HIRSCH

MICROSESAME - GUIDE DE DEMARRAGE RAPIDE

GD-10001-FR

05/02/2025

Table des matières

Liste des tableaux

Préface

1. Version logicielle

Les pastilles de couleur marron en haut de chaque page signalent que ce document est un guide de démarrage rapide.

Ce guide décrit comment installer, configurer et mettre en service le logiciel MICROSESAME :

- à partir de sa **version logicielle 2025.x**,
- dans le cadre d'une configuration prédéfinie 8, 16 ou 24 portes,
- avec des lecteurs Evolution *transparents*SCCP,
- dans une configuration non-*ANSSI*.

2. Contexte d'utilisation de ce manuel

Le responsable informatique du site (DSSI) a été prévenu à l'avance et a effectué les opérations décrites dans le chapitre 1. Il est présent lors de l'installation, pour fournir les accès administrateur.

Un partenaire HIRSCH installe MICROSESAME sur un poste serveur et sur un poste client. A l'issue de l'installation, il configure et il teste le fonctionnement de MICROSESAME.

3. 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.

4. Glossaire

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

Administrateur	Profil opérateur par défaut, l'administrateur possède tous les droits et permissions.
Alarme	Propriété qui signale un évènement anormal (intrusion, défaut technique, POTL...).

	Une alarme technique est en surveillance 24 h/24 et elle passe en alarme dès son passage au niveau actif. Une information de détecteurs de type alarme intrusion est en surveillance lorsque leur groupe d'appartenance est armé. Le passage en alarme est donc déterminé non seulement par leur passage à l'état actif mais aussi par l'état d'armement de leur groupe.
ANSSI	Acronyme d'Agence Nationale de Sécurité des Systèmes d'Information. Institution française qui a défini en 2012 pour les sites sensibles des recommandations de sécurité renforcées, lesquelles ont été complétées en 2020 dans la note n° 7. En jargon de la sécurité, on parle de site ANSSI ou non-ANSSI pour en désigner le niveau de sécurisation par rapport aux cyberattaques. Seuls les lecteurs "*transparent*s" sont conformes aux préconisations de l'ANSSI.
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.
Ethernet	Ensemble de protocoles de communication utilisés par les réseaux locaux.

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).
Identifiant	Élément permettant l'accès d'un identifié. Les identifiants peuvent faire appel à plusieurs technologies (porte clé, carte, plaque minéralogique, empreinte digitale, code numérique...) et divers types de lecteur pour les lire.
Identifié	Personne physique devant disposer d'un accès au site protégé par le système de contrôle d'accès. Un identifié peut être porteur d'un ou de plusieurs identifiants distincts. Les identifiés peuvent être : • Des utilisateurs réguliers du système de contrôle d'accès, (identifiés de type "permanent") • Des utilisateurs occasionnels du système de contrôle d'accès dans le cas de visites ou d'interventions externes par exemple, (identifiés de type "visiteur")
IP	Acronyme anglais d'Internet Protocol. Le protocole Internet permet aux équipements qui l'utilisent de communiquer entre eux par paquets, de type *TCP* ou *UDP*. Le protocole IP est transporté par des réseaux locaux filaires utilisant le protocole de connexion Ethernet. Les cartes ou interfaces réseau équipées de connecteurs de type *RJ45* y ont accès physiquement et y sont identifiées logiquement via leur adresse IP.
Lecteur	Dans un système de contrôle d'accès, équipement dont la fonction est d'authentifier une personne. Le lecteur lit un ou plusieurs identifiants présentés par cette personne (authentification simple ou double facteur). L'identifiant peut prendre différentes formes : badge, code clavier, empreinte biométrique, plaque minéralogique... Une fois la personne identifiée, la TILLYS contrôle son accès physique. Selon sa technologie, un lecteur peut être utilisé pour : • Assurer la simple détection du support de l'identifiant, par exemple un lecteur de type "transparent" qui se limite à détecter la présence d'un badge. • Assurer en plus la lecture d'un identifiant standard, par exemple un lecteur "simple" qui ne sait lire que le numéro de série d'un badge (identifiant *CSN*). • Assurer en plus la fonction de déchiffrement d'un identifiant sécurisé encodé dans un badge, par exemple

	un lecteur sécurisé dans lequel on enregistre la clé des badges.
MICROSESAME	Logiciel de supervision unifiée qui permet de centraliser toutes les informations électroniques du bâtiment : contrôle d'accès, détection intrusion, gestion technique, vidéo, interphonie... Le pilotage des différentes fonctions à travers une interface graphique commune rend leur exploitation beaucoup plus simple et les interventions plus efficaces. Les interactions entre les différents systèmes pouvant être complètement automatisées (actions sur évènements), la rapidité des traitements est également garantie.
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.
Opérateur	Employé qualifié pour utiliser *MICROSESAME* en tant que gestionnaire ou utilisateur. On peut lui assigner un profil pour restreindre ses droits, ses permissions et pour adapter les options visibles de l'interface correspondant à ses fonctions.
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.
PKCS#12	Format binaire de fichier utilisé en cryptographie. Ce type de fichier contient un certificat X.509 et une clé privée. Ces fichiers possèdent une extension .pfx et leur accès est protégé par mot de passe.
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.
SQL Server	Moteur de base de données gérant les informations d'une base de données. SQL Server utilise pour ceci des requêtes, basées sur un langage qui lui est propre.
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.
Synoptique	Représentation graphique d'une installation physique dans *MICROSESAME*. Sur un clavier intrusion, cette option permet d'afficher le visuel sur lequel les différents groupes de détecteurs définis sur la TILLYS peuvent être visualisés.

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*.
Transparent	Désigne la capacité d'un lecteur à gérer les aspects de cryptage conformément aux préconisations de l'ANSSI, qui précisent que le lecteur ne doit contenir aucune clé. Il se contente donc de lire la carte et de transmettre les informations lues à la *TILLYS* : il n'est pas capable de déterminer de manière autonome s'il peut ou non autoriser l'accès.
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. Préparation de l'installation de MICROSESAME par le DSSI

1.1. Liste des opérations préliminaires à l'installation de MICROSESAME

Effectuez les opérations listées dans le tableau ci-après.

Tableau 1.1. Opérations préliminaires à l'installation de MICROSESAME

A faire	Comment le faire
Préparez toutes les informations nécessaires à l'installation de MICROSESAME.	Imprimez la *Section 1.2, « Fiche de renseignements pour l'installation de MICROSESAME »* et la remplir.
Vérifiez que les *ports* indispensables au fonctionnement de MICROSESAME ne sont pas utilisés par une autre application et sont ouverts. Il s'agit des ports 80, 443, 14001 à 14005, 22, PING/ICMP, 443, 5353, 11010 et 55000.	Consultez la liste des ports dans la section Schémas des flux et ports MICROSESAME dans ce guide.
Installez le serveur MICROSESAME sur un serveur physique ou virtuel dédié. Le dimensionnement du serveur à utiliser dépend de la taille du site.	Réservez un serveur physique ou créez une machine virtuelle. La configuration de ce serveur doit être définitive (serveur de production).
Attribuez une adresse IP fixe au poste serveur, pour éviter les erreurs d'adressage qui peuvent se produire lorsque le nom d'hôte est utilisé.	Vérifiez que le serveur possède une adresse IP fixe. Si le serveur ne possède qu'un nom d'hôte, attribuez-lui une adresse IP fixe. Notez l'adresse IP fixe du serveur sur la fiche de renseignements imprimée.
Mettez à jour le serveur (réel ou virtuel) et le client avec les derniers patchs de sécurité Windows.	Vérifiez dans les informations système que le serveur et le client sont à jour des mises à jour Windows. Si ce n'est pas le cas, installez les dernières mises à jour de sécurité.
Configurez l'antivirus installé de manière à ne pas perturber le fonctionnement de MICROSESAME.	Excluez de l'analyse le répertoire <MICROSESAME> / Prog.

