indiquer l'**imprimante de cartes** qui sera utilisée (si des cartes de visite sont fournies aux visiteurs).
3. Dans la fenêtre Paramètres, indiquer le **modèle d'impression** qui sera utilisé (si des bordereaux de visite sont fournis aux visiteurs).

8.5.6. Cas d'usage

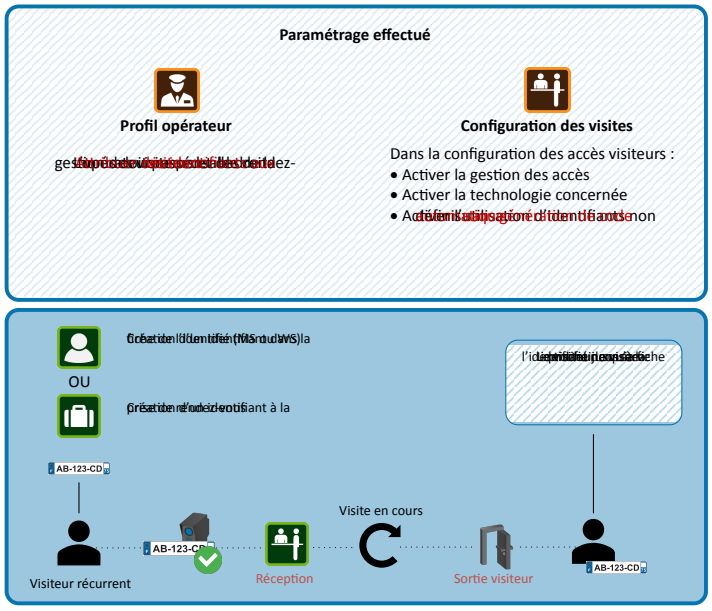
8.5.6.1. Assigner un identifiant conservable (conservation de l'identifiant après sortie visiteur)

Contexte :

- On souhaite enregistrer la plaque d'immatriculation d'un visiteur récurrent comme identifiant conservable.
- L'identifiant conservable assigné à l'identifié ne sera pas supprimé à la sortie du visiteur, celui-ci sera toujours valide.
- L'identifiant (immatriculation) n'est pas réutilisable.

A la sortie du visiteur, l'identifiant reste valide mais l'identifié n'est plus valide dés la fin de la visite. L'autorisation d'accès sera donc de nouveau possible à la création d'un prochain rendez-vous.

Figure 8.5. Conservation de l'identifiant après la sortie du visiteur



Pour les visiteurs, MICROSESAME **ne supporte pas** l'assignation de multiples identifiants dans une même technologie.

A la réception du visiteur, l'identifiant conservable est automatiquement recopié dans le champ associé de la technologie configurée.

NE PAS MODIFIER le code identifiant dans la fiche d'enregistrement.

8.6. La borne d'annonce visiteur

8.6.1. Mode de fonctionnement

La borne d'annonce visiteur permet de mettre un visiteur **en attente** et de le **signaler** au visité, suite à un **rendez-vous** (déclaré au préalable sur WEBSESAME) ou lors d'une **visite** inopinée (visite qui n'était pas planifiée sur WEBSESAME).

8.6.2. Utilisation de la borne

8.6.2.1. Lecture du code

Suite à l'enregistrement du rendez-vous, un **QR code** ou un **code barres** peut être envoyé au visiteur. Le visiteur peut présenter ce code à la borne. Il est possible de saisir le code à l'aide du **clavier tactile**.

La lecture du code permettra de retrouver la visite planifiée et passer à l'étape suivante.

Afin d'éviter des fausses manipulations, le bouton "Suivant" n'est pas affiché si le clavier est affiché sur l'écran.

Pour visualiser le bouton "Suivant", quitter le mode clavier.

8.6.2.2. Enregistrer les données du visiteur

Par défaut, seulement le champ **Nom** est obligatoire pour l'enregistrement d'un visiteur. Autres champs peuvent être obligatoires pour l'enregistrement du visiteur, en fonction du paramétrage appliqué. Les champs obligatoires sont entourés en rouge.

Si certaines données sont déjà connues du système, elles sont proposées en auto-complétion.

L'enregistrement est finalisé lorsque l'utilisateur appuie sur le bouton "Terminer".

Les pages contenant des données sur les personnes visitées/visiteurs (Déclaration de visite, récapitulatif visite/rendez-vous) seront fermées automatiquement après 30 secondes d'inactivité, si la page n'a pas été fermé avant par l'utilisateur. Cela évite l'affichage d'informations à personnes non concernées.

8.6.2.3. Envoyer la notification à la personne visitée et accueil physique

L'arrivée du visiteur est annoncé au visité par email (selon le paramétrage appliqué, voir "Mails").

La visite s'affiche dans le logiciel de l'accueil de visiteurs.

8.6.3. FAQ

Problème	Solution
La borne reste bloquée sur la fenêtre de login. Hôte inconnu.	• Absence ou problème de port, vérifier sesame.cfg.

Problème	Solution
	• Borne sans connexion au réseau: Fermer la fenêtre du login, la borne tentera de se reconnecter.
Tous les identifiés permanents visitables sont visibles sur la borne. Certains identifiés ne doivent pas être affichés sur la borne.	• Le paramétrage des personnes visitables non visibles sur la borne n'a pas été réalisé. • Paramétrer les personnes visitables non visibles sur la borne, voir "Personnes visitables non visibles sur la borne".

8.7. Gestion des habilitations

8.7.1. Généralités

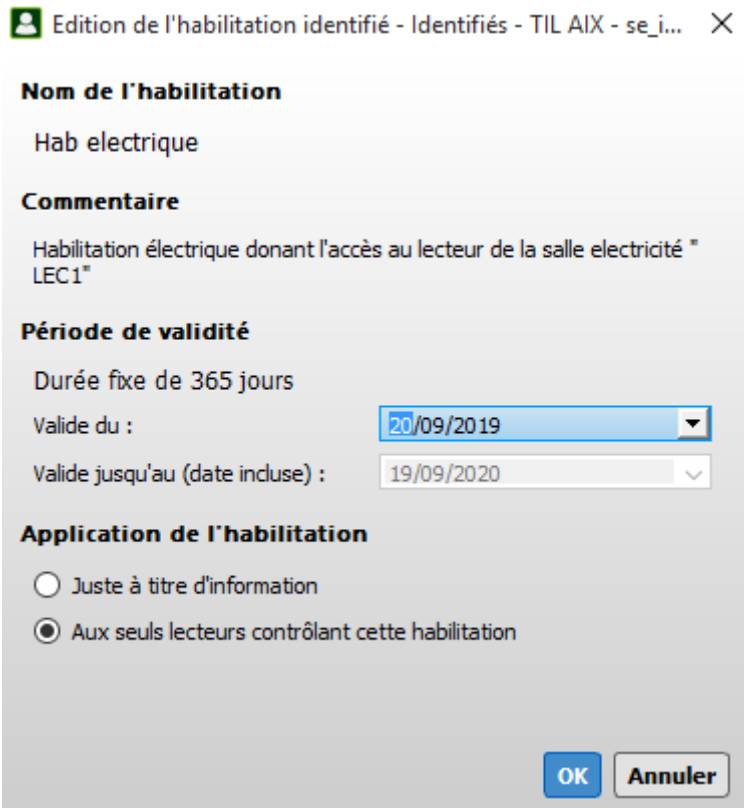
La fonctionnalité **Habilitations** de MICROSESAMEa pour objectif de compléter la gestion des autorisations d'accès qui s'appliquent aux identifiés avec le paramétrage du contrôle d'accès.

Cette fonctionnalité permet la mise en place de différents types d'habilitations, qui correspondent à des **obligations spécifiques**, de plusieurs types :

- Connaissances techniques (diplômes, certifications, habilitations techniques,...)
- Connaissance de l'entreprise (Plans de prévention, passeport professionnel, autorisation spécifique,...)
- Suivi médical (Visites périodiques, relevé de dosimètre,...) , etc.

8.7.2. Associer une habilitation à un identifié

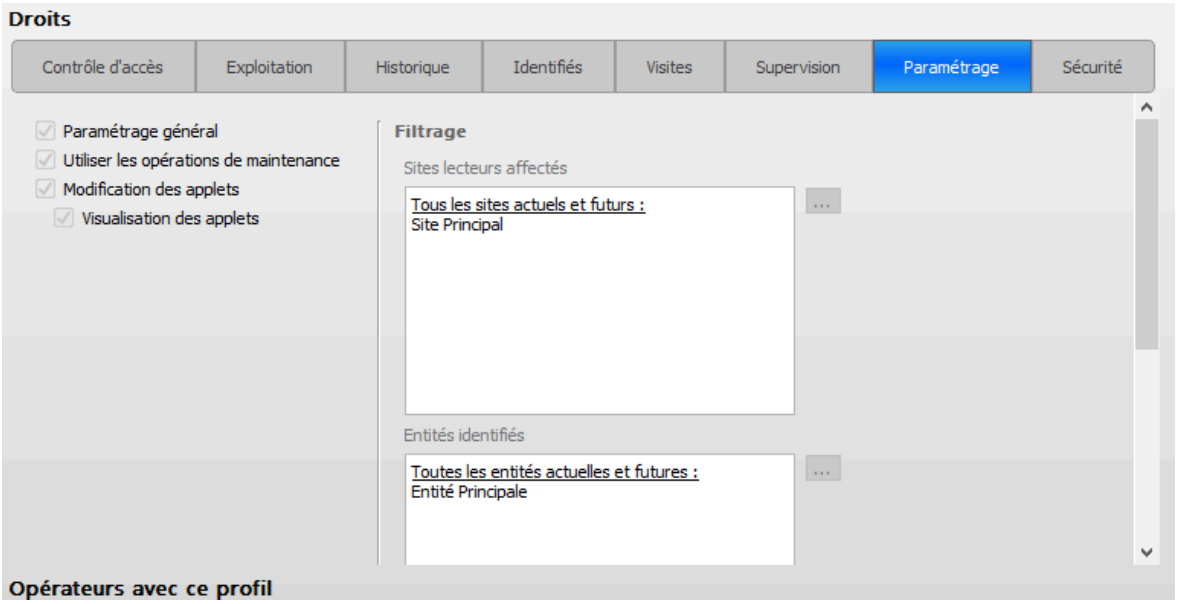
1. Dans la fiche identifié (Exploitation > Contrôle d'accès) de la personne concernée, aller à l'onglet **Habilitations**.
2. Rechercher l'habilitation à attribuer à l'identifié dans le tableau de droite.
3. Utiliser la flèche bleue pour la sélectionner. Les habilitations attribuées passent dans le tableau de gauche.
4. Lors de l'ajout de l'habilitation, la fenêtre **Édition de l'habilitation identifié** s'affiche. Indiquer le fonctionnement voulu puis cliquer "OK" pour fermer cette fenêtre. Enregistrer la fiche identifié pour sauvegarder les modifications réalisées.



8.7.3. Attribution des droits opérateurs

Pour accéder à la fenêtre de paramétrage des profils opérateurs suivre **Profils opérateurs > Paramétrage > Système**.

Le droit nécessaire pour l'opérateur chargé des habilitations est **Paramétrage > Paramétrage général**.



Sans ce droit, l'opérateur n'a pas accès à la fenêtre permettant la création et le paramétrage des habilitations.

Lors que les habilitations sont disponibles, l'onglet **Habilitations** est affiché dans la fiche identifié pour ajout/suppression d'habilitations (L'opérateur doit avoir un droit opérateur classique de gestion des identifiés).

8.7.4. Cas d'usage

8.7.4.1. Objectif et résultat

Cet exemple décrit :

1. la création d'une habilitation électrique dans MICROSESAME.
2. le paramétrage des lecteurs concernés par cette habilitation.
3. l'affectation de l'habilitation aux identifiés concernés par cette habilitation.

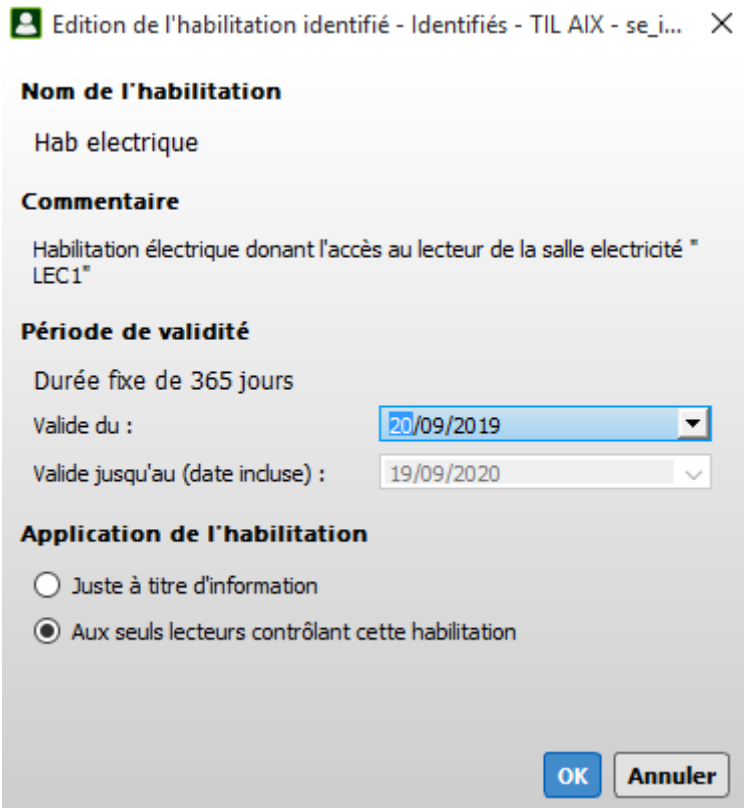
Cet exemple a comme résultat :

1. l'autorisation de l'identifié au lecteur associé à l'habilitation.
2. lors que l'identifiant de l'identifié concerné est détecté sur le lecteur, l'accès est autorisé.
3. les identifiés n'ayant pas cette habilitation (déclarée depuis la fiche identifié) obtiennent un accès refusé.

Ce type d'information sera affichée dans le Moniteur d'évènements et/ou l'Historique.

