

# Guide de la sécurité PSD Mobile V2



## Table des matières

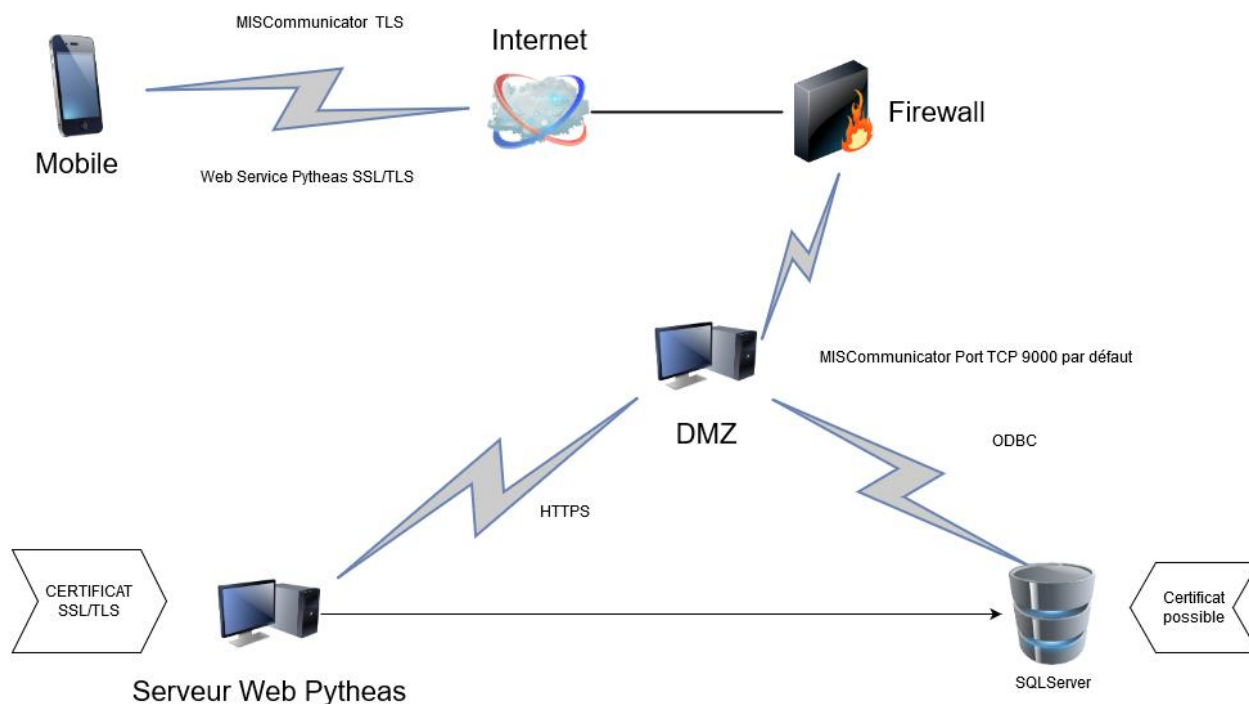
1. Introduction .....	3
2. Fonctionnement.....	3
2.1. Diagramme de communication.....	3
2.2. Description du fonctionnement.....	3
3. Flux de données .....	4
3.1. Accès du Mobile au Service MISCommunicator .....	4
3.2. Sécurité du service MISCommunicator.....	4
3.3. Connexion ODBC entre MISCommunicator et le serveur de base de données.....	5
3.3.1. Configuration ODBC .....	5
3.3.2. Données de sécurités d'accès PSD par MISCommunicator .....	5
3.4. Connexion Webservice -> PYTHEAS Service Desk .....	5
4. Annexes.....	6
4.1. Création d'un profil PYTHEAS Service Desk pour PSD Mobile .....	6
4.2. Droits à positionner.....	7
4.3. Mise en place d'un certificat auto généré pour le MISCommunicator.....	13

## 1. Introduction

Cette documentation décrit les flux et les outils utilisés par PSDMobile V2 pour accéder à PYTHEAS Service Desk.

## 2. Fonctionnement

### 2.1. Diagramme de communication



### 2.2. Description du fonctionnement

L'application PSDMobile V2 est une application écrite avec un outil nommé Kalipso. Cette application est une application native Android disponible sur Google Play.

L'application communique par l'intermédiaire de deux protocoles avec PSD :

- Par l'intermédiaire d'un service Windows nommé MIS Communicator qui utilise un lien direct entre le mobile et le serveur qui héberge ce service, par l'intermédiaire d'un lien TCP sur le port 9000 par défaut.
  - o Ce lien est crypté en TLS avec un certificat à créer à l'aide de MIS Communicator ou un certificat externe ; PSDMobile ne supporte pas pour l'instant un certificat côté client.
  - o Le serveur, où est hébergé le MIS est, dans le cas d'une utilisation à travers Internet, obligatoirement monté sur un serveur accessible directement.
  - o Le service MIS communique avec la base de données PYTHEAS Service Desk à l'aide d'un pilote ODBC 32 bits paramétré sur le serveur qui héberge le service ; les communications à travers ODBC peuvent être cryptées.
- Par l'intermédiaire d'un Web Service dans le cas des modules matériels et interventions, ce web service est hébergé par le module web de PYTHEAS Service Desk.
  - o Les communications à travers le web service peut être crypté en TLS dans le cadre du protocole https.

### 3. Flux de données

#### 3.1. Accès du Mobile au Service MISCommunicator

L'application PSDMobile communique d'abord avec la base de données en passant par un programme appelé MIS Communicator.

MIS Communicator ouvre un port TCP sur la machine cible afin que l'application PSDMobile puisse y accéder. Généralement le port configuré est le 9000 mais il peut être changé.