1.2. Fiche de renseignements pour l'installation de MICROSESAME

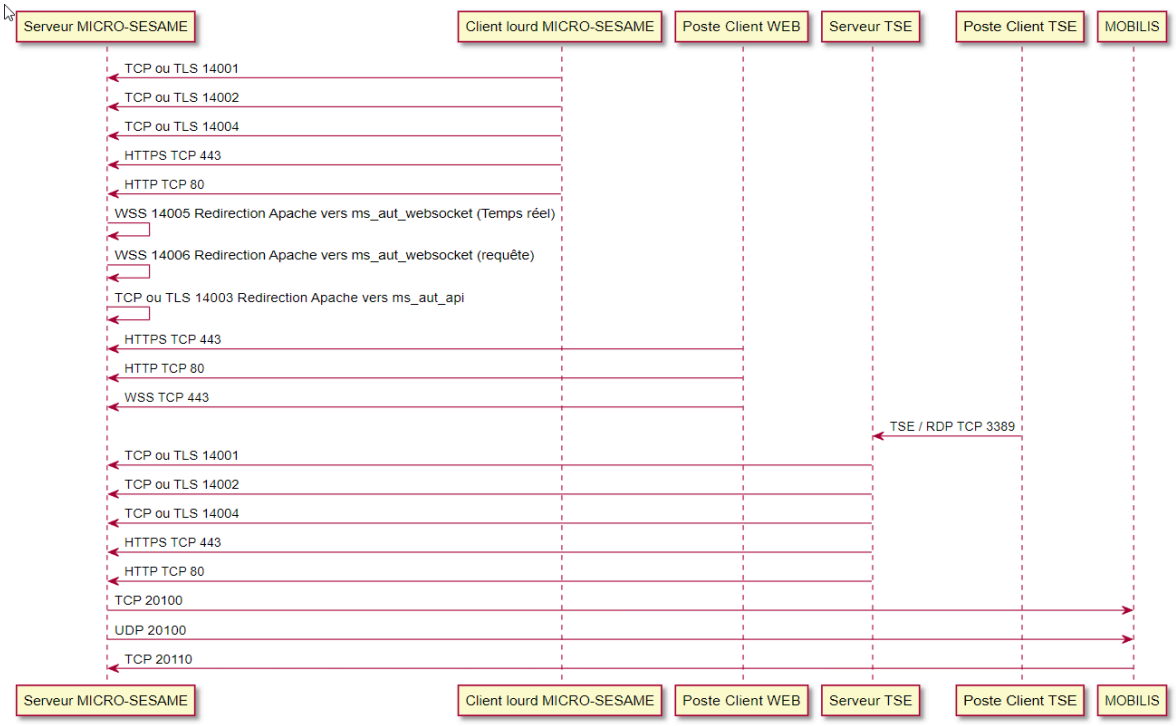
Imprimez cette page et reportez les informations du site dans la colonne de droite, pour pouvoir aider le partenaire HIRSCH lors de l'installation de MICROSESAME.

Tableau 1.2. Tableau des informations d'installation de MICROSESAME

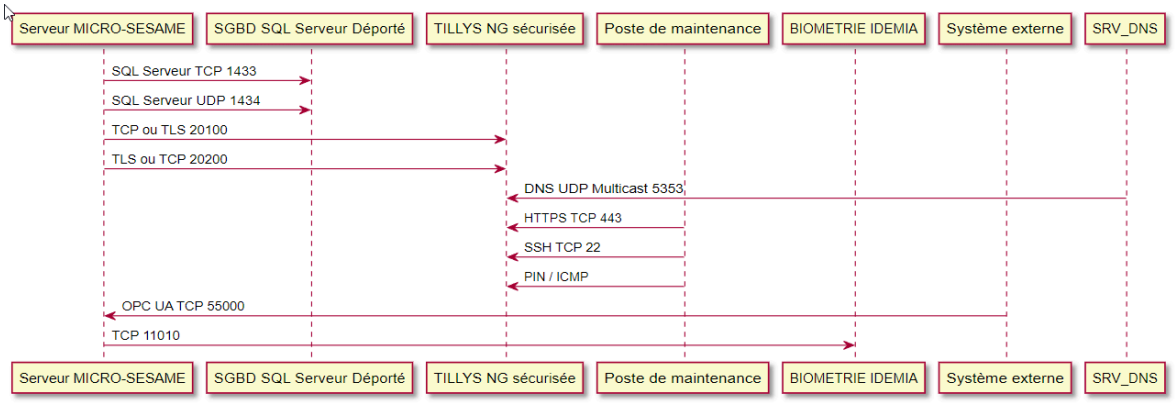
Information	Colonne pour saisir vos informations
Adresse IP du serveur MICROSESAME	.....
Nom du serveur SQL (si un serveur est déjà installé)	.....
Nom de l'instance SQL	.....
Nom de la base de données en lettres majuscules, minuscules ou chiffres (jamais de chiffre comme premier caractère et aucun espace)	.....
Nom du pilote de base de données (si spécifique)	.....
Nom utilisateur	.....
Mot de passe utilisateur	.....
Nom administrateur	.....
Mot de passe administrateur	.....

1.3. Ports nécessaires au fonctionnement ANSSI de MICROSESAME

Pour le fonctionnement de MICROSESAME, les *ports* présentés sur le schéma des flux ci-après doivent obligatoirement être ouverts. Ce schéma correspond à une installation certifiée **ANSSI** utilisant le driver **SQL TIL** pour l'installation des **postes clients**.



Les ports et flux représentés sur la figure suivante ne sont modifiables qu'à condition de spécifier de manière cohérente les nouvelles valeurs au niveau des logiciels et matériels interconnectés.



Chapitre 2. Installer et configurer MICROSESAME

Le responsable informatique du site (DSSI) doit être présent, avec le *Tableau 1.2, « Tableau des informations d'installation de MICROSESAME »* rempli.

Un partenaire HIRSCH procède à l'installation et à la configuration de MICROSESAME.

2.1. Installer MICROSESAME sur un poste serveur

2.1.1. Installer SQL Server Express

Si une base de données existe déjà sur le site, passez aux instructions de la section suivante.

Si aucune base de données n'a été installée, HIRSCH préconise d'installer *SQL Server* Express :

1. Copiez *l'assistant d'installation de Microsoft SQL Server Express* sur le bureau du poste serveur.
2. Double-cliquez sur l'icône de ***Microsoft SQL Server Express.exe*** et suivez les instructions d'installation.

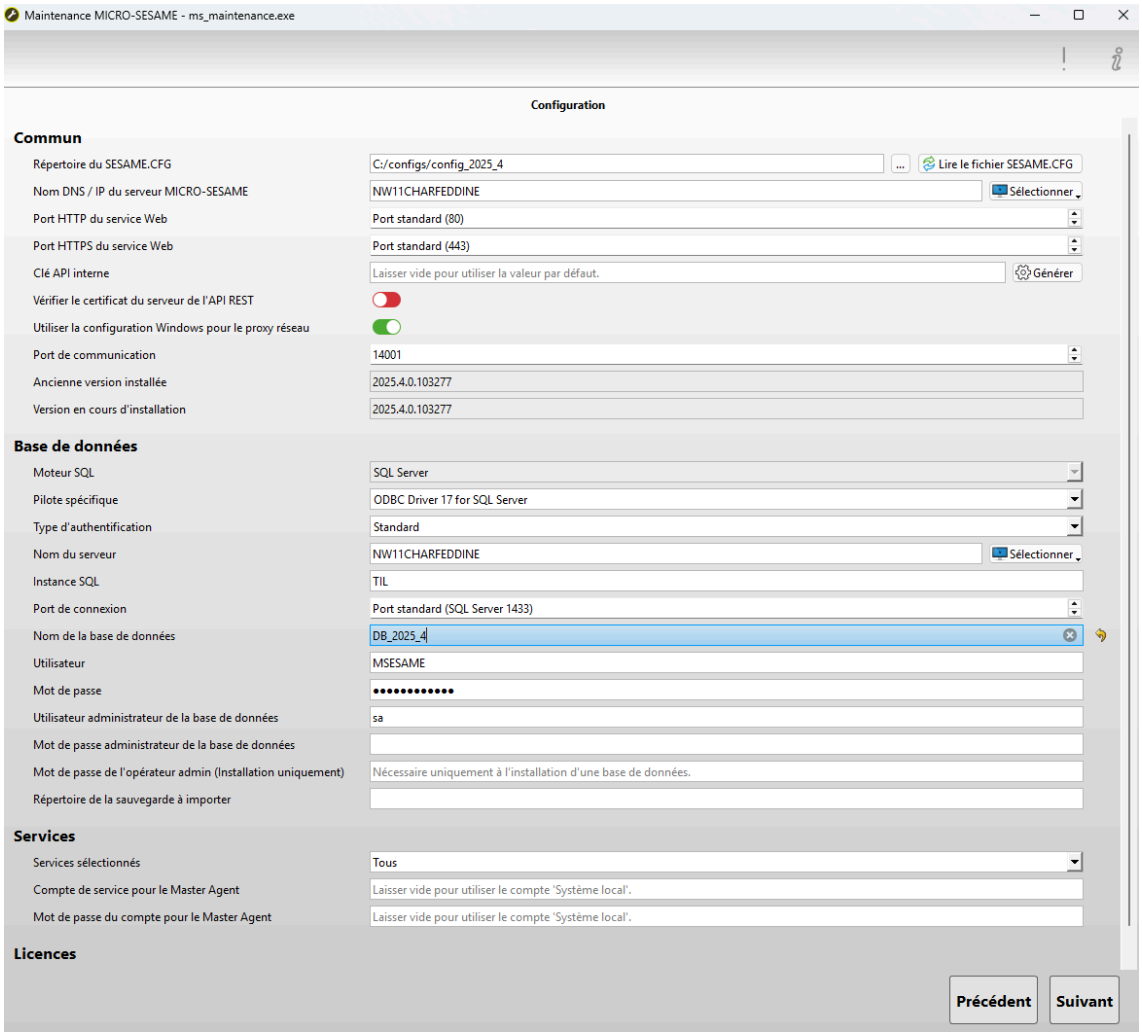
2.1.2. Installer MICROSESAME version serveur

