HIRSCH

MICROSESAME - GUIDE D'INSTALLATION, MIGRATION ET RESTAURATION

GI-10020-FR
02/03/2026

Table des matières

Liste des illustrations

Liste des tableaux

Préface

1. Version logicielle

Les pastilles de couleur jaune en haut de chaque page signalent que ce document est un guide d'installation.

Ce guide décrit comment installer, migrer et restaurer le logiciel MICROSESAME pour sa **version logicielle 2025**.

2. Contexte d'utilisation de ce manuel

Ce manuel s'adresse aux partenaires et aux personnes chargées de la mise à jour de MICROSESAME.

3. Voir aussi

- *Prérequis d'installation de MICROSESAME*
- *Mise en place des certificats TLS signés*
- *Mise à jour MICROSESAME avant 2018_2*
- Tableau des compatibilités OS & BDD

4. 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.

5. Glossaire

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

802.1.X	Standard d'authentification reposant sur la norme EAP (Extensible Authentication Protocol), utilisé dans les réseaux sans fil et qui permet de contrôler l'accès aux équipements. Il fonctionne sur les serveurs d'authentification. La TILLYS NG/CUBE intègre nativement ce protocole.

Administrateur	Profil opérateur par défaut, l'administrateur possède tous les droits et permissions.
ANSSI-PA-72	Guide des recommandations sur la sécurisation des systèmes de contrôle d'accès physique et de vidéoprotection version 2.0.
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.
Broadcast	Terme anglais recouvrant la diffusion de données à l'ensemble des ordinateurs d'un réseau.
Certificat	Un certificat numérique est une sorte de passeport électronique qui permet à une personne, un ordinateur ou une organisation d'échanger de manière sûre des informations sur Internet en s'appuyant sur une infrastructure à clé publique (PKI). Les échanges entre TILLYS et MICROSESAME se font par défaut de façon sécurisée, à l'aide de certificats auto-signés. Pour les sites nécessitant un niveau de certification de type ANSSI, des certificats signés doivent obligatoirement être mis en œuvre.
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.
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).
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.
MID	Certificat d'une autorité de certification intermédiaire, de niveau inférieur à l'autorité de certification racine.
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.
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.
Restauration	Cette opération consiste à restaurer/ré-installer une base de données à partir d'une sauvegarde réalisée au préalable.
RJ45	Format de connecteur à 8 contacts électriques utilisé en téléphonie et pour les réseaux Ethernet.
ROOT	Certificat racine de l'autorité de certification, situé à la base de la chaîne de confiance (fichier .crt).
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.
TCP	Acronyme anglais de Transmission Control Protocol. Protocole de communication bidirectionnel très fiable, utilisé avec *IP* et fonctionnant en mode connecté. L'émetteur s'assure ainsi que toutes les données transmises ont bien été réceptionnées par le récepteur. Ce protocole comporte trois phases : • l'établissement de la connexion, • les transferts de données, • la fin de la connexion.
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*.
TLS	Acronyme anglais de Transport Layer Security. Comme son prédécesseur, SSL, TLS est un protocole de sécurisation du transport des données sur les réseaux informatiques. Les deux chiffrent et garantissent la confidentialité et l'intégrité des données transmises. Tous les échanges entre serveur et postes clients MICROSESAME et les TILLYS sont réalisés en TLS, qui exploite par défaut des certificats auto-signés.
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.
UDP	Acronyme anglais de User Datagram Protocol. Protocole de communication très léger mais peu fiable, adapté aux applications où la perte de données occasionnelle est acceptable, comme le streaming en temps réel.
UTIL	*UTL* de la gamme V2.
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. Architecture informatique à mettre en place pour MICROSESAME

1.1. Généralités sur la sécurité des réseaux informatiques

La mise en œuvre de VPN et de VLAN dépend des équipements actifs du réseau. Sur les réseaux administrés, la mise en œuvre de ces procédures relève de l'administrateur réseau.

Sur les installations comportant un nombre important d'UTL, HIRSCH préconise la mise en œuvre d'un réseau de sécurité dédié, sous forme de VLAN ou de réseau physiquement indépendant. Sur tout système de sécurité centralisé en réseau les équipements gérant les accès ou la sécurité intrusion ainsi que les les accès physiques au serveur doivent être protégés.

Les UTIL V2 n'embarquent pas les couches TLS. La communication entre les UTL et le serveur peut cependant être chiffrée (AES 128).

Les TILLYS NG/CUBE gèrent le protocole TLS.

Le système supporte :

- L'activation d'un pare-feu (firewall).
- L'utilisation de réseaux VPN et VLAN.

1.2. Tableaux des flux : configuration sécurisée TILLYS / MICROSESAME

Les tableau des flux ci-après correspondent à une installation certifiée **ANSSI** utilisant le driver **SQL TIL** pour l'installation des **postes clients**.

Tableau 1.1. Flux et ports MICROSESAME

Protocole	Source	Destination	N° de port	Modifiable	Description
TCP ou TLS	Poste Client Lourd/ Serveur TSE	Serveur MICROSESAME	TCP 14001	OUI	Messagerie événementielle en temps réel
TCP ou TLS	Poste Client Lourd/ Serveur TSE	Serveur MICROSESAME	TCP 14002	OUI	Service Master Agent
TCP ou TLS	Poste Client Lourd/ Serveur TSE	Serveur MICROSESAME	TCP 14004	OUI	Service de licences
HTTP	Poste Client Lourd/ Serveur TSE/	Serveur MICROSESAME	TCP 80	OUI	Service Web, pouvant être utilisé pour :

Protocole	Source	Destination	N° de port	Modifiable	Description
	Poste client WEB				• WEB SESAME (redirection vers port sécurisé) • API REST (redirection vers port sécurisé) • Postes clients
HTTPS	Poste Client Lourd/ Serveur TSE/ Poste client WEB/ Intrusion CUBE	Serveur MICROSESAME	TCP 443	OUI	Service Web, pouvant être utilisé pour : • WEB SESAME * • API REST * • Postes clients * • TACTILLYS IP pour l'intrusion CUBE * * Certificats valides requis
WSS	Poste client WEB	Serveur MICROSESAME	TCP 443	OUI	Service Web, pouvant être utilisé pour : • WEB SESAME * • API REST * • Postes clients * * Certificats valides requis
TCP ou TLS	Serveur MICROSESAME	Serveur MICROSESAME	TCP 14003	OUI	Service Web, redirection Apache interne au serveur MICROSESAME

Protocole	Source	Destination	N° de port	Modifiable	Description
WSS	Serveur MICROSESAME	Serveur MICROSESAME	TCP 14005	OUI	Service Web, redirection Apache interne au serveur MICROSESAME (temps réel)
WSS	Serveur MICROSESAME	Serveur MICROSESAME	TCP 14006	OUI	Service Web, redirection Apache interne au serveur MICROSESAME (requête)

Tableau 1.2. Flux et ports SGBD SQL Server déporté

Protocole	Source	Destination	N° de port	Modifiable	Description
TCP	Serveur MICROSESAME	Serveur SQL déporté	TCP 1433	OUI	SQL Server Microsoft
UDP	Serveur MICROSESAME	Serveur SQL déporté	UDP 1434	OUI	SQL Server Microsoft

Tableau 1.3. Flux et ports de la TILLYS

Protocole	Source	Destination	N° de port	Modifiable	Description
TLS	Serveur MICROSESAME	TILLYS	TCP 20100	OUI	Configuration/ Téléchargement sécurisés TLS
TLS	Serveur MICROSESAME	TILLYS	TCP 20200	OUI	Échanges temps réel sécurisés
UDP Multicast	TILLYS	TILLYS	UDP 20100	OUI	Échanges sécurisés temps réel AntiPass Back
DNS	Serveur DNS	TILLYS	UDP 5353 multicast	NON	Configuration DNS
SSH	Poste Maintenance	TILLYS	TCP 22	NON	Réservé pour maintenance
HTTPS	Poste Maintenance	TILLYS	TCP 443	NON	Maintenance/ Configuration

Protocole	Source	Destination	N° de port	Modifiable	Description
PING / ICMP	Poste Maintenance	TILLYS	-	NON	Maintenance

Tableau 1.4. Flux et ports pour client léger TSE/RDP

Protocole	Source	Destination	N° de port	Modifiable	Description
TSE / RDP	Poste Client TSE	Serveur TSE	3389	NON	Serveur TSE / Client léger TSE ou Citrix

Tableau 1.5. Flux et ports pour passerelle OPC (serveur)

Protocole	Source	Destination	N° de port	Modifiable	Description
OPC-UA	Syst.externe	Serveur MICROSESAME	TCP 55000	OUI	MICROSESAME Serveur OPC

Tableau 1.6. Flux et ports pour lecteur biométrique MORPHO/IDEMIA

Protocole	Source	Destination	N° de port	Modifiable	Description
TCP	Serveur MICROSESAME	Lecteur Bio Morpho	TCP 11010		Chargement empreintes dans lecteur Biométrique MorphoBioToolBox

Tableau 1.7. Flux et ports pour passerelles inter-systèmes MICROSESAME (toutes versions)

Protocole	Source	Destination	N° de port	Modifiable	Description
UDP	Serveur(s) MICROSESAME Distant(s)	Serveur MICROSESAME	UDP 14200	OUI	Échanges temps réel inter MICROSESAME

Tableau 1.8. Flux et ports SAFEKIT avec redondance serveur MICROSESAME (toutes versions)

Protocole	Source	Destination	N° de port	Modifiable	Description
UDP		Serveurs 1 & 2	UDP 8888		Heartbeats : heart
rfs (LOCAL)		Serveurs 1 & 2	TCP 5700		rfs file replication : nfs port

Protocole	Source	Destination	N° de port	Modifiable	Description
rfs (LOCAL)		Serveurs 1 & 2	TCP 5701		rfs file replication : mount_port
rfs		Serveurs 1 & 2	TCP 5600		rfs file replication : replication request savenfs_port
rfs		Serveurs 1 & 2	TCP 5601		rfs file replication : replication request savemount_port
rfs		Serveurs 1 & 2	TCP 5603		rfs file replication : replication request savenfsr_port
HTTP		Serveurs 1 & 2	TCP 9010		Web Console, Admin role (unsecure HTTP)
HTTP		Serveurs 1 & 2	TCP 9011		Web Console, Control role (unsecure HTTP)
HTTP		Serveurs 1 & 2	TCP 9012		Web Console, Monitor role (unsecure HTTP)
HTTPS		Serveurs 1 & 2	TCP9453		Web Console Secure HTTPS
UDP (LOCAL)		Serveurs 1 & 2	UDP 6259		Safeadmin, Main & mandatory administration service défini dans C:\Windows\safeini.xml

Protocole	Source	Destination	N° de port	Modifiable	Description
UDP		Serveurs 1 & 2	UDP 3600		Safeagent SNMP (défini dans SAFE/ snmp/conf/ snmp.conf file

Tableau 1.9. Flux et ports pour serrures mécatroniques OFFLINE

Protocole	Source	Destination	N° de port	Modifiable	Description
TCP	Serveur MICROSESAME	Borne OSS Offline	TCP 20300	Oui	Téléchargement de la configuration et des accès dans les bornes OSS Offline
TCP	Serveur MICROSESAME	Serveur distant B-COMM	TCP 3001	Oui	Logiciel B-COMM pour gestion des serrures KABA ONLINE. Paramétrage de la configuration.

Tableau 1.10. Flux et ports pour lecteurs mobiles MOBILIS

Protocole	Source	Destination	N° de port	Modifiable	Description
TCP	Serveur MICROSESAME	MOBILIS	TCP 20100	OUI	Configuration serveur pour Contrôle d'Accès avec terminaux MOBILIS
UDP	Serveur MICROSESAME	MOBILIS	UDP 20100	OUI	Configuration serveur pour Contrôle d'Accès avec terminaux MOBILIS
TCP	MOBILIS	Serveur MICROSESAME	TCP 20110	OUI	Configuration des terminaux MOBILIS

Protocole	Source	Destination	N° de port	Modifiable	Description
					pour synchronisation

L'installation des postes clients avec les drivers **OBDC driver for SQL** reste possible (**non conforme ANSSI**). Dans ce cas il est impératif de prendre en compte l'ajout des ports de communications suivants, ainsi que de choisir une **Installation en mode avancé** pour la configuration des postes clients.

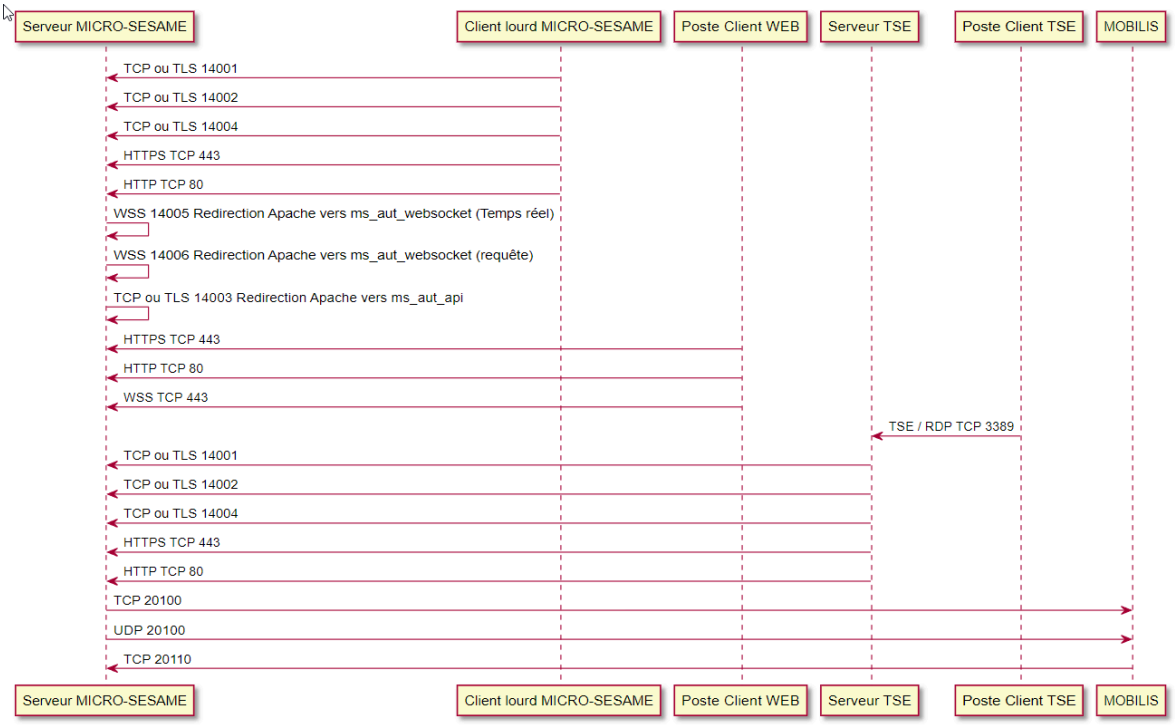
Tableau 1.11. Flux et ports pour postes clients via les drivers OBDC.

Protocole	Source	Destination	N° de port	Modifiable	Description
TCP	Poste client lourd/ Serveur TSE	Serveur SQL déporté	TCP 1433	OUI	SQL Server Microsoft
UDP	Poste client lourd/ Serveur TSE	Serveur SQL déporté	UDP 1434	OUI	SQL Server Microsoft

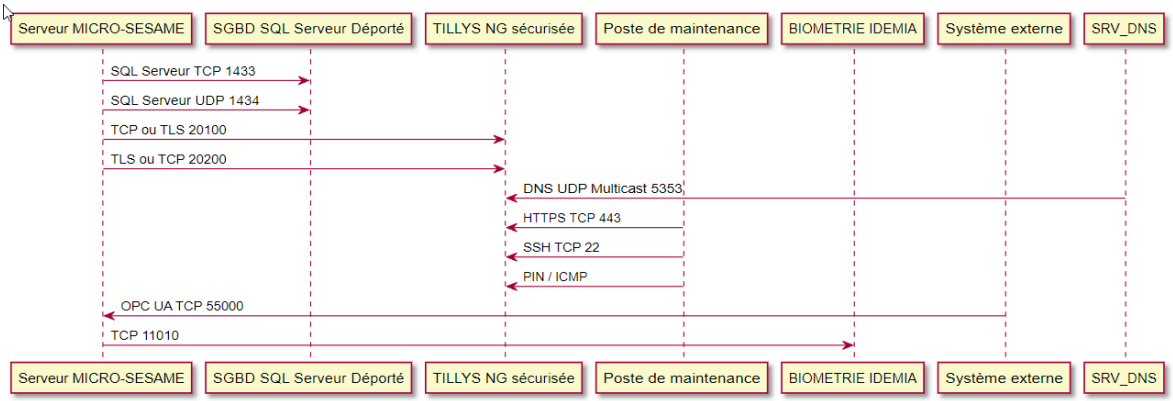
1.3. Schémas des flux et ports MICROSESAME

1.3.1. 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**.

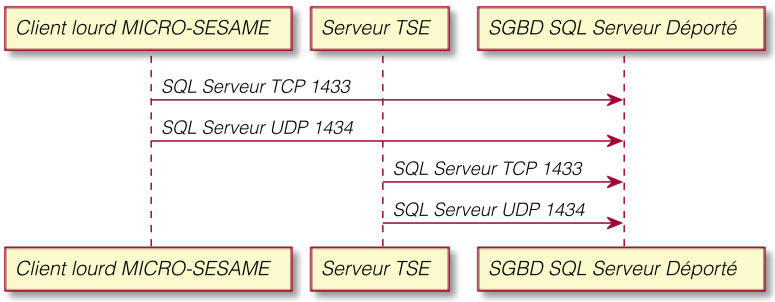


Les ports et flux représentés sur la figure suivante ne sont modifiables qu'à condition de spécifier de manière cohérente les nouvelles valeurs au niveau des logiciels et matériels interconnectés.

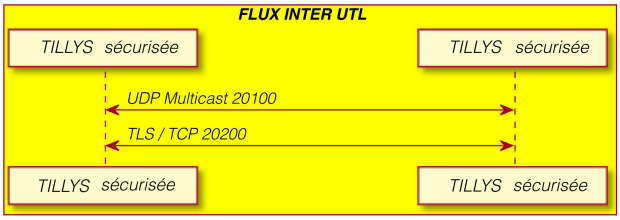


1.3.2. Ports des drivers ODBC pour SQL sur serveurs déportés

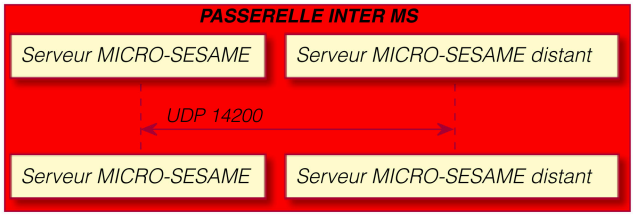
L'installation des postes clients avec les drivers **ODBC driver for SQL** reste possible (**non conforme ANSSI**). Dans ce cas il est impératif de prendre en compte l'ajout des ports de communications suivants, ainsi que de choisir une **Installation en mode avancé** pour la configuration des postes clients :



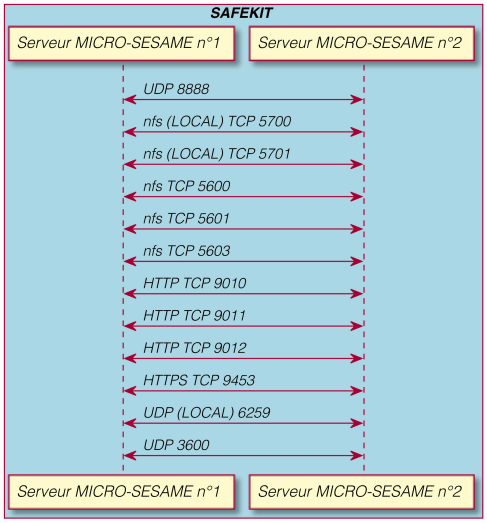
1.3.3. Ports pour flux inter-UTL



1.3.4. Ports pour passerelle inter-MICROSESAME



1.3.5. Ports spécifiques pour Safekit



1.3.6. Ports utilisés par la centrale intrusion SPC de Vanderbilt

Les ports suivants sont utilisés :

- Le port 52000 permet à la centrale SPC de communiquer avec la passerelle MICROSESAME. Si indisponible, cette valeur de port est incrémentée de 1, jusqu'au prochain port disponible.
- Le port 51211 est utilisé pour le fonctionnement interne local (en OPC-UA) de la passerelle. Si indisponible, cette valeur de port est incrémentée de 1, jusqu'au prochain port disponible.
- Les ports 80 et 443 sont utilisés pour la communication avec MICROSESAME (en local uniquement). Si indisponibles, les ports 8080 et 4443 sont utilisés. Si indisponible, chaque valeur de port est incrémentée de 1, jusqu'au prochain port disponible.

1.4. Consommations de bande passante

1.4.1. Bande passante consommée entre les UTL et le serveur

Les UTL sont IP en mode natif. Elles se connectent directement sur le réseau sans convertisseur. La bande passante est consommée pendant les opérations de téléchargement dans les automates. Le téléchargement utilise le protocole TCP.

Les volumes utiles transférés sont d'environ 100 octets par identifié. Les mesures donnent un temps de téléchargement d'environ 1 minute pour 4000 identifiés, soit une moyenne de 55 kbits/sec par UTL. Sur un même système MICROSESAME, le téléchargement est réalisé en multi-threads.

Comme chaque thread (ligne) traite simultanément 32 UTL (soit une bande passante de 1,76 Mbits/sec), les téléchargements des identifiés et des accès au niveau des automates sont optimisés. Le système ne transfère que les informations relatives aux identifiés dont les critères d'accès ont changé. Répartir les UTIL de manière équilibrée sur plusieurs lignes permet également d'optimiser les temps de téléchargement.

Les échanges liés aux événements temps réel (passage de badges, changement d'état, alarmes, ...) sont eux aussi transmis en TCP, et uniquement sur changement. Ils sont effectués à l'aide de trames de quelques dizaines d'octets, avec acquittement du destinataire. La bande passante consommée par ces échanges est faible.

1.4.2. Bande passante consommée entre le serveur et les postes clients

La bande passante est essentiellement consommée par les requêtes API générées par le poste client suivant les actions opérateurs. En plus du port utilisé par l'API, un canal TCP (port 14000) bidirectionnel est utilisé pour la diffusion des événements en temps réel.

Les valeurs de bandes passantes indiquées ci-dessous le sont à titre indicatif et n'ont pas de caractère contractuel. La bande passante effective d'un réseau dépend de plusieurs paramètres et notamment du temps de latence. Elle évolue très souvent suivant les heures de la journée.