8.7.4.2. Associer l'identifié et l'habilitation

1. Dans la fiche identifié de la personne concernée (Exploitation > Contrôle d'accès > Identifiés), aller à l'onglet **Habilitations**.
2. Rechercher l'habilitation à attribuer à l'identifié dans le tableau de droite.
3. Utiliser la flèche bleue pour la sélectionner. Les habilitations attribuées passent dans le tableau de gauche.
4. Lors de l'ajout de l'habilitation, la fenêtre **Édition de l'habilitation identifié** s'affiche. Pour limiter l'accès de l'identifié aux lecteurs contrôlant l'habilitation, sélectionner l'option.
5. Cliquer "OK" pour fermer cette fenêtre.
6. Enregistrer les modifications effectuées dans la fiche identifié pour qu'elle soient prises en compte correctement. Les données sont téléchargées de façon automatique depuis la fiche identifié.



8.8. Gestion des ascenseurs

La **TILLYS** permet la gestion des ascenseurs avec MICROSESAME

La gestion des ascenseurs est associée à un paramétrage spécifique, permettant de considérer chaque étage comme un accès lecteur. L'attribution de ces étages se fait depuis les interfaces de gestion des droits d'accès, au même titre qu'une porte classique. Les étages peuvent donc être intégrés aux profils d'accès.

Pour cette fonction, La TILLYS peut gérer 2 lecteurs "cabine ascenseur" et jusqu'à 63 étages ou groupes d'étages par ascenseur

Chapitre 9. Paramétrage

9.1. Mise en exploitation du paramétrage

9.1.1. Accéder à l'application d'application du paramétrage

Suite au paramétrage des différents éléments de l'installation (logiciel ou matériel), il est indispensable de réaliser une opération finale de mise en exploitation.

Cette opération permet d'appliquer les changements effectués au paramétrage et de les télécharger sur le matériel de l'installation (TILLYS, bornes...).

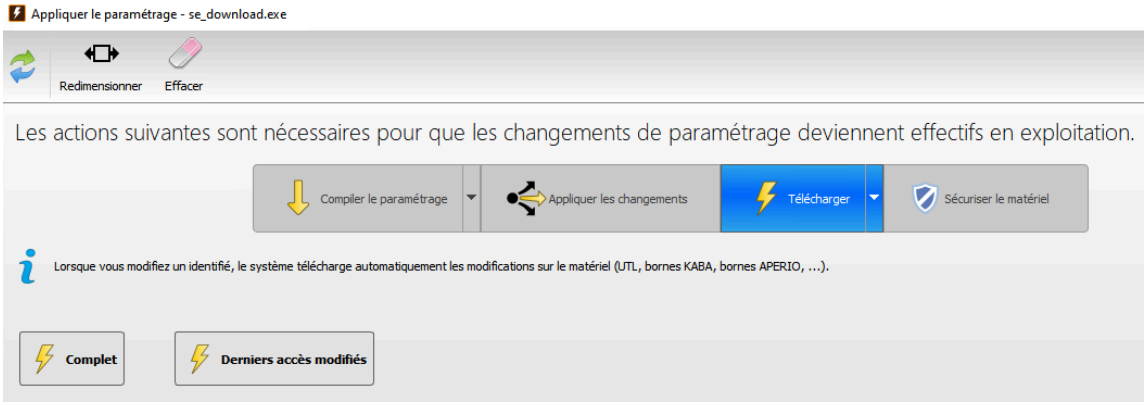
Pour accéder à l'application **Appliquer le paramétrage** suivre Paramétrage > Mise en exploitation > Appliquer le paramétrage.

9.1.2. Télécharger

L'onglet **Télécharger** est affiché par défaut à l'ouverture de la fenêtre.

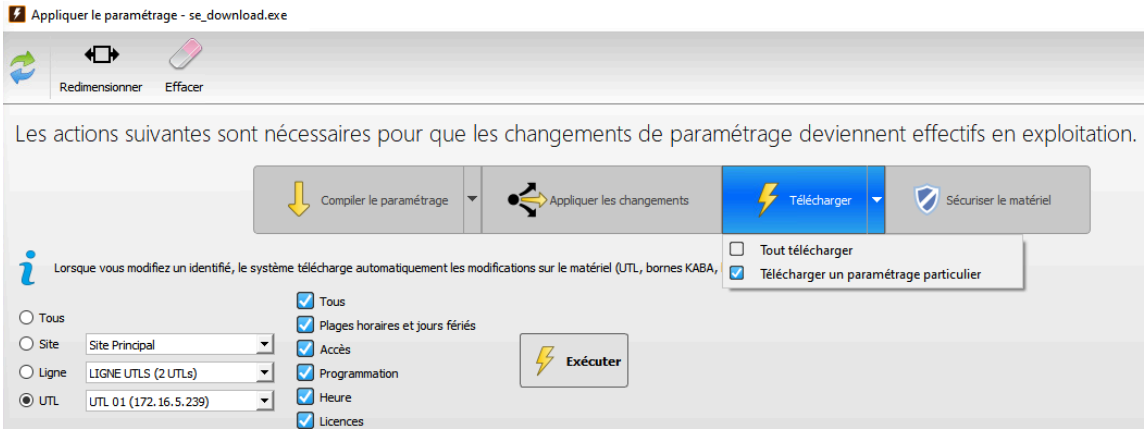
Afin que les changements deviennent effectifs en exploitation (par exemple, modification des identifiés) , le système devra télécharger les modifications sur le matériel.

- **Tout télécharger** : Un téléchargement **complet** (de tous les éléments) ou seulement des **derniers accès modifiés**peut être effectué.

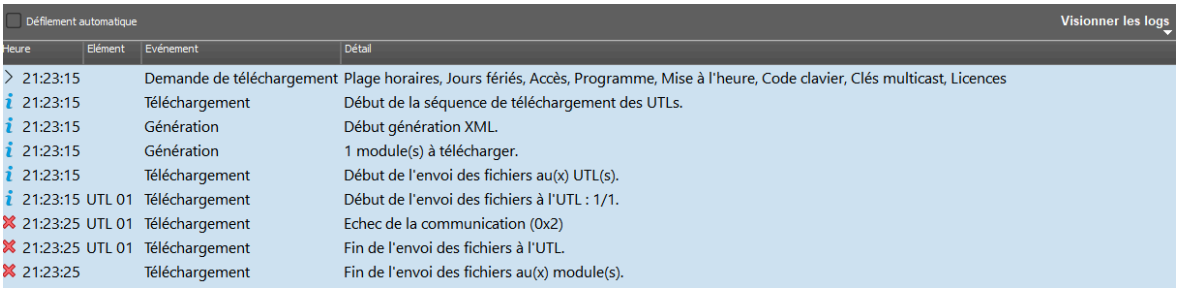


- **Télécharger un paramétrage en particulier** : Plusieurs options de téléchargement sont disponibles.
  - Plages horaires et jours fériés
  - Accès
  - Programmation
  - Heure
  - Licences (**Téléchargement des licences** seulement applicable aux **TILLYS CUBE**).

  Cliquer **Exécuter** pour procéder au téléchargement.



La partie inférieure de la fenêtre permet de consulter les évènements liés au téléchargement (opérations réalisée, erreurs de téléchargement...).



Cocher **Défilement automatique** pour visualiser les évènements en temps réel.

Cliquer sur **Visionner les logs** pour afficher l'application **Visionneuse de logs**.

Chapitre 10. Passerelles

10.1. Connecteur armoires Deister

10.1.1. Généralités

Cette passerelle est dédiée à l'interfaçage avec les **armoires à clés** DEISTER de type PROXSAFE. Ce connecteur permet d'effectuer les opérations suivantes directement depuis un poste client / serveur MICROSESAME :

- Déclarer le serveur et importer le matériel DEISTER dans la configuration MICROSESAME.
- Assigner les droits d'utilisation des armoires DEISTER depuis la fiche d'un identifié.
- Superviser les évènements relatifs aux armoires DEISTER et aux KeyTags depuis MICROSESAME
- Passer des télécommandes aux armoires DEISTER depuis MICROSESAME.

Le terme KeyTag réfère à un porte-clé RFID qui peut être rangé de manière sécurisée au sein de l'armoire.

Les éléments rattachés aux Keytags peuvent être de différents types:

- Clés
- Trousseau de clé
- Badge
- ...

Pour éviter toute confusion, seul le terme KeyTag sera utilisé dans cette documentation.

La remontée des évènements et la transmission de télécommandes aux objets de supervision DEISTER sont conditionnées par l'activation d'une licence LIC-PROXSAFE par keyTag à superviser.

A partir de la version 2023 de MICROSESAME, l'assignation des accès aux keytags est gérée nativement par MICROSESAME, de même les identifiants dédiés à l'exploitation des armoires sont téléchargés directement au serveur DEISTER.

L'ensemble des échanges s'opère de serveur à serveur via une connexion Ethernet.

Cette section traite uniquement du paramétrage et de l'exploitation de la passerelle côté MICROSESAME.

10.1.2. Assigner les droits d'accès aux identifiés

A partir de la version 2023 de MICROSESAME, l'assignation des keytags ou groupe de keytags est gérée nativement par MICROSESAME.

Tableau 10.1. Chronologie des étapes pour la gestion des accès DEISTER

N°	Etape	Interface	Détails
1	Déclaration des équipements	proxSafe®	Déclarer les armoires, keytags, groupes de keytags directement dans Proxsafe.
2	Import des équipements	MICROSESAME CUBE	Imports des éléments DEISTER dans MICROSESAMEdepuis l'interface de paramétrage DEISTER
3	Création des identifiés	MICROSESAME CUBE WEBSESAME CUBE	La création d'identifiés susceptibles d'utiliser les équipements DEISTER se fait directement dans la gestion des identifiés depuis MICROSESAME ou WEBSESAME.
3	Assignation des identifiants DEISTER	MICROSESAME CUBE WEBSESAME CUBE	L'assignation des identifiants DEISTER se fait directement dans la gestion des identifiés depuis MICROSESAMEou WEBSESAME.  Ajouter les identifiants pour la technologie définie dans l'interface de paramétrage DEISTER.
4	Assignation des accès DEISTER	MICROSESAME CUBE WEBSESAME CUBE	L'assignation des accès aux keytags et groupes de keytags se fait directement

N°	Etape	Interface	Détails
			dans la gestion des identifiés depuis MICROSESAME ou WEBSESAME. Dans MICROSESAME il est nécessaire d'afficher les keytags et groupes de keytags pour les assigner. Effectuer un clic-droit puis afficher les accès ou groupes d'accès correspondant. L'assignation des accès DEISTER supporte uniquement la plage horaire 24h/24 et ceux-ci ne peuvent avoir de dates de validité.

10.1.3. Générer des rapports sur les Keytags non retournés

MICROSESAME intègre par défaut une requête permettant de générer un rapport des Keytags non retournés.

Ce rapport présente les informations suivantes:

- Keytag non rendu

- Objet de supervision associé
- Date / heure du retrait du keytag
- Id de l'identifié à l'origine de l'opération de retrait
- Nom et prénom de l'identifié à l'origine de l'opération de retrait

Pour générer ce rapport, suivre la procédure suivante:

1. Depuis MICROSESAME se rendre dans l'onglet rapports du paramétrage général.
2. Activer l'automate des rapports.
3. Se connecter à WEBSESAME.
4. Se rendre dans l'onglet **Rapport > Générer**.
5. Sélectionner le rapport mentionné et cliquer sur valider.
6. Télécharger le rapport.

Pour plus d'informations sur la génération et la consultation des rapports, se référer au chapitre dédié de l'aide en ligne:

Partie 10: Journaux

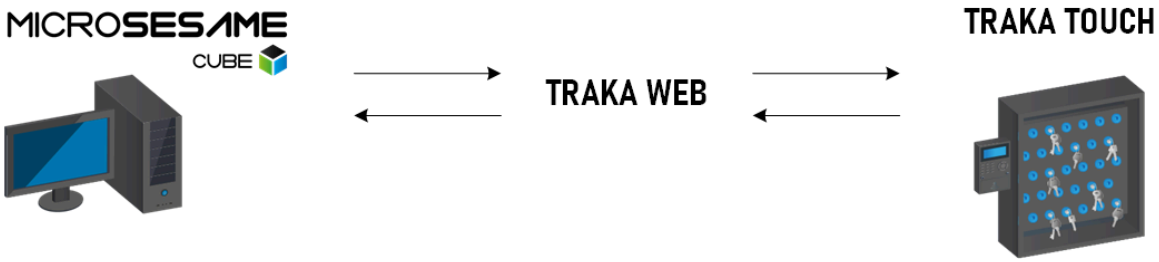
Chapitre 4: Rapports

10.2. Connecteur armoires à clé TRAKA

10.2.1. Généralités

Cette passerelle est dédiée à l'interfaçage entre MICROSESAME et le système d'armoire à clefs "TRAKA", ce connecteur échange des données par API avec le serveur "TRAKA WEB" et permet d'effectuer les opérations suivantes :

- Télécharger les identifiés avec leur identifiant badge, ainsi que leur droits d'accès aux objets de l'armoire depuis la fiche identifié MICROSESAME
- Superviser les évènements relatifs aux armoires "TRAKA" ainsi qu'aux objets qu'elles contiennent depuis les applications de supervision de MICROSESAM



1. Pour que la passerelle "TRAKA" soit fonctionnelle, il est nécessaire de posséder la licence MICROSESAME suivante : "LIC-TRAKA"

2. Seulement l'authentification par badge est géré entièrement depuis MICROSESAME, dans le cas où la fonctionnalité d'authentification par code clavier doit être utilisée, les codes seront à configurer dans le logiciel "TRAKA WEB" après un téléchargement des identifiés depuis MICROSESAME.