1. Copiez *l'assistant d'installation de MICROSESAME version serveur* sur le bureau du poste serveur.
2. En bas à gauche de l'écran, cliquez sur l'icône Démarrer, puis sur l'icône Compte utilisateur, et sur l'icône Modifier les paramètres de compte.
   Le profil doit être du type *administrateur*. Si ce n'est pas le cas, demandez au DSSI d'ouvrir une session *administrateur*.
3. Sur le bureau, faites un clic droit sur l'icône du programme **MSesameInstallerServeur_20xx.x.x.exe**, choisissez **Exécuter en tant qu'administrateur**, puis autorisez les modifications. L'écran d'installation s'affiche après quelques secondes.
4. Cliquez sur le bouton Suivant. Le répertoire d'installation par défaut s'affiche.
5. Vérifiez que tous les composants sont cochés (ou cliquer sur **Sélectionner tout**), puis cliquez sur Suivant. L'assistant d'installation est prêt à être installé.
6. Cliquez sur Suivant (l'espace disque requis pour l'installation est indiqué), puis sur Installer. La barre de progression de l'installation s'affiche.
7. En fin d'installation, cliquez sur Suivant. L'écran d'installation est remplacé par l'outil de maintenance de MICROSESAME.
8. Continuez à la section *Section 2.1.3, « Configurer la base de données »*.

2.1.3. Configurer la base de données

L'écran d'accueil de l'outil de maintenance de MICROSESAME (MS Maintenance) affiche trois icônes pour trois options différentes : Création, Migration et Restauration.

1. Cliquez sur l'icône **Création**. L'écran de configuration s'affiche.



2. Modifiez les valeurs par défaut selon des tableaux ci-après.

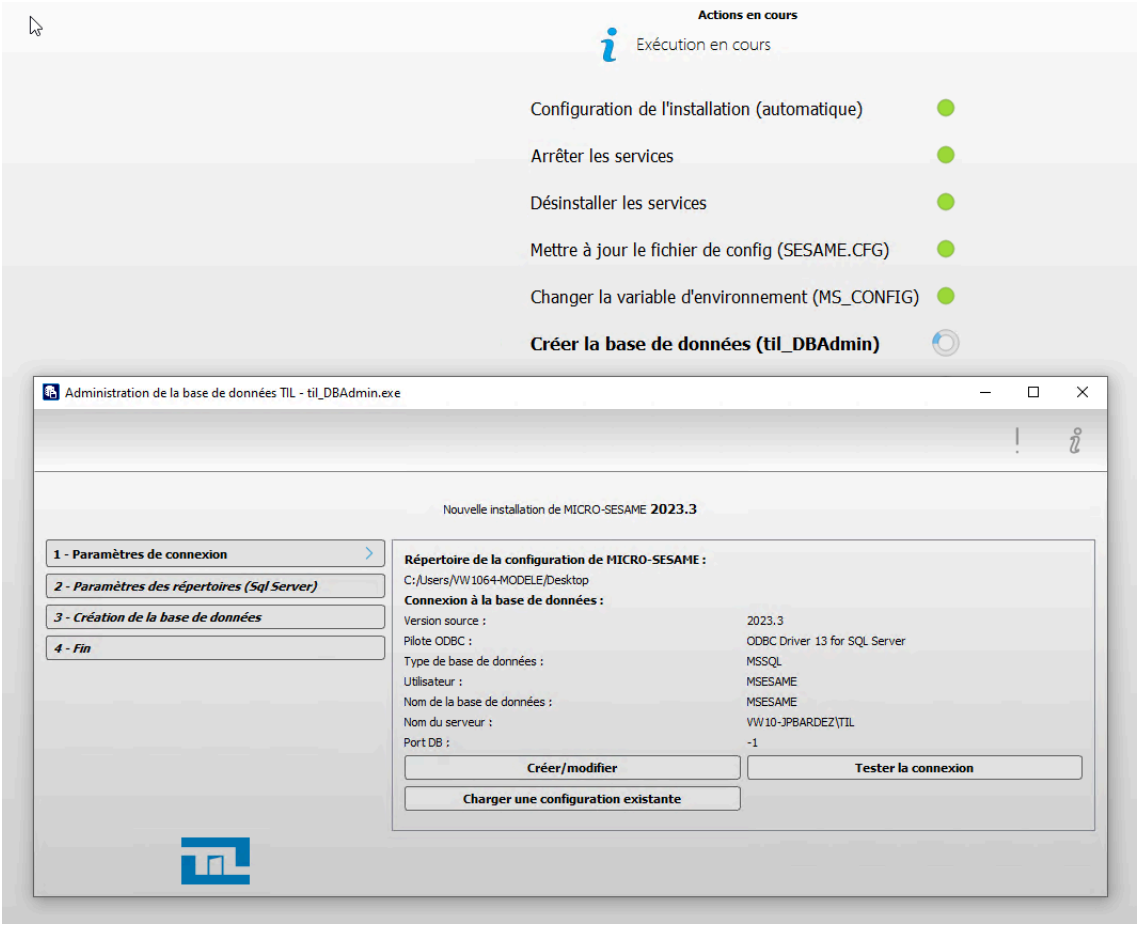
Tableau 2.1. Paramètres de configuration du serveur MICROSESAME

Section Commun	Action
Répertoire du fichier SESAME.CFG	Il est conseillé de modifier le nom du répertoire d'installation du fichier de configuration. Par exemple C:/ MICROSESAME**/Config**. Pour modifier le répertoire par défaut, cliquer sur le bouton [...]. En plus du fichier de configuration, ce dossier accueille les logs et les certificats.
Nom DNS/IP	Si l'adresse IP de la machine ne s'affiche pas automatiquement, cliquer sur [Sélectionner V] et choisir l'adresse IP dans la liste (voir *Tableau 1.2, « Tableau*

Section Commun	Action
	des informations d'installation de MICROSESAME ».).
Port HTTP du service Web (80) Port HTTPS du service web (443)	Ces ports par défaut peuvent être modifiés (par exemple, en 81 et 444) si une autre application les utilise déjà.
Vérifier le certificat de l'API REST	Oui, sauf si le certificat est autosigné.
Utiliser la configuration Windows pour le proxy réseau	Se référer à l'administrateur réseau.
Port de communication (14001)	14001 par défaut.
Section Base de données	**Action**
Moteur SQL	Par défaut *SQL Server*. Pour installer un système de base de données sous ORACLE, contacter le Support HIRSCH .
Pilote spécifique	Voir tableau *Tableau 1.2, « Tableau des informations d'installation de MICROSESAME »*.
Nom du serveur	DNS (nom de domaine) ou adresse IP
Instance SQL	TIL par défaut (si le moteur de base de données a été installé avec le programme d'installation HIRSCH).
Port de connexion (1433)	1433 par défaut.
Nom de la base de données	MSESAME par défaut. S'il est nécessaire de modifier, utiliser uniquement des lettres minuscules, majuscules ou des chiffres (mais pas en première position).
Utilisateur	**MSESAME** par défaut.
Mot de passe	**MSES@ME_1111** par défaut. Après modification, le noter dans le *Tableau 1.2, « Tableau des informations d'installation de MICROSESAME »*.
Utilisateur administrateur de la base de données	**sa** par défaut.
Mot de passe administrateur de la base de données	Facultatif : saisissez un mot de passe. Après saisie, le noter dans le *Tableau 1.2, « Tableau des informations d'installation de MICROSESAME »*. Le mot de passe saisi à cette étape sera pris en compte lors de l'installation.