Pour les sites disposant de bande passante inférieure à 5 Mbits/s, il est conseillé de procéder à des essais en situation réelle avec une application configurée et des bases de données chargées à leur niveau nominal d'utilisation.

Parmi les points à surveiller :

1. La taille des photos des identifiés enregistrées en base de données.
   Éviter d'archiver des photos dans des résolutions trop importantes. 96 dpi sont en général suffisants pour une personnalisation graphique des badges sans perte de qualité.
2. Pour l'accueil des visiteurs, l'auto-complétion des champs de type Nom peut utiliser les photos pour aider à la sélection de la personne. Sur les sites à faible bande passante, il est conseillé de désactiver la fonctionnalité.
3. Pour les synoptiques, éviter d'utiliser pour les fonds de plan des images avec une résolution trop importante (la résolution des écrans est en général relativement faible).

Dans les cas où peu de bande passante est disponible (< 2 Mbits/s), la mise en œuvre de postes client légers fonctionnant en TSE est la seule solution. Elle présente, de plus, l'avantage de simplifier la mise à niveau des postes clients lors des changements de version.

Un poste client lourd est néanmoins nécessaire pour :

- Les postes qui effectuent l'encodage des badges.
- Les postes d'accueil visiteur qui nécessitent des périphériques d'aide à la saisie (lecteur enrôleur, lecteur de documents d'identité, imprimante de badge visiteurs, etc...).

1.4.3. Tableau récapitulatif des consommations de bande passante

Le tableau ci-après affiche les valeurs minimales à respecter pour un fonctionnement optimal de MICROSESAME.

Tableau 1.12. Consommations de bande passante

Fonction	Valeur
Connexions clients / serveur	
Client léger TSE	1 Mb/s
Client léger Web	2 Mb/s
Client lourd	10 Mb/s
Dialogue automates (GTB, Contrôle d'accès, ...)	
Modules UTL, TILLYS	0.5 Mb/s
Ligne de dialogue Modbus et automates industriels	0.5 Mb/s
Ligne de dialogue OPC (OPC-DA, OPC-UA, inter serveurs)	1 Mb/s
Réplication de données	
Redondance SAFEKIT (connexion directe de serveur à serveur)	1Gb/s
Échanges inter-bases	
Synchronisation ressources humaines	Dépend du volume de données et de la fréquence de rafraîchissement
Web service	Dépend des développements spécifiques
Gestion des visiteurs	Dépend de la fréquentation des visiteurs
Authentification LDAP	Négligeable

1.5. Configuration mixte (TILLYS - UTIL V2) : MICROSESAME 2020 et supérieur

Cette section décrit un fonctionnement TILLYS non sécurisé et UTIL V2 (sans échanges UTIL - TILLYS NG). Cette configuration est **non conforme ANSSI**.

Tableau 1.13. Configuration mixte des ports entre TILLYS et UTIL V2

Protocole	Source	Destination	N° de port	Modifiable	Description
TCP	Serveur MICROSESAME	UTIL V2/ TILLYS	TCP 20100	OUI	Téléchargement - Chiffré AES 128
UDP	Serveur MICROSESAME UTIL V2	UTIL V2/ TILLYS	UDP 20100	OUI	Échanges temps réel
UDP Broadcast	UTIL V2/ TILLYS	UTIL V2/ TILLYS	UDP 20100	OUI	Échanges temps réel Anti-Pass Back inter-UTILV2
Telnet	Poste Maintenance	UTIL V2	TCP 23	OUI	Maintenance/ Configuration (Désactivable)
HTTP	Poste Maintenance	UTIL V2	TCP 80	OUI	Maintenance/ Configuration (Désactivable)
PING / ICMP	Poste Maintenance	UTIL V2/ TILLYS	-	NON	Maintenance
DNS	Serveur DNS	TILLYS	UDP 5353 multicast	NON	Configuration DNS
SSH	Poste Maintenance	TILLYS	TCP 22	NON	Réservé Maintenance
HTTPS	Poste Maintenance	TILLYS	TCP 443	NON	Maintenance/ Configuration
UDP	UTIL V2/ TILLYS NG	Serveur MICROSESAME	UDP 20100	OUI	Échanges temps réel
TLS	Poste Client Lourd	Serveur MICROSESAME	TCP 14001	OUI	Messagerie temps réel
TLS	Poste Client Lourd	Serveur MICROSESAME	TCP 14002	OUI	Service Master Agent

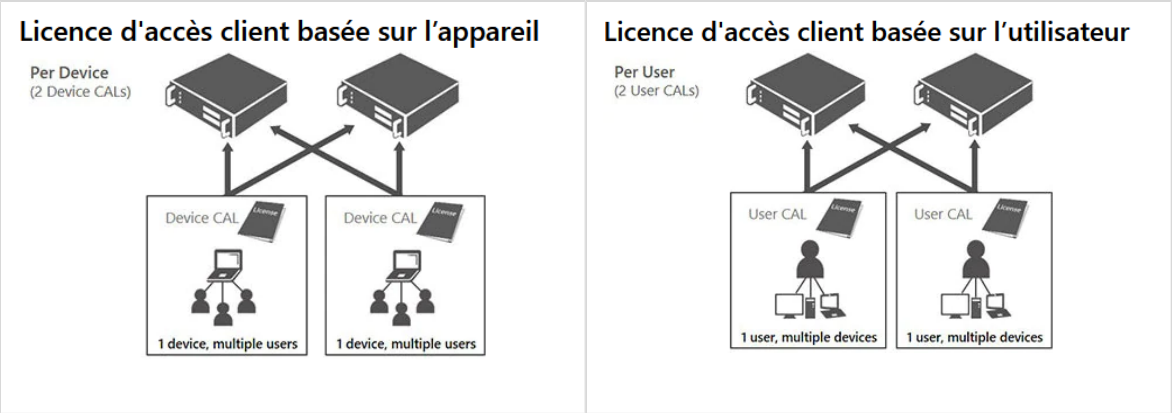
Protocole	Source	Destination	N° de port	Modifiable	Description
TLS	Poste Client Lourd	Serveur MICROSESAME	TCP 14004	OUI	Service des licences
HTTP	Poste Client WEB	Serveur MICROSESAME	TCP 80	NON	Redirection vers HTTPS
HTTPS	Poste Client WEB	Serveur MICROSESAME	TCP 443	OUI	WEB Sésame API REST
SGBD SQL Server					
SQL Server	Poste Client Lourd	Serveur SGBD	TCP 1433	OUI	SQL Server Microsoft
SQL Server	Poste Client Lourd	Serveur SGBD	UDP 1434	OUI	SQL Server Microsoft
Client léger TSE / RDP					
TSE / RDP	Poste Client TSE	Serveur TSE	3389	NON	Serveur TSE / Client léger TSE ou Citrix
Mobilis : Lecteurs mobiles					
TCP	Serveur MICROSESAME	MOBILIS	TCP 20100	OUI	Configuration serveur pour Contrôle d'Accès avec terminaux MOBILIS
UDP	Serveur MICROSESAME	MOBILIS	UDP 20100	OUI	Configuration serveur pour Contrôle d'Accès avec terminaux MOBILIS
TCP	MOBILIS	Serveur MICROSESAME	TCP 20110	OUI	Configuration des terminaux MOBILIS pour synchronisation

1.6. Préconisations postes serveurs et postes clients

1.6.1. Licences CAL (Client Access Licenses)

L'utilisation d'un logiciel de base de données pour un serveur nécessite l'achat de licences particulières afin d'activer l'accès aux données depuis un poste local ou distant. On distingue deux types de Licences d'Accès Client (CAL):

- Device CAL : permet de garantir l'accès au serveur depuis un appareil, quel que soit le nombre d'utilisateurs.
- User CAL : permet de garantir l'accès au serveur à un utilisateur, quel que soit le poste de travail utilisé.



Afin de dimensionner correctement le nombre et le type de licence à acheter en fonction des besoins, contacter le RSSI du site.

Les informations suivantes sont données à titre indicatif et elles ne dispensent pas de consulter le RSSI pour analyser les besoins. Le type de licence à implémenter dépend des usages et du mode de fonctionnement des employés sur les postes de travail.

- Poste Serveur MICROSESAME permanent : 1 Device CAL (poste fixe, mono-utilisation, multi-utilisateur).
- Poste Client MICROSESAME permanent : 1 Device CAL (poste fixe, permanent, un ou plusieurs utilisateurs).
- Poste Client MICROSESAME flottant :
  - S'il y a peu d'opérateurs MICROSESAME, 1 User CAL par opérateur.
  - S'il y a beaucoup d'opérateurs MICROSESAME, 1 Device CAL pour le poste.

1.6.2. Configuration d'un serveur MICROSESAME

La dimensionnement des serveurs dépend de la taille du site géré par *MICROSESAME*. C'est la caractéristique maximale du site qui sera l'élément déterminant pour le type de configuration à utiliser.

Le tableau ci-après présente le dimensionnement de la configuration en fonction des besoins.

Tableau 1.14. Dimensionnement du serveur MICROSESAME (postes clients, lecteurs, visiteurs et propriétés)

Configuration	Nb postes clients	Nb max. lecteurs	Nb max. visiteurs/jour	Nb max. propriétés
Configuration minimale	1 à 50	1 à 500	1 à 500	1 à 10000
Configuration intermédiaire	50 à 100	500 à 1000	500 à 1000	10000 à 20000
Configuration supérieure	100 à 200	1000 à 5000	1000 à 5000	20000 à 50000

Configuration supérieure - La configuration supérieure est obligatoire en cas d'alimentation redondante.

Il est vivement préconisé d'installer le serveur MICROSESAME sur un serveur physique ou virtuel dédié. Les configurations ci-après sont données à titre indicatif. D'autres configurations sont possibles notamment en utilisant des serveurs de base de données dédiés.

Tableau 1.15. Dimensionnement du serveur MICROSESAME (matériel et logiciel)

Configuration	Système d'exploitation	Base de données (SGBD)	Mémoire	Disque	Processeur
Configuration minimale	Windows Server Essentials	SQL Server Express	16 Go	2 x 1 To (Raid 1)	i7 ou équivalent
Configuration intermédiaire	Windows Server	SQL Server Standard	32 Go	2 x 1 To (Raid 1)	i7 ou équivalent
Configuration supérieure	Windows Server	SQL Server Standard	64 Go	2 x 1 To (Raid 1)	i7 ou équivalent

MS-SQL Express est limité à une base de données de 10 Go maximum (à partir de SQL Server 2012).

Compatibilité systèmes d'exploitation et bases de données - Pour plus d'informations sur la compatibilité entre serveurs/clients, consulter le tableau de compatibilités OS & BDD pour la version concernée de MICROSESAME.

Détail des licences Windows Server

- Essentials : licence par serveur. Jusqu'à 25 utilisateurs par serveur. Aucune licence CAL n'est nécessaire.
- Standard : licence par processeur. Pas de limite utilisateurs. Licence CAL obligatoire.

VMWare (ESX, Workstation etc.) est la seule solution de virtualisation qualifiée.

1.6.3. Administration de la base de données

Pour SQL Server, il convient de réserver à la base de données un espace mémoire équivalent à la taille qu'elle occupe sur le disque. Cette opération est réalisée avec les outils d'administration de SQL Server Enterprise Manager.

La performance du serveur dépend beaucoup de sa capacité mémoire. La taille mémoire du serveur est liée à la taille de la base de données sur le disque.

Enfin, il est recommandé de créer la base de données avec une taille initiale de l'ordre de 1,5 à 2 fois sa taille maximale. Un plan de maintenance de la base de données doit être défini pour :

- Assurer la sauvegarde des données de la base.
- Assurer la régénération des index.
- Assurer la récupération de l'espace disque libéré par les purges automatiques de l'historique faites par MICROSESAME.

Dans tous les cas, il faut contrôler l'évolution de l'espace disque consommé par la base de données. Cet espace est fonction de nombreux paramètres (nombre de badges, photos, nombre de propriétés, nombre de documents...), mais son évolution dépend surtout du nombre d'événements/jour enregistrés dans la base historique et de leur durée d'archivage. Le contrôle doit donc se faire sur une période supérieure à la durée maximale d'archivage des événements.

1.6.4. Configuration des postes client lourds

MICROSESAME poste client est compatible avec un PC bureautique actuel (contacter le service informatique du site) :

- OS : Windows (64 bits).
- RAM : 16 Go minimum.
- DD : 1 To minimum.
- Ethernet : connexion standard.

Dans le cas de l'utilisation de VISIOSESAME, vérifiez auprès du constructeur du système vidéo les prérequis spécifiques pouvant concerner les postes clients en charge de l'affichage d'une ou plusieurs séquences vidéo.

1.6.5. Configuration serveur si clients TSE/RDS

Si le serveur assure la double fonction de serveur MICROSESAME et de serveur TSE/RDS pour les postes clients légers, celui-ci devra être de type configuration supérieure. Les performances du processeur deviennent sensibles, la taille mémoire doit être majorée d'environ 1 Go par poste client. Au-delà de 15 postes clients TSE/RDS simultanés, privilégier une architecture avec serveur TSE/RDS séparé. Dans ce cas, contacter impérativement le service informatique du site.

1.6.6. Préconisations antivirus - poste client

Dans le cas de l'utilisation de certificats signés pour la sécurisation TLS entre poste serveur et poste client, les antivirus peuvent perturber l'initialisation de la communication.

Il est recommandé d'exclure le répertoire des programmes MICROSESAME de l'analyse antivirus.

Le répertoire à exclure de l'analyse est <MICROSESAME> / Prog.

Chapitre 2. Installer - Migrer - Restaurer MICROSESAME

2.1. Installer un poste serveur MICROSESAME

2.1.1. MICROSESAME et SQL Server

Vous devez dans un premier temps d'installer le logiciel de gestion de base de données et son moteur de base de donnée SQL Serveur.

Pour plus d'informations, consultez les *Prérequis d'installation de MICROSESAME CUBE*.

Un poste serveur peut héberger la base de données et son moteur relationnel (*SQL Server*).

Le moteur de la base ne doit pas être arrêté tant que l'application *MICROSESAME* est en fonctionnement.

Afin de préserver la stabilité du serveur, HIRSCH préconise :

- D'effectuer les sauvegardes de la base de données à chaud (bases ouvertes). Cela évite l'arrêt de la base et donc un arrêt fonctionnel du serveur. En cas de sauvegarde à froid (base arrêtée), l'arrêt de la base doit obéir à une procédure stricte, sous peine de dysfonctionnements graves de l'application.
- Le serveur *MICROSESAME* ne doit pas être serveur de domaine. Il peut être un serveur autonome ou être membre d'un domaine.

Si une version de MICROSESAME existe sur la machine, une phase de désinstallation préalable peut être nécessaire.

Pour l'installation et la désinstallation, un compte ADMIN est obligatoire sur Windows.

Dans le cas de l'installation d'un produit qualifié, vous devez respecter les recommandations du guide **ANSSI-PA-72** .

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

Effectuez les opérations listées dans le tableau ci-après.

Tableau 2.1. 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 2.1.3, « 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	Consultez la liste des ports dans la section Schémas des flux et ports MICROSESAME dans ce guide.

A faire	Comment le faire
et sont ouverts. Il s'agit des ports 80, 443, 14001 à 14005, 22, PING/ICMP, 443, 5353, 11010 et 55000.	
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.

2.1.3. 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 2.2. 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	.....

2.1.4. Installer MICROSESAME sur un poste serveur

2.1.4.1. 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.

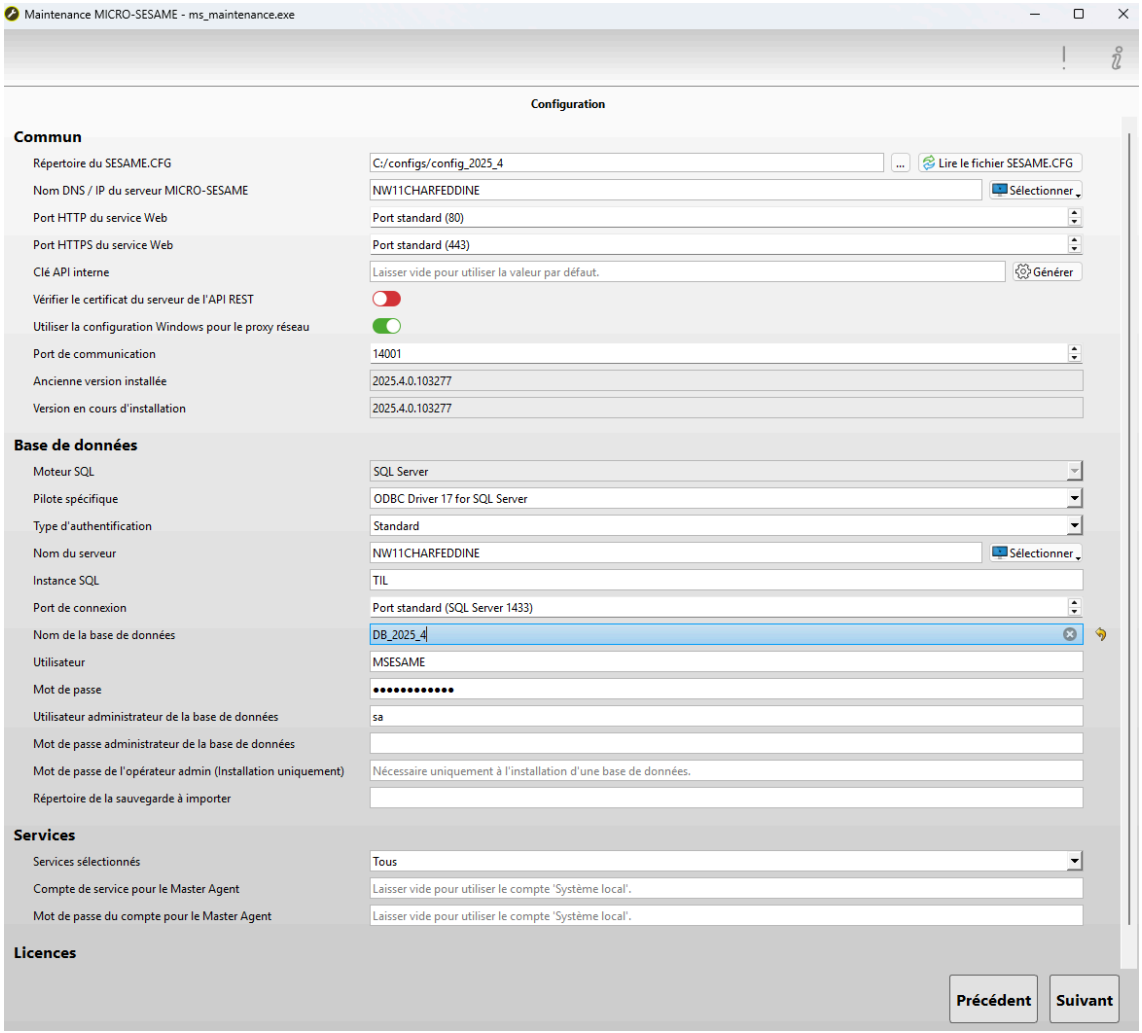
2.1.4.2. Installer MICROSESAME version serveur

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 2.1.4.3, « Configurer la base de données »*.

2.1.4.3. 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.

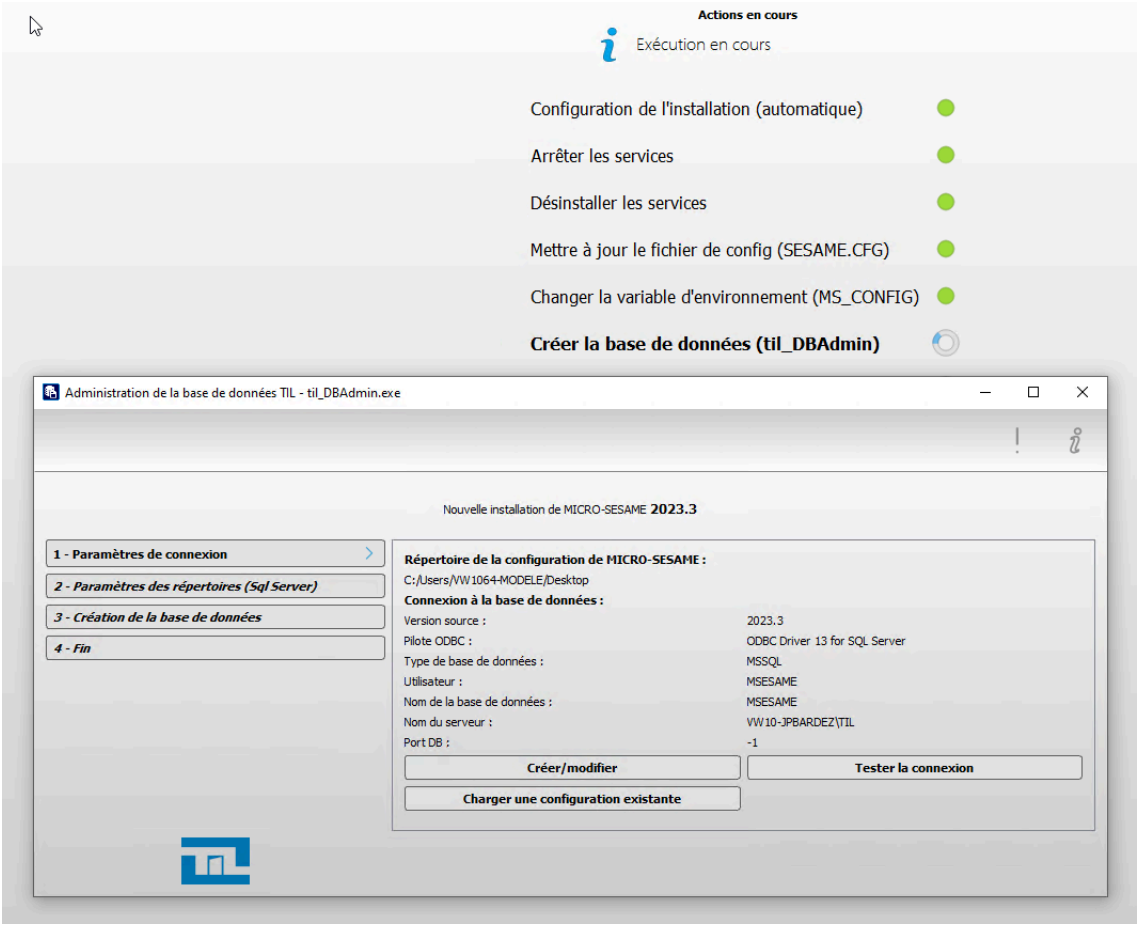
Tableau 2.3. Paramètres de configuration du serveur MICROSESAME

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 2.2, « 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 2.2, « 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 2.2, « 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 2.2, « 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.