10.2.2. Gérer les identifiés et les accès aux objets des armoires "TRAKA"

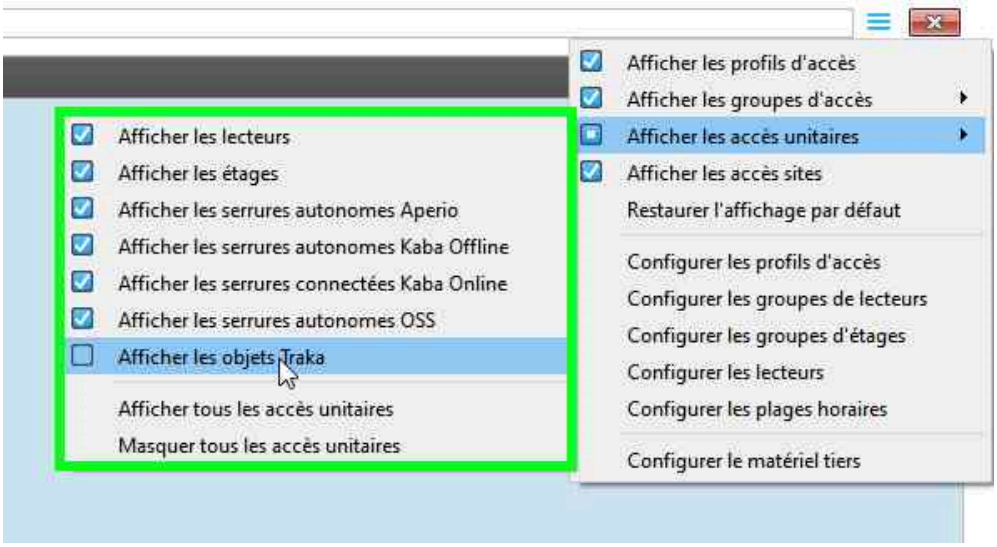
Pour pouvoir télécharger des accès à des identifiés aux différents objets des armoires "TRAKA", il est nécessaire :

- De créer l'identifié
- D'attribuer un identifiant à l'identifié
- D'attribuer l'accès aux objets de l'armoire

Pour cela :

1. Ouvrir l'application "Gestion des identifiés" de MICROSESAME : Menu MICROSESAME > exploitation > contrôle d'accès > identifiés
2. Cliquer sur le bouton "Nouveau" pour créer un nouvel identifié , ou, sélectionner un identifié déjà existant
3. Dans l'onglet "Accès" de la fiche identifié, cliquer sur le bouton "ajouter un nouvel accès", sélectionner l'accès à un des objets/groupe d'objets "TRAKA" et cliquer sur "ajouter"

Il se peut que les accès aux objets/Groupes d'objet TRAKA ne soient pas visible, si tel est le cas :
cliquer sur le bouton de filtres des accès, puis dans "afficher les accès unitaire" et "afficher les groupes d'accès", cocher les case correspondante aux objet TRAKA,



4. Dans l'onglet "identifiants" ajouter manuellement ou en utilisant un enrôleur l'identifiant du badge qui sera utilisé par l'identifié
5. Sauvegarder pour que les changements soient automatiquement téléchargés

Il est possible de télécharger une configuration complète des accès ou seulement les derniers changements effectué si nécessaire (après une coupure réseau lors des changements ... etc). Pour cela :

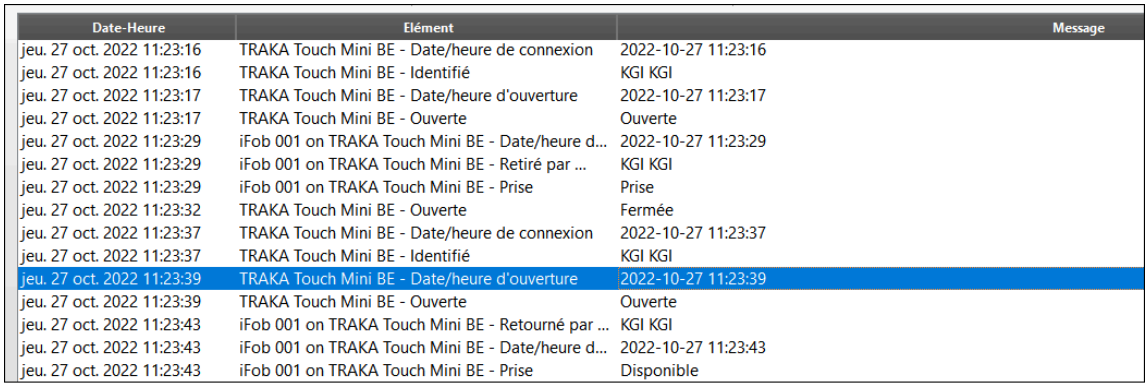
- Ouvrir le paramétrage général traka : menu MICROSESAME > paramétrage > gestion des clés > traka
- se placer dans l'onglet "serveur", effectuer un clic droit sur le serveur et cliquer sur "téléchargement complet" ou " téléchargement des derniers changements"

10.2.3. Moniteur d'évènements

Il est possible de superviser les évènements liés à l'armoire et aux différents objets qui la compose depuis l'application "moniteur d'évènement" de MICROSESAME: Menu MICROSESAME > Exploitation > Supervision > Moniteur d'évènements

Cette application contient 3 onglets

- Fil de l'eau : Cet onglet permet de voir les évènements du site au fur et à mesure qu'ils se réalisent.
  Par défaut, les évènements liés au système TRAKA n'apparaissent pas dans cet onglet, pour pouvoir voir ces évènements, il est nécessaire dans le paramétrage des propriétés de configurer le paramètre "visible dans le fil de l'eau" à la valeur "oui"



Date-Heure	Elément	Message
jeu. 27 oct. 2022 11:23:16	TRAKA Touch Mini BE - Date/heure de connexion	2022-10-27 11:23:16
jeu. 27 oct. 2022 11:23:16	TRAKA Touch Mini BE - Identifié	KGI KGI
jeu. 27 oct. 2022 11:23:17	TRAKA Touch Mini BE - Date/heure d'ouverture	2022-10-27 11:23:17
jeu. 27 oct. 2022 11:23:17	TRAKA Touch Mini BE - Ouverte	Ouverte
jeu. 27 oct. 2022 11:23:29	iFob 001 on TRAKA Touch Mini BE - Date/heure d...	2022-10-27 11:23:29
jeu. 27 oct. 2022 11:23:29	iFob 001 on TRAKA Touch Mini BE - Retiré par ...	KGI KGI
jeu. 27 oct. 2022 11:23:29	iFob 001 on TRAKA Touch Mini BE - Prise	Prise
jeu. 27 oct. 2022 11:23:32	TRAKA Touch Mini BE - Ouverte	Fermée
jeu. 27 oct. 2022 11:23:37	TRAKA Touch Mini BE - Date/heure de connexion	2022-10-27 11:23:37
jeu. 27 oct. 2022 11:23:37	TRAKA Touch Mini BE - Identifié	KGI KGI
jeu. 27 oct. 2022 11:23:39	TRAKA Touch Mini BE - Date/heure d'ouverture	2022-10-27 11:23:39
jeu. 27 oct. 2022 11:23:39	TRAKA Touch Mini BE - Ouverte	Ouverte
jeu. 27 oct. 2022 11:23:43	iFob 001 on TRAKA Touch Mini BE - Retourné par ...	KGI KGI
jeu. 27 oct. 2022 11:23:43	iFob 001 on TRAKA Touch Mini BE - Date/heure d...	2022-10-27 11:23:43
jeu. 27 oct. 2022 11:23:43	iFob 001 on TRAKA Touch Mini BE - Prise	Disponible

- Alarmes : Cet onglet permet de voir les propriétés définis en "alarmes" et dont la valeur est égale à celle défini dans le paramètre "valeur de déclenchement" dans l'application "gestion des objets et propriétés" de MICROSESAME
- Propriétés : Cet onglet permet d'effectuer une recherche parmi toutes les propriétés existante afin d'analyser toutes les informations en temps réel liées à ces dernières.

10.2.4. Synoptique - symboles TRAKA

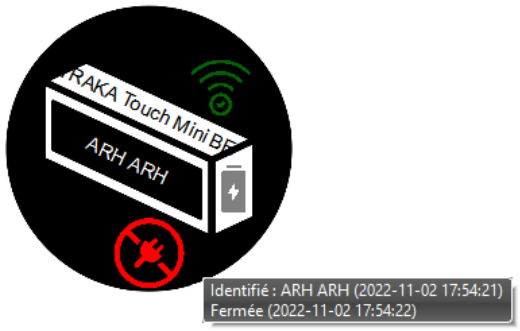
Il est aussi possible de superviser les éléments TRAKA de manière graphique par le biais de l'application "Animateur des Synoptiques"

Pour cela 3 symboles qui seront animés dynamiquement en fonction de l'état des propriétés sont mis à disposition depuis l'éditeur de synoptique

Le symbôle "trakaItem"

	position de l'objet dans l'armoire
	nom du dernier identifié ayant retiré l'objet + date de l'évènement
	nom du dernier identifié ayant retourné l'objet + date de l'évènement
	objet pris
	retour incorrect (rouge fixe)
	horaire dépassée (rouge clignotant)
	retrait inattendu (rouge clignotant)

Le symbôle "trakaCabinet"

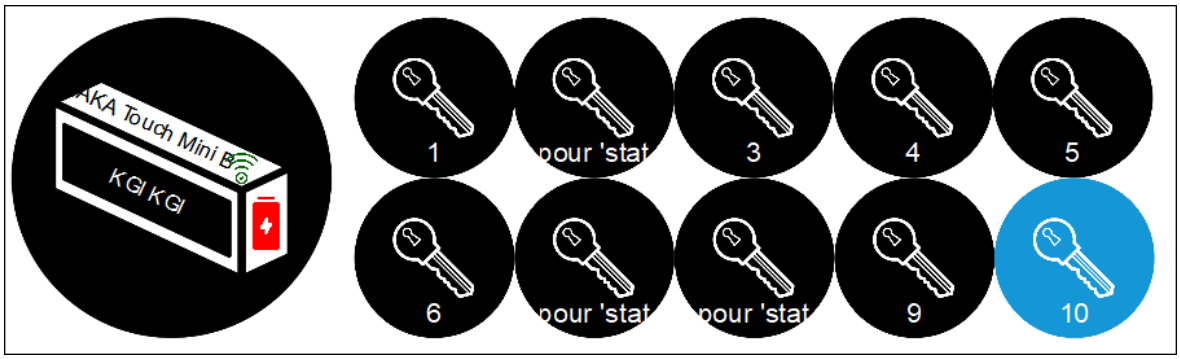
Symbôle : "traka cabinet"	
	État de vec le serveur
	uvert l'armoire
	État de l'alimentation sur secteur

Symbôle : "traka cabinet"	détails animation
	Porte de service ouverte
	Porte ouverte trop longtemps
	Arrachement
	Ouverture inattendue

Le symbôle "trakaCabinet"

Ce symbole anime l'armoire et toutes les clés qui la compose, il réunit donc le symbole "trakaCabinet" et tous les symboles "trakaItem" liés aux objets de l'armoire.

Le fonctionnement de chaque élément est comme décrit précédemment



10.2.5. Historique

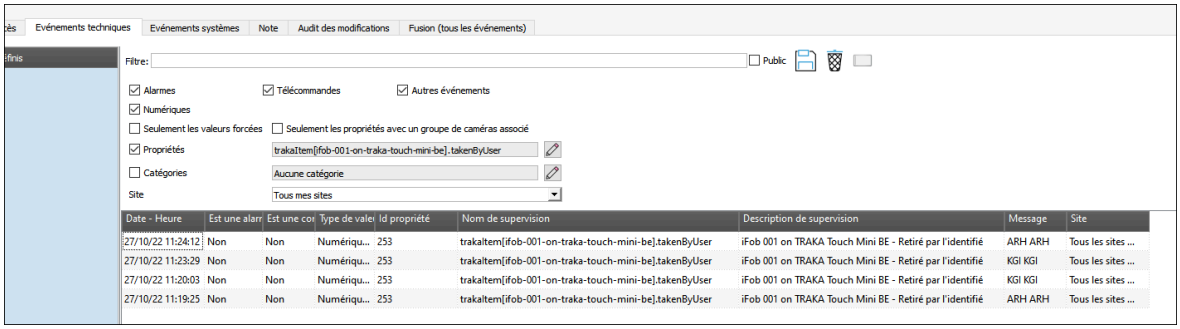
L'application "Historique" de MICROSESAME permet d'effectuer des recherches parmi tous les évènements qui se sont déroulés sur MICROSESAME (passage de badges, assignations d'accès, création d'identifiés ... etc), les deux onglets qui devront être utilisé pour rechercher les informations à propos du système TRAKA sont les suivants :

- onglet "Évènements technique"
- onglet "Audit des modifications"

c'est depuis l'onglet "évènements technique" que tous les évènements liés aux propriétés au système TRAKA pourront être trouvés (état d'ouverture d'une armoire, état de disponibilité d'un objet... etc).

Il sera donc possible d'effectuer des recherches précises comme par exemple :

- Réaliser une liste de tous les porteurs qu'a pu avoir un objet (filtre sur la propriété : <NomObjet>.takenByUser)
- Réaliser une liste des identifiés qui se sont authentifiés sur une armoire spécifique
- ... etc



C'est depuis l'onglet "Audit des modifications" que pourront être recherché des informations sur l'historique de configuration du système TRAKA (assignation d'accès, import d'une configuration d'une armoire ... etc).

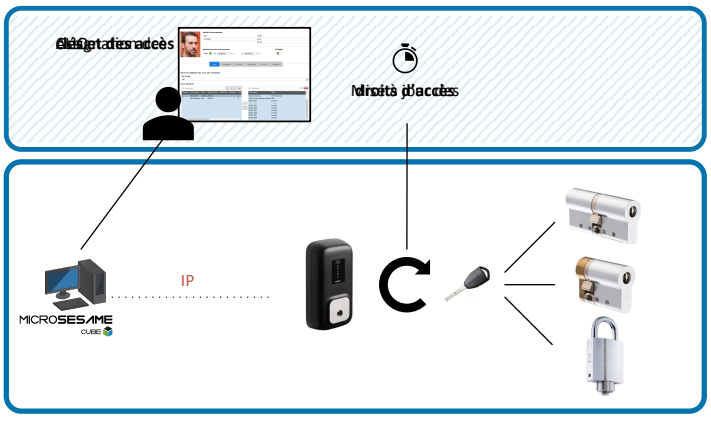
10.3. Connecteur CLIQ Abloy

10.3.1. Généralités

Cliq Abloy est un système de contrôle d'accès sur serrures mécatroniques mêlant clés physiques et puces RFID.

Les cylindres et serrures CLIQ sont chacun soumis à une licence MICROSESAME.

Figure 10.1. Fonctionnel CLIQ avec MICROSESAME



MICROSESAME intègre une interface permettant de gérer les éléments suivants directement depuis ses applications d'exploitation :

- Gestion des identifiés ayant accès aux serrures CLIQ
- Gestion des accès aux serrures CLIQ (par cylindres et groupes de cylindres)

- Gestion de la distribution des clés CLIQ (identifiants)
- Gestion de la validité des accès et des identifiés
- Supervision des boitiers et bornes de programmation CLIQ avec des objets de supervision
  - Etat de la borne
  - Date/heure de la dernière connection
  - mode (online / updater)
- Historique des évènements de contrôle d'accès

La configuration de cette passerelle nécessite d'effectuer une partie du paramétrage sur CliqWebManager.