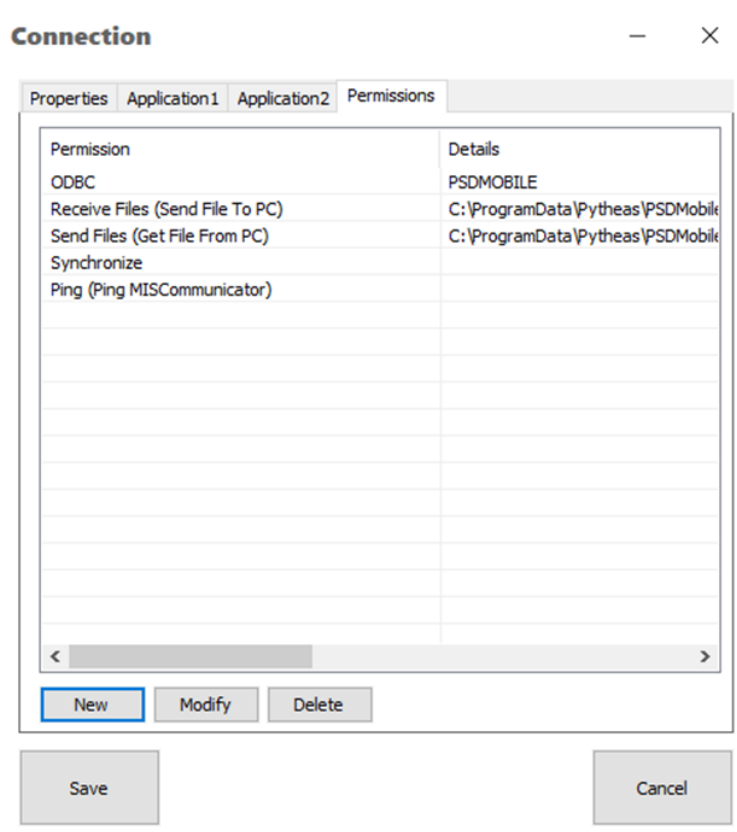
Les liaisons entre les deux points doivent être cryptées, PSDMobile est paramétré pour un cryptage TLS. La création d'un certificat est à la charge de l'administrateur, une procédure simplifiée de création existe dans la documentation PSDMobile V2.

#### 3.2. Sécurité du service MISCommunicator

Le service peut exécuter des opérations très diverses si on lui autorise. Les droits peuvent donc être limités sur la configuration PSDMobile dans MISCommunicator.

Dans l'onglet Permissions de la connexion.

- Synchronize : pour permettre la remontée des photos des interventions dans PSD
- ReceiveFiles sur C:\ProgramData\Pytheas\PSDMobile\MIS\TR0001\ToPC
- SendFiles sur C:\ProgramData\Pytheas\PSDMobile\MIS\TR0001\ToPDA
- ODBC sur la configuration ODBC PSDMOBILE
- Ping sur MISCommunicator



### 3.3. Connexion ODBC entre MISCommunicator et le serveur de base de données

#### 3.3.1. Configuration ODBC

Pour que MIS Communicator puisse dialoguer avec la base de données PYTHEAS Service Desk, il est nécessaire de créer une configuration ODBC sur le serveur qui héberge le MISCommunicator.

Dans le cadre d'une base de données SQL Server, la communication ODBC peut être sécurisée par l'intermédiaire d'un certificat serveur intégré à SQL Server. Il faut toutefois être attentif au fait que cela peut impacter le fonctionnement global de PYTHEAS Service Desk, les communications TLS ne sont pas des plus véloces.

<https://support.microsoft.com/fr-fr/help/3135244/tls-1-2-support-for-microsoft-sql-server>

<https://docs.microsoft.com/fr-fr/sql/database-engine/configure-windows/enable-encrypted-connections-to-the-database-engine?view=sql-server-ver15>

<https://docs.microsoft.com/fr-fr/sql/database-engine/configure-windows/manage-certificates?view=sql-server-ver15>

#### 3.3.2. Données de sécurités d'accès PSD par MISCommunicator

Les informations de communications sont cryptées dans un fichier qui est sauvegardé sur le serveur ou est hébergé le MISCommunicator.

Le fichier est crypté en AES256. Le fichier est renvoyé crypté sur le Mobile afin qu'il puisse donner les instructions d'ouverture de la base de données.

Le compte qui sert à ouvrir la communication doit avoir des droits spécifiques. A cette fin un profil peut être créé dans PYTHEAS Service Desk afin de limiter les droits aux données de PYTHEAS Service Desk.

### 3.4. Connexion Webservice -> PYTHEAS Service Desk

La communication entre le Mobile et PSD passe aussi selon les modules (Intervention et Gestion de parc) par une liaison entre le Mobile et le module Web Service de PSD.

Le Module Web n'est pas obligatoirement installé sur le même serveur que le MISCommunicator.

Le Module Webservice peut être installé sur un autre serveur que le module Web classique de PSD. Dans ce cas-là il faut installer le module Web et le paramétrer correctement puis désactiver le répertoire virtuel dans Internet Information Serveur.

Le module Webservice ne supporte pas de connexion SSO il faut donc que les intervenants utilisant PSDMobile connaissent leur mot de passe, la vérification du mot de passe se fait côté serveur.

Le module Webservice peut être sécurisé par une liaison TLS avec l'aide d'un certificat. L'installation se fait dans IIS de façon standard. La documentation du web Service permet de compléter cette installation.

Le paramétrage dans Pytheas Service Desk permet de définir si le serveur est en http ou en Https. La lecture du paramétrage à partir du MISCommunicator permet de paramétrer la liaison côté Mobile.

## 4. Annexes

### 4.1. Création d'un profil PYTHEAS Service Desk pour PSD Mobile

Nouveau Profil

Créer un nouveau profil

Nom du profil

PSDMOBILE

Profil à dupliquer

Aucun

Type de sécurité

Défaut

Gestion des listes

☐

Gestion des éditions et affichages

☐

Gestion des informations financières

☐

Associé WebUser

☐

Ok

Annuler

Nouvel utilisateur

Créer un nouvel utilisateur

Nom

MOBILESVC

Prénom

Login

MOBILESVC

Langue

français

Mot de passe

xxxx

Confirmation

xxxx

Associé WebUser

☐

Ok

Annuler

Utilisation de ODBC File Creator pour mettre le compte créé, attention ODBC File Creator ne supporte pas TLS il faut arrêter le service, désactiver le TLS, réactiver le service. Créer la connexion ODBC et copier le fichier dans le répertoire TOPDA. Arrêter à nouveau le service et réactiver le TLS.