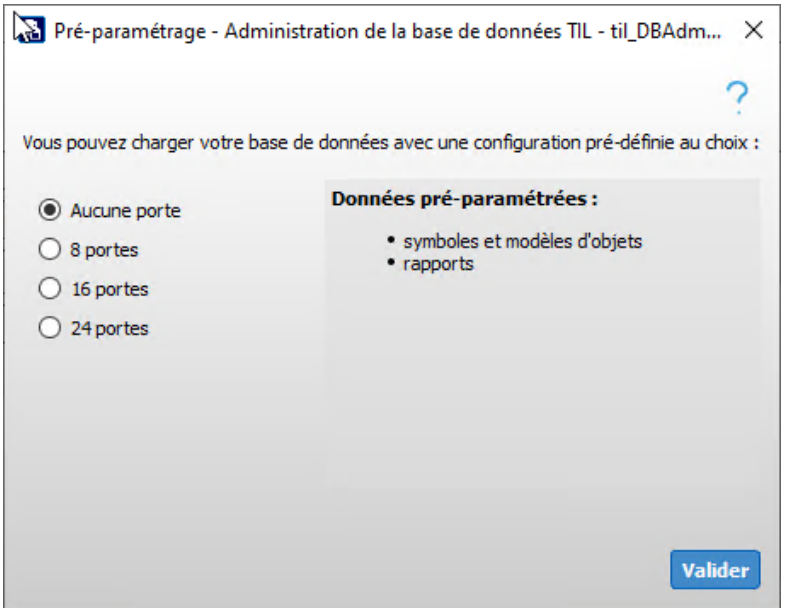
3. Cliquez sur Suivant. Le menu d'administration qui apparaît en surimpression donne accès à 4 boutons de paramétrage et affiche les paramètres de la connexion.



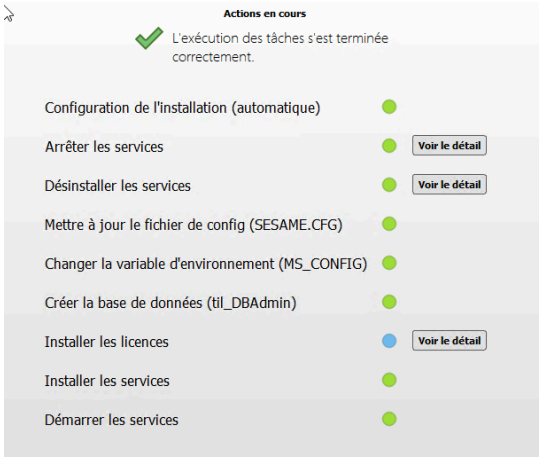
4. Suivez les instructions du tableau suivant.

Tableau 2.4. 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.

2.1.5. Premier lancement de MICROSESAME - Base prédéfinie

Si une base pré-définie 8, 16 ou 24 portes a été sélectionnée à l'installation de MICROSESAME, vous devez effectuer les actions suivantes au premier lancement de MICROSESAME :

1. Depuis le menu principal, suivre **Paramétrage > Mise en Exploitation > Appliquer le paramétrage**.
2. Cliquer sur le bouton **Tout compiler** à gauche.
3. Sélectionner l'onglet **Appliquer les changements**, puis :
   - Dans la liste déroulante, sélectionner **Appliquer les changements sur les propriétés**et cliquer sur le bouton **Exécuter**.
   - Dans la liste déroulante, sélectionner **Appliquer les changements sur les lignes** et cliquer sur le bouton **Exécuter**.
   - Dans la liste déroulante, sélectionner **Appliquer les changements sur les plages horaires**et cliquer sur le bouton **Exécuter**.

Une fois ces actions effectuées, les objets pré-définis par le système sont opérationnels.

2.1.6. Sécuriser la connexion entre la base de données et MICROSESAME

Suivez la procédure d'activation du chiffrement des communications, adaptée à la version de SQL Server installée, afin de sécuriser la connexion entre la base de données et MICROSESAME.

1. Exécutez "SQL Server Configuration Manager".
2. Sélectionnez "Protocoles pour MSSQL Server " et afficher les propriétés.
3. Forcez les chiffrements à "oui".
4. Redémarrez le service MSSQLSERVER.

La communication sera alors chiffrée avec un certificat auto-signé.

La génération/signature d'un certificat signé est de la responsabilité du client (service informatique).

Consultez *Section 2.1.9, « Mettre en place les certificats sur le serveur »*.

Vous pouvez modifier le certificat utilisé : contactez le DSSI du site.

2.1.7. Activer les échanges sécurisés TLS entre le serveur et les postes clients

Dans le cadre d'une installation sécurisée, vous devez activer les échanges TLS entre le serveur et les clients, ainsi que d'activer la vérification des certificats.

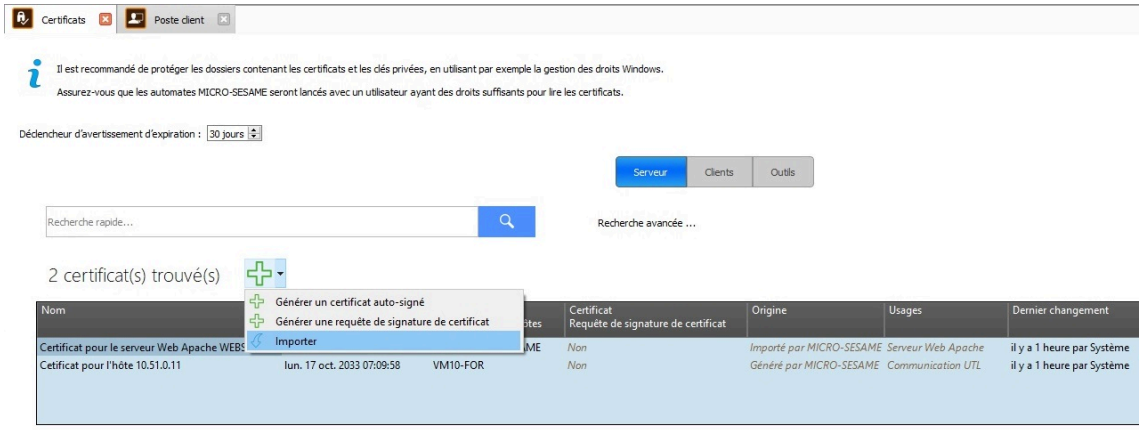
Contactez le DSSI du site afin d'obtenir des fichiers d'identification (certificat au format *.p12*) pour chaque poste serveur et client, nécessaires pour sécuriser les communications.

Pour la création de ces fichiers/certificats, voir *Mise en place des certificats TLS signés*.

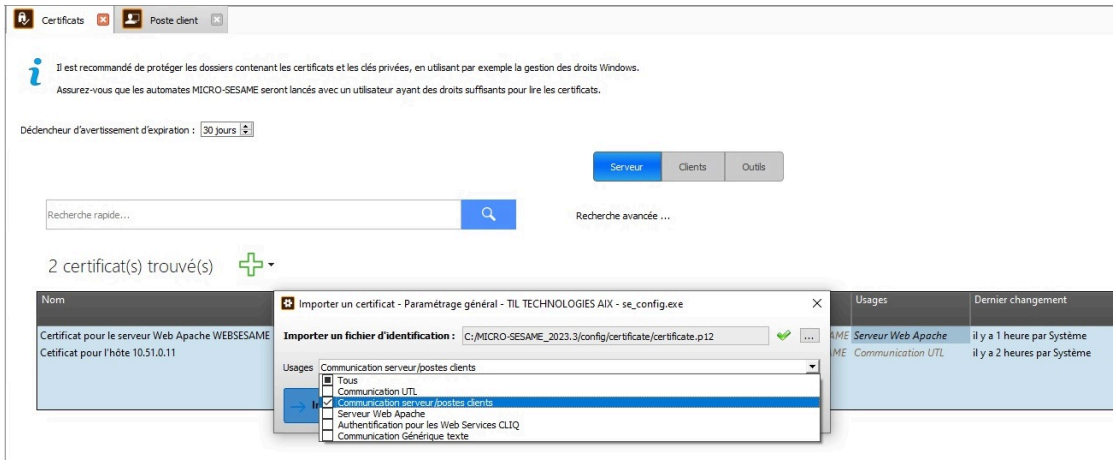
Pour utiliser correctement les fichiers d'identification, il faut impérativement qu'ils se nomment **certificate.p12** et qu'ils soient déposés dans le dossier **certificate** de MICROSESAME, sur chaque poste serveur et client.

Pour activer les échanges sécurisé TLS entre serveur et clients :

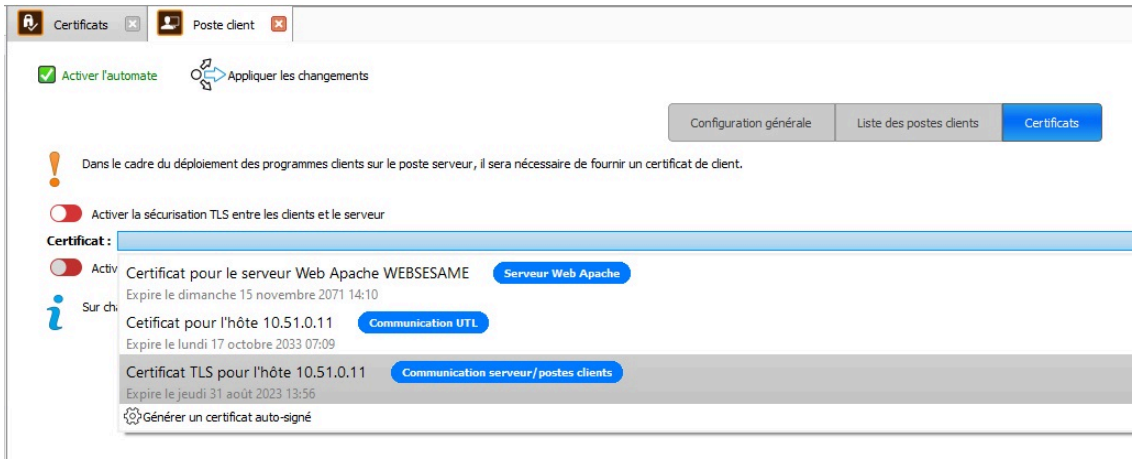
1. Dans l'explorateur Windows, ouvrez le dossier **certificate** créé par lors de l'installation de MICROSESAME. Par défaut : C:/MICROSESAME/config/certificate.
2. Copiez le fichier d'identification obtenu et renommez-le *certificate.p12*.
3. Depuis le menu principal, suivez **Paramétrage > Autres > Paramétrage général > Rubrique Système > Certificats**, puis cliquez sur le "+" vert et sélectionnez **Importer**.
4. Recherchez le fichier **certificate.p12**, puis cliquez sur **Ouvrir**.



5. Dans la boîte de dialogue qui s'affiche : dans le champ **Usages**, cochez la case **Communications serveur/postes clients**, puis cliquez sur le bouton **Importer**.



6. Une nouvelle ligne est créée dans le tableau récapitulatifs des certificats. Sauvegardez en cliquant sur l'icône **Disquette**.
7. Depuis le menu principal , suivez **Paramétrage > Matériel > Poste client**, puis cliquez sur le bouton **Certificats**.
8. Cliquez dans le champ **Certificats**, puis sélectionnez le certificat qui vient d'être importé.



9. Activez le commutateur **Activer la sécurisation TLS entre les clients et le serveur** (le faire passer au vert).
10. Activez le commutateur **Activer la vérification des certificats clients** (le faire passer au vert).
    Lorsque cette option est activée, les certificats auto-signés seront refusés. Vous devez impérativement utiliser un **certificat signé** par une autorité de confiance.
11. Vérifiez que la case **Activer l'automate** est bien cochée, enregistrez la configuration en cliquant sur l'icône **Disquette**, puis cliquer sur le bouton **Appliquer les changements**.
12. Sur chaque **poste client**, ajoutez le certificat associé à chacun des postes (renommés *certificate.p12*) dans le dossier **C:/MICROSESAME/config/certificate**

2.1.8. Fichier de logs

Dans le répertoire d'installation choisi (par défaut, C:/ MICROSESAME), un fichier de logs est généré automatiquement : **InstallationLog.txt**.

Ce fichier contient le registre des opérations réalisées avec l'installeur.

2.1.8.1. Vérifier le paramétrage du poste serveur

La communication entre le poste serveur et les postes clients s'effectue par l'intermédiaire du nom du serveur (Hostname) défini à l'installation, ainsi que du port de communication saisi.

Pour retrouver ces informations, consultez le fichier **ms_maintenance** ou recherchez-les dans le fichier **sesame.cfg**.

2.1.9. Mettre en place les certificats sur le serveur

Vous pouvez sécuriser les connexions aux applications suivantes en utilisant des certificats :

- **WEBSESAME :** mise en place de WEBSESAME avec serveur pour MICROSESAME, permettant l'accès via l'URL `https://nom_du_serveur:443` : paramétré par défaut à l'installation de MICROSESAME avec un certificat auto-signé.
- **UTL** : communication sécurisée avec les UTL. Paramétré par défaut avec un certificat auto-signé, si une configuration pré-définie 8, 16 ou 24 portes a été installée.
- **Dépôts https :**utiliser un mode sécurisé lors de l'installation des postes clients depuis MICROSESAME. Mise en place des dépôts https pour l'installeur client de MICROSESAME, via `https://nom_du_serveur:443/repository ou https:// nom du serveur:443/update` .
- **API REST :** mise en place de l'API REST de MICROSESAME (`https://nom_du_serveur:443/api`).

La génération/signature du certificat est de la responsabilité du client. Pour la mise en place des certificats, contactez le DSSI. Voir aussi *Mise en place des certificats TLS*.

2.1.10. Services MICROSESAME

Les communications de MICROSESAME reposent sur le fonctionnement de 2 services :

- **TIL - Master Agent**

- **TIL - Web Server**

L'application **Tableau de bord** dispose d'un jeu de commandes permettant de contrôler l'arrêt et le redémarrage des services. Un compte d'exécution particulier pour les services MICROSESAME - Master Agent et TIL-WebServer peut être spécifié.

2.1.11. Droits utilisateurs

Deux types d'utilisateurs peuvent être utilisés dans le cadre de l'installation de MICROSESAME :

- L'utilisateur Windows pour l'exécution de MICROSESAME depuis le poste.
- L'utilisateur SQL pour la création et l'accès à la base de données utilisée par MICROSESAME.

L'**utilisateur Windows** requiert des **droits d'administration** , afin de pouvoir réaliser l'installation/désinstallation de MICROSESAME et le démarrage/arrêt des services. Pour toute autre opération liée à MICROSESAME, un utilisateur sans droit spécifique suffit.

L'**utilisateur SQL** "MSESAME" avec droits d'administration de la base de données est nécessaire et créé par l'application *til_dbadmin.exe*, pendant le processus de création de la base de données.

Le couple identifiant/mot de passe MICROSESAME par défaut est MSESAME/ MSES@ME_1111.

Le nom de la base de données est MSESAME.

2.2. Installer WEBSESAME sur un serveur déporté

WEBSESAME permet aux agents d'accueil d'effectuer, entre autres, les opérations suivantes :

- Prendre des rendez-vous.
- Gérer les identifiés.
- Parcourir l'historique.
- Parcourir le fil de l'eau et les alarmes.

Les agents d'accueil utilisent souvent un réseau «bureautique» distinct du réseau « sécurité » sur lequel MICROSESAME fonctionne. Un pare-feu permet de gérer les quelques échanges autorisés entre les 2 réseaux. Dans ce type d'architecture réseau, les employés n'ont donc pas accès à WEBSESAME.

Pour que les agents d'accueil puissent utiliser WEBSESAME, il faut l'installer sur un serveur du réseau "bureautique" et autoriser ce dernier à communiquer avec le serveur MICROSESAME du réseau "sécurité", grâce à une règle définie au niveau du pare-feu.

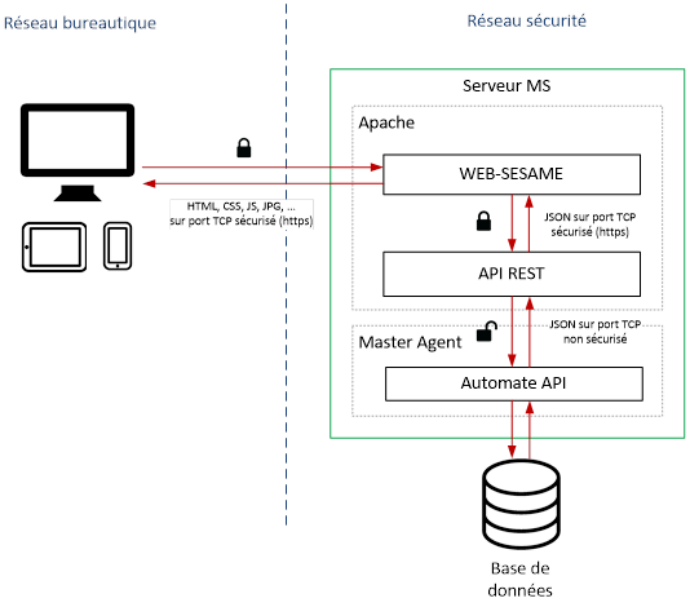
2.2.1. Collaborer avec le service informatique du client

Vous devez travailler en collaboration avec le service informatique du client, notamment pour :

- Configurer le pare-feu entre les 2 réseaux.
- Installer un serveur web ou le serveur embarqué avec MICROSESAME.
- Générer le certificat TLS.

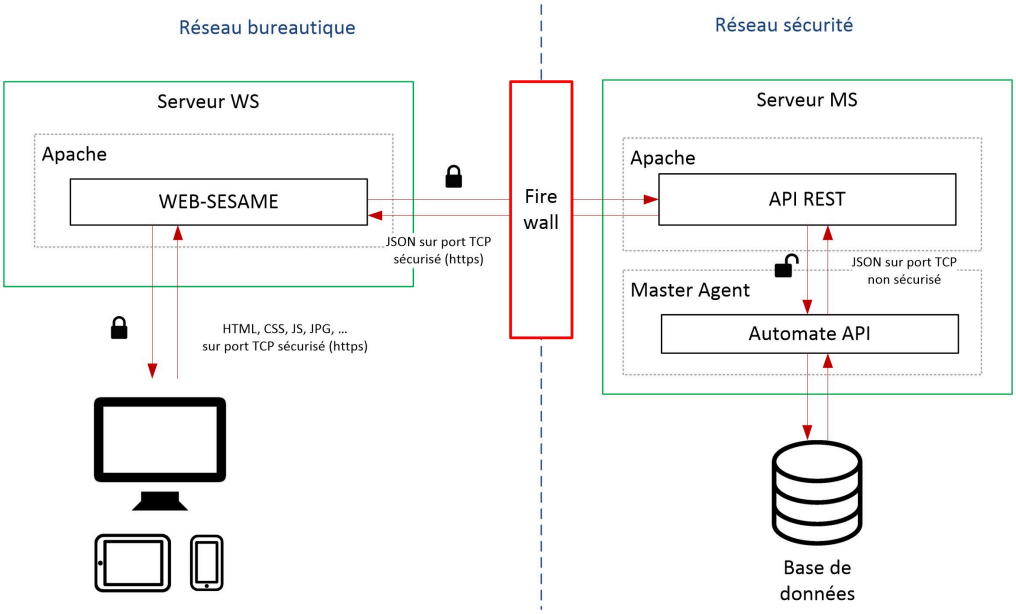
2.2.2. Architectures type

- Architecture simple (installation standard) :



Dans cette architecture, le serveur MS est directement accessible depuis n'importe quel poste du réseau bureautique.
Bien que certaines applications MICROSESAME écoutent uniquement en local (ex : l'automate API n'accepte que les connexions locales), le serveur MICROSESAME reste exposé.
Par défaut, les *clients légers* qui tentent de se connecter à WEBSESAME en HTTP sont automatiquement redirigés vers une connexion sécurisée HTTPS.
WEBSESAME ne dialogue jamais directement avec la base de données. Elle utilise exclusivement l'API REST (communication sécurisée).

- Architecture avancée (installation manuelle) :



Seule l'application WEBSESAME est désormais accessible par un poste du réseau bureautique.
Le pare-feu bloque toute tentative de connexion d'un poste du réseau bureautique au réseau sécurité.

2.2.3. Avant l'installation de WEBSESAME

2.2.3.1. Vérifier l'accessibilité de l'API REST au sein du réseau sécurité

Le port de l'API REST est par défaut le port TCP sécurisé 443.

1. Pour vérifier le port, consultez le fichier <CONFIG>/sesame.cfg sur le serveur MICROSESAME.
2. Sur un ordinateur du réseau «sécurité», tapez dans la barre d'adresse d'un navigateur : *https://serveurmicrosesame:443/api/licenses?prettyPrint* (modifiez l'adresse/port si besoin).
3. En cas d'erreur, vérifiez le service Master Agent et l'automate API.

2.2.3.2. Vérifier l'accessibilité de l'API REST depuis le serveur distant

De la même manière, vérifiez l'accessibilité du port API REST depuis le serveur distant du réseau «bureautique ».

Si une réponse est obtenue, c'est que le pare-feu est correctement configuré : passez à l'étape suivante.

Il se peut que le serveur WEBSESAME ne puisse résoudre le nom de machine du serveur MICROSESAME, car il n'a pas forcément accès au DNS du réseau "sécurité". Refaites un test avec l'adresse IP du serveur MICROSESAME, plutôt qu'avec son nom de machine.

Si aucune réponse n'est obtenue, contactez le service informatique pour ajouter une règle de trafic descendant, du serveur distant WEBSESAME au serveur MICROSESAME, sur le port sécurisé en question.

2.2.4. Installer WEBSESAME sur un serveur déporté sous Windows

2.2.4.1. Installer/configurer le serveur WEB

Soit le client veut maîtriser le serveur WEB et il prend en charge son installation, soit le client/partenaire utilise le serveur WEB fourni avec MICROSESAME.

WEBSESAME est validé avec le serveur WEB suivant. Nous conseillons d'utiliser la configuration ci-après.