Section Base de données	Action
Mot de passe de l'opérateur admin (Installation uniquement)	Nécessaire uniquement à l'installation d'une base de données.
Répertoire de la sauvegarde à importer	Vide par défaut. Pour effectuer la restauration d'une sauvegarde, indiquer le répertoire de cette sauvegarde.
Section Services	**Action**
	Ne rien modifier.
Section Licences	**Action**
Fichier de licence	Si un fichier licence est disponible (fichier TLIC), il est possible de le charger dès maintenant. Cliquer sur '**...**' et sélectionner le fichier licence à importer, à l'aide de l'explorateur de fichiers. Le fichier de licence peut également être installé plus tard. Son absence ne bloque pas l'étape de configuration de MICROSESAME.

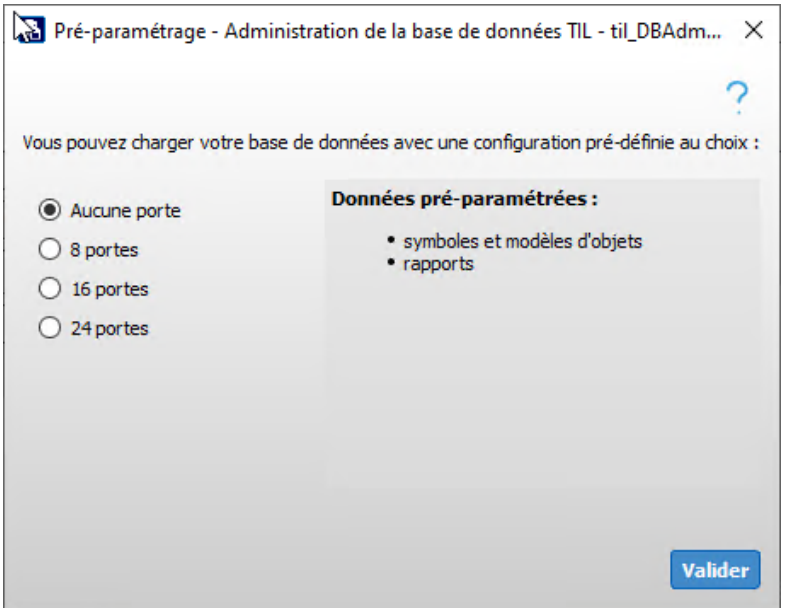
3. Cliquez sur Suivant. Le menu d'administration qui apparaît en surimpression donne accès à 4 boutons de paramétrage et affiche les paramètres de la connexion.



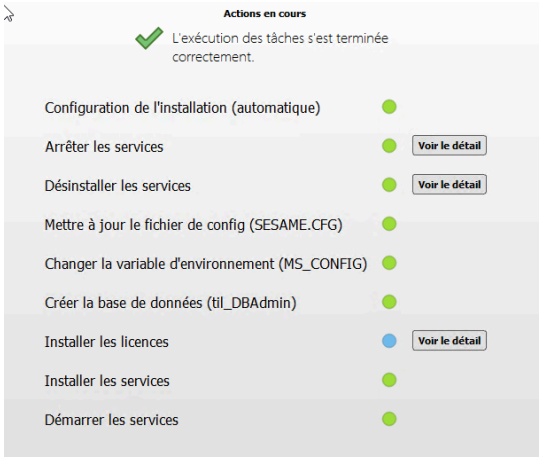
4. Suivez les instructions du tableau suivant.

Tableau 2.2. Création de la base de données

Sous-menu	Opérations à effectuer
1 - Paramètres de connexion	1) Cliquez sur Créer/modifier. 2) Vérifiez l'exactitude du nom du serveur. Dans le doute, cliquez sur l'icône Recharger. 3) Dans le champ **Port de connexion**, vérifiez que la valeur 433 s'affiche. 4) Renseignez le **Mot de passe** de connexion utilisateur défini lors de la configuration de la base de données et confirmez-le. Pour vérifier la correspondance entre le mot de passe et sa confirmation, cochez la case **Visible**. 5) Cliquez sur Valider et, si un message s'affiche demandant le remplacement du fichier SESAME.CFG, cliquez sur Oui.
2 - Paramètres des répertoires (SQL Server)	6) Cochez la case **Utiliser les répertoires par défaut** du serveur de base de données.

Sous-menu	Opérations à effectuer
	7) Si le moteur de la base de données a été installé avec l'application fournie par HIRSCH, saissez le mot de passe **TIL-technologies** (s'il s'agit d'une autre base de données, saisissez le mot de passe choisi lors de sa création), puis cliquez sur Tester la connexion. Une coche verte apparaît lorsque la connexion au serveur SQL est établie.
3 - Création de la base de données	8) Cochez la case **Exécuter automatiquement les tâches suivantes**. 9) Cliquez sur Créer la base de données. La fenêtre de pré-paramétrage s'affiche.  10) Pour faciliter la mise en service, sélectionnez l'une des 3 options 8 portes, 16 portes ou 24 portes, puis cliquez sur Valider. Une fenêtre de mise à jour de l'adresse IP s'affiche. 11) S'il existe plusieurs cartes réseau sur le serveur, choisissez l'**Adresse IP vue par le matériel**dans la liste déroulante, puis cliquez sur Valider. La création de la base de données prend plusieurs minutes. 12) Fermez la fenêtre de fin de création qui s'affiche lorsque la base de données est créée : l'installation et le

Sous-menu	Opérations à effectuer
	démarrage des services prend encore plusieurs minutes avant l'affichage de l'écran de fin de configuration.

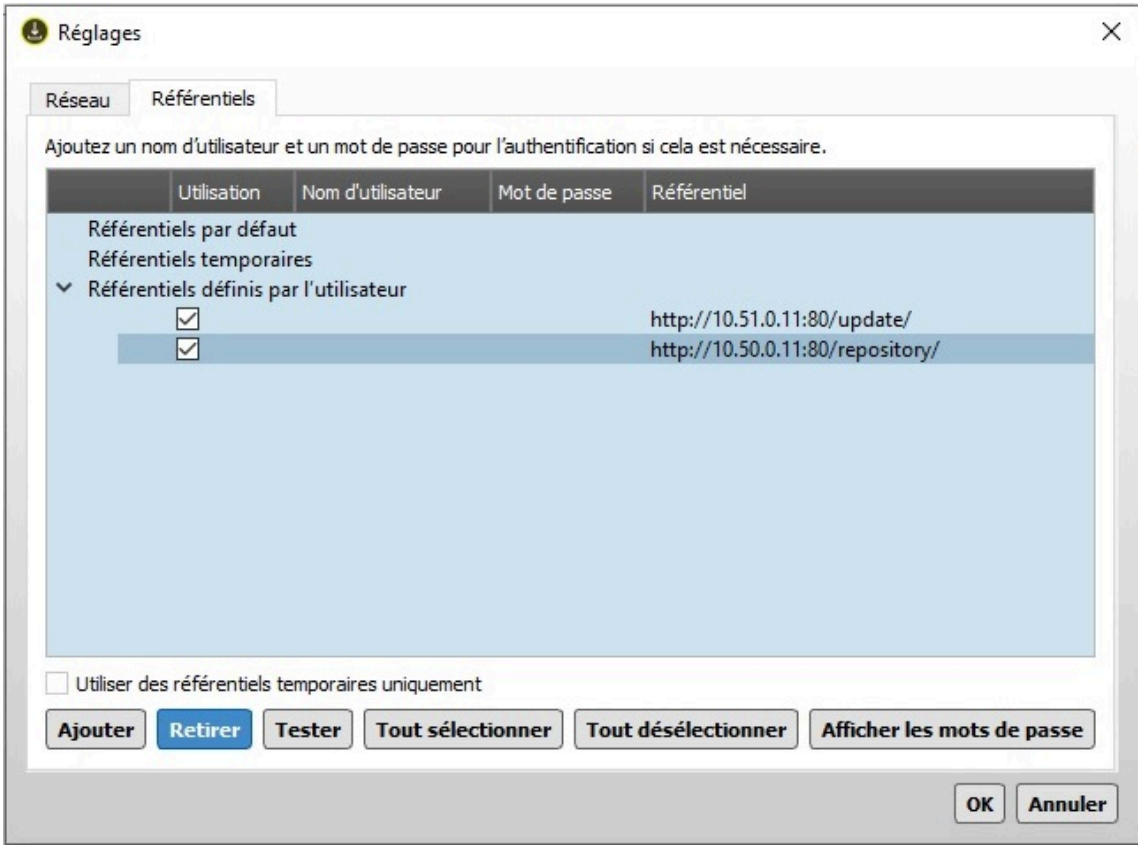


5. Pour que les changements soient pris en compte, si la configuration s'est effectuée sans erreur, cliquez sur Quitter. L'écran de configuration disparaît et les raccourcis des 7 modules MICROSESAME sont créés sur le bureau.