10.3.2. Gérer les accès CLIQ

Tableau 10.2. Chronologie des étapes pour la gestion des accès CLIQ

N°	Etape	Interface	Détails
1	Déclaration des équipements	CLIQ Web Manager	Déclarer les clés cylindres et groupes de cylindres dans CLIQWebManager
2	Import des équipements	MICROSESAME CUBE	Imports des éléments CLIQ dans MICROSESAME depuis l'interface de paramétrage CLIQ
3	Création des identifiés	MICROSESAME CUBE MICROSESAME CUBE	La création d'identifiés susceptibles d'utiliser les équipements CLIQ se fait directement dans la gestion des identifiés depuis MICROSESAME ou WEBSESAME. Les utilisateurs CLIQ définis directement dans CLIQWebmanager ne seront pas gérés par les

N°	Etape	Interface	Détails
			droits MICROSESAME
3	Assignation des identifiants CLIQ	MICROSESAME CUBE MICROSESAME CUBE	L'assignation des clés CLIQ se fait directement dans la gestion des identifiés depuis MICROSESAME ou WEBSESAME.
4	Assignation des accès CLIQ	MICROSESAME CUBE MICROSESAME CUBE	L'assignation des accès aux cylindres et groupes de cylindres CLIQ se fait directement dans la gestion des identifiés depuis MICROSESAMEou WEBSESAME.  Dans MICROSESAMEil est nécessaire d'afficher les cylindres et groupes de cylindres CLIQ pour les assigner. Effectuer un clic-droit puis afficher les accès ou groupes d'accès correspondant.  L'assignation des accès CLIQ supporte uniquement la plage

N°	Etape	Interface	Détails
			horaire 24h/24 et ceux-ci ne peuvent avoir de dates de validité.
3	Déploiement aux équipements CLIQ	MICROSESAME CUBE	• Depuis la configuration CLIQ, onglet Synchronisation. • Depuis **Paramétrage > Mise en exploitation > Appliquer le paramétrage** (si activé). • Téléchargement automatique à la modification de la fiche identifié (support CLIQ).

Les accès aux cylindres et groupes de cylindres CLIQ peuvent être ajoutés à des profils d'accès dans MICROSESAME

Dans CLIQWebManager > administration, il est impératif de régler le paramètre suivant comme suit :

Lors de la suppression de personnes : Marquer comme supprimé .

10.3.3. Visualiser l'historique de contrôle d'accès

Les évènements de contrôle d'accès sur les serrures CLIQ Abloy sont historisés dans la base de données MICROSESAME.

Evènements historisés :

- Accès AUTORISE
- Accès INTERDIT (hors plage ou non attribué)

WEBSESAME	Poste client
Suivre la procédure suivante pour accéder à l'historique de contrôle d'accès : 1. Lancer WEBSESAME 2. Se rendre dans l'onglet **Historique > Contrôle d'accès** 3. Définir une période de recherche et ajouter un filtre si nécessaire 4. Ajouter les colonnes souhaitées pour visualiser les informations présentées ci-dessous. 5. Cliquer sur **Rechercher**	**Suivre la procédure suivante pour accéder à l'historique de contrôle d'accès :** 1. Depuis le menu principal MICROSESAME, suivre **Exploitation > Journaux > Historique** 2. Se rendre dans l'onglet **Contrôle d'accès** 3. Définir une période de recherche et ajouter un filtre si nécessaire 4. Ajouter les colonnes souhaitées pour visualiser les informations présentées ci-dessous. 5. Cliquer sur **Rechercher** Pour personnaliser les colonnes, effectuer un clic-droit dans l'entête de la table des résultats.

Colonnes	Éléments historisés
Nom lecteur	Nom du cylindre CLIQ
Commentaire lecteur	Nom du groupe de cylindres
Référence graphique	Marquage de la clé

Les évènements de contrôle d'accès sont remontés lors de la mise à jour des droits d'accès sur la borne CLIQ.

L'historique de contrôle d'accès CLIQ est mis à jour périodiquement, l'intervalle de temps est paramétrable dans l'interface de configuration CLIQ.

10.3.4. Cas d'usage : Assigner des accès CLIQ par l'intermédiaire d'un profil d'accès

Le cas d'usage ci-dessous représente le déroulement général d'une opération d'assignation d'accès. Toute opération de l'installation CLIQ avec MICROSESAME hors de la procédure présentée ne peut être garantie comme fonctionnelle.

Contexte

- On considère une installation CLIQ déjà configurée et les équipements importées dans la base MICROSESAME
- On souhaite créer un profil d'accès pour cet identifié comprenant des accès CLIQ

- La clé assignée à l'identifiée est nominative

N°	Etape	Détails
1	Création du profil d'accès	**Dans MICROSESAME > Profils d'accès :** 1. Créer un profil d'accès et le renommer en fonction des besoins d'assignation (EX: Acces_RDC). 2. Ajouter les cylindres ou groupes de cylindres CLIQ Seule la plage 24h/24 est disponible à l'assignation.
2	Création de la fiche identifié	Dans la gestion des identifiés depuis MICROSESAMEou WEBSESAME, L'opérateur créé un identifié permanent.
3	Assignation du profil à l'identifié	Depuis MICROSESAMEou WEBSESAME, dans la fiche de l'identifié permanent, l'opérateur ajoute le profil d'accès créé précédemment dans la liste de ses accès. De cette manière il est possible de donner une plage de validité aux accès CLIQ.
4	Assignation d'une clé à l'identifié	Depuis MICROSESAME ou WEBSESAME, dans la fiche de l'identifié permanent, l'opérateur ajoute la clé CLIQ a partir de la liste d'identifiants permanents (grâce à la référence graphique/marquage de la clé)

N°	Etape	Détails
5	Actualisation des droits sur la clé CLIQ	L'identifié récupère sa clé et l'insère dans une borne de programmation afin de mettre à jour les accès dans la clé.
6	Supervision des bornes de programmation (boitiers de programmation à distance)	Les objets de supervision créés automatiquement dans MICROSESAME lors du paramétrage de la passerelle.

10.3.5. Cas d'usage : Supprimer des accès CLIQ à un identifié

Le cas d'usage ci-dessous représente le déroulement général d'une opération d'assignation d'accès. Toute opération de l'installation CLIQ avec MICROSESAME hors de la procédure présentée ne peut être garantie comme fonctionnelle.

Contexte

- On considère une installation CLIQ déjà configurée et les équipements importées dans la base MICROSESAME
- On souhaite retirer les accès aux cylindres ou groupes de cylindres CLIQ à un identifié permanent

Tableau 10.3. Méthode 1 : suppression des profils d'accès

N°	Etape	Détails
1	Suppression des accès de l'identifié	Dans **MICROSESAME> Identifiés** : Dans la fiche de l'identifié permanent, l'opérateur supprime le ou les accès CLIQ dans la liste de ses accès. les modifications sont automatiquement déployées à l'enregistrement de la fiche identifiée. Dans le cas ou le support CLIQ n'a pas été activé, il est nécessaire d'effectuer un téléchargement complet.

N°	Etape	Détails
2	Actualisation des droits sur la clé CLIQ	L'identifié permanent insère sa clé CLIQ dans un boitier de programmation afin de mettre à jour ses accès. Il n'a désormais plus accès aux cylindres supprimés.
3	Revalidation des droits d'accès	A l'issue de l'intervalle de revalidation définie dans l'interface MICROSESAME de paramétrage CLIQ, les accès de l'identifié seront dévalidés et il sera nécessaire de repasser sur la borne pour les actualiser.

Tableau 10.4. Méthode 2 : Dé-validation de l'identifié

N°	Etape	Détails
1	Dé-validation de l'identifié	Dans **MICROSESAME > Identifiés** : Dans la fiche de l'identifié permanent, l'opérateur dé-valide l'identifié. L'identifié n'est pas supprimé côté CLIQWebManager mais il est "marqué comme supprimé", il perd donc tous ses accès et la clé qu'il possède est ainsi vidée de ses accès.
2	Actualisation des droits sur la clé CLIQ	L'identifié permanent insère sa clé CLIQ dans un boitier de programmation afin de mettre à jour ses accès. Tous ses accès sont supprimés.
3	Revalidation des droits d'accès	A l'issue de l'intervalle de revalidation définie dans l'interface MICROSESAME de paramétrage CLIQ,

N°	Etape	Détails
		les accès de l'identifié seront dévalidés et il sera nécessaire de repasser sur la borne pour les actualiser.

10.3.6. Cas d'usage : Rendre une clé CLIQ

Le cas d'usage ci-dessous représente le déroulement général d'une opération d'assignation d'accès. Toute opération de l'installation CLIQ avec MICROSESAME hors de la procédure présentée ne peut être garantie comme fonctionnelle.

Contexte

- On considère une installation CLIQ déjà configurée et les équipements importées dans la base MICROSESAM
- On souhaite récupérer la clé CLIQ d'un identifié
- On souhaite supprimer tous les accès de la clé pour la préparer à une nouvelle assignation

N°	Etape	Détails
1	Suppression de l'identfiiant	Dans **MICROSESAME > Identifiés** : Dans la fiche de l'identifié permanent, l'opérateur supprime l'identifiant associé à la clé CLIQ dans la liste de ses identifiants.
2	Actualisation des droits sur la clé CLIQ	La clé est ensuite insérée dans un boitier de programmation afin de mettre à jour ses accès. Tous les accès ont désormais été supprimés de la clé.
3	Remise de la clé	L'identifié remet la clé à un opérateur MICROSESAME, l'identifiant associé est réutilisable et peut être assigné à un nouvel identifié.

En cas de suppression de l'identifié de la base MICROSESAME, il est nécessaire de s'assurer que tous les identifiants associés à des clés CLIQ qui lui ont été assignés aient été supprimés avant de procéder à la suppression.

Chapitre 11. Journaux

11.1. Calcul du temps de présence

11.1.1. Généralités

11.1.1.1. Introduction

Certaines législations du travail imposent que soit respecté un temps de repos minimal entre chaque journée de travail ainsi qu'un temps de repos un peu plus important le week-end (ex: la législation française impose un temps de repos de 11h minimum entre chaque journée et un repos de 35h minimum pour le week-end : articles L3131-1 et L3131-2 du code du travail).

Le logiciel MICROSESAME incorpore, de manière native, un mécanisme permettant de calculer le temps de présence d'un employé sur un site, une zone ou un groupe de lecteurs.

Les rapports de temps de présence sont calculés pour la période correspondant à la semaine précédant la consultation.

L'analyse du temps de présence peut être réalisé de manière automatisée avec l'application ou de manière manuelle avec les rapports de MICROSESAME

A partir de la version 2021.3 , une interface de consultation des temps de présence est intégrée directement dans WEBSESAME

11.1.1.2. Prérequis

- Un système d'exploitation Windows 7 (64 bits) ou supérieur est nécessaire
- Le programme de calcul de temps de présence doit être présent dans le répertoire des programmes MICROSESAME (par défaut : C:\MSESAME\PROG)
- Afin de pouvoir générer les rapports et les analyses nécessaires, le site doit posséder des lecteurs d'entrée et de sortie que les employés utilisent à chacun de leurs passages (horodatage des heures entrée et sortie).
- Une plage horaire de travail quotidien doit être définie, avec une heure de début et une heure de fin.
- La fonctionnalité d'archivage des passages de badge doit être disponible sur au moins 8 jours.

11.1.2. Consulter les analyses de temps de présence

11.1.2.1. Consulter le temps de présence dans WEBSESAME

L'interface de consultation des temps de présence dans WEBSESAME est disponible à partir de la version 2021.3

Se rendre dans l'onglet **Historique > Temps de présence** de WEBSESAME.

La fenêtre principale permet de filtrer les résultats :

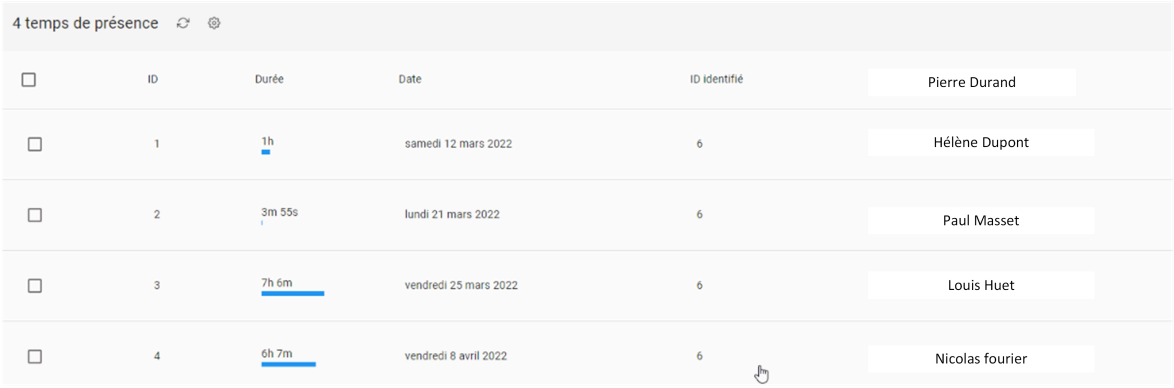
- Par période
- Par filtres avancés (nom de l'identifié, Id identifié, ...)

Une fois la requête de recherche paramétrée, l'opérateur peut cliquer sur Enregistrer la recherche pour réutiliser ces paramètres **ultérieurement**.

Les analyses de temps de présence sont calculées pour la semaine précédant la demande de consultation. Il est donc impossible de consulter le temps de présence des identifiés pour la semaine ou la journée en cours.

Les temps de rpésence correspondant aux filtres implémentés sont listés dans la fenêtre principale. Une barre de progression permet d'observer visuellement le temps passé **entre 0 et 12h** sur site.

L'opérateur peut cliquer sur un temps de présence pour détailler les créneaux de présence au cours de la jorunée.



11.1.2.2. Consulter le temps de présence dans les rapports

Consulter la section suivante pour plus d'informations sur la génération et la consultation des analyses de temps de présence dans les rapports :*???*.

11.2. Contrôle du temps de repos

11.2.1. Généralités

11.2.1.1. Introduction

Certaines législations du travail imposent que soit respecté un temps de repos minimal entre chaque journée de travail ainsi qu'un temps de repos un peu plus important le week-end (ex: la législation française impose un temps de repos de 11h minimum

entre chaque journée et un repos de 35h minimum pour le week-end : articles L3131-1 et L3131-2 du code du travail).

Le logiciel MICROSESAME incorpore, de manière native, un mécanisme permettant de calculer le temps de présence d'un employé dans un site, une zone ou un groupe de lecteurs et calculer le temps de repos postérieur qu'il doit respecter.