Tableau 2.5. Configuration du serveur WEB déporté hébergeant WEBSESAME

Élément	Fonction
Apache	Serveur web
Mod_PHP	Pages dynamiques

Élément	Fonction
Module SSL et OpenSSL	Chiffrement/Authentification HTTPS
Module rewrite	Redirection du port HTTP (par défaut 80) vers le port sécurisé (par défaut 443)
Extension PHP php_curl.dll	Appel à l'API REST depuis PHP

Installer le serveur WEB embarqué dans MICROSESAME :

1. Copiez le dossier **prog** du serveur MICROSESAME sur le serveur WEBSESAME (ex : C:/MSESAME/prog).
2. Créez un dossier de configuration (ex : C:/MSESAME/config). Les logs d'exécution seront stockés dans ce dossier.
3. Créez un fichier **sesame.cfg** vide dans le dossier précédent.
4. Exécutez **MS_starter** sur le serveur WEBSESAME et ajoutez une configuration avec ces 2 dossiers.
5. Dans la barre d'icônes supérieure, cliquez sur l'icône **Installer et démarrer** et sur l'option **Service 'TIL - Web Server'**. Cette étape va configurer Apache (<PROG>/apache/conf) et PHP (<PROG>/php/php.ini), installer le service Apache (<PROG>/apache/bin/httpd.exe) et le démarrer.
6. La fenêtre d'authentification de WEBSESAME devrait être accessible (l'erreur de certificat SSL est normale à cette étape). En revanche, l'authentification ne devrait pas fonctionner puisque WEBSESAME n'a pas encore connaissance de l'URL à utiliser pour accéder à l'API REST du serveur MICROSESAME.

2.2.4.2. Installer et configurer l'applicatif WEBSESAME

1. **Installer WEBSESAME**
   Si le client a géré lui-même l'installation du serveur web, le serveur WEB embarqué avec MICROSESAME n'a pas été installé. Il est donc nécessaire de copier le contenu du dossier **web/src** du serveur MICROSESAME dans le serveur WEBSESAME.
2. **Configurer WEBSESAME**
   Modifiez le fichier <WEBSESAME>/prog/web/apache/conf/**httpd.user.conf**, en ajoutant l'adresse vers le serveur dédié MICROSESAME et vérifiez la clé API (se_config.exe > API REST > Applications internes > WEBSESAME) :

   ```
   SetEnv API_KEY "{XXXXXXXX-XXXX-XXXX-XXXX-XXXXXXXXXXXX}"
   SetEnv API_URL "https://adresse-server-microsesame"
   ```

3. Supprimez le répertoire <MICROSESAME>/prog/web/src/back/var/cache, si existant. Redémarrez Apache depuis MS-starter, cliquez sur l'icône **Redémarrer les services**, puis sélectionnez **"Service TIL - Web Server"**.

   Attention : le fait d'installer de nouveau le service TIL - Web Server réinitialise la clé API_URL.

4. **Vérifier le fonctionnement de WEBSESAME**
   Ouvrez avec un login/mot de passe opérateur MICROSESAME la page d'authentification de WEBSESAME.

Utilisez l'application pour vérifier que les données sont bien accessibles (par exemple, en effectuant une recherche d'identifié).

2.2.4.3. Passer du certificat par défaut à un certificat auto-signé pour le service Apache de WEBSESAME

L'exécution de l'application WEBSESAME est sécurisée (HTTPS). WEBSESAME est livré, par défaut, avec un certificat auto-signé non valide. Seul le client final possède les informations nécessaires à la génération et à la signature, par une autorité de confiance, du certificat (nom de domaine, durée de validité, ...).

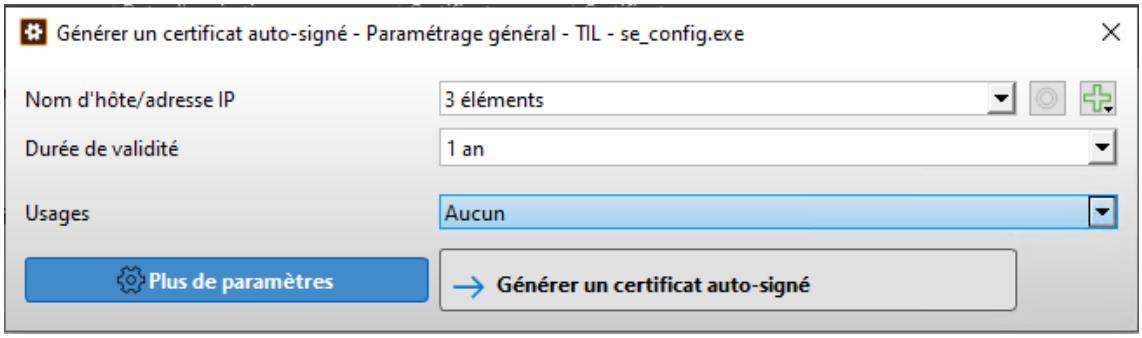
Si le client veut éviter que le navigateur des postes clients affiche une erreur lors de la connexion à WEBSESAME, il doit donc générer son propre certificat et le faire signer par son autorité de confiance.

Si le client utilise le serveur WEB embarqué avec MICROSESAME, la section suivante présente la procédure à suivre pour installer un certificat signé par un contrôleur de domaine, dans le service Apache de WEBSESAME.

Installer un certificat TLS auto-signé dans le service Apache de WEBSESAME

1. À partir du menu principal de MS, accédez à l'écran de paramétrage des **certificats** (Paramétrage > Système > Certificats).
2. Cliquez sur l'onglet Serveur.
   La liste des certificats existants s'affiche.
3. En partie supérieure de l'écran, vous pouvez choisir le nombre de jours à partir duquel vous serez prévenu de l'expiration d'un certificat.
4. Pour générer un certificat auto-signé, cliquez sur .
   Une fenêtre de saisie s'affiche.

Figure 2.1. Fenêtre de saisie des informations nécessaires pour la création d'un certificat auto-signé



5. Renseignez les champs de cette fenêtre selon le tableau ci-après.

Liste déroulante/ Champs	Valeur possible
Nom d'hôte/adresse IP	Normalement, tous les éléments de cette liste.

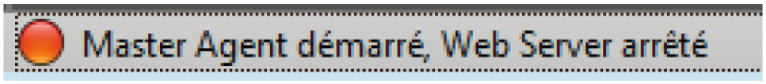
Liste déroulante/ Champs	Valeur possible
Durée de validité	Cette durée peut-être longue car la nature du certificat fait que vous le signez.
Usages	Serveur Web.
Plus de paramètres	Vous pouvez personnaliser ces paramètres avec le nom de votre société.

6. Cliquez sur -> Générer un certificat auto-signé.
   Le nouveau certificat s'affiche dans la liste des certificats.

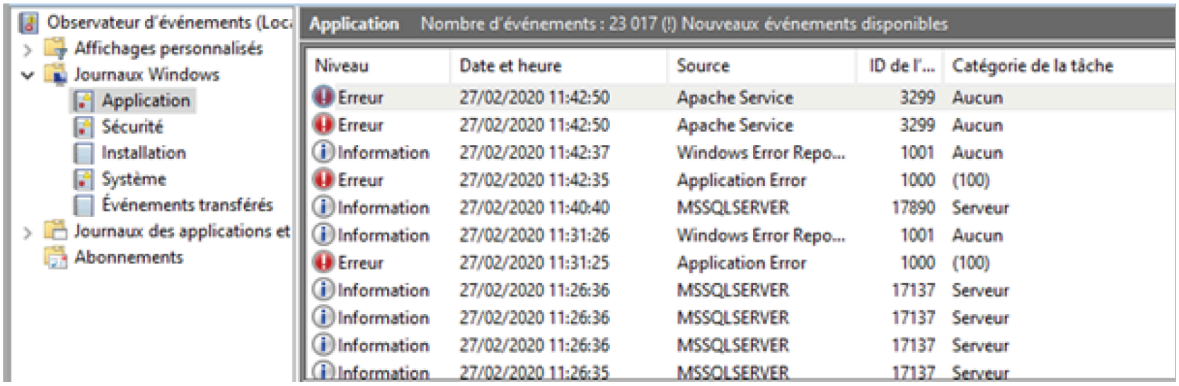
Erreurs de serveur Web possibles lors de la génération d'un certificat auto-signé

Le Web Server démarre puis s'arrête

Si le Web Server démarre puis s'arrête :

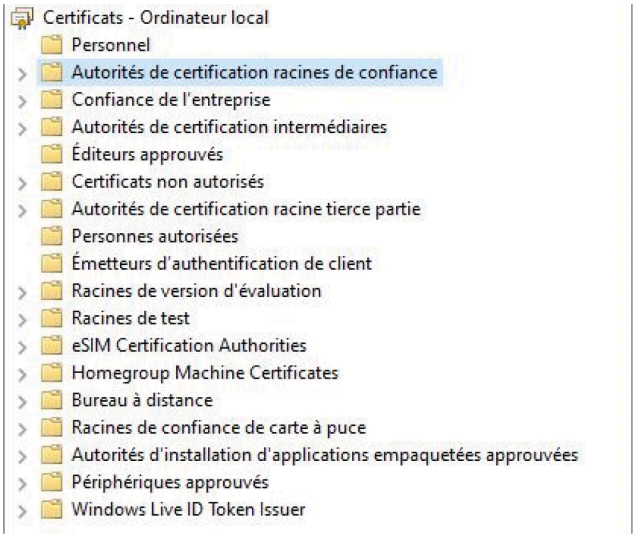


Consultez les erreurs des Journaux Windows de l'application « Observateur d'évènements » pour les corriger.



L'émetteur du certificat n'est pas reconnu comme étant digne de confiance

En lançant WEBSESAME, si l'émetteur du certificat n'est pas reconnu comme étant de confiance, ajoutez-le dans le dossier « Autorités de certification racines de confiance » du panneau de configuration **Microsoft Management Console** de l'ordinateur :



Si vous utilisez le navigateur "Mozilla Firefox", ajoutez le certificat dans la bibliothèque de certificats de ce navigateur

Contrairement autres navigateurs internet, Mozilla Firefox n'utilise pas la bibliothèque de certificats de confiance du système d'exploitation Windows. Il possède sa propre bibliothèque de certificats.

Pour ajouter le certificat d'autorité racine dans la bibliothèque de Firefox :

1. Cliquez sur **Outils**, puis sur **Option**.
2. Cliquez sur l'onglet **Vie privée et sécurité**, puis dans la section **Sécurité**.
3. Cliquez sur **Certificats**, puis sur Afficher les certificats.
4. Pour importer le ROOT, cliquez sur l'onglet Autorité, puis sur Importer.

Gérer une liste d'autorités de certification

Pour gérer une liste d'autorités de certification, vous devez préciser manuellement son chemin dans le fichier httpd.user.conf.

1. Ouvrez le fichier **httpd.user.conf** sous *prog\web\apache\conf\httpd.user.conf* du dossier MICROSESAME créé à l'installation.
2. Cherchez les lignes ci-après :

```
# Chemin vers le dossier des autorités de certification :
# Define TIL_SSL_CA_CERTIFICATE_PATH "C:/Path/To/Public"
```

3. Supprimez les signes « # » devant les chemins des fichiers :

```
# Chemin vers le dossier des autorités de certification :
Define TIL_SSL_CA_CERTIFICATE_PATH "C:/Path/To/Public"
```

4. Remplacez les chemins certificats exemples par les chemins des certificats signés par une autorité de certification :

```
# Chemin vers le dossier des autorités de certification :
Define TIL_SSL_CA_CERTIFICATE_PATH "C:/Path/To/Public"
```

Faites attention à écrire les noms des fichiers accompagnés de leur extension :
X **server-ca**
server-ca.crt

5. Sauvegardez le fichier **httpd.user.conf**
6. Lancez l'outil "ms_starter".
7. Pour arrêter le service du serveur Web, cliquez sur le bouton  .
8. Pour redémarrer le service du serveur Web, cliquez sur le bouton  .

Import du certificat de l'autorité racine dans la banque de certificats racines de confiance de Windows

Il est nécessaire d'importer le certificat *ROOT* ainsi que ceux des autorités intermédiaires (*MID*) dans la banque de certificats Windows (autorités de certification racines de confiance), sur tous les postes qui auront accès à l'application WEBSESAME, ainsi que dans la banque des postes clients lourds MICROSESAME.

C'est par l'intermédiaire de ce certificat que les postes vérifieront l'identité du serveur APACHE sur lequel ils se connecteront.

Le certificat doit être ajouté sur le compte ordinateur et non sur un compte utilisateur.

1. Ouvrez le gestionnaire des certificats de Windows (mmc.exe depuis l'invite de commande)
2. Suivez **Fichier > Ajouter/Supprimer un composant logiciel enfichable**.
3. Suivez **Certificats > Ajouter**, puis sélectionnez l'option **Un compte d'ordinateur**, pour que le certificat soit lié au poste.
4. Validez en cliquant sur Terminer puis sur OK.
5. Dépliez la liste **Certificats (ordinateur local)**, puis la liste **Autorités de certification racines de confiance**.
6. Faites un clic droit sur le dossier **Certificats**, puis cliquez sur **Toutes les tâches** et sur Importer.
7. Cliquez sur Suivant, sélectionnez le certificat ROOT, puis cliquez sur Suivant.
8. Si nécessaire, répétez ces opérations pour chaque certificat intermédiaire (MID).
9. Vérifiez que le certificat s'installe bien dans le magasin **Autorités de certification racines de confiance**.
10. Cliquez sur Suivant, puis sur Terminer.

2.2.4.4. Déclarer l'adresse du serveur déporté dans MICROSESAME

Une fois la configuration du serveur déporté effectuée, il est nécessaire de déclarer l'URL du serveur web correspondante.

L'adresse déclarée ci-après permettra d'envoyer des liens de connexion à WEBSESAME par mail.

1. Depuis le menu principal, se rendre dans **Paramétrage > Autres > Paramétrage général > Rubrique Système > WEBSESAME** .
2. Dans la rubrique **Serveur WEBSESAME**, renseignez l'adresse du serveur déporté dans le champ URL, en respectant le format suivant :

```
https://Adresse.serveur:Port/Path/to/WEBSESAME
```

3. Cliquez sur le bouton **Ouvrir dans un navigateur WEB** pour vérifier la validité de l'URL.

2.2.5. Installer WEBSESAME sur un serveur déporté sous Linux

Les balises suivantes représentent les répertoires d'installations des différents composants :

- <WEBSESAME> : racine du répertoire d'installation de WEBSESAME sur le serveur déporté.
- <MICROSESAME> : racine du répertoire d'installation de MICROSESAME sur le serveur.

Il est conseillé de conserver la structure des répertoires créée par défaut lors de l'installation du composant Apache.

2.2.5.1. Installer des composants sur le serveur déporté

Soit le partenaire veut maîtriser le serveur WEB et il prend en charge son installation, soit le partenaire suit pas à pas la procédure de configuration du serveur WEB recommandée par HIRSCH, décrite ci-après.

Pour connaître les versions des modules correspondant à une configuration conforme ANSSI, contacter HIRSCH .

Installer APACHE et PHP sur le serveur déporté

1. Installez APACHE et PHP sur le serveur déporté.
   Le répertoire d'installation <WEBSESAME> par défaut est var/www/html.
   Avec UBUNTU :

```
sudo su -
apt-get update
apt-get install apache2 php7
apt-get install libapache2-mod-php
```

2. Changez les valeurs suivantes dans le fichier de configuration PHP (PHP.ini).

```
post_max_size = 1G
upload_max_filesize = 1G
```

3. Installez et activez les 4 extensions PHP :

```
curl
fileinfo
openssi
sockets
```

Avec UBUNTU :

```
apt-get install php-curl php-gd php-curl
apt-get install php-dom php-intl php-json
apt-get install php-mbstring php-xml php-zip
```

4. Installez et activez les 7 modules Apache :

```
mod_rewrite
mod_setenvif
mod_proxy
mod_env
mod_socache_shmcb
mod_ssl
mod_php
```

Avec UBUNTU :

```
a2enmod rewrite env setenvif ssl proxy_http
a2ensite default-ssl
```

Copier les ressources WEBSESAME sur le serveur déporté

1. Sur le serveur principal, ouvrez le dossier <MICROSESAME> /prog/web/src.
2. Copiez les dossiers Front et Back.
3. Collez ces dossiers dans le répertoire d'installation <WEBSESAME> sur le serveur déporté.

En cas d'erreur lors de la manipulation du dossier Back, exécutez les commandes suivantes pour modifier les droits (adapter si nécessaire l'emplacement du dossier Back) :

```
sudo chmod 755 -R /var/www/html/back/vendor/
sudo chown www-data:www-data -R /var/www/html/back/var
sudo mkdir /var/www/html/back/var/cache
```

Copier le dossier des constantes sur le serveur déporté

1. Sur le serveur principal, ouvrez le dossier <MICROSESAME> /data.

2. Copiez le dossier **const**.
3. Collez le dossier **const** dans le répertoire d'installation <WEBSESAME> sur le serveur déporté.

2.2.5.2. Configurer Apache avec les paramètres MICROSESAME, sécuriser la connexion à WEBSESAME et la personnaliser

Vous devez maintenant configurer Apache avec les paramètres du serveur MICROSESAME et sécuriser la connexion à WEBSESAME. Vous devrez peut-être adapter certains des éléments décrits dans les fichiers de configuration Apache, ou ajouter de nouvelles commandes, afin de finaliser l'installation.

L'exécution de l'application WEBSESAME est sécurisée (HTTPS). Par défaut, WEBSESAME est livré avec un certificat auto-signé non valide. Seul le client final possède les informations nécessaires à la génération et à la signature du certificat (nom de domaine, durée de validité, ...) par une autorité de confiance.

Afin d'éviter que le navigateur des postes clients affiche une erreur lors de la connexion à WEBSESAME, le client doit générer son propre certificat et le faire signer par son autorité de confiance. Il est nécessaire d'ajouter l'émetteur du certificat dans la liste des autorités de confiance reconnues par l'ordinateur.

Configurer Apache avec la redirection HTTP vers HTTPS

La procédure suivante permet de configurer la redirection du HTTP vers le HTTPS lors d'une connexion à WEBSESAME :

1. Ouvrez le dossier de configuration Apache sur le serveur déporté et éditer le fichier **000-default.conf**.
2. Spécifiez que la racine du répertoire d'installation est WEBSESAME.

```
DocumentRoot <WEBSESAME>
SetEnv WS_BACK_PATH "/back/index.php"
```

3. Pour configurer la redirection de HTTP vers HTTPS lors d'une connexion à WEBSESAME, ajoutez les lignes suivantes (sans en modifier le contenu).

```
RewriteEngine On
RewriteCond %{HTTPS} off
RewriteRule ^ https://%{HTTP_HOST}%{REQUEST_URI}
```

4. Enregistrez le fichier **000-default.conf**.
5. Relancez le service WEB.

Configurer Apache avec les données du serveur MICROSESAME

1. Ouvrez le dossier de configuration Apache sur le serveur déporté et éditez le fichier **default-ssl.conf**.
2. À partir de la version 2024.3, s'il est nécessaire de personnaliser le champ mellon, vous pouvez ajouter la ligne suivante dans le httpd.conf du serveur Apache déporté.

```
Define TIL_SAML_BINDING_KEY "MELLON_MAIL"
```

3. Configurez le front-end WEBSESAME (mettez à jour la racine du répertoire d'installation de WEBSESAME).

```
DocumentRoot <WEBSESAME>/front
<Directory <WEBSESAME>/front>
    Require all granted
    DirectoryIndex index.html
    FallbackResource /index.html
</Directory>
```

4. Configurez le back-end WEBSESAME (mettez à jour la racine du répertoire d'installation de WEBSESAME).

```
Alias /back <WEBSESAME>/back/public
<Directory <WEBSESAME>/back/public>
    Require all granted
    DirectoryIndex index.php
    FallbackResource /index.php
    RewriteEngine On
    RewriteRule .* - [E=HTTP_AUTHORIZATION:%{HTTP:Authorization}]
</Directory>
```

5. Configurez les constantes (mettez à jour la racine du répertoire d'installation de WEBSESAME).

```
Alias /const /var/www/html/const
<Directory /var/www/html/const>
    Options FollowSymLinks
    AllowOverride None
    Options +Indexes
    Require all granted
    Header set Access-Control-Allow-Origin "*"
    Header set Access-Control-Allow-Methods "GET, OPTIONS"
    Header set Access-Control-Max-Age "3600"
    Header set Access-Control-Allow-Headers "Content-Type,
 Authorization, X-PROFILE, Accept-language"
</Directory>
```

6. Ajoutez les lignes de configuration des Websockets (sans en modifier le contenu).

```
SSLProxyEngine on
SSLProxyVerify none
SSLProxyCheckPeerCN off
SSLProxyCheckPeerName off
```

```
SSLProxyCheckPeerExpire off
```

7. Configurez les websockets.

```
<Location /realtime>
   ProxyPass "wss://adresse-server-microsesame/realtime"
 upgrade=websocket timeout=604800 connectiontimeout=10
</Location>
```

8. Redémarrez le serveur Apache afin de finaliser l'installation.

2.2.5.3. Exemple de configuration Apache

L'exemple de configuration suivant représente la configuration minimale requise du fichier **default-ssl.conf**, afin de faire fonctionner WEBSESAME en mode déporté.

```
<VirtualHost _default_:443>

    SetEnv WS_BACK_PATH "/back/index.php"

    # Mettre à jour avec les informations adaptées
    SetEnv API_KEY "{XXXXXXXX-XXXX-XXXX-XXXX-XXXXXXXXXXXX}"
    SetEnv API_URL "https://adresse-server-microsesame"
    SetEnv API_TOKEN_VALIDITY "+1 hour"

    # Ne pas modifier
    SetEnv APP_ENV "prod"
    SetEnv APP_SECRET "d0a74b279e2932e76f3dccc8a07b540f"

    # WEBSESAME Front-End (React)
    # Ne pas modifier
    DocumentRoot <WEBSESAME>/front
    <Directory <WEBSESAME>/front>
        Require all granted
        DirectoryIndex index.html
        FallbackResource /index.html
    </Directory>

    # WEBSESAME Back-end (PHP)
    # Ne pas modifier
    Alias /back <WEBSESAME>/back/public
    <Directory <WEBSESAME>/back/public>
        Require all granted
        DirectoryIndex index.php
        FallbackResource /index.php
        RewriteEngine On
        RewriteRule .* - [E=HTTP_AUTHORIZATION:
%{HTTP:Authorization}]
    </Directory>

    Alias /const /var/www/html/const
    <Directory /var/www/html/const>
        Options FollowSymLinks
        AllowOverride None
        Options +Indexes
        Require all granted
        Header set Access-Control-Allow-Origin "*"
        Header set Access-Control-Allow-Methods "GET, OPTIONS"
        Header set Access-Control-Max-Age "3600"
        Header set Access-Control-Allow-Headers "Content-Type,
 Authorization, X-PROFILE, Accept-language"
    </Directory>
```

```
    # Temps réel (websockets)
    # Ne pas modifier
    SSLProxyEngine on
    SSLProxyVerify none
    SSLProxyCheckPeerCN off
    SSLProxyCheckPeerName off
    SSLProxyCheckPeerExpire off

    <Location /realtime>
      # Mettre à jour avec les informations adaptées
      ProxyPass "wss://adresse-server-microsesame/realtime"
 upgrade=websocket timeout=604800 connectiontimeout=10
    </Location>

</VirtualHost>
```

2.2.5.4. Déclarer l'adresse du serveur déporté dans MICROSESAME

Une fois la configuration du serveur déporté effectuée, vous devez déclarer l'URL du serveur web correspondante.