VERIF

ODBC File Creator

✕

Adresse IP du serveur MIS :

192.168.0.146



Port du serveur MIS :

9000

Nom de la source ODBC :

PSDMOBILE

Login utilisateur :

MOBILESVC

Mot de passe :

\*\*\*

VALIDER

## 4.2. Droits à positionner

Famille	Type d'objet	Visualiser	Lire	Maj	Création	Suppression
Assistance	Contrat d'assistance	-1	0	0	0	0
Assistance	Module Assistance	-1	-1	-1	-1	-1
Assistance	Assistance	-1	0	0	0	0
Assistance	Intervention réalisée	-1	0	0	0	0
Assistance	Dossier	-1	0	0	0	0
Assistance	Contrat	-1	0	0	0	0
Assistance	Demande d'intervention	-1	0	0	0	0
Assistance	Expression de besoin	-1	0	0	0	0
Assistance	Projet	-1	0	0	0	0
Assistance	Tâche	-1	0	0	0	0
Catalogue	Catalogue général	-1	-1	-1	-1	-1
Catalogue	Catalogue local	-1	-1	0	0	0
Catalogue	Article	-1	-1	-1	-1	0
Catalogue	Logiciel catalogué	-1	-1	0	0	0
Catalogue	Question	-1	-1	0	0	0
Catalogue	Questionnaire	-1	-1	0	0	0
Catalogue	Kit de maintenance	-1	-1	0	0	0
Consommable	Module Consommables	-1	-1	-1	-1	-1
Consommable	Consommables	0	0	0	0	0
Consommable	Consommable catalogué	0	0	0	0	0
Consommable	Entrée de consommable	0	0	0	0	0
Consommable	Sortie de consommable	0	0	0	0	0
Consommable	Consommable	0	0	0	0	0
Financier	Module Financier	-1	-1	-1	-1	-1
Financier	Financier	0	0	0	0	0
Financier	Demande d'achat	0	0	0	0	0
Financier	Demande de devis	0	0	0	0	0
Financier	Commande	0	0	0	0	0
Financier	Bon de livraison	0	0	0	0	0
Financier	Facture	0	0	0	0	0
Financier	Contrat de financement	0	0	0	0	0
Financier	Budget	0	0	0	0	0
Financier	Centre de coûts	0	0	0	0	0
Financier	Clé de répartition	0	0	0	0	0
Financier	Marché	0	0	0	0	0
Informatique	Parcs informatiques	-1	-1	-1	-1	-1
Informatique	Parc Informatique	-1	-1	-1	-1	0
Informatique	Composant	-1	-1	-1	-1	0
Informatique	Périphérique	-1	-1	-1	-1	0
Informatique	Logiciel	-1	-1	-1	-1	0
Informatique	Fichier de configuration	-1	-1	-1	-1	0
Informatique	Pc	-1	-1	-1	-1	0

Famille	Type d'objet	Visualiser	Lire	Maj	Création	Suppression
Informatique	Carte	-1	-1	-1	-1	0
Informatique	Imprimante	-1	-1	-1	-1	0
Informatique	Ecran	-1	-1	-1	-1	0
Informatique	Processeur	-1	-1	-1	-1	0
Informatique	Mémoire de masse	-1	-1	-1	-1	0
Informatique	Partition	-1	-1	-1	-1	0
Informatique	CD-Rom	-1	-1	-1	-1	0
Informatique	Unité centrale	-1	-1	-1	-1	0
Informatique	Connexion réseau	-1	-1	-1	-1	0
Informatique	Disque dur	-1	-1	-1	-1	0
Informatique	Lecteur de disquette	-1	-1	-1	-1	0
Informatique	Mac	-1	-1	-1	-1	0
Informatique	Serveur	-1	-1	-1	-1	0
Informatique	Terminal X	-1	-1	-1	-1	0
Informatique	Station de travail	-1	-1	-1	-1	0
Informatique	Hub	-1	-1	-1	-1	0
Informatique	Routeur	-1	-1	-1	-1	0
Informatique	Port	-1	-1	-1	-1	0
Informatique	Commutateur	-1	-1	-1	-1	0
Informatique	Scanner	-1	-1	-1	-1	0
Informatique	Portable	-1	-1	-1	-1	0
Informatique	Terminal	-1	-1	-1	-1	0
Informatique	Station d'accueil	-1	-1	-1	-1	0
Informatique	Ups	-1	-1	-1	-1	0
Informatique	Rack	-1	-1	-1	-1	0
Informatique	Boîtier	-1	-1	-1	-1	0
Informatique	PDA	-1	-1	-1	-1	0
Informatique	Contrat de licence	-1	-1	-1	-1	0
Informatique	Licence	-1	-1	-1	-1	0
Informatique	Application	-1	-1	-1	-1	0
Informatique	Module	-1	-1	-1	-1	0
Informatique	Tablette	-1	-1	-1	-1	0
Informatique	Unité centrale fixe	-1	-1	-1	-1	0
Informatique	Unité centrale portable	-1	-1	-1	-1	0
Informatique	Unité centrale serveur	-1	-1	-1	-1	0
Informatique	Unité centrale mac	-1	-1	-1	-1	0
ITIL	Objets ITIL	-1	-1	-1	-1	-1
ITIL	Service desk	-1	0	0	0	0
ITIL	Base de connaissances	-1	-1	0	0	0
ITIL	Fiche de connaissances	-1	0	0	0	0
ITIL	Incident	-1	-1	0	0	0
ITIL	Modèle d'activité	-1	0	0	0	0
ITIL	Problème	-1	0	0	0	0
ITIL	Erreur connue	-1	0	0	0	0