Ce mécanisme permet :

- d'interdire l'accès à un identifié n'ayant pas respecté sa période de repos minimale obligatoire (mode blocage),
- de générer un rapport sans bloquer les accès de l'employé (mode rapport). En mode rapport, un fichier est généré contenant uniquement les temps de repos qui n'ont pas été respectés.

11.2.1.2. Prérequis

Afin d'utiliser pleinement cette fonction, les conditions suivantes doivent être respectées:

- Pour utiliser le mode "Rapport sans blocage", il est nécessaire d'avoir au minimum la version 2017.1.4 de MICROSESAME
- Pour utiliser le mode "blocage à la minute" il est nécessaire d'utiliser une TILLYS NG et d'avoir au minimum la version 2017.1 de MICROSESAME. Ce mode n'est pas compatible avec les UTL v2.
- La purge de l'historique des évènements autorisés doit obligatoirement être supérieur à 2 jours (par défaut : 30 jours)

11.2.2. Distribution d'un régime de repos à un identifié

Une fois le régime de repos créé et paramétré dans la fenêtre de "paramétrage général", il faut l'assigner aux identifiés concernés. Pour cela suivre les étapes ci-dessous :

1.. Accéder à la fiche identifié des identifiés concernés : *Menu MICROSESAME > Accès > Identifiés > Sélectionner l'identifié concerné*
2.. Dans la partie "**Contrôle de repos**" de l'onglet "*Accès*" Sélectionner "*Actif*" pour activer la fonctionnalité de contrôle du temps de repos.
3.. Dans le champ "*Régime de repos*", sélectionner le régime de repos à appliquer à l'identifié.
4.. Sauvegarder les modifications.

La gestion des droits opérateur permet d'autoriser la modification et/ou la visualisation du contrôle du temps de repos depuis la gestion des identifiés.

Pour modifier les droits opérateur :

1. Ouvrir la gestion des opérateurs : *Menu principal > Paramétrage > Profils opérateurs*

2. Cliquer sur l'onglet "Identifiés".
3. Cocher les cases "Visu", "Modif" en face de la ligne "Contrôle temps de repos" selon besoin.

L'attribution de ces droits doit être réalisé par un opérateur disposant de droits supérieurs.

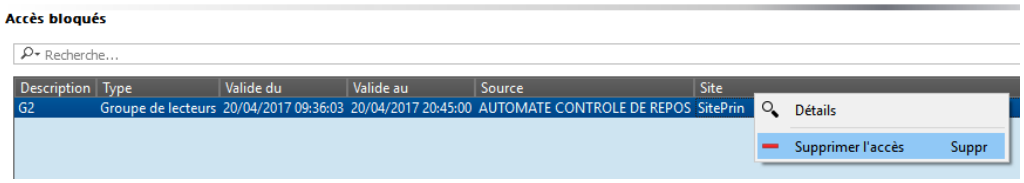
11.2.3. Suppression des accès bloqués

Dans le cas où le mode "rapport sans blocage" n'a pas été activé, tout identifié tout identifié étant sortit après après l'heure de fin de la plage horaire de travail sera automatiquement bloqué pendant le temps de repos quotidien ou hebdomadaire (selon le jour du badgeage) paramétré. Ces accès bloqués peuvent être débloqués de deux manières :

- A partir d'une fiche identifié, cette méthode consiste à supprimer l'accès bloqué d'un identifié spécifique.
- A partir de la fenêtre de paramétrage du régime de repos, cette méthode permet de supprimer tous les accès bloqués de tous les identifiés associés à ce régime de repos.

Suppression de l'accès bloqué d'un identifié

1. Ouvrir la fiche de l'identifié concerné : *Menu MICROSESAME> Accès > Identifiés > Rechercher et sélectionner l'identifié*
2. Dans la section "Accès bloqués" de l'onglet "Accès" se trouve le blocage effectué sur l'identifié par l'application de contrôle du temps de repos.
3. Il est possible de supprimer ce blocage en effectuant un clic droit sur la ligne correspondant à l'accès bloqué et en sélectionnant "Supprimer l'accès"



Suppression de tous les accès bloqués du régime de repos

1. Ouvrir la fenêtre de paramétrage du régime de repos : *Menu MICROSESAME > Paramétrage > Paramétrage général > Contrôle de temps de repos > Sélectionner le régime de repos concerné*
2. Cliquer sur le bouton "Réinitialiser les blocages"

11.2.4. Résultats et rapports

11.2.4.1. Résultats en mode "rapport sans blocage"

Cette fonction permets d'éditer un rapport dans lequel sont inscrits les identifiés n'ayant pas respecté le temps de repos paramétré.

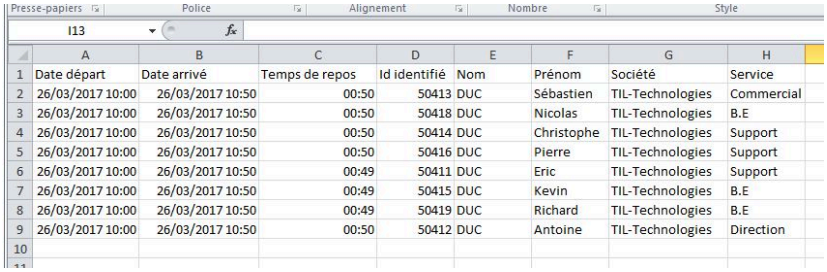
Dans ce mode, Les identifiés se présentant sur les lecteurs d'entrée avant la fin du temps de repos à respecter ne sont pas bloqués.

L'emplacement du fichier de résultats doit être indiqué lors du paramétrage de l'application (Voir "Paramétrage").

Le fichier de résultats généré est un fichier en format ".csv". Ce nom de fichier sera sous la forme ReposQuotidien_<NOM-DU-REGIME>_<ANNEE>-<MOIS>-<JOUR>.csv

Exemple `ReposQuotidien_2017-03-26.csv`

Le contenu du rapport a le format suivant :



	A	B	C	D	E	F	G	H
1	Date départ	Date arrivé	Temps de repos	Id identifié	Nom	Prénom	Société	Service
2	26/03/2017 10:00	26/03/2017 10:50	00:50	50413	DUC	Sébastien	TIL-Technologies	Commercial
3	26/03/2017 10:00	26/03/2017 10:50	00:50	50418	DUC	Nicolas	TIL-Technologies	B.E
4	26/03/2017 10:00	26/03/2017 10:50	00:50	50414	DUC	Christophe	TIL-Technologies	Support
5	26/03/2017 10:00	26/03/2017 10:50	00:50	50416	DUC	Pierre	TIL-Technologies	Support
6	26/03/2017 10:00	26/03/2017 10:50	00:49	50411	DUC	Eric	TIL-Technologies	Support
7	26/03/2017 10:00	26/03/2017 10:50	00:49	50415	DUC	Kevin	TIL-Technologies	B.E
8	26/03/2017 10:00	26/03/2017 10:50	00:49	50419	DUC	Richard	TIL-Technologies	B.E
9	26/03/2017 10:00	26/03/2017 10:50	00:50	50412	DUC	Antoine	TIL-Technologies	Direction
10								

Le contenu du fichier temps de repos est le suivant :

- Date de départ
- Date d'arrivé
- Temps de repos
- Id identifié
- Nom
- Prénom
- Société
- Service

11.2.4.2. Résultats via l'outil Rapports

L'outil Rapports permet de générer un rapport en effectuant une requête dans la base de donnée. Le rapport se récupère dans "WEBSESAME" en effectuant une opération manuelle.

Pour extraire la liste des identifiés bloqués (identifiés étant sortis après l'heure de fin de la plage horaire de travail paramétré dans le régime de repos), effectuer les étapes suivantes :

1. Ouvrir le paramétrage de l'outil Rapports : *Menu MICROSESAME > Paramétrage > Système> Rapports*.
2. Cliquer sur le bouton "Importer".
3. Sélectionner le fichier "requete_repos" se trouvant à l'emplacement suivant des PROG de MICROSESAME : *ScriptsSql\SqlServer\Requestor\FR* si base SQL.
4. Sauvegarder le paramétrage.
5. Lancer l'application "Web-Sesame", puis sélectionner "Rapports".
6. Dans la liste déroulante se trouvant dans la section "Requête" sélectionner la requête correspondante.
7. Cliquer sur le bouton "Exécuter la requête" se trouvant à la fin de la section "Paramètres".

8. Cliquer sur le bouton dans la ligne apparue dans la section "Résultats" afin de télécharger le résultat sous un fichier ".csv".

11.3. Historique

11.3.1. La fenêtre Historique

Pour accéder à la fenêtre de l'historique depuis le menu principal de MICROSESAME, suivre **Exploitation > Journaux** .

L'historique (se_findevents) permet d'accéder rapidement à des **événements** passés et permet à l'opérateur d'associer des **notes** aux évènements ("Notes"). L'affichage des évènements est réparti sur 5 catégories :

- Évènements liés au **contrôle d'accès**.
- Évènements **techniques**.
- Évènements **système**.
- **Audit des modifications**.
- **Fusion** de tous les évènements.

Pour lancer votre première requête, cliquer sur **Rechercher (F5)** . La requête remonte les informations historiques des éléments sur lesquels ont été placés une demande d'archivage. La requête ne peut pas renvoyer d'événements inférieurs (en date) à la valeur de rétention maximale. Par défaut, cette valeur est fixée à 30 jours.

Des **filtres** spécifiques peuvent être appliqués pour chaque catégorie d'évènements (Voir **Période de recherche**).

Les boutons **TXT et PDF** permettent de réaliser des exports de l'historique. Il est aussi possible d'**imprimer** l'historique.

Le bouton **Colonnes** permet de retailler les colonnes.

Le bouton **Fusion** affiche une fenêtre nommée **Événements chronologiques**.
Cette fenêtre est vide, il faut alors double-cliquer sur une ligne dans l'historique (un événement) pour que des événements soient affichés dans la fenêtre. Les informations affichées correspondent aux données affichées dans l'onglet "Fusion" (tous types d'événements avec comme date de début la ligne - 600 secondes et comme date de fin la ligne + 600 secondes).

Le bouton **Résultats** : Par défaut, dans l'historique, tous les événements ne sont pas affichés si ceux-ci sont trop nombreux. Il faut alors scroller dans la liste pour que des nouveaux événements apparaissent au fur et à mesure. Le bouton Résultats permet d'afficher les 255 lignes suivantes.

11.3.2. Période de recherche

Le tableau ci-après décrit les différentes possibilités de recherche d'événements :

Élément	Description
"Prédéfinie"	La période de recherche prédéfinie est sélectionnée par défaut. Elle permet

Élément	Description
	d'effectuer une requête sur des périodes prédéfinies (Par défaut, 7 jours). Cliquer sur le menu dépliant afin de changer la période prédéfinie.
"Durée"	La case "Durée" permet d'effectuer une requête à partir d'une date indiquée et pendant une durée spécifiée.
"Avancée"	La case "Avancée" permet d'effectuer une requête en sélectionnant la date et l'heure précises de début et de fin.

Tri chronologique

Indépendamment de la période sélectionnée pour la recherche, il est possible d'organiser les résultats de recherche par ordre chronologique normal ou inversé.

Après avoir indiqué la période de recherche, cliquer sur "Rechercher" ou le raccourci clavier "*F5*", pour exécuter la requête.

11.3.3. Les filtres prédéfinis

Les filtres prédéfinis offrent à l'utilisateur un gain du temps important. Ils sont spécifiques à l'onglet sélectionné, et permettent d'enregistrer les paramètres d'une requête.

Pour plus d'information, voir "Historique du contrôle d'accès" dans WEBSESAME.

11.3.4. Onglets de la fenêtre Historique

11.3.4.1. Contrôle d'accès

L'onglet contrôle d'accès regroupe uniquement les évènements liés aux accès :

- La zone d'affichage des filtres prédéfinis concerne uniquement l'onglet "Contrôle d'accès". Des filtres prédéfinis spécifiques au contrôle d'accès peuvent être enregistrés.
- La zone *Évènements badges* filtre le résultat en fonction du statut des badges. Une case cochée est égale à un filtre attribué.

La zone d'affichage du résultat de la requête permet de double cliquer sur un évènement pour le visualiser dans son contexte temporel et sur une durée fixe. Cet évènement sera présenté dans l'onglet " Évènements chronologiques" en surbrillance grisée.

Les différentes colonnes disponibles dans zone d'affichage des résultats peut être personnalisée : Cliquer droit sur les en-tête et cliquer l'option "Personnaliser les colonnes".

Choisir les éléments souhaités et cliquer sur "OK".

La position des colonnes sélectionnées peut être sauvegardé par l'utilisateur.

11.3.4.2. Évènements techniques

L'onglet "*Évènement techniques*" regroupe tous les évènements liés aux variables.

La zone d'affichage des filtres prédéfinis concerne uniquement l'onglet "Évènement techniques". Des filtres prédéfinis spécifiques aux évènements techniques peuvent être enregistrés.

Le filtre détaillé autorise les critères suivantes :

- Alarmes
- Télécommandes
- Autres évènements
- Numériques
- Seulement les valeurs forcées
- Listes des variables
- Catégories

Une case cochée est égale à un critère autorisé.

La zone d'affichage du résultat de la requête permet de double cliquer sur un évènement pour le visualiser dans son contexte temporel et sur une durée fixe. Cet évènement sera présenté dans l'onglet "*Évènements chronologiques*" en surbrillance grise.

Évènements chronologiques est la zone d'affichage de tous les évènements sur une durée fixe, et en fonction d'un évènement sélectionné dans le résultat de la requête. Cette durée est comprise entre -10min et +10min, suivant l'évènement sélectionné.

11.3.4.3. Évènements système

L'onglet "*Évènements système*" regroupe tous les évènement liés au système MICROSESAME (opérations des opérateurs, téléchargement de modules,...).

La zone d'affichage des filtres prédéfinis concerne uniquement l'onglet "Évènements système". Des filtres prédéfinis spécifiques aux évènements système peuvent être enregistrés.

Dans les champs textes libres, la règle de recherche correspond à la suivante: Champs concerné **Contient** la valeur renseigné dans le filtre.

Le filtre détaillé autorise les critères suivants :

- Sévérité : jeu d'icônes pour déterminer l'ordre de sévérité d'un évènement, comme ci-après :
  - Information
  - Avertissement
  - Erreur

- **Elément** de supervision MICROSESAME
- **Application** source de l'évènement.
- **Message**associé à l'évènement.
- **Description** description de l'évènement.
- **Opérateur** responsable de l'opération.
- **Poste** utilisé pour l'opération.
- **Processus** associé à l'évènement.
- **Etat** de la propriété associée à l'évènement.
- **ID ticket**: Permet de filtrer la recherche par l'ID du ticket de suivi main courante associé à l'évènement.