L'adresse déclarée ci-après permettra d'envoyer des liens de connexion à WEBSESAME par mail.

Depuis le menu-principal, se rendre dans le **Paramétrage général** :

1. Accédez à l'onglet **Menu principal**.
2. Dans la partie Serveur WEBSESAME, renseignez l'adresse du serveur déporté en respectant le format suivant :

   ```
   https://Adresse.serveur:Port/Path/to/WEBSESAME
   ```

3. Pour vérifier la validité de l'URL, cliquez sur le bouton Ouvrir dans un navigateur WEB.

2.3. Mettre en place un poste client MICROSESAME

- Avant de lancer l'assistant d'installation, vérifiez que toutes les mise à jour des postes clients ont été effectuées.
- Pour que l'installation du poste client se déroule correctement, le poste serveur et le poste client doivent pouvoir communiquer sur le même réseau. En cas de doute, contactez l'administrateur SI.

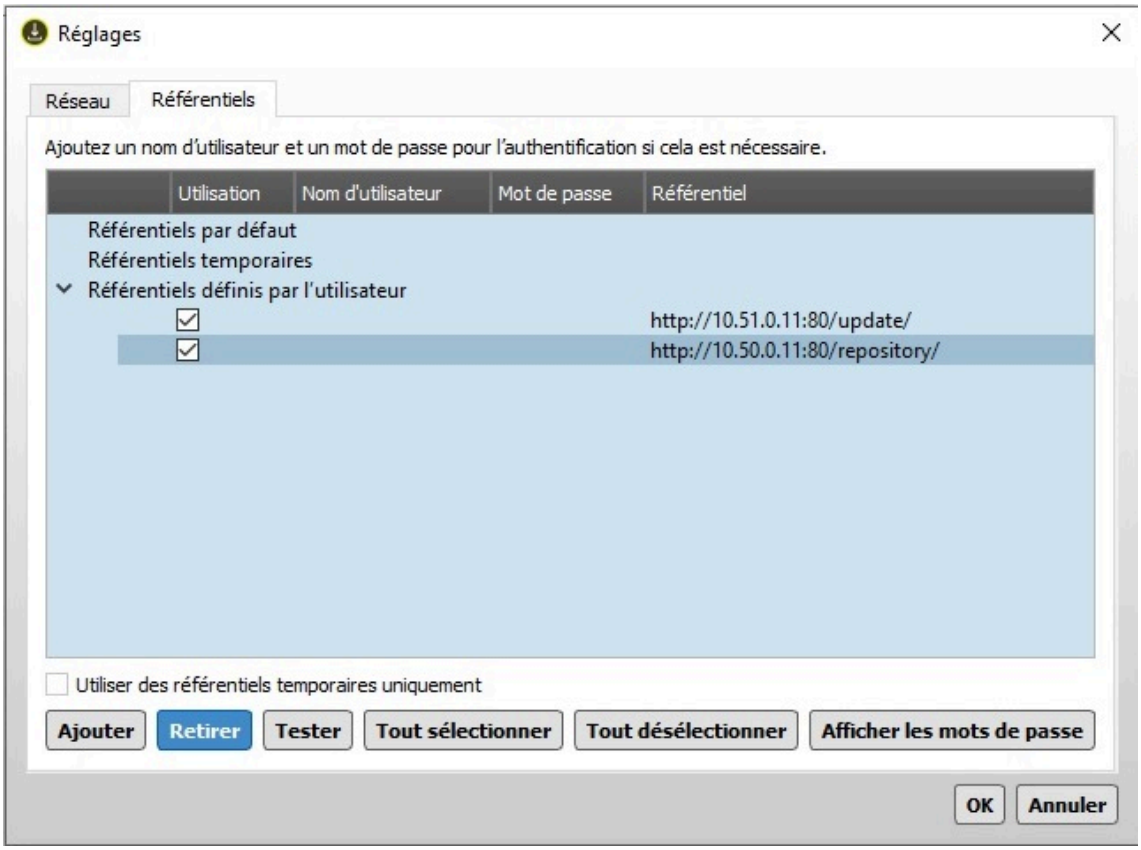
Dans le cas de l'installation d'un produit qualifié, vous devez respecter les recommandations du *guide ANSSI-PA-72* .

2.3.1. 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*.

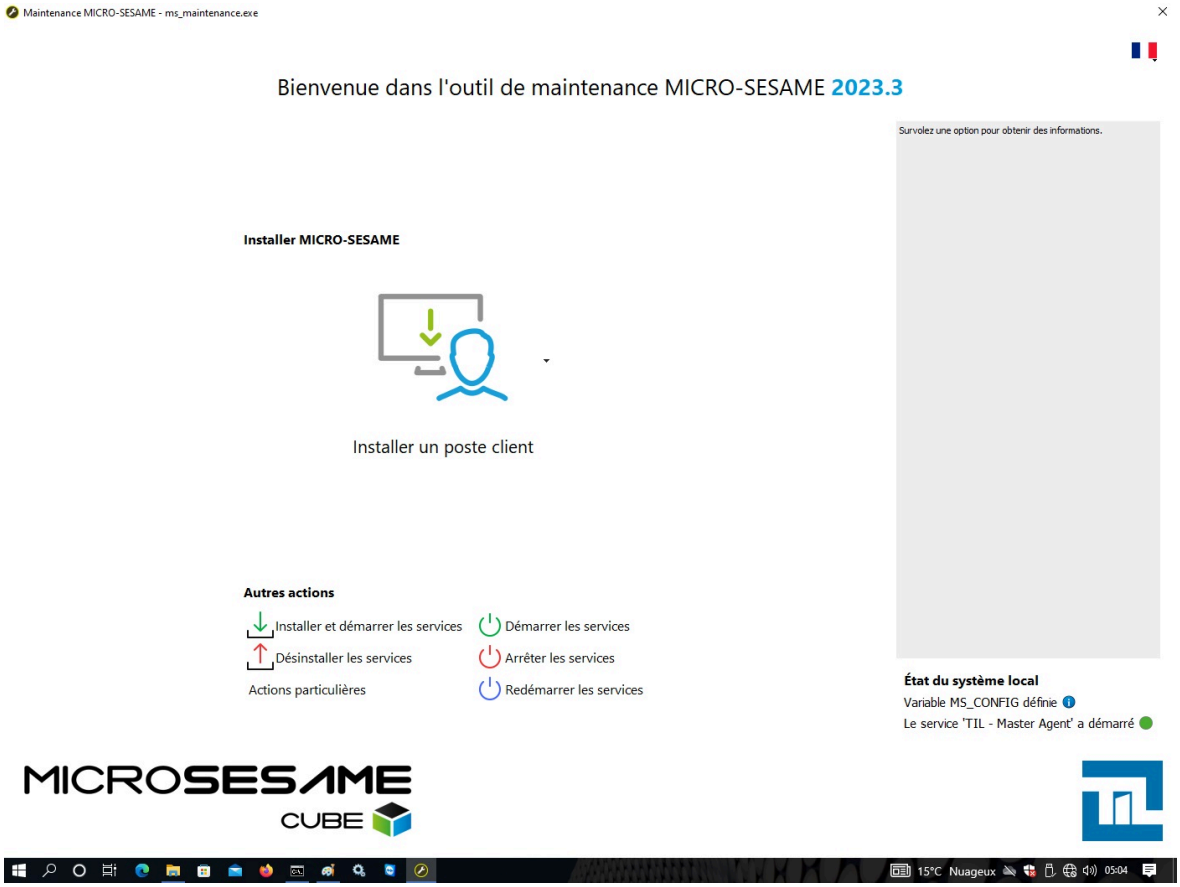
7. Sur les deux lignes, remplacez "hostname" par l'adresse IP du poste serveur, puis cliquez sur **Tester**.
8. Cliquez sur **Suivant**.
9. Par défaut l'assistant propose d'installer MICROSESAME dans le répertoire C:\MICROSESAME (laisser par défaut C:\MICROSESAME installera les programmes

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.

2.3.2. Connecter le poste client à la base de données et aux services MICROSESAME

Bienvenue dans **l'outil de maintenance MICROSESAME** (application *ms_maintenance.exe*).



1. A partir de l'écran de maintenance de MICROSESAME, cliquez sur **Installer un poste client**, puis choisissez **Installation rapide** (cas d'une nouvelle installation). La fenêtre de session s'ouvre.
2. Continuez avec *Section 2.3.2.1, « Installation rapide du poste client MICROSESAME »* ou avec *Section 2.3.2.2, « Installation avancée du poste client MICROSESAME »*.

2.3.2.1. Installation rapide du poste client MICROSESAME

1. Sélectionnez Installation rapide. La fenêtre de session s'ouvre.
2. Saisissez les **identifiants** de l'opérateur **Administrateur** pour finaliser l'installation de MICROSESAME : la fenêtre des **Actions en cours** s'ouvre et affiche l'exécution des dernières étapes (création du dossier *config* et du fichier *sesame.cfg*, changement de la variable d'environnement, installation et démarrage des services TIL.
3. Cliquez sur le bouton Quitter pour terminer. L'écran de configuration disparaît et les raccourcis des 7 modules MICROSESAME sont créés sur le bureau.

2.3.2.2. Installation avancée du poste client MICROSESAME

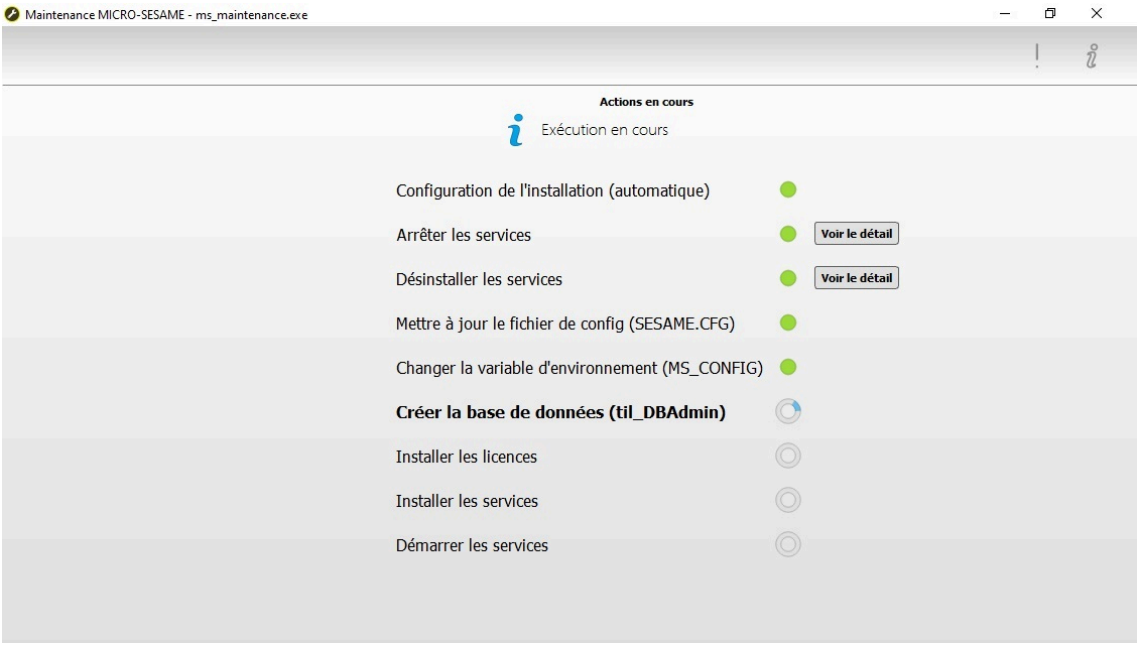
1. Cliquez sur **Installation avancée**. La fenêtre de session s'ouvre.
2. Saisissez les **identifiants** de l'opérateur **Administrateur** de MICROSESAME : la fenêtre de **Maintenance** s'ouvre et affiche l'exécution des dernières étapes (création du dossier *config* et du fichier *sesame.cfg*, changement de la variable d'environnement, installation et démarrage des services TIL.
3. Renseignez les champs détaillés dans les tableaux ci-après, puis cliquez sur Suivant.

Tableau 2.6. Paramètres de configuration du client MICROSESAME

Section Commun	Action
Répertoire du fichier SESAME.CFG	Saisissez le chemin vers le répertoire de configuration souhaité, dans lequel sera défini le fichier de configuration "sesame.cfg". Il est conseillé de nommer ce dossier **config** et qu'il soit créé dans le répertoire d'installation de MICROSESAME. Il est possible de cliquer sur le bouton "..." pour s'aider à définir le chemin. Exemple de saisie : C:/MICROSESAME/config. Si le dossier **config** n'a pa été préalablement créé, il le sera automatiquement par l'assistant de configuration.
Nom DNS IP	Il s'agit du nom du serveur MICROSESAME. Si le nom du serveur ne s'affiche pas automatiquement, cliquez sur le bouton **Sélectionner**. L'adresse IP peut être utilisée à la place du nom de la machine.
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	Non (sauf cybersécurité ANSSI). La clé API interne permet aux applications MICROSESAME de s'interfacer entre elles par l'intermédiaire de l'API REST. L'utilisation de cette clé est soumise à l'authentification de l'opérateur, mais reste un élément sensible qu'il ne faut pas divulguer. Une application pourrait utiliser cette clé pour tenter de s'interfacer avec le système installé. Si la clé API est modifiée sur le poste serveur, vous devez la modifier sur les postes clients, pour qu'ils puissent continuer de s'interfacer avec le serveur MICROSESAME. Avant toute modification de la clé API, contactez le DSSI. Générer une clé unique permet de renforcer la sécurité du système. Regénérer la clé API interne permet de

Section Commun	Action
	stopper tout interfaçage avec le serveur en cas d'attaque.
Utiliser la configuration Windows pour le proxy réseau	Laissez activé par défaut, sauf si l'accès au serveur utilise un proxy spécifique sur le réseau du site.
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, contactez le support HIRSCH .
Pilote spécifique	Pilote SQL TIL. Sélectionnez éventuellement le pilote requis dans la liste déroulante, en fonction de la version de SQL Server installée. Consultez le tableau *Tableau 2.2, « Tableau des informations d'installation de MICROSESAME »*.
Type d'authentification	Laissez Standard par défaut, dans le cas d'une authentification avec un utilisateur SQL. Dans le cas d'une authentification au serveur SQL, avec l'utilisateur de session Windows de la session en cours, choisissez WINDOWS.
Section Services	**Action**
Services sélectionnés	Master Agent.
Compte de service pour le Master Agent	Laissez vide, pour utiliser le compte " Système Local".
Mot de passe du compte pour le Master Agent	Laissez vide, pour utiliser le compte " Système Local".
Confirmation	Laissez vide.

4. La fenêtre **Actions en cours** s'affiche et permet de suivre l'avancement de la configuration.



2.3.3. Activer les échanges TLS entre le serveur et les postes clients

Dans le cadre d'un installation sécurisée, vous devez activer les échanges TLS entre le serveur et les clients, ainsi que la vérification des certificats.

1. Sur le **poste client**, ajoutez le certificat associé à ce poste (renommé *certificate.p12*) dans le dossier **C:/MICROSESAME/config>/certificate**.
2. Depuis le menu principal du poste serveur, suivez **Paramétrage > Matériel > Poste client**.
3. Cliquez sur l'onglet **Certificats**.
4. Cliquez dans le champ **certificat** et sélectionnez le certificat désiré.
5. Cliquez sur le commutateur **Activer la sécurisation TLS entre les clients et le serveur** (il passe au vert).
6. Cliquez sur le commutateur **Activer la vérification des certificats clients** (il passe au vert).
7. Activez l'automate, enregistrez la configuration et appliquez les changements.
8. Ajoutez un certificat signé par une autorité de confiance sur le **poste serveur**, à l'emplacement **C:/MICROSESAME/config>/certificate**.

2.3.4. Déclarer un poste client - vérifier le paramétrage du poste client

Après l'installation de MICROSESAME sur le poste client, vérifiez son paramétrage depuis le poste serveur.

Il n'est pas obligatoire de déclarer le poste client pour que ce dernier puisse se connecter au serveur. Cette opération de déclaration du poste client permet de le fermer ou de le bloquer à partir du poste serveur.

1. Depuis le menu principal de MICROSESAME du poste serveur, suivez **Paramétrage > Matériel > Poste client [POS]**.
2. Dans le fenêtre de paramétrage général, cliquez sur l'onglet **Liste des poste client**.

La liste affiche les différents postes clients trouvés (par défaut, la liste est vide si aucun poste client n'a été déclaré) . Vous pouvez effectuer une recherche rapide dans cette liste de postes clients.

3. Pour déclarer un nouveau poste client, cliquez sur l'icône "+" (**Créer un poste**).
4. Indiquez le nom et l'adresse IP du poste client à déclarer et enregistrez les modifications. Vous pouvez ajouter une description.

2.4. Comprendre la différence entre mise à jour et migration

Il est possible de faire évoluer MICROSESAME de deux façons bien distinctes : effectuer une simple **mise à jour** ou réaliser une **migration**.

Ces deux opérations ne doivent pas être confondues, car leur mise en œuvre implique des actions différentes.

2.4.1. Qu'est-ce qu'une mise à jour ?

La mise à jour est une **évolution mineure de la version** de MICROSESAME et ne **s'applique qu'à une version spécifique**, on parle alors de "patch".

Les caractéristiques de la mise à jour sont :

- Les programmes sont modifiés : évolutions mineures, mise à jour pour compatibilité avec les UTL, correction de bugs...
- La structure de la base de données reste inchangée.
- La licence est conservée.

Exemple : mon système est en version 2021.5.7.

1. J'ouvre le site du support HIRSCH et je télécharge le fichier de mise à jour nommé **MICROSESAME_REPOSITORY_FULL_2021.5.11.36488.prod.7z**
2. J'applique ce patch et après cette opération, mon système est en **version 2021.5.11**.

Je n'ai pas changé de version, mon système est resté en version 2021.5.

2.4.2. En quoi consiste la migration ?

Une migration est une **évolution majeure** de MICROSESAME qui se solde par un **changement de version**.

Les caractéristiques principales de la migration sont :

- Les programmes sont modifiés : évolutions majeures, implémentations de nouvelles fonctionnalités, compatibilités avec de nouveaux protocoles ou avec de nouveaux matériels.
- La structure de la base de données est modifiée : création de nouvelles tables, créations de nouveaux liens, etc.
- La licence est impactée et elle doit être renouvelée, puisque la version change.

Exemple : mon système est en **version 2021.5.11** et je souhaite bénéficier de nouvelles fonctionnalités présentes dans la version 2023.2.

1. J'ouvre le site du support HIRSCH et je télécharge le fichier nommé **MSesameInstallerServer_2023.2.3.36749.prod.exe**

2. J'installe cette nouvelle version sur le poste serveur, puis avec l'outil de maintenance, je lance une migration sur ma base de données **MS2021.5**.
   Lorsque la migration est achevée, mon système est désormais en **version 2023.2.**
3. J'installe la nouvelle licence que j'ai obtenue de TIL, puis j'effectue le changement de version sur chaque poste client, en utilisant l'outil de maintenance.
   La migration a fait passer mon système de la version 2021.5 à la version 2023.2.

J'ai changé de version.

2.4.3. Comment savoir si une mise à jour ou une migration est nécessaire ?

La version du logiciel MICROSESAME se présente sous la forme 202A.V.P.bbbbb, pour laquelle :

- **A** : correspond à l'**année de sortie**. Exemple : la version 202**1**.
- **V** : correspond à la **version majeure**. Exemple : la version 2021.**4** est une version et 2021.**5** en est une autre.
- **P** : correspond à la **mise à jour**, encore appelé "Patch". Exemple : les patch 2021.5.**3** et 2021.5.**7** sont des mises à jour de la version 2021.5.
  - **bbbbb** : correspond au "numéro de build". Ces chiffres ne servent qu'à distinguer une version de développement par rapport à une autre, dans une même version de MICROSESAME. Exemple : 2021.5.7.**29315** et 2021.5.7.**29587** sont des builds de la mise à jour 2021.5.7.

Pour savoir si une migration ou une simple mise à jour est à envisager, comparer la version envisagée avec la version en cours :

Si la version à mettre en place possède une année et une version majeure identiques à celles de la version en cours, il s'agit d'une simple **mise à jour**.

Exemple : la version actuelle est la 2021.5.3 : tous les patches commençant par 2021.5 permettent la mise à jour de cette version. Le nom du fichier à télécharger doit alors comporter le terme **REPOSITORY**.

Si la version majeure et/ou l'année est différente de celle de la version en cours, il est nécessaire d'effectuer une **migration**.

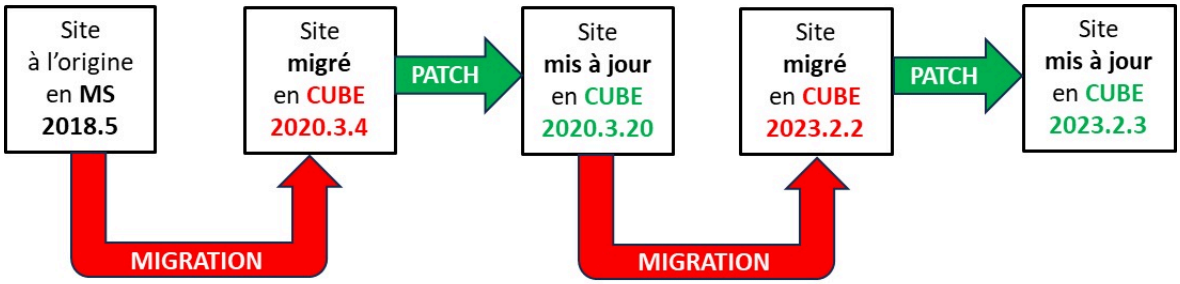
Exemple : la version en cours est la 2021.4.3 et je dois la faire évoluer en 2021.5.1. Comme la version majeure est différente, il faut installer cette nouvelle version, puis effectuer une migration. Le nom du fichier à télécharger doit comporter le terme **InstallerServer**.