Famille	Type d'objet	Visualiser	Lire	Maj	Création	Suppression
ITIL	Demande	-1	-1	0	0	0
ITIL	Intervention	-1	-1	-1	0	0
ITIL	Workflow	-1	0	0	0	0
ITIL	Configuration management	-1	0	0	0	0
ITIL	Configuration item	-1	0	0	0	0
ITIL	Service ITIL	-1	0	0	0	0
ITIL	Calendrier de service	-1	-1	0	0	0
ITIL	Contrat de service	-1	0	0	0	0
ITIL	Changement	-1	0	0	0	0
ITIL	KPI	-1	0	0	0	0
ITIL	Délai	-1	0	0	0	0
ITIL	Mise en production	-1	0	0	0	0
ITIL	Convention de service	-1	0	0	0	0
Localisation	Localisation	-1	-1	-1	-1	-1
Localisation	Site	-1	-1	0	0	0
Localisation	Bâtiment	-1	-1	0	0	0
Localisation	Etage	-1	-1	0	0	0
Localisation	Salle	-1	-1	0	0	0
Localisation	Prise	-1	-1	0	0	0
Matériel	Parcs matériels	-1	-1	-1	-1	-1
Matériel	Parc matériel	-1	-1	-1	-1	0
Matériel	Téléphone	-1	-1	-1	-1	0
Matériel	Bureau	-1	-1	-1	-1	0
Matériel	Véhicule	-1	-1	-1	-1	0
Matériel	Photocopieur	-1	-1	-1	-1	0
Matériel	Caisson	-1	-1	-1	-1	0
Matériel	Table	-1	-1	-1	-1	0
Matériel	Chaise	-1	-1	-1	-1	0
Matériel	Armoire	-1	-1	-1	-1	0
Matériel	Meuble appoint	-1	-1	-1	-1	0
Matériel	Etagère	-1	-1	-1	-1	0
Matériel	Cloison	-1	-1	-1	-1	0
Matériel	Porte	-1	-1	-1	-1	0
Matériel	Lampe	-1	-1	-1	-1	0
Matériel	Stores	-1	-1	-1	-1	0
Matériel	Extincteur	-1	-1	-1	-1	0
Matériel	Distributeur alimentaire	-1	-1	-1	-1	0
Matériel	Appareil hygiénique	-1	-1	-1	-1	0
Matériel	Tableau	-1	-1	-1	-1	0
Matériel	Téléviseur	-1	-1	-1	-1	0
Matériel	Magnétoscope	-1	-1	-1	-1	0
Matériel	Caméra	-1	-1	-1	-1	0
Matériel	Projecteur	-1	-1	-1	-1	0
Matériel	Chariot	-1	-1	-1	-1	0

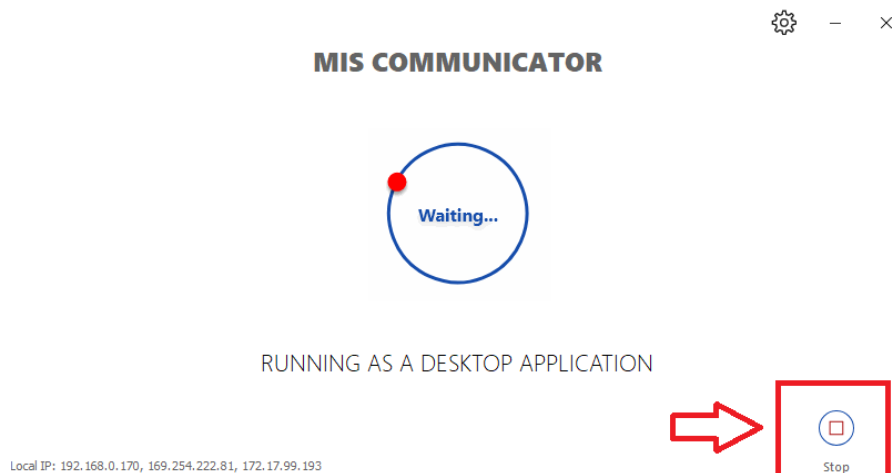
Famille	Type d'objet	Visualiser	Lire	Maj	Création	Suppression
Matériel	Onduleur	-1	-1	-1	-1	0
Matériel	Autocommutateur	-1	-1	-1	-1	0
Matériel	Téléphone portable	-1	-1	-1	-1	0
Matériel	Pager	-1	-1	-1	-1	0
Matériel	Répondeur	-1	-1	-1	-1	0
Matériel	Télécopieur	-1	-1	-1	-1	0
Matériel	Minitel	-1	-1	-1	-1	0
Matériel	Destructeur de papier	-1	-1	-1	-1	0
Matériel	Coffre fort	-1	-1	-1	-1	0
Matériel	Radiateur	-1	-1	-1	-1	0
Matériel	Climatiseur	-1	-1	-1	-1	0
Matériel	Carte magnétique	-1	-1	-1	-1	0
Matériel	Elément	-1	-1	-1	-1	0
Matériel	Rayonnage	-1	-1	-1	-1	0
Matériel	Elément médical	-1	-1	-1	-1	0
Matériel	Lit	-1	-1	-1	-1	0
Matériel	Bio Médical	-1	-1	-1	-1	0
Matériel	Chariot divers	-1	-1	-1	-1	0
Matériel	Chariot de soin	-1	-1	-1	-1	0
Matériel	Chaise Médicale	-1	-1	-1	-1	0
Matériel	Table patient	-1	-1	-1	-1	0
Matériel	Electro-ménager	-1	-1	-1	-1	0
Matériel	Armoire médicale	-1	-1	-1	-1	0
Matériel	Hi Fi	-1	-1	-1	-1	0
Matériel	Nettoyage	-1	-1	-1	-1	0
Matériel	Imprimerie	-1	-1	-1	-1	0
Matériel	Chariot repas	-1	-1	-1	-1	0
Matériel	Table médicale	-1	-1	-1	-1	0
Matériel	Appareil électronique	-1	-1	-1	-1	0
Matériel	Machine	-1	-1	-1	-1	0
Organisation	Organisation	-1	-1	-1	-1	-1
Organisation	Société	-1	-1	0	0	0
Organisation	Département	-1	-1	0	0	0
Organisation	Service	-1	-1	0	0	0
Organisation	Utilisateur	-1	-1	0	0	0
Organisation	Fournisseur	-1	0	0	0	0
Organisation	Profil	-1	-1	-1	-1	-1
Organisation	Contact	-1	0	0	0	0
Organisation	Unité organisationnelle	-1	-1	0	0	0
Pam	Expédition	-1	0	0	0	0
Pam	PAM	-1	0	0	0	0
Pam	Creation	-1	-1	-1	-1	-1
Pam	Historique	-1	-1	-1	-1	-1
Pam	ObjectType	-1	-1	-1	-1	-1