Pour afficher un résultat dans son contexte chronologique, cliquer sur l'icône **Fusion** dans le bandeau supérieur de la fenêtre et double-cliquer sur l'évènement concerné.

Celui-ci s'affiche en surbrillance grise dans son contexte temporel, l'opérateur peut ainsi visualiser tous les évènements qui ont précédés ou vont succéder à celui sélectionné.

L'onglet **Evènements chronologiques** affiche tous les évènements étant apparus entre 10 minutes avant et après l'évènement sélectionné.

Pour visualiser l'appartenance d'un évènement à un ticket main courante, suivre la procédure suivante:

1. Effectuer un clic-droit sur l'entête du tableau des résultats.
2. Choisir **Personnaliser les colonnes**.
3. Double-cliquer sur **Ticket main courante**.

Pour consulter le contenu d'un ticket de main courante, effectuer un clic-droit sur l'évènement concerné et choisir **Voir le ticket main courante**.

11.3.4.4. Notes

Pour utiliser les notes, il est nécessaire dans un premier temps d'activer la fonctionnalité. Pour se faire, se rendre dans l'onglet **Notes** du paramétrage général et définir les catégories.

Pour plus d'informations sur le paramétrage des notes, se référer à la section suivante du guide **MS_Cube_Aide**:

Partie 3: Exploitation

Chapitre 2: Opérateurs

Section 5: Notes opérateurs

L'onglet **Note** de l'historique permet de visualiser toutes les notes ayant été ajoutées par les opérateurs.

Les différents critères permettent de filtrer les résultats de la recherche dans le tableau:

- Catégorie et éléments de liste.

- Commentaire.

Les notes peuvent être ajoutés depuis le moniteur d'évènement ou directement depuis l'application historique, en effectuant un clic-droit sur la ligne concernée ou en utilisant le bouton dédié dans le bandeau supérieur de la fenêtre.

Pour plus d'informations sur les notes, se référer à la section dédiée de l'aide en ligne.

11.3.4.5. Audit des modifications

L'onglet "Audit des modifications" récapitule toutes les modifications produites sur les accès (suppression de badges, ajout de lecteurs, modifications de lignes,...). Le filtre détaillé autorise les critères par type d'évènement et/ou par action effectuée sur cet évènement.

Dans la zone d'affichage du résultat de la requête, double cliquer sur un évènement pour le visualiser dans son contexte temporel et sur une durée fixe. Cet évènement sera présenté dans l'onglet "*Évènements chronologiques*" en surbrillance grise.

Évènements chronologiques est la zone d'affichage de tous les évènements sur une durée fixe, et en fonction d'un évènement sélectionné dans le résultat de la requête. Cette durée est comprise entre -10min et +10min, suivant l'évènement sélectionné.

11.3.4.6. Fusion (tous les évènements)

L'onglet "*Fusion (tous les évènements)*" affiche le résultat de la requête sans filtration.

Il permet d'afficher tous les évènements par ordre chronologique.

11.3.5. Accès à l'historique depuis WEBSESAME

L'accès au service WEBSESAME se fait grâce à l'adresse suivante: `https://nom_du_serveur:443/`

Le port à renseigner dans l'URL d'accès à WEBSESAME est susceptible de changer en fonction de la configuration du poste serveur.

L'onglet **Historique** de WEBSESAME offre diverses possibilités en fonction des **droits** assignés à l'**opérateur**.

L'opérateur peut naviguer entre deux types d'historique:

- Contrôle d'accès (évènements liés au passage de badges)
- Évènement techniques (évènements techniques liés à l'installation)

L'opérateur peut visualiser les derniers évènements survenus ou effectuer des recherches avancées:

- Par période.
- Par dates.

- Grâce à la sélection de filtres.

Les filtres doivent êtres paramétrés et enregistrés au préalable dans MICROSESAME afin d'être utilisés dans WEBSESAME.

11.4. Rapports

11.4.1. Présentation de l'outil Rapports

L'outil Rapports permet l'extraction d'informations contenues dans les différentes tables de la base de données MICROSESAME.

L'outil Rapports génère, en sortie, un "fichier.CSV".

Par défaut, l'outil Rapports est vierge de toute requête. HIRSCH propose une prestation de développement de requêtes spécifiques, sur cahier des charges.

Une requête trop complexe ou mal construite peut générer un risque de surcharge du serveur.

ExcelViewer

ExcelViewer est mis à disposition lors de l'installation de MICROSESAME (version 2015.1.0 ou supérieur) pour permettre la visualisation de "fichiers.CSV" sur les machines sans tableur.

Pour accéder à la page de paramétrage des rapports, suivre **Paramétrage**> **Système** >**Rapports**" depuis le menu principal de MICROSESAME.

11.4.2. Accès aux rapports depuis WEBSESAME

L'accès au service WEBSESAME se fait grâce à l'adresse suivante: `https://nom_du_serveur:443/`

Le port à renseigner dans l'URL d'accès à WEBSESAME est susceptible de changer en fonction de la configuration du poste serveur.

L'opérateur peut aussi accéder à WEBSESAME depuis le menu-principal: **Exploitation > Journaux > Rapports**.

L'onglet **Rapport** de WEBSESAME, permet de rechercher, consulter ou générer des rapports d'informations concernant l'installation.

Le paramétrage ou l'importation de nouvelles requêtes SQL se fait obligatoirement depuis MICROSESAME,

Chapitre 12. Maintenance

12.1. Tableau de bord

12.1.1. Présentation du tableau de bord

La solution MICROSESAME possède un tableau de bord pour une supervision de ces process systèmes :

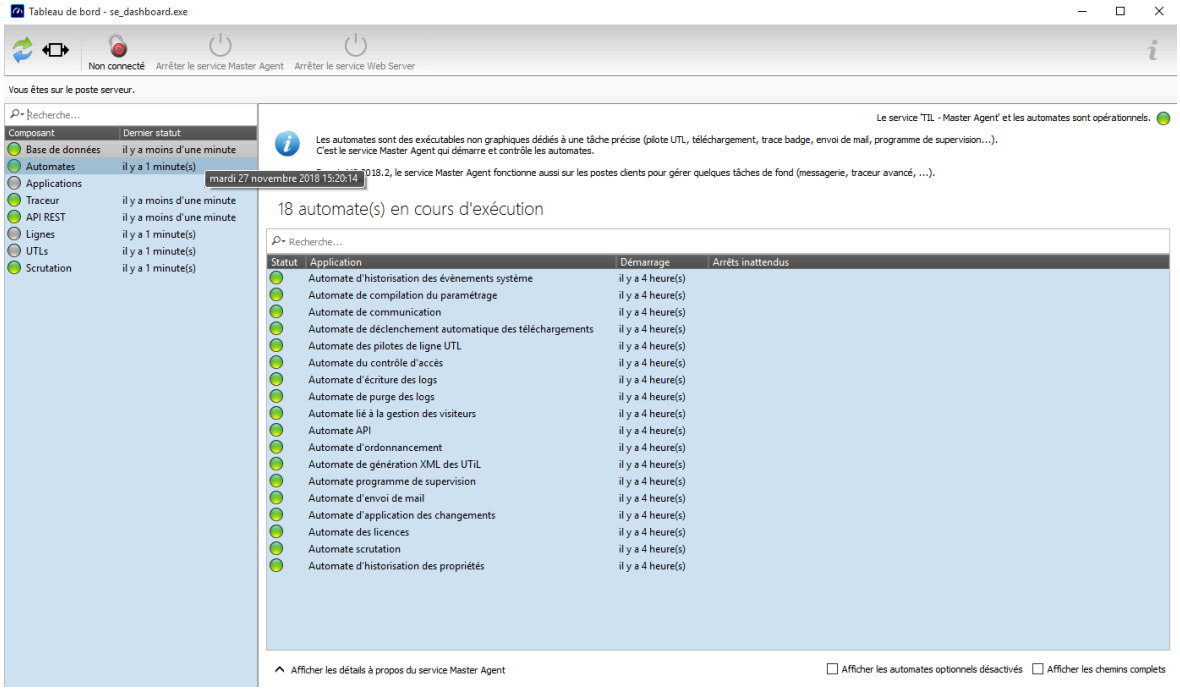
- Arrêter/démarrer manuellement des automates et des services,
- Statistiques sur la scrutation,...

12.1.2. Accès

Dans le menu principal de MICROSESAME, suivre **Maintenance > Autres** ou réaliser une recherche à l'aide du mot clé "tableau" ou "tableau de bord" dans la barre de recherche disponible dans le menu principal.

Le droit opérateur **Administrateur** est nécessaire afin de pouvoir accéder à l'application du tableau de bord.

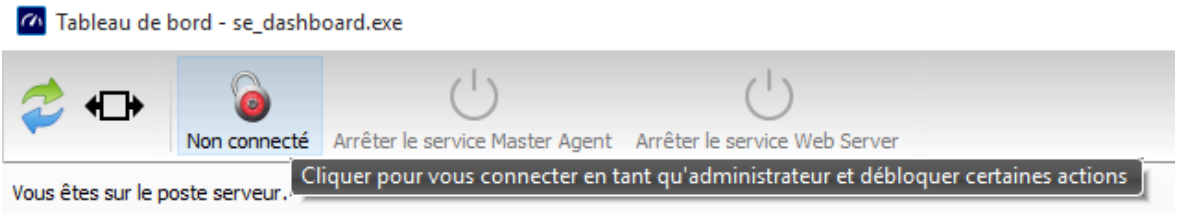
Le tableau de bord (se_dashboard.exe) s'ouvre:



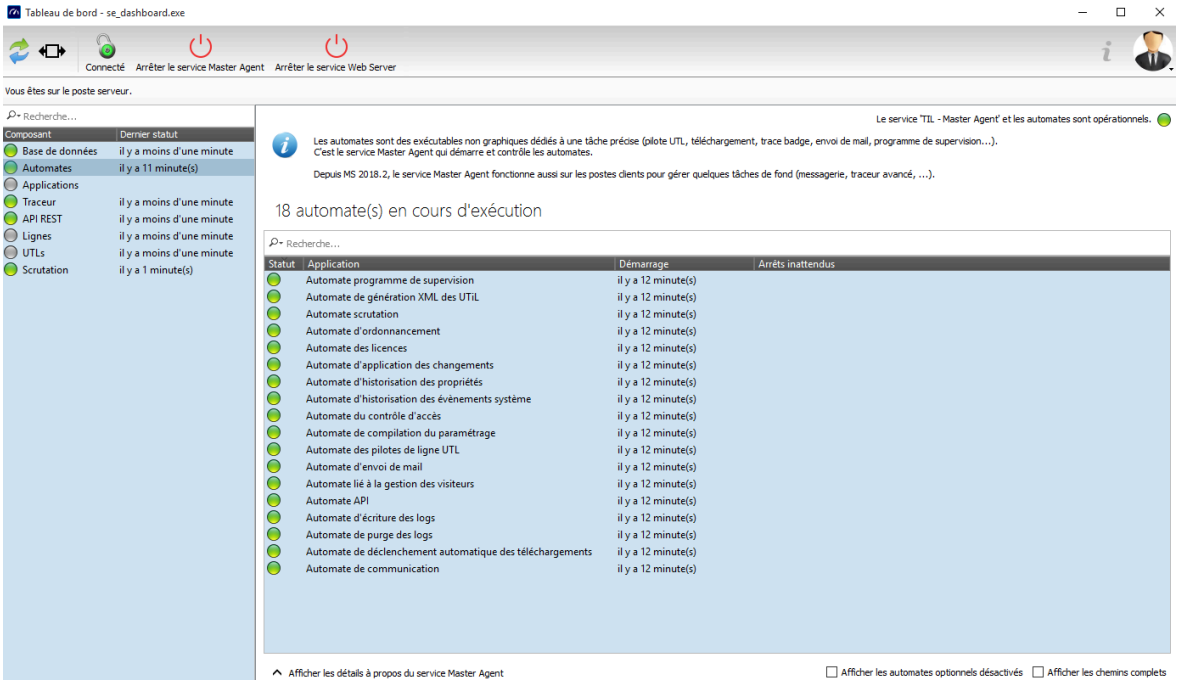
12.1.3. La fenêtre du tableau de bord

Le tableau de bord permet de **connaître l'état de fonctionnement** de MICROSESAME (accès à la Base de données, état des automates, état de la scrutation ...) et de **contrôler l'arrêt/marche** des services et de la scrutation (sur le serveur).

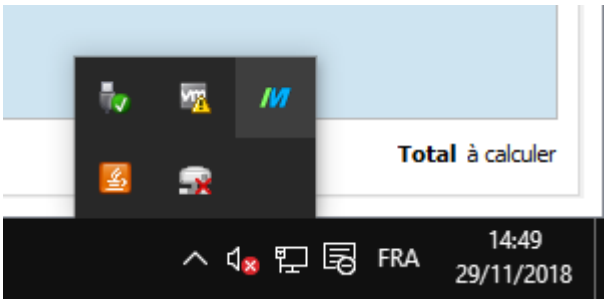
Une session **Administrateur** est nécessaire pour accéder et réaliser des actions depuis le tableau de bord:



Avec une session Administrateur, les services **Master Agent** et **Web Server** peuvent être arrêtés depuis la barre d'outils :



La tableau de bord se présente sous la forme d'une icône dans la zone de notifications de Windows.



L'icône du tableau de bord dans la zone de notifications de Windows affiche un statut global, agrégé des différents status du tableau de bord.