2.2. Installer un poste client MICROSESAME

Le *poste client* doit être raccordé au même réseau *Ethernet* que le *poste serveur*.

1. Copiez *l'assistant d'installation de MICROSESAME version client* sur le bureau du poste client.
2. En bas à gauche de l'écran, cliquez sur l'icône **Démarrer**, cliquez sur l'icône **Compte utilisateur**, puis sur **Modifier les paramètres de compte** : le profil doit être du type *administrateur*. Si ce n'est pas le cas, ouvrez une session administrateur.
3. Sur le bureau, faites un clic droit sur l'icône du programme **MSesameInstallerClient_20xx.x.x.exe**, choisissez **Exécuter en tant qu'administrateur**, puis autorisez les modifications. L'écran d'installation s'affiche après quelques secondes.
4. En bas à gauche de l'écran d'installation, cliquez sur le bouton **Réglages**.
5. Cliquez sur **Aucun proxy** (ou renseigner les informations de proxy), puis cliquez sur **Référentiels**.
6. Sous la ligne *Référentiel défini par l'utilisateur*, sur les deux lignes http:// mentionnant**update** et **repository** , remplacez "*hostname*" par l'adresse IP ou le nom du serveur.



Protocoles http et https :
L'utilisation du protocole **https** est recommandée. Dans ce cas, remplacez le port 80 par le port **443**.
Afin de pouvoir utiliser un référentiel en https, un certificat valide est nécessaire sur le poste client.
Pour plus de détails, consultez *Mise en place de certificats TLS signés*.

7. Sur les deux lignes, remplacez "hostname" par l'adresse IP du poste serveur, puis cliquez sur **Tester**.
8. Cliquez sur **Suivant**.
9. Par défaut l'assistant propose d'installer MICROSESAME dans le répertoire C:\MICROSESAME (laisser par défaut C:\MICROSESAME installera les programmes automatiquement dans un sous-répertoire **prog**). Utilisez **Parcourir** pour définir éventuellement un autre dossier, puis cliquez sur **Suivant**.
10. Sélectionnez éventuellement les composants que vous ne souhaitez pas installer, en fonction du profil de l'utilisateur du poste client (par exemple, l'utilisation ou non des outils de maintenance), puis cliquez sur **Suivant** .
11. Décochez éventuellement la case d'installation de certains raccourcis bureau, puis cliquez sur **Suivant**. L'assistant d'installation est prêt à installer et l'espace disque requis pour l'installation est indiqué.
12. Pour lancer l'installation, cliquez sur **Installer**. L'installation dure quelques minutes (une barre de progression s'affiche).
13. Cliquez sur **Installer poste client**. Une fenêtre de connexion s'affiche.
14. Saisissez le login/mot de passe administrateur.

15. Cliquez sur le bouton **Quitter**. L'écran de configuration disparaît et les raccourcis des 7 modules MICROSESAME sont créés sur le bureau.

2.3. Configurer MICROSESAME

Un partenaire HIRSCH procède à la configuration de MICROSESAME.

2.3.1. Lancer le menu principal de MICROSESAME et naviguer

1. Double-cliquez sur le raccourci **Menu principal** sur le bureau. La fenêtre de connexion à MICROSESAME s'ouvre.
2. Saisissez le login/mot de passe administrateur par défaut (admin/1111). Le menu principal s'affiche.

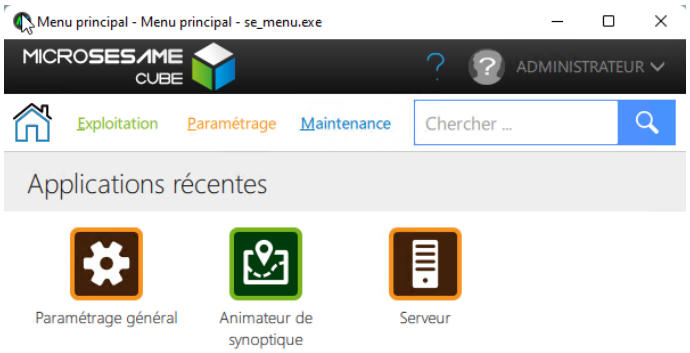


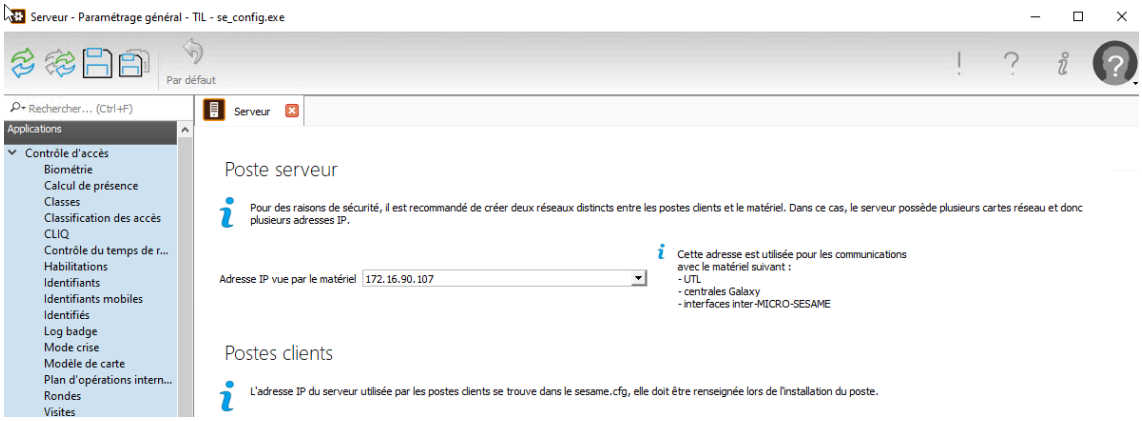
Tableau 2.3. Navigation dans MICROSESAME

Fonction de l'interface utilisateur	Actions
Accéder à un écran	Pour accéder à un écran, vous pouvez taper les trois premières lettres de la fonction recherchée dans le champ de recherche (ou naviguer en utilisant les trois options de couleur du menu (Exploitation, Paramétrage ou Maintenance) et les icônes suivantes. Dans les deux cas, une fenêtre s'affiche en surimpression. Exemple de **Fil d'Ariane >** et de **raccourci**) : Dans le menu principal du poste serveur, suivre **Paramétrage > Matériel > Serveur SER**.
Écrans fréquemment utilisés	Sans action spécifique, les derniers écrans utilisés s'affichent en haut de la liste. Pour les fonctions les plus utilisées, cliquez sur l'étoile jaune sur fond bleu, pour ajouter l'écran correspondant dans les favoris du navigateur.