La situation est identique pour passer d'une version 2021.4.3 à une version 2023.1.1 : l'année étant différente, une migration est nécessaire.

Une migration peut nécessiter le renouvellement de la licence MICROSESAME. En effet, si la l'**année de version** change lors de la migration (par exemple, migration de MICROSESAME 2021 en MICROSESAME 2023), alors la licence ne sera plus valide.

Avant d'entreprendre une migration, prendre contact avec le service commercial HIRSCH, afin de connaître les modalités d'obtention d'une nouvelle licence.

Figure 2.2. Exemple de la vie d'un site : de MS 2018.5 à MS 2023.2



2.5. Migrer un poste serveur

2.5.1. Rôle d'un serveur de validation lors des opérations de migration

La migration consiste à faire évoluer **la version** de MICROSESAME.

La société HIRSCH préconise de faire une migration sur un **serveur de validation** , dans le but de relever et de prévenir d'éventuelles anomalies qui n'impacteront pas le serveur de production.

Ce **serveur de test** doit être une copie du serveur MICROSESAME de production.

Résumé des actions à entreprendre pour assurer la migration du serveur de production à partir d'un serveur de validation :

1. Sur le **serveur de production** effectuer une sauvegarde (voir *Section 2.7.1, « Sauvegarder la base de données d'un poste serveur »*).
2. Sur le **serveur de validation** effectuer l'installation de la même version de MICROSESAME que celle présente sur le serveur de production.
3. Copier la sauvegarde effectuée, sur le serveur de validation.
4. Effectuer une restauration de cette sauvegarde (voir *Section 2.7.3, « Restaurer un poste serveur »*).
5. Vérifier que la sauvegarde s'est effectuée correctement, en ouvrant une session (présence des données dans MICROSESAME).
6. Procéder à la migration du serveur de validation, en utilisant la sauvegarde (voir *Section 2.5.2, « Migrer un serveur de validation »*).
7. Vérifier le fonctionnement de la nouvelle version de MICROSESAME après migration.
8. Effectuer une sauvegarde sur le serveur de validation.
9. Sur le **serveur de production** effectuer l'installation de la nouvelle version de MICROSESAME, en migrant la sauvegarde du serveur de validation (étape inverse de l'étape 6).
10. Vérifier le fonctionnement de la nouvelle version de MICROSESAME après migration.
11. Les deux versions de MICROSESAME sont maintenant présentes sur le serveur de production : version initiale et version migrée.

2.5.2. Migrer un serveur de validation

Afin de pouvoir réaliser la migration d'un serveur MICROSESAME, le composant **Migration serveur** doit avoir été installé (voir *Section 2.5.2.1, « Vérifier la présence du composant Migration serveur »*).

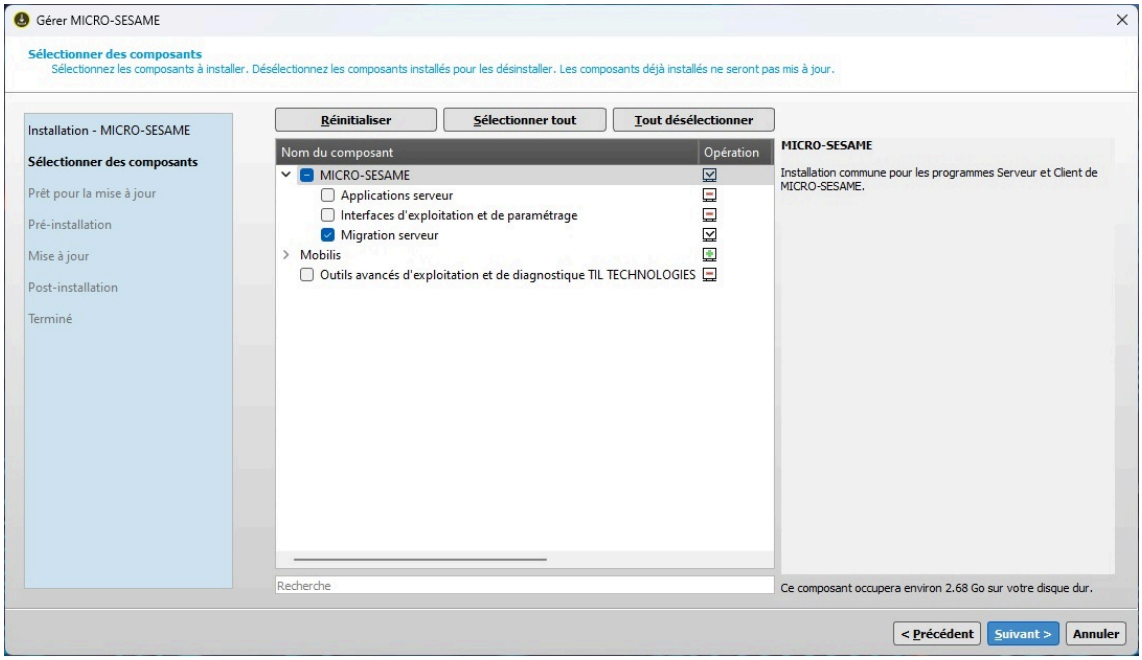
La procédure de migration en elle-même suppose que les étapes suivantes ont été effectuées sur le serveur de validation :

- Installer la même version de MICROSESAME que celle présente sur le serveur de production.
- Restaurer la sauvegarde issue du serveur de production.
- Vérifier le bon fonctionnement de MICROSESAME après restauration.

Lancer la migration (voir *Section 2.5.2.2, « Lancer la migration d'un serveur de validation »*).

2.5.2.1. Vérifier la présence du composant Migration serveur

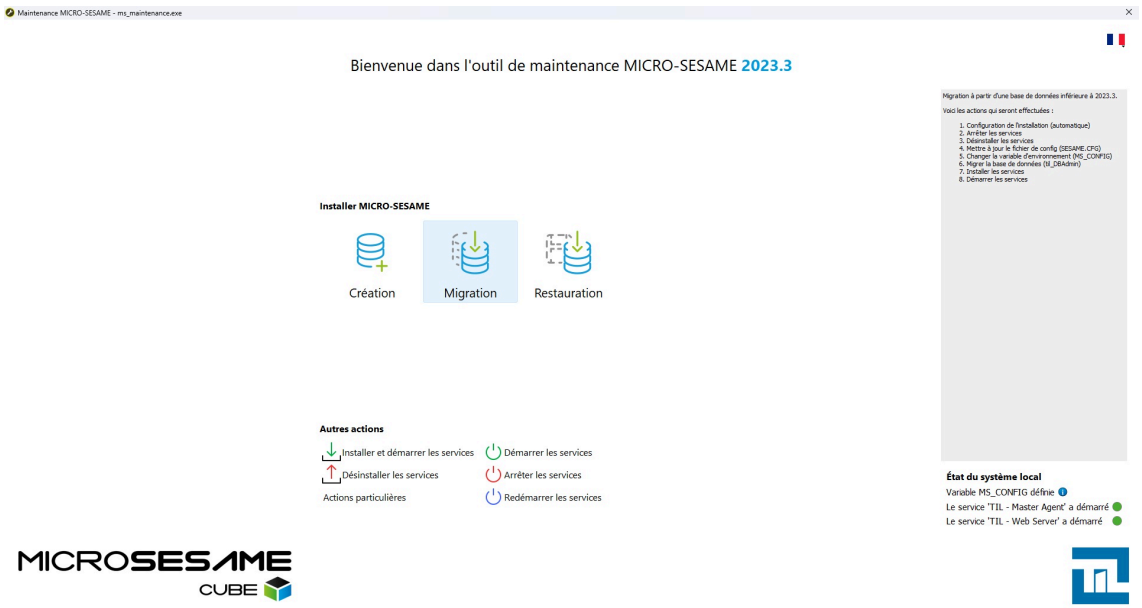
1. Faites un clic droit sur le raccourci créé sur le bureau nommé **Mettre à jour MICROSESAME** (ou**Update MICROSESAME**) , puis sélectionnez **Exécuter en mode Administrateur**.
2. Sélectionnez **Ajouter ou supprimer des modules**, puis cliquez sur **Suivant** .



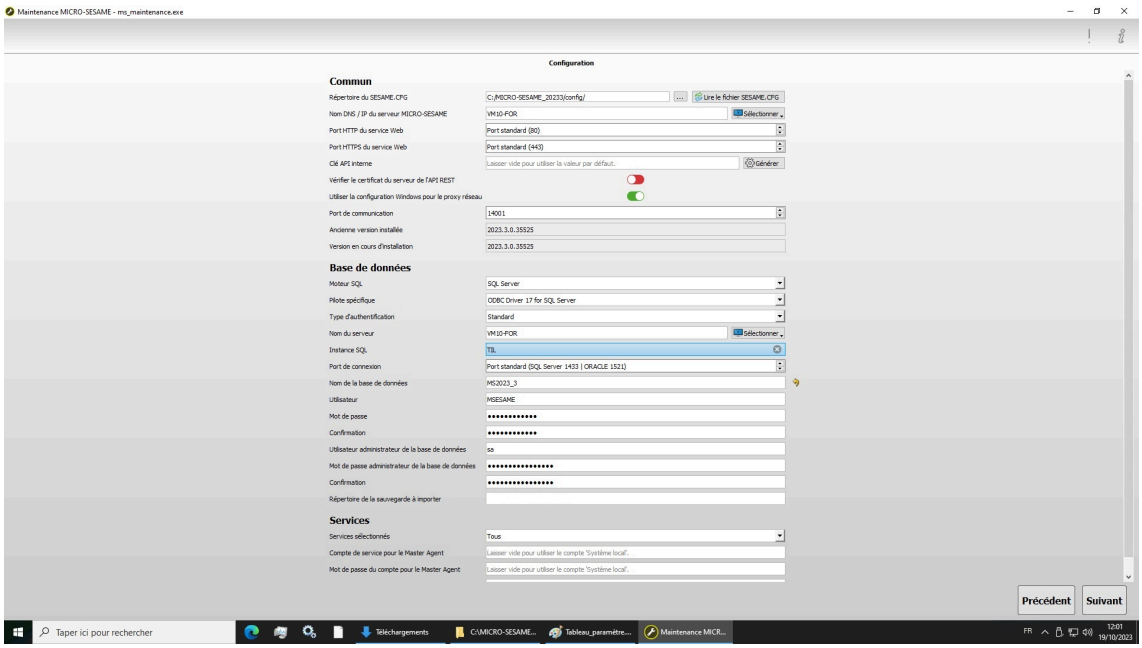
3. Si le composant est installé, sa version est mentionnée. Sinon cochez la case du composant **Migration serveur**, puis cliquez sur Suivant pour finaliser la procédure.

2.5.2.2. Lancer la migration d'un serveur de validation

1. Procédez à l'installation de la nouvelle version de MICROSESAME (consultez le chapitre 1.2), **en modifiant le nom du répertoire d'installation proposé par défaut** (étape 4).
   Cela permettra d'installer la nouvelle version dans un répertoire différent de celui de la version en cours.
   Exemple de répertoire d'installation : **C:/MICROSESAME_xxx**, où xxx correspond à la nouvelle version de MICROSESAME.
2. Lorsque la fenêtre **Outil de maintenance de l'installation MICROSESAME(ms_maintenance.exe)** s'affiche, cliquez sur le bouton **Migration** .



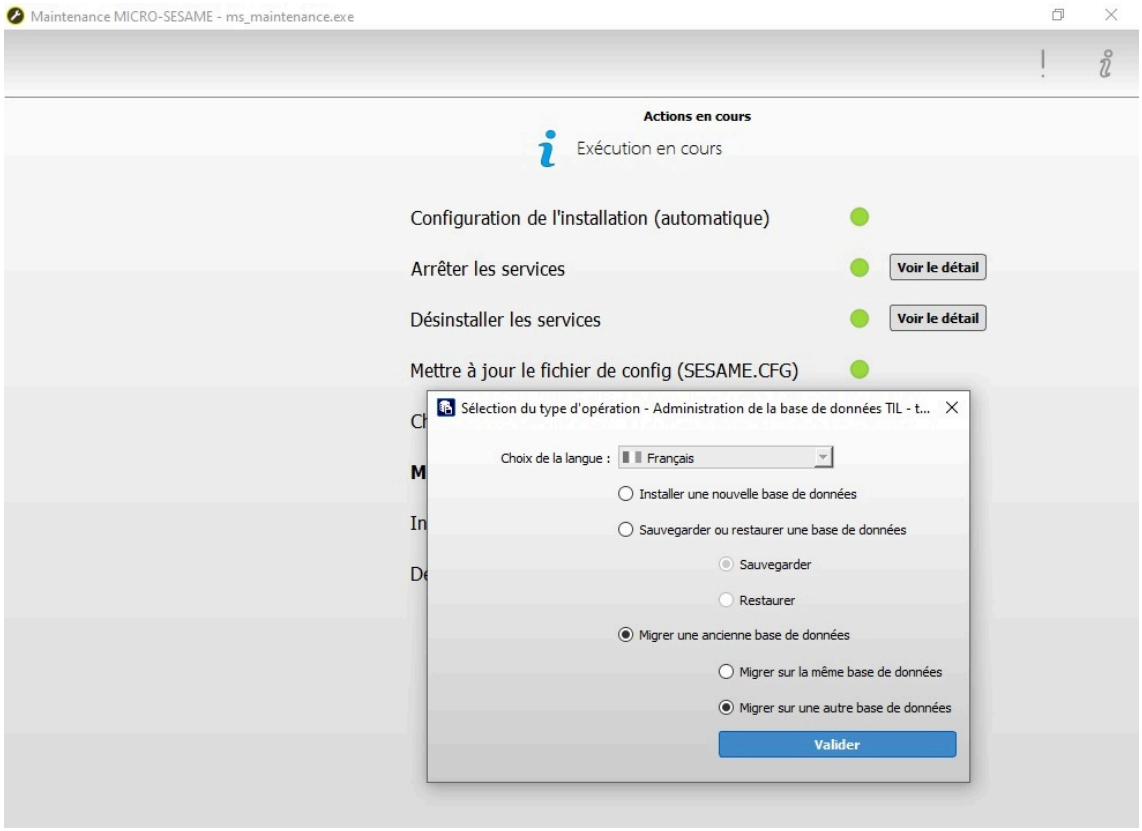
3. L'écran des paramètres de configuration s'affiche.



Respectez le paramétrage des deux paramètres qui suivent.

- Dans **Commun > Répertoire du SESAME.CFG**, indiquez le chemin vers le répertoire **config** , à définir dans le **dossier de la nouvelle installation**.
  Par exemple : **C:/MICROSESAME_xxx/config_xxx**, où xxx peut correspondre à la nouvelle version de MS.
- Dans **Base de données > Nom de la base de données**, saisissez obligatoirement un nom **différent** de la base de données déjà existante.
  Par exemple **MSESAME_xxx**, où xxx peut correspondre à la nouvelle version de MS.

4. Cliquez sur **Suivant**. La fenêtre des **Actions en cours** s'affiche et l'outil **Administration de la base de données** (**til_DBAdmin.exe**) est exécuté.



5. Sélectionnez **Migrer sur une autre base de données** puis cliquer sur le bouton **Valider**.
6. Cliquez sur le bouton 1 - Paramètres de connexion.
7. Cliquez sur le bouton **Créer/Modifier** pour éditer les paramètres de connexion à la base de données, puis renseignez les champs comme indiqué dans le tableau situé sous la capture d'écran.

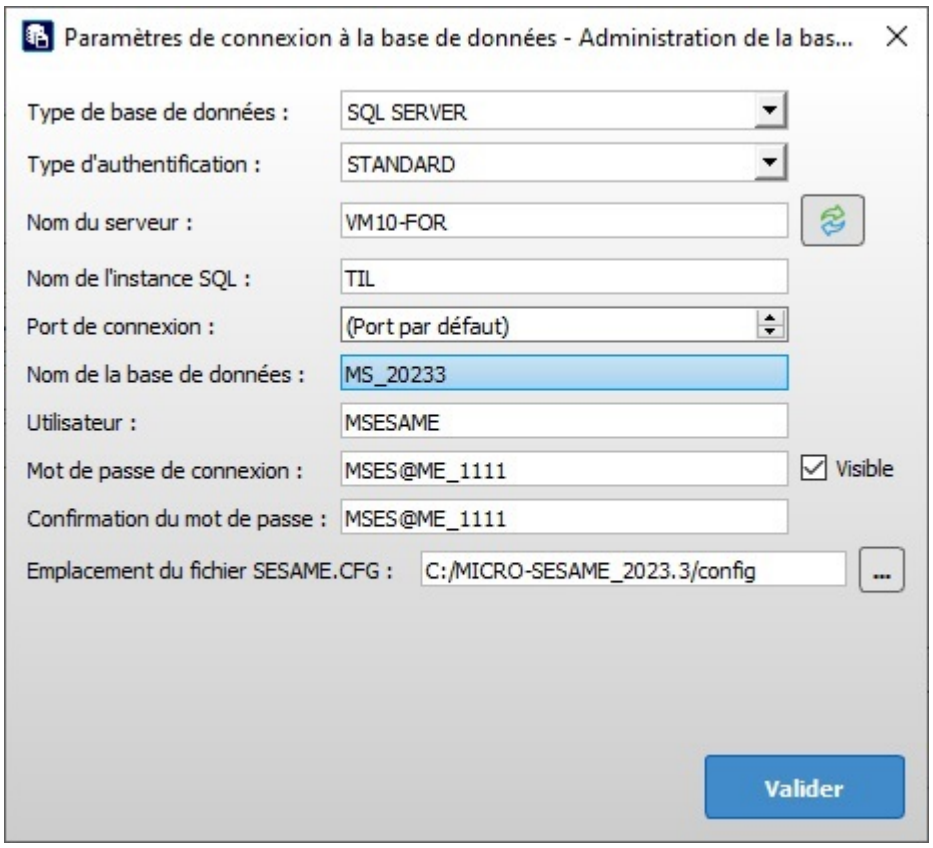


Tableau 2.7. Paramètres de connexion à la base de données

Champ	Valeur
Type de base de données	SQL Server, par défaut. Modifiez éventuellement, dans le cas d'utilisation d'un moteur Oracle.
Type d'authentification	Laissez Standard.
Nom du serveur	Nom du serveur contenant la base de données. Le nom par défaut correspond au nom du serveur MICROSESAME. Vérifiez l'exactitude du nom ou de l'adresse IP proposée. Si le nom n'apparaît pas, cliquez sur l'icône afin de renseigner le nom du serveur automatiquement. Saisissez éventuellement le nom d'un SQL externe.
Instance SQL	Dans le cas où le moteur de la base de données a été installé avec l'application fournie par HIRSCH "MS_SQL_2019_express_TIL_FRA.exe" (ou

Champ	Valeur
	MS_SQL_2019_express_TIL_ENU.exe), laissez l'instance HIRSCH . Dans le cas où le moteur de base de données pour le fonctionnement de MICROSESAME a été installé à partir d'une autre application que celle proposée par HIRSCH ou si le moteur SQL est installé sur un serveur externe, indiquez le nom de l'instance utilisée. Si aucune instance particulière n'a été paramétrée lors de l'installation du moteur de la base donnée, effacez " HIRSCH" et laissez ce champ vide.
Port de connexion	Laissez la valeur par défaut.
Nom de la base de données	Renseigné automatiquement avec le nom défini lors de l'étape de configuration. Vous pouvez le modifier, si nécessaire.
Utilisateur	MSESAME
Mot de passe de connexion	Saisissez le mot de passe pour la connexion à la base de données (il s'agit du mot de passe déjà demandé durant l'étape de configuration). Cocher la case **Visible**, puis saisissez le mot de passe (celui proposé par TIL est *MSES@ME_1111*). Il est recommandé de modifier ce mot de passe. Cette action peut cependant être réalisée à tout moment après l'installation, en utilisant un outil TIL.
Confirmation	Confirmez le mot de passe saisi dans le champ précédent.
Emplacement du fichier SESAME.CFG	Vérifiez l'exactitude du chemin indiqué.

Pour plus d'information sur les paramètres SQL Server, consultez *Prérequis d'installation de MICROSESAME*.

8. Cliquez sur Valider, puis, à l'affichage du message d'avertissement, cliquez sur Oui.
9. Cliquez sur le bouton 2 - Paramètres des répertoires (SQL Server), puis renseignez les champs comme indiqué dans le tableau situé sous la capture d'écran.