Le tableau suivant décrit les différentes notifications possibles dans la zone de notifications de Windows :

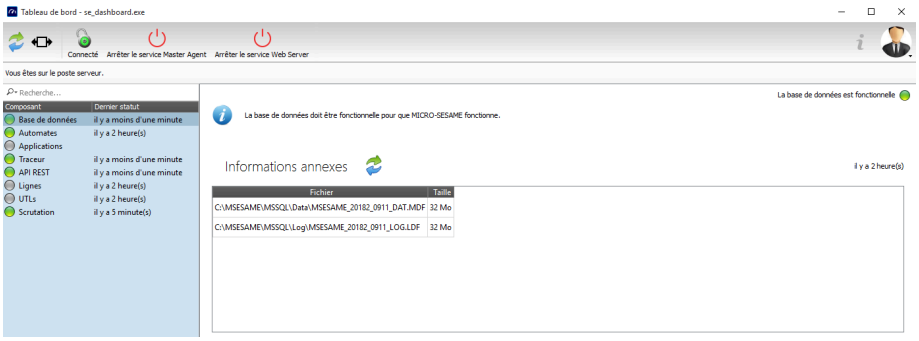
Notification	Description
	MICROSESAME fonctionnel
	État transitoire : MICROSESAMEinterroge les éléments sous surveillance

Notification	Description
	Avertissement lorsque des problèmes sont constatés : • le Master Agent n'a pas la même version que le tableau de bord • le Master Agent est en cours d'initialisation • Un automate ou plus a (ont) redémarré • Une durée de rétention du traceur a été paramétré a plus de 100 jours • tracer en mode debug Cet état a une priorité majeur que l'état d'intérrogation, et inférieure à l'état d'erreur.
	Erreur lorsqu'un des problèmes suivants est constaté : • problème de connexion à la base de données • un service ne réponds pas • un automate est arrêté • la scrutation est arrêtée Cet état a la priorité la plus élevée.

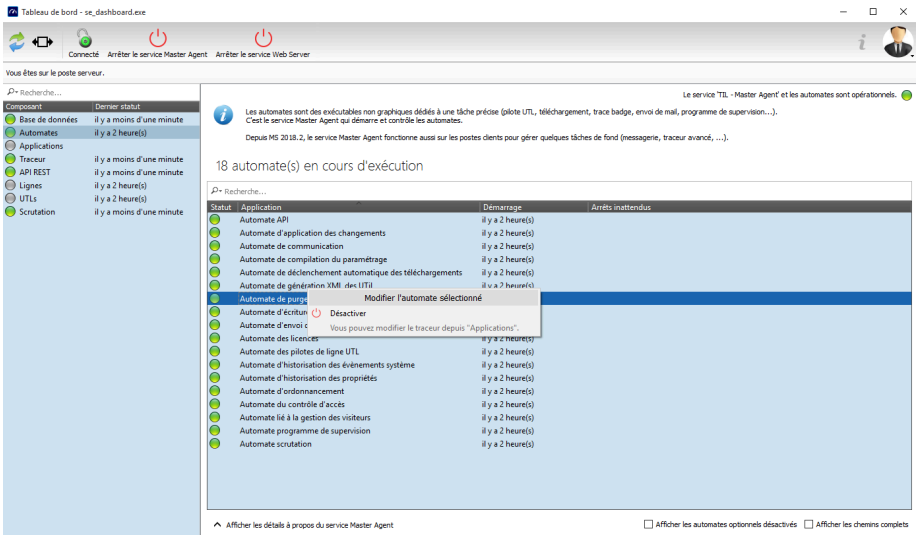
12.1.4. Fonctionnalités

Les composants suivants peuvent être monitorés depuis le tableau de bord :

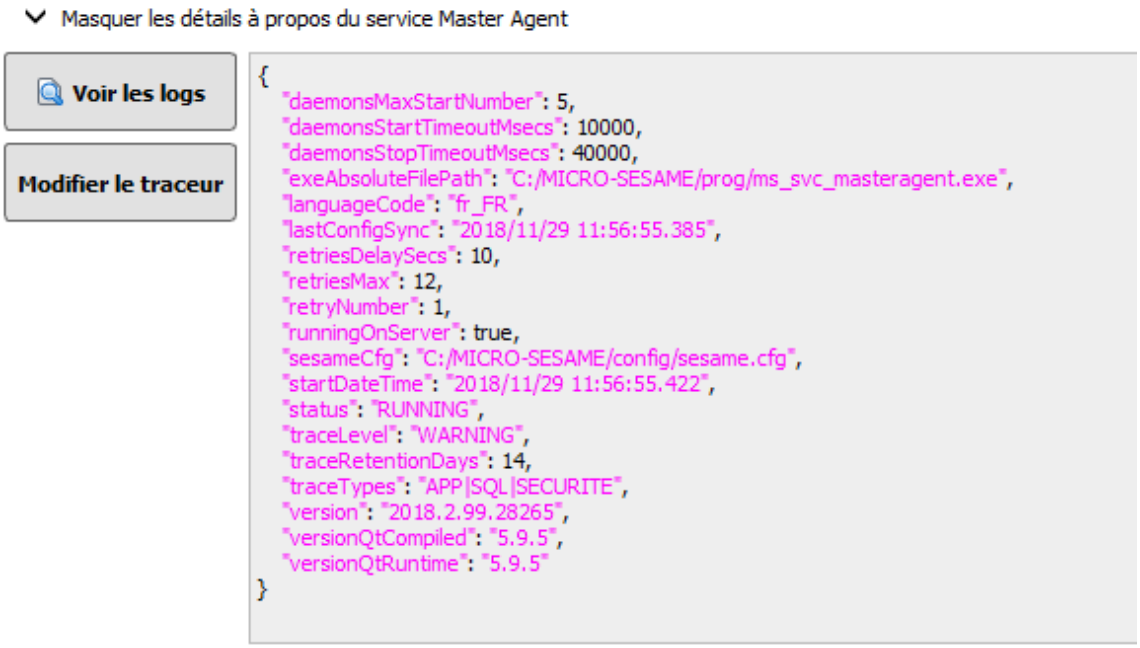
- **Bases de données**
  La base de données doit être fonctionnelle pour que MICROSESAME fonctionne.
  Vérifie que la base des données peut exécuter des requêtes.
  Affiche la taille des fichiers .mdf et .ldf (DATA et LOG) de la base de données.



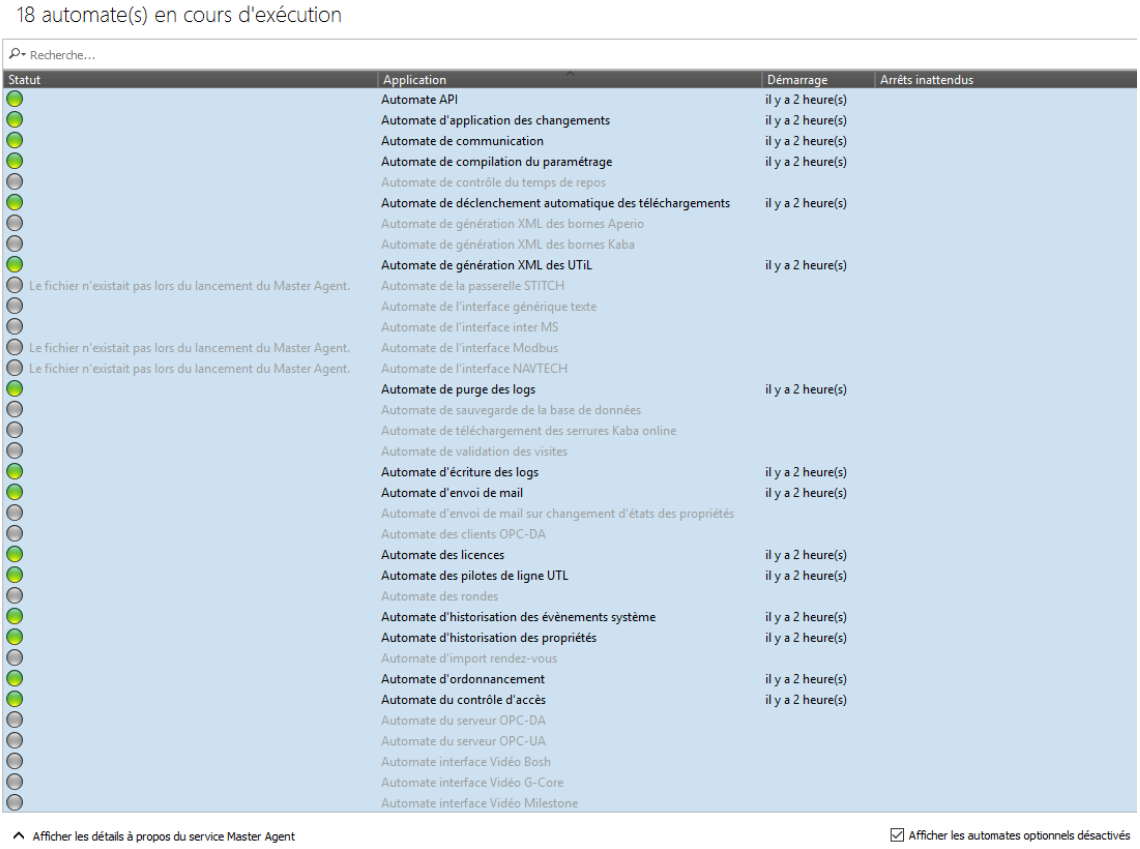
- **Automates**
  La liste affiche les automates en cours d'exécution et quelques informations liés à son statut.
  Les automates sont des exécutables non graphiques dédiés à une tâche.
  Le service Master Agent démarre et contrôle les automates pour le poste serveur.
  Depuis la version 2018.2 de MICROSESAME, ce service est utilisé aussi pour les postes clients (gestion de tâches de fond).
  Faire clic droit pour consulter le menu contextuel avec les actions disponibles :



Cliquer sur **Afficher les détails a propos du service Master Agent** pour déplier cette partie de l'interface :

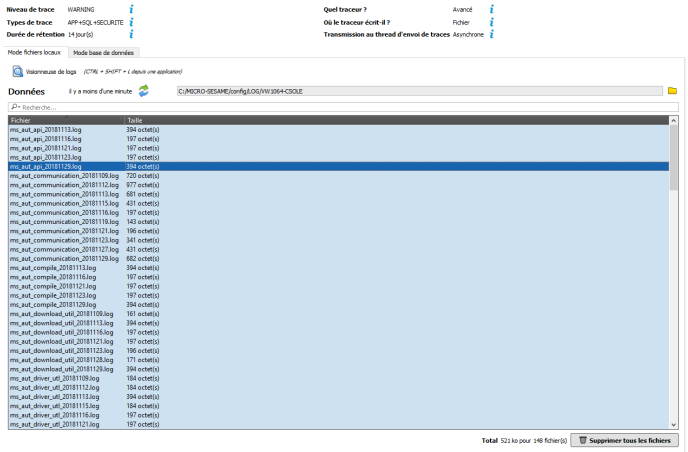


Cocher l'option **Afficher les automates optionnels désactivés** pour consulter la liste complète d'automates

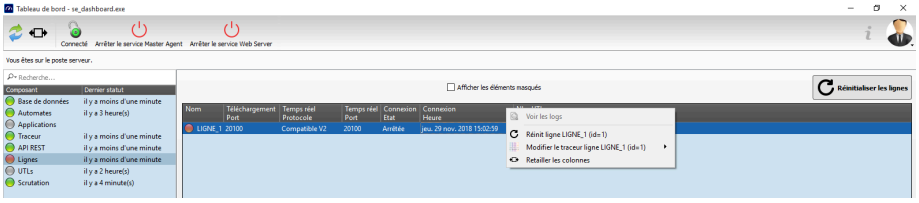


- **Applications**
  La liste contient les applications abonnées à la messagerie.

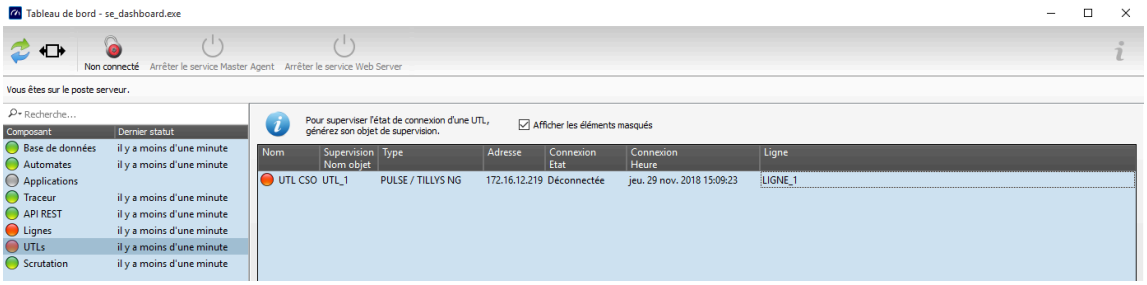
- **Traceur de logs**
  Vérifie que le volume des traces (fichiers logs) n'occupe pas trop d'espace ni ne ralentit le logiciel de contrôle d'accès MICROSESAME.
  Le traceur permet une investigation efficace des problèmes d'exécution de MICROSESAME.
  Cliquer sur un registre affiché pour lancer la visionneuse de logs et le consulter.
  Le bouton **Supprimer tous les fichiers** permet d'effacer tous les registres générés.
  Différents niveaux de trace sont disponibles : Un niveau de trace élevé permet une investigation efficace mais pénalise les performances du système. Le niveau DEBUG, étant le plus élevé, augmente considérablement l'occupation de disque et ralentit le système.
  Consulter le chapitre "Traces - Logs" pour plus de détails.



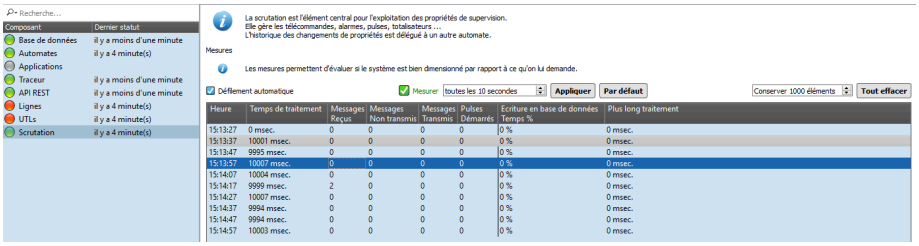
- **API REST**
  Vérifie que les web services "REST" sont accessibles.
  L'API REST nécessite le fonctionnement de l'automate API et du service "TIL-WebServer".
- **Lignes**
  Vérifie le fonctionnement des lignes existantes.
  Réinitialiser les lignes pour rafraîchir les données affichées.
  Cliquer droit pour afficher le menu contextuel avec les options disponibles



- **UTLs**
  Pour supérviser l'état de connexion d'une UTL, générez son objet de supervision depuis la fenêtre de paramétrage de l'UTL (écrire "UTL" dans la barre de recherche du menu principal), à l'aide du menu contextuel (clic droit, **Générer l'objet de supervision**).



- **Scrutation**
  La scrutation est l'élément central pour l'exploitation des propriétés de supervision. Elle gère les télécommandes, alarmes, pulses, totalisateurs ... L'historique des changements de propriétés est délégué à un autre automate.
  Les mesures permettent d'évaluer si le dimensionnement de la machine est approprié.