2.3.2. Vérifier la communication entre le poste serveur et les UTL

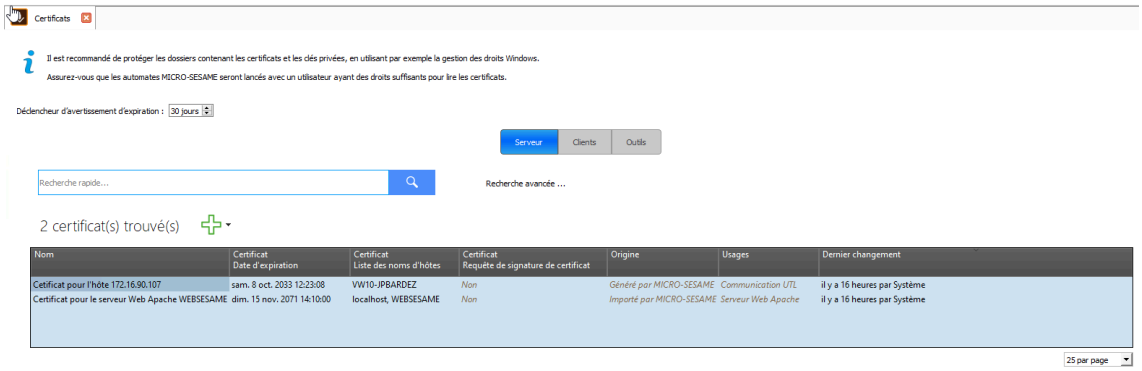
2.3.2.1. Vérifier la connexion IP

1. À partir du menu principal du poste serveur de MS, accédez à l'écran de paramétrage du **Serveur** (Paramétrage > Matériel > Serveur).
2. Vérifiez que **l'adresse IP vue par le matériel** correspond à l'adresse IP du poste serveur. Si ce n'est pas le cas, entrez la valeur correcte et cliquez sur **Enregistrer**, dans la barre supérieure de la fenêtre.



2.3.2.2. Vérifier les certificats

1. À partir du menu principal du poste serveur de MS, accédez à l'écran de **paramétrage** des **Certificats** (Paramétrage > Autres... > Paramétrage général > Système > Certificats).



2. Vérifiez que le champ **Nom** mentionne la présence d'un **Certificat TLS pour l'hôte "adresse du serveur"** et que la colonne **Usages** mentionne **Communication UTL**. Si ce n'est pas le cas, cliquez sur la croix verte, puis choisissez les usages de ce nouveau certificat (au moins *UTL*) et cliquez sur**Générer un certificat auto-signé**.

2.3.3. Installer des licences sur le poste serveur

Suite à votre commande, vous avez reçu un mail de **livraison@til-technologies.fr** contenant les informations suivantes :

- Lien vers l'espace web pour générer le fichier de licence: *https://licence.til-technologies.fr/*
- Login
- Mot de passe

Pour installer les licences sur le poste serveur :

1. Dans la barre d'état de MS en bas de l'écran, cliquez sur **MICROSESAME 20xx.x** .
2. Cliquez sur **Générer une demande de licences**. La fenêtre Paramètres de licence s'affiche.

Tableau 2.4. Champs de la fenêtre Poste serveur

Champ	Action
Code affaire	Obligatoire. Code référence présent sur le bon de commande HIRSCH .
Nom du site	Obligatoire.
Numéro de clé	S'applique uniquement au numéro de clé partenaire.
Dénomination serveur	Facultatif. Description personnalisée.
Adresse	Facultatif.
Complément d'adresse	Facultatif.
Code postal, ville	Facultatif.

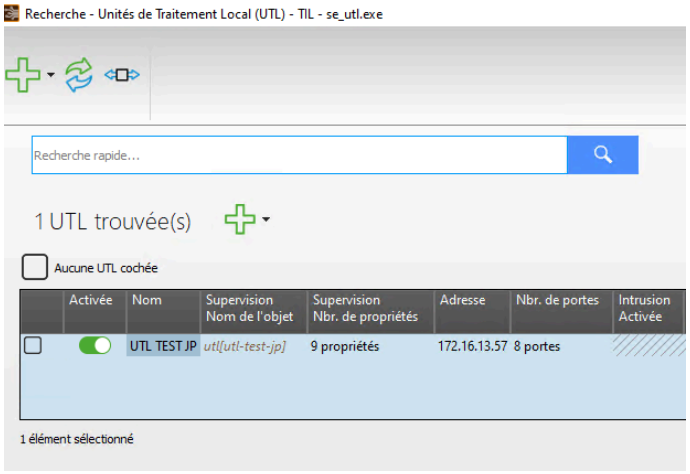
3. Renseignez au moins les deux premiers champs, puis cliquez sur **Générer le fichier d'identification de machine**.
4. Indiquez le dossier (par exemple, Téléchargement) dans lequel enregistrer le fichier empreinte du serveur **.TLOC**.
5. Saisissez *https://licence.til-technologies.fr/* dans la barre de recherche d'un navigateur web, puis entrer le login et le mot de passe d'accès à l'extranet des licences qui vous ont été envoyés par e-mail.
6. Cliquez sur le **Numéro de clé** associé à votre commande.
7. Téléversez le fichier **.TLOC** précédemment sauvegardé.
8. Téléchargez en retour le fichier **.TLIC** (fichier de licence final pour le serveur).
9. Dans la barre d'état en bas de l'écran, cliquez sur **MICROSESAME 20xx.x**.
10. Cliquez sur **Installer un fichier de licences**. Un message vous informe que le fichier de licence va être ajouté et remplacera le précédent.
11. Cliquez sur **Oui**.
12. Sélectionnez le fichier **.TLIC** à télécharger et attendez le message de validation d'installation.

2.3.4. Charger une configuration prédéfinie sur le poste serveur

Lors du chargement d'une configuration prédéfinie, MICROSESAME propose de créer toute une série de données interdépendantes. Ceci permet de gagner du temps pour la configuration du site.

Par contre, la modification des portes types configurées par MICROSESAME peut entraîner une incohérence des paramètres lors de la mise en service. Il est donc très fortement conseillé de **ne rien supprimer**.

1. À partir du menu principal du poste serveur de MS, accédez à l'écran de **paramétrage** des **UTL** (Paramétrage > Matériel > Unités de traitement local (UTL)).



2. Faites un double clic sur le nom de l'*UTL* créée lors de la configuration prédéfinie.
3. Remplacez l'adresse IP par défaut (172.16.5.239) par celle définie dans la TILLYS.
4. Vérifiez que le modèle de TILLYS proposé (TILLYS CUBE) correspond à celui de la TILLYS installée (sinon, cliquez sur le modèle correct dans la liste déroulante).
5. Dans l'onglet **Modules déportés**, dans la liste déroulante, cliquez sur la valeur correspondant au type de fonctionnement de chacun des trois bus.
6. Dans l'onglet **Contrôle d'accès**, vérifiez que toutes les icône présentes dans la colonne **Licence** (cubes) apparaissent bien en couleur (bleue/verte). Sinon, cliquez dans la cellule pour faire apparaître l'icône. Vérifiez également que tous les lecteurs sont activés (interrupteurs en vert). Pour faciliter la navigation, renommez les objets créés afin de les faire correspondre à l'architecture du site (donnez des noms significatifs aux portes et aux lecteurs).
7. Dans la barre supérieure de la fenêtre, cliquez sur **Compiler**.

2.3.5. Créer et configurer une nouvelle porte

Pour créer une nouvelle porte et pour la configurer manuellement, consultez le *Guide de création et de paramétrage des objets porte*.

2.3.6. Configurer MICROSESAME et modifier le paramétrage de la TILLYS

Après chaque modification du paramétrage de MICROSESAME, vous devez appliquer cette procédure, afin que les changements soient pris en compte au niveau de la TILLYS.

1. À partir du menu principal du poste serveur de MS, accédez à l'écran de d'**application du paramétrage** (Paramétrage > Mise en exploitation > Appliquer le paramétrage).
2. Dans la barre supérieure de la fenêtre, cliquez sur **Simple**.
3. Cliquez sur **Compiler le paramétrage**, puis sur **Tout compiler** (cette opération prend quelques minutes).
4. Cliquez sur **Appliquer les changements**, sur **Appliquer les changements aux propriétés**, puis sur **Exécuter**.
5. Toujours dans l'onglet **Appliquer les changements**, choisissez **Appliquer les changements aux lignes**, puis cliquez sur **Exécuter**.
6. Cliquez sur **Télécharger**, puis sur **Complet**. À l'affichage du message de fin d'envoi, MICROSESAME est opérationnel.

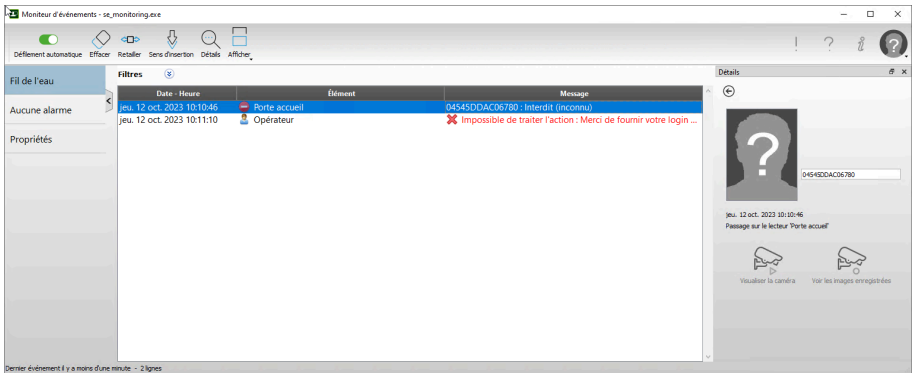
Continuez au chapitre *Chapitre 3, Mettre le contrôle d'accès en service*.