Famille	Type d'objet	Visualiser	Lire	Maj	Création	Suppression
Pam	ObjectProperty	-1	-1	-1	-1	-1
Pam	Object	-1	-1	-1	-1	-1
Pam	ObjectFinancial	-1	-1	-1	-1	-1
Pam	Token	-1	0	0	0	0
Pam	Document	-1	-1	-1	-1	0
Pam	Référence	-1	0	0	0	0
Pam	Typologie	-1	-1	0	0	0
Pam	Planning	-1	0	0	0	0
Pam	Réservation	-1	0	0	0	0
Pam	DocumentHTML	-1	0	0	0	0
Pam	ImagesHTML	-1	0	0	0	0
Pam	Document XML	-1	0	0	0	0
Pam	Objet système	-1	0	0	0	0
Pam	Query	-1	0	0	0	0
Pam	SubQuery	-1	0	0	0	0
Pam	Report	-1	0	0	0	0
Pam	SubReport	-1	0	0	0	0
Pam	Form	-1	0	0	0	0
Pam	Fonctionnalité	-1	0	0	0	0
Pam	Script	-1	0	0	0	0
Pam	View	-1	-1	-1	-1	-1
Pam	Contexte	-1	0	0	0	0
Pam	Action	-1	0	0	0	0
Pam	Format	-1	-1	-1	-1	-1
Pam	Customize	-1	0	0	0	0
Pam	ViewPAM	-1	0	0	0	0
Pam	TransformTemplate	-1	-1	-1	-1	-1
Pam	TransformModel	-1	-1	-1	-1	-1
Pam	Analyse	-1	0	0	0	0
Pam	Panier	-1	0	0	0	0
Pam	Lot	-1	0	0	0	0
Pam	Référence de stock	-1	0	0	0	0
Pam	Référence de stock secondaire	-1	0	0	0	0
Pam	Mouvement de stock	-1	0	0	0	0
Pam	Emplacement de stock	-1	0	0	0	0
Pam	Campagne d'inventaire	-1	-1	-1	-1	0
Pam	Modèle de Workflow	-1	0	0	0	0
Pam	Acteur	-1	0	0	0	0
Pam	Etape	-1	0	0	0	0
Pam	Condition	-1	0	0	0	0
Pam	Plan de maintenance	-1	0	0	0	0
Pam	Lien	-1	0	0	0	0
Pam	Notification	-1	0	0	0	0
Pam	Code script	-1	0	0	0	0

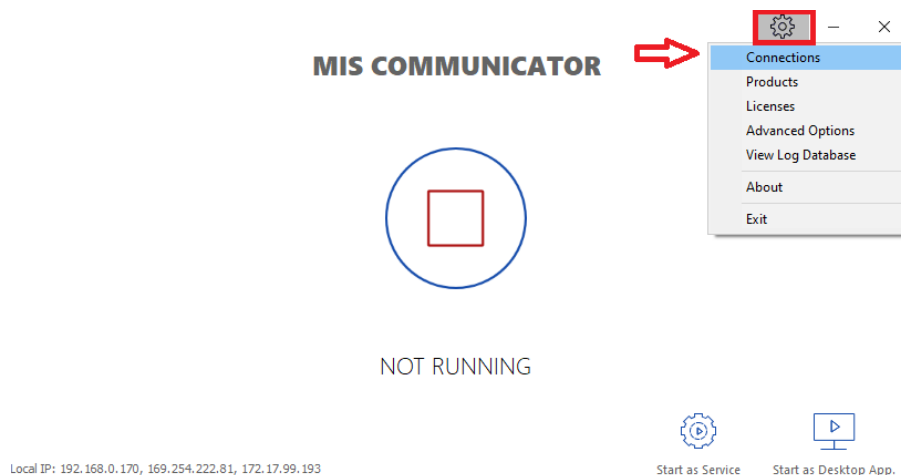
Famille	Type d'objet	Visualiser	Lire	Maj	Création	Suppression
Pam	Validation	-1	0	0	0	0
Pam	Diagram	-1	0	0	0	0
Pam	Message Mail	-1	0	0	0	0
Pam	Modèle mail	-1	0	0	0	0
Pam	Transfert	-1	0	0	0	0
Pam	Noeud analyse	-1	0	0	0	0
Pam	Ressource	-1	0	0	0	0
Pam	Calendrier	-1	-1	0	0	0
Pam	Intervenant	-1	-1	0	0	0