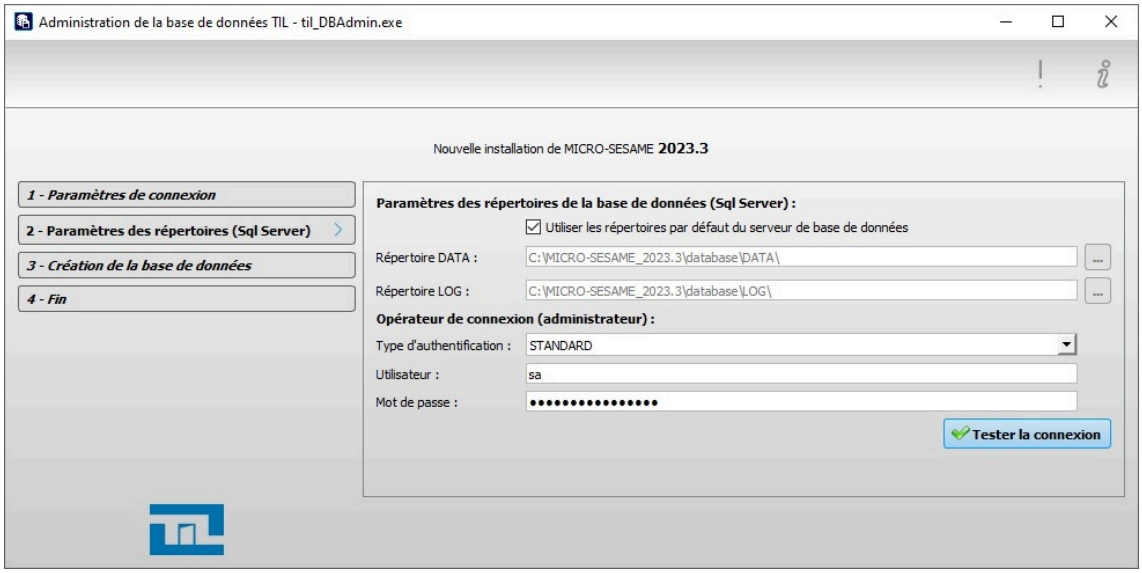


Tableau 2.8. Paramètres des répertoires (SQL Server)

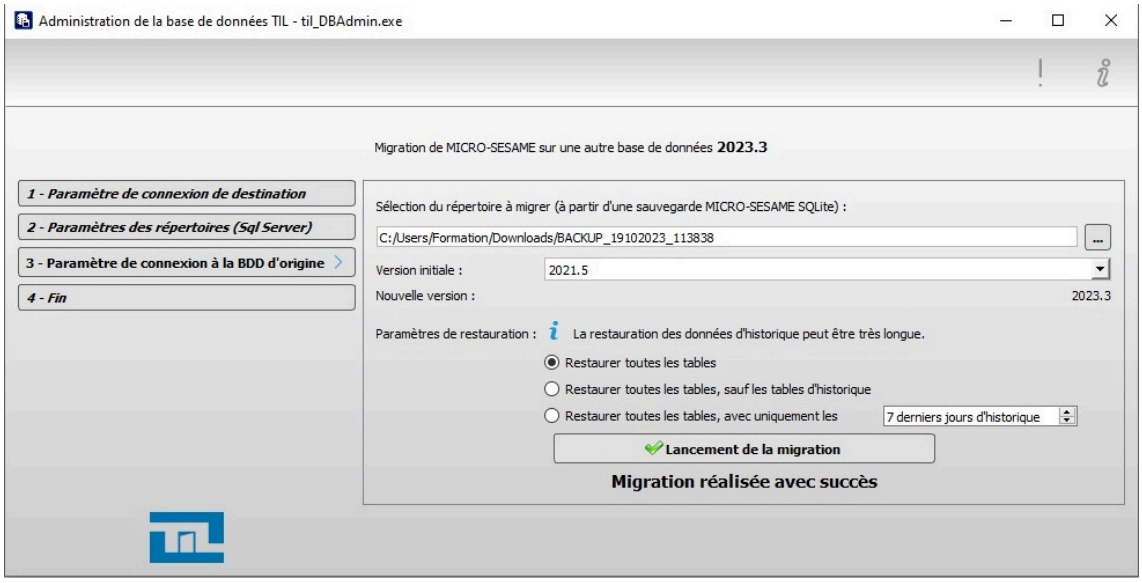
Champ	Valeur
Paramètres des répertoires de la base de données	Dans le cas d'une installation du moteur SQL avec l'application proposée par HIRSCH, cochez la case **Utiliser les répertoires par défaut du serveur**. Dans le cas d'une installation du moteur SQL depuis une autre application, cliquez sur les boutons "...", puis indiquez le chemin d'accès aux répertoires DATA et LOG, créés lors de l'installation SQL.
Type d'authentification	Laissez STANDARD par défaut. Dans le cas d'une authentification au serveur SQL, par l'utilisateur qui a ouvert la session WINDOWS en cours, sélectionnez WINDOWS.
Utilisateur	"sa" (system adminstrator) par défaut.
Mot de passe	"TIL-technologies" par défaut (si installation standard HIRSCH).

10. Pour vérifier que la connexion avec la base de données peut s'établir, cliquez sur le bouton **Test connexion**. Une coche verte sur le bouton signifie que la connexion s'est effectuée avec succès.
11. Cliquez sur le bouton 3 - Paramètre de connexion à la BDD d'origine, puis renseignez les champs comme indiqué dans le tableau ci-après.

Tableau 2.9. Paramètres de connexion à la base de données d'origine

Champ	Valeur
Sélection du répertoire à migrer	Cliquez sur le bouton "..." et sélectionnez le **répertoire de la sauvegarde** issue du serveur de production.
Version initiale	Affichage automatique de la version initiale.
Nouvelle version	Affichage automatique de la nouvelle version.
Restaurer toutes les tables	Option proposée par défaut. Vous pouvez supprimer les tables d'historiques ou les limiter à une durée paramétrable (en jours), pour éviter que la migration prenne trop de temps. A cette étape, il peut être nécessaire de consulter le client, pour savoir s'il est nécessaire de conserver tous les historiques du site. Plusieurs cas : • La migration effectuée ne sert qu'à effectuer un test : il est possible de supprimer les tables d'historique, afin que la migration s'effectue au plus vite. • La migration effectuée sera reportée directement sur le serveur de production : le client devra alors indiquer s'il souhaite conserver tout ou partie des historiques. Le choix devra être fait entre conserver des historiques indispensables et réduire le temps de migration. Les historiques occupant une très grande partie de la base de données, la migartion prendra d'autant plus de temps que la durée des historiques paramétrée est importante.

12. Cliquez sur le bouton Lancement de la migration.



13. Dans la boîte de dialogue qui s'ouvre, cliquez sur le bouton Tout écraser : la migration débute.
14. A la fin de la migration, dans la boîte de dialogue qui s'affiche, vérifiez l'adresse IP figurant dans le champ **Adresse IP vue par le matériel**. Si l'adresse est correcte, cliquez sur le bouton Valider. Sinon, cliquer dans le champ et sélectionner l'adresse dans la liste déroulante, puis cliquez sur Valider.
15. La migration est terminée.
16. Dans la fenêtre des **Actions en cours**, vous pouvez constater que les services TIL sont installés et démarrés.
17. Cliquez sur Quitter.

2.5.3. Mettre en service un serveur de validation après une migration

Après une migration, vous devez effectuer les actions suivantes au premier lancement de MICROSESAME :

1. Ouvrez une session MICROSESAME et, depuis le menu principal, suivez **Paramétrage > Mise en exploitation > Appliquer le paramétrage [APP]**.
2. Dans le bandeau supérieur, sélectionnez le mode **Simple**.
3. Dans l'onglet **Compiler le paramétrage**, cliquez sur **Tout compiler**.
4. Sélectionnez l'onglet **Appliquer les changements**, puis :
   - Dans la liste déroulante, sélectionnez **Appliquer les changements sur les propriétés**et cliquez sur le bouton Exécuter.
   - Dans la liste déroulante, sélectionnez **Appliquer les changements sur les lignes** et cliquez sur le bouton Exécuter.
   - Dans la liste déroulante, sélectionnez **Appliquer les changements sur les plages horaires**et cliquez sur le bouton Exécuter.
5. Vérifiez l'ensemble du fonctionnement.
6. Lorsque tout est opérationnel, procédez à une sauvegarde du serveur de validation (consultez *Section 2.7.1, « Sauvegarder la base de données d'un poste serveur »*).

2.5.4. Migrer un serveur de production

Procédure pour restituer la migration effectuée sur le serveur de validation :

1. Copiez la sauvegarde du serveur de validation qui vient d'être faite.
2. Procédez à la migration comme mentionné au **chapitre 5.2**, avec la différence suivante :
   "Cliquez sur le bouton 3 - Paramètre de connexion à la BDD d'origine :
   Dans le champ **Sélection du répertoire à migrer**, cliquer sur le bouton ... et sélectionner le **répertoire de la sauvegarde** issue du **serveur de validation**".
3. Procédez au premier démarrage du serveur de production (consultez *Section 2.7.4, « Mettre un serveur en service après une restauration »*).
4. Vérifiez le bon fonctionnement du serveur.

En utilisant l'outil **MS Starter**, vous pouvez définir les deux environnements présents sur le serveur. Ceci permet d'utiliser l'ancienne et la nouvelle version de MICROSESAME.

Pour démarrer l'un de ces environnements, faites un clic droit sur une ligne choisie, puis choisissez **Installer et démarrer un service > Tous les services**.

MS Starter modifie la variable d'environnement en conséquence.

2.5.5. Migrer des postes clients ?

Il n'existe pas de notion de migration pour les postes clients, qui ne font que permettre un accès à distance au serveur MICROSESAME.

Une fois le serveur migré, il suffit d'installer la nouvelle version client de MICROSESAME sur chaque poste client (consulter *Section 2.3, « Mettre en place un poste client MICROSESAME »*).

2.6. Installer une mise à jour (patch)

La mise à jour concerne une **version spécifique** de MICROSESAME, par exemple la version **2023.2**. Elle consiste à installer un simple patch et ne nécessite aucun changement dans la base de données. Il n'est pas nécessaire de respecter des "paliers" pour la mise à jour.

Exemple : la version en cours de MICROSESAME est **2023.2.1**.Il est possible d'installer directement la mise à jour **2023.2.3**, sans avoir préalablement installé le patch 2023.2.2.

Avant d'appliquer une mise à jour :

- Vérifiez que **tous les services sont arrêtés** (Master Agent et Web Server) et que **toutes les applications de MICROSESAME sont fermées**, sur le poste serveur et sur tous les postes clients.
- Réalisez une **sauvegarde** des programmes de MICROSESAME : copiez pour cela le dossier PROG (l'emplacement proposé par défaut à l'installation est C:\MSESAME \PROG).

Récupérer le fichier contenant la mise à jour :

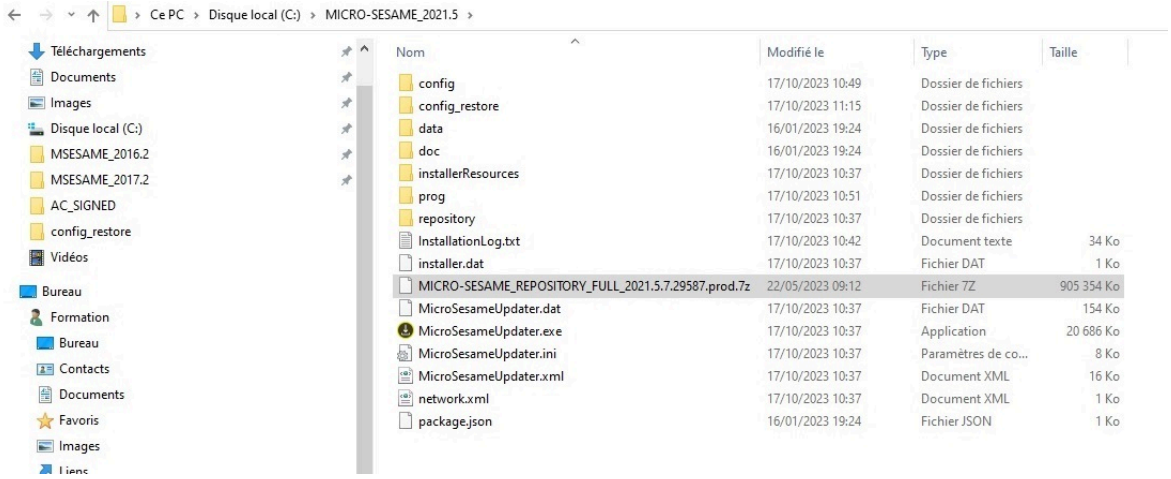
1. Ouvrez le *site du support de HIRSCH* dans un navigateur et connectez-vous.

2. Suivez **Téléchargements > MICROSESAME> Téléchargements**, puis cliquez sur le fichier **MICROSESAME_REPOSITORY_FULL_2023.V.x.xxxxx.prod.7z** (où V est la version de MICROSESAME installée).
3. Pour installer un patch MICROSESAME pour les versions à partir de la MS 2018.2, continuez avec *Section 2.6.1, « Installer une mise à jour MICROSESAME sur un poste serveur »* et *Section 2.6.2, « Installer une mise à jour MICROSESAME sur un poste client »*.
   Pour les versions antérieures, consultez *Mise à jour et migration MICROSESAME avant 2018.2*.

2.6.1. Installer une mise à jour MICROSESAME sur un poste serveur

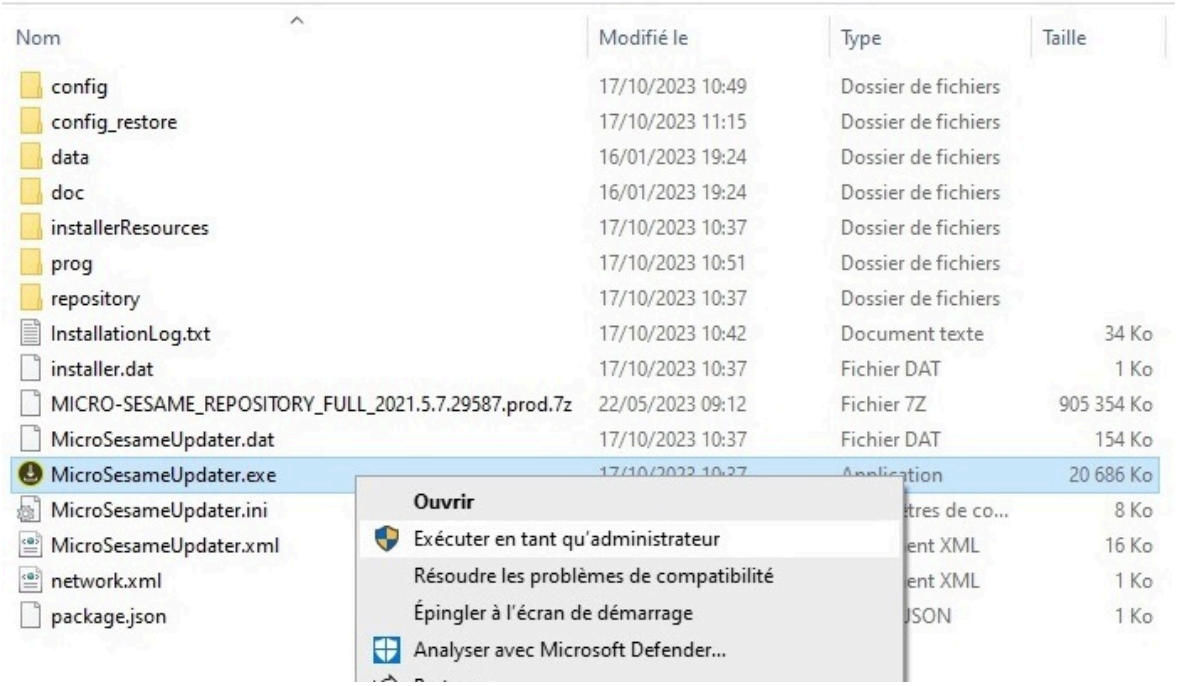
Pour toute autre version, une autre procédure doit être appliquée (voir la documentation dédiée "Documentation d'application des patchs à partir de MS 2016.1.x").

Placez le fichier zippé (.7z) contenant la mise à jour directement dans le répertoire contenant les différents sous répertoires et fichiers MICROSESAME (par défaut C:/ MICROSESAME) :



Il n'est pas nécessaire d'extraire les contenus du fichier zippé pour procéder à la mise à jour.

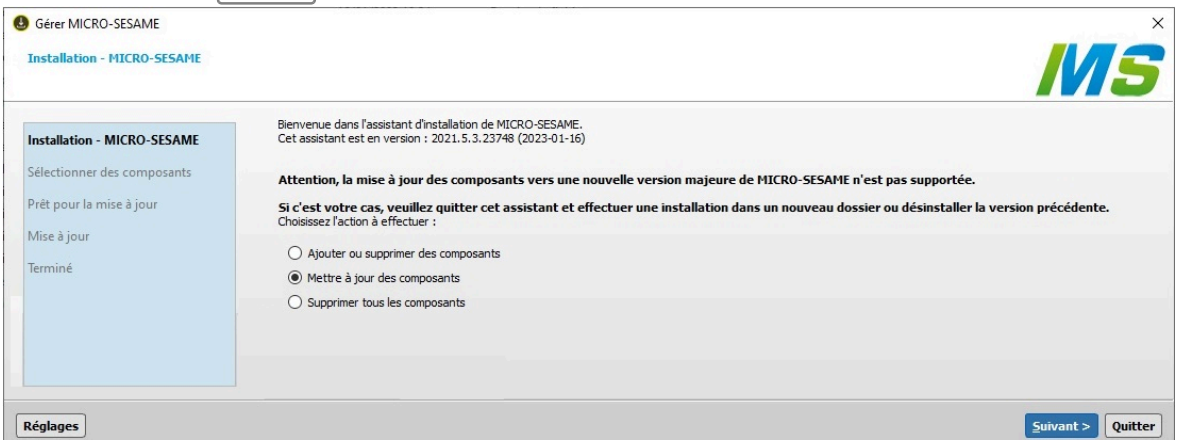
Lancez **MicroSesameUpdater** en tant qu'administrateur, puis cliquez sur OK dans la boîte de dialogue.



A l'apparition de la boîte de dialogue, cliquez sur OK : l'assistant d'installation de MICROSESAME s'ouvre.

Le déroulement des actions est indiqué dans la colonne de gauche.

Installation - MICROSESAME : sélectionner l'option **Mettre à jour des composants**, puis cliquez sur Suivant.



Sélectionner des composants : permet de consulter et modifier la liste de composants qui seront mis à jour. Cliquez sur Suivant pour continuer.

Prêt pour la mise à jour : confirmation de la mise à jour et notification de l'espace disque nécessaire. Cliquez sur Mettre à jour pour continuer.

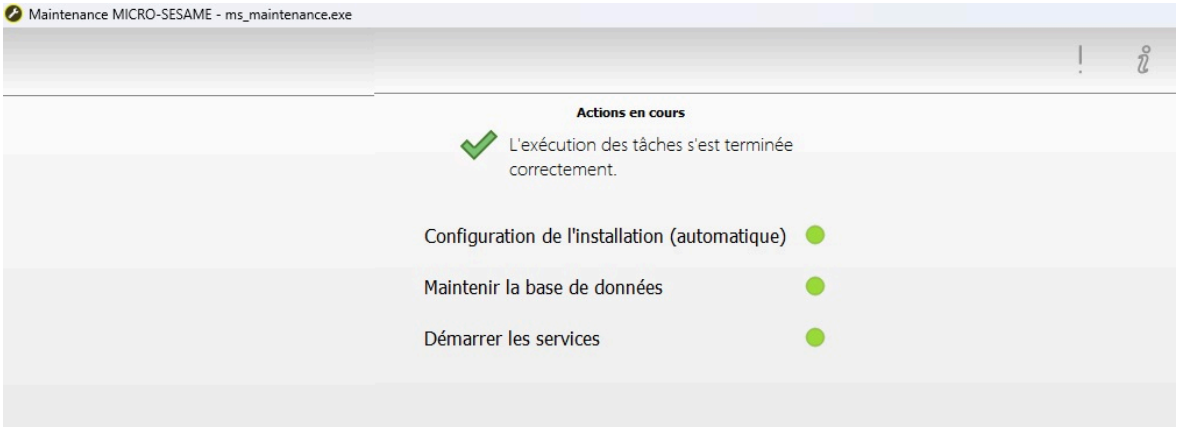
Pré-installation : arrêt des services et fermetures des programmes. Cliquez sur sur Suivant pour continuer.

Mise à jour : plusieurs notifications peuvent s'afficher pendant le déploiement du patch. Un bouton Afficher les détails permet de visualiser l'avancement de la mise à jour.

Au message mentionnant que le déploiement du patch est terminé, cliquez sur Suivant pour continuer.

L'application **Maintenance MICROSESAME** se lance automatiquement, afin de redémarrer les services.

L'état final doit afficher trois voyants verts.



Cliquez sur Quitter : la mise à jour est terminée.

Ouvrez une session MICROSESAME : dans la barre supérieure de la page d'accueil, cliquez sur "**?**", puis sur **A propos** et vérifiez que la version de produit affichée correspond bien à celle du patch appliqué.

Si la version des programmes ne correspond pas à la version du patch précédemment appliqué, contactez le support technique HIRSCH.

2.6.2. Installer une mise à jour MICROSESAME sur un poste client

La mise à jour d'un poste client consiste à **mettre à jour les programmes** utilisés par le poste client, depuis le poste serveur.

La mise à jour du serveur doit obligatoirement avoir été effectuée, avant de pouvoir la faire sur un poste client. Pour le déploiement d'un patch sur le poste serveur, consultez la procédure précédente **Déploiement d'un patch sur un poste serveur**. Le lien réseau entre le poste serveur et le poste client doit fonctionner.

2.6.2.1. Mettre à jour un poste client avec le référentiel serveur

Pour mettre à jour un poste client avec les données définies par l'utilisateur :

1. Faites un clic droit sur l'icône **Mettre à jour MICROSESAME** présente sur le bureau, puis choisissez **Exécuter en tant qu'Administrateur**.
2. À l'apparition de la boîte de dialogue, cliquez sur OK : l'assistant d'installation de MICROSESAME s'ouvre.
   Le déroulement des étapes à suivre est indiqué dans la colonne de gauche.

3. **Installation - MICROSESAME** : cliquez sur le bouton Réglages, en bas à gauche de l'écran.
   Dans l'onglet **Réseau**: renseignez éventuellement le proxy, si besoin.
   Dans l'onglet **Référentiels**, à la rubrique *Référentiel défini par l'utilisateur*, sur les deux lignes http:// **update** et **repository** , vérifiez la présence de l'adresse IP ou du nom du serveur, puis cliquez sur OK.
4. Dans la fenêtre d'installation, sélectionnez **Mettre à jour des composants**, puis cliquer sur Suivant.
5. **Sélectionner des composants** : permet de consulter et modifier la liste de composants qui seront mis à jour. Cliquez sur Suivant pour continuer.
6. **Prêt pour la mise à jour** : confirmation de la mise à jour et notification de l'espace disque nécessaire. Cliquez sur Mettre à jour pour continuer.
7. **Pré-installation** : arrêt des services et fermetures des programmes. Cliquez sur Suivant pour continuer.
8. **Mise à jour** : plusieurs notifications peuvent s'afficher pendant le déploiement du patch. Un bouton Afficher les détails permet de visualiser l'avancement de la mise à jour.
9. Au message indiquant que le déploiement du patch est terminé, cliquez sur Suivant pour continuer.
10. L'état final doit afficher deux voyants verts sur les rubriques **Configuration de l'installation** et **Démarrer les services**. Cliquez sur Quitter pour fermer.
11. Ouvrez une session MICROSESAME : dans la barre supérieure de la page d'accueil, cliquez sur "**?**", puis sur **A propos**et vérifiez que la version de produit affichée correspond bien à celle du patch appliqué.

2.7. Sauvegarder et restaurer une base de données

Il peut s'avérer nécessaire d'installer un serveur MICROSESAME à partir d'une copie de **sauvegarde**. Cette action constitue une **restauration** de cette base de données.