Chapitre 3. Mettre le contrôle d'accès en service

Un partenaire HIRSCH procède à la mise en service du contrôle d'accès de MICROSESAME.

3.1. Acquérir un identifiant non attribué dans MICROSESAME

1. À partir du menu principal de MS, accédez à l'écran d'exploitation du **Moniteur d'évènements** (Exploitation > Supervision > Moniteur d'évènements).
2. Passez un badge non attribué devant un lecteur de contrôle d'accès. Un signal sonore indique que le lecteur fonctionne mais l'accès est interdit car le badge est inconnu (il n'a pas encore été attribué).
   Son *identifiant* a été acquis par MICROSESAME (il est visible dans le moniteur d'événements) et il est disponible pour un nouvel identifié.
   Si le lecteur n'émet pas de signal sonore/visuel, reportez-vous à l'erreur 00003 dans la section Résolution de problèmes.
3. Cliquez sur l'icône **[Détails]**, en haut à gauche de l'écran. Le détail du badge apparaît dans la fenêtre de droite.



4. À droite de l'emplacement de la photo, placez l'identifiant en surbrillance avec la souris et tapez CTRL + C.
   L'identifiant est copié en mémoire.
5. Continuez à la section *Section 3.2, « Affecter un identifiant disponible à un nouvel identifié »*.

3.2. Affecter un identifiant disponible à un nouvel identifié

1. À partir du menu principal de MS, accédez à l'écran d'exploitation des **Identifiés** (Exploitation > Contrôle d'accès > Identifiés).
2. En haut à gauche de l'écran, cliquez sur **Ajouter** , renseignez le nom et le prénom du nouvel identifié, puis cliquez sur Créer.
3. Cliquer sur **Identifiants**, faites un clic droit dans la section inférieure de l'écran et cliquez sur Créer un identifiant.
4. Taper CRTL + V.
   L'*identifiant* copié (consultez *Section 3.1, « Acquérir un identifiant non attribué dans MICROSESAME »*) est collé dans la colonne Code.

5. Saisissez une date de début et de fin de validité, puis cliquez sur Entrée.
6. Cliquer sur **Enregistrer**.
   Les informations sont téléversées dans la TILLYS.
7. À partir du menu principal de MS, accédez à l'écran de supervision du **Moniteur d'évènements** (Exploitation > Supervision > Moniteur d'évènements) et passez le badge devant le lecteur.
   Le badge est maintenant associé au nom de la personne que vous avez saisi mais son accès est toujours interdit (pas d'accès au lecteur) et ceci est tout à fait normal car il n'est pas encore associé à des droits d'accès.
   Il ne possède pas non plus pour le moment de profil intrusion CUBE lui permettant d'accéder à un terminal TACTILLYS-IP CUBE.
8. Les instructions de configuration des accès et de configuration du profil intrusion de ce badge sont fournies dans les deux sections qui suivent.

3.3. Attribuer des droits d'accès à un nouvel identifié

1. À partir du menu principal de MS, accédez à l'écran d'exploitation des **Identifiés** (Exploitation > Contrôle d'accès > Identifiés).
2. Recherchez l'*identifié* précédemment créé.
3. Dans cette fiche identifié, cliquez sur **Accès**.
4. Dans la partie inférieure droite de l'écran, cliquez sur
5. Dans la liste qui s'ouvre, cliquer sur **Tous les sites actuels et futurs**.
6. Dans la fenêtre de paramétrage d'accès qui s'affiche, cliquez sur OK (validation des accès 24/24).
7. Cliquez sur **Enregistrer**.
8. Affichez le **Moniteur d'évènement**(depuis le menu principal, suivre **Exploitation > Supervision > Moniteur d'évènements**), passez le badge devant chaque lecteur attribué précédemment et vérifiez qu'en plus que l'identifié soit reconnu, son accès est maintenant autorisé.

3.4. Attribuer un profil intrusion CUBE à un nouvel identifié

Les identifiés chargés de gérer un clavier TACTILLYS-IP CUBE doivent disposer au minimum du profil intrusion correspondant à ce terminal.

Ils doivent également disposer de droits d'accès au bâtiment sur les lecteurs de contrôle d'accès.

1. À partir du menu principal de MS, accédez à l'écran d'exploitation des **identifiés** (Exploitation > Contrôle d'accès > Identifiés).
2. Recherchez l'*identifié* précédemment créé.
3. Dans sa fiche identifié, cliquez sur **Accès**.
4. Dans la partie inférieure droite cliquer sur le bouton
5. Cliquez sur le menu en milieu de la partie droite de l'écran, puis cochez la case **Afficher les profils intrusion CUBE**.

6. Dans la section droite, cliquer sur le profil intrusion, cliquez sur la flèche < pour faire passer ce profil dans la section gauche de l'écran.
7. Attribuez de la même manière les droits d'accès au bâtiment dont cet identifié a besoin.
8. Cliquez sur le bouton **Enregistrer**.
9. À partir du menu principal de MS, accédez à l'écran de paramétrage des **UTL** (Paramétrage > Matériel > Unités de Traitement Local).
10. Double-cliquez sur la ligne de la TILLYS (*UTL*) connectée au TACTILLYS.
11. Cliquez sur le bouton , puis sur le bouton .
12. Cochez la case **Accès** et cliquez sur le bouton Exécuter.

3.5. Attribuer un profil opérateur MICROSESAME à un identifié

1. À partir du menu principal de MS, accédez à l'écran d'exploitation des **identifiés** (Exploitation > Contrôle d'accès > Identifiés).
2. Recherchez l'*identifié* concerné et dans sa fiche identifié, cliquez sur l'onglet **Opérateur**.
3. Cliquez sur **Définir comme opérateur**.
4. Renseignez les informations de connexion pour créer le compte MICROSESAME de l'identifié (Login / Mot de passe), puis cliquez sur Valider.
5. Dans la partie inférieure droite, cliquez sur , puis double-cliquez sur le(s) profil(s) souhaité(s) dans la liste.
6. Cliquez sur **Enregistrer** .

L'identifié *opérateur* peut désormais se connecter avec son compte personnel sur un poste client MICROSESAME. Les fonctionnalités accessibles sur ce poste dépendent des droits et responsabilités attribués à l'opérateur.

Plusieurs profils opérateurs peuvent être attribués à un même opérateur. Par exemple, le responsable sécurité peut se voir attribuer les profils *Responsable sûreté* et *Agent de sûreté*.

Pour créer un profil partenaire, consultez *Section 3.6, « Créer un profil partenaire »*.

Par défaut, il existe deux types d'opérateur :

- Opérateur **Gestionnaire** : ce profil permet à l'opérateur de se connecter sur un poste client MICROSESAME ou bien sur l'interface *WEBSESAME* depuis un navigateur Internet.
- Opérateur **Utilisateur** : l'opérateur n'a accès qu'à l'interface *WEBSESAME* via un navigateur Internet.

3.6. Créer un profil partenaire

La version préconfigurée de MICROSESAME propose quatre profils opérateur : installateur, maintenance, agent de sûreté et responsable sûreté. Il est possible de

définir davantage de profils. Si, pour protéger sa responsabilité, le client ne souhaite pas laisser l'accès administrateur au partenaire, il est nécessaire de définir un profil partenaire distinct, disposant de droits d'accès similaires à l'administrateur.

1. À partir du menu principal de MS, accédez à l'écran de **paramétrage** des **profils opérateurs** (Paramétrage > Système > Profils opérateurs).
2. Cliquez sur **Créer un profil**.
3. Renseignez le nom du profil puis, si besoin, ajoutez une description dans le champ **Commentaire**.
4. Parcourez les différents onglets contenant les droits opérateurs disponibles.
5. Cochez les cases des droits d'accès nécessaires pour le profil partenaire.
6. Cliquez sur **Enregistrer**.

3.7. Utiliser un synoptique

Le *synoptique* est une interface graphique qui fournit une image globale du site.