### 4.3. Mise en place d'un certificat auto généré pour le MISCommunicator

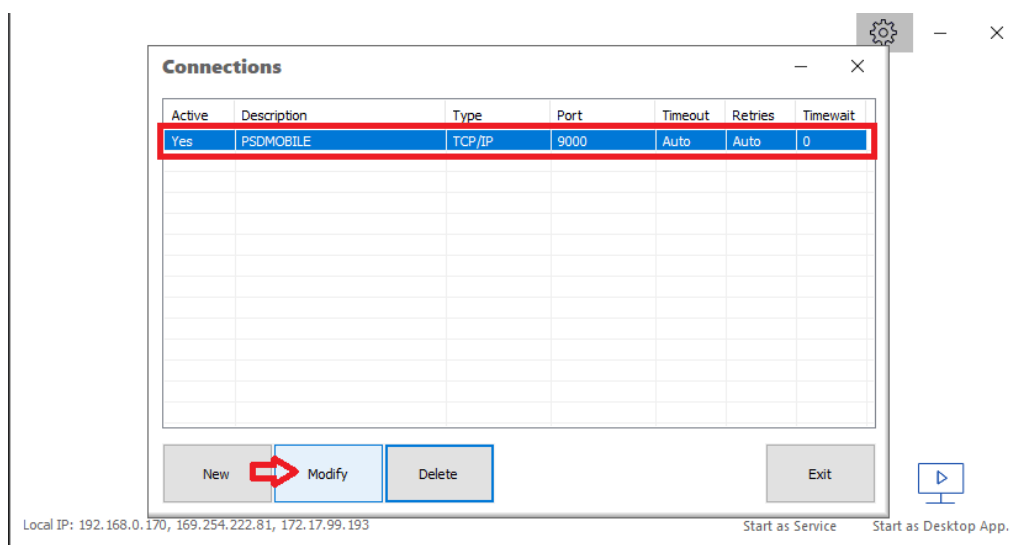
1. Ouvrir le MISInterfaceCommunicator.exe
2. Stopper le MIS s'il fonctionne



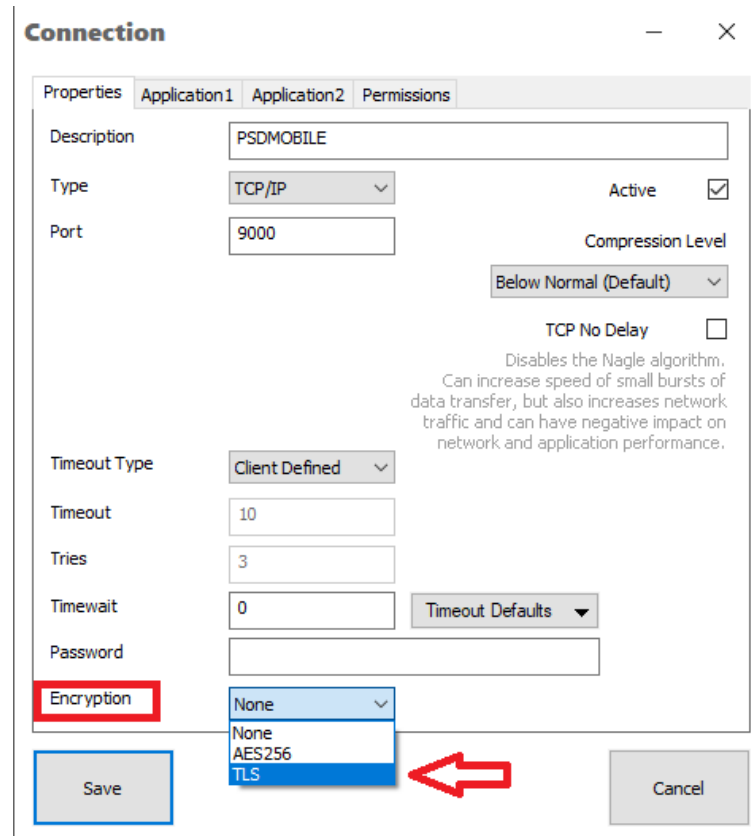
3. Ouvrir l'onglet connexions



4. Choisir la connexion paramétrée précédemment lors de l'installation du MIS :



5. En bas, choisir Encryption > TLS :



**Connection**

Properties Application1 Application2 Permissions

Description PSDMOBILE

Type TCP/IP Active ☒

Port 9000

Compression Level Below Normal (Default)

TCP No Delay ☐

Disables the Nagle algorithm.  
Can increase speed of small bursts of data transfer, but also increases network traffic and can have negative impact on network and application performance.

Timeout Type Client Defined

Timeout 10

Tries 3

Timewait 0 Timeout Defaults

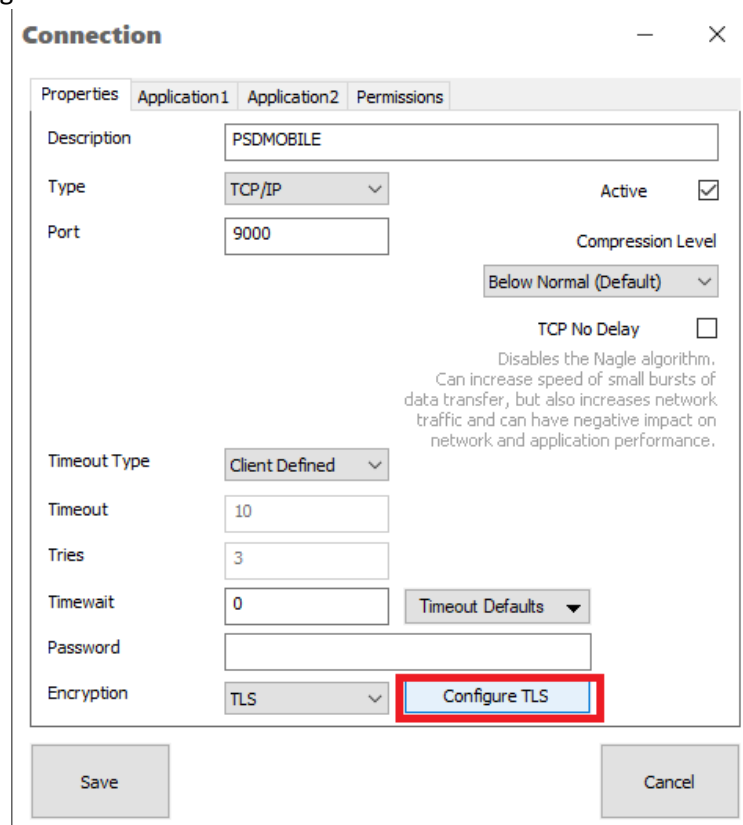
Password

Encryption **None**

None  
AES256  
TLS

Save Cancel

6. Cliquer sur « Configure TLS » :



**Connection**

Properties Application1 Application2 Permissions

Description PSDMOBILE

Type TCP/IP Active ☒

Port 9000

Compression Level Below Normal (Default)

TCP No Delay ☐

Disables the Nagle algorithm.  
Can increase speed of small bursts of data transfer, but also increases network traffic and can have negative impact on network and application performance.