2.7.1. Sauvegarder la base de données d'un poste serveur

1. À partir de l'écran d'accueil de MICROSESAME, suivez **Maintenance > Sauvegarde de la base de données [SAU]**. L'outil **Administration de la base de données** (**TIL_DBAdmin.exe**) est exécuté.
2. L'onglet en cours est : **1 - Paramètres de connexion**. Cliquez sur le bouton Tester la connexion. Une coche verte doit apparaître sur le bouton, indiquant que la connexion à la base de données est valide.
3. Sélectionnez l'onglet **2 - Sauvegarde d'une base de données**. Cliquez sur le bouton ..., puis indiquer le répertoire de destination de la sauvegarde.
   Par défaut, l'option de sauvegarde **Complète** est activée et sauvegarde l'ensemble de la base de données, ainsi que le répertoire **config**.
   En sélectionnant l'une des deux options suivantes, il est possible d'effectuer une sauvegarde sans tout ou partie des tables d'historique, pour ainsi gagner du temps.
   En cochant la case adéquate, vous pouvez également exclure le répertoire "config" de la sauvegarde.
4. Cliquez sur le bouton Sauvegarder : la sauvegarde débute.
5. Lorsque la sauvegarde est terminée, une boîte de dialogue s'ouvre qui doit mentionner le succès de l'opération. Cliquez sur OK.
6. Cliquez sur l'onglet **3 - Fin** pour fermer la fenêtre.

La sauvegarde est maintenant disponible dans le dossier nommé **Backup_date_heure**.

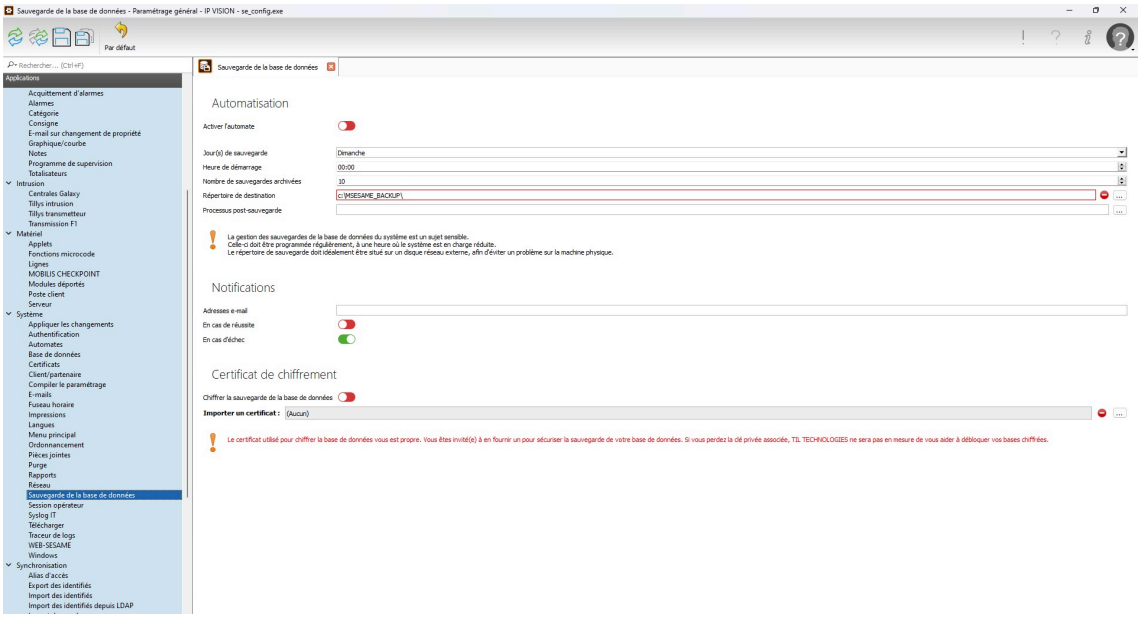
La sauvegarde ne prend pas en compte la configuration de Windows.

Vous pouvez également effectuer une sauvegarde en exécutant l'outil **TIL_DBAdmin.exe** depuis Windows. Cet outil se trouve généralement dans C:\MSESAME\prog. Sélectionnez l'option **Sauvegarde ou Restauration d'une base de données > Sauvegarde**. La procédure est ensuite identique à celle précédemment décrite.

2.7.2. Paramétrer la sauvegarde automatique

MICROSESAME permet l'automatisation de la sauvegarde de la base de données.

1. Depuis le menu principal de MICROSESAME, suivez **Paramétrage > Autres > Paramétrage général > Rubrique Système > Sauvegarde de la base de données**.
2. Paramétrez la sauvegarde avec les options souhaitées : consultez l'**Aide en ligne** de MICROSESAME.
3. Activez l'interrupteur **Activer l'automate**(il passe au vert), puis sauvegardez en cliquant sur l'icône **Disquette**.



2.7.3. Restaurer un poste serveur

La restauration de base de données, permet de :

- Restaurer une sauvegarde sur un **serveur existant**, qui présente des dysfonctionnements dans l'utilisation de MICROSESAME. Il s'agit alors d'effectuer une restauration sur la **même base de données**.
- Restaurer une sauvegarde sur un **nouveau serveur** (sur lequel SQL et MICROSESAME sont installés). Il s'agit alors d'une restauration sur une **nouvelle base de données**.
  C'est le cas lors du remplacement d'un serveur défectueux.

Seules les sauvegardes compatibles avec **la version en cours** des programmes de MICROSESAME peuvent être restaurées (même version majeure).

Par précaution, copier le dossier de la sauvegarde qui va être utilisée, dans un répertoire différent de celui qui sera choisi pour la restauration.

Procédure de restauration depuis Maintenance MICROSESAME :

1. Faites un double clic sur l'icône **Maintenance MICROSESAME**, puis dans la fenêtre de maintenance, cliquez sur la rubrique **Restauration**.
2. Dans la fenêtre des paramètres qui s'affiche, cliquez sur OK. L'outil **TIL_DBAdmin** est exécuté.
3. L'onglet en cours est 1 - Paramètres de connexion : cliquez sur le bouton Tester la connexion. Une coche verte doit apparaître sur le bouton, indiquant que la connexion à la base de données est valide.
4. Cliquer sur le bouton Créer/modifier :
   Type de base de données : SQL SERVER.
   Type d'authentification : Standard par défaut.
   Nom du serveur : si le nom n'apparaît pas, cliquer sur l'icône "double flèches".
   Nom de l'instance SQL : TIL proposé par défaut, si SQL a été installé avec l'application TIL. Dans le cas d'une installation de SQL autre, laissez vide ou indiquez le nom d'une instance, selon la paramétrage d'origine.
   Port de connexion : Port par défaut.
   Nom de la base de données : saisissez le nom de la base de données existante, pour une restauration sur la même base. Sinon, pour une restauration sur une nouvelle base de données, saisissez le nom à donner à la base.

   Dans le cas d'une restauration sur une nouvelle base de données, il est impératif que la base de données **ne soit pas existante**, pour que l'outil **TIL_DBAdmin** puisse la créer.

   Utilisateur : MSESAME par défaut.
   Mot de passe : cochez la case **Visible**, puis saisissez le mot de passe à utiliser et le confirmer.
   Emplacement du fichier SESAME.CFG : sur un serveur existant, doit mentionner normalement l'emplacement du dossier config existant. Sur un nouveau serveur, cliquez sur le bouton ..., puis indiquez l'emplacement pour la restauration du dossier **config**.
5. Au message qui s'affiche, cliquez sur Oui.
6. Cliquez sur le bouton 2 - Paramètres des répertoires (SQL Server) :
   Paramètres des répertoires de la base de données : cochez la case **Utiliser les répertoires par défaut du serveur** dans le cas d'une installation du moteur SQL avec l'application proposée par TIL. Dans le cas d'une installation du moteur SQL depuis une autre application, cliquez sur le bouton ..., puis indiquez le chemin d'accès aux répertoires DATA et LOG, créés lors de l'installation SQL.
   Type d'authentification : laissez STANDARD par défaut, dans le cas d'une authentification avec un utilisateur SQL. Sélectionnez éventuellement, WINDOWS dans le cas d'une authentification au serveur SQL, avec l'utilisateur de session Windows de la session actuelle.
   Utilisateur et mot de passe de l'administrateur de la base de données

En authentification Standard, l'utilisateur et le mot de passe par défaut de l'administrateur de la base de données sont les suivants :
Utilisateur : sa ("system administrator") par défaut.
Mot de passe : *TIL-technologies*, si SQL a été installé avec l'application proposée par TIL.
Dans le cas où le moteur SQL a été installé par le SI du site, l'un de ses représentants doit saisir le mot de passe.

7. Cliquez sur le bouton Test connexion, afin de vérifier que la connexion avec la base de données peut être établie. Une coche verte sur le bouton signifie que la connexion a été effectuée avec succès.
8. Cliquez sur le bouton 3 - Restauration d'une base de données. Cliquez sur le bouton ..., puis indiquez le dossier source de la sauvegarde.
   Par défaut, l'option de restauration **Complète** est activée, avec laquelle l'ensemble de la base de données, ainsi que le répertoire **config**, seront restaurés.
   En sélectionnant l'une des deux options suivantes, vous pouvez effectuer une restauration sans tout ou partie des tables d'historique, pour gagner du temps.
   En cochant la case correspondante, vous pouvez également exclure le répertoire "config" de la restauration.
   Vous pouvez aussi choisir de passer les éventuelles erreurs et de continuer la restauration.
   Cliquez sur Restaurer.
9. Dans la boîte de dialogue qui s'ouvre, cliquez sur **Tout écraser**, pour lancer la restauration.
10. **Paramètres du poste serveur** :
    Depuis cette boîte de dialogue, vous pouvez vérifier et mettre à jour l'adresse IP du poste serveur.
    Si le serveur est raccordé au réseau, une adresse IP est proposée. Dans le cas où le serveur possède plusieurs cartes réseau, vous pouvez choisir l'adresse IP, en la sélectionnant dans la liste déroulante. Cliquez ensuite sur Valider.
11. A l'apparition de la boîte de dialogue mentionnant que la restauration s'est réalisée avec succès, cliquez sur OK.
12. Cliquer sur le bouton 4 - Fin et fermez la fenêtre.
13. Ouvrez une session et vérifiez le bon fonctionnement du poste serveur.

2.7.4. Mettre un serveur en service après une restauration

Après une restauration, vous devez effectuer les actions suivantes, au premier lancement de MICROSESAME :

1. Depuis le menu principal, suivez **Paramétrage > Mise en Exploitation > Appliquer le paramétrage [APP]**.
2. Cliquez sur le bouton Tout compiler, situé à gauche de l'écran.
3. Cliquez sur le bouton Appliquer les changements, puis :
   - Dans la liste déroulante, sélectionnez **Appliquer les changements sur les propriétés** et cliquer sur le bouton Exécuter.
   - Dans la liste déroulante, sélectionnez **Appliquer les changements sur les lignes** et cliquer sur le bouton Exécuter.
   - Dans la liste déroulante, sélectionnez **Appliquer les changements sur les plages horaires** et cliquer sur le bouton Exécuter.

Chapitre 3. Licences MICROSESAME

3.1. Fonctionnement

MICROSESAME CUBE propose une solution évolutive sur trois niveaux de gamme : ENTRY, PRIME et HIGH SECURE.

Le niveau de sécurité est complet sur les trois gammes et conforme ANSSI, la différence entre les différentes gammes intervient sur la "maîtrise des secrets" permettant de sécuriser le système :

- ENTRY : la solution est packagée et prête à l'emploi. HIRSCH maîtrise tous les secrets, la sécurité est donc transparente pour le client.
  Cette gamme correspond aux sites voulant un système sécurisé sans avoir de contraintes ni de paramétrage à effectuer.
- PRIME : une partie des secrets est maîtrisée par HIRSCH une autre partie des secrets est maîtrisée par le client.
  Cette gamme correspond aux sites pouvant avoir des contraintes imposées par le RSSI ou voulant maîtriser le secret et la charte de leur badge RFID ou dématérialisé.
- HIGH SECURE : le client maîtrise la totalité des secrets permettant de sécuriser son système.
  Cette gamme correspond aux sites voulant le plus haut niveau de cybersécurité ou ayant l'obligation réglementaire de mettre en place une solution qualifiée ou certifiée ANSSI (sites sensibles, OIV, OSE...).

En plus du niveau de gamme, plusieurs applications comprises dans le logiciel MICROSESAME sont soumises à l'utilisation d'une **licence spécifique**.

La liste de fonctionnalités soumises à licence est détaillée ci-dessous, avec le nom de la licence à activer. Certaines licences ont un **seuil** d'activation, permettant l'activation d'une quantité définie d'équipements (par exemple, licence pour l'activation de 5 lecteurs, 10 caméras...). Une seule licence peut avoir un impact sur plusieurs applications MICROSESAME. L'activation de plusieurs licences peut être nécessaire, afin de débloquer l'ensemble de fonctionnalités pour une seule application.

Le téléchargement des données doit être réalisée depuis **Appliquer le paramétrage**, suite à des modifications concernant les licences, les seuils ou l'équipement associé à MICROSESAME.

La procédure de **génération, téléchargement et installation des licences** est également détaillée dans les sections suivantes.

La fenêtre **A propos** dans MICROSESAME contient les informations de licence. Pour y accéder depuis le menu principal, cliquer sur le bandeau inférieur indiquant la version de MICROSESAME. Dans la fenêtre **A propos**, aller à l'onglet **Licences**.

3.2. Génération d'un fichier d'identification Serveur (TLOC)

Afin de générer le fichier ".TLOC" qui permettra de réaliser une demande de licence auprès de HIRSCH, effectuer les étapes suivantes :

1. Accéder à la fenêtre "A propos" du menu principal de MICROSESAME à partir du poste SERVEUR :

Faire un double clic sur l'icône **Menu principal de MICROSESAME** présente sur le bureau, puis ouvrir une session en saisissant login et mot de passe.

2. Cliquer sur **MICROSESAME 202x.x** affiché en partie basse du menu principal : la fenêtre "A propos" s'ouvre sur la rubrique "Licences".
3. Cliquer sur le bouton **Générer une demande de licences**.
4. Dans la fenêtre "Paramètres de licence", remplir les informations demandées :
   - Code Affaire : donnée obligatoire, correspond au code référence donné par HIRSCH se trouvant sur le bon de commande.
   - Nom du site (donnée obligatoire).
   - Numéro de clé (optionnel, à remplir seulement dans le cas où cette donnée est connue).
   - Dénomination serveur (optionnel, permet de mettre une description personnalisée si souhaité).
   - Adresse (optionnel).
   - Complément d'adresse (optionnel).
   - Code postal, ville (optionnel).
5. Cliquer sur le bouton **Générer le fichier d'identification machine**.

3.3. Protection des licences : mécanisme de vérification de l'ordinateur

Le fichier de licence est chiffré en fonction des caractéristiques techniques du serveur de destination.

Le mécanisme de protection des clés MICROSESAME, via les fichiers TLOC, teste les éléments suivants :

Règle de contrôle	Nature de la vérification effectuée
N° de série de la carte mère	Si la carte mère a été remplacée, la licence devient invalide.
N° de série des processeurs du serveur	Si tous les processeurs sont remplacés, la licence devient invalide.
N° de série des différents disques durs connectés	Si tous les disque durs de la machine sont remplacés, la licence devient invalide.
Adresses MAC des équipements réseau du serveur	Si toutes les adresses MAC changent, la licence devient invalide.

Le mécanisme de protection vérifie que pour chacun des éléments testés, au moins un des équipements n'a pas été changé.

3.4. Changement du serveur hébergeant MICROSESAME

Afin de protéger les licences (voir section précédente), le numéro de série des processeurs et de la carte mère (identité du serveur) sont liés aux licences obtenues. En cas de changement de serveur, il est donc nécessaire de demander de nouvelles licences auprès du support technique.

3.5. Téléchargement du fichier de licence (TLIC)

3.5.1. e-mail permettant de générer le fichier de licence

Suite à votre commande, un mail vous a été envoyé par HIRSCH (livraison@hirschsecure.fr) fournissant 3 éléments permettant de générer le fichier de licence associé :

- *Le lien vers l'espace web permettant de générer le fichier de licence*.
- Le login associé à votre commande.
- Le mot de passe.

3.5.2. Génération et téléchargement du fichier de licence

1. Se connecter à *l'espace web permettant de générer le fichier de licence*.
2. Ouvrir la page **Espace de téléchargement des licences**.
3. Cliquer sur le "Numéro de clé" associé à votre commande.
4. Charger le fichier d'identification du serveur (TLOC) précédemment généré à partir du poste Serveur MICROSESAME.
5. Télécharger ensuite le fichier de licence (TLIC).

3.6. Installation du fichier de licence (TLIC) sur le serveur MICROSESAME

Afin d'installer le fichier licence :

1. Accéder à la fenêtre "A propos" du menu principal de MICROSESAME à partir du poste SERVEUR :
   Faire un double clic sur l'icône **Menu principal de MICROSESAME** présente sur le bureau, puis ouvrir une session en saisissant login et mot de passe.
2. Cliquer sur **MICROSESAME 20xx.x** affiché dans la partie basse du menu principal : la fenêtre "A propos" s'ouvre sur la rubrique "Licences".
3. Cliquer sur le bouton **Installer un fichier de licences**.
4. Un message d'information apparaît pour signaler que le fichier licence qui va être ajouté va écraser le précédent fichier de licence.
5. Valider la réponse en cliquant sur **OUI**.
6. Sélectionner le fichier licence fournis (fichier de type "*.TLIC") , puis cliquer sur **Ouvrir**.
7. Valider le message d'installation réussi.

Pour la solution de **redondance** SAFEKIT, une licence par serveur est nécessaire.

3.7. Applet permettant de gérer progressivement le passage du niveau de licence de ENTRY à PRIME ou HIGH SECURE

Cette applet est disponible à partir de la version 7.3.0.

Lors du passage du niveau de sécurité ENTRY à un niveau plus élevé, il est presque impossible de remplacer tous les badges simultanément. Pendant la période de

transition, les lecteurs doivent donc pouvoir lire des badges de plusieurs niveaux de sécurité.

Or, avec les badges de type ENTRY, il n'est pas possible de créer des applets pour gérer cette transition. Une nouvelle commande, CCmdPreProcessApplet, a donc été intégrée dans le firmware. Elle peut être appelée dans l'applet ENTRY pour lire les badges ENTRY.

Pour l'utiliser, il est nécessaire d'ouvrir cette applet dans MICROSESAME ou dans l'interface web de la TILLYS, pour :

1. Ajouter la méthode read_entry_badge dans l'applet ENTRY,
2. Préciser le mode de lecture comme argument,
3. Définir un cas d'erreur.

Il est nécessaire de disposer d'un slot de variable. Voir **read_entry_badge** dans *Guide de paramétrage applet pour ML5.x et UTL 6.x*.

3.8. Procédure d'abaissement du niveau de sécurité de licence CUBE

3.8.1. Licences PRIME et ENTRY

L'abaissement du niveau de sécurité entre les licences PRIME et ENTRY ne nécessite pas de procédure avancée.

Pour passer d'une licence PRIME à une licence ENTRY

1. Depuis le menu-principal, cliquer sur l'icône puis choisir **Licences**, l'application se_checkversion.exe se lance automatiquement.
2. Cliquer sur **Installer** et importer le fichier de licence ENTRY; vérifier que MICROSESAME confirme l'installation de la nouvelle licence.
3. Depuis l'application **Appliquer les paramétrages**, effectuer un téléchargement vers les TILLYS pour propager le passage à la licence ENTRY.

Le passage au niveau de sécurité ENTRY implique obligatoirement la désactivation des fonctionnalités d'encodage et d'applets.

Les clés badges seront automatiquement supprimées dans les modules et l'applet sera remplacée par celle **par défaut**.

3.8.2. Licence HIGHSECURE

L'abaissement du niveau de sécurité depuis la licence HIGHSECURE nécessite de suivre une procédure particulière. Le point essentiel étant de désensibiliser tous les éléments de l'installation pour assurer la communication, après le passage au niveau inférieur de sécurité.

1. Vérifier que tous les éléments de l'installation concernés par cette procédure sont bien connectés (modules déportés, lecteurs...).
2. Vérifier que tous les éléments de l'installation **non concernés** par cette procédure sont bien déconnectés (modules déportés, lecteurs...).
3. Lancer l'interface de configuration WEB de la TILLYS dans un navigateur.

4. Dans l'interface WEB de la TILLYS, suivre **Maintenance > Erase keys**.
5. Cliquer sur l'icône Aide et lire la procédure de désensibilisation, puis désensibiliser tous les lecteurs et modules concernés.
6. Remettre la TILLYS en configuration usine (voir le chapitre 53 dans le *Guide de référence de la TILLYS*).
7. Générer le nouveau fichier de licence, comme décrit en *Section 3.5.2, « Génération et téléchargement du fichier de licence »*.
8. Installer ce fichier de licence, comme décrit en *Section 3.6, « Installation du fichier de licence (TLIC) sur le serveur MICROSESAME »*.
9. Télécharger ce nouveau paramétrage dans la TILLYS (voir le chapitre 46 dans le *Guide de référence de la TILLYS*).

3.9. Document récapitulatif de renouvellement des licences (MSL)

A partir de la version 2023.1, MICROSESAME permet de générer un document récapitulant le nombre d'éléments déclarés, par rapport aux licences disponibles et par type d'éléments.

Ce document peut être demandé afin de dimensionner au mieux le renouvellement de licences pour l'installation.

1. Depuis le menu principal, suivre **Maintenance > Autres > A propos**.
2. Cliquer sur le bouton **Licences**.
3. Cliquer sur **Imprimer les informations pour le renouvellement MSL**.

Chapitre 4. Résolution des pannes d'accès à WEBSESAME en configuration déportée sous LINUX

4.1. Affichage du message "le jeton de rafraîchissement est requis" dans WEBSESAME

La variable WS_BACK_PATH manque et le rafraîchissement de session est impossible.

1. Ajouter la ligne SetEnv WS_BACK_PATH "/back/index.php", comme décrit dans la section *Section 2.2.5.2, « Configurer Apache avec les paramètres MICROSESAME, sécuriser la connexion à WEBSESAME et la personnaliser »*.
2. Configurer le ProxyPass dans l'applicatif WEBSESAME (voir *Section 2.2.5.2, « Configurer Apache avec les paramètres MICROSESAME, sécuriser la connexion à WEBSESAME et la personnaliser »*).

4.2. Échec de la connexion à l'automate de temps réel en configuration déportée sous LINUX de WEBSESAME

Erreur de module utilisé pour le proxy websocket (voir *Section 2.2.5.2, « Configurer Apache avec les paramètres MICROSESAME, sécuriser la connexion à WEBSESAME et la personnaliser »*).