Le synoptique est utilisable immédiatement après avoir appliqué le paramétrage à la TILLYS (voir *Section 2.3.6, « Configurer MICROSESAME et modifier le paramétrage de la TILLYS »*).

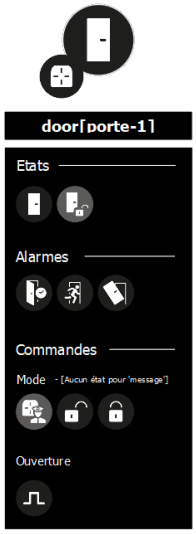
Dans le cas d'une installation avec configuration prédéfinie, MICROSESAME a généré automatiquement un synoptique avec 8, 16 ou 24 portes.

À partir du menu principal de MICROSESAME, suivre **Exploitation > Supervision > Animateur de synoptique [ANI].**

MICROSESAME a configuré automatiquement trois synoptiques. Deux d'entre eux présentent des symboles différents et sont directement accessibles depuis le synoptique Accueil, affiché par défaut :

- **Toutes les portes** : Vue synthétique de l'état de la TILLYS, ainsi que de toutes les portes présentes sur chacun de ses bus A, B ou C. Le symbole de porte utilisé dans ce synoptique nécessite un clic-droit sur le pictogramme central, afin d'accéder aux télécommandes disponibles (menu contextuel). Les états de la porte s'affichent sous forme de petits pictogrammes qui apparaissent tout autour du pictogramme central.
- **UTL 1 - BUS** : Vue synthétique de toutes les portes présentes sur le bus A, B ou C. Le symbole utilisé pour ce synoptique nécessite un simple clic sur le pictogramme représentant la porte. Une fenêtre s'affiche alors, dans laquelle sont recensés à la fois les télécommandes disponibles et les différents états de la porte.

Depuis la vue **UTL 1 - BUS**, cliquer sur le pictogramme de la porte pour accéder aux informations :



Pour chaque porte, le synoptique permet de visualiser :

- L'état de ses *alarme*s
- L'état d'ouverture
- L'état de verrouillage
- Pour visualiser les remontées de passage de badge, cliquer sur le pictogramme **Lecteur** .

	État de la porte : Ouverte / Fermée
	État du verrouillage de la porte : Déverrouillée / Verrouillée
	État de la commande manuelle d'ouverture (BP) : Commande actionnée (s'affiche en bleu) ou non
	Alarme POTL : Se déclenche lorsque la porte reste ouverte trop longtemps (s'affiche en rouge)
	Alarme Ouverture inattendue (s'affiche en rouge)
	Alarme Ouverture d'urgence actionnée (s'affiche en rouge)

Le synoptique permet aussi d'envoyer des commandes :

- Choisir le mode de contrôle de la porte : contrôlé, libre ou bloqué
- Commander le déverrouillage à distance, comme ci-dessous :

	Envoi d'une impulsion sur le relais d'ouverture de la porte

Vous pouvez acquitter une alarme directement depuis la fenêtre **Alarmes**, présente dans la partie gauche du synoptique.
Pour ce faire, cliquez sur l'icône cloche, saisissez le commentaire d'acquittement et cliquez sur OK.

3.8. Former un client

La formation de base du client final au moment de la mise en service par le partenaire inclut les éléments suivants :

- Accès à MICROSESAME et présentation de la navigation (voir *Section 2.3.1, « Lancer le menu principal de MICROSESAME et naviguer »*).
- Présentation du *synoptique*
- Enregistrement d'un *identifié*
- Définition d'un *opérateur*
- Définition d'un groupe de *lecteurs*
- Définition de plages horaires
- Définition de profils d'accès (plages horaires et actions).

Chapitre 4. Résolution de pannes lors de l'installation de MICROSESAME

Les sections ci-après répertorient des situations de panne possibles et leurs procédures de résolution. Si vous en rencontrez d'autres, merci de *nous les signaler*.

4.1. Création de base de données impossible

- Dans le cas ou une instance à été créée lors de l'installation du moteur de *base de données*, vérifiez que le nom d'instance est bien renseigné. Dans le cas où le moteur de la *base de données* a été installé avec l'application fournie par HIRSCH, remplissez le champ avec le nom d'instance **TIL**.
- Vérifiez que le nom ou l'adresse *IP* du serveur ont été correctement renseignés.
- Vérifiez que le mot de passe de la session administrateur (onglet Paramètres SQL Server) a été correctement renseigné.
- Dans le cas d'une nouvelle tentative de création de base de données, renseignez obligatoirement un nouveau nom pour la base de données.

4.2. Difficulté d'authentification au démarrage de MICROSESAME

Cas 1 : vérification que le mot de passe du compte ADMIN a été correctement renseigné

Cas 2 : affichage du message d'erreur "Impossible de contacter l'API REST" :

1. Lancez l'outil de maintenance MICROSESAME **ms_maintenance.exe**
2. Cliquez sur **Démarrer les services**
3. Vérifiez que **Tous** les services ont été sélectionnés
4. Effectuez une nouvelle tentative d'accès.

Cas 3 : affichage du message d'erreur "not found" :

1. Lancez l'outil de maintenance MICROSESAME **ms_maintenance.exe**.
2. Cliquez sur **Installer et démarrer les services**.
3. Dans le champ port HTTPs du service web, renseignez **444**.
4. Effectuez une nouvelle tentative d'accès.

Cas 4 : vérification de l'accessibilité des ports réseaux en contactant directement l'administrateur SI.

4.3. Au passage d'un badge, les lecteurs ne réagissent pas

- **Cas 1** : dans l'application Identifiants de MICROSESAME, vérifiez que le pilote et le protocole sélectionnés dans les listes déroulantes correspondent au lecteur utilisé (consultez la fiche technique du lecteur).
- **Cas 2** : dans l'application *UTL* (unité de traitement local) de MICROSESAME, onglet Contrôle d'accès, vérifiez le type de fonctionnement de chaque bus qui doit être accepté par l'UTL (le type CUBE ne peut être validé que pour des TILLYS CUBE)

4.4. Absence de communication entre un module et la TILLYS

Vérifiez que le type de bus sélectionné dans la fenêtre de paramétrage de l'*UTL* est compatible avec le module qui y est raccordé.

MDv2 : Le module doit être de type MDv2

MLv3 (1.x) : Le module doit être de type MLv3 avec un firmware impérativement en version 1.x

MLv3 (2.x) : Le module doit être de type MLv3 avec un firmware impérativement en version 2.x ou 3x

CUBE : Le module doit être de type CUBE avec un firmware impérativement en version 4.x ou supérieure.

Sur la TILLYS, observez la LED rouge positionnée à côté du bus sur lequel est raccordé le module : si la LED est éteinte ou fixe, débranchez le bus au niveau de la TILLYS, attendez environ 20 secondes, rebranchez le bus, puis vérifiez que la LED clignote.

4.5. Message d'erreur " Les automates n'ont pas pu appliquer les changements"

Malgré les modifications de paramétrage dans MICROSESAME, les changements ne sont pas répercutés.

1. Lancez l'application **Appliquer le paramétrage**.
2. Dans l'onglet **Compiler le paramétrage**, cliquez sur **Tout compiler**.
3. Retentez d'appliquer les changements.

4.6. Lors du passage d'un badge, aucune remontée d'information dans le moniteur d'évènement

1. Pas de remontée de l'*UTL* vers *MICROSESAME*. Voir l'écran Tableau de bord : les lignes et l'UTL doivent être verts.
2. **Appliquer le paramétrage**. Cliquez sur **Tout compiler**.
3. Appliquer les changements > Appliquer les changements sur les lignes > Exécuter.
4. Télécharger / Complet (ou Avancé et choix de l'UTL).
5. Rafraîchissez l'affichage du tableau de bord.

4.7. Dans le synoptique, aucun changement de couleur de l'objet porte, malgré un changement d'état ou l'envoi de commandes

1. À partir de l'écran **Appliquer le paramétrage** de MICROSESAME, cliquez sur **Appliquer les changements**.
2. Dans la liste déroulante, sélectionnez **Appliquer les changements sur les propriétés**, puis cliquez sur **Exécuter**.
3. Dans la même liste déroulante, sélectionnez ensuite **Appliquer les changements sur les lignes**, puis cliquez sur **Exécuter**.
4. Cliquez sur **Télécharger**, puis sur **Complet**.