12.2. Déplacement de données

12.2.1. Présentation du déplacement de données

L'outil de déplacement de données (**til_movedata.exe**) est un outil de maintenance qui facilite le déplacement des données présentes dans la base de données concernant la fiche identifié.

Les données présentes dans des libellés personnalisables peuvent être déplacées ou copiées vers des champs fixes de la fiche identifié.

Les modifications réalisées avec l'outil de déplacement de données seront appliquées sur tous les identifiés présents dans la base de données.

Aussi, la fiche identifié permet d'organiser les valeurs attribués à certains champs.

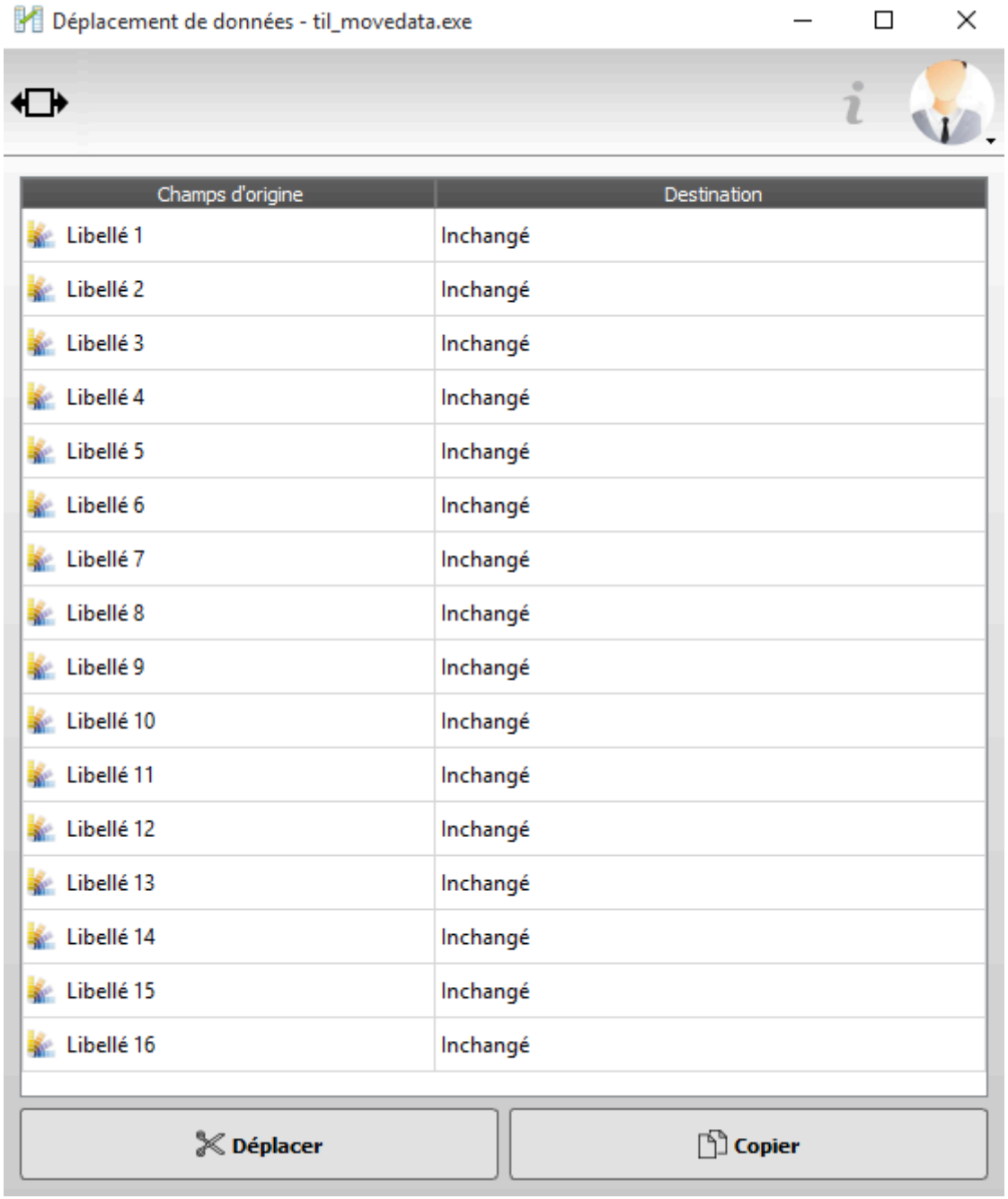
12.2.2. Prerequis

Pour configurer les onglets affichés dans la fiche identifié, suivre **Paramétrage général > Contrôle d'accès > Identifiés**. Pour plus de détails concernant le paramétrage des identifiés, consulter le guide de contrôle d'accès basique.

Afin d'utiliser l'outil de déplacement de données, une connexion ADMINISTRATEUR à MICROSESAME avec les droits opérateurs nécessaires est obligatoire pour pouvoir accéder à cet outil. L'accès à cet outil est contrôlé par le **droit opérateur Maintenance** uniquement disponible par l'**administrateur MICROSESAME**. Pour paramétrer les droits opérateurs, suivre Menu Principal > Paramétrage > Exploitation > Profils opérateurs. Pour plus de détails concernant le paramétrage des droits opérateurs, consulter le guide de contrôle d'accès basique.

12.2.3. Accès

Cet outil est disponible depuis le menu principal de MICROSESAME> Maintenance > Déplacement de données.

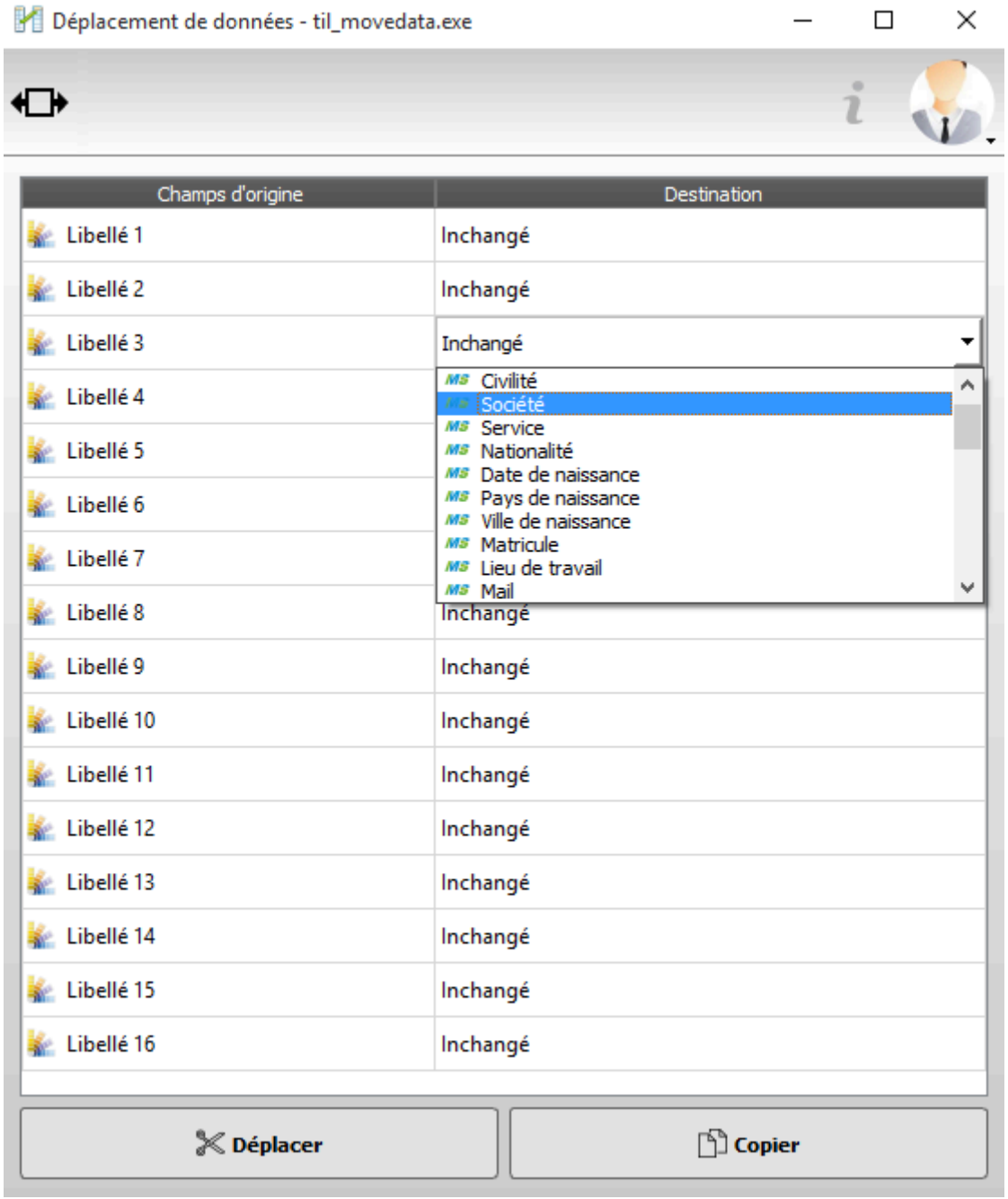


12.2.4. Fonctionnement

Depuis l'outil de déplacement des données :

Dans la colonne de gauche (**Champs d'origine**) se trouvent les données qui sont prêtes à être copiées ou déplacées.

La colonne de droite (**Champs de destination**) contient un menu dépliant avec le liste de champs fixes d'un identifié et la liste de libellés personnalisables. Cette liste est non-paramétrable.



L'utilisateur sélectionne le champ d'origine à modifier et envoie ces données dans le champ de destination souhaité.

Au lancement, l'outil essaye de trouver une correspondance entre les champs d'origine et les champs fixes disponibles. Une sélection est proposé automatiquement.

Les modifications réalisées avec l'outil de déplacement de données seront appliquées sur tous les identifiés présents dans la base de données.

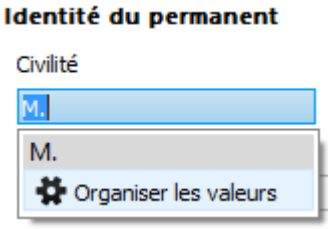
Après avoir placé les données, indiquer l'**action** à réaliser : copier ou déplacer les données.

Lorsque que les modifications sont en cours un pop-up de progression indique l'avancement. Il est possible d'annuler l'opération pendant qu'elle est en cours. En cas d'**annulation**, aucune modification aura été effectuée dans la base de données.

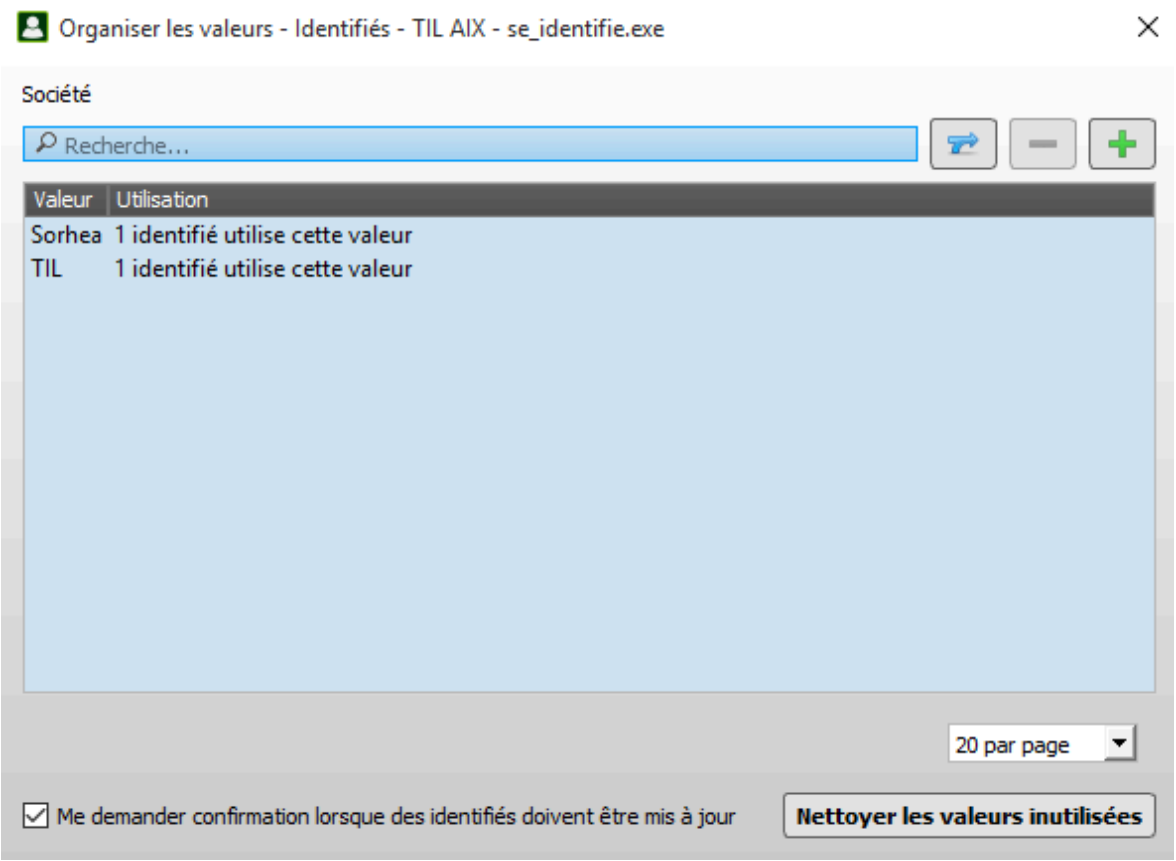
Pour ne pas écraser ou perdre des données, il est fortement recommandé d'effectuer tout les déplacements ou copies en **une seule opération**.

Depuis la fiche identifié

Une fois les données modifiées, certains champs fixes permettent l'organisation des valeurs attribués à ce champ : Sur la ficher identifié, cliquer sur un champ pour l'éditer. L'option **Organiser les valeurs** est proposée.



La fenêtre Organiser les valeurs s'affiche :



- Fusionner permet la fusion de deux valeurs existantes pour le même champ.
- Les boutons + ou - permettent de créer ou de supprimer une valeur existante.
- La barre de recherche permet de chercher entre les différentes valeurs existantes pour ce champ.
- Nettoyer les valeurs inutilisées permet d'effacer des valeurs existante pour ce champ qui ne sont pas utilisées par aucun des identifiés de la base de données.