Timeout Type Client Defined

Timeout 10

Tries 3

Timewait 0 Timeout Defaults

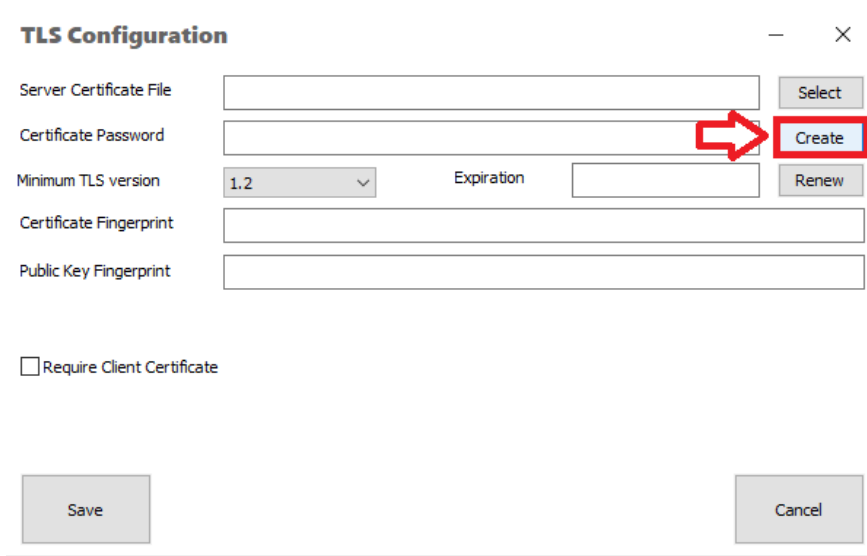
Password

Encryption TLS

**Configure TLS**

Save Cancel

7. Cliquer sur «Create » :



**TLS Configuration**

Server Certificate File

Certificate Password

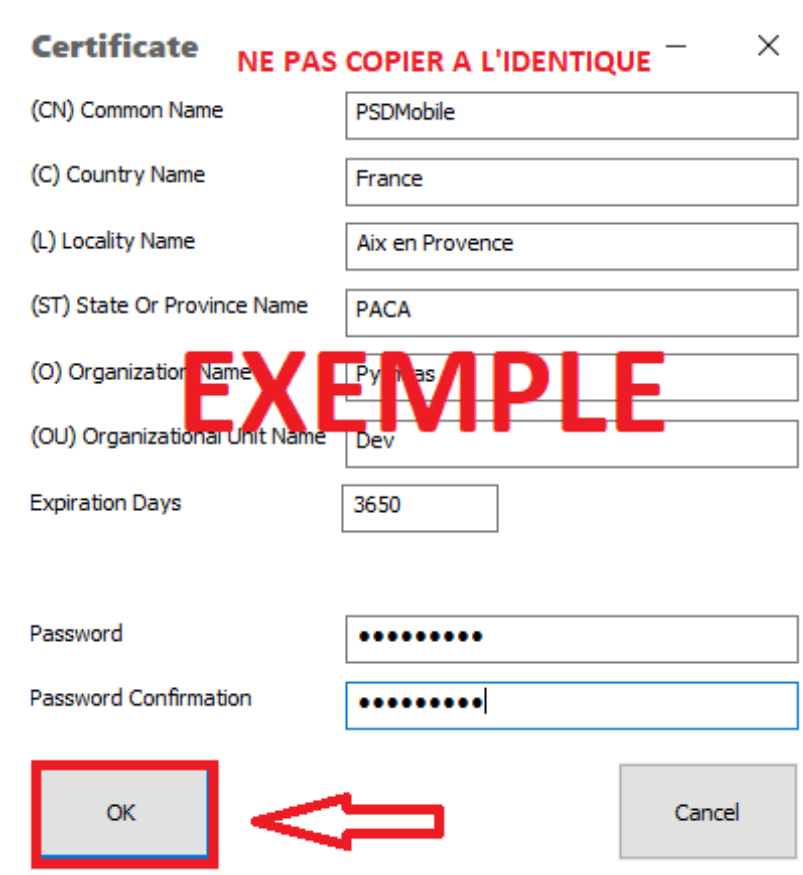
Minimum TLS version  Expiration

Certificate Fingerprint

Public Key Fingerprint

☐ Require Client Certificate

8. Remplir le certificat :



**Certificate** **NE PAS COPIER A L'IDENTIQUE**

(CN) Common Name

(C) Country Name

(L) Locality Name

(ST) State Or Province Name

(O) Organization Name

(OU) Organizational Unit Name

Expiration Days

Password

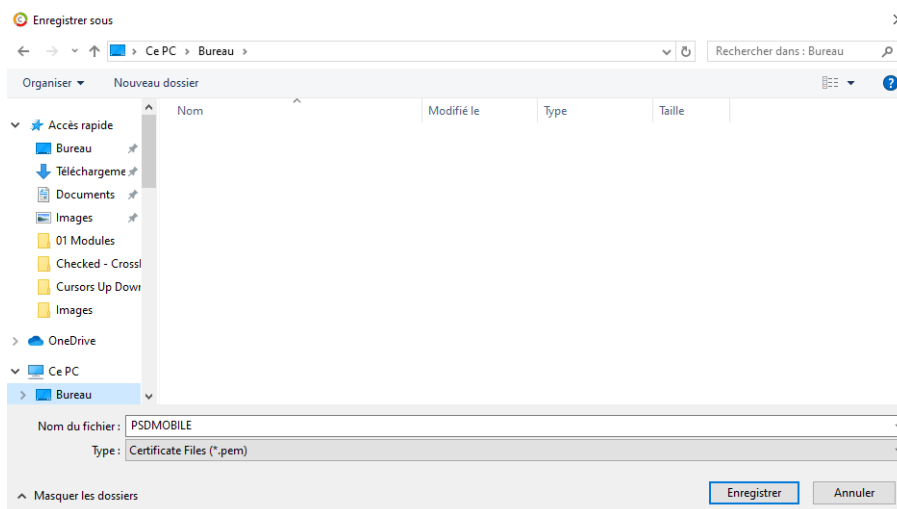
Password Confirmation

**EXEMPLE**

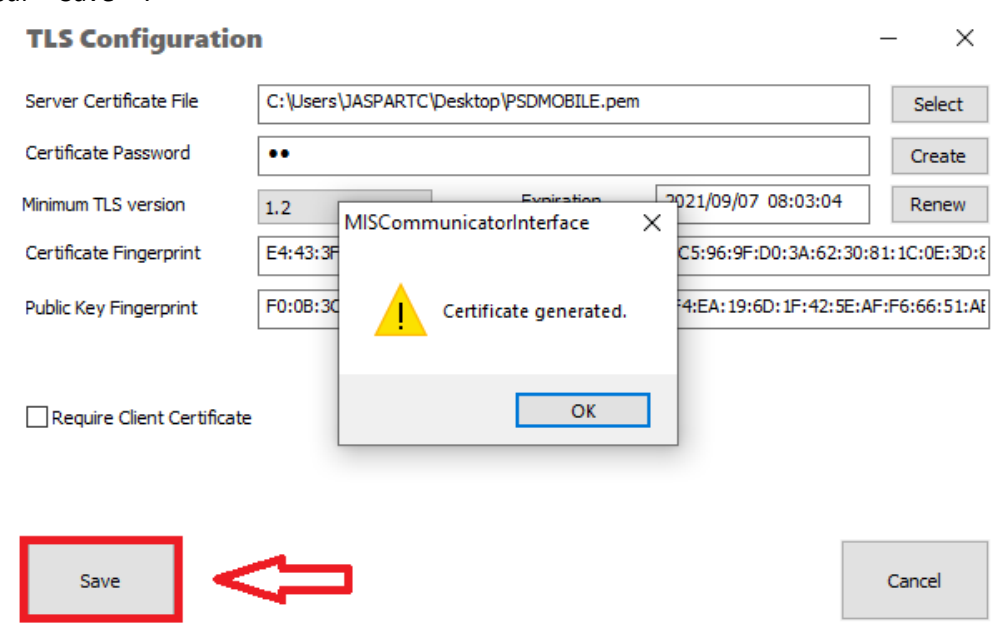
9. Enregistrer le certificat dans le répertoire du MIS, par exemple, dans un nouveau dossier que l'on nommera « Certificat » :

Il faut que ce répertoire soit Public afin de pouvoir être accédé par le service.

Par exemple c:\ProgramData\Pytheas\PSDMobile\Certificat

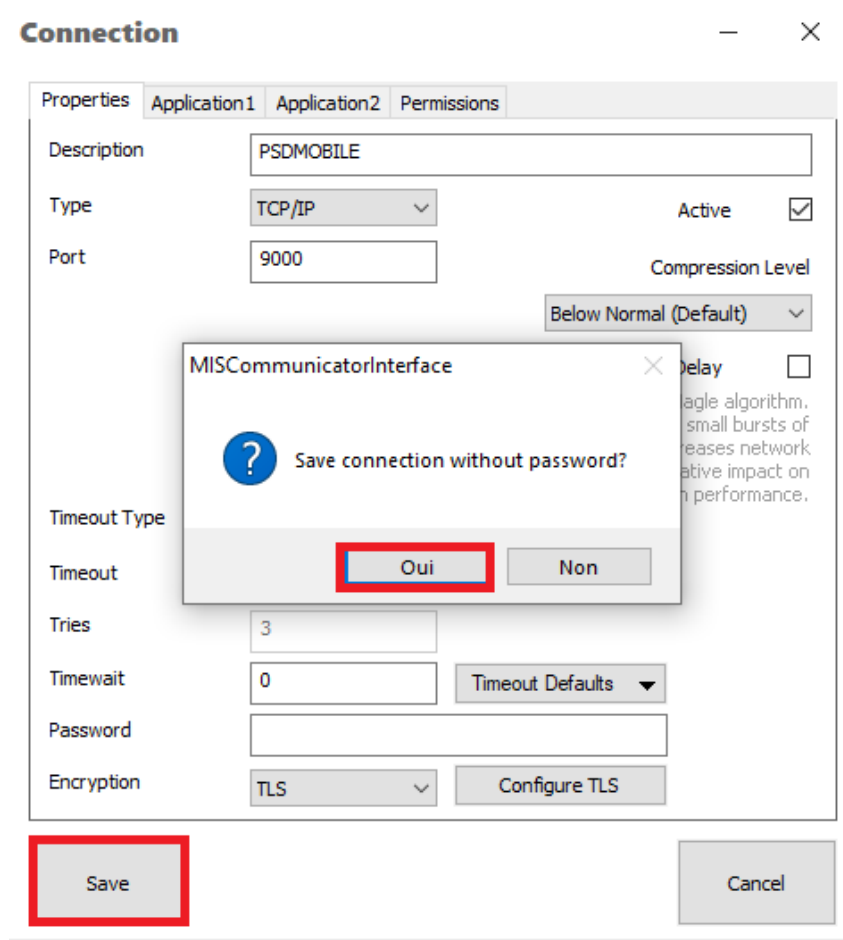


10. Cliquer sur « Save » :





11. Cliquer à nouveau sur « Save » et enregistrer sans mot de passe :



12. La mise en place du TLS est terminée. Vous pouvez redémarrer le MIS.